BRUNO
RICARDO
BIONI

PROTEÇÃO DE DADOS PESSOAIS

a função e os limites do consentimento

Apresentação
Cíntia Rosa Pereira de Lima

2ª edição revista, atualizada e reformulada

Prefácio
Danilo Doneda

De acordo com:
- **Modificação da Lei Geral de Proteção de Dados** – Lei 13.853/2019
- **Inclusão automática de consumidores no Cadastro Positivo** – LC 166/2019
- **Convenção 108+ do Conselho Europeu**

gen | Editora FORENSE

PROTEÇÃO DE DADOS PESSOAIS

a função e os limites do consentimento

O GEN | Grupo Editorial Nacional – maior plataforma editorial brasileira no segmento científico, técnico e profissional – publica conteúdos nas áreas de concursos, ciências jurídicas, humanas, exatas, da saúde e sociais aplicadas, além de prover serviços direcionados à educação continuada.

As editoras que integram o GEN, das mais respeitadas no mercado editorial, construíram catálogos inigualáveis, com obras decisivas para a formação acadêmica e o aperfeiçoamento de várias gerações de profissionais e estudantes, tendo se tornado sinônimo de qualidade e seriedade.

A missão do GEN e dos núcleos de conteúdo que o compõem é prover a melhor informação científica e distribuí-la de maneira flexível e conveniente, a preços justos, gerando benefícios e servindo a autores, docentes, livreiros, funcionários, colaboradores e acionistas.

Nosso comportamento ético incondicional e nossa responsabilidade social e ambiental são reforçados pela natureza educacional de nossa atividade e dão sustentabilidade ao crescimento contínuo e à rentabilidade do grupo.

BRUNO
RICARDO
BIONI

PROTEÇÃO DE DADOS PESSOAIS

a função e os limites do consentimento

2ª edição revista, atualizada e reformulada

gen | Editora FORENSE

- Capa: Aurélio Corrêa
Produção digital: Geethik

- Data de fechamento: 13.11.2019

- **CIP – BRASIL. CATALOGAÇÃO NA FONTE.**
SINDICATO NACIONAL DOS EDITORES DE LIVROS, RJ.

B514p
Bioni, Bruno Ricardo

Proteção de dados pessoais: a função e os limites do consentimento / Bruno Ricardo Bioni. – 2. ed. – Rio de Janeiro Forense, 2020.

Inclui bibliografia
ISBN 978-85-309-8876-0

1. Internet (Redes de computação) – Legislação. 2. Redes sociais on-line. 3. Direito à privacidade. 4. Habeas-data - Brasil. I. Título.

19-61183 CDU: 34:004.738.5

Meri Gleice Rodrigues de Souza – Bibliotecária CRB-7/6439

Às minhas três mães, Maria, Élida e Edila, ao meu pai, Mauricio, e ao meu irmão, Vinicius, sem vocês nada teria sentido e possibilidade.

À Cecília, por todo o amor e carinho.

A Deus, por iluminar e abençoar o caminho percorrido até aqui.

AGRADECIMENTOS

A trajetória de qualquer profissional não se resume a um único projeto ou a uma empreitada singular. Como é o caso deste livro, que é, em parte, resultado de dissertação de mestrado aprovada na Faculdade de Direito da Universidade de São Paulo. Eu devo muito a uma série de pessoas que extrapolam os três anos durante o curso de mestrado no Largo São Francisco. E, como pesquisador, aprendi que os agradecimentos dos textos revelam a jornada do autor e as suas respectivas influências, de modo que essas páginas também podem ser úteis ao leitor.

Eu tenho plena consciência de que as próximas linhas não expressarão o tamanho da minha gratidão, deixando, inclusive, de nomear pessoas que contribuíram para esse momento. Desculpo-me, desde logo!

Mais do que dedicar este trabalho à minha família, eu devo agradecer a vocês pelo apoio incondicional nessa caminhada. Às minhas três mães, Maria, Élida e Edila. Aos meus melhores amigos, ao meu pai, Mauricio, e ao meu irmão, Vinicius. Ao grande amor da minha vida, Maria Cecília, que tem me apoiado incondicionalmente e por quem eu tenho uma enorme admiração em todos os sentidos. Vocês são a minha essência e a força que me trouxe até aqui, obrigado do fundo do meu coração.

À Fundação de Amparo à Pesquisa do Estado de São Paulo/FAPESP pelo financiamento d pesquisa em âmbito nacional e no exterior, o que possibilitou me dedicar exclusivamente aos estudos ao longo de dois anos e meio.

À minha orientadora, Professora Cíntia Rosa Pereira de Lima, pela confiança depositada. Sem o seu incentivo, nada disso seria possível. Mais do que um exemplo acadêmico, enxergo em você um exemplo de ser humano. Obrigado pela orientação e pela amizade.

Aos professores da Faculdade de Direito da Universidade de São Paulo/FADUSP por cada aula reflexão e discussão tida ao longo da nossa convivência. Em especial, ao Professor Antonio Carlos Morato, por ter me aceitado como seu monitor na graduação e pelas discussões sobre sociedade da informação que exercem forte influência sobre este trabalho; ao Professor José Fernando Simão, que também me aceitou como seu monitor na graduação e pelas discussões sobre direitos da personalidade que inspiraram essa pesquisa; ao Professor Newton de Lucca, pelas valiosas reflexões trazidas na banca de qualificação e que hoje é meu orientador durante o doutorado.

Aos amigos que a FADUSP meu deu, Ana Carolina Moares Aboin, Daniel Pires Novaes Dias Fernando Taveira Júnior e Silvano José Flumignan, pelas conversas que extrapolaram o jurídico para desaguar em uma relação de amizade.

À Faculdade Metropolitana Unidas/FMU, da qual sou filho da graduação. Em especial, ao Professor Roberto Senise Lisboa, a quem tenho uma dívida intelectual e acadêmica impagável; ao Professor Alessandro Segalla, quem primeiro acreditou no meu sonho de ingresso no mestrado e o

apoiou. Aos amigos que a FMU me deu e que carrego comigo, Danilo Melchor, Marco J. Eugle e Fabrício de Araújo Caldas.

Ao Centro de Tecnologia, Direito e Sociedade da Universidade de Ottawa pelo período como pesquisador visitante, que me permitiu enxergar com outros olhos o tema da proteção de dados pessoais. Ao Professor Michael Geist pela coorientação; à Philippa Lawson pelas sugestões na pesquisa; aos amigos, Channarong Intahchomphoo não só por toda a ajuda na biblioteca da faculdade de direito, mas, sobretudo, pelas conversas regadas sempre com muito bom humor; à Sarah Rooney e a toda a sua família, que, com uma amizade sincera, tornaram o inverno canadense e o Natal longe da família mais calorosos.

À Professora Helen Nissembaum por ter me recebido tão bem durante alguns encontros no Privacy Research Group, na Universidade de Nova York, e, sobretudo, pelo diálogo intelectual que permeia grande parte deste trabalho.

Ao Grupo de Políticas Públicas para o Acesso à Informação/GPoPAI da USP por ter me acolhido como mais um GPoPalo. A minha gratidão é imensa por ter encontrado pessoas cheias de energia que me mostraram novas perspectivas sobre privacidade e vigilância. Em especial, aos professores e coordenadores Pablo Ortellado, Jorge Machado e Márcio Moretto Ribeiro pela confiança depositada. Ao Márcio eu devo conversas que me deram fôlego para finalizar esta pesquisa, quando eu pensei que ela estava saturada. Muito obrigado mesmo, GPoPalos!

Ao Conselho da Europa que me aceitou como *study visitor* na Unidade de Proteção de Dados Pessoais. Em especial à Sophie Kwasny por todo o aprendizado e paciência no curto, mas intenso período na linda Strasbourg.

Ao NIC. Br e CGI.br pelo seu tradicional seminário de proteção à privacidade e aos dados pessoais que influencia muito este trabalho e, também, por me aceitarem como parte do time que faz a governança da Internet no Brasil acontecer. Em especial ao Demi Getschko e à Kelli Angelini por apoiaram e incentivarem o meu lado acadêmico e de professor, sem o que não teria sido possível acumular conhecimento para a revisão deste livro. Aos camaradas de Assessoria às Atividade do CGI.br, Prof. Glaser, Carlinhos Cecconi, Diego Canabarro, Juliano Cappi, Marcelo Oliveira, Jea Carlos, Nathalia Sautchuk e Vinicius O. Santos. Aos meus colegas do Jurídico, em especial Diego Sigoli. A tod@s @s demais colegas de departamentos do NIC.br pelas conversas, que me mostraram uma outra dimensão da rede das redes no Brasil.

