

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ
ESCOLA DE DIREITO
PROGRAMA DE PÓS GRADUAÇÃO EM DIREITO

GIOVANNA MICHELATO ALMADA

NUDGING DATA PROTECTION: O PATERNALISMO LIBERTÁRIO APLICADO À
PROTEÇÃO DOS DADOS PESSOAIS NA INTERNET

CURITIBA

2020

GIOVANNA MICHELATO ALMADA

***NUDGING DATA PROTECTION: O PATERNALISMO LIBERTÁRIO APLICADO À
PROTEÇÃO DOS DADOS PESSOAIS NA INTERNET***

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná, área de concentração de Direito Socioambiental, linha de pesquisa Estado, Sociedades e Meio Ambiente, como requisito parcial para obtenção do título de Mestre em Direito.

Orientadora: Prof^a. Dr^a. Cinthia Obladen de Almendra Freitas.

CURITIBA

2020

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central
Pamela Travassos de Freitas – CRB 9/1960

A444n
2020 Almada, Giovanna Michelato
Nudging data protection : o paternalismo libertário aplicado à proteção dos dados pessoais na internet / Giovanna Michelato Almada ; orientadora: Cinthia Obladen de Almendra Freitas. – 2020.
100 f. : il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná,
Curitiba, 2020
Bibliografia: f. 94-101

1. Direito à privacidade. 2. Direito e informática. 3. Economia do mercado.
4. Internet-Medidas de segurança. 5. Paternalismo. 6. Proteção de dados.
7. Sociedades civis. 8. Sociedade da informação. 9. Tecnologia da informação.
I. Freitas, Cinthia Obladen de Almendra. II. Pontifícia Universidade Católica
do Paraná. Pós-Graduação em Direito. III. Título.

CDD 20. ed. – 341.2738

GIOVANNA MICHELTO ALMADA

***NUDGING DATA PROTECTION: O PATERNALISMO LIBERTÁRIO APLICADO À
PROTEÇÃO DOS DADOS PESSOAIS NA INTERNET***

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná, área de concentração de Direito Socioambiental, como requisito parcial para obtenção do título de Mestre em Direito.

COMISSÃO EXAMINADORA

Prof^a. Dr^a. Cinthia O. A. Freitas
Pontifícia Universidade Católica do Paraná

Prof^a. Dr^a. Danielle Anne Pamplona
Pontifícia Universidade Católica do Paraná

Prof. Dr. Vinícius Borges Fortes
IMED-RS

Curitiba, 27 de março de 2020.

Para o meu avô. Aquele que sempre cuidou de
mim e, agora, me acompanha até quando estou
sozinha.

Te amo e sinto sua falta.

AGRADECIMENTOS

Agradeço a todos que me acompanharam e me deram forças nesses últimos anos. Ainda que essa dissertação tenha meu nome na capa e horas e horas de pesquisa solitária, ela é resultado de relações que construí ao longo da minha vida. Talvez, aqui está a parte mais importante dela, já que é um pedacinho de todo o carinho, suporte e amor que recebi e recebo de vocês.

À Nicole que me deu todo o apoio possível (e impossível), mesmo de longe, acreditando em mim mesmo quando eu não achei que conseguiria. Você é a pessoa mais importante do mundo, para sempre.

Agradeço à minha mãe, uma psicanalista que criou uma filha que estuda ciências comportamentais. Eu tenho certeza que Freud também deve explicar isso.

À minha avó, uma fortaleza que se provou mais forte do que nunca. Seu amor, carinho e cuidado alegre e esquentam o meu coração! À Carla, por ser essa tia e madrinha tão dedicada, preocupada e participativa. Você sabe o quanto eu sou grata por te ter por perto. Thank you, uncle Rumi. You are a father to me, and I am so grateful for having you in my life. You can be sure that you and your career have a huge influence on this work. I love you a lot!

Agradeço ao Douglas Picussa (e família) por ter esse coração imenso e sinceridade em todas as palavras. Por pegar na minha mão quando eu precisei, me mostrar o caminho quando eu estava perdida e sempre ser tão bondoso comigo.

Às minhas amigas que estão comigo há mais de 15 anos e entenderam minhas ausências, meu cansaço, meu espaço e meu jeitinho. Ana Beatriz Alves, Catherine Glok, Dainah Rocha, Giovanna DePauli, Isabella Camargo e Mariana Barth. O amor é sempre o mesmo.

Agradeço o meu melhor amigo, André Enrique Lubascher, por estar do meu lado e sempre me lembrar sempre que nada é impossível, que sou forte o suficiente e vou conseguir. Meu coração transborda amor e gratidão por você.

Àqueles que me fizeram companhia nesses dois turbulentos anos. André Vaccari, Ana Luiza Fang, Otávio Socachewsky, Eduardo Venturi, Felipe Assahida, Kiyu Matsugaki, Henrique Albuquerque, Larissa von Biveniczko, Daniel Rocha, Matheus Casagrande e Alexandre Precoma. Vocês me ajudaram a respirar e sair de casa quando estava cansada, me acolheram e me entenderam quando estive mais triste, e me fizeram rir (e fazem) quando eu mais precisei. E é claro, Guilherme Reis Bonfim que esteve do meu lado, dividiu os melhores e piores momentos (com seus respectivos pesos), conheceu um pedacinho mundo comigo, me

fez dançar mesmo quando eu não conseguia, me fez rir das situações mais difíceis e sempre, mas sempre mesmo, sempre acreditou em mim. Vocês pisam!

Agradeço ao Jonathan Nassur. Por ser o mestre e amigo que eu não esperava encontrar. Por me ensinar tanto. Por ser a luz quando eu mais precisei. Por ser minha inspiração. Por ser quem você é. Repito mais uma vez: é muito orgulho ser sua cria. E Natália Macedo, por estar por perto. Por acreditar no meu potencial e sempre oferecer ajuda.

À minha querida equipe do Baril que se tornou a minha família e me deu forças no momento mais difícil, me trouxe tanta alegria. Alysson Oikawa, por me inspirar. Mariana Chacur, por me acolher. Maikon Oliveira, por me fazer forte. Paula Belotto, pela sinceridade e cumplicidade. Yasmin Schultz, pela gentileza e pelas risadas. Anabelle Meira, pelo carinho e pela proteção. Raissa de Barros, por me fazer rir e não parar de dançar um minuto. Luca Schirru, pelo suporte, companhia e empatia. E Natan, por me permitir fazer parte de tudo isso.

Agradeço ao CGI.br que acreditou e acredita em jovens como eu, dando espaço e força para crescermos no ecossistema da Governança da Internet. Especialmente, agradeço com todo o meu coração ao Tiago Tavares e Nathalia Sautchuk por conduzirem o programa dos Youths com tanto amor e dedicação. Sem vocês, eu não teria nem 10% da bagagem que eu tenho. O impacto das ações de vocês é gigante. Mudam vidas. E, também, à *Internet Society* por me dar oportunidades únicas que me mantiveram ativa e engajada na GI.

Aos meus amigos de Governança que dividiram angústias e aflições, me lembraram diversas vezes que eu não deveria ser tão dura comigo mesma e que é necessário parar e respirar. Obrigada pelas discussões de alto nível e por todo o conhecimento compartilhado.

Agradeço a todos meus amigos de mestrado, mas, especialmente, ao Lucas Saikali que escutou mais que ninguém as minhas angústias e sempre me entendeu. É muito gratificante poder dividir isso com você.

À Coordenação de Aperfeiçoamento de Pessoal do Ensino Superior – CAPES, pela bolsa de estudos. Sem ela não seria possível ter continuado com a minha pesquisa.

À Prof. Dra. Cinthia Obladen de Almendra Freitas. Agradeço a orientação que transcendeu à uma orientação de como conduzir uma pesquisa. Ter uma orientadora tão empática fez toda a diferença nesses dois anos difíceis.

E, obrigada aos professores do Data Privacy Brasil, Renato Leite Monteiro, Maria Cecília Oliveira Gome, Rafael Zanatta e, especialmente, ao Bruno Bioni, cujo trabalho serviu como base para essa dissertação. Vocês me ensinaram tanto em 2 meses e me fizeram ter mais certeza que esse trabalho não está pronto – e agora eu conviverei diariamente com a ansiedade da dissertação inacabada!

"Todos tenemos tres vidas, una vida pública, una vida privada y una vida secreta".
Gabriel García Márquez

RESUMO

A Sociedade de Informação, estruturada em torno da coleta e tratamento de dados pessoais impulsionou não só o desenvolvimento tecnológico, mas, também discussões quanto à violação da privacidade e à necessidade de proteção de dados pessoais. A premissa inicial é de que o direito fundamental à privacidade vem sendo desafiado pelo Poder Público e Privado, especialmente no que tange à proteção de dados pessoais na *Internet*. Ainda que exista consentimento ou que dados sejam transferidos a terceiros por iniciativa do usuário, as trocas nem sempre são reflexo de um processo de tomada de decisão consciente, o que pode ser prejudicial às garantias e aos direitos fundamentais. Nesse sentido, o objetivo da pesquisa foi verificar se os *nudges* (empurrões), a partir do Paternalismo Libertário, são uma solução para diminuir as “decisões ruins” que os usuários da *Internet* fazem com relação à proteção de seus dados pessoais. Para o desenvolvimento da pesquisa, utilizou-se o método dedutivo, uma vez que se desenhou a aplicação dos *nudges* do Paternalismo Libertário na privacidade e proteção de dados na *Internet*. Para verificar tal hipótese, a pesquisa foi dividida em três partes. A primeira buscou identificar em qual contexto a proteção de dados está inserida na Sociedade Informacional, desde a privacidade até a proteção de dados. Apresentaram-se os conceitos básicos, como o de privacidade, informação e dado. Na sequência, foi descrito o Paternalismo Libertário e seus *nudges*, com sua forma de emprego, seus benefícios e as críticas feitas à teoria. Na terceira e última parte, foi analisado como “empurrões” podem ser empregados na proteção de dados pessoais. Para tanto, aprofundou-se o estudo sobre Economia da Privacidade, a qual tem seu foco em estudos justamente nos *trade-offs* (trocas) que os usuários da *Internet* fazem entre seus direitos e o uso de produtos/serviços. Com isso, o estudo verificou que algumas políticas públicas e privadas para a proteção de dados podem ser consideradas *nudges* e auxiliam sim no processo de tomada de decisão do usuário na *Internet*. No entanto, algo que aparentemente seria um “empurrão” para guiar o usuário a fazer uma boa escolha, pode ser ter sido desenhado para influenciar diretamente no processo de escolha, diminuindo a liberdade do indivíduo. Finalmente, conclui-se que os *nudges* são, de forma geral, uma solução para a proteção dos usuários da *Internet*, principalmente porque os usuários não possuem, em sua grande maioria, informações técnicas suficientes e não mensuram com precisão o preço real das trocas (*trade-offs*) que realizam ao utilizar, por exemplo, redes sociais.

Palavras-chave: Sociedades. Novas Tecnologias. Proteção de Dados Pessoais. Economia da Privacidade. Economia Comportamental.

ABSTRACT

The Informational Society, which is structured around the collection and treatment of personal data, has boosted not only technological development but also discussions regarding the violation of privacy and the necessity of protecting personal data. The initial premise is that the fundamental right to privacy has been challenged by public and private authorities, especially regarding the protection of personal data on the Internet. Even if there is consent or if the data is transferred to third parties by the user's initiative, exchanges are not always a reflection of a conscious decision-making process, which can be harmful to fundamental rights and guarantees. In this sense, the objective of the research was to verify whether the nudges from the Theory of Libertarian Paternalism are a solution to reduce the 'bad decisions' that Internet users make when it comes to protecting their data. For the research development, the method used to draw an application of the nudges was the deductive method. The research was divided into three parts. The first sought to identify in what context data protection is in the Information Society, beginning from the privacy theories to data protection theories. Some fundamental concepts were presented, such as privacy, information, and data. Sequentially, Libertarian Paternalism and its nudges were described, with their form of employment, their benefits, and the criticisms suffered. In the third and last part, it was analyzed how the nudges may be used to protect personal data. To this end, the study on Privacy Economics was deepened, focusing on studies of the trade-offs (exchanges) between their rights and the use of products/services made by Internet users. Thus, the study found that some public and private policies for data protection can be considered nudges and do assist in the user's decision-making process on the Internet. However, something that apparently would be a nudge to guide the user to make the right choice may have been designed to directly influence the choice process, decreasing the individual's freedom. Finally, the research conclusion was that nudges are, in general, a solution for the protection of Internet users. It is a solution mainly because the vast majority of users do not have sufficient technical information and do not accurately measure the real price of the trade-offs they perform when using, for example, social networks.

Keywords: Societies. New technologies. Personal Data Protection. Economics of Privacy. Behavioral Economics.

LISTA DE FIGURAS

Figura 1 - Diagrama de Venn	46
Figura 2 - Tela notificação de dados de localização da Apple	72

LISTA DE TABELAS

Tabela 1 - Conceito dos vieses da heurística da representatividade	39
Tabela 2 - Exemplo dos vieses da heurística da representatividade	40
Tabela 3 - Vieses da heurística da disponibilidade.....	43
Tabela 4 - Descrição dos tipos de evento	45
Tabela 5 - Categorias de nudges	50

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
Artigo	Art.
Artigos	Arts.
GDPR	<i>General Data Protection Regulation</i>
ISBN	<i>International Standard Book Number</i>
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PETs	<i>Privacy Enhancing Technologie</i>
PUCPR	Pontifícia Universidade Católica do Paraná
TI	Tecnologia da Informação
TIC	Tecnologia de Informação e Comunicação
TICs	Tecnologias de Informação e Comunicação

SUMÁRIO

1	INTRODUÇÃO.....	14
2	A PROTEÇÃO DE DADOS PESSOAIS NA <i>INTERNET</i> NO CONTEXTO DA SOCIEDADE INFORMACIONAL.....	17
2.1	DADO E INFORMAÇÃO	18
2.2	DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS NA <i>INTERNET</i>	20
2.3	SOCIEDADE INFORMACIONAL: OS DADOS E A <i>INTERNET</i>	26
2.4	DADOS PESSOAIS: DE DIREITO À ATIVO	29
3	PATERNALISMO LIBERTÁRIO, <i>NUDGES</i> E O PROCESSO DE ESCOLHA DOS USUÁRIOS	37
3.1	HEURÍSTICAS E VIÉSES	38
3.1.1	A heurística da representatividade	38
3.1.2	A heurística da disponibilidade.....	42
3.1.3	A heurística dos ajustes e ancoragem	44
3.1.4	Outros vieses.....	46
3.2	O PATERNALISMO LIBERTÁRIO DE THALES E SUNSTEIN	47
3.2.1	Os <i>nudges</i>	48
3.2.2	As críticas ao Paternalismo Libertário e aos <i>nudges</i>	51
4	A ECONOMIA DA PRIVACIDADE, OS <i>NUDGES</i> E A PROTEÇÃO DE DADOS PESSOAIS NA <i>INTERNET</i>	54
4.1	PROCESSO DE DECISÃO E ESCOLHA DO USUÁRIO NA <i>INTERNET</i>	58
4.1.1	Os <i>trade-offs</i>	63
4.1.2	A incerteza dos usuários	64
4.1.3	As heurísticas e vieses no processo de proteção à privacidade e aos dados pessoais..	67
4.2	OS <i>NUDGES</i> NA PRIVACIDADE E NA PROTEÇÃO DE DADOS PESSOAIS NA <i>INTERNET</i>	69
4.2.1	A dimensão da Informação e os <i>nudges</i>	70
4.2.2	A dimensão da Apresentação e os <i>nudges</i>	73
4.2.3	A dimensão dos Padrões e os <i>nudges</i>	75
4.2.4	A dimensão dos Incentivos e os <i>nudges</i>	80
4.2.5	A dimensão da Reversibilidade (<i>resiliência aos erro</i>)	81
4.2.6	A dimensão do <i>Timing</i> e os <i>nudges</i>	82

4.3	NUDGES NA PRÁTICA: EMPURRÃO PARA A ESCOLHA CERTA OU PATERNALISMO EXACERBADO?	83
4.4	QUEM DEVE DESENHAR OS <i>NUDGES</i> ?.....	87
5	CONCLUSÃO	91
	REFERÊNCIAS	94

1 INTRODUÇÃO

Seres humanos são seres de hábitos. Hábitos que, quando repetidos, transformam-se em padrões. Esses padrões são dissecados e estudados e, conseqüentemente, é possível prever novos comportamentos. Esse é objeto de estudo das ciências comportamentais que tentam entender o comportamento, as decisões dos indivíduos, e se essas escolhas são feitas com base em vieses ou escolhas (ir)racionais.

Thaler e Sunstein¹ expõem que a fragilidade das escolhas “falhas” dos seres humanos é reflexo de limitações cognitivas, vieses ou hábitos. Como solução a essas falhas, tais autores entendem que as pessoas precisam de *nudges* para serem guiados a uma escolha certa.

Esses *nudges* podem ser conceituados como uma sugestão indireta que influem positivamente no processo de tomada de decisões, devendo promover políticas públicas mais efetivas, reduzindo os custos governamentais que uma escolha ruim pode criar.² Eles têm sua origem na ciência behavioristas e podem ser aplicados em diversas áreas, da ciência política até psicologia e, no presente estudo, nos desafios relacionados à privacidade e à proteção dados pessoais.

Cientistas sociais presumem que as pessoas possuem um entendimento pessoal quanto à questão da privacidade e, de acordo com este entendimento, realizam trocas entre sua privacidade e outros objetivos. Contudo, Acquisti³ entende que essa lógica não é precisa, uma vez que os seres humanos não fazem escolhas tão boas quanto acreditam.

As escolhas atinentes à privacidade muitas vezes envolvem o balanço entre o controle do que é compartilhado e os custos e benefícios deste compartilhamento ou omissão de informações. Assim, torna-se necessário o estudo desses *trade-offs*, de modo a entender e até quantificar os custos e os benefício que indivíduo titular destes se sujeita ou aproveita quando esses dados pessoais são mantidos em segredo e quando são compartilhados.⁴

Ainda, entende-se que os usuários possuem vaga e limitada informação no que tange às ações que podem tomar para proteger seus dados. Logo, possuem um conhecimento restrito sobre quem é aquele que coleta seus dados, assim como e para o quê os utilizam.

¹ SUNSTEIN, C. R.; THALER, R. H. Libertarian Paternalism Is not an Oxymoron. **University of Chicago Law Review**, v. 70, n. 40, p. 1159–1202, 2003.

² IGLESIAS, D. **Nudging Privacy**: benefits and limits of persuading human behaviour online, 2017. Disponível em: <<https://itsrio.org/wp-content/uploads/2017/03/Daphnee-Iglesias-.doc-B.pdf>>. Acesso em: 20 jan. 2020.

³ ACQUISTI, A. Nudging Privacy: The Behavioral Economics of Personal Information. **IEEE Security & Privacy Magazine**, s.l., v. 7, n. 6, p. 72-85, novembro 2009.

⁴ ACQUISTI, A. Nudging Privacy: The Behavioral Economics of Personal Information. **IEEE Security & Privacy Magazine**, s.l., v. 7, n. 6, p. 72-85, nov 2009.

Como resposta a esse problema, o Paternalismo Libertário poderia assegurar a proteção dos usuários da Internet, no qual os *nudges* se inserem. Segundo Thaler e Sunsteins, o Paternalismo Libertário é uma versão branda do Paternalismo. Sendo, então, “[...] an approach that preserves freedom of choice but authorizes both private and public institutions to steer people in directions that will promote their welfare”⁶. Segundo Acquist *et al.*⁷, o Paternalismo Libertário, por meio dos *nudges*, pode ser empregado como solução para garantir a privacidade e a proteção de dados dos usuários da *Internet*.

Assim, a pesquisa buscou responder se o os *nudges*, do Paternalismo Libertário, são uma solução para diminuir as “decisões ruins” que os usuários da *Internet* fazem no que tange à proteção de seus dados pessoais. Tal ideia parte, em sua origem, do entendimento de que o processo de tomada de decisão é racional, no qual os indivíduos objetivam maximizar a utilidade de suas preferências.⁸

A hipótese básica verificada é de que o Paternalismo Libertário pode ser utilizado como ferramenta para “empurrar” as pessoas para a escolha mais benéfica aos interesses dos usuários da *Internet* quanto à proteção dos direitos de privacidade e à proteção de seus dados pessoais.

O objetivo desta dissertação, então, foi verificar a possibilidade de o Paternalismo Libertário, por meio dos *nudges*, auxiliar os usuários da *Internet* no processo de tomada de decisão quanto à proteção de direitos de privacidade e à proteção de dados pessoais na *Internet*. Para tanto, os objetivos específicos foram (i) análise de *trade-offs* feitos em detrimento da utilização de tecnologia, sob a ótica da Sociedade Informacional; (ii) entender como os *nudges* auxiliam no processo de decisão; e, conseqüentemente, (iii) como esses *nudges* poderiam ser inseridos na proteção dos direitos de privacidade e na proteção de dados na *Internet*.

Para tanto, foi adotado o método dedutivo, para se desenhar a aplicação dos *nudges* do Paternalismo Libertário na proteção dos direitos de privacidade e na proteção de dados na sociedade regida por algoritmos. O procedimento de pesquisa foi o monográfico, utilizando-se da pesquisa bibliográfica e documental, tanto para o estudo do processo de escolha dos *trade-offs*, quanto da teoria do Paternalismo Libertário.

⁵ SUNSTEIN, C. R.; THALER, R. H. Libertarian Paternalism Is not an Oxymoron. **University of Chicago Law Review**, v. 70, n. 40, p. 1159–1202, 2003.

⁶ Tradução livre “[...] uma abordagem que preserva a liberdade de escolha, mas autoriza instituições privadas e públicas a orientar as pessoas em direções que promoverão seu bem-estar.”

⁷ ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and human behavior in the age of information. **Science** **347** (6221), 509-514., New York, v. 347, n. 6221, p. 509-514, 2017. ISSN 1095-9203.

⁸ ACQUISTI, A.; TAYLOR, C.; WAGMAN, L. The Economics of Privacy. **Journal of Economic Literature**, v. 54, n. 2, p. 442-492, 2016.

O estudo e seus resultados estão divididos em três partes. A primeira parte é dedicada a identificar o contexto em que a proteção de dados está inserida na Sociedade Informacional, partindo da ideia de privacidade e de seu desenvolvimento ao longo do tempo, até chegar na proteção de dados na *Internet*. Conseqüentemente, demonstram-se as transformações que a própria Sociedade Informacional ocasionou, apresentando a visão de dados pessoais como direito a ser protegido e ativo econômico a ser explorado.

A segunda parte tem como objetivo apresentar o paternalismo libertário e seus *nudges*. Para isso, explica-se o processo de escolha dos indivíduos, com suas diversas heurísticas e seus vieses.

Na terceira e última parte, analisou-se como os *nudges* podem ser empregados na proteção de dados pessoais. Para tanto, aprofundou-se o estudo sobre Economia da Privacidade, a qual tem seu foco em estudos justamente nos *trade-offs* que os usuários da *Internet* fazem entre seus direitos e o uso de produtos/serviços, e a incerteza que os usuários possuem sobre suas preferências e ações. Conseqüentemente, descobriu-se que as heurísticas anteriormente citadas também se encontram no âmbito dessas escolhas. Em seguida, o estudo tratou de buscar *nudges* já existentes na proteção de dados pessoais na *Internet*, incluindo políticas públicas e privadas que auxiliam sim no processo de tomada de decisão do usuário na *Internet*.

Esta dissertação delinea como o usuário da *Internet* pode usufruir delas de maneira integral, sem que seus direitos e garantias sejam violados, visto que o trabalho tem por premissa que, quando o uso está condicionado à diminuição de um direito ou liberdade, o propósito da *Internet* se perde.

Como contribuição, desenha-se um panorama de como pequenas interferências sociais, que forneçam conhecimento, capacidade de escolha e diminuam a assimetria informacional, podem melhorar o uso e desenvolvimento da *Internet*, mantendo, ainda, a universalidade, abertura e descentralização da *Web*.

2 A PROTEÇÃO DE DADOS PESSOAIS NA *INTERNET* NO CONTEXTO DA SOCIEDADE INFORMACIONAL

A sociedade sempre se organizou em torno de um elemento central de seu desenvolvimento que serviram como estrutura para definir os marcos históricos. Durante a sociedade agrícola, organizavam-se em torno da terra, a fonte de riquezas. Na era industrial, as protagonistas eram máquinas a vapor e a eletricidade que moviam as indústrias e geravam, assim, riquezas. Após a Segunda Guerra Mundial, a sociedade se modificou, tornando a prestação de serviços “a mola propulsora da economia”.⁹⁻¹⁰

Já no final século do século XX e no século XXI, uma nova transformação social ocorreu, colocando a informação como fonte do desenvolvimento econômico. Como fonte da produtividade está a tecnologia de geração de conhecimento, de processamento e de comunicação. O processamento das informações e grande impulsor dessa revolução foi o desenvolvimento tecnológico, que proporcionou a coleta, o tratamento e a transmissão de informações ultrapassando barreiras geográficas e temporais.¹¹⁻¹²

Essa mudança é motivo de preocupação para Alec Ross¹³, mais especificamente no que tange ao gerenciamento e à administração de dados na atualidade. Segundo o autor, decisões relacionadas a como os dados serão gerenciados, serão tão importantes quanto aquelas decisões tomadas sobre a administração da terra durante a era agrícola, ou aquelas sobre a administração industrial durante a era industrial.

O sistema de organização de uma sociedade sempre dependeu da coleta e do tratamento de informações como forma de organização e controle da própria história, das relações sociais e de seus indivíduos. Durante a história, o principal agente de tratamento de dados foi o Estado, justamente porque para uma administração pública ser eficiente se presume o conhecimento sobre a população.^{14,15}

⁹ BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 3.

¹⁰ CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016.

¹¹ BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 3.

¹² CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016

¹³ ROSS, A. **The Industries of the Future**. New York: Simon & Schuster, 2016.

¹⁴ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2 ed. São Paulo: Thomson Reuters Brasil, 2019. p. 33

¹⁵ GARFINKEL, S. **Database Nation: The Death of Privacy in the 21st Century**. Sebastopol: O'Reilly Media, 2000.

O avanço da tecnologia permitiu que a coleta, o armazenamento e o tratamento de dados tomassem uma escala muito maior do que apenas o registro do Estado. A transformação das economias modernas em torno da produção de conhecimento e o grande avanço das tecnologias da informação (TI), influenciou diretamente na quantidade de dados coletados, armazenados e tratados. O avanço das Tecnologias de Informação e Comunicação (TICs), por sua vez, tornou a coleta de dados escalável de forma a atingir qualquer um, sendo possível a sua comercialização.^{16,17,18}

O direito ao respeito da vida privada está em um componente individual, impedindo a interferência na esfera privada de alguém, a proteção estática e negativa. A proteção de dados pessoais, em contraste, “estabelece regras sobre os mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas”.¹⁹

Por esse ponto de vista, a proteção de dados pode se constituir em direito fundamental autônomo, o que o torna indispensável para o desenvolvimento da personalidade. Devido a esse fato, esse “novo direito” pode ser entendido como um conjunto de direitos essenciais que formam a cidadania do novo milênio.²⁰

2.1 DADO E INFORMAÇÃO

Inicialmente, é necessário destacar que dado e informação, ainda que pareçam e sejam utilizados como sinônimo, possuem diferentes definições.²¹ “Dados” possuem diversos significados e são empregados de diferentes formas – assim como acontece com a palavra “privacidade”. Eles podem ser quantitativos ou qualitativos; estruturados, semi-estruturados, ou não-estruturados; de origem primária, secundária ou terciária; capturados, derivados, ou

¹⁶ BOLZAN, J. L.; NETO, E. J. D. M. A Insuficiência do Marco Civil da Internet na Proteção das Comunicações Privadas Armazenadas e do Fluxo de Dados a Partir do Paradigma de Surveillance. In: GEORGE SALOMÃO LEITE, R. L. **Marco Civil da Internet**. São Paulo: Atlas, 2014.

¹⁷ GOLDFARB, A.; TUCKER, C. Privacy and Innovation. **Innovation Policy and the Economy**, v. 12, p. 65–90, 2012.

¹⁸ BRANDIMARTE, L.; ACQUISTI, A. The Economics of Privacy, p. 547-571, 2012. Disponível em: <<http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780195397840.001.0001/oxfordhb>>. Acesso em: 22 dez. 2019.

¹⁹ RODOTÀ, S. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008. p. 17

²⁰ BOFF, S. O.; FORTES, Vinicius B.; FREITAS, Cinthia Obladen D. A. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2018. pp. 71-72

²¹ “Em relação à utilização dos termos ‘dado’ e ‘informação’, é necessário notar preliminarmente que o conteúdo de ambos se sobrepõe em várias circunstâncias, o que justifica uma certa promiscuidade na sua utilização. Ambos os termos servem a representar um fato, um determinado aspecto de uma realidade. [...]” DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 136

transitórios; e de diversos tipos, indexais, atributos ou metadados.²² No entanto, essas classificações não são objeto deste estudo, mas sim seu conceito dentro do contexto da Sociedade Informacional e, mais especificamente, da *Internet*.

O primeiro pode ser visto como uma pré-informação, já que é com o seu tratamento que se transforma em uma informação.^{23;24} Assim, como exposto por Bruno Bioni²⁵, “[o] dado é o estado primitivo da informação, pois não é algo *per se* que acresce conhecimento”. São desorganizados, aleatórios, simples e abstratos. Por ter essas características, os dados sozinhos, sem contexto, podem não fazer muito sentido.

A Lei Geral de Proteção de Dados (LGPD)²⁶, por sua vez, apresenta o conceito de três tipos de dados:

Art. 5º Para os fins desta Lei, considera-se:

- I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
- II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; [...]²⁷

Em contrapartida, informação é “algo além da representação contida no dado, chegando ao limiar da cognição”²⁸. Ou seja, são dados organizados, interpretados por um certo processo, transformando-se em material útil. Tornam-se informação quando são aplicados para um determinado propósito, adicionando valor para o analista desta informação.²⁹

²² BOFF, S. O.; FORTES, Vinicius B.; FREITAS, Cinthia Obladen D. A. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2018. p. 202.

²³ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 33

²⁴ MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

²⁵ BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 36.

