Pontifícia Universidade Católica de São Paulo

JULIANA ABRUSIO FLORÊNCIO

Proteção de Dados na Cultura do Algoritmo

Doutorado em Direito

São Paulo

2019

Pontifícia Universidade Católica de São Paulo

JULIANA ABRUSIO FLORÊNCIO

Proteção de Dados na Cultura do Algoritmo

Tese apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de DOUTORA em Direito, na subárea Filosofia do Direito, sob a orientação do Professor Doutor Willis Santiago Guerra Filho.

São Paulo

2019

Pontifícia Universidade Católica de São Paulo

JULIANA ABRUSIO FLORÊNCIO

Proteção de Dados na Cultura do Algoritmo

Tese apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de DOUTORA em Direito, na subárea Filosofia do Direito, sob a orientação do Professor Doutor Willis Santiago Guerra Filho.

Aprovada em: ____/____/____.

Banca Examinadora

Professor Doutor Willis Santiago Guerra Filho (Orientador).
Instituição: Pontifícia Universidade Católica de São Paulo
Julgamento _____Assinatura_____

Professor(a) Doutor(a) _____
Instituição: _____
Julgamento: _____
Assinatura: _____

Professor(a) Doutor(a) _____
Instituição: _____
Julgamento: _____
Assinatura: _____

Professor(a) Doutor(a) _____
Instituição: _____
Julgamento: _____
Assinatura: _____

Professor(a) Doutor(a) _____
Instituição: _____
Julgamento: _____
Assinatura: _____

Dedico esta tese

A Deus, o Criador de todas as coisas;

Ao meu marido Marco Aurélio, pelo amor e por ser uma fonte de inspiração;

Ao meus filhos Gabriel e Maria Eduarda, por ressignificarem minha vida.

AGRADECIMENTOS

Depois de seis anos tentando, sem êxito, viver o sonho da maternidade, tomei a decisão de prestar a prova do doutorado. Agradeço ao meu marido, Marco Aurélio Florêncio Filho, e ao meu orientador, Willis Santiago Guerra Filho, pelo caloroso incentivo e imenso apoio que me dirigiram nesse momento. Sem eles, eu não teria me encorajado a trilhar esse caminho.

Durante o curso do doutorado, por obra divina, tive a felicidade de ter dois filhos maravilhosos, Gabriel e Maria Eduarda. Agradeço a esses dois pequenos seres que, apesar do tempo tomado com seus cuidados – o que me foi sempre gratificante – encheram-me de alegria, regozijo e amor, fazendo a diferença para que eu caminhasse adiante, superando as dificuldades e pesares que apareceram no meio do caminho. Um dia, meus filhos entenderão quão importantes foram nesse momento de minha vida.

Para conseguir me dedicar à pesquisa e à elaboração da tese, tive a felicidade e o privilégio de contar com uma pessoa que não mediu esforços para sempre me ajudar: minha mãe, Maria Ines, é a prova de que o amor materno é o único que pode ser comparado ao amor divino. Agradeço, ainda, ao meu pai, Ricardo, que sempre esteve disposto a me ajudar, opinar e contribuir com o texto. Ele foi essencial em me transmitir calma, serenidade, fé e ânimo, ao longo do percurso.

Agradeço, de forma muito especial, ao meu orientador Willis, por ter sido meu porto seguro nos momentos de insegurança; por ter sido um antídoto à minha ansiedade; por ter sido um verdadeiro amigo e orientador, que sempre acreditou que seria possível, dando-me as condições necessárias para que a tese se desenvolvesse.

Agradeço aos colegas e amigos que me subsidiaram com textos e ideias: primeiramente ao meu orientador, que, dentre outras indicações, em especial, compartilhou sua tese de doutorado em Comunicação e Semiótica, cujo texto abriu minha mente e me ajudou a formular ideias que não as teria sem essa leitura. Agradeço também à Maitê Fabbri Moro e ao Thiago Matsushita, pelas orientações e conselhos. Além disso, agradeço ao meu marido, Marco Aurélio Florêncio Filho, que, a todo momento, direcionava-me textos e obras, além de palavras de ânimo e incentivo, na incansável vontade

de sempre me ajudar. Ainda, agradeço, com carinho, ao Henrique Garbellini Carnio, o qual, num momento de crise, ajudou-me a seguir em frente. Por fim, agradeço as indicações de André Brandão, Alexandre Pacheco, Juliano Maranhão e Nuria Lopez. Todas elas foram muito úteis e fizeram a diferença.

Agradeço às minhas amigas do coração, que sempre me incentivaram e apoiaram. A vida com amigos fica muito mais leve e prazerosa.

Agradeço ao meu diretor mackenzista Felipe Chiarello que me ajudou proporcionando que eu fizesse uma pausa nas aulas da graduação.

Ainda, reconheço a ajuda de colegas de trabalho do escritório (equipes jurídica e administrativa), especialmente nos momentos mais alucinantes da advocacia. Aos que me ajudaram e apoiaram, minha gratidão.

Por fim, porém o mais importante, agradeço a Deus, criador e mantenedor da vida, por Seu sublime amor, por Seu cuidado e por Sua infinita misericórdia. Durante os obstáculos e crises ao longo desse percurso, foi em Deus que encontrei as respostas e o conforto para seguir em frente. Foi nEle que busquei e achei abrigo e entendimento. A Ele seja toda glória, toda honra e todo louvor.

RESUMO

A presente tese investiga as transformações trazidas pelo paradigma informacional inserido na atualidade, e que levaram ao deslocamento da sociedade pós-industrial para a sociedade da informação. Analisa-se seus principais fenômenos, como a massificação dos dados (*big data*)*;* a conectividade onipresente e a datificação advinda da 'internet das coisas'; bem como a cultura do algoritmo, apoiada nas tecnologias do aprendizado de máquina (*machine learning*) e na inteligência artificial. Verifica-se como o mercado de atenção, mediante a incessante produção de dados pessoais, consiste na nova engrenagem da economia de dados. Uma vez sendo os dados pessoais o insumo desse mercado, a pesquisa volta-se a analisar a privacidade, desde os seus primórdios, até à sua feição de proteção de dados, pautada pela doutrina da autodeterminação informativa. Percorre-se, ademais, a evolução normativa que culminou em regulações na Europa, no Brasil, e com mais brevidade, nos Estados Unidos. Ainda, a pesquisa aprofunda o olhar para aspectos específicos advindos da cultura do algoritmo, tais como: a centralização de controle de atos da vida dos indivíduos; as questões de valores éticos; as associações discriminatórias; e a desigualdade de oportunidades. Ainda, volta-se ao caráter 'black box' e à opacidade dos algoritmos, analisando os principais desafios para o cumprimento do princípio da transparência, bem como do direito à explicação, quanto aos sistemas de inteligência artificial responsáveis pela definição de perfis (*profiling)* e pela tomada de decisões automatizadas, como meios de garantir a proteção de dados pessoais. Examina-se como construções jurídicas atuais, tal qual o consentimento e a anonimização de dados, são ineficientes. Por fim, analisa-se como as formas de regulação de arquitetura de *design*, incluindo o princípio da inteligência artificial explicável, podem contribuir para a proteção de dados pessoais na cultura do algoritmo.

Palavras-chave: Sociedade da informação. Privacidade. Proteção de dados. *Big data*; Algoritmos. *Machine learning.* Inteligência artificial.

ABSTRACT

This thesis investigates the transformations brought by the information paradigm inserted in the present time, which have led to the displacement of postindustrial society to information society. It analyzes its main phenomena, such as big data; the omnipresent connectivity and the datification of the 'internet of things'; as well as the algorithm culture, backed on machine learning and artificial intelligence technologies. It is also verified how the market of attention, through the incessant production of personal data, is the new gear of data economy, and once the personal data is the input of this market, the research aims at analyzing the privacy, from its beginning to its feature of data protection, guided by the doctrine of informational self-determination. Furthermore, the normative evolution that culminated in regulations in Europe, Brazil, and briefness, in the United States is examined. Further, the research deepens the study to specific aspects arising from the culture of the algorithm, such as: the centralization of control of acts of individuals' lives; matters of ethical values in the use of the algorithmic machine; discriminatory associations in algorithm calculations; and the inequality of opportunities imposed by the algorithms. Also, it turns to the 'black box' character and the opacity of the algorithms, analyzing the main challenges to comply with the principle of transparency, as well as the right to explanation, regarding the artificial intelligence systems responsible for profiling definition and by automated decision making, as a way to guarantee the protection of personal data. It is examined how current legal constructions, such as data consent and rendered anonymous, are inefficient. Finally, it is analyzed how the ways of regulating design architecture, including the principle of explainable artificial intelligence, can contribute to the protection of personal data in the algorithm culture.

Keywords: Information Society; Privacy, Data Protection; Big data; Algorithms, Machine Learning; Artificial intelligence

SUMÁRIO

	INTRODUÇÃO	11
1	PARADIGMA INFORMACIONAL NA SOCIEDADE CONTEMPORÂNEA	17
1.1	Sociedades da informação, pós-industrial ou pós-moderna: definição do(s) ponto(s) de partida	17
1.2	Dos computadores às redes sociais	30
1.3	A sociedade do *hiper*	38
1.4	Desconfiguração da ditadura do coração e o panóptico digital	45
1.5	*Data is the new oil*	50
2	AS TECNOLOGIAS DA SOCIEDADE DE DADOS E O DESAFIO DE SUA REGULAÇÃO	59
2.1	Dilema de causalidade: dados e tecnologia	59
2.2	A massificação de dados e o *big data*	63
2.3	Internet das coisas: a conectividade onipresente e a datificação da vida	76
2.4	Entropia dos algoritmos e aprendizagem de máquina	83
2.5	Inteligência, consciência e a fusão homem-máquina	95
2.6	O direito na era da sociedade da informação e na sociedade de dados	107
3	DA PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO	118
3.1	A reinvenção da privacidade: do ‘direito de estar só’ ao ‘controle dos dados pessoais’	118
3.2	A proteção de dados e as vulnerabilidades trazidas pelas novas tecnologias	134
3.3	Autodeterminação informativa	145
3.4	Direito fundamental à garantia da confidencialidade e integridade dos sistemas técnico-informacionais	155
3.5	Das dimensões da proteção de dados pessoais	159
3.6	O caminho percorrido em âmbito da proteção de dados pessoais no continente europeu nas primeiras décadas do século XXI	165
3.7	Regulamento Geral de Proteção de Dados (GDPR)	171
3.8	Análise comparativa da tutela da proteção de dados pessoais nos Estados Unidos da América	184
3.9	Sistema de proteção de dados pessoais no direito brasileiro	197
4	CULTURA DO ALGORITMO	210
4.1	Novas formas de controle	210
4.2	Ética algorítmica	216
4.3	Opacidade dos algoritmos	223
4.4	A proteção de dados e a inteligência artificial	233
4.5	Decisões automatizadas sobre indivíduos e a prática de *profiling*	236
4.6	Inteligência artificial e o direito à explicação	244
4.7	A (in)eficiência do consentimento	262
4.8	A contribuição da tecnologia na regulação de proteção de dados	277

4.9 Princípio da inteligência artificial explicável 285

CONCLUSÃO 290

REFERÊNCIAS 293

INTRODUÇÃO

Uma tese consiste na resposta que o pesquisador pretende dar ao problema colocado, objeto da investigação. Daí a necessidade de se delimitar o objeto e problematizá-lo, visando balizar o desenrolar da pesquisa. A presente tese, nesse sentido, tem por objeto de investigação a privacidade, fruto de uma concepção da modernidade, compreendida, prioritariamente, como o direito negativo de ser deixado em paz, mas que, na travessia do século XX, assume um significado dinâmico, referente ao controle de dados pessoais do próprio indivíduo. Essa transformação do instituto em comento ocorreu em razão da evolução tecnológica da informação, em cujo bojo surgiram as ameaças do Estado, e também das empresas privadas, contra os cidadãos, ocorridas a partir da segunda metade do século passado, pautadas pela distopia *orwelliana*.

A referida evolução tecnológica proporcionou o aumento do acesso a informações pessoais, como também a maior capacidade de armazenar e processar dados, fazendo com que os debates sobre o assunto tomassem as seguintes direções: i) os problemas individuais específicos da privacidade tornam-se conflitos que afetam a todos; ii) a concepção de esfera pública não se apresenta como antes, porquanto a sociedade de rede transpassou, em grande parte, a sociedade de organizações, quando a produção de informação era mais centralizada nos meios de comunicação, diluindo-se, portanto, a oposição clássica entre as esferas pública e privada; iii) a dinâmica das novas tecnologias, ligadas à inteligência artificial e *machine learning*, possível graças aos fenômenos da datificação e da massificação de dados, aptas a construir o palco social, político e econômico da cultura do algoritmo, passam a desafiar a atual estrutura de regulação jurídica.

A pergunta, portanto, que norteia a investigação é: como proteger os dados pessoais do indivíduo em uma sociedade imersa na cultura do algoritmo?

A presente pesquisa se justifica em razão da grande importância assumida pela privacidade diante da incessante captura e tratamento de dados pessoais, com fins econômicos e de controle. A maioria dos teóricos, atualmente, classifica a privacidade como um dos temas mais relevantes a serem enfrentados pelas ciências sociais, a exemplo de Luciano Floridi que, em sua obra “4th Revolution: how the

infosphere is reshaping human reality", menciona: "the ethical problem of privacy has become one of the defining issues of our hyperhistorical time" (p.102).

O método utilizado para a elaboração da presente tese foi o hipotético-dedutivo, comum às pesquisas jurídicas, posto que parte do âmbito geral para chegar à regra, perseguindo, outrossim, averiguar teses e antíteses, com o fito de atribuir alto grau de credibilidade à pesquisa.

Percorridas as considerações iniciais de caráter metodológico, adentramos ao desenvolvimento linear da presente tese.

No primeiro capítulo, analisamos como o paradigma informacional inserido nas teorias sociais contemporâneas, como consequência da mundialização e da aceleração da sociedade, provocou o deslocamento para uma nova era – imediatamente posterior à última fase da modernidade (sociedade pós-industrial) – denominada sociedade da informação.

Diante dessa nova ordem social, constatamos como a rápida evolução das tecnologias da informação alterou a geometria e a dinâmica das relações sociais, tais quais: a diversidade de culturas, a construção de uma chamada inteligência coletiva de rede e uma nova topologia da violência do indivíduo para si mesmo.

A partir daqui, destacamos como o desenvolvimento social informacional pode ser nocivo, diante de um contexto imediatista e menos interpessoal, cujo panorama desafia o bem-estar do homem contemporâneo. Constatamos que estamos diante de uma sociedade mais superficial, exibicionista e fugaz, pautada pelo oráculo Google e exposto ao confessionário Facebook, cujas empresas do gênero adotam cada vez mais formas panópticas.

Verificamos, ainda, como o atual cenário da desconfiguração da ditadura do coração, instaurada por Rousseau, acarreta maior cansaço, a seres tidos como zumbis, elevando os casos de doenças neurais, como a depressão e a síndrome de *burnout*, delineando a nova paisagem patológica do início do século XXI. Isso porque a mesma tecnologia que liberta parece aprisionar o próprio homem, explorado de si mesmo, e cerrado em algemas não mais da disciplina, mas do desempenho e do poder ilimitado, de que tudo pode (sempre), numa sociedade da positividade, com pessoas alienadas, embora antenadas, as quais atuam igualmente, no consumo e na produção de informações ditadas por sistemas inteligentes. É o que menciona Stefano Rodotà ao referir-se à "esquizofrenia tecnológica" em seus escritos.

Analisamos como essa paisagem foi propícia a criar uma sociedade de dados, esta produto da própria sociedade da informação, tida como uma das consequências mais claramente visíveis da informatização, e da dinâmica social de excesso de estímulos e impulsos. Passamos, então, a investigar o motivo dos dados pessoais terem alcançado tanto valor econômico, fazendo com que uma empresa tal qual o Facebook valha sete vezes mais que a Petrobras – o Facebook vale atualmente cerca de 400 bilhões de dólares. A Petrobras, mesmo sendo a segunda empresa mais valiosa listada na BOVESPA, vale sete vezes menos, na marca dos 300 bilhões de reais (cálculo comparativo considerado sobre informações de mercado de outubro de 2018).

No segundo capítulo, apresentamos as principais tecnologias da informação que integram esse ecossistema, como o *behavioral targeting* e as técnicas ligadas a *trackings*, dentre outras.

Investigamos, ainda, como os dados pessoais assumem uma nova dimensão com a consagração do *big data*, e como esse fenômeno de massificação, ancorado no *data mining,* alterou a natureza dos negócios, dos mercados e da sociedade, e ainda, como pode implicar, na esfera jurídica, numa ameaça à privacidade, especialmente pela característica da possibilidade de associação e inferência de dados, gerando padrões quanto aos perfis dos indivíduos.

Em seguida, dirigimos o olhar da pesquisa para a Internet das Coisas, a qual consagra o feito da datificação da vida, contribuindo para correlações e cruzamentos de dados, uma vez que consiste na conectividade entre vários dispositivos utilizados no cotidiano do homem. Questiona-se a possibilidade de (des)controle nesse cenário, em especial no que toca à proteção de dados pessoais.

Ainda no segundo capítulo, passamos a uma exposição histórica e conceitual sobre os algoritmos e quanto à aprendizagem de máquina, destacando como essas tecnologias podem identificar padrões de comportamento, para construir e refinar modelos matemáticos de dados que podem ser usados para fazer previsões e tomar decisões automatizadas.

Voltamo-nos, então, à tecnologia do *machine learning*, dotada do atributo de autotransformação, e cuja condição abre espaço a questionar se os algoritmos seriam sistemas autopoiéticos, uma vez que dependem de *inputs* e *outputs* para se reproduzir. Não é possível saber exatamente quais os efeitos decorrentes das ações

que sofrem, porquanto a máquina pode aprender consigo mesma, na medida do grau de entropia de seu sistema.

Debruçamo-nos, então, sobre o homem pós orgânico, que deixou para trás a separação entre a *phsis* e a *technè,* criando novas formas de acoplamentos estruturais, envolvendo homens e máquinas, no quadrante da inteligência artificial. Para tanto, apresentamos os principais marcos temporais do assunto, de Alan Turing aos dias atuais.

A partir daqui, analisamos a nova cibernética e como o direito na era da sociedade informacional e na sociedade de dados é (in)capaz de regular a proteção de dados pessoais diante das tecnologias e fenômenos expostos. Verificamos a existência dos caminhos da regulação tradicional, da autorregulação, da autorregulação regulada, e da regulação pela arquitetura da rede. Isso exposto, adentramos à análise histórica e dogmática da privacidade e da proteção de dados, para maior compreensão do melhor caminho a ser trilhado na resolução de conflitos envolvendo a proteção de dados e os algoritmos.

Assim, no terceiro capítulo investigamos a origem, a evolução e a reinvenção da privacidade, cujo processo deságua no conceito de controle que o indivíduo deve ter sobre seus dados pessoais, consagrado pelas doutrinas da autodeterminação informativa e da liberdade informática, como se cada qual fosse um lado de uma mesma moeda: privacidade e proteção de dados pessoais.

Em seguida, apresentamos as principais vulnerabilidades à proteção de dados, inseridas no atual cenário social, especialmente no que toca à atuação das gigantes da Internet, as quais, pela aplicação de suas invenções, acabam comprometendo os direitos fundamentais da pessoa humana.

Na sequência, analisamos as dimensões percorridas pelo instituto jurídico, desde a promulgação da *Datenshutz*, em 1970, pelo Estado Alemão de Hasse, e da célebre decisão, de 1983, do Tribunal Constitucional Federal alemão, *Volkszahlungsurteil*, até os atuais regulamentos sobre a matéria, acossados pela realidade do *big data* e da inteligência artificial. Nesse sentido, fazemos uma exposição dogmática dos regimes jurídicos da Europa e do Brasil, com breve olhar aos Estados Unidos da América, com fins comparativos de seus sistemas.

Analisamos, nesse interregno, o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais, proclamado, em 2008, no âmbito de uma reclamação constitucional, ajuizada contra dispositivos

da lei do Estado alemão de Nordrhein-Westfalen, que regulamentava a busca e a investigação remota de computadores de pessoas suspeitas de cometer ilícitos criminais.

Finalmente, o quarto capítulo verticaliza a investigação no tocante à problematização afeita à cultura do algoritmo. Para tanto, averiguamos o surgimento de novas formas de centralização de controle, que acabam por ditar a dinâmica dos indivíduos em muitos setores de suas vidas, sob a influência da capacidade de persuasão dos processos algorítmicos. Verificamos, assim, como a identidade do indivíduo, atualmente, tem sido percebida por construções e padrões digitais, de modo que se pode afirmar que os algoritmos acabam integrando a percepção da construção da própria identidade. Examinamos como essa condição representa uma mudança na premissa sobre o que significa governar a si mesmo e ser governado por outros, para mobilizar o poder político e influenciar percepções, escolhas e comportamentos de pessoas.

Voltamo-nos, na sequência, aos debates sobre a ética algorítmica, com especial ênfase à nova ética digital estar baseada no direito fundamental à privacidade e à proteção de dados pessoais, no uso da inteligência artificial, visando combinar o uso de máquinas com os valores éticos e morais do ser humano. Ademais, analisamos como as novas possibilidades de discriminações algorítmicas representam uma ameaça à igualdade de oportunidades. Isso porque os algoritmos não estão isentos de apresentarem um viés (*bias*) injusto ou equivocado, de modo que não podem ser tidos como neutros, como alguns querem fazer crer, para a definição de perfis e tomada de decisões automatizadas.

Em decorrência, examinamos as principais implicações de privacidade vinculadas à inteligência artificial como resultado de sua capacidade de inferir dados, com o consequente reconhecimento de padrões, extraindo o perfil mais íntimo possível do indivíduo, sendo possível, inclusive gerar informações sensíveis a partir de dados não sensíveis.

O progresso do assunto nos leva a investigar o caráter '*black box*' dos algoritmos, cuja expressão relaciona-se ao grau com que os elementos que compõem determinado algoritmo podem ser compreendidos. Verificamos como a opacidade está no centro das novas preocupações sobre algoritmos, tanto entre estudiosos de direito como entre cientistas sociais, podendo ser classificado como

um problema social, haja vista que diversos mecanismos de classificação social dependem, frequentemente, de cálculos algoritmos.

Investigamos, ainda, os atuais desafios quanto à possível incompatibilidade de transparência e auditoria dos algoritmos frente à propriedade intelectual que está por trás dos sistemas de algoritmos, e, ainda, como a complexidade dos algoritmos pode servir de justificativa para que não sejam fornecidas informações aos titulares de dados. Analisamos, em seguida, no que consiste o direito à explicação, presente nas principais regulações de proteção de dados existentes.

Além disso, voltamo-nos a estampar como tradicionais remédios legais, tal qual o consentimento e a minimização de dados, consistem em mecanismos muito limitados, porquanto, ineficientes, para garantir ao titular a proteção de seus dados pessoais. Assim, a linha argumentativa abre espaço a nos debruçarmos ao estudo de como a própria tecnologia pode contribuir na regulação da matéria. Portanto, investigamos o caminho das *Privacy Enhancing Technologies* – PETs, aprofundando os pilares e os desdobramentos dos conceitos de *privacy by design* e *privacy by default.*

Por fim, e em decorrência da análise anterior, investigamos no que consiste o princípio da inteligência artificial explicável (*Explainable Artificial Inteligence – XAI*), e a importância de aplicá-lo às técnicas de *machine learning*, a fim de que os usuários humanos compreendam, confiem adequadamente e gerenciem com eficácia a geração emergente de parceiros artificialmente inteligentes.

1 PARADIGMA INFORMACIONAL NA SOCIEDADE CONTEMPORÂNEA

> Não é difícil ver como nossa era seja de gestação e transferência para uma nova era; o espírito quebrou as pontes com o mundo do ser e de sua representação, que durou até hoje; está prestes a deixar tudo isso no passado e entrar em um período conturbado de transformação.
> **Georg Wilhelm Friedrich Hegel (1770 – 1831)**

1.1 Sociedades da informação, pós-industrial ou pós-moderna: definição do(s) ponto(s) de partida

Há alguns anos existe um intenso debate sobre em qual momento histórico a sociedade se encontra. Desde o final do século XX, muitos argumentam que estamos no "limiar de uma nova era, a qual as ciências sociais devem responder e que está nos levando para além da própria modernidade"[1], por isso as expressões sociedades pós-industrial, pós-moderna e informacional.

O deslocamento do sistema baseado na manufatura de bens materiais para sistemas de produção centralizados na informação trouxe preocupação e discussão envolvendo a definição da era social na qual vivemos.

A sociedade pós-industrial, conforme análise de Willis Santiago Guerra Filho, implica no surgimento de uma sociedade na qual se desenvolve um quarto setor, visto que é baseada essencialmente na circulação e na troca de informação:

> By "post-industrial society" is not meant, for instance, the original concept proposed by D. Bell (1977), as a society in a development stage where the service sector of the economy is prevalent. What is envisioned here is the emergence of societies where a new, "fourth" sector is developed, since those societies rely basically on the circulation and exchange of information – and that in an increasingly intense and sophisticated way.[2]

Ao comparar a era da informação e a sociedade industrial, o sociólogo Yoneji Masuda[3] ressalvou, já na década de 1980, que a configuração final da futura

---

[1] GIDDENS, Anthony. **As conseqüências da modernidade**. Tradução de Raul Fiker. São Paulo: Unesp, 1991, p.11.

[2] GUERRA FILHO, Willis Santiago. **Immunological theory of law**. Alemanha, Saarbrücken: Lambert Academic Publishing, 2014, p.3. Tradução livre: "Por 'sociedade pós-industrial' não se entende, por exemplo, o conceito original proposto por D. Bell (1977), como sendo uma sociedade em fase de desenvolvimento na qual prevalece o setor de serviços de economia. O que se vê aqui é o surgimento de sociedades nas quais se desenvolve um novo 'quarto' setor, visto que essas sociedades se apoiam basicamente na circulação e troca de informações – e isto se dá de forma cada vez mais intensa e sofisticada".

[3] MASUDA, Yoneji. **A sociedade da informação como sociedade pós-industrial**. Tradução do inglês de Kival Charles Weber e Angela Melim. Rio de Janeiro: Rio, 1982, p.46.

sociedade da informação dependeria da confirmação de suas previsões ao longo do tempo. Assim, expôs que enquanto a tecnologia inovadora da sociedade industrial consistia na máquina a vapor (energia), cuja principal função era substituir e amplificar o trabalho físico do homem, a tecnologia inovadora vinculada à sociedade da informação consistiria no computador (memória e processamento de dados) e sua principal função seria substituir e amplificar o trabalho mental do homem, possibilitando a produção automatizada em massa de informação, tecnologia e conhecimento cognitivos. Ainda, na sociedade da informação, a unidade produtora de informação, formada por banco de dados e redes de informação, substituiu a fábrica como símbolo social e tornou-se o centro de produção e de distribuição de bens informacionais.

Para Tercio Sampaio Ferraz Junior, a terceira revolução industrial é a que implica a substituição das máquinas por aparelhos eletrônicos, cada vez mais miniaturizados em unidades de convergência tecnológica. Para ele, disso acarreta uma mudança da topologia do mundo ambiente, pois os espaços da fabricação começam a perder importância:

> Em seu lugar aparece uma nova relação homem-mundo, ou seja, a relação homem-aparelho eletrônico, em que, de um lado, a relação de dependência é reversível: o homem carrega seu aparelho onde quer que esteja; de outro, ele só age conforme a capacidade do seu aparelho. Nessa reversibilidade, sua atividade depende da atividade do outro de uma forma diferente: nem mecânica nem orgânica, mas *em rede*[4].

Estamos diante de uma condição mais complexa daquela que predicou o mundo como moderno. Segundo Willis Santiago Guerra Filho, vivemos numa *postmodern condition*, num mundo muito mais complexo e diferente daquele vivenciado em passado recente. Não há mais espaço para *grand theories* versus *big stories*, nem para postulados pré-formulados capazes de resolver cada problema social baseado em pretensas verdades científicas[5].

---

[4] FERRAZ JUNIOR, Tercio Sampaio. Direito e realidade: a erosão do real jurídico pelo mundo virtual. In: FERRAZ JUNIOR, Tercio Sampaio. **O direito entre o futuro e o passado**. São Paulo: Noeses, 2014, p.36-37.

[5] Segundo Willis Santiago Guerra Filho (no original): “The great amount of information available – and the velocity of its circulation, its fast substitution for new information due to the manner they are transmitted by the media, plus the very nature of such information, makes it not fashioned to the preservation of individual or collective memory and values. This also why it is impossible for any ideological coordination of action in a determined "historical path" to succeed. […] I am aware of the fact that the expression "postmodernity" is very emotionally-laden, since it usually provokes in the most part of intellectuals today two kind of opposite and extreme reactions: to reject or to adhere to it, as if it was some kind of modern viz. postmodern credo. People "against" postmodernity mostly insists in the permanence (or incompleteness) of modernity. Often in those attacks it is linked some kind of conservative ideology with the defense of postmodernity – frequently the "ideology of the end of ideologies".

A informação passa a ocupar um importante papel na vida social e econômica. Com a geração de máquinas inteligentes, "o caráter proteiforme da informação se aprofundará. A interpenetração, a sobreposição, as equivalências entre a informação, o saber, o conhecimento, a cultura e a comunicação não serão menos recorrentes"[6].

É justamente esse ambiente que foi alterado, consoante define Tercio Sampaio Ferraz Junior, por essa *não coisa* (*no-thing, Unding, non-chose*) que hoje chamamos de *informação* (*information*):

> A *informação* em sentido *informático* tem que ver com equipamentos técnicos que permitem apresentar nas telas algoritmos (fórmulas matemáticas) *em forma de* imagens, imagens coloridas, imagens em movimento, até mesmo textos, textos-imagem (*e-books*), que não possuem matéria a ser *informada*. Ao contrário, trata-se de *formas* (códigos numéricos) que permitem fazer aparecer outros mundos de *formas*, o que torna os critérios para distinguir o *falso* do *verdadeiro* e, por consequência, o *correto* (direito, certo) do *incorreto* (torto, errado), objeto de uma tarefa inteiramente nova. Isso porque, ao contrário do mundo tradicional em que o *imaterial* (a *forma*) permitia à *matéria* aparecer e sua *adequação* era tomada, vulgarmente, como um registro de verdade, agora lidamos com mundos apenas *virtuais*[7].

Para Armand Mattelart, a sociedade da informação ganhou um conceito instrumental, sem trazer em si um significado maior que determinará um novo destino:

> A imprecisão que envolve a noção de informação coroará a de "sociedade da informação". A vontade precoce de legitimar politicamente a ideia da realidade *hit et nunc* desta última justificará os escrúpulos da vigilância epistemológica. A tendência a assimilar a informação a um termo proveniente da estatística (*data*/dados) e a ver informação somente onde há dispositivos técnicos se acentuará. Assim, instalar-se-á um conceito puramente instrumental de sociedade da informação. Com a atopia social do conceito apagar-se-ão as implicações sociopolíticas de uma expressão que supostamente designa o novo destino do mundo[8].

(GUERRA FILHO, Willis Santiago. **Immunological theory of law**. Alemanha, Saarbrücken: Lambert Academic Publishing, 2014, p.3-4). Tradução livre: A grande quantidade de informação disponível – e a velocidade de sua circulação, sua rápida substituição por novas informações devido à maneira pela qual são transmitidas pela mídia, mais a própria natureza de tais informações, não se moldam à preservação de memórias e valores individuais ou coletivas. Isto também porque é impossível para qualquer coordenação ideológica de ação em um determinado "caminho histórico" ter sucesso. [...] Eu estou ciente do fato de que a expressão "pós-modernidade" é muito carregada emocionalmente, uma vez que geralmente provoca na maior parte dos intelectuais de hoje dois tipos de reações opostas e extremas: rejeitar ou aderir a ela, como se houvesse uma espécie de credo de moderno vs. pós-moderno. As pessoas "contra" a pós-modernidade insistem principalmente na permanência (ou incompletude) da modernidade. Muitas vezes, nesses ataques, está ligada a algum tipo de ideologia conservadora com a defesa da pós-modernidade – frequentemente à "ideologia do fim das ideologias".

[6] MATTELART, Armand. **História da sociedade da informação**. 2.ed. São Paulo: Loyola, 2006, p.70.

[7] FERRAZ JUNIOR, Tercio Sampaio. Direito e realidade: a erosão do real jurídico pelo mundo virtual. In: FERRAZ JUNIOR, Tercio Sampaio. **O direito entre o futuro e o passado**. São Paulo: Noeses, 2014, p.34-35.

[8] MATTELART, Armand. **História da sociedade da informação**. 2.ed. São Paulo: Loyola, 2006, p.71.

A sociedade da informação, para Yoneji Masuda, poderia ser considerada uma oposição ao sistema de consumo material desenfreado, visando um estado geral de florescimento da criatividade intelectual humana[9], porém o consumismo foi ainda mais intensificado na era da informação, estimulado pela publicidade comportamental, graças ao uso e tratamento massivo de dados individuais.

David Lyon, por sua vez, considerou que a dependência baseada em novas tecnologias não leva além da modernidade. Nesse sentido, ponderou que "as novas tecnologias de informação e de comunicação, conquanto em si mesmas não produzam nem a sociedade pós-industrial nem a pós-moderna"[10] fazem parte de importantes transformações sociais modernas.

O mais adequado, segundo Willis Santiago Guerra Filho, seria considerar que existem várias versões de pós-modernidade e, inversa e correspondentemente, de anti-pós-modernidade[11]. Nessa fase, surgem alguns termos, como "sociedade da informação", atribuídos à nova ordem social.

Não há dúvidas de que mais importante que as emoções em torno da definição e da nomenclatura a qual se aproprie, ou seja, a definição de apenas um ponto de partida, o principal é identificar, na nova era, as questões colocadas pelas complexidades antes não experimentadas. Nesse sentido, salutar é a reflexão de Willis Santiago Guerra Filho:

> Estou plenamente consciente da circunstância de que a expressão ´pós-modernidade´ mobiliza emoções as mais diversas e contraditórias, bem como extremadas, tanto no sentido de uma adesão como no de uma rejeição do pós-moderno, como se se tratasse de uma nova crença. Aqueles que são contra a ideia de pós-modernidade costumam afirmar a permanência (ou inacabamento´) da modernidade, associando alguma

[9] Se o objetivo da sociedade industrial pode ser representado pelo consumismo de bens duráveis ou pelo consumo em massa, centrado na motorização, a sociedade da informação pode ser classificada como uma sociedade de alta criatividade intelectual, onde as pessoas podem desenhar os seus projetos numa tela invisível, bem como perseguir e alcançar a sua autorrealização. (MASUDA, Yoneji. **A sociedade da informação como sociedade pós-industrial**. Tradução do inglês de Kival Charles Weber e Angela Melim. Rio de Janeiro: Rio, 1982, p.19).

[10] LYON, David. **Pós-modernidade**. São Paulo: Paulus, 1998, p.60. Nesse ponto, inclusive, cabe a crítica de Luis Alberto Warat: "[...] a modernidade encontra-se em trânsito para outras formas de sensibilidade e de razão. Chamo essa situação de transmodernidade. [...] Os que falam de pós estão obcecados pela idéia do fim, por isso prefiro o prefixo trans". (WARAT, Luis Alberto. **A ciência jurídica e seus dois maridos**. Santa Cruz do Sul: EDUNISC, 2000, p.46-47).

[11] No original: "As a matter of fact, there are many versions of postmodernisms and, correspondly, of anti-postmodernisms. I would like to use the expression in a as neutral as possible way, just to remark a historical change in material an intellectual process within contemporary (world-)society, when it arrives to a "Informationszeitalter". If I can chose an ideological categorization of approach I want to propose here, then I would it qualify it as a "postmodern critical theory". (GUERRA FILHO, Willis Santiago. **Immunological theory of law**. Alemanha, Saarbrücken: Lambert Academic Publishing, 2014, p.3-4). Ver também: GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lumen Juris, 2018, p.14.

> ideologia conservadora à postulação da pós-modernidade – geralmente, a ideologia do 'fim das ideologias'[12].

O que se pretende, portanto, deve ir muito além de uma datação de era de mundo, mas enaltecer o que é novo em relação ao velho. A máquina a vapor impulsionou a revolução industrial e trouxe modificações ao sistema econômico e político da época, por meio do capitalismo. A era da informação, por sua vez, implica em transformações mais profundas e prolongadas. Nas palavras de Yoneji Masuda:

> Quando aparece uma inovação tecnológica criadora de uma época, ocorrem mudanças na sociedade existente e surge uma nova sociedade. A máquina a vapor precipitou a revolução industrial, provocando modificações que levaram a um novo sistema econômico e político: o sistema capitalista e a democracia parlamentar. A época da informação, resultante da tecnologia de telecomunicações e informática, provocará uma transformação social tão grande ou maior do que a da revolução industrial[13].

Tomando por base o método axiomático[14], é preciso, sob o mecanismo chamado 'análise' – engenho da matemática – distinguir dificuldades para melhor resolvê-las, com o que se dá uma progressão do pensamento no sentido de uma crescente abstração, para em momento diverso, retornar ao problema concreto, que deverá ter os elementos que o constituem individualizados para melhor compreensão ('síntese')[15].

Há, ainda, quem enxergue uma era da informação em todas as fases da história, como Luciano Floridi. Para o autor, história é sinônimo de era da

---

[12] GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lumen Juris, 2018, p.14.

[13] MASUDA, Yoneji. **A sociedade da informação como sociedade pós-industrial**. Tradução do inglês de Kival Charles Weber e Angela Melim. Rio de Janeiro: Rio, 1982, p.86.

[14] Segundo Chaïm Perelman e Olbrechts-Tyteca, "Na lógica moderna, oriunda de uma reflexão sobre o raciocínio matemático, os sistemas formais já não são correlacionados com uma evidência racional qualquer. O lógico é livre para elaborar como lhe aprouver a linguagem artificial do sistema que constrói, para determinar os signos e combinações de signos que poderão ser utilizados. Cabe a ele decidir quais são os axiomas, ou seja, as expressões sem prova consideradas válidas em seu sistema, e dizer quais são as regras de transformação por ele introduzidas e que permitem deduzir, das expressões válidas, outras expressões igualmente válidas no sistema. A única obrigação que se impõe ao construtor de sistemas axiomáticos formalizados e que torna as demonstrações coercitivas é a de escolher signos e regras que evitem dúvidas e ambigüidades. Cumpre que, sem hesitar e mesmo mecanicamente, seja possível estabelecer se uma seqüência de signos, se é considerada válida, por ser um axioma ou uma expressão dedutível, a partir dos axiomas, de um modo conforme às regras de dedução. Qualquer consideração relativa à origem dos axiomas ou das regras de dedução, ao papel que se presume que o sistema axiomático represente na elaboração do pensamento, é alheia à lógica assim concebida, na medida em que ela sai do âmbito do formalismo em questão. A busca da univocidade indiscutível chegou a levar os lógicos formalistas a construírem sistemas nos quais não há preocupação com o sentido das expressões: ficam contentes se os signos introduzidos e as transformações que lhes dizem respeito ficam fora de discussão. Deixam a interpretação dos elementos do sistema axiomático para os que o aplicarão e terão de se preocupar com sua adequação ao objetivo pretendido. (PERELMAN, Chaïm; OLBRECHTS-TYTECA, Lucie. **Tratado da argumentação**: a nova retórica. São Paulo: Martins Fontes, 2005, p.15-16).

[15] O método axiomático foi trabalhado por BOURBAKI, N. Dir Architekur der Mathematik, 1974. Tivemos acesso à formulação em: GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lumen Juris, 2018, p.32.

informação, ao considerar que a humanidade viveu em diversos tipos de sociedades da informação, pelo menos, desde a era do bronze, a era que marca a invenção da escrita na Mesopotâmia e outras regiões do mundo (quarto milênio a.C.). Ou seja, várias sociedades podem ter projetado a si a expoente evolução de alcançar a informação, limitando a morte dos que a antecederam e o nascimento daqueles que ainda viriam. Por isso, de certo modo, toda geração se imagina especial e mais evoluída em relação as que viveram anteriormente. Daí a relevância de se manter o assunto em perspectiva[16].

Dentre calorosos debates, preferimos nos filiar à posição de que *sociedade da informação* ou *sociedade informacional* ocupou o que era denominado como sociedade ´pós-moderna`, ou `pós-modernidade´, consoante observa Willis Santiago Guerra Filho[17]: "a sociedade pós-industrial, típica da pós-modernidade, seria, então, denominada com maior propriedade, *sociedade informacional*"[18]. Segundo o autor, o período imediatamente anterior ao que vivemos, já foi a última fase da modernidade, em contraposição ao posicionamento de Niklas Luhmann e Jürgen Habermas, os quais, na década de 1990, compreenderam pela continuidade e inacabamento da modernidade, o que seria denominado de 'modernidade intermédia'[19].

O paradigma informacional foi inserido nas teorias sociais como condição e consequência da mundialização da sociedade[20], conforme será aprofundado adiante.

---

[16] Ainda segundo Luciano Floridi, no terceiro milênio a.C., Ur representou o que havia de mais evoluído no mundo. Até antes da Guerra do Golfo (1991) e a Guerra do Iraque (2003-2011), ainda existia uma biblioteca com centenas de tábuas de argila. Mesmo assim, Ur não é o que nós tipicamente temos em mente quando se fala em *sociedade da informação.* "Podem existir várias explicações, mas uma parece mais convincente do que outras: apenas muito recentemente o progresso e bem-estar humanos começou a ser não apenas *relacionado a,* mas sobretudo *dependentes da*, bem-sucedida e eficiente maneira do ciclo da vida da informação." Tamanha dependência significou a recente entrada na fase da *hyperhistoria*. Ur dependia muito mais de suas tecnologias ligadas à agricultura do que, por exemplo, às suas tábuas de argila. A fase *hyperhistorica* diz respeito a indivíduos cujo bem-estar social depende das Tecnologias da Informação e Comunicação (TIC), o que diferenciaria da fase *histórica* na qual indivíduos apenas se relacionavam com as TICs. "Em sociedades *hyperhistoricas* as TICs e sua capacidade de processamento de dados não são apenas importantes, mas condições essenciais para a manutenção e o desenvolvimento do bem-estar social". (FLORIDI, Luciano. **The 4th Revolution**. How the infosphere is reshaping human reality. Oxford University Press: New York, 2010, p.3).

[17] Em "nota explicativa", o autor esclarece que 20 anos após a primeira edição da obra, animou-se a reeditá-la por lhe parecer que algo de seu conteúdo encontraria melhor ressonância, agora, do que quando de sua publicação há duas décadas. E, nesse sentido, o autor decide por alterar o título original de sua obra, uma vez que "a sociedade de que se trata da autopoiese do Direito não a qualificamos mais de 'pós-moderna' e sim de 'informacional'" por entender ser na atualidade uma caracterização mais adequada". (GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lumen Juris, 2018).

[18] GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lumen Juris, 2018, p.16.

[19] GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lumen Juris, 2018, p.23.

[20] ACOSTA JUNIOR, Jorge Alberto de Macedo. Prefácio à 2.ed. de GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lumen Juris, 2018.

A disseminação da noção de sociedade da informação ocorre nos organismos internacionais, tal qual em 1975, a Organização de Cooperação e de Desenvolvimento Econômico (OCDE) estreia a noção do termo[21]. Em 23 de novembro de 1979, em Bruxelas, por ocasião das conferências de chefes de Estado e de Governo na Europa, que seriam realizadas em Dublin nos dias posteriores, fez-se constar em documento:

> A sociedade europeia de hoje já se configura em uma "Sociedade da Informação", na qual a atividade científica e intelectual, as transações econômicas e a vida cotidiana descansam sobre uma rede de informação engenhosa[22].

Foi a partir da elaboração do livro 'Crescimento, competitividade e emprego – desafios e pistas para entrar no século XX' (COM (93) 700, Bruxelas, 5 de dezembro de 1993) que a expressão sociedade da informação tornou-se mais conhecida.

Segundo Henrique Garbellini Carnio, "o surgimento da 'Sociedade da Informação', consequência da globalização e da crescente aceleração nos meios de comunicação, propicia uma nova pauta de debates, em especial no âmbito jurídico"[23].

Em 1995, na cúpula de Bruxelas do G8, foi discutida a noção de "sociedade global da informação". Em 2000, o G8, reunido em Okinawa, proclamou uma Carta da sociedade global da informação e criou um grupo de especialistas sobre o acesso às novas tecnologias da informação, preocupados em perseguir a redução das desigualdades de acesso ao ciberespaço[24].

Em 2003, a Unesco contribuiu para organizar uma cúpula mundial sobre a sociedade da informação, cujas conferências ocorreram na sede da União Internacional das Telecomunicações (IUT), em Genebra, visando a desenvolver um entendimento e uma visão comuns da sociedade da informação e elaborar um plano estratégico que permitisse colocá-los em prática.

Nas palavras de Armand Mattelart,

> As conferências preparatórias para a Cúpula aceleraram a disseminação administrativa da noção de sociedade da informação, sem com isso eliminar a confusão que a envolve. Alguns governos caem no ciberdeterminismo e

[21] MATTELART, Armand. **História da sociedade da informação**. 2.ed. São Paulo: Loyola, 2006, p.118-119.
[22] CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.40.
[23] CARNIO, Henrique Garbellini. Conhecimento e direito digital: acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos na Lei do Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo. **Marco civil da internet**. São Paulo: Atlas, 2014, p.262.
[24] MATTELART, Armand. **História da sociedade da informação**. 2.ed. São Paulo: Loyola, 2006, p.157-158.

> reciclam pela enésima vez o discurso da "modernização" sem atacar as lógicas regressivas de concentração de renda que andam lado a lado com a dos usos da tecnologia. Outros aproveitam a ocasião para apropriar-se da noção e tentar transformá-la em outra coisa. A incorporação do tema das tecnologias da informação e da comunicação na agenda política torna-se, então, ao menos para os setores reformistas, uma ocasião para iniciar um debate de fundo sobre a técnica, a sociedade e as liberdades individuais e, indiretamente, catalisa a reflexão sobre incompatibilidade do modelo de desenvolvimento inscrito nas lógicas extremadas do liberalismo com os cenários de construção de uma sociedade do conhecimento para todos e por todos[25].

O termo 'sociedade da informação' passou a ser utilizado, portanto, nas últimas décadas do século passado, em substituição à 'sociedade pós-industrial'.

Ao contrário da vaga expressão 'sociedade pós-industrial', a expressão 'sociedade da informação' descreve o "fato de que a produção de valores informacionais, e não valores materiais, será a força motriz da formação e do desenvolvimento dessa sociedade"[26].

Conforme se vê, as autodescrições da sociedade contemporânea podem apresentar algumas variações entre si, mas há um ponto em comum, qual seja, "quase todas buscam enfatizar a função da informação no mundo atual: sociedade da informação ou sociedade do conhecimento, economia da informação ou sociedade em rede" [27]. Nesse sentido contribui Laura Schertel Mendes:

> Essa diversidade de expressões já é suficiente para constatar o papel fundamental que o fenômeno da informação desempenha na sociedade contemporânea e em todos os seus subsistemas. Torna-se assim, essencial para o Direito reconhecer o papel constitutivo da informação na nossa sociedade e buscar compreender as formas de lidar com esse fenômeno e os seus efeitos[28].

Dentro da progressão do que se concebeu por sociedade da informação, verifica-se que os maiores impactos sobrevieram com a chegada da internet, capaz de conectar as diversas redes existentes – por isso é chamada de 'rede das redes'.

Segundo Brandão e Suárez, a rápida evolução das tecnologias da informação nas últimas décadas modificou a geometria e a dinâmica das relações sociais. Segundo os autores:

---

[25] MATTELART, Armand. **História da sociedade da informação**. 2.ed. São Paulo: Loyola, 2006, p.163.
[26] MASUDA, Yoneji. **A sociedade da informação como sociedade pós-industrial**. Tradução do inglês de Kival Charles Weber e Angela Melim. Rio de Janeiro: Rio, 1982, p.45.
[27] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.19.
[28] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.19.

> La rápida evolución de las tecnologías de información en las últimas décadas ha cambiado la geometría y la dinámica de las relaciones sociales. La comunicación humana es intermediada, o sea, ha pasado a ocurrir también por otros medios. Nació en este paradigma lo que se ha llamado de era o sociedad de información, en el que la información adquiere el status de bien esencial, quizá más rentable e importante de todos[29].

Não chama a atenção o fato de que, desde a década de 1980, Yoneji Masuda já alertara: a revolução da informação na sociedade estava ocorrendo de três a seis vezes mais rapidamente do que a revolução da energia motora (revolução industrial):

> Por exemplo, a revolução da energia motora precisou de 57 anos para que o desenvolvimento da máquina de Newcomen atingisse 1000 unidades, e de mais uns 35 anos para que a máquina de James Watt se difundisse na indústria moderna, como foi o caso das indústrias do aço, mineração de carvão e de fiação. A difusão do computador ocorreu, aproximadamente, 4,6 vezes mais depressa do que a difusão da máquina a vapor. Outro exemplo: levou 49 anos para que as primeiras 1000 máquinas industriais de fiar fossem vendidas, mas levou apenas 9 anos para que o processamento eletrônico de dados fosse introduzido nas empresas[30].

Sob a perspectiva da tipologia das máquinas, Gilles Deleuze compara suas formações às diferentes sociedades, não porque as máquinas sejam determinantes, mas porque elas exprimem as formas sociais capazes de lhes darem nascimento e de utilizá-las. Nesse sentido afirma o autor:

> As antigas sociedades de soberania manejavam máquinas simples, alavancadas, roldanas, relógios; mas as sociedades disciplinares[31] recentes tinham por equipamentos máquinas energéticas, com o perigo passivo da entropia e o perigo ativo da sabotagem; as sociedades de controle operam por máquinas de uma terceira espécie, máquinas de informática e computadores, cujo perigo passivo é a interferência, e, o ativo, a pirataria e a introdução de vírus. Não é uma evolução tecnológica sem ser, mais profundamente, uma mutação do capitalismo[32].

---

[29] BRANDÃO, André Martins; SUÁREZ, Nuria Lopez Cabaleiro. Sociedad de información: la nueva topología del poder. In: (Orgs.) REY, Paula Requeijo; PISONERO, Carmen Gaona. **Contenidos inovador en la Universidad actual**. Madrid: McGraw-Hill, 2014, p.01.

[30] MASUDA, Yoneji. **A sociedade da informação como sociedade pós-industrial**. Tradução do inglês de Kival Charles Weber e Angela Melim. Rio de Janeiro: Rio, 1982, p.62.

[31] "Foucault situou as *sociedades disciplinares* nos séculos XVIII e XIX; atingem seu apogeu no início do século XX. Elas procedem à organização dos grandes meios de confinamento. O indivíduo não cessa de passar de um espaço fechado a outro, cada um com suas leis: primeiro a família, depois a escola (´você não está mais na sua família´), depois a caserna (´você não está mais na escola´), depois a fábrica, de vez em quando o hospital, eventualmente a prisão, que é o meio de confinamento por excelência. [...] Mas o que Foucault também sabia era da brevidade deste modelo: ele sucedia às *sociedades de soberania* cujo objetivo e funções eram complementares e diferentes (açambar, mais do que organizar a produção, decidir sobre a morte mais do que gerir a vida); a transição foi feita progressivamente, e Napoleão parece ter operado a grande conversão de uma sociedade à outra". (DELEUZE, Gilles. **Conversações**. Tradução Peter Pál Pelbart. São Paulo: Editora 34, 2013, p. 223).

[32] DELEUZE, Gilles. **Conversações**. Tradução Peter Pál Pelbart. São Paulo: Editora 34, 2013, p.227. "É uma mutação já bem conhecida que pode ser resumida assim: o capitalismo do século XIX é de concentração, para a produção, e de propriedade. Por conseguinte, erige a fábrica como meio de confinamento, o capitalista sendo o proprietário dos meios de produção, mas também eventualmente proprietário de outros espaços concebidos por

A velocidade da modernização, na forma como se concebe e verifica, também traz à reflexão o desenvolvimento social nocivo que pode ser acarretado à própria humanidade. “Não devemos querer nos modernizar, se isso significa adotar uma organização social que isola as pessoas. Se isso significa viver na superficialidade, no efêmero e no fugaz”[33]. Paul Virilio pondera como seria possível viver verdadeiramente se “o aqui não o é mais, e se tudo é agora”[34].

Segundo Lucia Santaella, a plasticidade implicada na rápida adaptação da memória humana está nos tornando simbióticos com nossos computadores, na convivência com sistemas interconectados que nos levam a conhecer menos sobre o conteúdo específico das informações em contrapartida ao muito que passamos a saber[35].

Umberto Eco, em carta aberta escrita ao seu neto, adverte sobre os malefícios trazidos pela tecnologia da internet para as gerações atuais. Chega a atribuir o comprometimento da memória ao uso demasiado do computador e da internet, os quais podem criar a ilusão ao indivíduo de que seriam capazes de responder a qualquer pergunta em qualquer instante. Por isso, ao comparar o músculo das pernas com o músculo do cérebro, recomenda ao neto que saiba exercitar sua mente durante sua vida, ocupando-se de memorizar versos, livros, momentos históricos, etc[36]. Não à toa, em outra ocasião, o escritor afirma que as redes sociais da internet trouxeram uma invasão de imbecis (sic)[37].

Segundo Byung-Chul Han, visto a partir de uma perspectiva patológica, o começo do século XXI não é definido como bacteriológico nem viral, mas neural:

---

analogia (a casa familiar do operário, a escola). Quanto ao mercado, é conquistado ora por especialização, ora por colonização, ora por redução dos custos de produção. Mas atualmente, o capitalismo não é mais dirigido para a produção, relegada com frequência à periferia do Terceiro Mundo, mesmo sob as formas complexas do têxtil, da metalurgia ou do petróleo. É um capitalismo de sobreprodução. Não compra mais matéria-prima e já não vende produtos acabados: compra produtos acabados, ou monta peças destacadas. O que ele quer vender são serviços, e o que quer comprar são ações. Já não é um capitalismo dirigido para a produção, mas para o produto, isto é, para a venda ou para o mercado”.

[33] GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lumen Juris, 2018, p.17.

[34] VIRILIO, Paul. **O espaço crítico**. Tradução de Paulo Roberto Pires da edição de 1984. São Paulo: Editora 34, 2014, p.121.

[35] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.46.

[36] ECO, Umberto. Caro Nipote, studia a memoria. In: **La Repubblica.it**. Publicado em: 03 jan. 2014. Disponível em: <http://espresso.repubblica.it>. Acesso em: 30 jul. 2018.

[37] “I social media danno diritto di parola a legioni di imbecilli che prima parlavano solo al bar dopo un bicchiere di vino, senza danneggiare la collettività. Venivano subito messi a tacere, mentre ora hanno lo stesso diritto di parola di un Premio Nobel. È l'invasione degli imbecilli”. (Disponível em: <https://www.ilmessaggero.it/>. Acesso em: 30 jul. 2018).

> Doenças neurais como a depressão, transtorno de déficit de atenção com síndrome de hiperatividade (TDAH), Transtorno de Personalidade Limítrofe (TPL) ou a Síndrome de Burnout (SB) determinam a paisagem patológica do começo do século XXI. Não são infecções, mas enfartos, provocados não pela *negatividade* de algo imunologicamente diverso, mas pelo excesso de *positividade.* Assim, eles escapam a qualquer técnica imunológica, que tem a função de afastar a negatividade daquilo que é estranho[38].

Vê-se, com efeito, como a conectividade cotidiana, com o consequente contexto hiperinformacional, imediatista e menos interpessoal, vem causando problemas que desafiam o bem-estar do homem contemporâneo.

Para Zygmunt Bauman, o uso excessivo das ferramentas digitais está trazendo o que o autor denomina de morte social, porque os indivíduos se relacionam mais com os equipamentos eletrônicos do que com outras pessoas[39].

A necessidade de exibição pública faz com que o pensamento de Hannah Arendt nunca estivesse tão presente:

> A admiração pública é também algo a ser usado e consumido; e o *status*, como diríamos hoje, satisfaz uma necessidade como o alimento satisfaz outra: a admiração pública é consumida pela vaidade individual da mesma forma como o alimento é consumido pela fome[40].

Ademais, desenvolveu-se na sociedade atual a constante cobrança de que os indivíduos estejam sempre conectados e disponíveis. Nesse sentido reflete Paula Sibilia:

> Os muros das empresas também desabam: os funcionários ou colaboradores são aparelhados com tecnologias de conexão permanente (telefones móveis, computadores portáteis, acesso a internet, dispositivo de geolocalização) que embaçam os limites entre lugar de trabalho e lugar de lazer, tempo de trabalho e tempo de lazer. Tais ´coleiras eletrônicas´ – como as batizara Deleuze, em alusão aos sistemas que permitem monitorar os presos em regimes semi-abertos – constituem apenas uma das várias formas sociotécnicas que hoje se desenvolvem. Afinal, isso ocorrre numa era que apregou a digitalização total e na qual tudo pode ser monitorado, ou deveria poder sê-lo, pois se considera desejável que todos estejam sempre disponíveis, ligados *online*[41].

Sob outra perspectiva, em ‘Sociedade do Cansaço’, Byung-Chul Han compara a sociedade disciplinar de Michel Foucault com a sociedade de desempenho[42]. Enquanto o modelo disciplinar foucaultiano era dominado pelo *não*, na sociedade do

---

[38] HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.7-8.
[39] BAUMAN, Zygmunt. **Vida para consumo**: a transformação das pessoas em mercadoria. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2008, p.9.
[40] ARENDT, Hannah. **A condição humana**. 10.ed. Rio de Janeiro: Forense, 2003, p.66.
[41] SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.38.
[42] HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.23.

desempenho o *poder* ilimitado é o verbo modal positivo, sempre vinculado ao refrão *Yes, we can.* No lugar de proibição, mandamento ou lei, entram projeto, iniciativa e motivação. Em sua negatividade, a sociedade disciplinar gerava loucos e delinquentes, enquanto a sociedade do desempenho, ao contrário, produz depressivos e fracassados, agravada pela carência de vínculos acarretados pelos meios digitais. O sujeito de desempenho é cansado (cansaço solitário) porque está em guerra consigo mesmo. Ademais, o cansaço do esgotamento não é um cansaço da potência positiva, porquanto incapacita de fazer qualquer coisa[43].

Ainda segundo Byung-Chul Han, o paradigma da disciplina, para elevar a produtividade, é substituída pelo paradigma do desempenho. "A positividade do poder é bem mais eficiente que a negatividade do dever"[44]. Sobre essas reflexões, Alessandra Parente argumenta:

> Com a ideia de poder, a engrenagem do sistema capitalista recente gira de modo mais veloz e eficiente do que pela lógica do dever – o sujeito do desempenho continua disciplinado, mas agora age disciplinarmente por livre e espontânea vontade[45].

O excesso de trabalho e o desempenho acabam gerando uma exploração de si mesmo, que culmina em infartos-psíquicos. O imperativo do desempenho faz do homem um explorado de si-mesmo, sem qualquer coação estranha. A autoexploração, diga-se, é mais eficiente que uma exploração do outro, pois caminha de mãos dadas com o sentimento de liberdade. Explorador e explorado, agressor e vítima, se confundem na mesma pessoa e não são mais distinguíveis. Sobre isso expõe Byung-Chul Han:

> Essa autorreferencialidade gera uma liberdade paradoxal que, em virtude das estruturas coercitivas que lhe são inerentes, se transforma em violência. Os adoecimentos psíquicos da sociedade de desempenho são precisamente as manifestações patológicas dessa liberdade paradoxal[46].

---

[43] Byung-Chul Han diz que o cansaço que inspira é um cansaço da potência negativa, ou seja, do *não-para.* Nesse sentido, destaca o Sabah, que originalmente, segundo ele, significa *parar:* é um dia do *não-para*, um dia que está livre de todo *para-isso*. É um *tempo intermédio.* "Depois de terminar sua criação, Deus chamou ao sétimo dia de sagrado. Sagrado, portanto, não é o dia do *para-isso*, mas o dia do *não-para*, um dia no qual seria possível o uso do inútil. É o dia do cansaço". (HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.76). O resgate ao sábado judaico, tido como sagrado, ou seja, separado, dentro da sociedade do cansaço, consiste em uma proposta de resgate do homem, inserido na sociedade informacional, a voltar-se à contemplação e ao esvaziamento da positividade e desempenho.
[44] HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.25.
[45] PARENTE, Alessandra. **Cibernética e neoliberalismo**: a crítica como mercadoria. (No prelo), p.17.
[46] HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.30.

E dentro desse imperativo, o sujeito do desempenho não está submisso a ninguém. Ele explora a si mesmo até chegar a consumir-se totalmente. Propriamente, ele já não é sujeito, dentro do qual inabita ainda alguma subjugação. Há um deslocamento de *sujeito* para *projeto*[47].

Na análise de Byung-Chul Han, essa mudança não faz desaparecer a violência, uma vez que em lugar da coerção exterior surge a autocoerção, o sujeito imagina ser livre. Esse fenômeno integra a produção capitalista, posto que a partir de um certo nível de produção a autoexploração é muito mais intensa do que a exploração alheia, pois o sujeito se acha livre. Portanto, a sociedade de desempenho é uma sociedade de autoexploração, na qual surge a autoagressividade[48]. Assim, há uma mudança topológica da violência[49], que se volta ao próprio sujeito, dentro da dinâmica expressa pelo superdesempenho, superprodução e supercomunicação, como um hiperchamar a atenção e hiperatividade. Trata-se de uma violência subcutânea e invisível[50].

Conforme pondera Willis Santiago Guerra Filho, "como sociedade, estamos fracassando de maneira paralela à genética molecular e à dita Civilização ocidental, no que esta se aplica a nós mesmos e ao ser". E justamente porque o ser não se volta a si mesmo, e por não saber o que é o próprio ser, é que vivemos numa

---

[47] Sobre o tema, Paula Sibilia reflete: Em gradativo afastamento da dura lógica mecânica que comandou o industrialismo, cada vez mais investidos pelo novo regime digital, os corpos contemporâneos se apresentam como perfis cifrados nas bases moleculares de sua constituição bioquímica. Nos âmbitos mais diversos, agora eles são pensados e tratados como sistemas de processamento de dados e feixes de informação; e, graças às potências do novo arsenal tecnocientíficos, essa última é manipulável, quase sempre visando a otimizar seu desempenho e seu bem-estar. Desse modo, entregue às novas cadências da tecnociência da mídia e do mercado, o corpo humano parece ter perdido tanto sua definição clássica como a analógica solidez que outrora o constituira. Na esteira digital, ele se torna mais permeável, projetável, reprogramável. (SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.17).

[48] A preocupação por um viver bem dá lugar à histeria por sobreviver. A redução da vida a processos biológicos, vitais, provoca seu desnudamento; a simples sobrevivência se torna obscena. Com isso, retira-se da vida sua *vivacidade*, que é algo bem mais complexo do que a mera vitalidade e a saúde. O delírio pela saúde surge quando a vida se torna desnuda. Diante da atomização da sociedade e da erosão social resta somente o *corpo do eu*, que precisa ser conservado sadio, a qualquer custo. A vida desnudada faz desaparecer toda e qualquer teleologia, todo e qualquer "para que", em função dos quais o ser humano deveria ser sadio. A saúde torna-se autorreferente e se esvazia, tornando-se uma *teleologia sem telos.* A vida nunca foi tão transitória quanto hoje em dia; não há nada que prometa duração e persistência. Diante da *falta de ser*, o que surge é o nervosismo. Nesse contexto, a hiperatividade e a aceleração do processo de vida seriam tentativas de sair daquele *vazio* que anuncia a morte. Mas uma sociedade dominada pela histeria do sobreviver é uma sociedade de *mortos-vivos* que não conseguem viver nem morrer. (HAN, Byung-Chul. **Topologia da violência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.49-50).

[49] Ainda segundo Byung-Chul Han, "a internalização psíquica é um dos deslocamentos topológicos centrais da violência na modernidade; a violência toma forma de conflito intrapsíquico. Tensões destrutivas são suportadas internamente, em vez de serem descarregadas para fora; o *front* de batalha não se desenrola externamente, mas dentro das pessoas". (HAN, Byung-Chul. **Topologia da violência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.22).

[50] Sobre a mudança da topologia da violência e o sujeito do desempenho: HAN, Byung-Chul. **Topologia da violência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017.

perspectiva insegura, com atenção demasiada à máquina em desatenção ao próprio ser. Nas palavras do autor:

> Precisamente porque o ser simplesmente é, por não se auto-questionar, e por não termos uma definição adequada do que é ser, é que se torna altamente insegura a continuidade deste ser, que é de maneira única em nós. Uma nova filosofia do espírito, que trará uma espiritualização da filosofia em uma nova forma, igualmente científica, porque quântica, poderá ainda nos redimir? Vamos insistir em apenas cuidar de "espiritualizar" os dispositivos cibernéticos, valendo-nos, iterativamente, do quanto vai nos permitindo avançar aqueles de que já dispomos e cada vez mais, para recorrer ao diagnóstico heideggeriano, dispõem de nós?[51]

A melhor imagem do homem atual corresponde a zumbis, alienados, embora sempre antenados, que mal sabem as razões intrínsecas de seus movimentos. O novo modo de produção não está apartado do consumo – enquanto o sujeito consome informações pelas redes, está produzindo conteúdos para a máquina algorítmica[52].

1.2 Dos computadores às redes sociais

No contexto da sociedade da informação, ocorreu uma evolução desde o surgimento do computador até a popularização das redes sociais, na consagração da *web 2.0*[53], essa assim considerada quando o seu usuário passa a, além de receber e consumir informações, também a gerá-las. Passa-se a analisar esse caminhar.

O computador remete a um passado mais distante do que se costuma imaginar. Em plena Revolução Industrial, Charles Babbage (1792-1871), que ficou conhecido como o pai do computador, aprimorou as máquinas de calcular[54], criando

---

[51] GUERRA FILHO, Willis Santiago. **Quantum critic**: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.149.

[52] PARENTE, Alessandra. **Cibernética e neoliberalismo**: a crítica como mercadoria. (No prelo), p.17-18.

[53] Segundo Stefano Rodotà, a Web 2.0 representa uma passagem da internet dos indivíduos para aquele das redes sociais, permanecendo as redes, porém, sobre as pessoas. O autor aponta a chegada da Web 3.0, a qual descreve a mudança de paradigma ao interno da própria rede: "La crescita esponeziale dele informazione disponibili, peraltro, determina um cambiamento di scala non soltanto quantitativo, ma qualitativo. Aumentando le possibilità combinatorie che, già socialmente assai rilevanti quando non vi sai uma direta implicazione dele persone, possono divenire dirompenti per il sistema dei diritti. L´identità personale è sfidata, l´autonoma capacità di decisione resulta impoverita, l´invocazione della privacy può divenire ancora più vana, in definitiva si percepisce uma perdita di controlo sul sé che può indurre ala rassegnata conclusione della vanità di ogni resistenza". (RODOTÀ, Stefano. **Il diritto di avere diritti**. Bari/Italia: Laterza, 2012, p.323).

[54] Foi nos séculos XVI e XVII que surgiu a primeira máquina para tratar os números. A primeira máquina para processar números foi construída por Wilhelm Schickard (1592-1635), realizando quase todas as operações básicas da matemática; soma, subtração e divisão. Durante a Guerra dos Trinta Anos, Blaise Pascal (1623-1662)

o calculador analítico, o qual guardava aspectos em comum com o que se conhece atualmente por computador. Contudo, por falta de recursos financeiros, faleceu sem terminar sua invenção.

É possível afirmar que o computador eletrônico representa um desenvolvimento da máquina de calcular. Essas seriam a pré-história da construção dos computadores eletrônicos. A máquina de calcular, própria da época de Blaise Pascal e de Gottfried Wilhelm Leibniz, está diretamente ligada aos mecanismos de relojoaria que constituíam um dos setores tecnológicos mais aperfeiçoados na ciência mecânica dos séculos XVII e XVIII[55].

A realidade dos computadores pessoais e microprocessadores conhecida hoje, por sua vez, passados os caminhos por cartão perfurado e cartão contínuo, surgiu na Bay Area da costa sudoeste dos Estados Unidos, no centro do movimento da contracultura e da iniciativa *hippie*[56]. No início da década de 1970, houve uma mudança de mentalidade. Conforme John Markoff evidenciou em seu estudo sobre a convergência da contracultura com a indústria de computadores, "a computação deixou de ser considerada uma ferramenta de controle burocrático para ser adotada como um símbolo de expressão individual e libertação"[57].

Segundo Stewart Brand[58],

> a maioria das pessoas da nossa geração desprezava os computadores como a personificação de controle centralizado, [...] um contingente minúsculo — chamado depois de *hackers* — aderiu aos computadores e

---

construiu a primeira calculadora, a qual recebeu o nome de Pascaline, operando apenas soma e subtrações e cujo projeto foi, mais adiante, aprimorado por Gottfried Nilhem Leibinz (1646-1716).

[55] LOSANO, Mario G. **Lições de Informática jurídica**. São Paulo: Resenha Tributária, 1974, p.69.

[56] Conforme relato de Isaacson na biografia de Steve Jobs, referindo-se ao vocalista do U2: "O músico Bono, que mais tarde se tornou amigo de Jobs, discutiu muitas vezes com ele porque o pessoal imerso na contracultura rebelde do rock e das drogas da Bay Area acabou ajudando a criar a indústria dos computadores pessoais. "As pessoas que inventaram o século XXI eram *hippies* que fumavam maconha, andavam de sandálias e eram da Costa Oeste, como Steve, porque viam as coisas de forma diferente", diz ele. "Os sistemas hierárquicos da Costa Leste, da Inglaterra, da Alemanha e do Japão não estimulam esse pensamento diferente. Os anos 60 produziram uma mentalidade anárquica que é ótima para imaginar um mundo que ainda não existe." (ISAACSON, Walter. **Steve Jobs**: a biografia. Tradução de Berillo Vargas, Denise Bottmann e Pedro Maia Soares. São Paulo: Companhia das Letras, 2011, p.93).

[57] MARKOFF, John. **What the dormouse said**: how the sixties counterculture shaped the personal computer industry. Disponível em: <https://www.amazon.com>. Acesso em: 20 maio 2018.

[58] Segundo Isaacson, Stewart Brand encorajou os cidadãos da contracultura a compartilhar da mesma causa dos hackers. "Visionário travesso que gerou diversão e ideias ao longo de muitas décadas, Brand participou no início dos anos 1960 de um dos primeiros estudos sobre lsd em Palo Alto. Ele se uniu a seu companheiro de assunto Ken Kesey para produzir em 1966 o Trips Festival (uma celebração do lsd), apareceu na cena de abertura de 'O teste do ácido de refresco elétrico', de Tom Wolfe, e trabalhou com Doug Engelbart para criar uma apresentação seminal de som e luz de novas tecnologias chamada "A mãe de todas as demos". (ISAACSON, Walter. **Steve Jobs**: a biografia. Tradução de Berillo Vargas, Denise Bottmann e Pedro Maia Soares. São Paulo: Companhia das Letras, 2011, p.93).

> começou a transformá-los em instrumentos de libertação. Isso veio a ser o verdadeiro caminho real para o futuro[59].

A combinação dos computadores com as tecnologias de informação possibilitou a formação de redes. Segundo Yoneji Masuda, "essa rede vem se transformando em um sistema que se assemelha aos mecanismos de informação de um corpo vivo, ou seja, um organismo"[60]. Em verdade, vivemos numa complexa sociedade cujos sistemas estão ligados e integrados por redes de informação, possibilitando uma sociedade altamente orgânica, com capacidade de reação e dinamismo frente aos problemas.

Em relação ao desenvolvimento da informatização, baseado no uso dos computadores, há quatro estágios sugeridos por Yoneji Masuda. O *primeiro estágio*, chamado de *científico*, ocorreu entre 1945 e 1970, período em que o computador começou a ser usado extensivamente em projetos nacionais, tais como a defesa nacional e a exploração espacial. O *segundo estágio* se estende entre 1955 e 1980, aproximadamente, e consiste na passagem das ciências naturais para a gestão empresarial – *informatização da gestão empresarial*. À medida que a informatização é aplicada às áreas de gerência e administração, tanto no governo como na iniciativa privada, o uso do computador fará melhorar a eficiência operacional de seus órgãos. O *terceiro estágio* abrange o período de 1970 em diante, quando o computador passa a ser usado para o benefício da sociedade como um todo. É um período voltado ao Bem-Estar Nacional Bruto (BNB), ao invés de acréscimos no Produto Nacional Bruto (PNB). O computador passa a ser usado para resolver problemas em todas as áreas da sociedade, envolvendo os cidadãos como um todo. O último estágio sugerido por Yoneji Masuda é voltado para solucionar as necessidades individuais, e tem seu marco a partir de 1975, quando surgiram os circuitos integrados[61]. As pessoas passaram a dispor de soluções para resolver problemas individuais[62].

---

[59] E adiciona: "Um campo de poder íntimo e pessoal está se desenvolvendo – poder do indivíduo de conduzir sua própria educação, encontrar sua própria inspiração, dar forma ao seu próprio ambiente e compartilhar sua aventura com quem quer que esteja interessado". (ISAACSON, Walter. **Steve Jobs**: a biografia. Tradução de Berillo Vargas, Denise Bottmann e Pedro Maia Soares. São Paulo: Companhia das Letras, 2011, p.93-94).

[60] MASUDA, Yoneji. **A sociedade da informação como sociedade pós-industrial**. Tradução do inglês de Kival Charles Weber e Angela Melim. Rio de Janeiro: Rio, 1982, p.74.

[61] No Brasil, os circuitos integrados recebem proteção na área de propriedade intelectual por sua topografia conforme a Lei n.11.484, de 31 de maio de 2007.

[62] Segundo Yoneji Masuda, "nesse estágio, a sociedade da informação terá alcançado um nível equivalente ao estágio mais avançado da sociedade industrial, o estágio do consumo em massa, em que as pessoas possuem bens duráveis, tipo televisões e automóveis". (MASUDA, Yoneji. **A sociedade da informação como sociedade pós-industrial**. Tradução do inglês de Kival Charles Weber e Angela Melim. Rio de Janeiro: Rio, 1982, p.56).

A facilidade de acesso à informação e ao conhecimento estimula o florescimento da criatividade humana, consistindo no mais alto grau da informatização, chamado por Yoneji Masuda de sociedade da criação do conhecimento em massa. A principal característica dessa fase é que cada pessoa será o sujeito do desenvolvimento da informatização.

Na década de 1990, os computadores – caracterizados por serem autônomos e descentralizados – passaram a compor uma grande rede, "por meio da interconexão de dispositivos de processamento de dados, existentes em diversos formatos"[63].

A internet, por sua vez, aliada ao hardware e ao software, concretiza o auge da razão humana, dentre as inovações trazidas na modernidade. Conforme esclarece Zygmunt Bauman, o modelo de capital Fordista, baseado na rotina de fábrica, foi transformado com o capitalismo centralizado no *software*[64], modificando completamente a sociedade, ainda que ela determine o seu funcionamento, conforme defende Stefano Rodotá[65].

Transcorridas mais de quatro décadas desde o nascimento dos computadores pessoais, a computação hoje avança sobre diversas áreas das ciências, desde a cibernética na biologia molecular, dos microchips instalados em sementes vegetais, internet das coisas à inteligência artificial espalhada por diversos segmentos na incessante busca do homem de acelerar seus processos e de buscar a perfeição.

Paradoxalmente, a busca por aprimoramento traz uma significativa perda no que concerne aos empregos e ao consequente meio de subsistência dos indivíduos. Ouve-se novos gritos ludistas. Na sociedade da informação, a robótica e a inteligência artificial estão transformando as carreiras e os empregos da forma como os conhecemos até recentemente.

Uma pesquisa sobre automação da McKinsey Global Institute[66] revela que 30% dos empregos atuais poderão ser automatizados até 2030, o que acarretará em

---

[63] CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia, sociedade e cultura. v.1. São Paulo: Paz e Terra, 2011, p.89.

[64] "O tempo congelado da rotina de fábrica, junto com os tijolos e argamassa das paredes, imobilizava o capital tão eficientemente quanto ao trabalho que este empregava. Tudo isso mudou, no entanto, com o advento do capitalismo de software e de modernidade 'leve'". (BAUMAN, Zygmunt. **Modernidade líquida**. Tradução de Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2001, p.135).

[65] "A rede mudou a sociedade, mas é esta última que age para determinar as modalidades de funcionamento, e portanto, essa mesma modifica a rede". (RODOTÀ, Stefano. **Il mondo nella rete**. Quali i diritii, quali i vincoli. Roma: Laterza, 2014, p.55).

[66] McKINSEY Global Institute. **Jobs lost, jobs gained**: workforce transitions in a time of automation. Dez. 2017. Vide também: GALEON, Dom. **World bank chief**: robots have put us on a dangerous "crash course". Disponível em: <https://futurism.com/world-bank-chief-robots-have-put-us-on-a-dangerous-crash-course>. Acesso em: 25

cerca de 800 milhões de pessoas com necessidade de arrumar outro emprego para sobreviver. Por outro lado, a mesma pesquisa aponta que enquanto muitos empregos desaparecerão, vários outros serão criados; alguns que sequer podem ser pensados nos dias de hoje.

Sob outra perspectiva, diante desse novo paradigma computacional e tecnológico nos deparamos com uma nova dinâmica quanto à exposição das informações, a qual despertou a seguinte pergunta em Pierre Levy: “Mas e o caos, a confusão, o caráter diluviano da informação e da comunicação no ciberespaço?”

Nesse sentido, pondera o autor:

> De fato, a profusão do fluxo informacional, sua ausência de ordem global *a priori* não impedem que as pessoas ou coletivos nele se orientem e organizem por sua própria conta hierarquias, seleções, uma estrutura. Definitivamente desapareceram as seleções, as hierarquias ou as estruturas de conhecimentos pretensamente válidos para todos a qualquer momento, a saber o universal totalizante. Como já indiquei, para a organização de uma ordem local e provisória na desordem global, há ‘mecanismos de busca’, índices on-line e instrumentos de navegação cada vez mais aperfeiçoados a serviço do internauta[67].

Por sua vez, Luciano Floridi indaga, não o que virá depois, mas o que ficou para trás, o que foi realmente deixado na sociedade após o advento das tecnologias que a impactaram. Nesse sentido, questiona: “Is there a unifying perspective from which all these phenomena may be interpreted as aspects of a single, macroscopic trend?”[68] E responde:

> Part of this difficulty, in answering this question, is that we are still used to looking at ICTs as tools for interacting with the world and with each other. In fact, they have become environmental, anthropological, social, and interpretative forces. They are creating and shaping our intellectual and physical realities, changing our self-understanding, modifying how we relate to each other and ourselves, and upgrading how we interpret the world, and all this pervasively, profoundly, and relentlessly[69].

---

ago. 2018; MITCHELL, Tom; BRYNJOLFSSON, Erik. **Track how technology is transforming work**. Disponível em: <https://www.nature.com/news/track-how-technology-is-transforming-work-1.21837>. Acesso em: 25 ago. 2018.

[67] LEVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. 3.ed. Janeiro: Editora 34, 2010, p.252.

[68] FLORIDI, Luciano. **The 4th Revolution**. How the infosphere is reshaping human reality. Oxford University Press: New York, 2010, p.vi. Tradução livre: Existe uma perspectiva unificadora a partir da qual todos esses fenômenos podem ser interpretados como aspectos de uma única tendência macroscópica?

[69] FLORIDI, Luciano. **The 4th Revolution**. How the infosphere is reshaping human reality. Oxford University Press: New York, 2010, p.vii. Tradução livre: “Parte dessa dificuldade, respondendo a essa questão, é que ainda estamos acostumados a considerar as TICs como ferramentas para interagir com o mundo e mutuamente. De fato, elas se tornaram forças ambientais, antropológicas, sociais e interpretativas. Estão criando e moldando nossas realidades físicas e intelectuais, mudando nossa autocompreensão, modificando nosso relacionamento mútuo e com nós mesmos, e aprimorando a forma como interpretamos o mundo, e tudo de forma penetrante, profunda e implacável”.

A conexão permanente proporcionada pela banda larga alavancou a era das plataformas de redes sociais: “graças à explosão das redes sociais, os princípios baseados em troca, participação, colaboração e compartilhamento expandiram-se notavelmente”[70].

Além disso, não se pode deixar de lembrar da célebre ‘Declaração de Independência do Cyberespaço’, capitaneada por John Perry Barlow[71], publicada na Revista Wired, em 1996, em resposta à promulgação da reforma da lei de telecomunicações americana. O documento consistiu em uma declaração de discordância e resistência ao regramento estatal sobre os ambientes existentes na internet:

> Ó, governos do mundo industrial, esgotados gigantes de carne e aço, eu venho do ciberespaço, a nova morada da mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. Vocês não são bem-vindos entre nós. Vocês não têm soberania onde nos reunimos. [...] Declaro que o espaço social global que estamos construindo é naturalmente independente das tiranias que vocês querem nos impor. Vocês não têm o direito moral de nos impingir regras [...] Governos derivam seus verdadeiros poderes a partir do consentimento dos governados. Vocês nunca solicitaram nem receberam nosso consentimento. Nós não convidamos vocês. Vocês não nos conhecem, nem conhecem nosso mundo. O ciberespaço não se situa dentro de suas fronteiras. Não pensem que podem construí-lo como se fosse um projeto de construção pública, vocês não podem. É um ato da natureza e cresce através de nossas ações coletivas.[72]

Chama a atenção que as palavras extremadas do documento acima, da década de 1990, possuem pontos de ligação com a forma pela qual atualmente algumas plataformas de serviços de internet têm se posicionado, é dizer, com aparente descaso à Justiça brasileira. Enquadra-se como exemplo a rede social de mensageria instantânea, muito utilizada pelos brasileiros, chamada WhatsApp. Por algumas vezes, nos últimos três anos, houve determinação judicial para que essa plataforma fosse removida[73].

---

[70] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.54.

[71] Ativista norte-americano de ciberdireitos, professor da Harvard Law School, e fundador da Electronic Frontier Foundation (EFF), organização sem fins lucrativos, formada em 1990, para a defesa dos direitos e liberdades no mundo digital.

[72] BARLOW, John Perry. ‘Declaração de Independência do Cyberespaço’. **Revista Wired**, 1996. Disponível em: <https://www.wired.com/1996/06/declaration-independence-cyberspace/>. Acesso em: 24 dez. 2018.

[73] A primeira ordem judicial nesse sentido foi de 19 de fevereiro de 2015, quando o Juiz Luiz Moura Correia, da Central de Inquéritos da Comarca de Teresina-Piauí, ordenou aos provedores de acesso e conexão o bloqueio. Nessa ocasião, contudo, o aplicativo não saiu do ar, pois as próprias operadoras de internet impetraram um mandado de segurança perante o Tribunal de Justiça do Piauí e conseguiram cassar a ordem do juiz de primeira instância. Em 11 de dezembro de 2015, porém, a história foi diferente. A juíza Sandra Regina Nostre Marques, da 1ª Vara Criminal de São Bernardo do Campo-São Paulo, determinou aos principais provedores de internet o bloqueio do aplicativo. Os brasileiros então, pela primeira vez, experimentaram o dissabor de passar algumas poucas horas sem a ferramenta, até que o próprio WhatsApp Inc. impetrou mandado de segurança no Tribunal

Da mesma base em relação a essas decisões de bloqueio do WhatsApp, encontra-se a investigação de crimes como tráfico de drogas e organização criminosa e o reiterado descumprimento das ordens judiciais que determinam ao WhatsApp a entrega de dados necessários às investigações[74].

No contexto desses casos de bloqueio, salta aos olhos a atitude de desrespeito e descaso para com o Poder Judiciário brasileiro demonstrada pelas empresas WhatsApp e Facebook. Em um dos bloqueios, diante da ordem judicial[75] encaminhada ao Facebook do Brasil, sob pena de aplicação de multa coercitiva diária no valor de R$50.000,00, além de eventual configuração de crime de obstrução à Justiça e suspensão dos serviços até cumprimento da ordem judicial, a empresa se resumiu a encaminhar um email, escrito em inglês, o que gerou a manifestação da juíza do caso, Daniela Barbosa Assumpção de Souza, no seguinte sentido: "como se esta fosse a língua oficial deste país, em total desprezo às leis nacionais, inclusive porque se trata de empresa que possui estabelecida filial no

---

de Justiça de São Paulo e conseguiu reverter a decisão. O terceiro caso ocorreu na Comarca de Lagarto-Sergipe, quando o Juiz Marcel Maia Montalvão, após já ter até mesmo mandado prender o executivo do Facebook Brasil (ambas as empresas fazem parte do mesmo grupo econômico) por não cumprimento de ordem judicial, decidiu determinar o bloqueio do WhastApp. Novamente, a população amargou a experiência de permanecer algumas horas sem o venerado aplicativo. Esse segundo episódio de bloqueio também não durou muito. O Tribunal de Justiça de Sergipe cassou a ordem do Juiz de Lagarto, no Mandado de Segurança impetrado pelo WhatsApp Inc. A quarta e – até agora – última decisão nesse sentido, é de 19-07-2016. A juíza Daniela Barbosa Assumpção de Souza, da 2ª Vara Criminal de Duque de Caxias-RJ, determinou que os principais provedores de conexão à Internet bloqueassem a ferramenta. No mesmo dia, porém, tanto o Tribunal de Justiça do Rio de Janeiro, quanto o Supremo Tribunal Federal proferiram decisões ordenando o restabelecimento do WhatsApp no Brasil. A decisão do Supremo Tribunal Federal se deu através do seu Presidente, Ministro Ricardo Lewandowski, o qual deferiu pedido elaborado pelo Partido Popular Socialista (PPS) na Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 403/SE. No caso do Tribunal de Justiça do Rio de Janeiro, a ordem para suspender o bloqueio foi provocada pelo próprio WhatsApp, em Mandado de Segurança, e concedida pelo Desembargador Roberto Távora.

[74] A Lei n.9.296/1996, que cuida da interceptação de fluxo telefônico, informático e telemático, no Brasil, determina que não será admitida a interceptação de comunicações quando a prova puder ser feita por outros meios disponíveis (artigo 2º, II). Espera-se, portanto, que nos casos noticiados, não houvesse, realmente, outra maneira senão a de quebrar o sigilo perante o WhatsApp. Além disso, a temática exige, ainda, alterações na lei em comento, que cuida da interceptação de fluxo telefônico, informático e telemático, no Brasil, posto que essa remonta a uma época das sociedades das organizações na qual as detentoras de informações de interesse ao combate de crimes apenados com reclusão se restringiam apenas a "concessionárias de serviço público" (artigo 7º), o que não mais se verifica nos dias atuais, quando diversas empresas prestam serviços privados de comunicação e passam a ser repositórios de dados ocasionalmente almejados pela Justiça. Mas de toda forma, deve-se destacar que o bloqueio não parece ser a melhor forma para resolver este impasse em processos isolados, visto que não se soluciona, assim, a apuração do fato criminoso investigado e, também, não se resolve a postura do WhatsApp em não fornecer as informações. Nestes casos a única prejudicada, de fato, é a população.

[75] A decisão de Duque de Caxias inovou em relação às anteriores ao determinar especificamente a desabilitação da chave de criptografia. A juíza ressalta em sua decisão que: "não solicitou em momento algum o envio de mensagens pretéritas nem o armazenamento de dados [...]. Em verdade, o juízo requer, apenas, a desabilitação da chave de criptografia, com a interceptação do fluxo de dados, com o desvio em tempo real em uma das formas sugeridas pelo Ministério Público, além do encaminhamento das mensagens já recebidas pelo usuário e ainda não criptografadas, ou seja, as mensagens trocadas deverão ser desviadas em tempo real (na forma que se dá com a interceptação de conversações telefônicas), antes de implementada a criptografia".

Brasil e, portanto, sujeita às leis e à língua nacional, tratando o país como uma "republiqueta" com a qual parece estar acostumada a tratar".

Em todas as oportunidades nas quais o WhatsApp se manifestou nos processos que culminaram em ordem judicial para seu bloqueio, o discurso mantido foi o mesmo: não seria possível fornecer os dados telemáticos, na medida em que seria parte ilegítima para responder pelo pedido judicial, pois a empresa não está juridicamente estabelecida no Brasil (apesar do Facebook integrar o mesmo grupo econômico), e há inviabilidade técnica de acesso às mensagens privadas de seus usuários, ocasionada pela criptografia ponta-a-ponta implementada pelo aplicativo[76].

Esse aspecto faz lembrar que não à toa o Ministro do Superior Tribunal de Justiça, Luis Felipe Salomão, em decisão que também envolvia resistência a cumprir ordem judicial, por parte de um grande provedor de aplicação de internet, consignou que se o aplicativo criara "um monstro indomável, é apenas a ele que devem ser imputadas eventuais consequência geradas pela falta de controle" (Recurso Especial n. 1175676).

Portanto, a falta de colaboração da empresa com a Justiça nacional faz com que as palavras escritas na Declaração de Independência da Cibernética ainda ecoem com profusão. Ademais, desses episódios é possível inferir duas realidades: a primeira de que o WhatsApp parece ser um espaço inalcançável pelo Estado, e, a segunda, a constatação da necessidade e dependência criada pelos brasileiros em torno desse serviço.

O aplicativo de mensageria instantânea citado é apenas um exemplo dentre vários outros utilizados em massa pelos indivíduos, como redes sociais e inúmeros aplicativos que integram a vida contemporânea, movidos sob a engrenagem de algoritmos, e os quais revelam a insuficiência da atuação do direito aos meios tecnológicos, cujo assunto será abordado no próximo capítulo. Essa realidade cria um novo palco social e econômico, ao que chamamos de 'sociedade do hiper', a qual – por todas as suas características, conforme se verá a seguir – cria as

[76] O WhatsApp divulgou massivamente aos seus usuários o disclaimer "As mensagens que você enviar para este grupo agora são protegidas com criptografia de ponta-a-ponta, o que significa que elas não podem ser lidas ou ouvidas pelo WhatsApp ou por terceiros", de modo a blindar as comunicações que trafegam em suas redes. Essa tecnologia da criptografia ponta a ponta foi criada por Moxie Marlinspike, dono da Whisper System, empresa com a qual o WhatsApp fez sua parceria. A empresa acertou em trazer um mecanismo que garanta a privacidade de seus usuários, mas errou ao criar um controle que não lhe permite, segundo alega, desabilitar a criptografia implementada, o que foi feito por meio de empresa terceira, a qual, porém, submete-se à vontade e ordem de quem a contratou.

condições para a sociedade informacional também ser considerada como uma sociedade de dados.

1.3 A sociedade do *hiper*[77]

As relações cibernéticas vêm sendo estudadas sob novos ângulos. É o caso dos debates em torno da 'Ecologia das mídias'[78], conjunto de tecnologias de informação e comunicação e de todas as expressões culturais a que elas dão origem e forma[79]. Para Manuel Castells, nossos meios de comunicação são nossas metáforas, e assim o sendo – mediada e determinada pela comunicação – criam o conteúdo de nossa cultura, de modo que nossos sistemas de crenças e códigos historicamente produzidos são transformados de maneira fundamental pelo novo sistema tecnológico[80].

Segundo Willis Santiago Guerra Filho, na sociedade *hiper*complexa, encontramos uma crescente diversidade de culturas como até esse momento não havia constado em comparação a fases pretéritas:

> Nesta sociedade mundial em que vivemos, com sua hiper-complexidade e multicentralidade, tal como descrito pela teoria de sistemas sociais autopoiéticos, encontraremos uma crescente diversidade de culturas convergindo de forma sem paralelo em tempos passados. O que se segue é uma proposta de, primeiro, considerar um tal estado de coisas observando-o através do ponto de vista do atual estágio de diferenciação dos sistemas na sociedade multicultural que está em formação atualmente, e segundo, estimular o desenvolvimento de uma avaliação segundo o que podemos denominar uma abordagem crítica desconstrutivista[81].

A sociedade atual é, pois, formada por cidadãos inseridos nessa sociedade *hiper*complexa*,* capazes de gerar uma "inteligência coletiva", conforme designado por Pierre Levy, cuja condição de desenvolvimento é o próprio ciberespaço.

---

[77] A origem etmológica do prefixo 'hiper' vem do grego, *hyper*, e significa "posição superior, além, excesso".

[78] Segundo Henrique Garbellini Carnio, a "ecologia das mídias" consiste em um campo teórico bastante fértil e ainda não muito explorado no universo acadêmico. (CARNIO, Henrique Garbellini. Conhecimento e direito digital: acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos na Lei do Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo. **Marco civil da internet**. São Paulo: Atlas, 2014, p.259-260).

[79] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.13. Segundo a autora, essa tornou-se corrente a partir do momento em que passamos a viver numa sociedade "mediatizada" e "midiatizada".

[80] CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia, sociedade e cultura. v.1. São Paulo: Paz e Terra, 2011, p.414.

[81] GUERRA FILHO, Willis Santiago. Crise autoimunitária na autopoiese jurídica da sociedade mundial In: **Revista FMU Direito**, São Paulo, ano 27, n.39, 2013, p.144.

Segundo esse autor, o crescimento desse ambiente é impulsionado por três princípios: a interconexão, as comunidades virtuais e a inteligência coletiva[82].

A inteligência coletiva, formada por meio de uma cognição distribuída, marca a dinâmica da vida atual. A natureza do *hiper*texto é fruto da ruptura do leitor anterior. É dizer, a participação coletiva proporcionada pelo ciberespaço, integrando e conferindo vozes a todos os entes que lhe estão em torno, consiste em uma das características mais empolgantes e determinantes do que a internet é hoje. Conforme valorizado pelo racionalismo, a troca de informações e de conhecimentos consiste no principal motor do progresso e do conhecimento. E nesse sentido, verifica-se que "a rede valoriza a participação em comunidade de debate e de argumentação. [...] Encoraja uma forma de reciprocidade essencial nas relações humanas".

Para Lucia Santaella, a *hiper*sociabilidade como característica, produto dessa sociedade *hiper*complexa,

> significa tornar-se capaz de distinguir entre diferentes linguagens e mídias, suas naturezas comunicativas específicas, suas injunções político-sociais e, a partir disso, ter condições para desenvolver a capacidade de levantar perguntas acerca de tudo que lemos, vemos e escutamos.[83]

A cibercultura surge como solução parcial para os problemas da época anterior. Não obstante, constitui em si mesma um imenso campo de problemas e de conflitos para os quais nenhuma perspectiva de solução global conseguiu ser traçada claramente[84].

Outra característica inerente da cibercultura é o compasso com que as sobreposições de inovações são colocadas, fazendo o novo se tornar o antigo, chegando ao ostracismo. É o caso dos grupos de *chats* que inicialmente tomaram conta da internet, mas hoje já esquecidos. O email, por sua vez, vem sendo substituído paulatina, mas rapidamente, pelos programas de mensageria instantânea, como o WhatsApp e o Telegram. Há aqueles que já não mais utilizam o *email* no mundo profissional.

Segundo Luciano Floridi, vivemos uma profunda *revolução cultural*, porquanto as tecnologias da comunicação e informação estão afetando nosso senso como

---

[82] LEVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. 3.ed. Rio de Janeiro: Editora 34, 2010, p.129.
[83] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.13.
[84] Para aprofundar o assunto: LEVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. 3.ed. Rio de Janeiro: Editora 34, 2010, p.255.

indivíduos; como nos relacionamos uns com os outros, e como moldamos e interagimos com nosso mundo. A inquietação desse filósofo também está relacionada ao que virá depois de tantas recentes inovações no campo da tecnologia da informação – como nanotecnologia, internet das coisas, web 2.0, *cloud computing, smartphones*, *tablets*, GPS, drones, carros sem motorista, *wearable computing devices*, impressoras 3D, redes sociais e guerra cibernética, dentre outras[85].

Porém, independentemente das predições que possam ser feitas, uma conclusão parece estar bem próxima da certeza, segundo Lucia Santaella: "as tecnologias da inteligência vieram para ficar, crescer e se multiplicar, pois a inteligência, como a vida, não pode parar de crescer"[86]. Vivemos a era da *hiper*inteligência, aquela advinda não do humano mas de máquinas que 'aprendem' por si mesmas[87].

Ainda, segundo Jean Baudrillard, o virtual não é mais que uma *hipér*bole da tendência a passar do simbólico para o real e, nesse sentido, o virtual coincide com a noção de *hiper-realidade*:

> O virtual se opõe ao real, mas sua súbita emergência, pelo viés das novas tecnologias, dá a impressão de que, a partir de então, ele marca a eliminação, o fim desse real. Do meu ponto de vista, como já disse, fazer acontecer um mundo real é já produzi-lo, e o real jamais foi outra coisa senão uma forma de simulação. Podemos, certamente, pretender que exista um efeito de real, um efeito de verdade, um efeito de objetividade, mas o real, em si, não existe. [...] O virtual é o que está no lugar do real, é mesmo sua solução final na medida em que efetiva o mundo em sua realidade definitiva e, ao mesmo tempo, assinala sua dissolução[88].

Além disso, a sociedade do *hiper* também é a sociedade da *hiper*atividade, não imunológica, mas representação da massificação do positivo. O excesso de positividade, conforme tratou Byung-Chul Han em 'Sociedade do cansaço', está relacionado não apenas à *hiper*atividade, mas também à depressão e à síndrome de

---

[85] FLORIDI, Luciano. **The 4th Revolution**. How the infosphere is reshaping human reality. Oxford University Press: New York, 2010, p.vii.
[86] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.54.
[87] Sobre a hiperinteligência, ver as preocupações do filósofo Nick Bostrom sobre a emergência de máquinas mais inteligentes do que humanos em: BOSTROM, Nick. **Superintelligence**: paths, dangers and strategies. Oxford University Press: Nova Iorque, 2014.
[88] BAUDRILLARD, Jean. **Senhas**. Tradução de Maria Helena Kuhner da edição de 1929. Rio de Janeiro: Difel, 2007, p.41.

burnout[89]. Isso porque a violência neuronal escapa a toda ótica imunológica, pois não tem negatividade[90].

A isso relacionado, depara-se com a técnica temporal e de atenção *multitasking*, que não deixa de ser uma técnica de atenção, e a qual não se pode atribuir qualquer progresso civilizatório. Antes, é um retrocesso, que compromete desempenhos culturais e filosóficos da humanidade, os quais requerem atenção profunda e contemplatividade, ambos comprometidos pela *hiper*atenção. "Essa atenção dispersa se caracteriza por uma rápida mudança de foco entre diversas atividades, fontes informativas e processos"[91], comprometendo o processo criativo.

Dificilmente, hoje, um indivíduo se encontra em estado dedicado ao desempenho de uma tarefa única. Ao que parece, perdeu-se em algum momento a capacidade de se debruçar, horas a fio, sobre a leitura de um livro. Mais do que nunca, o indivíduo precisa de domínio próprio para poder findar o que se dispõe a fazer.

O comportamento e as características *hiper* do indivíduo atual também se devem ao fato de que o leitor é ubíquo, conforme se explicará adiante.

O leitor no ciberespaço tem uma postura mais 'ativa' do que o leitor em papel. Verifica-se um empoderamento do leitor que reverbera na escolha de suas fontes e de seus conteúdos. A audiência torna-se, portanto, mais seletiva. O espectador escolhe o que e quando irá assistir e ouvir. Ademais, rompe sua postura passiva e atinge o protagonismo de construir o hipertexto, por meio de *blogs,* redes sociais, comentários a notícias e outras formas de participação coletiva na rede. Nesse sentido, a tese de Fayga Silveira Bedê:

> Desde logo, é importante anteciparmos que a natureza virtual do hipertexto admite múltiplas e infinitas "dobras", devido à sua contextura aberta, de caráter interativo, que convida o leitor a uma espécie de co-autoria. Esse "leitor-autor", forjado pelo hipertexto, é levado a construir seu próprio itinerário, definindo o percurso que sua leitura irá tomar por meio das

[89] Para aprofundar as patologias vinculadas à era contemporânea e às tecnologias, ver: LORIOL, Marc. A sociological stance on fatigue and tiredness: social inequalities, norms and representation. In: **Neurophysiol clin**. 2017 Apr; 47(2):87-94. doi: 10.1016/j.neucli.2016.12.001. Epub 2017 Feb 2. Disponível em: <https://www.ncbi.nlm.nih.gov>. Acesso em: 22 ago. 2018; SCHAFFNER, AK. Exhaustion and the pathologization of modernity. In: **J Med Humanit**. 2016 Sep. Disponível em: <https://www.ncbi.nlm.nih.gov>. Acesso em: 25 ago. 2018. Nesse último artigo, o autor analisa seis casos de teorias da exaustão relacionadas às condições desde o início do século XVIII até o presente, explorando as formas nas quais George Cheyne, George Beard, Richard von Krafft-Ebing, Sigmund Freud, Alain Ehrenberg e Jonathan Crary usam ideias médicas sobre exaustão, além de trazer críticas culturais relacionadas a transformações sociais e tecnológicas específicas.

[90] HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.20-21.

[91] HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.33.

> sucessivas escolhas que ele se vê impelido a fazer, ao decidir-se sobre as "janelas" que irá – ou não – abrir; ao mesmo tempo em que é instado a participar ativamente do processo, emitindo a sua opinião sobre o que leu e ajudando o autor a compor a tessitura desse novo corpus textual[92].

O sistema de comunicação de massa da televisão, caracterizado pela existência de um controle centralizado, é alterado para um novo sistema globalizado e descentralizado, que afeta o comportamento das pessoas inseridas na cultura cibernética. Tudo é mais amplo e mais rápido, por meio de uma tecnologia que se transforma, e nisso há uma quebra epistemológica; é uma geração na qual todos são especialistas em tudo.[93]

Na era da internet surge a figura do *prosumer*, consumidor que reúne em si a figura de usuário que consome informações e, ao mesmo tempo, também as produz, por meio de sua divulgação e criação. É produtor e consumidor. Nesse sentido contribui Fabiano Menke:

> É a característica da denominada Web 2.0, em que o usuário da internet passa a ter um papel muito mais ativo, saindo de sua condição de mero visitante de sítios de notícias, por exemplo, para a de protagonista da criação de conteúdo, com a colaboração em massa, disseminação de informações e imagens[94].

Lucia Santaella propôs, em 2004, a existência de três tipos de leitores[95]. O primeiro é o *contemplativo*, atribuído ao leitor meditativo da idade pré-industrial, da era do livro impresso e da imagem expositiva. Caracterizado por exercer uma leitura individual, solitária e silenciosa, dentro de uma relação íntima que era estabelecida entre o leitor e o livro, no seu manuseio, na sua reflexão. Tratava-se de uma leitura, acima de tudo, contemplativa. Além disso, uma característica marcante desse leitor era ter diante de si objetos e signos duráveis, imóveis, manuseáveis e, frise-se, localizáveis, à altura da mão e do olhar, e, portanto, contínua e repetitivamente revisitados.

---

[92] BEDÊ, Fayga Silveira. ***Ciberintimidade***: a escrita de si na era digital. Tese de Doutorado. Universidade Federal do Ceará. Centro de Humanidades. Departamento de Ciências Sociais. Programa de Pós-graduação em Sociologia. Fortaleza, 2010, p.17.

[93] NICHOLS, Tom. The death of expertise. In: **The Federalist**, 17 jan. 2014. Disponível em: <http://thefederalist.com/2014/01/17/the-death-of-expertise/>. Acesso em: 10 out. 2018.

[94] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.205. O autor informa que a expressão *prosumer* já aparecia nos trabalhos de Alvin Toffler, 'The Third Wave' (1980) e mais recentemente em 'Revolutionary Schock' (2006).

[95] Segundo Lucia Santaella, o surgimento de um tipo de leitor não leva o anterior ao desaparecimento. Os três tipos coexistem. (SANTAELLA, Lucia. **Navegar no ciberespaço**. O perfil cognitivo do leitor imersivo. São Paulo: Paulus, 2004).

O segundo tipo de leitor é o *movente*, inserido no mundo em movimento e dinâmico. É o filho da Revolução Industrial e da explosão demográfica, quando o jornal se massificou e na época em que a fotografia e o cinema passaram a ocupar grande destaque, juntamente com o apogeu da televisão. Ou seja, época em que "as coisas se fragmentam sob efeito da velocidade, do transitório, do excessivo e da instabilidade que marcam o psiquismo humano com a exacerbação dos estímulos e a tensão nervosa". Os signos lhe estão ao entorno em todo momento e em todos os lugares nos grandes centros urbanos. Aqui o leitor é mais ágil, mas também mais fugaz; revela ainda uma memória mais curta.

O terceiro tipo de leitor indicado pela autora é o *imersivo*, cognitivamente em estado de prontidão. Não é linear. É capaz de dar saltos que vão de um fragmento a outro. É quem, portanto, estabelece a sua ordem informacional.

Da ruptura do leitor contemplativo para o ingresso na dinâmica do leitor movente e do imersivo, verifica-se a ocorrência do fenômeno da "civilização da imagem"[96]. Sobre esse assunto expõem Alberto Filipe Araújo e Maria Cecília Sanchez Teixeira:

> O quase desaparecimento da chamada "galáxia de Gutemberg" (McLuhan) a favor de uma sociedade da informação muito baseada nas imagens visuais, desde as mais simples até às de alta definição ou imagens de síntese, compromete grandemente a condensação de imagens na alma humana, desencadeadas pela contemplação da natureza (terra, ar, água, fogo), pela leitura dos grandes romances e dos grandes poemas, pela audição da música sacra, dos grandes compositores clássicos, bem como pelas imagens, muito ricas afectivamente, estimuladas pelos laços comunitários[97].

A digitalização do texto e a desmaterialização dos instrumentos que lhe dão suporte modificam um passado romântico[98] que vem se dissipando:

> Passamos a compreender, de forma mais significativa, por que leitura e escrita na era digital, comparadas à experiência analógica, implicam uma alienação do corpo, em suas potencialidades sensoriais, ficando reduzidas a uma atividade predominantemente visual e – em menor escala –

---

[96] DURAND, Gilbert. **O imaginário**: ensaio acerca das ciências e da filosofia da imagem. Rio de Janeiro: Difel, 2001, p.5.

[97] ARAÚJO, Alberto Filipe; TEIXEIRA Maria Cecília Sanchez. Gilbert Durand e a pedagogia do imaginário. In: **Revista Eletrônica PUC RS Letras de Hoje**. Porto Alegre, v.44, n.4, p.7-13, out.-dez. 2009. Disponível em: <http://revistaseletronicas.pucrs.br>. Acesso em: 23 jul. 2018, p.7.

[98] Assim, o caráter multissensorial da leitura "analógica" se intensifica, entre outras coisas, em razão de que o livro, sendo móvel, e de fácil transporte, tem a propriedade de "colar" à leitura de seu texto, a lembrança de pessoas, lugares, sons, paladares e aromas, cuja memória se vai confundindo num amálgama de afetos e sentidos. (BEDÊ, Fayga Silveira. **Ciberintimidade**: a escrita de si na era digital. Tese de Doutorado. Universidade Federal do Ceará. Centro de Humanidades. Departamento de Ciências Sociais. Programa de Pós-graduação em Sociologia. Fortaleza, 2010, p.25).

auditiva.[99]

Retomando a proposta progressiva dos diferentes leitores, Lucia Santaella, dez anos depois, dadas as profundas transformações pelas quais a cultura digital passou, revisita suas colocações e entende por bem acrescentar um quarto tipo de leitor, batizado de *ubíquo* e caracterizado por estar presente em qualquer tempo e lugar, uma nova condição de leitura e de cognição "que está fadada a trazer enormes desafios para a educação, desafios que estamos apenas começando a vislumbrar"[100].

O leitor ubíquo reúne partes dos leitores que o antecederam: ao mesmo tempo em que está corporalmente presente, perambulando e circulando pelos ambientes físicos, lendo todos os signos que são emitidos (movente), pode ao toque de um celular, penetrar no ciberespaço informacional e conversar reservadamente com alguém:

> O que o caracteriza é uma prontidão cognitiva ímpar para orientar-se entre nós e nexos multimídia, sem perder o controle da sua presença e do seu entorno no espaço físico em que está situado. Que tipo de mente, de sistema nervoso central, de controle motor, de economia da atenção está aí posto em ato? [...] a atenção responde ao mesmo tempo a distintos focos sem se demorar reflexivamente em nenhum deles. Ela é continuamente parcial[101].

O objeto *smartphone* contextualiza bem o cenário no qual está inserido o leitor ubíquo. Ao mesmo tempo em que ele o utiliza para falar e ouvir uma ligação telefônica, o aparelho também serve para trocar mensagens instantâneas, ler *sites* de jornais, ouvir música e checar *e-mails*, esteja o leitor na calma de seu quarto ou no agito de um metrô lotado em horário de pico.

Destas situações decorre que o leitor ubíquo, em vez de focar nos detalhes relevantes, "responde a uma pluralidade de estímulos em um ambiente informacional complexo e responde a eles por meio daquilo que é chamado de multitarefas"[102].

A condição do 'leitor' ser participativo e responsivo a uma pluralidade de estímulos tem como consequência a geração frenética e infindável de mais e mais

---

[99] BEDÊ, Fayga Silveira. **Ciberintimidade**: a escrita de si na era digital. Tese de Doutorado. Universidade Federal do Ceará. Centro de Humanidades. Departamento de Ciências Sociais. Programa de Pós-graduação em Sociologia. Fortaleza, 2010, p.26.

[100] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.277.

[101] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.277-279.

[102] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.280.

dados pessoais que são capturados e tratados para finalidades econômicas e políticas, fazendo com que a sociedade possa ser comparada a um panóptico digital, no qual gigantes da rede aprisionam usuários em controle e vigilância para fins econômicos, o que será visto com mais demora no próximo item.

1.4 Desconfiguração da ditadura do coração e o panóptico digital

Sob outra perspectiva, vive-se uma desconfiguração da *ditadura do coração* instaurada por Jean-Jacques Rousseau. A ideia de mostrar um homem em sua verdade natural intacta, em sua obra 'Confissões', aponta para uma revelação implacável do *coração*.[103]

A convocação por transparência, de Jean-Jacques Rousseau, aos seus semelhantes, representa uma mudança de paradigma, visto que no panorama social da época imperava o jogo de aparências. Segundo a análise de Byung-Chul Hang,

> o universo do século XVIII ainda era um teatro; estava repleto de cenas, máscaras e figuras. A própria moda era teatral; não havia diferença entre vestes do dia a dia e os trajes usados no teatro. Também as máscaras estavam na moda; era muito comum as pessoas se apaixonarem representando, criavam ilusões nas cenas. [...] Tanto homens quanto mulheres pintavam parte de seu rosto com tintas vermelhas. O próprio rosto se transformava em palco onde se representavam certas propriedades características com o auxílio de adesivos de beleza (*mouche)* [...] Também o corpo era lugar de representação cênica. Nisso não estava em questão dar expressão sincera ao ´interior´ oculto (*l´intérieur*), mas sim, o´coração´. Ao contrário, o que importava era jogar e brincar com a aparência, com ilusões cênicas[104].

É justamente contra esse jogo de papéis que Jean-Jacques Rousseau apoia seu discurso da moral de transparência[105], o qual acaba se transmutando em tirania e leva à violência: "a proibição do teatro e da mimética, já prescrita pelo próprio Platão para seu ideal de Estado, concede à sociedade da transparência de Rousseau um caráter totalitário"[106]. A exigência de Rousseau por transparência do coração é, portanto, um imperativo moral.