A toda a comunidade que agita a discussão de proteção de dados pessoais no Brasil, o que possibilitou reflexões fundamentais para o desenvolvimento deste livro. Ao InternetLab, em especial ao Dennys Antonialli, Francisco Brito Cruz, Mariana Valente e Jacqueline Abreu; ao CTS/FGV, em especial à Marina Barros e os que por lá já passaram; à Coding Rights, em especial ao Lucas Teixeira; ao ITS, em especial ao Carlos Affonso de Souza, Eduardo Magrani e Ronaldo Lemos; ao Podcast Segurança Legal, em especial ao Guilherme Goulart; ao IRIS-UFMG, Lucas dos Anjo Luiza Brandão e Pedro Vilela; ao CEDIS-IDP, em especial à Laura Mendes e Sérgio Alves; A

Grupo de Ética e Tecnologia do IEE-USP, em especial ao Professor Ricardo Abramovay e ao "mosqueteiro" Rafael Zanatta; à Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade/LAVITS, em especial Fernanda Bruno, Marta Kanashiro, Rodrigo Firmino e Rafael Evangelista; ao Intervozes, em especial Bia Barbosa, Jonas Valente e Marina Pita; à Artigo 19, em especial ao Paulo Lara (Pajé); ao Centro de Pesquisa em Estudos e à Escola de Direito da Fundação Getulio Vargas de São Paulo, em especial a Alexandre Pacheco, Carlos Liguori e Monica Rosina, Danilo Doneda e Marília Monteiro, que, à frente do Ministério da Justiça, conduziram com maestria o processo de consulta pública do então anteprojeto de lei de proteção de dados pessoais e fez toda essa galera dialogar com mais intensidade; à Coalização Mutlissetorial que foi decisiva para que o Brasil viesse a aprovar a nossa tão aguardada Lei Geral de Proteção de Dados, em especial a Andriei Gutierrez, Sérgio Paulo Gallindo, Nathalie Gazzaneo, Marcel Leonardi, Fabricio da Mota Alves e; a todos os parlamentares brasileiros atentos à importância da pauta para o país, em especial ao Deputado Orlando Silva e deputada Bruna Furlan, respectivamente, relator e presidente da Comissão Especial de Proteção de Dados Pessoais, e ao Senador Eduardo Gomes, autor de uma proposta de Emenda à Constituição que visa a inscrever proteção de dados pessoais no rol de direitos fundamentais. Enfim, sou muito grato à comunidade brasileira de proteção de dados pessoais que é vigorosa e vibrante, este livro bebe diretamente dessa fonte.

Ao Data Privacy Brasil, em especial a tod@s @s alun@s que protagonizam todo o conhecimento gerado de maneira colaborativa, em cada uma das aulas. E, também, a todo o time que coloca de pé a estrutura dos cursos e faz tornar ainda mais prazerosa a docência, em especial ao meu parceiro Renato Leite Monteiro, que se tornou um grande amigo antes de qualquer coisa (valeu artilheiro!).

E a todos os familiares e amigos que estiveram comigo nessa jornada. Aos Aragão, em especial aos meus tios Tino, Vangelo (*in memoriam*) e Zé Alves; aos Bioni, em especial à nossa princesinha Vitória, Vó Araci e Vó José (*in memoriam*); aos Theodoro, em especial ao meu irmão de alma Vitor; aos Branco, em especial ao Alberto, a quem tenho uma profunda admiração; aos Morello, em especial ao Tino que compreendeu e apoiou a minha decisão de trilhar novos caminhos. Ao Marcelo Prisco (*in memoriam*), Vitor Nassar, Rafael Lorente, Roberta Amâncio, Antonio Carlos Malheiros e de todos aqueles que me fogem os nomes, mas que contribuíram para que este momento chegasse.

Um agradecimento especial à Maria Luciano, que me ajudou a revisar todo o conteúdo do livro e as suas novas linhas, períodos, parágrafos e notas de rodapé. Sem a sua colaboração, não teria sido possível alcançar a segunda edição deste trabalho.

Muito obrigado por terem compartilhado esse momento comigo, foi um privilégio. O melhor de tudo é saber que a vida segue e se ela é a arte dos encontros, eu vou tê-los junto comigo sempre!

SOBRE O AUTOR

Doutorando em Direito Comercial e Mestre com louvor em Direito Civil na Faculdade de Direito da Universidade de São Paulo. Foi study visitor do European Data Protection Board/EDPB e do Departamento de Proteção de Dados Pessoais do Conselho da Europa. Além disso, foi pesquisador visitante no Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa e assessor jurídico e de relações governamentais do Comitê Gestor da Internet Brasil/CGI.br e do Núcleo de Informação e Coordenação do Ponto BR/NIC.br. É membro da Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade/LAVITS e Fundador do Data Privacy Brasil. Atualmente, é consultor jurídico na área de regulação e tecnologia com ênfase em privacidade e proteção de dados.

NOTA DO AUTOR À 2ª EDIÇÃO

O ano de 2019 tem sido de grandes mudanças e expectativas para o campo da proteção de dados pessoais. No Brasil, a Medida Provisória 869/2018, convertida na Lei 13.853/2019, trouxe alterações à Lei Geral de Proteção de Dados e criou a Autoridade Nacional de Proteção de Dados (ANPD). A Lei do Cadastro Positivo (Lei 12.414/2011) foi alterada pela Lei Complementa 166/2019, tornando automática a inclusão de consumidores no cadastro positivo e estabelecendo novas previsões a respeito do uso de dados pessoais para fins de avaliação de crédito. Concomitantemente, discutiu-se o balanço do primeiro ano de vigência do Regulamento Europeu de Proteção de Dados Pessoais e a modernização da Convenção 108 do Conselho Europeu. Iniciou-se a contagem regressiva para a entrada em vigor da LGPD no Brasil.

Nesse cenário, uma segunda edição, revisada e ampliada, mostrou-se necessária. Para além de melhor compreender essas alterações normativas no regime de proteção de dados pessoais, esta segunda edição ampliou-se ao buscar apontar balizas e parâmetros para a aplicação prática da LGPD a partir de agosto de 2020. Em especial, listamos os seguintes acréscimos:

a) dois novos subcapítulos sobre o conceito de dado pessoal e 04(quatro) novas esquematizações (imagens, tabelas etc.), sendo que uma delas é um fluxograma que serve como um modelo analítico de comparação entre dado pessoal, dado pseudoanonimizado e dado anonimizado;

b) no capítulo relativo a evidências empíricas e consentimento, um novo subcapítulo que sintetiza os achados da pesquisa, conduzida na Universidade alemã de Bochum, sobre avisos de cookies (*cookies notices*);

c) no subcapítulo relativo aos "núcleos duros" das leis setoriais de proteção de dados pessoais, um novo item que analisa como a Lei do Cadastro Positivo impõe limitações quanto ao uso de dados pessoais para avaliação de crédito independentemente do consentimento do seu titular;

d) no subcapítulo relativo à aplicação da teoria da privacidade contextual a partir de elementos tradicionais da cultura jurídica brasileira, o acréscimo de um novo item para endereçar a figura do abuso do direito;

d) no subcapítulo relativo à base legal do legítimo interesse, o acréscimo de 03 (três) novos itens em torno das seguintes questões controversas: d.1) obrigatoriedade de executar e documentar o chamado teste de proporcionalidade ou avaliação de legítimo interesse (*legitimate interest impact assessment*/LIA); d.2) as possibilidades e os limites do direito de oposição d.3) a lógica de risco no uso de tal base legal, ilustrada a partir das tendências regulatórias no campo da publicidade comportamental;

e) um novo capítulo sobre a aplicação coordenada da LGPD diante das demais normas vigentes a partir da teoria do diálogo de fontes.

Esta segunda edição foi revista e acrescentou-se conteúdo considerável com a esperança de que

este livro ajude na qualificação do debate sobre proteção de dados pessoais no Brasil.

APRESENTAÇÃO

"O verdadeiro discípulo é aquele que supera o mestre."
Aristóteles

Com muito orgulho, apresento o advogado e professor Bruno Ricardo Bioni, o autor da obra intitulada *Consentimento na proteção de dados pessoais: função e limites*. Em 2011, tive a grata oportunidade de ser procurada pelo autor para iniciar seus estudos sobre tal tema de incontestável relevância social e pouco estudado pelos juristas brasileiros. Desde então, Bruno se dedicou intensamente à pesquisa, tendo sido contemplado com a Bolsa de Mestrado da Fundação de Amparo à Pesquisa do Estado de São Paulo/FAPESP, processo n. 2012/25509-0, em que o autor buscou fazer uma releitura do papel normativo do consentimento na proteção dos dados pessoais. Nessa ocasião, a FAPESP destacou o currículo acadêmico do autor, bem como a qualidade técnica dos resultados da pesquisa.

Além do tema desafiador, Bruno realizou, também com fomento FAPESP (processo 2014/08498-0), uma pesquisa no exterior, pouco comum em nível de mestrado. Ele não se intimidou com a escassez de fontes bibliográficas nacionais, ao contrário, foi buscar no Canadá, no Departamento de Proteção de Dados Pessoais do Conselho da Europa, parte do referencial teórico para desenvolver este belíssimo trabalho que ora se apresenta à sociedade brasileira.

O Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa foi exatamente onde eu realizei o meu estágio doutoral (2014-2015), sob a coordenação do Professor Michael Geist, querido amigo, com quem também o autor desenvolveu grande parte do seu trabalho, coletando artigos, livros, bem como entrevistando pesquisadores renomados no tema e do próprio órgão regulador canadense. Entre eles, recordo-me de que foi de grande valia a ida do Bruno a alguns dos encontros do *Privacy Research Group* da Faculdade de Direito de Nova York, sob coordenação da Professora Helen Nissembaum, um dos referenciais teóricos desta obra.