²⁶ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. **Diário Oficial**, Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 20 jan. 2020.

²⁷ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. **Diário Oficial**, Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 20 jan. 2020.

²⁸ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 136

²⁹ SANDERS, J. Defining Terms: Data, Information and Knowledge. **SAI Computing Conference**, London, n. July, p. 13-15, 2016 2016. Disponível em: <<https://searchdatamanagement.techtarget.com/feature/Defining-data-information-and-knowledge>>. Acesso em: 20 jan. 2020.

Esses conceitos podem ser ilustrados como um quebra cabeça. Os dados seriam várias peças individuais de um quebra-cabeça espalhadas desordenadamente. Ainda que não seja possível ter certeza de qual será a imagem a ser formada, sem consultar a embalagem, pode-se ter uma ideia do todo. Então, os dados são um quebra-cabeça não resolvido. Em contrapartida, o quebra-cabeça já organizado, montado, revelando sua imagem completa seria a informação.

A proteção dos dados pessoais se torna essencial na Sociedade Informacional, tendo em vista o poder de tratamento e transformação destes em informações. A violação do direito à privacidade tornou-se mais facilitada, como se verá adiante.

2.2 DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS NA *INTERNET*

A doutrina moderna do direito à privacidade, considerando o artigo *The right to privacy* de Samuel Warren e Louis Brandeis (1890)³⁰ como ponto inicial, vem modificando e adaptando o conceito de privacidade. Segundo os autores, esse direito seria "the right to be left alone"³¹, o que implica diretamente o caráter da autonomia individual em decidir o que é de conhecimento público e o que não é.

A ideia de privacidade como direito de ser deixado só está diretamente ligada ao direito de aproveitar a sua própria intimidade e da inviolabilidade da privacidade, o que denota uma percepção individualista e não um direito coletivo. Nesse mesmo sentido, usufruir da privacidade era possibilidade apenas da burguesia que, com sua posição social, estruturou um direito à propriedade "solitária".^{32,33,34}

Definir privacidade apenas como o direito de ser deixado só deixa o conceito amplo, uma vez que se pode concluir que "qualquer conduta direcionada a outra pessoa, quer ilícita ou não [...] seria uma violação de sua privacidade"³⁵. Assim, tutelar a privacidade sob essa ótica prejudica a análise em uma realidade de intenso fluxo de informações e possibilidade de invasão da vida privada.³⁶

³⁰ WARREN, S.; BRANDEIS, L. The right to privacy. *Harvard Law Review*, v. 4, n. 193, p. 193-220, dez. 1890.

³¹ Tradução livre: "o direito de ser deixado só".

³² DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 33

³³ MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 44.

³⁴ RODOTÀ, S. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

³⁵ LEONARDI, M. **Tutela e Privacidade na Internet**. São Paulo: Editora Saraiva, 2011

³⁶ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 33

Um desdobramento desse conceito de privacidade é ela como “o resguardo contra interferências alheias”³⁷, o que não significa a exclusão de um indivíduo do convívio de terceiros. Mas, sim, assegura a possibilidade de se recolher e/ou reservar. Assim, essa palavra se refere desde à noção do direito de ser “deixado sozinho”, à privacidade física, à privacidade informacional, até às questões como personalidade e apropriação de características pessoais.³⁸

Ainda, pode ser entendida como segredo ou sigilo de informações públicas ou privadas de um indivíduo. Richard A. Posner³⁹ entende que a privacidade se relaciona com a omissão de fatos difamatórios de uma pessoa sobre si mesmo, o que é um direito egoísta e que não contribui para o desenvolvimento econômico ou social.

A privacidade, sob a ótica do ordenamento jurídico brasileiro, é um dos direitos da personalidade – que possuem como característica serem “absolutos, extrapatrimoniais, intransmissíveis, imprescritíveis, impenhoráveis, vitalícios e necessários”⁴⁰. Ao longo da história do direito brasileiro, a privacidade esteve ligada a termos distintos, como “vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e até mesmo ‘privaridade’ e ‘privaticidade’, entre outros”⁴¹.

Um exemplo é que o art. 5º, inciso X, da Constituição Federal de 1988 não utiliza a expressão *privacidade*, mas protege a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação”.^{42,43} Do mesmo modo, não há qualquer menção à palavra no Código Civil de 2000, somente declarando ser inviolável a vida privada em seu art. 21.⁴⁴⁻⁴⁵ Quatorze anos depois, o Marco Civil da *Internet*

³⁷ LEONARDI, M. **Tutela e Privacidade na Internet...** p. 55

³⁸ CANNATACI, Joseph A. Report of the Special Rapporteur on the right to privacy. **Human Rights Council**, [S. l.], 2016.

³⁹ POSNER, R. A. Values and Consequences: An Introduction to Economic Analysis of Law. **Journal of Political Economy**, [S. l.], 1998.

⁴⁰ GOMES, Orlando. **Introdução ao Direito Civil**. 19ª. ed. Rio de Janeiro: Forense, 2007. p. 134

⁴¹ LEONARDI, M. **Tutela e Privacidade na Internet**. São Paulo: Editora Saraiva, 2011, p. 41

⁴² Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

⁴³ BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html>. Acesso em: 20 jan. 2020.

⁴⁴ Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

⁴⁵ BRASIL. Código Civil Brasileiro de 2002. **Lei nº 10.406, de 10 de janeiro de 2002**, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm>. Acesso em: 20 jan.2020.

(MCI) coloca a proteção da privacidade como um princípio que disciplina o uso da *Internet* no Brasil.⁴⁶⁻⁴⁷

O cerne da questão é que a privacidade é um conceito extremamente vago, compreendendo uma variedade de conceitos em diferentes culturas e comunidades.⁴⁸ Sua ligação é direta “[...] aos valores e projeções do homem de cada sociedade e, dentro de cada uma, aos diversos grupos sociais [...]”, razão pela qual é reflexo de conteúdo social e ideológico.⁴⁹ Até porque esse direito é socialmente maleável e pode ser moldado de acordo com interesses pessoais e sociais, inclusive com justificativa de que “if you are not doing anything wrong, you have nothing to hide and nothing to fear”⁵⁰.

Nas palavras de Leonardi, *privacidade* tornou-se uma “palavra camaleão”⁵¹, utilizada para se referir a diversos interesses distintos, desde a confidencialidade de informações pessoais até a autonomia reprodutiva. Nesse sentido, Danilo Doneda⁵² discorre sobre a dificuldade de formatar tal conceito:

A imensa dificuldade em enquadrarmos a privacidade em uma concepção coerente e unitária já é, por si só, um motivo para que ela não seja concretizada como um direito subjetivo. Esse não é o motivo mais significativo para essa recusa; maior é a necessidade de afastar a proteção da privacidade da lógica patrimonialista que, tendo acompanhado sua formação, apresenta-se agora como portadora de um complexo de valores diversos daqueles representados na privacidade. Dessa forma, enunciado de um “direito à privacidade”, que por si só apresenta o risco de induzir a sua caracterização como um direito subjetivo, há de ser utilizada com a consequência de que não a representa em sua integralidade – correndo-se o risco de que ocorra uma sinédoque.

A construção da privacidade como direito é reflexo da transformação do Estado liberal em um *welfare state*, seguido de demandas que clamavam pelos direitos individuais, e o alto desenvolvimento tecnológico.⁵³ Ainda que elevado a direito por meio de diversos instrumentos

⁴⁶ Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...]

II - proteção da privacidade;

⁴⁷ BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet do Brasil. **Diário Oficial**, Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 20 jan. 2020.

⁴⁸ BARUCH, J. J.; MILLER, A. R. The Assault on Privacy. **Harvard Law Review**, [S. l.], 1971.

⁴⁹ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p.126

⁵⁰ Tradução livre: “se você não está fazendo nada de errado, você não tem nada a esconder e temer”.

⁵¹ LEONARDI, M. **Tutela e Privacidade na Internet**. São Paulo: Editora Saraiva, 2011, p. 46

⁵² DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019. p.124

⁵³ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p.33

de âmbito internacional e nacional, seu “efeito camaleão” traz dificuldades na definição de políticas sociais e aplicação em casos práticos.⁵⁴

A partir da década de 1970, a privacidade passou a ser associada com os bancos de dados, devido ao seu uso ostensivo para o armazenamento de informações. O avanço da tecnologia com a possibilidade de armazenamento de grande quantidade de dados, então, contribuiu para mais uma mutação desse conceito. É nesse contexto, inclusive, que se dá a discussão da proteção de dados.

No entanto, conforme ensina Rodotà, há uma diferença entre a privacidade como respeito à esfera privada e a proteção de dados pessoais, isto, porque, esta última “[...] estabelece regras sobre mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas”. A proteção de dados seria, então, “[...] a soma de um o conjunto de direitos que configuram a cidadania de um novo milênio”⁵⁵, ou seja, principal manifestação contemporânea da proteção da própria privacidade.⁵⁶

Laura Mendes entende que a privacidade como “direito de ser deixado só”, foi complementada e agora também significaria “o controle dos dados pessoais pelo próprio indivíduo, que decide quando, como e onde os seus dados pessoais devem circular”⁵⁷. No entanto, paira uma dúvida se os usuários realmente possuem esse controle e, se o tiverem, se têm o poder de decisão e conhecimento adequado para exercê-lo.

Assim, adota-se a noção de privacidade não como o oposto de compartilhar, mas como o controle do que é compartilhado.⁵⁸ Controle que, como será demonstrado, o usuário padrão da *Internet* não detém completamente. Desse modo, a privacidade seria uma interação na qual o direito à informação de diversos entes colide.

A partir da década de 1960, com a transformação do Estado liberal em um *welfare state*, seguido de demandas que clamavam pelos direitos individuais e o alto desenvolvimento tecnológico, alterou a visão sobre o direito à privacidade do indivíduo. Até porque, antes do

⁵⁴ “A falta de clareza a respeito do que é privacidade cria complicações para definir políticas públicas e para resolver casos práticos, pois se torna muito complexo enunciar os danos ocorridos em uma situação fática, podendo dificultar ou mesmo inviabilizar sua tutela, principalmente diante da necessidade de seu sopesamento em face de interesses conflitantes, tais como a liberdade de manifestação de pensamento, a segurança pública e a eficiência de transações comerciais. [...]” LEONARDI, M. **Tutela e Privacidade na Internet**. São Paulo: Editora Saraiva, 2011, p. 47

⁵⁵ RODOTÀ, S. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008. p. 17

⁵⁶ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2 ed. São Paulo: Thomson Reuters Brasil, 2019. p.30.

⁵⁷ MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. p. 136.

⁵⁸ ACQUISTI, A.; TAYLOR, C.; WAGMAN, L. The Economics of Privacy. **Journal of Economic Literature**, v. 54, n. 2, 2016, p. 445.

advento da Internet e da *data-driven economy*⁵⁹, o correto funcionamento desse Estado dependia da coleta e do tratamento de dados.⁶⁰⁻⁶¹

Assim, surge a Primeira Geração de normas de proteção de dados, com legislações específicas e decisões judiciais que desenharam uma projeção de personalidade de indivíduo – o que mais tarde acabou se tornando um direito fundamental. Dentre as principais leis desse período, estão a Lei do Estado Alemão de Hesse (1970)⁶², a Lei de Dados da Suécia (1973)⁶³, o *Estatuto de Proteção de Dados do Estado* alemão de Rheinland-Pfalz (1974)⁶⁴, o *Fair Credit Reporting Act*⁶⁵ e o *Privacy Act*.⁶⁶⁻⁶⁷

As normas de Segunda Geração, por sua vez, endereçam o direito à privacidade e não procedimentos e processos, diferentemente do que os da Primeira Geração fizeram. É nesse momento que a proteção de dados passa a ser associado diretamente ao direito à privacidade, às liberdades negativas e à liberdade do indivíduo. Por conta disso, a questão da efetividade do consentimento é suscitada, juntamente com o real exercício da liberdade de escolha do cidadão. Questionamentos que persistem até hoje.⁶⁸

Um dos marcos para a evolução do conceito da privacidade e da Terceira Geração de normas da proteção de dados é a decisão do Tribunal Constitucional alemão quanto à constitucionalidade da *Lei de Recenseamento da População, Profissão, Moradia e Trabalho* de 1982.⁶⁹ A referida lei tinha como objetivo a coleta de dados dos cidadãos para que a

⁵⁹ Tradução literal: “economia guiada por dados”.

⁶⁰ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019. p. 33

⁶¹ MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 38.

⁶² ALEMANHA. **Hessisches Datenschutzgesetz**. Hesse, 1970. Disponível em: <<https://datenschutz.hessen.de/ueber-uns/geschichte-des-datenschutzes>>. Acesso em: 20 fev. 2020.

⁶³ SUÉCIA. **Sw. Datalagen**, de 1 maio 1973. Disponível em: <https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289>. Acesso em: 20 fev. 2020.

⁶⁴ ALEMANHA. **LDSG Rheinland-Pfalz**, jan. 1974. Disponível em: <<http://landesrecht.rlp.de/jportal/portal/t/vyz/page/bsrlpprod.psml;jsessionid=EB>>. Acesso em: 20 fev. 2020.

⁶⁵ ESTADOS UNIDOS. **Fair Credit Reporting Act**, 15 U.S.C. § 1681, de 26 de outubro de 1970. Disponível em: <<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>>. Acesso em: 17 fev 2020.

⁶⁶ ESTADOS UNIDOS. **Privacy Act of 1974**, Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552^a. Disponível em: <<https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf>>. Acesso em: 17 fev 2020.

⁶⁷ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 29

⁶⁸ MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 40.

⁶⁹ ALEMANHA. Corte Constitucional Federal. Bundesverfassungsgericht. Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 16 jul. 19691

administração pública pudesse medir o crescimento da população e seus efeitos. Aqueles que não se submetessem à consulta, estavam sujeitos à multa.⁷⁰⁻⁷¹

Como fundamentação para a inconstitucionalidade desta lei alemã, argumentou-se que esta violava o princípio do livre desenvolvimento da personalidade. O Tribunal alemão decidiu pela constitucionalidade da norma. Contudo, declarou nulo o dispositivo que permitia a comparação dos dados coletados com outras bases de dados públicas e sua transmissão.⁷²⁻⁷³

Assim, surge o direito da “autodeterminação informativa”, considerado o marco teórico para a proteção de dados pessoais. Nesse sentido, Laura Mendes destaca a importância desse caso, uma vez que se reconheceu “um direito subjetivo fundamental e [alçou] o indivíduo a protagonista no processo de tratamento de dados pessoais”⁷⁴, o que, conseqüentemente, causou a diminuição no poder legislativo no que tange à coleta e ao tratamento de dados pessoais. Diferentemente da Segunda Geração, a Terceira entende que a participação do indivíduo no tratamento dos seus dados deve ser feita continuamente, e não só em um ponto.⁷⁵

Em seqüência, a Quarta Geração tenta aprimorar questões antes não resolvidas, fortalecendo o indivíduo, aumentando o controle no processo de tratamento e reforçando o princípio da autodeterminação informativa. As normas gerais passam a ser complementadas com normas setoriais, como forma de reforçar a proteção ao indivíduo em suas particularidades.

No entanto, atualmente é possível identificar uma alteração no campo da proteção de dados. Rafael Zanatta entende que há uma risquificação da proteção de dados pessoais, ou seja, uma mudança jurídica influenciada pelo “[...] o uso intensivo de metodologias de gestão de risco e calibragem entre riscos”⁷⁶. Nas palavras de Bruno Bioni, o “[...] saldo normativo das novas leis de proteção de dados pessoais não se contabiliza apenas pelo objetivo de franquear

⁷⁰ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 33

⁷¹ MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 41.

⁷² DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 33

⁷³ MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 41.

⁷⁴ MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 42.

⁷⁵ “Nessa formulação de um direito à autodeterminação informativa, o Tribunal [alemão] reconheceu uma carga participativa muito maior que a reconhecida pelas interpretações das normas de proteção de dados pessoais em períodos anteriores”. MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 42.

⁷⁶ ZANATTA, Rafael A. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? In: **I Encontro da Rede de Pesquisa em Governança da Internet**. Rio de Janeiro: Rede de Pesquisa em Governança da Internet, 2018, p. 184.

controle aos cidadãos, mas [...] por uma arquitetura de prevenção de dados”⁷⁷. E isso se dá justamente pelo “acirramento da assimetria da informação” no contexto das transformações tecnológicas, incluindo a *Internet*.

2.3 SOCIEDADE INFORMACIONAL: OS DADOS E A *INTERNET*

Os computadores foram os grandes responsáveis pelo salto tecnológico do século XX. Em 1946, na Filadélfia, foi desenvolvido o ENIAC (*Electronic Numerical Integrator and Computer*), o primeiro computador⁷⁸ eletrônico. A primeira versão comercial, o UNIVAC-1 (*UNIVersal Automatic Computer*), foi criada somente em 1951. A IBM, que passaria a dominar a indústria em 1953, produziu sua primeira máquina em 1964. Tempos mais tarde, isso acarretou a criação do computador pessoal.⁷⁹

Paralelamente, na década de 1960, diversas pesquisas relacionadas à comutação de pacotes, dentre elas a *Advanced Research Projects Agency Network* (ARPANET) de 1969, rede de comutação de pacotes que implementou os protocolos *Transmission Control Protocol* e o *Internet Protocol* (TCP/IP). Esses protocolos foram os responsáveis pela interligação de redes, o *internetworking*, ou seja, a criação de ligações de diversas redes distintas, estabelecendo uma rede unificada e coordenada. Outras redes, como a MILNET (com fins militares), a CSNET e a BINET, surgiram na década de 1980, utilizando a ARPANET como *backbone*⁸⁰ da rede. Criava-se, então, uma rede de redes, chamada “ARPA-Internet”, mais tarde apenas *Internet*. Com mais de 20 anos de serviço, a ARPANET acabou obsoleta, encerrando suas atividades. Assim, a NSFNET, da *National Science Foundation*, tornando-se o *backbone* da *Internet* até 1995, estabelecendo uma rede de informações que eram disseminadas por meio de computadores autônomos, descentralizando o conhecimento até certo ponto.⁸¹

Em 1990, Tim Berners-Lee e Robert Cailliau publicaram o projeto da *World Wide Web* (WWW)⁸², como solução à incompatibilidade das plataformas e ferramentas da *Internet*, o que

⁷⁷ BIONI, Bruno R. Abrindo a “caixa de ferramentas” da LGPD parProteção de dados pessoais como regulação do risco: uma nova moldura teórica? In: **I Encontro da Rede de Pesquisa em Governança da Internet**. Rio de Janeiro: Rede de Pesquisa em Governança da Internet, 2018, p. 184.

⁷⁸ Durante a Segunda Guerra Mundial, foram desenvolvidas ferramentas com propósito bélico, como o Colossus (1943) e o Z-3 (1943), de origem britânica e alemã, respectivamente. ,

⁷⁹ CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016.

⁸⁰ Backbones são infraestruturas de interligação de redes, que funcionam como a espinha dorsal do funcionamento de tais redes.

⁸¹ CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016.

⁸² BERNERS-LEE, T.; CAILLIAU, R. **WorldWideWeb**: Proposal for a HyperText Project, 12 nov 1990. Disponível em: <<https://www.w3.org/Proposal>>. Acesso em: 3 jan 2020.

impossibilitava o acesso universal, com uma interface comum à rede.⁸³ Em seu primeiro ano, a WWW funcionou apenas dentro da Organização Europeia de Investigação Nuclear (CERN), tornando-se disponível mundialmente em 1991. Em 1992, a *National Science Foundation* cria a *Internet Society*⁸⁴, uma organização sem fins lucrativos para promover a liderança, estabelecendo os padrões da *Internet*, da educação, do acesso, e das políticas relacionadas a ela.

A *Internet* e o computador pessoal, reflexos do desenvolvimento de novas tecnologias da informação e da comunicação transformaram o método de organização da sociedade e de sua economia. Assim, há uma direta reestruturação no capitalismo que pode ser:

[...] percebido na flexibilidade e na descentralização das empresas; no fortalecimento do papel do capital em frente ao trabalho; na diversificação das relações de trabalho; na intervenção estatal para desregular e desfazer o estado do bem-estar social e no aumento da concorrência econômica global.⁸⁵

O desenvolvimento de tecnologias de informação, segundo Castells, tratou de uma revolução tecnológica essencial para a implementação de um processo de reestruturação do sistema capitalista. Sua perspectiva teórica é fundamentada na ideia de que “as sociedades organizadas em processos estruturados por relações historicamente determinadas de *produção, experiência e poder*”⁸⁶. “A *produção* é a ação da humanidade sobre a matéria (natureza) para apropriar-se dela e transformá-la em seu benefício, obtendo um produto, consumindo (de forma irregular) parte dele e acumulando o excedente para investimento”⁸⁷.

Os modos de desenvolvimento, nessa visão, são definidos pelo elemento fundamental que rege o aumento de produtividade no processo produtivo. O modelo informacional de desenvolvimento tem como fonte de produtividade a tecnologia, seja a de “geração de conhecimentos, de processamento da informação e de comunicação de símbolos”. Ainda que o conhecimento e a informação sejam cruciais também no modo agrícola e no industrial, o novo modelo se distingue dos anteriores por ter a “ação de conhecimentos sobre os próprios

⁸³ “The current incompatibilities of the platforms and tools make it impossible to access existing information through a common interface, leading to waste of time, frustration and obsolete answers to simple data lookup. There is a potential large benefit from the integration of a variety of systems in a way which allows a user to follow links pointing from one piece of information to another one. This forming of a web of information nodes rather than a hierarchical tree or an ordered list is the basic concept behind HyperText.com.

⁸⁴ “The Internet Society was founded in 1992 by a number of people involved with the Internet Engineering Task Force (IETF). From those early days, one of our principal rationales is to provide an organizational home for and financial support for the Internet standards process”. (INTERNET SOCIETY)

⁸⁵ BOFF, S. O.; FORTES, V. B.; FREITAS, C. O. D. A. **Proteção de dados e privacidade**: do direito às novas tecnologias da informação. Rio de Janeiro: Lumen Juris, 2018, p. 12

⁸⁶ CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016, p. 33.

⁸⁷ CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016, p. 71.

conhecimentos como fonte de produtividade”⁸⁸. Esse novo tipo de desenvolvimento, então, é chamado por Castells de *Informacionalismo*, criado a partir do novo paradigma tecnológico da tecnologia da informação:

[...] O processamento da informação é focalizado na melhoria da tecnologia do processamento da informação como fonte de produtividade, em um círculo virtuoso de interação entre as fontes de conhecimentos tecnológicos e a aplicação da tecnologia para melhorar a geração de conhecimentos e processamento da informação [...].⁸⁹

O desenvolvimento da tecnologia da informação é, então, paradigma que reestruturou a produção capitalista, tornando-se a base da globalização da economia.⁹⁰ Conseqüentemente, a sociedade se transforma em uma Sociedade Informacional, em que se busca mais a cultura e a busca de identidades, desfocando-se do sistema produtivo pela força de trabalho. Por conta disso, diferencia-se da Sociedade da Informação.

A Sociedade da Informação destaca o papel da informação, quase que ignorando que ela já foram cruciais para diversas sociedades ao longo da história. A Sociedade Informacional, por sua vez, “indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder”⁹¹, por conta dos avanços tecnológicos específicos desse período.⁹²

Assim, a Sociedade Informacional se organiza de forma que “a geração, o conhecimento e a transmissão da informação tornam-se fontes fundamentais de produtividade e poder”. É organizada como uma rede multicultural e conectada. E a *Internet* se torna uma grande representante dessa nova sociedade.

⁸⁸ CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016, p. 74.

⁸⁹ CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016, p. 74.

⁹⁰ BOFF, S. O.; FORTES, V. B.; FREITAS, C. O. D. A. **Proteção de dados e privacidade: do direito às novas tecnologias da informação**. Rio de Janeiro: Lumen Juris, 2018, p. 13

⁹¹ CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016, p.84

⁹² “[...] Minha terminologia tenta estabelecer um paralelo com a distinção entre indústria e industrial. Uma sociedade industrial. Uma sociedade industrial (conceito comum na tradição sociológica) não é apenas uma sociedade em que há indústrias, mas uma sociedade em que as formas sociais e tecnológicas de organização industrial permeiam todas as esferas de atividade, começando com as atividades predominantes localizadas no sistema econômico e na tecnologia militar e alcançando os objetos e hábitos da vida cotidiana. Meu emprego dos termos “sociedade informacional” e “economia informacional” tenta uma caracterização mais precisa das transformações atuais, além da sensata observação de quem a informação e os conhecimentos são importantes para nossa sociedade. Porém o conteúdo real de “sociedade informacional” tem de ser determinada pela observação e análise. [...] Por exemplo, uma das características principais da sociedade informacional é a lógica de sua estrutura básica em redes, o que explica o uso do conceito de “sociedade em rede”, definido e especificado na conclusão deste volume. Contudo outros componentes da “sociedade informacional”, como movimentos sociais ou o Estado, mostram características que vão além da lógica dos sistemas de redes, embora sejam muito influenciadas por essa lógica, típica da nova estrutura social. Dessa forma “a sociedade em rede” não esgota todo o sentido da “sociedade informacional.[...]”. CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016, p. 84.

A *Internet* se torna um “produto chave da era da informação”⁹³, não apenas uma tecnologia da informação e da comunicação. Expande o alcance da comunicação, alterando o poder de quem processa dados. Aqueles acostumados a consumir informações passam a se tornar fonte produtora delas, sem que tenham sido educados para tanto.⁹⁴⁻⁹⁵

No entanto, ao mesmo tempo que esse novo modelo cria fluxos informacionais, eles se descentralizam, não conseguindo os Estados fazer o controle e, muito menos, os próprios titulares-originários.⁹⁶ Com tanta informação disponível, foram desenvolvidas ferramentas para capturar esses rastros digitais, como forma de capitalizar os padrões que são estabelecidos. Dados como nome, idade, endereço, gênero e interesses em geral se tornaram ativos digitais de grande valor para empresas em seu processo de adaptação ao novo mundo digitalizado.

Tudo se torna *acessável* a qualquer tempo, em qualquer lugar, estando a tecnologia embarcada e presente na vida de quase toda a população sem que exista uma percepção disso, o que Greenfield denominou como paradigma *everyware*.⁹⁷

Como consequência, a coleta de informações e dados se torna cada vez mais facilitada e barata, o que reforça a ideia da existência de uma Sociedade Informacional. Assim, a transformação do capitalismo cria uma discussão sobre a natureza das informações e dos dados pessoais, uma vez que antes um direito protegido pela privacidade passa a ser considerado um ativo comercial, que pode ser coletado, comercializado e transmitido, muitas vezes sem o consentimento do seu titular.

2.4 DADOS PESSOAIS: DE DIREITO À ATIVO

O *World Economic Forum*, em 2011 e 2012, classificou dados pessoais como “the new oil”⁹⁸, um recurso valioso do século 21, atingindo todos os aspectos da sociedade. Cria-se nova classe de *assets* (ou ativos), uma “oportunidade pós-industrial”, de complexidade, variedade e

⁹³ CASTELLS, M. **A Galáxia Internet**: Reflexões sobre Internet, Negócios e Sociedade. Rio de Janeiro: Jorge Zahar, 2003, p. 251.

⁹⁴ BOFF, S. O.; FORTES, V. B.; FREITAS, C. O. D. A. **Proteção de dados e privacidade**: do direito às novas tecnologias da informação. Rio de Janeiro: Lumen Juris, 2018.

⁹⁵ CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016, p. 74

⁹⁶ O conceito de *titular* utilizado em toda a pesquisa é o mesmo da Lei Geral de Proteção de Dados (Lei nº 13.709/18), que dispõe em seu art. 5, inciso V, que é aquela “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.”

⁹⁷ GREENFIELD, A. **Everyware**: The dawning age of ubiquitous computing. Berkeley: New Riders, v. New Riders, 2006. p. 6.

⁹⁸ WORLD ECONOMIC FORUM. Personal data: **The emergence of a new asset class**. Davos, 2011. Disponível em: <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>. Acesso em: 12 dez. 2019.

alcance global sem precedente até então. Agregam valor às empresas e possibilitam a criação e perpetuação de serviços que, sem esses dados, não existiriam.

Assim, os dados pessoais podem servir como uma ferramenta para reduzir custos de produção, diminuir custos transacionais para uma empresa e para os consumidores, analisar riscos e criar publicidade focada em determinados perfis. Porém, dados são um produto por si só, ao observar a produção de conteúdo feita pelo próprio usuário, como ocorre nas redes sociais. Esse raciocínio é estruturado em torno do fato de que os dados pessoais são um capital estratégico que permite aos negócios desenvolver uma maior inteligência de mercado ou melhorar os processos já existentes.⁹⁹

Estudioso da Análise Econômica do Direito, **Richard E. Posner**¹⁰⁰ vincula a privacidade à ocultação ou omissão de informações. Segundo esse representante da Escola de Chicago, quando um indivíduo tem poder de controle sobre as suas informações, pode “manipular” como se apresenta perante a sociedade, de forma a não condizer com a realidade. Por conta disso, entende que a proteção da privacidade do usuário e a imposição de um dever de transparência às empresas seria um exemplo perverso de como os governos regulam a vida econômica e social.

Em complemento, George Stigler argumentou que a interferência do governo na privacidade, como forma de proteger uma das partes envolvidas, era “redundante” e muitas vezes “imprópria”.¹⁰¹ A existência de leis de proteção à privacidade poderia causar uma diminuição na qualidade e no nível de detalhe da informação que pode ser obtida, o que causa um resultado econômico ineficiente, com distribuição de recursos equivocadas, entre outros prejuízos.

Enquanto a Escola de Chicago via a privacidade como um impeditivo ao avanço econômico, pensadores como Hirshleifer entendiam que a coleta desenfreada desses dados era ineficiente. Segundo essa corrente de pensamento, até nos casos em que a informação era coletada sem custo, havia um incentivo de maximizar lucros, como realizando o *profiling* do usuário. Assim, o interesse público era colocado de lado para a maximização do lucro.¹⁰²

⁹⁹ WORLD ECONOMIC FORUM. Personal data: **The emergence of a new asset class**. Davos, 2011. Disponível em: <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>. Acesso em: 12 dez. 2019.

¹⁰⁰ POSNER, Richard A.. An Economic Theory of Privacy. **AEI Journal on Government and Society**, Regulation, p. 19-26, maio/jun. 1978.