Avançando o olhar sobre a sociedade da transparência de Rousseau, verifica-se o binômio controle e vigilância como seu produto. Sua estima repousava

---

[103] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo. São Paulo: Vozes, 2017, p.98-99.
[104] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo. São Paulo: Vozes, 2017, p.99.
[105] Não à toa, se contrapõe ao teatro enquanto representação de um lugar de dissimulação, de aparência e sedução, onde faltaria toda e qualquer transparência. (HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.100).
[106] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.101.

sobre um estado natural de observância mútua. Ele deixou em seus registros o apreço por “aquele romano que desejava que sua casa fosse edificada de tal modo que todos pudessem ver o que ali se passasse”.[107]

Num salto para a sociedade atual, percebe-se que as edificações que nos servem são equacionadas para proporcionar a proteção e a segurança necessárias para o resguardo físico, criar um ninho de conforto e descanso ao corpo e ao espírito, na pseudosensação de *estar só*. Ao mesmo tempo, porém, são penetradas pelo *vento digital* da comunicação e da informação, expressão usada por Byung-Chul Han para indicar como a rede digital acaba tornando tudo transparente, abstraído, contudo, da submissão ao imperativo *moral,* que conduzia os anseios rousseaunianos:

> É de certo modo desprovida de *coração*, que do ponto de vista da tradição foi um *médium* metafísico-teológico da verdade. A transparência digital não é cardiográfica, mas pornográfica, produzindo também panópticos econômicos. Neles não se busca acentuar a moral do coração, mas maximizar lucros, chamar a atenção. A iluminação total promete, pois, *uma exploração máxima*[108].

Nesse contexto, não parece extravagante comparar o mundo cibernético (considerando todos os seus reflexos no mundo real) com o “panóptico” de Jeremy Bentham, conforme descreve Michel Foucault. A visão axial de todos os vigiados induz a “um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder”.[109] O panóptico, “é uma máquina de dissociar o para ver-ser-visto: no anel periférico, se é totalmente visto, sem nunca ver; na torre central, vê-se tudo, sem nunca ser visto”.[110]

Na segunda metade do século XX, essa visão sobre o panóptico foi revista. Segundo Byung-Chul Han, a exigência de transparência na sociedade contemporânea, presente por todo lado, “intensifica-se de tal modo que se torna um fetiche e um tema totalizante, remontando a uma mudança de paradigma que não se limita ao âmbito da política e da sociedade[111]”:

---

[107] Jean-Jacques Rousseau apud HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017.
[108] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.102-103.
[109] FOUCAULT, Michel. **Vigiar e punir**. 30.ed. Petrópolis: Vozes, 2005, p.166.
[110] FOUCAULT, Michel. **Vigiar e punir**. 30.ed. Petrópolis: Vozes, 2005, p.167.
[111] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.9.

> A sociedade da negatividade dá espaço a uma sociedade na qual vai se desconstruindo cada vez mais a negatividade em favor da positividade. Portanto, a sociedade da transparência vai se tornando uma sociedade positiva. As coisas se tornam transparentes quando eliminam de si toda e qualquer negatividade, quando se tornam rasas e planas, quando se encaixam sem qualquer resistência ao curso raso do capital, da comunicação e da informação. As ações se tornam transparentes quando se tornam operacionais, quando se subordinam, a um processo passível de cálculo, governo e controle[112].

Byung-Chul Han analisa as posições de Jean Baudrillard, que ponderou sobre o fim do espaço perspectivístico e do panóptico, a partir dos impactos absorvidos pela sociedade por meio do uso da televisão. Ele argumenta que não vivemos o final do panóptico, mas o começo de um novo: *o panóptico digital* do século XXI, esse de característica aperspectivística na medida em que sua eficiência está no fato de não ser mais vigiado por um centro, por não ser mais supervisionado pela "onipotência do olhar despótico"[113]: "A permeabilidade transparente aperspectivística é muito mais eficiente do que a supervisão perspectivística, visto que é possível ser iluminado e tornado transparente a partir de todos os lugares, por cada um".

Em outras palavras, a perspectividade corresponde à transparência ocorrida apenas unilateralmente, e que dá fundamento à estrutura de poder e domínio. Ao revés, na sociedade do controle atual, a aperspectividade não se encontra sob um comando central, a ponto de, no panóptico digital, os que ali estão imaginam, ilusoriamente, estar em total liberdade[114].

Os aprisionados do panóptico digital rompem a separação anterior e estabelecem comunicação mútua, ligados em redes, interagindo a todo momento, e construindo um hipertexto comum. Nesse sentido, Pierre Levy observa:

> O navegador pode se fazer autor de maneira mais profunda do que percorrendo uma rede preestabelecida: participando da estruturação do hipertexto, criando novas ligações. Enfim, os leitores podem não apenas modificar as ligações, mas igualmente acrescentar ou modificar textos, imagens etc., conectar um hiperdocumento a outro e fazer assim de dois hipertextos separados um único documento, ou traçar ligações hipertextuais entre uma série de documentos[115].

---

[112] HAN, Byung-Chul**. Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.9-10.
[113] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.106.
[114] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.107.
[115] LEVY, Pierre. **O que é o virtual?** Tradução de Paulo Neves. 2.ed. Rio de Janeiro: Editora 34, 2011, p.45.

Esse ambiente, na forma como se apresenta, é incomparável com sistemas mais antigos como os jornais impressos, as revistas, o rádio e a televisão, os quais não foram capazes de conferir ao indivíduo o atributo de participante e gerador direto de conteúdo. No panóptico digital, o habitante passa a ter outra postura, assumindo um papel ativo na hipercomunicação cibernética, na manutenção de uma rede hiperdinâmica e hiperinterconectada, na qual os indivíduos contribuem para a produção e a troca infindável de hiperinformações.

O sistema de comunicação de massa da televisão, caracterizado pela existência de um controle centralizado, é alterado para um novo sistema globalizado e descentralizado, afetando, consequentemente o comportamento das pessoas inseridas na cultura cibernética.

Ainda sobre o panóptico digital, sua especificidade repousa no fato de que seus sujeitos atuam em prol de sua edificação e manutenção, desnudando-se a si mesmos, e assim se expõem não por coação externa, mas a partir de uma necessidade gerada por si mesmo; “onde, portanto, o medo de renunciar à sua esfera privada e íntima dá lugar à necessidade de se expor à vista sem qualquer pudor”, dentro de uma sociedade de supervisão, onde todos controlam todos, degradando a sociedade da transparência a uma sociedade de controle desumana, cuja situação leva à uniformização, posto que o controle total aniquila a liberdade de ação.[116]

O alcance globalizado dos ventos digitais transforma o mundo em um único panóptico: “não existe um fora do panóptico; ele se torna total, não existindo muralha que possa separar o interior do exterior”. Gigantes da rede como Google e Facebook apresentam-se como espaços de liberdade, porém, adotam cada vez mais formas panópticas[117], a exemplo das revelações feitas por Edward Snowden, em 2013, sobre o projeto PRISM, cujo programa permitia à Agência Nacional de Segurança dos Estados Unidos (NSA) obter praticamente o que quisesse das empresas de internet, franqueando à agência acesso a seus servidores. Segundo as revelações,

[116] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.108-110.
[117] HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.115-116. O presidiário do panóptico digital é ao mesmo tempo agressor e vítima, e nisso é que reside a dialética da liberdade, que se apresenta como controle.

participavam desse programa empresas como Facebook, Google, Apple e Skype, dentre outras[118].

Não é demais lembrar que problemas com espionagem e gravações clandestinas não é algo recente. Em sua obra 'Lições de informática jurídica', Mario Losano, em 1974, já apontara que "os escândalos das gravações clandestinas nos USA e na Itália, por exemplo, são sintomas particularmente evidentes de uma subterrânea e bem mais ampla revolução informática"[119].

A circulação de dados pessoais que se dá pela exposição desnuda dos indivíduos, aliada ao controle panóptico das gigantes digitais, impõe a tarefa de pensar se deve haver limites, e, nesse caso, quais seriam, para as práticas ocorridas nessa esfera, abrindo a discussão para uma regulamentação na área de proteção de dados pessoais, especialmente dos dados pessoais obtidos por meio das tecnologias da informação e comunicação, dentro da área do direito digital[120].

Para Lucia Santaella, falar em privacidade na atual sociedade de vigilância desperta alertas de caráter individualista, de privacidade autocentrada, que lembram o lema burguês 'minha casa é o meu castelo', além de evocar visões dramatizadas de vitimização subjetiva[121].

Brandão e Suárez, em investigação das tecnologias da informação como mecanismo de controle no modelo deleuziano, expõem que na construção do controle se mantém as técnicas de vigilância (como uma panóptico exacerbado, de onde não se sabe quem é vigiado e quem vigia) e a sanção normalizadora (para corrigir o curso da anormalidade, o exame ainda é substituído pelo controle e testes contínuos). Não apenas os documentos determinam o assunto, mas os testes

---

[118] GREENWALD, Glenn. **Sem lugar para se esconder**. Tradução de Fernanda Abreu. Rio de Janeiro: Sextante, 2014, p.81-82. Segundo Brandão e Suárez, "Casos como el PRISM, revelado en el 2013 por el ex-contratado de CIA Edward Snowden y de la Directiva 24 del 2006 de Unión Europea demuestran la tentativa de ejercicio de control en estos nuevos medios de información. Ahí se ha demostrado una intrincada y muy tecnológica red de acompañamiento y captación de información, muchas veces privadas, de personas, autoridades, empresas y Estados. El PRISM fue construido por agencias de seguridad estadunidenses, con el supuesto objetivo de proteger la seguridad nacional de ese país, aunque haya sido utilizado con fines de logro de manutención del control ejercido por los Estados Unidos". (BRANDÃO, André Martins; SUÁREZ, Nuria Lopez Cabaleiro. Sociedad de información: la nueva topología del poder. In: (Orgs.) REY, Paula Requeijo; PISONERO, Carmen Gaona. **Contenidos inovador en la Universidad actual**. Madrid: McGraw-Hill, 2014, p.01.

[119] LOSANO, Mario G. **Lições de Informática jurídica**. São Paulo: Resenha Tributária, 1974.

[120] GUERRA FILHO, Willis Santiago; CARNIO, Henrique Garbellini. Metodologia jurídica político-constitucional e o Marco Civil da Internet: contribuição ao direito digital. In: DEL MASSO, Fabiano Dolenc; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio. **Marco Civil da Internet**. São Paulo: RT, 2014.

[121] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.71.

realizados continuamente[122]. Para esses autores, “en ese escenario los mass media y el marketing pasan a ser instrumentos de control social, el gigantesco flujo de información se encuentra en el centro de las estratégias”[123].

A sociedade da informação, com efeito, é composta de todas essas condições que lhe estão entorno: é uma sociedade de controle e vigilância voltada ao tratamento de dados pessoais, por cuja conjectura delinea a feição do que hoje também se pode chamar por ‘sociedade de dados’.

1.5 *Data is the new oil*

Em 06 de maio de 2017, o jornal ‘The Economist’ publicou matéria intitulada ‘The world´s most valuable resource is no longer oil, but data’[124] fazendo trocadilho com expressão que alguns atribuem ao matemático inglês Clive Humby (*data is the oil*), proferida em 2013. Apesar das diversas críticas objetivas que poderiam ser feitas a essa frase de efeito, fato é que dados pessoais nunca tiveram tanto valor. Os dados pessoais permitem desenvolver psicometria quanto ao perfilhamento de indivíduos, em aspectos que geram valor, a exemplo de hábitos de consumo e de preferências políticas.

Conforme a tecnologia avança, o mercado aposta cada vez mais no mundo de dados. Os dados pessoais passam a ser convertidos em *rankings,* cáculos de risco, *scores,* na esteira da datificação. Câmeras ficam mais baratas a cada dia, sensores estão embutidos cada vez mais em mais lugares, celulares rastreiam nossos movimentos, programas registram o que digitamos e para onde olhamos nas

---

[122] BRANDÃO, André Martins; SUÁREZ, Nuria Lopez Cabaleiro. Sociedad de información: la nueva topología del poder. In: (Orgs.) REY, Paula Requeijo; PISONERO, Carmen Gaona. **Contenidos inovador en la Universidad actual**. Madrid: McGraw-Hill, 2014, p.05.

[123] BRANDÃO, André Martins; SUÁREZ, Nuria Lopez Cabaleiro. Sociedad de información: la nueva topología del poder. In: (Orgs.) REY, Paula Requeijo; PISONERO, Carmen Gaona. **Contenidos inovador en la Universidad actual**. Madrid:McGraw-Hill, 2014, p.06. Ainda segundo esses autores, na análise do pensamento de Gilles Deleuze: “Por todo eso, importa decir que al hablar de la sociedad de información no se puede dejar de fijarse que ella es consecuencia de todas as sociedades anteriores y que no está descolgada de su contexto. Eso importa para hacernos ver que la sociedad de información es, en realidad, una sociedad de control de la información. Los modelos teoréticos de sociedad coexisten y se entrelazan. Y eso lo tenemos claro cuando pensamos en los conflictos que se están juridicizando. La relación entre Derecho & Tecnología transparece la lucha por poder en ese espacio libre, que Deleuze tan bien caracterizó, como la mar, de espacio liso. Esta topología dibuja la ametricidad de las multiplicidades de la red. Al ver la sociedad de información como un sistema rizomático queda más fácil comprehender como un otro espacio (paralelo) puede interactuar con este en una dinámica de intentar aprehender elementos uno del otro en un movimiento de disolución (del espacio estriado) y de estriamiento (del espacio liso). Es un analisis desarrollada bajo la obra de Gilles Deleuze que demuenstra, muy didacticamente, la topología y la dinámica de esta nueva configuración social que tanto buscamos compreender” (p.10).

[124] THE ECONOMIST. **The world´s most valuable resource is no longer oil, but data**. Publicado Em: 06 maio 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 10 ago. 2018.

telas, microfones de dispositivos gravam o que e com quem falamos, etc. E todo esse dilúvio de dados alimenta a máquina algorítmica, formando perfis com especificidades e profundidade até hoje sem precedentes. Muito embora existam leis sobre a proteção de dados, muitos desses dados estão perdidos na imensidão dos processamentos de algoritmos.

Não há dúvidas, de outro lado, que os dados pessoais criam um enorme valor para a economia mundial, e em usos lícitos, podem impulsionar a inovação, a produtividade, a eficiência e o crescimento econômico[125].

A imensidão de dados existente está atrelada, outrossim, à rotina do homem da era contemporânea, o qual utiliza uma enxurrada de aparelhos eletrônicos, ditos inteligentes, que capturam dados, os quais, por sua vez, são tratados por algoritmos:

> Uma das consequências mais claramente visíveis da informatização de muitos aspectos de nossa vida cotidiana é justamente a possibilidade de registro de muitos dos diversos atos que realizamos através de meios informatizados. Em um novo paradigma com o qual ainda não nos acostumamos completamente, muitos dos nossos atos que antes seriam efêmeros e gerariam consequências apenas imediatas ou previsíveis dentro de determinados padrões já pré-concebidos, passam a ser não apenas atos mas também informações que podem ser utilizadas por nós mesmos e, frequentemente, por terceiros – abrindo a possibilidade, neste caso, de serem utilizadas em um contexto diferente daquele no qual praticamos nossos atos e com finalidades também diversas, eventualmente fugindo ao nosso poder de previsão e controle.[126]

Os dados pessoais dos consumidores estão inseridos na dinâmica econômica atual. A publicidade comportamental, aquela direcionada segundo o perfil do consumidor, é o que move diversos modelos de negócios da internet. Quanto mais dados são coletados, maior será a quantidade de informação que poderá ser vendida aos anunciantes. Segundo explica Paula Sibilia:

> Assim, sem pedir dinheiro em troca, são oferecidos serviços cada vez mais fundamentais para os sujeitos contemporâneos: contas de correio eletrônico ou páginas nas redes sociais, espaço para armazenar ou compartilhar arquivos, bem como para publicar *sites* ou *blogs*, acesso ao conteúdo de revistas e jornais, sistemas de busca de informações, inclusive a própria conexão à internet. Mas, em todos esses casos, o produto comprado e vendido é ele: o consumidor[127].

---

[125] Sobre o benefício do uso de dados, ver: TENE, Omer. Big data for all: privacy and user control in the age of analytics. In: **Northwestern Journal of Technology and Intellectual Property** 239, 20 set. 2012, p.1-36; 6.

[126] BRASIL. Escola nacional de defesa do consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. (Coord.) DONEDA, Danilo. Brasília: SDE/DPDC, 2010, p.61.

[127] SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.35.

Disso decorre um deslocamento das referências na sociedade contemporânea. Segundo Paula Sibilia, o sujeito é definido cada vez menos em função do Estado-nação como território geopolítico no qual nasceu ou reside e cada vez mais em virtude do seu relacionamento com as corporações do mercado global[128].

Vivemos num contexto bastante diferente daquele que serviu de palco à sociedade moderna em seu apogeu industrial, conforme já visto nesse trabalho. Para Paula Sibilia, cabe supor que estão emergindo novos modos de subjetivação, distintos daqueles que produziram os corpos dóceis e úteis dos sujeitos disciplinados descritos por Michel Foucault, eis que o capitalismo contemporâneo se ergue sobre uma imensa capacidade de processamento digital e metaboliza as forças vitais com voracidade inaudita, lançando e relançando constantemente no mercado novos produtos, serviços e subjetividades[129].

Segundo a autora:

> De maneira crescente, a identificação do consumidor passa pelo seu perfil: uma série de dados sobre sua condição socioeconômica, seus hábitos e sua preferências de consumo. Todas essas informações se acumulam por meio do preenchimento de fichas de cadastro e formulários de pesquisas, que são processados digitalmente para serem armazenados em bancos de dados conectados em rede. Estes, por sua vez, serão acessados, vendidos, comprados e usados pelas empresas em suas estratégias de marketing. Desse modo o consumidor passa a ser, ele mesmo, um produto à venda[130].

O produto é o próprio usuário. Os ganhos na economia capitalista da sociedade de dados estão diretamente ligados à publicidade, a qual, segundo Jean Braudrillard, se revela como o mais notável meio de comunicação de massas de nossa época[131].

Nota-se, claramente, que o dado pessoal se transformou em insumo da produção, apresentando um papel tão relevante quanto a força de trabalho e o capital. Nessa dinâmica, o consumidor, figura mais vulnerável por definição, se fragiliza ainda mais, sendo predicado como ´consumidor de vidro´ para denotar sua tamanha fragilidade. Nesse sentido, Laura Schertel Mendes:

---

[128] SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.36.
[129] SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.34
[130] SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.35.
[131] BRAUDRILLARD, Jean. **A sociedade de consumo**. Lisboa: Edições 70, 2010, p.161

> A vulnerabilidade do consumidor nesse processo de coleta e tratamento de dados pessoais é tão patente que se cunhou a expressão 'consumidor de vidro' para denotar a sua extrema fragilidade e exposição no mercado de consumo, diante de inúmeras burocracias privadas que tomam decisões e influenciam as suas oportunidades, a partir das informações pessoais armazenadas em bancos de dados[132].

A sequência de cliques (*clickstream*), também denominado rastro de cliques compõe o registro da trajetória que um usuário percorre ao clicar em determinado local em página da internet. Esses dados são capturados por tecnologias como *cookies*[133] e passam a ser analisados com vista a entregar resultado informativo – muitas vezes por meio de venda (*data broker*)[134] – para pesquisas de mercado, produtividade de empregados e, especialmente, para publicidade comportamental[135].

Conhecer a magnitude e a lucratividade desse mercado de dados pessoais faz compreender as cifras de algumas operações societárias envolvendo agentes econômicos do mundo da internet, a exemplo do aplicativo Waze que foi adquirido pela empresa Google pelo valor de $1.3 bilhões de dólares em 2013, ou ainda o

---

[132] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.93. A expressão 'consumidor de vidro' é atribuída à Susanne Lace, autora de 'The glass consumer: life in a surveillance'. Society.Bristol-UK: Policy Press, 2005.

[133] Os *cookies* permitem o agrupamento de indivíduos em categorias predeterminadas; detentor das informações, gera o perigo de uma discriminação silenciosa e indevida com base nestes dados. Tudo sem qualquer participação do usuário. (SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2011, p.162).

[134] Um exemplo de empresa desse setor é a Drawbridge e a LiveRamp, comprada pela Acxiom. E o que essas empresas fazem? Segundo Martinez: "Ever notice how you seem to get served ads online for products you bought in physical stores? That's not because Facebook is eavesdropping on your phone. It's done via what's known as "data onboarding," where personal data like your name, address, or phone number (which retailers know through loyalty-card programs and the like) are converted into ways to target you online. Middlemen like LiveRamp join online with offline by buying your personal data and then working with publishers – email newsletters, dating sites – to identify your browser cookies. Don't sweat the details; the net of all this hackery is a table with your personal data plus a browser cookie or mobile device ID, which allows, say, a pharmacy chain that knows your phone number (which you entered at checkout to save 5 percent) to link all your purchases to your online presence". (MARTINEZ, Antonio Garcia. **Why California's privacy law won't hurt Facebook or Google in wired**. Disponível em: <https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google/>. Acesso em: 02 nov.2018). Tradução livre: Já percebeu como você parece receber anúncios on-line de produtos comprados em lojas físicas? Isso não é porque o Facebook está espionando o seu telefone. Isso é feito por meio do que é conhecido como "integração de dados", em que dados pessoais como nome, endereço ou número de telefone (que os varejistas conhecem por meio de programas de fidelidade e similares) são convertidos em maneiras de segmentar você on-line. Intermediários como o LiveRamp se conectam on-line off-line, comprando seus dados pessoais e trabalhando com editores – boletins informativos por e-mail, sites de encontros – para identificar os cookies do seu navegador. Não se preocupe com os detalhes; a rede de toda essa pirataria é uma tabela com seus dados pessoais, além de um cookie de navegador ou ID de dispositivo móvel, que permite, digamos, uma rede de farmácias que conheçam seu número de telefone (que você digitou no checkout para economizar 5%) compras para sua presença online.

[135] Sobre as empresas Google e Facebook, Eli Pariser afirma: "a questão é que a base dos dois negócios é essencialmente a mesma: publicidade direcionada, altamente relevante. Os anúncios contextuais que o Google coloca ao lado dos resultados de pesquisas e em sites são sua única fonte significativa de lucro. E, embora as finanças do Facebook não sejam reveladas ao público, alguns insiders já deixaram claro que a publicidade está no âmago dos rendimentos da empresa. [...] Os dois competem pelos mesmos dólares advindos da publicidade". (PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012, p.41).

Instagram adquirido pelo Facebook pelo montante de U$1 bilhão de dólares em 2012, e mais recentemente, a compra do WhatsApp pelo Facebook pela quantia de $22 bilhões de dólares.

São operações de compras bilionárias referentes a empresas que oferecem serviços *gratuitos*. Isso se explica pelo *zero-price advertisement business model*, por meio do qual os usuários podem utilizar os serviços online gratuitamente, mas em troca permitem que seus dados pessoais sejam capturados e utilizados na venda para anunciantes que direcionarão com mais eficiência a publicidade ao consumidor.

Não à toa na sociedade da informação há um excesso de estímulos, informações e impulsos[136], com o que se relaciona diretamente a atual economia da atenção. Quanto mais atenção se obtém do usuário, mais navegação (rastro de cliques) e, portanto, mais oportunidades de captação de dados.

Além disso, no momento atual, as próprias pessoas não se importam em fornecer dados e informações sobre si mesmas[137]. A todo tempo, experiências, lugares e situações diversas em geral são postados, como registro da "vida social". Segundo Alessandra Parente, "do oráculo Google ao confessionário Facebook, somente alguns escapam à entrega de segredos íntimos às máquinas e, consequentemente, aos interesses das maiores corporações do universo contemporâneo"[138].

São aplicadas no mercado diversas técnicas aptas a utilizar *business intelligence* sobre essa matéria-prima de dados, permitindo a obtenção de diversos tipos de informações sobre os indivíduos a partir dos perfis virtuais. Nesse sentido são as palavras de Laura Schertel Mendes:

> A combinação de diversas técnicas automatizadas permite a obtenção de informações sensíveis sobre os cidadãos e a construção de verdadeiros perfis virtuais, que passam a fundamentar a tomada de decisões econômicas, políticas e sociais[139].

É fato que a vida imersa e conectada a aparelhos de tecnologia da informação implica na entrega de dados pessoais o tempo todo. Faz parte do cotidiano; atraídos por benefícios de diversas dimensões, o indivíduo concorda, com facilidade, em ceder dados relativos à sua vida. Esse emaranhado de dados

---

[136] HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017, p.31.
[137] O tema será aprofundado no capítulo 4.
[138] PARENTE, Alessandra. **Cibernética e neoliberalismo**: a crítica como mercadoria. (No prelo), p.3.
[139] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.22.

informados possibilita empresas especializadas na elaboração de estatísticas gerar perfis e percentuais relacionados aos hábitos e às preferências dos indivíduos. A massa de dados aumenta e sofistica campanhas publicitárias, as quais serão dirigidas para aqueles clientes que se moldem às características do produto ou do serviço anunciado. O *big data*, tema que será aprofundado mais adiante, possibilita que a engrenagem do mercado de dados se mantenha sempre funcionando.

Os dados computadorizados, antes medidos em bits e bytes, agora são medidos em teras, petas e zetas. A empresa Google processa mais de 24 petabytes de dados por dia, um volume que representa mil vezes a totalidade de material impresso acumulado até hoje pela Biblioteca do Congresso dos Estados Unidos. Pela rede social Facebook são postadas mais de dez milhões de novas fotos a cada hora, e o botão "curtir" dessa rede social é acionada quase três milhões de vezes por dia, de modo que todos esses movimentos (*clickstream*) acabam por gerar um imenso material de dados que serão trabalhados para identificar as preferências de cada indivíduo[140].

Se por um lado a identificação do perfil da pessoa pode gerar certo conforto ao consumidor em sua navegação e durante as compras virtuais, de outro lado, os mesmos dados que geram o conteúdo personalizado podem ser usados por marqueteiros para descobrir e manipular os pontos fracos pessoais. Segundo Eli Parisier, essa não é uma possibilidade hipotética: a pesquisadora da privacidade Pam Dixon descobriu que uma empresa de dados chamada PK List Management oferece uma lista de ´compradores impulsivos´; as pessoas incluídas na lista são descritas como altamente suscetíveis a ofertas apresentadas como prêmios. E provoca o autor: se a persuasão personalizada funciona no caso de produtos, também pode funcionar com ideias[141].

Stefano Rodotà utiliza a expressão "esquizofrenia tecnológica", referindo-se à concomitância de uma expansão dos direitos na esfera pública a uma redução na esfera privada: "si accentua così non la consapevolezza della natura bifronte della tecnologia, ma la schizofrenia tecnologica[142]".

---

[140] Dados obtidos em: MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. **Big data**. La revolución de los datos masivos. Tradução de Antonio Iriarte. Madri: Turner, 2013, p.7.

[141] PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012, p. 111: "Essas empresas estão ficando cada vez melhores no uso desses dados para traçar estratégias. No entanto, muitas vezes acreditamos excessivamente que essas empresas irão cuidar bem dessas informações e, quando nossos dados são usados para tomar decisões que nos afetam negativamente, em geral não ficamos sabendo. Em última análise, a bolha dos filtros pode afetar a nossa capacidade de decidir como queremos viver".

[142] RODOTÀ, Stefano. **Il mondo nella rete**. Quali i diritti, quali i vincoli. Roma-Italia: Laterza, 2014, p.7.

Recentemente, a imprensa divulgou a assinatura de um acordo fechado entre o Google e a Mastercard que permitiria ao buscador obter informações sobre vendas nos Estados Unidos realizadas com os cartões de crédito da bandeira. Com esses dados, o Google e as varejistas seriam capazes, por meio de algoritmos, de cruzar informações de dados pessoais com os cliques em anúncios *online*, dando uma ideia da taxa de conversão da publicidade. O mais grave é que, segundo a notícia, os 2 milhões de clientes da Mastercard não sabiam desse rastreamento, pois as companhias nunca revelaram a parceria ao público[143].

A enorme quantidade de dados pessoais processada por algoritmos – cujo tema será aprofundado no próximo capítulo – faz com que vivamos sob a ditadura do *taste profile.* Segundo Parisier, "os algoritmos que orquestram a nossa publicidade estão começando a orquestrar nossa vida"[144]. Em artigo publicado em *El Pais*, Verdu esclarece como a rotina contemporânea do ser humano acarreta em elevada produção de dados pessoais, e como as empresas, munidas de algoritmos captam e trabalham com os dados coletados. Além disso, esse artigo demonstra como as sugestões de plataformas como Netflix e Spotify elevam o risco de homogeneização da identidade:

> Às segundas-feiras pela manhã, os usuários do Spotify recebem uma lista personalizada de músicas que lhes permite descobrir novidades. Assim como os sistemas de recomendação da Amazon, Google, eBay e Facebook, este cérebro artificial consegue traçar um retrato automatizado do gosto de seus assinantes e constrói uma máquina de sugestões que não costuma falhar. O sistema se baseia em um algoritmo cuja evolução e usos aplicados ao consumo cultural são infinitos. De fato, plataformas de *streaming* cinematográfico como o Netflix começam a desenhar suas séries de sucesso como House of Cards rastreando o *big data* gerado por todos os movimentos dos usuários para analisar o que os satisfaz. O algoritmo constrói assim um universo cultural adequado e complacente com o gosto do consumidor, que pode avançar até chegar sempre a lugares reconhecíveis.
>
> Seu sistema de recomendação – talvez o mais avançado do mercado – se baseia em nossas buscas, a que gêneros as associamos, que significa para nós jazz ou soul ou a que horas e dias do ano damos play em determinadas músicas. O resultado é tão díspar que às vezes é impossível que um algoritmo relacione Don Cherry a Ornette Coleman (meus heróis musicais) com La Chatunga de Luis Aguilé (a arrebatada seleção da minha sogra na festa de São João Batista). A maioria dos sistemas simplesmente omite esse elemento discordante e começa a fechar o cerco do gosto em torno do mais óbvio – tipo "se gostou de x, gostará de y" – ao mais solicitado – no caso de recorrer a buscas similares de outros usuários. O Spotify conseguiu estabelecer um círculo que inclui essa canção dissonante e que esboça

[143] BERGEN, Mark; SURANE, Jennifer. **Google and mastercard cut a secret ad deal to track retail sales**. Publicado em: 30 ago. 2018. Disponível em: <https://www.bloomberg.com/>. Acesso em: 05 set. 2018.
[144] PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012, p.11.

> como, pouco a pouco, a inteligência artificial poderá superar o código e ser capaz de aprender por si mesma[145].

Dados pessoais consistem nas novas coordenadas de modelagem social, isso porque extratos do *big data* ameaçam tornar-se a base sobre a qual os indivíduos são classificados, avaliados, recompensados ou punidos. Essas mesmas categorias podem ser usadas para avaliar os méritos e as necessidades dos indivíduos, ou as oportunidades a que estão sujeitos. É a lição de Peter Burgess, Luciano Floridi, Aurélie Pols e Jeroen van Hoven:

> In this view of 'data-driven governance', the question arises whether the individual human person as a legal subject has a future and how one can ensure that individuals are not viewed only as temporary data aggregates exploitable on an industrial scale rather than subjects in their own right. Interactions based on algorithmic profiling may exacerbate information imbalances between decision-making governments and companies on the one hand and individuals on the other hand. As a result, 'data-rich' public and private organisations will have greater ethical responsibilities towards citizens and customers. Digital ethics must identify new perspectives, potential and boundaries for dealing with data ethically, by formulating the terms of a proactive approach to ethics, beyond mere legal avoidance measures. As such it will set out the terms of a social innovation that parallels the rapid technological innovation we are experiencing on a daily basis[146].

O processamento onipresente de dados decorre da relação de dependência entre o homem e a tecnologia e descreve o fenômeno *ubicomp*, que vem de *ubiquitous computing*[147], termo utilizado para descrever a presença constante da informática no cotidiano das pessoas, de forma tão natural que se torna imperceptível, e de modo a compor quase todas as áreas da vida do indivíduo.

---

[145] VERDÚ, Daniel. **EL País**. O gosto na era do algoritmo. Disponível em: <https://brasil.elpais.com/brasil/2016/07/07/cultura/1467898058_835206.html>. Acesso em: 26 ago. 2018.

[146] BURGESS, Peter; FLORIDI, Luciano; POLS, Aurélie; HOVEN, Jeroen van. **Ethics advisory group**. Towards a digital ethics. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf>. Acesso em: 18 nov. 2018, p.21. Tradução livre: Nessa visão de "governança orientada por dados", surge a questão de saber se a pessoa humana como sujeito de direito tem futuro e como pode garantir que os indivíduos não sejam vistos apenas como agregados de dados temporários exploráveis em escala industrial, em vez de sujeitos em seus próprios direitos. Interações baseadas em perfis algorítmicos podem exacerbar desequilíbrios de informação entre governos e empresas tomadores de decisão, de um lado, e indivíduos, de outro. Como resultado, organizações públicas e privadas "ricas em dados" terão maiores responsabilidades éticas em relação a cidadãos e clientes. A ética digital deve identificar novas perspectivas, potencialidades e limites para lidar com dados eticamente, formulando os termos de uma abordagem proativa à ética, além de medidas legais. Como tal, definirá os termos de uma inovação social que se assemelha à rápida inovação tecnológica que estamos experimentando diariamente.

[147] O termo foi cunhado pelo cientista de informática norte-americano Mark Weiser, em 1988, e publicado em 1991 em 'The Computer for the 21st Century'. Segundo Laura Schertel Mendes, os exemplos de ubiquidade são inúmeros: redes sociais (Facebook e outros), *sites* de produção de conhecimento com estrutura colaborativa (Wikipedia), *cloud computing*, publicidade comportamental, etiqueta RFID, IOT etc. (MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.78-79).

O principal efeito do fenômeno da ubiquidade da tecnologia da informação é o desequilíbrio de poderes entre o indivíduo e os organismos que processam os dados pessoais e a consequente perda de controle individual sobre o fluxo de seus dados. Verifica-se assim que esse novo cenário altera o pressuposto central no qual se baseia o conceito clássico de dados pessoais – conforme se verá no terceiro capítulo – que é a possibilidade do indivíduo de efetivamente controlar o fluxo dos dados pessoais na sociedade[148].

Existe uma convergência entre a sociedade da informação e a sociedade contemporânea de consumo, porquanto a economia passa a exigir uma quantidade enorme de dados pessoais, para o seu complexo funcionamento[149]. Para além do consumo, verificamos que a sociedade da informação desemboca no que se pode chamar de sociedade de dados, esta não substituindo aquela, mas coexistindo em uma nova dinâmica comparada à fase anterior ao surgimento do processamento de dados computacional.

É possível afirmar que os dados pessoais ganharam nova dimensão com a consagração do *big data* e *data mining*, e de tudo que lhes está em torno, como a internet das coisas, o uso de algoritmos, a inteligência artificial e o *machine learning*. Com o aumento da coleta de dados e a capacidade de processamento e armazenamento computacional, grandes quantidades de dados podem ser rastreadas e avaliadas usando algoritmos de padrão e contexto. Diante dessa realidade, necessário recortar para aprofundar os temas mencionados, antes de seguir ao assunto da proteção de dados pessoais inserido na cultura do algoritmo.

[148] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.78-79.
[149] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.89.

2 AS TECNOLOGIAS DA SOCIEDADE DE DADOS E O DESAFIO DE SUA REGULAÇÃO

> With enough data, the numbers speak for themselves
> **Chris Anderson (1961 -)**

2.1 Dilema de causalidade: dados e tecnologia

Conforme visto no capítulo anterior, a sociedade informacional revela-se, também, em uma sociedade de dados, na qual o mercado de atenção – mediante a incessante produção de dados pessois – consiste na nova engrenagem da economia. Esse cenário apenas é possível em virtude das novas tecnologias surgidas ao longo das últimas décadas. Em verdade, existe aqui um dilema de causalidade, qual seja, se as recentes tecnologias da informação que elevam exponencialmente a produção de dados pessoais ou se a imensidão de dados disponíveis é que favorece o advento destas tecnologias por serem convidativas à criação de novos negócios lastreados em dados. Seja como for, entendemos necessário percorrer as tecnologias que integram esse ecossistema.

Passado o tempo do computador como grande inovação, Omer Tene[150] sugere quais são as novas tecnologias mais significativas que desafiam a atual estrutura de regulação jurídica, geram discussões sobre a necessidade de soluções inovadoras para as relações sociais e, em especial, chamam a atenção para questões ligadas à proteção de dados e à privacidade.

A primeira delas é a internet, com a ressalva do autor de que seria estranho predicá-la de *nova* tecnologia, tendo em vista seu tempo de existência desde o protocolo *world wide web*, portanto, já enraizada na política, na cultura e na economia atuais.

A segunda tecnologia destacada nesse sentido é a *cloud computing* – uma metáfora[151] – cuja tradução literal seria 'computação em nuvem'. Ela determina o movimento de empresas e indivíduos que passaram a armazenar dados e

---

[150] TENE, Omer. Privacy: the new generations. **International Data Privacy Law**, 2011. v.1, n.1, p.15-27. Disponível em: <https://papers.ssrn.com/>. Acesso em: 08 ago. 2018.

[151] Um aspecto importante dessa metáfora reside no fato de que ela nos transmite a noção de indeterminação geográfica. (SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.43).

serviços[152] em servidores remotos (‘em nuvem’), ao invés de guardá-los em computadores locais. Embora não unânime, esse formato de armazenamento se justifica por questões de custo e de segurança, em que pese poder colocar a privacidade sob maior risco.

A expressão ‘computação em nuvem’ virou moda a partir de 2008. Não se trata, entretanto, de um conceito novo, uma vez que remonta em alguns aspectos ao tempo da computação com *mainframes* grandes que fazem o trabalho de computação para usuários remotos nas estações de trabalho[153].

Em seguida, Omer Tene destaca a tecnologia *behavioral targeting* também designada por *behavioral advertising*. Em português, o conceito é mais conhecido e utilizado pela expressão publicidade comportamental.

Por meio da publicidade comportamental, dados são capturados e processados de maneira a gerar valor para anunciantes que poderão direcionar seus anúncios com maiores chances de chamar o interesse do consumidor:

> A publicidade comportamental utiliza-se, naturalmente, de informações sobre o comportamento de uma pessoa para que lhe seja especificado o tipo de abordagem que seria o mais adequado. Hoje, com a grande penetração da rede internet, uma das fontes de dados mais visadas para a obtenção de dados que permitem estabelecer o “perfil” de um consumidor a partir do seu comportamento é justamente o conjunto de hábitos de sua navegação na internet [154].

Sem embargo, quanto mais personalizado um anúncio, maiores as chances de conversão em “clique” por parte do internauta consumidor, o que é designado por CTR (*clickthrough rate*).

A utilização da técnica de *behavioral advertising* gera a cumulação[155] de informações sobre um determinado indivíduo, contendo dados relevantes, de

---

[152] No original: “‘Cloud services’ include both business-to-consumer tools, such as e-mail, instant messaging, and photo sharing services; and business-to-business applications, such as customer relationship management (CRM) and enterprise resource planning (ERP) software (software as a service, or SaaS); computing platforms offered as a service to facilitate low cost, rapid development and hosting of third party web service applications (platform as a service, or PaaS)”. (TENE, Omer. Privacy: the new generations. **International Data Privacy Law**, 2011. v.1, n.1, p.15-27. Disponível em: <https://papers.ssrn.com/>. Acesso em: 08 ago. 2018, p.16). Tradução livre: “Serviços de nuvem” incluem tanto ferramentas de negócios para consumidores, como serviços de e-mail, mensagens instantâneas e compartilhamento de fotos; aplicativos business-to-business, gerenciamento de relacionamento com o cliente (CRM) e software de planejamento de recursos empresariais (ERP) (software como serviço ou SaaS); plataformas de computação oferecidas como um serviço para facilitar o baixo custo, o rápido desenvolvimento e a hospedagem de aplicativos de serviço da web de terceiros (plataforma como serviço ou PaaS).

[153] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.43.

[154] BRASIL. Escola nacional de defesa do consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. (Coord.) DONEDA, Danilo. Brasília: SDE/DPDC, 2010, p.62.

[155] No original: “The application of privacy laws to behavioural targeting platforms may strain the definition of ‘personal data’. Most tracking technologies gather information through the use of ‘cookies’, which are stored on

natureza comercial e não comercial, que podem trazer sérias implicações à privacidade, desafiando a aplicação dos princípios da transparência e do livre consentimento.

Adicionamos à lista de Omer Tene, outras tecnologias ligadas à *tracking* capazes de monitorar situações inesperadas. O artigo publicado na Revista Wired[156] intitulado 'Como bloquear os sinais ultrassônicos que você não sabia que estavam lhe rastreando' dá notícias da tecnologia chamada *ultrassonic cross-device tracking* a qual incorpora tons de alta frequência, inaudíveis para humanos, em propagandas, *web pages*, e até mesmo em lojas físicas.

Estes *beacons* ultrassônicos emitem sequências de áudio com a função *speaker.* Na prática, qualquer microfone de dispositivo pode detectar o sinal e agregar uma figura de um anúncio visto pelo indivíduo, dos *sites* por ele examinados e até onde esteve. Segundo o pesquisador da University College London, Vasilios Mavroudis, ouvido na reportagem, a maior preocupação com essa tecnologia é a necessidade de capacitar o aplicativo para ouvir tudo em torno da pessoa.

A Federal Trade Comission (FTC) avaliou a tecnologia do rastreamento ultrassônico no final de 2015 e emitiu um comunicado[157], em março de 2016,

---

users' browsers and assigned random identifying numbers. Given that such identifiers are not connected in any way to users' offline identities or even IP addresses, it is not clear whether information stored on cookies constitutes 'personal data' at all. In recent years, online ad networks, and in some cases even Internet service providers, have begun to implement a technique known as deep packet inspection (DPI), formerly restricted to national security organizations, to monitor the content of Internet communications for users' interests and preferences. While DPI may have positive uses, such as cyber-security and network management, it also encroaches on users' privacy and raises the spectre of covert surveillance. Indeed, civil liberties groups have argued that such activity may run foul of wiretapping laws. At the same time, companies that use DPI for ad targeting argue that the matching of random identifiers with user interests does not involve the use of personal data. Yet, this distinction has arguably become irrelevant, given that advertisers who can track users pervasively often do not care about and have no interest in knowing such users' names or specific identity". (TENE, Omer. Privacy: the new generations. **International Data Privacy Law**, 2011, v.1, n.1, p.16-17). Tradução livre: 'A aplicação de leis de privacidade a plataformas de segmentação comportamental pode prejudicar a definição de' dados pessoais '. A maioria das tecnologias de rastreamento coleta informações por meio do uso de "cookies", que são armazenados nos navegadores dos usuários e recebem números de identificação aleatórios. Como esses identificadores não estão conectados de forma alguma às identidades off-line dos usuários ou até mesmo aos endereços IP, não está claro se as informações armazenadas nos cookies constituem "dados pessoais". Nos últimos anos, as redes de anúncios online e, em alguns casos, até os provedores de serviços de Internet começaram a implementar uma técnica conhecida como DPI (*Deep Packet Inspection),* anteriormente restrita a organizações de segurança nacional, para monitorar o conteúdo das comunicações da Internet para os interesses dos usuários e preferências. Embora o DPI possa ter usos positivos, como segurança cibernética e gerenciamento de rede, ele também invade a privacidade dos usuários e aumenta o espectro da vigilância encoberta. De fato, grupos de liberdades civis argumentaram que tal atividade pode violar as leis de escutas telefônicas. Ao mesmo tempo, as empresas que usam DPI para segmentação de anúncios argumentam que a correspondência de identificadores aleatórios com interesses de usuários não envolve o uso de dados pessoais. No entanto, essa distinção se tornou irrelevante, uma vez que os anunciantes que podem rastrear os usuários de maneira geral não se importam e não têm interesse em conhecer os nomes ou a identidade específica de tais usuários.

[156] WIRED. **How to block the ultrasonic signals you didn't know were tracking you**. Disponível em: <https://www.wired.com>. Acesso em: 07 nov. 2016.

[157] Conforme a FTC explica em seu comunicado: "This functionality is designed to run silently in the background, even while the user is not actively using the application. Using this technology, Silverpush could generate a

alertando empresas que utilizam a função de *áudio beacon*, desenvolvida pela empresa Silverpush, capaz de, potencialmente, rastrear o telespectador que estiver assistindo televisão, sem o seu conhecimento. A FTC alertou sobre a possível infração à Seção 5 do FTC Act, que proíbe atos ou práticas desleais ou enganosas no comércio. A FTC encoraja as empresas que utilizam dessa tecnologia a revelar a adoção dessa prática aos consumidores, capacitando-os a tomar uma decisão informada sobre quais informações devem ser divulgadas em troca do uso de sua aplicação. Por fim, a FTC informa que continuará monitorando o uso do *áudio beacon* na aplicação da empresa. Provavelmente, elas continuarão a usar a tecnologia uma vez que a FTC apenas alertou que o consumidor deve ser previamente informado sobre o uso do recurso[158]. Se ele souber e permitir o monitoramento, não haverá ressalvas.

Outra tecnologia destacada por Omer Tene é o *mobile data processing*. Os aparelhos móveis se popularizaram. Espera-se que até 2019 o número de celulares, no mundo, alcance a marca de 4.68 billhões[159], sem considerar outros aparelhos como *tablets, smart watches*, *netbooks* e *laptops*, todos capazes de se conectar à internet. Os *devices* portáteis estão, nas palavras de Omer Tene, tornando-se o principal método de acesso à internet. Além de transformar o mundo da computação e das comunicações, o celular levanta questões exclusivas de privacidade que representam novos desafios para o ordenamento[160].

---

detailed log of the television content viewed while a user's mobile phone was turned on". E ainda "your application requires permission to access the mobile device's microphone prior to install, despite no evident functionality in the application that would require such access". (UNITED STATES OF AMERICA. **Federal Trade Commission**. Disponível em: <https://www.ftc.gov>. Acesso em: 07 nov. 2016). Tradução livre: Essa funcionalidade foi projetada para ser executada silenciosamente em segundo plano, mesmo quando o usuário não está usando ativamente o aplicativo. Usando essa tecnologia, o Silverpush poderia gerar um registro detalhado do conteúdo da televisão visualizado enquanto o celular do usuário estava ligado. E ainda: "seu aplicativo requer permissão para acessar o microfone do dispositivo móvel antes da instalação, apesar de nenhuma funcionalidade evidente no aplicativo exigir esse acesso".

[158] Um pedido de patente (U.S. PATENT APPLICATION N.14/985089) depositado pelo Facebook, explora o uso do microfone do telefone para identificar os programas de televisão assistidos por determinado indivíduo e se os anúncios foram silenciados. Essa patente também se propõe a usar o padrão de interferência elétrica criado pelo cabo de alimentação para adivinhar qual programa está sendo reproduzido. Íntegra do pedido de patente no *site*. (Disponível em: <https://patents.google.com/patent/US20170195435A1/en>. Acesso em: 28 nov. 2018).

[159] Disponível em: <https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/>. Acesso em: 28 out. 2018.

[160] No original: "becoming the primary method of accessing the Internet. Beyond transforming the world of computing and communications, mobile raises unique privacy issues that pose further challenges to the Current Framework". (TENE, Omer. Privacy: the new generations. **International Data Privacy Law**, 2011. v.1, n.1, p.15-27. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1710688>. Acesso em: 08 ago. 2018). Tradução livre: Tornar-se o principal método de acesso à internet. Além de transformar o mundo da computação e das comunicações, o celular levanta questões exclusivas de privacidade que representam novos desafios para a Estrutura Atual.

Há, ainda, tecnologias de rastreamento de localização, incluindo o sistema de posicionamento global (*global positioning system*-GPS), triangulação por torres de telefonia celular, posicionamento sem fio e localização de IP, que abrem caminho para diversos aplicativos e serviços, como localizar amigos próximos, encontrar restaurantes recomendados, *check-in* em locais para receber descontos e cupons e obter relatórios de tráfego atualizados. Porém, muitos indivíduos podem não estar cientes de que a localização de seu dispositivo móvel está sendo gravada constantemente, independentemente de seu uso.

Outra tecnologia que pode colocar em risco direitos da privacidade é a rede inteligente de energia elétrica conhecida por *smart grids,* pela qual é possível monitorar o consumo de cada cliente em tempo real[161]. A "rede inteligente" utiliza tecnologia digital bidirecional para transportar eletricidade e informações para as residências dos consumidores. Ela é usada por fornecedores de eletricidade para economizar energia, reduzir custos, aumentar a transparência e controlar eletrodomésticos nas casas dos consumidores, notificando-os quando o refrigerador estiver com desempenho ruim ou se o aquecedor de água estiver ligado. Ao mesmo tempo, permite o monitoramento das atividades dos indivíduos em suas residências, coletando dados referentes às horas de vigília, férias, lavanderia, uso de TV e até consumo de cafeína.

Sem pretender esgotar todas as novas gerações de tecnologias existentes, cabe se debruçar sobre as temáticas *big data*, Internet das Coisas e algoritmos, esse último relacionado, em especial, ao objeto da presente pesquisa e cujo assunto abre campo à chamada inteligência artificial e ao *machine learning*, e cujas tecnologias desafiam a eficiência de uma regulação em proteção de dados pessoais. Em razão da necessidade de mais aprofundamento, trataremos os temas separadamente.

2.2 A massificação de dados e o *big data*

O termo *big data* descreve o grande volume de dados – estruturados e não estruturados – e está relacionado aos avanços na mineração de dados (*data*

[161] No Brasil as redes elétricas inteligentes começaram a ser implantadas em 2011. (HERZOG, Ana Luiza. O Brasil na onda das smart grids. **Revista Exame**. Publicada em: 29 abr. 2013. Disponível em: <https://exame.abril.com.br>. Acesso em: 28 nov. 2018). Segundo a reportagem: "Com o uso do medidor inteligente e de toda a parafernália tecnológica que a ele deve estar atrelada – uma rede elétrica automatizada e um sistema robusto de transmissão de dados – é possível monitorar o consumo de cada cliente em tempo real".

mining[162]), ao supreendente aumento do poder computacional e à capacidade de armazenamento de dados, que possibilita análises e correlações mais sofisticadas.

Em 2013, quando o canal You Tube do Google tinha cerca de 800 milhões de usuários, Viktor Mayer-Schönberger e Kenneth Cukier[163] indicaram que a cada segundo subiam mais de uma hora de vídeo no canal. Em 03 de maio de 2018, a CEO do YouTube, Susan Wojcicki, anunciou que o canal atingira a marca de 1.8 bilhões de usuários[164]. Ou seja, em cerca de 5 anos a base de usuários mais do que dobrou. Daí se infere que, atualmente, a base de dados inserida no canal You Tube pode ser mais de duas horas por segundo, o que gera um material de aproximadamente 172 mil horas por dia.

Se olharmos a história, quando da invenção da prensa de Johannes Gutenberg no século XV, veremos o quanto a sociedade da época foi impactada pela revolução informacional daquele tempo[165]. Após séculos de uma Europa Ocidental arreferida culturalmente, com baixa produção escrita (a pouca existente pertencia em especial aos monges copistas), chegou uma nova tecnologia capaz de reproduzir livros com uma capacidade nunca imaginada até então. Entre 1453 e 1503 foram impressos cerca de 8 milhões de livros, o que acabou, inclusive, ameaçando o poder totalizante da época, a monarquia). Essa análise histórica nos instiga a duvidar que tenhamos chegado ao final do percurso, ainda que a geração de dados e seu armazenamento sejam astronômicos. A tendência é aumentar além das escalas da Lei de Moore.

Segundo Viktor Mayer-Schönberger e Kenneth Cukier, “los datos masivos alteran la naturaleza de los negocios, los mercados y la sociedade”. No século 20, o valor mudou de infraestruturas físicas, como terrenos e fábricas, para intangíveis, como marcas e propriedade intelectual. Estes agora se expandem para dados, o

---

[162] Data mining is the process of analysing data from different perspectives and summarising it into useful new information. […] Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. It is commonly used in a wide range of profiling practices, such as marketing, surveillance, fraud detection and scientific discovery’ European Data Protection Supervisor. Vide Glossário da EUROPEAN DATA PROTECTION SUPERVISOR. Disponível em: <https://edps.europa.eu/data-protection/data-protection/glossary_en>. Acesso em: 18 out. 2018. Tradução livre: A mineração de dados é o processo de analisar dados de diferentes perspectivas e resumi-los em novas informações úteis. [...] Tecnicamente, mineração de dados é o processo de encontrar correlações ou padrões entre dezenas de campos em grandes bancos de dados relacionais. É comumente usado em uma ampla gama de práticas de criação de perfis, como marketing, vigilância, detecção de fraudes e descobertas científicas do European Data Protection Supervisor.

[163] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. Big data. **La revolución de los datos masivos**. Tradução de Antonio Iriarte. Madri: Turner, 2013, p.8-9.

[164] Disponível em: <https://www.theverge.com/>. Acesso em: 24 dez. 2012.

[165] Sobre o tema: EISENSTEIN, Elizabeth L. **The printing press as an agente of change**. Communications and culture transformations in early-modern Europe. v.I e II. New York-USA: Cambrigde University Press, 1979.

que está se tornando um importante ativo corporativo, um fator econômico vital e a base de novos modelos econômicos. Embora os dados ainda não sejam registrados em balanços contábeis das empresas, segundo os autores é provavelmente apenas uma questão de tempo para isto ocorrer[166].

As empresas Walmart e Capital One foram pioneiras no emprego de *big data* no varejo e no setor bancário, e assim modificaram seus negócios significativamente. Hoje, muitas dessas ferramentas foram democratizadas (embora não os dados) [167].

Segundo lição de Viktor Mayer-Schönberger e Kenneth Cukier[168], durante a maior parte da história, as maiores conquistas da humanidade emergiram da dominação da capacidade de medição e precisão. A busca pela precisão começou na Europa em meados do século XIII, quando os astrônomos e os sábios estavam encarregados da quantificação precisa do tempo. Enquanto isso, por sua vez, o perigo que paira sobre nós como indivíduos sai do escopo do privado para a probabilidade: os algoritmos irão prever a probabilidade de uma pessoa sofrer um ataque cardíaco (e, por isso, ter que pagar mais pelo seguro de saúde), as chances de um devedor parar de pagar a hipoteca (e, portanto, ter um crédito negado) ou a probabilidade de uma pessoa cometer um crime (e poder ser preso antes dos fatos), *à la* Minority Report[169].

---

[166] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**. La revolución de los datos masivos. Tradução de Antonio Iriarte. Madri: Turner, 2013, p.8-9.

[167] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**. La revolución de los datos masivos. Tradução de Antonio Iriarte. Madri: Turner, 2013, p.8-9.

[168] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**. La revolución de los datos masivos. Tradução de Antonio Iriarte. Madri: Turner, 2013, p.8-9.

[169] Na Itália foi criado o algoritmo X-Law. Segundo matéria, um homem foi preso graças ao novo sistema empregado pela polícia italiana. O programa informou que havia grandes chances de um crime ser cometido na região de Camorra entre 3h e 4h da madrugada do dia 16 de nov. “Na delegacia, foi verificado que o homem tinha vários antecedentes por roubos e outros crimes cometidos no passado. "Os criminosos costumam atuar sempre na mesma zona, com o mesmo modus operandi e os mesmos procedimentos. Conhecem o comportamento das pessoas, os horários em que as empresas fecham e quando os idosos vão ao banco retirar sua aposentadoria", disse o inspetor Elia Lombardo, criador da tecnologia. O inspetor informou que trabalhou na elaboração do sistema por 20 anos. As informações sobre crimes são introduzidas no sistema, que, a cada meia hora, envia um alerta sobre onde é mais provável que ocorra um delito nas duas horas seguintes. Esses cálculos matemáticos permitem que a polícia preveja a ocorrência de crimes com mais precisão e atue de forma mais eficaz. O X-law já havia sido testado em Nápoles e nas províncias de Prato e de Veneza. Se continuar a ter sucesso, será usado em toda a Itália para prevenir roubos. Além da Italia, em Chicago, a terceira cidade mais populosa dos Estados Unidos (e uma das mais violentas), a polícia usa desde 2017 um algoritmo que cria um sistema de pontuação, com base nos registros policiais de prisões, disparos e outras variáveis, para prever quem tem uma maior probabilidade de disparar uma arma contra outra pessoa ou de ser baleado. O sistema cria uma lista de suspeitos, e os agentes vigiam aqueles com as pontuações mais elevadas. A China também está desenvolvendo um software para obter informações sobre possíveis criminosos e evitar incidentes violentos com base em dados que indicam comportamentos ‘incomuns´ de cidadãos para estabelecer padrões de criminalidade”. (BBC. **Polícia usa algoritmo que prevê crimes para prender ladrão na Itália**. Veiculado em 19 nov. 2018. Disponível em: <https://www.bbc.com/>. Acesso em: 20 nov. 2018.

Hoje dispomos de sofisticadas ferramentas (estatísticas e algoritmos) e o equipamento necessário (processadores digitais e armazenamento) para realizar tarefas semelhantes com muito mais velocidade e eficiência, em escala e em contextos diversos[170].

Ademais, Viktor Mayer-Schönberger e Kenneth Cukier trazem uma importante reflexão, ou seja, que essa datificação leva a uma consideração ética do papel do livre arbítrio contra a ditadura dos dados:

> ¿Debería imponerse la voluntad del individuo a los datos masivos, aun cuando las estadísticas argumenten lo contrario? Igual que la imprenta preparó el terreno para las leyes que garantizaban la libertad de expresión –que no existían antes, al haber tan poca expresión escrita que proteger–, la era de los datos masivos precisará de nuevas reglas para salvaguardar la inviolabilidad del individuo. Puede advertirse un cambio similar, comparando la importancia de tener más datos en relación con otras mejoras, en el campo de la computación. Todo el mundo sabe cuánto ha aumentado a lo largo de los años la capacidad de procesamiento, como predijo la ley de Moore, que estipula que el número de transistores en un chip viene a duplicarse cada dos años. Este perfeccionamiento continuo ha hecho que los ordenadores sean más rápidos y con más memoria. Pero no todo el mundo sabe que la prestación de los algoritmos que impulsan muchos de nuestros sistemas también ha aumentado: en muchas áreas, más que la mejora de los procesadores según la ley de Moore. Muchos de los beneficios para la sociedad que traen los datos masivos, sin embargo, se producen no tanto por los chips más rápidos o los mejores algoritmos, sino porque hay más datos[171].

Quanto mais dados estiverem à disposição dos algoritmos, mais eficaz será o resultado de seu trabalho. Nesse sentido, mais valioso do que os próprios algoritmos, por mais sofisticados que sejam, está o valor dos próprios dados: “una vez que se ha datificado el mundo, los usos potenciales de la información no tienen más limite”[172].

O “projeto” no qual está focada a era atual é a datificação. Segundo Viktor Mayer-Schönberger e Kenneth Cukier:

> Los acueductos hicieron posible el crecimiento de las ciudades; la imprenta facilitó la Ilustración; los periódicos permitieron el auge del estado-nación. Pero estas infraestructuras estaban enfocadas hacia flujos: de agua, de conocimiento. Otro tanto cabe decir del teléfono y de internet. En cambio, la datificación representa un enriquecimiento esencial de la comprensión

[170] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**. La revolución de los datos masivos. Tradução de Antonio Iriarte. Madri: Turner, 2013, p.8-9.
[171] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**. La revolución de los datos masivos. Tradução de Antonio Iriarte. Madri: Turner, 2013, p.8-9.
[172] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**. La revolución de los datos masivos. Tradução de Antonio Iriarte. Madri: Turner, 2013, p.8-9.

> humana. Con la ayuda de los datos masivos, nuestro mundo dejará de parecernos una sucesión de acontecimientos que explicamos como fenómenos naturales o sociales: veremos un universo constituido esencialmente por información[173].

Conforme ponderação de Solon Barocas e Helen Nissenbaum, a expressão *big data* reflete mais um paradigma do que uma determinada tecnologia, método ou prática. Assim, *big data*, enquanto paradigma, é uma maneira de pensar sobre o conhecimento através de dados e um arcabouço para apoiar a tomada de decisões, racionalizando a ação e orientando a prática:

> Taking into consideration wide-ranging uses of 'big data' in public discussions, specialized applications, government initiatives,research agendas, and diverse scientific, critical, and popular publications, we find that the term better reflects a paradigm than a particular technology, method, or practice. There are, of course, characteristic techniques and tools associated with it, but, more than the sum of these parts, big data, the paradigm, is a way of thinking about knowledge through data and a framework for supporting decision making, rationalizing action, and guiding practice[174].

Conforme constou na opinião 03/2013, da Comissão Europeia, sobre *purpose limitation*, *big data* refere-se ao crescimento exponencial tanto na disponibilidade quanto no uso automatizado da informação:

> it refers to gigantic digital datasets held by corporation, governments and other large organisations, which are then extensively analysed (hence the name: analytics) using computer algorithms. Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individual[175].

Na concepção de Viktor Mayer-Schönberger e Kenneth Cukier *big data:*

> Big data refers to things one can do at a large scale that cannot be done at a samaller one, to extract new insights or create new forms of value, in ways

---

[173] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. Big data. **La revolución de los datos masivos**. Tradução de Antonio Iriarte. Madri: Turner, 2013, p.8-9.

[174] Tradução livre: Levando em consideração as amplas utilizações de 'big data', tanto em discussões públicas, como em aplicações especializadas, iniciativas governamentais, agendas de pesquisa, e em diversas publicações científicas, críticas e populares, entendemos que o termo reflete melhor um paradigma do que uma determinada tecnologia, método ou prática. Há, é claro, técnicas e ferramentas características associadas ao big data, porém, mais do que a soma dessas partes, big data, enquanto paradigma, é uma maneira de pensar sobre o conhecimento através de dados e um arcabouço para apoiar a tomada de decisões, racionalizando a ação, e orientando a prática.(BAROCAS, Solon; NISSENBAUM, Helen. Big data's end run around anonymity and consent. In: (Coords.) LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen. **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.3).

[175] Tradução livre: refere-se a gigantescos conjuntos de dados digitais mantidos por corporações, governos e outras grandes organizações, que são extensivamente analisados (daí o nome: *analytics*) usando algoritmos de computador. *Big data* pode ser usado para identificar tendências e correlações mais gerais, mas também pode ser processado para afetar diretamente. (EUROPEAN COMMISSION. **Opinion 03/2013 on purpose limitation**. Disponível em: <http://ec.europa.eu/newsroom/article29/news-overview.cfm>. Acesso em: 31 out. 2017).

> that change markets, organizations, the relationship between citzens and governments, and more[176]

Para André Martins Brandão, a tecnologia do *big data* é desenvolvida "com a ambição de possibilitar uma navegação mais rápida e eficiente no oceano de dados produzidos diariamente (e que só tende a crescer) – possibilitando ainda novas modulações de controle"[177].

Segundo K. Krasnow Waterman e Paula Bruening, as análises realizadas em *big data* vasculham montanhas de dados para identificar ou prever fatos sobre determinados indivíduos e usá-los em decisões relacionadas a diversos aspectos, que variam desde publicidade direcionada até indicação de tratamento médico[178].

É comum encontrar a expressão *big data* associada aos "3 Vs": volume, velocidade e variedade. Kirk Borne[179], porém, propõe um salto para "10 Vs":

> 1. **Volume**: = lots of data.
> 2. **Variety**: = complexity, thousands or more features per data item, the curse of dimensionality, combinatorial explosion, many data types, and many data formats.
> 3. **Velocity**: = high rate of data and information flowing into and out of our systems, real-time, incoming!
> 4. **Veracity**: = necessary and sufficient data to test many different hypotheses, vast training samples for rich micro-scale model-building and model validation, micro-grained "truth" about every object in your data collection, thereby empowering "whole-population analytics".
> 5. **Validity**: = data quality, governance, master data management (MDM) on massive, diverse, distributed, heterogeneous, "unclean" data collections.
> 6. **Value**: = the all-important V, characterizing the business value, ROI, and potential of big data to transform your organization from top to bottom (including the bottom line).
> 7. **Variability**: = dynamic, evolving, spatiotemporal data, time series, seasonal, and any other type of non-static behavior in your data sources, customers, objects of study, etc.
> 8. **Venue**: = distributed, heterogeneous data from multiple platforms, from different owners' systems, with different access and formatting requirements, private vs. public cloud.
> 9. **Vocabulary**: = schema, data models, semantics, ontologies, taxonomies, and other content- and context-based metadata that describe the data's structure, syntax, content, and provenance.
> 10. **Vagueness**: = confusion over the meaning of big data[180].

---

[176] Tradução livre: *Big data* refere-se a coisas que uma pessoa pode fazer em grande escala que não poderiam ser feitas em um nível mais baixo, para extrair novos insights ou criar novas formas de valor, de maneira que são capazes de provocar a modificação em mercados, organizações, relacionamento entre cidadãos e governos e muito mais. (MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. CUKIER, Kenneth. **Big data**: a revolution that will transform how we live, work and think. New York: Houghton Mifflin Publishing, 2013, p.6).

[177] BRANDÃO, André Martins. **Sujeito e decisão na sociedade de dados**. Tese (Doutorado). Pontifícia Universidade Católica de São Paulo, São Paulo, 2017, p.208.

[178] WATERMAN, K. Krasnow; BRUENING Paula J. Big Data analytics: risks and responsabilities. ***International Data Privacy Law***, v.4, 2.ed. maio 2014, p.89-95. Disponível em: <https://doi.org/10.1093/idpl/ipu002>. Acesso em: 22 out. 2018, p.91.

[179] BORNE, Kirk. Knowledge is power. Publicado em: 11 abr. 2014. Disponível em: <https://mapr.com/blog/top-10-big-data-challenges-serious-look-10-big-data-vs/>. Acesso em: 12 out. 2018.

Há quem opine que o termo *big data* consiste em expressão ampla, vaga e imprecisa[181]. De qualquer forma, não há dúvidas de que esse conjunto de dados, designado por *big data,* é capaz de trazer vários benefícios à sociedade. Porém, ao simultaneamente, emerge um risco de uso inadequado e indevido das informações pessoais contidas nesses dados. Por isso, o *big data* pode implicar numa ameaça à privacidade[182].

---

[180] Tradução livre: I) Volume (Volume): muitos dados; apelidado de Tonnabytes, haja vista que se trata, em um sentido metafórico, de "toneladas de bytes"; II) Variety (Variedade): complexidade, milhares ou muitas características por item de dados, grande dimensionalidade, explosão combinatória, muitos tipos de dados e muitos formatos de dados; III) Velocity (Velocidade): alta taxa de dados e informações que fluem para dentro e para fora de nossos sistemas em tempo real; IV) Veracity (Veracidade): dados necessários e suficientes para testar muitas hipóteses diferentes, vastas amostras de treinamento para a modelagem de formatos em microescala e a validação do modelo, a verdade micro-granulada de cada objeto em sua coleta de dados, capacitando assim a análise da "população inteira"; V) Validity (Validade): qualidade dos dados, governança, gerenciamento de dados mestres (MDM) em coletâneas de dados maciços, diversos, distribuídos, heterogêneos e "impuros"; VI) Value (Valor): trata-se do "V" mais importante, pois caracteriza o valor do negócio; VII) Variability (Variabilidade): dados dinâmicos e evolutivos; VIII) Venue (espaço): dados distribuídos, heterogêneos de múltiplas plataformas, de diferentes sistemas de proprietários, com diferentes requisitos de acesso e formatação; nuvem privada versus nuvem pública; IX) Vocabulary (Vocabulário): esquema de modelos de dados, semânticas, ontologias, taxonomias e outros metadados baseados em conteúdo e contexto que descrevem a estrutura, sintaxe, conteúdo e proveniência dos dados; X) Vagueness (Vagueza): confusão sobre o significado de grandes dados.

[181] CRAWFORD, Kate; SCHULTZ, Jason. Big data and due process: toward a framework to redress predictive privacy harms. **Boston College Law**, v.55, n.1, 2014.

[182] De outro lado, há aqueles que defendam a máxima utilização dos proveitos que possam ser extraídos do *big data*, ainda que isso signifique comprometer a privacidade. Essa é a opinião arrojada de Barocas e Nissenbaum: Privacy and big data are simply incompatible and the time has come to reconfigure choices that we made decades ago to enforce certain constraints. The arguments presented here give further reason to dislodge privacy from its pedestal and allow the glorious potential of big data to be fulfilled. Tradução livre: Privacidade e big data são simplesmente incompatíveis e chegou a hora de reconfigurar as escolhas que fizemos há décadas para impor certas restrições. Os argumentos apresentados aqui fornecem mais motivos para desalojar a privacidade de seu pedestal e permitir que o glorioso potencial do Big Data seja atendido. (BAROCAS, Solon; NISSENBAUM, Helen. Big data's end run around anonymity and consent. In: (Coords.) LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (Coord.). **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.8). Acrescente-se da opinião dos autores: We think these people are wrong in part because they adhere to a mistaken conception of privacy, often as control or as secrecy. Because they see privacy at odds with any distribution and use of data instead of focusing only on the inappropriate, they set up a false conflict from the start. They also may wrongly be conflating the operationalization of informed consent with informed consent itself. Others say that we should remain concerned about ethical issues raised by big data, that, while privacy may be a lost cause, the real problems arise with use. Those deserving urgent attention include unfair discrimination, being limited in one's life choices, being trapped inside stereotypes, being unable to delineate personal boundaries, being wrongly judged, embarrassed, or harassed. Pursuing privacy as a way to address these issues is not only retrograde but a fool's errand, a conclusion reinforced by the arguments in our paper. Better, they would say, to route around privacy and pursue directly its ends. We agree that individual interests and ethical and, we would add, context-specific values are vitally important, but we think that it is reckless to sever, prematurely, the conceptual and practical ties between privacy and these moral and political ends. To fathom the ways that big data may threaten interests and values, we must distinguish among the origins and nature of threats to individual and social integrity, between, say, unfair discrimination originating in inappropriate information flows and unfair discrimination originating from other causes. For one thing, different sources may indicate different solutions. We are not yet ready to give up on privacy, nor completely on anonymity and consent. The paradigm shift of big data calls for a paradigm shift in our responses and, though it may seem that the arguments of this chapter leave no place for anonymity and consent and, for some, therefore, no place for privacy, we reach different conclusions. Tradução livre: Achamos que essas pessoas estão erradas em parte porque aderem a uma concepção errônea de privacidade, muitas vezes como controle ou como sigilo. Porque eles vêem privacidade em desacordo com qualquer distribuição e uso de dados em vez de se concentrar apenas no inadequado, eles criaram um falso conflito desde o início. Eles também podem erroneamente confundir a operacionalização do consentimento informado com o próprio consentimento informado. Outros dizem que devemos continuar preocupados com questões éticas levantadas pelo *big data*, que, embora a privacidade possa ser uma causa perdida, os problemas reais surgem com o uso. Aqueles que merecem atenção urgente incluem a discriminação injusta, sendo limitados em suas escolhas de vida, sendo

André Martins Brandão ratifica a opinião de que o *big data* gera impactos nesse setor:

> Parte-se da hipótese de que na atual sociedade de dados o uso das tecnologias de inteligência artificial e *big data* gera impactos sobre os mais diversos campos que são tocados pelo fenômeno jurídico, como privacidade, discriminação, direito público à informação, democracia e até automação da tomada de decisão (jurídica), dentre muitos outros[183].

Manon Oostveen, ao passo que reconhece o *big data* com grande potencial de fazer com que as empresas gerem grandes receitas, permitir que os cientistas resolvam questões vitais e ajudar os governos a tomar decisões políticas informadas, por outro lado alerta para a enorme coleta e uso de dados pessoais que coloca em risco questões voltadas à proteção dessas informações:

> Big data is the present and the future. It holds the potential to make corporations create big revenues, to let scientists solve vital issues and to help governments make informed policy decisions. Yet the massive collection and use of personal data also raises a host of issues, particularly for individuals' privacy and data protection rights[184].

São justamente as regulações advindas da soberania da lei que devem impor limites à gestão do *big data* por agentes econômicos e também pela administração pública. Os princípios plasmados em lei devem servir para o balizamento das práticas de coleta e uso dos dados pessoais[185].

As regulações de proteção de dados atuais buscam proteger o indivíduo, enquanto consumidor e cidadão, de potenciais lesões. Nesse sentido, o Estado

---

presos dentro de estereótipos, sendo incapazes de delinear limites pessoais, sendo injustamente julgados, constrangidos ou assediados. Perseguir a privacidade como uma forma de abordar essas questões não é apenas retrógrado, mas uma tarefa tola, uma conclusão reforçada pelos argumentos em nosso artigo. Melhor, eles diriam, rotear a privacidade e perseguir diretamente seus fins. Concordamos que os interesses individuais e os valores éticos e, digamos, específicos do contexto, são de vital importância, mas achamos imprudente romper, prematuramente, os laços conceituais e práticos entre a privacidade e esses fins morais e políticos. Para compreender as formas como o *big data* pode ameaçar interesses e valores, devemos distinguir entre as origens e a natureza das ameaças à integridade individual e social, por exemplo, discriminação injusta originada em fluxos de informações inadequados e discriminação injusta originada de outras causas. Por um lado, fontes diferentes podem indicar soluções diferentes. Ainda não estamos prontos para desistir da privacidade, nem completamente do anonimato e do consentimento. A mudança de paradigma do *big data* exige uma mudança de paradigma em nossas respostas e, embora possa parecer que os argumentos deste capítulo não deixam lugar para anonimato e consentimento e, para alguns, portanto, não há lugar para privacidade, chegamos a conclusões diferentes.

[183] BRANDÃO, André Martins. **Sujeito e decisão na sociedade de dados**. Tese (Doutorado). Pontifícia Universidade Católica de São Paulo, São Paulo, 2017, p.208.

[184] OOSTVEEN, Manon. Identifiability and the applicability of data protection to big data, **International Data Privacy Law**, v.6, 4.ed, nov. 2016, p.299-309. Disponível em: <https://doi.org/10.1093/idpl/ipw012>. Acesso em: 12 out. 2018.

[185] Vide WATERMAN, K. Krasnow; BRUENING Paula J. Big Data analytics: risks and responsabilities. ***International Data Privacy Law***, v.4, 2.ed. maio 2014, p.89-95. Disponível em: <https://doi.org/10.1093/idpl/ipu002>. Acesso em: 22 out. 2018, p.93.

impõe formas de coletar, agregar, armazenar e utilizar os dados pessoais contidos nos diversos bancos de dados hoje contruídos, visando harmonizar o fenômeno do *big data* e a proteção dos dados pessoais. Na opinião de Katherine Strandburg, porém, o faz de modo insuficiente:

> Current privacy laws are not well adapted to the privacy concerns that arise in the big data context, in which risks tend to be probabilistic and the connection between particular harms and data handler behavior tends to be attenuated because of the importance of aggregation and hard to trace. […] The privacy torts' emphasis on outrageous behavior is clearly inapropos to the privacy concerns associated with large aggregations of data. Moreover, the reliance on inference fundamental to big data practices means that privacy law's categorical treatment of certain pieces of infonnation as private or public is unlikely to correlate with big data privacy harms. Recent judicial recognition of this problem in the context of location tracking is only the tip of the iceberg of the data aggregation issue. The ubiquity of data collection also undennines the effectiveness of regulatory regimes that rely on the expertise of entities in particular sectors[186] .

Essa também é a opinião de Manon Oostveen, ao afirmar que, quanto à regulação europeia, é incerto se esta é:

> In Europe, data protection regulation is widely regarded as the answer to these issues. Through regulating data flows and providing individuals control over their personal data, some of big data's possible undesired effects may be prevented. Yet upon closer scrutiny, it is uncertain whether European data protection legislation suffices to address these negative consequences. The practices in big data projects and the threshold for data to fall within the material scope of EU data protection legislation raise[187].

Na década de 1970, o desenvolvimento de computadores digitais, aliado à crescente complexidade da adminstração estatal levou à expansão das operações

---

[186] STRANDBURG, Katherine J. Monitoring, datafication, and consent: legal approaches to privacy in the big data context. In: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen. **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.24. Tradução livre: As atuais leis de privacidade não são bem adaptadas às preocupações com privacidade surgidas no contexto do big data, em que os riscos tendem a ser probabilísticos e a relação entre danos pessoais e a postura dos responsáveis pelos dados tende a ser maior devido à facilidade de agregar dados e à dificuldade de rastreá-los. [...] A ênfase das violações de privacidade em comportamento ultrajante é claramente inadequada às preocupações relacionadas à privacidade que dizem respeito às agregações de dados. Além disso, a confiança na inferência das práticas de big data significa que o tratamento categórico da lei de privacidade de certas partes da informação como privada ou pública é improvável de corresponder a danos à privacidade no contexto do big data. O recente reconhecimento judicial desse problema no contexto do rastreamento de localização é apenas a ponta do iceberg do problema de agregação de dados. A ubiquidade da coleta de dados também prejudica a eficácia dos regimes regulatórios que contam com a expertise de entidades em setores específicos.

[187] OOSTVEEN, Manon. Identifiability and the applicability of data protection to big data, **International Data Privacy Law**, v.6, 4.ed, nov. 2016, p.299-309. Disponível em: <https://doi.org/10.1093/idpl/ipw012>. Acesso em: 12 out. 2018. Tradução livre: Na Europa, a regulação da proteção de dados é amplamente considerada como a resposta a essas questões. Através da regulação dos fluxos de dados e do controle dos indivíduos sobre seus dados pessoais, alguns dos possíveis efeitos indesejados do Big Data podem ser evitados. No entanto, após um exame mais minucioso, é incerto se a legislação europeia de proteção de dados é suficiente para lidar com essas consequências negativas. As práticas em projetos de big data e o limiar para os dados se enquadrarem no escopo material da legislação de proteção de dados da UE aumentam.

de armazenamento de registros baseadas em computador por parte de governos e de algumas outras grandes instituições, como os bancos. Essa nova atuação causou temores em relação ao uso indevido dos dados e em relação à tomada de decisões injustas e sem transparência. Eis aqui o início do fenômeno *big data.*

Nessa época, tanto na Europa quanto nos Estados Unidos começaram a ser aprovadas legislações para regular o uso de dados, especialmente por agências governamentais.

Entretanto, a formação do banco de dados das décadas de 1970 e 1980 é diferente da atual, conforme explicam Steven Koonin e Michael Holland:

> Traditional microdata resulting from censuses, sample surveys, administrative records, and statistical modeling differ from big data in several technical aspects [...]. Much of the usual microdata encompass records numbering in the hundreds of millions, while big datasets are many orders of magnitude greater. The computational challenges associated with massive data management are substantially different from those for static datasets in terms of scale and throughput. Technical advances are required to scale data infrastructure for curation, analytics, visualization, machine learning, data mining, as well as modeling and simulation to keep up with the volume and speed of data[188].

Ao pousar o olhar de análise sobre as últimas duas décadas, verifica-se que houve uma intensificação das fontes geradoras e de captação de dados. Rápidos avanços foram vistos em sensores, em tecnologias de banco de dados, em mecanismos de busca, na mineração de dados, no aprendizado de máquina *(machine learning*), e em estatística. Estas tecnologias que sustentam o *big data* permitem que as organizações adquiram, transmitam, armazenem e analisem todos os tipos de dados em maior volume, com maior velocidade e maior variedade.

Atualmente muitas pessoas têm mais de um *device* particular conectado em rede, entre *smartphone*, *tablet*, relógio, *notebook* etc. O "aparelhamento" da sociedade acarreta em maior produção de dados de granularidade, cobertura e

[188] Tradução livre: Os dados tradicionais resultantes de censos, pesquisas por amostragem, registros públicos e modelagem estatística diferem do big data de hoje em vários aspectos técnicos. Muitos dos dados usuais abrangem registros com centenas de milhões, enquanto big data apresenta ordem de grandeza muito maior. Os desafios computacionais associados ao gerenciamento massivo de dados são substancialmente diferentes daqueles para conjuntos de dados estáticos em termos de escala e taxa de transferência. São necessários avanços técnicos para dimensionar a infraestrutura de dados para curadoria, análise, visualização, aprendizado de máquina, mineração de dados, bem como modelagem e simulação para acompanhar o volume e a velocidade dos dados. (KOONIN, Steven E.; HOLLAND, Michael J. The value of big data for urban science. In: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (Coords.) **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.8).

oportunidade sem precedentes. Há um *tsunami* de dados que está cada vez mais impactando as esferas comercial e acadêmica[189].

Há uma década e meia atrás, era notícia que o Walmart estava usando a análise preditiva para antecipar as necessidades de estoque em face de eventos climáticos severos futuros. Atualmente, campanhas de varejo (gerenciamento de estoques), publicidade (mecanismos de recomendação on-line), seguros (melhor estratificação de risco), financeiro (estratégia de investimento, detecção de fraudes), imobiliária, de entretenimento e política, rotineiramente adquirem, integram e analisam grandes quantidades de dados para melhorar seu desempenho[190].

O paradigma do *big data* é uma ameaça à proteção de dados pessoais, outrossim, pela característica da possibilidade de associação de dados. Segundo Steven Koonin e Michael Holland, o valor de qualquer grande conjunto de dados urbano é aprimorado por meio de sua associação com outros dados. O poder dessa ligação na produção de novas informações é significativo e cada vez mais reconhecido. Por exemplo, saber o CEP de um indivíduo permite localizá-la de 1 em 30.000 (a população média de um CEP, nos Estados Unidos da America). Por sua vez, a vinculação de um CEP a uma data de nascimento reduz o conjunto a aproximadamente 1 em 80. Já a inclusão do gênero e do ano de nascimento nessa associação é capaz de especificar um determinado indivíduo[191].

Segundo André Martins Brandão, o ponto nevrálgico do *big data* é o reconhecimento de padrões ou correlações em complexidades de dados:

> As tecnologias que trabalham com *big data* lidam com o oceano complexo de dados de forma a reconhecer padrões ou correlações. Assim, o ponto nevrálgico do *big data* é o reconhecimento de padrões ou correlações em complexidades de dados, gerando informações e conhecimentos úteis e relevantes. A máquina passa a possuir auspícios – a capacidade de ler a providência. A ação humana, em diversos meios, guia-se por essa leitura, realizando o indicado pela máquina[192].

---

[189] KOONIN, Steven E.; HOLLAND, Michael J. The value of big data for urban science. In: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (Coords.) **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.1.

[190] KOONIN, Steven E.; HOLLAND, Michael J. The value of big data for urban science. In: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (Coords.) **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.1.

[191] KOONIN, Steven E.; HOLLAND, Michael J. The value of big data for urban science. In: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (Coords.) **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.9.

[192] BRANDÃO, André Martins. **Sujeito e decisão na sociedade de dados**. Tese (Doutorado). Pontifícia Universidade Católica de São Paulo, São Paulo, 2017, p.230.

Por vezes, são informados dados neutros que podem produzir informações consistentes em dados ultrassensíveis. Cuida-se da teoria do mosaico, segundo a qual dados em princípio neutros podem se converter, pela associação, em dados ultrassensíveis "por la simple interconexión de ficheiros, o el cambio de finalidade para la que fueron recogidos, dando la clave esencial que sirva para catalogar a uma determinada persona"[193].

No entanto, a mineração de dados, a vinculação de dados e as análises estatísticas não são as únicas fontes de risco apresentadas pelas tecnologias de *big data*. A confiança em recursos de computação distribuída ou em nuvem pode criar riscos adicionais à privacidade, incluindo riscos em relação a dados não criptografados armazenados na nuvem.

Segundo *Policy Paper*, do Grupo de Ensino e Pesquisa em Inovação da FGV Direito São Paulo, intitulado 'Um novo mundo de dados', publicado em 29 de agosto de 2017:

> Em um contexto de massificação das atividades de coleta e tratamento de dados nos meios digitais, o debate sobre privacidade e proteção de dados pessoais é imprescindível em ao menos dois níveis: a garantia de direitos fundamentais, como privacidade e intimidade, e a necessidade de assegurar segurança jurídica para viabilizar novos modelos de negócios e políticas públicas, dependentes, cada vez mais, do uso de dados[194].

O *big data* também está relacionado à dinâmica das cidades inteligentes (*smart cities*)[195], em políticas públicas, tais quais WiFi público e estacionamento rotativo digital. Em 21 de dezembro de 2016, a Corte de Justiça da União Europeia decidiu dois importantes e polêmicos casos (C-203/15 e C-698/15), os quais dscutiram sobre regras que impunham o armazenamento indiscriminado de dados relativos à localização de tráfego de dados em comunicações eletrônicas, envolvendo cidadãos da Irlanda, da Noruega e do Reino Unido, e se isso consistiria em risco de vigilância excessiva, em especial por parte das empresas que guardam

---

[193] CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.63. Um exemplo da aplicação da teoria do mosaico é a interconexão de um banco de dados médico e outro escolar, cujo cruzamento pode trazer informações de condições congênitas das crianças, incidentes de saúde, como tais fatos tem influenciar seu rendimento escolar, se estão aptos a continuar os estudos, quais carreiras seriam as mais adequadas às suas capacidades, etc.

[194] SILVA, Alexandre Pacheco da (Coord.). **Um novo mundo de dados**. Policy Paper do Grupo de Ensino e Pesquisa em Inovação da FGV Direito SP. Publicado em 29 ago. 2017, p.7. Disponível em: <https://direitosp.fgv.br/sites/direitosp.fgv.br/files/arquivos/unmd_policy_paper_fgv.pdf>. Acesso em: 10 jan. 2019.

[195] Sobre o fenômeno do big data inserido no contexto das cidades inteligentes: REMEDIO, José Antonio; SILVA, Marcelo Rodrigues. O uso monopolista do Big Data por empresas de aplicativos: políticas públicas para um desenvolvimento sustentável em cidades inteligentes em um cenário de economia criativa e de livre concorrência. **Revista Brasileira de políticas públicas**. Direito e Mundo Digital. Uniceub, v.7, n.3, dez. 2017.

os dados e dos Estados que podem acessá-los. A decisão da Corte de Justiça da União Europeia foi no sentido de que não se pode impor obrigação geral de conservar dados das comunicações eletrônicas, pois esta medida implicaria em ato de vigilância indiscriminada, incompatível com os direitos fundamentais, violando os princípios da proporcionalidade e da razoabilidade e os valores inscritos em uma sociedade democrática.

Outra questão preocupante que ronda o contexto do *big data*, na esfera da tutela dos dados pessoais, está ligada ao longo prazo de armazenamento praticado no mercado. A manutenção dos dados abrange períodos de tempo cada vez mais longos e contém detalhes e informações, sobre o indivíduo, coletados em intervalos cada vez mais frequentes, possibilitando *insights* que só podem ser obtidos de uma massa de dados detalhada e vinculada a um longo período de tempo.

Sobre a exploração a longo prazo do *big data*, Micah Altman, Alexandra Wood e David O´Brien e Urs Gasser comentam:

> Telecommunications providers, mobile operating systems, social media platforms, and retailers often collect, store, and analyse large quantities of data about customers' locations, transactions, usage patterns, interests, demographics, and more. Highly detailed personal information is used to provide targeted services, advertisements, and offers to existing and prospective customers. Governments are also experimenting with collecting increasingly detailed information in order to monitor the needs of their communities, from pothole and noise complaints to crime reports and building inspection records, and to improve their responsiveness and delivery of constituent services[196].

Os dados pessoais – comerciais e governamentais – que se acumulam ao longo do tempo permitem definir um retrato deveras detalhado da vida de um indivíduo, tornando esses dados altamente valiosos não apenas para as organizações que os coletam, mas também para os usuários secundários.

A coleta, o armazenamento e o uso de grandes quantidades de dados pessoais por longos períodos de tempo são objeto de recentes debates jurídicos e políticos que abrangem tópicos tão variados quanto o direito ao esquecimento, a

[196] ALTMAN, Micah; WOOD, Alexandra Wood; O´BRIEN David R; GASSER, Urs. Practical approaches to big data privacy over time. *International Data Privacy Law*, v.8, 1.ed. fev.2018, p.29-51. Disponível em: <https://doi.org/10.1093/idpl/ipx027>. Acesso em: 22 out. 2018, p.35. Tradução livre: Provedores de telecomunicações, sistemas operacionais móveis, plataformas de mídia social e varejistas geralmente coletam, armazenam e analisam grandes quantidades de dados sobre locais, transações, padrões de uso, interesses, informações demográficas e muito mais. Informações pessoais altamente detalhadas são usadas para fornecer serviços direcionados, anúncios e ofertas para clientes atuais e futuros. Os governos também estão experimentando coletar informações cada vez mais detalhadas a fim de monitorar as necessidades de suas comunidades, desde reclamações de buracos e barulho até relatórios criminais e registros de inspeção de prédios, e para melhorar sua capacidade de resposta e prestação de serviços constituintes.

discriminação algorítmica e a era da *digital dark*[197]. A extensão total do impacto derivado dessas práticas ainda está por ser vista. Sabe-se, porém, que a pesquisa de longo prazo com seres humanos está associada a danos significativos relacionados à privacidade devido à coleta de um grande volume de informações pessoais altamente sensíveis sobre os indivíduos[198].

O fenômeno *big data* será cada vez mais intensificado, outrossim, pelo crescente número de dispositivos e de sensores que agora estão conectados por redes digitais, gerando uma imensidão de dados, no contexto do que é conhecido por internet das coisas, cujo tema será analisado adiante.

2.3 Internet das coisas: a conectividade onipresente e a datificação da vida

O fenômeno Internet das Coisas (IoT – *Internet of Things*)[199] [200] consiste na conectividade entre vários tipos de dispositivos utilizados no cotidiano pelo homem (geladeira, relógio, óculos, trator[201], toalhas[202]) e que podem ser acessíveis pela

[197] Em 2015, Vincent Cerf, considerado o pai da Internet, em 2015, disse estar preocupado que todas as imagens e documentos que guardamos em computadores acabem sendo perdidos, quando hardware e software se tornam obsoletos. Ele teme que as futuras gerações terão pouco ou nenhum registro do século 21, quando entraremos no que ele descreve como uma "Idade das trevas digital" (Digital Dark age). (GHOSH, Pallab. Google's vint cerf warns of 'digital dark age'. **BBC News**, 13 fev. 2015. Disponível em: <https://www.bbc.com/news/science-environment-31450389>. Acesso em: 22 out. 2018).

[198] ALTMAN, Micah; WOOD, Alexandra Wood; O´BRIEN David R; GASSER, Urs. Practical approaches to big data privacy over time. ***International Data Privacy Law***, v.8, fev.2018, p.29-51. Disponível em: <https://doi.org/10.1093/idpl/ipx027>. Acesso em: 22 out. 2018, p.42.

[199] A criação do termo é atribuída a Kevin Ashton, fundador do Auto-ID Center no Massachusetts Institute of Technology (MIT).

[200] Em 2017, o BNDES, em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), apoiou a realização de um estudo para diagnosticar e propor um plano de ação estratégico para o país em Internet das Coisas (Internet-of-Things – IoT).

[201] Trator conectado à internet: em parceria com a Usina São Martinho, de Pradópolis (SP), e com o apoio do BNDES, o CPqD instalou sensores em máquinas agrícolas, que enviam dados sobre posição e desempenho dos equipamentos via rádio em frequência de 250 MHz para as estações instaladas nas torres da fábrica. Todos os dados sobre equipamentos como tratores e caminhões são enviados para uma plataforma que pode ser acessada por meio de dispositivos móveis. “O projeto atual começou em 2016. No primeiro ano, desenvolvemos os equipamentos e, agora, no segundo, estamos corrigindo e melhorando os produtos”, disse Rafael Moreno, diretor de sistemas sem fio do CPqD. Por enquanto, 20 terminais foram instalados na usina. Até o fim do ano, o total de unidades deve chegar a 108. (INGIZZA, Carolina. **O Estado de S. Paulo**. Três exemplos de como a internet das coisas já é usada no Brasil. Disponível em: <https://link.estadao.com.br/noticias/inovacao,3-exemplos-de-como-a-internet-das-coisas-ja-e-usada-no-brasil,70002026748>. Acesso em: 27 jul. 2018).

[202] Visando diminuir o número de subtrações de toalhas, três hotéis americanos, localizados em Nova York, Miami e Honolulu, colocaram em funcionamento toalhas com etiquetas RFID, que se utiliza da tecnologia IOT. Por meio de um sistema computadorizado é possível rastrear os tecidos e evitar que levem as toalhas. Um dos hotéis que adotou a solução conseguiu economizar US$ 15 mil dólares, diminuindo a quantidade de desvio de toalhas de 4 mil para 750 toalhas por mês. (WILSON, Jenny. **Revista Time**. Want to steal a hotel towel? Checking for a new tracking chip first. Disponível em: <http://newsfeed.time.com/2011/04/18/want-to-steal-a-hotel-towel-check-for-a-new-tracking-chip-first/>. Acesso em: 25 ago. 2018).

internet ou por outras tecnologias como radio-frequency identification (RFID[203]), wireless sensor networks (WSN) ou machine-to-machine interfaces (M2M).

Para o Article 29 Working Party[204]:

> The concept of the Internet of Things (IoT) refers to an infrastructure in which billions of sensors embedded in common, everyday devices – "things" as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities. As the IoT relies on the principle of the extensive processing of data through these sensors that are designed to communicate unobtrusively and exchange data in a seamless way, it is closely linked to the notions of "pervasive" and "ubiquitous" computing[205].

Importante anotar que a Internet das Coisas apenas é possível em razão do advento do modelo IPV6[206], sem o qual não haveria tantos números de protocolos disponíveis para conectar essa infinidade de aparelhos.

---

[203] Segundo Tene: Radio-frequency identification (RFID) enables wireless data collection by readers from electronic tags attached to or embedded in objects, and potentially also people. RFID systems give objects a unique identity, providing identification or location information and increasing efficiencies, such as by reducing warehousing and distribution costs, improving forecasting and planning, minimizing time to payment, or reporting patients' medical conditions without intrusive procedures. At the same time, RFID facilitates pervasive tracking, including monitoring individuals' location; enables the collection of personal data without data subject awareness; and may allow surreptitious tag scanning and use of data for purposes adverse to the interests of data subjects.Tradução livre: A identificação por radiofrequência (RFID) permite a coleta de dados sem fio por leitores a partir de etiquetas eletrônicas anexadas ou incorporadas em objetos e, potencialmente, também a pessoas. Os sistemas RFID proporcionam aos objetos uma identidade única, fornecendo informações de identificação ou localização e aumentando a eficiência, reduzindo os custos de armazenamento e distribuição, melhorando a previsão e o planejamento, minimizando o tempo de pagamento ou relatando as condições médicas dos pacientes sem procedimentos intrusivos. Ao mesmo tempo, o RFID facilita o rastreamento invasivo, incluindo o monitoramento da localização dos indivíduos; permite a coleta de dados pessoais sem conhecimento do titular dos dados; e pode permitir a varredura subreptícia de etiquetas e o uso de dados para fins adversos aos interesses dos titulares de dados. (TENE, Omer. Privacy: the new generations. **International Data Privacy Law**, v.1, n.01, p.15-27, 2011, p.19).

[204] The "Article 29 Working Party" is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States. The Working Party is composed of: representatives of the national supervisory authorities in the Member States; a representative of the European Data Protection Supervisor (EDPS); a representative of the European Commission (the latter also provides the secretariat for the Working Party). Vide Glossário da European Data Protection Supervisor. Disponível em: <https://edps.europa.eu/data-protection/data-protection/glossary_en>. Acesso em: 18 out. 2018. Tradução livre: O "grupo de trabalho do artigo 29" é a designação abreviada do Grupo de Trabalho para a Proteção de Dados estabelecido pelo artigo 29 da Diretiva 95/46/CE. Fornece à Comissão Europeia aconselhamento independente sobre questões de proteção de dados e ajuda no desenvolvimento de políticas harmonizadas para a proteção de dados nos Estados-Membros da UE. O grupo de trabalho é composto por: representantes das autoridades nacionais de supervisão nos Estados-Membros; um representante da Autoridade Europeia para a Proteção de Dados (AEPD); um representante da Comissão Europeia (este último também fornece o secretariado para o Grupo de Trabalho).

[205] ARTICLE 29 Data protection working party, Opinion 8/2014 on the **Recent developments on the internet of things**, tech. report, 16 de Setembro 2014. Disponível em: <https://www.pdpjournals.com/docs/88440.pdf>. Acesso em: 27 jul. 2018.

[206] Para entender o que significa "IPV6" e como esse protocolo possibilita a IoT, recorremos à explicação do Comitê Gestor da Internet no Brasil, a qual inclui um resumo da própria história da Internet, senão vejamos: A Internet começou com um projeto do Departamento de Defesa (DoD – Department of Defense) do governo estadunidense que, em 1966, por meio da Agência de Pesquisas e de Projetos Avançados (ARPA – Advanced Research Projects Agency), iniciou um projeto para a interligação de computadores em centros militares e de pesquisa. Este sistema de comunicação e controle distribuído com fins militares recebeu o nome de ARPANET,

Atualmente analisa-se o fenômeno da Internet das Coisas sob diversos ângulos. Um dos mais importantes é entender como essa tecnologia está gerando uma infinidade de dados (*big data*) e trazendo ainda mais desafios à proteção da privacidade e dos dados pessoais. Além disso, como a vida hiperconectada tem limitado e influenciado o dia a dia dos cidadãos.

Sobre esse assunto, consta do Relatório do plano de ação do estudo em Internet das Coisas, elaborado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES), em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC):

> A disseminação e o uso massivo de Internet das Coisas (ou Internet of Things – IoT, em inglês) irá transformar a economia e o dia a dia da população de maneira tão ou mais impactante do que a robótica avançada, tecnologias Cloud, e até mesmo do que a internet móvel. [...] Tanto gigantes multinacionais como startups já estão aproveitando essa tendência emergente de soluções tecnológicas que envolvem conexão máquina a máquina para criar novos modelos de negócios e otimizar os que já existem. Está em curso um processo irreversível de destruição criativa, termo usado pelo economista Joseph Schumpeter (1883-1950) para descrever a transformação industrial que destrói estruturas econômicas para criar outras.[207]

Os objetos conectados no universo IoT, também designados objetos (ou aparelhos ou produtos) inteligentes, são equipados com sensores capazes de captar dados pessoais relativos ao uso e consumo do aparelho. Em síntese, os produtos inteligentes possuem três elementos centrais:

---

tendo como principal objetivo teórico formar uma arquitetura de rede sólida e robusta capaz, mesmo com a queda de alguma estação, de funcionar com os computadores e ligações de comunicação restantes. Em 1969, são instalados os primeiros quatro nós dessa rede, localizados na Universidade de Los Angeles (UCLA), na Universidade da Califórnia em Santa Bárbara (UCSB), no Instituto de Pesquisas de Standford (SRI) e na Universidade de Utah. No início, a ARPANET trabalhava com diversos protocolos de comunicação, com enfoque no NCP (Network Control Protocol). No entanto, em primeiro de janeiro de 1983, quando a rede atingiu a marca de 562 hosts, todas as máquinas da ARPANET passaram a adotar como padrão os protocolos TCP/IP. Essa mudança ocasionou o crescimento ordenado da rede, pois eliminou restrições dos protocolos anteriores. A versão de protocolo utilizada, desde aquela época até os dias atuais, é a 4, comumente referida com o nome do protocolo de IPv4. Apesar dessa versão se mostrar muito robusta, de fácil implantação e interoperabilidade, seu projeto original não previu alguns aspectos como o crescimento das redes e um possível esgotamento dos endereços IP [...]; Esgotamento dos endereços IPv4 [...]. Em 1990, já existiam 313.000 hosts conectados a rede e estudos já apontavam para um colapso devido à falta de endereços. [...] Em dezembro de 1993 a IETF formalizou, através da RFC 1550, as pesquisas a respeito da nova versão do protocolo IP, solicitando o envio de projetos e propostas para o novo protocolo. Após esta definição, a nova versão do Protocolo Internet passou a ser chamado oficialmente de IPv6. (COMITÊ Gestor da Internet no Brasil. **A internet e o TCP IP**. Publicado em: 15 maio 2012. Disponivel em: <http://ipv6.br/post/introducao/>. Acesso em: 13 out. 2018).

[207] BNDES. Banco Nacional do Desenvolvimento. **Relatório do Plano de Ação**. Internet das Coisas. Nov. 2017. Disponível em: <https://www.bndes.gov.br>. Acesso em: 25 jul. 2018. Um estudo do McKinsey Global Institute estima que o impacto de IoT na economia global será de 4% a 11% do produto interno bruto do planeta em 2025 (portanto, entre 3,9 e 11,1 trilhões de dólares). Até 40% desse potencial deve ser capturado por economias emergentes. No caso específico do Brasil, a estimativa é de 50 a 200 bilhões de dólares de impacto econômico anual em 2025.

> All smart, connected products, from home appliances to industrial equipment, share three core elements: physical components (such as mechanical and electrical parts); smart components (sensors, microprocessors, data storage, controls, software, an embedded operating system, and a digital user interface); and connectivity components (ports, antennae, protocols, and networks that enable communication between the product and the product cloud, which runs on remote servers and contains the product's external operating system)[208].

São questões relacionadas ao pós-humano, que colocam em xeque a forma como o indivíduo se relaciona com o que lhe está em torno. Segundo Lucia Santaella,

> [...] em pouco tempo, minúsculos sistemas inteligentes estarão espalhados aos milhões em todo canto de nosso ambiente, incorporados às paredes, aos móveis, aos nossos aparelhos, nossa casa, nosso carro, penetrando na estrutura de nossas vidas. Será que, com isso as últimas trincheiras das velhas dicotomias epistemológicas entre sujeito e objeto irão, por fim, desabar?[209]

Além disso, é justamente nesse quadrante que emergem questões jurídicas voltadas à proteção de dados pessoais relacionadas à Internet das Coisas. Isso, porque, antes dos produtos inteligentes e conectados, dados eram primariamente obtidos por terceiros, a exemplo de pesquisas realizadas junto aos consumidores, ou por dados estruturados obtidos de provedores de aplicação na internet. A partir da IoT, a essas tradicionais fontes de dados soma-se outra, o próprio produto:

> Smart, connected products can generate real-time readings that are unprecedented in their variety and volume. Data now stands on par with people, technology, and capital as a core asset of the corporation and in many businesses is perhaps becoming the decisive asset. This new product data is valuable by itself, yet its value increases exponentially when it is integrated with other data, such as service histories, inventory locations, commodity prices, and traffic patterns. In a farm setting, data from humidity sensors can be combined with weather forecasts to optimize irrigation equipment and reduce water use. In fleets of vehicles, information about the pending service needs of each car or truck, and its location, allows service departments to stage parts, schedule maintenance, and increase the efficiency of repairs. Data on warranty status becomes more valuable when combined with data on product use and performance. Knowing that a customer's heavy use of a product is likely to result in a premature failure covered under warranty, for example, can trigger preemptive service that may preclude later costly repairs[210].

---

[208] PORTER, Michael E.; HEPPELMANN, James E. How smart, connected products are transforming companies. In: **Harvard Business Review**. Out. 2015. Disponível em: <https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies>. Acesso em: 25 jul. 2018; POSTMAN, Neil. **Technopoly**: the surrender of culture to technology. New York: Vintage Books, 1993.

[209] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.23.

[210] PORTER, Michael E; HEPPELMANN, James E. How smart, connected products are transforming companies. In: **Harvard Business Review**. Out. 2015. Disponível em: <https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies>. Acesso em: 25 jul. 2018.

De fato, a enorme quantidade de dados capturados no universo da IoT é uma grande ameaça à privacidade:

> In fact, the data deluge caused by billions of entities creating information is a big threat to privacy. Users must have tools that allow them to retain their anonymity in this superconnected world. Other tools must provide a snapshot of the information and policies surrounding a particular user, enabling transparency and preventing the notion that the IoT is silently controlling our lives. In fact, the IoT itself must seriously consider the implementation of the privacy by design principles, providing user-centric support for security and privacy from its very own foundations[211].

A disponibilidade generalizada de dados pessoais na Internet e a partir de dispositivos da Internet das Coisas, além da capacidade para encontrar correlações e criar ligações, pode tornar possível determinar, analisar e prever aspectos que digam respeito à personalidade ou ao comportamento, aos interesses e aos hábitos de uma pessoa[212].

Em 2013, a Comissão Europeia emitiu relatórios fruto de consultas públicas na área da IoT e das pesquisas e contribuições de especialistas no assunto. Dentre os diversos temas cobertos pelos relatórios estão segurança e privacidade:

> It's a matter of fact that if IoT become omnipresent – everyone (individuals and enterprises) will be concerned. Also crosslinking of objects offers new possibilities to influence and to exchange. This leads to a variety of new (as well as already known) potential risks concerning information security and both privacy and data protection, which must be considered. The severity and likeliness of each risk will depend on the circumstances in which each IoT application/system is deployed[213].

O grupo de trabalho Article 29 Working Party, em relatório emitido em 2014 sobre IoT também se posicionou pela preocupação dos desafios na área da privacidade e proteção de dados:

> The WP29 decided to issue this specific Opinion upon the consideration that IoT poses a number of significant privacy and data protection challenges, some new, some more traditional, but then amplified with regard to the exponential increase of data processing involved by its evolution. The importance of applying the EU data protection legal framework and the

[211] ROMAN, Rodrigo; ZHOU, Jianying; LOPEZ, Javier. On the features and challenges of security and privacy in distributed internet of things. **Computer Networks**, v.57, 2013, p.13.
[212] WP29 251 – Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, p.5.
[213] EUROPEAN Commission. **Report on the consultation on IoT governance**, tech. report, 16 jan. 2013. Disponível em: <https://ec.europa.eu/digitalagenda/en/news/conclusions-internetthings-public-consultation>. Acesso em: 27 jul. 2018.

> practical corresponding recommendations below must be viewed in the light of these challenges[214].

O relatório do US Government Accountability Office, de maio de 2017, observa que os dados pessoais coletados por meio da Internet das Coisas, provavelmente, exibirão "um grau sem precedentes de *intimacy*"[215].

Em vista de uma ordem de grandeza sobre a quantidade de dados capazes de serem capturados pela onda da Internet das Coisas, há a estimativa indicada pela Federal Trade Commission dos Estados Unidos: cerca de 10 mil habitantes podem gerar 150 milhões de dados informativos diariamente[216]. A pseudo solução para tamanha coleta e processamento de dados seria o caminho da anomização dos dados, a fim de preservar a identidade dos indivíduos, garantindo-lhes proteção à privacidade e dados pessoais. Porém, algumas pesquisas já demonstraram exaustivamente a facilidade de reidentificar dados anonimizados[217].

Além disso, mesmo nas situações em que objetos inteligentes interajam entre si, sem intermediação humana, os indivíduos são afetados:

> Even in the case of applications that don't directly target human beings, such as an industrial process in a factory, indirect information about humans can be collected and inferred. For a vast number of cases, the availability of devices and sensors in an environment can drastically increase the amount of personal data being gathered. That contributes to blurring the boundaries between a "physical world" and cyberspace, in the sense that many actions we perform will be monitored, recorded, and used[218].

A despeito dos incontáveis benefícios trazidos pela IoT, seu impacto negativo pode ser agravado porque os dados capturados dos sensores dos dispositivos podem ser utilizados conjuntamente aos dados pessoais já disponíveis, de forma a incrementar correlações e cruzamento de dados que podem ser feitos sem nenhum controle[219].

---

[214] ARTICLE 29 Data protection working party, Opinion 8/2014. **Recent developments on the internet of things**, tech. report, 16 set. 2014. Disponível em: <https://www.pdpjournals.com/docs/88440.pdf>. Acesso em: 27 jul. 2018, p.6.

[215] UNITED STATES Government Accountability Office (GAO). **Internet of things**, maio 2017. Disponível em: <http://www.gao.gov/assets/690/684590.pdf>. Acesso em: 22 out. 2018, p.35.

[216] FEDERAL TRADE COMMISION. **FTC staff report**. Internet of things. Privacy & Security in a connected world. Jan.2015. Disponível em: <https://www.ftc.gov/>. Acesso em: 27 ago. 2018, p.14.

[217] Sobre pseudoanonimização de dados, ver: MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV, 2018, p.97-98.

[218] DONEDA, Danilo; ALMEIDA, Virgílio; MONTEIRO, Marília. Governance challenges for the internet of things. **IEE Computer Society**, v.19, n.4, p.56-59, 2015, p.2.

[219] DONEDA, Danilo; ALMEIDA, Virgílio; MONTEIRO, Marília. Governance challenges for the internet of things. **IEE Computer Society**, v.19, n.4, p.56-59, 2015, p.3.

A disseminação de sensores é um ponto de atenção, por meio dos quais se aumentará a quantidade e a precisão dos dados coletados dentro das *cidades inteligentes.* Paradoxalmente a inteligência pode estar relacionada a devastar a vida de seus indivíduos. Não há como ser inteligente se não houver felicidade e bem comum, cujos valores, por sua vez, não podem ser apropriados pelo homem se não lhe forem respeitadas suas garantias individuais. A *smart city,* nessa toada, pode ser considerada hiperinteligência, porém dissociada de uma felicidade que vem sendo dissipada, ao se negar o próprio indivíduo, dentro da nova paisagem da *urbe.* Sob outra perspectiva, pode ser dito que um dos preços cobrados pela estrutura "inteligente" de uma sociedade é torná-la fadigada, cansada da própria tecnologia que lhe serve.

Porém, adverte Lucia Santaella, "não há cidades sem que sejam vivificadas pela dinâmica dos cidadãos que nelas habitam, trabalham, movimentam-se, divertem-se, angustiam-se e continuamente a transformam"[220]. Portanto, mais importante e determinante do que a tecnologia que serve ao indivíduo, é como o indivíduo servido pela tecnologia estabelece sua dinâmica em sociedade:

> As cidades e os corpos tornaram-se ubíquos pelo simples fato de que também se tornaram líquidos. À fisicalidade sólida das cidades e dos corpos vivos e dinâmicos aderiu-se a invisibilidade ubíqua dos "espaços informacionais" líquidos. Esses dados informacionais invisíveis, líquidos, ubíquos tomaram conta da superfície do planeta e nos rodeiam, onde quer que estejamos. É comum pensar que os dados estão na nuvem, mas eles baixam para nossas mãos e se dispõem ao nosso olhar ao toque de dedos. Isso está levando ao crepúsculo as tradicionais noções de espaço e tempo cuja crise os debates da pós-modernidade já haviam, até certo ponto, antecipado. Hoje os fluxos hipercomplexos da hipermobilidade urbana e social têm sido designados como cidades híbridas, cidades líquidas, cidade-ciborgue, cibercidade, cidade virtual, cidade como interface [...][221]

Qualquer tecnologia pode exercer grande impacto, alterando processos dos mais básicos possíveis. Segundo Neil Postman, as tecnologias não são neutras até que sejam colocadas para uso pelos seres humanos – para o bem ou para o mal. É dizer, o uso que é feito de qualquer tecnologia é amplamente determinado pela forma da própria tecnologia[222].

A realidade da Internet das Coisas concretiza o fenômeno da datificação, é dizer, os atos da vida são colocados em dados. O que antes pertencia ao mundo

---

[220] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.62.
[221] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p. 70.
[222] POSTMAN, Neil. **Technopoly**: the surrender of culture to technology. New York: Vintage Books, 1993.

analógico, passa a estar integrado no mundo *on-line*, gerando volumosos conjuntos de dados. A datificação proporcionada pela Internet das Coisas, portanto, aumentará exponencialmente a captura e o tratamento de dados pessoais, de diversas naturezas. Por meio de aparelhos conectados em todo lugar e a todo instante, e por meio de algoritmos, é possível perfilar rotinas de higiene, hábitos de exercícios físicos, preferencias de cardápio, costumes de vestuários e tantos outros dados dos indivíduos que serão coletados.

2.4 Entropia dos algoritmos e aprendizagem de máquina

A base do algoritmo é a matemática. Costuma-se comparar um algoritmo a uma receita de comida. São comandos que, quando atendidos, ao final, formam o produto esperado. Outro exemplo comparativo é o cálculo de índice de massa corporal. Com base no cálculo do (IMC), um algoritmo pode ser facilmente explicado. Para calcular referido índice é necessário usar uma fórmula matemática (IMC = peso ÷ altura x altura). Neste simples exemplo, o "problema" da avaliação do peso corporal foi calculado usando uma fórmula matemática (algoritmo). Isso pode ser calculado por meio de uma ferramenta, mas também no papel. Outros exemplos de algoritmo seriam instruções de uso, regras do jogo, manuais de construção e funções *hash*, dentre outros. Associado à ciência da computação, um algoritmo pode ser definido como um conjunto de instruções sobre como um computador deve realizar uma tarefa específica.