Entre orientadora e orientando há, e deve haver, uma simbiose; e de fato aconteceu entre mim (na qualidade de sua orientadora no mestrado) e Bruno. Assim, seguindo os meus passos, o autor foi muito além, motivo de enorme satisfação e plenitude da missão cumprida.

Nos últimos anos, desde 2011, destaco a colaboração intensa e muito produtiva entre nós, gerando artigos científicos, palestras e experiência em pesquisa e docência. Não obstante, o autor tem muita experiência prática, pois conta com *expertise* de ser advogado do Núcleo de Informação e Coordenação do Ponto Br/NIC.br, entidade responsável por implementar as decisões e projetos do Comitê Gestor da Internet/CGI.br.

Bruno, embora jovem, já apresenta profícuos artigos que foram publicados e até premiados,

como aconteceu com o prêmio de melhor monografia do III Concurso de Monografias do Instituto Brasileiro de Política e Direito do Consumidor/Brasilcon. Além disso, é autor de relatórios de pesquisa e palestrante em eventos nacionais e internacionais, todos com muito impacto na área sobre proteção de dados pessoais. Uma vez mais não será diferente, tamanha a sua seriedade e dedicação, esta obra representa um divisor de águas no cenário nacional quanto ao avanço nos estudos críticos sobre o papel do consentimento, sobretudo na construção de uma dogmática sofisticada da nossa nova Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Ribeirão Preto, 22 de agosto de 2018.

Cíntia Rosa Pereira de Lima

Professora-associada de Direito Civil da Faculdade de Direito de Ribeirão Preto. Livre-docente em Direito Civil Existencial e Patrimonial pela Faculdade de Direito de Ribeirão Preto (USP). Pós-doutora em Direito Civil na Università degli Studi di Camerino (Itália) com fomento CAPES (2014 – 2015). Doutora em Direito Civil pela Faculdade de Direito da USP (2004 – 2009) com estágio na Universidade de Ottawa (Canadá) com bolsa CAPES – PDEE – Doutorado sanduíche.

PREFÁCIO

Todo livro, queira ou não o seu autor, abre um diálogo com o seu próprio tempo e, em algum momento, costuma encontrar o seu lugar. O fato de ter sido escrito com um determinado propósito nem sempre implica que será marcado pelo que seu autor pretendeu ou planejou. Otto Maria Carpeaux, que com os livros tinha extraordinária familiaridade, identificava em alguns deles um caráter próprio, muitas vezes independente de sua qualidade literária. Assim, tinha alguns livros como amigos ou companheiros, outros como referência de alguma tendência ou acontecimento. Em outros casos, até mesmo considerava-os extremamente ruins, chegava a identificar um valor que transcendia a sua qualidade – alguns, por exemplo, porquanto mal escritos, deixam entrever a sinceridade extrema do autor ao descrever uma situação sem qualquer resquício de veleidade intelectual.

A obra de Bruno Bioni, *Proteção de Dados Pessoais: a função e os limites do consentimento*, a meu ver, não suscita muitas dúvidas quanto ao seu lugar. Ela surge vocacionada a desempenhar papel bastante claro e importante no panorama da produção jurídica brasileira relacionada à proteção de dados pessoais. E o diálogo que ela abre lança luz tanto sobre a obra em si quanto à matéria de que trata, o que é um primeiro bom indicativo de sua importância.

O texto é originário de sua dissertação de mestrado, defendida com talento na Faculdade de Direito da USP em 2016, de cuja banca examinadora tive a honra de participar na companhia da Professora Cíntia Rosa Lima, sua orientadora, e do Professor Antônio Carlos Morato – acredito que seja uma das primeiras, senão a primeira, dissertação a versar especificamente sobre o tema da proteção de dados apresentada naquela casa.

De fato, conheci o autor durante seus estudos de mestrado, em uma oportunidade em que estive na Faculdade de Direito da USP – Ribeirão Preto e me chamou muita atenção o interesse e a disposição com que Bioni se interessava por aspectos técnicos da matéria – algo que não era absolutamente usual na época. Desde então, tenho acompanhado a sua trajetória profissional, que, já no espaço de cerca de cinco anos, somente confirmaram as impressões iniciais sobre um pesquisador e advogado voluntarioso, atento e pronto a enveredar pelos recantos teóricos e práticos dos temas de proteção de dados pessoais com fôlego e determinação admiráveis.

Por felicidade, tais traços se fazem sentir vigorosamente na presente obra. E harmonizam-se com o aludido papel do livro, que, acredito, é justamente ajudar na construção de uma dogmática madura em matéria de proteção de dados pessoais. Tal disciplina, no Brasil, vinha se desenvolvendo em uma espécie de limbo: éramos até muito recentemente um dos pouquíssimos países com traços sócio-econômicos assemelhados que não contavam com uma legislação específica sobre proteção de dados pessoais. A promulgação, enfim, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) veio a sanar essa lacuna, ao mesmo tempo em que cria a demanda por uma reflexão aprofundada por

diversos dos elementos fundamentais da proteção de dados, muitos dos quais abordados neste livro, como os conceitos de dado pessoal e de dado anonimizado, os perfis comportamentais e o legítimo interesse, entre outros.

Há institutos jurídicos que permitem que se correlacionem vários desses elementos – a lei brasileira atual, tradições estrangeiras e padrões que almejam a escala global. Um dos mais importantes e significativos desses institutos foi escolhido por Bioni para o tema deste trabalho: o consentimento para o tratamento de dados. O foco no consentimento foi, acredito, opção pragmática do autor que, em um primeiro momento, havia batizado o trabalho originário (a dissertação de mestrado) em torno do conceito de autodeterminação informativa.

No entanto, ainda que se considere o riquíssimo e fundamental conceito cunhado em 1983 pelo Tribunal Constitucional Alemão, é efetivamente em torno do conceito de consentimento que é possível medir e articular uma comparação minimamente relevante entre diversos marcos regulatórios sobre proteção de dados – inclusive aqueles que não são dotados de uma regulamentação central e uniforme. Ao mesmo tempo, parcela considerável das discussões relacionadas à proteção de dados toca em território direta ou indiretamente ligado ao consentimento, seja Big Data ou inteligência artificial, os mecanismos de vigilância, as implementações de Smart Cities e tantos outros.

Tendo a seu favor o fato de ter identificado condições plenas de trabalho nesta "cartografia jurídica", Bioni aplica e coloca à prova com proficiência institutos pertinentes (porém lembrados muito menos do que o necessário) para a delimitação do problema, por exemplo, a boa-fé objetiva, juntamente com cortes dogmáticos úteis para a caracterização da situação brasileira, como a noção de privacidade contextual da Professora Helen Nissenbaum, em um "xeque-mate" – um termo caro ao autor – cujos contornos não pretendo antecipar para convidá-los à imediata leitura da obra, diante da minha garantia que valerá a pena!

26 de agosto de 2018

Danilo Doneda

LISTA DE ABREVIATURAS

APEC – Cooperação Econômica Ásia-Pacífico
CC – Código Civil
CDC – Código de Defesa do Consumidor
CoE – Conselho da Europa
CPF – Cadastro de Pessoas Físicas
DNT – *Do not track*
EFF – *Electronic frontier foundation*
LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018)
MCI – Marco Civil da Internet
P3P – *Platform for privacy preferences*
PET – *Privacy enhancing technology*
PIPEDA – *Personal information protection and electronic documents act*
PIT – *Privacy invasive technology*
PLPDP/EXE – Projeto de Lei de Proteção de Dados Pessoais do Executivo (PL 5.276/2016)
OCDE – Organização para a Cooperação e Desenvolvimento Econômico
STJ – Superior Tribunal de Justiça
UE – União Europeia

SUMÁRIO

Taylor Rodriguez[1] prepara-se para uma rápida viagem de negócios. Ela já arrumou a mala na noite anterior da sua partida e a deixou do lado de fora da casa, em frente à porta, para que alguém a apanhasse. Não há preocupação de que ela seja roubada, pois, além das câmeras das ruas estarem vigiando-a, cada item da sua mala possui etiquetas de radiofrequência. Eventual ladrão seria rastreado, juntamente com as roupas, e imediatamente detido.

Quem vem apanhar a mala é a própria agência de viagens, mas que não necessitou das instruções com relação à data e hora, pois tais informações já haviam sido sincronizadas entre o calendário do *smartphone* de Taylor e o cadastro dela na agência. Na verdade, todo o itinerário da viagem está na nuvem – *cloud computing* –, de modo que a bagagem estará esperando por ela em seu hotel, no destino final da sua viagem.

No dia seguinte, pela manhã, o chuveiro já está ligado e as torradas estão quase prontas, esperando pela Sra. Rodriguez. Todos os aparelhos da casa estão cronometrados com o itinerário da viagem. Inclusive, a sua geladeira, que já encomendou *bacon* e ovos ao supermercado, para quando Taylor retornar de viagem. Pouco mais de 30 (trinta) minutos, o táxi já está buzinando em frente à sua porta. O motorista já tem a rota do aeroporto e toca a *playlist* de músicas favoritas dela; mais uma vez todos os dados estão sendo compartilhados. É só descer do carro, o pagamento já foi realizado via cartão de crédito. Ela se dirige, então, diretamente ao portão de embarque, porque o aeroporto tem reconhecimento facial que faz o controle automatizado do acesso ao saguão.