¹⁰¹ STIGLER, G. J. An Introduction to Privacy in Economics and Politics. **The Journal of Legal Studies**, [S. l.], 1980.

¹⁰² HIRSHLEIFER, J. The Private and Social Value of Information and the Reward to Inventive Activity. In: **Uncertainty in Economics**. [S. l.: s. n.].

Conforme destacado por Brandimarte e Acquisti, com o avanço das tecnologias da informação, incluída aqui a *Internet*, a discussão da privacidade renasceu nos anos 1990s. A redução dos custos de tecnologias de armazenamento e processamento de dados acarretou o aumento da preocupação quanto ao tratamento de dados pessoais e demais informações.¹⁰³

No final dos anos 1990, Noam¹⁰⁴ reforçou os argumentos da Escola de Chicago. Utilizando o Teorema de Coase¹⁰⁵⁻¹⁰⁶ com o objetivo de alcançar eficiência em uma transação com custo zero, ainda que presentes externalidades, argumenta que a alocação de direitos de propriedade é arbitrária e sem efeitos e não influencia no equilíbrio final. Em uma relação entre uma parte que possui interesse em proteger seus dados pessoais e outra que possui interesse em adquiri-los, segundo o autor, iria prevalecer os interesses daquele que possui mais a perder.

Lawrence Lessig já entendia, em 1998, dados como *assets*¹⁰⁷, recursos que se tornaram valiosos e que, por sua vez, o mercado tenta explorar. Tendo em vista o custo desse uso, o autor sugere a construção de um regime em que o sujeito que usará os dados internalizaria os custos, de forma a arcar com esses. O regime de propriedade, então, seria uma modelo no qual os indivíduos possuem o direito de controlar seus dados. No entanto, o autor não apresenta os danos que essa comercialização de dados poderia causar.¹⁰⁸

Nesse mesmo sentido, Laudon propõe a criação de um “mercado nacional de informações”, pelo qual os titulares de seus dados podem transferir os direitos destes para outros, em troca de dinheiro. Para o acadêmico, a proteção da privacidade é ultrapassada e defende que um sistema baseado na propriedade de direitos de dados pessoais seria tanto de interesse dos usuários, quando das companhias – uma solução híbrida que integra o mercado, a tecnologia e a regulação.¹⁰⁹

¹⁰³ BRANDIMARTE, L.; ACQUISTI, A. *The Economics of Privacy*, p. 547-571, 2012. Disponível em: <<http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780195397840.001.0001/oxfordhb>>. Acesso em: 22 dez. 2019.

¹⁰⁴ NOAM, E. **Privacy and self-regulation: Markets for electronic privacy**. [s. l.], 1997.

¹⁰⁵ COASE, R. H. The Problem of Social Cost. **The Journal of Law and Economics**, [S. l.], 1960.

¹⁰⁶ Em linhas gerais, o Teorema de Coase diz que “[d]esde que os direitos de emissão de externalidades sejam adequadamente definidos e que não haja custos de transação entre as partes, a livre negociação entre as mesmas deve levar ao nível ótimo de emissão destas externalidades”. COSTA, S. Introdução à economia do meio ambiente. **Análise**, [S. l.], p. 301–323, 2005.

¹⁰⁷ Tradução literal: “ativos”.

¹⁰⁸ “The laws of property are one such regime. If individuals can be given the rights to control their data, or more precisely, if those who would use data had first to secure the right to use it, then a negotiation could occur over whether, and how much, data should be used. The market, that is, could negotiate these rights, if a market in these rights could be constructed.” LESSIG, L. **The Architecture of Privacy**, Draft 2, p. 17, 1998. Disponível em: <http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf>. Acesso em: 11 dez 2019.

¹⁰⁹ LAUDON, K. Extensions to the theory of markets and privacy: mechanics of pricing information. **NYU Working Paper no. IS-97-04**, jan 1997. Disponível em: <<https://ssrn.com/abstract=1283008>>. Acesso em: 20 fev. 2020.

A adoção do pensamento de Lessig é criticada por Laura Mendes já que, segundo a autora, conceber esse direito como um direito de propriedade traria problemas no âmbito individual e democrático, o que ela fundamenta em três argumentos. O primeiro é o entendimento que ao colocar um preço nos dados, viola-se o princípio da igualdade, conceituado como “a distribuição de iguais liberdades a todos os cidadãos”¹¹⁰. Sob a ótica desse argumento, o direito de propriedade sobre os dados pessoais acarretaria uma discriminação social, uma vez que uma parte da população teria a opção de escolha de não vender ou ceder seus dados pessoais. O valor dos dados poderia variar de acordo com o sexo, poder de compra, profissão, entre outras variáveis.

Até porque, conforme coloca Danilo Doneda, a preocupação com proteção de dados pessoais surge em países desenvolvidos, uma vez que a percepção do problema é proporcional aos níveis educacionais e financeiros.¹¹¹⁻¹¹² Além do poder socioeconômico, o problema do controle sobre os dados pessoais é intrinsicamente ligado a problemas de escolha pessoal e autonomia.¹¹³ E, como será visto adiante, a sensação de urgência na utilização de um serviço ou produto acaba se sobressaindo em uma reflexão sobre possíveis malefícios.

Então, torna-se um problema significativo o fato de que as normas de proteção da privacidade não se moldam ao conceito de contratos e, conseqüentemente, à ideia de dados pessoais como dinheiro. Há, de fato, um crescente consenso de que a privacidade pode ser renunciada e monetizada. Contudo, não se desenvolve ao mesmo tempo as condições nas quais as relações contratuais de privacidade seriam consideradas válidas.

O segundo argumento trazido por Mendes foca na supressão da individualidade e o surgimento de indivíduos *market oriented*¹¹⁴, ou seja, aqueles que são direcionados ao mercado. A autora apresenta a hipótese de personalidades serem forjadas para realizarem determinados

¹¹⁰ MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 122.

¹¹¹ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 45.

¹¹² “Não é por acaso que a proteção de dados pessoais foi assunto que entrou em pauta primeiramente nos países desenvolvidos: a sensibilidade dos cidadãos para o problema aumenta em proporção aos próprios níveis educacionais e financeiro. [...] Confirma-se, assim, que a necessidade de uma sociedade em estabelecer mecanismos de proteção de dados pessoais varia conforme o padrão médio de consumo de sua população, assim como de outros fatores como sua educação e a própria penetração da tecnologia no cotidiano, ecoando a sensação de Albert Bendich, de que “privacidade e pobreza são absolutamente contraditórios”.

¹¹³ ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and human behavior in the age of information. *Science* **347** (6221), 509-514., New York, v. 347, n. 6221, 2017. p. 509.

¹¹⁴ Tradução literal: “orientados pelo mercado”.

tipos de atividades, como forma de se encaixar às necessidades do mercado. Assim, haveria uma oferta ideal às demandas crescentes do mercado.¹¹⁵

Por último, o terceiro argumento apresenta a ameaça à democracia. Isso, porque, segundo a autora, “o funcionamento da sociedade democrática depende da capacidade autônoma de ação e participação de cada indivíduo para a formação da vontade comum”¹¹⁶. Isso, porque, quando se substitui o direito à proteção de dados por um modelo de mercado, não há mais garantia de proteção de direitos da personalidade, incluindo direitos fundamentais como o direito à privacidade.

Além disso, há a dificuldade em mensurar o valor de um dado ou informação pessoal, principalmente ao se entender que este é um reflexo de um direito fundamental inalienável. Como constatado por Spiekermann *et al.*, diversos estudos econômicos experimentais tentaram capturar o preço de itens de dados pessoais, mas “[...] it is hard to map these data points into a consistent picture, due to heuristics and biases which may significantly affect individuals privacy choices, including in fact their valuations of their personal data [...]”¹¹⁷⁻¹¹⁸.

Recentemente, Jeffrey Prince e Scott Wallsten, do *Technology Policy Institute*, publicaram um artigo que mensurou o valor da privacidade *online* em diversos países e de diversos tipos de dados, como dados pessoais financeiros. Dentre suas descobertas, está que as pessoas são mais preocupadas em divulgar dados biométricos, uma vez que estes não seriam substituíveis, e também dados financeiros. Em contrapartida, não possuem muito ócio em receber anúncios, já que, ainda que seja incômodo, pode ser útil.¹¹⁹

A pesquisa do *Technology Policy Institute* calculou que o valor que um indivíduo “cobraria” pelo direito de as instituições financeiras divulgarem seus extratos seria de USD 9/mês e USD 7,50/mês para o fabricante de celular divulgar seus dados biométricos. Já o valor que atribuem para bloquear o recebimento de anúncios é muito menor, assim como os de localização que é de USD 1,82/mês.

115 MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 122.

116 MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 122.

117 SPIEKERMANN, Sarah *et al.* The challenges of personal data markets and privacy. **Electronic Markets**, [S. l.], v. 25, n. 2, 2015, p. 63.

118 Tradução livre: “[...] é difícil mapear esses pontos de dados em uma imagem consistente, devido a heurísticas e vieses que podem afetar significativamente as escolhas individuais de privacidade, incluindo, de fato, avaliações de seus dados pessoais. [...]”.

119 PRINCE, J.; WALLSTEN, S. **How Much is Privacy Worth Around the World and Across Platforms?**. [S. l.], 2020. Disponível em: https://techpolicyinstitute.org/wp-content/uploads/2020/01/Prince_Wallsten_How-Much-is-Privacy-Worth-Around-the-World-and-Across-Platforms.pdf. Acesso em: 20 fev. 2020.

Há também a diferença entre os valores em regiões e países. Como já mencionado, países com níveis educacionais e financeiros mais elevados acabam atribuindo um valor mais elevado à privacidade que outros. Isso pode ser visto quando se compara a Alemanha e países da América Latina, por exemplo. Dentre os tipos de dados, essa disparidade é evidenciada na análise de anúncios. Diferentemente dos alemães que tem aversão à exibição de anúncios, os latinos preferem que eles sejam mostrados em seus celulares.¹²⁰

Ao discutir dados como ativos, não se pode fugir da questão da propriedade dos dados, ou seja, a quem eles pertencem. A propriedade dos dados gera poder de controle, sobre quem acessa dados, quem não acessa, impondo condições de uso.¹²¹

No contexto da Sociedade da Informação surge então a *data-driven economy*¹²², uma vez que, como já mencionado, os dados se tornaram recurso essencial para o crescimento econômico, criação de empregos e progresso social. Sobre o tema, em 2017, a Comissão Europeia emitiu comunicado *Building an European Data Economy* para o Parlamento Europeu¹²³, para o Conselho, para o Comitê Econômico e Social e para o Comitê das Regiões. Nele, definiu que a economia de dados é caracterizada por um ecossistema de diferentes tipos de atores de mercados – como pesquisadores ou provedores – que colaboram entre si para garantir que os dados são acessíveis e utilizáveis. Assim, isso faz com que seja possível a extração de valor desses dados, pela criação de uma variedade de aplicações com grande potencial de melhorar a vida diária¹²⁴ – no entanto, como será visto, isso não é sempre positivo.

Contudo, essa *data-driven economy* é construída sobre assimetrias informacionais, uma vez que são somente alguns atores que possuem recursos suficientes para investir em tecnologias para tratar grandes conjuntos de dados. Ademais, quanto mais dados seus serviços geram e/ou coletam, mais facilmente poderão utilizar algoritmos para agregar valor aos dados brutos, transformando-os em informação e conhecimento. Esse movimento perpetua o poder de

¹²⁰ PRINCE, J.; WALLSTEN, S. **How Much is Privacy Worth Around the World and Across Platforms?**. [s. l.], 2020. Disponível em: https://techpolicyinstitute.org/wp-content/uploads/2020/01/Prince_Wallsten_How-Much-is-Privacy-Worth-Around-the-World-and-Across-Platforms.pdf. Acesso em: 18 fev. 2020

¹²¹ SCASSA, T. Data Ownership. **Centre for International Governance Innovation**, n. 187, set 2018. Disponível em: <https://www.cigionline.org/sites/default/files/documents/Paper%20no.187_2.pdf>. Acesso em: 20 fev. 2020

¹²² Tradução livre “Economia orientada por dados”.

¹²³ As assimetrias informacionais também serão tratadas mais adianta, no que tangem as escolhas dos usuários.

¹²⁴ EUROPEAN COMMISSION. **Communication on Building a European Data Economy**, 10 janeiro 2017. p. 2. Disponível em: <<https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy>>. Acesso em: 11 fev. 2020.

mercado desses atores, já que mais dados criarão mais informação e conhecimento que, por sua vez criarão mais dados.¹²⁵ Luã Fergus¹²⁶ se aprofunda nessa questão:

A lógica do capitalismo de vigilância, impulsionada pelas grandes companhias de tecnologia, é baseada em um patrulhamento intensificado de seus usuários, e conseqüentemente, na exploração dos dados pessoais dos usuários pela criação de perfis minuciosos deste público com o objetivo final de aumentar e tornar mais fácil a comercialização de produtos. Dessa forma, alguns especialistas afirmam que há uma transferência de trabalho da empresa para os usuários e consumidores, uma vez que estes trabalham produzindo dados, mas sem remuneração, sendo, portanto, considerados como “escravos digitais”.

Seguindo a mesma lógica, a assimetria informacional também ocorre entre países. Isso porque alguns países não têm a oportunidade de se beneficiar das tecnologias digitais da forma que os países mais desenvolvidos. Nota-se, ainda, que os grandes atores da *data-driven economy* são originários de países desenvolvidos, o que perpetua essa disparidade, uma vez que quanto menos desenvolvido o país nesse tipo de tecnologia, menos oportunidade tem de se beneficiar e competir frente às TICs.

O desenvolvimento da *Internet* confirmou as previsões da Escola de Chicago, uma vez que o próprio mercado induziu uma eficiente disseminação de informações privadas, sem regulamentação compassada.¹²⁷ Mas isso não significa que a auto-regulamentação do mercado foi eficiente. Tanto assim é que existe uma crescente movimentação para a criação de diversas políticas de regulamentação desse novo modelo de economia, surgindo então a Governança de Dados, como se verá adiante.

O poder de processamento das tecnologias contemporâneas faz com que serviços e produtos mais aperfeiçoados sejam oferecidos. Assim, não só o setor privado, o Estado e os usuários se beneficiam com tais melhorias. Por outro lado, o potencial de abuso do uso de dados pessoais cresce. Assim, a erosão da privacidade pode ameaçar a autonomia individual, inclusive como cidadãos, já que o compartilhamento de dados pessoais nem sempre significa mais progresso, eficiência e igualdade.

¹²⁵ AARONSON, S. A. Data Is a Development Issue. **CIGI Papers**, 2019. p. 2. Disponível em: <[https://www.cigionline.org/sites/default/files/documents/paper no.223.pdf](https://www.cigionline.org/sites/default/files/documents/paper%20no.223.pdf)>. Acesso em: 11 fev. 2020.

¹²⁶ FERGUS, Luã. Mi casa es su casa: o impacto dos assistentes digitais sobre privacidade na América Latina. In: BELLI, L.; CAVALLI, O. **Governança e regulações da Internet na América Latina: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance**. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2019.

¹²⁷ BRANDIMARTE, L.; ACQUISTI, A. **The Economics of Privacy**, p. 547-571, 2012. Disponível em: <<http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780195397840.001.0001/oxfordhb>>. Acesso em: 22 dez. 2019.

Logo, torna-se importante o desenvolvimento de políticas estruturais para a correção dos desvios comportamentais e para que direitos sejam assegurados. Dessa forma, analisa-se a seguir o Paternalismo Libertário, por meio dos *nudges*, como mecanismo para tanto.

3 PATERNALISMO LIBERTÁRIO, *NUDGES* E O PROCESSO DE ESCOLHA DOS USUÁRIOS

A presunção de que os indivíduos devem ser completamente livres para tomar suas próprias decisões tem por base a assunção de que estes fazem boas escolhas ou que, ao menos, feriam-nas de uma melhor maneira do que um terceiro assim incumbido. Esse indivíduo com a capacidade de tomar as melhores decisões para atender suas particularidades, seria uma espécie de *Homo economicus*, ou *homem econômico*, que se enquadra na imagem do ser humano idealizada por economistas. Contudo, ele se restringiria a ser apenas uma figura teórica, uma vez que o homem-real não possuiria tal capacidade.¹²⁸

Thaler e Sunstein entendem que escolhas comportamentais ruins de seres humanos são consequência de limitações cognitivas, além de questões relacionadas a vieses e a hábitos desses indivíduos. Isso, por sua vez, é mais um reflexo do processo de definição do comportamental do ser humano, nem sempre liderado por uma ideia racional e consciente.¹²⁹

Em seu ensaio, Chaiken e Trope apresentaram a *dual process theories*¹³⁰, na qual dividiram o processo mental relativo ao comportamento e julgamentos sociais. Na primeira categoria se encaixam aqueles processos mentais que são automaticamente operados, tendo quatro principais características: (i) são provocados inintencionalmente; (ii) necessitam poucos recursos cognitivos; (iii) não podem ser parados voluntariamente; (iv) ocorrem fora do estado de consciência. Já na segunda estão os feitos de modo controlado, por processo que são caracterizados como: (i) iniciados intencionalmente; (ii) necessitam de recursos cognitivos consideráveis; (iii) podem ser parados voluntariamente; (iv) ocorrem de modo consciente.¹³¹⁻

132

Kahneman, por sua vez, intitula esses dois sistemas como Sistema Intuitivo (ou Sistema 1) e o Sistema Racional (ou Sistema 2). Enquanto situações cotidianas são coordenadas pelo Sistema 1, o que comumente se chama de “piloto automático”, o Sistema 2 fica responsável por aquelas atividades que demandam atenção. Logo, assim que uma situação mais delicada ou

¹²⁸ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

¹²⁹ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

¹³⁰ Tradução livre: “teorias do processo dual”.

¹³¹ GAWRONSKI, B.; CREIGHTON, L. A. Dual Process Theories. In: CARLSTON, D. **The Oxford Handbook of Social Cognition**. New York: Oxford University Press, v. pp. 282-312, 2013.

¹³² CHAIKEN, S.; TROPE, Y. **Dual-process theories in social psychology**. New York: Guilford Press, 1999.

um momento de decisão mais importante surja, o Sistema Intuitivo deve sair de cena, deixando a responsabilidade à cargo do Sistema Racional.¹³³

As características da *dual process theory* são trazidas por Thaler e Sunstein, agora com o nome de Sistema Automático e Sistema Reflexivo, para classificar os tipos de decisões tomadas. Para os autores, o *homem econômico* nunca tomaria qualquer decisão sem utilizar o Sistema Reflexivo, razão pela qual suas escolhas seriam mais assertivas e promoveriam o seu bem-estar. Porém, a maioria dos indivíduos só conseguiria fazer o contrário, tomando decisões rápidas e apressadas, que culminariam em prejuízo pessoal.¹³⁴

3.1 HEURÍSTICAS E VIÉSES

Em todas as etapas de construção de conhecimento, assim como de tomada de decisões, os indivíduos apoiam-se em princípios heurísticos, para avaliar probabilidade e prever valores. Segundo Kahneman, “[h]eurística é um procedimento simples que ajuda a encontrar respostas adequadas, ainda que geralmente imperfeitas, para perguntas difíceis”¹³⁵. Assim, são artifícios utilizados para agilizar a tomada de decisões, mesmo que inconscientemente.

No entanto, decisões baseadas em heurísticas nem sempre são acertadas, tendo em vista vieses derivados desses atalhos mentais. Assim, ainda que facilitadores, as heurísticas podem criar erros sistemáticos e previsíveis.¹³⁶

Não há um consenso na literatura sobre quais e quantas são as heurísticas e os vieses existentes. Amos Tversky e Daniel Kahneman¹³⁷ identificaram três heurísticas que são empregadas para avaliar probabilidade e prever valores: 1) representatividade; 2) disponibilidade; 3) ajustes e ancoragem.

3.1.1 A heurística da representatividade

¹³³ KAHNEMAN, D. **Rápido e devagar**. duas formas de pensar. Rio de Janeiro: Objetiva, 2012, p. 25.

¹³⁴ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

¹³⁵ KAHNEMAN, D. **Rápido e devagar**. duas formas de pensar. Rio de Janeiro: Objetiva, 2012.

¹³⁶ TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, p. 1124-1131, 1974.

¹³⁷ TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, p. 1124-1131, 1974.

A *representatividade*, podendo também ser chamada de heurística da *similaridade*¹³⁸, trata de tirar conclusões ao comparar com outros cenários anteriores, quando é necessário julgar a probabilidade de um evento ocorrer. Segundo Bazerman¹³⁹, “[a]o fazer um julgamento sobre um indivíduo, um objeto ou um evento tendem a procurar peculiaridades que ele possa ter que correspondam a estereótipos formados anteriormente”.

Thaler e Sunstein exemplificam essa heurística com a assumpção de que um afro-americano de mais de dois metros de altura teria muito mais a probabilidade de ser um jogador de basquete profissional do que um judeu branco de 1,60 m. Isso, porque, parte-se do estereótipo padrão de um jogador de basquete.¹⁴⁰

Tversky e Kahneman entendem que os seguintes vieses comportamentais são derivados dessa heurística, conforme Tabela 1: (i) *insensitivity to prior probability of outcomes*; (ii) *insensitivity to sample size*; (iii) *misconceptions of chance*; (iv) *insensitivity to predictability*; (v) *illusion of validity*; e (vi) *misconceptions of regression*¹⁴¹. A Tabela 2 apresenta exemplos de vieses com base na heurística da representatividade.

Tabela 1 - Conceito dos vieses da heurística da representatividade

Viés	Conceito
Insensitivity to prior probability of outcomes ¹⁴²	Os indivíduos tendem a ignorar a probabilidade de certos resultados acontecerem, ignorando informações que sejam apresentadas. ¹⁴³
Insensitivity to sample size ¹⁴⁴	Os indivíduos, para avaliar a probabilidade de obter um determinado resultado em uma amostra estatística, tendem a não levar em consideração o tamanho da amostra. ¹⁴⁵

¹³⁸ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

¹³⁹ BAZERMAN, M. H. **Processo decisório para cursos de administração, economia e MBAs**. Elsevier, 2007, p. 7

¹⁴⁰ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

¹⁴¹ Em tradução livre: (i) insensibilidade aos índices básicos; (ii) insensibilidade ao tamanho da amostra; (iii) interpretação errada da chance; (iv) regressão a média; (v) falácia da conjunção; e (vi) equívocos de regressão.

¹⁴² Tradução livre: “insensibilidade à previa probabilidade dos resultados”.

¹⁴³ “One of the factors that have no effect on representativeness but should have a major effect on probability is the prior probability, or base-rate frequency, of the outcomes.” TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, 1974, p. 1124.

¹⁴⁴ Tradução livre: “insensibilidade ao tamanho da amostra”

¹⁴⁵ “To evaluate the probability of obtaining a particular result in a sample drawn from a specified population, people typically apply the representativeness heuristic. [...]” Cf.: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, 1974, p. 1125.

Viés	Conceito
Misconceptions of chance ¹⁴⁶	As pessoas ignoram que eventos aleatórios são aleatórios, buscando um certo padrão com base nos eventos passados. ¹⁴⁷
Insensitivity to predictability ¹⁴⁸	Os indivíduos ignoram a confiabilidade de uma descrição e prestam atenção nos fatores relacionados.
illusion of validity ¹⁴⁹	Indivíduos tendem prever selecionando o resultado que mais se encaixa à informação já existente. A confiança que possuem em suas previsões depende principalmente do grau de representatividade (isto é, da qualidade da correspondência entre o resultado selecionado e a entrada) com pouca ou nenhuma consideração pelos fatores que limitam a precisão preditiva. ¹⁵⁰
Misconceptions of regression ¹⁵¹	É uma crença equivocada de que dois eventos combinados (conjunções) teriam mais probabilidade de ocorrer, do que apenas um dos eventos isolados.

Tabela 2 - Exemplo dos vieses da heurística da representatividade

Viés	Exemplo
Insensitivity to prior probability of outcomes ¹⁵²	Uma breve descrição de diversos indivíduos, de amostras aleatórias de um grupo de 100 profissionais (engenheiros e advogados), foi apresentada para certos indivíduos. Esses indivíduos deviam decidir se era descrição de um advogado ou engenheiro. Um grupo foi informado que havia 70 engenheiros e 30 advogados, e outro o contrário. No primeiro cenário as chances de as descrições serem de um engenheiro e não de um advogado são muito maiores. No entanto, essa proporcionalidade foi esquecida por conta de estereótipos dessas profissões.
Insensitivity to sample size ¹⁵³	Uma cidade tem dois hospitais. No hospital maior, cerca de 45 bebês nascem todos os dias. Já no hospital menor, 15 bebês nascem por dia. Metade de todos eles são meninos, ainda que a porcentagem não seja esta em todos os dias, podendo ser menos ou mais que 50%. Quando perguntados qual hospital teve mais dias em que essa porcentagem foi maior que 60%, 53 pessoas responderam que os dois tiveram a mesma média; 21 escolheram o hospital maior e 21 o hospital menor. No entanto, estatisticamente, as chances de o hospital maior ter a proporção mais próxima de 50%, do que a do hospital menor. ¹⁵³

¹⁴⁶ Tradução livre: “equivocos do acaso”.

¹⁴⁷ “People expect that a sequence of events generated by a random process will represent the essential characteristics of that process even when the sequence is short TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, 1974, p. 1125.

¹⁴⁸ Tradução livre: “insensibilidade à previsibilidade”.

¹⁴⁹ Tradução livre: “ilusão de validade”.

¹⁵⁰ “As we have seen, people often predict by selecting the outcome (for example, an occupation) that is most representative of the input (for example, the description of a person). The confidence they have in their prediction depends primarily on the degree of representativeness (that is, on the quality of the match between the selected outcome and the input) with little or no regard for the factors that limit predictive accuracy.” Cf.: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, 1974, p. 1125.

¹⁵¹ Tradução livre: “equivocos de regressão”.

¹⁵² Tradução livre: “insensibilidade à previa probabilidade dos resultados”.

¹⁵³ “A certain town is served by two hospitals. In the larger hospital about 45 babies are born each day, and in the smaller hospital about 15 babies are born each day. As you know, about 50 percent of all babies are boys. However, the exact percentage varies from day to day. Sometimes it may be higher than 50 percent, sometimes lower.

Viés	Exemplo
Misconceptions of chance	Ao jogar moedas para ver se o resultado é cara ou coroa, por exemplo, os indivíduos são mais propensos à acreditar que a sequência “cara-coroa-cara-coroa-cara-coroa” possui mais chance de acontecer, do que a sequência “cara-cara-cara-coroa-coroa-coroa”, que não parece ser aleatória, ou que a sequência “cara-cara-cara—cara-cara-coroa”, que não representativa ou representaria? a “justiça” da moeda. ¹⁵⁴
Insensitivity to predictability	Foi solicitado a alguns sujeitos que avaliassem a qualidade da lição descrita no parágrafo em pontuações percentuais, em relação a uma população especificada. Outros participantes foram solicitados a prever, também em porcentagens, a posição de cada professor aluno 5 anos após a aula prática. Os julgamentos feitos sob as duas condições foram idênticos. Ou seja, a previsão de um critério remoto (sucesso de um professor após 5 anos) era idêntica à avaliação das informações nas quais a previsão se baseava (a qualidade da aula prática). Os estudantes que fizeram essas previsões estavam indubitavelmente cientes da previsibilidade limitada da competência de ensino com base em uma única lição experimental, cinco anos antes; no entanto, suas previsões foram tão extremas quanto suas avaliações. ¹⁵⁵
Illusion of validity	As pessoas expressam mais confiança em prever a média da nota final de um aluno cujo registro do primeiro ano consiste inteiramente de notas B do que em prever a média da nota de um aluno cujo registro do primeiro ano inclui muitos A e C. Padrões altamente consistentes são observados com mais frequência quando as variáveis de entrada são altamente redundantes ou correlacionadas. Portanto, as pessoas tendem a ter grande confiança nas previsões baseadas em variáveis de entrada redundantes. No entanto, um resultado elementar nas estatísticas de correlação afirma que, dadas as variáveis de entrada com validade declarada, uma previsão baseada em várias dessas entradas pode atingir maior precisão quando são independentes uma da outra do que quando são redundantes ou correlacionadas. Assim, a redundância e as entradas longas diminuem a

For a period of 1 year, each hospital recorded the days on which more than 60 percent of the babies born were boys. Which hospital do you think recorded more such days? (a) The larger hospital (21); (b) the smaller hospital (21); or (c) about the same (that is, within 5 percent of each other) (53)

The values in parentheses are the number of undergraduate students who chose each answer. Most subjects judged the probability of obtaining more than 60 percent boys to be the same in the small and in the large hospital, presumably because these events are described by the same statistic and are therefore equally representative of the general population. In contrast, sampling theory entails that the expected number of days on which more than 60 percent of the babies are boys is much greater in the small hospital than in the large one, because a large sample is less likely to stray from 50 percent. This fundamental notion of statistics is evidently not part of people's repertoire of intuitions.” Cf.: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. *Science*, v. 185, n. 4157, 1974, p. 1125.

¹⁵⁴ “In considering tosses of a coin for heads or tails, for example, people regard the sequence H-T-H-T-T-H to be more likely than the sequence H-H-H-T-T-T, which does not appear random, and also more likely than the sequence H-H-H-H-T-H, which does not represent the fairness of the coin.” Cf.: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. *Science*, v. 185, n. 4157, 1974, p. 1125.

¹⁵⁵ Some subjects were asked to evaluate the quality of the lesson described in the paragraph in percentile scores, relative to a specified population. Other subjects were asked to predict, also in percentile scores, the standing of each student teacher 5 years after the practice lesson. The judgments made under the two conditions were identical. That is, the prediction of a remote criterion (success of a teacher after 5 years) was identical to the evaluation of the information on which the prediction was based (the quality of the practice lesson). The students who made these predictions were undoubtedly aware of the limited predictability of teaching competence on the basis of a single trial lesson 5 years earlier; nevertheless, their predictions were as extreme as their evaluations. Cf.: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. *Science*, v. 185, n. 4157, 1974, p. 1126.