De modo geral, um algoritmo oferece uma maneira de resolver um problema. Com base nesse plano de solução, os dados de entrada são convertidos em dados de saída em etapas únicas. Assim, é possível afirmar que um algoritmo é qualquer procedimento de computador bem definido que possua algum valor agregado na qualidade de suas entradas (*input*), gerando outros valores na saída (*output*), de forma que pode ser considerado uma ferramenta para resolver um problema[223].

Especialmente na ciência da computação, os algoritmos desempenham um papel importante. Eles representam uma base de programação e são independentes de uma linguagem de programação específica. No entanto, os algoritmos não são encontrados apenas em ciência da computação ou matemática. Eles não são

[223] CORMEN, Thomas H.; LEISERSON, Charles E.; RIVEST, Ronald L., STEIN, Clifford. **Introduction to algorithms**. 3.ed. Massachusetts–EUA, The MIT Press, 2009, p.5-6.

executados mecanicamente por um computador, mas podem ser formulados e processados por pessoas em linguagem "natural".

Os algoritmos são usados por diversas organizações para a tomada de decisões e alocação de recursos, tendo por base grandes conjuntos de dados. Combinando cálculo, processamento e raciocínio, os algoritmos podem ser excepcionalmente complexos, codificando milhares de variáveis em milhões de pontos de dados[224]. Desse modo, decisões importantes sobre a vida das pessoas são cada vez mais ocasionadas por sistemas computacionais e algoritmos, como direcionar vagas de empregos e conceder crédito. Fato é que os algoritmos estão moldando nossas vidas. A questão é como os algoritmos, fechados em suas estruturas e definições, podem limitar oportunidades e, principalmente colocar em risco direitos fundamentais dos cidadãos.

Sua etimologia remonta ao sistema de numeração decimal posicional hindu[225]. Um dos algoritmos mais antigos de que se tem notícia é o algoritmo de Euclides, cuja obra *Elementos* remonta a 300 a.C.[226] A inteligência foi associada aos computadores, delegando-lhes a execução das regras. Assim, com o poder dos computadores, o trabalho de execução dos algoritmos foi alargado e sofisticado desde sua origem.

Conforme se verá adiante, os algoritmos não coincidem com a criação dos sistemas computacionais; apesar de hoje estarem praticamente indissociados do computador, com este não se confundem. É nesse sentido a definição da organização Article 19:

---

[224] CAPLAN, Robyn; DONOVAN, Joan; HANSON, Lauren; MATTHEWS, Jeanna. Algorithmic accountability: a primer. **Data & Society**. Publicado em 18 abr. 2018. Disponível em:<https://datasociety.net/output/algorithmic-accountability-a-primer/>. Acesso em: 26 ago. 2018.

[225] MOL, Rogério Santos. **M717i Introdução à história da matemática**. Belo Horizonte: CAED-UFMG, 2013, p.67: um dos mais notáveis estudiosos vinculados a essa academia foi o matemático e astrônomo Muhammad ibn Musa al-Khwarizmi (c. 780-850). Duas de suas obras exerceram uma influência decisiva nos rumos tomados pela matemática. A primeira delas é o tratado de aritmética intitulado 'Livro da Adição e da Subtração segundo o Cálculo dos Indianos'. Em seu texto são discutidos o sistema de numeração decimal posicional hindu e as operações feitas nesse sistema, incluindo a multiplicação e a divisão. Séculos mais tarde, as traduções latinas desse livro criariam na Europa a impressão de que o sistema de numeração nele descrito eram uma criação de seu autor. Os numerais indo-arábicos ficaram então conhecidos com sendo de al-Khwarizmi, o que resultou nas palavras algarismo e algoritmo, incorporadas às línguas europeias modernas.

[226] Trata-se de método para encontrar o máximo divisor comum entre dois números inteiros diferentes de zero (MOL, Rogério Santos. **M717i Introdução à história da matemática**. Belo Horizonte: CAED-UFMG, 2013, p.51): As duas primeiras proposições do livro VII de Euclides apresentam aquilo que hoje é conhecido como o algoritmo de Euclides para encontrar o maior divisor comum (maior medida comum, na linguagem de Euclides) de dois números. O processo é uma aplicação repetida do Postulado de Eudoxo.

> Algorithm can refer to any instruction, such as computer code, that carries out a set of commands: this is essential to the way computers process data. […] it refers to 'encoded procedures for transforming input data into the desired output, based on specific calculations[227].

Hoje em dia, até mesmo uma obra artística pode ser executada por um algoritmo. Artistas algorítmicos, também conhecidos por algoristas[228], são aqueles que introduzem e controlam algoritmos originais no seu trabalho de criação. Exemplo, nesse sentido, é a obra 'The next Rembrandt'[229], elaborada em 2017, por um grupo de holandeses, financiada pelas empresas ING e Microsoft, com apoio do museu 'Het Rembrandthuis'. Esse grupo desenvolveu algoritmos capazes de capturar as características do artista do século XVII, a partir de suas famosas obras, resultando em uma nova pintura, a qual, quiçá, pudesse ser atribuída ao pintor impressionista holandês, por um crítico de arte[230]. O mesmo ocorre no mundo da música, com o hiperinstrumento[231], resultante do emprego de algoritmos que transcendem os limites tradicionais do humano no processo criativo, redefinindo a expressão musical.

---

[227] Tradução livre: Algoritmo pode se referir a qualquer instrução, como código de computador, que executa um conjunto de comandos: isso é essencial para o modo como os computadores processam os dados. Para os propósitos deste documento, ele se refere a "procedimentos codificados para transformar dados de entrada na saída desejada, com base em cálculos específicos". (ARTICLE 19 Global Human Rights Organisation. **Privacy and freedom of expression In the age of artificial intelligence**, abr. 2018. Disponível em: <https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf>. Acesso em: 26 ago. 2018, p.6).

[228] O neologismo é atribuído a Roman Verostko, pioneiro da arte algorítmica. (VEROSTKO, Roman. **Algorithmic**. Disponível em: <http://verostko.com/algorithm.html>. Acesso em: 26 ago. 2018).

[229] CAN the great master be brought back to create one more painting? Disponível em: <https://www.nextrembrandt.com>. Acesso em: 14 ago.2018.

[230] Sobre críticas contemporâneas à "catástrofe da arte", ver: VIRILIO, Paul; LOTRINGER, Sylvère. **The accidente of art**. Tradução de Mike Taormina. Nova Iorque, 2005: "There is a catastrophe within contemporary art. What I call the "optically correct" is at stake. The vision machine and the motor have triggered it, but the visual arts haven't learned from it. Instead, they've masked this failure with commercial success. This "accident" is provoking a reversal of values. In my view, this is positive: the accident reveals something important we would not otherwise know how to perceive". Tradução livre: "Existe uma catástrofe na arte contemporânea. O que eu chamo de 'oticamente correto' está em jogo. A máquina de visão e o motor provocaram isso, mas as artes visuais não aprenderam com isso. Em vez disso, eles mascararam essa falha com sucesso comercial. Esse "acidente" está provocando uma reversão de valores. Na minha opinião, isso é positivo: o acidente revela algo importante que, de outra forma, não saberíamos perceber".

[231] Termo proposto por Tod Machover, professor de música e tecnologia do Media Lab do Massachusetts Institute of Technology (MIT), nos Estados Unidos da América, um dos principais centros de tecnologia do mundo e que ousa unir o mundo da música erudita à era digital. (CAMPOS, Cleber da Silveira; MANZOLLI, Jônatas. Sistemas interativos musicais aplicados à percussão mediada. **XX Congresso da Associação Nacional de Pesquisa e Pós-Graduação em Música**. Florianópolis, 2010. Disponível em: <http://repositorio.ufrn.br>. Acesso em: 26 ago. 2018): "[...] a partir de 1985 foram desenvolvidas novas interfaces inicialmente para serem executadas por músicos virtuosos e posteriormente (anos 90) por "leigos". O objetivo foi estabelecer relações diretas com ações humanas e não apenas simular ou substituí-las. Nessa época, surgiram as suas primeiras "invenções", as quais Machover viria posteriormente denominar Hyperinstruments. Exemplos desses instrumentos são a Cadeira Sensorial, a qual através de um campo elétrico invisível, detecta-se o movimento do corpo de uma pessoa, transformando-o em diversos sons. Há outras invenções como a tela melódica (mesa digital onde manipula-se uma melodia); árvores falantes (grava vozes e interage com a internet em tempo real); muro dos gestos (captação de movimentos e gestos transformados em sons)" (p.2).

Os algoritmos possuem as seguintes características[232]: a) sem ambiguidade: um algoritmo não deve ter uma descrição contraditória. Deve ser único; 2) executabilidade: cada etapa deve ser executável; 3) finitude: a descrição do algoritmo deve ser finita; 4) entrega: após um número finito de etapas, o algoritmo deve terminar e entregar um resultado; 5) determinação: o algoritmo deve sempre dar o mesmo resultado sob as mesmas condições; 6) determinismo: em qualquer momento da execução, há no máximo uma possibilidade de continuação. O passo subsequente é, portanto, determinado de maneira única.

Uma das principais decisões tomadas pelos algoritmos é a relevância de cada conjunto de dados para outros pontos de dados. Os dados são coletados e tratados para finalidades, em regra, de perfilamento[233]. Determinar o perfil do indivíduo pode valer muito a anunciantes, a seguradoras, e ao próprio Estado. A China, por exemplo, país de 1,4 bilhão de habitantes, tem utilizado uma combinação de vigilância, algoritmos, inteligência artificial e uma imensidão de dados para monitorar a vida e o comportamento das pessoas em detalhes minuciosos[234].

Na área privada, é conhecido o caso de como a rede de lojas Target descobriu que uma adolescente estava grávida antes de seu pai, com base em análise do perfil de compras: a rede de lojas Target, com base no perfil de compras de uma adolescente, constatou que havia uma chance de 87% dela estar grávida,

---

[232] CZERNIK, Agnieszka. **Was ist ein algorithmus**. Definition und Beispiele, 14.10.2016. Disponível em: <https://www.datenschutzbeauftragter-info.de/was-ist-ein-algorithmus-definition-und-beispiele/>. Acesso em: 19 nov.2018.

[233] Segundo o artigo 4 (4) da GDPR: “Definição de perfis”: qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

[234] Para uma visão mais detalhada de como a China tem incorporado uma sociedade de dados para sustentar seus interesses políticos e econômicos, ver: LARSON, Christina. Who needs democracy when you have data? Publicado em: 20 ago. 2018 In: Massachusetts Institute of Technology. **Technology Review**. Disponível em: <https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/>. Acesso em: 27 ago. 2018. Da reportagem, destacamos: “Nenhum governo tem um plano mais ambicioso e de tanto alcance para utilizar o poder dos dados para mudar a maneira como governa, do que o governo chinês", diz Martin Chorzempa, do Instituto Peterson de Economia Internacional, em Washington, DC. Tradução livre de: “No government has a more ambitious and far reaching plan to harness the power of data to change the way it governs than the Chinese government,” says Martin Chorzempa of the Peterson Institute for International Economics in Washington, DC.” E ainda sobre o assunto do Sistema de Crédito Social Chinês, por meio de um programa de pontuação sobre os seus cidadãos, classificando-os de acordo com as informações contidas em um enorme banco de dados, alimentado com milhares de informações pessoais (em grande maioria coletadas pela internet), tais como histórico de navegação na internet, itens adquiridos em compras, probabilidade de adimplemento das obrigações, etc., vide: GOMES, Rodrigo Dias de Pinho. **Big Data**: desafios à tutela da pessoa humana na sociedade da informação. Rio de Janeiro: Lumen Juris, 2017, p.50-51. Por fim, importante ressaltar que a tutela à privacidade e proteção de dados na China não é comparável à proteção conferida no Ocidente. Nos últimos anos, entretanto, vários casos foram julgados pelos tribunais chineses sobre o assunto e iniciativas legislativas estão sendo desenvolvidas. Para um panorama da privacidade e proteção de dados na China, ver: ONG, Rebecca. Recognition of the right to privacy on the Internet in China. **International Data Privacy Law**, v.1, 3.ed. ago. 2011, p.172-179. Disponível em: <https://doi.org/10.1093/idpl/ipr008>. Acesso em: 10 out. 2018.

com previsões, inclusive, da data do parto. Diante dessa constatação, a rede de lojas passou a enviar cupons de descontos para sua casa. Quando seu pai viu que a filha estava recebendo esse material, dirigiu-se furioso ao Target para conversar com o gerente e reclamar pelo fato de a loja incentivar a gravidez em uma adolescente, visto qu a filha ainda estava no ensino médio. O gerente se desculpou e ligou alguns dias depois para fazê-lo novamente. Na ocasião, o pai, ao telefone, disse ao gerente que quem devia desculpas era ele, pois descobrira que a filha estava realmente grávida e que o parto estava programado para o mês exato estimado pela loja. Isso só foi possível pois os algoritmos dos bancos de dados da rede de lojas foram programados para estabelecer uma determinada correlação, visando identificar, dentre suas consumidoras, quais teriam mais chances de estar grávidas e, portanto, teriam maior probabilidade de comprar determinados produtos.

Os algoritmos, desde certo tempo, podem ser criados para identificar, portanto, os perfis e respectivos padrões de comportamento de consumo dos indivíduos, visando prever quais serão as próximas aquisições.

Existe uma vigilância permanente sobre os indivíduos, que alimenta a máquina propulsora de consumo da economia atual, baseada em dados pessoais. Na atual sociedade da informação, existe uma fusão entre o homem e a técnica que está se tornando mais crucial e problemática[235].

A utilização de algoritmos não é nova, porém, recentemente ganhou maior relevância, tanto pela atenção popular, como pela qualidade de objeto de estudos e pesquisas, inclusive na área jurídica. Alguns fatores, segundo Jatinder Singh, Ian Walden, Jon Crowcoft e Jean Bacon levaram a essa maior conscientização, tal qual o surgimento do *Big Data* e da Internet das Coisas, como fontes crescentes de dados pessoais, cujo fenômeno à luz da "revolução dos dados", está motivando a pesquisa por novas percepções e soluções baseadas em dados:

> there is a need for new and better mechanisms for dealing with the volume of data available: to assist in finding the signals within the noise, the needles within the ever-growing haystacks; as well as for increasing scope for automation[236].

[235] SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.14. Segundo a autora, plástico, moldável, inacabado, versátil, o ser humano tem se configurado de diversas maneiras pelas histórias e pelas geografias. Mas parece terem sido as sociedades baseadas na economia capitalista – desenvolvidas nos últimos três séculos no mundo ocidental – as que inventaram o leque mais abundante de tecnologias para a moldagem de corpos e de subjetividade.

[236] SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. **Responsibility and machine learning**: part of a process. Publicado emj: 27 out. 2016. Disponível em: <https://ssrn.com/abstract=2860048>. Acesso em: 18 out. 2018, p.2. Tradução livre: Há necessidade de novos e melhores mecanismos para lidar com o volume de

Como um algoritmo é formulado, seu escopo para erro ou correção, o impacto que pode ter em um indivíduo – e sua capacidade de compreender ou contestar essa decisão – são questões cada vez mais relevantes.

É inegável que os algoritmos desempenham um papel cada vez mais importante no mundo. Os programas e aplicativos de software, os algoritmos estão alimentando a todo momento nossos *devices*. Os algoritmos ajudam a filtrar e refiltrar as informações no mundo. Encontramos algoritmos diariamente no trabalho, em nosso tempo livre, enfim, são uma parte indispensável da vida contemporânea. Principalmente útil, mas nem sempre seguro[237], os algoritmos estão se tornando cada vez mais importantes.

Os computadores com os quais interagimos diariamente têm um conjunto de algoritmos extremamente básicos, conhecidos como Basic Input/Output System (BIOS), que dizem às partes mecânicas do computador o que fazer. No topo desses algoritmos, é executado o sistema operacional que pode iniciar outros programas de software e desligá-los. E todos os programas que usamos, de navegadores da Web a processadores de texto, são algoritmos reunidos para realizar tarefas específicas[238]. Eles estão ainda nos sistemas de navegação, indicando o caminho mais curto; nos embates em jogos contra "a máquina", na indicação de um parceiro adequado em encontros *on-line*, dentre tantos outros exemplos[239].

O algoritmo responde a entradas e saídas específicas antecipadas pelo programador. Se algo der errado, o programador pode voltar às instruções do programa para descobrir o que houve e corrigi-lo.

Os algoritmos que trarão maior complexidade quanto aos efeitos no campo jurídico são aqueles afetos à categoria dos que são capazes de aprender. Segundo Andrew Tutt, esses algoritmos são conhecidos por muitos nomes: *machine learning*, *predictive analytics* e *artificial intelligence*[240], dentre outros. Os algoritmos desse tipo já são onipresentes. Cuida-se da ubiquidade algoritmica. Como o Google adivinha

---

dados disponíveis: para ajudar a encontrar os sinais dentro do ruído, as agulhas dentro dos montes de feno sempre crescentes; bem como para aumentar o escopo de automação.

[237] CZERNIK, Agnieszka. **Was ist ein algorithmus**. Definition und Beispiele, 14.10.2016. Disponível em: <https://www.datenschutzbeauftragter-info.de/was-ist-ein-algorithmus-definition-und-beispiele/>. Acesso em: 19 nov.2018.

[238] TUTT, Andrew. An FDA for Algorithms. Publicado em: 15 mar. 2016. In: **69 Admin. L. Rev**. 83, 2017. Disponível em: <https://ssrn.com/abstract=2747994>. Acesso em: 18 nov. 2018, p.92.

[239] CZERNIK, Agnieszka. **Was ist ein algorithmus**. Definition und Beispiele, 14.10.2016. Disponível em: <https://www.datenschutzbeauftragter-info.de/was-ist-ein-algorithmus-definition-und-beispiele/>. Acesso em: 19 nov.2018.

[240] TUTT, Andrew. An FDA for Algorithms. Publicado em: 15 mar. 2016. In: **69 Admin. L. Rev**. 83, 2017. Disponível em: <https://ssrn.com/abstract=2747994>. Acesso em: 18 nov. 2018, p.94.

se uma consulta de pesquisa foi digitada incorretamente? Como o Netflix escolhe quais filmes ou séries o indivíduo teria interesse? Como a Amazon sugere produtos de interesse do cliente? Como o Facebook e o Instagram organizam seus *feeds*? Resposta a todas essas perguntas: algoritmos de aprendizado de máquina.

Vale lembrar, ainda, o episódio do virus H1N1 e o trabalho dos algoritmos do Google. Em 2009, o H1N1 estava se espalhando rapidamente. Os centros de controle e prevenção de doenças, nos Estados Unidos, conseguiam rastrear a disseminação da doença com um atraso de duas semanas apenas. Diante disso, o Google lançou um algoritmo que usava termos de pesquisa como recurso procurando correlações entre os termos de pesquisa e as taxas de infecção por H1N1[241]. Foi, então, que o algoritmo parametrizou 45 termos de pesquisa que poderiam ser usados para prever onde o H1N1 estava em tempo real, sem um atraso de duas semanas, com capacidade de mapear a doença em todo território nacional e por regiões específicas, incluindo a pesquisa por Estados. Os engenheiros do Google publicaram um artigo na revista científica Nature[242] causando grande *frisson* entre os funcionários de sanidade pública e entre os científicos da computação[243].

A técnica *machine learning é* um subconjunto da inteligência artificial extremamente significativa uma vez que programas desse segmento se aprimoram com a própria experiência. Além disso, têm capacidade de aprender sem programação específica para tanto, posto que podem alterar e melhorar seus algoritmos por conta própria. Conforme explica Andres Munoz:

> Arthur Samuel in 1959 defined machine learning as the “field of study that gives computers the ability to learn without being explicitly programmed”. At the beginning this field was mainly algorithmic and without much foundations, it was probably thanks to the work of Valiant who introduced the

[241] “Dado que Google recibe más de tres mil millones de consultas a diario y las archiva todas, tenía montones de datos con los que trabajar. Google tomó los cincuenta millones de términos de búsqueda más corrientes empleados por los estadounidenses y comparó esa lista con los datos de los CDC sobre propagación de la gripe estacional entre 2003 y 2008. La intención era identificar a los afectados por el virus de la gripe a través de lo que buscaban en internet. Otros ya habían intentado hacer esto con los términos de búsqueda de internet, pero nadie disponía de tantos datos, capacidad de procesarlos y know-how estadístico como Google”. (MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**. La revolución de los datos masivos. Tradução de Antonio Iriarte. Madri: Turner, 2013, p.3).

[242] GINSBERB, Jeremy; MOHEBBI, Matthew H.; PATEL, Rajan S.; BRAMMER, Lynnette; SMOLINSKI, Mark S.; BRILLIANT, Larry. Detecting influenza epidemics using search engine query data. **Nature**, v.457, 19 fev. 2009, p.1012-1014.

[243] Sobre os desdobramentos do assunto, ver: LAZER, David; KENNEDY, Ryan; KING, Gary; VESPIGNANI, Alessandro. The parable of Google flu: traps in big data analysis.**Science** v.343, 14 mar.2014, p.1203-1205; BUTLER, Declan. When Google got flu wrong. **Nature**, 14 fev.2013, v.494, p.155-156; LAZER, David; KENNEDY, Ryan. What we can learn from the epic failure of Google flu trends. **Wired**, 10 jan. 2015. Disponível em: <https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/>. Acesso em: 19 nov.2018.

> framework of PAC learning (probably approximately correct learning) that a real theory of the learnable was established. Another milestone in the theory of learning was set by Vapnik in Vapnik casts the problem of 'learning' as an optimization problem allowing people to use all of the theory of optimization that was already given. Nowadays machine learning is a combination of several disciplines such as statistics, information theory, theory of algorithms, probability and functional analysis. But […] optimization is still at the heart of all modern machine learning problems[244].

Os algoritmos de aprendizagem de máquina trabalham para descobrir padrões em dados, para construir e refinar modelos matemáticos de dados que podem ser usados para fazer previsões, e, ainda, descrever dados para ganhar conhecimento e *insight.* Implica padrões de aprendizagem e relacionamentos a partir dos dados para construir modelos generalizáveis que, quando exposto a dados novos ou não vistos, ajudam em uma série de tarefas gerais, incluindo categorização, perfil, priorização, filtragem e previsão[245]. Estão associados a uma combinação de várias disciplinas, como à estatística, à teoria da informação, à teoria dos algoritmos e à probabilidade.

Aplicações práticas de *machine learning* implicam na presença de determinadas funcionalidades, como o reconhecimento de imagem e fala, o processamento de linguagem natural (*natural language processing* – NLP), análises preditivas (um ramo de *data mining*), e *deep learning,* cujas funcionalidades permitem que os computadores "vejam" e "distinguam" objetos e textos em imagens e vídeos. Segundo Dimitra Kamarinou, Christopher Millar e Jatinder Singh,

> Industry applications are also diverse, ranging from using machine learning technology in the banking system to detect fraud, in the media and entertainment sector to predict users' preferences and provide product recommendations, to using deep learning in healthcare to identify patterns in health data and reveal hidden causal relationships between biological data and drug compounds.Meanwhile, IBM's Watson is receiving training in

[244] MUNOZ, Andres. **Machine learning and optimization**. Courant institute of mathematical sciences. New York. Disponível em < https://cims.nyu.edu/~munoz/files/ml_optimization.pdf >. Acesso em 18 out. 2018. Tradução livre: Arthur Samuel, em 1959, definiu o aprendizado de máquina como o "campo de estudo que dá aos computadores a capacidade de aprender sem serem programados explicitamente". No início, este campo era principalmente algorítmico e sem muitos fundamentos, provavelmente foi graças ao trabalho de Valiant, que introduziu a estrutura do aprendizado do PAC (aprendizado Provável e Aproximadamente Correto) que uma teoria real do aprendível foi estabelecida. Outro marco na teoria da aprendizagem foi definido por Vapnik em Vapnik, que coloca o problema do "aprendizado" como um problema de otimização, permitindo que as pessoas usem toda a teoria da otimização que já foi dada. Atualmente, o aprendizado de máquina é uma combinação de várias disciplinas, como estatística, teoria da informação, teoria dos algoritmos, probabilidade e análise funcional. Mas [...] a otimização ainda está no centro de todos os problemas modernos de aprendizado de máquina.

[245] SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. **Responsibility and machine learning**: part of a process. Publicado emj: 27 out. 2016. Disponível em: <https://ssrn.com/abstract=2860048>. Acesso em: 18 out. 2018, p.3-4.

> diagnostics from specialists at the Memorial Sloan Kettering Cancer Center[246].

Uma evolução dessa técnica está atrelada ao *deep learning*[247]. Em que pese vários benefícios trazidos pelo avanço do *deep learning*, a complexidade da estrutura de seus algoritmos desafia ainda mais transpassar a característica *opaca* dos algoritmos[248]. Esse predicativo é aplicado quando a estrutura do algoritmo ou da rede neural artificial provê pouca luz e visão sobre a estrutura ou modelo subjacente, conforme se verá com mais detalhes no quarto capítulo.

Além disso, grande parte do aumento do entusiasmo em relação ao *machine learning* decorre de sua promessa de possibilitar novos *insights* e eficiências em uma ampla gama de áreas, com destaque para medicina, transportes, cybersegurança e finanças.

Segundo Jatinder Singh, Ian Walden, Jon Crowcroft e Jean Bacon,

> Much of the surge in enthusiasm regarding ML stems from its promise of enabling new insights and efficiencies in a wide range of areas,4 including medicine (diagnostics, precision medicine), finance (fraud detection, trend prediction), transport (automated cars, traffic management), cyber security (intrusion detection) to name but a few. ML is already actively used in a number of areas, for example for voice and handwriting recognition, spam detection, automated translation, and e-commerce recommendation systems[249].

---

[246] KAMARINOU, Dimitra; MILLARD, Christopher; SINGH, Jatinder. Machine learning with personal data (November 7, 2016). **Queen Mary School of Law Legal Studies**. Research Paper n.247, 2016. Tradução livre: Os aplicativos do setor também são diversos, desde o uso de tecnologia de aprendizado de máquina no sistema bancário para detectar fraudes, no setor de mídia e entretenimento para prever preferências de usuários e fornecer recomendações de produtos, usando aprendizagem profunda em saúde para identificar padrões em dados de saúde e revelar relações casuais ocultas entre dados biológicos e compostos de medicamentos. Enquanto isso, o Watson da IBM está recebendo treinamento em diagnósticos de especialistas do Memorial Sloan Kettering Cancer Center.

[247] Deep learning é um tipo de machine learning que treina computadores para realizar tarefas como seres humanos, o que inclui reconhecimento de fala, identificação de imagem e previsões, por meio de várias arquiteturas tais como redes neurais.

[248] There is, however, ongoing research into mechanisms for rule extraction, to assist in understanding by extracting knowledge from more opaque approaches and expressing it in a more intelligible form, such as a decision tree. There are also ways to try to describe what aspects of the input led to a particular decision (rather than describing the model as a whole) such as highlighting features of an image that led to a particular classification. These assist in assessing the appropriateness of the model. Control tends to be more challenging for the more opaque models; though there is continuing work on general means for improving and providing control (such as 'fairness') across approaches (SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. **Responsibility and machine learning**: part of a process. Publicado em: 27 out. 2016. Disponível em: <https://ssrn.com/abstract=2860048>. Acesso em: 18 out. 2018, p.7). Tradução livre: Há, no entanto, pesquisas contínuas sobre mecanismos de extração de regras, para auxiliar na compreensão, extraindo conhecimento de abordagens mais opacas e expressando-as de uma forma mais inteligível, como uma árvore de decisão. Há também maneiras de tentar descrever quais aspectos da entrada levaram a uma decisão específica (em vez de descrever o modelo como um todo), como destacar recursos de uma imagem que levaram a uma classificação específica. Estes auxiliam na avaliação da adequação do modelo. O controle tende a ser mais desafiador para os modelos mais opacos; embora haja trabalho contínuo em meios gerais para melhorar e fornecer controle (como "equidade") em várias abordagens.

[249] SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. **Responsibility and machine learning**: part of a process. Publicado emj: 27 out. 2016. Disponível em: <https://ssrn.com/abstract=2860048>. Acesso em: 18 out. 2018, p.2. Tradução livre: Grande parte do aumento do entusiasmo em relação ao ML decorre de sua

É graças aos algoritmos de *machine learning* que feitos antes vistos apenas em filmes de ficção se tornaram realidade, como computadores que se comunicam com seres humanos, que dirijem carros de forma autônoma, que escrevem e publicam relatórios de jogos esportivos e que localizam suspeitos de terrorismo[250].

Em relação ao assunto, Andrew Tutt alerta que essa nova família de algoritmos deve causar preocupação. Segundo o autor, eles não são programados para resolver problemas específicos, mas para aprender a resolver problemas. Para Andrew Tutt, algoritmos ligados ao aprendizado de máquina que tentam prever quais filmes as pessoas vão querer assistir, ou qual marca de sabão elas vão querer comprar, por exemplo, não são necessariamente perigosos se falharem. Porém, os algoritmos vinculados ao *machine learning* também são usados para resolver problemas que algoritmos comuns nunca resolveram antes. Nesse caso, em muitas dessas aplicações, representam riscos significativos para indivíduos e para a sociedade se vierem a falhar (tais quais algoritmos de aprendizado de máquina consultados para fazer diagnósticos médicos e auxiliar em cirurgias). Em muitas dessas aplicações, a vida das pessoas pode depender da segurança e da eficácia desses algoritmos. No entanto, devido a sua enorme complexidade, pode ser quase impossível saber com antecedência quando e como eles irão falhar[251].

Segundo Andrew Tutt, esses algoritmos guardam uma enorme promessa, mas também apresentam novos e incomuns perigos. Algoritmos de aprendizado de máquina resolverão problemas que a programação preditiva comum nunca conseguiu. Mas os algoritmos de aprendizado de máquina são imprevisíveis, quase por definição. Eles são programados para aprender a resolver problemas, depois são ensinados a resolver esses problemas e, depois, são solicitados a resolver esses problemas em situações extremas no mundo real. Mas como os algoritmos de aprendizado de máquina aprendem – e como raciocinam da experiência à prática –

---

promessa de possibilitar novos insights e eficiências em uma ampla gama de áreas, incluindo medicina (diagnósticos, medicina de precisão), finanças (detecção de fraudes, previsão de tendências), transporte (carros automatizados, gerenciamento de tráfego), segurança cibernética (detecção de intrusão), para citar apenas alguns. Machine Learning já é usado ativamente em um número de áreas, por exemplo, para reconhecimento de voz e escrita, detecção de spam, sistemas de recomendação de tradução e e-commerce.

[250] MARR, Bernard. A short history of machine learning – every manager should read. **Forbes**. Publicado em: 19 fev. 2016. Disponível em: <https://www.forbes.com/sites/bernardmarr/2016/02/19/a-short-history-of-machine-learning-every-manager-should-read/#20f5f5e15e78>. Acesso em: 21 out. 2018.

[251] TUTT, Andrew. An FDA for algorithms. Publicado em: 15 mar. 2016. In: **69 Admin. L. Rev**. 83, 2017. Disponível em: <https://ssrn.com/abstract=2747994>. Acesso em: 18 nov. 2018, p. 85. Segundo o autor, aprendizado de máquina não é coisa de ficção científica ou de um futuro distante. Algoritmos sofisticados de aprendizado de máquina já estão sendo usados.

é quase inteiramente alienígena[252]. Os algoritmos de aprendizado de máquina não aprendem nem raciocinam como os humanos, e isso pode dificultar a previsão e a dificuldade de explicar seus resultados. A consequência é que, em algumas das aplicações mais importantes para as quais eles poderiam um dia ser colocados, estaremos confiando nossos destinos a máquinas que não conhecemos e talvez nem possamos entender. Existem exemplos de algoritmos de aprendizado de máquina que falham de maneira significativa e com proporções inimagináveis. Como exemplo, citamos o algoritmo de reconhecimento de imagem do Google que, ensinado a rotular fotos, rotulou fotos de pessoas negras como "gorilas" [253].

Os algoritmos de aprendizado de máquinas consistem numa evolução frente aqueles incapazes de se autotransformar. Mas seria, então, o algoritmo um sistema autopoiético[254]? Ele depende de entradas (*inputs*) e saídas (*outputs*) para se reproduzir, mas em um momento posterior à sua estruturação, na sua evolução *machine learning*[255], poder-se-ia cogitar sua relação reiterativa e circular entre si?

---

[252] TUTT, Andrew. An FDA for algorithms. Publicado em: 15 mar. 2016. In: **69 Admin. L. Rev**. 83, 2017. Disponível em: <https://ssrn.com/abstract=2747994>. Acesso em: 18 nov. 2018, p.88.

[253] GUYNN, Jessica. Google Photos Labeled Black People “Gorillas”. In: **USA TODAY**, 01 jul. 2015. Disponível em: <http://www.usatoday.com/story/tech/2015/07/01/google-apologizes-after-photos-identify-black-people-as-gorillas/29567465>. Acesso em: 18 nov. 2018.

[254] Sistema autopoiético é aquele dotado de organização autopoiética, onde há a (re)produção dos elementos de que se compõe o sistema e que geram sua organização, pela relação reiterativa, circular ("recursiva") entre eles. Esse sistema é autônomo porque o que nele se passa não é determinado por nenhum componente do ambiente mas sim por sua própria organização, formada por seus elementos.Essa autonomia do sistema tem por condição sua clausura, quer dizer, a circunstância de o sistema ser "fechado", do ponto de vista de sua organização, não havendo "entradas" (inputs) e "saídas" (outputs) para o ambiente, pois os elementos interagem no e através dele, que é "como o agente que conecta as extremidades do sistema (como se fosse uma gigantesca sinapse) e o mantém fechado, autopoiético". [...] Só a comunicação autoproduz-se, donde se qualificar como autopoiéticos os sistemas de comunicação da sociedade. O sentido da comunicação varia de acordo com o sistema no qual ela está sendo veiculada e as pessoas são meios (media) dessas comunicações, assim como computadores, faxes, telefones, etc. Esses componentes, contudo, não pertencem aos sistemas sociais e, sim ao seu meio ambiente. Os seres humanos, enquanto seres biológicos, são sistemas biológicos autopoiéticos e enquanto seres pensantes, são também sistemas psíquicos autopoiéticos. Sem a consciência decorrente do aparato psíquico, é claro, não haveria comunicação e logo também não haveria sistemas sociais. Sem a rede neuronal não haveriam pensamentos. O que não há é uma relação causal entre imagens e pensamentos como os que temos, enquanto seres humanos, como demonstra o fato de que os demais seres portadores de redes neuronais não dispõem de uma elaboração simbólica como nós. É a linguagem, então a primeira condição para que se dê o acoplamento (estrutural) entre sistemas auto(conscientes) e sistemas sociais (autopoiéticos) de comunicação. Os sistemas sociais, como todo sistema, se mantêm sem dissipar-se no meio-ambiente em que existem enquanto se mantém sua estrutura e enquanto for apto para diferenciar-se nesse meio ambiente, com o qual “faz fronteira”. Sistemas psíquicos (biológicos) e sistemas de comunicação (sociais), por mais que estejam cognitivamente abertos para o meio ambiente, para dele se diferenciarem, fecham-se em um operar, o que significa reagir ao (e no) ambiente por autorreferência, sem contato direto com ele. (GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.216-226).

[255] Para Willis Santiago Guerra Filho, a Inteligência Artificial pode ser considerada um sistema autopoiético: “Inicialmente, vale destacar que se trata de um paradigma oniabrangente, transclássico, como a cibernética, pioneiramente, se propôs a ser, e antes dela a semiótica o foi, pois no âmbito dele se pode pensar e ampliar conhecimentos nas mais diversas áreas, cruzando as fronteiras todas estabelecidas pelo modo clássico, analítico, de se fazer ciência(s). Caracterizando-o, ou melhor, estabelecendo seu parentesco epistemológico, pode-se dizer que tem dentre seus antepassados mais remotosa Teoria Geral de Sistemas, de von Bertalanffy, além da já referida a semiótica, sobretudo em suas derivações mais recentes, como a semiótica computacional e

Note-se que o algoritmo não persiste em si, porquanto se não houver dados, inexiste a engrenagem de seu funcionamento. Daí se depreende que mais importante do que a sua própria composição, são os dados que o alimentam. A cultura do algoritmo, assim, somente é possível em razão da realidade da sociedade de dados, como consequência da sociedade informacional.

Segundo Willis Santiago Guerra Filho, "a autoimunidade é uma aporia"[256], de forma que aquilo que tem por objetivo nos proteger é o que nos destrói, ainda que existam pessoas que apostem de maneira otimista, na capacidade de reação que oferece a crescente virtualização de mercados, instituições políticas e jurídicas[257]. Sobre os executivos do Google, comenta:

> Este é precisamente o caso dos executivos da Google Inc., esperançosos na capacidade de árbitros on line darem conta do que aparenta mais lhes interessar, que é a proteção dos direitos de propriedade, sobretudo intelectual, extraindo, assim, da fonte do problema, também a sua solução, a fim de implementar a defesa contra a crescente ameaça à privacidade e insegurança pessoal, no mundo pós-9/11, para garantir a segurança coletiva. Para estes, não haveria ruptura paradigmática, pois não reconhecem que já estão operando com uma lógica autoimunitária, pois pretendem, literalmente, vacinar-se contra o seu/nosso problema doentio inoculando-se com ele em pequena dosagem, ou seja, em formas e dimensões compatíveis com sua capacidade de reação, para assim ir tornando-a ainda maior[258].

---

a bio-semiótica, as teorias da comunicação e da informação, dentre outras, sendo que, novamente, com ênfase para versões mais recentes, como aquelas dos sistemas auto-organizativos e, mais especificamente, aqueles autopoiéticos, inclusive em I.A., a ponto de já se puder falar em "máquinas semióticas" no sentido próprio. A versão (ou "virada") imunológica dentro deste paradigma destaca este tipo de sistema inteligente, o imunológico (abrev.: SI), tal como se manifesta em seres vivos, sobretudo vertebrados, onde além daquele inato desenvolve-se o SI adaptativo. Este é um sistema complexo de solução de problemas a partir dos elementos fornecidos pelos próprios problemas, apesar (ou por causa) da memória ser uma das propriedades do sistema, especialmente de alguns de seus componentes". (GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.216-226).

[256] "O paradoxo da autopoiese do sistema do direito terminando em autoimunidade revela o paradoxo da inevitável circularidade do Direito e suas raízes políticas nas constituições. Nos tribunais constitucionais, nacionais e transnacionais, fundem-se os sistemas do direito com o da política, e este colapso ameaça liquidar o já combalido sistema social global, que assim chega a um quantum critic, a partir do qual se há de transmutar, renovando-se ou perecendo". (GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p. 221.

[257] GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.272.

[258] GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.222.

Para além de outras tecnologias, como a fotografia[259], nos algoritmos não se sabe exatamente quais os efeitos (*outputs*) decorrentes das suas ações (*inputs*), porquanto a máquina pode aprender consigo mesma, na medida do grau da entropia de seu sistema. Ainda nas palavras de Willis Santiago Guerra Filho: "este é um sistema complexo de solução de problemas a partir dos elementos fornecidos pelos próprios problemas, apesar (ou por causa) da memória ser uma das propriedades do sistema, especialmente de alguns de seus componentes"[260].

Sob outro aspecto, os algoritmos de aprendizagem de máquina podem ser comparados à entropia, princípio da física termodinâmica, ao passo que alteram o estado de organização de seus comandos iniciais, criando novas condições de seus sistemas, de modo irreversível, em um processo de (des)organização.

A partir daqui, passa-se a questionar e analisar a nova forma de inteligência revelada pelas máquinas na sociedade na qual estamos inseridos.

2.5 Inteligência, consciência e fusão homem-máquina

Até algumas décadas atrás, existia uma clara separação entre natural e artificial. A cada uma dessas áreas pertencia seus próprios problemas e soluções. Porém, a partir de meados da segunda metade do século XX, essa situação mudou. A fronteira que separava os dois campos foi dissipada. Segundo contribuição de Paula Sibilia, "ao longo de muitos séculos vigorou, na tradição ocidental, uma distinção radical entre *phsis* e *techné* (em termos gregos), ou *natura* e *ars* (em termos latinos): natural e artificial"[261]:

> Ou seja: de um lado, o ser que é princípio do seu próprio movimento; de outro, as operações humanas para utilizar, imitar e ampliar o escopo do natural – dois mundos claramente distintos, quase antagônicos. Mas a fronteira que separava esses dois universos vem se dissipando, e são inúmeras as repercussões dessa cisão, tanto em nossa cotidianidade como no imaginário contemporâneo [262].

---

[259] FLUSSER, Vilém. **Filosofia da caixa preta**. Ensaios para uma futura filosofia da fotografia. São Paulo: É Realizações, 2018.

[260] GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.224. Em relação ao trecho citado, o autor se refere ao sistema inteligente, o imunológico.

[261] SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.69-70.

[262] SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.69-70.

Willis Santiago Guerra Filho também comenta sobre a *techné*, ao pontuar que esta se caracteriza como uma forma de conhecimento, mais próprio das contingências da vida, e explica que os gregos a utilizavam em sentido bem diverso do atual, enquanto conhecimento operativo, instrumental e produtivo, limitado e finito, uma vez que era voltado ao atendimento de finalidades específicas, mas sempre revelador de potencialidades[263].

Para Paula Sibilia, certos discursos dos meios de comunicação, da ciência e das artes estão engendrando um novo personagem: o homem pós-orgânico, cuja criatura é fruto do ideário fáustico[264]da tecnociência mais atual, que tem se expandido pelo tecido social para atingir as áreas mais diversas, turvando muitas definições que outrora pareciam claras e inquestionáveis; uma delas é, justamente, a de ser humano [265].

Segundo observação de Willis Santiago Guerra Filho, é fundamental investigar as novas formas de acoplamentos estruturais[266] que estão surgindo,

---

[263] GUERRA FILHO, Willis Santiago. **Quantum critic**: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.5. Mais adiante em sua tese, o autor cita uma conferência proferida em 1962 por Heidegger, na qual explica o termo 'técnica' da seguinte maneira: "O termo 'técnica' deriva do grego 'technikon'. Isto designa o que pertence à 'technè'. Este termo tem, desde o começo da língua grega, a mesma significação que 'epistéme' - quer dizer: velar sobre uma coisa, compreendê-la. 'Technè' quer dizer: conhecer-se em qualquer coisa, mais precisamente no facto de produzir qualquer coisa". (HEIDEGGER, M. **Überlieferte Sprache und technische Sprache**, St. Gallen: Erker, 1989. (Língua de tradição e língua técnica). Tradução de Mário Botas. 2.ed. Lisboa: Vega, 1999, p.21).

[264] A autora faz alusão ao predicativo "fáustico", referindo-se ao personagem mítico Fausto, que vende sua alma ao inimigo do bem, movido por uma vontade de crescimento infinito e pelo desejo de superar suas próprias possibilidades. (SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.45).

[265] SIBILIA, Paula. **O homem pós-orgânico.** A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.69.

[266] Sobre as formas de acoplamentos estruturais, explica Willis Santiago Guerra Filho: "Postular que a sociedade contemporânea, organizada em escala mundial, "globalizada", é o produto da diferenciação funcional de diversos (sub)sistemas, como os da economia, ética, direito, mídia, política, ciência, religião, arte, ensino etc. – sistemas autopoiéticos, que operam com autonomia e fechados uns em relação aos outros, cada um com sua própria "lógica" – postular isso não implica negar que haja influência ("irritações", nos termos empregados pela própria teoria aqui enfocada, ou "perturbações") desses sistemas uns nos outros. Entre eles dá-se o que a teoria de sistemas autopoiéticos denomina "acoplamento estrutural". Assim, o sistema da política acopla-se estruturalmente ao do direito através das constituições dos Estados, enquanto o direito se acopla à economia através dos contratos e títulos de propriedade, e a economia, através do direito, com a política, por meio dos impostos e tributos, e com a ciência, através de publicações, diplomas e certificados". E ainda, sobre a teoria de sistemas sociais autopoiéticos, em linhas gerais, ensina Willis Santiago Guerra Filho: A teoria em apreço pretende se desenvolver a partir de um conceito de sociedade que não é nem "humanista" nem "regionalista", adotando assim uma posição que, de partida, evita dois dos maiores – se não forem mesmo os dois maiores – pressupostos incitadores da crise "epistemo-ecológica" antes referida. Isso significa que para a teoria ora em apreço a sociedade não é formada pelo conjunto de seus integrantes, os seres humanos, assim como não há para ela uma sociedade delimitada por critérios geo-políticos – a "sociedade brasileira", "latino-americana", "européia" etc. Sociedade para a teoria de sistemas luhmanniana é a "sociedade mundial" (Weltgesellschaft), que se forma modernamente. O que a compõe não são os seres humanos que a ela pertencem, mas sim a comunicação entre eles, que nela circula de várias formas, nos diversos subsistemas funcionais (direito, economia, política, ética, mídia, religião, arte, ciência, educação etc.). (GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.148-149).

envolvendo homens e máquinas, nas casas e cidades em que arquitetos e urbanistas estão projetando, neste limiar do advento de uma era pós-humana – que pode até mesmo ser mais humana, segundo o autor – favorecendo o desenvolvimento das potencialidades do ser humano, em ambientes com um *design* pensado para propiciar tal favorecimento[267].

Ademais, Paula Sibilia pondera que os corpos contemporâneos, tão intimidados como seduzidos pelas pressões de um meio ambiente amalgamado com o artifício, não conseguem fugir das tiranias e das delícias do upgrade. Essa mania de aprimoramento sem pausa não aposta em qualquer direção; ela tem um norte bem preciso, no qual lateja o desejo de ajustar a própria compatibilidade com o tecnocosmo digitalizado[268] .

Segundo Gilles Deleuze, os indivíduos tornaram-se “dividuais”, divisíveis, e as massas tornaram-se amostras, dados, mercados ou “bancos”[269]. Entraram em crise várias ideias e valores que pareciam firmemente estabelecidos. “Nada menos que o ser humano, a natureza, a vida e a morte hoje atravessam turbulências, despertando todo tipo de discussões e perplexidades que apontam para a sua redefinição”[270] .

A relação entre o homem e as máquinas se inverteu. Antes os instrumentos cercavam os homens, porém, em um momento posterior, as máquinas eram por eles cercadas. Igualmente, os instrumentos funcionavam em função do homem; depois, o homem passou a funcionar em função das máquinas. Nesse sentido é o pensamento de Vilém Flusser:

> Quando os instrumentos viraram máquinas, sua relação com o homem se inverteu. Antes da Revolução Industrial, os instrumentos cercavam os homens; depois, as máquinas eram por eles cercadas. Antes, o homem era a constante da relação, e o instrumento era a variável; depois, a máquina passou a ser relativamente constante. Antes, os instrumentos funcionavam

[267] GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.214-215.
[268] SIBILIA, Paula. ***O homem pós-orgânico***. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.14.
[269] DELEUZE, Gilles. **Conversações**. Tradução Peter Pál Pelbart. São Paulo: Editora 34, 2013, p.227.
[270] SIBILIA, Paula. O **homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.15. “Algumas propostas tecnocientíficas bem atuais proclamam um replanejamento da espécie humana, insinuando o advento de uma nova era comandada pela evolução pós-humana ou mesmo por certa pós-evolução de toda a biosfera; ou seja, um tipo de evolução que não seria mais natural, porém artificial. Esses processos superariam em velocidade e eficiência os lentos ritmos da velha natureza, acelerando e turbinando a biologia com os mais novos recursos tecnocientíficos” (p.15). “Alguns pesquisadores aspiram conquistas ambiciosas, como remover a mente do cérebro humano e transferi-la a um dispositivo inorgânico” (p.58).

> em função do homem; depois, grande parte da humanidade passou a funcionar em função das máquinas[271].

Sob outra perspectiva, na lição de Willis Santiago Guerra Filho, não devemos confundir a existência do corpo com a existência do ser. A zoé, o estar vivo, e o ser não são a mesma coisa:

> Uma coisa antecede a outra, mas o ser não existe em um corpo vivo com cérebro morto, tal como prescrito nas legislações atuais, e enquanto não se cumpra o prognóstico de Ray Kurzweil – no seu livro publicado em 1999, "The Age of Spiritual Machines: When Computers Exceed Human Intelligence" – até podemos falar em vida artificial, com Manuel DeLanda, mas não que se encontre a presença do ser que somos ou que é em nós, nos corpos de silício em que habitam os programas de computador – logo, não devemos confundir a existência do corpo com a existência do ser [272] .

A capacidade de ver, entender e aprender, antes atributos do ser humano, e dos animais, agora adentrou a esfera das máquinas. O homem consegue a proeza de imprimir a sistemas inorgânicos aptidões animalescas.

No reflorescer intelectual da escolástica houve um ponto de transmutação no campo da filosofia e da "ciência". Nesse momento da história, pelo desenvolvimento exponencial da tecnologia, estamos em uma nova transmutação. Essa é a opinião de Willis Santiago Guerra Filho. Segundo ele, em pese vivermos esse momento com entusiasmo, é necessário atentar para os riscos da programação de máquinas em substituição de seus programadores, tornando-se autopoiéticas, e podendo entrar em competição com o próprio homem:

> Na escolástica medieval verificamos um ponto de transmutação dentro de um processo de busca da unificação da geometria e do número, ou mais vulgarmente, da filosofia e da ciência. Agora, estaríamos prestes a atingir um outro, pelo desenvolvimento exponencial da tecnologia, ao qual se vem referindo, em geral de maneira entusiasta, como uma "singularidade", quando precisamos atentar para os riscos de assim estarmos programando máquinas para substituírem com incomensurável vantagem seus programadores, tornando-se autopoiéticas, como a vida, e daí quem sabe entrem em competição conosco, tal como soe acontecer na natureza[273] .

---

[271] FLUSSER, Vilém. **Filosofia da caixa preta**. Ensaios para uma futura filosofia da fotografia. São Paulo: É Realizações, 2018, p.31-32.

[272] GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.148-149.

[273] GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.265-266.

Segundo Willis Santiago Guerra Filho, a progressiva informatização e robotização seria um sintoma de um resultado que aponta para a objetivação/realização/artificialização total do sujeito, que assim "aperfeiçoado" ingressaria no fim de sua história. Sobre os dois fenômenos – a progressiva informatização e a robotização – comenta:

> A primeira decompõe decisões em bits, o que permite o seu cálculo, projetando-os em uma escalada de abstração crescente, que afasta sempre mais as decisões do contato com a experiência concreta da vida. Já a outra, a robotização, também corta o vínculo dos atos humanos com a empiria, pois tais atos são decompostos em seus elementos constitutivos, a fim de recompô-los em atos maquínicos[274].

Como resultado desse fenômeno, aponta Willis Santiago Guerra Filho que, "atos e decisões, antes considerados características definidoras do sujeito humano, uma vez tornados artifícios, rebatem sobre ele/nós, artificializando-(n)os"[275]. E assim, tendencialmente, "irá desaparecendo a diferença entre operações humanas e artificiais, todas encetadas relacionalmente, mediadas por aparelhos técnicos, inclusive em campos como o da política e o das relações pessoais"[276].

Willis Santiago Guerra Filho constata: "a artificialização generalizada, inclusive dos sonhos, tudo agora deliberadamente calculado, ensejaria uma grande nostalgia do modo oposto de sermos: espontâneos, inspirados, artísticos"[277] .

Tomando emprestadas as reflexões de Vilém Flusser, pode-se dizer que se trata de uma 'automação estúpida' (sic) de nossas vidas:

> Constata-se, em nosso entorno, como os aparelhos se preparam para programar, com automação estúpida, as nossas vidas; como o trabalho está sendo assumido por máquinas automáticas, e como os homens vão sendo empurrados rumo ao setor terciário, onde brincam com símbolos vazios; como o interesse dos homens vai se transferindo do mundo objetivo para o mundo simbólico das informações: sociedade informática programada; como o pensamento, o desejo e o sentimento vão adquirindo caráter de

---

[274] GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.233.

[275] GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.233.

[276] GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.233.

[277] GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.234.

> jogo em mosaico, caráter robotizado; como o viver passa a alimentar aparelhos e ser por eles alimentado. O clima absurdo se torna palpável[278].

O homem tem se tornado escravo das máquinas sem, no entanto, se dar conta dessa condição, de forma que o indivíduo pensa ser livre para fazer escolhas, quando, na verdade, está submisso aos ditames e escolhas da máquina algorítmica, sendo incapaz de dominá-la inteiramente.

Não é demais citar que há diversas iniciativas mundiais com foco em acompanhar as liberdades individuais e o avanço dos algoritmos. Dentre tantas, destacamos quatro: *Algorithm Watch*[279], da Alemanha; o *Lawgorithms*[280], capitaneado pelo professor Juliano, da Faculdade de Direito da Universidade de São Paulo; a *International Association for Artificial Intelligence and Law*[281], e o projeto CLAUDETTE[282], liderado pelos professores Giovanni Sartor e Hans-W. Micklitz, em cooperação com os engenheiros da Universidade de Bologna, da Universidade de Modena e de Reggio Emilia.

Alguns cientistas acreditam que um computador nunca “pensará” como um cérebro humano e que comparar a análise computacional e os algoritmos de um

---

[278] FLUSSER, Vilém. **Filosofia da caixa preta**. Ensaios para uma futura filosofia da fotografia. São Paulo: É Realizações Editora, 2018, p.99.

[279] Disponível em: <https://algorithmwatch.org/de/>. Acesso em: 24 dez. 2018. O AlgorithmWatch é uma iniciativa dos pesquisadores Lorena Jaume-Palasí, Lorenz Matzat, Matthias Spielkamp e Prof. Dr. med. Katharina Anna Zweig e é apoiada pelas autoridades da mídia estatal de Hesse, Baviera, Baden-Württemberg, Renânia-Palatinado, Sarre e Saxônia. Tem foco nos algoritmos da gigante Google, bem como nas eleições do país.

[280] Lawgorithm é uma associação independente, sem fins lucrativos, fundada por professores de ciência da computação, engenharia, direito, economia e filosofia da USP, dedicada à pesquisa sobre inteligência artificial aplicada ao direito e sobre as implicações jurídicas, econômicas, sociais e culturais da inteligência artificial. Da perspectiva da inteligência artificial para o direito (IA&Direito), o Lawgorithm promove a pesquisa sobre ferramentas computacionais inteligentes capazes de tornar mais eficiente a atuação de juristas e de gerar informações sobre as atividades legislativa e jurisdicional. Da perspectiva do direito da inteligência artificial (Direito da IA), pretende refletir sobre novas questões jurídicas trazidas pela atuação de agentes digitais. O Lawgorithm parte de quatro convicções orientadoras de seus projetos de pesquisa: 1. O raciocínio jurídico é complexo, envolvendo: a) identificação das regras a serem aplicadas; b) o significado dos termos contidos nas regras perante conceitos jurídicos fundamentais c) a adequação das soluções indicadas pelas regras em relação a propósitos de políticas públicas e princípios valorativos; 2. Ferramentas gerais de Inteligência Artificial serão mais eficientes e adequadas quando forem empregadas no direito com base em representação de conhecimento, análise e inferências típicas dos juristas (conforme convicção 1) 3. Os juristas atuarão com mais qualidade e produtividade quando se desvencilharem de tarefas repetitivas e puderem ter acesso rápido e eficiente ao conhecimento específico necessário ao seu labor intelectual (por ferramentas que satisfaçam 2). 4. A inteligência artificial deve ser compreendida de perspectiva multidisciplinar, considerando suas condições técnicas, impactos econômicos, sociais e culturais, como pressuposto de qualquer regulação ou interpretação de suas implicações jurídicas. (LAWGORITHM. Disponível em: <http://www.lawgorithm.com.br/>. Acesso em: 24 dez. 2018).

[281] INTERNATIONAL Association for artificial intelligence and law. Disponível em: <http://www.iaail.org/?q=page/ai-law>. Acesso em: 24 dez. 2018.

[282] CLAUDETTE – “automated CLAUse DETectEr” – is an interdisciplinary research project hosted at the Law Department of the European University Institute. The research objective is to test to what extent is it possible to automate reading and legal assessment of online consumer contracts and privacy policies, to evaluate their compliance with EU’s unfair contractual terms law and personal data protection law (GDPR), using machine learning and grammar-based approaches. (EUROPEAN University Institute. **CLAUDETTE machine learning powered analysis of consumer contracts and privacy policies**. Disponível em: <https://claudette.eui.eu/about/>. Acesso em: 24 dez. 2018).

computador com as maquinações da mente humana é como comparar ‘maçãs e laranjas’[283]. De qualquer forma, fruto dessa associação bioinformática é uma disciplina cujo nome já revela tal combinação: a inteligência artificial, concebida há cerca de 70 anos, pelo matemático britânico Alan Turing, cujo nome marca o início do desenvolvimento dessa disciplina.

Precursor nessa área e no desenvolvimento da ciência da computação e do algoritmo, Alan Turing ficou célebre, também, pela pôlemica pergunta ‘As máquinas podem pensar?´ Em 1950, introduziu o “teste de Turing”: uma máquina poderia ser considerada inteligente se pudesse emitir reações que seriam indistinguíveis das de um humano. Para passar no teste, portanto, um computador deveria ser capaz de enganar um humano, acreditando que também é humano. A seguir será apresentada a cronologia dos principais marcos na linha da história da inteligência artificial[284]. Aqui vale esclarecer que o presente trabalho não tem o condão de fazer maiores aprofundamentos de caráter técnico. Apresentar-se-á, portanto, os principais marcos temporais do assunto, como base para melhor compreensão da dimensão do estado da técnica, no campo dos algoritmos e da inteligência artificial.

Em 1952, Arthur Samuel escreveu o primeiro programa de aprendizado de computador. O programa feito com um jogo de damas e o computador IBM melhorava suas jogadas quanto mais jogava, estudando quais movimentos compunham as estratégias vencedoras e incorporando esses movimentos ao seu programa.

A expressão ´inteligência artificial´ foi cunhada em 1955 por John McCarthy, em uma conferência de especialistas celebrada em Darmouth Colege, Estados Unidos da América.

Para John McCarthy, inteligência artificial é a ciência de construir máquinas e sistemas inteligentes, especialmente programas de computador inteligentes. Está relacionada à tarefa semelhante de usar computadores para entender a inteligência humana. Entretanto, a inteligência artificial não precisa se limitar a métodos

[283] MARR, Bernard. A short history of machine learning – every manager should read. **Forbes**. Publicado em: 19 fev. 2016. Disponível em: <https://www.forbes.com/sites/bernardmarr/2016/02/19/a-short-history-of-machine-learning-every-manager-should-read/#20f5f5e15e78>. Acesso em: 21 out. 2018.

[284] Referida linha cronológica foi baseada em MARR, Bernard. A short history of machine learning – every manager should read. **Forbes**. Publicado em: 19 fev.2016. Disponível em: <https://www.forbes.com/sites/bernardmarr/2016/02/19/a-short-history-of-machine-learning-every-manager-should-read/#20f5f5e15e78>. Acesso em: 21 out. 2018.

biologicamente observáveis. Em outras palavras, inteligência artificial é a parte computacional da capacidade de atingir objetivos no mundo[285] .

Ainda segundo John McCarthy, não há uma definição de inteligência artificial que não dependa de relacioná-la com a inteligência humana, posto que ainda não podemos caracterizar, de forma geral, quais tipos de procedimentos computacionais devem ser designados inteligentes[286]. Além disso, nesse quadrante, nem sempre se está a simular a intiligência humana:

> On the one hand, we can learn something about how to make machines solve problems by observing other people or just by observing our own methods. On the other hand, most work in AI involves studying the problems the world presents to intelligence rather than studying people or animals. AI researchers are free to use methods that are not observed in people or that involve much more computing than people can do[287].

Em 1957, Frank Rosenblatt projetou a primeira rede neural para computadores, o perceptron, que simulava os processos de pensamento do cérebro humano. Sobre redes neurais para computadores se falará mais adiante.

Em 1967, o algoritmo *nearest neighbor* foi desenvolvido, permitindo que os computadores começassem a utilizar um reconhecimento de padrões muito básico. O objetivo desse algoritmo foi mapear uma rota para vendedores ambulantes, começando por uma cidade aleatória, mas garantindo que eles visitassem todas as cidades durante um pequeno circuito.

Em 1970 foi publicado na Stanford Law Review o artigo Some Speculation about Artificial Intelligence and Legal Reasoning, de Buchanan and Headrick, no qual foram discutidas as possibilidades de pesquisa para análise legal e construção de argumentos com o uso da Inteligência artificial. Essa publicação marca o início da Inteligência Artificial nas pesquisas jurídicas[288].

---

[285] MCCARTHY, John. **What is artificial intelligence**. Stanford University, 12. nov.2007. Disponível em: <http://www-formal.stanford.edu/jmc/whatisai/node1.html>. Acesso em: 12 out. 2018.

[286] MCCARTHY, John. **What is artificial intelligence**. Stanford University, 12. nov.2007. Disponível em: <http://www-formal.stanford.edu/jmc/whatisai/node1.html>. Acesso em: 12 out. 2018.

[287] MCCARTHY, John. **What is artificial intelligence**. Stanford University, 12. nov.2007. Disponível em: <http://www-formal.stanford.edu/jmc/whatisai/node1.html>. Acesso em: 12 out. 2018. Tradução livre: Por um lado, podemos aprender algo sobre como fazer máquinas resolverem problemas observando outras pessoas ou apenas observando nossos próprios métodos. Por outro lado, a maioria dos trabalhos em IA envolve estudar os problemas que o mundo apresenta à inteligência, em vez de estudar pessoas ou animais. Os pesquisadores de IA são livres para usar métodos que não são observados em pessoas ou que envolvem muito mais computação do que as pessoas podem fazer.

[288] Muito embora o artigo de seja significativo, vale notar que “Many years before that, Layman Allen had begun his research program on using logic as a tool to improve drafting and interpretation of legal documents.7 In 1977, the Harvard Law Review published a landmark paper by L. Thorne McCarty on his TAXMAN system, which pursued a theorem-proving approach to reasoning with issues in corporate tax law. (RISSLANDA, Edwina L.;

Em 1979, os estudantes da Universidade de Stanford inventam o “Stanford Cart”, que poderia andar por obstáculos, em uma sala, por conta própria. Em 1981, Gerald Dejong introduz o conceito de Explanation Based Learning (EBL), ou Aprendizagem Baseada na Explicação, em português. Através desse conceito, um computador analisa dados de treinamento e cria uma regra geral que pode ser seguida descartando dados sem importância. Em 1985, Terry Sejnowski inventa o NetTalk, que aprende a pronunciar as palavras tal como um bebê. Em 1990, os pesquisadores começam a criar programas para computadores com o desiderato de analisar grandes quantidades de dados e tirar conclusões – ou "aprender" – a partir dos resultados. Portanto, o trabalho sobre aprendizado de máquina muda de uma abordagem orientada pelo conhecimento para uma abordagem baseada em dados. Em 1997, o Deep Blue da IBM venceu o campeão mundial no xadrez, Garry Kasparov, ressalvada as polêmicas revelações que sobrevieram anos depois, sobre ter ocorrido um problema no programa de computador[289].

Em 2006, Geoffrey Hinton utilizou o termo *deep learning* para explicar novos algoritmos que permitem aos computadores ver e distinguir objetos e textos em imagens e vídeos. Em 2010, o Microsoft Kinect conseguiu rastrear 20 recursos

---

ASHLEYB, Kevin D., LOUIC, R. P. **AI and law**: a fruitful synergy. Disponível em: <http://www.iaail.org/>. Acesso em: 18 nov. 2018.

[289] Segundo notícia veiculada na imprensa, com base no documentário “The Man vs. The Machine”. Disponível em: <http://espn.go.com/video/clip?id=espn:11694550 >, dirigido por Frank Marshall: “Precisaram passar 17 anos para que um mistério fosse revelado: foi um erro no software do supercomputador Deep Blue, da IBM, que o fez vencer o Grande Mestre Garry Kasparov no segundo desafio entre homem e máquina ocorrido em 1997, em Nova York. O 44º lance, executado pelo Deep Blue, confundiu totalmente o russo por ser absolutamente contraintuitivo. Era um movimento maluco, sem qualquer razão de ser. Não era estratégico, nem ofensivo e nem defensivo. O Deep Blue chegou a uma falha no código do programa e entrou em ‘loop’, uma condição em que o software fica rodando em círculos eternamente. Mas, como em qualquer programa bem feito, havia uma salvaguarda de segurança para casos de loop infinito. Se o módulo vigilante notasse que a execução tinha entrado em “abraço mortal”, soltaria um comando para o programa principal ordenando-o a fazer qualquer movimento válido de uma peça no tabuleiro, só para o jogo não empacar. Essa foi então a explicação do estranho lance 44. Só que, por não saber disso, Kasparov interpretou o ilógico movimento como “sinal de uma inteligência superior”. E ficou intimidado, embatucado por não conseguir penetrar na supostamente avançada estratégia do oponente. Como resultado, desistiu do jogo seguinte, perdendo a segunda batalha. Kasparov sabia que tinha a capacidade de calcular até 15 lances adiante. E, como não viu sentido naquele lance nº 44, incorretamente concluiu que o Deep Blue podia antever jogadas mais do que ele próprio. E aí se desequilibrou emocionalmente pelo resto do match. Os programadores também não entenderam naquele momento e concluíram que era algo de menor importância e que precisaria ser consertado mais tarde. Só anos depois concluíram que, na verdade, o estranho movimento foi efeito de um bug. Só que, por não saber disso, Kasparov interpretou o ilógico movimento como “sinal de uma inteligência superior”. E ficou intimidado, embatucado por não conseguir penetrar na supostamente avançada estratégia do oponente. Como resultado, desistiu do jogo seguinte, perdendo a segunda batalha. Kasparov sabia que tinha a capacidade de calcular até 15 lances adiante. E, como não viu sentido naquele lance nº 44, incorretamente concluiu que o Deep Blue podia antever jogadas mais do que ele próprio. E aí se desequilibrou emocionalmente pelo resto do match. Os programadores também não entenderam naquele momento e concluíram que era algo de menor importância e que precisaria ser consertado mais tarde. Só anos depois concluíram que, na verdade, o estranho movimento foi efeito de um bug. (TEIXEIRA, Carlos Alberto. **O Globo**. Revelado: Foi erro no computador Deep Blue da IBM que o fez vencer Kasparov em 1997. Publicado em: 24 out.2014. Disponível em: <https://oglobo.globo.com/economia/tecnologia/revelado-foi-erro-no-computador-deep-blue-da-ibm-que-fez-vencer-kasparov-em-1997-14349363>. Acesso em: 21 out. 2018).

humanos a uma média de 30 vezes por segundo, permitindo que as pessoas pudessem interagir com o computador através de movimentos e gestos. Em 2011, o IBM Watson venceu seus concorrentes humanos no Jeopardy, um tradicional programa de TV americano de perguntas e respostas. Durante três dias, o computador da IBM competiu contra Ken Jennings e Brad Rutter, os dois campeões de maior sucesso da história do programa, no ar desde 1964.

No mesmo ano, o Google Brain é criado como célula da gigante empresa de tecnologia para o desenvolvimento da inteligência artificial [290]. Ainda em 2010, a mesma empresa lança o XLab[291], outra célula de inovação e avanços tecnológicos, que desenvolveu, em 2012, um algoritmo de aprendizado de máquina capaz de navegar de forma autônoma em vídeos do YouTube para identificar os vídeos que contêm gatos. Em 2014, a empresa Facebook desenvolveu o DeepFace, um algoritmo de software capaz de reconhecer pessoas em fotos. Em 2015, a Amazon lança sua própria plataforma de aprendizado de máquina[292], gerando um marco mercadológico no sentido da oferta a ferramentas e serviços de aprendizado de máquina a custo acessível, escaláveis e armazenados. No mesmo sentido, a criação, pela Microsoft, no mesmo ano, do Distributed Machine Learning Toolkit, que permite a distribuição eficiente de problemas de aprendizado de máquina em vários computadores.

Em 2016, o algoritmo de inteligência artificial do Google vence um jogador profissional no jogo de tabuleiro chinês Go, considerado o jogo de tabuleiro mais complexo do mundo e muitas vezes mais difícil que o próprio xadrez. O algoritmo

---

[290] Google Brain é uma equipe de pesquisa de inteligência artificial de aprendizagem profunda no Google. Formado no início de 2010, o Google Brain combina pesquisa de aprendizado de máquina aberta com engenharia de sistemas e recursos de computação em escala do Google. (Google Brain Team https://ai.google/research/teams/brain) . Segundo consta em seu site: “Google’s mission is to organize the world’s information and make it universally accessible and useful. AI is helping us do that in exciting new ways, solving problems for our users, our customers, and the world. AI is making it easier for people to do things every day, whether it’s searching for photos of loved ones, breaking down language barriers in Google Translate, typing emails on the go, or getting things done with the Google Assistant. AI also provides new ways of looking at existing problems, from rethinking healthcare to advancing scientific Discovery”. Elegem como princípios para o desenvolvimento de IA: 1. Be socially beneficial; 2. Avoid creating or reinforcing unfair bias; 3. Be built and tested for safety; 4. Be accountable to people; 5. Incorporate privacy design principles; 6. Uphold high standards of scientific excellence; 7. Be made available for uses that accord with these principles.

[291] Segundo consta em seu site https://x.company/: “X is a diverse group of inventors and entrepreneurs who build and launch technologies that aim to improve the lives of millions, evenions, of people. Our goal: 10x impact on the world’s most intractable problems, not just 10% improvement. We approach projects that have the aspiration and riskiness of research with the speed and ambition of a startup”.

[292] Amazon Mechanical Turk provides a very large-scale, cloud-based, crowdsourced market for what Amazon’s Jeff Bezos has called ‘artificial artificial intelligence’ in which human ‘Workers’ (aka ‘Turkers’) bid to undertake ‘Human Intelligence Tasks’ to feed into learning processes. Tradução livre: (AMAZON Mechanical Turk. Disponível em: <https://www.mturk.com/>. Acesso em: 25 dez. 2018).

AlphaGo, desenvolvido pelo Google DeepMind, conseguiu vencer cinco dos cinco jogos da competição Go.

Conforme se observa da cronologia acima, o intervalo entre as principais invenções nesse campo torna-se cada vez mais curto. O compasso das invenções acelerou. Os avanços são exponenciais[293] e os escândalos são frequentes. Em 2017, um documento interno da empresa Facebook Austrália tornou públicas revelações que detalharam como a rede social monitorava *posts* de usuários e oferecia a clientes de anúncios a possibilidade de atingir, com precisão, adolescentes psicologicamente instáveis e vulneráveis. Os algoritmos do Facebook na Austrália levantaram pessoas de até 14 anos associadas a termos como “derrotadas”, “sobrecarregadas”, “estressadas”, “ansiosas”, “nervosas”, "estúpido", "bobo", "inútil" e "fracasso". Assim, o Facebook, que posteriormente se desculpou, desenvolveu uma maneira de medir a vulnerabilidade cognitiva, embora ainda não esteja claro como exatamente a métrica foi construída, visando explorar uma determinada faixa de potenciais clientes[294].

Está claro que o Facebook pode explorar os humores e as inseguranças de adolescentes, portanto, pode fazê-lo para outras faixas etáreas, usando a associação de inteligência artificial para benefício potencial dos anunciantes e de si mesmo.

Anualmente, a Revista Time publica ranking das melhores invenções do ano[295], segundo escolha de especialistas da publicação. Na lista de 2017, por exemplo, quase a totalidade dos vencedores utilizam algum tipo de inteligência artificial.

Por outro lado, infelizmente, alguns campos perigosos também se imiscuíram nessa seara. Não à toa, em 2015, mais de 3 mil pesquisadores de inteligência artificial e robótica, apoiados, dentre outros, por Stephen Hawking, Elon Musk e Steve Wozniak, assinaram uma carta aberta[296] alertando sobre o perigo de armas

---

[293] Para uma revisão história da pesquisa em inteligência artificial e direito, sob a perspectiva de esquemas de argumentação: PRAKKEN, Henry. Artificial intelligence & law, logic and argument schemes. In: HITCHCOK, David; VERHEIJ, Bart. **Arguing on the toulmin model**: new essays in argument analysis and evaluation. Nova Iorque-EUA: Springer, 2006, p.231-245.

[294] WHIGHAM, Nick. **Leaked document reveals Facebook conducted research to target emotionally vulnerable and insecure youth**. Publicado em: 01 maio 2017. Disponível em: <https://www.news.com.au>. Acesso em: 23 out. 2018.

[295] THE 25 BEST Inventions of 2017. Publicado em 16 nov. 2017. Disponível em: <http://time.com/5023212/best-inventions-of-2017/>. Acesso em: 21 out. 2018.

[296] FUTURE of life institute. **Autonomous weapons**: an open letter from al & robotics researchers. Disponível em: <https://futureoflife.org/open-letter-autonomous-weapons>. Acesso em: 25 dez. 2018.

autônomas que selecionam e engajam alvos sem intervenção humana, a qual foi lançada, em 28 de julho de 2015, na abertura da Joint Conference on Artificial Intelligence (IJCAI-15).

Sob o ângulo de análise da associação com a Internet das Coisas, vinculada às técnicas de Inteligência Artificial, é possível afirmar que novas preocupações são formadas, visto que existe uma interação maior entre o humano e o ambiente[297]. Para citar um exemplo, dados pessoais coletados via Internet das Coisas e processados com o poder da Inteligência Artificial podem ser usados para um tipo específico de comportamento estratégico, que é cada vez mais investigado na literatura econômica, mas largamente negligenciado pelo debate jurídico nesse contexto: contratos de exploração. Segundo Philipp Hacker:

> Such contracts are tailored to vulnerabilities of counterparties that become apparent in data patterns. In the economic literature, a contract is considered exploitative if 'the economically central considerations driving it derive from trying to profit from the agent's mistake'. Similarly, in legal analysis, contracts are deemed exploitative if a party consciously takes advantage of a position of strategic advantage vis-à-vis the counterparty to influence the formation of a contract. Such contracts not only materially disadvantage the exploited party, but also contradict notions of autonomy and fairness inherent in contractual dealing[298].

Com tecnologias de Inteligência Artificial cada vez mais inseridas na área de *marketing* e análise de clientes, o reconhecimento de vulnerabilidades será facilitado e as oportunidades de exploração provavelmente crescerão no futuro. As ofertas contratuais oferecidas para reter os clientes podem ser caras; a prática de *data mining* bem-sucedida permite que as publicidades sejam precisamente direcionadas àqueles clientes com maior chance de compra. Um desafio fundamental para a lei,

---

[297] HACKER, Philipp. Personal data, exploitative contracts, and algorithmic fairness: autonomous vehicles meet the internet of things. **International Data Privacy Law**, v.7, ed.4, nov.2017, p.266-286. Disponível em: <https://doi.org/10.1093/idpl/ipx014>. Acesso em: 16 out. 2018, p.266.

[298] HACKER, Philipp. Personal data, exploitative contracts, and algorithmic fairness: autonomous vehicles meet the internet of things. **International Data Privacy Law**, v.7, ed.4, nov.2017, p.266-286. Disponível em: <https://doi.org/10.1093/idpl/ipx014>. Acesso em: 16 out. 2018, p.267. Tradução livre: Esses contratos são adaptados às vulnerabilidades das partes que se tornam evidentes nos padrões de dados. Na literatura econômica, um contrato é considerado explorador se "as considerações economicamente centrais que o impulsionam derivam de tentar lucrar com o erro do agente". Da mesma forma, na análise jurídica, os contratos são considerados exploradores se uma parte aproveitar conscientemente uma posição de vantagem estratégica em relação à outra parte para influenciar a formação de um contrato. Tais contratos não apenas prejudicam materialmente a parte explorada, mas também contradizem as noções de autonomia e justiça inerentes à negociação contratual.

portanto, é acomodar essa ambivalência e conter a contratação de exploração baseada em dados[299].

Diante das apresentações realizadas até o momento, em especial quanto aos fenômenos tecnológicos, visto à dificuldade de sua regulação, passa-se a analisar a nova cibernética; as formas de regulação dessas tecnologias, verificando se o direito é capaz de resolver as controvérsias nessa sociedade da informação, que também se revela em sociedade de dados, mormente às questões afeitas à proteção de dados pessoais.

2.6 O direito na era da sociedade da informação e na sociedade de dados

Faz todo o sentido compreender o direito digital como uma nova disciplina contendo características como a transversalidade e a imprescindível aproximação a campos científicos não jurídicos. Nesse sentido, Willis Santiago Guerra Filho e Henrique Garbellini Carnio:

> [o direito digital] é composto pela incidência de normas, jurídicas e outras, no chamado ciberespaço, tanto que em inglês é comumente designado *Cyberlaw*. Em alemão é que se pode encontrar referência a uma *Digitalverfassung* (constituição digital), como no seminário apresentado na Universidade de Frankfurt am Main por Rudolf Wiethölter e Günther Teubner, com a colaboração de G-P Callies e outros, no semestre de inverno de 2002/2003. Ocorre que o foco em ambos os países, sob essa rubrica, é o direito da internet, a *lex informatica*. Propomos que o direito digital, além da internet, cuide da regulação, normativa, governamental ou não (*Soft Law*), de tudo que se relacione às mídias eletrônicas. E que ele contemple ainda um outro aspecto, uma espécie de reverso deste que se vem mencionar, pois seria a constituição de um campo de estudo no Direito que se dedique a aplicar nele os desenvolvimentos da digitalização eletrônica.[300]

Um dos traços mais característicos do pensamento ocidental é a busca da sistematização. Segundo Mario Losano, "já na época da filosofia grega, procurou-se organizar o caos num cosmos, o conhecimento fragmentário em conhecimento sistemático"[301]. Esta tendência alcançou o seu apogeu com a filosofia clássica

---

[299] HACKER, Philipp. Personal data, exploitative contracts, and algorithmic fairness: autonomous vehicles meet the internet of things. **International Data Privacy Law**, v.7, ed.4, nov.2017, p.266-286. Disponível em: <https://doi.org/10.1093/idpl/ipx014>. Acesso em: 16 out. 2018, p.269.

[300] GUERRA FILHO, Willis Santiago; CARNIO, Henrique Garbellini. Metodologia jurídica político-constitucional e o Marco Civil da Internet: contribuição ao direito digital. In: DEL MASSO, Fabiano Dolenc; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurelio. **Marco Civil da Internet**. São Paulo: RT, 2014, p.2.

[301] LOSANO, Mario G. **Lições de Informática jurídica**. São Paulo: Resenha Tributária, 1974, p.1.

alemã, e parece estar indissociável da forma de raciocinar da qual o homem ocidental se apropriou.

O aparecimento e o sucesso da cibernética podem ser relacionados à necessidade de unidade sistemática de todo o conhecimento humano, que antigamente era tarefa da filosofia. Para Mario Losano, juscibernética é um termo convencional para indicar as relações entre o direito e a cibernética[302].

A cibernética foi apresentada por Norbert Wiener, matemático de origem alemã, que lecionou no Massachusetts Institute of Technology, e para quem os campos mais fecundos são os que se encontram na fronteira entre as várias disciplinas. Sob a tese de Norbert Wiener, baseada na obra 'Cibernética e sociedade – o uso humano dos seres humanos', observa-se:

> A sociedade só pode ser compreendida através de um estudo das mensagens e das facilidades de comunicação de que disponha; e de que, no futuro desenvolvimento dessas mensagens e facilidades de meios de comunicação, as mensagens entre o homem e as máquinas, entre as máquinas e o homem, e entre a máquina e a máquina, estão destinadas a desempenhar papel cada vez mais importante[303].

A informação é uma condição necessária à eficácia de uma ação, no sentido desta atingir determinados objetivos. Os sistemas funcionam com uma meta e, para isso ocorrer, Norbert Wiener introduziu um dos princípios norteadores da cibernética, o controle, mecanismos de regulação ou homeostase. São estratégias de ação dos sistemas, máquinas ou organismos vivos para manter sua estabilidade ou organização. Muitas vezes, essas ações incorrem em circularidade – que parte da saída (*output*) e é direcionada novamente como entrada no processo (*input*), denominado mecanismo *feedback*[304].

---

[302] LOSANO, Mario G. **Lições de Informática jurídica**. São Paulo: Resenha Tributária, 1974, p.1;6: "O Direito do qual nos ocupamos na informática jurídica é o Direito positivo, isto é, o conjunto das normas da convivência social, providas de sanção (p.6), ao contrário da Filosofia do Direito, que se ocupa do inteiro sistema jurídico (p.2). Para Habermas, porém, em resposta à pergunta "No cenário hipertecnologizado de hoje, onde triunfam os saberes úteis, por assim dizer, qual o papel e sobretudo qual o futuro da filosofia?" [...] "Veja, sou da antiquada opinião de que a filosofia deveria continuar tentando responder às perguntas de Kant: o que é possível saber?, o que devo fazer?, o que me cabe esperar? e o que é o ser humano?. No entanto, não tenho certeza de que a filosofia, como a conhecemos, tenha futuro. Atualmente segue, como todas as disciplinas, a corrente no sentido de uma especialização cada vez maior. E isso é um beco sem saída, porque a filosofia deveria tentar explicar o todo, contribuir para a explicação racional de nossa forma de entender a nós mesmos e ao mundo". (HERMOSO, Borja. Entrevista a Jürgen Habermas. **El País**. Publicada em: 07 maio 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/04/25/eps/1524679056_056165.html> Acesso em: 24 ago. 2018).

[303] WIENER, Norbert. **Cibernética e sociedade**. O uso humano dos seres humanos. 2.ed. Tradução de José Paulo Paes. São Paulo: Cultrix, 1968, p.16.

[304] CHAVES, Viviane Hengler Corrêa. **Norbert Wiener**: a teoria cibernética de um matemático. Tese de Doutorado. Universidade Estadual Paulista "Júlio de Mesquita Filho". Instituto de Geociências e Ciências Exatas Campus de Rio Claro. Orientador: Prof. Dr. Irineu Bicudo, 2016, p.19.

Segundo o autor, certas funções de controle e de processamento de informações em máquinas, seres vivos e organizações sociais são equivalentes e redutíveis aos modelos e leis matemáticas:

> A cibernética é um campo mais vasto, que inclui não apenas o estudo da linguagem, mas também o estudo das mensagens como meios de dirigir a maquinaria e a sociedade. Abrange, também, o desenvolvimento de máquinas computadoras e outros autômatos, certas reflexões acerca da psicologia e do sistema nervoso, e uma nova teoria conjetural do método científico[305].

Diante das inovações desde a cibernética de Norbert Wiener, não podemos permanecer inertes às transformações. A proposta é buscar os instrumentos necessários para responder ao caso concreto, uma vez que "a tarefa do jurista não é certamente a de refutar o 'novo' na obstinada defesa do antigo, mas de individualizar as linhas de 'longa permanência' de um fenômeno, para individualizar novas formas organizadoras da já existente"[306].

Willis Santiago Guerra Filho, ao analisar a obra de Vilém Flusser, destaca a importância da cibernética:

> Daí a importância da cibernética para esclarecer o modo como passam a imperar as imagens eletrônicas, telemáticas e digitais, sem que se precise saber como – nem por que ou para que – pois a noção fundamental da "caixa preta" é, afinal, a de um dispositivo que não se conhece em dado sistema, mas do qual se sabe quais os efeitos (*outputs*) decorrentes das ações que ele sofre (*inputs*)[307].

O que se percebe, atualmente, é uma inclinação para o estudo da informação como objeto de regulação. Nesse sentido, Laura Schertel Mendes articula: "o estudo da informação como objeto de regulação é tema que há muito ocupa as disciplinas jurídicas"[308].

Portanto, se considerarmos o direito como produto de uma específica realidade socioeconômica, a tarefa de Mario Losano do que chamou por *jurista*

---

[305] WIENER, Norbert. **Cibernética e sociedade**. O uso humano dos seres humanos. 2.ed. Tradução de José Paulo Paes. São Paulo: Cultrix, 1968, p.15.
[306] DI MAJO, Adolfo; FERRI, Giovanni Battista; FRANZONI, Massimo. **Il contrato in generale**. L'invalidità del contratto. t.VII. Torino: Giufrrè, 2002, p.456.
[307] GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p. 229.
[308] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.19.

informático é também "formular propostas para que o direito assuma novas formas, a fim de que ele não se torne um obstáculo ao uso de técnicas mais avançadas"[309].

De outro lado, a tecnologia não pode imperar a qualquer custo. É preciso harmonizá-la com os direitos da pessoa humana, visando não violá-los: "o direito não deve render-se à razão tecnológica"[310].

E complementa, a respeito da importância do estudo da matéria de forma autônoma no campo ateneo: "o preparo informático do jurista é uma tarefa de importância capital para as universidades modernas"[311]. Segundo Mario Losano:

> Ao jurista que, como dizia Jhering, voa no céu das abstrações jurídicas, gostaria de contrapor com a chave de fenda: não o engenheiro social idealizado pelos norte-americanos, mas o mecânico da Justiça que – entre os meios que lhe são oferecidos pela técnica moderna – procura os que podem contribuir para o melhor funcionamento da velha máquina da Justiça e para movimentar com mais facilidade o desumano 'bulldozer' do Estado contemporâneo[312].

A cibernética pode ser considerada uma ciência transclássica, de características holísticas, a qual, segundo Willis Santiago Guerra Filho,

> [...] toma como distinção fundamental não mais aquela entre sujeito-do-conhecimento-como-observador-objetivo e objeto-do-conhecimento-observado-independentemente, mas sim, outras, como aquele entre 'sistema' e seu 'meio ambiente', para explicar tudo a partir dessa distinção, entre o que pertence a determinado sistema e o que está fora, no ambiente circundante, embora, circule dentro do sistema – que não é fechado 'para' e sim 'com' o ambiente[313].

É essencial praticar a interdisciplinaridade, o que exige, então, ter um paradigma unificador (paradigma da complexidade), uma perspectiva integradora em epistemologia, capaz de articular explicações de natureza sociológica, econômica, jurídica, biológica, química, física, filosófica, e até teológica, para não mencionar artes e jogos[314].

---

[309] LOSANO, Mario G. **Lições de Informática jurídica**. São Paulo: Resenha Tributária, 1974, p.3.
[310] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.10.
[311] LOSANO, Mario G. **Lições de Informática jurídica**. São Paulo: Resenha Tributária, 1974, p.5: "Somente conhecendo as possibilidades e os limites do meio técnico que lhe é oferecido, o jurista informático poderá prever os desenvolvimentos positivos e negativos, decidindo, com conhecimento de causa, se e quando é oportuno aceitar os primeiros na presença dos segundos".
[312] LOSANO, Mario G. **Lições de Informática jurídica**. São Paulo: Resenha Tributária, 1974, p.7.
[313] GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lumen Juris, 2018, p.116.
[314] GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lumen Juris, 2018, p.116.

Mas as críticas acompanham a evolução. Quando retornou às salas de aula em 1994, após um período dedicado à política, Stefano Rodotà passou a ensinar seu novo curso “tecnologias e direito”. Para muitos de seus colegas, parecia uma extravagância, pois eles eram incapazes de identificar o conteúdo jurídico que o curso poderia agregar:

> [...] pareciam ser questões marginais, pareciam questões que com o direito tinham pouco a ver, enquanto hoje sabemos muito bem que os temas ligados à bioética e à informática são não apenas temas capitais para a pesquisa do jurista, mas temas que transformam profundamente também o modo como o jurista olha a realidade e obrigaram-no a rever categoriais como o corpo e a pessoa. São categorias que estavam fora da atenção do jurista[315].

Thomas Vesting, por sua vez, traz à tona uma reflexão correlata de profunda importância: “quais serão as consequências da invenção do computador para a evolução futura do direito?” Um dos desafios do jurista, desde o advento do computador, e, em especial, da internet, tem sido analisar os caminhos para regulação:

> [...] Uma vez reconhecido que a internet não passa de ‘um computador gigante´, de um sistema de informação complexo, que se auto-organiza, no qual não ocorre uma transmissão central de dados, a teoria do Direito também deverá deslocar para primeiro plano a reprodução de sistemas contínua, dinâmica, não hierárquica e em forma de rede. [...] Hoje, a produção de dados do sistema jurídico depende em uma medida nunca antes vista de sobreposições, formas híbridas e ´acoplamentos estruturais´ com outros sistemas sociais, que, provavelmente, não mais podem ser facilmente apreendidas com a diferença (baseada no conceito de sentido) entre sistema e ambiente[316].

Ademais, na linha do que ensina Willis Santiago Guerra Filho, parece correto afirmar que, na pós-modernidade, se verifica uma aceitação da variedade de saberes que compõem o conhecimento científico, por meio dos quais se torna possível uma qualidade mais elevada daquele conhecimento. Sua abordagem é holística, porque relacionada com uma necessidade de convergência dos diversos sistemas de conhecimento, os quais se autolegitimam em sua prática e se tornam válidos na medida em que nos conscientizamos de que todos estão fundamentados

---

[315] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.5.
[316] VESTING, Thomas. **Teoria do direito**. São Paulo: Saraiva, 2015, p.314-315.

em opções arbitrárias com caráter localizado, o que os caracterizam como dogmáticos também[317].

As ciências transclássicas, no ensinamento de Willis Santiago Guerra Filho, estão inseridas não no tradicional paradigma simplificador das ciências clássicas, modernas, mas em um paradigma da complexidade, pertencente à pós-modernidade, e ao qual integram ciências como a cibernética e a teoria de sistemas[318].

Em 1996, o juiz norte-americano Frank Easterbrook, então vinculado à Universidade de Chicago, proferiu palestra, cujo conteúdo foi publicado como artigo 'Cyberspace and the law of the horse'[319], no qual se posicionava contra a ideia de um direito afeto à internet. Com a expressão *law of the horse*, ele se referia à internet como um instrumento, a exemplo do que no passado representou o cavalo, ou seja, um mero instrumento em casos de compra e venda, casos de acidentes causados pelo animal, ou, ainda, corridas de cavalos. Assim, para Easterbrook, nas Faculdades de Direito, os cursos deveriam se limitar a ensinar disciplinas que pudessem iluminar todo o direito: "The best way to learn the law applicable to specialized endeavors is to study general rules" [320] [321].

---

[317] "É a consciência dessas limitações, e o consenso em torno dos requisitos essenciais para o entendimento mútuo, que tornam possível a troca de conhecimentos entre esses sistemas". (GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.209).

[318] "Reafirma-se, agora, a necessidade de que se pratique de forma tão intensa quanto possível a in(ter/trans)disciplinariedade, o que exige, então, que tenhamos um paradigma unificador, uma perspectiva integradora em epistemologia, capaz de articular explicações de natureza sociológica, econômica, jurídica, biológica, química, física, filosófica e, até, teológica, para não mencionar artes e jogos. Um paradigma com essa característica "uni-totalizante" (Ein-und Allheit, para empregar expressão que remonta a Schelling, filósofo idealista alemão do século XIX) é o que se vem desenvolvendo por aqueles, como Edgar Morin, na esteira de Ilya Prigogine, que defendem a superação do tradicional paradigma simplificador das ciências clássicas, modernas, em favor de um paradigma da complexidade, em que se inserem "ciências transclássicas" (S. Maser), pós-modernas, como são a cibernética e a teoria de sistemas". (GUERRA FILHO, Willis Santiago. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017, p.209).

[319] EASTERBROOK, Frank H. Cyberspace and the law of the horse. In: **Journal Articles University of Chicago Law School**, 1996, n.207. Disponível em: <https://chicagounbound.uchicago.edu>. Acesso em: 25 ago. 2018.

[320] Tradução livre: "A melhor maneira de aprender a lei aplicável a esforços especializados é estudar regras gerais".

[321] Extrai-se do artigo de Easterbrook, Frank H: Dean Casper's remark had a second meaning that the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching 100 [*208] percent of the cases on people kicked by horses will not convey the law of torts very well. Far better for most students better, even, for those who plan to go into the horse trade to take courses in property, torts, commercial transactions, and the like, adding to the diet of horse cases a smattering of transactions in cucumbers, cats, coal, and cribs. Only by putting the law of the horse in the context of broader rules about commercial endeavors could one really understand the law about horses. Tradução livre: A observação de Dean Casper teve um segundo significado de que a melhor maneira de aprender sobre qual é a lei aplicável a questões especializadas é estudar

Em resposta, Lawrence Lessig se contrapõe (‘*a respectful disagreement essay*’) e escreve o artigo ‘The law of the horse: what cyberlaw might teach’[322], no qual pondera sobre a importância em investir no pensamento a respeito de como a lei e o ciberespaço se conectam[323].

A partir daí, Lawrence Lessig desenvolve a tese *Code is law.* Para ele, o código é capaz de impactar e delimitar o comportamento dos sujeitos. Não é apenas o direito (código que advém do Estado) que determina as regras no ciberespaço. Trata-se de um *puzzle* mais complexo, também formado pelas normas sociais, econômicas e pela arquitetura da rede – o código, entendido como “as instruções incorporadas no software e hardware que fazem o ciberespaço funcionar”[324].

Ao comentar sobre as discussões de regulação na Internet, Thomas Vesting reconhece que “tem sido frequentemente argumentado que normas técnicas têm um

---

regras gerais. Muitos casos lidam com vendas de cavalos; outros lidam com pessoas chutadas por cavalos; Ainda, há os que lidam com o licenciamento e corridas de cavalos, ou com os cuidados veterinários dado aos cavalos, ou com prêmios em shows de cavalos. Qualquer esforço para coletar essas vertentes em um curso sobre "A Lei do Cavalo" está condenado a ser superficial e a perder princípios unificadores. Ensinar 100 por cento dos casos em relação a pessoas chutadas por cavalos não irá transmitir a lei dos delitos devidamente. Muito melhor para a maioria dos estudantes, até mesmo, para aqueles que planejam entrar no comércio de cavalos para fazer cursos de propriedade, contratos, transações comerciais e afins, acrescentando à dieta dos casos de cavalos um punhado de transações em pepinos, gatos, carvão e berços. Somente colocando a lei do cavalo no contexto de regras mais amplas sobre empreendimentos comerciais é que alguém poderia realmente entender a lei sobre cavalos.

[322] LESSIG, Lawrence. The law of the horse: what cyberlaw might teach. **Harvard Law Review**, v.CXIII, 1999, p.501-546. É a partir das ideias expostas nesse artigo que Lessig escreveu seu primeiro livro ‘Code and Other Laws of Cyberspace’, em 1999.

[323] This general point is about the limits on law as a regulator and about the techniques for escaping those limits. This escape, both in real space and in cyberspace,5 comes from recognizing the collection of tools that a society has at hand for affecting constraints upon behavior. Law in its traditional sense — an order backed by a threat directed at primary behavior6 — is just one of these tools. The general point is that law can affect these other tools — that they constrain behavior themselves, and can function as tools of the law. The choice among tools obviously depends upon their efficacy. But importantly, the choice will also raise a question about values. By working through these examples of law interacting with cyberspace, we will throw into relief a set of general questions about law’s regulation outside of cyberspace. I do not argue that any specialized area of law would produce the same insight. I am not defending the law of the horse. My claim is specific to cyberspace. We see something when we think about the regulation of cyberspace that other areas would not show us. (LESSIG, Lawrence. The law of the horse: what cyberlaw might teach. **Harvard Law Review**, v.CXIII, 1999, p.501-546. Disponível em: <https://cyber.harvard.edu/works/lessig/finalhls.pdf>. Acesso em: 25 ago. 2018). Tradução livre: Este ponto geral é sobre os limites do direito como um regulador e sobre as técnicas para escapar desses limites. Essa fuga, tanto no espaço real quanto no ciberespaço, vem do reconhecimento da coleção de ferramentas que uma sociedade tem à mão para afetar as restrições sobre determinados comportamentos. A lei em seu sentido tradicional – uma ordem apoiada por uma ameaça direcionada ao comportamento primário – é apenas uma dessas ferramentas. O ponto geral é que a lei pode afetar essas outras ferramentas – elas restringem o comportamento e podem funcionar como ferramentas da lei. A escolha entre ferramentas obviamente depende de sua eficácia. Porém, mais importante, a escolha também levantará uma questão sobre valores. Ao trabalhar com esses exemplos de lei interagindo com o ciberespaço, lançaremos em relevo um conjunto de questões gerais sobre a regulamentação da lei fora do ciberespaço. Não defendo que qualquer área especializada do direito produza o mesmo insight. Eu não estou defendendo a lei do cavalo. Minha reivindicação é específica para o ciberespaço. Vemos algo quando pensamos sobre a regulação do ciberespaço que outras áreas não nos mostrariam.

[324] LESSIG, Lawrence. **Code**. v.2. New York: Basic Books, 2006, p.72.

impacto significativo na variedade e diversidade dos fluxos de comunicação da net"[325]:

> Although I am generally sympathetic to the position that a novel "Lex Informatica" poses new legal and political challenges for nation-states, it should, however, be clear from the outset that the attention for "code" and "architecture" is something different to a paraphrase of the ever-expanding role of technology in modern society. This has to be emphasized because the discourse of "the technological", which was already a prominent subject in the anti-modernist debate during the Weimar Republic, still casts a shadow on the contemporary legal discussion about the role of technical standards on the Internet[326].

Ainda, ao comentar a obra 'Code' de Lawrence Lessig, o professor da Universidade de Frankfurt/Main expõe que o "código" em si está incorporado em um ambiente de poder e interesses políticos. E ao direcionar sua análise por Froomkin e Benkler salienta:

> The starting point for any outline of the Internet has to be the fact that the Net is not a homogenous subject (or object) with stable boundaries. As Michael Froomkin points out, the Internet is not one thing, but the interconnection of many things. Arguing along these lines Yochai Benkler has usefully suggested distinguishing between "the physical infrastructure, logical infrastructure and content layers" when law is involved in framing digitally networked environments. I basically agree with these suggestions, but to be more precise in a theoretical sense I would neither use the term "infrastructure" for the technological layer of the Net nor the concept of a "communication system", as, for example, Lawrence Lessig does. The Internet is an intelligent network, i.e., the technology is not limited to a service function for content. Consequently, in contrast to other early electronic communication media like telephone or television, a hierarchical relationship between content and technology does not exist on the Internet yet it is exact this hierarchical relationship the word "infra-structure" presupposes[327].

---

[325] VESTING, Thomas. The autonomy of law and the formation of network standards. In: **German Law Journal**, n.6, 2004, p.639. [...] it has often been argued that technical standards have a significant impact on the variety and diversity of the Net's communication flows". Tradução livre: "[...] tem sido frequentemente argumentado que os padrões técnicos têm um impacto significativo na variedade e diversidade dos fluxos de comunicação da Internet".

[326] VESTING, Thomas. The autonomy of law and the formation of network standards. In: **German Law Journal**, v.5. n.6, 2004, p.639. Tradução livre: Embora eu seja geralmente simpático à posição de que um romance "Lex Informatica" coloca novos desafios legais e políticos para os Estados-Nação, deve ficar claro, desde o início, que a atenção para o "código" e para a "arquitetura" é algo diferente a uma paráfrase do papel sempre crescente da tecnologia na sociedade moderna. Isso tem de ser enfatizado porque o discurso do "tecnológico", que já era assunto de destaque no debate antimodernista durante a República de Weimar, ainda lança uma sombra sobre a discussão jurídica contemporânea sobre o papel das normas técnicas na Internet.

[327] VESTING, Thomas. The autonomy of law and the formation of network standards. In: **German Law Journal**, v.5. n.6, 2004, p.640. Tradução livre: O ponto de partida para qualquer esboço da Internet deve ser o fato de que a Rede não é um assunto (ou objeto) homogêneo com fronteiras estáveis. Como Michael Froomkin aponta, a Internet não é uma coisa, mas a interconexão de muitas coisas. Argumentando ao longo dessas linhas, Yochai Benkler sugeriu, de forma útil, a distinção entre "a infraestrutura física, a infraestrutura lógica e as camadas de conteúdo" quando a lei está envolvida no enquadramento de ambientes digitalmente conectados em rede. Concordo basicamente com essas sugestões, mas para ser mais preciso em um sentido teórico eu não usaria o termo "infraestrutura" para a camada tecnológica da Internet nem o conceito de "sistema de comunicação", como, por exemplo, Lawrence Lessig faz. A Internet é uma rede inteligente, ou seja, a tecnologia não se limita a uma função de serviço para o conteúdo. Consequentemente, em contraste com outros meios de comunicação eletrônica como o telefone ou a televisão, uma relação hierárquica entre conteúdo e tecnologia não existe na Internet, mas é exata essa relação hierárquica que a palavra "infraestrutura" pressupõe.

Para Tercio Sampaio Ferraz Junior, a noção clássica de liberdade como espaço de ação não restrito pela liberdade dos outros, que se manifesta sobre bens cujo uso exclui o uso dos outros, no âmbito da sociedade de informação, tende a sofrer uma revisão. Na verdade, atira-nos a um limite de abstração, cujo conceito parece ir além de um uso alternativo atípico. No campo informático, dada a inexistência de limitação física, tratamos de bens (informação e conhecimento), cujo uso por alguém não exclui o uso por outro [...][328]. Para o autor, o ciberespaço, por exemplo, somente se constrói à medida que cada espaço de ação de cada sujeito é voltado para a comunicação com os outros, sem a qual o próprio ambiente perde sentido. Não é propriamente "espaço" como *res materialis* ou *immaterialis*. Assim, embora não nos retire do espaço no qual vivemos, culturalmente o supera[329]. E dessa revolução cultural trazida pelo mundo digital faz-nos perceber que, aos poucos, antigas e sedimentadas noções, como a de direito subjetivo, além de deixar de ser "o conceito central do direito privado" (*"der zentrale Begriff des Privatsrechts"*), não é mais capaz de lidar com essa desintegração em pedaços (*bits*) da estrutura íntegra das coisas. Isso porque a revolução cultural que nos torna aptos a construir universos alternativos e paralelos ao mundo supostamente *dado*, converte-nos de *sub-jecti* – indivíduos únicos – em *projecti* – de vários mundos[330].

Em uma sociedade na qual praticamente tudo se encontra conectado, verificamos um deslocamento de poder. O novo *institutio principis* decorre de programações algorítmicas.

O atual horizonte apresenta a interação entre dispositivos inteligentes, sensores e indivíduos. Por vezes, sem se dar conta, as limitações da esfera de poder das pessoas são definidas pela arquitetura da rede.

Em assunto de regulação para conflitos oriundos da internet, as principais correntes doutrinárias, segundo Marcel Leonardi, são:

> a) autorregulação, mediante regras e princípios estabelecidos pelos próprios participantes 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; d) abordagem mista,

[328] FERRAZ JUNIOR, Tercio Sampaio. Direito e realidade: a erosão do real jurídico pelo mundo virtual. In: FERRAZ JUNIOR, Tercio Sampaio. **O direito entre o futuro e o passado**. São Paulo: Noeses, 2014, p.52.
[329] FERRAZ JUNIOR, Tercio Sampaio. Direito e realidade: a erosão do real jurídico pelo mundo virtual. In: FERRAZ JUNIOR, Tercio Sampaio. **O direito entre o futuro e o passado**. São Paulo: Noeses, 2014, p.52.
[330] FERRAZ JUNIOR, Tercio Sampaio. Direito e realidade: a erosão do real jurídico pelo mundo virtual. In: FERRAZ JUNIOR, Tercio Sampaio. **O direito entre o futuro e o passado**. São Paulo: Noeses, 2014, p.56-57.

> utilizando o sistema jurídico em conjunto com a própria arquitetura da internet[331].

Há, ainda, um outro caminho de regulação da rede, consistente na chamada autorregulação regulada, adotada na Alemanha. Segundo explicam Juliano Maranhão e Ricardo Campos:

> Uma forma moderna de lidar com a crescente incerteza do ponto de vista regulatório encontra-se no instituto da autorregulação regulada. Este procura trabalhar no liame entre duas tradicionais formas de regulação: autorregulação e regulação por um terceiro normalmente o Estado (*Fremdregulierung*). Por um lado, a autorregulação tem a vantagem da eficiência pela disposição do conhecimento interno e dinâmica de constante revisão de conceitos. Por outro, tem a desvantagem por não necessariamente perseguir interesses e valores públicos. Já a regulação por terceiro (*Fremdregulierung*) tem a vantagem de poder ser implementada por coerção em nome do interesse público e a desvantagem de, em ambientes dinâmicos, não dispor de conhecimento suficiente para lograr êxito na persecução do objetivo. A autorregulação regulada oferece uma outra e nova possibilidade de lidar com as incertezas, ao conciliar vantagens das duas abordagens alternativas: a regulação *versus* a autorregulação. Foca-se no importante momento de auto-organização conforme expertise e dinâmica própria da indústria, estimulando-se, porém, alguns parâmetros gerais de interesses públicos caros ao Estado e sociedade. Nesse sentido, a autorregulação regulada consegue "induzir" o setor privado a contribuir para o cumprimento de tarefas públicas. Essa forma de regulação pode lidar melhor com uma sociedade que cada vez mais se locomove, e se distancia, de uma sociedade centrada em organizações conseguindo absorver melhor as incertezas e construir parâmetros melhores de eficácia na regulação[332].

A fórmula da autorregulação regulada está na linha de estabelecer um procedimento em plataforma digital, por meio da qual podem ser inseridas provocações de reclamações, contestações em resposta a medidas de controle adotadas pelos provedores de redes sociais, medidas essas balizadas previamente pelo Estado, que não as aplicará diretamente, porém, pela parametrização, assume papel determinante na forma como as aplicações atuarão na autorregulação[333].

Ademais, conforme será visto no próximo capítulo, princípios como *privacy by design, privacy by default, privacy by business model,* e inteligência artificial

---

[331] LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012, p.130. Segundo o autor, as discussões sobre a regulação da Internet e sobre a tutela de direitos em seu âmbito estão em estágio mais avançado nos Estados Unidos, especialmente em razão das obras de Lawrence Lessig, Yochai Benkler, Jack L. Goldsmith, Tim Wu, Jonathan L. Zittrain e Daniel Solove.

[332] MARANHÃO, Juliano; CAMPOS, Ricardo. Exercício de autorregulação regulada das redes sociais no Brasil. In: NERY, N. Campos; ABBOUD, George. (Orgs). ***Fake news* e regulação**. São Paulo: RT, 2018, p.5-6.

[333] MARANHÃO, Juliano; CAMPOS, Ricardo. Exercício de autorregulação regulada das redes sociais no Brasil. In: NERY, N. Campos; ABBOUD, George. (Orgs). ***Fake news* e regulação**. São Paulo: RT, 2018, p.7-8.

explicável consistem em caminhos que visam regular a proteção de dados por meio da arquitetura da tecnologia.

Apesar da tentativa de se regular a proteção de dados, também, pela norma jurídica, é certo que há grande dificuldade de se estruturar um sistema normativo informático, principalmente, diante da rápida evolução/modificação das tecnologias.

Assim, não há que se negar que a resolução dos conflitos tecnológicos deve ter como ponto de partida o próprio sistema tecnológico e não o sistema jurídico, já que este último possui dificuldades em acompanhar aquele no rápido compasso de suas evoluções.

Todavia, o direito não pode ficar à margem da discussão e nem acreditamos que o direito deva estar distante da tecnologia. O que acreditamos é que o caminho a ser perseguido deve ser de uma intervenção mínima do direito na esfera da tecnologia, diante da própria dificuldade do sistema jurídico acompanhar sua evolução. Nesse sentido, é imprescindível analisarmos o percurso normativo que culminou em regulações das tecnologias e proteção de dados na Europa e no Brasil, com um breve olhar aos Estados Unidos, para que possamos compreender qual o melhor caminho a ser trilhado na resolução de conflitos envolvendo proteção de dados e os algoritmos.

3 DA PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO

> Uma vida passada inteiramente em público, na presença de outros, se torna, podemos dizer, rasa. Mantendo sua visibilidade, tal vida perderia a qualidade de se entregar ao olhar, vindo de um lugar mais escuro que deve permanecer oculto se você não quiser perder profundidade num sentido genuinamente real, não subjetivo.
> **Hannah Arendt (1906-1970)**

3.1 A reinvenção da privacidade: do 'direito de estar só' ao 'controle dos dados pessoais'

Desde a antiguidade, pessoas em quase todas as sociedades debateram questões de privacidade. Como não poderia ser diferente, com o desenvolvimento de novas tecnologias da informação durante o século passado, conforme tratado em capítulo anterior, especialmente pelo processamento de informações via computador no pós-guerra, as questões vinculadas à privacidade assumiram patamares intensos e nunca antes tão debatidos.

As bases do conceito de privacidade encontram-se alicerçadas no individualismo liberal e em noções de separação entre Estado e sociedade civil: "Privacy, therefore, tends to reinforce individuation, rather than community, sociability, trust and so on. It is about me, and nobody else"[334]. A proteção à privacidade teve, portanto, um caráter fortemente individualista em seus primórdios[335].

Segundo Pablo Lucas Murillo, o fundamento da atual noção de privacidade procede, basicamente, do pensamento anglo-saxão. É no âmbito dos debates políticos e filosóficos de autores ingleses – tais como John Locke, Robert Price e John Stuart Mill – que brotam as noções de liberdade e autonomia que, ao final, conduzem à privacidade. Há a aproximação a uma série de ideias que vão especificando o marco próprio da vida privada: a liberdade em suas facetas de autonomia, isolamento e exclusão de intervenções públicas[336].

---

[334] Tradução livre: "A privacidade tende a reforçar o individualismo em lugar da comunidade, sociabilidade, confiança, etc. Ela diz respeito exclusivamente a mim e a nada mais". (BENNET, Collin. In defence of privacy. The concept and the regime. **Surveillance & Society**, v.8, n.4, 2011, p.486).

[335] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p. 28.

[336] LUCAS MURILLO, Pablo. **El derecho a la autodeterminación informativa**. Madri/Espanha: Tecnos, 1990, p.49.

Thomas Hobbes, segundo pondera Pablo Lucas Murillo, utiliza um artifício racional e, portanto, moderno, para sustentar o absolutismo. Ao contrário de outros de seu tempo, que usavam teses transcendentes da legitimidade monárquica, ele percebe a existência de uma esfera privada estritamente relacionada à liberdade do súdito. John Locke, por sua vez, segundo Pablo Lucas Murillo, é o autor no qual encontramos as principais bases. Tanto na obra 'Essay of Civil Government' (1690), quanto na 'Letter Concerning Toleration' (1689), desenvolve suas ideias de liberdade que implicam na autonomia para dispor, como melhor lhe pareça, de sua pessoa, de seus atos, de seus bens e de tudo quanto lhe pertença, submetendo-se às leis sob as quais vive. Enfim, é a exclusão de toda submissão à vontade arbitrária do outro, a fim de seguir livremente a sua. Quanto à John Stuart Mill, apesar de nunca ter usado as expressões 'vida privada', 'privacidade' ou 'intimidade', é evidente que no desenvolvimento de suas ideias, esses conceitos aparecem, porque sustenta que deve existir uma separação nítida entre o âmbito próprio da liberdade humana, regrado pela autonomia individual, e, de outro lado, a esfera pública[337].

Em que pese a noção atual sobre a privacidade ser fruto de uma concepção da modernidade, continua a ser um conceito bastante discutido. Nesse sentido, Daniel Solove considera que privacidade é um conceito em *desordem*, dada a dificuldade de seu significado:

> Privacy, however, is a concept in disarray. Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.[338]

Existe uma modificação de partida no debate atual sobre privacidade, qual seja, aquela concepção de *esfera pública* de Jünger Habermas não se figura como antes[339]. O primeiro a definir o público e o privado como esferas distintas foi Aristóteles, para quem a esfera da política e das atividades políticas, a *polis*,

---

[337] LUCAS MURILLO, Pablo. **El derecho a la autodeterminación informativa**. Madri/Espanha: Tecnos, 1990, p.9-54.

[338] Tradução livre: Privacidade, no entanto, é um conceito em desordem. Ninguém consegue articular o que significa. Atualmente, a privacidade é um conceito amplo, englobando (entre outras coisas) liberdade de pensamento, controle sobre o corpo, solidão em casa, controle de informações pessoais, liberdade de vigilância, proteção de sua reputação e proteção contra pesquisas e interrogatórios. (SOLOVE, Daniel J. **Understanding privacy**. Cambridge, London: Harvard University Press, 2008, p.13).