Enquanto Taylor espera para embarcar na aeronave, ela acessa a sua rede social e compartilha com seus amigos o local para onde está viajando. Ela avança na sua *timeline* e curte uma série de *posts* sobre os protestos que ocorreram na cidade ontem. Ela aproveita o tempo ocioso para convidar seu colega, que está esperando por ela para a reunião de trabalho, para um jantar. A cidade é reconhecida internacionalmente por seus restaurantes de *fast food*; eles já acordaram que vão sair da dieta. Nesse meio-tempo, já se passaram 30 (trinta) minutos e o seu relógio começa a apitar, ela tem que se movimentar e seguir a sua rotina de alongamentos. Ela não consegue, pois tem que entrar no avião e seguir viagem.

O avião pousa. A Sra. Rodriguez chega finalmente ao seu destino e desativa o modo avião do seu *smartphone*. Ela começa a receber anúncios de restaurantes de *fast food*, cuja localização é coincidentemente a cidade onde ela se encontra, bem como de livros sobre ativismo. Ela não tem que se preocupar com a reserva do restaurante, pois seu colega já o fizera, exceto pelo fato de que ela recebeu ofertas com preço superior ao que foi oferecido a ele. O seu relógio, que apitava momentos antes do embarque, já acrescentou mais 01 (um) quilômetro ao seu treino de corrida para amanhã de manhã, por conta da sua indisciplina registrada minutos antes do embarque.

Na mesma hora, ela recebe um *e-mail* da sua seguradora com as novas condições contratuais para

renovar seu plano de saúde. O prêmio sofreu um aumento fora dos patamares dos anos anteriores, pois, segundo a explicação da corretora, a propensão de ela adquirir algum problema de saúde aumentou.

Um último detalhe, talvez o mais importante. Taylor aceitou os termos das políticas de privacidade da agência de viagens, da fornecedora dos aparelhos domésticos da sua casa, da companhia de táxi (ou da plataforma de "caronas pagas"), do aeroporto, da companhia aérea, do seu relógio, da rede social, do hotel (ou da plataforma de "acomodação"), do aplicativo de mensagens de treinos para corrida e, por fim, da sua seguradora de saúde.

Deixando de lado alguns elementos futuristas, o exemplo hipotético da vida da Sra. Rodriguez não é muito diferente do que vivenciamos atualmente. Nossas vidas tornaram-se mais convenientes com a tecnologia. As interações sociais são cada vez mais mediadas pela tecnologia, sendo tudo "datificado". O fluxo das nossas informações pessoais é exponencial e os caminhos por ele percorrido estão, em tese, descritos nas políticas de privacidade, cujos textos são longos, de difícil compreensão e nos deixam poucas escolhas.

É intuitivo o questionamento: *as pessoas têm realmente controle sobre seus dados pessoais*?

Historicamente, a proteção dos dados pessoais tem sido compreendida como o direito de o indivíduo autodeterminar as suas informações pessoais: *autodeterminação informacional*. Recorre-se, por isso, à técnica legislativa de eleger o consentimento do titular dos dados pessoais como seu pilar normativo. Por meio do consentimento, o cidadão emitiria autorizações sobre o fluxo dos seus dados pessoais, controlando-os.

Contudo, o exemplo hipotético mostra-nos que há um solo epistemológico[2] que desafia tal paradigma normativo. Esse trabalho absorve essa percepção crítica com intuito de investigar qual é o *papel normativo a ser desempenhado pelo consentimento na proteção dos dados pessoais: sua função e limites*. Ele se divide em duas partes e em cinco capítulos.

A primeira parte consiste em uma abordagem descritiva. O capítulo 1 aborda a inserção dos dados pessoais na economia da informação, diagnosticando como a maioria dos modelos de negócios é deles dependente, a ponto de se instaurar uma economia de vigilância. O capítulo 2 aloca dogmaticamente a proteção dos dados pessoais como um direito da personalidade autônomo frente à privacidade. Práticas discriminatórias – *e.g.*, de preço (*price discrimination*) – e processos de decisões automatizadas – *e.g.*, análises preditivas – são apenas alguns exemplos de como os dados têm atropelado a pessoa de carne e osso, parametrizando as oportunidades de suas vidas – o mundo da Sra. Rodriguez não é tão hipotético assim!

Com base nesse mapeamento, identifica-se que há uma tensão entre os interesses econômicos e as esferas das pessoas que têm o livre desenvolvimento da sua personalidade afetado pela circulação dos seus dados. Há um *cabo de forças* entre o livre trânsito e processamento dessas informações pessoais para alimentar toda uma economia deles dependente e, de outro lado, a necessidade de se impor limites para a tutela dos interesses extrapatrimoniais da pessoa. Não há, de antemão, uma

resposta conclusiva para acomodar tais interesses conflitantes[3].

Com essa provocação, passa-se à segunda parte do trabalho. O capítulo 3 analisa a travessia do consentimento nas legislações de proteção de dados pessoais, verificando-se que ele teve altos e baixos, mas que se firmou como protagonista ao longo do seu progresso geracional. O maior exemplo disso é que o consentimento continua a ser *venerado*, ganhando, cada vez mais, qualificadores. Inclusive, esse movimento é notado na lei geral e legislação setorial brasileira de proteção de dados pessoais.

Os capítulos 4 e 5 são o coração deste trabalho, momento no qual se reavalia o consentimento como elemento cardeal da proteção de dados pessoais e, em última análise, o conteúdo do que é autodeterminação informacional.

De início, sinaliza-se o descompasso entre tal estratégia normativa e a demanda contemporânea subjacente à proteção dos dados pessoais. Recorreu-se à análise sociológica fundada nos conceitos de vigilância líquida e distribuída, bem como a evidências empíricas que apontam haver uma erosão da esfera de controle dos dados pessoais. Emitiu-se o diagnóstico de que a estratégia normativa eleita é incoerente com a condição de (hiper)vulnerabilidade dos titulares dos dados pessoais, sobretudo por eles estarem inseridos em meio a uma relação assimétrica que lhes tolhe o poder de autodeterminação sobre seus dados. Pondera-se, assim, se o consentimento deve ser o elemento normativo central para a proteção dos dados pessoais.

Com isso, pavimenta-se o caminho de acesso ao problema de pesquisa que este livro procura responder: *Qual é a (re)leitura que deve ser feita sobre o paradigma normativo da autodeterminação informacional e o consequente papel do consentimento para a proteção dos dados pessoais*?

Nossa estratégia para responder a essa pergunta foi *ambivalente*, trabalhando-se com duas lentes de análise que não se repelem, mas se complementam.

Primeiro, identificou-se que a maneira pela qual tem sido operacionalizada a autodeterminação é falha. Questiona-se a sua contratualização – políticas de privacidade –, apontando-se para a necessidade em se pensar novos mecanismos que capacitem o cidadão com o controle de suas informações pessoais. A própria arquitetura da rede deveria funcionalizar essa autonomia, levando-se em conta a condição de (hiper)vulnerável do titular dos dados pessoais. Ao final dessa primeira parte, emprestou-se densidade legal a tal reavaliação *procedimental* sob as arestas do dever-direito de informação.

Segundo, propôs-se outro relato normativo que não deixa ao reino do indivíduo toda a carga da proteção dos dados pessoais. Recorreu-se à *privacidade contextual*, elaborada por Helen Nissenbaum, que permite uma releitura da proteção dos dados pessoais de acordo com o seu valor social. Tal referencial teórico está alinhado com a alocação dogmática da proteção dos dados pessoais entre os direitos da personalidade, bem como que o fluxo informacional deve respeitar as legítimas expectativas do titular dos dados. A privacidade contextual tem como possíveis vetores de

aplicação os princípios da boa-fé e confiança e a teoria dos contratos relacionais e cativos de longa duração no ordenamento jurídico brasileiro.

Cava-se, então, uma abordagem que limita a autonomia da vontade (privada) e desafia a dinâmica tradicional da autodeterminação baseada no consentimento específico. Foca-se no que chamamos de *consentimento contextual*, que endossa a referenciada compreensão de que o fluxo informacional deve ser adequado para o livre desenvolvimento da personalidade e, ao mesmo tempo, condizente aos desafios normativos dos usos secundários dos dados na era do *Big Data*.

O produto dessa reavaliação é a confirmação da hipótese de pesquisa deste trabalho. Conclui-se que as relações do mercado de consumo demandam um novo tipo de dirigismo – *dirigismo informacional* – que se afasta daquele do século passado – dirigismo contratual. Deve haver uma *releitura ambivalente* do paradigma da autodeterminação informacional – *procedimental e substantiva* – que embora mantenha o papel de protagonismo do consentimento, empresta-lhe um novo roteiro normativo: *a percepção de que o titular dos dados pessoais amarga uma (hiper)vulnerabilidade, o que demanda, respectivamente, o seu empoderamento para emancipá-lo e a sua intervenção para assisti-lo*.