Viés	Exemplo
	precisão, ao mesmo tempo em que aumentam a confiança, e as pessoas geralmente confiam em previsões que provavelmente estão erradas. ¹⁵⁶
Misconceptions of regression	Suponha que um grande grupo de crianças tenha sido examinado em duas versões equivalentes de um teste de aptidão. Se alguém selecionar dez filhos dentre os que se saíram melhor em uma das duas versões, ele geralmente achará o desempenho deles na segunda versão um tanto decepcionante. Por outro lado, se alguém selecionar dez filhos dentre os que tiveram pior desempenho em uma versão, eles encontrarão, em média, um desempenho melhor na outra versão. De maneira mais geral, considere duas variáveis X e Y que têm a mesma distribuição. Se você selecionar indivíduos cuja pontuação média em X se desvia da média de X por k unidades, a média de suas pontuações em Y geralmente se desvia da média de Y em menos de k unidades. ¹⁵⁷

Fonte: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. *Science*, v. 185, n. 4157, p. 1124-1131, 1974.

Ainda que estereótipos e, também, a heurística da representatividade muitas vezes acertem, quando há divergências entre a similaridade e a frequência de ocorrência das observações podem existir vieses. Assim, surgem diversas distorções em percepção de padrões, principalmente daqueles relacionados aos acontecimentos aleatórios.

3.1.2 A heurística da disponibilidade

A *disponibilidade*, por sua vez, trata de avaliar o risco de uma situação ou as chances de algo ocorrer, partindo de o ponto da facilidade desse evento ser pensado pelo indivíduo. Um exemplo é um indivíduo calcular que possui uma maior chance de ter uma doença ‘x’ ao lembrar de pessoas próximas que as tiveram, ainda que não exista nenhum indicativo para tanto.

¹⁵⁶ “[...] people express more confidence in predicting the final grade-point average of a student whose first-year record consists entirely of B's than in predicting the grade point average of a student whose first-year record includes many A's and C's. Highly consistent patterns are most often observed when the input variables are highly redundant or correlated. Hence, people tend to have great confidence in predictions based on redundant input variables. However, an elementary result in the statistics of correlation asserts that, given input variables of stated validity, a prediction based on several such inputs can achieve higher accuracy when they are independent of each other than when they are redundant or correlated. Thus, redundancy along inputs decreases accuracy even as it increases confidence, and people are often confident in predictions that are quite likely to be off the mark (I).”

¹⁵⁷ “Suppose a large group of children has been examined on two equivalent versions of an aptitude test. If one selects ten children from among those who did best on one of the two versions, he will usually find their performance on the second version to be somewhat disappointing. Conversely, if one selects ten children from among those who did worst on one version, they will be found, on the average, to do somewhat better on the other version. More generally, consider two variables X and Y which have the same distribution. If one selects individuals whose average X score deviates from the mean of X by k units, then the average of their Y scores will usually deviate from the mean of Y by less than k units. These observations illustrate a general phenomenon known as regression toward the mean, which was first documented by Galton more than 100”. Cf.: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. *Science*, v. 185, n. 4157, 1974, p. 1126.

Tversky e Kahneman entendem pela existência dos seguintes vieses derivados da heurística da disponibilidade, conforme Tabela 3: “(i) biases due to the retrievability of instances; (ii) biases due to the effectiveness of a search set; (iii) biases of imaginability; e a (iv) illusory correlation”.¹⁵⁸

Tabela 3 - Vieses da heurística da disponibilidade

Viés	Conceito/Exemplo
Biases due to the retrievability of instances ¹⁵⁹	Se um evento é saliente, ele se torna visivelmente mais disponível. Os indivíduos ouviram uma lista de personalidades conhecidas de ambos os sexos e, posteriormente, foram convidados a julgar se a lista continha mais nomes de homens do que de mulheres. Diferentes listas foram apresentadas a diferentes grupos de sujeitos. Em algumas listas, os homens eram relativamente mais famosos que as mulheres, e em outras, as mulheres eram relativamente mais famosas que os homens. Em cada uma das listas, os sujeitos julgaram erroneamente que a classe (sexo) que tinha as personalidades mais famosas era a mais numerosa. ¹⁶⁰
Biases due to the effectiveness of a search set ¹⁶¹	Ver exemplo. Tendo como base uma amostra aleatória de palavras em inglês, de três letras ou mais, seria mais provável que elas começassem com a letra “R” ou que essa fosse a terceira da palavra? A maioria das pessoas resolve esse problema lembrando as palavras que conhecem que começam com a letra “R”, já que são mais salientes que as outras. Por sua vez, a maioria responde ser menos provável que elas apareçam em terceiro lugar. No entanto, a probabilidade de que elas estejam em terceiro é muito maior, já o número de palavras na língua inglesa é muito maior que iniciando com “R”. ¹⁶²
Biases of imaginability ¹⁶³	O indivíduo entende pela probabilidade de um evento ocorrer não com base em instâncias de sua memória, mas de acordo com determinada regra ou atividade. A imaginabilidade desempenha um papel importante na avaliação de probabilidades em situações da vida real. O risco envolvido em uma expedição de aventura, por exemplo, é avaliado imaginando contingências com as quais a

¹⁵⁸ Tradução livre: (i) viés da recuperabilidade de instâncias; (ii) viés devido à eficácia de um conjunto de pesquisa”; (iii) viés da imaginabilidade; e (iv) correlação ilusória.

¹⁵⁹ Tradução livre: viés da recuperabilidade de instâncias”

¹⁶⁰ “[...] subjects heard a list of well-known personalities of both sexes and were subsequently asked to judge whether the list contained more names of men than of women. Different lists were presented to different groups of subjects. In some of the lists the men were relatively more famous than the women, and in others the women were relatively more famous than the men. In each of the lists, the subjects erroneously judged that the class (sex) that had the more famous personalities was the more numerous (6)”. Cf.: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, 1974, p. 1127.

¹⁶¹ Tradução livre: “viés devido à eficácia de um conjunto de pesquisa”.

¹⁶² “[...] Suppose one samples a word (of three letters or more) at random from an English text. Is it more likely that the word starts with r or that r is the third letter? People approach this problem by recalling words that begin with r (road) and words that have r in the third position (car) and assess the relative frequency by the ease with which words of the two types come to mind. Because it is much easier to search for words by their first letter than by their third letter, most people judge words that begin with a given consonant to be more numerous than words in which the same consonant appears in the third position. They do so even for consonants, such as r or k, that are more frequent in the third position than in the first. [...]” Cf.: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, 1974, p. 1127.

¹⁶³ Tradução livre: “viés da imaginabilidade”.

Viés	Conceito/Exemplo
	expedição não está equipada para lidar. Se muitas dessas dificuldades são vividamente retratadas, a expedição pode parecer extremamente perigosa, embora a facilidade com que os desastres sejam imaginados não deva refletir sua probabilidade real. Por outro lado, o risco envolvido em uma empresa pode ser subestimado se alguns perigos possíveis forem difíceis de conceber ou simplesmente não vierem à mente. ¹⁶⁴
Illusory correlation ¹⁶⁵	Há uma correlação ilusória no julgamento de que dois eventos vão co-concorrer. A disponibilidade fornece uma explicação natural para o efeito de correlação ilusória. O julgamento da frequência com que dois eventos co-ocorrem poderia se basear na força do vínculo associativo entre eles. Quando a associação é forte, é provável que se conclua que os eventos foram frequentemente pareados. Consequentemente, julga-se que associados fortes ocorreram juntos com frequência. De acordo com essa visão, a correlação ilusória entre suspeita e desenho peculiar dos olhos, por exemplo, deve-se ao fato de que a suspeita é mais facilmente associada aos olhos do que a qualquer outra parte do corpo. ¹⁶⁶

Fonte: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, p. 1124-1131, 1974

3.1.3 A heurística dos ajustes e ancoragem

Por último, os *ajustes e a ancoragem* correspondem às situações em que uma estimativa é feita a partir de um valor já conhecido, que será ajustado até responder uma determinada questão. Dentre os vieses possíveis, estão casos em que os ajustes são insuficientes ou próprios vieses na avaliação dos eventos conjuntivos e disjuntivos, que podem ser exemplificados como na Tabela 4:

à

¹⁶⁴ “The imaginability plays an important role in the evaluation of probabilities in real-life situations. The risk involved in an adventurous expedition, for example, is evaluated by imagining contingencies with which the expedition is not equipped to cope. If many such difficulties are vividly portrayed, the expedition can be made to appear exceedingly dangerous, although the ease with which disasters are imagined need not reflect their actual likelihood. Conversely, the risk involved in an undertaking may be grossly underestimated if some possible dangers are either difficult to conceive of, or simply do not come to mind.” Cf.: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, 1974, p. 1128.

¹⁶⁵ Tradução livre: “correlação ilusória”.

¹⁶⁶ “Availability provides a natural account for the illusory-correlation effect. The judgment of how frequently two events co-occur could be based on the strength of the associative bond between them. When the association is strong, one is likely to conclude that the events have been frequently paired. Consequently, strong associates will be judged to have occurred together frequently. According to this view, the illusory correlation between suspiciousness and peculiar drawing of the eyes, for example, is due to the fact that suspiciousness is more readily associated with the eyes than with any other part of the body.” Cf.: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, 1974, p. 1128.

Tabela 4 - Descrição dos tipos de evento

Evento simples (elementar)	Evento conjuntivo	Evento disjuntivo.
Sortear uma bolinha vermelha de uma bolsa, cujo seu conteúdo é de 50% bolinhas brancas e 50% de bolinhas vermelhas.	Sortear uma bolinha vermelha sete vezes seguidas de uma bolsa, com reposição, de uma bolsa, contendo 90% de bolas vermelhas e 10% de bolinhas brancas.	Sortear ao menos uma vez uma bola branca, dentro de 7 tentativas sucessivas, com substituição, de uma bola contendo 10% de bolas vermelhas e 90% de bolinhas brancas.

Fonte: TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. *Science*, v. 185, n. 4157, p. 1124-1131, 1974

Segundo o estudo de Tversky e Kahneman¹⁶⁷, de modo geral, a probabilidade de um evento conjuntivo ocorrer é menor que a probabilidade de um evento simples. Assim como na avaliação de risos, as pessoas tendem a subestimar a probabilidade de os eventos disjuntivos ocorrer, mesmo que a essa seja maior que probabilidade que um evento elementar.

Assim, a falácia da conjunção é uma crença equivocada de que dois eventos combinados (conjunções) teriam mais probabilidade de ocorrer, do que apenas um dos eventos isolados. Daniel Kahneman¹⁶⁸ apresenta a seguinte situação:

Linda tem 31 anos de idade, é solteira, franca e muito inteligente.
É formada em filosofia.
Quando era estudante, preocupava-se profundamente com questões de discriminação e justiça social, e também participava de manifestações antinucleares. [...]

Em um de nossos experimentos apresentamos aos participantes uma lista de oito situações possíveis para Linda.

Linda é professora numa escola primária
Linda trabalha numa livraria e faz aula de ioga.
Linda é ativa no movimento feminista.
Linda é assistente social de psiquiatria.
Linda é membro da Liga das Mulheres Eleitoras.
Linda é caixa de banco.
Linda é vendedora de seguros.
Linda é caixa de banco e ativa no movimento feminista.

O autor contextualiza essas afirmações com diversas informações importantes. A Liga das Mulheres não é tão proeminente como era, o movimento feminista também é visto como antiquado. No entanto, o perfil de Linda seria adequado para um movimento feminista, o que

¹⁶⁷ TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. *Science*, v. 185, n. 4157, p. 1124-1131, 1974.

¹⁶⁸ KAHNEMAN, D. **Rápido e devagar**. duas formas de pensar. Rio de Janeiro: Objetiva, 2012.

também seria adequado para alguém trabalharia em uma livraria e de quem faz ioga. Tudo baseado em julgamentos e estereótipos.

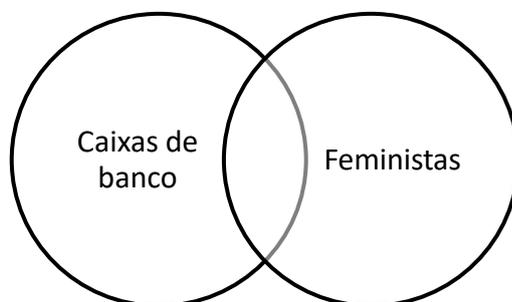
O autor destaca o que acredita ser o item mais crítico: Linda é somente uma caixa de banco, ou uma caixa de banco feminista? Devido às suas características, Linda não é estereotipada como uma caixa de banco, o que faz com que se suponha que se encaixa mais no perfil de “caixa de banco feminista”, do que somente ter essa profissão. No entanto, isso não é tão provável assim:

O conjunto das caixas de banco feministas está inteiramente incluso no conjunto das caixas de banco, já que toda caixa de banco feminista é uma caixa de banco. Logo, a probabilidade de que Linda seja uma caixa de banco feminista *deve* ser menor do que a probabilidade de ela ser uma caixa de banco. Quando você especifica um possível evento em maiores detalhes, você só pode reduzir sua probabilidade. Desse modo, o problema estabelece um conflito entre a intuição da representatividade e a lógica da probabilidade.

Nosso

O autor sugere pensar nos termos do diagrama de Venn, no qual o grupo de caixas de banco feministas está inteiramente incluso no conjunto de caixa de bancos e também no de feministas:

Figura 1 - Diagrama de Venn



Fonte: da autora.

A chance de Linda ser caixa de banco e ativa no movimento feminista é menor ou igual a probabilidade de ser caixa em um banco. Contudo, ao serem perguntados, entre 85% e 90% respondeu que ela era os dois, violando a regra elementar.

3.1.4 Outros vieses

Segundo Cass R. Sunstein e Christine Jolls, pesquisas realizadas por psicólogos e economistas comportamentais levantaram uma série de vieses que criam julgamentos imprecisos. Um dos exemplos é o “viés do otimismo”, que se refere à tendência de as pessoas

acreditarem que a possibilidade de se deparar com uma situação complicada ou ruim é muito menor do que a realidade.¹⁶⁹

A aversão à perda, por sua vez, reflete na inércia que é a vontade de manter suas posses ou sua situação. Por conta desse “medo”, o indivíduo “reluta em abrir mão do que possui porque não deseja perder, acaba rejeitando trocas que teria feito numa situação diferente”¹⁷⁰. Na hipótese, ou na mínima alusão à perda, há espécie de *nudge cognitivo*, que impede tais mudanças, independentemente se estas forem de interesse pessoal.

Além da aversão à perda, há o chamado *viés do status quo*, assim cunhado por William Samuelson e Richard Zeckhauser. Muitas das vezes, as pessoas tendem a manter uma situação, ainda que não seja totalmente benéfica. Uma das causas desse viés seria a falta de atenção, fazendo com que exista uma negligência nas decisões, fazendo com que aquela opção definida com padrão seja mantida sem reflexão alguma.¹⁷¹

3.2 O PATERNALISMO LIBERTÁRIO DE THALES E SUNSTEIN

O termo “Paternalismo Libertário” é formado por dois conceitos que podem ser considerados contraditórios entre si. Thaler e Sunstein combinaram os dois termos por acreditar que eles refletem o bom senso e se tornam mais atraentes quando juntos. O problema, então, reside nos dogmas criados em torno dos termos.¹⁷²

O lado libertário da teoria está na “convicção de que as pessoas devem ter liberdade para fazer o que quiserem, inclusive recusar acordos desvantajosos”¹⁷³. Assim, objetiva-se a criação de políticas que mantenham ou aumentem a liberdade de escolha. O adjetivo “libertário”, então, serve para suavizar o substantivo “paternalismo”, visando a preservação da liberdade individual.¹⁷⁴

¹⁶⁹ JOLLS, C.; SUNSTEIN, C. R. Debiasing through law. *Journal of Legal Studies*, [S. l.], v. 35, n. 1, p. 199–241, 2006.

¹⁷⁰ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade [e-book]. São Paulo: Objetiva, 2019, n.p.

¹⁷¹ SAMUELSON, W.; ZECKHAUSER, R. J. Status Quo Bias in Decision Making. *Journal of Risk and Uncertainty*, mar. 1988, v. 1 n. 1, pp. 7–59.

¹⁷² THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade [e-book]. São Paulo: Objetiva, 2019, n.p.

¹⁷³ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019.

¹⁷⁴ “O lado libertário das nossas estratégias se encontra na convicção de que as pessoas devem ter liberdade para fazer o que quiserem, inclusive recusar acordos desvantajosos. Citando uma expressão do falecido economista Milton Friedman, os paternalistas libertários prezam a “liberdade de escolha”. Procuramos criar políticas que mantenham ou aumentem a liberdade de escolha. Quando usamos o adjetivo “libertário” para modificar o

O paternalismo, então, resume-se na “[...] ideia de que os arquitetos de escolha têm toda a legitimidade para tentar influenciar o comportamento das pessoas, desde que seja para tornar a vida delas mais longa, mais saudável e melhor”¹⁷⁵. Assim, o setor público e privado deve trabalhar de forma a direcionar as pessoas para que essas façam escolhas melhores.

O paternalismo libertário é um tipo de paternalismo relativamente fraco, brando e não intrusivo, pois não cria impedimentos ou obstáculos às escolhas. Se as pessoas querem fumar, se entupir de doces, escolher um tipo de plano de saúde pouco vantajoso ou torrar todo o dinheiro antes da aposentadoria, os paternalistas libertários não vão forçá-las a fazer o contrário — aliás, nem sequer vão colocar empecilhos nessa jornada. Ainda assim, a abordagem que recomendamos é considerada paternalista, pois os arquitetos de escolhas, sejam elas públicas ou privadas, não estão apenas identificando ou colocando em prática as decisões que esperam que as pessoas tomem; na verdade, estão, conscientemente, induzindo as pessoas a seguir caminhos que melhorarão sua vida. Estão dando um *nudge*.¹⁷⁶

Em linhas gerais, o paternalismo libertário une a filosofia política do paternalismo que visa a promoção do bem-estar individual ao libertarismo, respeitando a liberdade do indivíduo, sem aplicação de qualquer tipo de coerção. A grande justificativa para isso, então, está no fato de as pessoas tomarem decisões ruins, opostas àquelas que teriam caso tivessem todas as informações necessárias, capacidades cognitivas ilimitadas, autocontrole ou atenção. Ele serve como uma via de mão dupla, protegendo o bem-estar individual e evitando perdas econômicas e sociais.

3.2.1 Os *nudges*

Os *nudges*, segundo Thaler e Cass R. Sunstein, são sugestões indiretas que podem influenciar positivamente o processo de escolha. De maneira alguma podem impor uma ou outra opção, ou minimizar as chances de escolha de uma opção.¹⁷⁷

substantivo “paternalismo”, é apenas no sentido de preservar a liberdade. E estamos falando sério em relação a preservar a liberdade. Os paternalistas libertários querem que cada vez mais as pessoas sigam seu próprio caminho, e não impor obstáculos.” THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade [e-book]. São Paulo: Objetiva, 2019, n.p.

¹⁷⁵ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

¹⁷⁶ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

¹⁷⁷ “Nudges are interventions that steer people in particular directions but that also allow them to go their own way. A reminder is a nudge; so is a warning. A GPS nudges; a default rule nudges. To qualify as a nudge, an intervention must not impose significant material incentives. A subsidy is not a nudge; a tax is not a nudge; a fine or a jail sentence is not a nudge. To count as such, a nudge must fully preserve freedom of choice. If an intervention imposes significant material costs on choosers, it is not a nudge.” Cf.: SUNSTEIN, C. R. The Ethics of Nudging. *SSRN Electronic Journal*, [S. l.], v. 24, n. 6, p. 27, 2014. Disponível em: <http://www.ssrn.com/abstract=2526341>

Esse *nudge*, na nossa concepção, é um estímulo, um empurrãozinho, um cutucão; é qualquer aspecto da arquitetura de escolhas capaz de mudar o comportamento das pessoas de forma previsível sem vetar qualquer opção e sem nenhuma mudança significativa em seus incentivos econômicos. Para ser considerada um *nudge*, a intervenção deve ser barata e fácil de evitar. Um *nudge* não é uma ordem. Colocar as frutas em posição bem visível é um exemplo de *nudge*. Simplesmente proibir a *junk food*, não. ¹⁷⁸

Inclusive, a palavra *nudges* também é um anacronismo que serve como parâmetro para estruturar intervenções:

IN centives
U nderstand mappings,
D efaults
G ive feedback,
E xpect errors,
S alience/Structuring complex
choices

Decisões podem ser difíceis por inúmeros motivos, por desafiar a capacidade de autocontrole, por não existir tempo para reflexão, entre outras razões. Os *nudges* seriam empregados então, nas situações em que as pessoas costumam tomar decisões não tão boas, combatendo falhas cognitivas, influenciando as escolhas de forma a atingir o bem-estar desses indivíduos.

Thaler e Sunstein apresentam 05 (cinco) situações relacionadas às “decisões difíceis”, nas quais os *nudges* poderiam ser inseridos. A primeira, “benefícios agora, custos depois”, são aquelas relativas aos “bens de investimentos”, bens e/ou hábitos que vão ser benéficos, ainda que demorem tempo para se provar assim. Como exemplo, há a prática de exercício físico, que de pronto não oferece tantos resultados, mas que ao longo prazo, sim. No sentido oposto, existem os “bens pecaminosos”, como cigarro, álcool, doces, entre outros, que trazem prazer na hora e consequências tardias. As escolhas atreladas a essa primeira categoria muito se relacionam à capacidade de autocontrole do indivíduo.¹⁷⁹

¹⁷⁸ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

¹⁷⁹ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

A segunda categoria é o “grau de dificuldade” que versa sobre a frequência que não se tem ao alcance ferramentas, conhecimento ou tecnologias adequadas para se embasar a tomada de decisão. A terceira categoria, “frequência”, diz respeito à evolução que a prática causa. Por óbvio, não há como se praticar a maioria das decisões importantes, mas é possível empregar *nudges* para evitar que sejam tomadas decisões ruins.

O *feedback*, a quarta categoria, é necessário para com que se aprenda após cada tentativa. No entanto, o *mundo real* nem sempre oferece essa possibilidade e, quando oferece, foca-se apenas das opções escolhidas e não nas rejeitadas. Por último, na quinta categoria está “saber do que você gosta”. Segundo os autores, quando não se consegue traduzir as escolhas que se faz nas experiências que serão proporcionadas, não é tão fácil tomar boas decisões.

Para Acquisti *et al.*, esses *nudges* podem ser divididos em 06 (seis) categorias: informação, apresentação, padrões, incentivos, reversibilidade e resiliência à erros, e *timing*, como mostrado na Tabela 5.180 Essas, por sua vez, estão interligadas e não são mutualmente exclusivas.

Tabela 5 - Categorias de nudges

Dimensão	Subdimensão	Obstáculos direcionados
Informação. Reduz as assimetrias de informação e fornece uma perspectiva realista dos riscos.	Educação Feedback	Informação assimétrica e incompleta, heurística da disponibilidade Informação assimétrica e incompleta, racionalidade limitada, heurística de disponibilidade, viés de otimismo e excesso de confiança
Apresentação. Fornece as sugestões contextuais necessárias na interface do usuário para reduzir a carga cognitiva e transferir o nível apropriado de risco.	Enquadramento Ordem Destaque Estruturação	Aversão à perda, viés de otimismo e excesso de confiança, heurística de representatividade Erros pós-conclusão, ancoragem Heurística de disponibilidade, viés do otimismo e excesso de confiança Racionalidade limitada, heurística da disponibilidade, representatividade
Padrões. Reduz o esforço do usuário, configurando o sistema de acordo com as expectativas dos usuários.	-	Viés do status quo

180 ACQUISTI, A. *et al.* Nudges for Privacy and Security. *ACM Computing Surveys*, [S. l.], v. 50, n. 3, 2017, p. 44:2

Dimensão	Subdimensão	Obstáculos direcionados
Incentivos. Motiva os usuários a se comportarem de acordo com as preferências declaradas.	Aumento de custos Recompensas /Punições	Aversão à perda. Desconto hiperbólico, preferências de aversão à perda.
Reversibilidade (resiliência aos erros). Limita o impacto dos erros.	-	Nenhum em particular. O objetivo é permitir que os usuários se recuperem de decisões sub-ótimas potencialmente causadas por preconceitos comportamentais.
Timing. Define o momento certo para empregar o <i>nudge</i> .	-	Cada técnica de cutucada pode ser necessária em diferentes momentos

Fonte: ACQUISTI, Alessandro *et al.* Nudges for Privacy and Security: Understanding and Assisting Userss Choices Online. **SSRN Electronic Journal**, [S. l.], v. 50, n. 3, 2016. Disponível em: <https://www.ssrn.com/abstract=2859227>

Os *nudges* são extremamente benéficos quando se analisa o comportamento dos seres humanos em face das opções padrão. Kapsner and Sandfuchs exemplificam esse fato com a quantidade de doadores de órgãos na Áustria e na Alemanha. Enquanto no primeiro país todos os cidadãos são doadores, exceto se optarem pelo contrário, na Alemanha ocorre o oposto.¹⁸¹ Contudo, isso não significa que não existam críticas ou problemas nessa teoria.

3.2.2 As críticas ao Paternalismo Libertário e aos *nudges*

Por óbvio, alguns tipos de *nudges* e modelos de arquitetura de escolha podem suscitar discussões éticas. Isso, porque eles podem ser utilizados tanto para promover discriminações (raciais, sexuais, religiosas, entre outras), quanto reforçar informações falsas. Ainda que eles não possuam um objetivo ilícito, há falha ética em sua construção e aplicação.¹⁸²

Sunstein pontua quatro principais preocupações relativas aos *nudges* e os modelos de arquitetura de escolha, que devem ser sempre pautados pelo bem-estar, a autonomia de escolha, a dignidade e o autogoverno. Essas preocupações envolvem: autonomia, dignidade, manipulações e aprendizagem, sendo que por todos estes aspectos se concluiriam que os *nudges*

¹⁸¹ KAPSER, A. SANDFUCHS, B. Nudging as a Threat to Privacy. **Rev. Phil. Psych**, 2015, 6:455– 468, p. 455. Disponível em: <<http://link.springer.com/article/10.1007/s13164-015-0261-4>>. Acesso em: 20 fev. 2020.

¹⁸² SUNSTEIN, C. R. The Ethics of Nudging. **SSRN Electronic Journal**, v. 24, n. 6, 2014, p. 3.

poderiam ou violariam direitos individuais. Inclusive, isso poderia ocorrer mesmo nos casos em que não há intenção de causar um ilícito.¹⁸³

As críticas feitas ao Paternalismo quanto à possibilidade de cerceamento da autonomia dos indivíduos, violando direitos da personalidade, também recaem ao Paternalismo Libertário, aqui na figura da arquitetura das escolhas. No entanto, o último é uma forma muito mais branda de Paternalismo, cuja liberdade de escolha é orientada por seus meios. Dessa forma, não haveria uma supressão de garantias fundamentais e de liberdades individuais.¹⁸⁴

Em sentido parecido, há a preocupação de que os *nudges* sejam, na verdade, um método de coerção para a retirada de um indivíduo da inércia, sem que esse realmente tenha este desejo. No entanto, para evitar esse tipo de situação, os arquitetos de escolhas devem incorporar esse risco, de maneira que permitam a liberdade de escolha irrestrita.

No entanto, a maioria das críticas comete o equívoco de que existiriam alternativas ao Paternalismo, quando na verdade não há. Agentes públicos e privados, constantemente, tomam decisões que afetam a vida de outras pessoas. Essas decisões, então, podem ser tomadas sob a ótica do paternalismo libertário que abranda a intervenção no processo de escolha.¹⁸⁵

Por exemplo, uma cafeteria será obrigada a escolher como irá organizar seus produtos, mesmo que seja para deixá-los expostos de maneira aleatória. E a forma de disposição impactará diretamente nas vendas. O paternalismo libertário sugeriria, então, organizar os produtos de forma a incentivar uma escolha mais racional e que cause a reflexão no sujeito que a faz.

Com a aplicação dos *nudges* do paternalismo libertário em diferentes áreas do conhecimento, as críticas acima são complementadas por problemáticas exclusivas de cada tema. Por conta disso, o próximo Capítulo tem como função aprofundar e expandir a aplicação

¹⁸³ SUNSTEIN, C. R. The Ethics of Nudging. *SSRN Electronic Journal*, v. 24, n. 6, p. 1-32, 2014.

¹⁸⁴ “To be sure, some behavioral biases are not easy to analyze in these terms. If people suffer from present bias, is a nudge a form of paternalism about means? Suppose that people eat high calorie food, or drink a great deal, or fail to exercise, because they value today and tomorrow, and not so much next year or next decade. If a nudge succeeds in getting people to focus on their long-term interests, it might increase aggregate (intrapersonal) welfare over time. But is such a nudge focused solely on means? If a person is seen a series of selves extending over time, the choice architect is effectively redistributing welfare from earlier selves to later ones (and by hypothesis maximizing welfare as well). But it is not clear that we can speak, in such cases, of means paternalism. And if a person is seen as continuous over time, and not a series of selves, efforts to counteract present bias are, by hypothesis, undermining the ends of the chooser at the time of choice. It is hard question whether the relevant ends are those that the chooser has at that time or at a later time, or whether it is best (as I tend to think) to identify the chooser’s ends by focusing on some aggregation or index of selves over a lifetime.” SUNSTEIN, C. R. The Ethics of Nudging. *SSRN Electronic Journal*, [S. l.], v. 24, n. 6, p. 27, 2014. Disponível em: <http://www.ssrn.com/abstract=2526341>. Acesso em: 20 fev. 2020.

¹⁸⁵ SUNSTEIN, Cass. R.; THALER, Richard. H. Libertarian Paternalism Is not an Oxymoron. *University of Chicago Law Review*, v. 70, n. 40, 2003, p. 1161.

e, conseqüentemente, as discussões e os problemas na aplicação nesta teoria na privacidade e proteção de dados pessoais.