[339] A esfera pública moderna denota a forma como a Constituição e a circulação da informação política e social é estruturada dentro de um Estado, tornando-se parte essencial e basilar de todas das democracias liberais modernas. (MARANHÃO, Juliano; CAMPOS, Ricardo. Exercício de autorregulação regulada das redes sociais no Brasil. In: NERY, N. Campos; ABBOUD, George. (Orgs). ***Fake news* e regulação**. São Paulo: RT, 2018).

pertencia ao âmbito do público, enquanto a esfera doméstica da família e de seu lar, o *oikos*, pertencia ao âmbito privado.

Há uma concentração de poder em algumas empresas que acabam na construção da esfera pública. Houve, portanto, uma transformação dessa esfera. A forma como as informações circulam e são compreendidas mudou, porquanto a sociedade de rede transpassou, em grande parte, a sociedade de organizações, quando a produção de informação era mais centralizada nos meios de comunicação em massa. Segundo Juliano Maranhão, "se antes a esfera pública era centrada na produção de informação por jornais impressos e televisão, a esfera pública atualmente é centrada em redes e plataformas digitais[340]". E acrescenta:

> Com a popularização do mundo digital e o papel cada vez mais relevante dos usuários não só no consumo, mas na própria produção do conteúdo (os chamados "produmidores"), a centralidade das organizações aos poucos perde seu valor. Esse fato se dá acima de tudo porque aquele "contato interrompido" entre emissor (grandes empresas jornalísticas) e receptor (público geral), que caracterizava a esfera pública na sociedade das organizações, volta a se restabelecer. Com as redes sociais, a produção de informação nova pode se dar de forma desvinculada das organizações jornalísticas, ou seja, da interação entre o emissor e o receptor, interação entre leitores em blogs, em posts no facebook etc. Isso, sem que a informação produzida de modo pulverizado perca seu alcance, que não só tem profusão abrangente, como também tem sua eficácia ampliada pela possibilidade de direcionamento para públicos específicos[341].

Na contribuição de Paula Sibilia, tanto a definição como o uso dos espaços estão sendo alterados em função do processamento digital e do controle cada vez mais intenso realizado sobre os indivíduos, diluindo-se a oposição clássica entre as esferas pública e privada para dar à luz outras modalidades, de modo que "é lógico supor, portanto, que as subjetividades e os corpos contemporâneos se veem afetados pelas tecnologias da virtualidade e da imortalidade, bem como pelos novos modos de vivenciar os limites espaço-temporais que essas ferramentas inauguram"[342].

O raciocínio binário "público ou privado", ademais, é muito perigoso quando adotado como fundamento para negar a tutela ao direito à privacidade. O aumento da acessibilidade impacta não apenas na quantidade, mas também na qualidade,

---

[340] MARANHÃO, Juliano; CAMPOS, Ricardo. Exercício de autorregulação regulada das redes sociais no Brasil. In: NERY, N. Campos; ABBOUD, George. (Orgs). ***Fake news* e regulação**. São Paulo: RT, 2018 (no prelo).
[341] MARANHÃO, Juliano; CAMPOS, Ricardo. Exercício de autorregulação regulada das redes sociais no Brasil. In: NERY, N. Campos; ABBOUD, George. (Orgs). ***Fake news* e regulação**. São Paulo: RT, 2018 (no prelo).
[342] SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015, p.65.

elevando o risco dos prejuízos decorrentes da revelação. Na lição de Daniel Solove, o aumento da acessibilidade faz uma diferença de quantidade se transformar em uma diferença de qualidade, aumentando o risco dos prejuízos decorrentes da revelação. Isso proque o aumento da acessibilidade faz com que um evento ocorrido em um contexto seja alterado significativamente, transformando-se em um acontecimento permanente e amplamente difundido[343]. Como exemplo desse raciocínio citamos o caso envolvendo a modelo brasileira Daniela Cicarelli, ocorrido em 2007, quando ela e seu namorado, na praia de Cádiz, na Espanha, tiveram um momento bastante íntimo no mar. Não obstante estivessem em um local público (praia), aquele momento do casal foi filmado e espalhado pela internet, violando seus direitos fundamentais de intimidade e privacidade.

Muitas vezes o termo privacidade é usado como o direito de não ser molestado, reforçando a noção de que privacidade seria algo sobre isolamento e separação. Outros aproximam o conceito de privacidade à solidão, segredo, confidencialidade e anonimato. Mas há um consenso crítico, segundo Lucia Santaella, sobre o fato de que os problemas sociais relativos à privacidade são mais complexos do que a simples invasão da privacidade individual[344].

Nesse sentido, pondera Collin Bennett que os caminhos argumentativos da privacidade são estreitos, e que esse conceito nunca poderá servir como antídoto para a vigilância:

> Privacy' and all that it entails is argued to be too narrow, too based on liberal assumptions about subjectivity, too implicated in rights-based theory and discourse, insufficiently sensitive to the social sorting and discriminatory aspects of surveillance, culturally relative, overly embroiled in spatial metaphors about invasion' and 'intrusion', and ultimately practically ineffective. As a concept, and as a way to frame the arious global challenges encountered within 'surveillance societies', it is profoundly inadequate. It is not, and can never be, the 'antidote to surveillance'[345].

Segundo a teoria das esferas, desenvolvida pelo Tribunal Constitucional alemão, é possível distinguir três esferas, com intensidade de proteção decrescente:

---

[343] LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012, p.363.

[344] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.76.

[345] BENNET, Collin. In defence of privacy. The concept and the regime. **Surveillance & Society**, v.8, n.4, 2011, p.485. Tradução livre: A privacidade e tudo o que ela implica é considerada como sendo demasiado estreita, baseada em hipóteses liberais sobre a subjetividade, muito implicada em teoria e discurso baseados em direitos, insuficientemente sensível aos aspectos sociais e discriminatórios da vigilância, culturalmente relativa, excessivamente envolvida em metáforas espaciais sobre "invasão" e "intrusão" e, em última instância, praticamente ineficazes. Como um conceito, e como uma forma de enquadrar os vários desafios globais encontrados nas "sociedades de vigilância", é profundamente inadequado. Não é, e nunca poderá ser, o "antídoto para a vigilância".

a) a esfera mais interior (último e inviolável âmbito de liberdade humana, âmbito mais interno (íntimo), esfera íntima inviolável, esfera nuclear da configuração da vida privada, protegida de forma absoluta); b) a esfera privada ampliada, que inclui o âmbito privado que não pertence à esfera mais interior; e c) a esfera social, que inclui tudo aquilo que não for atribuído nem ao menos à esfera privada ampliada[346].

A privacidade possui um valor moral que funciona como um escudo protetor ao garantir certa liberdade e independência, mantendo os indivíduos livres da vigilância, do preconceito, da pressão e da submissão ao conformismo, à exploração e ao julgamento do outro[347].

Lucia Santaella expõe o debate em torno da crítica à privacidade, no sentido de que esse direito seria, na verdade, um direito derivado de um feixe de outros direitos: propriedade, liberdade e segurança do próprio corpo. Esse aspecto crítico se torna mais nítido quando analisados casos envolvendo violação da privacidade. Nesse sentido, pontua a autora que embora as críticas contra a privacidade tenham certa consistência, "é bem maior o número de estudiosos que buscam defini-la com mais clareza para melhor defendê-la"[348].

Para Daniel Solove, uma boa metáfora a ser aplicada à privacidade é compará-la a um guarda-chuva, visto que abrange diversos direitos da mesma família. E dentro desse rol dos direitos da privacidade, destacam-se o direito ao sigilo, à intimidade, à imagem, à honra e à proteção aos dados pessoais[349].

Além disso, a privacidade tem características plásticas, variando conforme a cultura, o tempo e o local. Nesse sentido ponderam Erick Lucena Campos Peixoto e Marcos Ehrhardt Júnior, que ao longo da história, nas diferentes sociedades existentes, a noção de privacidade foi sentida de uma maneira muito própria em cada círculo social, daí a razão de se dizer que a privacidade tem feição plástica, que varia conforme a época e o local, de modo que pode ser "adaptável, valorada de um jeito por uma cultura, e até dispensável para outra"[350].

---

[346] ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução Virgilio Afonso da Silva. São Paulo: Malheiros, 2008, p.360-361.
[347] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.81.
[348] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.77-78.
[349] SOLOVE, Daniel J. **Understanding privacy**. Cambridge, London: Harvard University Press, 2008.
[350] PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. In: **Revista Brasileira de Direito Civil** – RBDCivil | Belo Horizonte, v.16, p.35-56, abr.-jun., 2018, p.36. "Desde que o homem resolveu demarcar limites, estabelecendo um espaço para sua convivência apartada dos demais, surge a noção que mais tarde se consubstanciaria no que se denomina privacidade. Desse modo, é possível afirmar que a privacidade começa no sentido físico".

No início do século XX, a privacidade chegou a ser qualificada, em decisão da Suprema Corte Americana[351], como o "the most comprehensive of rights and the right most valued by civilized men[352]". Na maioria dos países, ela é considerada um direito fundamental. Tanto assim que Daniel Solove observa:

> Privacy is an issue of profound importance around the world. In nearly every nation, numerous statutes, constitutional rights, and judicial decisions seek to protect privacy. In the constitutional law of countries around the globe, privacy is enshrined as a fundamental right.[353].

Retomando aos primórdios, verifica-se que foi com a chegada da fotografia e a facilidade para reproduzir imagens, junto ao poder de disseminação da informação por meio da mídia impressa, que surgem as primeiras preocupações envolvendo o

[351] Olmstead v. United States, 277 U.S. 438 (1928). The Court reviewed whether the use of wiretapped private telephone conversations, obtained by federal agents without judicial approval and subsequently used as evidence, constituted a violation of the defendant's rights provided by the Fourth and Fifth Amendments. In a 5-4 decision, the Court held that neither the Fourth Amendment nor the Fifth Amendment rights of the defendant were violated. This decision was later overturned by Katz v. United States in 1967. Tradução livre: A Corte analisou se o uso de conversas telefônicas privadas interceptadas por telefone, obtidas por agentes federais sem aprovação judicial e posteriormente usadas como prova, constituía uma violação dos direitos do réu com arrimo na Quarta e Quintas Emendas Constitucionais. Em uma decisão de 5 a 4 votos, a Corte considerou que nem a Quarta Emenda nem os direitos da Quinta Emenda do réu foram violados. Esta decisão foi posteriormente revogada por Katz v. Estados Unidos em 1967.

[352] Tradução livre: "o mais compreensivo dos direitos e o direito mais valioso para os homens civilizados".

[353] Tradução livre: "A privacidade é uma questão de profunda importância em todo o mundo. Praticamente todos os países procuram proteger a privacidade por meio de seus numerosos estatutos, direitos constitucionais e decisões judiciais. Na lei constitucional dos países em todo o mundo, a privacidade é consagrada como um direito fundamental. (SOLOVE, Daniel J. **Understanding privacy**. Cambridge, London: Harvard University Press, 2008, p.13). When privacy is not directly mentioned in constitutions, the courts of many countries have recognized implicit constitutional rights to privacy, such as Canada, France, Germany, Japan, and India (p.15). In addition, thousands of laws protect privacy around the world. Multinational privacy guidelines, directives, and frameworks have influenced the passage of privacy laws in a vast number of nations. In 1980, the Organization for Economic Cooperation and Development (OECD) issued its Privacy Guidelines. In 1995, the European Union's Directive on Data Protection specified fundamental principles for privacy protection in Europe. The Asia-Pacific Economic Cooperation (APEC), with over twenty member nations, set forth a Privacy Framework in 2004. Numerous countries have enacted extensive privacy protections, such as Canada's Personal Information Protection and Electronic Documents Act of 2000, Japan's Personal Information Protection Law of 2003, Australia's Privacy Act of 1988, and Argentina's Law for the Protection of Personal Data of 2000, to name just a few. In the United States, hundreds of laws at state and federal levels protect privacy. Courts in most states recognize four torts to remedy privacy wrongs. Since 1970, the U.S. Congress has passed several dozen statutes to protect the privacy of government records, student records, financial information, electronic communications, vídeo rental data, and drivers' records, among other things. (p.15) Tradução livre: Quando a privacidade não é mencionada diretamente nas constituições, os tribunais de vários países reconhecem os direitos constitucionais implícitos à privacidade, como o caso do Canadá, França, Alemanha, Japão e Índia (p.15). Além disso, milhares de leis protegem a privacidade em todo o mundo. Diretrizes, diretivas e estruturas de privacidade multinacionais influenciaram a aprovação de leis de privacidade em um grande número de nações. Em 1980, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) publicou suas Diretrizes de Privacidade. Em 1995, a Diretiva da União Européia sobre Proteção de Dados especificou princípios fundamentais para a proteção da privacidade na Europa. A Cooperação Econômica Ásia-Pacífico (APEC), com mais de vinte países membros, estabeleceu um Quadro de Privacidade em 2004. Vários países promulgaram amplas proteções à privacidade, como a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos do Canadá de 2000, a Lei de Proteção de Informações Pessoais do Japão. de 2003, a Lei de Privacidade da Austrália de 1988 e a Lei de Proteção de Dados Pessoais da Argentina de 2000, para citar apenas alguns exemplos. Nos Estados Unidos, centenas de leis a níveis estadual e federal protegem a privacidade. Tribunais na maioria dos estados americanos reconhecem quatro violações como forma de proteção da privacidade. Desde 1970, o Congresso dos EUA aprovou dezenas de estatutos para proteger a privacidade de registros do governo, registros de alunos, informações financeiras, comunicações eletrônicas, dados de locação de vídeo e registros de motoristas, entre outras coisas.

assunto. Esse cenário, segundo Erick Lucena Campos Peixoto e Marcos Ehrhardt Júnior, consiste na antessala dos problemas da privacidade enfrentados hoje.[354]

O início dos debates em torno da privacidade é contemporâneo ao advento das mídias trazidas pela Revolução Industrial, quais sejam, a impressão em massa dos jornais, a fotografia e o aumento do fluxo publicitário. Em seguida, viriam ainda, o cinema, o fonograma, a televisão e o computador. Mais recentemente a sociedade é desafiada pelo uso massivo dos algoritmos e das técnicas de *machine learning*, que resultam em tomadas de decisão automatizadas.

Sobre o jornal, ainda que não fosse algo exatamente novo, sua circulação aumentara exponencialmente. Houve uma elevação de 1000% de 1850 a 1890 na circulação dos impressos. E sob a perspectiva dos leitores, de 800 mil leitores em 1850, subiu para 8 milhões em 1890[355]. Ademais, houve uma mudança de foco dos jornais, os quais passaram a relatar casos mais sensacionalistas, como escândalos e fofocas da vida das pessoas, um tipo de jornalismo que ficou conhecido nos Estados Unidos como *yellow journalism.*

Quanto às câmeras de fotografia, a verdadeira ameaça repousou sobre a sua sofisticação. No início eram grandes, caras, e não muito portátil. Em 1884, a Eastman Kodak produziu a *snap camera*, uma câmera portátil para uso geral do público, de modo que facilitara às pessoas fotografarem em público. Esse aparelho, associado à nova inclinação dos jornais da época de exploração sensacionalista, passou a consistir uma clara ameaça à vida privada das pessoas[356].

O célebre conceito associado ao "direito de estar só" foi desenvolvido por Warren e Brandeis[357], no final do século XIX, embora a frase em si mesma ("the right to be let alone") seja atribuída a Thomas McIntyre Cooley[358].

Warren e Brandeis dissociaram a proteção da vida privada à propriedade, aproximando-a à inviolabilidade da personalidade. Trata-se de um marco importante,

---

[354] PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. In: **Revista Brasileira de Direito Civil** – RBDCivil | Belo Horizonte, v.16, p.35-56, abr.-jun. 2018, p.36.

[355] SOLOVE, Daniel, J. A brief history of information privacy law. In: **Proskauer on privacy**, PLI. Washington: George Washington Law Faculty Publications, 2006, p.11.

[356] SOLOVE, Daniel, J. A brief history of information privacy law. In: **Proskauer on privacy**, PLI. Washington: George Washington Law Faculty Publications, 2006, p.12.

[357] Stefano Rodotà adverte que esse notório conceito do "direito a ficar só" foi na verdade concebido quarenta anos antes por Robert Kerr. (RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.7).

[358] COOLEY, Thomas McIntyre. **A treatise on the law of torts, or the wrongs which arise independent of contract**. Chicago: Callaghan and Company, 1879. Disponível em: <http://www.hathitrust.org/>. Acesso em: 04 set. 2018.

ao defenderem, pela primeira vez, que os escritos pessoais e outras produções pessoais devem ser protegidos não pelo princípio da propriedade privada, mas pelo princípio da inviolabilidade da personalidade. Os autores buscaram construir um direito à privacidade na *common law*, a partir de precedentes de julgados das Cortes inglesas.

A noção desse direito estava vinculada a questões patrimoniais, conforme observa Daniel Solove, sobre decisão de 1604: "better-known is a judicial pronouncement in *Semayne's Case*7 in 1604 that ´the house of everyone is to him as his castle and fortress´[359].

Além disso, contrariando as decisões da Suprema Corte na época, Warren e Brandeis dissociaram o direito à privacidade não apenas da propriedade, mas também do direito à liberdade. O direito à liberdade, segundo eles, assegura amplos privilégios civis, mas não a privacidade.

O artigo de Warren e Brandeis, 'The right to privacy', de 1890, demonstra a preocupação do homem moderno com a invasão dos jornais, fotografias – então novas tecnologias para a época – em seus domínios da vida privada e doméstica, destinando ao consentimento do indivíduo o limite de sua privacidade. Nas palavras dos autores, "The right to privacy ceases upon the publication of the facts by the individual, or with his consent"[360]. Eles defenderam, ainda, que a alegação de veracidade da informação pelo agressor não exclui a violação do direito, assim como a conduta despida de dolo igualmente não exclui a violação desse direito. Por fim, outro ponto importante discutido no artigo é que o direito à privacidade não impede a publicação do que é de interesse geral.

O objetivo desses autores, ao escrever o artigo, foi estabelecer um limite jurídico que vedasse as intromissões da imprensa na vida privada. O motivo concreto que impulsionou Samuel Warren a escrever sobre o assunto e a pedir a ajuda de Louis Brandeis – que futuramente se tornou juiz da Suprema Corte dos Estados Unidos[361] – foi a intromissão escandalosa dos periódicos de Boston em sua

---

[359] SOLOVE, Daniel, J. A brief history of information privacy law. In: **Proskauer on privacy**, PLI. Washington: George Washington Law Faculty Publications, 2006, p.5. Tradução livre: mais conhecido é um pronunciamento judicial no Caso de Semayne, em 1604, que "a casa de todos é para ele como seu castelo e fortaleza".

[360] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v.IV, n.5, 1890, p.218. Tradução livre: O direito à privacidade cessa com a publicação de fatos pelo indivíduo ou com o seu consentimento.

[361] Anos mais tarde, Louis D. Brandeis, como Juiz da Suprema Corte dos EUA, participou do caso Olmstead v. United States (1928), tendo seu voto, porém, vencido. O caso diz respeito a uma decisão na qual a Corte analisou se o uso de conversas telefônicas privadas, obtidas por agentes federais sem aprovação judicial e posteriormente usadas como prova, constituía uma violação dos direitos do réu fornecidos pela Quarta e Quinta

vida conjugal[362]. Isso porque, em 1890, a Sra. Warren – uma então jovem dona de casa de Boston, Massachusetts, filha de um senador de Delaware e mulher de um jovem e bem-sucedido fabricante de papel que tinha desistido da prática jurídica para tomar conta do negócio que havia herdado de Samuel Dennis Warren – tinha por costume realizar em sua casa uma série de eventos sociais. O jornal local 'Saturday Evening Gazette' cobria suas festas em detalhes altamente pessoais e embaraçosos. Não bastasse esse incômodo, a gota d´água se deu quando jornais tiveram um furo do casamento de uma das filhas do casal Warren. Foi a partir daí que Warren procurou seu sócio na advocacia, Louis Dembitz Brandeis, e juntos reuniram decisões antigas cujas soluções se deram com base em difamação, violação de algum direito de propriedade, violação de confiança ou contrato implícito. O resultado foi o já mencionado artigo 'The right to privacy', publicado em 1890, na Harvard Law Review, cuja conclusão apontou que o remédio para os crescentes abusos da imprensa através de um nível mais profundo de proteção do indivíduo contra a imposição de sofrimento mental deveria estar atrelado a um princípio mais amplo, e o qual merecia ser reconhecido autonomamente. A esse princípio Warren e Brandeis chamaram de direito à privacidade (*right to privacy*)[363].

No início, esse direito portava uma feição individualista (*zero*-relationship), com cunho eminentemente patrimonialista, fazendo da privacidade, em sua gênese, uma prerrogativa reservada a extratos sociais bem determinados[364] (a privacidade e a pobreza seriam incompatíveis?). O direito de ser deixado em paz é fruto da era burguesa. Não obstante, Stefano Rodotà reconhece que mesmo com o feitio de seus primórdios, esse direito emerge, outrossim, como um instrumento de proteção das minorias, da livre manifestação e ao direito de desenvolver livremente a personalidade:

Emendas à Constituição. Por 5 votos contra 4 votos, a Corte considerou que os direitos do réu não foram violados. Esta decisão foi posteriormente anulada pelo caso Katz v. United States em 1967. Esse último caso, considerado histórico, a Suprema Corte dos Estados Unidos, ao discutir a natureza do direito à privacidade, enfrentou os limites do direito de obter ligações telefônicas, por medida de busca e apreensão. Foi considerado como invasivo, com base na Quarta Emenda Constitucional, a busca a esse tipo de dados, com base na "expectativa razoável de privacidade" do indivíduo. Esse caso se tornou paradigma e usado em vários outros, em especial com o avanço da tecnologia.

[362] LUCAS MURILLO, Pablo. **El derecho a la autodeterminación informativa**. Madri/Espanha: Tecnos, 1990, p. 57.

[363] Mais detalhes em: PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. In: **Revista Brasileira de Direito Civil** – RBDCivil | Belo Horizonte, v.16, p.35-56, abr.-jun., 2018, p.39.

[364] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.10.

> O direito de ser deixado em paz não foi construído meramente com a expressão da era de ouro da burguesia, que havia protegido sua esfera imaterial por meio da mesma proibição ao esbulho que por muito tempo foi a principal característica da propriedade imobiliária. Sob o impulso dado por Louis Brandeis, emergiu uma visão na qual a privacidade foi vista também como uma ferramenta de proteção a minorias e opiniões dissonantes e, portanto, à livre manifestação e ao direito de livremente desenvolver a personalidade[365].

Ainda conforme descortina Stefano Rodotá, surge um aparente paradoxo: "a forte proteção da esfera privada em última instância não resguarda a privacidade nem a mantém protegida do olhar indesejável; na verdade, permite que crenças e opiniões individuais sejam tornadas públicas livremente"[366].

Ao longo das décadas do século XX, segue-se uma produção científica intensa sobre o conceito e os limites do direito à privacidade, a exemplo dos artigos de William Lloyd Prosser[367]e Edward Bloustein[368].

O primeiro, em 1960, publica um artigo repudiando a posição de Warren e Brandeis, ao sugerir que a privacidade não era um valor independente, mas uma composição de interesses na área de reputação, tranquilidade emocional e propriedade intangível[369].

William Lloyd Prosser sugere uma formulação de que o direito à privacidade compreende quatro tipos diferentes de violação ao indivíduo, reunidos por um mesmo nome, mas que não mantém quase nada em comum, exceto o fato de que cada um representa uma interferência contra o direito do demandante de ser deixado em paz. Os quatro tipos de violação, segundo o autor, são[370]: (i) intrusão na solidão e reclusão de uma pessoa, ou nos seus assuntos pessoais (*intrusion*); (ii) revelação pública de fatos particulares embaraçosos sobre o demandante (*public disclosure of private facts*); (iii) publicidade que coloca uma pessoa sob falsa luz aos olhos públicos, ou seja, publicidade na qual o demandante é apresentado de modo

---

[365] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.16.

[366] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.16.

[367] William Lloyd Prosser (1898–1972) foi professor em algumas universidades americanas e é um dos doutrinadores de sua época na área do direito privado. Foi professor decano da Faculdade de Direito na Universidade da California Berkeley.

[368] Edward J. Bloustein (1925-1989), reconhecido doutrinador americano, em 1964, em resposta ao artigo de Prosser, propõe uma teoria geral da privacidade individual que reconciliará as vertentes divergentes do desenvolvimento jurídico, "que colocará as palhas de volta no palheiro". A necessidade desta teoria, segundo o autor à época, "é urgente". Segundo ele, "em primeiro lugar, a desordem nos casos e comentários ofende o cânone primário de toda ciência de que um único princípio geral de explicação deve ser preferido sobre um conjunto de regras discretas". (BLOUSTEIN, Edward. Privacy as an aspect of human dignity: an answer to dean prosser. **New York University Law Review** 39, 1964, p.156).

[369] PROSSER, William L. Privacy. **California Law Review**, v.48, n.3, ago.1960.

[370] PROSSER, William L. Privacy. **California Law Review**, v.48, n.3, ago.1960, p.389.

equivocado para o público (*false light in the public eye*); (iv) apropriação, para obter vantagem, do nome ou da imagem do demandante (*apropriation*).

Em 1964, o professor de Direito da Universidade de New York, Edward Bloustein, respondeu à proposição de William Lloyd Prosser, propondo uma teoria geral da privacidade individual que reconcilia todas as suas divergências. Segundo Edward Bloustein, a personalidade inviolável é o valor social protegido pela privacidade, pois inclui a dignidade individual e a integridade, a autonomia pessoal e a independência. Portanto, para o autor, a invasão da privacidade é uma violação à dignidade humana[371].

No mesmo ano, o jornalista Vance Packard questiona em seu *best seller* 'The naked society' como as mudanças trazidas pelas tecnologias estão transformando a vida dos indivíduos, a ponto de a privacidade estar rapidamente evaporando[372]. Nessa época, curiosamente, as tecnologias em pauta eram microfones e câmeras escondidos e o detector de mentiras do polígrafo.

Verifica-se, assim, que desde a década de 1960, passou-se a questionar sobre a possível morte da própria privacidade.

O professor da Columbia University, Allan Westin, esboçou uma profunda preocupação com a preservação da privacidade sob as novas pressões da tecnologia de vigilância com a publicação de sua obra, em 1968[373].

Antes ainda, em 1956, um juiz federal americano[374] caracterizou o estado da lei da privacidade, comparando-a a um palheiro em um furacão. E, desde então, seguiram-se diversas manifestações e discursos escatológicos sobre a destruição, a morte e o fim da privacidade. Segundo Daniel Solove:

> It is proclaimed inviolable but decried as detrimental, antisocial, and even pathological. Some claim that privacy is nearing extinction; others argue that the threat to privacy is illusory. It seems as though everybody is talking about "privacy," but it is not clear exactly what they are talking about. Americans care about privacy mainly in the abstract. Although polls indicate that people care deeply about privacy, people routinely give out their personal information and willingly reveal intimate details about their lives on the Internet[375].

---

[371] BLOUSTEIN, Edward. Privacy as an aspect of human dignity: an answer to dean prosser. **New York University Law Review** 39, 1964.

[372] BISHOP, Joseph. Book review: the naked society in the Yale Law Journal. **Yale Law School Legal Scholarship Repository**. v.74, p.194-199. Disponível em: <https://digitalcommons.law.yale.edu>. Acesso em: 04 set. 2018.

[373] WESTIN, Alan Furman. **Privacy and freedom**. New York: Atheneum, 1968.

[374] Biggs C. J. caso Ettore v. Philco Television Broadcasting Co, 229 F. 2d 481 (3d Cir. 1956).

[375] SOLOVE, Daniel J. **Understanding privacy**. Cambridge, London: Harvard University Press, 2008, p.5.Tradução livre: É proclamado inviolável, mas denunciado como prejudicial, anti-social e até patológico. Alguns afirmam que a privacidade está se aproximando da extinção; outros argumentam que a ameaça à

Em 2008, Fábio Ulhoa Coelho foi categórico: “a privacidade acabou”. Segundo ele, a disseminação dos meios tecnológicos de invasão da esfera privada de nossa vida seria de tal ordem que pouco ou nada poderiam fazer os legisladores e juízes ao redor do mundo. Para o autor, mesmo diante do fim da privacidade, talvez não fosse o caso de nutrir pessimismo, posto que um mundo sem privacidade poderia ser mais seguro e tolerante.[376]

Em que pesem as vozes contrárias, preferimos nos associar aos mais otimistas, que ao invés de apontarem para a morte da privacidade, descrevem um processo de sua inexorável reinvenção. Depois da definição histórica sobre ‘o direito de ser deixado em paz’, desenvolvida por Warren e Brandeis, ao longo do século XX, outras definições surgiram para responder a diferentes anseios. Na sociedade de dados, na qual nossas informações estão em incessante movimento, o direito de controlar o modo como outros utilizarão essas informações tornou-se inafastável, até mesmo porque a coleta e o tratamento desses dados poderão levar a uma discriminação ou a um estigma social. Assim, a privacidade deve ser considerada, hoje, também como “o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular”[377].

Na mesma linha, Rosen Jeffrey entende que o atual significado de privacidade esteja relacionado à capacidade de exercer controle sobre informações pessoais, pontuando, sabiamente, que as expectativas de privacidade podem variar diante de diferentes contextos, como a idade da pessoa:

---

privacidade é ilusória. Parece que todos estão falando de “privacidade”, mas não está claro exatamente do que estão falando. Os americanos se preocupam com privacidade principalmente no abstrato. Embora as pesquisas indiquem que as pessoas se importam profundamente com a privacidade, as pessoas normalmente revelam suas informações pessoais e revelam detalhes íntimos de suas vidas na internet.

[376] COELHO, Fábio Ulhoa. Sabe aquilo que chamávamos de privacidade? **Folha de S. Paulo**. Publicado em: 21 ago. 2008. Disponível em: <https://www1.folha.uol.com.br/fsp/opiniao/fz2108200808.htm>. Acesso em: 04 set. 2018: “Câmaras de vídeo estão espalhadas por estacionamentos, lojas, bancos, edifícios, ruas, por todos os lugares. Sofisticados apetrechos eletrônicos gravam conversas à distância, dispensando a implantação de microfones no ambiente monitorado. Telefonemas e mensagens transmitidas pela internet são interceptados sem dificuldade. Já se organizam gigantescos bancos de dados reunindo simplesmente todas as informações existentes sobre todos nós. Nem mesmo nossos pensamentos e desejos íntimos parecem estar a salvo. Está em fase de finalização para lançamento no mercado a Epoc, uma máquina que lê pensamentos. Ainda é um tanto rude e sua eficácia depende, às vezes, de movimentos “interpretativos” dos braços. Será inicialmente usada para entretenimento em jogos eletrônicos, mas, logo mais, virão o aperfeiçoamento e outros usos; nem meditando teremos sossego. A tecnologia acabou com a privacidade e vai acabar com o direito à privacidade. Por algum tempo, legisladores e juízes ainda vão fingir que o protegem, mas esse direito, como tantos outros, não resistirá ao cerco da tecnologia. O constitucionalista norte-americano Lawrence Lessig insiste, há quase duas décadas, que a lei não é mais feita pelos legisladores, e sim pelos programadores de informática. O *software* (“code”) é a lei. Ou, de modo mais geral, a tecnologia é a lei”.

[377] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.15.

> By privacy, then, I mean the ability to exercise control over personal information, and by personal information, I mean information over which I reasonably expect to exercise control. The legitimacy of my expectations might vary in different contexts[378].

Com o aumento do acesso a informações pessoais resultante de técnicas modernas e sofisticadas de processamento automatizado, os debates sobre privacidade foram alterados, segundo Spiros Simitis, de três maneiras: em primeiro lugar, as considerações de privacidade não surgem mais de problemas individuais específicos, mas expressam conflitos que afetam a todos. Em segundo lugar, a vigilância perdeu seu caráter excepcional e se tornou uma prática cada vez mais rotineira. Em terceiro lugar, as informações pessoais são cada vez mais usadas para impor padrões de comportamento. O processamento de informação está se desenvolvendo, portanto, como um elemento essencial das estratégias de manipulação de longo prazo destinadas a moldar e ajustar a conduta individual[379].

Em detida análise, verifica-se que o germe dessa transformação teve início com Alan Westin, o qual inovou ao definir privacidade como o direito de controlar o uso que outros fazem das informações referentes ao indivíduo[380]. Daí em diante, a privacidade vem, ainda, considerada como “tutela das escolhas de vida contra toda

---

[378] Tradução livre: Por privacidade, então, quero dizer a capacidade de exercer controle sobre as informações pessoais e, por informações pessoais, quero dizer informações sobre as quais eu razoavelmente espero exercer controle. A legitimidade das minhas expectativas pode variar em diferentes contextos. ROSEN, Jeffrey. The purpose of privacy: a response. **Georgetown Law Journal**, v.89, Disponível em: <https: //papers.ssrn.com/sol3/papers.cfm?abstract_id=283988>. Acesso em: 04 set.2018. Essa obra consiste na resposta formulada pelo autor a oito artigos escritos sobre o seu livro ‘The Unwanted Gaze’ [...] Published as part of a special symposium issue of the Georgetown Law Journal. The eight contributors to the symposium were Professors Anita Allen, Julie Cohen, Rosa Ehrenreich, Lawrence Lessig, Sanford Levinson, Robert Post, Jed Rubenfeld and Nadine Strossen. Rosen defends his argument that privacy protects against the dangers of being judged out of context, insisting that invasions of privacy can lead to social misinterpretations that constitute an injury distinct from injuries to dignity or autonomy. He expands on his claim that some of the indignities currently defined as gender discrimination under sexual harassment law are better conceived as invasions of privacy, and he explores the distinction between offenses against honor and offenses against dignity. Finally, he discusses the tensions between privacy and free speech, insisting that the most appropriate remedies for social misunderstanding are often social rather than legal. Tradução livre: Publicado como parte de uma edição especial do simpósio do Georgetown Law Journal. Os oito colaboradores do simpósio foram os professores Anita Allen, Julie Cohen, Rosa Ehrenreich, Lawrence Lessig, Sanford Levinson, Robert Post, Jed Rubenfeld e Nadine Strossen. Rosen defende seu argumento de que a privacidade protege contra os perigos de ser julgado fora de contexto, insistindo que invasões de privacidade podem levar a interpretações sociais equivocadas que constituem uma lesão distinta de danos à dignidade ou à autonomia. Ele expande sua alegação de que algumas das indignidades atualmente definidas como discriminação de gênero sob a lei do assédio sexual são melhor concebidas como invasões de privacidade, e ele explora a distinção entre ofensas contra a honra e ofensas contra a dignidade. Finalmente, ele discute as tensões entre privacidade e liberdade de expressão, insistindo que os remédios mais apropriados para o mal-entendido social são freqüentemente sociais, e não legais.

[379] SIMITIS, Spiros. Reviewing privacy in an information society. **University of Pensilvania Law Review**, v.135, p.707-746. Pensilvania: University of Pensilvania, 1987. Disponível em: <https://scholarship.law.upenn.edu>. Acesso em: 27 set. 2018, p. 709-710.

[380] WESTIN, Allan. **Privacy and freedom**. New York: Atheneum, 1970.

forma de controle público e de estigma social[381]" e como "reivindicação das limitações que impedem a qualquer um de ser simplificado, objetivado e valutado fora de contexto"[382].

Na travessia de praticamente um século de distanciamento, parte-se da proteção do indivíduo garantindo-lhe controle contra o acesso à sua vida privada, em direção a uma privacidade de controle sobre os dados pessoais. Na lição de Erick Lucena Campos Peixoto e Marcos Ehrhardt Júnior,

> A privacidade, nos moldes em que é conhecida hoje, desenvolve-se a partir do século XIX nos Estados Unidos como o "direito de ser deixado em paz", que fundamentava a proteção do indivíduo, garantindo que este tivesse o controle de quem tem acesso ou não à sua vida privada e do modo como os outros poderiam influenciar em suas decisões existenciais. Junto dessa privacidade decisional, a privacidade espacial compõe o modo tradicional de enxergar a privacidade. Com os avanços tecnológicos do pós-guerra do século XX, é acrescentada à privacidade uma dimensão informacional, voltada à proteção de dados pessoais[383].

A privacidade, antes compreendida, prioritariamente, como o direito negativo de ser deixado em paz, passa a significar também o controle dos dados pessoais pelo próprio indivíduo, que decide quando, como e onde os seus dados pessoais devem circular[384].

Observa-se um processo de reinvenção da privacidade. Com o passar dos anos, verificou-se, de fato, a insuficiência da proteção concebida por Warren e Brandeis. O viés da privacidade evoluiu para o "direito à autodeterminação informativa", o qual visa conceder um real poder sobre as próprias informações e dados do indivíduo. Abordaremos essa doutrina mais adiante.

Para Stefano Rodotá, percebe-se aqui um caminhar na evolução do conceito originário de privacidade (*the right to be let alone*) para o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada[385]. Por esse ângulo, o direito à privacidade também conquista a qualidade de instrumento fundamental contra a discriminação, e a favor da

---

[381] FRIEDMAN, Lawrence M. **The republic of choicem law, authority and culture**. Cambridge (Mass.): Harvard University Press, 1990, p.184.

[382] ROSEN, Jeffrey. The purpose of privacy: a response. **Georgetown Law Journal**, v.89, Disponível em: <https://papers.ssrn.com>. Acesso em: 04 set. 2018, p.20.

[383] PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. In: **Revista Brasileira de Direito Civil** – RBDCivil | Belo Horizonte, v.16, p.35-56, abr.-jun. 2018, p.35.

[384] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.36.

[385] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.7.

igualdade e da liberdade, atribuindo-lhe dimensões coletivas da privacidade. Nota-se, com efeito, que a evocação da privacidade supera o tradicional quadro individualista e se alarga para uma dimensão coletiva.

O século XX é o período percorrido para essa evolução que separa a privacidade, de um lado, da proteção de dados, de outro, como se fossem duas faces da mesma moeda. O direito à privacidade transforma-se para dar espaço à construção da disciplina da proteção de dados pessoais, de forma a se adaptar aos desafios impostos pela tecnologia. “Assim, a proteção de dados pessoais pode ser compreendida como uma dimensão do direito à privacidade, que, por consequência, partilha dos mesmos fundamentos: a tutela da personalidade e da dignidade do indivíduo”[386].

Na análise de Stefano Rodotà, enquanto a tutela à privacidade é estática e negativa, a proteção de dados é dinâmica:

> [...] no direito ao respeito à vida privada e familiar manifesta-se, sobretudo, o momento individualista e o poder exaure-se substancialmente na exclusão da interferência de outrem; a tutela, portanto, é estática e negativa. Já a proteção dos dados pessoais, ao contrário, fixa regras sobre a modalidade de tratamento dos dados e concretiza-se em poderes de intervenção; a tutela é dinâmica, segue os dados em sua circulação[387].

A proteção de dados adquire um âmbito mais abrangente em relação à proteção da privacidade. Isso porque passa a ser compreendida como um fenômeno coletivo, na medida em que os danos causados pelo processamento impróprio de dados pessoais são, por natureza, difusos, exigindo igualmente uma tutela jurídica coletiva.

Para Danilo Doneda, o direito de proteção de dados, que nasceu sob a égide da privacidade e hoje se sofisticou, assumindo características próprias, alcança não somente a privacidade, mas também a pessoa que deve ser tutelada contra o controle indevido e contra a discriminação, isto é, em aspectos fundamentais de sua própria liberdade pessoal. E não é mais a pessoa humana, individualmente, a ser a única atingida – um antigo paradigma do direito à privacidade – porém, inteiras classes e grupos sociais[388].

---

[386] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.35.
[387] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.18.
[388] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.3.

Sob outro olhar, é possível afirmar que reinventar a proteção de dados constitui, também, um processo indispensável para impedir que novas sociedades se tornem sociedades de controle, vigilância e seleção social[389].

Não é apenas a revolução tecnológica, por si só, que serviu de condição para a reinvenção da privacidade, mas também as ameaças do Estado contra os cidadãos, ocorridas a partir da segunda metade do século passado, perseguidas pela distopia orwelliana.

Foi o Estado a se perceber, em primeiro lugar, capaz de utilizar largamente informações pessoais. Conforme observa Danilo Doneda, "os motivos são razoavelmente claros: basta a constatação de que um pressuposto da administração pública eficiente é o conhecimento tão acurado e profundo quanto possível da população"[390].

Segundo Laura Schertel Mendes – para quem graças à transformação da função do Estado, no decorrer do século XX, aliada à revolução tecnológica, houve a contribuição que sustentou a mudança quanto ao sentido e o alcance do direito à privacidade – "de um direito com uma dimensão estritamente negativa e com uma conotação quase egoísta, passou a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático"[391].

Assim, dois entes se colocam em torno das transformações ocorridas em relação ao direito da privacidade: o Estado e o mercado, isto é, o controle e a eficiência[392].

Com o progressivo avanço da sociedade moderna, que resultou na capacidade ilimitada de compilar dados através de computadores e sistemas que conjuntamente permitem estabelecer correlações dentre as informações obtidas, foi se calando, pouco a pouco, na consciência da cidadania digital, desde aproximadamente os anos 1960, o sentimento de ameaça e prejuízo aos recantos da esfera pessoal[393], advindos tanto por parte do Estado como do mercado, que não

---

[389] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.21.
[390] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.13.
[391] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.29.
[392] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.13-24.
[393] CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.52.

eram cobertos adequamente pelas primeiras formulações que constituíram o direito à privacidade.

A proteção à privacidade se desdobra na proteção de dados pessoais. Ambas as dimensões desse direito compreendem os mesmos pressupostos ontológicos[394]. De um olhar aos interesses do indivíduo, a matéria passa a abranger dimensão coletiva, ao repousar atenção que vai além, alcançando o interesse desse indivíduo enquanto inserido em um determinado grupo social.

3.2 A proteção de dados e as vulnerabilidades trazidas pelas novas tecnologias

Na sociedade contemporânea, estamos continuamente sendo “etiquetados”. O controle sobre as informações a respeito de si e o direito de saber quem utiliza nossos dados significa adquirir, concretamente, um poder sobre si mesmo[395]. E esse é um valor que não pode ser tolhido do cidadão na atualidade, após as conquistas alcançadas nas últimas décadas. Discute-se hoje, porém, meios efetivos de concretizar esse direito já reconhecido ao indivíduo.

A aparição do direito fundamental à proteção de dados, assim definido como um direito do século XXI[396], tem como núcleo matriz de desenvolvimento as novas tecnologias, “nas quais o incessante processo de desenvolvimento protagonizado pela humanidade culmina em um acontecimento de dimensões colossais: a aparição da internet”[397].

A invasão de nosso entorno pessoal é tanto mais agressiva quanto maior é a facilidade de coleta dos dados pessoais, seu armazenamento e posterior tratamento.

---

[394] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.27.

[395] RODOTÀ, Stefano. Nessuna censura sulla privacy. **La Repubblica**, Publicado em: 13 maio 1997. Disponível em: <http://ricerca.repubblica.it/>. Acesso em: 03 set. 2018. “Nasce nel secolo passato negli Stati Uniti e subito si presenta come un diritto tipico dell' età dell' oro della borghesia. Ma in Italia arriva con lo Statuto dei lavoratori, si proietta al di là della richiesta d' essere "lasciato solo" e diviene uno strumento per opporsi alle discriminazioni. Ora dilaga, in tutta la società: dal "diritto all' autodeterminazione informativa", dalla possibilità di controllare la circolazione delle proprie informazioni dipende ormai il modo stesso d' essere cittadini”.

[396] Não obstante seja uma realidade tangível desde meados da segunda metade do século XX. Sobre o assunto: “Podemos estruturar os direitos fundamentais entre direitos de primeira geração, relativos a direitos civis e políticos; direitos de segunda geração, que correspondem aos direitos sociais, econômicos e culturais; e, por último, uma terceira geração de direitos, integrada pelos direitos definidos como direitos de solidariedade. Fala-se, ainda, de uma quarta geração de direitos, que parte da doutrina referente aos direitos de biotecnologia e das telecomunicações. Esses direitos também são chamados de direitos do século XXI”. (CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.53).

[397] CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.54.

Evidentemente que as novas tecnologias da informação e comunicação tornaram mais simples o que antes era uma tarefa mais trabalhosa.

As fronteiras da privacidade eram definidas pelos elementos do tempo e do espaço. O primeiro procurava, com seu transcurso, que se esvanecessem as memórias de acontecimentos passados, impedindo, assim, a configuração de uma história linear, ininterrupta e inesquecível sobre a pessoa. O segundo, a distância imposta até pouco tempo, impedia que tivéssemos conhecimento dos fatos protoganizados por outras pessoas em lugar distante. O tempo e o espaço exerciam, assim, um papel de salvaguarda da privacidade da pessoa. Porém, tanto um como outro desapareceram, haja vista que as modernas técnicas de comunicação permitem aproximar lugares e armazenar uma infinidade de informações sobre a pessoa, as quais podem ser resgatadas em segundos.

Nessa vereda, na exposição de motivos da lei espanhola n.5/1992, de 29 de outubro, é apresentado um cenário no qual os elementos tempo e espaço foram esvanecidos:

> Los más diversos datos sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado “dinero plástico”, sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, por poner sólo algunos ejemplos- relativos a las personas podrían ser, así, compilados y obtenidos sin dificultar. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él autorice. Aún más: El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos.

A sociedade atual exige a redefinição de conceitos, atitudes, habilidades da administração pública. A informática, diferente de outros meios de comunicação que a antecederam, oferece possibilidades de se armazenar e tratar informações que possibilitam novos tipos de controles. Segundo Davara Rodríguez:

> La informática, con las posibilidades que oferece de almacenamiento y tratamento de la documentación y de recuperación de la información registrada em soportes magnéticos, permite controlar esa información y puede llegar a convertirse en un instrumento de presión y controlo social[398].

[398] DAVARA RODRÍGUEZ, Miguel Angel. **La proteccion de datos en europa** – princípios, derechos y procedimento. Madri/Espanha: Asnef Equifax, 1998, p.16.

As novas tecnologias de rede e de telecomunicação ampliaram a capacidade e a velocidade de transmissão de dados. Os bancos de dados não são mais passíveis, em regra, de serem localizados fisicamente, pois estão armazenados em redes e não mais em uma central identificável de processamento, podendo ser transferidos em segundos.

O desenvolvimento dos meios tecnológicos e o crescente recurso a meios eletrônicos que deixam *pegadas eletrônicas* (movimentação de contas bancárias, comércio eletrônico, postagens eletrônicas, utilização da telefonia móvel, visita de sites na internet, meios de videovigilância eletrônica, etc.) tornam cada vez mais importantes as garantias contra o tratamento e a utilização abusiva de dados pessoais informatizados[399].

Assim, sem perder de vista os inúmeros benefícios trazidos pela internet como o fomento à cultura e à educação, a profileração de informações úteis à sociedade, não se pode deixar de lado que os incômodos acompanham os cômodos e, nessa toada, a nova tecnologia submete o indivíduo a novos controles:

> Em definitiva, este nuevo médio, al tiempo que proporciona uma herramienta verdadeiramente eficaz para la difusión de la información y los conocimientos, y em consecuencia, para el ejercicio de la libertad ideológica reconocida em calidad de Derecho fundamental em todas las Constituciones modernas, somete al ser humano a la inquietante situación de sentirse observado por el ojo-que-todo-lo-ve de Orwell, em 1984, o bajo la asfixiante dirección de Huxley, en un mundo feliz.[400]

Não à toa, durante o século XX, foi possível acompanhar as diversas inserções legislativas, inclusive em âmbito constitucional, de preocupações relacionadas à privacidade, conforme se verá mais detalhadamente adiante.

Ao passo que adquire um caráter positivo e seja reconhecido, especialmente, no âmbito internacional, o direito à privacidade transformou-se para fazer emergir à dimensão de proteção de dados pessoais, à medida que surgiram novos desafios ao ordenamento jurídico a partir do tratamento informatizado dos dados[401].

Essas novas tecnologias foram comprimindo os espaços individuais das pessoas, corroendo “o sentido da privacidade como esfera doméstica, junto com o

---

[399] CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. **Constituição da República Portuguesa Anotada**. v.1. São Paulo: Editora RT; Coimbra, PT: Coimbra, 2007, p.550.
[400] CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.57.
[401] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.29; DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

temor da invasão da privacidade pela disseminação pública de detalhes relativos à vida privada de uma pessoa"[402].

A partir daqui, visando personalizar a produção e o *marketing* e diminuir os riscos dos negócios, "o setor privado armazena e processa grande quantidade de informações quase cotidiana dos consumidores e de seus hábitos de consumo[403]", ao custo de riscos à violação da personalidade do indivíduo.

É o que vivemos hoje com o custo por nós pago pela utilização de soluções de aplicações tecnológicas, como *Google* e *WhatsApp,* que se impregnaram na vida cotidiana, a ponto de causar certa paranoia em algumas pessoas quando, por algum motivo, deixam de ter acesso às ferramentas. O custo referido não diz respeito a valores diretamente monetários, mas à imensidão de dados pessoais colhidos pelos aplicativos. Atualmente, o direito busca regular essas novas situações de (des)controle.

De outro lado, há aqueles que argumentam que os direitos afetos à privacidade, no qual também estão inseridos os de proteção de dados pessoais, deveria ceder espaço a medidas estatais em prol da segurança.

Segundo Stefano Rodotà, a receita 'menos privacidade, mais segurança' é falsa. Nesse sentido, o autor recorre à comparação do homem de vidro, de concepção nazista, cuja ideia é totalitária porque se baseia na pretensão do Estado de conhecer tudo, até os aspectos mais íntimos da vida das pessoas, colocando como suspeito todo aquele que quiser proteger sua vida privada, sob o amparo de que 'quem não deve, não teme, e nada tem a esconder'.

Para esse autor italiano, na sociedade de vigilância, os indivíduos são assediados por computadores, espiados por olhos furtivos e filmados por telecâmeras invisíveis. Os cidadãos correm o risco de parecer homens de vidro: uma sociedade que a informática e a telemática estão tornando totalmente transparente[404].

Stefano Rodotá confirma que há uma progressiva extensão das formas de controle social, sempre apoiadas em discursos de segurança. Com isso, a vigilância passa a ser a regra. Com o aumento de incidentes terroristas ao redor do mundo,

---

[402] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.78.
[403] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.22.
[404] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.8.

esse discurso tem encontrado cada vez mais adeptos. Nos Estados Unidos, desde o 11 de setembro e da aprovação do *Patrioct Act*, a privacidade e a proteção de dados têm sido escanteadas em prol da segurança. Essa equação é especialmente desafiadora nos Estados Unidos, em cujo país não há, até esse momento, uma lei geral de proteção da privacidade. Conforme reflete Stefano Rodotà:

> Depois do 11 de setembro, a privacidade na era do terror parece estar condenada. A privacidade, além de não ser mais vista como um direito fundamental é, de fato, frequentemente considerada um obstáculo à segurança, sendo superada por legislações de emergência[405].

Esse movimento tem sido sentido cada vez mais na Europa[406], berço dos grandes avanços legislativos na área da proteção de dados. Os tristes casos de terrorismo têm, obviamente, afetado a população e colocado os Estados em uma situação de pressão popular para solucionar o problema. O grande desafio é ser efetivo no combate sem comprometer os direitos do cidadão, mas essa fórmula é bastante difícil de ser alcançada. É como um cobertor curto em dia de frio: ou cobre o ombro ou cobre os pés.

Além disso, não se pode deixar de dirigir o olhar para o uso massivo das redes sociais. Verifica-se como as relações entre vigilância e exposição estreitam-se cada vez mais. A vida do espetáculo público coloca diante de nós novas indagações, que vão desde a necessidade de tanta exposição, como de que forma o direito pode proteger os direitos fundamentais dos indivíduos na atualidade.

Vivemos a geração dos *Youtubers*. Centenas de vídeos caseiros são feitos diariamente, inclusive por crianças, que desejam se expor ao mundo e, muitas vezes o fazem na expectativa de ganhar dinheiro com os conteúdos divulgados e enriquecer com esse espetáculo público. Igualmente, a audiência televisiva a programas do estilo *reality show*[407] demonstra o interesse da sociedade por esse

---

[405] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.14.

[406] Por ocasião do *Patrioct Act* americano a Europa já decidira colaborar com a transferência para os EUA de dados dos passageiros de linhas aéreas e sobre a retenção de dados quanto às comunicações eletrônicas.

[407] Josh Harris who, shocked by Peter Weir's film The Truman Show (1998) created Quiet (1999) and We Live in Public (2000), two new episodes of personal overexposure focusing on online sharing. In Quiet, a group of volunteers were locked together in a large New York basement adapted as a living space, where all their actions were recorded and shared live over the Internet. In We Live in Public, Harris and his partner shared their daily life from their apartment on-line, adding the possibility that online users could post any kind of comment in a chat. Both experiments ended earlier than expected, and both ended badly, but the seed had taken root. (The first Big Brother was launched on Dutch television the same year as Quiet): (BAIGORRI, Laura. **CTRL + [SELF]**: intimacy, extimacy & control in the age of the overexposure of self. Disponível em: <https://htmlles.net/wp-content/uploads/2016/11/Curatorial-text_Baigorri_EN.pdf>. Acesso em: 10 ago. 2018). Tradução livre: Josh Harris que, chocado com o filme de Peter Weir, The Truman Show (1998), criou Quiet (1999) e We Live in Public (2000), dois novos episódios de superexposição pessoal com foco no compartilhamento online. Em Quiet, um

tipo de exposição. São programas que usam a vigilância e o confinamento para entreter o público.

Segundo Lucia Santaella, embora os conceitos psicanalíticos do prazer, do exibicionismo e do *voyeurismo* sejam, de fato, chaves para o entendimento de fenômenos do tipo *reality show*, as redes sociais que emergiram com a web 2.0 estão anunciando processos novos relativos à privacidade que reclamam por modos de ver mais perscrutantes de sua especificidade[408].

Fato é que a *proteção* e a *projeção* de si estão tão intimamente ligadas e confundidas pelo próprio ente por trás dessas *aspirações* e *aparições*, que colocam o assunto sob auspícios de complexidade.

A *extimidade*[409], expressão cunhada por Jacques Lacan em 1958, explica a dinâmica das redes sociais: a exposição de segredos em público. O atual significado de *extimidade*, porém, como uma tendência das pessoas de revelarem sua intimidade, foi criada pelo psiquiatra e psicanalista Serge Tisseron[410].

Segundo Zygmunt Bauman, a 'sociedade confessionário' marcou o triunfo definitivo daquela invenção esquisitamente moderna que é a privacidade:

> Os adolescentes equipados com confessionários eletrônicos portáteis nada mais são do que aprendizes em formação e formados na arte de viver em uma sociedade-confessionário, uma sociedade notória por ter apagado o

---

grupo de voluntários estava trancado em um grande porão de Nova York, adaptado como um espaço vivo, onde todas as suas ações eram registradas e compartilhadas ao vivo pela Internet. Em We Live in Public, Harris e seu parceiro compartilhavam o cotidiano de seu apartamento on-line, adicionando a possibilidade de que os usuários on-line pudessem postar qualquer tipo de comentário em um bate-papo. Ambos os experimentos terminaram antes do esperado, e ambos terminaram mal, mas a semente criou raízes. (O primeiro Big Brother foi lançado na televisão holandesa no mesmo ano que Quiet).

[408] SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013, p.85.

[409] Across the mirror we find extimacy (extimité), a neologism Jacques Lacan formulated in his seminar The Ethics of Psychoanalysis (1958) to problematize that which is at once interior and exterior, interiority and exteriority; extimacy is not something opposed to intimacy but its reflection, because the "extime" is, essentially, the most intimate (of course, this is a paradoxical formulation characteristic of psychoanalytic discourse). (BAIGORRI, Laura. **CTRL + [SELF]**: intimacy, extimacy & control in the age of the overexposure of self. Disponível em: <https://htmlles.net/wp-content/uploads/2016/11/Curatorial-text_Baigorri_EN.pdf>. Acesso em: 10 ago. 2018). Tradução livre: Do outro lado do espelho, encontramos a extimidade (extimité), um neologismo que Jacques Lacan formulou em seu seminário A Ética da Psicanálise (1958), para problematizar aquilo que é ao mesmo tempo interior e exterior, interioridade e exterioridade; a extimidade não é algo que se opõe à intimidade, mas à sua reflexão, porque o "tempo" é, essencialmente, o mais íntimo (é claro que essa é uma formulação paradoxal característica do discurso psicanalítico).

[410] The particularity of Tisseron's formulation is that the subject does not expose herself with the aim to share her experiences, but rather uses other subjects as a mirror of self-affirmation. Tisseron poses this reflection based on the study of a "Big Brother" group-type of French television, however, it quickly applied to the social media environment where it all seems to make sense. (BAIGORRI, Laura. **CTRL + [SELF]**: intimacy, extimacy & control in the age of the overexposure of self. Disponível em: <https://htmlles.net/wp-content/uploads/2016/11/Curatorial-text_Baigorri_EN.pdf>. Acesso em: 10 ago. 2018). Tradução livre: A particularidade da formulação de Tisseron é que o sujeito não se expõe com o objetivo de compartilhar suas experiências, mas usa outros sujeitos como um espelho de autoafirmação. Tisseron propõe essa reflexão com base no estudo de um grupo de televisão francesa do tipo "Big Brother", no entanto, ela se aplica rapidamente ao ambiente de mídia social, onde tudo parece fazer sentido.

> limite que tempos atrás separava público e privado, por ter feito da exposição pública do privado uma virtude pública e um dever, e por ter retirado da comunicação pública qualquer coisa que resista a se deixar reduzir a confidências privadas, junto com aqueles que se recusam a fazer isso. [...] Ser membro da sociedade dos consumidores é uma árdua tarefa, um percurso de subida que não termina nunca. O temor de não conseguir se conformar foi suplantado pelo temor da inadequação, mas nem por isso se tornou menos atormentado. Os mercados dos consumidores estão ávidos por capitalizar esse temor, e as indústrias que desenfornam bens de consumo disputam o status de guias/ajudantes mais confiáveis para os seus clientes, submetidos ao esforço incessante de estarem à altura da tarefa.[411]

Sob outro ângulo de análise, na perspectiva de quem controla os dados, vale analisar a compilação publicada pelo jornal 'The New York Times', feita por seu editor gráfico Chinoy, de algumas patentes – depositadas e algumas já deferidas – cujos pedidos revelam invenções (ou potenciais invenções para aquelas ainda não deferidas) que colocam em perspectiva os limites de atuação de empresas de internet na coleta de dados pessoais[412]. Em um dos casos, as câmeras voltadas para frente dos dispositivos são usadas para analisar as expressões e detectar se a pessoa está entediada ou surpresa com o que vê no *feed* da rede social. Por meio de outras técnicas, sistemas são aplicados para adivinhar se a pessoa vai se casar em breve, prever seu *status* socioeconômico e acompanhar se o indivíduo está dormindo, dentre outras técnicas invasivas.

Ao ser confrontado sobre o polêmico conteúdo desses pedidos de patentes, o Facebook, por meio de seu vice-presidente, vice-conselheiro geral e responsável pela área de propriedade intelectual da empresa, justificou que a maioria das

---

[411] BAUMAN, Zygmunt. **"Extimidade"**: o fim da intimidade. Tradução de Moisés Sbardelotto. Publicado em 9 abr. 2011. Disponível em: <http://www.ihu.unisinos.br/>. Acesso em: 24 ago. 2018: "o segredo é, por definição, aquela parte do conhecimento cujo compartilhamento com outros é rejeitado ou proibido e/ou estritamente controlado. O segredo, por assim dizer, caracteriza e contradistingue os limites da privacidade, sendo esta última a esfera destinada a ser própria, o território da própria soberania indivisa, dentro do qual tem-se o poder total e indivisível de decidir "o que sou e quem sou" a partir da qual podem ser lançadas e relançadas as campanhas para fazer com que sejam reconhecidas e respeitadas as próprias decisões e mantê-las como tais. Em uma surpreendente inversão com relação aos hábitos dos nossos antepassados, porém, perdemos a coragem, a energia e principalmente a vontade de persistir na defesa desses direitos, daqueles insubstituíveis elementos constitutivos da autonomia individual. Aquilo que nos assusta hoje não é tanto a possibilidade da traição ou da violação da privacidade, mas sim o seu oposto, isto é, a perspectiva de que todas as vias de saída possam ser bloqueadas. A área de privacidade se transforma assim em um lugar de aprisionamento, e o proprietário do espaço privado é condenado a cozinhar em seu próprio caldo, constrangido em uma condição marcada pela ausência de ávidos ouvidores, ansiosos por extrair e arrancar os nossos segredos dos bastiões da privacidade, de jogá-los como alimento ao público, de fazer deles uma propriedade compartilhada por todos e que todos desejam compartilhar. Pelo que parece, não sentimos mais alegria ao ter segredos, a menos que se trate daquele gênero de segredos capaz de exaltar o nosso ego, atraindo a atenção dos pesquisadores e dos autores dos talk-shows televisivos, das primeiras páginas dos tablóides e das capas das revistas de papel envernizado [...].

[412] CHINOY, Sahil. What 7 **Creepy patentes reveal about Facebook**. Publicado em: 21 jun. 2018. Disponível em:<https://www.nytimes.com/interactive/2018/06/21/opinion/sunday/facebook-patents-privacy.html>.Acesso em: 05 set. 2018.

tecnologias descritas nos pedidos de patente não eram utilizados[413]. Sobre o assunto, não é demais lembrar que o próprio Mark Zuckerberg tem por hábito bloquear com fita adesiva a *webcam* e o microfone do seu Macbook[414]. Fica a dúvida; ou eis a explicação.

Passamos a analisar parte desses pedidos de patente com mais detalhes.

O pedido de patente U.S. Patent Application n.14/295, 543, feito pelo Facebook, analisa se o indivíduo está em um relacionamento romântico, usando informações como quantas vezes visitou a página de outro usuário, o número de pessoas na sua foto de perfil e a porcentagem de seus amigos de um sexo diferente[415]. Outra patente, da mesma empresa (U.S. Patent n.9,740,752), propõe usar posts e mensagens para inferir traços de personalidade. Por meio dessa análise, descreve o quanto o indivíduo é extrovertido, sua abertura social ou estabilidade emocional, usando essas características para selecionar notícias ou anúncios e direcioná-las ao indivíduo[416]. Outra patente (U.S. Patent Application n. 12/839,350) revela como o Facebook prevê o futuro dos internautas, pela análise de posts e mensagens, além das transações e localização do cartão de crédito, para prever quando pode ocorrer um grande evento da vida, como nascimento, morte ou formatura[417].

O uso de geolocalização é a chave para várias técnicas de segmentação de dados, a exemplo da patente (U.S. Patent n.9,369,983) cuja invenção se propõe a correlacionar a localização de determinado telefone com as localizações dos telefones de amigos da rede para deduzir com quem o indivíduo se socializa com mais frequência. Essa técnica também tem por objetivo monitorar quando o telefone está parado para verificar por quantas horas determinada pessoa costuma dormir[418].

---

[413] Facebook has said repeatedly that its patent applications should not be taken as indications of future product plans. “Most of the technology outlined in these patents has not been included in any of our products, and never will be,” Allen Lo, a Facebook vice president and deputy general counsel, and the company’s head of intellectual property, said in an email. Tradução livre: O Facebook afirmou repetidamente que seus pedidos de patente não devem ser considerados como indicações de planos futuros de produtos. "A maior parte da tecnologia descrita nestas patentes não foi incluída em nenhum de nossos produtos, e nunca será", disse Allen Lo, vice-presidente do Facebook e vice-conselheiro geral, e chefe de propriedade intelectual da empresa, em um e-mail.

[414] A foto largamente divulgada em 21-06-2016 na imprensa nacional e internacional, de Mark Zuckerberg comemorando o crescimento do Instagram, que atingira 500 milhões de usuários, e em cuja imagem foi possível constatar que o criador do Facebook bloqueava a webcam e o microfone do seu Macbook com pedações de fita adesiva.

[415] Disponível em: <https://patents.google.com/patent/US20150356180A1/en>. Acesso em: 29 nov. 2018.

[416] Disponível em: <https://patents.google.com/patent/US9740752B2/en>. Acesso em: 29 nov. 2018.

[417] Disponível em: <https://patents.google.com/patent/US20120016817A1/en>. Acesso em: 27 nov. 2018.

[418] Disponível em: <https://patents.google.com/patent/US9369983B2/en>. Acesso em: 27 nov. 2018.

Também com base em dados de geolocalização é o pedido de patente que visa acompanhar a rotina do indivíduo. Segundo descrição do pedido, o Facebook pretende monopolizar a técnica de usar a localização do telefone no meio da noite para checar onde mora o indivíduo[419].

São várias, portanto, as técnicas, que se tornam públicas, em razão da publicação dos pedidos de patentes, e que demonstram o nível de ameaça aos dados pessoais, incluindo até mesmo o lançamento de brinquedos, como o Teddy Bear de patente do Google[420], e meios de controle em ambiente de trabalho, tal qual a pulseira objeto de pedido de patente da Amazon, que revela o que os funcionários estão fazendo durante o expediente de trabalho[421].

Sem dúvida, as redes sociais são solos férteis para a captura de dados. Diante de brincadeiras aparentemente inofensivas, como “veja como seria seu rosto se você fosse do sexo oposto” etc., às quais os usuários aderem com facilidade, são capturados milhares de dados individuais.

Nem mesmo após o escândalo Cambridge Analytica[422], o Facebook deixou de ocupar os jornais como responsável por novas violações de privacidade. Em 4 de

---

[419] Disponível em: <https://patents.google.com/patent/US20160316341A1/en>. Acesso em: 27 nov. 2018.

[420] Conforme descritivo da patente (Disponível em: <https://patents.google.com/patent/US20150138333A1/>: an anthropomorphic device, perhaps in the form factor of a doll or toy, may be configured to control one or more media devices. Upon reception or a detection of a social cue, such as movement and/or a spoken word or phrase, the anthropomorphic device may aim its gaze at the source of the social cue. In response to receiving a voice command, the anthropomorphic device may interpret the voice command and map it to a media device command. Then, the anthropomorphic device may transmit the media device command to a media device, instructing the media device to change state. (Disponível em: <https://patents.google.com/patent/US20150138333A1/en>. Acesso em: 29 nov. 2018). Tradução livre: Um dispositivo antropomórfico, talvez no fator de forma de um boneco ou brinquedo, pode ser configurado para controlar um ou mais dispositivos de mídia. Na recepção ou na detecção de uma sugestão social, como movimento e/ou palavra falada ou frase, o dispositivo antropomórfico pode apontar seu olhar para a fonte da sugestão social. Em resposta ao recebimento de um comando de voz, o dispositivo antropomórfico pode interpretar o comando de voz e mapeá-lo para um comando do dispositivo de mídia. Em seguida, o dispositivo antropomórfico pode transmitir o comando do dispositivo de mídia para um dispositivo de mídia, instruindo o dispositivo de mídia a mudar de estado.

[421] US Patent n.0278051. Detalhes em: YEGINSU, Ceylan. If workers slack off, the wristband will know. (and Amazon has a patent for It.). **The New York Times**, 01 fev. 2018. Disponível em: <https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html>. Acesso em: 02 nov. 2018.

[422] A empresa britânica Cambridge Analytica usou testes de personalidade e curtidas no Facebook para coletar dados de usuários do Facebook em 2014. Essas informações revelaram o perfil psicológico completo de 87 milhões de pessoas que estão na rede social e passaram a receber propaganda eleitoral altamente personalizada. Com esses dados, a Cambridge agiu para influenciar nos resultados da campanha presidencial dos EUA em 2016, que elegeu Donald Trump, e do Brexit, o plebiscito do ano passado que levou o Reino Unido a deixar a União Europeia. O Brasil também está no meio, com 443.117 usuários atingidos. O escândalo explodiu em 17 de março de 2018, depois que um ex-funcionário da Cambridge Analytica, chamado Christopher Wylie, revelou que a consultoria pegava dados das pessoas que fizeram o teste e também de seus amigos sem consentimento. Mark Zuckerberg, chefe do Facebook (e do Instagram e do WhatsApp, vale dizer) vem tentando dar explicações, admitiu que errou e tomou algumas providências, mas muitas perguntas ficaram no ar. Em sua turnê de desculpas, o empresário depôs ao Senado e ao Congresso dos Estados Unidos. Ao Senado, Zuckerberg pediu desculpas e voltou a assumir os erros que ele e sua empresa cometeram, enquanto ao Congresso ele afirmou ter sido uma das vítimas dos vazamentos de dados feitos pela Cambridge Analytica. Em maio, Zuckerberg falou ao Parlamento Europeu. Em meio a mais desculpas, explicou a postura da rede social

junho de 2018, o Facebook, ao lado da Apple, Amazon, BlackBerry, Microsoft e Samsung foram alvo de nova denúncia, posto que teriam existido diversos acordos, ao longo da última década, com ao menos 60 fabricantes de smartphone, tablets e dispositivos móveis que permitem acessar dados pessoais de milhares de usuários sem o consentimento dos clientes. O jornal 'The New York Times' apurou que a maior parte destes acordos de compartilhamento de dados pessoais ainda estaria em vigor e por meio deles, o Facebook poderia estender seu raio de ação, deixando os fabricantes livres para oferecer e difundir aos próprios clientes alguns dos seus serviços mais populares. Em troca, o Facebook teria permitido que empresas como Apple e Samsung acessassem informações pessoais dos usuários da rede e de seus "amigos" na plataforma social, inclusive em casos de pessoas que se dizem convencidas de que negaram o compartilhamento dos próprios dados[423].

O Facebook é investigado em vários países ao redor do mundo por violações à privacidade. Na Alemanha, Andreas Mundt, presidente do Federal Cartel Office, oficiou a empresa de rede social, com uma série de perguntas, pedindo esclarecimentos sobre o abuso de seu domínio no mercado ao reunir dados sobre pessoas sem o consentimento delas[424].

Em 10 e 11 de abril de 2018, Mark Zuckerberg compareceu ao Congresso norte-americano para esclarecer o caso do abuso de dados da Cambridge Analytica, dentre outros assuntos polêmicos[425].

Em agosto de 2016, o serviço de mensagens instantâneas WhatsApp anunciou que começaria a compartilhar algumas informações *online* de seus usuários com o Facebook, cuja empresa pertence ao mesmo grupo econômico.

---

sobre supostamente diminuir o alcance ou bloquear conteúdos de páginas de direita. "Não queremos estar na posição do Facebook dizer o que é verdade ou falso. Por isso trabalhamos com checadores terceiros", argumentou. (UOL NOTÍCIAS. **O que sabemos do escândalo do Facebook e por que você deve se preocupar**. Publicado em: 21 mar.2018. Disponível em: <https://tecnologia.uol.com.br/listas/o-que-sabemos-do-escandalo-do-facebook-e-por-que-voce-deve-se-preocupar.htm>. Acesso em: 05 nov. 2018).

[423] ISTO É. **Facebook cedeu dados de usuários a 60 empresas, denuncia NYT**. Publicado em: 04 jun. 2018. Disponível em: <https://istoe.com.br/facebook-cedeu-dados-de-usuarios-a-60-empresas-denuncia-nyt/>. Acesso em: 05 set. 2018. Em resposta à denúncia levantada pelo "The New York Times", o vice-presiente do Facebook, Ime Archibong, disse que a empresa cedeu o acesso aos dados dos usuários aos fabricantes de dispositivos móveis apenas para que os aparelhos tivessem a rede social, "em uma época em que não existiam aplicativos". O executivo ressaltou que os 60 fabricantes assinaram acordos que impediam o uso dessas informações para fins diversos, e garantiu que sempre foi solicitada a permissão dos usuários.

[424] BUSVINE, Douglas. Dados ocultos do Facebook carregam problemas apontados pelo regulador alemão. **Terra**. Publicado em: 23 abr. 2018. Disponível em: <https://www.terra.com.br>. Acesso em: 05 set. 2018.

[425] RIBEIRO, Gabriel Francisco; PADRÃO, Márcio. O que é verdade no depoimento de Zuckerberg sobre o Facebook. **UOL**. Publicado em: 12 abr. 2018. Disponível em: <https://tecnologia.uol.com.br>. Acesso em: 05 set. 2018.

Nessa ocasião, vários usuários expressaram insatisfação com a atitude da empresa, pois sua privacidade no meio digital estaria em risco[426].

Johannes Caspar, autoridade de proteção de dados e liberdade da informação de Hamburgo, na Alemanha (The Hamburg Commissioner for Data Protection and Freedom of Information) determinou ao Facebook, em 27 de setembro de 2016, que deixasse de coletar e armazenar dados dos usuários do WhatsApp na Alemanha. A autoridade de proteção de dados exigiu, ainda, que a rede social apagasse todas as informações até então coletadas do WhatsApp.

Em comunicado escrito à imprensa[427], a autoridade alemã considerou:

> Facebook and WhatsApp are independent companies that process their user's data on the basis of their own Terms and Conditions and Data Privacy Policies. After the acquisition of WhatsApp by Facebook two years ago, both parties have publicly assured that data will not be shared between them. The fact that this is now happening is not only a misleading of their users and the public, but also constitutes an infringement of national data protection law. Such an exchange is only admissible if both companies, the one that provides the data (WhatsApp) as well as the receiving company (Facebook) have established a legal basis for doing so. Facebook, however, neither has obtained an effective approval from the WhatsApp users, nor does a legal basis for the data reception exist. It is clear that Facebook must respect German data protection law after the ECJ confirmed in its ruling from July, that national data protection laws are applicable if a company processes data in connection with a national subsidiary. Facebook is doing this through its subsidiary in Hamburg, which is responsible for the operation of the marketing business in Germanspeaking regions[428].

O Comissário Johannes Caspar assim se posicionou: “This administrative order protects the data of about 35 million WhatsApp users in Germany. It has to be

---

[426] SCOTT, Mark. Facebook ordered to stop collecting data on whatsApp users in Germany. In: **The New York Times**. Disponível em: <http://www.nytimes.com/2016/09/28/technology/whatsapp-facebook-germany.html?_r=4>. Acesso em: 30 set. 2016.

[427] HAMBURG. **Der Hamburgirsche Beaufitragte fur Datenzschutz und Informationsfreiheit**. Comunicado à imprensa. Disponível em: <https://www.datenschutz-hamburg.de>. Acesso em: 30 set. 2016.

[428] Tradução livre: Facebook e WhatsApp são empresas independentes que processam os dados dos usuários com base em seus respectivos Termos e Políticas de Privacidade. Após a aquisição do WhatsApp pelo Facebook há dois anos, ambas empresas asseguraram publicamente que dados não seriam compartilhados entre elas. O fato ocorrido agora não constitui apenas um engano, mas também uma infração das leis nacionais de proteção de dados. Tal compartilhamento apenas seria admitido se ambas as empresas, a que provê os dados (WhatsApp) bem como a que os recebe (Facebook) tivessem estabelecido base jurídica para tal prática. O Facebook, porém, não obteve efetiva aprovação por parte dos usuários do WhatsApp, e também não possui fundamento jurídico para receber os dados existentes. Está claro que o Facebook deve respeitar as leis de proteção de dados da Alemanha após a ECJ confirmar em seu regramento de julho, que as leis nacionais de proteção de dados são aplicáveis se a empresa processa dados em conexão com uma subsidiária nacional. O Facebook está praticando tal ato por meio de sua subsidiária em Hamburgo, a qual é responsável pela operação de negócios de marketing nos locais de língua alemã (Disponível em: <https://www.datenschutz-hamburg.de>. Acesso em: 30 set. 2016).

their decision, whether they want to connect their account with Facebook. Therefore, Facebook has to ask for their permission in advance. This has not happened"[429] .

Os relatos desses acontecimentos colocam duas importantes questões em perspectiva. A primeira relacionada à resistência de gigantes de internet em se submeterem e cumprirem regras de proteção de dados pessoais já em vigor. A segunda vinculada ao *enforcement*, ou seja, uma vez impingidas a cumprir a lei por meio das autoridades garantidoras da proteção de dados e da privacidade, ou mesmo por outros órgãos tal qual de defesa da concorrência, ou ainda pelo próprio Poder Judiciário. Quais são os meios para garantir que a determinação realmente foi cumprida pela empresa, a exemplo do pedido do Comissário de Hamburgo para que o WhatsApp apagasse informações coletadas preteritamente sem autorização?

Estas questões ocupam o debate centrado na doutrina da autodeterminação informativa, que demanda uma análise mais acurada, a ser feita posteriormente.

3.3 Autodeterminação informativa

O termo autodeterminação informativa se toma da tradição alemã (*Recht auf informationelle Selbstbestimmung*). A inteligência dessa doutrina confere ao indivíduo o poder, de ele próprio decidir sobre a utilização e divulgação de seus dados pessoais.

Segundo Fabiano Menke, uma das preocupações fundamentais do instituto da proteção de dados é o indivíduo não ser manipulado por informações que os seus interlocutores – entes estatais ou privados – tenham sobre sua pessoa, sem ele saber disso. Isso porque nos casos de conhecimento prévio das informações sobre a outra parte, quem tem a informação invariavelmente fica numa posição privilegiada. Trata-se, portanto, da importância de proteger os dados em relação a sua faceta de *pressuposto funcional da comunicação democrática*. Sobre esse aspecto, completa:

> Ele atalha os caminhos. Tem poder de manipulação e de direcionamento. Pode fazer colocações e perguntas dirigidas, pois todo um caminho que

[429] Tradução livre: "a ordem administrativa protege os dados de cerca de 35 milhões de usuários do WhatsApp na Alemanha. Deve ser decisão deles se eles querem conectar suas contas com o Facebook. Portanto, o Facebook deve solicitar sua permissão antecipada. E isso não aconteceu". (Disponível em: <https://www.datenschutz-hamburg.de/>. Acesso em: 30 set. 2016).

> teria de ser traçado para que chegasse a uma informação não precisa ser percorrido[430].

Porém, além de ser um pressuposto funcional da comunicação democrática, é ao mesmo tempo pressuposto de uma ´autodeterminada decisão contratual´ e, por consequência, pressuposto funcional da economia de mercado. Uma decisão livre das partes contratantes, ou seja, uma decisão sem manipulações, em especial quanto aos consumidores, só é possível quando o fornecedor tenha ciência dos dados entregues pelo consumidor ou, no mínimo, este conheça as informações relativas à sua pessoa de que o fornecedor disponha[431].

Segudo José Joaquim Gomes Canotilho e Vital Moreira, o moderno direito à autodeterminação informacional impede que a pessoa se transforme em ´simples objeto de informações´, ao passo que confere a cada um o direito de controlar a informação disponível a seu respeito. Ao comentarem o artigo 35 da Constituição Portuguesa[432], afirmam que se reconhece e se garante, assim, um conjunto de direitos fundamentais em matéria de defesa contra o tratamento informático de dados pessoais, cuja proteção analisa-se fundamentalmente em três direitos:

> (a) direito de acesso das pessoas aos registros informáticos para conhecimento de seus dados pessoais deles constantes (n.1), bem como a rectificação e complementação dos mesmos; (b) direito ao sigilo em relação aos responsáveis de ficheiros automatizados e a terceiros dos dados pessoais informatizados e direito à sua não interconexão (n.4); (c) direito ao não tratamento informático de certos tipos de dados pessoais. A proibição do número nacional único (n.5) funciona como garantia daqueles direitos,

---

[430] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.211.

[431] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.212.

[432] Artigo 35.º Da CRP: Utilização da informática. 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

> dificultando o tratamento informático de dados pessoais e a sua interconexão, que seria facilitada com um identificador numérico comum[433].

Nesse sentido, os autores portugueses afirmam: “o direito de conhecer a finalidade a que se destinam os dados informatizados recorta-se, hoje, como um direito à autodeterminação informativa de particular relevo”. E completam:

> Em rigor, trata-se de um *direito à autodeterminação sobre informações referentes a dados pessoais* que exige uma proteção clara quanto ao ´desvio dos fins´ a que se destinam essas informações. Daí as exigências jurídico-constitucionais relativas às finalidades das informações: (1) *legitimidade;* (2) *determinabilidade;* (3) *explicitação;* (4) *adequação e proporcionalidade;* (5) *exactidão e actualidade;* (6) *limitação temporal.* Todos esses requisitos permitem o controle dos fins, impedindo-se, designadamente, que haja tratamento de dados relativos a finalidades não legítimas ou não especificadas, excessivas relativamente a estas mesmas finalidades ou que tenham como referência dados inexactos ou desactualizados ou, ainda, mantidos por lapsos temporais injustificados[434].

Ao analisar a autodeterminação informativa, importante entender sua relação com a intimidade. Para tanto, nos valemos de Marc Carrillo, o qual explica que enquanto a função do direito à intimidade é proteger qualquer invasão que possa ocorrer no âmbito da vida pessoal e familiar, e que a pessoa deseja excluir do conhecimento alheio e das intromissões de terceiros contra a sua vontade, o direito à proteção de dados, por sua vez, busca garantir um poder de controle sobre seus dados pessoais, seu uso e seu destino, com o objetivo de evitar um tráfico ilícito e lesivo da dignidade e do direito do afetado. Com efeito, o direito fundamental da proteção de dados amplia a garantia constitucional aos dados relevantes ou incidentes no exercício de qualquer dos direitos da pessoa e, portanto, independentemente de estarem ou não relacionadas à honra, ideologia, privacidade pessoal e familiar ou qualquer outra proteção constitucional. O objeto da autodeterminação informativa ou liberdade computacional não se reduz à proteção de dados relativos à intimidade ou à honra da pessoa como, em princípio, deve ser pensada, mas também se estende a outros, sejam ou não pertencentes à esfera íntima, cujo conhecimento ou emprego por terceiros possa afetar seus direitos, fundamentais ou não[435].

---

[433] CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. **Constituição da República Portuguesa Anotada**. v.1. São Paulo: RT; Coimbra, PT: Coimbra, 2007, p.551.
[434] CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. **Constituição da República Portuguesa Anotada**. v.1. São Paulo: RT; Coimbra: Coimbra, 2007, p.553.
[435] CARRILLO, Marc. **El derecho a nos ser molestado**: información y vida privada. Navarra: Editorial Aranzadi, 2003, p.95-96.

A doutrina da liberdade informática[436], ao lado da doutrina da autodeterminação informativa foram fundamentais para o desenvolvimento dos atuais sistemas de proteção de dados pessoais e da privacidade.

A cada sujeito deve ser dado o poder de decisão sobre quando e dentro de quais limites procede revelar situações ou aspectos de sua própria vida, "pues es precisamente em esa autodeterminación consciente y responsable del sujeto, donde radica el derecho fundamental a la protección de datos de carácter personal"[437].

Ao Estado cabe o dever de proteção do *direito à autodeterminação informativa,* estabelecendo restrições à atividade privada de colheita, tratamento e utilização de dados pessoais por parte de entidades privadas, sobretudo quando a conexão eletrônica de dados e a sua colocação em rede através da internet é implementada por parte de poderosas empresas *multimídia*[438].

Em relação à propriedade de dados, não é adequado falar, nessa seara, em propriedade por parte do indivíduo dos dados relativos à pessoa. Segundo Fabiano Menke, a concepção do ordenamento jurídico relativo à proteção de dados não se coaduna com a ideia de propriedade sobre os mesmos. O mais adequado é que se considerem os dados relacionados a uma pessoa como resultado de uma observação social ou de um processo de comunicação social multirrelacional[439]. Nas palavras do autor:

> Assim, o direito da proteção de dados não regula a propriedade, mas sim consiste num ordenamento sobre a informação e a comunicação a eles relacionada, determinando quem, em qual relação, e em que situação, está autorizado a lidar com os modelos de uma determinada pessoa de uma determinada maneira[440].

Sobre esse assunto, segundo Danilo Doneda, em uma interpretação liberal sobre o que venha a ser autodeterminação informativa, poder-se-ia considerar,

---

[436] A doutrina da liberdade informática foi particularmente mais desenvolvida na Espanha e se estrutura, na maioria das vezes, como um direito específico de conhecimento e controle de dados pessoais. (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.199).

[437] CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.138.

[438] CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. **Constituição da República Portuguesa Anotada**. v.1. São Paulo: RT; Coimbra: Coimbra, 2007, p.554.

[439] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.213: "Como modelos da realidade, teriam os dados pessoais sempre um autor e um objeto. Os dados têm relação com um objeto, mas também com o autor. Não podem ser associados exclusivamente ao objeto".

[440] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.213.

eventualmente, que ela se concentraria no ato do consentimento da pessoa para o tratamento de seus dados pessoais e assumiria contornos negociais. Assim, prestar-se-ia ao afastamento da matéria do âmbito dos direitos da personalidade. Tal leitura pode induzir à impressão de que as pessoas teriam um direito de propriedade sobre suas informações, transportando esta fenomenologia para o campo das situações patrimoniais.

Portanto, a autodeterminação informativa não pode ser compreendida como garantidora de um domínio absoluto da pessoa sobre os dados a ela relacionados, como se fossem *seus* dados numa relação de exclusão de todos os demais membros da sociedade, de modo que o direito da proteção de dados resguarda a pessoa não como proprietária de seus dados, mas a auxilia como titular de interesses e tomadora de decisões no contexto do ordenamento comunicacional e informacional. O foco da proteção é a tomada de decisões pelo próprio indivíduo[441].

Quanto aos dados sob o controle do titular, importante esclarecer que não se reduzem apenas aos relativos à vida íntima[442], mas se expandem a qualquer informação que identifique ou permita identificar o titular, e que possa servir para elaborar seu perfil sociocultural, ideológico, racial, religioso, sexual, sanitário, econômico ou de qualquer outra natureza, ou ainda, que possa servir de qualquer utilidade que, em momento determinado, constitua uma ameaça à privacidade do indivíduo, independentemente da modalidade de captação, armazenamento, organização ou acesso[443].

Os dados pessoais, com efeito, não estão relacionados apenas ao direito à privacidade, mas à proteção da identidade da pessoa. Tanto assim que o direito de oposição a decisões automatizadas, como o direito à retificação de dados, não

---

[441] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.214-215.

[442] A autora espanhola Castillo Vázquez dá notícias de que o Tribunal Constitucional espanhol, por muito tempo, manteve o critério de que o controle exercido pelo titular dizia respeito somente aos concernentes a sua vida íntima. (CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.70-73). Tal critério, também utilizado em outros países, não mais se sustenta com a moderna doutrina da autodeterminação informativa.

[443] Nesse sentido reconhece a decisão alemã que se comentará adiante. Nas palavras de Fabiano Menke: "A esfera de proteção do direito à autodeterminação informativa não estaria limitada, segundo o Tribunal Constitucional Federal, às informações, que consoante a sua natureza são sensíveis, portanto, já estão constitucionalmente protegidas. Também o contato com os dados pessoais, conforme o objetivo perseguido pelo acesso e as possibilidades de tratamento e de associação, poderá ter influência sobre a privacidade e a liberdade comportamental do indivíduo". (MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.219).

guarda relação direta com a privacidade, mas com a identidade da pessoa cujos dados foram coletados, sob o entendimento de que os dados pessoais são um prolongamento do próprio indivíduo.

O direito à autodeterminação informática, como âncora constitucional da proteção de dados, integra o direito geral da personalidade. Conforme Laura Schertel Mendes, o direito geral da personalidade vem sendo desenvolvido pelo Tribunal Constitucional Federal desde 1950 e é derivado da combinação dos artigos 1º, §1º (dignidade da pessoa[444] [445]) e 2º, §1º (liberdade), da Lei Fundamental. Sua atuação em conjunto garante a cada indivíduo a possibilidade de desenvolver sua própria personalidade[446].

A dignidade, nas palavras de Willis Santiago Guerra Filho, é definidora do núcleo essencial dos direitos fundamentais[447], "que cobran su razón de ser a partir del reconocimiento de la individualidade del sujeto y el contenido de su espiritualidad, y al colocarle en el vértice del mundo, le hacen portador singular de derechos"[448].

---

[444] Sobre a dignidade humana, esta "trasciende la memoria colectiva para convertirse em la premissa antropológica del orden político-social, que a partir de 1789, conduce a su plasmación en los textos constitucionales, no ya como norma, sino como legado cultural de un pueblo que eleva la condición humana a sua máxima consideración. (CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.133).

[445] A Grundgesetz declara, em seu artigo 1, I, a dignidade humana como "intocável". Logo em seguida (art. 1 I 2 GG), ordena a todos os poderes estatais observá-la e protegê-la. O dever de observação é próprio de todos os direitos fundamentais como direitos de resistência contra intervenções estatais: o Estado observa a liberdade ou direito individual enquanto omite uma ação perturbadora. O dever de proteção diz respeito a mandamento de ação direcionado ao Estado, ação contra agressões da dignidade da pessoa humana proveniente de particulares. Se, por um lado, os mandamentos relativos à dignidade da pessoa humana são claros, difícil é a sua definição. Não existe unanimidade na literatura especializada alemã. Muitos são os pontos de ênfase e formas de tratamento da matéria. Os comentários à Grundgesetz dedicam ao Art. 1 I GG muitas páginas. Mais bem-sucedida tem sido uma definição negativa: uma definição que parte da intervenção ou violação da dignidade humana (visto que uma intervenção não pode ser justificada, pois a outorga do Art. I GG é ilimitada). Por isso, a preocupação dogmática se volta toda para a verificação do momento em que se pode dizer que a dignidade humana foi atingida. Para tanto, a definição de sua área de proteção tem enorme importância, pois nenhuma intervenção poderá ser justificada. Outra tese bastante corrente na literatura especializada é que boa parte (alguns afirmam erroneamente que todos) dos direitos fundamentais teriam um lastro na garantia da dignidade humana. Entre eles, destaque-se o Art. 2 I GG (livre desenvolvimento da personalidade), que abrange os direitos gerais da personalidade, funcionando como *lex generalis* em face de garantias mais específicas dos Art. 3 et seq. GG, como a inviolabilidade do domicílio (Art. 13 I GG) ou do sigilo telefônico (Art. 10 I GG), direito à incolumidade física ou mesmo a liberdade de locomoção contra os seus mais diversos cerceamentos, incluindo os legais (Art. 2 II c.c. Art. 104 I 1 GG). (SCHWABE, Jürgen. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. (Org.) Leonardo Martins. Tradução de Beatriz Hennig, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro, Vivianne Geraldes Ferreira. Berlim-Alemanha: Fundación Konrad-Adenauer-Stiftung, 2005, p.177-178.

[446] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.31. E acrescenta: "Nessa formulação de um direito à autodeterminação informativa, o Tribunal reconheceu uma carga participativa muito maior que a reconhecia pelas interpretações das normas de proteção de dados pessoais em períodos anteriores" (p.41-42).

[447] GUERRA FILHO, Willis Santiago. **Processo constitucional e direitos fundamentais**. 6.ed. São Paulo: SRS, 2006, p.187.

[448] CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.134.

Para além da autodeterminação informativa, no que toca à dignidade, há um estreito vínculo com o desenvolvimento da personalidade e da integridade pessoal. Conforme observam José Joaquim Gomes Canotilho e Vital Moreira, quanto mais os dados relacionam dignidade, personalidade e autodeterminação das pessoas, tanto mais se impõem restrições quanto ao seu uso e recolha (banco de dados). É neste contexto que se situam dois problemas fundamentais relativos ao processamento de dados informáticos: determinação das *categorias* de dados (i.); e graduação das ingerências necessárias à proteção de outros bens constitucionais (ii.)[449].

Ademais, não se pode dirigir o mesmo olhar para conflitos de direitos fundamentais que antes se davam no mundo analógico, para os dilemas que ora se colocam no mundo digital, no qual há uma circulação incontrolada de dados de caráter pessoal:

> Hay uma serie de rasgos que son absolutamente decisivos para entender la verdadeira colisión del viejo mundo analógico – donde se desenvuelven com normalidade los clásicos derechos fundamentales -, com el nuevo fenômeno digitalizador, y su consecuencia sobre los derechos fundamentales del siglo XXI, llamados ambos a encontrar um punto de equilíbrio que complazca a la sociedad, en la defensa de intereses encontrados[450].

Voltando aos primórdios, constata-se que o nascimento da doutrina da autodeterminação informativa está relacionado a um importante julgado do Tribunal Constitucional Alemão[451]. Foi justamente por meio dessa decisão que se formulou a

---

[449] CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. **Constituição da República Portuguesa anotada**. v.1. São Paulo: RT; Coimbra: Coimbra, 2007, p.551. "A operatividade de todos estes direitos exige que a informatização de direitos pessoais obedeça a certos princípios que a doutrina tem sublinhado: (a) publicidade, isto é conhecimento da criação e manutenção de registros informáticos; (b) justificação social, a criação e manutenção de ficheiros, bases de dados e bancos de dados deve ter um objetivo geral e usos específicos socialmente aceitos; (c) a transparência, ou seja, a clareza dos registros, quanto às espécies ou categorias de dados recolhidos e tratados, quanto à existência ou não de fluxos de informação, quanto ao tempo de tratamento, e quanto à identificação do responsável do ficheiro; (d) a especificação de finalidades, ou seja, as finalidades da recolha e o processamento devem ser especificados logo no momento de recolha; (e) a limitação da recolha, que deve ser feita por meios lícitos – conhecimento da pessoa a que respeitam ou autorização legal – restringir-se aos dados necessários para as finalidades especificadas (princípios da necessidade, da adequação e da proporcionalidade); (f) princípio da fidelidade, os dados devem ser exactos, completos e actuais; (g) a limitação da utilização, isto é, os dados, uma vez recolhidos e processados, devem ser exclusivamente utilizados para a prossecução dos fins previamente especificados; (h) as garantias de segurança, que impõem a adopção de medidas tendentes a proteger e garantir os dados contra perda, destruição e acesso de terceiros; (i) a responsabilidade, que se traduz em imposição de especiais deveres legais e deontológicos aos responsáveis pelos ficheiros; (j) princípio da política de abertura, os ficheiros, bancos e bases de dados devem garantir a transparência da acção administrativa, sobretudo quanto à clareza dos registros, às espécies e categorias de dados recolhidos e tratados, à existência ou não de fluxos de informação, ao tempo de tratamento e à identificação do responsável do ficheiro; (l) princípio de limitação no tempo, os dados devem ser cancelados, uma vez obtida as finalidades a que se propunham.

[450] CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.58.

[451] Aqui cabe uma pausa para registrar que é na Alemanha onde existem, em regra, os maiores debates em torno desse assunto. Segundo Fabiano Menke, "a Alemanha pode ser considerada um dos países que apresentam o maior desenvolvimento doutrinário e valorização quanto à proteção de dados, sendo que o tema

concepção do direito à autodeterminação da informação, ao reconhecer um direito subjetivo fundamental ao indivíduo, criando um marco para a teoria da proteção de dados, irradiando inspiração para a formulação de normas nacionais e europeias sobre o assunto.

A decisão paradigmática do Tribunal Constitucional Federal alemão é denominada *Volkszahlungsurteil,* ou caso do censo demográfico, e foi resultado do julgamento da Lei do Recenseamento de População, Profissão, Moradia e Trabalho de 25/03/1982.

O julgamento, por sua vez, ocorreu em 15/12/1983. O caso cuidava de várias reclamações constitucionais ajuizadas por grupos de cidadãos que impugnavam a lei federal de recenseamento alemã. Detalhe curioso é que dita lei fora aprovada *por unanimidade* tanto pelo Parlamento quanto pelo Conselho Federal.

Fabiano Menke fornece detalhes do caso: o texto legal previa que em 1983 seria realizado um censo por parte de funcionários públicos e demais agentes encarregados, que não se limitaria apenas a fazer o levantamento do número de habitantes do país, mas também coletaria uma série de dados pessoais dos cidadãos:

> Em sede de liminar, o Tribunal Constitucional Federal suspendeu os efeitos da lei de recenseamento e acabou por julgar parcialmente procedentes as reclamações constitucionais. Em sua base, a realização do censo foi mantida, mas foi consideravelmente modificada, conforme as ordens do Tribunal, para que fosse procedida por meios que resguardassem a segurança dos dados dos cidadãos a serem entrevistados, como, por exemplo, pela proibição de que alguns dados obtidos, como nome e endereço, fossem transferidos a outros órgãos do governo[452].

Importante, ainda, contextualizar o ambiente histórico em que foi julgado o processo. Segundo Fabiano Menke, as previsões do livro de 1984, de George Orwell, que chamava a atenção para os perigos do Estado espião, pode ter influenciado na acentuada onda de protestos contra os temores dos cidadãos alemães. Some-se a esse fato, ainda segundo o autor, que o desenvolvimento computacional da época estava em estágio inicial; o armazenamento e o tratamento

---

apresenta tamanha importância que pode até mesmo ser classificado como um instituto autônomo (Datenschutz)". (MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.205.

[452] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.207.

de dados se davam a partir de grandes computadores centralizados, pesados e volumosos. Não havia disseminação e descentralização da informação como ocorre atualmente com a internet tampouco a acessibilidade a computadores pessoais, que permite à maioria das pessoas ser usuária e produtora da informação. Na época, as discussões da opinião pública concentravam-se nos temores e nos riscos da informação centralizada na figura do Estado[453].

Em dado momento, na sociedade da informação, dada a alta possibilidade de tratamento de dados[454] já existente, foi necessário reconhecer um direito autônomo que protegesse a pessoa, elevando a proteção de dados como um direito fundamental. Sobre o tema, Laura Schertel Mendes adverte:

> A disciplina da proteção de dados pessoais emerge no âmbito da sociedade da informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais[455].

Além disso, não se pode deixar de lembrar que à época havia grandes preocupações em relação à proliferação do terrorismo na Alemanha. Segundo Fabiano Menke, “a decisão, portanto, é uma reação à reação”, no sentido de que a primeira reação foi a do Estado, no plano legislativo, para tentar evitar que o terrorismo continuasse a se proliferar em solo alemão. A segunda reação foi a do Tribunal Constitucional Federal, reafirmando o direito de proteção da personalidade do cidadão ao realizar o controle dos excessos das leis que tentavam conter as ameaças do terrorismo[456].

A Corte Constitucional alemã reconheceu que o moderno processamento de dados pessoais constitui uma grave ameaça à personalidade do indivíduo, na medida em que possibilita o armazenamento ilimitado de dados, além de permitir

---

[453] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.207.

[454] O valor das informações obtidas não reside apenas na capacidade de armazenamento de grande volume de dados, mas, principalmente, na possibilidade de obtenção de novos elementos informativos a respeito dos cidadãos a partir do tratamento desses dados. (MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.33).

[455] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.32.

[456] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.218.

sua combinação de modo a formar um retrato completo da pessoa, sem sua participação ou conhecimento. Na reflexão de Laura Schertel Mendes:

> Como se pode perceber, a partir do momento em que a tecnologia passa a permitir o armazenamento e o processamento rápido e eficiente de dados pessoais, dá-se a associação entre a proteção à privacidade e informações pessoais. Nesse contexto, percebe-se uma alteração não apenas do conteúdo do direito à privacidade, mas também do seu léxico, passando a ser denominada privacidade informacional, proteção de dados pessoais, autodeterminação informativa, entre outros. Dessa forma, opera-se na dogmática e na prática jurídica uma clara evolução no direito à privacidade[457].

Ainda segundo a autora, outro grande mérito da decisão foi elevar o indivíduo a protagonista no processo de tratamento de seus dados:

> A sentença da Corte Constitucional, na sua formulação de um direito à autodeterminação da informação, criou o marco para a teoria da proteção de dados pessoais e para as subsequentes normas nacionais e europeias sobre o tema, ao reconhecer um direito subjetivo fundamental e alçar o indivíduo a protagonista no processo de tratamento de seus dados. Dessa forma, o grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais baseia-se em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado. Isso significa uma limitação ao poder legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação da informação[458].

Chega-se ao auge da separação entre privacidade e proteção de dados. O Tribunal Constitucional Federal reconhece que a autodeterminação informativa vai além da proteção da privacidade, porquanto essa doutrina confere ao indivíduo o poder de basicamente determinar por si próprio sobre a divulgação e a utilização de seus dados pessoais. Porém, isso não significa que não exista correlação entre a autodeterminação informativa e a privacidade. Pelo contrário. A autodeterminação informativa complementa a proteção constitucional da liberdade comportamental e da privacidade[459].

---

[457] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.32. Ver também: RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.17.

[458] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.31. "Nessa formulação de um direito à autodeterminação informativa, o Tribunal reconheceu uma carga participaiva muito maior que a reconhecia pelas interpretações das normas de proteção de dados pessoais em períodos anteriores" (p.41-42).

[459] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.219.

Outrossim, a função desse direito autônomo não é a de proteger os dados em si, mas de proteger a pessoa titular dos dados. Além disso, diante da decisão alemã, fica ainda mais claro que a proteção de dados pessoais se distancia da bifurcação público e privado.

Segundo Danilo Doneda, um dos pontos de influência da decisão alemã foi a solidificação do entendimento segundo o qual a proteção de dados pessoais, como direito fundamental, requer um embasamento constitucional direto. Ainda segundo esse autor, outro ponto é a importância para uma mudança de perspectiva que se fez ver na doutrina, influenciada pela ideia de um direito à 'liberdade informática'[460].

Diante de todas as questões colocadas, é possível dizer que a decisão alemã do censo se consagra como um verdadeiro marco da proteção de dados, "por ter fixado várias diretrizes dessa disciplina que influenciaram legislações, doutrina e jurisprudência de diversos países"[461], e por ter consolidado o princípio da finalidade e especificação de propósito em torno dos dados pessoais, que serve como um vetor limitador em sua coleta.

3.4 Direito fundamental à garantia da confidencialidade e integridade dos sistemas técnico-informacionais

Em 27 de fevereiro de 2008, o Tribunal Constitucional Federal produziu novo marco na história da proteção de dados ao reconhecer um novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais (*Grundrecht auf Gewahrleistung der Vertraulichkeit und Integritat informationstechnischer Systeme*), proclamado no contexto de uma reclamação constitucional ajuizada contra dispositivos da lei do Estado de Nordrhein-Westfalen[462] que regulamentavam e permitiam a busca ou investigação remota de computadores de pessoas suspeitas de cometer ilícitos criminais.

---

[460] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.198. Para o autor, "a doutrina da liberdade informática é uma leitura particular do direito à autodeterminação informativa, que tende a aproximar-se dos direitos da personalidade como uma subespécie destes, relacionando-se diretamente com o direito à privacidade; um tal enfoque generalista do problema da informação, que privilegia a busca de uma liberdade em um novo "meio", está na raiz do pensamento que veio a despontar no instituto brasileiro do *habeas data*".

[461] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.208.

[462] Apesar de a mencionada lei não ter chamado muito a atenção logo após ser editada, passou a ser foco de intensa discussão a partir do momento em que o ministro de Estado Wolfgang Schauble resolveu propor, em nível federal, a adoção dos mesmos dispositivos que autorizavam o monitoramento remoto de computadores de suspeitos da lei de Nordrhein-Westfalen. (MENKE, Fabiano. A proteção de dados e o novo direito fundamental à

Segundo explica Fabiano Menke, a proteção reconhecida pela Corte Constitucional alemã incide em casos que compreendem sistemas informacionais – considerados individualmente ou acerca de suas possibilidades de conexões técnicas – que contenham tantos dados pessoais de determinado indivíduo, que se torne capaz de extrair seu perfil em violação à sua pessoa:

> Esclarecendo ainda mais quando atua o novo direito fundamental, o Tribunal Constitucional Federal determina que a sua proteção serve para os casos em que a intervenção compreenda sistemas informacionais que, considerados individualmente ou acerca de suas possibilidades de conexões técnicas, contenham dados pessoais do indivíduo numa extensão e numa variedade que o acesso a esse sistema possibilite vislumbrar as diversas facetas da condução de sua vida pessoal ou até mesmo uma ´fotografia´ de sua personalidade[463].

Segundo Willis Santiago Guerra Filho, os direitos fundamentais são, originalmente, direitos humanos. Contudo, estabelecendo um corte epistemológico, para estudar sincronicamente os direitos fundamentais, devemos distingui-los enquanto manifestações positivas do direito, com aptidão para produzir efeitos no plano jurídico dos direitos humanos enquanto pautas ético-políticas, "direitos morais", situados em uma dimensão suprapositiva, deonticamente diversa daquela em que se situam as normas jurídicas – especialmente aquela de direito interno[464].

Há que se distinguir, ainda, direitos fundamentais dos direitos de personalidade, por serem esses direitos, na doutrina de Willis Santiago Guerra Filho, que se manifestam em uma dimensão privatista, onde também se revelam os direitos fundamentais, mas de forma indireta, reflexa[465].

Não se pode confundir, outrossim, direitos fundamentais como direitos subjetivos públicos, pois, segundo explica Willis Santiago Guerra Filho, se os primeiros são direitos que os sujeitos gozam perante o Estado, não há aí uma

---

garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.216). Além disso, "há que se relacionar a edição das leis impugnadas perante o Tribunal Constitucional Federal que ensejaram a proclamação desse novo direito fundamental ao contexto de reação ao terrorismo. É conhecida a realidade de que muitos dos terroristas do 11 de setembro de 2001 fundaram células em solo alemão, como na região do Vale do Ruhr, e a célula mais famosa de todas, a de Hamburgo, que funcionou ao longo de vários anos com integrantes que estudavam na Universidade Técnica de Hamburg-Harburg" (p.217-218).

[463] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.221-222.

[464] GUERRA FILHO, Willis Santiago. **Processo constitucional e direitos fundamentais**. 6.ed. São Paulo: SRS, 2006, p.40.

[465] GUERRA FILHO, Willis Santiago. **Processo constitucional e direitos fundamentais**. 6.ed. São Paulo: SRS, 2006, p.41.

relação biunívoca, já que nem todo direito subjetivo público é direito com a estatura constitucional de um direito fundamental[466].

Além disso, e o mais importante segundo Willis Santiago Guerra Filho, os direitos fundamentais não têm apenas uma dimensão subjetiva, mas também uma objetiva. Essa última é aquela onde os direitos fundamentais se mostram como princípios conformadores do modo como o Estado que os consagra deve organizar-se e atuar. Já a dimensão subjetiva é de onde 'brotam' as demais, condicionando-as[467].

Em comparação com a decisão do censo demográfico de 1983 (*Volkszahlungsurteil*), o contexto, entretanto, é um pouco diverso. Segundo Fabiano Menke, enquanto a mais antiga foi prolatada num cenário de temores do controle do Estado sobre o indivíduo, a decisão mais recente se insere numa realidade em que não apenas o Estado é o foco de preocupação, mas também a iniciativa privada, em cujo cenário estão inseridos vários modelos de negócio que colocam em risco os indivíduos, quanto à coleta de dados e informações relativos à sua personalidade[468].

Ainda no plano comparativo, para Stefano Rodotá existem duas questões essenciais que distinguem a decisão de 2008 do precendente anterior:

> La prima riguarda il fatto che la nozione di riservatezza viene dilatata per definire um quadro d´insieme che impedisca la riduzione della persona, dunque dell´umano, a semplice entità materiale. Da questo, ed é il secondo punto relevante, resulta una nuova forma di garanzia, che supera la dicotomia tra *habeas corpus,* legata al corpo *físico,* e *habeas data*, concepito come estensione di quella garanzia storica al corpo *elettronico.* Non vi sono più oggetti distinti della tutela, ma un oggetto unico: la persona nelle diverse sue configurazioni, via via determinate dal suo rapporto com le tecnologie, che non sono soltanto quelle elettroniche[469].

---

[466] GUERRA FILHO, Willis Santiago. **Processo constitucional e direitos fundamentais**. 6.ed. São Paulo: SRS, 2006, p.41.

[467] GUERRA FILHO, Willis Santiago. **Processo constitucional e direitos fundamentais**. 6.ed. São Paulo: SRS, 2006, p.42.

[468] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.217: "A decisão do Tribunal Constitucional Federal chama a atenção para a importância que a utilização dos sistemas informáticos adquiriu para o desenvolvimento da personalidade do indivíduo nas últimas décadas, algo que antes não era previsível. À medida que parcela considerável da população passa a ter acesso a computadores e estes começam a desempenhar papel de destaque no seu dia a dia, tem-se a abertura de novas possibilidades, mas ao mesmo tempo concorrem com essas possibilidades novos riscos para a sua personalidade" (p.217).

[469] RODOTÀ, Stefano. **Il diritto di avere diritti**. Bari/Italia: Laterza, 2012, p.317-318. Tradução livre: "A primeira diz respeito ao fato de que a noção de confidencialidade é ampliada para definir um arcabouço que impeça a redução da pessoa, portanto do humano, a uma entidade material simples. A partir disso, e é o segundo ponto relevante, está uma nova forma de garantia, que vai além da dicotomia entre o *habeas corpus*, ligado ao corpo físico, e o *habeas data*, concebido como uma extensão dessa garantia histórica ao corpo eletrônico. Não há mais objetos distintos de proteção, mas um único objeto: a pessoa em suas várias configurações, gradualmente determinada por sua relação com as tecnologias, que não são apenas eletrônicas".

A decisão do Tribunal Constitucional Federal põe luz sobre a importância adquirida pela utilização dos sistemas informáticos para o desenvolvimento da personalidade do indivíduo nas últimas décadas. Com o aparelhamento da sociedade com seus *smartphones, tablets, notebooks* e computadores, surgem novos riscos à personalidade do indivíduo.

Ademais, um dos desafios após a decisão alemã de 2008 ocorreu no campo de como essa se relacionaria com a já consagrada doutrina da autodeterminação informativa. Isso porque o Tribunal Constitucional Federal, na decisão mais recente, considerou que há uma lacuna de proteção, uma vez que a autodeterminação informativa não consegue defender o indivíduo de todas as ameaças à personalidade, como as existentes nos casos em que o usuário de um sistema técnico-informático confia em dados desse sistema ou os envia a outrem. É possível que um terceiro que tenha acesso a esse sistema possa ter conhecimento de um extenso conjunto de dados, sem estar submetido a regras acerca da coleta e do tratamento desses dados. Na contribuição de Fabiano Menke:

> Esse amplo acesso, segundo entende o Tribunal Constitucional Federal, extrapola o "peso" para a personalidade do indivíduo das coletas individuais de dados, objeto da proteção da autodeterminação informativa. Aqui, portanto, uma diferença: a autodeterminação informativa protege o dado individualmente considerado, ou até mesmo um conjunto de dados, enquanto o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais resguarda o próprio sistema e os dados vistos no seu sentido mais amplo[470].

Mais a mais, no enquadramento dogmático do instituto, o Tribunal alemão esclarece que no caso de não existir proteção suficiente para os perigos aos quais a personalidade do indivíduo está exposta quando da utilização dos sistemas técnico-informacionais, o direito geral de personalidade deverá incidir para, na sua função supletiva, ou seja, de preenchimento de lacunas, além de atuar nos casos

[470] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.219: "A decisão do Tribunal Constitucional Federal recebeu algumas críticas da doutrina alemã. Nesse sentido, por exemplo, não há que se falar em lacuna a ser preenchida por um novo direito fundamental, mas sim em aplicação da já consagrada autodeterminação informativa juntamente com o teste da proporcionalidade, para que se pesquise, no caso concreto, se a intensidade da intervenção fere os preceitos constitucionais. Nesse sentido, a privacidade e a integridade dos sistemas técnico-informacionais não devem ser aplicadas paralela/sucessivamente com a autodeterminação informativa, mas são subespécie desta" (p.225-227).

conhecidos, nos quais até então vinha se manifestando, também garantir a privacidade e a integridade dos sistemas técnico-informacionais[471].

Em uma outra perspectiva, é possível dizer que a decisão de 2008 da Corte Constitucional alemã reconhece que entre o humano e a máquina não existe apenas interação, mas também compenetração, estabelecendo-se uma continuidade entre esses dois entes, de modo a se verificar uma nova antropologia, que reage às suas categorias jurídicas e modifica suas qualidades, eis que a *riservatezza* – qualidade do humano – transfere-se para a máquina. Há, com efeito, uma constatação de que se está delineando uma ordem social e jurídica das máquinas que reivindica uma autonomia própria e que pode não apenas determinar conflitos com a tradicional autonomia das pessoas, mas produzir uma nova antropologia[472].