[1] Peço licença para introduzir este trabalho de uma maneira pouco usual. Um exemplo hipotético (adaptado) extraído do relatório do Conselho Presidencial de Assessores de Ciência e Tecnologia dos Estados Unidos que permitirá dar a dimensão do problema da pesquisa enfrentado neste trabalho. Executive Office of the President President's Council of Advisors on Science and Technology. Report to the president big data and privacy: a technological perspective, p. 17-18. Disponível em: <https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_pri _may_2014.pdf>.

[2] Seguimos a ponderação metodológica de Orlando Gomes para quem a ciência jurídica não deve se distanciar da realidade social subjacente, sob pena de entrar em crise: GOMES, Orlando.*A crise do direito*. São Paulo: Max Limonad, 1955. p. 5-6: "A realidade social subjacente, ferida nos seus pontos vitais, rebela-se, em desespero, contra as formas em que se condensa. E, nessas altitudes a que se guindara, pelo poder de levitação dos ideólogos, instaura-se a crise, projetada para cima, como se um gigantesco esguicho arremessasse para o alto os átomos libertados pela desintegração da estrutura econômica. É nessas frases que o cunho funcional do direito se revela com maior nitidez".

[3] Por essa razão, esse trabalho foi originalmente intitulado *Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet*, fruto de dissertação de mestrado defendida e aprovada com louvor no Departamento de Direito Civil da Universidade de São Paulo.

Parte I

DADOS PESSOAIS ENTRE A ECONOMIA DA INFORMAÇÃO E OS DIREITOS DA PERSONALIDADE

Capítulo I

SOCIEDADE DA INFORMAÇÃO E DADOS PESSOAIS

1.1 A SOCIEDADE DA INFORMAÇÃO

A sociedade, ao longo do tempo, sofreu diversas formas de organização social[1]. Em cada época, existiu um elemento central para o seu desenvolvimento, sendo o modo pelo qual ele se estruturou o fator determinante para se estabelecer os seus respectivos marcos históricos.

Na *sociedade agrícola*, a fonte de riquezas provinha da terra. Era o produto agrícola que impulsionava a economia por meio da prática do escambo, sendo esta a primeira prática comercial[2].

Em um segundo momento, sobreveio a criação das máquinas a vapor e da eletricidade que detiveram papel central na produção fabril e, por conseguinte, na formação das riquezas (*sociedade industrial*).

Em um terceiro momento, especialmente após a Segunda Guerra Mundial, os serviços angariaram papel de destaque no arranjo socioeconômico. A sociedade – dita *sociedade pós-industrial* – não se caracterizava mais pelo que se poderia produzir, mas pelo que os serviços poderiam ofertar. A prestação de serviços passava a ser a mola propulsora da economia, citando-se, a título de exemplo, os setores bancário, securitário, educacional, de assistência médica e de consultoria jurídica/legal[3].

No estágio atual, a sociedade está encravada por uma nova forma de organização em que a informação é o elemento nuclear para o desenvolvimento da economia[4], substituindo os recursos que outrora estruturavam as sociedades agrícola, industrial e pós-industrial[5].

Essa nova forma de organização social foi sedimentada em razão da evolução tecnológica recente[6], que criou mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais imaginável. Os relacionamentos sociais foram energizados por um fluxo informacional que não encontram mais obstáculos físicos distanciais. Há uma nova compreensão (mais abreviada) da relação entre tempo-espaço[7], o que outrora acarretava maior cadência às interações sociais.

Um exemplo sintomático foram as manifestações de junho de 2013[8]. Nelas, o exercício da cidadania foi revitalizado por um fluxo informacional – em especial das redes sociais – que conectou seus manifestantes, facilitando a organização e a disseminação dos protestos. Verificou-se, sobretudo, um novo instrumento de engajamento social.

Por isso, a informação avoca um papel central e adjetivante da sociedade: *sociedade da informação*. A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como o

fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial.

Ainda que essa nova forma de organização social não se resuma apenas ao meio ambiente virtual[9], a computação eletrônica e a Internet são as ferramentas de destaque desse processo. É justamente em razão desse seu maior impacto que este trabalho investigará a regulação dos bancos de dados eletrônicos, em especial o que mudou no formato da economia e do capitalismo e que é capaz de gerar efeitos (colaterais) sobre o cidadão.

A ciência jurídica como um fato social[10] deve adequar, ou, pelo menos, repensar as suas categoriais para encarar os novos desafios regulatórios emergentes deste novo quadro.

Cumpre, assim, investigar como e quando a informação passou a avocar tal papel de protagonismo, a ponto de imprimir uma completa alteração do padrão em que se estruturam as relações sociais[11].

1.1.1 Virtualização da informação: economia da informação

A grande guinada para o estágio atual da capacidade de processamento de informação foi a transição da plataforma na qual ela é sobreposta.

Antes, o acúmulo, o armazenamento e a transmissão da informação davam-se na forma de átomos[12]. Isto é, por meio da conjugação de partículas que resultavam em algo denso material e fisicamente, como, por exemplo, um livro ou um ficheiro em que o papel absorvia, por meio da técnica da escrita, as informações que se pretendia condensar, até que se descobriram os *bits*[13], que conseguiram agregar, por meio do sistema binário de dígitos (1 e 0), a informação em unidades menores[14]. Tal técnica empregou uma linguagem compreensível para que o computador pudesse processar e armazenar as informações (aglutinadas binariamente) e, até mesmo, responder a comandos predeterminados, como, por exemplo, o uso de palavras-chaves para a finalidade de busca de tais informações.

Dessa forma, os *bits* desmaterializaram a informação, permitindo a sua introdução em computadores[15]. E, com o passar do tempo, todo tipo de informação passou a ser digitalizado, tal como o áudio e o vídeo[16].

Isso implicou uma virada exponencial na *quantidade* de informações processadas. Com a linguagem binária, permitiu-se um acúmulo de informação inimaginável e em novas plataformas – *e.g.*, *compact disk* (CD), *pen drive,* computadores pessoais etc.[17] – em comparação ao suporte primitivo dos átomos – papel[18].

Para além desse progresso quantitativo, experimentou-se, também, uma mudança de ordem *qualitativa* no processamento de informações. A técnica binária permitiu que a informação fosse mais precisamente organizada, facilitando, em última análise, o seu próprio acesso.

Pense, por exemplo, na experiência da pessoa que tem todo o seu arquivo pessoal em papéis (átomos). A primeira variável é ela ser ou não organizada, a ponto de catalogar seus arquivos em

pastas temáticas e/ou em ordem alfabética para facilitar o início da busca pela informação. Se ela nem sequer realiza tal organização manual, há uma grande probabilidade de não ser encontrada a informação desejada. Mas, mesmo que a pessoa proceda a tal organização manual, deverá, ainda, vasculhar as respectivas pastas e papéis arquivados para encontrar tal informação, o que, sem dúvida, consumir-lhe-á um tempo razoável.

Pense, agora, naquele indivíduo que tem todo o seu arquivo digitalizado e salvo em algum dispositivo. Para ele, bastará efetuar uma busca no *search* com as palavras-chaves[19] do arquivo pretendido, havendo, inclusive, a opção de a busca alcançar palavras que estão no próprio corpo do documento. Nesse caso, portanto, até mesmo os mais desorganizados, que não nomeiam seus arquivos, poderão ter acesso à informação desejada e, sobretudo, rapidamente.

Ainda exemplificando, hoje é muito mais fácil efetuar qualquer pesquisa, sobretudo de ordem acadêmica, por meio dos *softwares* das bibliotecas que filtram a sua busca por autor, título, assunto principal, assuntos secundários e outras categorizações. No passado, cabia ao pesquisador acessar o ficheiro da biblioteca, que, frequentemente, estava catalogado somente com o nome do autor da obra, para ter acesso ao conteúdo propriamente dito (assunto principal, secundário etc.).

Tal revolução binária não somente comprimiu *tangivelmente* o armazenamento da informação, mas, igualmente, permitiu a ela um acesso mais facilitado. Houve, portanto, um progresso *quantitativo* e *qualitativo* do processamento informacional[20].

É a conjunção destes dois fatores – aliados e complementados pela criação da Internet – que *virtualizaram*[21] a informação, rompendo com o modelo fordista de produção para instaurar um novo "padrão sócio-técnico-econômico"[22].

1.1.2 Do taylorismo ao modelo organizacional em rede: *informação e conhecimento*

Antes mesmo da criação da Internet, já se havia constatado o papel de centralidade da informação[23] para otimizar o desenvolvimento econômico[24]. Com o *taylorismo*, passou-se a estudar o próprio processo de produção, investindo-se, por exemplo, em treinamento dos operários para se alcançar melhores taxas de produtividade[25]. Portanto, desde a sociedade industrial, já se reconhecia a informação como um fator determinante para a geração de riquezas.

Contudo, é apenas com a mencionada evolução de ordem quantitativa e qualitativa no processamento das informações, que é selado o processo de transição da sociedade pré-informacional para a sociedade informacional. Quem bem elucida tal processo é o sociólogo Manuel Castells, ao pontuar a diferença entre tais formas de organização social, com base no exemplo dos modelos das empresas organizadas em rede.

Ao contrário de uma única empresa centralizar e verticalizar em si todo o processo de produção – da fase de concepção à distribuição de um bem de consumo –, o modelo organizacional em rede prima por um conjunto de empresas que atuam de maneira colaborativa. Cada qual atua de acordo com uma função pré-estipulada[26], o que torna a atividade empresarial descentralizada e horizontal[27].