4 A ECONOMIA DA PRIVACIDADE, OS *NUDGES* E A PROTEÇÃO DE DADOS PESSOAIS NA *INTERNET*

O estudo da privacidade também é objeto da análise econômica do direito, a qual se foca na questão da privacidade informacional, ou seja, nas informações pessoais e os problemas e oportunidades criadas por sua coleta, seu processamento, disseminação e invasão. Assim, tem como objetivo “[...] avaliar os custos e benefícios associados à mudança dos limites entre as esferas públicas e privadas, e da proteção ou divulgação de informações e/ou dados pessoais, tanto aqueles tangíveis quanto intangíveis”.¹⁸⁶

Decisões relacionadas à privacidade muitas vezes envolvem o balanço entre controle daquilo que é compartilhado e os custos e benefícios de compartilhar ou esconder alguma informação pessoal. A Economia da Privacidade aborda exatamente esses *trade-offs* associados ao equilíbrio das esferas públicas e privadas, entre organizações, governo e indivíduos. Aqui interessa a dimensão informacional que compreende exatamente na intersecção da proteção e da divulgação de informações pessoais:

Broadly speaking, privacy economics deals with informational trade-offs: it tries to understand, and sometimes quantify, the costs and benefits that data subjects (as well as potential data holders) bear or enjoy when their personal information is either protected or shared. Privacy economics also tries to understand how to use market mechanisms, technology, or policy to achieve a desirable balance between information revelation and protection, with satisfaction shared among the individual, organizations, and society as a whole.¹⁸⁷

Em 2014, Acquisti iniciou uma pesquisa que consistia na aplicação de teorias e metodologias de economia comportamental para entender o processo de decisão. Focou nos vieses comportamentais e cognitivos, da aversão aos riscos à gratificação imediata. Concluiu ser necessário mais teorias para entender como os desafios e os obstáculos afetam a maneira como decisões são tomadas sobre informações pessoais. Essas dificuldades podem vir de

¹⁸⁶ “The economics of privacy can highlight the costs and benefits associated with the changing boundaries between public and private spheres, and in particular, with the protection and revelation of personal information.” BRANDIMARTE, L.; ACQUISTI, A. **The Economics of Privacy**, [S. l.: s. n.]. 2012., p. 550. Disponível em: <<http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780195397840.001.0001/oxfordhb>>. Acesso em: 22 dez. 2019.

¹⁸⁷ Tradução livre: “Em termos gerais, a economia da privacidade lida com trocas informacionais: tenta entender e, algumas vezes, quantificar os custos e benefícios que os titulares dos dados (assim como os possíveis titulares de dados) suportam ou desfrutam quando suas informações pessoais são protegidas ou compartilhadas. A economia da privacidade também tenta entender como usar mecanismos, tecnologia ou política de mercado para alcançar um equilíbrio desejável entre revelação e proteção de informações, com satisfação compartilhada entre o indivíduo, as organizações e a sociedade como um todo.” ACQUISTI, A. Nudging privacy: the behavioral economics of personal information. **IEEE Digital Enlightenment Yearbook 2012**, 2012, p. 83.

diversos fatores, como “inconsistent preferences and frames of judgment”; “information about risks, consequences, or solutions inherent to provisioning (or protecting) personal information”; “bounded cognitive abilities that limit our ability to consider or reflect on the consequences of privacy-relevant actions”, etc.^{188,189,190}

A forma com que as pessoas tendem a fazer escolhas relativas à privacidade são influenciadas diretamente pela assimetria informacional. Isso significa que o indivíduo, objeto da coleta de dados, sabe menos sobre o processo que aquele que a coleta – e muitas vezes até mais sobre o próprio indivíduo. Em outras palavras, aqueles que coletam dados para suas atividades possuem mais conhecimento sobre a magnitude desse processo e suas implicações presentes e futuras.

A sociedade se modificou pela forma que a *Internet* é organizada e que os dados são coletados e utilizados. Essa mudança causou diversas consequências que a maioria das pessoas não consegue mensurar. Assim, não há como concluir que, em geral, os indivíduos são capazes de analisar esse fenômeno.¹⁹¹ Essa “cegueira” é chamada de *bounded rationality*, uma vez que seres humanos, frequentemente, substituem os métodos de tomada de decisões por simplificados modelos mentais e heurísticas.¹⁹²

Ainda se o acesso a todas essas informações for possível, não se pode assegurar que os usuários escolheriam da melhor forma. Diversas anomalias comportamentais e vieses fazem com que as pessoas escolham diferentemente como previsto pela teoria da escolha racional.¹⁹³

A realidade, no entanto, é de que as escolhas de um usuário da *Internet* serão geralmente feitas com base em informações incompletas. O controle pessoal sobre a esfera

¹⁸⁸ ACQUISTI, A. Nudging privacy: the behavioral economics of personal information. **IEEE Digital Enlightenment Yearbook 2012**, 2012, p. 83.

¹⁸⁹ “Such hurdles might stem from a combination of factors: inconsistent preferences and frames of judgment; opposing or contradictory needs (such as the need for publicity combined with the need for privacy); incomplete information about risks, consequences, or solutions inherent to provisioning (or protecting) personal information; bounded cognitive abilities that limit our ability to consider or reflect on the consequences of privacy-relevant actions; and various systematic (and therefore predictable) deviations from the abstractly rational decision process. ACQUISTI, A. Nudging privacy: the behavioral economics of personal information. **IEEE Digital Enlightenment Yearbook 2012**, 2012, p. 83.

¹⁹⁰ “Especially in the presence of complex, ramified consequences associated with the protection or release of personal information, our innate bounded rationality limits our ability to acquire, memorize, and process all relevant information, and it makes us rely on simplified mental models, approximate strategies, and heuristics”. ACQUISTI, A.; GROSSKLAGS, Jens. Privacy and rationality in individual decision making. **IEEE Security & Privacy Review**, Jan./Feb. 2005. p. 27.

¹⁹¹ ACQUISTI, A.; GROSSKLAGS, J. What Can Behavioral Economics Teach Us about Privacy? In: ACQUISTI, A. et al. **Digital Privacy: Theory, Technologies and Practices**. London: Auerbach Publications, 2008, p. 356.

¹⁹² THALER, R. H.; SUNSTEIN, C. R. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. São Paulo: Objetiva, 2019.

¹⁹³ CAMERER, C. F.; LOEWENSTEIN, G. **Behavioural Economics: Past, Present, Future**. 2002. Available at: <<http://people.hss.caltech.edu/~camerer/ribe239.pdf>>. Acesso em: 08 jun 2019.

informacional é no mínimo difícil de se autodeterminar.¹⁹⁴ Um exemplo disso, como suscitado por Acquisti e Grossklags, é que a informação assimétrica “often prevent a subject from knowing when another entity has gained access to or uses their personal information”¹⁹⁵. Consequentemente, o objeto pode não ter todo o conhecimento sobre as possíveis consequências da violação de privacidade.

A informação incompleta e a assimetria informacional possuem significados distintos. Segundo Acquisti *et al*, o primeiro termo pode ser utilizado para se referir àquelas situações em que os agentes econômicos possuem informações incompletas sobre uma situação concreta. Já o segundo termo é utilizado para se referir àquelas situações em que os agentes possuem diferentes níveis de informação, um conhece muito, o outro nem tanto.¹⁹⁶

Para Rodotà, os usuários da *Internet* estão em uma situação de disparidade de poder em relação aos fornecedores desses serviços.¹⁹⁷

Pode-se acrescentar, de modo mais geral, que o usuário de serviços informáticos e telemáticos se encontra em tal situação de disparidade de poder em relação aos fornecedores de tais serviços que, a rigor, não se pode falar em consentimento livremente manifestado para transações referentes à privacidade.

Assim, aquele que possui mais informações possui uma vantagem sobre aquele que

The term “incomplete information” can be used to refer to situations where economic agents lack information pertaining to a transaction. The term “asymmetric

¹⁹⁴ POSNER, R. A. Values and Consequences: An Introduction to Economic Analysis of Law. **Journal of Political Economy**, [S. l.], 1998.

¹⁹⁵ ACQUISTI, A.; GROSSKLAGS, Jens. What Can Behavioral Economics Teach Us about Privacy? In: ACQUISTI, A. et al. **Digital Privacy: Theory, Technologies and Practices**. London: Auerbach Publications, 2008, p. 356.

¹⁹⁶ “The term “incomplete information” can be used to refer to situations where economic agents lack information pertaining to a transaction. The term “asymmetric information” can be used to refer to situations where agents who interact in a transaction have differential access to information relevant to that transaction: one party may have more or better information than other parties. The party who is better informed is often in an advantageous position when completing the transaction; however, asymmetric information can cause widespread adverse effects and inefficiencies. [...]

Consider the market for used cars. The seller of a used car knows the car’s actual history and quality, while its potential buyers have limited information. The uncertainty regarding the car’s quality leads potential buyers to discount the value of used cars sold on the market: because the used car could be a “lemon,” buyers’ willingness to pay for the average car is lower than what it would have been under symmetric, complete information. As a result, owners of good cars may stop selling them, when their reservation price is higher than buyers’ average evaluation of used cars. Thus, asymmetric information may crowd the best cars out of the market, leaving only lower-quality cars for sale. Anticipating this result, potential buyers for? Then reduce their willingness to pay for the average car, giving rise to a vicious circle that may result in the market’s failure ”.” ACQUISTI, A. *et al*. Nudges for Privacy and Security: Understanding and Assisting Users Choices Online. **SSRN Electronic Journal**, [S. l.], v. 50, n. 3, 2016, p. 44:4. Disponível em: <<https://www.ssrn.com/abstract=2859227>>. Acesso em: 20 fev. 2020.

¹⁹⁷ RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008. p. 76.

information” can be used to refer to situations where agents who interact in a transaction have differential access to information relevant to that transaction: one party may have more or better information than other parties. The party who is better informed is often in an advantageous position when completing the transaction; however, asymmetric information can cause widespread adverse effects and inefficiencies.[...]

Consider the market for used cars. The seller of a used car knows the car’s actual history and quality, while its potential buyers have limited information. The uncertainty regarding the car’s quality leads potential buyers to discount the value of used cars sold on the market: because the used car could be a “lemon,” buyers’ willingness to pay for the average car is lower than what it would have been under symmetric, complete information. As a result, owners of good cars may stop selling them, when their reservation price is higher than buyers’ average evaluation of used cars. Thus, asymmetric information may crowd the best cars out of the market, leaving only lower-quality cars for sale. Anticipating this result, potential buyers further reduce their willingness to pay for the average car, giving rise to a vicious circle that may result in the market’s failure.¹⁹⁸

A assimetria informacional e as informações incompletas são questões que permeiam privacidade e segurança da informação. Isso, porque, como apresentado pelo autor, o defensor poderá não ter conhecimento de que artimanha o “adversário” utilizará para “atacar”, assim como o agente de tratamento possui mais informações sobre o propósito da coleta e as condições de uso futuro desses dados.¹⁹⁹

Os que defendem a habilidade de discernimento dos usuários veem políticas públicas que visam à proteção da privacidade como interferências no desenvolvimento das TICs e nos benefícios que estas podem trazer. Os que possuem opinião contrária se preocupam exatamente com a habilidade individual de administrar essa questão em meio de complexos *trade-offs*. Assim, as ferramentas existentes no processo de decisão de privacidade, como escolhas e

¹⁹⁸ Tradução livre: “O termo “informação incompleta” pode ser usado para se referir a situações em que os agentes econômicos não possuem informações referentes a uma transação. O termo “informação assimétrica” pode ser usado para se referir a situações em que agentes que interagem em uma transação têm acesso diferencial a informações relevantes para essa transação: uma parte pode ter mais ou melhor informação do que outras. A parte que está melhor informada geralmente fica em uma posição vantajosa ao concluir a transação; no entanto, informações assimétricas podem causar efeitos adversos generalizados e ineficiências. [...]

Considere o mercado de carros usados. O vendedor de um carro usado conhece o histórico e a qualidade reais do carro, enquanto seus potenciais compradores têm informações limitadas. A incerteza em relação à qualidade do carro leva os potenciais compradores a descontar o valor dos carros usados vendidos no mercado: porque o carro usado pode ser um “limão”, a disposição dos compradores de pagar pelo carro médio é menor do que seria informações completas e simétricas. Como resultado, os proprietários de bons carros podem parar de vendê-los, quando o preço da reserva for superior à avaliação média dos compradores de carros usados. Assim, informações assimétricas podem afastar os melhores carros do mercado, deixando apenas carros de qualidade inferior à venda. Antecipando esse resultado, os compradores em potencial se destacam? reduzem sua disposição de pagar pelo carro médio, dando origem a um círculo vicioso que pode resultar em falha do mercado.” ACQUISTI, A. *et al.* Nudges for Privacy and Security: Understanding and Assisting Userss Choices Online. **SSRN Electronic Journal**, [S. l.], v. 50, n. 3, 2016, p. 44:4. Disponível em: <<https://www.ssrn.com/abstract=2859227>>. Acesso em: 20 fev. 2020.

¹⁹⁹ ACQUISTI, A. *et al.* Nudges for Privacy and Security: Understanding and Assisting Userss Choices Online. **SSRN Electronic Journal**, [S. l.], v. 50, n. 3, 2016. Disponível em: <<https://www.ssrn.com/abstract=2859227>>. Acesso em: 20 fev. 2020.

consentimento, não seriam suficientes para proteção. Deve-se alterar o foco da responsabilidade individual para uma intervenção regulatória como forma de balanço dos interesses do indivíduo e o poder dos órgãos governamentais e da iniciativa privada.

O ser humano, segundo o pensamento de Westin enfrenta a privacidade de modo situacional, podendo ser pragmático, fundamentalista, sem consciência, dependendo do contexto, do momento e do local em que se encontra.²⁰⁰ Essa pluralidade de interesses é mantida e se intensifica com o advento da *Internet*, uma vez que os benefícios da divulgação são muito maiores por conta da própria tecnologia.

As diretrizes utilizadas pelas pessoas ao administrar a privacidade variam de situação para situação e são aprendidas com o tempo, baseada em motivações, critérios culturais e situacionais. Por conta disso, torna-se necessário entender o processo de decisão e as escolhas.

4.1 PROCESSO DE DECISÃO E ESCOLHA DO USUÁRIO NA *INTERNET*

Os benefícios provenientes da abertura de seus dados pessoais para terceiros, não são apenas de natureza econômica para quem os cede. Ao usar um celular, por exemplo, absorve-se o risco de que o provedor de serviço pode monitorar as ligações e a forma que a *Internet* é utilizada, por exemplo.²⁰¹ Aqui, a conveniência de poder usufruir de um serviço é suficiente, independentemente de contraprestação monetária para o usuário.

Como já mencionado, a preocupação frente ao tema depende também do tipo de informação solicitada. Enquanto dados financeiros e bancários acendem uma luz vermelha, dados relacionados a interesses e aos costumes normalmente não levantam preocupações dos usuários. Do mesmo modo, a sensação de controle do uso posterior ou da disseminação dessas informações também é correlata à preocupação.²⁰²

Ainda que a privacidade e a proteção de dados possa ser uma preocupação dos usuários de *Internet*, existem inconsistências e contradições a respeito de como são abordadas, já que os usuários, voluntariamente, compartilham essas informações. Inclusive, evidências empíricas

²⁰⁰ WESTIN, A. F. **Privacy and Freedom**. New York: Athenäum, 1967.

²⁰¹ ANTONIALLI, Denny. ABREU, Jacqueline. **Vigilância das comunicações pelo Estado Brasileiro**. Internetlab, 2017.

²⁰² ACQUISTI, A.; BRANDIMARTE, L. The Economics of Privacy. *In: Threats arising from digitization and the Internet*. [S. l.: s. n.]. p. 547–571.

corroboram essa afirmação, mostrando que existe uma lacuna entre as preferências expressas e aquelas reveladas.²⁰³⁻²⁰⁴

Berendt *et al.* conduziram experimento cujo objetivo inicial era investigar os fatores determinantes e os impedimentos da interação *online* em geral. A hipótese era que as preocupações com a privacidade fossem um dos principais impeditivos para uma interação *online* profunda e verdadeira. Desse modo, o estudo focou em como as essas preocupações se relacionavam com o comportamento real, às autorreferidas, e ao impacto final nas declarações feitas.²⁰⁵

No experimento, 206 participantes deviam comprar, *online*, câmeras e jaquetas com seu próprio dinheiro. Como incentivo para participar, os produtos eram oferecidos com um desconto de 60% quando comparados com lojas locais.

Antes de iniciar a compra, os participantes preencheram um questionário, sendo que ¼ (25%) das perguntas era relacionado à privacidade, quanto disposição em compartilhar dados privados, sua confiança geral nas declarações de privacidade e as reações pretendidas a vários cenários. Foi pedido para que os participantes assinassem a declaração de privacidade da loja, aceitando a venda de seus dados a um patrocinador anônimo da pesquisa.

Um grupo recebeu uma declaração de privacidade cordial, informando que seus dados de navegação seriam entregues ao patrocinador que era uma empresa europeia de boa reputação. Assim, informaram os seus direitos segundo a Diretiva Europeia de Proteção Dados (95/46/EC)²⁰⁶, ou seja, o direito de ser informado sobre quem processa os dados e para qual finalidade; de inspecionar os dados; de impor a alteração de dados incorretos; e se recusar a consentir com tipos específicos de uso. Por sua vez, o outro grupo recebeu uma declaração de privacidade concisa, que não mencionava a Diretiva, mas somente que não se sabia como o patrocinador usaria os dados coletados.

Para auxiliar em suas compras, estava a Luci, um *bot* de compras antropomórfico. Assim, no começo do experimento ela se apresentava e explicava sua função. E, antes de entrar

²⁰³ BERENDT, B; GÜNTHER, O; SPIEKERMANN, S. Privacy in e-commerce. **Communications of the ACM**, [S. l.], v. 48, n. 4, p. 101–106, 2005. Disponível em: <http://portal.acm.org/citation.cfm?doid=1053291.1053295>

²⁰⁴ HERMSTRÜWER, Y. Contracting Around Privacy. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, [S. l.], v. 45, n. 8, p. 9–26, 2017.

²⁰⁵ BERENDT, Bettina; GÜNTHER, Oliver; SPIEKERMANN, Sarah. Privacy in e-commerce. **Communications of the ACM**, [S. l.], v. 48, n. 4, p. 101–106, 2005. Disponível em: <http://portal.acm.org/citation.cfm?doid=1053291.1053295>. Acesso em: 20 fev. 2020.

²⁰⁶ PARLAMENTO EUROPEU. **Diretiva 95/46/EC**, de 24/10/1995. Disponível em <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31995L0046> >. Acesso em: 22 fev. 2020

na loja, era ofertada ao usuário a oportunidade de preencher seu endereço, sem que houvesse qualquer requisito para isso.

Os usuários, então, eram convidados para responder uma série de 56 perguntas para que se chegasse em uma lista personalizada de 10 produtos. O *bot* não se focava somente nas especificações dos produtos, mas também fazia perguntas que poderiam ser feitas em uma venda física. O objetivo era incluir mais questões que trouxessem mais informações pessoais que não mudariam a escolha do melhor modelo.

A última análise, então, comparou as preferências autodeclaradas com o real comportamento dos indivíduos. Em suma, o experimento apresentou os seguintes resultados e conclusões:

- a) quatro grandes grupos de usuários:
 - os “fundamentalistas da privacidade” (30%);
 - os que possuem aversão ao *profiling* (26%): mais preocupados em revelar informações sobre seus interesses, como hobbies, preferências etc.;
 - os marginalmente preocupados (24%);
 - os preocupados com a identidade (20%): mais prováveis em revelar informações como nome, e-mail, endereço etc.
- b) a proporção de informações reveladas era menor entre os *fundamentalistas da privacidade*, quando comparados com os *marginalmente preocupados*;
- c) entre os *preocupados com a identidade* e os que possuem *aversão ao profiling*, foi demonstrado uma proporção intermediária de compartilhamento, relativamente de acordo com as preferências declaradas;
- d) o tipo de declaração de privacidade entregue não teve um impacto significativo na estatística, ainda que aquele que citava a Diretiva fez com que mais pessoas preenchessem seu endereço;
- e) a maioria dos participantes gostaram do meio de comunicação empregado e se sentiram pessoalmente abordados e auxiliados pela Luci, mesmo quando os produtos indicados não foram satisfatórios.

O mais alarmante, contudo, foi que ao contrário do que se esperava, o nível absoluto de compartilhamento de informações entre todos os grupos foi muito maior, desmentindo as preferências previamente expressadas, que demonstravam relutância para a divulgação de dados e informações pessoais.

Este estudo reforça a ideia da existência de um paradoxo, uma dicotomia entre as preferências de privacidade e o real comportamento. Em outras palavras, uma lacuna entre as preferências expressadas e aquelas reveladas.²⁰⁷⁻²⁰⁸⁻²⁰⁹

Segundo a teoria das preferências revelada, as escolhas de privacidade podem ser vistas como uma direta expressão das verdadeiras preferências de privacidade dos usuários. Contudo, a teoria ignora por completo evidências psicológicas da incerteza das preferências, o fato de que alguns indivíduos não as compreendem de modo completo. Por conta disso, a Economia da Privacidade coloca em xeque a relação entre escolha, interesse próprio, utilidade e bem estar.²¹⁰

Para Acquisti e Grossklags²¹¹, a dificuldade no processo de tomada de decisão é influenciada e dificultada por uma série de barreiras, como a assimetria informacional, racionalidade limitada e vieses cognitivos e comportamentais. Esses últimos, por sua vez, induziriam o indivíduo a se desviar sistematicamente de uma estratégia que seria ideal (maximização da utilidade) para o ser humano racional. Há uma visível vulnerabilidade na relação agentes de tratamento-usuários. Nesse sentido, Bruno Bioni²¹²:

Tome-se como exemplo a cadeia de agentes econômicos do mercado informacional, notadamente a plêiade de atores da rede (network) da publicidade comportamental (vide subcapítulo 1.2.2.4). Em geral, apesar de as tradicionais relações de consumo envolverem mais de um ator na sua cadeia de produção, elas jamais alcançam a miríade de agentes presentes no arranjo da economia da informação. Logo, o fosso da assimetria, seja ela econômica ou informacional, é maior por concentrar mais sujeitos no outro polo da relação, a desequilibrá-la mais ainda.

Complementarmente, o autor entende que “[a] própria lógica do trade-off da economia dos dados pessoais é traiçoeira, portanto, frente a tal arquitetura de escolha de decisões,

²⁰⁷ ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and human behavior in the age of information. *Science* **347 (6221)**, 509-514, New York, v. 347, n. 6221, 2017, p. 509

²⁰⁸ HERMSTRÜWER, Y. Contracting Around Privacy. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, [S. l.], v. 45, n. 8, p. 9-26, 2017.

²⁰⁹ Como pontuado Garfinkel e Laura Mendes, a criação de uma dicotomia entre tecnologia e privacidade não seria a melhor solução. Isso porque o desenvolvimento tecnológico deve ocorrer em observância da preservação da privacidade dos cidadãos.

Garfinkel (2000) faz uma ligação com a crise ambiental das décadas de 1950 e 1960, na qual diversos recursos ambientais foram desperdiçados e destruídos “em nome do progresso”. Esse foi o custo para o desenvolvimento econômico, criação de empregos e outros avanços que a sociedade entendia ser necessário à época. No entanto, hoje é sabido que o desenvolvimento sustentável não só é possível, como é essencial para a preservação da vida humana na Terra. Desse modo, não seria diferente no âmbito do desenvolvimento tecnológico atual.

²¹⁰ HERMSTRÜWER, Y. Contracting Around Privacy. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, [S. l.], v. 45, n. 8, p. 9-26, 2017.

²¹¹ ACQUISTI, A.; GROSSKLAGS, J. Economics of Information Security. *IEEE Security and Privacy*, [S. l.], 2005.

²¹² BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 224.

notadamente por essa idiossincrasia entre gratificações imediatas e prejuízos mediatos/distantes”.²¹³ Logo, a falsa percepção que o cidadão é capaz de desempenhar processos genuínos de tomada de decisão, na tentativa de controle consciente de seus dados pessoais, é desafiada pela própria complexidade do tema. Existe uma vulnerabilidade específica, justamente pela relação assimétrica.

Ainda, o autor comenta a operação econômica, em que não existe deslocamento patrimonial, cuja contraprestação pelo bem de consumo é fixada pecuniariamente. Isso, porque, segundo a lógica dessa economia digital, “os dados são a moeda de troca pelo bem de consumo”²¹⁴. Por conta da coleção de dados e da complexidade de fluxos informacionais, o usuário, consumidor de ferramentas e plataformas da *Internet*, não possui qualquer tipo de domínio sobre os custos da transação econômica, tendo em vista a incerteza do alcance do fluxo dos dados pessoais, do tratamento possível e as consequências que esse último pode trazer. E tanto o tipo de dano causado, quanto o seu tamanho, muitas vezes não pode ser antevista.

Hermstrüwer entende que a maioria das pessoas coloca os custos e benefícios do consentimento, no que chama de diferentes “contas mentais”. Ainda que relutantes em pagar por privacidade, o autor entende que isso não significa que os usuários nunca estariam dispostos a incorrer em custos para a proteção de dados. Na verdade, isso reforça ainda mais que as preferências de privacidade são dependentes e determinadas conforme o contexto, por processos psicológicos frente às escolhas.²¹⁵

Por conta disso, afirma que, “[t]he obvious challenge for privacy law results from the fact that it cannot capture and regulate every context feature that might push users to disclose personal information”²¹⁶. Como solução, propõe a determinação de características estruturais que são, em grande parte, independentes do contexto.

No âmbito regulatório e legal, por sua vez, é importante entender as razões que explicam os fatores estruturais que permeiam o paradoxo da privacidade. Isso, porque, sem esse entendimento, o direito à privacidade utilizará instrumentos não tão adequados para empoderar

²¹³ BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 209.

²¹⁴ BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 224.

²¹⁵ HERMSTRÜWER, Y. Contracting Around Privacy. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, [S. l.], v. 45, n. 8, p. 9–26, 2017.

²¹⁶ Tradução livre: “O desafio óbvio da lei de privacidade resulta do fato de que ela não pode capturar e regular todos os recursos de contexto que podem levar os usuários a divulgar informações pessoais”. HERMSTRÜWER, Y. Contracting Around Privacy. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, [S. l.], v. 45, n. 8, 2017, p. 17.

peças e mantê-las livres e informadas de suas escolhas. Por isso, a seguir são apresentados tais fatores estruturais para, posteriormente, entender quais são os instrumentos adequados.²¹⁷

4.1.1 Os *trade-offs*

Muitas vezes, as experiências passadas criam preocupações. Em outras não, como é o caso do *Facebook*. Ainda que a empresa tenha sido ligada a diversos escândalos relacionados ao vazamento de dados ou à invasão de privacidade²¹⁸⁻²¹⁹⁻²²⁰, a rede social continua sendo utilizada por milhões de usuários. Tais escândalos não são restritos às empresas privadas, mas também são relacionados à vigilância governamental²²¹, como exposto pelo Wikileaks e por Edward Snowden.

Como exposto anteriormente, ainda que a privacidade e a proteção de dados possam ser uma preocupação dos usuários de *Internet*, existem inconsistências e contradições a respeito de como são abordadas. Por um lado, entende-se que os usuários possuem a capacidade total de proteger suas informações sensíveis e pessoais. Do outro, acabam abrindo mão dessas, em troca de pequenas recompensas.²²²

Os chamados *trade-offs* associados com as decisões de privacidade, ou de segurança, não só são complexos, mas são nuances. Isso, porque, são pouquíssimas as vezes em que segurança e privacidade são tarefas primárias dos usuários finais que possuem recursos limitados para avaliar opções e prever as consequências de suas ações.

Se segurança e privacidade raramente são tarefas primárias dos usuários finais e, ainda, os usuários têm recursos mentais limitados para avaliar todas as opções e consequências possíveis de suas ações²²³, pode-se entender que há um aumento da incerteza e ambiguidades

²¹⁷ HERMSTRÜWER, Y. Contracting Around Privacy. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, [S. l.], v. 45, n. 8, p. 9–26, 2017.

²¹⁸ LAPOWSKY, I. Facebook exposed 87 million users to Cambridge Analytica. **WIRED**, 4 abr 2018. Disponível em: <<https://bit.ly/2IUlptC>>. Acesso em: 08 jun. 2018.

²¹⁹ CONFESSORE, N. Cambridge Analytica and Facebook: the scandal and the fallout so far.. **The New York Times**, 4 abr 2018. Disponível em: <<https://nyti.ms/2GBQ4Lm>>. Acesso em: 08 jun. 2018.

²²⁰ OSBORNE, H. What is Cambridge Analytica? The firm at the centre of Facebook's data breach. **The Guardian**, 18 mar 2018.. Disponível em: <<https://bit.ly/2prhWXb>>. Acesso em: 08 jun 2018.

²²¹ BOLZAN, J. L.; NETO, E. J. D. M. A Insuficiência do Marco Civil da Internet na Proteção das Comunicações Privadas Armazenadas e do Fluxo de Dados a Partir do Paradigma de Surveillance. In: LEITE, R. **Marco Civil da Internet**. São Paulo: Atlas, 2014.

²²² ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and human behavior in the age of information. **Science** **347** (6221), 509-514., New York, v. 347, n. 6221, 2017. p. 509

²²³ Herb Simon chama esse fenômeno de “bonded rationality que seria “[...] The capacity of the human mind for formulating and solving complex problems is very small compared with the size of the problems whose solution

inerentes, associadas com esses *trade-offs*, de modo que as configurações “[...] may be key to unlocking additional functionalities and to deriving (seemingly) more value from a given system”²²⁴.

Para analisar os *trade-offs* entre os custos da privacidade e os benefícios de transações da Internet, Dinev e Hart desenvolveram e testaram empiricamente um modelo de preferências de privacidade. Ainda que as preocupações reduzam a vontade do indivíduo em completar transações na *Internet*, a confiança entre o vendedor e o controle sobre os dados contribuem de forma a gerar uma sensação de segurança que diminui essas preocupações. Consequentemente, o indivíduo fica mais disposto a compartilhar seus dados.²²⁵

A grande questão em torno dos *trade-offs* é o desvio da escolha racional que possui diretamente impacto significativo para a tomada de decisão em assuntos de privacidade e segurança. Como explicado por Acquisti, essas tomadas de decisão sobre privacidade podem envolver divulgação, o que traz aos indivíduos alguma gratificação imediata, como interação social ou acesso aos serviços desejados, enquanto os sujeita a custos de privacidade que podem ser somente percebidos meses ou até anos depois.²²⁶

4.1.2 A incerteza dos usuários

Alessandro Acquisti diz que os indivíduos administram os limites do público e privado de diversos modos, como pela separação, reserva e anonimidade, protegendo suas informações pessoais, mas também dissimulando informações. Esses limites são traçados por diversas

is required for objectively rational behavior in the real world — or even for a reasonable approximation to such objective rationality. SIMON, H. A. A behavioral model of rational choice. **The Quarterly Journal of Economics**, vol. 69, n. 1, feb. 1957, p. 198.