3.5 Das dimensões da proteção de dados pessoais

A doutrina divide a evolução da proteção de dados pessoais em gerações[473]. Com alicerce na doutrina de Willis Santiago Guerra Filho, preferiremos a expressão *dimensões* a *gerações.* Isso porque as gerações anteriores não desaparecem com o surgimento das mais novas; os direitos 'gestados' em uma geração, quando aparecem em uma ordem jurídica que já traz direitos da geração sucessiva, assumem uma outra dimensão, pois os direitos de geração mais recente tornam-se pressuposto para entendê-los de forma mais adequada e, consequentemente, também, para melhor realizá-los[474].

À semelhança, Stefano Rodotà ensina que diante desses vários tecidos e contínuas conexões entre situações diversas, existe uma indivisibilidade dos direitos,

---

[471] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015, p.220.

[472] RODOTÀ, Stefano. **Il diritto di avere diritti**. Bari/Italia: Laterza, 2012, p.315-318: È l´umano che ingloba in sé la machina, non il contrario. Si riconosce che tra l´uomo e la machina non vi è soltanto interazione, ma compenetrazione. Questo è um dato strutturalmente evidente, di cui viene riconosciuta la rilevanza costituzionale. Il diritto ristabilisce così la priorità dell´umano, ma manifesta la sua potenza dicendo che nel mondo esite uma nuova entità, costituita appunto dalla persona e dall´apparato técnico al quale essa affida i suoi dati. Tra persona e macchina si stabilisce um *continuum:* riconoscendo, il diritto ci consigna anche una nuova antropologia, che reagisce sulle categorie giuridiche e ne modifica la qualità. La riservatezza, qualità dell´umano, si trasferisce alla machina.

[473] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. **Technology and privacy**, Cambridge-MA/EUA, 1997, p.219-241; DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006; CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007; MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014.

[474] GUERRA FILHO, Willis Santiago. **Processo constitucional e direitos fundamentais**. 6.ed. São Paulo: SRS, 2006, p.43.

no sentido de que “i diritti in rete non sono gerarchizzabili, perchè é la rete stessa che rifiuta le gerarchie, e così promuovo una cittadinanza sempre più orizzontale”[475].

Pois bem, na *primeira dimensão* vê-se a consolidação de um conceito de privacidade ligado à proteção de dados pessoais. Nesse período (década de 1970) há uma reação ao processamento tanto em empresas privadas como na administração pública. Segundo Laura Schertel Mendes:

> A primeira geração das normas de proteção de dados pessoais surgiu como reação ao processamento eletrônico de dados nas administrações públicas e empresas privadas, bem como às ideias de centralização dos bancos de dados em gigantes bancos de dados nacionais[476].

Dentre as normas fruto dessa primeira dimensão, em âmbito europeu, podem ser citadas as leis do Estado Alemão de Hesse (1970)[477], a Lei de Dados da Suécia (1973) – a primeira em âmbito federal da Europa[478] – o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977) [479].

Do outro lado do Atlântico, em território norte-americano, na década de 1970, foram aprovados o Fair Credit Reporting Act (1970), sobre a regulação dos relatórios de crédito dos consumidores, e o Privacy Act (1974), aplicável à administração pública e fruto do escândalo Watergate, diante do temor sobre o uso que o governo poderia exercer sobre computadores e sistemas informáticos. Ambos regulamentos tiveram por base os Fair Practice Principles (FIPPs), conjunto de cinco práticas principiológicas, elaboradas, em 1973, pelo Departamento de Saúde, Educação e

---

[475] RODOTÀ, Stefano. **Il mondo nella rete**. Quali i diritii, quali i vincoli. Roma: Laterza, 2014, p.27.

[476] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.30.

[477] Em 7 de abril de 1970, foi promulgada pelo Estado Alemão de Hasse a *Datenshutz*. Por meio da proteção trazida por essa norma aos dados de caráter pessoal, o objetivo foi impedir a lesão de bens dignos de tutela, garantindo a reserva dos dados relativos às pessoas frente aos abusos cometidos por ocasião de seu armazenamento, transmissão, modificação ou cancelamento. Em 27 de fevereiro de 1977, o parlamento federal alemão seguiu os passos do Parlamento regional de Hesse e aprovou a *Datenshutz* federal, criando um comissário federal para a proteção de dados (*Bundesbeauftragter fur den Datenshutz*).

[478] Em 11 de maio de 1973, foi aprovada a lei *Data Lag* que protege os indivíduos do mau uso de seus dados e da informação pessoal, por meio de registros e arquivos. A Suécia foi o primeiro país europeu a ter uma lei nacional sobre o tema. Esta lei sueca foi responsável por introduzir conceitos, como o registro central de informação de processamento de dados pessoais e o procedimento de licenciamento, com o qual o registro público foi aberto ao escrutínio dos cidadãos e consumidores, usado como uma ferramenta de cumprimento da lei pelas agências de proteção de dados. Estes conceitos foram o pilar das primeiras legislações europeias de proteção de dados. (PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. **Breves notas sobre a ressignificação da privacidade**. In: **Revista Brasileira de Direito Civil** – RBDCivil | Belo Horizonte, v.16, p.35-56, abr.-jun. 2018, p.40-41).

[479] “O impulso para o surgimento dessas normas foi o contexto generalizado do Estado Social, que requeria, para o funcionamento de sua burocracia, de planejamento sofisticado, o que, por sua vez, somente poderia ser alcançado por meio da coleta e do processamento dos dados dos cidadãos”. (MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.38).

Bem-Estar dos Estados Unidos (HEW Report – Health, Education, and Welfare) e constantes do Records, Computers, and the Rights of Citizens[480], que exerceram um papel significativo na elaboração de leis de privacidade nos Estados Unidos.

Além das legislações locais, surgiram importantes marcos internacionais – já avançando para as dimensões seguintes – que ratificam a privacidade sob o viés da proteção de dados pessoais. Aqui podem ser citados os importantes textos da Convenção 108 do Conselho da Europa (1981), as Diretrizes da OCDE para proteção da privacidade e dos fluxos transfronteiriços de dados pessoais (1980) e a Diretiva Europeia 95/46/CE relativa à proteção de dados pessoais (1995).

A *segunda dimensão* da tutela de proteção de dados pessoais suscita uma controvérsia bastante interessante, relacionada à efetividade do consentimento do cidadão e do real exercício de sua liberdade de escolha, em um contexto no qual a não disponibilização dos dados pode acarretar a sua exclusão social. Nesse sentido informa Laura Schertel Mendes:

> [...] na relação entre privados é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca de suas informações pessoais.[481]

Se na *primeira dimensão* o grande temor da população estava relacionado à formação de um banco de dados estatal centralizado (o que não chegou a se concretizar[482]), o destaque do medo da população, na segunda, desloca-se para o

---

[480] *Fair Practice Principles* (FIPPs): 1. There must be no personal data record-keeping systems whose very existence is secret. 2. There must be a way for a person to find out what information about the person is in a record and how it is used. 3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent. 4. There must be a way for a person to correct or amend a record of identifiable information about the person. 5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data. Tradução livre: *Fair Practice Principles* (FIPPs): 1. Não deve haver sistemas de guarda de registros de dados pessoais cuja própria existência seja secreta. 2. Deve haver uma maneira de uma pessoa descobrir quais informações sobre ela estão em um determinado registro e como são usadas. 3. Deve haver uma maneira de uma pessoa impedir que a informação sobre ela que tenha sido obtida para um propósito seja usada ou disponibilizada para outros fins sem o consentimento da pessoa. 4. Deve haver uma maneira de uma pessoa corrigir ou emendar um registro de informações identificáveis sobre a pessoa. 5. Qualquer organização que crie, mantenha, utilize ou divulgue registros de dados pessoais identificáveis deve assegurar a confiabilidade dos dados para o uso pretendido e deve tomar precauções para evitar usos indevidos dos dados.

[481] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p. 40-41.

[482] Segundo Laura Schertel Mendes, isso, no entanto, deve-se menos às reivindicações sociais e mais à transformação tecnológica que possibilitou que unidades organizacionais, tanto do governo como da iniciativa privada, utilizassem processamento de dados eletrônicos de modo descentralizado[482]. Essa circunstância levou à proliferação da quantidade de bancos de dados existentes e, consequentemente, expôs a fragilidade da regulamentação das normas de primeira geração que estabeleciam procedimentos em detrimento de direitos. Deste modo, ficou latente a necessidade de alteração das regras e é aqui, justamente, que se adentra à segunda

temor da existência de milhares de bancos de dados descentralizados, mas conectados em rede, tanto públicos como privados.

A *terceira dimensão* de tutela de proteção de dados pessoais é marcada pela decisão paradigmática, já comentada nesse trabalho, emanada do Tribunal Constitucional alemão, de 1983, que declarou a inconstitucionalidade de parte da Lei do Censo.

A principal diferença em relação à dimensão anterior é que o cidadão passa a ter um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como a opção entre ´tudo ou nada´.[483]

Porém, segundo Laura Schertel Mendes, provou-se não ser factível o ideal participativo dos cidadãos no controle das informações pessoais:

> Mais uma vez, no entanto, pode-se dizer que o ideal participativo dos cidadãos no controle das informações pessoais, consubstanciado na ideia de autodeterminação informativa, provou-se não ser factível no mundo real. Isso porque, semelhante ao que ocorreu com a segunda geração das normas de proteção de dados pessoais, os cidadãos não estavam dispostos a arcar com os altos custos monetários e sociais de exercer o seu direito e, por consequência, ser privado do acesso a bens e serviços ou a benefícios. [...] Ademais, tendo em vista que o consentimento do indivíduo autorizava o processamento dos dados pessoais, em caso de violação ao seu direito à privacidade, não teria ele condições de lutar pela reparação daquela violação, na medida em que tinha consentido para o tratamento de seus dados[484].

A *quarta dimensão* de tutela de proteção de dados pessoais surge como fase de busca para resolver problemas dos períodos anteriores. Segundo Laura Schertel Mendes, isso é feito por meio de duas soluções:

> Primeiramente, algumas das normas tiveram o objetivo de fortalecer a posição dos indivíduos, tornando mais efetivo o seu autocontrole sobre os dados pessoais. Isso foi possível, por exemplo, a partir da previsão de "*no fault compensation"* para reclamações individuais a respeito da violação à

---

geração das normas e proteção de dados pessoais. Tais normas buscavam tratar prioritariamente do direito à privacidade, em vez de procedimentos. A temática da proteção de dados pessoais passa a se associar diretamente ao direito à privacidade, às liberdades negativas e à liberdade individual em geral. Como consequência, a privacidade informacional é inserida nos textos das Constituições da Áustria, Espanha e Portugal. (MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.39-40). Além disso, as leis de proteção de dados da Áustria, da França, da Dinamarca e da Noruega integram a segunda geração de tutela de proteção de dados pessoais.

[483] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.41-42. Segundo a autora, são exemplos dessa fase as leis dos Estados alemães após a decisão do Tribunal Constitucional, a emenda à lei Federal de Proteção de Dados Pessoais alemã de 1990, a emenda da lei da Áustria de 1986, a alteração da lei da Noruega e a previsão constitucional da proteção de dados pessoais da Holanda

[484] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.42-43.

> proteção de dados pessoais, que se deu na Alemanha, com a emenda à Lei Federal de Proteção de Dados alemã, sendo que nome semelhante já existia na legislação da Noruega em menor extensão. Em outros casos, as normas retiraram da esfera do controle do indivíduo determinados assuntos, por compreenderem que alguns temas relativos aos dados pessoais são tão relevantes para o citado que merecem ser extremamente protegidos, não podendo estar na esfera de disposição individual. Tal pode ser observado na proibição, total ou parcial, imposta para o tratamento dos dados pessoais considerados sensíveis, que são aqueles cujo tratamento tem grande potencial de acarretar discriminação, tais como os dados relativos à etnia, opção sexual, opinião política e religião[485].

É na *quarta dimensão*, ainda, que surgem, em vários países, normas setoriais complementares às normas gerais sobre a proteção de dados:

> Tal fato tem como finalidade ampliar a proteção do indivíduo nos diversos setores em que é possível o tratamento dos seus dados pessoais, de modo que a legislação possa contemplar as diversas especificidades setoriais existentes. Assim, na maioria dos países europeus, percebe-se a existência de uma regulamentação geral sobre proteção de dados, mas com leis setoriais suplementares[486].

A essa altura parece inquestionável a vinculação entre a própria liberdade e a dignidade do ser humano e a conseguinte limitação imposta por cada indivíduo sobre o poder informático[487]. Daí o Informe Bangemann[488] ter expressado a necessidade inevitável de proteger a intimidade dos sujeitos mediante o tratamento eletrônico do dado. Fica claro, portanto, da análise evolutiva das normas de proteção de dados, que essa disciplina percorreu uma transformação rápida e dinâmica, acompanhando o compasso das modificações tecnológicas. Ademais, conforme observa Laura Schertel Mendes, é notável como ao longo do desenvolvimento da disciplina de proteção de dados pessoais, "fortaleceu-se o conceito da tutela da personalidade do cidadão, tanto na sua vertente da proteção da autodeterminação como na vertente de proteção dos dados sensíveis"[489].

---

[485] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.43.
[486] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.44.
[487] CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.43.
[488] O Informe Bangemann diz respeito à decisão da União Europeia de intervir no processo de criação da Sociedade da Informação. O Conselho Europeu solicitou que um grupo de personalidades elaborasse um informe para sua reunião de 24-25 de junho de 1994, sobre as medidas que devem estudar a comunidade europeia e seus Estados membros para estabelecer infraestruturas no âmbito da informação. O Informe Bangemann foi emitido como Recomendação no dia 26 de maio de 1994.
[489] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.44.

Nessa toada, o documento “Resolución sobre Europa e sobre a sociedade global da informação – recomendações ao Conselho Europeu” a respeito de uma comunicação da Comissão das Comunidades Europeias intitulada "Europa en marcha hacia la sociedad de la información. Plan de actuación" (COM (94)0347 - C4-0093/94), coloca como uma consequência social e um direito dos cidadãos:

> subraya que el principal objetivo de las autoridades políticas en relación con la emergencia de la sociedad de la información debe ser permitir que los individuos controlen la información y puedan utilizarla con fines individuales o colectivos, como receptores y como autores, en vez de utilizar la información par controlar a los indivíduos[490].

Nesse contexto é aprovada a Diretiva Europeia sobre proteção de dados pessoais de 1995, como produto da evolução dimensional pela qual passou a disciplina da proteção de dados pessoais na Europa. Essa Diretiva n.45/96 possui como foco central a participação do indivíduo no processo de tratamento dos dados pessoais, condicionando o consenso expresso e informado do indivíduo no tratamento de dados sensíveis.

A Diretiva 95/46 foi adotada, segundo a Comissão Europeia, com dois objetivos: assegurar o direito fundamental à proteção de dados e garantir a livre circulação de dados pessoais entre os Estados membros[491].

No ano seguinte, a frase “os indivíduos devem controlar a informação e não a informação controlar os indivíduos” foi cravada no Informe do Parlamento Europeu com Recomendações ao Conselho Europeu (documento Resolución sobre Europa e sobre a sociedade global da informação – recomendações ao Conselho Europeu – Plan de actuación – COM (94)0347-C4-0093/94):

> subraya que el principal objetivo de las autoridades políticas en relación con la emergencia de la sociedad de la información debe ser permitir que los individuos controlen la información y puedan utilizarla con fines individuales o colectivos, como receptores y como autores, en vez de utilizar la información para controlar a los indivíduos[492].

A *quinta dimensão*, esta ainda não assim definida pela doutrina, pode ser atribuída à fase em que o tratamento do dado pessoal está atrelado ao uso massivo de algoritmos, inteligência artificial e *machine learning*, desafiando as autoridades

[490] Disponível em: <http://www.europarl.europa.eu>. Acesso em: 23 ago. 2018.
[491] EUROPEAN Commission. Impact Assessment (including annexes) accompanying the proposed Regulation and the proposed Directive, SEC (2012) 72 final. Disponível em: <https://eur-lex.europa.eu/. Acesso em: 18 out. 2018, p.7
[492] Disponível em: <http://www.europarl.europa.eu/>. Acesso em: 23 ago. 2018.

europeias a repensar a regulação existente no início do século XXI. Não à toa países europeus, e também de outros lugares do mundo, estão criando cargos governamentais voltados apenas ao assunto da inteligência artificial, a exemplo da Alemanha e dos Emirados Árabes[493].

3.6 O caminho percorrido em âmbito da proteção de dados pessoais no continente europeu nas primeiras décadas do século XXI

É certo que a proteção de dados pessoais sempre foi uma pauta deveras importante para o bloco europeu. Além dos documentos históricos mencionados, quais sejam, a Convenção 108 do Conselho da Europa (1981) e as Diretrizes da OCDE[494] para proteção da privacidade e dos fluxos transfronteiriços de dados pessoais (1980), foi elaborada, em 2000, a histórica Carta de Direitos Fundamentais da União Europeia, que reconheceu a proteção de dados como um direito autônomo. Segundo Stefano Rodotà, este pode ser considerado o último ponto de uma longa evolução, que culmina por separar a privacidade da proteção de dados[495]:

> A distinção entre o direito ao respeito da vida privada e familiar e o direito à proteção dos dados pessoais não é bizantina. O direito ao respeito da vida privada e familiar reflete, primeiro e principalmente, um componente individualista: este poder basicamente consiste em impedir a interferência na vida privada e familiar de uma pessoa. Em outras palavras, é um tipo de proteção estático, negativo. Contrariamente, a proteção de dados estabelece regras sobre os mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas – i.e. é um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos. Adicionalmente, a supervisão e outros poderes não são somente conferidos às pessoas interessadas (os sujeitos de dados), mas são também entregues a uma autoridade independente[496]. A proteção não é mais deixada somente aos sujeitos de dados, uma vez que existe um órgão público permanente responsável por isso. É de fato o fim da linha de um longo processo evolutivo experimentado pelo conceito de privacidade – de uma definição original como o direito de ser deixado em paz, até o direito de

[493] Em outubro de 2017 foi criado o cargo de Ministro de Estado para Inteligência Artificial. A primeira pessoa a assumir o cargo foi Omar Bin Sultan Al Olama, de 27 anos de idade. Na Alemanha, em junho de 2017, o Ministério dos Transportes e de Infraestrutura Digital (*Bundesministerium für Verkehr und digitale Infrastruktur),* por sua Comissão Ética, publicou Guia para o uso de carros automatizados. Disponível em: <https://www.bmvi.de/SharedDocs/EN/Documents/G/ethic-commission-report.pdf?__blob=publicationFile>. Acesso em: 10 jan. 2019.

[494] Versão de 1980. Disponível em: <http://www.oecd.org/>.

[495] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.16.

[496] A lei brasileira que cria um marco legal de proteção de dados no país recebeu veto presidencial quanto à criação de autoridade nacional de dados. Há quem argumente que a lei, sem a devida autoridade, não terá a efetividade necessária para estabelecer um sistema de proteção de dados no país. Aguarda-se, portanto, uma "solução" ao problema formado. O argumento do veto não foi de ordem material. Segundo o presidente, o legislativo não teria competência para criar órgão dentro da estrutura do Executivo, nos moldes previstos pela Constituição Federal.

> controle sobre as informações de alguém e determinar como a esfera privada deve ser construída[497].

Ademais, com base na Carta de Direitos Fundamentais da União Europeia, Stefano Rodotà reconheceu que se atingira a verdadeira reinvenção da proteção de dados – não somente porque ela estava expressamente considerada como um direito fundamental autônomo, mas também porque se tornou uma ferramenta essencial para o livre desenvolvimento da personalidade[498].

A aparição do ambiente digital moveu, também, os pilares da dignidade humana. "A informação concernente à vida particular dos indivíduos é enfrentada, cada vez mais, com maior energia, para as transmissões *on-line* por redes telemáticas como internet; o que comporta uma potencial agressão à esfera privada da pessoa"[499].

No Tratado que estabelece uma Constituição para a Europa (outubro/2004), foi reconhecida a proteção de dados como um direito autônomo, destacado da privacidade (artigos 7º, II e 8º, II), a exemplo do que já havia sido reconhecido na Carta dos Direitos Fundamentais da União Europeia, em seus artigos 7º e 8º.

Não se pode deixar de mencionar, também, importante documento aprovado em 2009. Trata-se dos *Standards* Internacionais sobre Proteção de Dados Pessoais, aprovado em Madri, por 80 autoridades, na 31ª Conferência Internacional de Autoridades de Proteção de Dados. Segundo analisa Laura Schertel Mendes, o principal aspecto convergente se relaciona ao paradigma do controle, que "prevê princípios gerais e mecanismos legais para que seja atribuída aos indivíduos maior liberdade de controle sobre a informação coletada, armazenada, processada e disseminada[500]".

No mesmo ano (2009) entra em vigor o Tratado de Lisboa[501], no qual consta, em seu artigo 16, que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito".

---

[497] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.17.
[498] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.17.
[499] CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007, p.55.
[500] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.44.
[501] O Tratado de Lisboa entrou em vigor em 1 de dezembro de 2009. Foi assinado em Lisboa, em 13 de dezembro de 2007 e é composto pelos dois principais Tratados da UE revistos: o Tratado da União Europeia

Em 2010, a Comissão Europeia publicou um comunicado[502] sobre os novos desafios em matéria de proteção de dados pessoais. Ao passo que reconheceu que a Diretiva de Proteção de Dados de 1995 constituira um marco na história da proteção de dados pessoais na União Europeia, cujos princípios consagrados permaneciam válidos, também reconheceu que após quinze anos, a rapidez dos avanços tecnológicos e da globalização alterou profundamente o mundo e trouxe novos desafios à proteção dos dados pessoais.

As tecnologias como as redes sociais, com centenas de milhões de membros em todo o mundo, permitiam – e ainda permitem – que as pessoas partilhassem facilmente informações acerca dos seus comportamentos e preferências, tornando-as públicas e globalmente acessíveis numa escala sem precedentes. Além disso, também marcava a súbita e recente evolução tecnológica e a larga utilização da computação em nuvem (em que o software, os recursos partilhados e as informações em servidores remotos também colocavam em risco os dados ali armazenados).

Simultaneamente, as formas de coletar dados pessoais se tornaram mais elaboradas e difíceis de detectar. A utilização de ferramentas sofisticadas, a onipresença de dispositivos móveis e de sensores físicos que transmitem informações de localização geográfica e o crescente uso de tecnologias de mineração de dados que permitem a agregação e a análise de dados de múltiplas fontes colocou em xeque a regulamentação em vigor à época. Nesse cenário, a pedra de toque estava ligada a práticas de *profiling* e *data mining,* enrebustecidos com o uso de algoritmos, inteligência artificial e *machine learning.*

Tudo isto suscitou, inevitavelmente, questionamentos se a legislação de proteção de dados da União Europeia ainda teria condições suficientes para enfrentar plena e eficazmente estes novos desafios da época.

Tanto assim que as diretrizes relativas à proteção de dados pessoais e ao fluxo de dados transfronteiriços da OCDE de 1980 foram revisitadas, de modo que, em que pese grande parte dos conceitos das diretrizes originais ter sido mantida, a atualização de 2013 trouxe novidades interessantes: programas gerenciais de privacidade, a serem implementados pelo controlador, visando adotar medidas de

---

(TUE) e o Tratado que institui a Comunidade Europeia (designado Tratado sobre o Funcionamento da União Europeia – TFUE), além de vários protocolos e declarações.

[502] EUROPEAN Commission Communication. 'A comprehensive approach on personal data protection in the European Union' COM (2010) 609 final. Disponível em: <https://eur-lex.europa.eu/>. Acesso em: 05 out. 2018.

segurança e realizar análise de risco do processamento de dados aos indivíduos (*privacy risk assessment* art. 15, a, III); a possibilidade de prever notificação em caso de vazamento de dados *(data breach notification* – art. 15,c) [503].

Na Comissão Europeia, presenciava-se um processo de revisão do quadro normativo vigente, promovendo conferências, consulta pública e vários estudos sobre a matéria, em especial junto ao Grupo de Trabalho do Artigo 29º[504], que emitiu dois significativos estudos (WP 168 e WP 173). As conclusões confirmaram que os princípios nucleares da Diretiva de 1995 deveriam ser preservados. Contudo, chegou-se ao entendimento da existência de várias questões problemáticas, que representavam desafios específicos, *inter alia*: equacionar o impacto das novas tecnologias; reforçar a vertente de protecção de dados do mercado interno; equacionar a globalização e melhorar as transferências de dados internacionais; obter um quadro institucional mais firme para a aplicação efetiva das normas de proteção de dados, de modo que o papel das autoridades deveria ser reforçado.

Na redação do comunicado da Comissão Europeia de 2010 constou:

> Tal como a tecnologia, a forma como os nossos dados pessoais são utilizados e partilhados na nossa sociedade está constantemente a mudar. Para o legislador, o desafio consiste em estabelecer um quadro normativo que resista à passagem do tempo. No final do processo de reforma, as normas de protecção de dados devem continuar a garantir, durante várias gerações, um elevado nível de protecção e segurança jurídica aos particulares, às administrações públicas e às empresas. Independentemente da complexidade da situação ou do grau de sofisticação da tecnologia, as normas que as autoridades nacionais devem aplicar e que as empresas e os criadores de tecnologia devem cumprir têm de ser claras. Para as pessoas singulares é também importante que sejam claros os direitos que lhes assistem[505].

Além disso, em 2012, a Comissão Europeia se manifestou retificando: “o principal objetivo da tutela jurídica em matéria de protecção de dados é garantir um elevado nível de proteção de dados para todas as pessoas na UE”. E no mesmo documento constou: “todos estes objetivos, que permanecem totalmente válidos

---

[503] THE OECD PRIVACY FRAMEWORK. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 29 nov. 2018.

[504] O Grupo de Trabalho do Artigo 29º é um órgão consultivo composto por um representante dos Estados membros, das autoridades de protecção de dados, da Autoridade Europeia para a Protecção de Dados (AEPD) e da Comissão (sem direito de voto), assegurando esta última também o secretariado do grupo. Disponível em: <http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm>. Acesso em: 29 nov. 2018.

[505] Item 3 do Comunicado European Commission Communication, ‘A comprehensive approach on personal data protection in the European Union’ COM (2010) 609 final. Disponível em: <https://eur-lex.europa.eu>. Acesso em: 05 out. 2018.

hoje, foram apenas parcialmente alcançados no quadro legal atual[506]. Mostrava-se de forma bastante clara a inclinação para fortalecer os direitos do indivíduo dentro da economia digital.

Surgem, assim, novos desafios para a proteção de dados pessoais que não podiam ser previstos em 1995, quando a Diretiva foi adotada, ligados à evolução tecnológica, em especial ao desenvolvimento da internet. Os dados pessoais poderiam ser processados mais facilmente e numa escala sem precedentes tanto por empresas privadas como por autoridades públicas, aumentando, assim, os riscos para os direitos dos indivíduos e, desafiando a capacidade de se manter o controle sobre seus próprios dados.

No documento *Impact Assessment accompanying the proposed Regulation and the proposed Directive*, *SEC* (2012), elaborado pela Comissão Europeia, expôs-se a dificuldade de os indivíduos exercerem efetivamente seus direitos de proteção a dados pessoais:

> There is a strong likelihood that the current difficulties in maintaining control over one's own data and in effectively exercising data protection rights will increase, given the large and growing volume of personal data collected and the ease with which it can be processed and communicated thanks to new technologies. Individuals are likely to encounter increasing problems with the protection of their personal data, or refrain from fully using the internet as a medium for communication and commercial transactions. The 75% of individuals currently not feeling in complete control of their personal data on social networking sites (and 80% when shopping online) is not likely to decrease without regulatory intervention which can support the confidence of individuals. Such a development could counteract the key performance target of the Digital Agenda for Europe for 50 % of the population to buy online by 2015. Individuals are also likely to face increasing difficulties in knowing what their data protection rights are when their data are processed by companies or public authorities involved in cross border data processing, in particular with the development of cloud computing. They would increasingly be unable to foresee the scope of their data protection rights in order to adapt their behaviour[507].

---

[506] EUROPEAN Commission. Impact Assessment (including annexes) accompanying the proposed Regulation and the proposed Directive, SEC (2012) 72 final. Disponível em: <https://eur-lex.europa.eu>. Acesso em: 18 out. 2018, p.10-11.

[507] EUROPEAN Commission. Impact Assessment accompanying the proposed regulation and the proposed Directive, SEC (2012) 72 final. Disponível em: <https://eur-lex.europa.eu/>. Acesso em 18 out. 2018, p.37. Tradução livre: Existe uma forte probabilidade de que as atuais dificuldades em manter o controle sobre os próprios dados e em exercer efetivamente os direitos de proteção de dados aumentem, dado o grande e crescente volume de dados pessoais coletados e a facilidade com que podem ser processados e comunicados graças a novas tecnologias. É provável que os indivíduos encontrem problemas crescentes com a proteção de seus dados pessoais ou se abstenham de usar totalmente a Internet como meio de comunicação e para transações comerciais. Os 75% de indivíduos que atualmente não se sentem no controle completo de seus dados pessoais em sites de redes sociais (e 80% ao fazer compras on-line) provavelmente não diminuirão sem que sobrevenha uma intervenção regulatória que possa apoiar a confiança dos indivíduos. Tal desenvolvimento poderia contrariar a meta de desempenho da Agenda Digital para a Europa para 50% da população comprar on-line até 2015. As pessoas também provavelmente enfrentarão dificuldades crescentes em saber quais são seus direitos de proteção de dados quando seus dados são processados pelas empresas ou autoridades públicas envolvidas no processamento de dados transfronteiriços, em particular com o desenvolvimento da computação

O resultado desse processo de revisão da legislação, por parte da Comissão Europeia, culminou na publicação de sugestão de texto de regulamento, em janeiro de 2012, o qual foi discutido e caminhou para a aprovação de um novo Regulamento Europeu.

Assim, em 12/03/2014, o novo Regulamento Europeu de proteção de dados e privacidade foi votado no Parlamento europeu com 621 votos a favor, 10 contra e 22 abstenções. Em 27/07/2015, a Autoridade Europeia para a Proteção de Dados apresentou sugestão de texto final para o novo Regulamento europeu, para então, em 15/12/2015, o Parlamento, Conselho e Comissão Europeia chegarem a um acordo sobre o Regulamento (UE) 2016/679, atual Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (UE), comumente designado, no Brasil, pela sigla em inglês GDPR (General Data Protection Regulation). Este Regulamento estabelece as regras pertinentes ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na União Europeia, com a ressalva de que não se aplica ao tratamento de dados pessoais de pessoas falecidas ou coletivas. O GDPR será analisado mais detalhadamente em momento oportuno nesta pesquisa.

Mais recentemente, a Convenção n.108 foi modernizada, após sete anos de intensos trabalhos[508]. Na 128ª Sessão Ministerial do Comité de Ministros do Conselho da Europa, realizada em Elsinore, na Dinamarca, em 18 de maio de 2018, foi adotado o Protocolo que altera a Convenção relativa à proteção das pessoas quanto ao processamento automático de dados pessoais, de 1981[509]. A nova versão da convenção é referida como “Convenção 108+”.

---

em nuvem. Eles seriam cada vez mais incapazes de prever o alcance de seus direitos de proteção de dados, a fim de adaptar seu comportamento.

[508] O trabalho de modernização começou com a preparação de um relatório destinado a identificar áreas em que a Convenção 108 precisaria ser modernizada para enfrentar novos desafios, e uma consulta multilateral foi lançada pelo Secretário-Geral por ocasião da 5ª edição do dia de proteção de dados e o trigésimo aniversário da Convenção 108, em 28 de janeiro de 2011. Essa consulta pública permitiu que pessoas e instituições interessadas enviassem seus comentários e ideias sobre a modernização da Convenção 108. A primeira fase do trabalho foi confiada ao Comitê da Convenção 108 e um acordo sobre as propostas foi alcançado na 29ª Reunião Plenária do Comitê em 27-30 de novembro de 2012. Essas propostas foram posteriormente analisadas em 2013 e 2014 por um comitê intergovernamental (comitê ad hoc sobre proteção de dados – CAHDATA). Seu trabalho foi finalizado em 16 de junho de 2016. (CONSELHO DA EUROPA. Disponível em: <https://www.coe.int/en/web/data-protection/background-modernisation>. Acesso em: 08 nov. 2018. A última fase do trabalho foi realizada ao nível do Comitê de Ministros. O Comitê de Ministros e o seu grupo de relatores para a cooperação judiciária (GR-J) analisaram as propostas do CAHDATA de 2016 a 2018 e adotaram o protocolo de alteração em 18 de maio de 2018.

[509] Tabela comparativa entre a redação de 1981 e a atual elaborada pelo Conselho da Europa. Disponível em: <https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958> . Acesso em: 29 nov. 2018.

Sua modernização buscou atingir dois objetivos principais: enfrentar os desafios resultantes do uso de novas tecnologias de informação e comunicação e fortalecer a efetiva implementação da Convenção[510].

Aberta para ratificação em 10 de outubro de 2018, foi assinada por 20 países[511] nessa mesma data. Dentre eles, o Uruguai, que não pertence ao Conselho da Europa[512].

A Europa além de grande produtora de normas na disciplina de proteção de dados, também exerce uma significativa influência em vários outros países no mundo, na escolha do sistema de regulação a ser adotada. A possibilidade de países em todo mundo poderem aderir à Convenção 108+, demonstra o papel de incentivo dirigido às demais nações para tutela dos dados pessoais.

3.7 Regulamento Geral de Proteção de Dados (GDPR)

Na evolução da proteção de dados no velho continente, ganha destaque e, por isso, trataremos em item separado o novo Regulamento Europeu, advindo de negociações do trílogo[513], que entrou em vigor em 25 de maio de 2018, seja porque foi a norma inspiradora do legislador brasileiro, seja porque a Europa é considerada celeiro de replicação como modelo de *gold standards* das regras de privacidade e proteção de dados ao mundo. Dito isso, importante também situar que, embora não seja objetivo desse trabalho tratar de detalhes dogmáticos da GDPR, seguir-se-á com uma análise geral do regulamento, sob o viés dogmático. O objetivo é ter presente o produto final – até esse momento, pelo menos – da travessia e da evolução do direito à privacidade, percorridos desde a sua gênese no final do século

[510] CONSELHO DA EUROPA. The modernised Convention 108: novelties in a nutshell. Disponível em: <https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8>. Acesso em: 08 nov. 2018.

[511] Áustria, Bélgica, Bulgária, República Tcheca, Estônia, Finlândia, França, Alemanha, Irlanda, Letônia, Lituânia, Luxemburgo, Mônaco, Holanda, Noruega, Portugal, Espanha, Suécia, Reino Unido, Uruguai. A atualização com os países que aderiram e quem venham futuramente aderir, além de eventuais reservas efetuadas pelos respectivos países pode ser consultada em site pertencente ao Conselho da Europa. (Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures. Acesso em: 29 nov. 2018).

[512] Ao total, hoje, o Comitê da Convenção 108 reúne os 53 países que se comprometeram a respeitar e implementar os princípios da Convenção. O Comitê também inclui países na qualidade de observadores, autoridades de proteção de dados de países que não são membros da Convenção, organizações internacionais e organizações não-governamentais. No total, cerca de 70 países (2018) participam nos trabalhos do Comitê, que se reúne em sessão plenária duas vezes por ano em Estrasburgo. O Comitê oferece, assim, um fórum único de intercâmbio e cooperação. O Brasil foi admitido como observador do Comitê da Convenção 108 em 12 de outubro de 2018, mesma data que a Comissão de Proteção de Dados do Gabão se juntou ao Comitê.

[513] As "negociações do trílogo" se referem a uma série de reuniões entre a Comissão Europeia, o Conselho e o Parlamento, visando adotar um texto final para o GDPR. Para aprofundar a base jurídica do trílogo: PROUST, Oliver. Unravelling the mysteries of the GDPR trilogues'. In: **Privacy, security and information law**, 2015. Disponível em: <http://privacylawblog.fieldfisher.com>. Acesso em: 15 nov. 2018.

XIX, nos Estados Unidos, até 2016, na Europa, quando foi aprovado o novo regulamento, sob à luz das práticas e tecnologias atuais e amplamente aplicadas, tais quais *data mining, profiling*, *big data, IoT* e *inteligência artificial*. O regulamento foi considerado o mais ambicioso esforço, até hoje já realizado, para garantir os direitos da pessoa humana no mundo digital, conforme se verá adiante.

O atual Regulamento introduz novos direitos no texto normativo, tais quais o direito de ser esquecido[514] e a portabilidade de dados[515], além de impor novas responsabilidades aos controladores de dados, incluindo proteção de dados *by design* e *by default* (artigo 25).

Embora não sejam vinculantes, foram inseridos 173 itens "considerandos", cem a mais em comparação à Diretiva 95/46, instruída com 72 itens no preâmbulo da norma. Ademais, enquanto a Diretiva 95/46 trazia oito itens na sua parte de definições (artigo 2º, Diretiva 95/46), o GDPR traz o dobro, ou seja, 16 itens (artigo

[514] Artigo 17. Direito ao apagamento dos dados (direito a ser esquecido): 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6º, n.1, alínea a), ou do artigo 9º, n.2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21, n.1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21, n.2; d) Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado membro a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8º, n.1. 2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos. 3. Os n.1 e 2 não se aplicam na medida em que o tratamento se revele necessário: a) Ao exercício da liberdade de expressão e de informação; b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9º, n.2, alíneas h) e i), bem como do artigo 9º, n.3; d) Para fins de arquivo de interesse público, investigação científica, histórica ou estatísticos, nos termos do artigo 89, n.1, na medida em que o direito referido no n.1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial. Sobre o direito a ser esquecido, ver também o Considerando 65 do GDPR.

[515] Artigo 20. Direito de portabilidade dos dados: 1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se: a) O tratamento se basear no consentimento dado nos termos do artigo 6º, n.1, alínea a), ou do artigo 9º, n.2, alínea a), ou num contrato referido no artigo 6º, n.1, alínea b); e b) O tratamento for realizado por meios automatizados. 2. Ao exercer o seu direito de portabilidade dos dados nos termos do n.1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível. 3. O exercício do direito a que se refere o n.1 do presente artigo aplica-se sem prejuízo do artigo 17. Esse direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. 4. O direito a que se refere o n.1 não prejudica os direitos e as liberdades de terceiros. Sobre o direito a ser esquecido, vide, ainda, o Considerando 68 do GDPR: [...] os responsáveis pelo tratamento de dados deverão ser encorajados a desenvolver formatos interoperáveis que permitam a portabilidade dos dados. [...]

3º, GDPR), cujo simples e mero detalhe aponta para a importância da sofisticação do ecossistema de dados, que adquiriu a sociedade nesse ínterim de tempo. Sobre o caráter não vinculante dos "considerandos", esclarecem Sandra Wachter, Brent Mittelstadt e Luciano Floridi: "recitals provide guidance on how to interpret the Articles, but are not themselves legally binding"[516].

Da análise do Regulamento, e compactuando com Ira Rubinstein, percebe-se que o texto está centrado, principalmente, no aumento da transparência[517] [518]como princípio cardeal do início ao fim de suas regras.

Para além da transparência, e em intersecção com esse princípio, é possível dizer que a pedra angular do Regulamento Geral de Proteção de Dados (GDPR) é a noção de confiança. Segundo Giovanni Buttarelli:

> It aims to entrench privacy on the ground and allows different sectors to contribute to new norms and best practices appropriate to specific circumstances. Its cornerstone is the notion of trust: trust in data controllers to treat personal information responsibly, and trust that the rules will be effectively enforced. It will be incumbent on Europe's independent data protection authorities, working through a reinforced cooperation facility called the European Data Protection Board, to foster that trust and accountability, by being transparent and accessible to stakeholders and efficient in providing relevant and timely guidance on compliance[519].

Sob outro enfoque, uma das consequências indiretas do Regulamento Geral de Proteção de Dados (GDPR), segundo Giovanni Buttarelli, Supervisor de Proteção de Dados na União Europeia[520], foi elevar o nível das leis de proteção de dados em todo o mundo[521]. De fato, isso se confirma em relação ao cenário

---

[516] FLORIDI, Luciano; WACHTER, Sandra; MITTELSTADT, Brent. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, v.7, 2.ed. 1 maio 2017, p.80. Disponível em: <https://doi.org/10.1093/idpl/ipx005>. Acesso em: 16 out. 2018. Tradução livre: os considerandos fornecem orientações sobre como interpretar os artigos, mas não são vinculantes.

[517] RUBINSTEIN, Ira S. Big data: the end of privacy or a new beginning? **International Data Privacy Law**, v.3, 2.ed. 1 maio 2013, p.74-87. Disponível em: <https://doi.org/10.1093/idpl/ips036>. Acesso em: 18 out. 2018.

[518] Vide, ainda, sobre transparência, artigos 5, 12, 14, alínea 2; artigo 40 e artigo 88, além dos Considerandos 39, 58, 60, 70 e 100, todos do Regulamento Geral de Proteção de Dados (GDPR).

[519] BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. **International Data Privacy Law**, v.6, 2.ed., 01 maio 2016, p.77-78. Disponível em: <https://doi.org/10.1093/idpl/ipw006>. Acesso em: 18 out. 2018. Tradução livre: Sua pedra angular é a noção de confiança: confiar nos controladores de dados para tratar as informações pessoais com responsabilidade e confiar que as regras serão efetivamente aplicadas. Competirá às autoridades independentes de protecção de dados da Europa, através de um mecanismo de cooperação reforçada denominado European Data Protection Board, promover essa confiança e responsabilização, ser transparente e acessível às partes interessadas e ser eficiente na orientação relevante e antecipada do cumprimento.

[520] Giovanni Buttarelli foi escolhido por uma decisão colegiada pelo Conselho e Parlamento Europeu, em 4 de dezembro de 2014, para um mandato de 5 anos.

[521] BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. **International Data Privacy Law**, v.6, 2.ed., 01 maio 2016, p.77-78. Disponível em: <https://doi.org/10.1093/idpl/ipw006>. Acesso em: 18 out. 2018.

legislativo brasileiro. Após a *vacatio legis* de dois anos, o GDPR entrou em vigor em 25 de maio de 2018, influenciando a casa legislativa brasileira para a necessidade de continuar a caminhada para a aprovação de uma lei local nessa área, o que ocorreu, finalmente, em 10 de agosto em 2018, quando o Senado aprovou o Projeto de Lei n. 53/2018, que já havia sido submetido à Câmara dos Deputados, seguindo para a sanção presidencial, em 15 de agosto do mesmo ano, com alguns vetos presidencias.

Às vésperas da aprovação, Giovanni Butarelli reconheceu que embora o texto pudesse não ser perfeito, consistia no mais ambicioso esforço, até hoje já realizado, para garantir os direitos da pessoa humana no mundo digital:

> we do not pretend that the final outcome is perfect, and in some ways it is quite far from the ideal. Nevertheless, we intend to be among the loudest champions of this reform, which is quite simply, and by a long way, the most ambitious endeavour so far to secure the rights of the individual in the digital realm for a generation[522].

Segundo o atual Supervisor de Proteção de Dados na União Europeia, o GDPR implica em duas importantes consequências estratégicas. A primeira diz respeito ao fato de o Regulamento Geral de Proteção de Dados (GDPR) configurar uma plataforma genuína para parcerias globais, dentro do cenário econômico no qual existem e surgem a todo momento modelos de negócios criativos e disruptivos, os quais utilizam dados pessoais. Mais da metade dos países do mundo possuem uma lei de proteção de dados. A consequência disso é a forte influência da abordagem europeia na regulação do assunto, gerando uma tendência para a ubiquidade global da proteção de dados[523].

---

[522] BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. **International Data Privacy Law**, v.6, 2.ed., 01 maio 2016, p.77-78. Disponível em: <https://doi.org/10.1093/idpl/ipw006>. Acesso em: 18 out. 2018. Tradução livre: [...] não pretendemos que o resultado final seja perfeito e, de certa forma, esteja muito longe do ideal. No entanto, pretendemos estar entre os mais contundentes defensores dessa reforma, que é simplesmente, e de longe, o mais ambicioso esforço até agora para garantir os direitos do indivíduo no mundo digital por uma geração.

[523] BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. **International Data Privacy Law**, v.6, 2.ed., 01 maio 2016, p.77-78. Disponível em: <https://doi.org/10.1093/idpl/ipw006>. Acesso em: 18 out. 2018. Sobre a primeira consequência trazida pelo GDPR, completa: The regulation promises a wider scope for cooperation between authorities and data controllers both within the EU and internationally. It should galvanise efforts for a more consistent standard contractual clauses, speed up the validation process for binding corporate rules, and help them dovetail with similar arrangements elsewhere in the world. I hope that the new provisions for codes of conduct, seals, certification, and accreditation processes will incentivise controllers inside and outside the EU to take the initiative in devising standards which are both business friendly and in the interests of individuals. Tradução livre: O regulamento promete um âmbito mais vasto de cooperação entre as autoridades e os responsáveis pelo tratamento dos dados, tanto na UE como em âmbito internacional. O regulamento deve galvanizar os esforços por cláusulas contratuais padrão mais consistentes, acelerar o processo de validação para vincular regras corporativas e ajudá-las a se adaptar a arranjos semelhantes em outras partes do mundo. Espero que as novas disposições relativas aos códigos de conduta, selos, certificação e

A segunda consequência, segundo Giovanni Buttarelli, é a proteção de dados não se apresentar mais como um “opcional”. O Tribunal de Justiça da União Europeia aplica estritamente estas regras, interpretando-as à luz da Carta dos Direitos Fundamentais da União Europeia e favorecendo os direitos e interesses do indivíduo acima de interesses empresariais, muito embora sejam razoáveis e legítimos: “The EU cannot retreat from these core values. Data protection authorities will have to be vigilant in monitoring implementation of the GDPR and applying the newly amplified range of possible sanctions in case of violation”[524].

O novo regulamento europeu obriga entidades públicas e privadas coletarem e processarem dados pessoais do funcionário ou consultor externo especialista em proteção de dados pessoais (artigo 37[525] da GDPR). É o Data Protection Officer

processos de acreditação incentivem os controladores, dentro e fora da UE, a tomarem a iniciativa de elaborar normas que favoreçam as empresas e os interesses dos indivíduos.

[524] Tradução livre: A União Europeia não pode recuar destes valores fundamentais. As autoridades de proteção de dados deverão ser vigilantes no monitoramento da implementação do GDPR, e aplicar a nova gama amplificada de possíveis sanções em caso de violação. BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. **International Data Privacy Law**, v.6, 2.ed., 01 maio 2016, p.77-78. Disponível em: <https://doi.org/10.1093/idpl/ipw006>. Acesso em: 18 out. 2018. E completa: The regulation promises a wider scope for cooperation between authorities and data controllers both within the EU and internationally. It should galvanise efforts for a more consistent standard contractual clauses, speed up the validation process for binding corporate rules, and help them dovetail with similar arrangements elsewhere in the world. I hope that the new provisions for codes of conduct, seals, certification, and accreditation processes will incentivise controllers inside and outside the EU to take the initiative in devising standards which are both business friendly and in the interests of individuals. O regulamento promete um âmbito mais vasto de cooperação entre as autoridades e os controladores de dados, tanto na UE como a nível internacional. Ele deve galvanizar os esforços por cláusulas contratuais padrão mais consistentes, acelerar o processo de validação de regras corporativas vinculantes e ajudá-las a se adaptar a arranjos semelhantes em outras partes do mundo. Espero que as novas disposições relativas aos códigos de conduta, selos, certificação e processos de acreditação incentivem os controladores, dentro e fora da UE, a tomarem a iniciativa de elaborar normas que favoreçam as empresas e os interesses dos indivíduos.

[525] Artigo 37. Designação do encarregado da proteção de dados. 1.O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que: a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional; b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º. 2. Um grupo empresarial pode também designar um único encarregado da proteção de dados desde que haja um encarregado da proteção de dados facilmente acessível a partir de cada estabelecimento. 3. Quando o responsável pelo tratamento ou o subcontratante for uma autoridade ou um organismo público, pode ser designado um único encarregado da proteção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão. 4. Em casos diferentes dos visados no n.1, o responsável pelo tratamento ou o subcontratante ou as associações e outros organismos que representem categorias de responsáveis pelo tratamento ou de subcontratantes podem, ou, se tal lhes for exigido pelo direito da União ou dos Estados membros, designar um encarregado da proteção de dados. O encarregado da proteção de dados pode agir em nome das associações e de outros organismos que representem os responsáveis pelo tratamento ou os subcontratantes. 5. O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39. 6. O encarregado da proteção de dados pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços. 7.O responsável pelo tratamento ou o subcontratante publica os contactos do encarregado da proteção de dados e comunica-os à autoridade de controlo.

(DPO), ou encarregado de proteção de dados, em português. Dentre suas funções estão informar e aconselhar o responsável pelo tratamento ou o subcontratante – trabalhadores que tratem os dados – a respeito das suas obrigações; aconselhar, quando tal lhe for solicitado, sobre avaliação de impacto sobre a proteção de dados e controlar sua realização[526] e ser o elo com a autoridade nacional de proteção de dados (artigo 39, GDPR). Segundo levantamento do IAPP[527], o GDPR implica na criação de cerca de 75 mil novas vagas para DPO.

Quanto à sua aplicação, o Regulamento será aplicável em território europeu, mas produz efeitos a cidadãos e empresas localizados em outros países. A regra não é definida, portanto, pela cidadania do titular dos dados. Isso porque o Regulamento se aplica aos responsáveis pelo tratamento de dados situados na Europa e também àquelas empresas que, mesmo sem representação nesse continente, ofereçam serviços ao mercado europeu ou utilizem dados de pessoas que se encontrem na região, independentemente de sua nacionalidade. Tanto assim que a primeira notificação emitida pela autoridade britânica de proteção de dados, o Information Commissioner Office (ICO), após a vigência do Regulamento Geral de Proteção de Dados (679/2016/EU), foi emitido contra uma empresa localizada no Canadá[528], sem presença física no continente europeu.

Ademais, o novo Regulamento traz maior especificidade em relação aos requisitos do consentimento na coleta e tratamento de dados pessoais, em especial quanto às finalidades dessa coleta. Cai por terra a presunção de que o titular dos dados tenha autorizado o uso de suas informações, de maneira que mecanismos como o *opt out* não poderão mais ser utilizados. Em destaque existem casos específicos, como o tratamento de dados sensíveis (artigo 9), a transferência internacional de dados (artigo 49) e as decisões automatizadas (artigo 22). Em todos

[526] Segundo artigo 35 do GDPR, é obrigatória, em determinados casos, a "Avaliação de impacto" sobre a proteção de dados. Conforme alínea 1: Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. E a alínea 2 do mesmo artigo determina que "ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado.

[527] IAPP. **Preparing for the GDPR**: DPOs, PIAs, and Data Mapping. Disponível em: <https://iapp.org/media/pdf/resource_center/Preparing-for-GDPR_FINAL-1.0.pdf>. Acesso em: 02 nov. 2018.

[528] A empresa é a AggregateIQ Data Services Ltd, cujas atividades se relacionam à análise de dados em campanhas políticas. Consta que teria sido utilizada para o referendo relativo ao Brexit.

esses casos o consentimento exigido é mais rigoroso, devendo ser expresso por parte do titular dos dados.

Quando o tratamento for realizado com base no consentimento, o responsável deve dispor de um meio para demonstrar que o titular dos dados de fato consentiu para o tratamento dos seus dados pessoais[529]. Ainda, se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples[530].

Além disso, o Regulamento europeu garante que o consentimento possa ser retirado pelo titular dos dados a qualquer momento:

> A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar. (artigo 7º, alínea 3).

Tanto assim que o Regulamento europeu garante aos usuários em determinados casos o direito à limitação do tratamento de seus dados por parte das empresas e entidades (artigo 18). Por meio deste direito, o usuário pode, por exemplo, limitar a utilização dos seus dados enquanto houver equívocos em seus registros, ou seja, contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar sua exatidão.

Fica proibido condicionar a execução de contratos ou a prestação de serviços a uma autorização para a coleta e tratamento de dados não essenciais à sua execução, porquanto não seria livre o consentimento obtido após influência indevida sobre o contratante. Nesse sentido, é a alínea 4 do artigo 7º:

> Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.

[529] Artigo 7º, alínea 1.
[530] Artigo 7º, alínea 2.

Ponto bastante controvertido e que deverá ser desenvolvido pela doutrina e jurisprudência é a extensão e o significado de “necessário” (para a execução desse contrato).

Mais a mais, o GDPR exige requisitos especiais para o processamento de dados sensíveis segundo os considerandos 10 e 51 do Regulamento Geral sobre a Proteção de Dados[531]. Por sua vez, o artigo 9º, 1, assim rege sobre dados sensíveis:

> É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa[532].

[531] Considerando 10: [...] O presente regulamento também dá aos Estados membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais (“dados sensíveis”). Nessa medida, o presente regulamento não exclui o direito dos Estados membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais. Considerando 51: Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo “origem racial” no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados membros pode estabelecer disposições específicas de proteção de dados, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais.

[532] A alínea 2 do mesmo artigo excepciona a regra da alínea 1: O disposto no n.1 não se aplica se se verificar um dos seguintes casos: a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado membro previr que a proibição a que se refere o n.1 não pode ser anulada pelo titular dos dados; b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados membros ou ainda por uma convenção coletiva nos termos do direito dos Estados membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados; c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento; d) Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares; e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular; f) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da suas função jurisdicional; g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos

Porém, não obstante o olhar especial do atual Regulamento ao processamento de dados sensíveis, parte da doutrina afirma não estar claro se os requisitos propostos no texto normativo são suficientes para evitar o risco associado a esse processamento, porque esse risco não está claramente definido[533].

O consentimento envolvendo crianças, em razão dessa classe merecer proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais[534], segue regra especial[535]. No que respeito à oferta direta de serviços da internet às crianças, será considerado lícito se elas tiverem ao menos 16 anos. Antes dessa idade, o tratamento somente será lícito na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança. Ressalte-se que o marco de 16 anos pode ser modificado pelos Estados membros até o limite de 13 anos. Ainda quanto às crianças, dispõe o regulamento que a tomada de decisões

---

fundamentais e os interesses do titular dos dados; h) Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.3; i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional; j) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89, n.1, com base no direito da União ou de um Estado membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados. 3.Os dados pessoais referidos no n.1 podem ser tratados para os fins referidos no n.2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados membros ou de regulamentação estabelecida pelas autoridades nacionais competentes. 4.Os Estados-membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde.

[533] Nesse sentido: RHOEN, Michiel; FENG, Qing Yi. Why the 'computer says no': illustrating big data's discrimination risk through complex systems science. **International Data Privacy Law**, v.8, 2.ed., 1 maio 2018, p.140-159. Disponível em: <https://doi.org/10.1093/idpl/ipy005>. Acesso em: 17 out. 2018. Segundo os autores: Furthermore, the GDPR's clauses on the processing of – and profiling based on – sensitive data do not sufficiently account for the fact that individual data subjects are parts of complex systems, whose emergent properties betray sensitive traits from non-sensitive data. Tradução livre: "Além disso, as cláusulas do GDPR sobre o processamento – e o perfil com base em – dados sensíveis não explicam suficientemente o fato de indivíduos de dados individuais serem partes de sistemas complexos, cujas propriedades emergentes traem características sensíveis de dados não sensíveis".

[534] Considerando 38: As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados ao tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços oferecidos diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente à criança.

[535] Artigo 8º, GDPR

exclusivamente com base no tratamento automatizado não pode ser aplicado às crianças, mesmo sob as hipóteses permitidas em lei[536].

Consoante Elizabeth Sablich[537], o foco da GDPR repousa nos direitos de dados individuais. Assim, coloca, em teoria, os seres humanos no centro das práticas de proteção de dados pessoais. O processo de cumprimento de seus requisitos detalhados forçou as empresas a analisarem de perto os dados coletados, a utilidade, como são mantidos e compartilhados – o que provou não ser uma tarefa pequena. Embora a regulamentação da UE seja rígida em vários aspectos, ela pode ser mais sutil do que parece à primeira vista. Mais notavelmente, a exigência de que o consentimento seja explícito e dado livremente é frequentemente apresentada em relatórios resumidos proibindo a coleta de quaisquer dados pessoais sem o consentimento; na verdade, o regulamento permite outros motivos para coletar dados. Um dos efeitos da definição estrita de consentimento é enfatizar esses outros fundamentos. No entanto, algumas dessas sutilezas irão depender de como 40 reguladores diferentes em toda a UE aplicam a lei. Grupos de defesa europeus já estavam buscando reivindicações contra "les GAFAM" (Google, Amazon, Facebook, Apple, Microsoft) quando o regulamento entrou em vigor[538].

Além disso, o Regulamento Geral de Proteção de Dados (GDPR) propõe obrigações de transparência mais estritas e uma definição mais rígida de consentimento. Segundo o artigo 4º, alínea 11, por *consentimento* do titular dos dados entende-se “uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento”[539].

Consoante o considerando 32[540],

> o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral.

---

[536] Considerando 71, GDPR.
[537] SABLICH, Elizabeth. Why protecting privacy is a losing game today – and how to change the game. In: **Brooking**. Disponível em: <https://www.brookings.edu>. Acesso em 02 nov. 2018.
[538] Disponível em: <https://gafam.laquadrature.net/>. Acesso em: 29 nov. 2018.
[539] Na Diretiva 46/95, por sua vez, consentimento era definido como qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento (artigo 2º, h, Diretiva 46/95).
[540] Sobre consentimento, importante verificar os Considerandos 42 e 43 do Regulamento Geral de Proteção de Dados (GDPR).

> O consentimento pode ser dado validando uma opção ao visitar um sítio web na internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido.

O novo regramento europeu também trata da pseudonimização. Conforme dispõe a primeira parte do considerando n. 28, "a aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento e os seus subcontratantes a cumprir as suas obrigações de proteção de dados".

Segundo o artigo 4º, alínea 5 do GDPR, por pseudonimização compreende-se o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável. O Regulamento encoraja os agentes a usar esse tratamento como medida de segurança e redução de riscos. Nesse sentido dispõe o artigo 32, 1, do GDPR, indicando a pseudonimização e a cifragem dos dados pessoais como técnicas avançadas e adequadas para garantir os direitos e as liberdades das pessoas singulares[541], sem prejuízo da aplicação de outras técnicas conforme dispõe a parte final do considerando n. 28: "A introdução explícita da pseudonimização no presente regulamento não se destina a excluir eventuais outras medidas de proteção de dados".

[541] Artigo 32 GDPR: 1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: a) A pseudonimização e a cifragem dos dados pessoais; b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Quanto aos incidentes de vazamento de dado pessoais, o Regulamento impõe às empresas o dever de comunicar o fato à autoridade de controle em até 72 horas, após tomar conhecimento do incidente, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares, cuja exceção é certo que dependerá de análise subjetiva de cada caso. Na hipótese de o prazo ser descumprido por qualquer motivo, o regulamento impõe que o responsável pelo tratamento de dados informe o motivo do envio serôdio (artigo 33[542]).

O novo regulamento europeu atribui poder investigativo e corretivo[543] às autoridades de proteção de dados locais, que podem aplicar multas de até 4% do faturamento da empresa (ou 20 milhões de euros), o que for maior[544]. As autoridades devem se pautar pela efetividade, proporcionalidade e dissuasão da conduta, sempre considerando condições agravantes e atenuantes para o cálculo das multas, seguindo os parâmetros do Regulamento (artigo 83 (1) e (2) da GDPR).

---

[542] Artigo 33: Notificação de uma violação de dados pessoais à autoridade de controle. 1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida em 72 horas, é acompanhada dos motivos do atraso. 2. O subcontratante notifica o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais. 3. A notificação referida no n. 1 deve, pelo menos: a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registros de dados pessoais em causa; b) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações; c) Descrever as consequências prováveis da violação de dados pessoais; d) Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos; 4.Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada. 5. O responsável pelo tratamento documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo.

[543] Artigo 58 (1) e (2) da GDPR.

[544] Artigo 83. 4. A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n. 2, a multas de até 10 000 000 EUR ou, no caso de uma empresa, até 2% do seu volume de negócios anual em âmbito mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado: a) As obrigações do responsável pelo tratamento e do subcontratante nos termos dos artigos 8º, 11º, 25. a 39. e 42. e 43; b) As obrigações do organismo de certificação nos termos dos artigos 42 e 43; c) As obrigações do organismo de supervisão nos termos do artigo 41, n.4; 5. A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.2, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4% do seu volume de negócios anual em âmbito mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado: a) Os princípios básicos do tratamento, incluindo as condições de consentimento, nos termos dos artigos 5, 6, 7 e 9; b) Os direitos dos titulares dos dados nos termos dos artigos 12 a 22; c) As transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional nos termos dos artigos 44 a 49; d) As obrigações nos termos do direito do Estado membro adotado ao abrigo do capítulo IX; e) O incumprimento de uma ordem de limitação, temporária ou definitiva, relativa ao tratamento ou à suspensão de fluxos de dados, emitida pela autoridade de controlo nos termos do artigo 58, 2, ou o facto de não facultar acesso, em violação do artigo 58, n.1. 6. O incumprimento de uma ordem emitida pela autoridade de controlo a que se refere o artigo 58, n.2, está sujeito, em conformidade com o n.2 do presente artigo, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado.

Segundo Giovanni Buttarelli, além do aspecto financeiro, a multa tem um caráter simbólico, a fim de reforçar a confiança dos consumidores[545].

O Regulamento exige que os países legislem, ao menos, sobre dados pessoais, liberdade de expressão[546] e penalidades aplicáveis.

Por outro lado, mesmo com a recente entrada em vigor do novo regulamento europeu, desenvolvido sobre os racionais, dentre outros, das tecnologias de *profiling* e *data mining,* já se fala na criação de nova Diretiva na área de proteção de dados. Dessa vez, com o olhar específico para harmonizar a regulação das operadoras de telecomunicações e dos serviços de *email* e de mensagem instantânea, como o Skype e o WhatsApp[547].

---

[545] REVISTA Exame. **RGPD**: as primeiras multas devem chegar antes do fim do ano. 10 out. 2018. Disponível em: <http://exameinformatica.sapo.pt/noticias/mercados/2018-10-10-RGPD-as-primeiras-multas-devem-chegar-antes-do-fim-do-ano>. Acesso em: 18 out. 2018. Destaque-se, ainda, dessa matéria: Giovanni Buttarelli diz que só na França e na Espanha aumentou 53% o número de irregularidades descobertas e o poder de autuar as empresas que não estejam conforme os reguladores nacionais. Buttarelli acredita que as primeiras multas e sanções surjam ainda antes do final do ano. Há muitas empresas e instituições públicas a serem investigadas nesse momento, embora os nomes não tenham sido confirmados.

[546] Artigo 85º. Tratamento e liberdade de expressão e de informação. 1.Os Estadosm membros conciliam por lei o direito à proteção de dados pessoais nos termos do presente regulamento com o direito à liberdade de expressão e de informação, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária. 2. Para o tratamento efetuado para fins jornalísticos ou para fins de expressão académica, artística ou literária, os Estados membros estabelecem isenções ou derrogações do capítulo II (princípios), do capítulo III (direitos do titular dos dados), do capítulo IV (responsável pelo tratamento e subcontratante), do capítulo V (transferência de dados pessoais para países terceiros e organizações internacionais), do capítulo VI (autoridades de controlo independentes), do capítulo VII (cooperação e coerência) e do capítulo IX (situações específicas de tratamento de dados) se tais isenções ou derrogações forem necessárias para conciliar o direito à proteção de dados pessoais com a liberdade de expressão e de informação. 3. Os Estados membros notificam a Comissão das disposições de direito interno que adotarem nos termos do n.2 e, sem demora, de qualquer alteração subsequente das mesmas.

[547] Segundo Giovanni Buttarelli: urge os países e legisladores a unirem-se para criar uma diretiva destinada à e-privacidade, que harmonize a regulação das operadoras de telecomunicações e dos serviços de email e de mensagem instantânea, como o Skype ou o WhatsApp. REVISTA Exame. **RGPD**: as primeiras multas devem chegar antes do fim do ano. 10 out. 2018. Disponível em: <http://exameinformatica.sapo.pt>. Acesso em: 18 out. 2018; WP29 240 – Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC). Disponível em: <https://ec.europa.eu/>. Acesso em: 29 nov. 2018. The Data Protection Authorities of the European Union, united in the European Data Protection Board, consider that the revision of the current ePrivacy Directive (2002/58/EC, amended by 2009/136/EC) is an important and necessary step that has to be concluded rapidly. The use of IP based communication services has become widespread since 2009, and these 'Over-theTop' services are currently not covered by the existing Directive; in order to ensure that endusers' confidentiality of communications is protected while using these new services and to create a level playing field for providers of electronic communication and functionally equivalent services, we call on the European Commission, Parliament and Council to work together to ensure a swift adoption of the new ePrivacy Regulation, replacing the current Directive as soon as possible after the coming into effect of the General Data Protection Regulation in May this year. (EDPB. Disponível em: <https://edpb.europa.eu>. Acesso em: 29 nov. 2018). Tradução livre: As autoridades de proteção de dados da União Europeia, reunidas no Comitê Europeu para a Proteção de Dados, consideram que a revisão da atual Diretiva sobre privacidade eletrônica (2002/58/CE, alterada pela Directiva 2009/136/CE) é um passo importante e necessário que deveria ser concluído rapidamente. A utilização de serviços de comunicação baseados em IP tornou-se generalizada desde 2009, e estes serviços "Over-the-top" não são atualmente abrangidos pela diretiva existente; a fim de assegurar que a confidencialidade das comunicações dos utilizadores finais seja protegida ao utilizar estes novos serviços e criar condições equitativas para os fornecedores de comunicações eletrônicas e serviços funcionalmente equivalentes, apelamos à Comissão Europeia, ao Parlamento e ao Conselho para que trabalhem em conjunto para garantir uma adoção rápida de nova Diretiva relativa à privacidade eletrônica, substituindo a atual directiva o quanto antes após a entrada em vigor do Regulamento Geral sobre Protecção de Dados, em Maio deste ano.

3.8 Análise comparativa da tutela da proteção de dados pessoais nos Estados Unidos da América

De outro lado, não se pode deixar de olhar para os Estados Unidos, berço do direito *right to be alone*, considerado como ponto de partida da evolução que levou ao direito autônomo da proteção de dados pessoais, na forma de todas as dimensões apresentadas.

Em relação à diferença da evolução da matéria ocorrida entre o novo e o velho mundo, observam Erick Lucena Campos Peixoto e Marcos Ehrhardt Júnior que a principal delas é de ordem temporal:

> Enquanto que nos Estados Unidos a discussão ganhava corpo ainda no século XIX, na Europa só se passa a uma preocupação mais concreta no pós-guerra, justamente depois da invenção do computador. A privacidade americana, no seu sentido inicial, dizia respeito ao direito de não ser incomodado, era uma derivação do direito à vida, de não ter nenhum mal infligido ao corpo, o que posteriormente foi levado para o aspecto moral. Não ser incomodado, ser deixado em paz, ou deixado só são os sentidos possíveis do *right to privacy*[548].

Na Europa, por sua vez, e conforme visto[549], o movimento pela privacidade surgido na segunda metade do século XX se desvincula do sentido físico do *right to privacy* americano, bifurcando a sistemática da matéria.

Ainda distinguindo Estados Unidos e Europa, Erick Lucena Campos Peixoto e Marcos Ehrhardt Júnior informam que a preocupação dos europeus com a privacidade também difere da preocupação dos americanos no sentido de que a proteção dos dados pessoais é uma medida necessária, inicialmente, contra o Estado, numa relação vertical, ao passo que nos Estados Unidos, o direito à privacidade surge como uma garantia contra os abusos cometidos por particulares, ou seja, horizontalmente:

> As raízes da privacidade nos Estados Unidos estão em um direito do indivíduo, de caráter negativo, enquanto as raízes europeias estão também na sociedade, apresentando características de direito positivo, no qual se exige do Estado que se tomem medidas para garantir a proteção de dados pessoais, como a instalação de órgãos de controle, além de a proteção visar grupos minoritários que podem sofrer discriminações com a exposição

[548] PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. In: **Revista Brasileira de Direito Civil** – RBDCivil | Belo Horizonte, v.16, p.35-56, abr.-jun.2018, p.42.

[549] "A preocupação aqui é com o novo paradigma tecnológico que potencializou o processamento de dados através do uso do computador. Preocupa-se, então, com os dados pessoais e com o controle sobre eles. (PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. In: **Revista Brasileira de Direito Civil** – RBDCivil | Belo Horizonte, v.16, p.35-56, abr.-jun.2018, p.42).

> de seus dados pessoais. Na Europa se desenvolve o aspecto social da privacidade[550].

Nos Estados Unidos, o Federal Trade Commission (FTC) tem sido a principal agência federal em política de privacidade e fiscalização desde 1970, quando começou a aplicar uma das primeiras leis federais de privacidade, o Fair Credit Reporting Act (FCRA).

O contexto que envolve o nascimento dessa lei diz respeito a dados sobre as condições financeiras do indivíduo. No século XX, com o crescimento da população e a sofisticação dos negócios, os credores passaram a contar com registros e documentos para avaliar a reputação das pessoas. Esses passos resultaram na formação de agências de informação de crédito, consistentes em empresas que obtêm e reportam informações sobre as pessoas, seu histórico de crédito – onde constam detalhes sobre a conta corrente, dívidas pendentes, pedidos de falência, decisões judiciais e ônus reais – dentre outras informações. As três principais agências de relatórios de crédito nos Estados Unidos são Equifax, Experian e Trans Union, as quais, juntas, possuem a compilação de dados que abrangem praticamente todos os cidadãos americanos adultos[551].

Nesse ambiente, passou-se a verificar uma série de reclamações sobre relatórios de crédito errados e a falta de capacidade de atendimento e de resposta das agências de informação de crédito. A situação levou o Congresso americano a aprovar o Fair Credit Reporting Act (FCRA), em 1970. Segundo Daniel Solove, porém, o FCRA fornece proteções limitadas aos indivíduos. Se, por um lado, permite às pessoas acessarem seus registros e restringe a maneira pela qual os registros são divulgados, além de possibilitar o questionamento sobre imprecisões em seus relatórios, por outro, o FCRA imuniza credores e agências de informação de crédito de processos por “difamação, invasão de privacidade ou negligência”, exceto quando a informação é “fornecida com malícia ou intenção de prejudicar tal consumidor[552].

---

[550] PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. In: **Revista Brasileira de Direito Civil** – RBDCivil | Belo Horizonte, v.16, p.35-56, abr.-jun.2018, p.42.

[551] SOLOVE, Daniel, J. A brief history of information privacy law. In: **Proskauer on privacy**, PLI. Washington: George Washington Law Faculty Publications, 2006, p.29-30.

[552] SOLOVE, Daniel, J. A brief history of information privacy law. In: **Proskauer on privacy**, PLI. Washington: George Washington Law Faculty Publications, 2006, p.38.

Outro importante marco nos Estados Unidos diz respeito ao Privacy Act, de 1974. A lei regula a coleta e o uso de registros por agências federais e concede aos indivíduos o direito de acessar e corrigir seus dados pessoais e informações. Embora o Privacy Act tenha dado passos importantes no sentido de colocar os sistemas de informação do governo sob controle, a Lei possui várias deficiências. Uma delas é o fato de não se aplicar ao setor privado, nem a agências estaduais ou locais. Outra limitação é a exceção "uso rotineiro", pela qual a informação pode ser divulgada para qualquer "uso de rotina" se a divulgação for "compatível" com o propósito para o qual a agência coletou as informações. Essa exceção consiste numa enorme lacuna, fruto de diversas críticas de especialistas.

Ainda, destaca-se no horizonte legal norte-americano o Electronic Communications Privacy Act (ECPA) de 1986. Nesse ano, o Congresso dos Estados Unidos revisitou sua lei sobre escutas telefônicas de 1968 e expandiu a tutela legal para novas formas de comunicação, com foco particular em computadores e dados armazenados em provedores como Internet Service Provider.

Em 1996, o Health Insurance Portability and Accountability Act (HIPAA) é aprovado e consiste no primeiro estatuto federal a abordar diretamente a privacidade na área da saúde. Essa lei determina que o Departamento de Saúde e Recursos Humanos (Health and Human Service-HHS) elabore regulamentos para proteger a privacidade de registros. Por sua vez, estes regulamentos, dentre outros deveres, exigem autorização dos indivíduos para uso e divulgação dos seus dados de saúde se não forem exclusivamente para tratamento, pagamento ou operação de tratamentos de saúde.

Apesar de não existir uma autoridade nacional de proteção de dados, como se verifica na Europa, recai sobre o Federal Trade Commission (FTC) atuar sobre diversas situações vinculadas à matéria. Segundo seu pronunciamento recente, "mudanças rápidas na tecnologia levantaram novos desafios de privacidade"[553], o que faz com que este órgão tenha como um dos focos de atuação a proteção permanente sobre os consumidores[554] e, em especial, as crianças[555].

[553] Disponível em: <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security>. Acesso em: 27 nov. 2018.

[554] Como exemplos de tutela no setor podem ser mencionadas as regulações no setor financeiro (i.) Instituições financeiras são obrigadas a tomar medidas para proteger a privacidade das finanças dos consumidores sob uma lei federal chamada Financial Modernization Act de 1999, também conhecida como Lei Gramm-Leach-Bliley. A FTC é uma das agências federais que aplica as cláusulas do Gramm-Leach Bliley, e a lei abrange não apenas os bancos, mas também as corretoras de títulos, companhias de seguros e empresas que fornecem muitos outros tipos de produtos e serviços financeiros. Segundo a lei, as agências aplicam a Financial Privacy Rule, que

Em meio a discussões entre o Parlamento Europeu e os Estados Unidos sobre transferência internacional de dados[556], há notícias de que a Casa Branca

rege como as instituições financeiras podem coletar e divulgar informações financeiras pessoais dos clientes; a Regra de Salvaguardas, que exige que todas as instituições financeiras mantenham salvaguardas para proteger as informações dos clientes; e outra cláusula destinada a impedir que indivíduos e empresas tenham acesso às informações financeiras pessoais dos consumidores sob falsos pretextos, uma prática conhecida como "pretexting". Além disso, também possui regramente voltado à Segurança de Dados (ii.) a FTC realiza estudos, workshops e publica relatórios sobre os principais tópicos relacionados à tecnologia. Por exemplo, a FTC realizou um workshop anual chamado PrivacyCon, onde estudiosos discutem pesquisas recentes sobre questões de privacidade e segurança. A FTC também emitiu relatórios, como um relatório sobre as práticas dos corretores de dados e um relatório sobre práticas de atualização de segurança móvel; (iii.) setor de saúde (health data) – Health Insurance Portability and Accountability Act (HIPAA); (iv.) informações genéticas; (v.) student records; (vi.) e electronic communications (with differing rules for telecommunications carriers, cable providers, and emails). A deficiência da proteção setorial é comentada por Sablich com a proposição de um exemplo: Take my smart watch, for one example: data it generates about my heart rate and activity is covered by the Health Insurance Portability and Accountability Act (HIPAA) if it is shared with my doctor, but not when it goes to fitness apps like Strava (where I can compare my performance with my peers). Either way, it is the same data, just as sensitive to me and just as much of a risk in the wrong hands. (SABLICH, Elizabeth. Why protecting privacy is a losing game today – and how to change the game. In: **Brooking**. Disponível em: <https://www.brookings.edu>. Acesso em 02 nov. 2018). Tradução livre: (v.) registros de alunos; (vi.) e comunicações eletrônicas (com regras diferentes para operadoras de telecomunicações, provedores de cabo e e-mails). A deficiência da proteção setorial é comentada por Sablich com a proposição de um exemplo: Pegue meu relógio inteligente, por exemplo: os dados gerados sobre minha frequência cardíaca e atividade são cobertos pela Lei de Portabilidade e Responsabilidade em Seguros de Saúde (HIPAA), se for o caso. compartilhado com meu médico, mas não quando se trata de aplicativos de fitness como o Strava (onde posso comparar meu desempenho com meus colegas). De qualquer forma, são os mesmos dados, tão sensíveis a mim e tão arriscados nas mãos erradas.

[555] O Congresso Americano e a FTC tomaram medidas especiais para garantir que as crianças com menos de 13 anos não compartilhem suas informações pessoais na Internet sem a aprovação expressa de seus pais. O Congresso aprovou a Lei de Proteção à Privacidade Online para Crianças (Children's Online Privacy Protection Act – COPPA), em 1998, e a FTC criou uma regra para implementar a lei, que foi revisada em 2012.

[556] Em 5 de julho, o Parlamento Europeu recomendou, por meio de uma resolução não vinculante de sua Comissão de Liberdades Civis, Justiça e Assuntos Internos. (Disponível em: <http://www.europarl.europa.eu/>. Acesso em: 29 nov. 2018) que a Comissão suspendesse o Privacy Shield entre UE e EUA – acordo que foi aprovado em 12 de julho de 2016 e entrou em vigor em 01 agosto 2016, após a desativação do Safe Harbor, que permite a transferência de dados pessoais da UE para empresas dos EUA que prometeram aderir às normas europeias de proteção de dados – a menos que até 01 set. 2018, todas as ações corretivas definidas fossem tomadas pelo Departamento de Comércio dos EUA. Dentre essas ações corretivas estavam as obrigações de que o Privacy Shield seja totalmente compatível com o GDPR e com as recomendações feitas pelo Grupo de Trabalho do Artigo 29 (agora o European Data Protection Board). Em resumo, o Privacy Shield foi formulado visando proteger os direitos fundamentais de qualquer pessoa na UE cujos dados pessoais são transferidos para os Estados Unidos para fins comerciais. O acordo também buscou trazer segurança e clareza jurídica para as empresas que dependem de transferências de dados transatlânticas. Nesse sentido, o acordo previu obrigações rigorosas em matéria de proteção de dados para as empresas que recebem dados pessoais da EU, além de salvaguardas sobre o acesso do governo dos EUA aos dados, proteção eficaz e reparação para os indivíduos, e uma revisão conjunta anual pela UE e EUA para monitorar a correta aplicação do acordo (EU-US Privacy Shield. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en>. Acesso em: 02 nov. 2018). A Europa aguarda que os EUA estejam em total conformidade para reativar o acordo. O assunto foi polemizado pelas audiências do CEO do Facebook no Parlamento Europeu, após o escândalo Cambridge Analytica, em cuja ocasião os deputados europeus demonstraram a clara irritação com a falta de respostas por parte da empresa. Segundo o eurodeputado britânico Claude Moraes, que preside o comitê de liberdades civis e liderou a ação contra o Privacy Shield: "This resolution makes clear that the Privacy Shield in its current form does not provide the adequate level of protection required by EU data protection law and the EU Charter. Progress has been made to improve on the Safe Harbor agreement but this is insufficient to ensure the legal certainty required for the transfer of personal data. The law is clear and, as set out in the GDPR, if the agreement is not adequate, and if the US authorities fail to comply with its terms, then it must be suspended until they do." (BAKER, Jennifer. **European Parliament**: suspend privacy shield unless US fully complies. Disponível em: <https://iapp.org/news/a/parliament-suspend-privacy-shield-until-u-s-fully-complies/>. Acesso em: 02 nov. 2018). Tradução livre: "Esta resolução deixa claro que o Privacy Shield em sua forma atual não fornece o nível adequado de proteção exigido pela lei de proteção de dados da UE e pela Carta da UE. Houve progressos para melhorar o acordo Safe Harbor, mas isso é insuficiente para garantir a segurança jurídica necessária para a transferência de dados pessoais. A lei é clara e, conforme estabelecido no GDPR, se o acordo não for adequado, e se as autoridades dos EUA não cumprirem seus termos, ele deverá ser suspenso até que seja cumprido". Em 18 de outubro de 2017, por meio de sua assessoria de imprensa, a Comissão Europeia publicou manifestação da Comissária da Justiça, Consumidores e Igualdade de Género, Vera Jourová: "As transferências

está trabalhando em uma proposta de regras federais de privacidade e proteção de dados[557]. O Departamento de Comércio dos Estados Unidos se reuniu com empresas como Facebook, Google, AT&T e Comcast, além de grupos de defesa do consumidor, visando produzir princípios gerais para as entidades lidarem com informações privadas dos consumidores. Esta seria a primeira lei federal de proteção de dados e privacidade do país[558]. Além disso, existe um projeto de lei, elaborado em 2012, em âmbito federal, o Consumer Privacy Bill of Rights[559], que

---

de dados transatlânticas são essenciais para a nossa economia, mas o direito fundamental à protecção de dados também deve ser assegurado quando os dados pessoais saírem da UE. Nossa primeira análise mostra que o Privacy Shield funciona bem, mas há espaço para melhorar sua implementação. O Privacy Shield não é um documento colocado em uma gaveta. É um sistema de convivência que tanto a UE quanto os EUA devem monitorar ativamente para garantir que mantenhamos nossos altos padrões de proteção de dados". (EUROPEAN Commission EU-U.S. **Privacy shield**: first review shows it works but implementation can be improved. 18 out. 2017. Disponível em: <http://europa.eu/rapid/press-release_IP-17-3966_en.htm>. Acesso em: 02 nov. 2018). Dito isso, ressalte-se que a questão está sob análise. Os EUA não cumpriram totalmente as obrigações impostas mas já percorreram grande parte das adequações. Segundo Silverstone, Wunderlich, Prasow e Grynwajc, ainda que os EUA não se adequem completamente, o acordo não será suspenso efetivamente. (SILVERSTONE, Ariel; WUNDERLICH, John; PRASOW, Sholem; GRYNWAJC, Stephan. **European Parliament voted to suspend privacy shield**: now what? Disponível em: <https://iapp.org/news/a/european-parliament-voted-to-suspend-privacy-shield-now-what/>. Acesso em: 02 nov.2018). Em 19-10-2018, o Secretário de Comércio dos EUA, Wilbur Ross, e a Comissária Vera Jourová declararam a respeito do segundo relatório anual dos EUA-E.U para revisão do privacy shield: "Autoridades do governo dos Estados Unidos, da Comissão Europeia e das Autoridades Europeias de Proteção de Dados estão reunidas em Bruxelas nesta semana para conduzir a segunda revisão anual da estrutura EU-US Privacy Shield. Os dois dias de discussões detalhadas estão abordando todos os aspectos do seu funcionamento. A revisão beneficiou-se grandemente da contribuição da indústria e da sociedade civil. Desde o início do programa, em 2016, quase 4 mil empresas assumiram compromissos legais para cumprir sua estrutura. O crescimento significativo do programa no ano passado destaca a importância vital da Privacy Shield para a proteção de dados e comércio transatlântico. As autoridades dos EUA e da UE continuarão a trabalhar em estreita colaboração para assegurar o funcionamento da estrutura conforme pretendido, incluindo questões relacionadas à segurança comercial e nacional. Antes do final do ano, a Comissão publicará um relatório contendo suas conclusões sobre o funcionamento do Privacy Shield". (Disponível em: <https://www.commerce.gov/news/press-releases/2018/10/joint-press-statement-commissioner-vera-jourova-and-secretary-commerce>. Acesso em: 05 nov. 2018).

[557] ROMM, Tony. The Trump administration is talking to Facebook and Google about potential rules for online privacy. **The Washington Post**, 27/07/2018. Disponível em: <https://www.washingtonpost.com>. Acesso em: 02 nov. 2018.

[558] Não obstante a ausência de uma lei geral, no que toca à notificação por *data breach,* todos os 50 estados norte americanos têm leis que exigem notificação de violações de dados (com variações sobre quem deve ser notificado, com que rapidez e em quais circunstâncias).

[559] The of rights articulated seven basic principles that should be legally enforceable by the Federal Trade Commission: individual control, transparency, respect for the context in which the data was obtained, access and accuracy, focused collection, security, and accountability. These broad principles are rooted in longstanding and globally-accepted "fair information practices principles." To reflect today's world ofions of devices interconnected through networks everywhere, though, they are intended to move away from static privacy notices and consent forms to a more dynamic framework, less focused on collection and process and more on how people are protected in the ways their data is handled. Not a checklist, but a toolbox. This principles-based approach was meant to be interpreted and fleshed out through codes of conduct and case-by-case FTC enforcement—iterative evolution, much the way both common law and information technology developed. (SABLICH, Elizabeth. Why protecting privacy is a losing game today – and how to change the game. In: **Brooking**. Disponível em: <https://www.brookings.edu>. Acesso em 02 nov. 2018). Tradução livre: Os direitos são guiados por sete princípios básicos que deveriam ser legalmente exigíveis pelo FTC: controle individual, transparência, respeito pelo contexto no qual os dados foram obtidos, acesso e precisão, coleta focada, segurança e responsabilidade. Esses princípios gerais estão enraizados em "princípios de práticas de informação justa" aceitos desde longa data e globalmente aceitos. Para refletir as atuais seções de dispositivos interconectados através de redes em todos os lugares, elas pretendem se afastar de avisos estáticos de privacidade e formulários de consentimento para uma estrutura mais dinâmica, menos focado na coleta e no processo e mais em como as pessoas são protegidas na maneira como seus dados são manipulados. Não é uma lista de verificação, mas uma caixa de ferramentas. Essa abordagem baseada em princípios deveria ser interpretada e aperfeiçoada por meio de

conforme opinaram especialistas, ainda que dependa de adaptações, pode ser usado para conferir uma tutela em âmbito nacional em matéria de proteção de dados e privacidade[560]. Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson e Orla Lynskey falam sobre o assunto:

> Even the White House, which for years had seemed to oppose any large-scale federal legislation to deal with data processing in the private sector, has called for enactment of a Consumer Privacy Bill of Rights Act to grant increased protection to the online processing of personal data[561].

Cameron Kerry defende a necessidade de uma lei geral de proteção de dados e privacidade para os Estados Unidos. Em artigo publicado nesse sentido, argumenta ser fundamental uma legislação no país para garantir que os indivíduos possam confiar que os dados sobre eles serão usados, armazenados e compartilhados de maneira consistente com seus interesses e as circunstâncias para as quais foram coletados. Segundo o autor, isso deve acontecer independentemente de como os dados são coletados, de quem os recebe ou ainda, independente dos usos para os quais serão destinados; sendo dados pessoais, devem ter proteção duradoura. A confiança consiste na *golden rule of privacy*. Segundo o autor, "such trust is an essential building block of a sustainable digital world"[562].

Mais recentemente, os Estados Unidos marcam momento histórico com a aprovação de lei geral (estadual) sobre privacidade. Aprovada pelo governador da Califórnia em 28 de junho de 2018, a nova lei – California Consumer Privacy Act

---

códigos de conduta e fiscalização do FTC caso a caso – evolução iterativa, da mesma forma que o *common law* e a tecnologia da informação se desenvolveram.

[560] Disponível em: <https://www.nytimes.com>; <http://www.latimes.com>; <https://www.economist.com/>. Acesso em: 29 nov. 2018.

[561] Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, Orla Lynskey; The data protection credibility crisis. ***International Data Privacy Law***, v.5, Issue 3, 1 August 2015, p.161-162, p.161. Tradução livre: Até mesmo a Casa Branca, que durante anos parecia se opor a qualquer legislação federal de grande escala para lidar com o processamento de dados no setor privado, pediu a promulgação de uma Lei de Declaração de Privacidade do Consumidor para conceder maior proteção ao processamento online de dados pessoais.

[562] KERRY, Cameron F. Protecting privacy is a losing game today – and how to change the game. In: **Brookings**. Publicado em 12 jul. 2018. Disponível em: <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>. Acesso em: 15 nov.2018. Tradução livre: essa confiança é um componente essencial de um mundo digital sustentável. E completa o autor: It is what enables the sharing of data for socially or economically beneficial uses without putting human beings at risk. By now, it should be clear that trust is betrayed too often, whether by intentional actors like Cambridge Analytica or Russian "Fancy Bears," or by bros in cubes inculcated with an imperative to "deploy or die." Tradução livre: É o que permite o compartilhamento de dados para usos social ou economicamente benéficos sem colocar os seres humanos em risco. Por agora, deve ficar claro que a confiança é traída com muita frequência, seja por atores intencionais, como Cambridge Analytica ou Russian Fancy Bears, ou by bros em cubos inculcados com um imperativo de "implantar ou morrer".

(CaCPA) – volta-se à proteção de dados pessoais dos consumidores e entrará em vigor a partir de 1º de janeiro de 2020.

Por meio dessa lei – fruto da iniciativa do rico empresário do setor imobilário, Alastair Mactaggart[563] – os consumidores terão mais controle sobre a disseminação de suas informações pessoais *on-line*, criando uma das regulamentações mais significativas a supervisionar as práticas de coleta de dados das empresas de tecnologia nos Estados Unidos. Além disso, torna mais difícil compartilhar ou vender dados sobre indivíduos menores de 16 anos.

Um dos autores da nova lei, o congressista e democrata Ed Chau, tentou em 2017 aprovar um projeto de lei que exigia dos provedores de serviços de internet pedirem permissão aos usuários antes de acessar, vender ou compartilhar sua atividade no navegador. O projeto de lei, porém, permaneceu parado no comitê, demonstrando como a influência das empresas de telecomunicações e tecnologia na Califórnia foi capaz de barrar esse tipo de iniciativa. Entretanto, com o aumento da conscientização sobre como as empresas de tecnologia estão obtendo informações do usuário – o que ficou evidente com as revelações do caso Cambridge Analytica – a legislação passou de rascunho para lei em uma semana[564].

O California Consumer Privacy Act (CaCPA) consiste na primeira tentativa dos Estados Unidos de obter uma lei abrangente de proteção de dados[565]. Na opinião de alguns, é o mais rigoroso regime de proteção de dados nos Estados Unidos[566].

Além de estar entre as regiões com maior economia do mundo, a Califórnia é a sede de várias gigantes da tecnologia da informação, daí sua maior atenção e importância. Por isso também a Califórnia é, tradicionalmente, um estado mais atuante nas questões de tecnologia e privacidade em relação aos demais estados

---

[563] Detalhes sobre a história do projeto de lei. (CONFESSORE, Nicholas. The unlikely activists who took on Silicon Valley — and Won, Aug. 14, 2018. **The New York Times Magazine**. Disponível em: <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html >. Acesso em: 02 nov. 2018.

[564] WAKABAYASHI, Daisuke. California passes sweeping law to protect online privacy image, June 28, 2018. **The New York Times**. Disponível em: <https://www.nytimes.com/>. Acesso em: 02 nov. 2018.

[565] DE LA TORRE, Lydia. GDPR matchup: The California consumer privacy act 2018. **International Association of Privacy Professionals (IAPP) News**, 31 jul. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/>. Acesso em: 07 set. 2018. Segundo a autora, tradicionalmente, a California é um Estado que define tendência para a proteção de dados e da privacidade nos EUA.

[566] GHOSH, Dipayan. What you need to know about California's new data privacy law, July 11, 2018. **Harvard Business Review**. Disponível em: <https://hbr.org>. Acesso em: 02 nov. 2018.

norte-americanos. A medida poderá servir como catalisador para outros aprovarem leis similares[567].

O texto normativo do California Consumer Privacy Act é modelado no GDPR. Entretanto, a conformidade com o regulamento europeu, por mais que este seja considerado como um *gold standard*, não equivale à conformidade com o CaCPA. Portanto, mesmo as empresas que já estivessem em conformidade com a Europa, teriam um trabalho adicional.

Por meio dessa lei, os consumidores (californianos[568]) têm o direito de exigir a exclusão dos seus dados, impedir sua venda pelas empresas sem perderem o acesso aos serviços ou serem cobrados por um preço mais alto. Para tanto, as empresas deverão divulgar as informações armazenadas, a finalidade e os terceiros com quem compartilha esses dados.

Uma das principais diferenças entre os dois textos é o fato de que a lei californiana não tem princípios de processamento de dados e, de fato, impõe poucas restrições sobre o que um determinado negócio pode realizar internamente com dados pessoais. Enquanto o regulamento europeu traz seis bases legais para justificar o processamento de dados pessoais, o CaCPA não contém nenhuma disposição similar. A regra geral é permitir o processamento embora faculte aos residentes da Califórnia optar por não fazer certos tipos de processamento (o que o CaCPA define como “vender”). Outrossim, o CaCPA não limita, expressamente, a

[567] FLEISHMAN, Glenn. California passes groundbreaking consumer data privacy law with fines for violations, June 2018. **Fortune**. Disponível em: <http://fortune.com/>. Acesso em: 02 nov. 2018.

[568] Sobre o alcance da lei, explica Dipayan Ghosh: While the law, which is set to come into effect at the start of 2020, technically applies only to California residents, it will most likely have much broader implications. Most major companies that deal in consumer data, from retailers to cellular network providers to internet companies, have some Californian customers. That will leave those companies with two main options: either reform their global data protection and data rights infrastructures to comply with California’s law, or institute a patchwork data regime in which Californians are treated one way and everyone else another. That last option can be more expensive for companies, and could disgruntle non-Californian customers should they be given fewer data privacy options by the service provider. Indeed, similar questions about Americans’ data rights arose during Mark Zuckerberg’s congressional testimony in regard to Facebook’s compliance with new European regulations. (GHOSH, Dipayan. What you need to know about California’s new data privacy law, July 11, 2018. **Harvard Business Review**. Disponível em: <https://hbr.org>. Acesso em: 02 nov. 2018). Tradução livre: Embora a lei, que deve entrar em vigor no início de 2020, tecnicamente se aplique apenas aos moradores da Califórnia, ela provavelmente terá implicações muito mais amplas. A maioria das grandes empresas que lidam com dados de consumidores, de varejistas a provedores de redes celulares a empresas de internet, tem alguns clientes californianos. Isso deixará a essas empresas duas opções principais: reformar suas infraestruturas globais de proteção de dados e direitos de dados para cumprir a lei da Califórnia ou instituir um regime de dados de retalhos no qual os californianos são tratados de uma maneira e todos os demais. Essa última opção pode ser mais cara para as empresas e pode desgrudar os clientes não californianos, caso recebam menos opções de privacidade de dados pelo provedor de serviços. De fato, questões semelhantes sobre os direitos de dados dos americanos surgiram durante o testemunho do Congresso de Mark Zuckerberg em relação à conformidade do Facebook com as novas regulamentações europeias.

possibilidade de processamento automatizado de dados, ao contrário da maioria (senão de todas) das leis de proteção de dados pelo mundo[569].

Quanto ao 'dado pessoal', o CaCPA o define como "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"[570]. A lei californiana também considera como dado pessoal a definição de perfis: "Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes"[571]. A lei, porém, não dispõe sobre decisões automatizadas, tomadas com o uso de algoritmos.

Em relação às principais figuras reconhecidas em texto legal, enquanto o regulamento europeu traz as funções do *data controller* e do *data processor,* o California Consumer Privacy Act traz as seguintes pessoas: *businesses*, *service providers*, *third parties* e *consumers*. Esses últimos são os consumidores residentes na Califórnia[572]. Quanto à definição de dados pessoais, é feita de forma expansiva

---

[569] DE LA TORRE, Lydia. GDPR matchup: The California consumer privacy act 2018. **International Association of Privacy Professionals (IAPP) News**, 31 jul. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/>. Acesso em: 07 set. 2018.

[570] Title 1.81.5. Section 1798.140 (o) (1). Tradução livre: informações que identificam, relacionam, descrevem, são capazes de se associarem, ou poderem ser razoavelmente vinculadas, direta ou indiretamente, com um determinado consumidor ou residência.

[571] Title 1.81.5. Section 1798.140 (k). Tradução livre: Inferências extraídas de qualquer informação identificada nesta subdivisão para criar um perfil sobre um consumidor refletindo as preferências, características, tendências psicológicas, preferências, predisposições, comportamento, atitudes, inteligência, habilidades e aptidões do consumidor. Ainda sobre dado pessoal, a lei em comento dispõe que: "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information Title 1.81.5. Section 1798.140 (k) (2). Tradução livre: "Dados pessoais" não incluem informações publicamente disponíveis. Para esses fins, "publicamente disponível" significa informações legalmente disponibilizadas pelos registros do governo federal, estadual ou local, se houver alguma condição associada a tais informações. "Publicamente disponível" não significa informações biométricas coletadas por uma empresa sobre um consumidor sem o conhecimento do consumidor. As informações não estão "publicamente disponíveis" se esses dados forem usados com uma finalidade que não seja compatível com a finalidade para a qual os dados são mantidos e disponibilizados nos registros do governo ou para os quais são mantidos publicamente. "Publicamente disponível" não inclui informações do consumidor que são deidentificadas ou informações agregadas ao consumidor.

[572] To summarize, if we were to translate the CaCPA into GDPR jargon, a "consumer" is a data subject, a "business" is a controller that meets certain requirements, and also includes some entities in the controller's group; a "service provider" is a processor for a "business" that meets certain requirements; and a "third party" is any entity that is neither a"business" nor a "service provider". (DE LA TORRE, Lydia. GDPR matchup: The California consumer privacy act 2018. **International Association of Privacy Professionals (IAPP) News**, 31 jul. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/>. Acesso em: 07 set. 2018). Tradução livre: Resumindo, se fôssemos traduzir o CaCPA em jargão GDPR, um "consumidor" é um sujeito de dados, um "negócio" é um controlador que atende a certos requisitos e também inclui algumas

no CaCPA, porque dados pessoais “identificam, relacionam-se, descrevem, são capazes de estar associados, ou podem ser razoavelmente vinculados, direta ou indiretamente, a um consumidor ou agregado familiar”. Além disso, a lei da Califórnia lista vários exemplos de dados pessoais, como endereços IP, *cookies*, *beacons*, *pixel tags*, geolocalização, dados biométricos, histórico de navegação na internet e dados psicométricos. Segundo Lydia De La Torre, essa definição é potencialmente mais ampla do que a definição de dados pessoais no âmbito do GDPR[573].

---

entidades no grupo do controlador; um “provedor de serviços” é um processador para um “negócio” que atende a certos requisitos; e um “terceiro” é qualquer entidade que não seja um “negócio” nem um “provedor de serviços”.

[573] DE LA TORRE, Lydia. GDPR matchup: The California consumer privacy act 2018. **International Association of Privacy Professionals (IAPP) News**, 31 jul. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/>. Acesso em: 07 set. 2018. Ainda segundo essa autora: The GDPR contains the traditional rights of access, rectification, correction and opposition, which are a common feature of most comprehensive data protection frameworks around the world. It also includes additional rights such as the right to data portability and the so-called “right to an explanation”. The CaCPA confers six rights on California residents. The first one, the right to access personal data, is very similar to the access rights under the GDPR but the others are not. For example, the CaCPA contains a right to cancel (erase) data but it only applies to data that is collected by a “business” “from” the California resident exercising the right. What exactly that means is not clear at this point but we can anticipate a debate over whether data collected by CCTV cameras or data scraped from online public profiles is subject to the CaCPA's erasure right. One thing we can know for sure is that the CaCPA would not support a case like Spain's Costeja case, because Google did not collect the now famous (or infamous) newspaper bankruptcy report from Mr. Costeja but from a third party. One final point: The exceptions to the right to erase under CaCPA are also very different from the grounds that justify erasure and the balancing tests built into the GDPR and will require separate analysis.The CaCPA contains two rights to know: The right to know what information has been collected, and the right to know what information has been shared. These rights are fairly prescriptive; however, the current version of the CaCPA contains contradictions that make providing a clear interpretation of exactly what will have to be disclosed impossible. What seems clear is that businesses will have to evaluate their practices to identify what sharing is to be considered for “business purposes” and what sharing is to be considered for “commercial purposes” under the CaCPA, as those two purposes will need to be separately disclosed. As opposed to the GDPR, the CaCPA allows businesses to “sell” personal data but gives individuals the right to opt out of (or, in the case of minors under 16, the option to opt in to) the selling of their data (referred to as "the right to say no"). In GDPR terms, this right would be a limited version of the right to restrict processing under Article 18. The definition of a “sale” is not clear, it refers to transfers to “third parties” or “other businesses” for “monetary or other valuable consideration," and guidance from the California attorney general on this point is expected. As with the GDPR, the CaCPA does not allow for discrimination against individuals who exercise their rights under the act. The CaCPA expressly allows for financial incentives so long as they are not “unjust, unreasonable, coercive, or usurious in nature.” The CaCPA's provisions on discrimination are unclear and somewhat contradictory. For example, the CaCPA states specifically that business are not prohibited from “charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer if that difference is reasonably related to the value provided to the consumer by the consumer’s data.” It is unclear exactly what is the value provided to the consumer by their own data. Tradução livre: O GDPR contém os direitos tradicionais de acesso, retificação, correção e oposição, que são uma característica comum da maioria das estruturas abrangentes de proteção de dados em todo o mundo. Também inclui direitos adicionais, como o direito à portabilidade de dados e o "direito a uma explicação". O CaCPA confere seis direitos aos moradores da Califórnia. O primeiro, o direito de acessar dados pessoais, é muito semelhante aos direitos de acesso sob o GDPR, mas os outros não são. Por exemplo, o CaCPA contém o direito de cancelar (apagar) dados, mas só se aplica a dados coletados por um “negócio” “do” residente da Califórnia que exerce o direito. O que exatamente isso significa não está claro neste momento, mas podemos antecipar um debate sobre se os dados coletados por câmeras de CCTV ou dados extraídos de perfis públicos on-line estão sujeitos ao direito de eliminação do CaCPA. Podemos ter certeza de que o CaCPA não apoiaria um caso como o caso Costeja da Espanha, porque o Google não coletou o famoso (ou infame) relatório de falência do jornal de Costeja, mas de um terceiro. Um último ponto: as exceções ao direito de apagar sob o CaCPA também são muito diferentes das razões que justificam o apagamento e os testes de balanceamento embutidos no GDPR e exigirão análises separadas. O CaCPA contém dois direitos para saber: O direito de saber quais informações foram coletadas e o direito de saber quais delas foram compartilhadas. Esses direitos são bastante prescritivos; no entanto, a versão atual do CaCPA contém contradições que dão uma interpretação clara do que deverá ser revelado impossível. As empresas deverão avaliar suas práticas para identificar qual compartilhamento deve ser considerado para “fins comerciais” e qual deve ser considerado para “fins comerciais” sob o CaCPA, já que esses dois propósitos precisarão ser separadamente divulgados. Ao contrário do GDPR, o CaCPA permite que as empresas “vendam”

Igualmente ao GDPR, o CaCPA reconhece uma autoridade temática, qual seja, a Procuradoria Geral da Califórnia (cargo por eleição). As multas podem chegar até a US$ 7.500 por violação. Para ações judiciais, a lei confere 30 dias para a empresa resolver o problema, como condição de procedibilidade da ação. No entanto, a lei da Califórnia afetará qualquer negócio que tenha clientes na Califórnia que atendam a um ou mais dos seguintes testes: faturar pelo menos US$ 25 milhões por ano; interagir com informações para 50 mil ou mais pessoas, lares ou dispositivos; ou fazer metade de sua receita anual com a venda de informações pessoais.

Segundo especula Dipayan Ghosh[574], a principal questão das empresas é o fato de que os requisitos da lei podem ameaçar os modelos de negócios estabelecidos em todo o setor digital. Por exemplo, as empresas que geram receita de publicidade direcionada em plataformas de internet – como Facebook, Twitter e Google – devem, como a lei atualmente prescreve, permitir que os residentes da Califórnia excluam seus dados ou os tragam para provedores de serviços alternativos. Essa restrição pode se estender a provedores de serviços de internet, como AT&T e Verizon, que coletam dados de atividade de banda larga (dados de navegação na web) e poderiam tentar usá-los para gerar perfis comportamentais para permitir a publicidade digital. Essas medidas podem reduzir significativamente os lucros que essas empresas desfrutam atualmente, ou forçar ajustes em suas estratégias de crescimento de receita. Eles também poderiam impactar ainda mais as empresas que anunciam em plataformas digitais, já que o serviço que estão comprando – publicidade altamente segmentada – pode se tornar menos preciso, como resultado das novas proteções oferecidas a consumidores individuais. Algumas empresas podem perder ainda mais, tal qual os *data brokers*, como Acxiom, Epsilon, Experian e Oracle, por exemplo, geram lucros coletando

---

dados pessoais, mas dá aos indivíduos o direito de recusar (ou, no caso de menores de 16 anos, a opção de aceitar) a venda dos seus dados (referidos para como "o direito de dizer não"). Em termos GDPR, esse direito seria uma versão limitada do direito de restringir o processamento nos termos do Artigo 18. A definição de "venda" não é clara, refere-se a transferências para "terceiros" ou "outros negócios" para "transações monetárias ou outra consideração valiosa, "e a orientação do Procurador Geral da California sobre este ponto é esperada. Assim como o GDPR, o CaCPA não permite a discriminação contra indivíduos que exercem seus direitos sob o ato. A CaCPA permite expressamente incentivos financeiros desde que eles não sejam "injustos, irracionais, coercitivos ou de natureza usurária". As provisões da CaCPA sobre discriminação são pouco claras e contraditórias. Por exemplo, o CaCPA declara especificamente que os negócios não estão proibidos de "cobrar do consumidor um preço ou taxa diferente, ou de fornecer um nível ou qualidade diferente de bens ou serviços ao consumidor se essa diferença estiver razoavelmente relacionada ao valor fornecido ao consumidor. Não está claro exatamente qual é o valor fornecido ao consumidor pelos seus próprios dados".

[574] Fellow da New America e da Harvard Kennedy School foi conselheiro de política econômica e tecnológica na Casa Branca de Obama que já atuou em questões de privacidade e políticas públicas no Facebook.

quantidades de dados de consumidores individuais e vendendo-os a terceiros – sejam eles redes de anúncios, profissionais de marketing, varejistas ou qualquer outro tipo de negócio interessado. Esses são precisamente os tipos de práticas diretamente ameaçadas pelos direitos do consumidor de excluir e recusar a venda de dados[575].

Por outro lado, há quem opine que a lei da Califórnia não será um peso para as gigantes da tecnologia sediadas na região. Para Antonio Garcia Martinez, autor do livro 'Chaos Monkeys: Obscene Fortune and Random Failure in Silicon Valley' – indicado como *bestseller* pelo jornal 'The New York Times', é inconcebível pensar que uma lei dessa magnitude não estaria alinhada, previamente, com as empresas de tecnologia[576]. Além disso, o autor, que já trabalhou no Facebook (*monetization team*), explica como o ecossistema de anúncios dessa empresa trata os dados e os parceiros externos:

> To understand why the CCPA won't impact Facebook in any meaningful way requires understanding (at a high level, not to worry) how Facebook's ads ecosystem treats data and outside partners. Unlike much of the ad-tech world, Facebook lives in a walled garden where no data leaves and very little enters. When an advertiser wants to retarget you, it exchanges your contact information with Facebook, both sides agreeing to a pseudonym for you, before placing you in one or more targeting buckets ("shoe shoppers," for example). For Facebook's most powerful and invasive micro-targeting, almost no data is shared between advertiser and publisher, and data middlemen are largely absent. Which is why, if you download your data from Facebook, the juiciest information is in the least remarkable section: "Advertisers Who Uploaded a Contact List With Your Information." Users and journalists fixate on the supposed creepiness of Facebook having a call log for you, for example, but the real targeters are buried in that list of companies sharing contact information. The CCPA won't change this[577].

---

[575] GHOSH, Dipayan. What you need to know about California's new data privacy law, July 11, 2018. **Harvard Business Review**. Disponível em: <https://hbr.org>. Acesso em: 02 nov. 2018. Ver também: DETERMANN, Lothar. **Analysis**: The California consumer privacy act of 2018, 02.jul.2018. Disponível em: <https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/>. Acesso em: 02 nov. 2018; FORBES Technology Council. **How will California's consumer privacy law impact the data privacy landscape?** Forbes. Disponível em: <https://www.forbes.com>. Acesso em: 02 nov. 2018.

[576] Nas palavras de Antonio Garcia Martinez: "Look through the rah-rah triumphalism of the piece, however and you'll see that far from succumbing to some irresistible activist push, incumbents Google and Facebook craftily shaped the legislation to suit themselves. When in the history of American democracy have state legislators voted to severely and onerously regulate trillion-dollar companies in their home districts, motivated only by an overweening concern for consumer rights (and not donor pressure)? Never, is the answer—which is why the implications of CCPA could use some further scrutiny. (Spoiler alert: Facebook doesn't hate the law)". (MARTINEZ, Antonio Garcia. **Why California's privacy law won't hurt Facebook or Google**. Disponível em: <https://www.wired.com>. Acesso em: 02 nov. 2018). Tradução livre: No entanto, veja o triunfalismo rah-rah da peça e você verá que, longe de sucumbir a algum impulso ativista irresistível, os responsáveis pelo Google e pelo Facebook moldaram habilmente a legislação para se adequarem a si mesmos. Quando na história da democracia americana os legisladores estaduais votaram para regular severa e onerosa empresas de trilhões de dólares em seus distritos de origem, motivados apenas por uma preocupação arrogante com os direitos do consumidor (e não com a pressão dos doadores)? Nunca, é a resposta – e é por isso que as implicações do CCPA poderiam usar um pouco mais de escrutínio. (Alerta de *spoiler*: o Facebook não odeia a lei).

[577] MARTINEZ, Antonio Garcia. **Why California's privacy law won't hurt Facebook or Google in wired**. Disponível em: <https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google/>. Acesso em: 02 nov.2018. Tradução livre: Para entender por que o CCPA não impactará o Facebook de maneira

Decorre disso que a lei californiana atinge, especialmente, os tipos de empresas, já comentadas nesse trabalho, conhecidas por *data brockers,* tal qual a Drawbridge e a LiveRamp, cujas atividades são voltadas à prática conhecida como *data onboarding*. Nelas, dados pessoais (nome, endereço ou número de telefone) – que os varejistas tomam conhecimento ao coletar por meio de programas de fidelidade e similares – são convertidos em maneiras de segmentar o indivíduo *on-line*. São justamentes os intermediários, como as empresas Drawbridge e LiveRamp, que conectam *on-line* com *off-line*, comprando os dados pessoais e trabalhando com bases de dados de serviços da internet. Essas empresas fornecem um ecossistema de segmentação alternativo que compete com o *one-stop-shop* do Facebook. A rede de farmácia americana Walgreens, por exemplo, pode usar o LiveRamp, ou concorrentes similares, para segmentar pessoas por meio de trocas de anúncios em tempo real, ou enviar os dados pessoais de seus clientes para o Facebook[578].

Nessa toada, se os articuladores da lei californiana miraram as gigantes da internet, como o Facebook, podem ter errado o alvo e atingido agentes menores ao seu redor[579].

---

significativa, é necessário entender (em um nível alto, não se preocupar) como o ecossistema de anúncios do Facebook trata os dados e parceiros externos. Ao contrário de grande parte do mundo da ad-tech, o Facebook vive em um jardim murado onde nenhum dado sai e muito pouco entra. Quando um anunciante deseja redirecioná-lo, ele troca suas informações de contato com o Facebook, ambos os lados concordam com um pseudônimo para você, antes de colocá-lo em um ou mais grupos de segmentação ("compradores de sapatos", por exemplo). Para a micro-segmentação mais poderosa e invasiva do Facebook, quase nenhum dado é compartilhado entre anunciante e editor, e os intermediários de dados estão praticamente ausentes. É por isso que, se você baixar seus dados do Facebook, as informações mais interessantes estão na seção menos notável: "Anunciantes que enviaram uma lista de contatos com suas informações". Usuários e jornalistas se fixam na suposta estranheza do Facebook com um registro de chamadas para você, por exemplo, mas os alvos reais estão enterrados nessa lista de empresas que compartilham informações de contato. O CCPA não vai mudar isso.