Por essa estrutura, uma série de empresas está *interconectada* para fornecer um bem de consumo. Por exemplo, a Benetton não produz propriamente suas roupas, que nem são por ela comercializadas. O processo fabril acontece em algum país do sudeste asiático ou do leste europeu[28] e a distribuição acontece em lojas que são em sua grande maioria franqueadas.

Ou seja, a Benneton processa basicamente informações. Ela verifica as tendências do mercado para a projeção dos seus produtos, transmitindo-as[29] às outras empresas responsáveis pelo processo fabril[30].

O mesmo sucede com outra multinacional do segmento de vestuário: a Zara. Os seus lojistas registram os dados das vendas, compartilhando-os com o centro de criação da marca em La Coruña. Uma vez constatada a reação do mercado, isto é, quais itens foram mais aceitos pelos consumidores, os produtos são (re)projetados com base em tal padrão de consumo. Somente após tal retroalimentação, inicia-se, novamente, o processo de produção do bem de consumo.

Muitas outras empresas poderiam ser citadas, que também operam com base em tal modelo organizacional em rede[31]. O fato é, no entanto, que tal estruturação somente foi aperfeiçoada por conta do citado avanço em termos de tecnologias da informação e comunicação/TICs[32]. Isso permitiu ao fluxo informacional[33] avocar o papel de recurso determinante no ciclo econômico[34], preponderando sobre quaisquer outros meios de produção[35].

Essa afluência de fatores é o que organiza a trama[36] da economia informacional. Realocando a semântica de virtualização[37], pode-se dizer que tal conjuntura estabelece uma nova dinâmica para a geração de riquezas[38]. Trata-se de uma economia que passa a ser "*interconectada por um sistema nervoso eletrônico*"[39].

A menção ao termo no sentido figurado – "sistema nervoso eletrônico" – esclarece não se tratar, apenas, de uma economia da informação, mas, necessariamente, do conhecimento. A informação em si não é o que alavanca eficiência na atividade empresarial, mas o seu processamento-organização a ser transformado em um conhecimento aplicado[40]. No caso da Zara, os bens de consumo são reprojetados de acordo com a reação do mercado consumidor, sendo este o conhecimento gerado dos dados extraídos das vendas junto ao seu público-alvo.

E, nesse sentido, as informações sobre os hábitos de consumo dos cidadãos, afora outros dados pessoais, permitem empreender de forma mais eficiente no mercado[41]. Aumentam-se as possibilidades de êxito junto à audiência, seja melhorando a concepção e a segmentação de um produto ou serviço, seja no que pertine à abordagem publicitária para promovê-los.

A informação deve ser, assim, convertida em um conhecimento[42], a fim de torná-la produtiva e estratégica para a atividade empresarial[43]. Por isso, é a matéria-prima de uma economia redimensionada pelos avanços das TICs, destacando-se os dados pessoais dos cidadãos que passam a ditar uma (nova) lógica de acumulação de capital[44] para a geração de riquezas[45].

1.2 OS DADOS PESSOAIS DOS CONSUMIDORES COMO UM ATIVO NA ECONOMIA D INFORMAÇÃO

Com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (*marketing*) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação.

E, com a possibilidade de organizar tais dados de maneira mais escalável (*e.g.*, *Big Data*), criou-se um (novo) mercado cuja base de sustentação é a sua extração e comodificação[46]. Há uma "economia de vigilância" que tende a posicionar o cidadão como um mero expectador das suas informações[47].

Esse é um diagnóstico necessário, sem o qual não se poderia avançar na investigação do papel do consentimento na proteção dos dados pessoais, especialmente, por rivalizar com tal condição de passividade atribuída ao cidadão quanto ao fluxo de suas informações pessoais.

1.2.1 A metáfora do sorvete social: *prosumer*

Scoopville era uma cidade famosa pela produção de sorvetes. Todos os seus moradores produziam os seus próprios "gelatos", cujos sabores variavam de acordo com as suas respectivas preferências. Foi dessa forma que o pequeno vilarejo ficou conhecido como a "Disneylândia" do sorvete, em razão da alta variedade com que o produto era ofertado.

No entanto, os visitantes ficavam simplesmente desnorteados com o volume de opções. Até que um dos comerciantes teve a ideia de colocar um painel, em frente à sua loja, para que os consumidores emitissem as suas opiniões sobre os diversos tipos de sorvetes.

Esses comentários passaram a influenciar não só o consumo por parte dos novos visitantes da cidade, mas, principalmente, a própria fabricação do produto. A sua escala de produção passou a ser orientada pelos tipos de sorvetes mais bem avaliados. Com isso, o produto foi melhorando de forma colaborativa, emergindo daí a metáfora de que o sorvete era social[48].

A Internet e a sua camada de aplicações, principalmente a *web* com *blogs*, redes sociais, *websites* etc., capilarizou esses painéis de opiniões. Os consumidores compartilham e trocam, com mais frequência, em diversos canais e quase em tempo real, informações sobre as suas experiências de consumo: um *blog* em que consumidores de vinhos comentam as suas aspirações de *sommelier*, ou, simplesmente, um consumidor que reclama sobre uma determinada funcionalidade de um produto em uma rede social. Em todas essas situações, eles passam a ser "ouvidos" por seus milhares de pares, parametrizando o próprio movimento de consumo.

É com essa voz ativa, que a popular lição promocional do "boca a boca" se potencializou na sociedade da informação[49], passando o consumidor a atuar como se fosse um assistente de vendas sem custos[50]. Além de ele divulgar o bem de consumo, a informação por ele produzida auxilia em seu processo de produção. O produto ou serviço tende a ser modelado de acordo com os pontos negativos e positivos assinalados por esse elo final da cadeia de consumo, que nunca teve tantos

mecanismos para vocalizar a sua opinião[51].

Esse é um dos componentes essenciais para viabilizar os chamados sistemas flexíveis de produção (subcapítulo 1.1.1)[52], em que tais tendências do mercado consumidor[53] orientam[54] dinamicamente a concepção de um bem de consumo.

O consumidor deixa, portanto, de ter uma posição meramente passiva no ciclo do consumo. Ele passa a ter uma participação ativa[55], que condiciona a própria confecção, distribuição e, em última análise, a segmentação do bem de consumo, transformando-se na figura do *prosumer*[56]. O consumidor não apenas consome (*consumption*), mas, também, produz o bem de consumo (*production*): *prosumer*.

1.2.2 A publicidade direcionada como a tônica dos modelos de negócios na Internet

O cenário acima descrito revela como são valiosas as informações pessoais dos consumidores, evidenciando que o seu gerenciamento é um elemento estratégico transformador do *marketing* em geral[57]. Além disso, ele é também um vetor de mutação da atividade publicitária[58] como a tônica da grande maioria dos modelos de negócios na Internet.

1.2.2.1 Publicidade direcionada: contextual, segmentada e comportamental

A publicidade pode ser conceituada como a comunicação estabelecida entre consumidor/comprador e fornecedor/vendedor de um produto ou serviço, por meio da qual não só se informa a respeito das características do bem de consumo, como, também, promove-se a persuasão ao ato de consumo[59].

Vale dizer que a publicidade se insere no movimento da chamada *despersonalização* das relações privadas[60]. Trata-se de um método de abordagem que visa a alcançar uma gama de consumidores, difundindo informações de um objeto (produto) ou atividade (serviço) a um universo de pessoas[61].

Os anúncios em revistas, jornais e televisão são autoexplicativos. O leitor ou telespectador é uma massa, uma coletividade, a que se busca transmitir uma mensagem para promover um bem de consumo e, ao final, induzir o seu consumo.

Ainda que seja paradoxal, a ciência mercadológica percebeu que tal comunicação em massa era ineficiente, uma vez que se desperdiçavam esforços com um público que não teria qualquer propensão a consumir o bem anunciado. Nesse contexto é que surge a publicidade direcionada, a fim de mitigar tal caráter estandardizado de abordagem.

Seria muito mais efetivo canalizar tal processo comunicativo para um público específico, que se mostrasse mais inclinado a adquirir o bem ofertado. Por exemplo, há uma maior probabilidade de que leitores de revistas de carros tenham interesse na aquisição de tal bem, já que se subentende que quem está pesquisando sobre o assunto tende a ser um potencial comprador.

Do mesmo modo, o anúncio de um livro sobre política tende a ser mais efetivo se hospedado no

caderno de política de um determinado jornal, uma vez que os leitores daquele caderno específico têm predileção sobre tal assunto. Direciona-se, assim, a publicidade em um ambiente propício para captar a atenção do consumidor, facilitando-se, pois, o encontro entre comprador e vendedor, que é o desiderato último da publicidade[62].

Ou seja, a publicidade direcionada é uma prática que procura personalizar, ainda que parcialmente, tal comunicação social, correlacionando-a a um determinado fator que incrementa a possibilidade de êxito da indução ao consumo. Essa prática subdivide-se em publicidade (direcionada) contextual, segmentada e comportamental – espécies do gênero publicidade direcionada.