²²⁴ Tradução livre: “[...] pode ser a chave para desbloquear funcionalidades adicionais e obter (aparentemente) mais valor de um determinado sistema”. ACQUISTI, A. *et al.* Nudges for Privacy and Security: Understanding and Assisting Userss Choices Online. **SSRN Electronic Journal**, [S. l.], v. 50, n. 3, 2016, p. 44:2. Disponível em: <<https://www.ssrn.com/abstract=2859227>>. Acesso em: 21 fev. 2020.

²²⁵ DINEV, T.; HART, P. An extended privacy calculus model for e-commerce transactions. **Information Systems Research**, [S. l.], v. 17, n. 1, p. 61–80, 2006.

²²⁶ “For instance, privacy decision making may involve disclosure, which brings individuals some immediate gratification, such as social interaction or access to desired services, while simultaneously subjecting them to privacy costs that may be incurred months or even years later. For example, Jentzsch et al. [2012] found that given a choice of two movie ticket providers requiring different amounts of personal information and charging different prices, people preferred monetary savings (an immediate gain) over privacy (a longer term risk). However, when the tickets were offered at the same price, the privacy-friendly provider gained the larger market share, suggesting that people do care about privacy, but they often heavily discount the risk of disclosing personal information.” ACQUISTI, A. *et al.* Nudges for Privacy and Security: Understanding and Assisting Userss Choices Online. **SSRN Electronic Journal**, [S. l.], v. 50, n. 3, 2016. Disponível em: <<https://www.ssrn.com/abstract=2859227>>. Acesso em: 21 fev. 2020.

razões, como a necessidade da intimidade e resguardo pessoal, ou pelo desejo de se proteger contra a influência da sociedade e controle.²²⁷

Portanto, Acquisti associa o motivo dessa incerteza à assimetria informacional, causada diretamente pelos avanços da tecnologia e a transformação da coleta e do tratamento de dados pessoais em uma ação invisível, longe dos olhos de seu titular. Logo, não é simples ou corriqueiro se ter o conhecimento de quais dados ou informações são acessadas por terceiros, ou como são utilizados. Conseqüentemente, a incerteza reflete sobre o que devem, o que não devem, quando e como devem divulgá-las. Ainda que muitas pessoas aleguem se preocupar com sua privacidade e desejem proteger dados e informações pessoais.

Acquisti apresenta 02 (dois) fatores que tornam difícil medir as conseqüências do comportamento da privacidade. Em primeiro lugar, aponta que, enquanto alguns malefícios são tangíveis, como prejuízos financeiros causados por uso indevido de dados pessoais, outros são intangíveis, como a divulgação de histórias de uma pessoa. Em segundo lugar, a privacidade sempre envolve *trade-offs*. Contudo, existem elementos que mitigam esses fatores, seja aumentando a visibilidade dos malefícios intangíveis, quanto destacando os *trade-offs* de maneira a fazê-los compreensíveis e explícitos.

Além disso, as pessoas são incertas quanto suas preferências de privacidade. Segundo o autor, o estudo da incerteza de preferência demonstrou que pessoas têm pouca percepção de quanto gostam de produtos, serviço e até outras pessoas – o que faz com que a privacidade não seja uma exceção:

[...] This can be illustrated by research in which people were asked sensitive and potentially incriminating questions either point-blank, or followed by credible assurances of confidentiality. Although logically such assurances should lead to greater divulgence, they often had the opposite effect because they elevated respondents' privacy concerns, which without assurances would have remained.²²⁸

²²⁷ ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and Human Behavior in the Information Age*. In: **The Cambridge Handbook of Consumer Privacy**. [S. l.: s. n.]. p. 184–197.

²²⁸ Tradução livre: “[...] Isso pode ser ilustrado por pesquisas nas quais as pessoas foram submetidas a perguntas sensíveis e potencialmente incriminadoras à queima-roupa ou seguidas de garantias credíveis de confidencialidade. Embora logicamente essas garantias devam levar a uma maior divulgação, elas geralmente têm o efeito oposto, porque elevam as preocupações com a privacidade dos entrevistados, que sem garantias teriam permanecido”. ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and human behavior in the age of information. **Science** **347** (6221), 509-514., New York, v. 347, n. 6221, 2017. ISSN 1095-9203. Disponível em: <<https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHu>, p. 510. Disponível em: <https://www.cambridge.org/core/product/identifier/9781316831960%23CN-bp-10/type/book_part>. Acesso em: 20 fev. 2020.

As situações envolvendo transação de privacidade ocorrem com muita frequência. Inclusive, os *trade-offs* não desaparecem mesmo quando são intangíveis, ou quando a troca de dados pessoais não é a fonte primária desse movimento.

A incerteza é impulsionada pela motivação individual e contraditória de ser público e privado, divulgar e resguardar, sem com que consiga fazer essas divisões de forma pormenorizada. Como já mencionado, a natureza humana é social, logo, a troca de informação é uma peça central na estrutura social, econômica e comportamental.

Assim, essa incerteza e a dependência do tempo, espaço e contexto, é prova de que as pessoas e, por consequência, os usuários da *Internet*, não estão completamente preparados para administrar os riscos dos *trade-offs*. Há uma constante falta de informação sobre o que é divulgado, de como será utilizada e suas consequências, além da incerteza quanto as suas preferências de privacidade – são raras as situações em que os usuários possuem total conhecimento das consequências.

Além disso, pessoas são facilmente influenciadas sobre a quantidade de informações que pretendem compartilhar. E tais informações compartilhadas acabam por influenciar suas emoções, pensamentos e comportamento em diversos aspectos em sua vida. Ainda que essa influência nem sempre seja maléfica, a renúncia ou a maleabilidade do controle sobre a privacidade e dados pessoais altera o equilíbrio de poder entre quem detém os dados e aqueles que são os sujeitos desses dados.²²⁹

Tendo em vista que as pessoas estão à deriva quando se trata das consequências e, também, dos seus sentimentos sobre privacidade, acabam se orientando por pistas ou comportamento alheios para guiar suas escolhas. Por isso, as preferências são maleáveis e influenciadas, tanto pelo contexto, pelos interesses envolvidos, ou até mesmo pelas informações que o indivíduo tem acesso.

Ademais, seres humanos são animais sociais, sendo o compartilhamento de informações uma característica central da conexão humana. Inclusive, a *Social Penetration Theory* sugere que aumentar progressivamente os níveis de auto revelação é uma evolução natural e desejável dos relacionamentos interpessoais. Para tanto, torna-se necessário diminuir barreiras de intimidade.²³⁰

²²⁹ ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and Human Behavior in the Information Age*. In: **The Cambridge Handbook of Consumer Privacy**. [S. l.: s. n.]. p. 184–197. E-book. Disponível em: <https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHumanBeh.pdf>. Acesso em: 24 maio 2018.

²³⁰ ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and Human Behavior in the Information Age*. In: **The Cambridge Handbook of Consumer Privacy**. [S. l.: s. n.]. p. 184–197. E-book. Disponível em: <https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHumanBeh.pdf>. Acesso em: 24 maio 2018.

Logo, não há razão para supor que em todas as situações em que decidem por uma determinada preferência de privacidade, farão escolhas coerentes quanto se trata dos *trade-offs* da privacidade e outros objetivos.²³¹ Isso é corroborado por Thaler e Sunstein, quando dizem que os seres humanos não são tão precisos quanto presumem e não fazem escolhas tão boas quando se é esperado.²³²

4.1.3 As heurísticas e vieses no processo de proteção à privacidade e aos dados pessoais

Pesquisas no campo da economia comportamental, mais especificamente do processo de tomada de decisão, encontraram diversas incongruências nas escolhas do usuário. As preferências, em geral, são influenciadas por fatores contextuais. Pessoas criam preferências baseadas em como as alternativas são moldadas ou como a informação é apresentada quando assim existem. Então, as escolhas são feitas com base em comparações e de acordo com o *background* de quem as faz.

Como mencionado, a heurística da disponibilidade diz respeito ao cálculo da probabilidade que um indivíduo faz para definir se um evento “x” acontecerá e, com isso, tomar uma decisão. Como parâmetro, utiliza-se eventos próximos, com relação e/ou impacto direto ou indireto à vida da pessoa que está realizando essa comparação, ou daqueles a sua volta.

Ao aplicar essa heurística na tomada de decisões relacionadas à privacidade e à proteção de dados, os mesmos parâmetros são utilizados. Diferentemente de casos de doenças, como apresentado no exemplo do item 3.1.2, eventos alarmantes de violação a esses direitos não possuem um impacto direto e mensurável à vida da maioria dos cidadãos.

O *Facebook* é um exemplo de empresa frequentemente relacionada a vazamentos de dados pessoais. Em setembro de 2018, um ataque às suas redes expôs dados pessoais de 50 milhões de usuários.²³³⁻²³⁴ Em abril de 2019, a empresa UpGuard revelou que o *Facebook* havia

²³¹ ACQUISTI, A. Nudging Privacy: The Behavioral Economics of Personal Information. **IEEE Security & Privacy Magazine**, s.l., v. 7, n. 6, p. 72-85, nov. 2009.

²³² THALER, Richard H.; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade [e-book]. São Paulo: Objetiva, 2019, n.p.

²³³ ISAAC, M; FRENKEL, S. Facebook Security Breach Exposes Accounts of 50 Million User. **New York Times**, New York, 28 set. 2018. Disponível em: <<https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html>>. Acesso em: 20 fev. 2020

²³⁴ W WONG, J. C. Facebook says nearly 50m users compromised in huge security breach. **The Guardian**, Londres, 29 sep 2018. Disponível em: <<https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach>> Acesso em: 20 fev. 2020

feito *upload* de mais de 540 milhões de dados pessoais nos servidores de nuvem da Amazon, contendo nomes, fotos, informações sobre amigos, eventos, reservas de viagem etc.²³⁵ Em dezembro do mesmo ano, mais de 267 milhões de IDs de usuários, números de telefones e nomes foram expostos em uma base de dados de acesso público.²³⁶ Todos esses incidentes ocorreram após o grande escândalo do Cambridge Analytica.

Independentemente dos escândalos dos últimos dois anos, o número de usuários diariamente ativos do Facebook cresceu em 9% (nove por cento) em 2019 em comparação ao ano anterior, chegando em 1.62 bilhões de usuários.²³⁷ Ou seja, a probabilidade de um incidente ocorrer não diminuiu o uso e a adesão de novos usuários à rede social.

As consequências da violação da privacidade não são facilmente estimadas ou previstas pelos usuários. A principal razão para isso é que a proteção de dados é muitas vezes adiada e distorcida por eles. Como exemplo está o fato de que os Termos de Uso e Políticas de Privacidade são ignorados, já que são documentos extensos, muitas vezes cheios de informações técnicas e de difícil compreensão²³⁸ ou, nas palavras de Ari E. Waldman “[p]rivacy policies are confusing, inconspicuous, and inscrutable”²³⁹.

Além disso, muitos usuários acreditam erroneamente que a existência de Termos de uso e Políticas de Privacidade, por si só, são grandes indicativos preocupação dos agentes de tratamento com a proteção de dados do titular:

Various so-called “antecedents” affect privacy concerns and can be used to influence privacy behavior. For instance, trust in the entity receiving one’s personal data soothes concerns. Moreover, because some interventions that are intended to protect privacy can establish trust, concerns can be muted by the very interventions intended to protect privacy. Perversely, 62% of respondents to a survey believed (incorrectly) that the existence of a privacy policy implied that a site could not share their personal information without permission, which suggests that simply posting a policy that consumers do not read may lead to misplaced feelings of being protected.²⁴⁰

²³⁵ <https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/>

²³⁶ WONG, Queenie. Millions of Facebook user phone numbers exposed online, security researchers say. **CNET**, 19 dec. 2019. Disponível em <<https://www.cnet.com/news/millions-of-facebook-user-phone-numbers-exposed-online-security-researchers-say/>>. Acesso em: 27 fev. 2020.

²³⁷ FACEBOOK. **Facebook Reports Third Quarter 2019 Results**. Disponível em: <<https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Third-Quarter-2019-Results/default.aspx>>. Acesso em: 20 fev. 2020.

²³⁸ ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and Human Behavior in the Information Age. In: **The Cambridge Handbook of Consumer Privacy**. [S. l.: s. n.]. p. 184–197. *E-book*. Disponível em: <https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHumanBeh.pdf>. Acesso em: 24 maio 2018.

²³⁹ WALDMAN, Ari E. Privacy, Notice, and Design. **Stanford Tech Law Review**, v. 21:1, 2018, p. 76.

²⁴⁰ Tradução livre: “Vários dos chamados “antecedentes” afetam as preocupações com a privacidade e podem ser usados para influenciar o comportamento da privacidade. Por exemplo, confiar na entidade que recebe os dados pessoais alivia preocupações. Além disso, como algumas intervenções destinadas a proteger a privacidade podem estabelecer confiança, as preocupações podem ser silenciadas por essas próprias intervenções destinadas a proteger

As preocupações quanto à privacidade diversas vezes estão em função de experiências já vivenciadas²⁴¹ – ou seja, vinculada à heurística da ancoragem. Nesse sentido, Oulasvirta *et al.* desenvolveram uma pesquisa em Helsinki, na qual foi instalado um sistema de detecção e monitoramento em algumas casas. Inicialmente, os membros da família modificaram o seu comportamento, principalmente em relação a conversas, à nudez e ao sexo. No entanto, a preocupação com a privacidade diminuía depois de fazer certas ações pela primeira vez, como caminhar nus na cozinha em frente aos sensores. Assim, foi visível que os participantes se acostumaram com a presença da tecnologia com o passar do tempo, relevando seus impactos.²⁴²

As heurísticas são recorrentes no pensamento dos seres humanos e são acompanhadas de vieses. No entanto, acredita-se ser possível minimizar danos, diminuir ou ao menos compensar a assimetria informacional, alinhando as preferências declaradas de privacidade, com as ações de fato dos usuários.

4.2 OS NUDGES NA PRIVACIDADE E NA PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

Os *nudges* podem ser empregados em diversas áreas como uma forma suave de intervenção paternalística para auxiliar na tomada de decisão de privacidade e segurança no âmbito da *Internet*. Assim, como pontuado Acquisti *et al.*, as discussões relacionadas a essas intervenções se encontram em diferentes posições ao longo do espectro do paternalismo e do libertarismo.²⁴³

a privacidade. Perversamente, 62% dos participantes de uma pesquisa acreditavam (incorretamente) que a existência de uma política de privacidade implicava que um site não podia compartilhar suas informações pessoais sem permissão, o que sugere que simplesmente publicar uma política que os consumidores não leem pode levar a sensações equivocadas de estar protegido.”ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and human behavior in the age of information. *Science* 347 (6221), 509-514., New York, v. 347, n. 6221, 2017. ISSN 1095-9203. Disponível em: <<https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHu>, p. 556. Disponível em: https://www.cambridge.org/core/product/identifier/9781316831960%23CN-bp-10/type/book_part. Acesso em: 20 fev. 2020.

²⁴¹ ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and human behavior in the age of information. *Science*, [S. l.], v. 347, n. 6221, p. 509–514, 2015. Disponível em: https://www.cambridge.org/core/product/identifier/9781316831960%23CN-bp-10/type/book_part

²⁴² OULASVIRTA, A. *et al.* Long-term effects of ubiquitous surveillance in the home. In: 2012, **UbiComp’12 - Proceedings of the 2012 ACM Conference on Ubiquitous Computing**. [S. l.: s. n.]

²⁴³ “We acknowledge, however, that the discussed interventions may be at different positions along the spectrum between strict paternalistic and libertarian approaches—with some, like transparency, being designed to provide limited influence on an individual’s choice, and others, like defaults, more forcefully and predictably affecting users’ decisions.” ACQUISTI, A. *et al.* Nudges for Privacy and Security. *ACM Computing Surveys*, [S. l.], v. 50, n. 3, 2017, p. 44:2

Como ferramenta para o desenho dessas, se retoma o anacronismo de *nudges*, ou seja, “iNcentives, Understand mappings, Defaults, Give feedback, Expect errors, Saliency/Structuring complex choices”, mas também adicionando pesquisa de usabilidade, reversão de vieses e tecnologias persuasivas. A desconstrução desses vieses engloba ações que tentam ajudar a tomada de decisão humana, diminuindo a cegueira causada por um comportamento racional limitado.

As tecnologias persuasivas são sistemas de computação, produtos ou aplicações que foram desenhadas intencionalmente para mudar a atitude ou comportamento de uma determinada forma. Sua aplicação é vasta, desde para a melhora da alimentação, para prática de exercício, mudança de rotas de trânsito, diminuição de consumo de energia elétrica, entre outras aplicações.²⁴⁴

Para a análise dos *nudges* na proteção de dados na Sociedade Informacional, utiliza-se das categorias apresentadas no item 3.2.1. O principal objetivo, então, é entender as bases concretas de aplicação desses empurrões na proteção da privacidade e dos dados pessoais dos usuários.

4.2.1 A dimensão da informação e os *nudges*

Os *nudges* de informação têm principal objetivo reduzir os malefícios da assimetria informacional, a racionalidade limitada e as heurísticas da disponibilidade, o viés do otimismo e o excesso de confiança. Assim, seu método de ação é o fornecimento de informações para criar uma consciência sobre os riscos de segurança e privacidade. Para tanto, os arquitetos desses *nudges* precisam considerar esses diferentes vieses, inclusive de modo a incentivar um comportamento adequado, ou, então, para evitar resultados indesejados. Essa dimensão é dividida nas subdimensões da *educação* e do *feedback*.

A educação fornece informações para os usuários frente a determinado sistema ou característica, sendo o que, inicialmente, norteia as decisões. Os usuários devem decidir sobre diversas opções de preferências de privacidade ao usar aplicativos ou plataformas. Assim, antes mesmo de fazer esse uso, pode ser educado quanto aos benefícios e aos riscos associados.

²⁴⁴ SEGERSTÅHL, Katarina; OINAS-KUKKONEN, Harri. Distributed User Experience in Persuasive Technology Environments. *In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. [S. l.: s. n.]. p. 80–91. *E-book*. Disponível em: <http://link.springer.com/10.1007/978-3-540-77006-0_10>. Acesso em: 20 fev. 2020

O MCI apresenta que o dever constitucional do Estado na prestação da educação também inclui a capacitação para o uso seguro, consciente e responsável da *Internet*, para o exercício da cidadania, cultura e desenvolvimento tecnológico. No entanto, essa responsabilidade não cabe apenas Poder Público, mas também aos provedores de conexão e aplicação da *Internet* e a sociedade civil.

A existência de documentos que descrevam quais dados são coletados e como serão tratados, não significa que existe um processo de educação. Até porque, na maioria dos casos, Termos de Uso e Políticas de Privacidade não são realmente lidos, por conta da sua extensão e complexidade.

Outro ponto a ser ressaltado é que o uso de plataformas na *Internet* estabelece contratos de adesão, regidos por uma política de “[...] pegar ou largar, dando assim aos [Termos de Serviços] a força de uma ‘lei da plataforma’, que é estabelecida e modificável de forma exclusiva pelo provedor da plataforma”.²⁴⁵ Desse modo, é estabelecido um controle unilateral sobre as ações permitidas ou não dos usuários e, principalmente, quais, como e quantos dados serão coletados e o seu tratamento.²⁴⁶ A melhor forma de informar os usuários, então, é utilizar informações concisas e claras para identificar as diferentes configurações de privacidade, afastando-se do tecnicismo que envolve o funcionamento da *Internet*.

A educação dos usuários, com a disponibilização de informações concisas, é um objetivo desejável. Porém, isso não é garantia de que os usuários podem atingir as suas preferências declaradas em cenários complexos. Ainda que disponíveis, informações destacadas podem ser ignoradas quando vieses entram em cena no processo de decisão.

Por sua vez, o *feedback* deve ser fornecido ao longo do uso do sistema. O mecanismo de *feedback* permite que os usuários façam decisões melhores ao longo do tempo, podendo também apresentar um paralelo entre os resultados esperados e aqueles que serão obtidos de acordo com a decisão tomada. *Feedbacks* bem desenhados, portanto, fazem com que os usuários verifiquem que houve alguma modificação no resultado, mitigando os efeitos da assimetria informacional ou da racionalidade limitada.

²⁴⁵ BELLI, L.; FRANCISCO, P. A.; NOTA, N. Z. Lei do Estado ou lei da Plataforma? Cuidado com a privatização da regulação e da polícia. In: BELLI, L.; CAVALLI, O. **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2019, p. 540.

²⁴⁶ BELLI, L.; VENTURINI, J. Private ordering and the rise of terms of service as cyber-regulation. **Internet Policy Review**, 5(4), v. 5, n. 4, 2016.

A teoria da escolha racional assume que os indivíduos são racionais e possuem um conjunto de preferências estáveis. Assim, os usuários se tornam capazes de processar quantidade indefinida de informações, além de sempre pautar suas escolhas na maximização da sua utilidade.

A Teoria dos Jogos, por sua vez, também se baseia no paradigma da escolha racional e analisa as interações estratégicas entre os atores. Por essa abordagem, o consentimento depende de escolhas ou, mais precisamente, das estratégias escolhidas pelas companhias e os outros usuários. O consentimento, então, terá as características de uma escolha em um jogo estratégico.²⁴⁷

Como resultado, a erosão da privacidade não resulta necessariamente da racionalidade limitada dos usuários. Em contrapartida, o consentimento para o processamento de dados e informações pessoais poderá ser o resultado de um cálculo racional. Então, combater a racionalidade limitada pode facilitar escolhas estratégicas para usuários sofisticados e acelerar a erosão da privacidade, mostrando os limites e possíveis inconvenientes de reverter o viés de instrumentos normativos sobre o tema.²⁴⁸

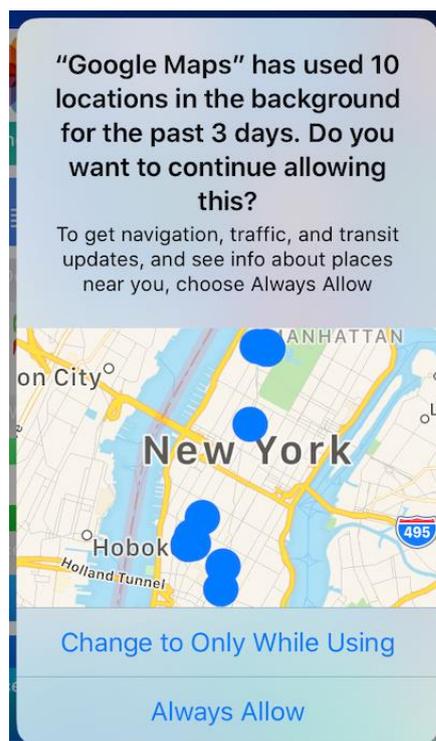
Avisos de privacidade pontuais fazem com que as práticas de *websites* se destaquem, funcionando como *nudges*, incentivando os usuários da *Internet* a utilizar serviços que possuam políticas de dados mais respeitadoras. Um exemplo disso são os medidores de segurança de senhas que demonstram se a senha escolhida por um usuário é fraca, média ou forte, fazendo com que se escolha uma combinação mais benéfica ao usuário. Nesse caso há um *feedback* em tempo real.

Outro exemplo é uma funcionalidade do sistema operacional iOS 13, da Apple, que, de tempos em tempos, demonstra por meio de notificação o quanto um aplicativo está utilizando de seus dados de localização, inclusive quando ele não está em uso. Essa notificação dá a possibilidade de, na mesma tela, restringir que o uso desses dados seja feito somente quando o aplicativo for utilizado, como mostrado na Figura 2.

Figura 2 - Tela notificação de dados de localização da Apple

²⁴⁷ HERMSTRÜWER, Yoan. Contracting Around Privacy. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, [S. l.], v. 45, n. 8, p. 9–26, 2017.

²⁴⁸ HERMSTRÜWER, Yoan. Contracting Around Privacy. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, [S. l.], v. 45, n. 8, p. 9–26, 2017.



Fonte: WHITTAKER, Z. iOS 13: Here are the new security and privacy features you need to know. **Tech Crunch**. 03 set. 2019. Disponível em: <<https://techcrunch.com/2019/09/19/ios-13->

Esse tipo de *nudge* faz com que chamada de atenção quanto às configurações de privacidade remetam às preferências declaradas. Assim, tal mecanismo se apresenta como eficiente para reduzir possíveis malefícios. Como será visto adiante, o uso do *privacy by design* é uma prática alinhada com essa questão.

Em contrapartida, também são utilizados recursos de *design* que frustram ou até confundem os usuários de forma que divulguem mais dados e informações que gostariam, prática chamada de *malicious interface design*²⁴⁹, ou *dark patterns*²⁵⁰, que são interfaces de *design* que guiam os usuários terem determinados comportamentos por meio de interações maliciosas.²⁵¹

4.2.2 A dimensão da Apresentação e os *nudges*

²⁴⁹ CONTI, Gregory; SOBIESK, Edward. Malicious interface design: Exploiting the user. In: 2010, **Proceedings of the 19th International Conference on World Wide Web, WWW '10**. [S. l.: s. n.]

²⁵⁰ Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. **Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems**, 2020. Disponível em: <https://arxiv.org/abs/2001.02479v1>. Acesso em: 20 fev. 2020.

²⁵¹ ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and Human Behavior in the Information Age*. In: **The Cambridge Handbook of Consumer Privacy**. [S. l.: s. n.], p. 512. Disponível em: <<https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHumanBeh.pdf>>. Acesso em: 24 maio. 2018.

Os *nudges* de apresentação são aqueles que fornecem sugestões contextuais na interface do usuário, com o objetivo de reduzir a carga cognitiva e transferir o nível apropriado de risco. Eles combatem informações e escolhas baseadas em vieses comportamentais, como aversão à perda, otimismo irrealista e excesso de confiança e heurísticas de representatividade. Para tanto, são divididos em 04 (quatro) subdimensões, o enquadramento, a regulamentação, a projeção e a estruturação.

Conforme explica Acquisti *et al.*, o *enquadramento* se preocupa com a forma como os benefícios e os riscos das escolhas são comunicados. Isso, porque as informações que são transmitidas aos usuários podem ser apresentadas de forma a facilitar a avaliação dos riscos envolvidos em uma transação específica. Assim, quando um indivíduo não compreende o risco da forma que deveria, por conta do viés de excesso de confiança, o arquiteto do *nudge* pode exagerar a forma com a qual o risco se apresenta, como uma maneira de compensar a interpretação suavizada.²⁵²

Utilizando-se do viés de aversão à perda, é possível apresentar esses riscos como uma perda clara. O exemplo trazido por Acquisti *et al.* é do excesso de confiança de um motorista que subestima o risco de acelerar e superestima a economia de tempo por fazer isso.²⁵³

O mesmo acontece com os usuários na *Internet*. Nesse caso, é possível mitigar a heurística da representatividade, auxiliando os usuários na avaliação de riscos com maior precisão. Para tanto, é necessário que as informações sejam estruturadas de forma a apoiar os usuários na distinção entre a representatividade de um evento e a probabilidade de esse ocorrer.

Como já mencionado, a maneira de apresentação das opções ou a forma com que um fluxo deve ser seguido, influenciam na escolha dos usuários. Inclusive, é sabido que, por conta do viés de ancoragem e ajuste, a primeira informação oferecida afeta a percepção do usuário sobre as opções restantes. Aqui se encontra a subdimensão da *ordem*.²⁵⁴

O *destaque*, por sua vez, relaciona-se ao *enquadramento* e à *ordem*, uma vez que pode atenuar ou alavancar vieses de disponibilidade e excesso de confiança. Isso, porque pode fazer com que as pessoas se concentrem e pensem em certos elementos, em vez de outros, ao tomar uma decisão.²⁵⁵

²⁵² ACQUISTI, A. *et al.* Nudges for Privacy and Security. *ACM Computing Surveys*, [S. l.], v. 50, n. 3, 2017, p. 44:2

²⁵³ ACQUISTI, A. *et al.* Nudges for Privacy and Security. *ACM Computing Surveys*, [S. l.], v. 50, n. 3, 2017, p. 44:2

²⁵⁴ ACQUISTI, A. *et al.* Nudges for Privacy and Security. *ACM Computing Surveys*, [S. l.], v. 50, n. 3, 2017, p. 44:2

²⁵⁵ ACQUISTI, A. *et al.* Nudges for Privacy and Security. *ACM Computing Surveys*, [S. l.], v. 50, n. 3, 2017, p. 44:2

Ainda que o *enquadramento*, a *ordem* e o *destaque* sejam utilizados para superar obstáculos na tomada de decisão, é necessária a existência de uma *estrutura*. Ela serve como estratégia essencial para lidar com obstáculos em decisões complexas que exigem a avaliação de várias opções e alternativas.

4.2.3 A dimensão dos Padrões e os *nudges*

As configurações padrão são importantes ferramentas utilizadas em diversas frentes na divulgação de informações. Como já demonstrado por Thaler e Sunstein, elas são convenientes e, portanto, acabam sendo adotadas sem uma reflexão de serem ou não benéficas. São interpretadas como recomendações implícitas.²⁵⁶

Essas configurações acabam por maximizar lucros e interesses dos agentes de dados, justamente pela ciência do comportamento dos usuários. Em uma rede social, por exemplo, a coleta de informações será sempre maximizada e, conseqüentemente, os padrões serão sempre os mais abertos possíveis. Além disso, ao permitir uma maior visibilidade de um perfil, há direta interferência no comportamento relativo à privacidade, uma vez que os usuários se sentem mais à vontade para divulgar informações já que os outros também o fazem. Assim, essas configurações padrões podem ser desenhadas para preservar a privacidade dos usuários.

Os padrões reduzem o esforço do usuário ao configurar o sistema de acordo com uma expectativa presumida. Podem ser aplicados em diferentes áreas, como aposentadorias, doação de órgãos, seguro de saúde, ou, como será exposto, na proteção de dados.