[578] MARTINEZ, Antonio Garcia. **Why California's privacy law won't hurt Facebook or Google in wired**. Disponível em: <https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google/>. Acesso em: 02 nov.2018: “Here’s why Facebook is better positioned for CCPA, or GDPR: It has a direct relationship with you. How does it know every device you use? Because the first thing you do when you buy a new device is log into Facebook, Instagram, or WhatsApp. How does it know your name, phone number, and address? Because you told it those things, or opted into sharing your location via the Facebook app. The California and European privacy rules favor these first-party relationships. Data coming from elsewhere – known as third-party data – is viewed with more suspicion, so this privileged state of affairs is unlikely to change soon. So long as Facebook’s apps remain as addictive as they are, Facebook will know who you are, where you are, and every digital pseudonym for you, whether a browser cookie or a mailing address. Tradução livre: Veja por que o Facebook está melhor posicionado para o CCPA ou o GDPR: ele tem um relacionamento direto com você. Como ele sabe de todos os dispositivos que você usa? Porque a primeira coisa que você faz quando compra um novo dispositivo é entrar no Facebook, Instagram ou WhatsApp. Como ele sabe seu nome, número de telefone e endereço? Porque você disse essas coisas, ou optou por compartilhar sua localização através do aplicativo do Facebook. As regras de privacidade da Califórnia e da Europa favorecem esses relacionamentos de primeiro nível. Dados vindos de outros lugares – conhecidos como dados de terceiros – são vistos com mais desconfiança, portanto é improvável que esse estado de coisas privilegiado mude em breve. Enquanto os aplicativos do Facebook continuarem tão viciantes quanto eles, o Facebook saberá quem você é, onde você está e todo pseudônimo digital para você, seja um *cookie* de navegador ou um endereço de correspondência.

[579] Ultimately, the CCPA is a fatal blow not to Facebook but to the competing middlemen. Shortly before GDPR took effect, Drawbridge announced it was leaving the European market. Then it announced it was leaving advertising altogether. LiveRamp is reported to be up for sale. Facebook itself shut down its Partner Categories

Por fim, importante delimitar que não é tarefa deste trabalho analisar todos os marcos legais sobre privacidade de proteção de dados existentes no mundo. Buscou-se, por meio da exposição realizada nesse item, apresentar o cenário atual e a evolução pela qual passaram o bloco europeu e os Estados Unidos, com vista a situar na pesquisa as dimensões pelas quais a disciplina transcorreu, e, ainda, para verificar como a situação existente pode amparar o uso de algoritmos e os dados pessoais. Isso, porém, não significa que as informações aqui se esgotam de modo que não existam outros países e organizações[580]. A legislação do Canadá, por exemplo, embora não tenha sido abordada, consiste em pioneiro e importante paradigma da área. Porém, essa não é a sede para esgotar o assunto em relação aos diversos regimes existentes. Além disso, até novembro de 2018, o número de países com lei geral de proteção de dados e privacidade no globo alcançava 130 nações.

3.9 Sistema de proteção de dados pessoais no direito brasileiro

Visto a evolução do assunto na Europa e nos Estados Unidos, passamos a dirigir o olhar para o cenário brasileiro. A Constituição Federal de 1988 protege a privacidade e os direitos correlatos[581]. O legislador ao optar por garantir os direitos fundamentais da intimidade e da vida privada (artigo 5º, X) guiou-se pela 'teoria dos

---

program that used targeting segments from data brokers like Acxiom, cutting off its last connection to that world. Under CCPA and GDPR, if you want to target consumers across devices, or use your trove of offline consumer data online, you'll have to use Facebook instead of the few competitors that once eked out a business outside its walled garden. (MARTINEZ, Antonio Garcia. **Why California's privacy law won't hurt Facebook or Google in wired**. Disponível em: <https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google/>. Acesso em: 02 nov.2018). Tradução livre: Em última análise, o CCPA é um golpe fatal não para o Facebook, mas para os intermediários concorrentes. Pouco antes de o GDPR entrar em vigor, a Drawbridge anunciou que deixaria o mercado europeu. Então anunciou que estava deixando a publicidade completamente. O LiveRamp está à venda. O próprio Facebook fechou seu programa de categorias de parceiros que usava segmentação de intermediários de dados como a Acxiom, cortando sua última conexão com esse mundo. De acordo com o CCPA e o GDPR, se você deseja segmentar consumidores em vários dispositivos ou usar seus dados de consumidor off-line ou on-line, você precisará usar o Facebook em vez dos poucos concorrentes que já conseguiram uma empresa fora de seu jardim murado.

[580] Sobre o assunto cite-se apanhado de Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, Orla Lynskey; The data protection credibility crisis, *International Data Privacy Law*, Volume 5, Issue 3, 1 August 2015, pp. 161–162, p. 161: Regional organizations such as Asia-Pacific Economic Cooperation, the Council of Europe, the Organization of American States, the Economic Community of West African States, the Organisation for Economic Co-operation and Development, and others have also done extensive work to enact new privacy instruments or amend their existing ones. All this activity has also had an effect at the global level, with the UN General Assembly passing a resolution that affirms the 'right to privacy in the digital age'. Tradução livre: Organizações regionais como a Cooperação Econômica Ásia-Pacífico, o Conselho da Europa, a Organização dos Estados Americanos, a Comunidade Econômica dos Estados da África Ocidental, a Organização para a Cooperação e o Desenvolvimento Econômico, e outros também fizeram um extenso trabalho para promulgar novos instrumentosa de privacidade ou emendar os já existentes. Toda essa atividade também teve um efeito em nível global, com a Assembléia Geral da ONU aprovando uma resolução que afirma o "direito à privacidade na era digital".

[581] Artigo 5º, XI, XII, IX, XIV, XXXII e XXXIV e artigo 220, todos da Constituição Federal de 1988.

círculos concêntricos da esfera da vida privada' ou 'teoria das esferas da personalidade'[582], formulada na década de 1950, pela doutrina alemã de Heinrich Hubmann e Heinrich Henkel[583].

A Constituição Federal de 1988 também prevê uma modalidade de direito de acesso e retificação dos dados pessoais, conhecida como habeas data. Segundo Willis Santiago Guerra Filho, esse instituto deriva do mandado de segurança, à igualdade do mandado de injunção, fora inspirado na doutrina de José Afonso da Silva,

> e poderá ser empregado na defesa do cidadão contra agressões à sua privacidade e dignidade, perpetrada não apenas pelo Estado mas por entidades privadas, mas que devem igualmente respeito aos direitos fundamentais e podem violá-los com o mesmo grau de intensidade – senão até, com maior intensidade ainda[584].

É possível afirmar que a proteção de dados pessoais também recebe tutela constitucional, embora não venha reconhecida expressamente, conforme observa Danilo Doneda:

> Ao derivarmos a proteção de dados pessoais diretamente da privacidade, tal qual espécie e subespécie, existe uma extensão da tutela da privacidade à proteção de dados pessoais. Tal operação se basta para abarcar a disciplina sob a égide constitucional, arrisca, porém, simplificar os fundamentos da tutela dos dados pessoais e eventualmente limitar o seu alcance[585].

A proteção de dados se revela no ordenamento brasileiro pela ação de habeas data, introduzida pela Constituição Federal de 1988 regulamentada pela Lei n. 9.507/1997[586].

Outros dispositivos foram introduzidos no ordenamento brasileiro nos últimos dez anos a respeito da proteção de dados pessoais. Nesse sentido, a lei do cadastro positivo (Lei n.12.414/2011), que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou jurídicas, para formar histórico de crédito, e cujo texto legal trouxe, pela primeira vez, definição

---

[582] Por essa teoria, a esfera da vida privada do indivíduo possui esferas correspondentes a três círculos concêntricos, como a estrutura de uma cebola. O círculo mais distante do centro corresponde à privacidade, a intermediária corresponde à intimidade e o menor, ao segredo. Essa teoria está ultrapassada e foi abandonada para fins de proteção de dados pessoais, pelo Tribunal Constitucional Alemão, no julgamento do caso do censo, de 1984.

[583] COSTA JUNIOR, Paulo José da. **O direito de estar só**. Tutela penal da intimidade. São Paulo: RT, 1995.

[584] GUERRA FILHO, Willis Santiago. **Processo constitucional e direitos fundamentais**. 6.ed. São Paulo: SRS, 2006, p.186-187.

[585] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.325-326.

[586] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.326.

sobre quais dados podem ser considerados sensíveis (aqueles pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas – artigo 2º, §3º). Ainda, pode ser citada a Lei da Transparência (Lei n.12.527/2011), que trouxe em seu âmbito a definição de que informação pessoal é aquela relacionada à pessoa natural identificada ou identificável (artigo 4º, IV). A primeira lei brasileira, por sua vez, a reconhecer expressamente a distinção entre privacidade e proteção de dados foi o Marco Civil da Internet (Lei n.12.964/2015), ao prever que a disciplina do uso da internet no Brasil tem como princípios, dentre outros, proteger a privacidade (inciso II) e proteger dados pessoais (inciso III).

Dada a sua importância nos deteremos no habeas data, figura original[587] e consistente em uma inovação do constituinte de 1988, plasmada no artigo 5º, LXXII da Constituição Federal. Segundo esse dispositivo, o habeas data será concedido para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; ou para retificar dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo. Segundo o artigo 7º da Lei n.9.507/1997, que regula o direito de acesso a informações e disciplina o rito processual do habeas data, acrescentou-se às duas hipóteses constitucionais, uma terceira, qual seja, o cabimento do remédio constitucional para anotar nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro, mas justificável, que esteja sob pendência judicial ou amigável.

O habeas data foi introduzido para conferir ao cidadão um meio de tomar conhecimento, e, se o caso, alterar as informações sobre sua pessoa armazenadas em bancos de dados de caráter público. Relaciona-se, diretamente, à proteção de dados pessoais do indivíduo, sob o manto da liberdade informacional.

Se requeridas as informações pessoais ou sua retificação perante órgão ou entidade depositária do registro ou banco de dados, e sobrevenha a recusa do ente – que tem o prazo legal de 48h para se manifestar, e mais 24h para comunicar a decisão ao requerente (Lei n.9.507/1997, artigo 2º) – nasce o direito de impetrar o habeas data. É condição de procedibilidade da ação a recusa do órgão, conforme cristalizado em Súmula do Superior Tribunal de Justiça: não cabe o *habeas data*

[587] SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2011, p.136.

(artigo 5º, LXXII, "a") se não houve recusa de informações por parte da autoridade administrativa (Súmula n. 2, DJ 18/05/1990). Nesse sentido pondera Marcel Leonardi:

> A utilização do *habeas data* está diretamente relacionada à existência de uma pretensão resistida, consubstanciada na recusa prévia do mantenedor do cadastro em responder ao pedido de acesso, retificação ou complementação das informações, seja de forma explícita ou implícita, tal como nos casos de omissão ou atraso injustificado[588].

O quadrante de atuação do instrumento constitucional é limitado. Conforme dispõe a lei, os direitos de conhecer ou retificar informações pessoais limitam-se aos dados constantes de registros ou bancos de dados de entidades governamentais ou de caráter público. Segundo o artigo 1º, parágrafo único da Lei n. 9.507/1997, "considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações".

Antes, porém, da lei que regulamentou o *habeas data*, foi previsto no Código de Defesa do Consumidor (Lei n.8078/1990) o direito do consumidor de acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele e suas respectivas fontes (Lei n.8078/1990, artigo 43)[589]. Trata-se, pois, de importante marco na legislação brasileira que resguarda o direito de proteção de dados pessoais do consumidor.

Além disso, por meio da lei consumerista de 1990, foram equiparados a entidades de caráter público os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres (§4°, artigo 43 da Lei n. 8078/1990), de forma que, não obstante o Código de Defesa do Consumidor tenha recebido veto[590]na disposição que previa expressamente a aplicação de *habeas data* à tutela dos direitos e interesses dos consumidores, é possível utilizar o *habeas data* para pedido judicial de conhecimento de dados ou retificação relativa a

---

[588] LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012, p.201-202.

[589] Segundo §3° do artigo 43: O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

[590] O artigo 86, cuja redação vetada era "Aplica-se o habeas data à tutela dos direitos e interesses dos consumidores", recebeu a seguinte justificativa ao veto: "as ações de mandado de segurança e de hábeas data destinam-se, por sua natureza, à defesa de direitos subjetivos públicos e têm, portanto, por objetivo precípuo os atos de agentes do Poder Público. Por isso, a sua extensão ou aplicação a outras situações ou relações jurídicas é incompatível com sua índole constitucional. Os artigos vetados, assim, contrariam as disposições dos incisos LXXI e LXXII do artigo 5º da Carta Magna". (Disponível em: <http://www.planalto.gov.br>. Acesso em: 02 nov. 2018.

informações de consumidores, incluindo casos de internet, conforme pondera Marcel Leonardi:

> O *habeas data* é, portanto, um mecanismo de tutela à disposição do usuário de Internet que, vinculado a uma relação de consumo com um fornecedor, pretenda fazer valer seu direito de acessar os registros existentes em bancos de dados e em cadastros de consumo, bem como retificar ou apagar registros errôneos e complementar registros insuficientes ou incompletos[591].

Em que pese essa garantia, na prática, poucos são os consumidores que, além de não terem conhecimento sobre estes direitos, conseguem controlar suas informações:

> Na prática, porém, apesar da criação de mecanismos para a tutela do consumidor, eles têm pouca efetividade diante da realidade fática: o cidadão médio dificilmente consegue exercer algum controle sobre as suas informações pessoais registradas em inúmeros ´dossiês digitais´[592].

Para a doutrina portuguesa de José Joaquim Gomes Canotilho e Vital Moreira, o direito ao conhecimento dos dados pessoais existentes em registros informáticos é uma espécie de direito básico nesta matéria e equivale ao que já foi chamado de *habeas data.* Por sua vez, esse direito desdobra-se em vários outros: (a) o direito de acesso, ou seja, o direito de conhecer os dados constantes de registros informáticos, quaisquer que eles sejam (públicos ou privados); (b) o direito ao conhecimento da identidade dos responsáveis e o direito ao esclarecimento sobre a finalidade dos dados; (c) o direito de contestação, ou seja, o direito à rectificação dos dados e sobre identidade e endereço do responsável; (d) o direito de actualização (cujo escopo fundamental é corrigir conteúdo dos dados em caso de desactualização); (e) finalmente, o direito a eliminar dados cujos registros são interditos. O direito de acesso, além de universal (vale para todos os registros, públicos ou privados), não pode ficar dependente de condições que restrinjam o seu exercício (*v.g.* pagamento de uma taxa excessivamente onerosa)[593].

Para Willis Santiago Guerra Filho, aplicações ‘criativas’ do *habeas data*, na tutela da ordem jurídica constitucional subjetiva, seria possível, em face de ameaças oriundas do exercício do poder, estatal ou não, através de meios informatizados[594]:

---

[591] LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012, p.200-201.
[592] LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012, p.203.
[593] CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. **Constituição da República Portuguesa Anotada**. v.1. São Paulo: RT; Coimbra: Coimbra, 2007, p.551-552.
[594] GUERRA FILHO, Willis Santiago. **Processo constitucional e direitos fundamentais**. 6.ed. São Paulo: SRS, 2006, p.188.

> Já vem ocorrendo casos em que somos rebaixados na nossa dignidade de sujeitos à condição de meros objetos diante de uma parafernália anônima, eletrônica, mas obviamente controlada por agentes humanos, que nos cerceia direitos básicos como o de perceber integralmente os salários, sem que saibamos como reagir pronta e eficazmente contra tais abusos. Por que não nos valermos do *habeas data*, para nos livrarmos dessa opressora manipulação de dados?[595]

Na análise de Stefano Rodotà, o *habeas data "*si mette in evidenza come forme adeguate di tutela esigano piena consapevolezza dele relazioni di potere implicate dalla dimensione della sorveglianza, e si aggiunge anche che l´appello alla privacy può fornire solo risposte individualizzanti, in se limitate"[596]. Na linha de pensamento do professor italiano, ainda que seja perigoso dizer que *noi siamo i nostri dati,* é verdadeiro que nossa representação social é cada vez mais confiada a informações espalhadas em uma multiplicidade de bancos de dados e aos *profili* que sobre essas bases vem construídos[597].

Para além da proteção instituída pelo artigo 43 do Código de Defesa do Consumidor, existem, ainda, outros deveres de conduta que incidem sobre quem capta ou utiliza informação alheia no mundo *online*. Conforme lembra Anderson Schreiber, não obstante o artigo 43, §2º do Código de Defesa do Consumidor vede a prática de *sites* brasileiros não solicitarem a prévia pemissão do usuário para utilizar *cookies*, armazenar e tratar as informações[598], a imensa maioria deles não segue essa determinação legal nas relações de consumo[599].

Segundo Danilo Doneda, uma análise instrumental para possibilitar a atuação dos direitos de privacidade e proteção de dados pessoais deixa entrever uma proteção que, embora devesse corresponder a uma proteção integrada e dirigida pela tábua axiológica constitucional, atua fracionada, em focos determinados[600].

Esse cenário reforça a necessidade de se criar um sistema específico de proteção aos dados pessoais, o qual demorou a chegar no Brasil.

Antes, porém, importante observar que o legislador do Código Civil brasileiro cometeu uma grande falha, posto que na extensa reforma desse diploma legal, concluída em 2001, ou seja, dentro da sociedade de dados, pouco ou nada fez para

---

[595] GUERRA FILHO, Willis Santiago. **Processo constitucional e direitos fundamentais**. 6.ed. São Paulo: SRS, 2006, p.189.
[596] RODOTÀ, Stefano. **Il diritto di avere diritti**. Bari/Italia: Laterza, 2012, p.31.
[597] RODOTÀ, Stefano. **Il diritto di avere diritti**. Bari/Italia: Laterza, 2012, p.31.
[598] Artigo 43, §2° do Código de Defesa do Consumidor: "A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele".
[599] SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2011, p.151.
[600] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.29.

resguardar a proteção de dados dos *civis.* Ao relacionar o *habeas data* com o Código Civil, Anderson Scheireber destaca:

> Figura original na experiência jurídica, o *habeas data* apresenta-se como instrumento utilíssimo para evitar e corrigir violações à privacidade. [...] A marcha promissora e criativa do direito brasileiro na proteção à privacidade deteve-se, contudo, por aí. O voo auspicioso do texto constitucional não alcançou o Código Civil de 2002, nem qualquer dos diplomas normativos editados na última década. Excessivamente abstrata, a regulação da privacidade permaneceu nas nuvens dos comandos genéricos. E o Código Civil cometeu o disparate de dedicar um único artigo ao tema[601].

O Código Civil brasileiro foi omisso ao deixar de tratar de tema de tamanha relevância, da proteção de dados pessoais[602]. As discussões na Europa sobre o assunto estavam em seu auge porque poucos anos antes fora aprovada regulamentação sobre o tema (Diretiva n. 46/95). Além disso, na América Latina, países como Chile e Argentina já discutiam e aprovavam suas leis setoriais a respeito. Nada disso parece ter sido suficiente para mobilizar o legislador do Código Civil brasileiro a inserir a tutela de proteção de dados pessoais em seu diploma.

Vê-se no Brasil, com atraso, o início de uma formação de 'consciência de proteção de dados'. É justamente nesse sentido que Stefano Rodotà pregou não acreditar que a única reação possível seja a da aceitação acrítica, quase uma rendição, em direção a uma sociedade inevitavelmente transparente[603]. Para Danilo Doneda, sendo o perfil da população brasileira heterogênea, seu interesse primordial está voltado para outras tutelas relativas às necessidades básicas. Além disso, para esse autor, a necessidade de uma sociedade de estabelecer mecanismos de proteção de dados pessoais varia conforme o padrão médio de consumo de sua população e da própria penetração da tecnologia em seu cotidiano[604].

---

[601] SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2011, p.136: "O Código Civil brasileiro deu à privacidade um tratamento inadequado. Em primeiro lugar, dedicou um único artigo à matéria, cuja importância se renova a cada dia na sociedade contemporânea. Nesse dispositivo solitário, o legislador limitou-se, [...] a um enunciado genérico, que não acrescenta rigorosamente nada ao que já se encontrava previsto na Constituição. Perdeu, assim, a oportunidade de oferecer parâmetros para a solução de diversos conflitos concretos ligados à tutela da privacidade. Não bastasse isso, empregou a expressão vida privada, revelando certa indiferença à recente evolução do conceito de privacidade, que abandonou uma concepção mais restrita, limitada ao círculo da intimidade da pessoa humana, para abarcar a proteção aos dados e informações pessoais. Sobre esse último aspecto, a codificação não trouxe uma palavra sequer. Não é exagero dizer que o Código Civil ignorou a vasta amplitude do tema, cuja compreensão é essencial para perceber o importante papel reservado à tutela da privacidade no século XXI" (p.128).

[602] Segundo Anderson Schriber, o estrago só não é maior porque o Código de Defesa do Consumidor ocupa-se do assunto em seu artigo 43. (SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2011, p.150).

[603] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.9.

[604] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.29.

Porém, utilizar o argumento de um direito fundamental de menor magnitude seria uma via retórica de uso político[605] e econômico para investir no desenvolvimento da disciplina de privacidade e da proteção de dados pessoais.

A história se repete. Na América Latina, o Brasil foi o último país a adotar um Código Civil (o primeiro foi o Chile, em 1855). Incrivelmente, até 1916, eram as ordenações reais portuguesas que regulamentavam os atos civis dos brasileiros, não obstante já se distanciasse em muitos anos a data da independência. Novamente, o Brasil está no final da fila. É um dos últimos países no cone sul da América a incorporar um sistema legal de proteção de dados. São os chilenos, outra vez, a começar (1999), seguidos pelos argentinos (2000) e outros na sequência (Uruguai, México, Peru, Costa Rica, Nicarágua, Colômbia e República Dominicana).

É inevitável que o direito caminhe com atraso em relação à tecnologia, mas, no Brasil, a demora para se aprovar um sistema de proteção de dados pessoais já tinha esgotado o mais paciente dos virtuosos. Além disso, a aprovação da lei consiste em condição para o Brasil pleitear uma vaga na Organização para a Cooperação e Desenvolvimento Econômico (OCDE)[606].

O Brasil tinha previsão para proteger dados em leis esparsas – a exemplo do Marco Civil da Internet e de breves disposições no Código Civil e no Código de Defesa do Consumidor, dentre poucos outros textos legais, que não eram suficientes para a realidade do mercado de dados atual. A economia do *big data*, impulsionada pela internet das coisas, das cidades inteligentes e da inteligência artificial não poderia resistir ao vácuo das regras jurídicas do jogo. A cultura atual dos algoritmos exige uma posição do Estado para regulamentar o assunto, sob pena de comprometer direitos fundamentais dos cidadãos (liberdade, privacidade, livre desenvolvimento da personalidade). E não apenas isso. A existência de lei específica traz mais segurança jurídica, o que fomenta a economia e atrai investidores ao país, uma vez que, agora, as regras são mais claras em relação ao tratamento de dados pessoais.

Finalmente, em 14 de agosto, o Presidente Michel Temer sancionou a Lei Geral de Proteção de Dados (Lei n.13.709/2018), que dispõe sobre a proteção de dados pessoais no Brasil, inspirada no sistema europeu, e insere o país, com certo

---

[605] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.29-30.
[606] TRUFFI, Renan. Por vaga na OCDE, governo articula criar órgão para proteção de dados na internet. 13 de abril 2018. **O Estado de S. Paulo**. Disponível em: <https://economia.estadao.com.br/noticias/geral,por-vaga-na-ocde-governo-articula-criar-orgao-para-protecao-de-dados-na-internet,70002266200>. Acesso em: 02 nov. 2018.

atraso, no rol dos países mundiais possuidores de marco legal na área de proteção de dados[607]. O Brasil torna-se o 127º país, no mundo, a ter uma legislação de proteção de dados pessoais.

O veto ao dispositivo que criaria uma autoridade nacional de proteção de dados[608], à qual caberia implementar, fiscalizar e deliberar sobre a aplicação da nova lei, causou grande decepção aos especialistas[609]. Nesse sentido, Ronaldo Lemos predicou a lei brasileira de desgovernada, acéfala, texto fantasma, e lei morta-viva[610]. Porém, no apagar das luzes do governo federal, o presidente Michel Temer editou a Medida Provisória n. 869 de 27 de dezembro de 2018, que alterou a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e criar a Autoridade Nacional de Proteção de Dados[611], composta pelo Conselho Diretor (órgão máximo de direção); Conselho Nacional de Proteção de Dados Pessoais e da Privacidade[612]; corregedoria; ouvidoria; órgão de assessoramento jurídico próprio; e unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.

---

[607] Paradoxalmente, tramita com celeridade no Congresso Nacional uma proposta de lei (Projeto de Lei n. 441/2017) que visa conceder aos birôs de crédito uma ampla gama de dados sobre todos os brasileiros maiores de idade e economicamente ativos, e cuja proposta vem sendo criticada por entidades representantes dos consumidores.

[608] O veto aos artigos 55 a 59, os quais se conferiam à criação da Autoridade Nacional de Proteção de Dados (ANPD), como integrante da administração pública federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça, com suas respectivas atribuições (artigo 56), receitas (artigo 57), composição (artigo 58) e função (artigo 59). A Presidência da República apresentou como razões do veto: "Os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, §1º, II, 'e', cumulado com o artigo 37, XIX da Constituição." (Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm>. Acesso em: 05 nov. 2018).

[609] O próprio texto da Exposição de Motivos da Medida Provisória n. 869/2018, que será mencionado em seguida, reconheceu em sua alínea 6: "Sobre a urgência e relevância da medida, necessário ressaltar que embora a ANPD estivesse prevista na Lei nº 13.709, de 2018, sua inclusão se deu de forma irregular, gerando vício de iniciativa na proposta, o que levou à necessidade do veto presidencial ao capítulo que tratava da matéria. O veto, acabou por gerar grande risco de insegurança jurídica para a Sociedade Civil em face da falta de definição do órgão responsável pela regulação, controle e fiscalização da aplicação da Lei, o que deve ser definido o quanto antes para permitir que o órgão criado esteja em pleno funcionamento quando da entrada em vigor desta proposta, para garantir sua plena e total aplicabilidade".

[610] LEMOS, Ronaldo. Lei de dados nasceu desgovernada. **Folha de S. Paulo**, 20 ago. 2018. "O resultado é a aprovação de uma lei que cria pesadas obrigações jurídicas, mas é acéfala. Em outras palavras, é uma lei morta-viva. Tal como um zumbi de seriado de televisão, suas normas serão colocadas em movimento. Mas esse movimento será errático e imprevisível. Em vez de haver uma autoridade que uniformiza sua aplicação, a lei será interpretada de forma atomizada por cada um dos mais de 17 mil juízes de primeira instância do país. Serão necessários três a quatro anos de vigência para que as decisões comecem a chegar aos tribunais superiores, quando só então começarão a se uniformizar. Até lá, valerá a incerteza.

[611] Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados – ANPD, órgão da administração pública federal, integrante da Presidência da República."

[612] Artigo 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: I – propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; II – elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; III – sugerir ações a serem realizadas pela ANPD; IV – elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e V – disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral.

Dentre outras alterações, a Medida Provisória ampliou o prazo de *vacatio legis* de 18 para 24 meses a contar da publicação da Lei.

A lei de proteção de dados pessoais (LGPD) regula o tratamento de dados pessoais realizado por pessoa natural ou jurídica de direito público ou privado, visando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade do indivíduo. Por tratamento entende-se qualquer operação de tratamento, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que (i.) a operação de tratamento seja realizada no território nacional, exceto os provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência; (ii.) a atividade de tratamento tenha por objetivo oferecer ou fornecer bens, serviços ou tratamento de dados de indivíduos localizados no território nacional; (iii.) os dados pessoais objeto do tratamento tenham sido coletados no território nacional, ou seja, os dados pessoais cujo titular nele se encontre no momento da coleta.

O âmbito da LGPD não alcança o tratamento de dados pessoais (i.) realizado por pessoa natural para fins exclusivamente particulares e não econômicos; (ii.) realizado para fins exclusivamente jornalísticos e artísticos, ou acadêmicos; ou (iii.) para fins de segurança pública; defesa nacional; segurança do Estado; ou de atividades de investigação e repressão de infrações penais[613]; ou (iv.) provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

No ecossistema da proteção de dados, a LGPD introduziu, além do *titular* (pessoa natural a quem se referem os dados pessoais objeto de tratamento), o *controlador*, pessoa natural ou jurídica, de direito público ou privado, a quem

[613] Para esses casos de tratamento de dados deverá sobrevir legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. (§1º do artigo 4º da LGPD). Para esses casos em referência é vedado o tratamento dos dados por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional, mas jamais podendo, à pessoa de direito privado, receber a totalidade dos dados pessoais de banco de dados (§§2º e 4º do artigo 4º da LGPD). A nova redação dada pela MP n. 869/2018 modificou a redação para: [...]

competem decidir sobre o tratamento de dados pessoais; do *operador*, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; do *encarregado*, pessoa[614] indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional. O controlador e o operador são, legamente, *agentes de tratamento.*

O legislador brasileiro elencou como fundamentos da proteção de dados, o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania (artigo 3º).

As atividades de tratamento de dados pessoais deverão observar os princípios da boa-fé, da finalidade, da adequação, da necessidade, da qualidade dos dados, da transparência, da segurança da prevenção, da não discriminação e da responsabilização e prestação de contas, conforme dispõe o artigo 6º da LGPD[615].

O tratamento de dados pessoais só será realizado (artigo 7º da LGPD), na hipótese de: (i.) fornecimento de consentimento pelo titular; (ii.) para cumprir obrigação legal ou regulatória pelo controlador, caso em que o titular deverá ser avisado do tratamento; (iii.) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos

[614] A redação da Lei previa a indicação de pessoa *natural*, o que foi alterado com a MP n. 869/2018, de forma a possibilitar que o DPO seja tanto pessoa física como jurídica, a exemplo da sistemática do GDPR.

[615] Artigo 6º da LGPD: I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

congêneres, casos em que o titular deve ser avisado; (iv.) para realizar estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (v.) quando necessário para executar contrato ou procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; (vi.) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; (vii.) para proteger a vida ou incolumidade física do titular ou de terceiro; (viii.) para tutelar a saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; (ix.) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou (x.) para proteger o crédito, inclusive quanto ao disposto na legislação pertinente.

Das hipóteses permissivas para tratamento de dados pessoais, têm gerado mais discussões aquelas relativas ao consentimento e ao legítimo interesse. Não é objetivo desse trabalho ingressar nesse tema, mas importante registrar o balizamento legal do artigo 10 da LGPD, cujo dispositivo determina que o interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam ao apoio e à promoção de atividades do controlador; e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais previstas em lei. Ademais, quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, de maneira que o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

No caso do tratamento de dados pessoais cujo acesso seja público, deve ser considerada a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. Nos casos em que os dados se tornaram manifestamente públicos pelo titular, é dispensada a exigência do consentimento, resguardados os direitos do titular e os princípios legais, nos moldes dos §§3º e 4º do artigo 7º da LGPD.

Toda essa explicação dogmática, porém, não retira de vista que um dos maiores desafios, ainda, no Brasil, é incutir no cidadão comum a autoconsciência de

seus direitos sobre a proteção de dados pessoais[616]. A aprovação da lei tem uma finalidade material objetiva, e é absolutamente destituída da capacidade de, *per si*, gerar transformação social. A questão se torna ainda mais preocupante ao perceber, conforme exaustivamente comentado ao longo desse trabalho, que os dados pessoais dos brasileiros estão sendo usados, em larga escala, pelo mercado de dados, com a sofisticação de aplicação da inteligência artificial e *machine learning,* as quais pela complexidade que lhes são inerentes derivadas da técnica, afastam, ainda mais, o cidadão da compreensão sobre o tratamento de seus dados e como (e se poderia) exercer controle sobre eles. A partir dessa reflexão, adentra-se à última parte da pesquisa, focada nas implicações da área de proteção de dados pessoais na cultura do algoritmo.

[616] Marcel Leonardi comenta o desprezo dos indivíduos sobre a tutela de situações envolvendo problemas de privacidade na internet. (LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012, p.367-368).

4 CULTURA DO ALGORITMO

> Quanto maior a nossa capacidade de entender a experiência humana, melhor o design que teremos.
> **Steve Jobs (1955 – 2011)**

4.1 Novas formas de controle

Há anos, diversos teóricos se voltaram ao estudo da fórmula social da informação inserida na vida contemporânea, conforme visto no primeiro capítulo do presente trabalho.

A cibernética e o modelo neoliberal, diversamente do esperado, acabaram comprometendo a liberdade individual ao invés de alargá-la[617]. O horizonte de maior liberdade, prometido pela chegada da internet e das redes sociais, por um determinado aspecto, portanto, retrocedeu[618]. “A web falhou em seu objetivo de salvar a humanidade” afirmou, recentemente, Tim Berners-Lee, inventor do protocolo word wide web. A crescente centralização da internet, diz ele, “acabou produzindo um fenômeno de larga escala que é anti-humano”[619].

A cultura do algoritmo, presente na sociedade da informação, apoiada na economia de dados e no mercado da atenção, acarreta uma centralização de controle, que acaba por ditar a dinâmica dos indivíduos em muitos setores de suas vidas. O panóptico digital, agora, é estruturado por algoritmos. Em decorrência de seu controle, os gigantes da internet determinam o que será exibido; o aplicativo de trânsito indica qual o melhor caminho a seguir; o site de relacionamentos propõe quais os pares mais indicados para um encontro; cálculos algoritmos decidem sobre concessão de crédito e até mesmo avaliam e decidem sobre pedidos judiciais, dentre outros exemplos. Esta situação faz lembrar a época do direito vulgar na Idade Média, quando, diante de significativo arrefecimento cultural, o poder da escrita e da

---

[617] PARENTE, Alessandra. **Cibernética e neoliberalismo**: a crítica como mercadoria. (no prelo).

[618] Em outro enfoque, sobre liberdade democrática e inteligência artificial: MARANHÃO, Juliano Souza de Albuquerque. E-Democracia é democracia. **JOTA**, publicado em 26.dez.2018. Disponível em: <https://www.jota.info/?pagename=paywall&redirect_to=//www.jota.info/opiniao-e-analise/artigos/e-democracia-26122018>. Acesso em: 07 jan. 2019.

[619] BROOKER, Katrina; BERNERS-LEE, Tim. The man who created the world wide web, has some regrets. **Vanity Fair Magazine**, ago. 2018. Disponível em: <https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets>. Acesso em: 15 dez. 2018; CARNEIRO, Rafael. A internet falhou. 23.jul.2018 **Revista Época**. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2018/07/internet-falhou-diz-criador-da-world-wide-web.html>. Acesso em: 15 dez. 2018. Da reportagem, destacamos outra afirmação de Tim Berners-Lee: "Há pessoas trabalhando e tentando imaginar como a web poderia ser diferente. Como a sociedade na internet poderia ser diferente. O que aconteceria se as pessoas tivessem privacidade e controle sobre seus dados”.

reprodução pertencia a uma pequena classe, concentrada nos monges beneditinos. É justamente nesse sentido que Alessandra Parente articula seu argumento:

> Com a cultura do algoritmo vê-se, então, uma revoada de grande magnitude. Estamos às voltas com uma espécie de comando do saber e das escolhas equiparável apenas ao que ocorria sob os poderes da Igreja Católica. Se antes o domínio da leitura e da escrita era exclusivo de padres, bispos, abades e monges, hoje são poucos aqueles que dominam a linguagem algorítmica e detém o poder das diferentes plataformas da internet. Comparável às exegeses bíblicas da Idade Média, realizadas apenas por grupos fechados, temos atualmente poucas empresas que dominam a Cultura do Algoritmo, capaz de governar a maior parte do globo[620].

Existe uma reserva cibernética, diante da qual se verifica que algumas poucas pessoas tomam a decisão de como nos comportamos[621]. Há quem defenda a necessidade de romper o monopólio dessas empresas antes que elas consigam controlar e manipular todos os setores da sociedade. Em 01.11.2017, um executivo do Facebook admitiu publicamente que entre janeiro de 2015 e agosto de 2017, cerca de 146 milhões de usuários podem ter visto conteúdos mentirosos e enganadores veiculados por agentes do Kremlin.

Ainda, em junho de 2014, um estudo revelou que a rede social Facebook, durante uma semana, manipulou o *feed* de notícias de aproximadamente 700 mil usuários para avaliar o 'contágio emocional' das publicações. Os testes foram realizados em janeiro de 2012 e revoltaram usuários da plataforma. O estudo – que não foi comunicado previamente às 'cobaias digitais' – foi realizado em conjunto com a Universidade de Cornell e com a Universidade da Califórnia, e pretendeu verificar se o número de palavras positivas ou negativas nas mensagens lidas pelos usuários resultaria em atualizações positivas ou negativas de seus posts. O Facebook manipulou o algoritmo usado para distribuir os *posts* no *feed* de notícias do usuário para verificar como isso afetava seu humor. A conclusão resultou no estudo publicado nos anais da Academia Nacional de Ciências[622].

A força de manipulação do Facebook, do Google e de outras gigantes do ramo de tecnologia é inegável. E tal força advém de seus algoritmos, por meio dos

---

[620] PARENTE, Alessandra. **Cibernética e neoliberalismo**: a crítica como mercadoria. (no prelo), p.3.

[621] ABRUSIO, Juliana. Big Data e as fragilidades do sistema internacional nos meios digitais. Congresso Internacional Para a Promoção de Debates Acerca do Direito da Concorrência e Inovação Tecnológica Diante da Realidade e Desafios da Economia Digital, 2018, São Paulo. **Concorrência e Inovação** v.1. São Paulo: Scortecci, 2017, p.47-41.

[622] KRAMER, Adam D. I.; GUILLORY, Jamie E.; HANCOCK, Jeffrey T. **Experimental evidence of massive-scale emotional contagion through social networks**. Proceedings of the National Academy of Sciences of the United States of America (17/06/2014). Disponível em: <http://www.pnas.org/content/111/24/8788.full>. Acesso em: 21 ago. 2018.

quais manipulam a forma de vida contemporânea, valendo-se dos dados pessoais. Tamanho domínio de mercado atinge não apenas a falta de concorrência, mas é uma ameaça à liberdade individual, à autonomia de construir a própria personalidade e à proteção de dados pessoais.

Do indivíduo ao sujeito digital, a vida atual lida com essa crescente demanda por experiências e encontros no mundo digital, pautados por determinações algorítmicas. As características de uma determinada pessoa – verdadeiras ou não – hoje em dia, são mais detectáveis através da mineração e triangulação de múltiplas fontes vinculadas aos seus dados pessoais, com a afirmação de sua identidade por reconhecimento de grupos, redes sociais e outras presenças digitais. Vê-se como a identidade, hoje, tem sido percebida por construções e padrões digitais. Nesse contexto, há uma forte influência da capacidade de persuasão dos processos algorítmicos, que buscam otimizar as interações humanas em um número crescente de setores. Os algoritmos, portanto, integram a percepção da construção da própria identidade.

Pode ser assustador pensar que o uso de algoritmos aplicados a uma imensidão de dados disponíveis é capaz de moldar e direcionar a vida dos indivíduos, os quais são cada vez mais influenciados, e, portanto, governados, com base nos dados gerados a partir dos comportamentos e das interações ditados pela máquina algoritma. As tradicionais representações de identidade – de si mesmo e do outro (alteridade) – da moralidade, das relações sociais, da cultura, estão passando por uma série de mudanças socioculturais devido à cultura dos algoritmos. Na lição de Peter Burgess, Luciano Floridi, Aurélie Pols e Jeroen Van Hoven:

> The distinction between the forces that govern everyday life and persons who are governed within it thus become more difficult to discern. In some contexts, algorithmic profiling – carried out by means of behavioural economics for purposes ranging from exploiting detected vulnerabilities in personalised marketing strategies to the influencing of human behaviours through environmental, contextual, informational stimuli – gradually transform how we may govern ourselves[623].

[623] BURGESS, Peter; FLORIDI, Luciano; POLS, Aurélie; HOVEN, Jeroen van. **Ethics advisory group**. Towards a digital ethics. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf>. Acesso em: 18 nov. 2018, p.11. Tradução livre: A distinção entre as forças que governam a vida cotidiana e as pessoas que são governadas dentro dela torna-se assim mais difícil de discernir. Em alguns contextos, o perfil algorítmico – realizado por meio da economia comportamental para fins que vão desde a exploração de vulnerabilidades detectadas em estratégias de marketing personalizadas até a influência de comportamentos humanos através de estímulos ambientais, contextuais e informativos – transforma gradualmente como podemos nos governar.

Algoritmos também são capazes de analisar nosso comportamento, incluindo análises preditivas, ou seja, antes mesmo do comportamento ocorrer, conforme já abordado nesse trabalho. Por esse viés, é possível afirmar que os algoritmos controlam e influenciam o presente e o futuro da vida dos indivíduos. Ao analisar o que os gigantes da Internet são capazes de operar, Agnieszka Czernik opina:

> Google, Facebook und Co. berechnen, was wir noch selbst nicht wissen und zeigen uns im Internet die Dinge, die wir sehen sollen bzw. dürfen. So erhalten beispielsweise zwei Nutzer unterschiedliche Ergebnisse, wenn sie in der Suchmaschine den gleichen Begriff eingeben. Am Ende entscheidet der Suchalgorithmus, welche Inhalte dem Nutzer angezeigt werden[624].

Dito isso, a autora formula, então, as seguintes indagações: mas os algoritmos realmente possuem cada vez mais controle sobre nós e nossas atitudes e decisões? É possível, de fato, que os algoritmos sejam capazes de influenciar seres complexos como o ser humano de modo a orientar seus próprios pensamentos? Segundo Agnieszka Czernik, certamente os algoritmos tem parcela significativa nas influências de um indivíduo, mas a ação propriamente dita permanece conosco, de modo que nós decidimos clicar ou não em um determinado conteúdo; somos nós, segundo Agnieszka Czernik, quem decidimos quais dos nossos dados divulgamos e se continuamos a usar o Google e o Facebook como nosso principal canal de informações: “Das sollte jeder für sich selbst entscheiden, bewusster mit der Preisgabe seiner Daten umgehen und (wenn möglich) auch mal den Stecker ziehen”[625].

Em parte discordamos da respeitada posição da autora, uma vez que não é mais possível ter a exata dimensão de quais dados divulgamos durante nossa rotina inserida na ubiquidade computacional. A vida contemporânea praticamente exige a utilização de diversas ferramentas, sites, aplicativos, sem os quais o dia a dia seria mais difícil. Abrir mão do uso de tantos recursos, em defesa de uma ideologia de manter consigo os dados pessoais, seria escolher a via de um eremita analógico em

---

[624] CZERNIK, Agnieszka. **Was ist ein algorithmus**. Definition und Beispiele, 14.10.2016. Disponível em: <https://www.datenschutzbeauftragter-info.de/was-ist-ein-algorithmus-definition-und-beispiele/>. Acesso em: 19 nov. 2018. Tradução livre: Google, Facebook e companhia calculam o que nem sequer nos conhecemos e nos mostram na Internet as coisas que devemos ou podemos ver. Por exemplo, dois usuários recebem resultados diferentes quando inserem o mesmo termo no mecanismo de pesquisa. No final, o algoritmo de busca decide qual conteúdo é exibido para o usuário.

[625] CZERNIK, Agnieszka. **Was ist ein algorithmus**. Definition und Beispiele, 14.10.2016. Disponível em: <https://www.datenschutzbeauftragter-info.de/was-ist-ein-algorithmus-definition-und-beispiele/>. Acesso em: 19 nov.2018.Tradução livre: Todos devem decidir por si mesmos, conscientemente lidar com a divulgação de seus dados e (se possível), por vezes, puxar o plugue.

meio a uma selva digital. Talvez esse caminho não seja mais possível na complexa vida do século XXI.

Na análise de Virgílio Almeida e Danilo Doneda, os algoritmos, associados a grandes massas de dados, tem criado serviços globais extremamente eficientes e convenientes, como plataformas de busca na internet, serviços de comunicação por mensagens, redes sociais, comércio eletrônico e serviços financeiros. Entretanto, por outro lado,

> esses algoritmos, que cada vez mais influenciam o comportamento dos indivíduos e da sociedade, são extremamente complexos. Por isso mesmo cresce a necessidade de se obter informações sobre como e por que os algoritmos tomam suas decisões, afim de que não se tornem caixas pretas que operam em função de interesses muitas vezes ocultos[626].

O caráter *black box*, ou seja, a opacidade associada aos algoritmos, é uma das maiores fontes de atenção e preocupação na atualidade. Isto posto, é importante fazer um recorte axiológico aqui. O desenvolvimento tecnológico precisa conviver em harmonia com a preservação da privacidade e proteção de dados pessoais. Não se pode, simplesmente, atacar a tecnologia, visando extirpá-la a fim de proteger esse direito fundamental. Nas palavras de Laura Schertel Mendes:

> Ao se analisar o tema da proteção de dados pessoais na sociedade da informação, é fundamental compreender que o cerne do problema não está situado na tecnologia. Afinal, a tecnologia não se encontra em um vácuo, devendo ser compreendida a partir do meio social, econômico e político em que está inserida. Isso porque a própria tecnologia é criada pela sociedade para atingir determinados fins e o grau de sua regulação é estabelecido pela sociedade que a criou. Nesse sentido, é fundamental que o debate sobre a proteção de dados pessoais tenha como foco as opções jurídicas e econômicas relativas às funções que a tecnologia deve assumir na sociedade, rejeitando-se a ideia de que ela é a responsável pela perda de privacidade pessoal da sociedade contemporânea. Isto é, não é a tecnologia em si a causa do problema da privacidade, mas as decisões que tomamos em relação à tecnologia[627].

Não adianta lamentar ou atacar a nova vida ditada por algoritmos. É irreversível. Por isso mesmo, com a utilização cada vez mais frequente do aprendizado de máquinas, é necessário que o Brasil – a fim de garantir a não violação do direito à privacidade e à proteção de dados pessoais – conforme alertam Virgílio Almeida e Danilo Doneda, “discuta políticas e os princípios que devem reger

---

[626] ALMEIDA, Virgílio; DONEDA, Danilo. **A política e os algoritmos**: o caso do STF. 08 fev. 2017. Disponível em: <https://www.poder360.com.br>. Acesso em: 01 out. 2018.

[627] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.34.

as decisões baseadas em algoritmos, sob o risco de que se consolide mais uma camada de opacidade em mecanismos decisórios"[628]. E nesse sentido, infelizmente, não se pode deixar de destacar, com toda ênfase, que houve um retrocesso no texto da MP n. 869/2018, que modificou a LGPD, ao retirar a possibilidade de revisão por pessoa natural em sistemas algoritmos. Com isso, praticamente, aniquilou-se o denominado 'direito à explicação'. Além disso, faltou inserir na lei, diretamente, conceitos de *privacy by design* e *by default*[629]*.*

Retomando o assunto do caráter *black box* associado aos algoritmos, Frank Pasquale, ao escrever 'The Black Box Society: the secret algorithms that control money and information', aponta que um tipo de situação adversa está em jogo, em que o adversário é a propria regulação em si, instigando a seguinte hipótese: e se os controladores mantiverem, propositadamente, seus feitos de forma opaca, justamente para evitar ou confundir a regulação?[630] Por isso adverte que "secrecy is approaching critical mass, and we are in the dark about crucial decisions. Greater openness is imperative"[631].

Para Frank Pasquale deve haver menor esforço de concentração em tentar controlar a coleta de dados, e mais esforço em regular o uso desses dados – como as empresas e os governos estão realmente implantando regras para tomar decisões[632].

O acesso propriamente dito aos dados é apenas uma das questões a se cuidar, visto que as decisões críticas são tomadas não com base nos dados em si, mas na base de dados analisadas pela máquina algorítmica. Frank Pasquale, nessa vereda, opine: "failing clear understanding of the algorithms involved – and the right to challenge unfair ones – disclousure of underlying data will do little to secure reputational justice"[633]. A partir daqui, percebe-se claramente que o assunto envolve

---

[628] ALMEIDA, Virgílio; DONEDA, Danilo. **A política e os algoritmos**: o caso do STF. 08 fev. 2017. Disponível em: <https://www.poder360.com.br>. Acesso em: 01 out. 2018.

[629] Tanto o direito à explicação como os conceitos de *privacy by design* e *by default* serão abordados mais adiante no presente capítulo.

[630] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p.2.

[631] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p.3. Tradução: o sigilo está se aproximando da massa crítica, e estamos no escuro sobre decisões cruciais. Maior abertura torna-se imperativa.

[632] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p.141.

[633] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p. 19-20. Tradução livre: Falhar na compreensão clara dos algoritmos envolvidos – e o direito de desafiar os injustos – a divulgação de dados subjacentes fará pouco para garantir a justiça da reputação.

uma discussão ética de grande revelância, o que se passa a analisar, com mais demora, no próximo item.

4.2 Ética algorítmica

Atualmente, há intensos debates, em especial na Europa, sobre se a "ética algorítmica" deve ser introduzida ou mesmo regulada pela política.

Jack Balkin cunhou a expressão *information fiduciary* para descrever a obrigação ética e legal das empresas de tecnologia, incluindo as mídias sociais, para com os titulares de dados pessoais, sendo esses últimos dependentes e vulneráveis perante aqueles[634]. Segundo Jack Balkin, as empresas de tecnologia, com base na confiança de seus usuários, não podem manipulá-los. O autor insere esse princípio, em especial, no uso da inteligência artificial e algoritmos de aprendizagem de máquina, cujos processadores devem ser considerados fiduciários das informações de seus usuários. Além disso, segundo Jack Balkin, as empresas que operam com tomada de decisões automatizadas não podem incorrer no que chama de *algorithmic nuisance,* ou seja, utilizar dados pessoais para discriminar e manipular indivíduos, transferindo os custos das decisões automatizadas algorítmicas para o público em geral[635]. A observância de não incorrer nesse "inconveniente algorítmico" é considerado, por Jack Balkin, como uma das novas leis da robótica, a qual deve ser direcionada não às máquinas, mas aos seres humanos e às organizações que as projetam, as possuem e as operam[636].

A autoridade de proteção de dados da União Europeia, *European Data Protection Supervisor*, criou, em 03 de dezembro de 2015, o *Ethics Advisory Group* sobre as dimensões éticas da proteção de dados. Em 2018, esse grupo emitiu o Relatório denominado *Towards a digital ethics*[637], cujo documento reconhece que a nova ética digital está baseada no direito fundamental à privacidade e à proteção de dados pessoais, entendendo crucial essa observância ética para a proteção da dignidade humana, que é a base da Carta de Direitos Fundamentais da União

---

[634] BALKIN, Jack M. Information fiduciaries and the first amendment. **UC Davis Law Review**, v.48, p.1183-1234.
[635] BALKIN, Jack M. Sidley Austin distinguished lecture on big data law and policy: the three laws of robotics in the age of big data. **Ohio State Law Journal**, v.78, 2017, p.1217-1241.
[636] BALKIN, Jack M. Algorithms and big data. **Entrevista concedida à Yale Law School**. Disponível em: <https://www.youtube.com/watch?v=6nKNAa1R4H4>. Publicado em 23 fev.2017. Acesso em: 24 dez. 2018.
[637] BURGESS, Peter; FLORIDI, Luciano; POLS, Aurélie; HOVEN, Jeroen van. **Ethics advisory group**. Towards a digital ethics. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf>. Acesso em: 18 nov. 2018. Composição desse grupo em 2018: J. Peter Burgess, Luciano Floridi, Jaron Zepel Lanier, Aurélie Pols, Antoinette Rouvroy, Jeroen van den Hoven.

Europeia. Ademais, o documento, ao passo que reconhece a evolução tecnológica, impõe que esta deve ser norteada por valores humanos, os quais devem permanecer intocados pelas tecnologias. Nesse sentido, identifica várias iniciativas tecnológicas e diversas tendências que exigem um repensar entre a relação da tecnologia e do humano.

Ainda, o relatório (do *Ethics Advisory Group*) classifica os temas da transparência e da *accountability* dos algoritmos dentre os mais vividamente debatidos dos nossos tempos. Porém, ao mesmo tempo em que fazem esse importante reconhecimento, alertam os autores do relatório que, não obstante a essa condição, tornar os algoritmos mais transparentes e responsáveis não pode significar qualquer diminuição ou alívio na responsabilidade dos próprios agentes humanos. Nesse sentido, "algorithmic transparency and accountability are among the most vividly debated themes of our time, yet, rendering algorithms more transparent and accountable can never decrease or alleviate the responsibility of human agents"[638].

Os autores do relatório, Peter Burgess, Luciano Floridi, Aurélie Pols e Jeroen Van Hoven, questionam se a representação digital dos indivíduos pode expô-los a novas formas de vulnerabilidades e danos. Destacamos a colocação de que a "proteção de dados pessoais não é uma questão técnica ou legal, mas uma profunda questão humana":

> Data protection is not a technical or legalistic matter. It is a profoundly human one. The reflection of the EAG [Ethics Advisory Group] and the present report have consistently drawn upon the wide-reaching premise of an ontological shift in governance from an analogue logic to a digital one. Individuals, as well as public and private organisations, experience the world differently as a result of the socio-cultural shifts of the digital age[639].

[638] BURGESS, Peter; FLORIDI, Luciano; POLS, Aurélie; HOVEN, Jeroen van. **Ethics advisory group**. Towards a digital ethics. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf>. Acesso em: 18 nov. 2018, p.14. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf>. Acesso em 18 nov.2018. Tradução livre: A transparência algorítmica e a responsabilização estão entre os temas mais vividamente debatidos de nosso tempo, no entanto, tornar os algoritmos mais transparentes e responsáveis nunca pode diminuir ou aliviar a responsabilidade dos agentes humanos.

[639] BURGESS, Peter; FLORIDI, Luciano; POLS, Aurélie; HOVEN, Jeroen van. **Ethics advisory group**. Towards a digital ethics. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf>. Acesso em: 18 nov. 2018, p.11. Tradução livre: A proteção de dados não é uma questão técnica ou legal. É uma profunda questão humana. O reflexo do EAG [Ethics Advisory Group] e o presente relatório têm recorrido de forma consistente à premissa abrangente de uma mudança ontológica na governança de uma lógica analógica para uma lógica digital. Indivíduos, bem como organizações públicas e privadas, experimentam o mundo de forma diferente, como resultado das mudanças socioculturais da era digital.

Vale ressaltar que o *Ethics Advisory Group* trabalha sobre questões ontológicas da metaética e não propriamente com a ética normativa[640]. Seu trabalho consiste em lidar com formulações sobre ética e valores da conduta humana na era digital, quando tais condutas estão sob a pressão da interconectividade, da tomada de decisão algorítmica, do aprendizado de máquina, da vigilância digital e da enorme recolta de dados pessoais, envolvendo questões do que pode ou não ser mantido e o que pode e deve ser adaptado da tradicional ética normativa.

Como combinar o uso de máquinas com os valores éticos e morais do ser humano é de fato um desafio. O *ethical knob*, por exemplo, usado no campo dos veículos autônomos (AVs)[641], e que numa tradução literal significa *botão ético*, é um exemplo do que o homem tem feito nesse campo. Trata-se de um dispositivo que permite aos passageiros personalizar eticamente seus AVs, podendo escolher entre diferentes configurações correspondentes a diferentes aplicações morais[642]. Por meio desse sistema os condutores dos AVs poderiam ajustar as configurações de seu carro para que ele funcionasse como "altruísta total", "egoísta total" ou "imparcial", permitindo que ele decidisse com base na maneira como o condutor valoriza a própria vida, ou a vida de outros, diante de um dilema ético em meio à iminência de um acidente. Embora pareçae óbvio que os AVs devam ser sempre programados para minimizar o número de mortos, uma pesquisa do MIT Lab[643] indicou uma preferência por andar em carros que protegessem seus passageiros. Paradoxalmente, a maioria dos participantes prefere que os outros usem AVs imparciais – para os quais todas as vidas têm igual importância – enquanto cada um deles, como passageiro, faria uma escolha mais egoísta.

Em uma economia baseada em riscos, a avaliação destes é realizada usando técnicas de cálculo de probabilidade. Quanto mais informações puderem ser coletadas e cruzadas entre si para o melhor *output,* maiores as chances de uma

---

[640] Existem quatro ramos tradicionais da ética, quais seja, ética descritiva, ética normativa, ética aplicada e metaética. Enquanto a ética normativa repousa seu olhar para o que deve ser feito, a metaética se preocupa com qual o certo a ser feito.

[641] Conforme mencionado no capítulo anterior, vale lembrar que na Alemanha, em junho de 2017, o Ministério dos Transportes e de Infraestrutura Digital (*Bundesministerium für Verkehr und digitale Infrastruktur),* por sua Comissão Ética, publicou um guia para o uso de carros autônomos. Disponível em: <https://www.bmvi.de/SharedDocs/EN/Documents/G/ethic-commission-report.pdf?__blob=publicationFile>. Acesso em: 10 jan. 2019.

[642] CONTISSA, Giuseppe; LAGIOIA, Francesca; SARTOR, Giovanni. **The ethical knob**: ethically-customisable automated vehicles and the law, 17 out. 2017. Disponível em: <https://ssrn.com/abstract=2881280>. Acesso em: 18 nov. 2018.

[643] BONNEFON, Jean-François; SHARIFF, Azim; RAHWAN, Iyad. The social dilemma of autonomous vehicles **Science 24**, v.352, jun. 2016, p.1573-1576.

tomada de decisão correta para algo futuro (predição). Assim, usando estatística e probabilidade, os indivíduos são agrupados em situações com o mesmo nível de risco, como elementos para ponderação de custos entre ganhos e perdas. Algoritmos podem fornecer uma elevada e detalhada compreensão de comportamentos e propensões do indivíduo, permitindo avalições de risco mais individualizadas e o rateio dos custos reais para cada indivíduo. Ocorre que essa avaliação de risco pode acarretar em violação aos direitos da pessoa humana[644].

Além disso, essas novas formas de discriminações algorítmicas representam uma ameaça à igualdade de oportunidades. Uma pessoa, por resultado de cálculos algoritmos, pode vir a ter retirada de si uma oportunidade a ponto de lhe trazer prejuízo, ou ainda, de igual modo, o inverso, uma oportunidade que diante dela é colocada pode lhe trazer um risco e ameaça.

Segundo Frank Pasquale, os assim chamados sistemas de reputação[645] estão criando novas minorias, e em grande parte invisíveis, desfavorecidas devido a erro ou injustiça. Qualquer pessoa pode ser rotulada em um banco de dados como "não confiável", "custo médico alto", "renda em declínio", dentre outras expressões depreciativas. Muitos estigmas injustos podem ser criados. Os algoritmos não estão imunes ao problema da discriminação visto que pressupostos negativos e infundados se transformam em preconceito. Eles são programados por seres humanos, cujos valores estão embutidos em seu software[646].

Situações de particular preocupação estão relacionadas a casos em que estejam ocorrendo associações discriminatórias. Imagine-se uma situação em que um sistema de recomendação seja usado para auxiliar decisões de contratação de emprego, porém tal sistema contém variáveis ou associações inadequadas, como características ligadas à raça ou gênero. A possibilidade de verificação e compreensão de um algoritmo pode colocar luz sobre eventuais situações discriminatórias.

Há poucos anos, nos Estados Unidos, houve um escândalo envolvendo escolhas automatizadas com viés racista. O sistema, em tese, inteligente, utilizado

---

[644] BURGESS, Peter; FLORIDI, Luciano; POLS, Aurélie; HOVEN, Jeroen van. **Ethics advisory group**. Towards a digital ethics. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf>. Acesso em: 18 nov. 2018, p.12.

[645] PASQUALE, Frank. Reputation regulation: disclosure and the challenge of clandestinely commensurating computing. In: LEVMORE, Saul; NUSSBAUM, Martha C.; The offensive internet: speech, privacy, and reputation. Cambridge, MA, **Harvard University Press**, 2010, p.107-123.

[646] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p.38.

pelo sistema judiciário americano, chamado *Compas*, abreviação de *Correctional Offender Management Profiling for Alternative Sanctions*, servia para analisar dados e trazer predições sobre a chance de reincidência de condenados pela justiça daquela país. A entidade de investigação jornalística ProPublica, após analisar cerca de dez mil casos de pessoas presas em um Condado da Flórida, constatou que o algoritmo *Compas* previa que os réus da raça negra teriam maiores riscos de reincidência do que de fato eles deveriam ter, enquanto os réus de raça branca teriam índices mais baixos do que eles realmente deveriam ter. Em que pese o resultado desse estudo apresentado pela ProPublica, a empresa responsável pelo desenvolvimento do algoritmo, Northpointe Inc., que já havia se negado a "abrir" os algoritmos, contestou esse resultado[647].

Outros casos recentes, envolvendo programas desenvolvidos por empresas de vanguarda na pesquisa de inteligência artificial, também trazem à tona resultados com viés discriminatórios de raça, etnia e gênero. Por exemplo, um programa de publicidade do LinkedIn mostrou uma preferência por nomes masculinos em buscas[648]. Em um caso de *chatbot* da Microsoft, chamado Tay, depois de um dia de aprendizado com o conteúdo da rede Twitter, começou a postar mensagens antissemitas[649]. Ainda em outro exemplo, um estudo de dezembro de 2015, realizado pela *Harvard Business School* apontou que pessoas da raça afrodescendente têm cerca de 16% menos chances de serem aceitos no sistema do Airbnb[650]. Diante do resultado, a empresa anunciou novas medidas para combater a

---

[647] Sobre o tema: ISRANI, Ellora Thadaney. When an algorithm helps send you to prison. **The New York Times**. Publicado em: 26 out. 2017. Disponível em: <https://www.nytimes.com>. Acesso em: 22 out. 2018; ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. Machine bias. There's software used across the country to predict future criminals. And it's biased against blacks. **Pro Publica**. Publicado em: 23 maio 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 22 out. 2018; BURANYI, Stephen. Rise of the racist robots – how AI is learning all our worst impulses. **The Guardian**. Publicado em: 08 ago. 2017. Disponível em: <https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses>. Acesso em: 22 out. 2018; PASQUALE, Frank. Secret algorithms threaten the rule of law. In: **MIT Thecnology Review**, 01 jun. 2017. Disponível em: <https://www.technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law/>. Acesso em: 28 nov. 2018.

[648] THE SEATTLE TIMES. **How LinkedIn's search engine may reflect a gender bias**. Disponível em: <https://www.seattletimes.com/business/microsoft/how-linkedins-search-engine-may-reflect-a-bias/>. Acesso em: 25 dez. 2018.

[649] THE GUARDIAN. **Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter**. Disponível em: <https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter>. Acesso em: 25 dez. 2018.

[650] EDELMAN, Benjamin; LUCA, MichaeL; SVIRSKY, Dan. **Racial discrimination in the sharing economy**: evidence from a field experiment. Disponível em:<http://www.benedelman.org/publications/airbnb-guest-discrimination-2016-09-16.pdf>. Acesso em: 24 dez. 2018.

discriminação após uma série de denúncias e denúncias sobre racismo, homofobia e sexismo por parte dos anfitriões[651].

Outro caso envolvolveu a gigante Amazon, acusada de exclusão de determinados CEPs dos EUA do acesso ao serviço de entrega no mesmo dia da Amazon Prime. De acordo com uma análise da Bloomberg, esses códigos postais representavam predominantemente bairros negros. A Amazon negou categoricamente que a corrida fosse um fator ao decidir quais áreas de CEP seriam cobertas pelo serviço e, em vez disso, argumentou que sua principal consideração é o custo associado à entrega no mesmo dia e uma série de fatores que afetam esse custo[652].

Importante notar, porém, que remover variáveis de possível preocupação da fonte de dados, como raça ou gênero, pode não ser suficiente para evitar o caráter discriminatório. Sobre o assunto, contribuem os autores Jatinde Singh, Ian Walden, Jon Crowcroft e Jean Bacon:

> In terms of control, note that it is often not enough simply to remove variables of possible concern (e.g. race in a discrimination context) from the data source (or model), as not only does this reduce the information available for learning, but these variables might be highly correlated with other attributes of the dataset (e.g. postcodes that represent particular demographics), and/or the issues may be the result of combining variables (e.g. age, gender and postcode). Work is being done on constraining the learning process to prevent such improper features and associations from being made[653].

Algoritmos também podem ser usados para esconder falhas, conforme pondera Nicole Kobie. Uma empresa acusada de políticas de contratação racista pode apontar para seu software de classificação de currículos, afirmando que o departamento de Recursos Humanos ou os executivos da empresa não podem ser responsabilizados, pois é a máquina que fez o trabalho questionado.

---

[651] WIRED. **Airbnb introduces anti-discrimination rules to clamp down on bigoted hosts**. Disponível em: <https://www.wired.co.uk/article/airbnb-new-anti-discrimination-rules>. Acesso em: 24 dez. 2018.

[652] INGOLD, David; SOPER, Spencer Soper. 'Amazon doesn't consider the race of its customers. Should It?' (**Bloomberg**, 21. Abr.2016). Disponível em: <http://www.bloomberg.com/graphics/2016-amazon-same-day/>. Acesso em: 07 jan. 2019.

[653] SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. **Responsibility and machine learning**: part of a process. Publicado em: 27 out. 2016. Disponível em: <https://ssrn.com/abstract=2860048>. Acesso em: 18 out. 2018, p.5. Tradução livre: Em termos de controle, note que muitas vezes não é suficiente remover variáveis de possível preocupação (por exemplo, raça em um contexto de discriminação) da fonte de dados (ou modelo), pois isso não apenas reduz as informações disponíveis para aprendizado, mas também variáveis podem ser altamente correlacionadas com outros atributos do conjunto de dados (por exemplo, códigos postais que representam dados demográficos específicos) e/ou os problemas podem ser o resultado da combinação de variáveis (por exemplo, idade, sexo e código postal). O trabalho está sendo feito para restringir o processo de aprendizado para evitar que tais características e associações impróprias sejam feitas.

A pseudoneutralidade apresentada pelos algoritmos é um persuasivo e atraente discurso da atualidade, ao prometerem neutralidade na tomada de decisões realizadas por seus complexos algoritmos. Porém, se considerarmos que um algoritmo é uma ordem embutida em comandos matemáticos automáticos, aufere-se, rapidamente, que os algoritmos não são neutros como querem fazer crer, porque parte de uma prévia determinação: "E, como opiniões, todos os algoritmos são diferentes. Alguns algoritmos privilegiam um determinado grupo de pessoas em detrimento de outro"[654]. Segundo Robyn Caplan, Joan Donovan, Lauren Hanson e Jeanna Matthews,

> There is a need for greater reflection on models of power and control, where the sublimation of human decision-making to algorithms erodes trust in experts. Ultimately, regulators and researchers are ill-equipped to audit algorithms or enforce any regulation under these conditions[655].

Há quem defenda que o uso de algoritmos para a definição de perfis e tomada de decisão automatizada ainda é melhor do que escolhas humanas. Nesse sentido, a governança baseada em dados é frequentemente apresentada como um modo de governança "revolucionário" emancipado dos jugos do que é tido como uma representação humana tendenciosa, ambígua, feita a partir de uma análise humana, com pontos de vista subjetivos. Porém, não se trata da permanência de uma em detrimento da outra, ou de que uma seja boa e a outra seja ruim, mas sim

---

[654] CAPLAN, Robyn; DONOVAN, Joan; HANSON, Lauren; MATTHEWS, Jeanna. Algorithmic accountability: a primer. **Data & Society**. Publicado em 18 abr. 2018. Disponível em: <https://datasociety.net/output/algorithmic-accountability-a-primer/>. Acesso em: 26 ago. 2018, p.3: "Quando um algoritmo está sendo criado, ele é estruturado pelos valores de seu projetista, que pode não ser neutro. E depois que um algoritmo é criado, ele deve ser treinado – alimentado com grandes quantidades de dados sobre decisões passadas – para ensiná-lo a tomar decisões futuras. Se esses dados de treinamento forem tendenciosos, o algoritmo pode herdar esse viés. Por estas e outras razões, as decisões tomadas por computador não são fundamentalmente mais lógicas e imparciais do que as decisões tomadas por pessoas". Tradução livre de "When an algorithm is being created, it is structured by the values of its designer, which might not be neutral. And after an algorithm is created, it must be trained – fed large amounts of data on past decisions – to teach it how to make future decisions. If that training data is itself biased, the algorithm can inherit that bias. For these reasons and others, decisions made by computer are not fundamentally more logical and unbiased than decisions made by people". E ainda: Os algoritmos replicam os valores sociais, mas também os incorporam aos sistemas, criando novos padrões e expectativas para o que é importante em um determinado contexto. Embora existam leis proibindo o compartilhamento ou a venda de dados financeiros e de saúde por hospitais e bancos, a discriminação ocorre porque há poucas proteções em vigor para intermediação de dados do consumidor, em que pontos de dados discretos atuam como *proxies* para categorias protegidas reunidas em perfis vendidos. Isso pode levar a um sinal vermelho tecnológico. Tradução livre de: "Algorithms replicate social values but also embed them into systems, creating new standards and expectations for what is important in a given context. While there are laws prohibiting the sharing or sale of health and financial data by hospitals and banks, discrimination occurs because there are few protections in place for consumer data brokering, where discrete data points act as proxies for protected categories that are then assembled into profiles that are sold. This can lead to technological redlining" (p.9).

[655] CAPLAN, Robyn; DONOVAN, Joan; HANSON, Lauren; MATTHEWS, Jeanna. **Algorithmic accountability**: a primer. Data & Society. Publicado em: 18 abr. 2018. Disponível em: <https://datasociety.net/output/algorithmic-accountability-a-primer/>. Acesso em: 26.ago.2018. Tradução livre: Há necessidade de maior reflexão sobre os modelos de poder e controle, onde a sublimação da tomada de decisão humana aos algoritmos corrói a confiança dos especialistas. Em última análise, os reguladores e pesquisadores estão mal equipados para auditar algoritmos ou impor qualquer regulamentação sob essas condições.

de aplicar princípios e regras visando evitar violações ao direito da pessoa, independente do sistema ser automatizado ou não por algoritmos.

Vale lembrar que algoritmos não têm personalidade jurídica. Sempre o humano que lhe está por trás será o responsável, mesmo quando se tratar de aprendizado de máquina.

Segundo Frank Pasquale, as empresas são analíticas para prever questões como quem seja mentalmente doente, mau funcionário, estudante deficiente, criminoso ou terrorista. Conforme o autor, essas avaliações devem ser implantadas com a máxima cautela, pois uma vez usadas para aconselhar a polícia, ou empregadores, não são meras opiniões que circulam em um fluxo livre de ideias. Ao invés disso, podem ter impacto direto sobre a liberdade da pessoa. Para Frank Pasquale, se não puderem ser explicados de maneira inteligível, e acrescentamos, justificados de acordo com o direito, não deveriam ser usados de maneira alguma sem o consentimento direto da pessoa que estão avaliando[656], quiçá não deveriam ser usados de forma alguma, ainda que houvesse consentimento.

Inferências equivocadas podem ocorrer. Se um indivíduo possui um carro de grande porte mas não tem filhos, pode existir uma suposição de que o dono do veículo está acima do peso. Se esses dados forem repassados para uma seguradora de saúde, isso influenciará na decisão do serviço. Porém, se esses dados estiverem incorretos, como por exemplo, o modelo do carro, ou se uma suposição estiver falsa, a exemplo do proprietário ter esse tipo de carro para transportar equipamentos esportivos, não há como corrigi-lo[657].

Todas as questões ligadas a inferências equivocadas, discriminações, e oportunidades desiguais estão umbilicalmente relacionadas à transparência na utilização dos algoritmos. Em outras palavras, qual o grau de opacidade algorítmica, o que passamos a analisar com mais profundidade.

4.3 Opacidade dos algoritmos

Quando mencionamos sobre o caráter ‘caixa preta’ dos algoritmos, vimos que esse quadro está relacionado à variação no que tange às possibilidades dos

[656] PASQUALE, Frank. Secret algorithms threaten the rule of law. In: **MIT Thecnology Review**, 01 jun. 2017. Disponível em: <https://www.technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law/>. Acesso em: 28 nov. 2018.

[657] KOBIE, Nicole. **Who do you blame when an algorithm gets you fired?** Disponível em: <https://www.wired.co.uk/article/make-algorithms-accountable>. Acesso em: 24 dez. 2018.

algoritmos serem compreendidos. Ou seja, alguns algoritmos são mais passíveis de verificação do que outros. Para Jenna Burrell, a opacidade parece estar no centro das novas preocupações sobre "algoritmos", tanto entre estudiosos de direito como entre cientistas sociais[658].

Nessa vereda, falar em transparência em um contexto de algoritmos significa fazer referência ao grau com que os elementos que compõe determinado algoritmo podem ser acessados, lidos (enquanto código de programação) e compreendidos. Sobre o assunto, explicam os autores Jatinder Singh, Ian Walden, Jon Crowcroft e Jean Bacon:

> for instance, exposing the features of the data the learned model takes into account, the associations and rules that were derived, and the extent to which the model relies on these. Notions of control are very much related, concerning how algorithms can be managed and constrained, for example to prevent particular associations being made, or setting bounds on outputs[659].

Ao passo que algoritmos são ferramentas usadas para simplificar decisões, aumentar a eficiência e oferecer conveniência – e, por esse lado, são extremamente positivos – quando existe opacidade e não se consegue entender como funcionam ou até mesmo se funcionam, adentramos em um cenário nebuloso e que pode ser negativo. Segundo a hipótese de Nicole Kobie, se um *data broker* incluir um fato falso no perfil de uma pessoa, ou se a análise fizer uma suposição incorreta, isso poderá afetar negativamente a vida de alguém[660]. E como saber se, de fato, isso ocorreu?

Frank Pasquale usa o termo *defective by design*, como expressão crítica à infraestrutura que possa prejudicar as pessoas, mas não emitir correções[661]. Se um determinado estigma for inserido nos sistemas de reputação, deveria existir alguma forma de se permitir sua remoção tão rapidamente quanto se espalha. Acrescentamos que para ter direito à remoção, é preciso existir, *ex ante*, o direito de conhecer os dados pessoais utilizados para cristalizar determinado estigma.

---

[658] BURRELL, Jenna. How the machine ‘thinks’: understanding opacity in machine learning algorithms. In: **Big Data & Society**, jan.-jun. 2016. Disponível em: <http://journals.sagepub.com> Acesso em: 21 out. 2018, p.1.

[659] SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. **Responsibility and machine learning**: part of a process. Publicado em: 27 out. 2016. Disponível em: <https://ssrn.com/abstract=2860048>. Acesso em: 18 out. 2018, p.4. Tradução: por exemplo, expondo as características dos dados que o modelo aprendido lconsidera, as associações e regras que foram derivadas, e até que ponto o modelo nelas se baseia. As noções de controle são muito relacionadas, sobre como os algoritmos podem ser gerenciados e restringidos, por exemplo, para evitar que associações específicas sejam feitas ou para estabelecer limites em saídas

[660] KOBIE, Nicole. **Who do you blame when an algorithm gets you fired?** Disponível em: <https://www.wired.co.uk/article/make-algorithms-accountable>. Acesso em: 24 dez. 2018.

[661] KOBIE, Nicole. **Who do you blame when an algorithm gets you fired?** Disponível em: <https://www.wired.co.uk/article/make-algorithms-accountable>. Acesso em: 24 dez. 2018.

Sob outra perspectiva, a opacidade dos algoritmos pode ser considerada um problema social, haja vista que diversos mecanismos de classificação social dependem, frequentemente, de algoritmos e, ultimamente, dependem da técnica de *machine learning* para fazer este trabalho de classificação, a exemplo de filtros de spam, detecção de fraude de cartão de crédito, motores de busca, sugestão de leitura de notícias, publicidade, seguro, aptidão para contrair empréstimo, pontuação de crédito, etc[662]. Segundo Jenna Burrel, esses algoritmos operam dados pessoais e nas situações em que parte ou a totalidade da política do algoritmo é desconhecida, surgem perguntas: quais as razões para este estado de não saber? É porque o algoritmo é de caráter proprietário? Porque é complexo ou altamente técnico? Ou existem, talvez, outras razões? Nas palavras da autora:

> The algorithms in question operateon data. Using this data as input, they produce na output; specifically, a classification (i.e. whether to give an applicant a loan, or whether to tag an email as spam). They are opaque in the sense that if one is a recipient of the output of the algorithm (the classification decision), rarely does one have any concrete sense of how or why a particular classification has been arrived at from inputs. Additionally, the inputs themselves may be entirely unknown or known only partially.The question naturally arises, what are the reasons for this state of not knowing? Is it because the algorithm is proprietary? Because it is complex or highly technical? Or are there, perhaps, other reasons?[663]

Ela oferece uma classificação no que tange às formas de opacidade e cuja divisão pode clarear os caminhos diante das perguntas formuladas. Segundo a autora, existem três formas distintas de opacidade:

> (1) opacity as intentional corporate or institutional self-protection and concealment and, along with it, the possibility for knowing deception; (2) opacity stemming from the current state of affairs where writing (and reading) code is a specialist skill and; (3) an opacity that stems from the mismatch between mathematical optimization in high-dimensionality characteristic of machine learning and the demands of humanscale reasoning and styles of semantic interpretation[664].

---

[662] BURRELL, Jenna. How the machine ‘thinks’: understanding opacity in machine learning algorithms. In: **Big Data & Society**, jan.-jun. 2016. Disponível em: <http://journals.sagepub.com>. Acesso em: 21 out. 2018, p.1.

[663] BURRELL, Jenna. How the machine ‘thinks’: understanding opacity in machine learning algorithms. In: **Big Data & Society**, jan.-jun. 2016. Disponível em: <http://journals.sagepub.com>. Acesso em: 21 out. 2018, p.1. Tradução livre: Os algoritmos em questão operam em dados. Usando esses dados como *input*, eles produzem um *output*; especificamente, uma classificação (ou seja, se dar um empréstimo a um interessado ou se marcar um email como spam). Eles são opacos no sentido de que se alguém é um receptor do *output* do algoritmo (da decisão de classificação), raramente alguém tem um senso concreto de como ou porque uma particular classificação foi alcançada pelos *inputs*. Além disso, os próprios *inputs* podem ser totalmente desconhecidos ou conhecidos apenas parcialmente. A questão que surge naturalmente é: quais são as razões para este estado de não saber? É porque o algoritmo é de caráter proprietário? Porque é complexo ou altamente técnico? Ou existem, talvez, outras razões?

[664] Essa classificação é feita por BURRELL, Jenna. How the machine ‘thinks’: understanding opacity in machine learning algorithms. In: **Big Data & Society**, jan.-jun. 2016. Disponível em: <http://journals.sagepub.com> Acesso

A terceira forma de opacidade – frequentemente confundida com a segunda forma como parte do senso geral de que os algoritmos e o código são muito técnicos e complexos – é o foco particular do artigo desenvolvido por Jenna Burrell. Ao analisar essa forma de opacidade, a autora assinala as deficiências em torno das 'auditorias' de algoritmos, como forma, inclusive, de avaliar a classificação discriminatória[665].

Por muitas vezes, a opacidade, em determinado nível, existe devido a preocupações proprietárias. Os algoritmos estão fechados justamente para manter a vantagem competitiva e os segredos do negócio. Diante disso, seria muito improvável que os algoritmos sejam totalmente revelados. Para Gianclaudio Malgieri, as regras de equilíbrio na lei de proteção de dados e no direito do segredo comercial são vagas e esquizofrênicas[666].

Como antídodo a esse cenário, Jenna Barrell propõe o uso de códigos *open source* na elaboração dos algoritmos[667]. Porém, parece-nos claro que não se pode impedir o uso do modelo proprietário, dentro da livre iniciativa de mercado. Outra propoposta da autora, é educar uma faixa mais ampla da sociedade em relação à programação de códigos e habilidades computacionais visando diminuir o problema de uma reduzida elite de pessoas técnicas que compreendem o assunto. Porém, a própria autora admite que os algoritmos envolvidos em *machine learning* constituem um desafio que vai muito além, uma vez que as máquinas aprendem com si mesmas, podendo escapar à plena compreensão humana – mesmo para aqueles com treinamento especializado e cientistas da computação[668].

Desconstruir as caixas pretas não é tarefa fácil. Ainda que exista uma vontade de expor seus métodos ao público, haveria um desafio muito grande para entender

---

em: 21 out. 2018, p.2. Tradução livre: (1) opacidade como autoproteção e ocultação corporativa ou institucional intencional e, com ela, a possibilidade de se conhecer o engano; (2) opacidade decorrente do atual estado de coisas onde escrever (e ler) código é uma habilidade especializada e; (3) uma opacidade que decorre do descompasso entre otimização matemática em alta dimensionalidade característica da aprendizagem de máquina e as demandas do raciocínio de escala humana e estilos de interpretação semântica.

[665] BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: **Big Data & Society**, jan.-jun. 2016. Disponível em: <http://journals.sagepub.com>. Acesso em: 21 out. 2018, p.2.

[666] MALGIERI, Gianclaudio. Trade secrets *v.* personal data: a possible solution for balancing rights. International **Data Privacy Law**, v.6, 2.ed. 1 maio 2016, p.102-116. Disponível em: <https://doi.org/10.1093/idpl/ipv030>. Acesso em: 16 out. 2018.

[667] BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: **Big Data & Society**, jan.-jun. 2016. Disponível em: <http://journals.sagepub.com> Acesso em: 21 out. 2018, p.4.

[668] BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: **Big Data & Society**, jan.-jun. 2016. Disponível em: <http://journals.sagepub.com> Acesso em: 21 out. 2018, p.10.

tais métodos. Frank Pasquale, por sua vez, aponta três formas estratégicas para manterem as caixas pretas fechadas: sigilo real, sigilo legal e ofuscação[669].

Por sigilo real pode ser entendida a situação que estabelece uma barreira entre o conteúdo escondido e o acesso não autorizado a esse conteúdo. Um exemplo desse caso é o email que protegemos com uma senha.

O sigilo legal, por sua vez, obriga que determinados dados e informações mantenham seu conteúdo sigiloso, a exemplo de um empregado de banco que é obrigado seja por força de lei, seja por força do contrato de trabalho, a não revelar o saldo de seus clientes a terceiros.

Já a ofuscação guarda relação com atos deliberados de ocultação quando o sigilo não pode ser alegado na situação. Como exemplo, cite-se uma empresa que, em resposta a um pedido de informações, entrega milhares de páginas de documentos, forçando o interessado a perder tempo, como a tarefa de procurar uma agulha no palheiro.

Para Frank Pasquale todas essas formas (sigilo real, sigilo legal e ofuscação) podem ser consideradas *opacidade*, a cujo termo o autor atribui o significado de "incompreensibilidade remediável"[670].

Ao analisar a incompatibilidade de transparência e auditoria dos algoritmos frente à propriedade intelectual que lhes está por trás, Howard Yu pondera que o problema é que a legislação não protege os dados mais preciosos para empresas de tecnologia, aqueles inferidos e produzidos por algoritmos e usados por anunciantes[671]. Nesse sentido, o autor questiona a opacidade dos algoritmos, protegidos por direitos de propriedade intelectual, porém, descobertos quanto ao direito de proteção de dados pessoais. Nessa esteira, exemplifica:

> For example, if TV network HBO wants to advertise the new season of Game of Thrones to anyone reading an article about the show on the New York Times website, then all HBO needs is an algorithm that understands the behavioural correlation, not a demographic profile. And those all-knowing algorithms, the under-the-hood machine learning tools that power everything from Facebook's news feed to Google's self-driving cars, remains opaque and unchallenged. In fact they have their own protections in the form of

[669] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p.4-5.
[670] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p.6.
[671] YU, Howard. GDPR isn't enough to protect us in an age of smart algorithms. **The Conversation**, 29 maio 2018. Disponível em: <https://theconversation.com/gdpr-isnt-enough-to-protect-us-in-an-age-of-smart-algorithms-97389>. Acesso em: 01 dez. 2018.

> intellectual property rights, making them trade secrets much like the Coca-Cola recipe[672].

Howard Yu contesta, nessa vereda, que Facebook e Coca Cola possuem modelos de negócios bastante diversos, posto que a rede social, assim como Google, Snapchat e outros, geram suas receitas por meio de publicidade. Enquanto os consumidores pagam por sua Coca-Cola, os internautas recebem seus serviços digitais de graça. Tal serviço, aparentemente gratuito, introduziu o que os economistas chamam de problema "agente- principal"[673], com o que acarreta na postura das empresas de tecnologia não agirem no melhor interesse dos consumidores porque justamente esses são o produto e não os clientes.

Segundo Howard Yu, isso, porém, não é insolúvel. Ele sugere que as empresas de tecnologia poderiam ser obrigadas a nomear revisores independentes, cientistas da computação e pesquisadores acadêmicos para realizar auditorias de algoritmos para garantir que a definição de perfis e as decisões automatizadas sejam imparciais e éticas.

Para Frank Pasquale, muitas empresas que processam dados, como as dos setores de internet e financeiro, alegam que mantem técnicas rígidas de sigilo para preservar suas respectivas propriedades intelectuais, "but their darker motives are also obvious"[674]. Segundo o autor, as empresas se escondem atrás do escudo da proteção legal da propriedade intelectual. Nessa linha, Frank Pasquale pondera que mais transparência ajudaria analistas verificarem em mercados de "irrational exuberance" condutas indevidas que hoje podem ser facilmente escondidas. Poderia, por exemplo, expor concorrência desleal e práticas discriminatórias.

---

[672] YU, Howard. GDPR isn't enough to protect us in an age of smart algorithms. **The Conversation**, 29 maio 2018. Disponível em: <https://theconversation.com/gdpr-isnt-enough-to-protect-us-in-an-age-of-smart-algorithms-97389>. Acesso em: 01 dez. 2018. Tradução livre: Por exemplo, se a rede de TV HBO quiser anunciar a nova temporada de Game of Thrones para qualquer pessoa que leia um artigo sobre o programa no site do New York Times, então a HBO precisa de um algoritmo que compreenda a correlação comportamental, não um perfil demográfico. E esses algoritmos que tudo sabem, as ferramentas de aprendizado de máquinas que alimentam tudo, desde o feed de notícias do Facebook até os carros autônomos do Google, permanecem opacos e incontestáveis. Na verdade, eles têm suas próprias proteções na forma de direitos de propriedade intelectual, tornando-os segredos comerciais muito parecidos com a receita da Coca-Cola.

[673] The problem of motivating one party (the agent) to act on behalf of another (the principal) is known as the principal-agent problem, or agency problem for short. Agency problems arise when the incentives between the agent and the principal are not perfectly aligned and conflicts of interest arise. As a result the agent may be tempted to act in his or her own interest rather the principal's. Conflicts of interest are almost inevitable. (FINANCIAL Times Lexicon. Disponível em:<http://lexicon.ft.com/term?term=principal/agent-problem>. Acesso em: 24 dez. 2018).

[674] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p. 9.

Frank Pasquale sugere o caminho da regulação, reconhecendo, porém, que essa não é suficiente:

> But as I propose regulatory measures, I will repeatedly make the point that transparency is not enought, particularly in the finance setor. When companies parry with complexity too great to monitor or understand, disclousure becomes na emptygesture. We need to put na end to the recursive games of ´disclousure´ and ´tricks to defeat disclousure´ that have plagued regulator. Transactions that are too complex to explain to outsiders may well be too complex to be allowed to exist[675].

Frank Pasquale entende ainda que as empresas de internet e do setor financeiro deveriam receber padrões mais altos do que as demais empresas de mercado, quanto ao dever de revelar o que estão fazendo. Na medida em que essas empresas de internet e finanças exercem mais influência sobre a economia, estabelecem os padrões pelos quais empresas e pessoas são julgadas. É assim que o autor defende que qualquer solução de transparência para problemas de caixa preta deve ser específica sobre três principais questões: quanto a empresa precisa revelar? para quem deve revelá-lo? em qual prazo a revelação deve ocorrer? Portanto, existem três vetores a serem cumpridos: profundidade da revelação, âmbito de divulgação e prazo da revelação[676].

Para Andrew Tutt, no futuro a maioria dos algoritmos será *treinada* e não *projetada*. Isso significa que a operação de muitos algoritmos será opaca e haverá significativa dificuldade no que o autor chama de *to predict in border cases*, e, ainda, a responsabilidade por seus danos será difusa e de difícil atribuição. Além disso, Consoante Andrew Tutt, embora os algoritmos *projetados* já desempenhem papéis importantes em muitas situações da vida ou da morte (de aterrissagens de emergência a sistemas automatizados de frenagem), haverá um aumento de algoritmos cada vez mais *treinados* implementados nessas aplicações de missão crítica[677].

---

[675] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p. 15. Tradução livre: Mas, ao propor medidas reguladoras, repetirei repetidamente que a transparência não é suficiente, particularmente no setor financeiro. Quando as empresas demonstram uma complexidade muito grande para monitorar ou entender, a divulgação torna-se um vazio. Precisamos pôr fim aos jogos recursivos de "desilusão" e "truques para derrotar a divulgação" que atormentaram o regulador. Transações que são muito complexas para serem explicadas a pessoas de fora podem ser muito complexas para permitir a existência.

[676] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p.141-142.

[677] TUTT, Andrew. An FDA for algorithms. Publicado em: 15 mar. 2016. In: **69 Admin. L. Rev**. 83, 2017. Disponível em: <https://ssrn.com/abstract=2747994>, p.94. Acesso em: 18 nov. 2018. Curiosamente, o Prof. Tutt é da área da oncologia, medicina.

Na proposta de Andrew Tutt, a regulamentação algorítmica exigirá uniformidade federal, julgamento especializado, independência política e análise pré-mercado para evitar – sem sufocar a inovação – a introdução de algoritmos inaceitavelmente perigosos no mercado. O autor propõe que uma nova agência reguladora especializada seja criada para regulamentar a segurança algorítmica. É o que o autor chama de *FDA* para algoritmos:

> Such a federal consumer protection agency should have three powers. First, it should have the power to organize and classify algorithms into regulatory categories by their design, complexity, and potential for harm (in both ordinary use and through misuse). Second, it should have the power to prevent the introduction of algorithms into the market until their safety and efficacy has been proven through evidence-based pre-market trials. Third, the agency should have broad authority to impose disclosure requirements and usage restrictions to prevent algorithms' harmful misuse.[678]

A utilização da expressão *An FDA for algorithms* se dá em razão de Andrew Tutt afirmar que as preocupações que impulsionam a regulamentação de alimentos, medicamentos e cosméticos se assemelham às preocupações que devem impulsionar a regulação de algoritmos. Isso porque com relação ao funcionamento de muitos medicamentos, os exatos mecanismos que podem produzir – tanto benefícios como gerar danos – não são bem compreendidos. Segundo o autor, o mesmo ocorrerá, muito brevemente, em relação aos principais algoritmos utilizados no futuro e potencialmente perigosos[679].

Em nossa opinião, utilizar o subterfúgio da dualidade absoluta da transparência *versus* proteção à propriedade intelectual acaba desviando a verdadeira pauta do debate. Descortinar o caráter 'caixa preta' não implica violar os direitos da propriedade intelectual. O segredo de negócio e os direitos de propriedade intelectual devem permanecer intocáveis. O que se defende é que esses direitos – mantendo-os preservados, ressalte-se – não formem muralhas instransponíveis contra o caráter *black box.* É possível seguir, por exemplo, na ideia de Howard Yu sobre revisores independentes, ou ainda, um modelo de depósito

[678] TUTT, Andrew. An FDA for Algorithms. Publicado em: 15 mar. 2016. In: **69 Admin. L. Rev**. 83, 2017. Disponível em: <https://ssrn.com/abstract=2747994>. Acesso em: 18 nov. 2018, p.120. Tradução livre: Essa agência federal de proteção ao consumidor deve ter três poderes. Primeiro, deve ter o poder de organizar e classificar algoritmos em categorias regulatórias por seu *design*, complexidade e potencial de danos (tanto no uso comum quanto pelo uso indevido). Segundo, deve ter o poder de impedir a introdução de algoritmos no mercado até que sua segurança e eficácia tenham sido comprovadas por meio de testes, em fase pré-mercado baseados em evidências. Terceiro, a agência deve ter ampla autoridade para impor requisitos de divulgação e restrições de uso para evitar o uso indevido de algoritmos.

[679] TUTT, Andrew. An FDA for Algorithms. Publicado em: 15 mar. 2016. In: **69 Admin. L. Rev**. 83, 2017. Disponível em: <https://ssrn.com/abstract=2747994>. Acesso em: 18 nov. 2018, p.119.

perante terceiro de confiança dos dados pertinentes[680], ou na ideia trazida por Andrew Tutt, sem perder de vista os esforços de regulação.

Há que se diferenciar duas situações: os dados que estão sendo tratados e a ´fórmula´ de atuação dos algoritmos. Para que essa distinção se torne mais clara, vale esclarecer que as 'redes neurais artificiais', em uma forma comum na qual se encontram, consistem, em regram, em três camadas, cada uma com um número de 'nós' (*nodes*): uma camada de entrada (*input layer*), na qual os dados de entrada são recebidos, uma camada oculta (*hidden layer*), na qual várias operações são executadas e uma camada de saída (*output layer*) para os resultados. As camadas são totalmente interconectadas. Cada nó de uma camada é conectado a todos os demais nós da camada adjacente. Cada conexão é associada a um peso, de maneira que um nó recebe uma entrada ajustada de acordo com o peso da conexão pela qual foi recebida. Um nó executa um cálculo com base nas entradas recebidas e, dependendo do resultado, enviará vários *outputs* para os nós conectados. A aprendizagem dos algoritmos implica ajustar os pesos dessas conexões, refinando assim a rede geral[681].

Portanto, conforme se apreende do esclarecimento acima, há duas situações distintas que os dados devem ser protegidos: na camada de entrada e na camada de saída, que contém os resultados inferidos pelos cálculos algoritmos. Ressalte-se que a terceira camada pode apresentar dados não inseridos na primeira delas justamente pelo trabalho algoritmo.

Para Luca Bolognini, Enrico Pelino e Camila Bistolfi, o titular dos dados deve conhecer pelo menos a lógica (pois o *know-how* e os processos subjacentes são outra coisa) do processamento automatizado e dos dados pessoais que lhe são atribuídos como resultado da criação de perfil ou do processamento automatizado[682].

---

[680] Frank Pasquale sobre esse caminho expõe que uma sociedade totalmente transparente seria um pesadelo de invasão de privacidade, voyeurismo e violação de propriedade intelectual. Um dos possíveis caminhos para a investigação ordenada e produtiva seria confiar o trabalho a um terceiro de confiança. (PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p.144).

[681] SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. **Responsibility and machine learning**: part of a process. Publicado emj: 27 out. 2016. Disponível em: <https://ssrn.com/abstract=2860048>. Acesso em: 18 out. 2018, p.6. Segundo os autores, "when discussing ML as a 'black-box', artificial neural networks are often the 'go to' example".

[682] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milão-Itália: Giuffrè, 2016, p.272.

A revelação da primeira camada é apta a indicar quais dados pessoais estão sendo utilizados, em cumprimento à regra da autodeterminação informacional. Entretanto, além do controle sobre os dados que consistem no *input* da primeira camada, existe o direito de conhecer a finalidade a que se destinam. Isso porque o direito de conhecer a finalidade dos dados informatizados é atualmente um direito particularmente relevante à autodeterminação informativa"[683]. Ainda, quais dados serão inferidos pela máquina algorítmica. Ademais, é importante manter em perspectiva o princípio do respeito pelo contexto. Segundo Helen Nissenbaum:

> To assess privacy interests, it is crucial to know the context—who is gathering the information, who is analyzing it, who is disseminating and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances[684].

Sob outro enfoque, poder-se-ia cogitar que o caminho de elevadas punições, de caráter pecuniário[685], poderia garantir o *enforcement*, e trazer maior proteção aos dados pessoais nesse ecossistema. Entretanto, sem desconsiderar que esse regime retributivo também deva existir, nele não nos fidamos como forma de solucionar o problema da opacidade. Nessa vereda, fazemos coro com Frank Pasquale, para quem as multas pecuniárias impostas contra o Facebook, por exemplo, por violações envolvendo proteção de dados foram minúsculas: menos de algumas horas de lucro. E o mesmo se pode dizer em relação a várias outras empresas que receberam multas aparentemente 'pesadas'. Para Frank Pasquale, os reguladores precisam começar a forçar essas empresas a dar aos indivíduos uma noção do tamanho dos dados coletados sobre eles – e seu conteúdo, pois para esse autor, não podemos permitir, aos "senhores" da nuvem, controle irrestrito e sigiloso sobre o uso e a definição de perfis de dados[686]. Esse autor indaga que tipo de

---

[683] CANOTILHO, J. J. Gomes; MOREIRA, Vital. **Constituição da República Portuguesa Anotada**. v.1. São Paulo: RT; Coimbra: Coimbra, 2007, p.550. "Daí as exigências jurídico-constitucionais relativas às finalidades das informações: (1) legitimidade; (2) determinabilidade; (3) explicitação; (4) adequação e proporcionalidade; (5) exactidão e actualidade; (6) limitação temporal Todos esses requisitos permitem o controle dos fins, impedindo-se, designadamente, que haja tratamento de dados relativos a finalidades não legítimas ou não especificadas, excessivas relativamente a estas mesmas finalidades ou que tenham como referência dados inexactos ou desactualizados ou, ainda, mantidos por lapsos temporais injustificados".

[684] NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford, CA: Stanford University Press, 2009. Tradução livre: Para avaliar os interesses de privacidade, é crucial conhecer o contexto – quem está coletando as informações, quem está analisando, quem está divulgando e para quem, a natureza da informação, as relações entre as várias partes e ainda outras circunstâncias sociais e institucionais.

[685] Sobre as diretrizes de aplicação e fixação de multas para efeitos do GDPR, vide documento elaborado pelo Grupo de Trabalho do artigo 29, WP 253, adotado em 03 out. 2017.

[686] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p.145.

sociedade está sendo criada [diante da cultura do algoritmo] e responde a si mesmo afirmando que cria economias desiguais[687].

Ainda, a complexidade dos algoritmos, outrossim, não pode servir de justificativa para não serem fornecidas informações aos titulares de dados. Nesse sentido, exemplos[688] trazidos pelo documento WP251 demonstram a separação de assuntos, e como a opacidade pode ser rompida, em vista de atender ao direito do titular dos dados, sem violar o direito de propriedade intelectual do responsável pelo tratamento.

4.4 A proteção de dados e a inteligência artificial

As implicações de privacidade e proteção de dados vinculadas à inteligência artificial resultam de sua capacidade de inferir dados, com o consequente reconhecimento de padrões, extraindo o perfil mais íntimo possível do indivíduo.

Por meio de métodos de inteligência artificial é possível gerar informações sensíveis a partir de dados não sensíveis. Nesse sentido, segundo a organização Article 19:

> Artificial Intelligence methods are being used to identify people who wish to remain anonymous; Artificial Intelligence methods are being used to infer and generate sensitive information about people from their non-sensitive data; Artificial Intelligence methods are being used to profile people based upon population-scale data; and Artificial Intelligence methods are being used to make consequential decisions using this data, some of which profoundly affect people's lives[689].

---

[687] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p.191.

[688] Um responsável pelo tratamento utiliza uma pontuação de crédito para avaliar e rejeitar um pedido de empréstimo de uma pessoa. A pontuação pode ter sido transmitida por uma agência de referência de créditos ou calculada diretamente com base em informações na posse do responsável pelo tratamento. Independentemente da fonte (devendo ser fornecidas informações sobre a fonte ao titular dos dados, em conformidade com o artigo 14.º, n.º 2, alínea f), quando os dados pessoais não forem recolhidos junto do titular), se o responsável pelo tratamento tiver por base essa pontuação, deverá ser capaz de a explicar e de fundamentar a lógica subjacente junto do titular dos dados. O responsável pelo tratamento explica que este processo o ajuda a tomar decisões de concessão de empréstimo equitativas e responsáveis. Fornece os dados relativos às principais características consideradas na tomada da decisão, a fonte dessas informações e a sua relevância, o que pode incluir, por exemplo: as informações fornecidas pelo titular dos dados no formulário de pedido; informações sobre a anterior gestão própria da conta, incluindo eventuais atrasos em pagamentos; e informações de registos públicos oficiais, designadamente informações de registos de fraudes e registos de insolvências. O responsável pelo tratamento inclui igualmente informações com vista a indicar ao titular dos dados que os métodos de pontuação de crédito utilizados são testados periodicamente para garantir a sua equidade, eficácia e imparcialidade. O responsável pelo tratamento faculta ao titular dos dados contactos através dos quais pode pedir para que seja revista qualquer decisão de recusa, em conformidade com o artigo 22º nº 3 (WP 251).

[689] ARTICLE 19 Global Human Rights Organisation. **Privacy and freedom of expression in the age of artificial intelligence**, abril 2018. Disponível em: <https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf>. Acesso em: 26 ago. 2018, p.18. Tradução livre: Métodos de IA estão sendo usados para identificar pessoas que desejam permanecer anônimas; Métodos de IA estão sendo usados para inferir e gerar informações confidenciais sobre pessoas a partir de seus dados não sensíveis; Métodos de IA estão sendo usados para traçar pessoas com base em dados de escala

E quando dados sensíveis, como os que envolvem etnia, religião, crenças políticas, saúde e sexualidade podem ser inferidos a partir de dados tidos como não sensíveis, segundo classifição legal, surge diante de nós um grande desafio pela construção de perfis que podem resultar em discriminação e que violam a autonomia de construir a própria identidade social.

Acrescente-se que inferências sobre o estado emocional do indivíduo, por exemplo, confiança, nervosismo, tristeza e cansaço, podem ser previstos até mesmo a partir de padrões de digitação em um teclado de computador, ou ainda, por meio da análise do comportamento em uma rede social, conforme já visto nesse trabalho.

Essas capacidades dependem do processamento de grandes quantidades de dados, o que não parece ser um problema na sociedade do *big data*. Muito pelo contrário, dados existem aos montes.

Nesse sentido, destaca-se a matéria publicada no jornal *The Guardian*, em cujo texto, Judith Duportail relata sua experiência como usuária do Tinder (aplicativo para encontro de pares amorosos). Com base no direito garantido a todo cidadão europeu pelo Regulamento Geral de Proteção de Dados, solicitou ao aplicativo cupido todos os dados pessoais que este detinha sobre ela. Para sua surpresa, 800 páginas foram-lhe enviadas com informações a respeito de sua vida pessoal[690].

Os consumidores são comumente confrontados com uma assimetria informacional sobre quais tipos e quantos dados seus dispositivos, redes e plataformas geram, processam ou compartilham. Os diferentes tipos de aplicações existentes, associados ao uso da inteligência artificial podem afetar o direito à privacidade e proteção de dados pessoais em diferentes formas.

Segundo a organização *Article 19*, com o aumento de dispositivos inteligentes dentro dos lares e dos locais de trabalho, a educação ao público sobre os impactos relacionados se torna premente:

> As we bring ever-more smart and connected devices into our homes, workplaces, public spaces, and even our bodies, educating the public about such data exploitation becomes increasingly pressing; Identification and tracking: AI applications can be used to identify and thereby track individuals across different devices, in their homes, at work, and in public spaces. For example, while personal data is routinely (pseudo-) anonymised within datasets, AI can be employed to de-anonymise this data, challenging the

populacional; e os métodos de IA estão sendo usados para tomar decisões consequentes usando esses dados, alguns dos quais afetam profundamente a vida das pessoa.

[690] DUPORTAIL, Judith. 26/09/2017. I asked tinder for my data. It sent me 800 pages of my deepest, darkest secrets In: **The Guardian**. Disponível em: <https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold>. Acesso em: 26 ago. 2016.

> distinction between personal and non-personal data, on which current data protection regulation is based[691].

Os produtos de consumo e sistemas autônomos acionados por inteligência artificial são frequentemente equipados com sensores que geram e coletam grandes quantidades de dados sem o conhecimento ou o consentimento daqueles que estão próximos.

Ademais, o reconhecimento facial é outro meio pelo qual os indivíduos podem ser rastreados e identificados em espaços públicos. Recentemente foi anuciado pela imprensa brasileira que sistema de reconhecimento facial chinês pode ser importado ao Brasil ainda em 2019, para ser usado, em princípio, na cidade do Rio de Janeiro[692]. A preocupação em torno desse assunto é que o reconhecimento facial pode permitir que as autoridades identifiquem indivíduos sem causa provável, suspeita razoável ou qualquer outro fundamento legal, em clara ameaça à privacidade. Pense-se, por exemplo, em uma manifestação popular, em que esse sistema é capaz de captar e classificar o perfil dos indivíduos que compareceram ao evento.

Assim, por meio da aplicação de métodos de inteligência artificial, com base em cálculos algoritmos de aprendizagem de máquina é possível criar perfis e classificar indivíduos por aspectos inferidos que poderiam não ter sido autorizados pelo titular, em clara desconformidade com a inteligência da autodeterminação informativa na proteção de dados pessoais. A criação de perfil para classificar, pontuar, categorizar, avaliar e classificar indivíduos e grupos pode ser desenvolvida pela aplicação de inteligência artificial, diante do emaranhado de dados disponíveis, e sem que os indivíduos relacionados saibam ou tenham dado consentimento para tal finalidade. E, pior ainda, sem terem sequer a possibilidade de contestar os

---

[691] ARTICLE 19 Global Human Rights Organisation. **Privacy and freedom of expression in the age of artificial intelligence**, abril 2018. Disponível em: <https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf>. Acesso em: 26 ago. 2018, p.18. Tradução livre: À medida que trazemos dispositivos cada vez mais inteligentes e conectados para nossas casas, locais de trabalho, espaços públicos e até mesmo nossos corpos, a educação do público sobre essa exploração de dados torna-se cada vez mais premente; Identificação e rastreamento: os aplicativos de IA podem ser usados para identificar e, assim, rastrear indivíduos em diferentes dispositivos, em suas casas, no trabalho e em espaços públicos. Por exemplo, enquanto os dados pessoais são rotineiramente pseudoanonimizados nos conjuntos de dados, a inteligência artificial pode ser empregada para desanonimizar esses dados, desafiando a distinção entre dados pessoais e não pessoais, nos quais a atual regulamentação de proteção de dados é baseada.

[692] RINALDI, Camila. Sistema de reconhecimento facial chinês pode chegar ao Brasil ainda em 2019. In: **Olhar Digital**, 16.jan.2019. Disponível em: <https://olhardigital.com.br/noticia/sistema-de-reconhecimento-facial-chines-pode-chegar-ao-brasil-ainda-em-2019/81271>. Acesso em: 16 jan. 2019. Sobre o assunto, vale lembrar que desde 2016, o sistema de reconhecimento facial já é utilizado em aeroportos do Brasil, como o de Cumbica.

resultados e as decisões tomadas sobre eles, ou mesmo, terem acesso a uma explicação sobre a lógica utilizada.

4.5 Decisões automatizadas sobre indivíduos e a prática de *profiling*

A discussão em torno do uso de métodos de inteligência artificial sobre dados pessoais, como também envolvendo o caráter *black box* dos algoritmos se deve, em especial, ao fato da crescente utilização desses comandos para a definição de perfis, isto é, a prática de *profiling*[693], e para a tomada de decisões automatizadas, as quais são utilizadas cada vez mais, tanto por empresas[694] como pelo setor público, para aumentar a eficiência e a otimização de serviços, gerando economia de recursos em diversas aplicações comerciais. O insumo dessas práticas é o dado pessoal, daí a interconexão com o assunto da privacidade e da proteção dos dados pessoais. Dito isso, julgamos importante fazer um recorte neste capítulo para explicar no que consistem a 'definiçao de perfis' e 'as decisões individuais automatizadas'.

A consolidação do *big data,* impulsionado cada vez mais pela *internet das coisas*, com a aplicação da *inteligência artificial* e *machine learning* – conforme visto ao longo desse trabalho – facilita a criação de perfis e a prática da tomada de decisões automatizadas, o que pode implicar em cerceamento das liberdades individuais.

Segundo consta no documento "Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679":

> Os avanços tecnológicos e as potencialidades da análise de megadados, da inteligência artificial e da aprendizagem automática tornaram mais fácil criar perfis e tomar decisões automatizadas, podendo ter um impacto significativo nos direitos e nas liberdades das pessoas[695].

A pedra de toque em torno desse assunto é que os processos para aplicação dos métodos de *profiling* e de decisões automatizadas podem ser pouco transparentes, opacos e desconhecidos às pessoas. Não se sabe exatamente o que

---

[693] Para KAMARINOU, Dimitra; MILLARD, Christopher; SINGH, Jatinder. Machine learning with personal data (nov.7, 2016). Queen Mary School of Law Legal Studies. **Research Paper** n.247, 2016, p.8: *Profiling* é uma subcategoria de processo automatizado.

[694] Na área privada, os principais segmentos da economia ao qual tais práticas estão relacionadas para apoiar a tomada de decisões são: bancário e financeiro, sáude, seguros e publicitário e marketing.

[695] WP29 251 – Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, p.5.

está sendo definido e construído sobre elas. O resultado dessas contruções será utilizado em diversas ocasiões dos atos de suas vidas, inclusive em atos jurídicos, eventualmente podendo trazer algum tipo de prejuízo ao indivíduo. É o que acontece nos casos da criação de estereótipos e de ocorrência de discriminação. Nessa vereda dispõe o documento do Conselho da Europa, a Recomendação CM/Rec (2010)13:

> through this linking of a large number of individual, even anonymous, observations, the profiling technique is capable of having an impact on the people concerned by placing them in predetermined categories, very often without their knowledge[696].

Ademais, a definição de perfis *(profiling*) pode afetar diretamente a liberdade de escolha do indivíduo quanto a determinados serviços ou produtos. Nesse sentido são válidas as palavras contidas no documento em questão:

> A definição de perfis é suscetível de perpetuar os estereótipos existentes e a segregação social. Pode igualmente amarrar as pessoas a uma categoria específica e limitá-las às respectivas preferências sugeridas, pondo assim em causa a sua liberdade para escolher, por exemplo, determinados produtos ou serviços, tais como livros, música ou fluxos de notícias. Em certos casos, a definição de perfis é suscetível de resultar em previsões imprecisas. Noutros casos, poderá dar origem a uma negação de serviços e bens e a uma discriminação injustificada.

A definição de *profiling* também pode ser encontrada no GDPR:

> qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações[697].

A prática de *profiling* não se cinge apenas a tratamento exclusivamente automatizado. Ela pode alcançar práticas híbridas que combinem o tratamento automatizado com alguma forma de intervenção humana.

---

[696] Recommendation CM/Rec(2010)13 and explanatory memorandum adopted by the Committee of Ministers of the Council of Europe on 23 November 2010 and explanatory memorandum. The protection of individuals with regard to automatic processing of personal data in the context of profiling. 23 nov. 2010. Disponível em: <https://rm.coe.int/16807096c3>. Acesso em: 09 jan. 2019, p.6. Tradução livre: Através da ligação de um grande número de dados pessoais, mesmo anônimos, a técnica de criação de perfil é capaz de ter um impacto sobre as pessoas envolvidas, colocando-as em categorias predeterminadas, muitas vezes sem o seu conhecimento.

[697] Artigo 4, alínea 4, GDPR.

O *profiling* envolve três elementos: deve existir uma forma de tratamento automatizado (exclusivo ou híbrido com intervenção humana); deve ser efetuada sobre dados pessoais; e visar avaliar aspectos pessoais de uma pessoa natural.

Segundo Dimitra Kamarinou, Christopher Millard e Jatinder Singh, o processo de *profiling* pode ser dividido em três elementos: data collection, model development (through use of machine learning algorithms), and decision making[698].

Uma simples classificação de pessoas tendo por parâmetro características básicas como idade, sexo, peso e altura não implica, necessariamente, em prática de *profiling*. Para caracterizar ´definição de perfil´ deve existir a finalidade de analisar ou prever determinadas capacidades, interesses ou comportamentos do indivíduo[699].