Os exemplos acima citados enquadram-se na denominada *publicidade contextual*, que correlaciona a temática de um determinado ambiente (*aspecto objetivo*), seja ele o conteúdo de um determinado caderno de um jornal impresso (*off-line*) ou de um *website* (*on-line*), ao objeto anunciado[63]. Contextualiza-se, pois, a abordagem ao potencial consumidor, levando-se em conta o meio na qual é promovido o bem de consumo.

Ao passo que a *publicidade segmentada* se foca no *aspecto subjetivo*, isto é, no próprio público-alvo do bem ofertado. Não importa propriamente o conteúdo do ambiente em que será direcionada a publicidade, mas o público que a ele tem acesso. Se o bem de consumo direciona-se ao público feminino de meia-idade, adolescentes ou pessoas idosas, a abordagem será, então, realizada em ambientes onde a audiência de tal público seja predominante. Segmenta-se, portanto, a publicidade a uma determinada camada da massa de consumidores, independentemente de qual seja o contexto da plataforma em que a publicidade está sendo veiculada[64].

Há, por fim, a chamada *publicidade comportamental on-line*, que é outra espécie da publicidade direcionada[65]. Esta última prática publicitária permitiu uma *personalização* maior ainda do contato entre compradores e vendedores, sendo mais efetiva em relação às anteriores[66].

Cada vez mais, os usuários da Internet subvertem-se em consumidores, sendo uma clara amostra de tal afirmação o crescimento exponencial do comércio eletrônico. No Brasil, o *e-commerce* acumula taxas de crescimento significativas, tendo faturado a quantia expressiva de R$ 44,4 bilhões no ano de 2016[67]. Assim, cresce, em igual importância, os anúncios publicitários *on-line* para induzir o usuário ao consumo.

Nesse sentido, a ciência mercadológica percebeu que a Internet poderia propiciar uma abordagem publicitária mais efetiva. Por meio de diversas ferramentas tecnológicas[68], dentre as quais se destacam os *cookies*[69], tornou-se possível rastrear a navegação do usuário e, por conseguinte, inferir seus interesses para correlacioná-los aos anúncios publicitários.

Por meio do registro da navegação dos usuários cria-se um rico retrato[70] das suas preferências, personalizando-se o anúncio publicitário. A abordagem publicitária passa a ser atrelada com precisão ao perfil do potencial consumidor. Sabe-se o que ele está lendo, quais os tipos de *websites* acessados, enfim, tudo aquilo em que a pessoa está efetivamente interessada[71] e, em última análise, o

que ela está mais suscetível a consumir com base nesse perfil comportamental.

Quando o usuário navega na Internet, há uma série de cliques (*clickstream*)[72] que revela uma infinidade de informações sobre as suas predileções, possibilitando que a abordagem publicitária as utilize para estar precisamente harmonizada com elas. Desta forma, a publicidade *on-line* pode ser direcionada com um grau de personalização jamais alcançado pela publicidade *off-line*.

Por isso, a publicidade comportamental *on-line* reduz os custos da ação publicitária[73], uma vez que o bem de consumo anunciado é correlacionado cirurgicamente aos interesses do consumidor abordado. A comunicação com o público-alvo daquele produto ou serviço é praticamente certeira, ocasionando maior probabilidade[74] de êxito quanto à indução ao consumo.

Mais do que isso, os próprios cliques permitem mensurar a eficiência do anúncio publicitário, sendo o potencial consumidor também monitorado com relação ao seu efetivo interesse na comunicação estabelecida. Por exemplo, o mecanismo de buscas do Google, além de estabelecer uma correlação entre as palavras buscadas pelo usuário à publicidade direcionada[75], define que a contraprestação somente será devida se o potencial consumidor clicar no correspondente anúncio (Google AdWords).

De maneira similar, as redes sociais acumulam os mais diversos dados pessoais dos seus usuários, que são extraídos ao longo de toda a sua interação com a aplicação. Uma vez *logado*, o usuário passa a fornecer um rico perfil de si, que é o que viabiliza o direcionamento da publicidade[76].

Diversos outros serviços utilizam da mesma técnica, catalogando o comportamento do usuário para, a partir daí, direcionar uma publicidade condizente ao seu perfil inferido. O usuário da rede é, portanto, a todo momento, monitorado, acumulando-se uma série de dados (comportamentais), que são aplicados para a personalização da abordagem publicitária.

A ciência mercadológica reverte tal vigilância em um conhecimento[77] para agregar eficiência à publicidade veiculada no ambiente virtual, encerrando-se, pois, um ciclo, como acima demonstrado, da economia da informação e do conhecimento. Os dados pessoais dos usuários são uma peça singular dessa engrenagem.

1.2.2.2 Dos hábitos de navegação dos consumidores, localização geográfica à publicidade basea nas emoções: o consumidor de vidro

Para além do monitoramento dos hábitos de navegação dos usuários, a Internet, juntamente com a tecnologia móvel, permitiu avançar mais ainda no direcionamento das ações publicitárias.

Se em um passado próximo questionava-se qual seria o tamanho do mercado de aparelhos celulares, pode-se dizer que, com a criação da Internet móvel, tais incertezas diluíram-se completamente. Esse mercado ascendeu de forma exponencial[78], o que foi impulsionado pela demanda do seu público em eleger o celular como o principal dispositivo de acesso à Internet, em comparação ao computador[79].

Com isso, as pessoas estão cada vez mais conectadas. Há uma imbricação entre os ambientes *on-line* e *off-line*, já que tais dispositivos nos acompanham ao longo de toda a nossa jornada.

Essa onipresença da Internet permitiu, de forma acoplada com a possibilidade do monitoramento da localização geográfica (*global positioning system*/GPS)[80] dos *smartphones*[81], que as publicidades também sejam direcionadas com base em tal informação. Leva-se, assim, em conta, a proximidade física do potencial consumidor ao bem de consumo ofertado, como, por exemplo, seria o caso de um restaurante[82].

Esse é um dos motivos pelos quais o aplicativo Waze, que captura a geolocalização de seus usuários, foi adquirido pela Google pela quantia expressiva de US$ 1,3 bilhão[83]; ou, ainda, por que uma rede social permite ao usuário marcar os locais que frequenta – "*check-in*". Tais dados de geolocalização são extremamente valiosos[84].

Não é, portanto, uma mera coincidência que surja um anúncio publicitário, cujo bem de consumo esteja bem próximo geograficamente[85] do cidadão ao utilizar um *smartphone*. A publicidade baseada na localização do potencial consumidor é uma (nova) estratégia mercadológica[86].

É o chamado *mobile marketing* que implementa uma integração entre publicidade, Internet e telefone celular, sendo mais uma ferramenta para colocar consumidores e fornecedores em contato[87].

Além disso, os *smartphones* e seus *apps* substituem, cada vez mais, outros meios de comunicação. Por exemplo, o serviço de mensagem de textos passou a ser superado por aplicativos de mensagens, como o WhatsApp[88]. Com isso, as pessoas comunicam-se e, cada vez mais, expressam-se no ambiente virtual. Tal ubiquidade tornou possível inferir até mesmo o estado emocional das pessoas.

Ao se comunicar com alguém por meio de um ícone de expressão – os chamados *emoticons*[89]; ao responder à sua rede social como está se sentindo[90] ou nela emitir uma opinião sobre um determinado assunto[91]; ao interagir com um aplicativo de música para que ele forneça faixas musicais de acordo com o seu humor[92], as pessoas fornecem um rico retrato das suas emoções[93].

Nesse cenário, há um movimento de empresas que buscam captar, interpretar e utilizar tais sentimentos[94]. Novamente, a ciência mercadológica vale-se de tais informações para potencializar a mensagem publicitária "com base em uma análise detalhada sobre o impacto emocional deles [delas] no usuário"[95].

Não por outro motivo, Microsoft, Apple e Google têm realizado investidas nesse sentido, respectivamente com: **i)** o patenteamento da tecnologia de direcionamento de anúncios com base em emoções[96]; **ii)** a implementação de um sistema de processamento de movimentos (M7), o qual identifica os deslocamentos dos usuários para precisar o estado mental deles no momento de interação com o celular[97]; **iii)** projeção de um sistema para detectar sorrisos e outras expressões faciais de quem assiste a vídeos no YouTube[98].

É uma realidade, portanto, a estruturação de bases de dados de emoções[99], a fim de personalizar ainda mais a ação publicitária. Há, por isso, uma *vigilância imperativa* das pessoas, em especial do

potencial consumidor, o que varia desde os seus hábitos de navegação e comportamento na Internet às suas próprias emoções, tornando-o, totalmente, transparente. A expressão "consumidor de vidro"[100], cunhada por Susanne Lace, alcança seu êxtase[101].

1.2.2.3 Os modelos de negócios na Internet: entre o "gratuito" e o freemium

Desnecessário mapear ou trazer o percentual dos produtos e serviços *on-line* para dizer que eles são em sua grande maioria "gratuitos", não havendo uma *contraprestação pecuniária direta* para a sua fruição por parte dos usuários.

De fato, na tela dos computadores prevalece o acesso "livre" às redes sociais, *e-mails*, mecanismos de busca, *softwares*, portais de notícias e aos mais diversos aplicativos para *smartphones*. Raros são os serviços ou produtos em que é necessário despender alguma quantia em dinheiro, a título de contraprestação, para o seu *download* e/ou acesso.