Quando se trata de TICs, os usuários se deparam com diversas opções de configuração ou customização. E, como já mencionado, não possuem conhecimento adequado para tomar tais decisões. Mackay investigou como usuários configuravam um *software* durante um período de 04 (quatro) meses. Descobriu que a falta de tempo e de conhecimento eram as duas principais barreiras na hora de customizar as preferências, já que os usuários preferiram passar mais tempo utilizando o produto em si para realizar suas tarefas.²⁵⁷

Os padrões no âmbito da privacidade e da segurança da informação são essenciais para determinar como uma aplicação vai proteger ou divulgar dados pessoais. Ao desenhar um

²⁵⁶ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

²⁵⁷ MACKAY, Wendy E. Triggers and barriers to customizing software. In: 1991, **Conference on Human Factors in Computing Systems - Proceedings**. [S. l.: s. n.]

sistema, os padrões são criados e, por conta da agressividade do mercado orientado por dados, acabam por ser autorizações genéricas que permitem a coleta e o tratamento de dados pessoais.

Em 2006, Acquisti e Gross descobriram maiores evidências sobre as configurações padrões não serem trocadas pelos usuários e que estas não protegem a privacidade ou dados pessoais. Em sua pesquisa, expuseram que esses padrões, por exemplo do *Facebook*, permitiam que todas as informações de um perfil fossem publicamente acessadas e que os usuários as mantinham assim ao longo do uso da referida rede social.²⁵⁸

No mesmo ano Lai e Hui publicaram um estudo em que se abordava a diferença entre práticas de *opt-in* e *opt-out* no recebimento de *newsletter* de *websites*. A política de *opt-in* fazia com que uma tela de “Por favor, me envie *newsletter*” aparecesse, com um campo para inserir o e-mail. Já a de *opt-out*, a mensagem era oposta, “Por favor, não me envie *newsletter*” – sendo o padrão baseado na *opt-in*. O que sob a presente análise é uma desvantagem para o usuário. Descobriu-se que os participantes tinham maior probabilidade de escolher a opção padrão. No entanto, eles encontraram um efeito de moderação das preocupações de privacidade existentes, pois os usuários com altas preocupações com a privacidade tinham menos probabilidade de serem influenciados pela configuração padrão.²⁵⁹

A Microsoft, por exemplo, possui como prática no desenvolvimento de *software* o respeito da proteção da privacidade como padrão, seguindo 06 (seis) principais princípios: controle do usuário, proteção legal, transparência, o não-uso de conteúdo para publicidade direcionada, segurança e benefício dos usuários.²⁶⁰ A empresa utiliza-se de *privacy by design*, conceito desenvolvido pela Dra. Ann Cavoukian, *ex-Information and Privacy Commissioner for the Canadian* (Ontario, Canadá)²⁶¹.

Por meio da utilização de *privacy by design*, Cavoukian defende que o futuro da privacidade não pode ser garantido apenas pela observância de leis e regulações. Assim, é necessária que sua garantia seja assegurada por um modo de operação padrão pelo agente de tratamento de dados, ampliando a responsabilidade para uma trilogia de aplicações

²⁵⁸ ACQUISTI, Alessandro; GROSS, Ralph. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. *In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. [S. l.: s. n.]. p. 36–58. *E-book*. Disponível em: <http://link.springer.com/10.1007/11957454_3>. Acesso em: 20 fev. 2020.

²⁵⁹ LAI, Yee-Lin; HUI, Kai-Lung. Internet Opt-In and Opt-Out: Investigating the Roles of Frames, Defaults and Privacy Concerns. **2006 ACM SIGMIS CPR Conference on Computer Personnel Research**, [S. l.], 2006.

²⁶⁰ MICROSOFT. **Microsoft Privacy Statement**. Fev. 2020. Disponível em: <<https://privacy.microsoft.com/en-us/privacystatement>>. Acesso em: 20 fev. 2020.

²⁶¹ CAVOUKIAN, A. **Privacy by Design: the 7 Foundational Principle**. Disponível em: <<https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>>. Acesso em: 20 fev. 2020.

compassadas: os sistemas de TI, práticas comerciais responsáveis; e um projeto físico e infraestrutura de rede.

Assim, é o objetivo da *privacy by design* é garantir a privacidade e fornecer controle pessoal sobre as informações e, para as organizações, obter uma vantagem competitiva sustentável. Ou, nas palavras de Bruno Bioni, “é a ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviços, devendo eles ser embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais”.²⁶²

Cavoukian entende ser necessário respeitar 7 (sete) princípios fundamentais²⁶³:

- a) Proativo e não reativo; preventivo e não corretivo: por meio dessa abordagem, são adiantados os riscos, sem que se espere a materialização de atentados contra a privacidade.
- b) Privacidade como configuração padrão: parte-se de um alto grau de privacidade, como garantia de que os dados pessoais sejam automaticamente protegidos, sem necessidade de ação do usuário;

²⁶² BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 231.

²⁶³ “1. Proactive not Reactive; Preventative not Remedial: [...] PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

2. Privacy as the Default Setting: [...] seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

3. Privacy Embedded into Design: privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality — Positive-Sum, not Zero-Sum: privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Security — Full Lifecycle Protection: privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. Visibility and Transparency — Keep it Open: Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy — Keep it User-Centric: Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.” CAVOUKIAN, A. **Privacy by Design: the 7 Foundational Principles**. Disponível em: <<https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>>. Acesso em: 20 fev. 2020.

c) Privacidade incorporada ao design: ela está incorporada no *design* e na arquitetura da tecnologia da informação e da prática dos negócios, não sendo apenas um complemento;

d) Funcionalidade total (soma positiva): busca acomodar todos os interesses os objetivos legítimos de maneira positiva;

e) Segurança de ponta a ponta: a *privacy by design* é incorporada em todo o sistema, inclusive antes do primeiro elemento de informação ser coletado, se estende com segurança por todo o ciclo de vida dos dados envolvidos;

f) Visibilidade e Transparência: procura garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, ela esteja de fato operando de acordo com as promessas e objetivos declarados, sujeita a verificação independente;

g) Respeito à privacidade do usuário: exige que os agentes de tratamento e os arquitetos da informação mantenham os interesses do indivíduo em primeiro plano, oferecendo medidas como padrões de privacidade fortes, aviso apropriado e opções poderosas para o usuário.

Para tanto, propõe como principal ferramenta as *Privacy Enhancing Technologies* (PETs), que são tecnologias que auxiliem na privacidade.²⁶⁴ Dentre diversas tecnologias, é possível identificar uma multidisciplinariedade, uma vez que elas abarcam não só o direito ou TICs, mas também o design *per se*.

A ideia do *privacy by design* foi incorporada pela *General Data Protection Regulation* da União Europeia (GDPR)²⁶⁵ e respingou, de certo modo, na LGPD. Essa prática entende que todas as etapas do desenvolvimento de um produto ou serviço que fará o tratamento de dados deve se basear na proteção da privacidade dos usuários, como se fosse costurada no projeto.

O artigo 25 da GDPR dispõe que:

Article 25 - Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which **are designed to implement data-**

²⁶⁴ “A tradução literal – PETs como tecnologias que reforçam-melhoram a privacidade – denota abrangência do termo que, como um guarda-chuva, é capaz de abarcar toda e qualquer tecnologia que seja amigável e facilitadora à privacidade”. Cf.: BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 231.

²⁶⁵ CONSELHO DA UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR)**. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>>. Acesso 20 fev. 2020.

protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that **by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.**

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.²⁶⁶ (grifo nosso)

Além dessa prática, existe a *privacy by default*, prática que entende pelo padrão uma configuração que restringe o tratamento de dados ao mínimo possível.²⁶⁷ Assim, é necessária a autorização expressa do usuário para que informações adicionais sejam coletadas. Como destacado acima, a GDPR também incluiu no artigo 25 (2) tal definição.²⁶⁸

A LGPD e o MCI²⁶⁹ também tratam do tema, ainda que não expressamente. Enquanto o MCI já dispunha como deveria ser um processo genuíno de tomada de decisão, anos depois, a LGPD, por meio do princípio da necessidade e da responsabilização e prestação de contas, reforça a preocupação do legislador com a *privacy by design*. É o que se vislumbra no art. 6º, incisos III e X:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

²⁶⁶ Tradução: “Artigo 25 - Proteção de dados desde a concessão e por defeito

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 uma 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 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 números 1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42.”

²⁶⁷ CAVOUKIAN, A. **Privacy by Design: the 7 Foundational Principles**. Disponível em: <<https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>>. Acesso em: 20 fev. 2020.

²⁶⁸ CONSELHO DA UNIÃO EUROPEIA. General Data Protection Regulation (GDPR). Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>>. Acesso 20 fev. 2020.

²⁶⁹ BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet do Brasil. **Diário Oficial**, Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm>. Acesso em: 20 jan. 2020.

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;

[...]

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.²⁷⁰

Então, conforme destaca Bruno Bioni, torna-se necessário “[...] checar a maneira pela qual o design de um ambiente (on-line e off-line) deve incutir no cidadão um controle visceral sobre seus dados, em vez de manipular as suas escolhas.[...]”.²⁷¹ Inclusive, o mesmo autor assevera que isso já é explorado na contratação eletrônica, no que tange aos comportamentos concludentes, devendo ser analisado interdisciplinarmente, da ciência comportamental ao *design*.

4.2.4 A dimensão dos Incentivos e os *nudges*

A dimensão dos incentivos motiva os usuários a se comportar conforme as preferências que declararam. Com elas, a aversão à perda e o desconto hiperbólico podem ser reduzidos, como exemplificam Acquisti *et al.*:

Providing the right incentives can help mitigate hyperbolic discounting bias that often prevents users from appreciating negative long-term consequences. For example, people tend to underestimate the future consequences of CO2 emissions and too often make inefficient use of motorized vehicles. High Occupancy Vehicle (HOV) lanes are intended to reward those drivers who are willing to carpool by enabling a faster commute, and in the process help reduce CO2 emissions and the number of cars on the road.²⁷²

Podem ser aproveitadas para moldar a percepção e a eficácia das recompensas e punições. Desse modo ao “[...] framing a punishment as a loss might have a stronger effect on users’

²⁷⁰ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. **Diário Oficial**, Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 20 jan. 2020.

²⁷¹ BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019, p. 231.

²⁷² Tradução livre: “O fornecimento dos incentivos corretos pode ajudar a atenuar o viés de desconto hiperbólico que muitas vezes impede os usuários de apreciarem consequências negativas a longo prazo. Por exemplo, as pessoas tendem a subestimar as consequências futuras das emissões de CO2 e frequentemente fazem uso ineficiente de veículos motorizados. As faixas de veículos de alta ocupação (HOV) destinam-se a recompensar os motoristas dispostos a trocar de carro, permitindo um deslocamento mais rápido e, no processo, ajudam a reduzir as emissões de CO2 e o número de carros na estrada.” Cf.: ACQUISTI, A. *et al.* Nudges for Privacy and Security. *ACM Computing Surveys*, [S. l.], v. 50, n. 3, 2017, p. 44:22.

behavior than framing it as a simple penalty”.²⁷³ Assim, é possível afirmar que incentivos ou recompensas não-monetárias podem influenciar em comportamento de usuários:

Increasing the cost or difficulty of choosing specific configurations, even at the simple level of requiring multiple confirmations, is a “punishment” that could prevent non-experts or inexperienced users from selecting risky settings. On the other hand, secure or less risky configurations can be made easier to select, encouraging users to choose them. Punishments and rewards can further be applied in response to users’ choices.²⁷⁴

É importante frisar que os usuários não possuem um método fácil e acessível para quantificar os custos de suas decisões de privacidade e segurança. Ainda que ignorar os riscos à segurança pode ser decisão racional para aqueles usuários que não serão atingidos por consequências, este comportamento causa externalidades que atingem outros usuários da *Internet*. É nesse sentido que os *nudges* se tornam importantes para destacar informações sobre tais custos e externalidades negativas que os comportamentos inseguros podem trazer. Os incentivos à segurança, então, podem ser úteis para as próprias empresas como forma de estratégia corporativa.²⁷⁵

4.2.5 A dimensão da Reversibilidade (*resiliência aos erros*)

Os seres humanos são propensos a cometer erros se distanciando da visão de “ser humano perfeito”.²⁷⁶ Assim, *reversibilidade*, ou *resiliência aos erros*, limita os impactos dessas

²⁷³ Tradução livre: “Aumentar o custo ou a dificuldade de escolher configurações específicas, mesmo no nível simples de exigir várias confirmações, é uma “punição” que pode impedir que não especialistas ou usuários inexperientes selecionem configurações de risco. Por outro lado, pode-se facilitar a seleção de configurações seguras ou menos arriscadas, incentivando os usuários a escolhê-las. Punições e recompensas também podem ser aplicadas em resposta às escolhas dos usuários.” Cf.: ACQUISTI, A. *et al.* Nudges for Privacy and Security. **ACM Computing Surveys**, [S. l.], v. 50, n. 3, 2017, p. 44:22

²⁷⁴ Tradução livre: “O fornecimento dos incentivos corretos pode ajudar a atenuar o viés de desconto hiperbólico que muitas vezes impede os usuários de apreciarem consequências negativas a longo prazo. Por exemplo, as pessoas tendem a subestimar as consequências futuras das emissões de CO2 e frequentemente fazem uso ineficiente de veículos motorizados. As faixas de veículos de alta ocupação (HOV) destinam-se a recompensar os motoristas dispostos a trocar de carro, permitindo um deslocamento mais rápido e, no processo, ajudam a reduzir as emissões de CO2 e o número de carros na estrada.” Cf.: ACQUISTI, A. *et al.* Nudges for Privacy and Security. **ACM Computing Surveys**, [S. l.], v. 50, n. 3, 2017, p. 44:22

²⁷⁵ “Security. Incentives can be used to improve security as part of corporate strategy. Users who handle email attachments in a careless manner can be punished by restricting their email accounts to official communications. A user who is more cautious with email attachments can be rewarded by allowing use of the corporate account for personal emails. B”. ACQUISTI, A. *et al.* Nudges for Privacy and Security. **ACM Computing Surveys**, [S. l.], v. 50, n. 3, 2017, p. 44:23.

²⁷⁶ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

decisões equivocadas, visando proteger “people from inadvertent errors that can be caused by decision-making hurdles”²⁷⁷. Dessa forma:

Nudging systems can mitigate post-completion errors originating from tasks that have both primary and secondary goals by either forcing people to take an action or automatically completing secondary tasks. These nudging systems are present in many aspects of our lives, such as driving. Drivers’ primary task is to drive to their destination. However, there are many associated secondary tasks that some drivers tend to forget, such as switching on their headlights.²⁷⁸

Como exemplo prático desse tipo de *nudge* está a possibilidade de se deletar marcações feitas por terceiros em fotos. Em pesquisa realizada por Besmer e Lipford, descobriu que as pessoas preferem opções de remover marcações feitas por amigos, que solicitar para que esses o façam. Desse modo, permite-se que os usuários se recuperem de decisões não tão boas, potencialmente causadas por preconceitos comportamentais.²⁷⁹

4.2.6 A dimensão do *Timing* e os *nudges*

Os *nudges* até então expostos podem ser aplicados em diversos momentos, assim como incentivos. A análise do contexto pode então determinar qual tipo de prática é a melhor a ser empregada, sendo, inclusive, necessária a alteração do desenho do sistema. Isso, inclusive, é requisito da *privacy by design*.

É importante saber quando os *nudges* devem ser empregados. Como destacado por Acquisti *et al.*, *feedbacks* podem ser fornecidos antes e durante o uso do sistema. Quando bem empregado, provavelmente influenciará o comportamento para uma melhor escolha.²⁸⁰

Nesse sentido, Egelman *et al.* conduziu pesquisa para estimar se os participantes de um estudo tinham mais probabilidade de pagar um *website premium* com melhores práticas de privacidade. Esse estudo revelou que o *timing* em que os *nudges* surgiam eram cruciais, uma

²⁷⁷ Tradução livre: “[...] pessoas de erros inadvertidos que podem ser causados por obstáculos à tomada de decisão.”

²⁷⁸ Tradução livre: “Os sistemas de cutucada podem atenuar os erros pós-conclusão originados de tarefas que têm objetivos primários e secundários, forçando as pessoas a tomar uma ação ou concluindo automaticamente tarefas secundárias. Esses sistemas de cutucada estão presentes em muitos aspectos de nossas vidas, como dirigir. A principal tarefa dos motoristas é dirigir até o destino. No entanto, existem muitas tarefas secundárias associadas que alguns motoristas tendem a esquecer, como acender os faróis.” Cf.: ACQUISTI, Alessandro *et al.* Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online. *SSRN Electronic Journal*, [S. l.], v. 50, n. 3, 2016. Disponível em: <<https://www.ssrn.com/abstract=2859227>>. Acesso em: 20 fev. 2020.

²⁷⁹ BESMER, Andrew; RICHTER LIPFORD, Heather. Moving beyond untagging: Photo privacy in a tagged world. In: 2010, **Conference on Human Factors in Computing Systems - Proceedings**. [S. l.: s. n.]

²⁸⁰ ACQUISTI, A. *et al.* Nudges for Privacy and Security. *ACM Computing Surveys*, [S. l.], v. 50, n. 3, 2017, p. 44:28.

vez que quando esses eram apresentados antes de visitar o *site*, causam um impacto muito maior do que após o fazerem.

4.3 NUDGES NA PRÁTICA: EMPURRÃO PARA A ESCOLHA CERTA OU PATERNALISMO EXACERBADO?

Como apresentado e defendido até o momento, os *nudges* são ferramentas úteis em contextos de *trade-offs* incertos, envolvendo assimetria informacional ou possíveis danos significativos a direitos de privacidade e à proteção de dados. Ainda que diversos autores entendam que o legislador possui o papel de, ou ao menos teria, induzir o usuário a divulgar menos informações pessoais, outros entendem os *nudges* como ameaça à privacidade e à liberdade individual.

Algumas críticas foram traçadas contra o art. 6º, § 1º, da GDPR, qualificando-o como “paternalismo intervencionista”. Críticas também foram feitas contra a regra da *privacy by default*, contida no art. 25º, § 2, da GDPR como um *nudge* do paternalismo libertário²⁸¹. Os artigos dispõem que:

Article - Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

[...]

Article 25 –Data protection by design and by default [...]

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and

²⁸¹ CONSELHO DA UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR)**. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>>. Acesso 20 fev. 2020.

their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. 282

No entanto, para Yoan Hermstrüwer, essas afirmações são baseadas em um entendimento vago do que são *nudges* 283. Isso, porque, ainda que Thaler e Sunstein tenham definido os *nudges* como uma forma de intervir na arquitetura de escolhas, alterando o comportamento das pessoas de uma forma previsível sem que a liberdade de escolha seja tolhida, outros entendem o paternalismo libertário de forma mais abrangente, como qualquer tipo de intervenção que é projetada para superar vieses cognitivos, a qualquer custo.²⁸⁴

Em muitos casos, contudo, não há escolha certa ou errada óbvia. Desse modo, Acquisti *et al.* entendem ser necessário perguntar: até que ponto os *nudges* devem ir à tentativa de influenciar as decisões de segurança ou privacidade de um usuário?²⁸⁵

O desenho dos *nudges*, em algumas situações, pode beneficiar muito mais o agente de tratamento dos dados do que o próprio usuário, ou podem ser desenhados de forma maliciosa. Como indica Acquisti *et al.*, a parte dos *nudges* maliciosos, todos os outros “have the inherent

282 Tradução: “Artigo 6º - Lícitude do tratamento

1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

- a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
- b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
- c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
- d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
- e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
- f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.

Artigo 25 - Proteção de dados desde a concessão e por defeito

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 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.

²⁸³ HERMSTRÜWER, Y. Contracting Around Privacy. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, [S. l.], v. 45, n. 8, p. 9–26, 2017.

²⁸⁴ THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019, n.p.

²⁸⁵ ACQUISTI, A. *et al.* Nudges for Privacy and Security. *ACM Computing Surveys*, [S. l.], v. 50, n. 3, 2017, p. 44:28.

quality of encouraging an individual to make a particular choice”²⁸⁶. Dessa forma, o desenho de um empurrão irá pressupor que uma entidade, esteja em melhor posição para decidir qual escolha o indivíduo deve fazer.

No entanto, não é uma tarefa fácil otimizar o benefício desses *nudges* para todos os usuários. Eles podem ser otimizados para benefício individual ou social, ou seu impacto pode variar para diferentes tipos de usuários, justamente porque aqueles que os desenham devem decidir o quão transparente serão para os usuários e, também, pelo fato de que o impacto dos *nudges* pode ser difícil de avaliar.²⁸⁷

Como resposta a essa questão, Acquisti *et al.* propõem dois resultados para orientar a implementação de sugestões de privacidade e segurança: a) *minimizar o arrependimento* e b) *alinhar o comportamento dos indivíduos às suas preferências declaradas*. Segundo os autores, *minimizar o arrependimento* compreende em aplicar os *nudges* em situações que divulgações de dados ou informações de indivíduos provavelmente causarão efeitos negativos e até irreversíveis.²⁸⁸

Alinhar o comportamento dos indivíduos às suas preferências, por sua vez, são *nudges* que influenciam os usuários a limitar a divulgação de dados ou informações que são contrárias ao que desejam. Aqui, também se considera contextos propensos a cutucar, nos quais os indivíduos incorrem em um alto custo de privacidade ou segurança em troca de funcionalidades limitadas.²⁸⁹

Assim, o cerne do debate dos *nudges* é que seus objetivos e efeitos são, frequentemente, “varridos pra baixo do tapete”. Logo, não há uma discussão acurada sobre esses objetivos e efeitos, ou como eles deveriam ser relacionados. De forma errônea, então, todos os tipos de ferramentas regulatória ou intervenção passam a ser considerados *nudges*, mesmo quando não há em sua razão de ser um. Nesse sentido, o Hermstrüwe exemplifica:

²⁸⁶ Tradução livre “[...] todos os empurrões têm a qualidade inerente de incentivar um indivíduo a fazer uma escolha específica.” ACQUISTI, A. *et al.* Nudges for Privacy and Security. **ACM Computing Surveys**, [S. l.], v. 50, n. 3, 2017, p. 44:28.

²⁸⁷ ACQUISTI, A. *et al.* Nudges for Privacy and Security. **ACM Computing Surveys**, [S. l.], v. 50, n. 3, 2017, p. 44:2.

²⁸⁸ “[...] For example, disclosures made under the influence of alcohol or drugs, using offensive language, or discussing contentious political issues could be appropriate instances for privacy nudges as they have a higher likelihood of being regretted in the future [...]” ACQUISTI, A. *et al.* Nudges for Privacy and Security. **ACM Computing Surveys**, [S. l.], v. 50, n. 3, 2017, p. 44:29.

²⁸⁹ “For example, we may find that a majority of individuals are concerned about disclosing their political or religious affiliation to potential employers. Thus, nudges that influence users to limit such disclosures to employers, or nudges encouraging users to limit access to such disclosures, may be justified. Along these lines, we may also consider contexts ripe for nudging in which individuals incur a steep privacy or security cost in return for”. ACQUISTI, A. *et al.* Nudges for Privacy and Security. **ACM Computing Surveys**, [S. l.], v. 50, n. 3, 2017, p. 44:29.

Consider default options in privacy law. Without any further specification of the objective and effects of a default rule, it does not make sense to qualify a default option as a nudge. As I have shown above, an opt-in default may be justified on different legal grounds.

If the purpose of an opt-in default is to set a strategic incentive for companies to disclose better information for users, it aims at reducing information asymmetries and hence a market failure. Similarly, an opt-in default could be used to mitigate collective action problems and the negative externalities associated with an unconstrained disclosure of personal information.²⁹⁰

Logo, o principal propósito de tal padrão não poderia ser proteger os usuários de uma escolha errada ou baseada em assimetria informacional, mas sim aprimorar a eficiência contratual entre usuários e empresas. Ou seja, não se poderia qualificar esse hipotético *nudge* como uma intervenção baseada no paternalismo libertário, uma vez que a “[...] default rule could more aptly be justified within the standard economic framework and the traditional approach to market failures”²⁹¹.

Yoan Hermstrüwer reforça os benefícios da aplicação dos *nudges*, uma vez que são meios menos coercitivos, ainda que altamente eficazes. Para ele, essas intervenções não precisam ser subliminares, mas apenas transparentes e sujeitas ao escrutínio judicial.²⁹²

Assim, Yoan Hermstrüwer ressalva que a criação de estímulos efetivos poderá ser complexa e cara. O desenho dessas configurações de privacidade requer um recorte preciso da realidade e das verdadeiras necessidades. Consequentemente, coloca como fator crucial a dúvida se os benefícios dos empregos dos *nudges* superarão seus custos. Sugere, então, que essas decisões sejam avaliadas no ponto de equilíbrio do princípio da proporcionalidade. Assim, resta a dúvida sobre quem deveria implementar os *nudges* de segurança e privacidade. Seriam reservados somente ao poder público?

²⁹⁰ Tradução livre: “Considere as opções padrão na lei de privacidade. Sem nenhuma especificação adicional dos objetivos e efeitos de uma regra padrão, não faz sentido qualificar uma opção padrão como uma cutucada. Como mostrei acima, um padrão de aceitação pode ser justificado por diferentes motivos legais.

Se o objetivo de um padrão de adesão é definir um incentivo estratégico para as empresas divulgarem informações melhores para os usuários, ele visa reduzir as assimetrias de informações e, portanto, uma falha de mercado. Da mesma forma, um padrão de aceitação pode ser usado para mitigar os problemas de ação coletiva e as externalidades negativas associadas a uma divulgação irrestrita de informações pessoais.” Cf.: HERMSTRÜWER, Y. Contracting Around Privacy. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, [S. l.], v. 45, n. 8, p. 9–26, 2017.

²⁹¹ Tradução livre: “[...] a regra padrão poderia ser mais adequadamente justificada dentro da estrutura econômica padrão e da abordagem tradicional para falhas de mercado.” HERMSTRÜWER, Y. Contracting Around Privacy. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, [S. l.], v. 45, n. 8, p. 9–26, 2017.

²⁹² Segundo o autor, “[...] Nudges or soft regulation will usually be the least coercive means with the potential to be as effective as outright coercion. Notably, the effect of default options is not weaker when people are told that the chosen default is usually effective.119 Therefore, soft interventions need not be subliminal; they can and should be transparent and be subject to judicial scrutiny. Perhaps the most importante consideration is that designing effective nudges will often be complex and costly.

4.4 QUEM DEVE DESENHAR OS *NUDGES*?

Os *nudges* de segurança e privacidade são, em um primeiro momento, vistos como políticas públicas que asseguram a proteção de dados e o direito à privacidade. O papel do poder público é muito importante, uma vez que possui o dever de proteger os cidadãos da exploração de seus dados e fornecer educação necessária para tanto. Tendo em vista que o objetivo de uma política é estabelecer proteção adequada da privacidade, torna-se necessário criar e manter aquelas que protejam o usuário na tomada de decisão, para que sejam feitas de forma racional e informada. Isso é chamado de *fair information practices*²⁹³.

Como apresentado por Bruno Bioni, torna-se necessário buscar ferramentas regulatórias alternativas com o objetivo de equilibrar a assimetria informacional do mercado, redesenhando a sua dinâmica de poder. Com isso, é possível um controle aceitável sobre dados:

Deve-se, contudo e concomitantemente, pensar em disposições normativas complementares que interfiram no próprio fluxo informacional, não deixando, apenas, sobre os ombros dos titulares dos dados pessoais, o *fardo normativo* da proteção de dados pessoais. A tutela jurídica deve ir muito além do *raciocínio bifásico* centrado na escolha do indivíduo em consentir ou não com o tratamento dos seus dados pessoais.

Trata-se, portanto, de se afastar de uma estratégia regulatória puramente liberal, que é incoerente com a posição de vulnerabilidade do sujeito em causa. Necessário se faz uma maior intervenção, seja do ponto de vista do desenho normativo ou da formulação de políticas públicas em *lato sensu* para que se empodere o sujeito vulnerável e, por outro lado, que não se foque apenas na instrumentalização do controle dos dados pessoais a ponto de se pensar em uma normatização *substantiva* da privacidade informacional.²⁹⁴

Com base nesse raciocínio, o paternalismo libertário, focado em desenhar estratégias regulatórias que protejam e auxiliem o cidadão, vulnerável, na tomada de decisão, é uma solução. Inclusive, para Hoofnagle *et al.* “[...] the policymakers should fully appreciate the idea that consumer privacy interventions can enable choice, while the alternative, pure marketplace approaches can deny consumers opportunities to exercise autonomy”²⁹⁵.

Vint Cerf entende que “devemos trabalhar nos aspectos técnicos e de políticas regulatórias a fim de dar aos usuários as ferramentas para compreender como funcionam os

²⁹³ GELLMAN, Robert. Fair Information Practices: A Basic History. *SSRN Electronic Journal*, [S. l.], 2014.

²⁹⁴ BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 220.

²⁹⁵ Trafusão livre “[...] aqueles que formulam políticas devem apreciar plenamente a idéia de que as intervenções de privacidade do consumidor podem permitir a escolha, enquanto as abordagens alternativas e de mercado puras podem negar oportunidades aos consumidores de exercer autonomia”. HOOFNAGLE, Chris Jay *et al.* Behavioral Advertising: The Offer You Can’t Refuse. *Harvard Law & Policy Review*, [S. l.], v. 6, 2012.

serviços online e proteger sua privacidade”²⁹⁶. Até porque, como salienta Doneda, a proteção de dados não é uma demanda uniforme entre os brasileiros, justamente porque a “[...] a percepção da relevância de sua tutela desenvolve-se somente depois que uma série de outras necessidades básicas estejam satisfeitas”²⁹⁷. Tanto o Marco Civil da *Internet* quanto a LGPD corroboram com a visão de Doneda, uma vez que sua votação no Congresso Nacional foi impulsionada por escândalos de violação à privacidade e aos dados pessoais.

Portanto, não se pode esperar que essas práticas venham somente do setor público, ou do privado – até porque o primeiro também se aproveita da vulnerabilidade e da assimetria informacional do cidadão. Em complemento, Rodotà desenha crítica ao poder normativo no âmbito da *Internet*.