---

[698] KAMARINOU, Dimitra; MILLARD, Christopher; SINGH, Jatinder. Machine learning with personal data (nov. 7, 2016). Queen Mary School of Law Legal Studies. **Research Paper** n. 247, 2016, p.8. Tradução livre: coleta de dados, desenvolvimento de modelos (através do uso de algoritmos de aprendizado de máquina), e tomada de decisão. Ainda, segundo aprofundam os autores: Data collection will not necessarily precede algorithmic processes, but it makes sense to consider data collection first because machine learning algorithms learn models from data. The collection of personal data (whether directly from the data subject or not) should comply with the data protection principles and the requirement that there be a lawful ground for processing. Personal data should only be collected for specified, explicit, and legitimate purposes and should not be processed subsequently in a manner that is incompatible with those purposes. Important factors in relation to compatibility are likely to include the nature of the data, the way in which they are processed, and the potential impact of such processing on data subjects. According to Article 21(1) of the GDPR, data subjects have the right to object at any time to the processing of their personal data which is based on Article 6(1)(e) and (f),48 including profiling based on those provisions. A machine learning algorithm may develop a profile from data that has been provided either by the data controller or by a third party or by both. Cloud will often be useful49 given that the process may require significant resources in terms of computational power and/or storage. It may also be that profiles are constructed in real time. Depending on the nature of the application, this might take place locally on the data controller's machines while at the same time a copy of the 'real time data' is sent to the cloud to continue the dynamic training of the algorithm. Tradução livre: A coleta de dados não precederá necessariamente os processos algorítmicos, mas faz sentido considerar a coleta de dados primeiro porque os algoritmos de aprendizado de máquina aprendem os modelos a partir dos dados. A coleta de dados pessoais (diretamente do titular dos dados ou não) deve obedecer aos princípios de proteção de dados e à exigência de que haja uma base legal para o processamento. Os dados pessoais só devem ser coletados para fins específicos, explícitos e legítimos e não devem ser processados posteriormente de maneira incompatível com esses fins. Fatores importantes relacionados com a compatibilidade podem incluir a natureza dos dados, a forma como são processados e o impacto potencial de tal processamento nos titulares de dados. De acordo com o n.º 1 do artigo 21.º do GDPR, os titulares dos dados têm o direito de se opor a qualquer momento ao tratamento dos seus dados pessoais, que se baseia no artigo 6.º, n.º 1, alíneas e) ef) 48, incluindo a definição de perfis com base nessas disposições. Um algoritmo de aprendizado de máquina pode desenvolver um perfil a partir de dados que foram fornecidos pelo controlador de dados ou por um terceiro ou por ambos. A nuvem geralmente será útil, pois o processo pode exigir recursos significativos em termos de poder computacional e/ou armazenamento. Também pode ser que os perfis sejam construídos em tempo real. Dependendo da natureza do aplicativo, isso pode ocorrer localmente nas máquinas do controlador de dados e, ao mesmo tempo, uma cópia dos "dados em tempo real" é enviada para a nuvem para continuar o treinamento dinâmico do algoritmo.

[699] Nesse sentido são os exemplos colhidos das orientações do WP29 antes referidas: uma empresa pode pretender classificar os seus clientes em função da idade ou do género para fins estatísticos e com vista a obter uma visão de conjunto dos seus clientes, sem realizar quaisquer previsões nem tirar ilações sobre as pessoas. Neste caso, a finalidade não é fazer uma apreciação de características individuais, pelo que não se trata de uma definição de perfis. Outro exemplo: Um corretor de dados recolhe dados a partir de diferentes fontes públicas e privadas, quer em nome dos seus clientes quer para os seus próprios interesses. O corretor de dados compila os dados para desenvolver perfis relativos às pessoas e insere estas últimas em diversos segmentos. Vende essa informação a empresas que desejem melhorar a adequação dos seus bens e serviços ao público-alvo. O corretor de dados procede à definição de perfis, inserindo uma pessoa em determinada categoria de acordo com os seus interesses. (WP29 251 – Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, p.7-8).

A prática de *profiling* envolve três fases distintas: coletar dados, analisar de forma automatizada para identificar correlações, e, finalmente, aplicar as correlações a uma pessoa visando identificar características comportamentais presentes ou futuras[700].

Os dados pessoais dos indivíduos não são processados apenas para criar perfis descritivos sobre eles, mas também verificar [seus perfis] em relação a padrões pré-definidos de comportamento normal e determinar se eles se encaixam ou se desviam deles[701].

As decisões automatizadas, por sua vez, têm um âmbito de aplicação diferente e podem ser praticadas em conjunto com a prática de *profiling*. Isso porque a ´definição de perfis' ocorre por tratamento automatizado (exclusivo ou híbrido), porém, sem necessariamente serem realizadas decisões automatizadas. Por outro lado, em um procedimento iniciado com decisão automatizada, posteriormente, poderá ser realizado procedimento baseado em *profiling*. Para melhor compreensão, veja-se exemplo trazido pelo WP29:

> A aplicação de multas por excesso de velocidade com base exclusivamente em provas obtidas através de radares de velocidade constitui um processo de decisão automatizada que não implica necessariamente uma definição de perfis. No entanto, passaria a constituir uma decisão tomada com base na definição de perfis se os hábitos de condução da pessoa fossem controlados ao longo do tempo e, por exemplo, se o montante da multa aplicada resultasse de uma avaliação que tivesse em conta outros fatores, como a reincidência ou não do excesso de velocidade ou o facto de o condutor ter incorrido recentemente em infrações rodoviárias[702].

A tomada de decisão pode ser exclusivamente humana mas baseada em *profiling* quando, por exemplo, um ser humano decide se um crédito deve ou não ser concedido, com base num perfil elaborado de forma automatizada, com finalidade específica de análise. Essa mesma decisão poderia ser tomada sem a intervenção

---

[700] Recommendation CM/Rec (2010)13 and explanatory memorandum adopted by the Committee of Ministers of the Council of Europe on 23 November 2010 and explanatory memorandum. The protection of individuals with regard to automatic processing of personal data in the context of profiling. 23 nov. 2010. Disponível em: <https://rm.coe.int/16807096c3>. Acesso em: 09 jan. 2019, p.25.

[701] KAMARINOU, Dimitra; MILLARD, Christopher; SINGH, Jatinder. Machine learning with personal data (November 7, 2016). **Queen Mary School of Law Legal Studies**. Research Paper n.247, 2016, p.9.

[702] WP29 251 – Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, p.9. As decisões que não são exclusivamente automatizadas podem igualmente incluir a definição de perfis. A título de exemplo, antes da concessão de um crédito hipotecário, um banco poderá tomar em consideração a pontuação de crédito do mutuário, com uma intervenção humana adicional e significativa antes de ser aplicada qualquer decisão a uma pessoa (p.9).

humana, ou seja, de forma exclusivamente automatizada, por meio de um algoritmo decidindo e comunicando à pessoa sobre o resultado da concessão do empréstimo.

O tratamento de dados em decisões automatizadas pode, ademais, ter efeitos significativos em determinados grupos da sociedade, em especial grupos minoritários ou pessoas mais vulneráveis. Por exemplo, uma pessoa que está em dificuldades financeiras e a quem sejam regularmente dirigidos anúncios de empréstimos com juros altos, poderá contratar essas ofertas e, eventualmente, incorrer num maior endividamento. Nesse sentido o WP 251:

> As decisões automatizadas que resultem em preços diferenciados com base em dados pessoais ou características pessoais são igualmente suscetíveis de ter efeitos significativos se, por exemplo, se verificarem preços proibitivos, que excluam efetivamente alguém de certos bens ou serviços. Também podem ser originados efeitos similarmente significativos a partir de ações de pessoas que não aquela a quem a decisão automatizada diz respeito, tal como ilustrado: hipoteticamente, uma empresa de cartões de crédito pode reduzir o limite do cartão de um cliente, baseando-se, não no histórico de reembolso desse cliente, mas em critérios de crédito menos comuns, por exemplo, uma análise de outros clientes que residem na mesma zona e façam compras nas mesmas lojas. Como tal, alguém poderia não ter acesso a oportunidades com base nas ações de outros. Numa perspectiva diferente, o recurso a este tipo de características poderá ter a vantagem de alargar o crédito a pessoas que não dispõem de um histórico de crédito convencional e a quem, de outra forma, teria sido recusado[703].

O *profiling* e as decisões individuais automatizadas (independentemente de incluírem ou não a definição de perfis) devem ser pautados pelo princípio legal da transparência, terem os devidos fundamentos jurídicos para o tratamento dos dados pessoais, além de sempre possibilitarem o direito de oposição e de explicação. Em outras palavras, o responsável pelo tratamento deve fornecer ao titular dos dados informações concisas, transparentes, inteligíveis e de fácil acesso sobre o tratamento dos seus dados pessoais, e com finalidade específica[704]. Segundo

[703] WP29 251 – Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, p.24-25.

[704] Exemplos dado pelo WP29 nesse sentido: 1) Algumas seguradoras oferecem tarifas e serviços de seguros com base no comportamento da pessoa ao volante. Nestes casos, os elementos tidos em conta poderiam incluir a distância percorrida, o tempo passado a conduzir e o trajeto realizado, bem como previsões baseadas noutros dados recolhidos pelos sensores presentes nos automóveis (inteligentes). Os dados recolhidos são utilizados para a definição de perfis, no intuito de identificar maus comportamentos ao volante (a saber, acelerações e travagens bruscas, ou excesso de velocidade). Estas informações podem ser cruzadas com dados de outras fontes (por exemplo, as condições climatéricas, o tráfego ou o tipo de via rodoviária) para ter uma melhor noção do comportamento do condutor. Compete ao responsável pelo tratamento certificar-se de que tem um fundamento lícito para esse tipo de tratamento. O responsável pelo tratamento deve igualmente fornecer ao titular dos dados informações sobre os dados recolhidos e, se for caso disso, sobre a existência de decisões automatizadas referidas no artigo 22º, n.1 e 4, a lógica subjacente e a importância e as consequências previstas de tal tratamento. 2) Algumas aplicações móveis disponibilizam serviços de localização que permitem ao utilizador encontrar restaurantes próximos com oferta de descontos. Contudo, os dados recolhidos são

orientação do WP29: “Os responsáveis pelo tratamento podem proceder à definição de perfis e a decisões automatizadas, desde que estejam em condições de respeitar todos os princípios e tenham um fundamento lícito para o tratamento”[705].

Existem debates sobre o tema com ênfase em ambos os lados, ou seja, tanto por parte dos titulares de dados, quanto da indústria que realiza os processos automatizados. Nesse último caso, alegam, dentre outros fundamentos, que serem forçados a explicar como métodos automatizados complexos funcionam poderia ameaçar seus direitos de propriedade intelectual[706].

Em novembro de 2017, a European Banking Federation emitiu um parecer comentando o documento de Orientações do WP29, em relação à tomada de decisões automatizadas sobre indivíduos e *profiling* (WP251). Dentre outros posicionamentos a federação bancária defendeu as práticas de *profiling* ponderando que essa técnica não necessariamente deve ter um impacto negativo sobre os consumidores:

> In the EBF’s views, it is important to clarify that profiling activities should not necessarily be perceived as having a negative impact on customers. More generally, as far as the banking sector is concerned, profiling is a technique used to provide products and services tailored to customer’s needs, facilitate creditworthiness assessment to ensure responsible lending and more importantly to help combating financial crimes in a constantly evolving digital environment where banks are on the front line and where consumers’ trust is key[707].

Ainda, segundo a Federação de Bancos da Europa, a tomada de decisão automatizada pode ser benéfica para os indivíduos e para a sociedade:

---

igualmente utilizados para criar um perfil do titular dos dados para fins de comercialização – no sentido de determinar as suas preferências gastronómicas ou, de forma geral, o seu estilo de vida. O titular dos dados supõe que os seus dados sirvam para encontrar restaurantes, mas não espera receber anúncios de entrega de pizas apenas porque a aplicação detetou que chega tarde a casa. Esta utilização posterior dos dados de localização pode não se coadunar com as finalidades para as quais foram inicialmente recolhidos, podendo, por isso, exigir o consentimento da pessoa em causa (WP29 251, p.10-12).

[705] WP29 251 – Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, p.10.

[706] Ao considerar a relação entre explicação e segredos comerciais, as mudanças textuais no GDPR alteram o equilíbrio em favor da explicação. Não há, porém, justificativa para tratar as restrições do segredo comercial como axiomáticas sob uma lei inteiramente nova, com uma nova ênfase.

[707] EUROPEAN Banking Federation’s Comments on The Article 29 Working Party Guidelines on Automated Individual Decision-Making And Profiling (WP251). Disponível em: <https://www.ebf.eu/wp-content/uploads/2017/12/EBF_029539-EBF-comments-on-WP29-guidelines-on-automated-decision-making-and-profiling.pdf>. Acesso em: 13 nov. 2018. Tradução livre: Nas opiniões do EBF, é importante esclarecer que as atividades de criação de perfil não devem necessariamente ser vistas como tendo um impacto negativo nos clientes. Mais genericamente, no que diz respeito ao setor bancário, o perfil é uma técnica usada para fornecer produtos e serviços adaptados às necessidades do cliente, facilitar a avaliação de crédito para garantir empréstimos responsáveis e, mais importante, ajudar a combater crimes financeiros em um ambiente digital em constante evolução onde os bancos estão na linha de frente e onde a confiança dos consumidores é fundamental.

> It is important to keep in mind that human decisions are often biased and automated decision-making can therefore help make fairer and more accurate decisions. As stated by the WP29 in its guidelines, automated decision-making can "potentially allow for greater consistency or fairness" or reduce "the risk of customers failing to meet payments for goods or services". We believe this point should also be stressed in the introduction to the guidelines and should be reflected in the interpretation and implementation of the automated decision-making regulatory framework. It is important that the profiling and automated decision-making regulatory framework as a whole puts in place appropriate safeguards without blocking the legitimate and socially beneficial uses of these techniques[708].

Como é de se esperar, a federação que representa o interesse dos bancos – setor de mercado que utilizará cada vez mais, em larga escala, o *profiling* e as tomadas de decisões autotizadas – tem uma postura contrária ao excesso de imposições e restrições a tais práticas. Tanto assim que sugere modificações específicas no texto do WP29[709] e critica os exemplos apostos no documento emitido por essa entidade:

> Although we appreciate the efforts of the WP29 to provide clarity and reassure stakeholders of their rights, we believe some of the examples provided do not reflect the general practice of the banking sector but represent more marginal examples. This approach could be misleading and could lead data subjects to make false assumptions about their banks. We thus offer changes and amendments to highlight more effectively the potential (and, in many cases, already existing) benefits of automated decision-making and profiling in relation to the financial industry[710].

Os debates sobre o assunto são calorosos e tendem a ampliar em razão do exponencial aumento das práticas aqui comentadas. Para os mais conservadores,

---

[708] EUROPEAN Banking Federation's Comments on The Article 29 Working Party Guidelines On Automated Individual Decision-Making And Profiling (WP251). Disponível em: <https://www.ebf.eu/wp-content/uploads/2017/12/EBF_029539-EBF-comments-on-WP29-guidelines-on-automated-decision-making-and-profiling.pdf>. Acesso em: 13 nov.2018. Tradução livre: É importante ter em mente que as decisões humanas são frequentemente tendenciosas e a tomada de decisões automatizada pode, portanto, ajudar a tomar decisões mais justas e precisas. Conforme declarado pelo WP29 em suas diretrizes, a tomada de decisão automatizada pode "potencialmente permitir uma maior consistência ou justiça" ou reduzir "o risco de clientes não conseguirem receber pagamentos por bens ou serviços". Acreditamos que este ponto também deve ser enfatizado na introdução das diretrizes e deve ser refletido na interpretação e implementação do marco regulatório automatizado de tomada de decisão. É importante que a estrutura regulatória de tomada de decisões e automatizada como um todo estabeleça salvaguardas adequadas sem bloquear os usos legítimos e socialmente benéficos dessas técnicas.

[709] EUROPEAN Banking Federation's Comments on The Article 29 Working Party Guidelines on Automated Individual Decision-Making And Profiling (WP251). Disponível em: <https://www.ebf.eu/wp-content/uploads/2017/12/EBF_029539-EBF-comments-on-WP29-guidelines-on-automated-decision-making-and-profiling.pdf>. Acesso em: 13 nov.2018, p.4.

[710] EUROPEAN Banking Federation's Comments on The Article 29 Working Party Guidelines on Automated Individual Decision-Making And Profiling (WP251). Disponível em: <https://www.ebf.eu/wp-content/uploads/2017/12/EBF_029539-EBF-comments-on-WP29-guidelines-on-automated-decision-making-and-profiling.pdf>. Acesso em: 13 nov.2018. Tradução livre: Embora apreciemos os esforços do WP29 para fornecer clareza e tranquilizar as partes interessadas de seus direitos, acreditamos que alguns dos exemplos fornecidos não refletem a prática geral do setor bancário, mas representam exemplos mais marginais. Essa abordagem poderia ser enganosa e poderia levar os titulares de dados a fazerem falsas suposições sobre seus bancos. Assim, oferecemos mudanças e alterações para realçar mais eficazmente os benefícios potenciais (e, em muitos casos, já existentes) da tomada de decisões e perfis automatizados em relação à indústria financeira.

como Andrew Selbst e Julia Powles, decisões automatizadas sem qualquer intervenção ou compreensão humana parecem desprezar as ideias europeias de autonomia e de personalidade[711]. Para os autores, esse debate é complicado, complexo e um desafio técnico não trivial para aproveitar todo o poder dos sistemas *machine learning* ou de inteligência artificial enquanto opera com lógica interpretável para os humanos[712].

Em resposta às questões apresentadas, para salvaguardar os direitos individuais do titular dos dados, estão os direitos à oposição e à explicação. O primeiro diz respeito ao direito do titular de dados de se opor ao tratamento de dados para a definição de perfil (*profiling*). Segundo parte final do art. 21.1 do GDPR:

> O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

O direito à explicação, por sua vez, permite ao titular dos dados requerer e obter intervenção humana por parte do responsável para contestar, se o caso, uma decisão automatizada. Para isso, é preciso que o responsável pelo tratamento seja capaz de *explicar* os elementos que compõem o processo de decisão.

O direito à explicação consiste em um instituto importante para a responsabilização e transparência em algoritmos, inteligência artificial, robótica e outros sistemas automatizados. Isso porque, conforme já abordado neste trabalho, estes sistemas podem implicar em muitos efeitos não intencionais e inesperados.

Segundo Sandra Wachter, Brent Mittelstadt e Luciano Floridi, a extensão desses problemas é difícil devido ao uso de mecanismos algorítmicos complexos e opacos[713]. O direito à explicação exige que os controladores de dados expliquem como esses mecanismos chegam às decisões. Dito isso, passa-se a analisar esse direito com mais demora no próximo item.

---

[711] SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v.7, Issue 4, 1 nov. 2017, p.233.
[712] SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v.7, Issue 4, 1 nov. 2017, p.233.
[713] FLORIDI, Luciano; WACHTER, Sandra; MITTELSTADT, Brent. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, v.7, 2.ed. 1 maio 2017, p.80. Disponível em: <https://doi.org/10.1093/idpl/ipx005>. Acesso em: 16 out. 2018, p.79.

4.6 Inteligência artificial e o direito à explicação

Segundo Andrew Selbst e Julia Powles, tem aumentado o interesse, sob uma perspectiva jurídica, de doutrinadores que começam a explorar tanto a importância do direito à explicação como um valor normativo no contexto de *machine learning* e inteligência artificial[714], além de verificar se existem requerimentos para esse direito sob o ponto de vista do direito positivo:

> There is also rapidly increasing interest from a legal perspective, with a number of scholars beginning to explore both the importance of explanation as a normative value within the ML or AI context, as well as whether there is a requirement for explanation as a matter of positive law[715].

As discussões em torno do assunto 'direito à explicação' estão causando consternação entre pesquisadores, advogados e outros envolvidos com decisões tomadas por *machine learning* ou inteligência artificial. "Os sistemas ML ou AI são, entre os modos possíveis de tomada de decisão, o único perigo de desafiar qualquer compreensão humana"[716].

Há poucos estudos e debates jurídicos sobre o tema. As contribuições mais proeminentes são dois artigos publicados em Oxford, que moldaram os recentes debates públicos. O primeiro deles, de Bryce Goodman e Seth Flaxman, afirma que o GDPR cria um ´direito à explicação´, mas não elabora muito além desse ponto. O segundo, assinado por Sandra Wachter, Brent Mittelstadt e Luciano Floridi, afirma que atualmente não existe ´direito à explicação´, mas sim, um 'direito diferente de ser informado'[717].

Antes, porém, de adentrar à pesquisa doutrinária, cabe verificar como o assunto está posicionado na LGPD e no GDPR.

---

[714] PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015, p.2; HILDEBRANDT, M. 'The new imbroglio: living with machine algorithms' in Janssens (ed), the art of ethics in the information society (Amsterdam UP 2016).

[715] SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v.7, 1 nov. 2017, p.234. Tradução livre: Há também um interesse crescente a partir de uma perspectiva legal, com um número de estudiosos começando a explorar a importância da explicação como um valor normativo dentro do contexto ML ou IA, bem como se há uma exigência de explicação como uma questão de positivar o assunto.

[716] SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v.7, 1 nov. 2017, p.233-242, p.233.

[717] Consoante Andrew Selbst e Julia Powles, a posição de Wachter *et al* distorce o debate, de modo que esses autores afirmam que até o momento não existe nenhum estudo preciso sobre o tema. (SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v.7, 1 nov. 2017, p.234).

Na redação da LGPD, sancionada em 15 de agosto de 2018, foi previsto no artigo 20: “o titular de dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses”. A redação da Medida Provisória n. 869/2018, por sua vez, alterou a redação para

> o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

A nova redação, ao mesmo tempo em que incluiu a ‘definição de perfil pessoal’, retirou a possibilidade de revisão por pessoa natural, diminuindo o âmbito de atuação dos direitos do titular. Da forma como se encontra, trata-se de uma previsão de lei vazia, pois foi retirada a revisão por pessoa natural, podendo a revisão ser feita por processo automatizado, de modo que inexiste proteção, portanto[718].

Importante mencionar que o Superior Tribunal de Justiça já enfrentou o tema sobre tomada de decisões automatizadas. O caso trata de decisão sobre *score* de crédito no qual foi decidido que o consumidor tem direito de saber quais informações pessoais a seu respeito foram valoradas na tomada de decisão automatizada que negou o crédito:

> PROCESSUAL CIVIL. RECURSO ESPECIAL SUBMETIDO À SISTEMÁTICA PREVISTA NO ART. 543-C DO CPC. AÇÃO CAUTELAR DE EXIBIÇÃO DE DOCUMENTOS. CREDISCORE. INTERESSE DE AGIR. DEMONSTRAÇÃO DE QUE A RECUSA DE CRÉDITO OCORREU EM RAZÃO DA FERRAMENTA DE SCORING, ALÉM DE PROVA DO REQUERIMENTO PERANTE A INSTITUIÇÃO RESPONSÁVEL E SUA NEGATIVA OU OMISSÃO. 1. A Segunda Seção do STJ, no julgamento do REsp 1.419.697/RS, submetido ao regime dos recursos repetitivos, definiu que, no tocante ao sistema *scoring* de pontuação, "apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas" (REsp 1419697/RS, Rel. Min. Paulo de Tarso Sanseverino, Segunda Seção, j.12-11-2014, DJe 17-11-2014). 2. Assim, há interesse de agir para a exibição de documentos sempre que o autor pretender conhecer e fiscalizar documentos próprios ou comuns de seu interesse, notadamente referentes a sua pessoa e que estejam em poder de terceiro, sendo que

[718] O teor dos §§1º e 2º do artigo não foram modificados e preveem: “§1º o controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. §2º Em caso de não oferecimento de informações de que trata o §1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.”

> "passou a ser relevante para a exibitória não mais a alegação de ser comum o documento, e sim a afirmação de ter o requerente interesse comum em seu conteúdo". (SILVA, Ovídio A Batista da. Do processo cautelar. Rio de Janeiro: Forense, 2009, fl. 376). [...] (Recurso Especial n. 1.304.736 – RS, Rel. Min. Luis Felipe Salomão, sob a sistemática dos Recursos Repetitivos, DJE 30/03/2016).

Com base no artigo 43 do Código de Defesa do Consumidor, reconheceu-se um direito de explicação, a fim de conferir ao consumidor o direito de saber quais de seus dados pessoais foram utilizados na tomada de decisão automatizada.

Já o novo Regulamento europeu sofisticou a regra anterior da Diretiva 95/46, contida em seu artigo 15[719], quanto às *decisões* tomadas exclusivamente com base no tratamento automatizado. Desde o fim do século XX esse instituto já ecoava na afirmação de uma sociedade dominada pelas máquinas[720]. Porém, de outro lado, a Diretiva de 1995 não trouxera, em seu texto, a definição de *profiling*, indicando que se trata de uma prática e preocupação mais recentes[721].

Ao comparar a Diretiva 95/46 e o GDPR, ponderam Sandra Wachter, Brent Mittelstadt e Luciano Floridi:

> Although Article 22 GDPR has not greatly changed from Article 15 of the Directive, a few changes are still noteworthy. First, the only safeguard against automated decision-making mentioned in the Directive is the opportunity to express one's views. Article 22(3) additionally names contesting the decision and the right to obtain human intervention as suitable measures. Secondly, explicit consent is included as a case in which automated decision-making is allowed (Article 22(2)c). Finally, as opposed to the provisions in Article 15 of the Directive, it is no longer necessary that the data subject requests the contract in order for automated decisionmaking to be lawful.[722].

---

[719] Artigo 15 da Diretiva 95/46: Artigo 15º. Decisões individuais automatizadas. 1. Os Estados membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento. 2. Os Estados membros estabelecerão, sob reserva das restantes disposições da presente directiva, que uma pessoa pode ficar sujeita a uma decisão do tipo referido no n.1 se a mesma: a) For tomada no âmbito da celebração ou da execução de um contrato, na condição de o pedido de celebração ou execução do contrato apresentado pela pessoa em causa ter sido satisfeito, ou de existirem medidas adequadas, tais como a possibilidade de apresentar o seu ponto de vista, que garantam a defesa dos seus interesses legítimos; ou b) For autorizada por uma lei que estabeleça medidas que garantam a defesa dos interesses legítimos da pessoa em causa.

[720] Mais recentemente, tanto o grupo WP29, como o Conselho da Europa emitiram documentos a respeito da proteção de indivíduos quanto ao processamento automatizado de dados pessoais no contexto do *profiling*, respectivamente: WP251 rev.01 Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679, adopted on 3 october 2017, as last revised and adopted on 6 february 2018. (Disponível em: <https://iapp.org/media/pdf/resource_center/W29-auto-decision_profiling_02-2018.pdf>. Acesso em: 09 nov. 2018); CONSELHO DA EUROPA. Recommendation CM/Rec (2010)13 and explanatory memorandum. The protection of individuals with regard to automatic processing of personal data in the context of profiling, de 23 nov. 2010. Disponível em: <https://rm.coe.int/16807096c3>. Acesso em: 9 nov. 2018.

[721] Em que pese não ter sido plasmado expressamente na Diretiva em comento, o artigo 16 do *explanatory memorandum* à proposta da Diretiva 95/46, escrita em 1992, dispôs sobre o assunto.

[722] FLORIDI, Luciano; WACHTER, Sandra; MITTELSTADT, Brent. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, v.7,

Para além da Diretiva de 1995, e em que pese o direito em questão não estar expressamente mencionado no artigo 8 Carta da União Europeia[723] de 2000, deve ser considerado incluído na disposição, como derivação do direito à proteção de dados pessoais, no mesmo nível dos outros direitos específicos indicados. Tampouco se encontra na Conveção 108, versão original de 1981.

Não obstante, essa temática se tornou central às autoridades de privacidade. Segundo Luca Bolognini, Enrico Pelino e Camilla Bistolfi,

> L´istituto [...] há portata indiscutibilmente attuale e riceve collocazione centrale nella matéria in comento, come conferma il fato che abbia costituito uno dei blocchi fondamentali su cui si è soffermata l´analisi dei Garanti europei a proposito dele garanzie fondamentali da osservare nell´Unione (WP251rev.01). In precedenza, era stato oggetto di attenzione monográfica nella raccomandazione CM/Rec (2010)13 del Consiglio d´Europa[724].

Trata-se da decisão realizada apenas com base em dados pessoais gerados artificialmente por meio de algoritmos, tendo como resultado a elaboração de conjuntos de informações bastante estruturadas ou 'definição de perfis', capazes de permitir análises e predições de comportamentos e até de atitudes morais do interessado. É essa a lição de Luca Bolognini, Enrico Pelino e Camilla Bistolfi:

> La decisione sull´interessato cui fa riferimento l´articolo in comento è quella che viene presa sulla *sola* base di dati personali artificialmente generati attraverso algoritmi (tipicamente fattori di calcolo matematici e processi statistici) applicati a um insieme di dati personali di partenza efetivamente riconducibili all´interessato. Gli esiti di tali elaborazione sono gruppi di informazioni suficientemente strtturate o veri e propri "profili", idonei a permetter *valutazioni, analisi* o perfino a *prevedere* comportamenti, modalità relazionali e perfino atteggiamenti morali dell´interessato[725].

2.ed. 1 maio 2017, p.80. Disponível em: <https://doi.org/10.1093/idpl/ipx005>. Acesso em: 16 out. 2018. Tradução livre: Embora o artigo 22.º do GDPR não tenha mudado substancialmente em relação ao artigo 15.º da Diretiva, algumas alterações são ainda dignas de nota. Em primeiro lugar, a única salvaguarda contra a tomada de decisões automatizada mencionada na diretiva é a oportunidade de expressar as suas opiniões. O Artigo 22.3 adiciona nomes contestando a decisão e o direito de obter intervenção humana como medidas adequadas. Em segundo lugar, o consentimento explícito é incluído como um caso no qual a tomada de decisão automatizada é permitida (Artigo 22.2.c. Por último, contrariamente ao disposto no artigo 15° da Diretiva, já não é necessário que o titular dos dados solicite o contrato para que a tomada de decisão automatizada seja lícita.

[723] Artigo 8º. Proteção de dados pessoais. 1.Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de acessar aos dados coletados que lhes digam respeito e de obter a respectiva rectificação. 3.O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

[724] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milano/Italia: Giuffrè, 2010, p.270.

[725] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milano/Italia: Giuffrè, 2010, p.267.

Ainda segundo os autores, o que conta para a aplicação desse instituto é que a base da decisão tenha se dado de forma automatizada:

> Va notato che non è richiesto che la decisione sia anch´essa automatizzata, ciò che conta è che essa, ancorchè umana, sai basata *in via exclusiva* su um tratamento automatizzato. Di conseguenza, uma decisione che tenga conto anche di altri fattori non reentra nella sfera aplicativa dela norma. Non dovrebbero giovare tuttavia al titolare scelte elusive volte a sottrarsi al precetto, surrettiziamente introducendo basi di valutazione non automatizzate ma del tutto irrilevanti ai fini dela decisione ultima[726].

Nesse sentido, o considerando 71 do GDPR aponta como direito do titular dos dados, o de não ficar sujeito a uma decisão gerada artificialmente por meio de algoritmos e de efeitos jurídicos que lhe afetem de modo significativo:

> O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspectos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana.

Cria-se um instrumento, portanto, em prol da defesa da pessoa humana, visando evitar decisões discriminatórias. É dizer, "la *ratio* dell instituto appare perciò quella di fornire uno strumento di contrasto per evitare, o contenere, pregiudizi all sfera giuridica dell´interessato che possano derivare da siffatte decisioni"[727].

Ademais, o considerando 71 esclarece que esse tratamento inclui a definição de perfis para avaliar aspectos pessoais relativos a uma pessoa singular, especialmente, mas não apenas, quanto à análise e previsão de aspectos relacionados ao desempenho profissional, à situação econômica, à saúde, às preferências ou aos interesses pessoais, e quanto à localização do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar.

No entanto, ainda com amparo no considerando em questão, existem alguns casos possíveis de tomada de decisões com base nesse tipo de tratamento, incluindo a definição de perfis: (i.) se expressamente autorizada pelo direito da União ou dos Estados membros aplicável ao responsável pelo tratamento, incluindo casos

---

[726] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milano/Italia: Giuffrè, 2016, p.271.

[727] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milano/Italia: Giuffrè, 2016, p.267. Tradução livre: "A *ratio* do Instituto, portanto, parece fornecer um meio de contraste para evitar ou conter preconceitos à esfera jurídica da parte interessada que possam derivar de tais decisões".

destinados ao controle e prevenção de fraudes e da evasão fiscal; (ii.) para garantir a segurança e a confiança no serviço prestado pelo responsável pelo tratamento, ou se for necessária para celebrar ou executar um contrato entre o titular dos dados e o responsável pelo tratamento; (iii.) mediante o consentimento explícito do titular.

Há, também, uma segunda hipótese relativa à derrogação de lei, que está condicionada ao indicativo de "casos destinados ao controle e prevenção de fraudes e da evasão fiscal".

Porém, não obstante a base legal permissiva, o tratamento deverá ser acompanhado das garantias adequadas, as quais deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão.

Ademais, o legislador europeu, pautado pela transparência, dispôs que a fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados – considerando a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados – o responsável pelo tratamento deverá (i.) utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis; (ii.) aplicar medidas técnicas e organizativas que garantam que os fatores erros sejam minimizados, e ainda (iv.) proteger os dados pessoais considerando os potenciais riscos para os interesses e os direitos do titular dos dados de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos[728]. Decidir e definir perfis automáticos baseados em categorias especiais de dados pessoais só será permitido em condições específicas.

Em parte vinculante, o Regulamento garante ao titular dos dados o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. Porém, esse direito é recuado em algumas situações, as quais já foram adiantadas no Considerando 71 e que o legislador repete quase integralmente, no artigo 22[729]. O caso, porém, de

[728] Considerando 71, GDPR.

[729] Artigo 22.2: O n.1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou

exceção, previsto no artigo 22.2.b, diversamente do previsto no considerando 71, traz cláusula finalística de salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados, que deve ser lido em conjunto com o artigo 52 da Carta UE[730]. Quanto aos outros dois casos de exceção, ambos fundamentados sob o consenso, na lição de Luca Bolognini, Enrico Pelino e Camilla Bistolfi:

> Quanto alle due ipotesi deroga delle lett. *a* e *c* [...] pare a chi scrive che non sai valorizzata la posizione di parte debole dell´interessato. Invero, mentre l´ipotesi *c* potrebbe essere ricondotta ai noti schemi di tutela riconosciuti nella matéria *de qua* all´interessato, legati a uma nozione molto rigorosa di libertà di determinazione non altrettanto può dirsi per l´ipotesi di cui alla lett. *a*[731].

No caso das bases permissivas desse tipo de tratamento, referente à celebração ou execução de um contrato entre o titular dos dados e um responsável pelo tratamento, quando também referente ao tratamento baseado no consentimento explícito do titular dos dados, o Regulamento determina que o responsável pelo tratamento deve aplicar as medidas adequadas para garantir os direitos, liberdades e legítimos interesses do titular dos dados, para, ao menos, obter a intervenção humana do responsável, manifestar o seu ponto de vista e contestar a decisão[732].

O GDPR veda expressamente que decisões tomadas exclusivamente com base no tratamento automatizado recaiam sobre dados sensíveis, ou seja, revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, o tratamento de dados genéticos, dados biométricos para identificar uma pessoa inequivocamente, dados relativos à saúde, à vida sexual ou à orientação sexual de uma pessoa. A vedação em relação aos dados sensíveis se estende mesmo às hipóteses permissivas do artigo 22.2 da GDPR, exceto em duas situações[733]: (i.) se o titular dos dados tiver consentido explicitamente para o tratamento de seus dados pessoais sensíveis para uma ou mais finalidades

---

do Estado membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas c) For baseada no consentimento explícito do titular dos dados.

[730] Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.

[731] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milão-Itália: Giuffrè, 2016, p.274.

[732] Artigo 22.3 GDPR

[733] Artigo 22.4: As decisões a que se refere o n.2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9º, n.1, a não ser que o n.2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

específicas, e desde que não venha a ser proibido pela União ou Estados membros o tratamento de dados pessoais[734]; e (ii.) se o tratamento for necessário por motivos de interesse público importante[735], com base no direito da União ou de um Estado membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados.

O direito em questão é exercido exclusivamente "nei confronti del titolare, che può delegare responsabili e personale dependente quali punti di contato per l´interessato e per lo svolgimento dele attività esecutive conseguenti all´esercizio del diritto"[736].

Em crítica ao artigo 22 do GDPR, Sandra Wachter, Brent Mittelstadt e Luciano Floridi ressaltam que um *direito à explicação* não é mencionado no dispositivo. Diz-se que após uma decisão ter sido tomada, e assumindo que a decisão preencha uma condição especificada no artigo 22.3.a (para aderir ou cumprir um contrato) ou no artigo 22.3.b (com consentimento explícito), os titulares dos dados recebem salvaguardas para obter intervenção humana, pontos de vista, ou contestar uma decisão, mas não exatamente para obter uma explicação da decisão alcançada[737].

No texto do GDPR, o direito à explicação somente é explicitamente mencionado no considerando 71 (não vinculante), segundo o qual uma pessoa que tenha sido objeto de um processo de decisão automatizado deve estar sujeito a salvaguardas adequadas, que devem incluir informações específicas à pessoa em causa e o direito de obter intervenção humana, expressar o seu ponto de vista, obter uma explicação da decisão tomada após essa avaliação e contestar a decisão. Ocorre que os considerandos não são vinculativos, e, ainda que o fossem, tratar-se-ia de uma explicação *ex post* de determinadas decisões.

Na lição de Sandra Wachter, Brent Mittelstadt e Luciano Floridi, um direito à explicação não seria, portanto, legalmente exigido pelos requisitos estabelecidos:

---

[734] Artigo 9.2.a: Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais [dados sensíveis] para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.o 1 não pode ser anulada pelo titular dos dados;

[735] Ipotesi connotata de censurabile genericità. (BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milão-Itália: Giuffrè, 2016, p.275).

[736] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milão-Itália: Giuffrè, 2016, p.267.

[737] FLORIDI, Luciano; WACHTER, Sandra; MITTELSTADT, Brent. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, v.7, 2.ed. 1 maio 2017, p.80. Disponível em: <https://doi.org/10.1093/idpl/ipx005>. Acesso em: 16 out. 2018, p.79.

> Article 22.3 lists the minimum requirements that have to be met for lawful automated decision-making. There are no ambiguities in the language that would require further interpretation with regard to the minimum requirements that must be met by data controllers. As long as these requirements are met, automated decision-making is lawful and in compliance with the GDPR. With this said, future jurisprudence can still interpret the meaning of 'suitable measures to safeguard', and establish future mandatory or case-to-case requirements to be met by data controllers, including a right to explanation. This is, however, only one possible future. A right to explanation is thus not currently legally mandated by the requirements set in Article 22.3[738].

Além disso, os direitos devem ser explícita e legalmente estabelecidos antes de sua aplicação. Esta ideia decorre da relação entre direitos e deveres. O escopo de um direito pode estar sujeito à interpretação; uma base legal para a sua existência deve, no entanto, primeiro se encontrar além da dúvida incontestável. Os direitos dos titulares de dados normalmente correspondem a um dever por parte do controlador de dados. A negligência em relação aos seus deveres pode ser punida através de multas e outros procedimentos. Seria altamente controverso impor multas aos controladores de dados sem ter esclarecido explicitamente quais deveres devem ser cumpridos. Caso contrário, entraria em conflito com os princípios de um julgamento justo (artigo 6º da Convenção Europeia dos Direitos do Homem e artigo 47º da Carta dos Direitos Fundamentais da União Europeia) e do Estado de Direito. Os procedimentos penais e administrativos devem ser estabelecidos com bases precisas[739]. Nesse sentido, ponderam Sandra Wachter, Brent Mittelstadt e Luciano Floridi:

> It can be concluded that data subjects will not be granted a legally binding ex post right to explanation of specific automated decisions on the basis of legal safeguards in Article 22 as it currently stands. That this is the case does not appear to be the result of an oversight or fiddling with subtle interpretations (eg the meaning of 'suitable measures to safeguard' in Article 22(3)). On the contrary, the omission of a right to explanation from Article 22 appears to be intentional. The safeguards specified in Recital 71 are almost identical to those in Article 22(3), with the significant difference of the further inclusion of a right 'to obtain an explanation of the decision reached after such assessment' in Recital 71. The purposeful omission of this text from Article

[738] FLORIDI, Luciano; WACHTER, Sandra; MITTELSTADT, Brent. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, v.7, 2.ed. 1 maio 2017, p.80. Disponível em: <https://doi.org/10.1093/idpl/ipx005>. Acesso em: 16 out. 2018, p.79. Tradução livre: O Artigo 22.3 lista os requisitos mínimos que devem ser cumpridos para a tomada de decisão automatizada. Não há ambigüidades na linguagem que exijam interpretação adicional em relação aos requisitos mínimos que devem ser atendidos pelos controladores de dados. Desde que esses requisitos sejam atendidos, a tomada de decisões automatizada é legal e está em conformidade com o GDPR. Dito isso, a futura jurisprudência ainda pode interpretar o significado de "medidas adequadas para salvaguardar" e estabelecer futuros requisitos obrigatórios ou requisitos caso a caso a serem cumpridos pelos controladores de dados, incluindo o direito à explicação. Este é, no entanto, apenas um futuro possível. Portanto, o direito à explicação não é legalmente exigido pelos requisitos estabelecidos no Artigo 22.3.

[739] FLORIDI, Luciano; WACHTER, Sandra; MITTELSTADT, Brent. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, v.7, 2.ed. 1 maio 2017, p.80. Disponível em: <https://doi.org/10.1093/idpl/ipx005>. Acesso em: 16 out. 2018, p.79.

> 22 may not be an oversight but suggests that legislators did not intend to implement a right to explanation of specific decisions in the GDPR[740].

Sobre a interpretação do art. 22.1 do GDPR, a European Banking Federation defende:

> Focus on the "right not to be subject to automated decision-making" in line with the GDPR instead of full prohibition: The EBF fully supports the objectives of the GDPR to increase transparency around personal data processing and to give data subjects more control over their data. However, the WP29's interpretation of Article 22(1) as a full prohibition is going further than what is prescribed by the GDPR. Instead of using the word 'prohibit' (which the GPDR uses in other articles for instance; see Article 9(1) on the 'processing of special categories of data'), Article 22(1) grants data subjects the right not to be subject to a decision based solely on automated processing of personal data. We believe that the guidelines should be better aligned with the intent of the GDPR and ensure that citizens and data subjects can fully benefit from the rights granted to them by the GDPR[741].

Para Sandra Wachter, Brent Mittelstadt e Luciano Floridi, tendo em vista que o artigo 22 do GDPR não trouxe um direito à explicação, resta olhar para os artigos 13 e 14 do mesmo diploma cujos dispositivos especificam deveres de notificação para controladores de dados relativos ao processamento de dados coletados do interessado (artigo 13º) ou de um terceiro (artigo 14º). As bases legais citadas servem de alicerce a um direito *ex post* de explicação de decisões específicas. A reivindicação, assim, começa com o artigo 13.2 e 14.2, os quais estabelecem que os responsáveis pelo tratamento de dados precisam: "fornecer ao titular dos dados as

---

[740] FLORIDI, Luciano; WACHTER, Sandra; MITTELSTADT, Brent. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, v.7, 2.ed. 1 maio 2017, p.80. Disponível em: <https://doi.org/10.1093/idpl/ipx005>. Acesso em: 16 out. 2018. Tradução livre: Pode ser concluído que os titulares de dados não receberão um direito à explicação *ex post* juridicamente vinculativo de decisões automatizadas específicas com base nas garantias jurídicas do artigo 22, na sua versão atual. Este é o caso que não aparenta ser o resultado de um esquecimento ou de uma interpretação sutil (por exemplo, o significado de "medidas adequadas a salvaguardar" no artigo 22.3). Pelo contrário, a omissão de um direito à explicação do Artigo 22 parece ser intencional. As garantias especificadas no considerando 71 são quase idênticas às do n.3 do artigo 22., com a diferença significativa entre a inclusão de um direito "para obter uma explicação da decisão alcançada após essa avaliação" no considerando 71. A omissão intencional do texto do Artigo 22 pode não ser um esquecimento, mas sugere que os legisladores não pretenderam implementar o direito à explicação de decisões específicas no GDPR.

[741] EUROPEAN Banking Federation's Comments on The Article 29 Working Party Guidelines on Automated Individual Decision-Making And Profiling (WP251). Disponível em: <https://www.ebf.eu/wp-content/uploads/2017/12/EBF_029539-EBF-comments-on-WP29-guidelines-on-automated-decision-making-and-profiling.pdf>. Acesso em: 13 nov. 2018. Tradução livre: Concentre-se no "direito de não estar sujeito à tomada de decisões automatizada" alinhado com o GDPR em vez da proibição total: O EBF apoia totalmente os objetivos do GDPR de aumentar a transparência em torno do processamento de dados pessoais e dar aos sujeitos dados mais controle sobre seus dados. No entanto, a interpretação do artigo 22 (1) do WP29 como uma proibição total está indo além do que é prescrito pelo GDPR. Em vez de utilizar a palavra «proibir» (que o GPDR utiliza noutros artigos, por exemplo; ver artigo 9º, nº 1, sobre o «tratamento de categorias especiais de dados»), o nº 1 do artigo 22º concede aos titulares das informações o direito de não serem sujeita a uma decisão baseada exclusivamente no tratamento automatizado de dados pessoais. Acreditamos que as diretrizes devem ser mais bem alinhadas com a intenção do GDPR e garantir que os cidadãos e os titulares de dados possam se beneficiar plenamente dos direitos concedidos a eles pelo GDPR.

seguintes informações necessárias para garantir um processamento justo e transparente".

De acordo com os artigos 13.2 e 14.2.g, essas informações incluem

> a existência de decisões automatizadas, a definição de perfis, referidas nos nºs 1 e 4 do artigo 22º e, pelo menos nesses casos, informações significativas sobre a lógica em causa, bem como a importância e as consequências previstas de tal tratamento para o assunto dos dados.

Estes deveres aplicam-se nos casos de tratamento automatizado que satisfaçam os requisitos do n.1 do artigo 22º ou do n.4 do artigo 22º.

Há aqueles que sugerem que os deveres de notificação dos artigos 13º a 14º, em combinação com as salvaguardas definidas no artigo 22.3, conferem um direito *ex post* à explicação da existência da lógica envolvida e das consequências previstas, quanto à automatização de tomada de decisão. Porém, segundo apontam Sandra Wachter, Brent Mittelstadt e Luciano Floridi, esse entendimento está errado por duas razões. Em primeiro lugar, apenas uma explicação *ex ante* da funcionalidade do sistema é explicitamente exigida pelos artigos 13.2.f e 14.2.g. Esses deveres de notificação precedem a tomada de decisão. A notificação ocorre antes de uma decisão ser tomada, no momento em que os dados são coletados para processamento. Isto permanece válido mesmo que o artigo 14 introduza algumas ambiguidades quando os dados são recolhidos de terceiros em vez do interessado titular dos dados (na medida em que o responsável pelo tratamento só precisa notificar o titular dos dados 30 dias após a coleta). E uma explicação da funcionalidade do sistema somente será lógica se ocorrer antes da tomada de decisão. Por conseguinte, os artigos 13º a 14º não podem ser utilizados como base para afirmar um direito *ex post* de explicação de determinadas decisões, que só podem ser logicamente dadas após a tomada de uma decisão (*timeline problem*). Em segundo lugar o entendimento está incorreto porque vincula os artigos 13.2.f e 14.2.g às salvaguardas do artigo 22.3, quando, na verdade, essa ligação não é feita no GDPR. Os artigos 13.2.f e 14.2.g se aplicam apenas aos artigos 22.1 e 22.4, os quais, por sua vez, não contemplam as salvaguardas contra a tomada de decisão automatizada. Nas palavras dos autores:

> The supposed link – between notification about the logic involved, significance, and envisaged consequences of automated decision-making in Articles 13-14, and the ex post right to explanation incorrectly attributed to Article 22(3) (which only features in Recital 71) – is therefore untenable and

> can be dismissed. The claim also conflates the legally binding notification duties, specified in Articles 13-14, and the non-binding right, specified in Recital 71. It follows that the claim for an ex post right to explanation of specific decisions is not correct. Any suggestion to the contrary fails to distinguish between (i) the legally binding duty to notify the data subject of the logic involved, significance, and envisaged consequences of automated decision-making system before decision-making occurs (timeline problem) (Articles 13-14), and (ii) the data subject's non-binding right to an explanation of specific decisions (Recital 71) after decision-making occurs.[742]

Para Andrew Selbst e Julia Powles, os artigos 13 a 15 fornecem direitos a "informações significativas sobre a lógica envolvida" em decisões automatizadas. Os autores consideram que faz sentido chamar isso de direito à explicação, mas esse ponto é menos importante do que a substância do direito em si. Acrescentam que o direito à explicação deve ser interpretado de forma funcional, flexível e deve, no mínimo, permitir que um titular de dados exerça os seus direitos ao abrigo do GDPR e da 'lei de direitos humanos'[743].

No que diz respeito à responsabilidade pelo tratamento de dados, na linha do considerando 74, o responsável pelo tratamento deverá ficar obrigado a executar as medidas adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas conforme o Regulamento europeu, incluindo a eficácia das medidas. Essas, por sua vez, deverão considerar a natureza, o âmbito, o contexto e

---

[742] Tradução livre: A suposta ligação – entre a notificação da lógica envolvida, a importância e as consequências previstas na tomada de decisão automatizada nos artigos 13. a 14. e o direito *ex post* à explicação incorretamente atribuída ao artigo 22, n. 3 (que apenas figura no considerando 71) portanto, é insustentável e pode ser descartado. A questão também combina os deveres de notificação juridicamente vinculativos, especificados nos artigos 13 a 14, e o direito não vinculativo, especificado no considerando 71. Daqui decorre que o pedido de um direito ex post de explicação de decisões específicas não é correto. Qualquer sugestão em contrário falha em distinguir entre (i) o dever legal de notificar o titular dos dados da lógica envolvida, significado e consequências previstas do sistema automatizado de tomada de decisões antes que ocorra a tomada de decisão (problema na linha do tempo) (Artigos 13-14), e ii) o direito não vinculativo da pessoa em causa a uma explicação de decisões específicas (considerando 71) após a tomada de decisões. (FLORIDI, Luciano; WACHTER, Sandra; MITTELSTADT, Brent. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, v.7, 2.ed. 1 maio 2017, p.80. Disponível em: <https://doi.org/10.1093/idpl/ipx005>. Acesso em: 16 out. 2018). The language used in Articles 13(2)f and 14(2)g also supports the interpretation that only an ex ante explanation is required. […] The language used suggests that data subjects must be provided with information about how an automated decision-making system works in general, for which purposes, and with what predicted impact, before automated decisions are made. Notably this cannot include any information about how a specific decision was made or reached, but rather addresses how the system itself functions, eg its decision tree or rules, or predictions about how inputs will be processed. For fully disclosed simplistic or linear models, this may show how specific decisions would be reached in the future (p.82-83). Tradução livre: A linguagem utilizada nos artigos 13.2.f e 14.2.g também reforça a interpretação de que apenas é necessária uma explicação ex ante. […] A linguagem usada sugere que os titulares de dados devem receber informações sobre como funciona em geral, um sistema de tomada de decisões automatizadas, para quais fins e qual o impacto previsto, antes que as decisões automatizadas sejam tomadas. Notavelmente, isso não pode incluir nenhuma informação sobre como uma decisão específica foi tomada ou atingida, mas, em vez disso, aborda como o próprio sistema funciona, por exemplo, sua árvore ou regras de decisão, ou previsões sobre como os *inputs* serão processados. Para modelos simplistas ou lineares totalmente divulgados, isso pode mostrar como decisões específicas seriam alcançadas no futuro.

[743] SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v.7, 4.ed. 1 nov. 2017, p.242.

as finalidades do tratamento dos dados, além do risco que possa implicar para os direitos e liberdades das pessoas singulares.

Quanto ao âmbito de aplicação desse direito, é necessária a presença cumulativa de duas condições: (i.) a decisão deve produzir efeitos sobre a esfera jurídica do interessado; e (ii.) a decisão deve ter sido baseada *unicamente* sobre um tratamento automatizado.

Em consonância com as limitações gerais do tema da disciplina, o instituto não se aplica nas hipóteses que saiam do âmbito material do Regulamento, cujas situações estão previstas em seu artigo 2[744], a exemplo do tratamento de uma atividade exclusivamente pessoal ou doméstica. Por outro lado, se enquadrado no âmbito material de aplicação, nota-se que o Regulamento traz hipóteses específicas de derrogação nos casos comentados acima, e indicados no §2º do artigo 22, vale dizer, derrogação contratual, por disposição legal, e após o consentimento explícito do interessado.

Observa-se, ademais, a aplicação das limitações gerais dispostas no artigo 23 e ao correlato considerando 73, no sentido de que o direito da União ou dos Estados membros a que estejam sujeitos o responsável pelo tratamento, ou o seu subcontratante, pode limitar por lei o alcance do direito à explicação contido no artigo 22 da GDPR, desde que tal limitação (i.) respeite a essência dos direitos e liberdades fundamentais e (ii.) seja medida necessária e digna de uma sociedade democrática para resguardar: a) a segurança do Estado; b) a defesa; c) a segurança pública; d) a prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; e) outros objetivos importantes do interesse público geral da União ou de um Estado membro, nomeadamente um interesse econômico ou financeiro importante da União ou de um Estado membro, incluindo nos domínios

[744] Artigo 2. Âmbito de aplicação material: 1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados. 2. O presente regulamento não se aplica ao tratamento de dados pessoais: a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União; b) Efetuado pelos Estados membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. 3. O Regulamento (CE) n.45/2001 aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n.45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no artigo 98. 4. O presente regulamento não prejudica a aplicação da Diretiva 2000/31/CE, nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12º a 15º.

monetário, orçamental ou fiscal, da saúde pública e da segurança social; f) a defesa da independência judiciária e dos processos judiciais; g) a prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas; h) uma missão de controle, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas "a", "e", "g"; i) a defesa do titular dos dados ou dos direitos e liberdades de outrem; j) a execução de ações cíveis.

Os Estados membros, outrossim, são convidados pelo Regulamento a estabelecerem limites ou isenções aos direitos assinalados no artigo 85.2[745], no que inclui o direito em voga, desde que estes atos sejam necessários para conciliar o direito à proteção de dados pessoais com a liberdade de expressão e de informação. Por sua vez, o legislador deixou de permitir similar limitação nos casos de decisões individuais automatizadas para arquivo de interesse público, investigação científica ou histórica ou para fins estatísticos[746].

Além disso, visando facilitar o exercício pelo titular dos dados dos direitos que lhe são conferidos ao abrigo do Regulamento, e em linha com o considerando 59, o responsável pelo tratamento deverá fornecer os meios necessários para que os pedidos possam ser apresentados por via eletrônica, em especial quando os dados forem tratados por essa via. Ainda, o responsável pelo tratamento deverá ser

[745] Artigo 85.2: Para o tratamento efetuado para fins jornalísticos ou para fins de expressão académica, artística ou literária, os Estados membros estabelecem isenções ou derrogações do capítulo II (princípios), do capítulo III (direitos do titular dos dados), do capítulo IV (responsável pelo tratamento e subcontratante), do capítulo V (transferência de dados pessoais para países terceiros e organizações internacionais), do capítulo VI (autoridades de controlo independentes), do capítulo VII (cooperação e coerência) e do capítulo IX (situações específicas de tratamento de dados) se tais isenções ou derrogações forem necessárias para conciliar o direito à proteção de dados pessoais com a liberdade de expressão e de informação.

[746] Artigo 89. Garantias e derrogações relativas ao tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos. 1. O tratamento para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, está sujeito a garantias adequadas, nos termos do presente regulamento, para os direitos e liberdades do titular dos dados. Essas garantias asseguram a adoção de medidas técnicas e organizativas a fim de assegurar, nomeadamente, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a pseudonimização, desde que os fins visados possam ser atingidos desse modo. Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo. 2. Quando os dados pessoais sejam tratados para fins de investigação científica ou histórica ou para fins estatísticos, o direito da União ou dos Estados membros pode prever derrogações aos direitos a que se referem os artigos 15, 16, 18 e 21, sob reserva das condições e garantias previstas no n.1 do presente artigo, na medida em que esses direitos sejam suscetíveis de tornar impossível ou prejudicar gravemente a realização dos fins específicos e que tais derrogações sejam necessárias para a prossecução desses fins. 3.Quando os dados pessoais sejam tratados para fins de arquivo de interesse público, o direito da União ou dos Estados membros pode prever derrogações aos direitos a que se referem os artigos 15, 16, 18, 19, 20e 21, sob reserva das condições e garantias previstas no n.1 do presente artigo, na medida em que esses direitos sejam suscetíveis de tornar impossível ou prejudicar gravemente a realização dos fins específicos e que tais derrogações sejam necessárias para a prossecução desses fins. 4. Quando o tratamento de dados previsto no n.2 e 3 também se destine, simultaneamente, a outros fins, as derrogações aplicam-se apenas ao tratamento de dados para os fins previstos nesses números.

obrigado a responder aos pedidos do titular dos dados sem demora injustificada, e no mais tardar, em um mês, além de expor suas razões quando tiver intenção de recusar o pedido. Por fim, o exercício desse direito deverá ser, em regra, gratuito conforme determinação legal, nos moldes do disposto no artigo 12.5 do GDPR[747].

Sob outra perspectiva, necessário considerar questão relevante sobre o tema: a geração de novos dados pessoais a partir do processamento automatizado, por meio de algoritmos, sobre os dados fornecidos pelo titular. Nesse sentido, explica o Conselho da Europa:

> Considering that profiles, when they are attributed to a data subject, make it possible to generate new personal data which are not those which the data subject has communicated to the controller or which she or he can reasonably presume to be known to the controller[748].

Coloca-se aqui quase o extremo oposto ao concebido pelo princípio da autodeterminação informativa. Aqui reside a pedra de toque, e, assim, um dos elementos mais preocupantes: o risco de o indivíduo ser expropriado do direito de construir e controlar a própria imagem social. Guarda, portanto, relação com o princípio da liberdade informacional.

Destaca-se, nesse quadrante, a tendência à opacidade do mecanismo criativo, baseada em procedimentos e algoritmos desconhecidos do interessado, e o desequilíbrio informacional, uma vez que o titular possui informações adicionais e enriquecidas em relação aos originais. É fundamental que a parte interessada dê instrumentos adequados para conhecer pelo menos a lógica (pois o *know-how* e os processos subjacentes são outra coisa) do processamento automatizado e dos dados pessoais que lhe são atribuídos como resultado da criação de perfil ou do processamento automatizado[749]. O objetivo é possibilitar o exercício do direito à explicação e, eventualmente, como desdobramento, atender ao pedido de correção

---

[747] Art. 12.5: As informações fornecidas nos termos dos artigos 13 e 14 e quaisquer comunicações e medidas tomadas nos termos dos artigos 15 a 22 e 34 são fornecidas a título gratuito. Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, o responsável pelo tratamento pode: a) exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas; ou b) Recusar-se a dar seguimento ao pedido. Cabe ao responsável pelo tratamento demonstrar o caráter manifestamente infundado ou excessivo do pedido.

[748] CONSELHO DA EUROPA. **Recommendation CM/Rec (2010)13 and explanatory memorandum**. The protection of individuals with regard to automatic processing of personal data in the context of profiling, de 23.nov.2010. Disponível em: <https://rm.coe.int/16807096c3>. Acesso em: 09 nov. 2018, p.6. Tradução livre: Considerando que os perfis, quando atribuídos a um titular de dados, permitem gerar novos dados pessoais que não aqueles que o titular dos dados informou ao controlador ou que ele ou ela razoavelmente presumem ser conhecidos pelo controlador.

[749] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milão-Itália: Giuffrè, 2016, p.272.

desde que estes sejam dados em atendimento do requisito legal sobre *informações úteis sobre a lógica utilizada* no tratamento tanto para fins do direito à informação do titular (cf. art. 13.2.f e 14.2.g), como para fins do direito de acesso do titular (regra art. 15.1.h).

Desta forma, ele será capaz de entender melhor a correlação entre o tratamento e o resultado da tomada de decisão e usar racionalmente o poder de obter intervenção humana pelo titular do tratamento, expressar sua opinião e contestar a decisão, nos casos em que a decisão foi autorizada oficialmente, por exemplo por um contrato, ou consentida pelo interessado (artigo 22.3). Além disso, não está sujeito à derrogação, nem mesmo em relação à hipótese do artigo 22.2, o direito do interessado de acessar o tratamento e exercer o poder de retificação (artigo 16) de informações incorretas ou de obter a complementação daquelas parciais ou incompletas[750].

Segundo Luca Bolognini, Enrico Pelino e Camilla Bistolfi, sempre que se faz referência não propriamente a um perfil real mas a um *processamento automatizado,* cuja expressão é dotada de um escopo amplo e geral, é preciso considerar (sem redimensionar indevidamente o amplo âmbito conceitual do artigo 22) os casos particulares que apresentam real afinidade com um perfil, ou seja, tratamentos que, embora não gerem modelos e perfis, elaboram um conjunto de informações de acordo com linhas suficientemente coerentes e estruturadas, de modo a permitir que sejam atribuídos de um *significado* e de modo a permitir inferências e avaliações sobre comportamentos ou qualidades pessoais ou morais ou de outros gêneros do interessado[751].

Os autores italianos dão um exemplo de processamento automatizado potencialmente atrelado a esse modelo: é a atividade de indexação realizada pelos provedores de busca em relação às pessoas físicas. A lista das informações retornadas na página de resultados não se refere de fato a um critério neutro, como por exemplo, a ordem alfabética de uma lista telefônica, mas a sofisticados

[750] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milão-Itália: Giuffrè, 2016, p.275.

[751] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milão-Itália: Giuffrè, 2016, p.272. Texto de apoio original: Ocorre premettere che tutte le volte che si fa riferimento non a uma vera e própria profilazione ma a um trattamento automatizzato, espressione di portata assai ampia e generica, bisognerebbe preferibilmente tenere conto (pur senza ridimensionare indebitamente l´ampio âmbito concettuale dell´art. 22) di quei particolari casi che presentino reali affinità con una profilazione, ossia trattamenti che, pur non generando modelli e profili, elaborino um insieme di informazioni secondo linee sufficientemente coerenti e strutturate, tali da permettere l´attribuzione ad esse di um significato e da autorizzare inferenze e valutazioni su comportamenti o qualità personali o morali o di altro genere dell´interessato.

algoritmos proprietários, que realizam escolhas seletivas entre os resultados, estabelecendo ordens de precedência entre eles e associando-os a diferentes informações não diretamente relacionadas ao interessado. Disso pode resultar, ao menos em algumas hipóteses, uma composição arbitrária e totalmente automatizada da imagem social da pessoa, o que potencializa de modo deformante alguns perfis, por vezes acrescentando, em outras omitindo informações. Em um caso concreto, basta pensar na decisão de excluir um candidato a uma posição de trabalho, na qual tal decisão foi feita exclusivamente com base na imagem social obtida por uma pesquisa em um provedor de busca[752].

Desse modo, a eventual decisão de terceiros baseada exclusivamente sobre os resultados de busca parece ser subsumível ao preceito normativo do artigo 22 da GDPR.

Além disso, os motores de busca mais comuns, como Google e Bing, não se limitam a fornecer listas organizadas de resultados, mas aplicam outras atividades *poiéticas*[753], como sugestões de pesquisas "relacionadas", funções de autocompletar campo de busca, capazes de colocar o indivíduo interessado dentro de determinadas categorias sociais, ou ainda, o uso de *snippet*[754], que por serem sínteses automáticas, também se revelam por vezes arbitrárias.

Dentre outros exemplos de decisões baseadas em tratamento automatizado capazes de gerar um impacto social ao indivíduo, voltamos à recusa de um financiamento, analisado e decidido tão somente com base em processamento automatizado, e por meio do qual são revelados a postura do indivíduo em cumprir ou não os pagamentos; a não atribuição de determinado trabalho a um indivíduo, baseado nos resultados de análises exclusivamente automatizadas sobre sua

---

[752] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milão-Itália: Giuffrè, 2016, p. 272.

[753] Expressão emprestada de BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milão-Itália: Giuffrè, 2016, p. 272.

[754] Segundo explicação do Google: "Quando um usuário faz uma pergunta na Pesquisa Google, poderemos apresentar um resultado da pesquisa em um bloco de snippet em destaque especial no topo da página de resultados da pesquisa. Esse bloco em destaque inclui um resumo da resposta, extraído de uma página da Web, além de um link para a página, o título da página e o URL. O resumo é extraído de maneira programática daquilo que um visitante vê na página web. A diferença de um snippet em destaque é que ele é ajustado para chamar a atenção do usuário na página de resultados. Quando reconhecemos que uma consulta faz uma pergunta, detectamos programaticamente páginas que respondem à pergunta do usuário e exibimos um resultado principal como um snippet em destaque nos resultados da pesquisa. Assim como todos os resultados da pesquisa, os snippets em destaque refletem as visões ou opiniões do site do qual os extraímos e não as do Google. Estamos sempre trabalhando para melhorar nossa habilidade de detectar o snippet mais útil. Por isso, os resultados podem mudar ao longo do tempo. É possível oferecer feedback sobre qualquer snippet em destaque clicando no link "Enviar comentários" na parte inferior da caixa. (GOOGLE. **Support**. Disponível em: <https://support.google.com>. Acesso em: 15 nov. 2018).

atitude relacional nos grupos de trabalho e a sujeição do indivíduo interessado ao processo em matéria fiscal com base unicamente numa previsão automatizada do volume de negócios.

Por meio destes exemplos fica clara a relevante exposição da esfera jurídica do indivíduo interessado, o potencial prejuízo às oportunidades de realizações, a dificuldade em defender-se de uma tipologia de tratamento baseada em elaborações abstratas, de árdua senão impossível verificação, potencialmente expostos à falácia, mas ainda assim fortemente determinantes no plano social, também devido à sua aparente objetividade, em virtude do emprego de modelos matemático-estatísticos e ao uso de dados de partida considerados genuínos[755].

A Europa se revela preocupada com esse assunto há tempos. No *explanatory memorandum* à proposta da Diretiva 95/46, escrita em 1992, em seu artigo 16 já se notava o alerta ao perigo do mau uso de decisões geradas por processamento automatizado, reconhecendo, ainda, que a questão se tornaria um problema maior no futuro:

> The danger of the misuse of data processing in decision-making may become a major problem in future: the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities. Article 16 (1) therefore lays down the principle that a person is not obliged to accept a decision of a public administration or of a private party which adversely affects him if it is based solely on automatic processing defining a personality profile[756].

Um dos grandes perigos das decisões tomadas com base em processamento automatizado é o falso sentimento e aparência de que, justamente por não envolver elemento humano na tomada de decisão, esta seria mais objetiva, o que não é verdade.

Adicione-se outro problema à aplicação do artigo 22 do GDPR. Casos como decisões de terceiros sobre concessão de financiamento ou seleção para tipos de

---

[755] BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milão-Itália: Giuffrè, 2016, p.272.

[756] COMMISSION OF THE EUROPEAN COMMUNITIES. COM (92) 422 final. Brussels, 15 October 1992. Tradução livre: O perigo do mau uso do processamento de dados na tomada de decisões pode se tornar um grande problema no futuro: o resultado produzido pela máquina, usando mais e mais softwares sofisticados e até mesmo sistemas especializados, tem um caráter aparentemente objetivo e incontroverso ao qual uma tomada humana de decisão pode atribuir muito peso, abdicando assim de suas próprias responsabilidades. Artigo 16. n.1: portanto, estabelece-se o princípio de que uma pessoa não é obrigada a aceitar uma decisão de uma administração pública ou de uma entidade privada que lhe cause prejuízo se se basear exclusivamente no processamento automatizado que define um determinado perfil de personalidade.

trabalho, são colocados sempre numa área de discricionariedade na qual as margens de controle e reação do interessado são bastante limitadas.

Por fim, entendemos relevante focar em uma das exceções aqui mencionadas para a prática permissa de definição de perfis e decisões automatizadas, qual seja, o consentimento, por entender que esse instituto revela uma dinâmica viva entre o titular de dados e o controlador.

4.7 A (in)eficiência do consentimento

Uma das soluções do legislador europeu para o tratamento de dados nas práticas de *profiling* e decisões automatizadas por algoritmos, é o de permiti-las se houver o consentimento explícito do titular[757]. Este, portanto, consiste em uma exceção à proibição das decisões automatizadas e do *profiling*, ao lado de duas outras exceções: quando as práticas forem necessárias para celebrar ou executar um contrato entre o titular dos dados e um responsável pelo tratamento[758], ou pelo legítimo interesse[759]. Nessa sede, interessa-nos focar, especificamente, no

[757] Artigo 22, GDPR: O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. 2. O n.1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) *For baseada no consentimento explícito do titular dos dados* (g.n.).

[758] Exemplo: Uma empresa publica um anúncio de vaga. Uma vez que o trabalho nessa empresa tem uma grande popularidade, a empresa recebe dezenas de milhares de candidaturas. Em virtude do volume excecionalmente elevado de candidaturas, a empresa poderá considerar que não é viável identificar os candidatos adequados sem recorrer previamente a meios totalmente automatizados para excluir as candidaturas incompatíveis. Neste caso, as decisões automatizadas poderão ser necessárias para elaborar uma lista restrita de potenciais candidatos, com o intuito de celebrar um contrato com um titular de dados. (WP 251, p.26). Exemplo negativo (ou seja, que não se aplica) dado WP251, p.14: Um usuário compra artigos numa loja online. Para dar cumprimento ao contrato, a loja de ecommerce deve tratar as informações do cartão de crédito do usuário para efeitos de pagamento, assim como o endereço do usuário para fins de entrega dos bens. A celebração do contrato não depende da criação de um perfil dos gostos e das opções de estilo de vida do usuário com base nas suas visitas ao site da loja. Mesmo que a definição de perfil seja explicitamente mencionada nas cláusulas em letra pequena do contrato, este fato, por si só, não torna essa definição de perfil *necessária* para a execução do contrato.

[759] Consoante a Comissão Europeia: "Uma empresa (ou organização) tem frequentemente que efetuar o tratamento de dados pessoais para realizar tarefas relacionadas com as suas atividades empresariais. O tratamento de dados pessoais neste contexto pode não se justificar necessariamente por uma obrigação legal ou ser levado a cabo para execução das cláusulas de um contrato com uma pessoa. Nestes casos, o tratamento de dados pessoais pode ser justificado por motivos de *legítimo interesse*. A empresa deve informar os titulares dos dados sobre o tratamento quando da coleta dos seus dados pessoais. A sua empresa deve, além disso, verificar se, ao prosseguir os seus legítimos interesses, não está a prejudicar gravemente os direitos e as liberdades dessas pessoas, caso contrário a empresa não poderá basear-se no legítimo interess para justificar o tratamento dos dados, devendo encontrar outro fundamento jurídico. Exemplo: a empresa tem um legítimo interesse quando o tratamento é efetuado no âmbito da relação com um cliente, quando efetua o tratamento de dados pessoais para efeitos de comercialização direta, para prevenir a fraude ou para garantir a segurança da rede e da informação nos seus sistemas informáticos". (**Comissão Europeia**. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_pt>. Acesso em: 15 jan. 2019).

consentimento. Isso porque, o *profiling* e a utilização de algoritmos podem ser pouco transparentes ao indivíduo. Por vezes, inclusive, baseia-se em dados obtidos ou inferidos a partir de outros dados, e não em dados diretamente fornecidos pelo titular dos dados.

Os responsáveis pelo tratamento de dados que se apoiarem no consentimento como fundamento para as práticas de *profiling* e decisões automatizadas deverão demonstrar que os titulares dos dados compreendem exatamente aquilo para o que estão consentindo, de modo que os titulares dos dados devem receber informação suficiente e pertinente sobre a utilização e as consequências previstas do tratamento, a fim de assegurar que qualquer consentimento por si dado represente uma escolha informada. Porém, essa fórmula dogmática jurídica do consentimento não parece trazer solução às questões postas na sociedade de dados, conforme será abordado a seguir.

Uma pesquisa recente realizada pela Symantec revelou que grande parte dos aplicativos gratuitos disponíveis no Google Play e na Apple Store pode solicitar permissões arriscadas ou acesso excessivo às informações pessoais do usuário, a exemplo da solicitação de rastrear o local. Quase metade dos aplicativos analisados solicita acesso à câmera do dispositivo do usuário. Em outros casos, alguns aplicativos do Android pedem para acessar o conteúdo das mensagens do celular e o registro de chamadas telefônicas[760].

Parece ser prática comum dos aplicativos solicitarem mais dados do que o necessário para interagirem com o usuário[761]. Mas não é esse ponto o que mais chama a atenção; é a falta de importância ou preocupação do titular dos dados diante dessa situação. Na maioria dos casos, o usuário quer passar o mais rápido possível por todas as telas que pedem seu “de acordo” para chegar ao destino, sem se importar *com o que* está consentindo.

A questão se torna ainda mais relevante ao lidarmos com a utilização de algoritmos para processar os dados dos indivíduos. Questiona-se o quanto o

---

Referências do legítimo interesse no GDPR: art. 6; considerandos 47, 48 e 49. Vide, ainda, **WP 217**, 844/14/PT. Parecer n. 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7º da Diretiva 95/46/CE, adotado em 09 abr. 2014.

[760] TI INSIDE ONLINE. **Maioria de apps expõe dados pessoais de usuários**. Disponível em: <http://tiinside.com.br/tiinside/29/08/2018/354288/#.W4grTsOOU0o.linkedin>. Acesso em: 05 set. 2018.

[761] Uma pesquisa sobre quais os dados pessoais coletados de forma anunciada pelas seis maiores empresas da Internet pode ser vista em “The data big tech companies have on you (or, at least, what they admit to). Security Baron. Disponível em: <https://securitybaron.com/blog/the-data-big-tech-companies-have-on-you-or-at-least-what-they-admit-to/>. Acesso em: 23 jan. 2018.

consentimento é apto para assegurar ao titular dos dados o verdadeiro conhecimento do que está sendo coletado e como seus dados serão tratados.

Desde já é possível responder que o pacto do consentimento é insuficiente para garantir ao indíviduo o conhecimento e o controle de seus dados na cultura do algoritmo. Em seguida será analisado o quanto as políticas de privacidade, em regra, consistem numa proposta fracassada. Acquisti et al resumem a ideia que aqui se pretende transmitir: in the current state of the digital economy, consent is ubiquitous, and its consequences are rarely understood[762]. Igualmente P. Blume pondera que “even when consent is founded upon information and furthermore is specific, most data subjects are not able to understand the kinds of processing that take place in the modern complex information society[763]. Nesse aspecto, torna-se relevante aprofundar o olhar e a pesquisa sobre a questão do consentimento na sociedade informacional.

Consentimento vem de *co-sentire*. Existe um envolvimento para conhecer e concordar com as bases as quais se consente. Porém, na toada da vida de hoje, de imediatismo e tempo escasso, parece não haver espaço para querer saber mais sobre as bases as quais se confere a concordância. As pessoas são rápidas, estão com pressa e sem paciência. Nesse contexto, há aqueles que pregam a morte das políticas de privacidade (de *sites* e aplicativos), pois entendem que de nada servem, uma vez que praticamente ninguém as lê.

No relatório da pesquisa efetuada pela *Annenberg School for Communication University of Pennsylvania*, chegou-se à conclusão de que a maioria dos americanos está resignada a desistir de seus dados pessoais. A renúncia ocorre quando uma pessoa acredita que um resultado indesejável é inevitável e se sente impotente para impedi-lo. Nessa toada, segundo o relatório, em vez de se sentir capaz de escolher, os americanos acreditam que é inútil gerenciar o que as empresas podem captar sobre eles. Ainda segundo o estudo, mais da metade dos 1.506 americanos entrevistados (todos acima de 18 anos) não quer perder o controle sobre suas informações, mas ao mesmo tempo acredita que essa perda de controle já aconteceu[764]. É uma condição esquizofrênica.

---

[762] ACQUISTI and others. The Economics of Privacy. 54 **Journal of Economic Literature**, 2016, p.442; 477-478.
[763] BLUME, P. The inherent contradictions in data protection law. **International Data Privacy Law 26**, 2012, p.29.
[764] TUROW, Joseph; HENNESSY, Michael; DRAPER, Nora. **The trade off fallacy**. How marketers are misrepresenting american consumers and opening them up to exploitation. Annenberg School for Communication University of Pennsylvania, jun. 2015. Disponível em: <https://www.asc.upenn.edu>. Acesso em: 02 nov.2018.

A garantia de controle do indivíduo sobre as próprias informações é, de fato, uma característica generalizada das diversas legislações nacionais sobre o tema, conforme é possível perceber a partir das expressões "autodeterminação informativa, consolidada no direito alemão, e liberdade informática, utilizada no direito espanhol, que expressam a importância que a dimensão da autonomia alcançou na temática da proteção de dados pessoais"[765] .

É no consentimento do titular que repousa o fundamento do exercício dessa liberdade de controle de dados do indivíduo, de modo a possibilitar, em tese, determinar o nível de proteção dos dados a ele referentes.

Na lição de Bruno Bioni, a proteção dos dados pessoais tem uma racionalidade regulatória *ex ante*, ao passo que a proteção contratual do consumidor tem, por excelência, um controle *ex post*, mediante a declaração de nulidade de cláusulas contratuais abusivas, ressalvado os casos da atuação no âmbito das esferas dos interesses difusos e coletivos, no qual outros consumidores podem se beneficiar das modificações efetuadas nas bases contratuais[766].

Esse modelo, do consentimento informado, foi útil há duas décadas, mas hoje é uma fantasia. Em um fluxo constante de interações *online*, especialmente nas telas pequenas de celulares, que agora são responsáveis pela maior parte do uso, não é realista, tampouco factível, confiar que as pessoas estejam lendo as políticas de privacidade[767].

Para Katherine Strandburg, o consentimento (assim como as práticas de anonimização) emergiram como panaceas porque apresentaram maneiras de "ter tudo". Para a autora, o consentimento inserido no universo do *big data* pode parecer atrativo como forma de solucionar o uso dos dados, porém, na prática se mostra evasivo:

> Anonymity and infonned consent emerged as panaceas because they presented ways to 'have it all'; they would open the data floodgates while ensuring that no one was unexpectedly swept up or away by the deluge. Now, as then, conscientious industry practitioners, policymakers, advocates, and researchers across the disciplines look to anonymity and infonned consent as counters to the worrisome aspects of emerging applications of big data. We can see why anonymity and consent are attractive: anonymization seems to take data outside the scope of privacy, as it no longer maps onto identifiable subjects, while allowing information subjects to

[765] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014, p.46.
[766] BIONI, Bruno Ricardo. **Proteção de dados pessoais**. A função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p.173.
[767] SABLICH, Elizabeth. Why protecting privacy is a losing game today – and how to change the game. In: **Brooking**. Disponível em: <https://www.brookings.edu>. Acesso em 02 nov. 2018.

> give or withhold consent maps onto the dominant conception of privacy as control over information about oneself. In practice, however, anonymity and consent have proven elusive, as time and again critics have revealed fundamental problems in implementing both[768].

No mesmo caminho opinam Solon Barocas e Helen Nissenbaum sobre a ineficácia do consentimento:

> In the case of consent, too, commonly perceived operational challenges have distracted from the ultimate inefficacy of consent as a matter of individual choice and the absurdity of believing that notice and consent can fully specify the terms of interaction between data collector and data subject[769].

Um estudo experimental, conduzido, em 2016, por dois professores Jonathan Obar, da York University, em Toronto, e Anne Oeldorf-Hirsch, da Universidade de Connecticut confirma o aparente óbvio: quase ninguém lê os termos de uso ou contratos *online* aos quais conferem consentimento. Os professores criaram uma

---

[768] STRANDBURG, Katherine J. Monitoring, datafication, and consent: legal approaches to privacy in the big data context. In: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen. **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.2. Tradução livre: O anonimato e o consentimento infundado emergiram como panaceas porque apresentaram maneiras de "ter tudo"; eles abririam as comportas de dados, ao mesmo tempo em que assegurariam que ninguém fosse inesperadamente levado pelo dilúvio. Agora, como então, os profissionais conscienciosos da indústria, formuladores de políticas, defensores e pesquisadores em todas as disciplinas buscam o anonimato e o consentimento infundado como contrapartida aos aspectos preocupantes das aplicações emergentes do Big Data. Podemos ver porque o anonimato e o consentimento são atraentes: a anonimização parece levar os dados para fora do escopo da privacidade, já que não mapeia mais em assuntos identificáveis, enquanto permite que os sujeitos da informação forneçam ou retenham mapas de consentimento sobre a concepção dominante de privacidade como controle sobre a informação. sobre si mesmo. Na prática, no entanto, o anonimato e o consentimento provaram-se evasivos, pois muitas vezes os críticos revelaram problemas fundamentais na implementação de ambos. O argumento que desenvolvemos neste capítulo vai além. Aqueles comprometidos com o anonimato e o consentimento não negam os desafios práticos; Sua solução é tentar com mais afinco, ser mais criativo, utilizar técnicas matemáticas e estatísticas mais sofisticadas e tornar-se astuto aos contornos cognitivos e motivacionais dos usuários. Embora aceitemos que melhorias possam resultar e resultar desses esforços (por exemplo, políticas de privacidade mais digeríveis, garantias mais robustas de anonimato, arquiteturas de escolha mais utilizáveis e políticas mais flexíveis), a transição para big data transformou linhas de falha de definições e práticas preocuparam políticos, especialistas, profissionais e acadêmicos em abismos intransponíveis. Depois de traçar dificuldades progressivas para o anonimato e o consentimento informado, respectivamente, revelamos desafios praticamente intratáveis para ambos. No caso do anonimato, onde um trabalho importante já demonstrou ser bastante evasivo, argumentamos que, mesmo onde fortes garantias de anonimato podem ser alcançadas, aplicações comuns de Big Data prejudicam os valores que o anonimato tradicionalmente protegia. Mesmo quando os indivíduos não são "identificáveis", eles ainda podem ser "alcançáveis", podem ainda ser representados de forma compreensível em registros que detalham seus atributos e atividades, e podem estar sujeitos a inferências e previsões conseqüentes tomadas com base nisso. No caso do consentimento, também, os desafios operacionais comumente percebidos se desviaram da ineficácia final do consentimento como uma questão de escolha individual e do absurdo de acreditar que a notificação e o consentimento podem especificar completamente os termos de interação entre o coletor de dados e o sujeito dos dados. Ambos, argumentamos, levam à conclusão inevitável de que abordagens processuais não podem substituir políticas baseadas em princípios morais e políticos substantivos que servem a objetivos e valores contextuais específicos.

[769] BAROCAS, Solon; NISSENBAUM, Helen. Big data's end run around anonymity and consent. In: (Coords.) LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (Coord.). **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.2. Tradução livre: No caso do consentimento, também, os desafios operacionais comumente percebidos se desviaram da ineficácia final do consentimento como uma questão de escolha individual e do absurdo de acreditar que a notificação e o consentimento podem especificar completamente os termos de interação entre o coletor de dados e o titular dos dados.

nova rede social, chamada NameDrop e divulgaram a diversos alunos. Centenas de estudantes universitários clicaram no botão “ao clicar em *participar* você concorda em obedecer aos nossos termos de serviço” para se tornarem membros da nova rede social, mas de acordo com o parágrafo 2.3.1 dos termos de serviço, eles concordaram em dar à NameDrop seus futuros filhos primogênitos[770].

O resultado apontou que apenas um quarto do total de 543 alunos se incomodou em ver as letras miúdas, e gastou um tempo maior no texto. A média desse “tempo maior” foi de um minuto, o que não impediu que todos os 543 concordassem com os termos de uso.

O fato de a contraprestação não ser em pecúnia favorece a condição do internauta desprezar uma análise mais detida ao contrato *online.* Ademais, muitos internautas não se preocupam em ler os termos com os quais concordam, haja vista saberem que Google, Facebook, Amazon e outros, não estão em posição de negociar seu próprio acordo separado, de modo que não gastam tempo em um contrato que não pode ser modificado.

Em outra pesquisa recente, realizada no âmbito do projeto CLAUDETTE[771], e que resultou na publicação de um relatório[772] contendo os resultados preliminares do estudo, a problemática do consentimento cultura do algoritmo é colocada em foco. A pesquisa teve por escopo avaliar, sob o ponto de vista legal, com base no GDPR, e usando inteligência artificial e *machine learning*, se as políticas de privacidade disponíveis estão de acordo com o GDPR, cuja norma recentemente entrou em vigor (25-05-2018). Assim, os pesquisadores descreveram os requisitos que uma política de privacidade deve cumprir segundo o GDPR (informações abrangentes, linguagem clara, processamento justo), além de como esses documentos poderiam ser considerados ilegais (se a informação obrigatória for insuficiente, a linguagem não estiver clara, ou se o tratamento for potencialmente injusto). Dessa feita, foram analisados o conteúdo das políticas de privacidade do Google, Facebook (e Instagram), Amazon, Apple, Microsoft, WhatsApp, Twitter, Uber, AirBnB, Booking.com, Skyscanner, Netflix, Jogos Steam e Epic. Os resultados das primeiras

[770] BERREBY, David. Click to agree with what? No one reads terms of service, studies confirm. In: **The Guardian**, 3 mar. 2017. Disponível em: <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>. Acesso em 02 nov. 2018.
[771] Automated CLAUse DETeCTER. Disponível em: <http://claudette.eui.eu>. Acesso em: 24 dez. 2018.
[772] CONTISSA, Giuseppe Contissa; DOCTER, Koen; LAGIOIA, Francesca; LIPPI, Marco; Micklitz, Hans-W; PALKA, Przemyslaw; SARTOR, Giovanni; TORRONI, Paolo. **CLAUDETTE meets GDPR**. Automating the evaluation of privacy policies using artificial intelligence. Study Report, 02 jul. 2018. Disponível em: <https://goo.gl/irpAaz>. Acesso em: 18 nov. 2018.

experiências conduzidas apontam que é possível utilizar as técnicas de aprendizado de máquina, para o mister proposto. Vale, portanto, dedicar tempo e esforço para iniciativas desse tipo, visando formar um instrumento em defesa do titular dos dados e do consumidor. O estudo indicou que nenhuma das informações analisadas referentes às políticas de privacidade constante do material atendeu aos requisitos do GDPR. Foram 3658 sentenças (80.398 palavras), das quais 401 (11,0%), classificadas como linguagem pouco clara e 1240 (33,9%) classificadas como cláusulas potencialmente ilícitas, ou seja, cláusulas de "processamento problemático" ou de "informação insuficiente", segundo as regras dos artigos 13 e 14 do GDPR.

Segundo David Hoffman, professor da Universidade da Pensilvânia, que pesquisa a lei e a psicologia dos contratos, essa condição e situação, contudo, não são novas. Elas existem desde os contratos de adesão impressos. Além disso, segundo ele, existe uma preocupação real de que as regras de proteção de dados estejam sendo engolidas por cláusulas de concordância *online*[773]. Estima-se que a leitura de contratos digitais tomaria quase 250 horas por ano de um americano[774].

O tudo ou nada está na toada do “take it or leave it” approach[775]. Em relação ao consentimento, fala-se, ainda, em *granularidade* das autorizações do usuário, ou seja, permite que sejam dadas autorizações de forma fragmentada. A inteligência dessa forma supera a problemática do ‘tudo’ ou ‘nada’. Consoante Parecer de 2013 do Article 29 Data Protection Working Party:

> In some cases users are able to give a granular consent, where consent is sought for each type of data the app intends to access. Such an approach achieves two important legal requirements, firstly of adequately informing the user about important elements of the service and secondly asking for specific consent for each[776].

---

[773] HOFFMAN, David A.; WILKINSON-RYAN, Tess.The psychology of contract precautions. **University of Chicago Law Review**, v.80, p.395, 2013.

[774] HOFFMAN, David A.; WILKINSON-RYAN, Tess.The psychology of contract precautions. **University of Chicago Law Review**, v.80, p.395, 2013.

[775] Horas após o GDPR entrar em vigor, o advogado austríaco ingressou com uma medida para contestar as políticas do Facebook. Nesse sentido: Within hours of the General Data Protection Regulation (GDPR) going into effect today, a privacy group accused Facebook (FB), Alphabet (GOOGL)'s Google, WhatsApp, and Instagram of violating Europe's strict new data-protection law.Austrian lawyer Max Schrems, a frequent critic of Facebook's privacy policies, on Friday filed complaints that claim the companies forced members to consent to terms of service with a "take it or leave it" threat. (SWARTZ, Jon. It’s day one of GDPR, and facebook, google are accused of breaking new rules, 25 maio 2018. Disponível em: <https://www.barrons.com/articles/its-day-one-of-gdpr-and-facebook-google-are-accused-of-breaking-new-rules-1527284532>. Acesso em: 24 dez. 2018).

[776] ARTICLE 29 Data protection working party. Opinion 02/2013 on apps on smart devices. Adotado em 27 fev. 2013. Disponível em: <https://www.pdpjournals.com/docs/88097.pdf>. Acesso em: 10 set. 2018. Tradução livre:
Em alguns casos, os usuários podem dar um consentimento granular, onde o consentimento é solicitado para cada tipo de dados que o aplicativo pretende acessar. Tal abordagem alcança dois requisitos legais importantes,

Trabalho mais recente do Article 29 sobre o assunto dispõe:

> A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR. […] If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom[777].

Recentemente, a Comissão Federal de Comércio americana (FTC) se posicionou sobre o consentimento nas atividades *on line* para segmentação de publicidade*,* em um relatório[778] enviado à *National Telecommunications and Information Administration* (Agência do Departamento de Comércio dos Estados Unidos que exerce o papel de consultora da Presidência sobre políticas de telecomunicações). Ao passo que, ao longo de todo relatório reconhece a importância da privacidade de dados, a tônica está na inovação baseada em dados:

> The FTC supports a balanced approach to privacy that weighs the risks of data misuse with the benefits of data to innovation and competition. Striking this balance correctly is essential to protecting consumers and promoting competition and innovation […] The digital economy has benefitted consumers in many ways, saving individuals' time and money, creating new opportunities, and conferring broad social and environmental benefits. Privacy standards that give short shrift to the benefits of data-driven practices may negatively affect innovation and competition. Moreover,

---

em primeiro lugar, de informar adequadamente o usuário sobre elementos importantes do serviço e, em segundo lugar, pedir o consentimento específico para cada um deles.

[777] ARTICLE 29 Data protection working party. Guidelines on consent under Regulation 2016/679. Adotado em 28 nov. 2017. Revisado em: 10 abr. 2018, p.10. Tradução livre: Um serviço pode envolver várias operações de processamento para mais de uma finalidade. Nesses casos, os titulares dos dados devem ter a liberdade de escolher qual o objetivo que aceitam, em vez de terem de concordar com um conjunto de finalidades de processamento. Em um determinado caso, vários consentimentos podem ser necessários para começar a oferecer um serviço, de acordo com o GDPR. [...] Se o controlador tiver combinado várias finalidades para o processamento e não tiver tentado obter um consentimento separado para cada finalidade, há falta de Liberdade. Exemplo dado no citado Parecer: Within the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group. This consent is not granular as there is no separate consents for these two separate purposes, therefore the consent will not be valid. In this case, a specific consent should be collected to send the contact details to commercial partners. Such specific consent will be deemed valid for each partner (whose identity has been provided to the data subject at the time of the collection of his or her consent, insofar as it is sent to them for the same purpose (in this example: a marketing purpose). Tradução livre: Dentro do mesmo pedido de consentimento, um varejista solicita a seus clientes o consentimento para usar seus dados para enviar marketing por e-mail e também para compartilhar seus dados com outras empresas de seu grupo. Esse consentimento não é granular, pois não há consentimentos separados para esses dois propósitos separados, portanto, o consentimento não será válido. Nesse caso, um consentimento específico deve ser coletado para enviar os detalhes de contato aos parceiros comerciais. Esse consentimento específico será considerado válido para cada parceiro (cuja identidade foi fornecida ao titular dos dados no momento da coleta de seu consentimento, na medida em que ele é enviado a eles para o mesmo propósito (neste exemplo: finalidade).

[778] FTC. **Developing the Administration's Approach to Consumer Privacy**, 09 nov. 2018. Disponível em: <https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf>. Acesso em: 20 nov. 2018.

> regulation can unreasonably impede market entry or expansion by existing companies; the benefits of privacy regulation should be weighed against these potential costs to competition. Transparency is another longstanding privacy tenet championed by the FTC. The challenge is how and when to be transparent—how and when to provide important information about data collection and use in a way that it is accessible and meaningful to consumers. The FTC has long encouraged a balanced approach to control. Giving consumers the ability to exercise meaningful control over the collection and use of data about them is beneficial in some cases. However, certain controls can be costly to implement and may have unintended consequences. For example, if consumers were opted out of online advertisements by default (with the choice of opting in), the likely result would include the loss of advertising-funded online content[779].

Para Katherine Strandburg, ao comentar o papel do FTC em relação ao consentimento:

> Another way to improve the functioning of notice and consent in the big data context would be to impose substantive requirements of clear and understandable notice, at least on larger entities. The FTC might be able to take this step immediately on the basis of its Section 5 authority by deeming a notice and consent process "unfair and deceptive" if it cannot be demonstrated that it is understandable by a reasonable consumer. Techniques such as consumer surveys and experiments, similar to those employed in trademark law, could be used to demonstrate understandability. While a substantive evaluation of this sort might be unreasonably expensive for smaller companies, the necessary testing would be well within the means of the larger companies that collect the bulk of personal information [780].

---

[779] FTC. **Developing the Administration's Approach to Consumer Privacy**, 09.11.2018. Disponível em: <https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf>. Acesso em: 20 nov. 2018. Tradução livre: O FTC apoia uma abordagem equilibrada à privacidade que pondere os riscos do uso indevido de dados frente aos benefícios dos dados para a inovação e a concorrência. Atingir corretamente este equilíbrio é essencial para proteger os consumidores e promover a concorrência e a inovação [...] A economia digital beneficiou os consumidores de várias maneiras, economizando tempo e dinheiro de indivíduos, criando novas oportunidades e conferindo amplos benefícios sociais e ambientais. Os padrões de privacidade que dão pouca atenção aos benefícios das práticas baseadas em dados podem afetar negativamente a inovação e a concorrência. Além disso, a regulamentação pode impedir a entrada ou a expansão do mercado pelas empresas existentes; os benefícios da regulamentação da privacidade devem ser ponderados em relação a esses custos potenciais para a concorrência. A transparência é outro princípio de privacidade de longa data defendido pela FTC. O desafio é como e quando ser transparente – como e quando fornecer informações importantes sobre a coleta de dados e usá-las de maneira acessível e significativa para os consumidores. O FTC há muito incentiva uma abordagem equilibrada de controle. Dar aos consumidores a capacidade de exercer controle significativo sobre a coleta e uso de dados sobre eles é benéfico em alguns casos. No entanto, certos controles podem ser caros de implementar e podem ter consequências indesejadas. Por exemplo, se os consumidores optassem por excluir anúncios on-line por padrão (com a opção de optar), o resultado provável incluiria a perda de conteúdo on-line financiado por publicidade.

[780] STRANDBURG, Katherine J. Monitoring, datafication, and consent: legal approaches to privacy in the big data context. In: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen. **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.29. Tradução livre: Outra maneira de melhorar o funcionamento da notificação e do consentimento no contexto do big data seria impor requisitos substantivos de notificação clara e compreensível, pelo menos em entidades maiores. A FTC poderá dar esse passo imediatamente com base em sua autoridade da Seção 5, ao considerar um processo de notificação e consentimento "injusto e enganoso" se não for possível demonstrar que é compreensível por um consumidor razoável. Técnicas como pesquisas com consumidores, semelhantes àquelas empregadas na lei de marcas registradas, poderiam ser usadas para demonstrar a compreensibilidade. Embora uma avaliação substancial desse tipo possa ser excessivamente cara para as empresas menores, os testes necessários estariam bem dentro dos meios das grandes empresas que coletam a maior parte das informações pessoais.

Voltando aos estudos e pesquisas realizados, estima-se que 98% dos usuarios não leem as políticas de privacidade. Segundo um estudo[781] de 2012, quando sequer existiam tantos sites e aplicativos como hoje, uma política de privacidade tem, em media, 2.518 palavras, com tempo médio de leitura de 10 minutos. Uma pessoa se depara, por ano, com aproximadamete 1.500 políticas de privacidade, o que equivale a quase 76 dias de leitura para tomar conhecimento de todos esses documentos[782].

Ainda, um recente estudo de campo destacou que 101 participantes, apesar das informações claras de que as respostas seriam compartilhadas com terceiros, responderam a perguntas sobre o passado de suas vidas sexuais. Se o consentimento é dado mesmo sob circunstâncias altamente íntimas, é possível presumir que as empresas que solicitam permissão para processar dados pessoais para ofertas personalizadas obterão o consentimento[783].

No mesmo rumo é a observação de Ben Shaar: "a number of studies suggest that privacy notices are almost never read, and consent is almost always given[784].Por sua vez, Bert-Jaap Koopes, sob o ponto de vista dos advogados, indica que "data protection lawyers are sceptical that the consent requirement adequately protects data subjects"[785].

Com o dever de revisão nas regras de proteção de dados, por conta do Regulamento europeu GDPR, em vigor desde 25 de maio de 2018, diversas pessoas foram inundadas com uma enxurrada de emails sobre as novas políticas de privacidade. Mas, pergunta-se: quanto desses avisos realmente foram apreendidos pelos titulares de dados que receberam tais notificações? A repórter do Wall Street

---

[781] THE ATLANTIC. Technology. **Reading the privacy policies you encounter in a year would take 76 work days**. Alexis C. Madrigal. Mar.1, 2012. Disponível em: <https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/>. Acesso em: 24 dez. 2018.

[782] Reflexão pertinente: Oltre al costo di produttività nazionale ipotizzato da questo studio, ci sarebbe da considerare anche il costo individuale. E qui ci si scontrerebbe con un paradosso. In una società equa, gli utenti – sebbene in termini di centesimi cada sito – dovrebbero essere pagati per dare i propri dati personali in pasto ad un sito che da questi trarrà profitto (ad esempio, quelle rivendendo i dati agli inserzionisti pubblicitari per finalità di profilazione). Ed invece, il "sistema" pretende che siano gli utenti a dover pagare, spendendo 76 giorni/anno (tempo potenzialmente sottratto a un lavoro retribuito) a sacrificare diottrie su verbosissime Privacy Policy. (PRIVACY IT. **L' Intelligenza Artificiale che legge le Privacy Policy al posto**. Disponível em: <https://www.privacy.it/2018/02/22/intelligenza-artificiale-lettura-privacy-policy/>. Acesso em: 24 dez. 2018).

[783] HACKER, Philipp. Personal data, exploitative contracts, and algorithmic fairness: autonomous vehicles meet the internet of things. **International Data Privacy Law**, v.7, ed.4, nov. 2017, p.266-286. Disponível em: <https://doi.org/10.1093/idpl/ipx014>. Acesso em: 16 out. 2018, p.271.

[784] SHAAR, O Ben; Chilton, A. Simplification of privacy disclosures: an experimental test' (2016) 45 Journal of Legal Studies S41; Y Bakos and others, 'Does anyone read the fine print? Consumer Attention to Standard-Form Contracts'. **43 Journal of Legal Studies**, 2014.

[785] KOOPES, Bert-Jaap. The trouble with european data protection law. **International Data Privacy Law**, 2014, p.250, 251-252.

Journal, Joanna Stern, tentou analisar todos os emails recebidos por conta do novo regramento europeu[786]. Após imprimir os documentos, disse ser possível esticar os papeis por mais do que o comprimento de um campo de futebol. Para além dessa curiosidade, verifica-se que as mais modernas soluções voltadas para aumentar a transparência e a escolha do consumidor, na verdade, consistem em respostas incompletas aos atuais desafios de privacidade e proteção de dados.

Daí surgem preocupações cada vez mais relacionadas aos 'problemas de *design* de interface'. Em outras palavras, pode contribuir para o problema de não leitura, determinadas adequações de *design* de interface com o usuário titular dos dados. Nesse sentido as melhores práticas nesse setor apontam no seguinte sentido:

> In order to make privacy notices effective and usable, they should not be tacked on after the system has been completed but instead be integrated into a system's design. Privacy notices and choice options can then be designed for specific audiences and their notice requirements, and take into account a system's opportunities and constraints. […] The design space should be leveraged as part of a comprehensive design process that focuses on audience-specific privacy notice requirements and considers a system's opportunities and constraints, in order to develop a notice and choice concept that is well integrated with the respective system, rather than bolted on. Notices should be evaluated in user studies[787].

Deve-se impor um parâmetro mínimo que contribua à maior percepção das informações do indivíduo e maior controle de seus dados. Nesse sentido, em termos gerais, o espaço conferido ao *design* vinculado a avisos que digam respeito a dados pessoais deve atender às seguintes dimensões: tempo de aviso (quando é fornecido); canal (como é entregue); modalidade (quais modelos de interação são usados) e controle (como as opções são fornecidas). Estas dimensões podem ser consideradas em paralelo, em detrimento do modo sequencial[788] .

Um exemplo disso está no ato do Facebook providenciar um pop-up para postar uma foto, indicar a informação em formato de pergunta: "quem pode ver isso?", e sinalizar facilmente ao usuário as opções possíveis. Certamente se essas informações estivessem ao longo de uma extensa política de privacidade, que fora

---

[786] NATIONAL PUBLIC RADIO. **How europe's new data privacy law is supposed to give users more control**. Disponível em: <https://www.npr.org/2018/05/28/615010156/how-europes-new-data-privacy-law-is-supposed-to-give-users-more-control>. Acesso em 12. nov. 2018.

[787] SCHAUB, Florian; BALEBAKO, Rebecca; DURITY, Adam L.; CRANOR, Lorrie Faith. A design space for effective privacy notices. **Symposium on Usable Privacy and Security** (SOUPS), 22 a 24 de de 2015, Ottawa, Canada. Disponível em: <https://www.usenix.org>. Acesso em: 12 nov. 2018.

[788] SCHAUB, Florian; BALEBAKO, Rebecca; DURITY, Adam L.; CRANOR, Lorrie Faith. A design space for effective privacy notices. **Symposium on Usable Privacy and Security** (SOUPS), 22 a 24 de de 2015, Ottawa, Canada. Disponível em: <https://www.usenix.org>. Acesso em: 12 nov. 2018, p.6.

lida, em tese, ao aderir à rede social, o titular não seria capaz – na remota hipótese de ter lido a política – de lembrar as condições contratadas.

Várias pesquisas já foram desenvolvidas e outras continuam em andamento visando estudar como melhorar a efetividade de termos e de políticas de privacidade. Porém, constata-se que há pouca orientação, ainda, para *designers* e desenvolvedores sobre aspectos de *design* que podem afetar ou contribuir com a eficácia de avisos de privacidade. Segundo Elizabeth Sablich, "some forms of notice are necessary and attention to user experience can help, but the problem will persist no matter how well designed disclosures are"[789] .

No contexto da inteligência coletiva emanada da própria rede, constata-se iniciativas que trazem solução alternativa ao mister exaustivo. A exemplo do *site* ´Terms of Service; Didn´t Read´[790], entidades se propõe a analisar termos de uso e políticas de privacidade espalhados pela web, e a classificá-los entre muito bom e muito ruim, em prol de ajudar, prontamente, internautas que não costumam ler o teor dos instrumentos. A questão que se deriva é quanto essas entidades terceiras possuem seriedade e confiança.

Para maior efetividade das cláusulas que tratam da proteção de dados, é essencial trabalhar na questão do *design* de interface. Capacitar usuários com controles de privacidade aumenta sua confiança e pode resultar em uso mais confortável e maior divulgação dos serviços.

Novas tecnologias e dispositivos integrados, como wearables e internet das coisas, colocam em perspectiva desafios para a utilização de diferentes meios de *design* para avisos e controles de privacidade. No mundo atual, a coleta de informações é contínua. Portanto, políticas públicas, leis e abordagens tecnológicas precisam ser aplicadas em conjunto a fim de permitir que os usuários gerenciem melhor seus dados pessoais[791] .

---

[789] SABLICH, Elizabeth. Why protecting privacy is a losing game today – and how to change the game. In: **Brooking**. Disponível em: <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>. Acesso em: 02 nov. 2018.

[790] Disponível em: <https://tosdr.org/>. Segundo o site: "We are a user rights initiative to rate and label website terms & privacy policies, from very good Class A to very bad Class E. Terms of service are often too long to read, but it's important to understand what's in them. Your rights online depend on them. We hope that our ratings can help you get informed about your rights. Do not hesitate to click on a service below, to have more details! You can also get the ratings directly in your browser by installing our web browser".

[791] SCHAUB, Florian; BALEBAKO, Rebecca; DURITY, Adam L.; CRANOR, Lorrie Faith. A design space for effective privacy notices. **Symposium on Usable Privacy and Security** (SOUPS), 22 a 24 de de 2015, Ottawa, Canada. Disponível em: <https://www.usenix.org>. Acesso em: 12 nov. 2018, p.12.

Em termos de redação de lei, na LGDP o legislador optou por exigir consentimento inequívoco (mais pragmático), enquanto o Marco Civil da Internet exige consentimento expresso (mais formal). A LGPD, portanto, privilegiou a certeza e não a formalidade. De todo modo, impõe-se uma formalidade ao consentimento, sem aceitá-lo tacitamente. É sabido que a regra geral preceitua a não imposição de forma para a validade do contrato. Portanto, o direito, desde o fim do império romano[792], incorporou o princípio do *solus consensus obligat.* Assim, embora do formalismo previsto no direito antigo[793] não tenha restado praticamente mais nada, o formalismo atual deve ser visto como uma tentativa de garantia aos direitos fundamentais da pessoa.

No âmbito da proteção de dados nota-se que a lei, em sua vontade soberana, considera ser fundamental existir uma sincronia de entendimento por parte do titular dos dados frente ao comunicado (contrato) de coleta e tratamento de suas informações. Trata-se, em verdade, de inteligência jurídica antiga, formulada pelos romanos[794]. Ocorre que, conforme se vê, a ferramenta do consentimento, por si só, parece ser ineficaz para a realidade atual.

---

[792] Pela regra instituída pela constituição do Imperador Leon, do ano de 472 d.C, o requisito de validade do uso de palavras solenes na realização da *stipulatio* deixou expressamente de ser exigido. As palavras desta constituição abriram espaço para muita interpretação. De início, se tende a considerar que este imperador dispensou a velha formalidade oral romana, consistente naquele ritual envolvendo uma pergunta e uma resposta, cujo procedimento naquela época deveria ser considerado já deveras antiquado. (ZIMMERMANN, Reinhard. **The law of obligations**. Oxford, New York, 1996, p.80). Os compiladores comentaram essa regra em sede das Instituições (I.3.15.1.1.) no sentido de que a constituição de Leon suprimira a solenidade das palavras. Porém, contra tal entendimento, defende-se que Leon não aboliu a *sollemnitas verborum*, como diz o texto, mas admitiu que a *stipulatio* pudesse ser aperfeiçoada *quibuscumque verbis*, considerada por *consensus* (BIONDI, Biondo. **Contratto e stipulatio**. Milano, 1953, p.289).

[793] No direito romano, mormente no período mais antigo, a forma dos negócios jurídicos, diferentemente dos tempos atuais, era da própria substância do ato. Se a forma, solenidade e gestos prescritos não fossem cumpridos, o contrato não seria aperfeiçoado, ainda que a vontade das partes fosse clara nos efeitos desejados. Em verdade, nas origens do direito romano existia uma rígida tipicidade negocial, e que se conservou, ainda, com certa atenuação por toda a idade clássica e parece superada apenas em idade pós-clássica. A distinção entre contratos formais e não formais foi proposta pela romanística mais recente; o *ius civile* não conhecia senão contratos formais, cuja solenidade não apenas revestia as vontades das partes, senão que tinha por si mesma plena eficácia. A forma consistia no elemento mais importante e por um defeito não seria produzido nenhum resultado jurídico. (OURLIAC, Paul; DE MALAFOSSE, Jehan. **Derecho romano y francês histórico**. Tradução ao espanhol e anotações de Manuel Fairén, t.I, 1960, p. 80).

[794] A exigência de congruência entre pergunta e resposta também pode ser identificada como preocupação concernente à substância, eis que a congruência necessária não está simplesmente no aspecto formal das palavras utilizadas, mas na preocupação de estabelecer o sentido da declaração do promissor em relação ao sentido do pedido do *stipulator*. Eis Gaio (Gai. 3.102) considerar que uma *stipulatio* é inválida se não se tivesse respondido à pergunta, como no caso de um estipular o montante de dez e o outro prometer cinco (O problema então tornar-se-ia de caráter interpretativo (CANNATA, Carlo Augusto. **Corso di Istituzioni di Diritto Romano**, II, 1, Torino, 2003, p.91-92). De tudo isto, resulta que a *stipulatio*, como contrato formal, possui tanto uma forma simples e livre, como uma forma rigorosa. Se a *stipulatio* é o modo para realizar *verbis* uma *obligatio*, e isto significa que a obrigação se aperfeiçoa pelos efeitos das palavras pronunciadas, é, portanto, o fato da pronúncia das palavras a produzir as obrigações: essa nasce, precisamente, quando o promissor efetuou sua resposta afirmativa à pergunta do *stipulator*.

O considerando 42 do GDPR dispõe que para o consentimento ser considerado informado “o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina”.

Pelo Parecer do Article 29 Working Party[795], para o consentimento ser ‘informado’, é necessário prover ao usuário determinados elementos cruciais para sua escolha, contendo um mínimo de informações[796] a serem obtidas para o consentimento ser válido. Dente elas, está a obrigação de revelar se os dados serão utilizados para tomada de decisão automatizada.

Sob outro enfoque, um dos problemas do antiquado modelo de notificação prévia e escolha individual é que esse formato desloca o ônus da proteção da privacidade e da proteção de dados sobre o indivíduo titular destes dados, resultando em uma barganha desigual.

A dinâmica dos contratos de adesão aponta para a assimetria de forças das relações de consumo, porquanto uma das partes é quem dita unilateralmente o teor do que será contratado. Segundo Bruno Ricardo Bioni, “isso significa, em termos de proteção de dados pessoais, que será o fornecedor quem determinará os rumos do

[795] ARTICLE 29 Data protection working party. Guidelines on consent under Regulation 2016/679. Adotado em 28.nov.2017. Revisado em 10.04.2018, p. 13. Tradução livre: .With regard to item (i) and (iii), WP29 notes that in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named. Processors do not need to be named as part of the consent requirements, although to comply with Articles 13 and 14 of the GDPR, controllers will need to provide a full list of recipients or categories of recipients including processors. To conclude, WP29 notes that depending on the circumstances and context of a case, more information may be needed to allow the data subject to genuinely understand the processing operations at hand. Tradução livre: No que diz respeito ao item (i) e (iii), o WP29 observa que, em um caso em que o consentimento solicitado deve ser invocado por vários controladores (conjuntos) ou se os dados devem ser transferidos ou processados por outros controladores que desejam confiar no consentimento original, todas essas organizações devem ser nomeadas. Os processadores não precisam ser nomeados como parte dos requisitos de consentimento, embora para cumprir os Artigos 13 e 14 do GDPR, os controladores precisarão fornecer uma lista completa de destinatários ou categorias de destinatários, incluindo processadores. Para concluir, o WP29 observa que, dependendo das circunstâncias e do contexto de um caso, podem ser necessárias mais informações para permitir que os titulares de dados compreendam verdadeiramente as operações de processamento disponíveis.

[796] (i) the controller’s identity, (ii) the purpose of each of the processing operations for which consent is sought, (iii) what (type of) data will be collected and used, (iv) the existence of the right to withdraw consent, (v) information about the use of the data for automated decision-making in accordance with Article 22.2.c where relevant, and (vi) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46. Tradução livre: (i) a identidade do controlador, (ii) os motivos de cada operação de processamento para o qual o consentimento é perquerido, (iii) qual o tipo de dado será coletado e usado (iv) a existencia do direito de retirar o consentimento; (v) informação sobre o uso de dados para tomada de decisão automatizada, de acordo com o artigo 22.2.c, (vi) sobre a possibilidade de riscos de transferencia de dados devido à falta de garantias adequadas e apropriadas conforme descrito no artigo 46. Cf. ARTICLE 29 Data protection working party. Guidelines on consent under Regulation 2016/679. Adotado em 28 nov. 2017. Revisado em 10 abr. 2018, p.13.

fluxo informacional dos seus usuários, eliminando, praticamente, qualquer faixa de controle a ser por eles operada"[797].