Siamo di fronte non a un vuoto, bensì a un formidabile pieno di regole. Ma può la democrazia accettare un esercizio del potere normativo nell’infinito universo di Internet senza un quadro definito di principi e diritti? L’argomento libertario deve essere rovesciato. Proprio la giusta pretesa di non essere sottoposti a regole restrittive esige la definizione di principi costituzionali che sono esattamente l’opposto di quel tipo di regole, avendo come fine appunto la garanzia di libertà e diritti. Né basta ritenere che democraticità e legittimità delle regole possano essere garantite dalla sola partecipazione alla loro definizione di tutti i portatori relativi di interessi, tutti sullo stesso piano. Una dichiarazione dei diritti, allora, consente di sfuggire al rischio di abbandonarsi ad un multistakeholderism senza principi, che crea le premesse per la prevalenza dell’interesse del più forte. Peraltro, i soggetti che con la loro attività unificando il mondo, come i cosiddetti over the top, manifestano in più di un caso interesse per principi comuni che possano rendere meno onerosa l’attività di gestione, sottratta alla variabilità delle regole da paese a paese. Ma proprio questo vantaggio non può non consentire un dominio privato sulla fissazione delle regole comuni.²⁹⁸

²⁹⁶ CERF, V. G. Questões e desafios da governança da Internet nas Américas. In: BELLI, L.; CAVALLI, O. **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2019. p. 9.

²⁹⁷ DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019. p. 33

²⁹⁸ “Não enfrentamos um vazio, mas sim um formidável conjunto de regras. Mas pode a democracia aceitar o exercício de poder normativo, no infinito universo da Internet que não possui estrutura definida de princípios e direitos? O argumento libertário deve ser revertido. Precisamente, a correta alegação de que não está sujeita às regras restritivas exige uma definição de princípios constitucionais que são exatamente o oposto desse tipo de regra, tendo como objetivo a garantia de liberdade e direitos.

Também não basta acreditar que a democracia e a legitimidade das regras possam ser garantida somente por sua participação na definição de todas as partes interessadas relevantes, todas no mesmo patamar. Uma declaração de direitos, portanto, permite que você escape do risco de se abandonar a um multissetorialismo sem princípios, o que cria as premissas para a prevalência do interesse dos mais fortes. Além disso, os sujeitos que, com seus negócios unificando o mundo, como os chamados exagerados, demonstram em mais de um caso interesse em princípios comuns que podem tornar as atividades de gerenciamento mais caras, afastadas da variabilidade das regras de país para país. . Mas precisamente essa vantagem não pode deixar de permitir um domínio privado sobre a definição de regras comuns” Cf.: RODOTÀ, Stefano. Prefazione. In: MASERA, Anna. SCORZA, Guido. **Internet, i nostri diritti**. Bari: Laterza, 2016. p. 8.

Conforme exposto por Luca Belli, a ausência de uma autoridade pública internacional fez com que atores privados preencham essa lacuna, instituindo sistemas de *private ordering*, ou regulação privada, do setor financeiro até a *Internet*. Essa última, em sua camada de aplicação, aproveita dessa ausência e da ascensão de uma autoridade privada como forma de aplicar seus próprios interesses, ditando sua própria regulação.²⁹⁹

A autorregulação e a ascensão da autoridade privada não são necessariamente ruins ou significariam a perda de soberania e do poder de decisão do Estado. O que se observa, na verdade, é uma governança híbrida, na qual o próprio poder público delega certas funções regulatórias aos entes privados. Essa divisão de responsabilidades entre o Estado e entidades privadas é reforçada pelo MCI, nos arts. 26 e 29, parágrafo único, e na LGPD, em seu art. 60.

Luca Belli³⁰⁰ explica que “[...] as plataformas digitais podem ser consideradas como ciberespaço no sentido de verdadeiros territórios virtuais, cujas fronteiras são definidas por sua arquitetura técnica”. Logo, se os usuários são ingênuos e ignorantes quanto ao poder das companhias de interferir em seu poder de escolha, o benefício estará somente na mão delas.

Exceto se houver uma regulamentação que garanta a privacidade, há um desequilíbrio entre as partes nessa transação. Caso estejam cientes em como seus dados são utilizados, essas leis e políticas são desnecessárias, uma vez que será do próprio interesse da companhia a observância das boas práticas de governança de dados, criada a partir da consciência coletiva.

Inclusive, é essa eficiência do *enforcement* das plataformas digitais que acabam levando os atores públicos a delegar cada vez mais funções reguladoras. Nesse sentido, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) já destacou o papel fundamental que os intermediários da *Internet* desempenham no desenvolvimento das políticas públicas.³⁰¹

Iglesias aponta um exemplo de *nudge*, feita pela Mozilla Foundation. Em fevereiro de 2013, eles lançaram um *patch* atualizado do Firefox para suas configurações de privacidade,

²⁹⁹ BELLI, L.; FRANCISCO, P. A.; NOTA, N. Z. Lei do Estado ou lei da Plataforma? Cuidado com a privatização da regulação e da polícia. In: BELLI, L.; CAVALLI, O. **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2019, p. 449.

³⁰⁰ BELLI, L.; FRANCISCO, P. A.; NOTA, N. Z. Lei do Estado ou lei da Plataforma? Cuidado com a privatização da regulação e da polícia. In: BELLI, L.; CAVALLI, O. **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2019, p. 449.

³⁰¹ OECD. **The Role of Internet Intermediaries in Advancing Public Policy Objectives**. [S. l.]: OECD, 2011. *E-book*. Disponível em: <https://www.oecd-ilibrary.org/science-and-technology/the-role-of-internet-intermediaries-in-advancing-public-policy-objectives_9789264115644-en>. Acesso em: 20 fev. 2020

com a suposição de que os usuários continuariam com a opção padrão. O padrão proibia a aceitação de *cookies* de terceiros durante a navegação na Internet. Sabendo que os usuários parecem seguir as opções padrão, esse *patch* aumentou positivamente a privacidade do indivíduo, pois apenas os sites que foram realmente visitados terão seus *cookies* permitidos.³⁰²

Por outro lado, apesar da violação de privacidade provocada pelos *cookies*, esses concedem muitas vantagens ao desenvolvedor do *site*, ao anunciante, ao administrador e aos usuários fazem uso do *site*. Inclusive, algumas operações do *site* da Internet dependem diretamente de *cookies*, como pedidos *on-line*, rastreamento do *site* e identificação dos usuários. O rastreamento da localização dos usuários e o tempo gasto navegando no *site* podem ajudar a fazer alterações para melhorar a experiência do usuário e modificar o conteúdo, aumentando assim a probabilidade de retorno do usuário.

No entanto, como aposta Acquisti *et al.*, não é claro que as forças do mercado levariam empresas privadas a implementar *nudges* que visam alinhar o comportamento das pessoas com suas preferências de privacidade.³⁰³ Isso porque algumas possuem no *core* de seu modelo de negócio o tratamento de dados, se dedicar ostensivamente à privacidade e proteção aos dados pessoais, com a implementação de ferramentas como *privacy by design*, ou *privacy by default*, é atingir diretamente o lucro, ao menos em um primeiro momento.

Assim, uma decisão mais acertada no que tange à privacidade e à segurança *online* depende, quase que unicamente, do equilíbrio entre o compartilhamento e o sigilo de dados pessoais. Desse modo, há a maximização do bem-estar de uma pessoa ou organização, enquanto se minimiza as chances de arrependimento. Os atores do setor público e privado, portanto, encontram-se exatamente na busca deste equilíbrio.

³⁰² IGLESIAS, D. **Nudging Privacy: benefits and limits of persuading human behaviour online**, 2017. Disponível em: <<https://itsrio.org/wp-content/uploads/2017/03/Daphnee-Iglesias-.doc-B.pdf>>. Acesso em: 20 jan, 2020.

³⁰³ ACQUISTI, A. *et al.* Nudges for Privacy and Security. **ACM Computing Surveys**, [S. l.], v. 50, n. 3, 2017, p. 44:2

5 CONCLUSÃO

De acordo com o aumento no uso das TICs, certamente haverá aumento do problema com a privacidade. Os riscos que os *trade-offs* criam estão intrinsicamente ligados à assimetria informacional e na confusão das preferências declaradas dos usuários e seu comportamento. Os vieses, somados com a falta de conhecimento técnico, não tiram os indivíduos da inércia de modificar qualquer tipo de configuração para salvaguardar seus direitos e proteger seus dados.

Por conta disso, é necessário o desenvolvimento de ferramentas e estratégias que assegurem direitos dos usuários e seu bem-estar, sem que suas liberdades de escolhas sejam cerceadas. Assim, como objetivo principal, buscou-se no Paternalismo Libertário, por meio dos *nudges*, auxílio no processo de tomada de decisão quanto à proteção de direitos de privacidade e à proteção de dados pessoais na *Internet*.

O primeiro capítulo forneceu um panorama geral sobre a privacidade e a proteção de dados pessoais, destacando a possibilidade de dados serem considerados ativos econômicos. O segundo capítulo desenhou o Paternalismo Libertário e seus *nudges*, explicando as heurísticas e vieses do processo de tomada de decisão. Como esses *nudges* poderiam ser inseridos na proteção dos direitos de privacidade e proteção de dados na *Internet*.

Logo, a pesquisa comprovou que o Paternalismo Libertário pode ser uma resposta satisfatória na proteção dos usuários frente aos problemas que o assunto envolve, na tentativa de melhorar as suas escolhas de privacidade na *Internet*. Por óbvio, continuarão existindo indagações e críticas como quem é o responsável por decidir qual deveria ser o melhor padrão de privacidade ou quem é o responsável por aplicar e fiscalizar os *nudges*. E, muito provavelmente, não serão respondidas tão cedo. Independentemente, o uso dos *nudges* são soluções satisfatórias no processo de tomada de decisão e na construção de tecnologia adequada para os usuários finais.

As ideias por trás do Paternalismo Libertário e dos ensinamentos dos processos comportamentais podem ser usadas para realmente ajudar o aprimoramento das opções dos indivíduos, projetando ferramentas e políticas que aprimoram a escolha, sem restringi-la. Ao mitigar e/ou explorar vieses comportamentais, tem-se como objetivo final o aumento do bem-estar individual, organizacional e social.

Por meio do Paternalismo Libertário, os usuários da *Internet* têm um risco de violação à privacidade ou exploração de seus dados pessoais muito menor. Com os *nudges*, é possível a escolha consciente do que é compartilhado, como e para quê.

Como decorrência de todas as ponderações apresentadas, entende-se que, diferentemente do sugerido por certos autores, o *nudge* e o Paternalismo Libertário aplicado ao tema, é muito menos invasivo ao direito à privacidade. Ao integrar diversas áreas do conhecimento, mas especialmente o Direito e as Ciência Comportamental, há um aumento significativo na capacidade de proteção dos indivíduos. Com isso, é possível solucionar, ou pelo menos minimizar, questões da privacidade que são alvo de ataque e falta de regulação e/ou políticas públicas e privadas de privacidade.

As legislações não conseguem acompanhar o desenvolvimento de novas tecnologias e o surgimento de novas problematizações. Por conta disso, a menor burocracia do setor privado em comparação com Estado acaba por fazer com que o primeiro regule pelo segundo. Como visto, isso não é de todo ruim, desde que princípios norteadores das legislações sobre o tema sejam respeitados. Ferramentas como o *privacy by design*, quando internalizadas por esses atores e transformadas em *nudges* servem não só como autorregulação, mas possuem papel educacional.

A dificuldade, no entanto, é demonstrar que a *data-driven economy*, que busca a capitalização baseada em dados, não necessita ser antiética. Como visto, é necessário equilíbrio real entre privacidade e compartilhamento, para maximizar o bem-estar individual ou social, inclusive no que tange ao desenvolvimento de outras tecnologias e facilidades à população.

A ideia por trás do paternalismo suave é que as lições aprendidas sobre os processos psicológicos subjacentes ao comportamento podem ser usadas para realmente ajudar esse comportamento, projetando ferramentas e políticas que aprimoram a escolha, sem restringi-la. O objetivo final de tais intervenções é aumentar o bem-estar individual, organizacional e social, mitigando ou explorando os vieses comportamentais das pessoas de uma maneira que leve as pessoas a fazer escolhas autônomas mais informadas e desejáveis.

É nesse sentido que essa Dissertação se mostra relevante. A ferramenta dos *nudges* serve, em diversas situações como solução ou prevenção de problemas relativos à privacidade e proteção de dados pessoais na *Internet*. Remediar possíveis danos, principalmente devido à assimetria informacional, diminui custos para empresas que poderiam ser responsabilizadas por leis de proteção de dados pessoais. Por outro lado, a necessidade de se legislar de forma paternalista, impossibilitando uma escolha livre, é diminuída por meio dos *nudges*.

Concluiu-se, então, que o Paternalismo Libertário pode ser utilizado como ferramenta para “empurrar” as pessoas para escolhas mais benéficas aos interesses dos usuários da *Internet* quanto à proteção dos direitos de privacidade e à proteção de seus dados pessoais. O que deve ser observado, portanto, é se o pretendido *nudge* realmente preservará a liberdade do usuário

em realizar sua escolha. Sem essa liberdade, não há “empurrão” para uma escolha mais adequada, mas sim imposição velada de uma vontade alheia.

REFERÊNCIAS

- AARONSON, S. A. Data Is a Development Issue. **CIGI Papers**, 2019. Disponível em: <[https://www.cigionline.org/sites/default/files/documents/paper no.223.pdf](https://www.cigionline.org/sites/default/files/documents/paper_no.223.pdf)>. Acesso em: 11 fev. 2020.
- ACQUISTI, A; GROSSKLAGS, J. Economics of Information Security. **IEEE Security and Privacy**, [S. l.], 2005.
- ACQUISTI, A. Nudging privacy: the behavioral economics of personal information. **IEEE Digital Enlightenment Yearbook**, S. l.: s. n., 2012.
- ACQUISTI, A.; BRANDIMARTE, L. The Economics of Privacy. *In: Threats arising from digitization and the Internet*. [S. l.: s. n.].
- ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and human behavior in the age of information. **Science** **347 (6221), 509-514.**, New York, v. 347, n. 6221, 2017. ISSN 1095-9203. Disponível em: <<https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHumanBeh.pdf>>. Acesso em: 24 maio 2018.
- ACQUISTI, A.; GROSSKLAGS, J. What Can Behavioral Economics Teach Us about Privacy? *In: ACQUISTI, Alessandro et al. Digital Privacy: Theory, Technologies and Practices*. London: Auerbach Publications, 2008.
- ACQUISTI, A.; TAYLOR, C.; WAGMAN, L. The Economics of Privacy. **Journal of Economic Literature**, v. 54, n. 2, 2016.
- ACQUISTI, Alessandro *et al.* Nudges for Privacy and Security: Understanding and Assisting Users Choices Online. **SSRN Electronic Journal**, [S. l.], v. 50, n. 3, 2016. Disponível em: <<https://www.ssrn.com/abstract=2859227>>. Acesso em: 20 fev. 2020.
- ACQUISTI, Alessandro; GROSS, Ralph. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. *In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. [S. l.: s. n.]. p. 36–58. *E-book*. Disponível em: <http://link.springer.com/10.1007/11957454_3>. Acesso em: 20 fev. 2020.
- ACQUISTI, Alessandro. Nudging privacy: the behavioral economics of personal information. **IEEE Digital Enlightenment Yearbook 2012**, 2012.
- ALEMANHA. Corte Constitucional Federal. Bundesverfassungsgericht. Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 16 jul. 1969.
- ALEMANHA. **Hessisches Datenschutzgesetz**. Hesse, 1970. Disponível em: <<https://datenschutz.hessen.de/ueber-uns/geschichte-des-datenschutzes>>. Acesso em: 20 fev. 2020.

ALEMANHA. **LDSG Rheinland-Pfalz**, jan. 1974. Disponível em: <<http://landesrecht.rlp.de/jportal/portal/t/vyz/page/bsrlpprod.psml;jsessionid=EB>>. Acesso em: 20 fev. 2020.

BARUCH, J. J.; MILLER, A. R. The Assault on Privacy. **Harvard Law Review**, [S. l.], 1971.
BAZERMAN, M. H. **Processo decisório para cursos de administração, economia e MBAs**. São Paulo: Elsevier, 2007.

BELLI, L.; FRANCISCO, P. A.; NOTA, N. Z. Lei do Estado ou lei da Plataforma? Cuidado com a privatização da regulação e da polícia. In: BELLI, L.; CAVALLI, O. **Governança e regulações da Internet na América Latina: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance**. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2019.

BELLI, L.; VENTURINI, J. Private ordering and the rise of terms of service as cyber-regulation. **Internet Policy Review**, 5(4), v. 5, n. 4, 2016.

BERENDT, B; GÜNTHER, O; SPIEKERMANN, S. Privacy in e-commerce. **Communications of the ACM**, [S. l.], v. 48, n. 4, 2005. Disponível em: <http://portal.acm.org/citation.cfm?doid=1053291.1053295>. Acesso em: 20 fev. 2020.

BERNERS-LEE, T.; CAILLIAU, R. **WorldWideWeb**: Proposal for a HyperText Project, 12 nov 1990. Disponível em: <<https://www.w3.org/Proposal>>. Acesso em: 3 jan 2020.

BESMER, Andrew; RICHTER LIPFORD, Heather. Moving beyond untagging: Photo privacy in a tagged world. In: 2010, **Conference on Human Factors in Computing Systems - Proceedings**. [S. l.: s. n.]

BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BOFF, S. O.; FORTES, V. B.; FREITAS, C. O. D. A. **Proteção de dados e privacidade: do direito às novas tecnologias da informação**. Rio de Janeiro: Lumen Juris, 2018.

BOLZAN, J. L.; NETO, E. J. D. M. A Insuficiência do Marco Civil da Internet na Proteção das Comunicações Privadas Armazenadas e do Fluxo de Dados a Partir do Paradigma de Surveillance. In: GEORGE SALOMÃO LEITE, R. L. **Marco Civil da Internet**. São Paulo: Atlas, 2014.

BRANDIMARTE, L; ACQUISTI, A. **The Economics of Privacy**, p. 547-571, 2012. Disponível em: <<http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780195397840.001.0001/oxfordh>>. Acesso em: 22 dez. 2019.

BRASIL. Código Civil Brasileiro de 2002. **Lei nº 10.406, de 10 de janeiro de 2002**, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm>. Acesso em: 20 jan. 2020.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html>. Acesso em: 20 jan. 2020.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet do Brasil. **Diário Oficial**, Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 20 jan. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. **Diário Oficial**, Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 20 jan. 2020.

CAMERER, C. F.; LOEWENSTEIN, G. **Behavioural Economics**: Past, Present, Future. 2002. Available at: <<http://people.hss.caltech.edu/~camerer/ribe239.pdf>>. Acesso em: 08 jun. 2019.

CANNATAKI, J. A. Report of the Special Rapporteur on the right to privacy. **Human Rights Council**, [S. l.], 2016.

CASTELLS, M. **A Galáxia Internet**: Reflexões sobre Internet, Negócios e Sociedade. Rio de Janeiro: Jorge Zahar, 2003.

CASTELLS, M. **A sociedade em rede**. 17 ed. São Paulo: Paz e Terra, v. I, 2016.

CAVOUKIAN, A. **Privacy by Design**: the 7 Foundational Principle. Disponível em: <<https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>>. Acesso em: 20 fev. 2020.

CERF, V. G. Questões e desafios da governança da Internet nas Américas. In: BELLI, L.; CAVALLI, O. **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2019.

CHAIKEN, S.; TROPE, Y. **Dual-process theories in social psychology**. New York: Guilford Press, 1999.

COASE, R. H. The Problem of Social Cost. **The Journal of Law and Economics**, [S. l.], 1960.

CONFESSORE, N. Cambridge Analytica and Facebook: the scandal and the fallout so far. **The New York Times**, 4 abr 2018. Disponível em: <<https://nyti.ms/2GBQ4Lm>>. Acesso em: 08 jun. 2018.

CONSELHO DA UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR)**. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504>>. Acesso 20 fev. 2020.

COSTA, S. Introdução à economia do meio ambiente. **Análise**, [S. l.], p. 301–323, 2005.

DINEV, T.; HART, P. An extended privacy calculus model for e-commerce transactions. **Information Systems Research**, [S. l.], v. 17, n. 1, 2006.

DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019.

ESTADOS UNIDOS. **Fair Credit Reporting Act**, 15 U.S.C. § 1681, de 26 de outubro de 1970. Disponível em: <<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>>. Acesso em: 17 fev. 2020.

ESTADOS UNIDOS. **Privacy Act of 1974**, Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552^a. Disponível em: <<https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf>>. Acesso em: 17 fev. 2020.

EUROPEAN COMMISSION. **Communication on Building a European Data Economy**, 10 janeiro 2017. p. 2. Disponível em: <<https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy>>. Acesso em: 11 fev. 2020.

FACEBOOK. **Facebook Reports Third Quarter 2019 Results**. Disponível em: <<https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Third-Quarter-2019-Results/default.aspx>>. Acesso em: 20 fev. 2020.

FERGUS, Luã. Mi casa es su casa: o impacto dos assistentes digitais sobre privacidade na América Latina. In: BELLI, L.; CAVALLI, O. **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2019.

GARFINKEL, S. **Database Nation**: The Death of Privacy in the 21st Century. Sebastopol: O'Reilly Media, 2000.

GAWRONSKI, B.; CREIGHTON, L. A. Dual Process Theories. In: CARLSTON, D. **The Oxford Handbook of Social Cognition**. New York: Oxford University Press, 2013.

GOLDFARB, A.; TUCKER, C. Privacy and Innovation. **Innovation Policy and the Economy**, v. 12, 2012.

GOMES, Orlando. **Introdução ao Direito Civil**. 19^a. ed. Rio de Janeiro: Forense, 2007.

GREENFIELD, A. **Everyware**: The dawning age of ubiquitous computing. Berkeley: New Riders, v. New Riders, 2006.

GROSSKLAGS, Jens. Privacy and rationality in individual decision making. **IEEE Security & Privacy Review**, Jan./Feb. 2005.

HERMSTRÜWER, Y. Contracting Around Privacy. **Journal of Intellectual Property, Information Technology and Electronic Commerce Law**, [S. l.], v. 45, n. 8, 2017.

HIRSHLEIFER, J. The Private and Social Value of Information and the Reward to Inventive Activity. In: **Uncertainty in Economics**. [S. l.: s. n.].

HOOFNAGLE, Chris Jay *et al.* Behavioral Advertising: The Offer You Can't Refuse. **Harvard Law & Policy Review**, [S. l.], v. 6, 2012.

IGLESIAS, D. **Nudging Privacy: benefits and limits of persuading human behaviour online**, 2017. Disponível em: <<https://itsrio.org/wp-content/uploads/2017/03/Daphnee-Iglesias-.doc-B.pdf>>. Acesso em: 20 jan. 2020.

ISAAC, M; FRENKEL, S. Facebook Security Breach Exposes Accounts of 50 Million User. **New York Times**, New York, 28 set. 2018. Disponível em: <<https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html>>. Acesso em: 20 fev. 2020.

JOLLS, C.; SUNSTEIN, C. R. Debiasing through law. **Journal of Legal Studies**, [S. l.], v. 35, n. 1, 2006.

KAHNEMAN, D. **Rápido e devagar**. duas formas de pensar. Rio de Janeiro: Objetiva, 2012.

KAPSER, A. SANDFUCHS, B. Nudging as a Threat to Privacy. **Rev. Phil. Psych**, 2015. Disponível em: <<http://link.springer.com/article/10.1007/s13164-015-0261-4>>. Acesso em: 20 fev. 2020.

LAI, Yee-Lin; HUI, Kai-Lung. Internet Opt-In and Opt-Out: Investigating the Roles of Frames, Defaults and Privacy Concerns. **2006 ACM SIGMIS CPR Conference on Computer Personnel Research**, [S. l.], 2006.

LAPOWSKY, I. Facebook exposed 87 million users to Cambridge Analytica. **WIRED**, 4 abr 2018. Disponível em: <<https://bit.ly/2IUlptC>>. Acesso em: 08 jun. 2018.

LAUDON, K. Extensions to the theory of markets and privacy: mechanics of pricing information. **NYU Working Paper no. IS-97-04**, jan 1997. Disponível em: <<https://ssrn.com/abstract=1283008>>. Acesso em: 20 fev. 2020.

LEONARDI, M. **Tutela e Privacidade na Internet**. São Paulo: Editora Saraiva, 2011.

LESSIG, L. **The Architecture of Privacy**, Draft 2, 1998. Disponível em: <http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf>. Acesso em: 11 dez. 2019.

MACKAY, Wendy E. Triggers and barriers to customizing software. *In*: 1991, **Conference on Human Factors in Computing Systems - Proceedings**. [S. l.: s. n.]

MÁRQUEZ, Gabriel García. *In*: MARTIN, Gerald. **Gabriel García Márquez: una vida**. Madrid: DEBATE, 2011.

MENDES, L.. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MICROSOFT. **Microsoft Privacy Statement**. Fev. 2020. Disponível em: <<https://privacy.microsoft.com/en-us/privacystatement>>. Acesso em: 20 fev. 2020.

NOAM, E. **Privacy and self-regulation: Markets for electronic privacy**. [s. l.], 1997.

OSBORNE, H. What is Cambridge Analytica? The firm at the centre of Facebook's data breach. **The Guardian**, 18 mar 2018. Disponível em: <<https://bit.ly/2prhWXb>>. Acesso em: 08 jun. 2018.

OULASVIRTA, Antti *et al.* Long-term effects of ubiquitous surveillance in the home. *In: 2012, UbiComp'12 - Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. [S. l.: s. n.]

PARLAMENTO EUROPEU. **Diretiva 95/46/EC**, de 24/10/1995. Disponível em<<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31995L0046>>. Acesso em: 22 fev. 2020

POSNER, Richard A. Values and Consequences: An Introduction to Economic Analysis of Law. **Journal of Political Economy**, [S. l.], 1998.

POSNER, Richard A.. An Economic Theory of Privacy. **AEI Journal on Government and Society**, Regulation, p. 19-26, maio/jun. 1978.

PRINCE, J.; WALLSTEN, S. **How Much is Privacy Worth Around the World and Across Platforms?** [s. l.], 2020. Disponível em: <https://techpolicyinstitute.org/wp-content/uploads/2020/01/Prince_Wallsten_How-Much-is-Privacy-Worth-Around-the-World-and-Across-Platforms.pdf>. Acesso em: 20 fev. 2020

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

ROSS, A. **The Industries of the Future**. New York: Simon & Schuster, 2016.

SAMUELSON, W.; ZECKHAUSER, R J. Status Quo Bias in Decision Making. **Journal of Risk and Uncertainty**, mar. 1988, v. 1 n. 1, pp. 7–59.

SANDERS, J. Defining Terms: Data, Information and Knowledge. **SAI Computing Conference**, London, n. July, 2016 2016. Disponível em: <<https://searchdatamanagement.techtarget.com/feature/Defining-data-information-and-knowledge>>. Acesso em: 20 fev. 2020.

SCASSA, T. Data Ownership. **Centre for International Governance Innovation**, n. 187, set 2018. Disponível em: <https://www.cigionline.org/sites/default/files/documents/Paper%20no.187_2.pdf>. Acesso em: 20 fev. 2020.

SEGERSTÅHL, Katarina; OINAS-KUKKONEN, Harri. Distributed User Experience in Persuasive Technology Environments. *In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. [S. l.: s. n.]. p. 80–91. *E-book*. Disponível em: <http://link.springer.com/10.1007/978-3-540-77006-0_10>. Acesso em: 20 fev. 2020.

SIMON, H. A. A behavioral model of rational choice. **The Quarterly Journal of Economics**, vol. 69, n. 1, feb. 1957.

SPIEKERMANN, Sarah *et al.* The challenges of personal data markets and privacy. **Electronic Markets**, [S. l.], v. 25, n. 2, 2015.

STIGLER, George J. An Introduction to Privacy in Economics and Politics. **The Journal of Legal Studies**, [S. l.], 1980.

SUÉCIA. **Sw. Datalagen**, de 1 maio 1973. Disponível em: <https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289>. Acesso em: 20 fev. 2020.

SUNSTEIN, C. R. The Ethics of Nudging. **SSRN Electronic Journal**, v. 24, n. 6, p. 1-32, 2014. Disponível em: <<http://www.ssrn.com/abstract=2526341>>. Acesso em: 20 fev. 2020

SUNSTEIN, C. R.; THALER, R. H. Libertarian Paternalism Is not an Oxymoron. **University of Chicago Law Review**, v. 70, n. 40, 2003.

SUNSTEIN, Cass R. The Ethics of Nudging. **SSRN Electronic Journal**, [S. l.], v. 24, n. 6, 2014. Disponível em: <<http://www.ssrn.com/abstract=2526341>>. Acesso em: 20 fev. 2020

THALER, R. H.; SUNSTEIN, C. R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade. São Paulo: Objetiva, 2019.

THALER, Richard H.; SUNSTEIN, Cass R. **Nudge**: como tomar melhores decisões sobre saúde, dinheiro e felicidade [e-book]. São Paulo: Objetiva, 2019, n.p.

TVERSKY, A.; KAHNEMAN, D. Judgment under Uncertainty: Heuristics and Biases. **Science**, v. 185, n. 4157, 1974.

WARREN, S.; BRANDEIS, L. The right to privacy. **Harvard Law Review**, v. 4, n. 193, dez. 1890.

WESTIN, A. F. **Privacy and Freedom**. New York: Athenäum, 1967.

WONG, J. C. Facebook says nearly 50m users compromised in huge security breach. **The Guardian**, Londres, 29 sep 2018. Disponível em: <<https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach>> Acesso em: 20 fev. 2020.

WONG, Queenie. Millions of Facebook user phone numbers exposed online, security researchers say. **CNET**, 19 dec. 2019. Disponível em <<https://www.cnet.com/news/millions-of-facebook-user-phone-numbers-exposed-online-security-researchers-say/>>. Acesso em: 27 fev. 2020.

WORLD ECONOMIC FORUM. Personal data: **The emergence of a new asset class**. Davos, 2011. Disponível em: <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>. Acesso em: 12 dez. 2019.

RODOTÀ, Stefano. Prefazione. In: MASERA, Anna. SCORZA, Guido. **Internet, i nostri diritti**. Bari: Laterza, 2016.