Nesse contexto, os usuários não têm possibilidade de discutir sobre suas preferências de privacidade. Na reflexão de Bruno Bioni:

> Isso somado à proeminência de uma série de plataformas que condicionam a própria participação social do cidadão, acaba por tornar falaciosa a prometida esfera de controle de dados pessoais. É nesse contexto que a lógica do 'tudo' ou 'nada' das políticas de privacidade acaba por mistificar a autodeterminação informacional. As políticas de privacidade, ora escoradas nessa dinâmica dos contratos de adesão, tem sido uma ferramenta inapropriada para garantir ao consumidor o controle dos seus dados pessoais.[798]

Além disso, a via de anonimizar dados pode ser igualmente ineficiente, pois mesmo quando os indivíduos não são "identificáveis", eles ainda podem ser "alcançáveis", podendo ainda ser representados de forma compreensível em registros que detalham seus atributos e atividades, e podem estar sujeitos a inferências e previsões. Nesse sentido é a lição de Solon Barocas e Helen Nissenbaum:

> Those committed to anonymity and consent do not deny the practical challenges; their solution is to try harder, to be more creative, to utilize more sophisticated mathematical and statistical techniques, and to become astute to the cognitive and motivational contours of users. Although we accept that improvements can result and have resulted from these efforts (e.g. more digestible privacy policies, more robust guarantees of anonymity, more usable choice architectures, and more supple policy), the transition to big data has turned definitional and practical fault lines that have worried policymakers, pundits, practitioners, and scholars into impassable chasms. […] In the case of anonymity, where important work has already shown it to be rather elusive, we argue that, even where strong guarantees of anonymity can be achieved, common applications of big data undermine the values that anonymity traditionally had protected. Even when individuals are not ' identifiable', they may still be 'reachable', may still be comprehensibly represented in records that detail their attributes and activities, and may be subject to consequential inferences and predictions taken on that basis[799].

---

[797] BIONI, Bruno Ricardo. **Proteção de dados pessoais**. A função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p.171.

[798] BIONI, Bruno Ricardo. **Proteção de dados pessoais**. A função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p.172.

[799] BAROCAS, Solon; NISSENBAUM, Helen. Big data's end run around anonymity and consent. In: (Coords.) LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (Coord.). **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014, p.2. Tradução livre: Aqueles comprometidos com o anonimato e o consentimento não negam os desafios práticos; sua solução é tentar com mais afinco, ser mais criativo, utilizar técnicas matemáticas e estatísticas mais sofisticadas e tornar-se astuto aos contornos cognitivos e motivacionais dos usuários. Embora aceitemos que melhorias possam resultar desses esforços (por exemplo, políticas de privacidade mais digeríveis, garantias mais robustas de anonimato, arquiteturas de escolha mais utilizáveis e políticas mais flexíveis), a transição para big data transformou linhas de falha de definições e práticas preocuparam políticos, especialistas, profissionais e acadêmicos em abismos intransponíveis. [...] No caso do anonimato, onde um trabalho importante já demonstrou ser bastante evasivo, argumentamos que, mesmo onde fortes garantias de anonimato podem ser alcançadas, aplicações comuns de

Omer Tene e Jules Polonetsky analisaram as tradicionais respostas legais, como consentimento e minimização de dados, rejeitando estas formas. Em seu lugar, eles propõem o que denominam de estratégia *sharing the wealth,* isto é, 'compartilhando a riqueza', vale dizer, em vista dos sérios desafios de privacidade levantados no *big data* e na cultura do algoritmo. Também diante das dificuldades de regulação, as organizações devem estar preparadas para compartilhar com os indivíduos a riqueza que seus dados ajudam a criar. A premissa dessa estratégia é que as organizações, controladoras de dados, devem fornecer aos indivíduos acesso prático e fácil a seus dados em um formato pronto para o uso, para que possam se tornar participantes ativos na economia de dados. Além disso, as organizações devem ser obrigadas a ser transparentes sobre os critérios de decisão subjacentes às suas atividades de processamento de dados[800].

Diante da apresentada impotência, é necessário adicionar outros meios, para além das formas tradicionais. Não se pode mais pensar com o viés tradicional em uma sociedade disruptiva. É o que será analisado no próximo item. O direito, por si só, é limitado para dar amparo às necessidades atuais, de maneira que é necessário recorrer à própria tecnologia.

4.8 A contribuição da tecnologia na regulação de proteção de dados

Há caminhos que buscam equalizar melhor a proteção de dados pessoais, cujo socorro não é delegado à lei propriamente dita, mas sim à própria tecnologia, conhecidas como Privacy Enhancing Technologies (PETs), tal qual o conceito do *privacy by design*, expressão cunhada na década 1990, por Ann Cavoukian, ex-comissária de Informação e Privacidade da Província de Ontário-Canadá.

Para além de se fidar tão somente em soluções trazidas unicamente pelo direito, verifica-se a necessidade de delegar à própria tecnologia padrões que elevem a proteção de dados do indivíduo. Segundo Bioni, as PETs são uma possível

---

Big Data prejudicam os valores que o anonimato tradicionalmente protegia. Mesmo quando os indivíduos não são "identificáveis", eles ainda podem ser "alcançáveis", podem ainda ser representados de forma compreensível em registros que detalham seus atributos e atividades, e podem estar sujeitos a inferências e previsões conseqüentes tomadas com base nisso. No caso do consentimento, também, os desafios operacionais comumente percebidos se desviaram da ineficácia final do consentimento como uma questão de escolha individual e do absurdo de acreditar que a notificação e o consentimento podem especificar completamente os termos de interação entre o coletor de dados e o sujeito dos dados. Ambos, argumentamos, levam à conclusão inevitável de que abordagens processuais não podem substituir políticas baseadas em princípios morais e políticos substantivos que servem a objetivos e valores contextuais específicos.

[800] TENE, Omer; POLONETSKY, Jules. Big data for all: privacy and user control in the age of analytics. **Northwestern Journal of Technology and Intellectual Property**, v. 239, ano 2013, p.1-36, p.8.

solução para equalizar as mencionadas assimetrias do mercado informacional, de maneira que podem desempenhar um papel multifacetado e emancipador para empoderar o cidadão no controle de dados[801] .

Em outras palavras, conceitos do direito à privacidade e proteção de dados pessoais são incorporados, desde à concepção da arquitetura dos sistemas (*by design*), e por padrões de configuração, de modo a garantir condições para que o usuário tenha possibilidade de controlar sua privacidade, a coleta e o tratamento de seus dados pessoais. Como exemplos, podem ser citados o uso da criptografia que assegura a confidencialidade nas comunicações, a anonimização dos dados pessoais e o uso de plataformas como a Plataform for Privacy Preferences (P3P)[802] .

O conceito privacy *by design* pode ser definido como uma metodologia

> for proactively embedding privacy into information technology, business practices, and networked infrastructures. The Privacy by Design measures are designed to anticipate and prevent privacy invasive events before they occur[803].

O conceito *privacy by design* enfatiza que as questões de privacidade devem ser consideradas desde o início, por isso também é conhecida por 'privacidade desde a concepção'. Segundo Michael Veale, Reuben Binns e Jef Ausloos, as questões, na verdade, devem ser observadas durante todo o processo de design, "through creative social and technical means"[804].

Por esse conceito, a proteção à privacidade e dados pessoais é apoiada em um tripé: (i) sistemas de tecnologia informação (IT systems); (ii) práticas negociais responsáveis (accountable business practices); e (iii) design físico e infraestrutura de rede (physical and networked infrastructure).

Decorre do conceito de *privacy by design*, o conceito de *privacy by default*, que se refere à metodologia que adota por padrão a configuração de privacidade mais segura possível para qualquer forma de tratamento de dados pessoais, a fim

---

[801] BIONI, Bruno Ricardo. **Proteção de dados pessoais**. A função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p.177.
[802] Plataforma de navegação pela qual o usuário pode determinar, por intermédio de configuração, quais tipos de dados poderiam lhe ser coletados.
[803] INFORMATION and information and privacy comissioner of Ontario. Privacy by design. Jan. 2018. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd-1.pdf>. Acesso em: 24 dez. 2018.
[804] VEALE, Michael; BINNS, Reuben; AUSLOOS, Jef. When data protection by design and data subject rights clash, **International Data Privacy Law**, v.8, 2.ed. 1 maio 2018, p.105-123, p.105.

de garantir sua proteção de modo automático. Em outras palavras, é a configuração por padrão dos sistemas da forma mais protetiva possível[805].

Os conceitos de *privacy by design* e *privacy by default* podem, ainda, ser ampliados, pois a necessidade de observância da privacidade vai além da concepção dos sistemas e de suas configurações, devendo atingir o próprio cerne do negócio, na forma como será estruturado o seu modelo. Daí também se falar em *privacy by business model*. Por esse último, o modelo de negócio deve observar, desde sua concepção e elaboração de seu plano inicial, a convergência à proteção de dados pessoais, baseados no empoderamento do consumidor. Segundo Rubinstein, os modelos de negócios até hoje existentes provaram repetidas vezes que a regulamentação da privacidade não é páreo para eles. As empresas inevitavelmente coletam e usam cada vez mais dados pessoais; embora os consumidores percebam muitos benefícios em troca, há pouca dúvida de que as empresas, e não os consumidores, controlam o mercado de dados pessoais com seus próprios interesses em mente[806].

Além disso, Ira Rubinstein propõe que novos modelos de negócios sejam capazes de deslocar o controle sobre a coleta e o uso de dados de empresas para indivíduos, de maneira a tornar a própria regulamentação eficaz, oferecendo aos indivíduos a capacidade de se beneficiar do *big data* e, consequentemente, a motivação para aprender e controlar como seus dados são coletados e usados[807].

A formulação de *privacy by design*, segundo a autoridade de proteção de dados canadense, é baseada em sete princípios fundamentais:

> 1. Proactive not Reactive; Preventative not Remedial
> Anticipate, identify and prevent privacy invasive events before they occur.
> 2. Privacy as the Default Setting
> Build in the maximum degree of privacy into the default settings for any system or business practice. Doing so will keep a user's privacy intact, even if they choose to do nothing.
> 3. Privacy Embedded into Design
> Embed privacy settings into the design and architecture of information technology systems and business practices instead of implementing them after the fact as an add-on.
> 4. Full Functionality — Positive-Sum, not Zero-Sum

[805] JIMENE, Camilla do Vale. Reflexões sobre privacy by design e privacy by default: da idealização à positivação. In: (Coords.) MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Comentários ao GDPR**. São Paulo: RT, 2018.
[806] RUBINSTEIN, Ira S. Rubinstein. Big data: the end of privacy or a new beginning? **International Data Privacy Law**, v.3, 2.ed. 1 maio 2013, p.74-87.
[807] RUBINSTEIN, Ira S. Rubinstein. Big data: the end of privacy or a new beginning? **International Data Privacy Law**, v.3, 2.ed. 1 maio 2013, p.74-87.

> Accommodate all legitimate interests and objectives in a positive-sum manner to create a balance between privacy and security because it is possible to have both.
> 5. End-to-End Security — Full Lifecycle Protection
> Embed strong security measures to the complete lifecycle of data to ensure secure management of the information from beginning to end.
> 6. Visibility and Transparency — Keep it Open
> Assure stakeholders that privacy standards are open, transparent and subject to independent verification.
> 7. Respect for User Privacy — Keep it User-Centric
> Protect the interests of users by offering strong privacy defaults, appropriate notice, and empowering user-friendly options[808].

O GDPR tratou sobre o tema em seu considerando 78[809]. No artigo 25 do Regulamento europeu é determinada a observância do *privacy by design* e *by default*:

> 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.
> 2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão

[808] INFORMATION and privacy comissioner of Ontario. Privacy by design. Jan.2018. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd-1.pdf>. Acesso em: 24 dez. 2018. Tradução livre: 1. Proactive not Reactive; Preventative not Remedial: postura preventiva, de modo a evitar incidentes de violação à privacidade; 2. Privacy as the Default Settin: a configuração padrão de determinado sistema deve preservar a privacidade do usuário; 3. Privacy Embedded into Design: a privacidade deve estar incorporada à arquitetura de sistemas e modelos de negócio; 4. Full Functionality – Positive-Sum, not Zero-Sum: devem ser acomodados todos os interesses envolvidos, evitando falsas dicotomias que levam à mitigação de direitos; 5. End-to-End Security – Full Lifecycle Protection: na medida em que a segurança de dados é incorporada ao sistema antes da coleta de qualquer informação, esta é estendida para todo o ciclo de vida da informação; 6. Visibility and Transparency – Keep it Open: deve ser assegurado a todos os envolvidos que os sistemas e negócio são operacionalizados de acordo com as premissas e objetivos informados; e 7. Respect for User Privacy – Keep it User-Centric: exigência aos operadores dos serviços que respeitem os interesses dos usuários, mantendo altos padrões de privacidade.

[809] A defesa dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige a adoção de medidas técnicas e organizativas adequadas, a fim de assegurar o cumprimento dos requisitos do presente regulamento. Para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito. Tais medidas podem incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança. No contexto do desenvolvimento, conceção, seleção e utilização de aplicações, serviços e produtos que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções, haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e conceção e, no devido respeito pelas técnicas mais avançadas, a garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados. Os princípios de proteção de dados desde a conceção e, por defeito, deverão também ser tomados em consideração no contexto dos contratos públicos.

> do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.
> 3. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas nos n.1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42.

Esses conceitos não estão expressamente previstos na lei brasileira (LGPD). Perde, portanto, o legislador brasileiro, a oportunidade de inserir na legislação um importante mecanismo de proteção de dados. Porém, de outro lado, vale notar que o Decreto n. 8.771/2016, que regulamenta o Marco Civil da Internet, estabelece em seu artigo 13[810]padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas, corroborando a importância da segurança dos dados pessoais dos usuários, por meio da adoção de medidas técnicas e de práticas de negócio adequadas, determinando a necessidade de se criar infraestrutura apropriada à preservação da privacidade e proteção de dados dos usuários.

Ademais, na LGPD podem ser extraídos, indiretamente, os conceitos *privacy by design* e *by default* na previsão dos princípios da transparência, segurança e prevenção, plasmados no artigo 6º. E, ainda, de forma mais específica, em seu artigo 46, ao determinar que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Estas medidas deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (§2º). Além disso, a lei prevê que a autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no *caput* deste artigo, considerando a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no artigo 6º desta Lei (§1º).

Pela redação conferida pela Medida Provisória n. 869 de 27 de dezembro de 2018, o artigo 55-J da LGPD, X, dispõe que compete à Autoridade Nacional de

[810] Artigo 13 Decreto n.8.771/2016: (i) o estabelecimento de controle estrito sobre o acesso aos dados pessoais e registros coletados, mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso a tais informações; (ii) a previsão de mecanismos de autenticação de acesso aos registros, de modo a assegurar a individualização do responsável pelo tratamento dos registros; (iii) a criação de inventário detalhado dos acessos aos registros armazenados, contendo o momento, a duração, a identidade do responsável pelo acesso e o arquivo acessado; e (iv) o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

Proteção de Dados “estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores”, em clara adesão indireta ao conceito de *privacy by design* e *by default*.

Segundo Cíntia Rosa Pereira Lima e Bruno Ricardo Bioni, em doutrina escrita antes do advento da LGPD, o conceito de *privacy as the default setting* remete à exigência de se obter consentimento constante no Marco Civil, pois, ao estabelecer como configuração padrão a maior privacidade possível ao usuário, exige-se que a coleta de informações, como por meio de cookies, dependa de interação do usuário com o sistema e, portanto, de seu consentimento expresso[811].

Segundo o WP Article 29, confidencialidade, transparência, minimização de =do *privacy by design*[812], sem a pretensão de que tais técnicas sejam suficientes em si para os fins que se propõe[813].

---

[811] LIMA, Cíntia Rosa Pereira; BIONI, Bruno Ricardo. “A proteção dos dados pessoais na fase de coleta: apontamentos sobre a adjetivação do consentimento implementado pelo artigo 7, incisos VIII e IX do Marco Marco Civil da Internet a partir da Human Computer Interaction e da Privacy By Default”. In: **Direitos & Internet** III – Marco Civil da Internet. t.I. São Paulo: Quartier Latin, 2015, p.281.

[812] O estudo menciona ainda: The following examples demonstrate how PbD can contribute to a better data protection: Biometric identifiers should be stored in devices under control of the data subjects (i.e. smart cards) rather than in external data bases. Video surveillance in public transportation systems should be designed in a way that the faces of traced individuals are not recognizable or other measures are taken to minimize the risk for the data subject. Of course, an exception must be made for exceptional circumstances such as if the person is suspected of having committed a criminal offence. Patient names and other personal identifiers maintained in hospitals' information systems should be separated from data on the health status and medical treatments. They should be combined only in so far as it is necessary for medical or other reasonable purposes in a secure environment. Where appropriate, functionality should be included facilitating the data subjects' right to revoke consent, with subsequent data deletion in all servers involved (including proxies and mirroring). 53. In practice, the implementation of the privacy by design principle will require the evaluation of several, concrete aspects or objectives. In particular, when making decisions about the design of a processing system, its acquisition and the running of such a system the following general aspects / objectives should be respected: Data Minimization: data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data at all or as few personal data as possible. Controllability: an IT system should provide the data subjects with effective means of control concerning their personal data. The possibilities regarding consent and objection should be supported by technological means. Transparency: both developers and operators of IT systems have to ensure that the data subjects are sufficiently informed about the means of operation of the systems. Electronic access / information should be enabled. (Art 29 Working Party, Working Party on Police and Justice, ‘The future of privacy: joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data’ (WP 168, 1 dez. 2009). Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf>. Acesso em 04.jan.2019.

[813] Segundo apontam VEALE, Michael; BINNS, Reuben; AUSLOOS, Jef*:* There is a danger that data controllers implement privacy design strategies that leave them with data that is difficult for them to re-identify […] The situation is worsened by the fact that a data controller may have relatively little technical re-identification capacity, while also having a very low tolerance for inaccuracy when it comes to their provision of core data protection rights, such as access or erasure. Indeed, to erroneously provide a data subject sensitive personal data of another in response to a subject access request would usually be in breach of the same law the controller would be seeking to comply with. Tradução livre: Existe o perigo de que os controladores de dados implementem estratégias de privacy by design que os tornem difíceis dos dados serem identificados novamente [...] A situação é agravada pelo fato de que um controlador de dados pode ter relativamente pouca capacidade técnica de re-identificação, tendo também uma tolerância muito baixa à imprecisão quando se trata de fornecer direitos básicos de proteção de dados, como acesso ou apagamento. De fato, para fornecer erroneamente dados pessoais confidenciais de um usuário de dados em resposta a uma solicitação de acesso de um indivíduo normalmente estaria em violação da mesma lei que o controlador estaria procurando cumprir. (VEALE, Michael;

Diversamente do paradigma de proteção de dados, que tem mudado cada vez mais para colocar obrigações de responsabilização sobre os controladores de dados, como guardiões confiáveis de dados pessoais, o paradigma PET parte de uma percepção diametralmente oposta, não do controlador de dados como um terceiro confiável, mas como um adversário. Cuida-se, portanto, de um caminho que independe da conformidade do controlador, visto que a concepção da própria tecnologia visa proteger dados[814].

Isso porque os atuais modelos regulatórios existentes no campo da proteção de dados estão aquém e, por isso, não funcionam da forma como deveria. Sobre esse cenário contribuem Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson e Orla Lynskey:

> The Italian Marxist theorist Antonio Gramsci once wrote (in translation) that 'the old is dying and the new cannot be born; in this interregnum, a great variety of morbid symptoms appear'. Although Gramsci was not speaking about data privacy, it seems to us that this statement could apply to the current state of data protection regulation around the world, which is marked by a realization that existing regulatory models are not working effectively, the lack of political will to explore alternatives, and general frustration about how to improve the situation. This has led to a credibility gap between the objectives of data protection law and how personal data are protected in practice.
> It should not be this way. The importance of data privacy has never been greater, and countries and regional organizations around the world are enacting legislation in an attempt to protect it[815].

Ao que parece, as leis contemporâneas sobre proteção de dados não alcançam, verdadeiramente, a proteção a que se propõem. Os autores

---

BINNS, Reuben; AUSLOOS, Jef. When data protection by design and data subject rights clash. ***International Data Privacy Law***, v.8, Issue 2, 1 May 2018, p.107).

[814] VEALE, Michael; BINNS, Reuben; AUSLOOS, Jef. When data protection by design and data subject rights clash. ***International Data Privacy Law***, v.8, Issue 2, 1 May 2018, p.105-123, p.107. "Unlike the data protection paradigm, which has increasingly shifted to placing accountability obligations upon data controllers in an effort to make them trusted custodians of personal data, the PET paradigm departs from a 'diametrically opposed perception', not of the data controller as a trusted third party, but as an adversary".Tradução livre: Diferentemente do paradigma de proteção de dados, que tem mudado cada vez mais para colocar obrigações de responsabilidade sobre os controladores de dados em um esforço para torná-los guardiões confiáveis de dados pessoais, o paradigma PET se afasta de uma 'percepção diametralmente oposta', não do controlador de dados como um terceiro confiável. partido, mas como adversário

[815] KUNER, Christopher; CATE, Fred H.; MILLARD, Christopher; SVANTESSON, Dan Jerker B.; LYNSKEY, Orla. The data protection credibility crisis IN ***International Data Privacy Law***, v.5, 3.ed. 1 ago. 2015, p.161. Tradução livre: O teórico marxista italiano Antonio Gramsci escreveu certa vez que "o velho está morrendo e o novo não pode nascer"; Nesse interregno, uma grande variedade de sintomas mórbidos aparece. Embora Gramsci não estivesse falando sobre privacidade de dados, parece-nos que essa afirmação poderia se aplicar ao estado atual da regulação da proteção de dados em todo o mundo, que é marcada por uma percepção. que os modelos regulatórios existentes não estão funcionando efetivamente, a falta de vontade política para explorar alternativas e a frustração geral sobre como melhorar a situação. Isso levou a uma lacuna de credibilidade entre os objetivos da lei de proteção de dados e como os dados pessoais são protegidos na prática. Não deveria ser assim. A importância da privacidade de dados nunca foi tão grande, e países e organizações regionais em todo o mundo estão promulgando legislação na tentativa de protegê-la.

mencionados, sobre as novas regulações, colocam, em perspectiva: tudo isso faz alguma diferença para aumentar a proteção da privacidade de dados na prática?[816].

Há uma dificuldade latente, em termos mundiais, quanto à eficácia da lei na regulação do processamento de dados pessoais, em especial aqueles *online* e tratados por meio de algoritmos. Há um longo caminho a seguir para encontrar o ideal equilíbrio entre regulação legal e autorregulação do setor privado sobre o assunto, além de qual seria a melhor forma de aplicar a lei. Nesse sentido, Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson e Orla Lynskey observam:

> To a large extent, these questions are not unique to data protection and tend to arise in any area that involves the regulation of technology. But coming to a consensus about them has proved intractable, as they often reflect differences in national and regional laws and cultures[817].

Outra dificuldade ligada ao assunto aponta para como conciliar a proteção de dados na cultura do algoritmo com a globalização. Com sofisticados tratamentos pelo uso de algoritmos, sob as técnicas da inteligência artificial e *machine learning,* torna-se muito desafiador determinar o local onde os dados são coletados, processados e armazenados, até porque nem sempre esses atos ocorrem no mesmo país. Diante dessa situação, os indivíduos ficam ainda mais vulneráveis para exercer controle sobre seus dados pessoais de maneira eficaz.

Por sua vez, os controladores de dados podem encontrar semelhante frustração pela aplicação concomitante de várias leis, em seus serviços oferecidos ao mercado global de dados. E não menos importante, encontram-se os reguladores e governos com suas dificuldades (questões políticas, falta de recursos, etc) de *enforcement*, ou seja, de fazer valer a lei. E daqui deriva um cenário desigual que, por muitas vezes, direciona o regulador a se concentrar nos casos que tomaram mais repercussão na mídia, deixando outros *a latere* que mereceriam igual, ou até maior, atenção[818].

---

[816] KUNER, Christopher; CATE, Fred H.; MILLARD, Christopher; SVANTESSON, Dan Jerker B.; LYNSKEY, Orla. The data protection credibility crisis. ***International Data Privacy Law***, v.5, 3.ed.1 ago. 2015, p.161.

[817] KUNER, Christopher; CATE, Fred H.; MILLARD, Christopher; SVANTESSON, Dan Jerker B.; LYNSKEY, Orla. The data protection credibility crisis. ***International Data Privacy Law***, v.5, 3.ed. 1 ago. 2015, p.161. Tradução livre: Em grande medida, essas questões não são exclusivas da proteção de dados e tendem a surgir em qualquer área que envolva a regulamentação da tecnologia. Mas chegar a um consenso sobre eles se mostrou intratável, já que eles geralmente refletem diferenças nas leis e culturas nacionais e regionais.

[818] Sobre essas dificuldades, cabe a ponderação de Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, Orla Lynskey: “some of the most intractable problems of data privacy regulation have nothing to do with data privacy per se but reflect such factors as legislative gridlock in the EU and the USA, growing fragmentation and nationalism in the EU, and an unwillingness of countries and regions to cooperate to

Há uma dificuldade latente, em termos mundiais, quanto à eficácia da lei na regulação do processamento de dados pessoais, em especial aqueles online. Ademais, ainda há um longo caminho a seguir para encontrar o ideal equilíbrio entre regulação legal e autorregulação do setor privado sobre o assunto, como também o qual seria a melhor forma de aplicar a lei. Nesse sentido Christopher Kuner observa:

> To a large extent, these questions are not unique to data protection and tend to arise in any area that involves the regulation of technology. But coming to a consensus about them has proved intractable, as they often reflect differences in national and regional laws and cultures[819].

Em igual sentido, Michael Veale, Reuben Binns, Jef Ausloos indicam que, historicamente, a lei de proteção de dados tem enfrentado desafios significativos quanto à fiscalização, porquanto autoridades de proteção de dados são subfinanciadas e desarmadas, com capacidade limitada de examinar as práticas dos controladores de dados, além da capacidade restrita de agir de forma significativa quando há suspeitas de violações[820].

4.9 Princípio da inteligência artificial explicável

Em relação ao uso de algoritmos em aprendizado de máquina, é importante que os conceitos expostos no item anterior sejam aplicados igualmente à inteligência artificial. Para tanto, a autoridade nacional de proteção de dados deveria se ocupar em determinar parâmetros técnicos mínimos que os operadores de dados devem aplicar no *design* de seus sistemas e operações algorítmicas, de forma a obrigar as organizações que operam na cultura do algoritmo a garantirem os direitos de proteção de dados dos indivíduos. Assim, a autoridade deve emitir regras com

---

reach common solutions to what are global problems. Better protection of privacy is thus at least partially dependent on the resolution of difficult political issues that are outside the powers of those in the data privacy world to influence". Tradução livre: alguns dos problemas mais intratáveis da regulamentação da privacidade de dados não têm nada a ver com a privacidade de dados, mas refletem fatores como o impasse legislativo na UE e nos EUA, crescente fragmentação e nacionalismo na UE, e a relutância dos países e regiões em cooperar. para chegar a soluções comuns para o que são problemas globais. Melhor proteção da privacidade é, portanto, pelo menos parcialmente dependente da resolução de questões políticas difíceis que estão fora dos poderes daqueles no mundo da privacidade de dados para influenciar. (KUNER, Christopher; CATE, Fred H.; MILLARD, Christopher; SVANTESSON, Dan Jerker B.; LYNSKEY, Orla. The data protection credibility crisis. ***International Data Privacy Law***, v.5, 3.ed. 1 ago. 2015, p.162).

[819] KUNER, Christopher; CATE, Fred H.; MILLARD, Christopher; SVANTESSON, Dan Jerker B.; LYNSKEY, Orla. The data protection credibility crisis. ***International Data Privacy Law***, v.5, 3.ed. 1 ago. 2015, p.161. Tradução livre: Em grande medida, essas questões não são exclusivas da proteção de dados e tendem a surgir em qualquer área que envolva a regulamentação da tecnologia. Mas chegar a um consenso sobre eles se mostrou intratável, já que eles geralmente refletem diferenças nas leis e culturas nacionais e regionais.

[820] VEALE, Michael; BINNS, Reuben; AUSLOOS, Jef. When data protection by design and data subject rights clash, **International Data Privacy Law**, v.8, 2.ed. 1 maio 2018, p.106.

medidas técnicas apropriadas a serem adotadas, mediante a publicação de guias técnicos específicos e vinculantes, de modo que “these principles [...] should be rooted into the code with defaults aligning both privacy and business imperatives”[821].

A tendência, dada à limitação das leis em regular as tecnologias na cultura do algoritmo, é a regulação pela arquitetura técnica. Na Alemanha, por exemplo, o Ministério dos Transportes e de Infraestrutura Digital (*Bundesministerium für Verkehr und digitale Infrastruktur),* por meio de sua Comissão Ética, publicou, em 2017, um guia para o uso de carros autônomos, no qual se constata que a regulação da matéria começa justamente pelo *design* da programação dos veículos[822].

O documento emitido pelo Ministério alemão estipula 15 regras para *softwares designers* atingirem as aspirações legais (segurança, dignidade humana, liberdade de escolha e autonomia).

Ademais, para além da imposição de medidas técnicas a serem inseridas no *design* dos sistemas algoritmos – a fim de cumprir a proteção de dados pessoais, é preciso existir um meio de explicá-los no tocante às suas operações, inferências e decisões *(outputs*).

Omer Tene e Jules Polonetsky também defendem que as organizações divulguem os critérios decisórios que sustentam seu mecanismo de análise de dados:

> In a big data world, it is often not the data but rather the inferences drawn from them that give cause for concern. Inaccurate, manipulative or discriminatory conclusions may be drawn from perfectly innocuous, accurate data. Much like in quantum physics, the observer in big data analysis can affect the results of her research by defining the data set, proposing a hypothesis or writing an algorithm. At the end of the day, big data analysis is an interpretative process, in which one’s identity and perspective informs one’s results. Like any interpretative process, it is subject to error, inaccuracy and bias[823].

---

[821] Tradução livre: Esses princípios [...] devem ser enraizados no código com padrões alinhando privacidade e negócios. (CAVOUKIAN, Ann; JONAS, Jeff. **Privacy by design in the age of big data**. Ontario-Ca: Information and Privacy Commissioner, 2012, p.8).

[822] Ethics Commission Automated and Connected Driving. German Federal Minister of Transport and Digital Infrastructure. Jun. 2017, p.6. Disponível em: <https://www.bmvi.de/SharedDocs/EN/Documents/G/ethic-commission-report.pdf?__blob=publicationFile>. Acesso em: 10 jan. 2019. Destacamos: This makes it essential that decisions be taken when programming the software of highly and fully automated driving systems (p.5). E ainda: The significant enhancement of road safety is the objective of development and regulation, starting with the design and programming of the vehicles such that they drive in a defensive and anticipatory manner, posing as little risk as possible to vulnerable road users (p.6).

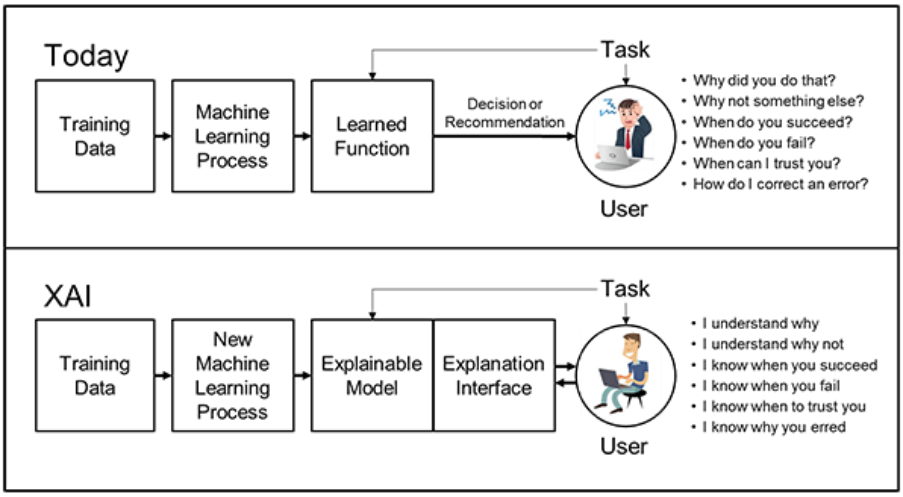
[823] TENE, Omer; POLONETSKY, Jules. Big data for all: privacy and user control in the age of analytics. **Northwestern Journal of Technology and Intellectual Property**, v.239, ano 2013, p.34. Tradução livre: Em um mundo de big data, muitas vezes não são os dados, mas as inferências deles que são motivo de preocupação. Conclusões imprecisas, manipulativas ou discriminatórias podem ser extraídas de dados perfeitamente inócuos e precisos. Assim como na física quântica, o observador na análise de big data pode afetar os resultados de sua pesquisa definindo o conjunto de dados, propondo uma hipótese ou escrevendo um algoritmo. No final das contas, a análise de big data é um processo interpretativo, no qual a identidade e a perspectiva da pessoa

Tornar os sistemas de inteligência artificial explicáveis é essencial para garantir direitos fundamentais como a proteção de dados pessoais, de modo a gerar a adequada confiança e a gestão eficiente de uma geração emergente de máquinas artificialmente inteligentes.

Pelo princípio da inteligência artificial explicável, também identificado pela sigla XAI (*Explainable Artificial Inteligence*), a criação de técnicas de *machine learning* devem produzir modelos mais explicáveis, mantendo um alto nível de desempenho de aprendizagem; devem ainda permitir que s usuários humanos compreendam, confiem adequadamente e gerenciem com eficácia a geração emergente de parceiros artificialmente inteligentes[824].

Para Omer Tener e Jules Polonetsky, os cientistas de dados que trabalham em empresas de tecnologia deveriam ser obrigados a garantir que qualquer algoritmo inteligente siga o princípio da "inteligência artificial explicável"[825].

Na figura abaixo, ilustra-se o uso de um sistema de *machine learning* com e sem a observância do princípio da Inteligência Artificial Explicável:



Fonte: Defense Advanced Research Project Agency[826]

---

informam os resultados da pessoa. Como qualquer processo interpretativo, está sujeito a erro, imprecisão e parcialidade.

[824] Defense Advanced Research Project Agency (DARPA. Disponível em: <https://www.darpa.mil/program/explainable-artificial-intelligence>. Acesso em: 24 dez. 2018.

[825] YU, Howard. GDPR isn't enough to protect us in an age of smart algorithms. **The Conversation**, 29 maio 2018. Disponível em: <https://theconversation.com/gdpr-isnt-enough-to-protect-us-in-an-age-of-smart-algorithms-97389>. Acesso em: 01 dez. 2018.

[826] Defense Advanced Research Project Agency (DARPA). Disponível em: <https://www.darpa.mil/program/explainable-artificial-intelligence>. Acesso em: 24 dez. 2018.

Os sistemas de *machine learning* devem ter, pelo princípio da inteligência artificial explicável, a capacidade de aclarar suas razões, caracterizar seus pontos fortes e fracos e transmitir uma compreensão de como eles se comportarão no futuro. A estratégia para atingir esse objetivo é desenvolver novas técnicas de *machine learning* que venham a produzir modelos mais explicáveis. Esses modelos devem ser combinados com técnicas de interface homem-computador de última geração capazes de traduzir modelos em diálogos de explicação compreensíveis e úteis para o usuário final[827].

Esse princípio contrasta com a realidade do caráter "caixa preta" na cultura do algoritmo. Não obstante, trata-se de um direito de todo indivíduo envolvido nas decisões provocadas pelos sistemas inteligentes. Há quem afirme que quanto menos opaco for o algoritmo, menos inteligente também o será. Além disso, a transparência deve ser proporcional ao 'poder do algoritmo' exercido.

Pela aplicação do princípio XAI, ao usuário devem ser fornecidas explicações do sistema de maneira a superar as questões de opacidade algoritma. Em outras palavras, os sistemas de inteligência artificial, que seguem o princípio XAI, incorporam processos de explicação que permitem aos usuários obter informações sobre os modelos e decisões do sistema, com a intenção de melhorar o desempenho do usuário em uma tarefa relacionada. Os modelos do sistema XAI podem ser aprendidos ou codificados manualmente e utilizados numa ampla variedade de tarefas de análise ou síntese. No entanto, a maioria dos sistemas de inteligência artificial não é dotada de processos de explicação. Enfrentar este desafio tornou-se mais urgente com a crescente dependência da cultura do algoritmo.

De 13 a 19 de julho de 2018 foram realizadas a 27ª Conferência Internacional em Inteligência Internacional, em conjunto com a 23ª Conferência Europeia em Inteligencia Artificial, ambas em Estocolmo, na Suécia (International Joint

[827] "A variety of techniques in order to generate a portfolio of methods that will provide future developers with a range of design options covering the performance-versus-explainability trade space".Tradução livre: Uma variedade de técnicas para gerar um portfólio de métodos que fornecerá aos futuros desenvolvedores uma gama de opções de design cobrindo o espaço de desempenho versus explicabilidade. (Defense Advanced Research Project Agency (DARPA). Disponível em: <https://www.darpa.mil/program/explainable-artificial-intelligence>. Acesso em: 24 dez. 2018. E ainda: At the end of the program, the final delivery will be a toolkit library consisting of machine learning and human-computer interface software modules that could be used to develop future explainable AI systems. After the program is complete, these toolkits would be available for further refinement and transition into defense or commercial applications. Tradução livre: No final do programa, a entrega final será uma biblioteca de kit de ferramentas que consiste em módulos de software de interface de aprendizagem de máquina e humano-computador que poderiam ser usados para desenvolver futuros sistemas de IA explicáveis. Depois que o programa estiver concluído, esses kits de ferramentas estarão disponíveis para refinamento adicional e transição para aplicações comerciais ou de defesa.

Conference on Artificial Intelligence and the 23rd European Conference on Artificial Intelligence – IJCAI-ECAI-18). Nessa ocasião, várias questões sobre sistemas XAI foram trazidas ao debate: como os modelos explicáveis devem ser projetados? como as interfaces do usuário devem comunicar a tomada de decisões? quais tipos de interação do usuário devem ser suportados? como a qualidade da explicação deve ser medida?[828].

Uma resposta adequada ao atual cenário deve combinar a questão legal com o uso da tecnologia em prol da proteção de dados, desde sua concepção, já em suas configurações de uso, inseridos em modelos de negócios voltados ao emporedamento do titular de dados, de forma que o sistema de inteligência artificial seja explicável e, de alguma maneira, possa ser auditado, conforme exposto nesse trabalho.

[828] IJCAI/ECAI 2018 Workshop on Explainable Artificial Intelligence (XAI). Disponível em: <http://home.earthlink.net/~dwaha/research/meetings/faim18-xai/>. Acesso em: 24 dez. 2018.

CONCLUSÃO

A sociedade informacional ocupou o que era denominado como sociedade pós-moderna, trazendo consigo complexidades antes não experimentadas, de forma a modificar a dinâmica das relações sociais, políticas e econômicas, bem como de modo a gerar novos debates, em especial no âmbito jurídico.

Nessa nova ordem social, o imperativo do desempenho faz do homem um explorado de si mesmo, deslocando a tipologia da violência para a forma subcutânea e invisível. O ser deixa de se voltar a si mesmo, e passa a ter atenção demasiada à máquina que lhe está em torno, provocando a morte social anunciada por Zygmunt Bauman, quanto ao uso excessivo de ferramentas digitais, com as quais o ser humano se relaciona em detrimento do convívio com outras pessoas. Há uma constante cobrança de que os indivíduos estejam sempre disponíveis e *online.*

Essa nova condição, a despeito de nociva, contribui para alimentar o mercado de atenção, cuja fórmula sintetiza que quanto mais interação do homem com a máquina, mais dados pessoais serão coletados e tratados, gerando informações com valor econômico, tal qual a previsão do que um indivíduo é mais propenso a consumir.

Para além desse exercício de poder, as características do leitor ubíquo, somadas à realidade presente e futura do advento da Internet das Coisas, também contribuem para incorpar o fenômeno do *big data*, como extrato da sociedade de dados, esta tida como uma derivação da sociedade da informação.

Quanto mais dados estiverem à disposição dos algoritmos, mais eficaz será o resultado de seu trabalho. Nessa toada, mais valioso do que os próprios algoritmos, por mais complexos e sofisticados que sejam, está o valor dos próprios dados. Portanto, a cultura do algoritmo apenas subsiste uma vez que esteja inserida na sociedade de dados. Daí a constatação de que a entropia dos algoritmos não persiste em si, porquanto se não houver dados, inexiste a engrenagem de seu funcionamento.

Sob outro enfoque, a pedra de toque em relação ao processamento algorítmico diz respeito à possibilidade de correlações, com reconhecimento de padrões e inferências, tal qual se revela na teoria do mosaico, segundo a qual dados, em princípio neutros, podem se converter, pela associação de processos algoritmos, em dados sensíveis.

Verificou-se como a vida hodierna tem sido pautada por processos algorítmicos, alterando o governo que o ser tem sobre si mesmo, uma vez que os algoritmos exercem grande persuasão no comportamento humano. Isso porque o homem tem se tornado dependente do processamento de dados por meio das máquinas sem, no entando, se dar conta dessa condição, de forma que pensa ser livre para fazer escolhas, quando, na verdade, está submisso aos ditames e escolhas da máquina algorítmica, sendo incapaz de dominá-la inteiramente.

A incapacidade desse controle se verifica, em especial, quanto à opacidade dos algoritmos, por cuja condição compromete-se o acesso aos dados da camada de entrada *(input*) das redes neurais, bem como impede-se o conhecimento da lógica existente na camada de processamento, que resultará (*output*) no estabelecimento de padrões e definição de perfis *(profiling*), para a tomada de decisões automatizadas.

A opacidade algorítmica, portanto, viola o princípio da transparência e desconstrói a doutrina da autoderminação informativa, ao passo que obsta que o titular exerça controle sobre seus dados pessoais, incluindo aqueles inferidos pelos sistemas de inteligência artificial.

A solução dogmática jurídica diante dessa problemática está no reconhecimento do direito de explicação conferido ao titular dos dados, cuja garantia foi plasmada no novo regulamento de proteção de dados europeu, porém, praticamente apagada da legislação brasileira, em claro retrocesso à tutela dos dados pessoais inseridos na cultura do algoritmo.

O direito à explicação, tal qual concebido pela dogmática, revela-se como insuficiente para garantir o pleno exercício dos direitos individuais, e também sociais, porquanto o caráter *black box* dos algoritmos podem, outrossim, ser considerados como problemas afetos à própria coletividade, ao atingir minorias e determinados grupos sociais.

Na construção do cenário simbiótico homem-máquina, constata-se que para além da lógica algorítmica, a opacidade está presente no próprio sujeito, sendo-lhe intrínseca à essência e à sua forma natural de ser (*natura* e *ars*). Isso porque o indivíduo está sofrendo um processo de artificialização de si mesmo, por meio do qual a fronteira entre a *phisis* e a *techné* está se dissipando, na criação do homem pós-orgânico.

Dada a grande dificuldade de se regular a proteção de dados pela norma jurídica, o ponto de partida deve ser a própria tecnologia (máquina), mormente diante da constatação de que o sistema jurídico tem dificuldades de acompanhar o compasso apressado das evoluções tecnológicas. Conceitos do direito à privacidade e proteção de dados pessoais devem ser incorporados, portanto, desde a concepção da arquitetura de seus sistemas.

No contexto da cultura dos algoritmos, passa a ser essencial tornar os sistemas de inteligência artificial explicáveis para garantir direitos fundamentais como a proteção de dados pessoais, de modo a gerar a adequada confiança e gestão com eficácia de uma geração emergente de máquinas artificialmente inteligentes. Trata-se do princípio da inteligência artificial explicável.

Os modelos utilizados nas práticas que se valem do *machine learning* devem ser produzidos de modo mais explicáveis, de forma a possibilitar que os usuários compreendam e confiem em sua lógica.

Recomendamos que a autoridade nacional de proteção de dados se ocupe em determinar regras de caráter técnico, a serem dirigidas aos operadores das máquinas algorítmicas na aplicação do *design* de seus sistemas, de modo a cumprir o princípio da inteligência artificial explicável.

REFERÊNCIAS

ACQUISTI and others. The Economics of Privacy. 54 **Journal of Economic Literature**, 2016.

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução Virgilio Afonso da Silva. São Paulo: Malheiros, 2006.

ALMEIDA, Virgílio; DONEDA, Danilo. **A política e os algoritmos**: o caso do STF. 08 fev. 2017. Disponível em: <https://www.poder360.com.br>. Acesso em: 01 out. 2018.

ALTMAN, Micah; WOOD, Alexandra Wood; O´BRIEN David R; GASSER, Urs. Practical approaches to big data privacy over time. **International Data Privacy Law**, v.8, 1.ed. fev.2018, p. 29–51. Disponível em <https://doi.org/10.1093/idpl/ipx027>. Acesso em: 22 out. 2018.

ÁLVAREZ, Luis Felipe López. **Protección de datos personales**: adaptaciones necessárias al nuevo reglamento europeo. Madrid: Francis Lefebvre, 2016.

AMAZON Mechanical Turk. Disponível em: <https://www.mturk.com/>. Acesso em: 25 dez. 2018.

ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. Machine bias. There's software used across the country to predict future criminals. And it's biased against blacks. **Pro Publica**. Publicado em: 23 maio 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 22 out. 2018.

ARENDT, Hannah. **A condição humana**. 10.ed. Rio de Janeiro: Forense Universitária, 2003.

ARAÚJO, Alberto Filipe; TEIXEIRA Maria Cecília Sanchez. Gilbert Durand e a pedagogia do imaginário. In: **Revista Eletrônica PUC RS Letras de Hoje**. Porto Alegre, v.44, n.4, p.7-13, out.-dez., 2009. Disponível em: <http://revistaseletronicas.pucrs.br>. Acesso em: 23 jul. 2018.

ARTICLE 29 Data protection working party, Opinion 8/2014 on the **Recent developments on the internet of things**, tech. report, 16 set.2014. Disponível em: <https://www.pdpjournals.com/docs/88440.pdf>. Acesso em: 27 jul. 2018.

ARTICLE 29 Data protection working party. Opinion 02/2013 on apps on smart devices. Adotado em 27 fev. 2013. Disponível em: <https://www.pdpjournals.com/docs/88097.pdf>. Acesso em: 10 set. 2018

_____. Global Human Rights Organisation. **Privacy and freedom of expression in the age of artificial intelligence**. Abr. 2018. Disponível em: <https://www.article19.org/>. Acesso em: 26 ago. 2018.

_____. **Algorithms and automated decision-making in context of crime prevention**: a briefing paper, 2016. Disponível em: <https://www.article19.org/> Acesso em: 28.ago. 2018.

AULA Magna da Cavallerizza Reale (Turim). Disponível em: <https://www.ilmessaggero.it/>. Acesso em: 30 jul. 2018.

BAGNOLI, Vicente. **The big data relevant market. Concorrenza e mercato**: antitrust, regulation, consumer welfare, intellectual property, v.23, p.73-94, 2016.

BAIGORRI, Laura. **CTRL + [SELF]**: intimacy, extimacy & control in the age of the overexposure of self. Disponível em: <https://htmlles.net>. Acesso em: 10 ago. 2018.

BAKER, Jennifer. **European Parliament**: suspend privacy shield unless US fully complies. Disponível em: <https://iapp.org/news/a/parliament-suspend-privacy-shield-until-u-s-fully-complies/>. Acesso em: 02 nov. 2018.

BAKER, Paul; POTTS, Amanda. Why do white people have thin lips? Google and the perpetuation of stereotypes via auto-complete search forms. In: **Critical discourse studies**, University Lancaster, 2013.

BALKIN, Jack M. Information fiduciaries and the first amendment. **UC Davis Law Review**, v.48.

_____. Sidley Austin distinguished lecture on big data law and policy: the three laws of robotics in the age of big data. **Ohio State Law Journal**, v.78, 2017.

_____. Algorithms and big data. **Entrevista concedida à Yale Law School**. Disponível em: <https://www.youtube.com/watch?v=6nKNAa1R4H4>. Publicado em 23 fev.2017. Acesso em: 24 dez. 2018.

BAROCAS, Solon; NISSENBAUM, Helen. Big data's end run around anonymity and consent. In: (Coords.) LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (Coord.). **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014.

BAUDRILLARD, Jean. **A sociedade de consumo**. Lisboa/PT: Edições 70, 2010.

_____. **Senhas**. Tradução de Maria Helena Kuhner da edição de 1929. Rio de Janeiro: Difel, 2007.

BBC. **Polícia usa algoritmo que prevê crimes para prender ladrão na Itália**. Veiculado em 19 nov. 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-46198655?ocid=socialflow_facebook>. Acesso em: 20 nov. 2018.

BENNET, Collin. In defence of privacy. The concept and the regime. **Surveillance & Society**, v.8, n.4, 2011.

BNDES. Banco Nacional do Desenvolvimento. **Relatório do Plano de Ação**. Internet das Coisas. Nov.2017. Disponível em: <https://www.bndes.gov.br>. Acesso em: 25 jul. 2018.

BAUMAN, Zygmunt. **Vida para consumo**: a transformação das pessoas em mercadoria. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2008.

_____. **Modernidade líquida***.* Tradução de Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2001.

_____. **"Extimidade"**: o fim da intimidade. Tradução de Moisés Sbardelotto. Publicado em 9 abr. 2011. Disponível em: <http://www.ihu.unisinos.br/noticias/42263-extimidade-o-fim-da-intimidade> Acesso em: 24 ago. 2018.

BEDÊ, Fayga Silveira. ***Ciberintimidade***: a escrita de si na era digital. Tese de Doutorado. Universidade Federal do Ceará. Centro de Humanidades. Departamento de Ciências Sociais. Programa de Pós-graduação em Sociologia. Fortaleza, 2010.

BERGEN, Mark; SURANE, Jennifer. **Google and mastercard cut a secret ad deal to track retail sales**. Publicado em: 30 ago. 2018. Disponível em: <https://www.bloomberg.com>. Acesso em: 05 set. 2018.

BERREBY, David. Click to agree with what? No one reads terms of service, studies confirm. In: **The Guardian**, 3.mar.2017. Disponível em: <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>. Acesso em 02.nov.2018.

BESSA, Leonardo Roscoe. **Cadastro positivo**: comentários à Lei 12.414/2011. São Paulo: RT, 2011.

BIONDI, Biondo. **Contratto e stipulatio**. Milano, 1953.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**. A função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BISHOP, Joseph. Book review: the naked society in the Yale Law Journal. **Yale Law School Legal Scholarship Repository**. v.74, p.194-199. Disponível em: <https://digitalcommons.law.yale.edu>. Acesso em: 04 set. 2018.

BLOUSTEIN, Edward. Privacy as an aspect of human dignity: an answer to dean prosser. **New York University Law Review** 39, 1964.

BLUME, P. The inherent contradictions in data protection law. **International Data Privacy Law 26**, 2012.

BÖHME, Rainer; KÖPSELL, Stefan. Trained to accept? A field experiment on consent dialogs. Conferencia: “**Proceedings of the 28th International Conference on Human Factors in Computing Systems**”, p.2403-2406, 2010, Atlanta, Georgia, USA, Abril 10-15, 2010. Disponível em: <https://www.researchgate.net/publication/221517054_Trained_to_accept_A_field_experiment_on_consent_dialogs>. Acesso em: 12 nov.2018.

BOLOGNINI, Luca; PELINO, Enrico; BISTOLFI, Camilla. **Il regolamento privacy europeo**. Milano/Italia: Giuffrè Editore, 2016.

BONAVIDES, Paulo. **Curso de direito constitucional**. 15.ed. São Paulo: Malheiros, 2006.

BONNEFON, Jean-François; SHARIFF, Azim; RAHWAN, Iyad. The social dilemma of autonomous vehicles **Science 24**, v.352, jun. 2016.

BORNE, Kirk. Knowledge is power. Publicado em: 11 abr. 2014. Disponível em: <https://mapr.com/blog/top-10-big-data-challenges-serious-look-10-big-data-vs/>. Acesso em: 12 out. 2018.

BOSTROM, Nick. **Superintelligence**: paths, dangers and strategies. Oxford University Press: Nova Iorque, 2014.

BRANDÃO, André Martins. **Sujeito e decisão na sociedade de dados**. Tese (Doutorado). Pontifícia Universidade Católica de São Paulo, São Paulo, 2017.

_____; SUÁREZ, Nuria Lopez Cabaleiro. Sociedad de información: la nueva topología del poder. In: (Orgs.) REY, Paula Requeijo; PISONERO, Carmen Gaona. **Contenidos inovador en la Universidad actual**. Madrid: McGraw-Hill, 2014.

BRASIL. Escola Nacional de defesa do consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. (Coord.) DONEDA, Danilo. Brasília: SDE/DPDC, 2010.

BRAUNEIS, Robert; GOODMAN, Ellen P. Algorithmic Transparency for the smart city, 2 de agosto de 2017. **Yale J. of Law & Tech**. 103 (2018); GWU Law School Public Law Research Paper; GWU Legal Studies Research Paper. Disponível em: <https://ssrn.com/abstract=3012499 or http://dx.doi.org/10.2139/ssrn.3012499>. Acesso em: 26 ago. 2018.

BRYAN; CAVE; LEIGHTON; PAISNER. **At a glance**: de-identification, anonymization, and pseudonymization. Disponível em: <https://www.bryancave.com/en/thought-leadership/at-a-glance-de-identification-anonymization-and-pseudonymization.html>. Acesso em: 24 dez. 2018.

BURANYI, Stephen. Rise of the racist robots – how AI is learning all our worst impulses. **The Guardian**. Publicaso em: 08 ago. 2017. Disponível em: <https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses>. Acesso em: 22 out. 2018.

BURGESS, Peter; FLORIDI, Luciano; POLS, Aurélie; HOVEN, Jeroen van. **Ethics advisory group**. Towards a digital ethics. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf>. Acesso em: 18 nov. 2018.

BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. In: **Big Data & Society**, jan.-jun. 2016. Disponível em: <http://journals.sagepub.com> Acesso em: 21 out. 2018.

BUSVINE, Douglas. Dados ocultos do Facebook carregam problemas apontados pelo regulador alemão. **Terra**. Publicado em: 23 abr. 2018. Disponível em: <https://www.terra.com.br>. Acesso em: 05 set. 2018.

BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. **International Data Privacy Law**, v.6, 2.ed., 01 maio 2016. Disponível em: <https://doi.org/10.1093/idpl/ipw006>. Acesso em: 18 out. 2018.

BUTLER, Declan. When Google got flu wrong. **Nature**, v.494, 14 fev. 2013.

CAMPOS, Cleber da Silveira; MANZOLLI, Jônatas. Sistemas interativos musicais aplicados à percussão mediada. **XX Congresso da Associação Nacional de Pesquisa e Pós-Graduação em Música**. Florianópolis, 2010. Disponível em: <http://repositorio.ufrn.br>. Acesso em: 26 ago.2018.

CAMPUZANO TOMÉ, Herminia. **Vida privada y datos personales**. Madri: Tecnos, 2000.

CAN the great master be brought back to create one more painting? Disponível em: <https://www.nextrembrandt.com>. Acesso em: 14 ago.2018.

CANCLINI, Néstor García. **Consumidores e cidadãos**. 7.ed. Rio de Janeiro: UFRJ, 2008.

CANELA, Guilherme; NASCIMENTO, Solano. **Acesso à informação e controle social de políticas públicas**. Brasília: ANDI, 2009.

CANNATA, Carlo Augusto. **Corso di istituzioni di diritto romano**, II, 1, Torino, 2003.

CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. **Constituição da República Portuguesa Anotada**, v.1. São Paulo: RT; Coimbra: Coimbra, 2007.

CANTARINI, Paola. **Princípio da proporcionalidade como resposta à crise autoimunitária do direito**. Rio de Janeiro: Lumen Juris, 2017.

CAPLAN, Robyn; DONOVAN, Joan; HANSON, Lauren; MATTHEWS, Jeanna. Algorithmic accountability: a primer. **Data & Society**. Publicado em 18 abr. 2018. Disponível em:<https://datasociety.net/output/algorithmic-accountability-a-primer/>. Acesso em: 26 ago. 2018.

CARNIO, Henrique Garbellini. Conhecimento e direito digital: acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos na lei do marco civil da internet. In: LEITE, George Salomão; LEMOS, Ronaldo. **Marco civil da internet**. São Paulo: Atlas, 2014.

CARRILLO, Marc. **El derecho a nos ser molestado**: información y vida privada. Navarra: Editorial Aranzadi, 2003.

CASANOVAS ROMEU, Pompeu. Derecho, internet y web semântica. In: GÓMEZ MARTÍNEZ, Carlos. Derecho a la intimidad y nuevas tecnologias. **Cuadernos de Derecho Judicial IX**. Madri: Consejo General del Poder Judicial, 2004.

CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia, sociedade e cultura v.1. São Paulo: Paz e Terra, 2011.

_____. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza Borges. Rio de Janeiro: Zahar, 2003.

CASTILLO VÁZQUEZ, Isabel-Cecilia del. **Protección de datos**: cuestiones constitucionales y administrativas. Navarra: Editorial Aranzadi, 2007.

CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005.

_____. **O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de setembro**. Disponível em:<http://www.buscalegis.ufsc.br/revistas/files/anexos/5544-5536-1-PB.pdf>. Acesso em: 25 ago. 2018.

CHAVES, Viviane Hengler Corrêa. **Norbert Wiener**: a teoria cibernética de um matemático. Tese de Doutorado. Universidade Estadual Paulista “Júlio de Mesquita Filho”. Instituto de Geociências e Ciências Exatas Campus de Rio Claro. Orientador: Prof. Dr. Irineu Bicudo, 2016.

CHINOY, Sahil. **What 7 creepy patentes reveal about Facebook**. Publicado em: 21 jun. 2018. Disponível em: <https://www.nytimes.com/>. Acesso em: 05 set. 2018.

COELHO, Fábio Ulhoa. Sabe aquilo que chamávamos de privacidade? **Folha de S. Paulo**. Publicado em: 21 ago. 2008. Disponível em: <https://www1.folha.uol.com.br/fsp/opiniao/fz2108200808.htm>. Acesso em: 04 set. 2018.

COMITÊ Gestor da Internet no Brasil. **A internet e o TCP IP**. Publicado em: 15 maio 2012. Disponível em: <http://ipv6.br/post/introducao/>. Acesso em: 13 out. 2018.

COMUNICADO à imprensa. Disponível em: <https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Press_Release_2016-09-27_Adminstrative_Order_Facebook_WhatsApp.pdf>. Acesso em: 30 set. 2016.

CONFESSORE, Nicholas. The unlikely activists who took on Silicon Valley – and Won, Aug. 14, 2018. **The New York Times Magazine**. Disponível em: <https://www.nytimes.com>. Acesso em: 02 nov. 2018.

CONSELHO DA EUROPA. Disponível em: <https://www.coe.int/en/web/data-protection/background-modernisation>. Acesso em: 08 nov. 2018.
_____. **The modernised Convention 108**: novelties in a nutshell. Disponível em: <https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8>. Acesso em: 08 nov. 2018.

_____. **Recommendation CM/Rec (2010) 13 and explanatory memorandum**. The protection of individuals with regard to automatic processing of personal data in the context of profiling, de 23 nov. 2010. Disponível em: <https://rm.coe.int/16807096c3>. Acesso em: 09 nov. 2018.

CONTISSA, Giuseppe; DOCTER, Koen; LAGIOIA, Francesca; LIPPI, Marco; Micklitz, Hans-W; PALKA, Przemyslaw; SARTOR, Giovanni; TORRONI, Paolo. **CLAUDETTE meets GDPR**. Automating the evaluation of privacy policies using artificial intelligence. Study Report, 02 jul. 2018. Disponível em: <https://goo.gl/irpAaz>. Acesso em: 18 nov. 2018.

CONTISSA, Giuseppe; LAGIOIA, Francesca; SARTOR, Giovanni. **The ethical knob**: ethically-customisable automated vehicles and the law, 17 out. 2017. Disponível em: <https://ssrn.com/abstract=2881280>. Acesso em: 18 nov.2018.

CONVENTION for the protection of individuals with regard to the processing of personal data (CETS 108). Disponível em: <https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958>. Acesso em: 29 nov. 2018.

COOLEY, Thomas McIntyre. **A treatise on the law of torts, or the wrongs which arise independent of contract**. Chicago: Callaghan and Company, 1879. Disponível em: <http://www.hathitrust.org/>. Acesso em: 04 set. 2018.

CORMEN, Thomas H.; LEISERSON, Charles E.; RIVEST, Ronald L., STEIN, Clifford. **Introduction to algorithms**. 3.ed. Massachusetts–EUA, The MIT Press, 2009.

COSTA JUNIOR, Paulo José da. **O direito de estar só**. Tutela penal da intimidade. São Paulo: RT, 1995.

CRAWFORD, Kate; SCHULTZ, Jason. Big data and due process: toward a framework to redress predictive privacy harms. **Boston College Law**, v.55, n.1, 2014.

CZERNIK, Agnieszka. **Was ist ein algorithmus**. Definition und Beispiele, 14.10.2016. Disponível em: <https://www.datenschutzbeauftragter-info.de/was-ist-ein-algorithmus-definition-und-beispiele/>. Acesso em: 19 nov. 2018.

DAVARA RODRÍGUEZ, Miguel Angel. **La protección de datos em Europa**. Madri: Asnef Equifax, 1998.

_____. **Derecho informático**. Navarra: Aranzadi, 1993.

DE LA TORRE, Lydia. GDPR matchup: The California consumer privacy act 2018. **International Association of Privacy Professionals (IAPP) News**, 31 jul. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/>. Acesso em: 07 set. 2018.

DELEUZE, Gilles. **Conversações**. Tradução de Peter Pál Pelbart. São Paulo: Editora 34, 2013.

DETERMANN, Lothar. **Analysis**: The California consumer privacy act of 2018, 02 jul.2018. Disponível em: <https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/>. Acesso em: 02 nov. 2018.

DI MAJO, Adolfo; FERRI, Giovanni Battista; FRANZONI, Massimo. **Il contrato in generale**. L'invalidità del contratto. t.VII. Torino: Giufrrè, 2002.

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

_____; ALMEIDA, Virgílio; MONTEIRO, Marília. Governance challenges for the internet of things. **IEE Computer Society**, v.19, n.4, p.56-59, 2015.

_____; MONTEIRO, Marília. O sistema da privacidade e proteção de dados no marco civil da internet. In: ARTESE, Gustavo. **Marco civil da internet** – análise jurídica sob uma perspectiva empresarial. São Paulo: Quartier Latin, 2015.

_____. Iguais mas separados: o *habeas data* no ordenamento brasileiro e a proteção de dados pessoais. **Cadernos da Escola de Direito e Relações Internacionais**, v.9, 2008. Disponível em: <http://revistas.unibrasil.com.br>. Acesso em: 25 ago. 2018.

DUPORTAIL, Judith. I asked tinder for my data. It sent me 800 pages of my deepest, darkest secrets In: **The Guardian**. Publicado em: 26 set. 2016. Disponível em: <https://www.theguardian.com>. Acesso em: 26 ago. 2016.

DURAND, Gilbert. **O imaginário**: ensaio acerca das ciências e da filosofia da imagem. Rio de Janeiro: Difel, 2001.

EASTERBROOK, Frank H. Cyberspace and the law of the horse. In: **Journal Articles University of Chicago Law School**, 1996, n. 207. Disponível em: <https://chicagounbound.uchicago.edu>. Acesso em: 25 ago. 2018.

ECO, Umberto. Caro nipote, studia a memoria. In: **La Repubblica.it**. Publicado em: 03 jan. 2014. Disponível em: <http://espresso.repubblica.it/visioni/2014/01/03/news/umberto-eco-caro-nipote-studia-a-memoria-1.147715>. Acesso em: 30 jul. 2018.

EDELMAN, Benjamin; LUCA, MichaeL; SVIRSKY, Dan. **Racial discrimination in the sharing economy**: evidence from a field experiment. Disponível em: <http://www.benedelman.org/publications/airbnb-guest-discrimination-2016-09-16.pdf>. Acesso em: 24 dez. 2018.
EDPB. Disponível em: <https://edpb.europa.eu>. Acesso em: 29 nov. 2018.

EISENSTEIN, Elizabeth L. **The printing press as an agente of change**. Communications and culture transformations in early-modern Europe. v.I e II. New York-USA: Cambrigde University Press, 1979.

ELIAS, Peter. A european perspective. In: (Coords.) LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen. **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014.

ESQUINAS VALVERDE, Patricia. **Protección de datos personales em la policía europea**. Valencia: Tirant le Blanch, 2010.

ETZIONI, Amitai. **Los limites de la privacidad**. Tradução de Alexander López Lobo. Ed. Edisofer S. L., Buenos Aires, 2012.

EUROPEAN Banking Federation's Comments on The Article 29 Working Party Guidelines on Automated Individual Decision-Making and Profiling (WP251). Disponível em: <https://www.ebf.eu/wp-content/uploads/2017/12/EBF_029539-EBF-comments-on-WP29-guidelines-on-automated-decision-making-and-profiling.pdf>. Acesso em: 13 nov. 2018.

EUROPEAN Commission. **Report on the consultation on IoT governance**, tech. report, 16 jan. 2013. Disponível em: <https://ec.europa.eu/digitalagenda/en/news/conclusions-internetthings-public-consultation>. Acesso em: 27 jul. 2018.

EUROPEAN Commission. **Impact assessment accompanying the proposed regulation and the proposed directive**, SEC (2012) 72 final. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN>. Acesso em: 18.out. 2018.

_____. **Opinion 03/2013 on purpose limitation**. Disponível em: <http://ec.europa.eu/newsroom/article29/news-overview.cfm>. Acesso em: 31 out. 2017

EUROPEAN Commission Communication. **A comprehensive approach on personal data protection in the European Union' COM (2010) 609 final**. Disponível em: <https://eur-lex.europa.eu/>. Acesso em: 05 out. 2018.

EUROPEAN Commission EU-U.S. **Privacy shield**: first review shows it works but implementation can be improved. 18 out. 2017. Disponível em: <http://europa.eu/rapid/press-release_IP-17-3966_en.htm>. Acesso em: 02 nov. 2018.

EUROPEAN University Institute. **CLAUDETTE machine learning powered analysis of consumer contracts and privacy policies**. Disponível em: <https://claudette.eui.eu/about/>. Acesso em: 24 dez. 2018

EU-US Privacy Shield. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en>. Acesso em: 02 nov. 2018.

FEDERAL TRADE COMMISION. **FTC staff report**. Internet of things. Privacy & Security in a connected world. Jan. 2015. Disponível em: <https://www.ftc.gov/>. Acesso em: 27 ago. 2018.

FERRAZ JUNIOR, Tercio Sampaio. **O direito, entre o futuro e o passado**. São Paulo: Noeses, 2014.

_____. Direito e realidade: a erosão do real jurídico pelo mundo virtual. In: FERRAZ JUNIOR, Tercio Sampaio. **O direito entre o futuro e o passado***.* São Paulo: Noeses, 2014.

FERNÁNDEZ DE MARCOS, Isabel Davara. **Hacia la estandarización de la protección de datos personales**. Madri: La Ley, 2011.

FINANCIAL Times Lexicon. Disponível em: <http://lexicon.ft.com/term?term=principal/agent-problem>. Acesso em: 24 dez. 2018.

FLEISHMAN, Glenn. California passes groundbreaking consumer data privacy law with fines for violations, June 2018. **Fortune**. Disponível em: <http://fortune.com/>. Acesso em: 02 nov. 2018.

FLORIDI, Luciano. **Should we be afraid of AI**? Disponível em: <https://aeon.co/essays/true-ai-is-both-logically-possible-and-utterly-implausible>. Acesso em: 26 ago. 2018.

_____. **Information**. Oxford/UK: Oxford University Press, 2010.

_____. **Philosohy of computing and information**. Malden/EUA: Bçackwell Publishing, 2004.

_____; WACHTER, Sandra; MITTELSTADT, Brent. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, v.7, 2.ed. 1 maio 2017, p.80. Disponível em: <https://doi.org/10.1093/idpl/ipx005>. Acesso em: 16 out. 2018.

_____; **4th Revolution**: How the infosphere is reshaping human reality. Oxford University Press: New York – EUA, 2014.

FLUSSER, Vilém. **Filosofia da caixa preta**. Ensaios para uma futura filosofia da fotografia. São Paulo: Annablume, 2011.

FORBES Technology Council. **How will California's consumer privacy law impact the data privacy landscape?** Forbes. Disponível em: <https://www.forbes.com>. Acesso em: 02 nov. 2018.

FOUCAULT, Michel. **Vigiar e punir**. 30.ed. Petrópolis: Vozes, 2005.

FRIED, Charles. Privacy. **Yale Law Journal**, v.77, n.3, jan. 1968. Disponível em: <https://www.cs.scranton.edu/~plishka/cmps184/Privacy.pdf>. Acesso em: 31 jul. 2018.

FRIEDMAN, Lawrence M. **The republic of choicem law, authority and culture**. Cambridge (Mass.): Harvard University Press, 1990.

FTC. **Developing the Administration's Approach to Consumer Privacy**, 09 nov. 2018. Disponível em: <https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf>. Acesso em: 20 nov. 2018.

FUTURE of life institute. **Autonomous weapons**: an open letter from aI & robotics researchers. Disponível em: <https://futureoflife.org/open-letter-autonomous-weapons>. Acesso em: 25 dez. 2018.

G1 – Tecnolgia e Games. **'Nomes Brasil', site que mostra CPFs de brasileiros sai do ar**. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/05/nomes-brasil-site-que-mostra-cpfs-de-brasileiros-sai-do-ar.html>. Acesso em: 24 dez. 2012.

GALEON, Dom. **World bank chief**: robots have put us on a dangerous "crash course". Disponível em: <https://futurism.com/world-bank-chief-robots-have-put-us-on-a-dangerous-crash-course>. Acesso em: 25 ago. 2018.

GARCÍA-LAJARA, Enrique Collado. **Protección de datos de carácter personal**: legislación, comentários, concordâncias y jurisprudência. Granada: Comares, 2000.

GHOSH, Dipayan. What you need to know about California's new data privacy law, July 11, 2018. **Harvard Business Review**. Disponível em: <https://hbr.org>. Acesso em: 02 nov. 2018.

GHOSH, Pallab. Google's vint cerf warns of 'digital dark age'. **BBC News**, 13 fev. 2015. Disponível em: <https://www.bbc.com/news/science-environment-31450389>. Acesso em: 22 out. 2018.

GIDDENS, Anthony. **As conseqüências da modernidade**. Tradução de Raul Fiker. São Paulo: Unesp, 1991.

GINSBERB, Jeremy; MOHEBBI, Matthew H.; PATEL, Rajan S.; BRAMMER, Lynnette; SMOLINSKI, Mark S.; BRILLIANT, Larry. Detecting influenza epidemics using search engine query data. **Nature**, v.457, 19 fev. 2009.

GOMES, Helton Simões. Bancos e lojas pagam até R$ 4,70 por acesso a dados do seu rosto. Publicado em: 06 ago. 2018. **UOL Notícias**. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/08/06/bancos-e-lojas-pagam-ate-r-47-para-acessar-dado-do-rosto-de-brasileiros.htm>. Acesso em: 05 set. 2018.

GONICK, Larry. **Introdução ilustrada à computação**. São Paulo: Harper & Row do Brasil, 1984.

GOOGLE. **Support**. Disponível em: <https://support.google.com>. Acesso em: 15 nov. 2018.

GOOGLE PATENTS. Disponível em: <https://patents.google.com/>. Acesso em: 28 nov. 2018.

GREENWALD, Glenn. **Sem lugar para se esconder**. Tradução de Fernanda Abreu. Rio de Janeiro: Sextante, 2014.

GREENWOOD, Daniel; STOPCZYNSKI, Arkadiusz; SWEATT, Brian; HARDJONO, Thomas; PENTLAND, Alex. **The new deal on data**: a framework for institutional controls. Cambridge University Press. New York: Columbia University, 2014.

LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen. **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014.

GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lumen Juris, 2018.

_____. **Introdução à sociologia do direito**. São Paulo: RT, 2016.

_____. **Immunological theory of law**. Alemanha, Saarbrücken: Lambert Academic Publishing, 2014.

_____. Crise autoimunitária na autopoiese jurídica da sociedade mundial In: **Revista FMU Direito**, São Paulo, ano 27, n.39, p.143-150, 2013.

_____. **Processo constitucional e direitos fundamentais**. 5.ed. São Paulo: RCS, 2006.

_____. ***Quantum critic***: conhecimento e comunicação em transmutação físico-matemática. Tese de Doutorado em Comunicação e Semiótica. Pontifícia Universidade Católica de São Paulo (PUC-SP), São Paulo. Orientadora: Profa. Dra. Leda Tenório da Motta, 2017.

_____; CARNIO, Henrique Garbellini. **Teoria política do direito**. 2.ed. São Paulo: RT, 2013.

_____; CARNIO, Henrique Garbellini. Metodologia jurídica político-constitucional e o Marco Civil da Internet: contribuição ao direito digital. In: DEL MASSO, Fabiano Dolenc; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio. **Marco Civil da Internet**. São Paulo: RT, 2014.

GUYNN, Jessica. Google Photos Labeled Black People “Gorillas”. In: **USA TODAY**, 01 jul. 2015. Disponível em: <http://www.usatoday.com/story/tech/2015/07/01/google-apologizes-after-photos-identify-black-people-as-gorillas/29567465>. Acesso em: 18 nov. 2018.

HÄBERLE, Peter. **El Estado constitucional**. Buenos Aires: Editorial Ástrea de Alfredo y Ricardo Depalma, 2007.

HACKER, Philipp. Personal data, exploitative contracts, and algorithmic fairness: autonomous vehicles meet the internet of things. **International Data Privacy Law**, v.7, ed.4, nov.2017, p.266-286. Disponível em: <https://doi.org/10.1093/idpl/ipx014>. Acesso em: 16 out. 2018.

HAMBURG. **Der Hamburgirsche Beaufitragte fur Datenzschutz und Informationsfreiheit**. Comunicado à imprensa. Disponível em: <https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Press_Release_2016-09-27_Adminstrative_Order_Facebook_WhatsApp.pdf>. Acesso em: 30 set. 2016.

HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017.

_____. **Sociedade do cansaço**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017.

_____. **Topologia da violência**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017.

HEIDEGGER, M. **Überlieferte Sprache und technische Sprache**, St. Gallen: Erker, 1989 (Língua de tradição e língua técnica). Tradução de Mário Botas. 2.ed. Lisboa: Vega, 1999.

HERMOSO, Borja. Entrevista a Jürgen Habermas. **El País**. Publicado em: 07 maio 2018. Disponível em: <https://brasil.elpais.com>. Acesso em: 24 ago. 2018.

HERZOG, Ana Luiza. O Brasil na onda das smart grids. **Revista Exame**. Publicada em: 29 abr. 2013. Disponível em: <https://exame.abril.com.br>. Acesso em: 28 nov. 2018.

HILDEBRANDT, Mireille. **Smart technologies and the end(s) of law**. Edward Elgar: Cheltenham, UK, 2015.

HOFFMAN, David A.; WILKINSON-RYAN, Tess.The psychology of contract precautions. **University of Chicago Law Review**, v.80, p.395, 2013. Disponível em: <https://ssrn.com/abstract=2000823>. Acesso em: 12.nov.2018.

IAPP. **GDPR matchup**: the California consumer privacy act 2018. Disponível em: <https://iapp.org>. Acesso em: 07 set. 2018.

_____. **White House taking first steps toward federal privacy law**. Disponível em:<https://iapp.org/news/a/white-house-taking-first-steps-forward-federal-privacy-law/>. Acesso em: 07 set. 2018.

_____. **European Parliament suspend privacy shield unless US fully complies**. Disponível em: <https://iapp.org/news/a/parliament-suspend-privacy-shield-until-u-s-fully-complies/>. Acesso em: 07 set. 2018.

_____. **Preparing for the GDPR**: DPOs, PIAs, and Data Mapping. Disponível em: <https://iapp.org/media/pdf/resource_center/Preparing-for-GDPR_FINAL-1.0.pdf>. Acesso em: 02 nov. 2018.

IJCAI/ECAI 2018 Workshop on Explainable Artificial Intelligence (XAI). Disponível em: <http://home.earthlink.net/~dwaha/research/meetings/faim18-xai/>. Acesso em: 24 dez. 2018.

INFORMATION and information and privacy comissioner of Ontario. Privacy by design. Jan. 2018. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd-1.pdf>. Acesso em: 24 dez. 2018.

INGIZZA, Carolina. **O Estado de S. Paulo**. Caderno Link. 3 exemplos de como a internet das coisas já é usada no Brasil. Disponível em: <https://link.estadao.com.br/>. Acesso em: 25 ago. 2018.

_____. **O Estado de S. Paulo**. Três exemplos de como a internet das coisas já é usada no Brasil. Disponível em: <https://link.estadao.com.br/noticias/inovacao,3-exemplos-de-como-a-internet-das-coisas-ja-e-usada-no-brasil,70002026748>. Acesso em: 27 jul. 2018.

INTERNATIONAL Association for artificial intelligence and law. Disponível em: <http://www.iaail.org/?q=page/ai-law>. Acesso em: 24 dez. 2018.

ISAACSON, Walter. **Steve Jobs**: a biografia. Tradução de Berillo Vargas, Denise Bottmann e Pedro Maia Soares. São Paulo: Companhia das Letras, 2011.

ISRANI, Ellora Thadaney. When an algorithm helps send you to prison. **The New York Times**. Publicado em: 26 out. 2017. Disponível em: <https://www.nytimes.com>. Acesso em: 22 out. 2018.

ISTO É. **Facebook cedeu dados de usuários a 60 empresas, denuncia NYT**. Publicado em: 04 jun. 2018. Disponível em: <https://istoe.com.br>. Acesso em: 05 set. 2018.

IT FORUM. **Site** '**Tudo sobre Todos' mostra dados pessoais de brasileiros**. Disponível em: <https://www.itforum365.com.br/seguranca/site-tudo-sobre-todos-mostra-dados-pessoais-de-brasileiros/>. Acesso em: 24 dez. 2018.

JASPERS, Karls. **Introdução ao pensamento filosófico**. Tradução de Leonidas Hegenberg e Octanny Silveira da Mota. São Paulo: Cultrix, 1973.

KAMARINOU, Dimitra; MILLARD, Christopher; SINGH, Jatinder. Machine learning with personal data (November 7, 2016). **Queen Mary School of Law Legal Studies**. Research Paper n.247, 2016.

KERRY, Cameron F. Protecting privacy is a losing game today – and how to change the game. In: **Brookings**. Publicado em 12 jul. 2018. Disponível em: <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>. Acesso em: 15 nov.2018.

KHUN, Thomas Samuel. **A estrutura das revoluções científicas**. São Paulo: Unesp, 2006.

KOBIE, Nicole. **Who do you blame when an algorithm gets you fired?** Disponível em: <https://www.wired.co.uk/article/make-algorithms-accountable>. Acesso em: 24 dez. 2018.

KOONIN, Steven E.; HOLLAND, Michael J. The value of big data for urban science. In: (Coords.) LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen. **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014.

KOOPES, B-J. The trouble with european data protection law. **International Data Privacy Law**, 2014.

KRAMER, Adam D. I.; GUILLORY, Jamie E.; HANCOCK, Jeffrey T. **Experimental evidence of massive-scale emotional contagion through social networks**. Proceedings of the National Academy of Sciences of the United States of America. 17 jun. 2014. Disponível em: <http://www.pnas.org/content/111/24/8788.full>. Acesso em: 21 ago. 2018.

LACE, Susanne. **The glass consumer**: life in a surveillance'. Society.Bristol-UK: Policy Press, 2005.

LARSON, Christina. Who needs democracy when you have data? Publicado em: 20 ago. 2018. In: Massachusetts Institute of Technology. **Technology Review**. Disponível em: <https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/>. Acesso em: 27 ago. 2018.

LAWGORITHM. Disponível em: <http://www.lawgorithm.com.br/>. Acesso em: 24 dez. 2018.

LAZER, David; KENNEDY, Ryan; KING, Gary; VESPIGNANI, Alessandro. The parable of Google flu: traps in big data analysis. **Science** v.343, 14 mar.2014.

LAZER, David; KENNEDY, Ryan. What we can learn from the epic failure of Google flu trends. **Wired**, 10 jan. 2015. Disponível em: <https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/>. Acesso em: 19 nov.2018.

LEMOS, Ronaldo. Lei de dados nasceu desgovernada. **Folha de S. Paulo**, 20 ago. 2018.

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

_____. Internet: elementos fundamentais. In: (Coords.) SILVA, Regina Beatriz Tavares da; SANTOS, Manoel J. Pereira dos. **Responsabilidade civil na internet e nos demais meios de comunicação**. 2.ed. São Paulo: Saraiva, 2012.

LESSIG, Lawrence. The law of the horse: what cyberlaw might teach. **Harvard Law Review**, v.CXIII, 1999.

_____. **Code**. v.2. New York: Basic Books, 2006.

LEVY, Pierre. **As tecnologias da inteligência**. O futuro do pensamento na era da informática. Tradução de Carlos Irineu da Costa. Rio de Janeiro: Editora 34, 2011.

_____. **Cibercultura**. Tradução de Carlos Irineu da Costa. 3.ed. Rio de Janeiro: Editora 34, 2010.

_____. **O que é o virtual?** Tradução de Paulo Neves. 2.ed. Rio de Janeiro: Editora 34, 2011.

LIMA, Cíntia Rosa Pereira de; BIONI, Bruno Ricardo. A proteção de dados pessoais na fase de coleta: apontamentos sobre a adjetivação do consentimento implementada pelo artigo 7º, inciso VIII e IX, do Marco Civil da Internet a partir da Human Computer Interaction e da Privacy by Default. In: DE LUCCA, Newton; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira de. **Direito & internet III** – Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015.

LIMBERGER, Têmis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

LIPOVETSKY, Gilles. **A Sociedade da decepção**. Barueri, SP: Manole, 2007.

LOPES, Ruy Sardinha. **Informação, conhecimento e valor**. São Paulo: Radical Livros, 2008.

LORIOL, Marc. A sociological stance on fatigue and tiredness: Social inequalities, norms and representation. In: **Neurophysiol clin**. 2017 Apr; 47(2):87-94. doi: 10.1016/j.neucli.2016.12.001. Epub 2017 Feb 2. Disponível em: <https://www.ncbi.nlm.nih.gov/pubmed/28162843>. Acesso em: 22 ago. 2018.

LOSANO, Mario G. **Lições de Informática jurídica**. São Paulo: Resenha Tributária, 1974.

LUCAS MURILLO, Pablo. **El derecho a la autodeterminación informativa**. Madri/Espanha: Tecnos, 1990.

LUFT, Eduardo; CIRNE-LIMA, Carlos. **Ideia e movimento***.* Rio de Janeiro: Civilização Brasileira, 2012.

LUHMANN, Niklas. **A realidade dos meios de comunicação**. Tradução de Ciro Marcondes Filho. São Paulo: Paulus, 2011.

LYON, David. **Pós-modernidade**. São Paulo: Paulus, 1998.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV, 2018.

MAGRANI, Eduardo José Guedes. **A internet das coisas**: privacidade e ética na era da hiperconectividade. Tese de Doutorado. Orientadora: Caitlin Sampaio Mulholland, 2018.

MAIN, Lucimara; MORO, Maitê Cecília Fabbri. Responsabilidade social corporativa das empresas: proteção legal de dados na utilização do *big data*. In: (Orgs.) CASTRO, Matheus de; PEZZELA, Maria Cristina Cereser; RECKZIEGEL, Janaína. **A ampliação dos direitos subjetivos no Brasil e na Alemanha**. t.II. v.2. Joaçaba: Unoesc, 2014.

MARANHÃO, Juliano Souza de Albuquerque; CAMPOS, Ricardo. Exercício de autoregulação regulada das redes sociais no Brasil. In: (Orgs.) NERY, N. Campos; ABBOUD, G. ***Fake news* e regulação**. São Paulo: RT, 2018.

_____. **Programa de computador implementado por programa de computador**: a inventividade dos juristas e a liberdade dos programadores. Revista Eletrônica do IBPI, v. 7, p.229-251, 2012.

_____. **Estudos sobre lógica e direito**. São Paulo: Marcial Pons, 2013.

_____. **Positivismo jurídico lógico-inclusivo**. São Paulo: Marcial Pons, 2012.

MARANHÃO, Juliano; CAMPOS, Ricardo. Exercício de autorregulação regulada das redes sociais no Brasil. In: (Orgs.) NERY, N. Campos; ABBOUD, George. ***Fake news* e regulação**. São Paulo: RT, 2018.

MARKOFF, John. **What the dormouse said**: how the sixties counterculture shaped the personal computer industry. Disponível em: <https://www.amazon.com/>. Acesso em: 20 maio 2018.

MARR, Bernard. A short history of machine learning – every manager should read. **Forbes**. Publicado em: 19 fev. 2016. Disponível em: <https://www.forbes.com/sites/bernardmarr/2016/02/19/a-short-history-of-machine-learning-every-manager-should-read/#20f5f5e15e78>. Acesso em: 21 out. 2018.

MARTINEZ, Antonio Garcia. **Why California's privacy law won't hurt Facebook or Google in wired**. Disponível em: <https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google/>. Acesso em: 02 nov. 2018.

MASUDA, Yoneji. **A sociedade da informação como sociedade pós-industrial**. Tradução do inglês de Kival Charles Weber e Angela Melim. Rio de Janeiro: Rio, 1982.

MATSUSHITA, Thiago Lopes. **O jus-humanismo normativo** – expressão do princípio absoluto da proporcionalidade. Tese de Doutorado. Orientador: Ricardo Hasson Sayeg. Pontifícia Universidade Católica de São Paulo, São Paulo, 2012.

MATTELART, Armand. **História da sociedade da informação**. 2.ed. São Paulo: Loyola, 2006.

MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. **Technology and privacy**, Cambridge-MA/EUA, 1997.

_____; CUKIER, Kenneth. **Big data**: a revolution that will transform how we live, work and think. New York: Houghton Mifflin Publishing, 2013.

_____. **Big data**. La revolución de los datos masivos. Tradução de Antonio Iriarte. Madri: Turner, 2013.

McKINSEY Global Institute. **Jobs lost, jobs gained**: workforce transitions in a time of automation. Dez. 2017.

MCCARTHY, John. What is artificial intelligence. **Stanford University**, 12 nov. 2007. Disponível em: <http://www-formal.stanford.edu/jmc/whatisai/node1.html>. Acesso em: 12 out. 2018.

MENDEL, Toby. **Freedom of information**: a comparative legal survey. 2.ed. Paris: UNESCO, 2008.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Saraiva, 2014.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. v.1. São Paulo: Saraiva, 2015.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. **MPDFT investiga venda ilegal de dados pessoais pelo site "Tudo sobre todos"**. Publicado em 10 jul. 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10182-mpdft-investiga-venda-ilegal-de-dados-pessoais-pelo-site-tudo-sobre-todos>. Acesso em: 24 dez. 2018.

MITCHELL, Tom; BRYNJOLFSSON, Erik. **Track how technology is transforming work**. Disponível em: <https://www.nature.com/news/track-how-technology-is-transforming-work-1.21837>. Acesso em: 25 ago. 2018.

MOL, Rogério Santos. **M717i Introdução à história da matemática**. Belo Horizonte: CAED-UFMG, 2013.

MORA, Vicente Luis. **Pangea**. Internet, blogs y comunicación en un mundo nuevo. Sevilla: Fundación José Manuel Lara, 2006.

MORO, Maitê Cecília Fabbri; MAIN, Lucimara. Reputação da organização: gerenciamento de crise da imagem, como forma de garantir a função social e sustentabilidade financeira da empresa. In: (Orgs.) ROVER, Aires José; CELLA, José Renato Gaziero; AYUDA, Fernando Galindo. **Direito e novas tecnologias**. Florianópolis: CONPEDI, 2014.

MUNOZ, Andres. **Machine learning and optimization**. Courant institute of mathematical sciences. New York. Disponível em: <https://cims.nyu.edu/~munoz/files/ml_optimization.pdf >. Acesso em: 18 out. 2018.

MURILLO, Pablo Lucas. **El derecho a la determinación informativa**. Madri: Tecnos, 1990.

NATIONAL PUBLIC RADIO. **How europe's new data privacy law is supposed to give users more control**. Disponível em: <https://www.npr.org/2018/05/28/615010156/how-europes-new-data-privacy-law-is-supposed-to-give-users-more-control>. Acesso em 12 nov. 2018.

NEGROPONTE, Nicholas. **El mundo digital**. Tradução de Marisa Abdala. Barcelona: Ediciones B, S.A., 1995.

NICHOLS, Tom. The death of expertise. In: **The Federalist**, 17 jan. 2014. Disponível em: <http://thefederalist.com/2014/01/17/the-death-of-expertise/>. Acesso em: 10 out. 2018.

NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford, CA: Stanford University Press, 2009.

NÖTH, Winnfried. Máquinas semióticas. In: (Org.) João Queiroz et.al. **Computação, cognição, semiose**. Salvador: EDUFBA, 2007.

NUNES, Marcelo Guedes. **Jurimetria**: como a estatística pode reiventar o direito. São Paulo: RT, 2016.

ONG, Rebecca. Recognition of the right to privacy on the internet in China. **International Data Privacy Law**, v.1, 3.ed., 1 ago. 2011, p.172-179. Disponível em: <https://doi.org/10.1093/idpl/ipr008>. Acesso em: 10 out. 2018.

OOSTVEEN, Manon. Identifiability and the applicability of data protection to big data. **International Data Privacy Law**, v.6, 4. ed, nov. 2016, p.299-309. Disponível em: <https://doi.org/10.1093/idpl/ipw012>. Acesso em: 12 out. 2018.

ORTEGA, Félix. **El mito de la modernización**. Barcelona: Anthropos, 1994.

OURLIAC, Paul; DE MALAFOSSE, Jehan. **Derecho romano y francês histórico**. Tradução ao espanhol e anotações de Manuel Fairén. t.I. 1960.

PADILLA, Margarita. **El kit de la lucha en Internet**. Cidade: Lemur, 2012.

PAGALLO, Ugo. **Il diritto nell´età dell´informazione**. Torino: G. Giappichelli Editore, 2014.

PARENTE, Alessandra. **Cibernética e neoliberalismo**: a crítica como mercadoria. (No prelo)

PARLIAMENT United Kingdom. **Algorithms in decision-making inquiry launched**, 28.fev.2017. Disponível em: <https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2015/algorithms-in-decision-making-inquiry-launch-16-17/>. Acesso em: 18 nov. 2018.

PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

PASQUALE, Frank. Secret algorithms threaten the rule of law. In: **MIT Thecnology Review**, 01 jun. 2017. Disponível em: <https://www.technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law/>. Acesso em: 28 nov.2018.

PASQUALE, Frank. The black box society: the secret algorithms that control money and information. **Harvard University Press**, Cambridge, Massachusetts, 2015.

PASQUALE, Frank. Reputation regulation: disclosure and the challenge of clandestinely commensurating computing. In: LEVMORE, Saul; NUSSBAUM, Martha C.; The offensive internet: speech, privacy, and reputation. Cambridge, MA, **Harvard University Press**, 2010.

PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. In: **Revista Brasileira de Direito Civil** – RBDCivil, Belo Horizonte, v.16, p.35-56, abr.-jun., 2018.

PEREIRA, Agostinho Oli Koppe; SILVA, Fabiana Barcelos da; GIRON, Jerônimo. Sociedade tecnológica: a informação e o consumo como reflexos da modernidade. In: **Novos Estudos Jurídicos**. Itajaí: Fundação Universidade do Vale do Itajaí, n.1, v.19, p.263-284, 2014.

PERELMAN, Chaïm; OLBRECHTS-TYTECA, Lucie. **Tratado da argumentação**: a nova retórica. São Paulo: Martins Fontes, 2005.

PÉREZ LUÑO, Antonio Enrique. **Cibercidadani@ o ciudadani@.com?** Barcelona: Gedisa, 2004.

_____. **Los derechos humanos em la sociedad tecnológica**. Madri: Editorial Universitas, 2012.

_____. La protección de los datos personales de carácter sanitario. In: SÁNCHEZ BRAVO, Álvaro (Ed.). **Derechos humanos y protección de datos personales en el siglo XXI**. Sevilla: Punto Rojo, 2013.

PILATI, José Isaac; OLIVO, Mikhail Vieira Cancelier de. Direito à privacidade: uma nova perspectiva. In: **Revista Novos Estudos Jurídicos (NEJ)**, Itajaí, SC, v.19, n.1, 2014.

PORTER, Michael E.; HEPPELMANN, James E. How smart, connected products are transforming companies. In: **Harvard Business Review**. Out. 2015. Disponível em: <https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies>. Acesso em: 25 jul. 2018.

POSTMAN, Neil. **Technopoly**: the surrender of culture to technology. New York: Vintage Books, 1993.

PRAKKEN, Henry. Artificial intelligence & law, logic and argument schemes. In: HITCHCOK, David; VERHEIJ, Bart. **Arguing on the toulmin model**: new essays in argument analysis and evaluation. Nova Iorque-EUA: Springer, 2006.

PRIVACY IT. **L' Intelligenza artificiale che legge le privacy policy al posto**. Disponível em: <https://www.privacy.it/2018/02/22/intelligenza-artificiale-lettura-privacy-policy/>. Acesso em: 24 dez. 2018.

PROSSER, William L. **Handbook of the law of torts**. St Paul: West, 1955.

_____. Privacy. **California Law Review**, v.48, n.3, ago. 1960.

PROUST, Oliver. Unravelling the mysteries of the GDPR trilogues'. In: **Privacy, security and information law**, 2015. Disponível em: <http://privacylawblog.fieldfisher.com>. Acesso em: 15 nov. 2018.

REMEDIO, José Antonio; SILVA, Marcelo Rodrigues. O uso monopolista do *Big Data* por empresas de aplicativos: políticas públicas para um desenvolvimento sustentável em cidades inteligentes em um cenário de economia criativa e de livre concorrência. **Revista Brasileira de políticas públicas**. Direito e Mundo Digital. Uniceub, v.7, n.3, dez. 2017.

REVISTA Exame. **RGPD**: as primeiras multas devem chegar antes do fim do ano. 10 out. 2018. Disponível em: <http://exameinformatica.sapo.pt/noticias/mercados/2018-10-10-RGPD-as-primeiras-multas-devem-chegar-antes-do-fim-do-ano>. Acesso em: 18 out. 2018.

RHOEN, Michiel; FENG, Qing Yi. Why the 'computer says no': illustrating big data's discrimination risk through complex systems science. **International Data Privacy Law**, v.8, 2.ed. 1 maio 2018, p.140-159. Disponível em: <https://doi.org/10.1093/idpl/ipy005>. Acesso em: 17 out. 2018.

RIBEIRO, Gabriel Francisco; PADRÃO, Márcio. O que é verdade no depoimento de Zuckerberg sobre o Facebook. **UOL**. Publicado em: 12 abr. 2018. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/04/12/uol-confere-o-que-e-verdade-no-depoimento-de-zuckerberg-sobre-o-facebook.htm>. Acesso em: 05 set. 2018.

RINALDI, Camila. **Entidades combatem câmeras do metrô de SP que leem emoções de passageiros para vender publicidade**. Publicado em: 31 ago. 2018. Disponível em: <https://theintercept.com/2018/08/31/metro-cameras-acao-civil/>. Acesso em: 05 set. 2018.

RISSLANDA, Edwina L.; ASHLEYB, Kevin D., LOUIC, R. P. **AI and law**: a fruitful synergy. Disponível em: <http://www.iaail.org/?q=page/ai-law#>. Acesso em: 18 nov. 2018.

RODOTÀ, Stefano. **Il mondo nella rete**. Quali i diritii, quali i vincoli. Roma: Laterza, 2014.

_____. **Il diritto di avere diritti**. Bari/Italia: Laterza, 2012.

_____. **A vida na sociedade da vigilância**: a privacidade hoje. (Org.) Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

_____. Nessuna censura sulla privacy. In: **La Repubblica**, Publicado em: 13 maio 1997. Disponível em: <http://ricerca.repubblica.it>. Acesso em: 03 set. 2018.

ROMAN, Rodrigo; ZHOU, Jianying, LOPEZ, Javier. On the features and challenges of security and privacy in distributed internet of things. **Computer Networks**, v.57, 2013.

ROMM, Tony. The Trump administration is talking to Facebook and Google about potential rules for online privacy. **The Washington Post**, 27 jul. 2018. Disponível em: <https://www.washingtonpost.com>. Acesso em: 02 nov. 2018.

ROSEN, Jeffrey. The purpose of privacy: a response. **Georgetown Law Journal**, v.89. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=283988>. Acesso em: 04 set. 2018.

ROUSSEAU, Jean-Jacques. **Confissões**. Tradução Wilson Lousada. São Paulo: Martin Claret, 2011.

RUBINSTEIN, Ira S. Big data: the end of privacy or a new beginning? **International Data Privacy Law**, v.3, 2.ed. 1 maio 2013, p.74-87. Disponível em: <https://doi.org/10.1093/idpl/ips036>. Acesso em: 18 out. 2018.

SABLICH, Elizabeth. Why protecting privacy is a losing game today – and how to change the game. In: **Brooking**. Disponível em: <https://www.brookings.edu>. Acesso em 02 nov. 2018.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1997.

SANTAELLA, Lucia. **Comunicação ubíqua**: repercussões na cultura e na educação. São Paulo: Paulus, 2013.
_____. **Navegar no ciberespaço**. O perfil cognitivo do leitor imersivo. São Paulo: Paulus, 2004.

SÁNCHEZ BRAVO, Álvaro. **La proteccíon del derecho de la liberdad informática em la Unión Europea**. Universidad de Sevilla: Sevilla, 1998.

SCHAFFNER, Anna Katharina. Exhaustion and the pathologization of modernity. In: **J Med Humanit**. 2016 Sep; 37(3):327-41. doi: 10.1007/s10912-014-9299-z. Disponível em: <https://www.ncbi.nlm.nih.gov/>. Acesso em: 22 ago. 2018.

SCHAUB, Florian; BALEBAKO, Rebecca; DURITY, Adam L.; CRANOR, Lorrie Faith. A design space for effective privacy notices. **Symposium on Usable Privacy and Security (SOUPS)**, Ottawa, Canadá, 2015. Disponível em: <https://www.usenix.org>. Acesso em: 12 nov. 2018.

SCHMIDT, Eric; COHEN, Jared. **The new digital age**. Reshaping the future of people, nations and business, New York: Alfred A. Knopf, 2013.

SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2011.

SCHWABE, Jürgen. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. (Org.) Leonardo Martins. Tradução de Beatriz Hennig, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro, Vivianne Geraldes Ferreira. Berlim-Alemanha: Fundación Konrad-Adenauer-Stiftung, 2005.

SCOTT, Mark. Facebook ordered to stop collecting data on whatsApp users in Germany. In: **The New York Times**. Disponível em: <http://www.nytimes.com/2016/09/28/technology/whatsapp-facebook-germany.html?_r=4>. Acesso em: 30 set. 2016.

SHAAR, O Ben; Chilton, A. Simplification of privacy disclosures: an experimental test' (2016) 45 Journal of Legal Studies S41; Y Bakos and others, 'Does anyone read the fine print? Consumer Attention to Standard-Form Contracts'. **43 Journal of Legal Studies**, 2014.

SIBILIA, Paula. **O homem pós-orgânico**. A alquimia dos corpos e das almas à luz das tecnologias digitais. Rio de Janeiro: Contraponto, 2015.

SILVA, Rosane Leal da. As tecnologias da informação e comunicação e a proteção de dados pessoais. **Anais do XIX Encontro Nacional do CONPEDI**. Fortaleza, 09-12 jun. 2010. Disponível em: <https://s3.amazonaws.com>. Acesso em: 25 ago. 2018.

SILVERSTONE, Ariel; WUNDERLICH, John; PRASOW, Sholem; GRYNWAJC, Stephan. **European Parliament voted to suspend privacy shield**: now what? Disponível em: <https://iapp.org/news/a/european-parliament-voted-to-suspend-privacy-shield-now-what/>. Acesso em: 02 nov. 2018.

SIMITIS, Spiros. Reviewing privacy in an information society. **University of Pensilvania Law Review**, v.135, p.707-746. Pensilvania: University of Pensilvania, 1987. Disponível em: <https://scholarship.law.upenn.edu/>. Acesso em: 27 set. 2018.

SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. **Responsibility and machine learning**: part of a process. Publicado em: 27 out. 2016. Disponível em: <https://ssrn.com/abstract=2860048>. Acesso em: 18 out. 2018.

SOLOVE, Daniel J. **Understanding privacy**. Cambridge, London: Harvard University Press, 2008.

_____. **The digital person**: technology and privacy in the information age. New York University Press: New York, 2004.

_____. A brief history of information privacy law. In: **Proskauer on privacy**, PLI. Washington: George Washington Law Faculty Publications, 2006.

STATISTA. **Statiscs Portal**. Disponível em: <https://www.statista.com>. Acesso em: 28 out. 2018.

STRANDBURG, Katherine J. Monitoring, datafication, and consent: legal approaches to privacy in the big data context. In: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen. **Privacy, big data, and public good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014.

STRECK, Lenio Luiz. Direito *high tech* não encurta orelha de alunos e professores. **Consultor Jurídico**. Publicado em: 23 ago. 2018. Disponível em: <https://www.conjur.com.br/2018-ago-23/senso-incomum-direito-high-tech-nao-encurta-orelha-alunos-professores>. Acesso em: 23 ago. 2018.

SWARTZ, Jon. It's day one of GDPR, and facebook, google are accused of breaking new rules, 25 maio 2018. Disponível em: <https://www.barrons.com/articles/its-day-one-of-gdpr-and-facebook-google-are-accused-of-breaking-new-rules-1527284532>. Acesso em: 24 dez. 2018.

TECNOBLOG. **MP investiga site Tudo sobre Todos que vende seu nome e CPF**. Disponível em: <https://tecnoblog.net/250771/mpdft-investiga-tudo-sobre-todos/>. Acesso em: 24 dez. 2018.

TEIXEIRA, Carlos Alberto. **O Globo**. Revelado: Foi erro no computador Deep Blue da IBM que o fez vencer Kasparov em 1997. Publicado em: 24 out. 2014. Disponível em: <https://oglobo.globo.com/economia/tecnologia/revelado-foi-erro-no-computador-deep-blue-da-ibm-que-fez-vencer-kasparov-em-1997-14349363>. Acesso em: 21 out. 2018.

TENE, Omer. Privacy: the new generations. **International Data Privacy Law**, v.1, n.01, p.15-27, 2011.

_____. Big data for all: privacy and user control in the age of analytics. In: **Northwestern Journal of Technology and Intellectual Property** 239, 20 set. 2012.

TERMS OF SERVICE DIDN'T READ Disponível em: <https://tosdr.org/>. Acesso em: 24 dez. 2018.

THE 25 BEST Inventions of 2017. Publicado em 16 nov. 2017. Disponível em: <http://time.com/5023212/best-inventions-of-2017/>. Acesso em: 21 out. 2018.

THE ATLANTIC. Technology. **Reading the privacy policies you encounter in a year would take 76 work days**. Alexis C. Madrigal. Mar.1, 2012. Disponível em: <https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/>. Acesso em: 24 dez. 2018.

THE ECONOMIST. **The world´s most valuable resource is no longer oil, but data**. Publicado em: 06 maio 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 10 ago. 2018.

THE GUARDIAN. **Police face legal action over use of facial recognition cameras**. Publicado em: 14 jun. 2018. Disponível em: <https://www.theguardian.com/technology/2018/jun/14/police-face-legal-action-over-use-of-facial-recognition-cameras?CMP=Share_iOSApp_Other>. Acesso em: 05 set. 2018.

_____. **Coalition could allow firms to buy access to facial recognition data**. Disponível em: <https://www.theguardian.com/technology/2017/nov/26/government-could-allow-firms-to-buy-access-to-facial-recognition-data?CMP=Share_iOSApp_Other. Acesso em: 07 set. 2018.

_____. **Google says sorry for racist auto-tag in photo app**. Disponível em: <https://www.theguardian.com/technology/2015/jul/01/google-sorry-racist-auto-tag-photo-app>. Acesso em: 25 dez. 2018.

_____. **Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter**. Disponível em: <https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter>. Acesso em: 25 dez. 2018.

THE NEW YORK TIMES. **Facebook ordered to stop collecting data on whatsApp users in Germany**. Disponível em: <http://www.nytimes.com/2016/09/28/technology/whatsapp-facebook-germany.html?_r=4>. Acesso em: 30 set. 2016.

THE OECD PRIVACY FRAMEWORK. Disponível em: <http://www.oecd.org/>. Acesso em: 29 nov. 2018.

THE SEATTLE TIMES. **How LinkedIn's search engine may reflect a gender bias**. Disponível em: <https://www.seattletimes.com/business/microsoft/how-linkedins-search-engine-may-reflect-a-bias/>. Acesso em: 25 dez. 2018.

TI INSIDE ONLINE. **Maioria de apps expõe dados pessoais de usuários**. Disponível em: <http://tiinside.com.br/tiinside/29/08/2018/354288/#.W4grTsOOU0o.linkedin>. Acesso em: 05 set. 2018.

TRUFFI, Renan. Por vaga na OCDE, governo articula criar órgão para proteção de dados na internet. Publicado em: 13 abr. 2018. **O Estado de S. Paulo**. Disponível em: <https://economia.estadao.com.br/noticias/geral,por-vaga-na-ocde-governo-articula-criar-orgao-para-protecao-de-dados-na-internet,70002266200>. Acesso em: 02 nov. 2018.

TUROW, Joseph; HENNESSY, Michael; DRAPER, Nora. **The trade off fallacy**. How marketers are misrepresenting american consumers and opening them up to exploitation. Annenberg School for Communication University of Pennsylvania. Jun. 2015. Disponível em: <https://www.asc.upenn.edu>. Acesso em: 02 nov.2018.

TUTT, Andrew. An FDA for Algorithms. Publicado em: 15 mar. 2016. In: **69 Admin. L. Rev**. 83, 2017. Disponível em: <https://ssrn.com/abstract=2747994>. Acesso em: 18 nov. 2018.

UNITED STATES OF AMERICA. **Federal Trade Commission**. Disponível em: <https://www.ftc.gov/system/files/attachments/press-releases/ftc-issues-warning-letters-app-developers-using-silverpush-code/160317samplesilverpushltr.pdf>. Acesso em: 07 nov. 2016.

UNITED STATES Government Accountability Office (GAO). **Internet of things**, maio 2017. Disponível em: <http://www.gao.gov/assets/690/684590.pdf>. Acesso em: 22 out. 2018.

U.S. **Department of Commerce**. Disponível em: <https://www.commerce.gov/news/press-releases/2018/10/joint-press-statement-commissioner-vera-jourova-and-secretary-commerce>. Acesso em: 05 nov. 2018.

VEIGA, Luiz Adolfo Olsen da; ROVER, Aires J. Dados e informações na internet: é legítimo o uso de robôs para a formação de base de dados de clientes? In: ROVER, Aires José (Org.). **Direito e informática**. São Paulo: Monole, 2004. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/luizvaires-livro_aires.pdf>. Acesso em: 25 ago. 2018.

VEROSTKO, Roman. **Algorithmic art**. Disponível em: <http://verostko.com/algorithm.html>. Acesso em: 26 ago. 2018.

VESTING, Thomas. **Teoria do direito**. São Paulo: Saraiva, 2015.

_____. The autonomy of law and the formation of network standards. In: **German Law Journal**, n.6, 2004.

VIRILIO, Paul. **O espaço crítico**. Tradução de Paulo Roberto Pires da edição de 1984. São Paulo: Editora 34, 2014.

_____; LOTRINGER, Sylvère. **The accidente of art**. Tradução de Mike Taormina. Nova Iorque: 2005.

WAKABAYASHI, Daisuke. California passes sweeping law to protect online privacy image, June 28, 2018. **The New York Times**. Disponível em: <https://www.nytimes.com/>. Acesso em: 02 nov. 2018.

WARAT, Luis Alberto. **A ciência jurídica e seus dois maridos**. Santa Cruz do Sul: EDUNISC, 2000.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v.IV, n.5, 1890.

WATERMAN, K. Krasnow; BRUENING Paula J. Big Data analytics: risks and responsabilities. **International Data Privacy Law**, v.4, 2.ed. maio 2014. Disponível em: <https://doi.org/10.1093/idpl/ipu002>. Acesso em: 22 out. 2018.

WESTIN, Allan. **Privacy and freedom**. New York: Atheneum, 1970.

_____. **Privacy and freedom**. New York: Atheneum, 1968.

WHIGHAM, Nick. **Leaked document reveals Facebook conducted research to target emotionally vulnerable and insecure youth**. Publicado em: 01 maio 2017. Disponível em: <https://www.news.com.au/technology/online/social/leaked-document-reveals-facebook-conducted-research-to-target-emotionally-vulnerable-and-insecure-youth/news-story/d256f850be6b1c8a21aec6e32dae16fd>. Acesso em: 23 out. 2018.

WIENER, Norbert. **Cibernética e sociedade**. O uso humano dos seres humanos. 2.ed. Tradução de José Paulo Paes. São Paulo: Cultrix, 1968.

WILSON, Jenny. **Revista Time**. Want to steal a hotel towel? Checking for a new tracking chip first. Disponível em: <http://newsfeed.time.com/2011/04/18/want-to-steal-a-hotel-towel-check-for-a-new-tracking-chip-first/>. Acesso em: 25 ago. 2018.

WIRED. **How to block the ultrasonic signals you didn't know were tracking you**. Disponível em: <https://www.wired.com/2016/11/block-ultrasonic-signals-didnt-know-tracking/?utm_content=buffer29d74&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer>. Acesso em: 07 nov. 2016.

WIRED. **Airbnb introduces anti-discrimination rules to clamp down on bigoted hosts**. Disponível em: <https://www.wired.co.uk/article/airbnb-new-anti-discrimination-rules>. Acesso em: 24 dez. 2018.

WP29 240 – Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC). Disponível em: <https://ec.europa.eu/>. Acesso em: 29 nov. 2018.

YU, Howard. GDPR isn’t enough to protect us in an age of smart algorithms. **The Conversation**, 29 maio 2018. Disponível em: <https://theconversation.com/gdpr-isnt-enough-to-protect-us-in-an-age-of-smart-algorithms-97389>. Acesso em: 01 dez. 2018.

ZIMMERMANN, Reinhard. **The law of obligations**. Oxford, New York, 1996.

Referências normativas
(Associação Brasileira de Normas Técnicas – ABNT)

ABNT NBR 6022: 2018 – Informação e documentação – Artigo em publicação periódica técnica e/ou científica – Apresentação

ABNT NBR 6027: 2012 – Informação e documentação – Informação e documentação – Sumário – Apresentação

ABNT NBR 14724: 2011 – Informação e documentação – Trabalhos acadêmicos – Apresentação

ABNT NBR 15287: 2011 – Informação e documentação – Projetos de pesquisa – Apresentação

ABNT NBR 6034: 2005 – Informação e documentação – Índice – Apresentação

ABNT NBR 12225: 2004 – Informação e documentação – Lombada – Apresentação

ABNT NBR 6024: 2003 – Informação e documentação – Numeração progressiva das seções de um documento escrito – Apresentação

ABNT NBR 6028: 2003 – Informação e documentação – Resumo – Apresentação

ABNT NBR 10520: 2002 – Informação e documentação – Citações em documentos – Apresentação

ABNT NBR 6023: 2002 – Informação e documentação – Referências – Elaboração