Como, então, podem ser lucrativos tais negócios?

A resposta para tal indagação já foi previamente construída nos itens anteriores, quando se discorreu sobre a inserção dos dados pessoais na economia da informação e como vetor central da publicidade comportamental.

No modelo de negócio "tradicional", consumidores trocam uma quantia pecuniária por um bem de consumo. Por exemplo, cada item de um carrinho de supermercado tem o preço exato a ser pago para a sua aquisição[102]. Trata-se de uma *relação bilateral* entre consumidor e fornecedor, cuja transação econômica é aperfeiçoada por uma transferência pecuniária.

Ao passo que, sob um novo modelo de negócio, consumidores não pagam em dinheiro pelos bens de consumo, eles cedem seus dados pessoais em troca de publicidade direcionada. São os anunciantes de conteúdo publicitário que aperfeiçoam o seu arranjo econômico. Dessa forma, tal relação torna-se *plurilateral*, uma vez que ela envolve, necessariamente, os anunciantes de conteúdo publicitário, para haver retorno financeiro nesse modelo de negócio.

Por essa lógica, o consumidor torna-se também um produto comercializável[103], já que seus dados integram a operação econômica em questão.

Trata-se de um modelo de negócio que é financiado[104] ou suportado[105] predominantemente pela publicidade comportamental. Em um primeiro momento, atrai-se o usuário para que ele usufrua de um serviço e/ou produto para, em um segundo momento, coletar seus dados pessoais e, então, viabilizar o direcionamento da mensagem publicitária, que é a sua fonte de rentabilização[106].

A terminologia *zero-price advertisement business model*[107] resume bem essa dinâmica. Os usuários não pagam uma quantia monetária (*zero-price*) pelo produto ou serviço. A contraprestação deriva do fornecimento de seus dados pessoais, o que possibilita o direcionamento de conteúdo publicitário, e cuja receita pagará, indiretamente, pelo bem de consumo (*advertisement business model*).

Há uma troca (*trade-off*)[108] dos dados pessoais pelo serviço ou produto[109]. O consumidor, quando

lê uma notícia em um portal, quando envia *e-mails*, quando posta em uma rede social, quando efetua uma busca e quando consome outros tipos de produtos ou serviços, acaba por movimentar tal ciclo econômico.

A formatação desse modelo de negócio confirma, portanto, a monetização dos dados pessoais, tornando coerente a *equação econômica* da grande gama de produtos e serviços que são "gratuitamente" disponibilizados na Internet.

A prevalência de tal engenharia comercial acaba por ser contagiante. Mesmo plataformas de negócios que têm a perspectiva de subverter tal lógica, ao impor uma contraprestação pecuniária direta, acabam por se curvar à escala do "gratuito". É o que se verifica nos denominados modelos de negócio *freemium*.

Freemium é a combinação de gratuito (*free*) com diferenciado (*premium*)[110]. Nesses modelos de negócios, permite-se o acesso livre e "gratuito" a um determinado tipo de serviço ou produto *on-line*, mas em sua versão limitada ou básica[111]. Para que se tenha acesso à versão completa de um *software* ou à íntegra de um portal de notícia – a versão *premium* – é necessário que haja uma contraprestação pecuniária direta – a versão "paga".

São, portanto, projetadas versões diferentes de um mesmo produto, o que, em princípio, corresponderia a diferentes modelos de negócios. No entanto, mesmo as versões *premium* não deixam de contabilizar os dados pessoais para rentabilizar mais ainda esses negócios. Por vezes, tais serviços e produtos acumulam fontes de rentabilização, como se nota da prática – por vezes comum – de se adotar a mesma política de privacidade para os usuários *premium* e *freemium* e, em última análise, do uso que se fará dos seus dados pessoais[112].

Nessa perspectiva, afirma-se comumente que o pagamento – seja ele integral ou parcial – de muitos serviços e produtos é realizado com os dados pessoais do próprio consumidor.

Deve-se aceitar com reservas tal ponderação. Isto porque o titular dos dados não sabe, na verdade, qual será o *custo efetivo* da transação. São inúmeras as possibilidades de uso que pode ser feito dos seus dados, especialmente no contexto do *Big Data* (vide subcapítulo 1.3.2). São uma verdadeira incógnita os eventuais prejuízos ou mesmo benefícios que tal operação econômica pode desencadear.

Traçando um paralelo com outras operações econômicas, cuja contraprestação pelo bem de consumo é fixada pecuniariamente, sabe-se exatamente o custo da transação caracterizado por um *deslocamento patrimonial*, enquanto na lógica da economia informacional, é incerto como a disponibilização de uma informação pessoal poderá afetar o seu titular e, por conseguinte, o "preço" a ser pago pelo bem de consumo.

Como será aprofundado mais à frente, mediante uma análise crítica da autodeterminação informacional, o titular dos dados não sabe, ao certo, como eles serão utilizados ou com quais outros pedaços de informação serão cruzados. Inviabiliza-se, dessa forma, qualquer tipo de inferência sobre os custos efetivos da operação econômica em questão (vide subcapítulo 4.1.2).

Além disso, a coleta dos dados pessoais é contínua. Na medida em que se usufrui de um produto ou serviço, várias informações estão sendo coletadas e agregadas, sendo incerto o fluxo informacional e o que dele se pode extrair. Ainda que seja paradoxal, "compra-se agora para pagar depois", dado esse quadro de incertezas[113].

1.2.2.4 A multidão de atores da rede da publicidade direcionada on-line

A exponencialidade do fluxo e da agregação dos dados pessoais torna-se ainda mais evidente quando se analisa o *ecossistema* da publicidade *on-line*. Como dito, o *zero-price advertisement business model* quebrou com a tradicional bilateralidade das relações de consumo, tornando-as plurilaterais. Há uma complexa rede de atores que operacionaliza a entrega de publicidade *on-line* para rentabilizar os serviços e produtos "gratuitos" *on-line*.

A percepção de que os mesmos anúncios publicitários perpassam não apenas um determinado *website*, mas boa parte da navegação[114] do usuário, é um indicativo de que tais *players* agem cooperativamente[115] para o direcionamento da mensagem publicitária. Tal prática somente é possível em razão da existência das chamadas redes de publicidade (*ad networks*)[116]. Elas conectam milhares de aplicações, como *websites* que exibem (*publishers*) publicidade aos fornecedores, que querem anunciar (*advertisers*) um bem de consumo.

Os veiculadores (*publishers*) associam-se a tais redes, terceirizando a venda, total ou parcialmente, dos seus espaços publicitários. Assim, mediante tais acordos, um anunciante (*advertisers*) poderá capilarizar a promoção de seu produto por todos os *publishers* dessa rede[117], em vez de fazê-lo, isoladamente, apenas em uma determinada aplicação.

Tal como a terceirização da comercialização do espaço publicitário, delega-se, também, o rastreamento do potencial consumidor. Via de regra, as *ad networks* são quem instalam as tecnologias de monitoramento da navegação do usuário (*third-party tracking*)[118], criando uma *arquitetura* que o acompanha junto a todas as aplicações integradas à rede e que, potencialmente, corresponde a uma parcela significativa de toda a sua navegação. Constrói-se, assim, um perfil mais rico[119] sobre as preferências do indivíduo, tornando, em última análise, a publicidade comportamental mais precisa.

Com tal intuito, as próprias redes de publicidade comportamental também cooperam entre si (*ad exchanges*)[120], transacionando as suas respectivas bases de dados para maximizar o alcance e a precisão da ação publicitária. Há, dessa forma, uma *sobreposição de redes de publicidade*, cuja lógica é estruturar bases de dados mais volumosas que sejam capazes de cobrir todo o comportamento do potencial consumidor para uma promoção mais persistente e personalizada do bem de consumo.

Com base nessa lógica de acumular a maior quantidade possível de dados[121] é que surgem os *data brokers*. O mote dessa indústria é reunir pedaços de informações de inúmeras fontes, bases de dados públicas (governamentais) e privadas (adquiridas do setor privado), que não se restringem ao

ambiente *on-line*[122], para vender e revender os dados pessoais dos cidadãos[123]. O prefixo utilizado "re", que denota a repetição de uma atividade, enfatiza a característica marcante dessa indústria, que é extrair a máxima rentabilidade dessa economia de vigilância.

Nesse sentido, os tipos de serviços ofertados extrapolam o campo da publicidade direcionada, consistindo em um modelo de negócio ainda mais intrusivo[124]. Por exemplo, os *data brokers* prometem otimizar a qualidade das bases de dados pessoais de outros atores, certificando que elas contêm informações atualizadas para que, dentre outros motivos, a publicidade direcionada corresponda às preferências de um indivíduo[125]. Além disso, com o processamento de bases de dados cada vez mais volumosas, eles conseguem segmentar grupos de prováveis consumidores com base numa determinada característica comum deles[126] e alcançar qualquer tipo de potencial consumidor (*matching and targeting*). O resultado desejado é a predição comportamental desses indivíduos para refinar as campanhas publicitárias (*data analytics*)[127].

Sem a pretensão de esgotar cada ator inserido nessa teia complexa da rede da publicidade comportamental, há a seguinte multidão de sujeitos envolvidos:

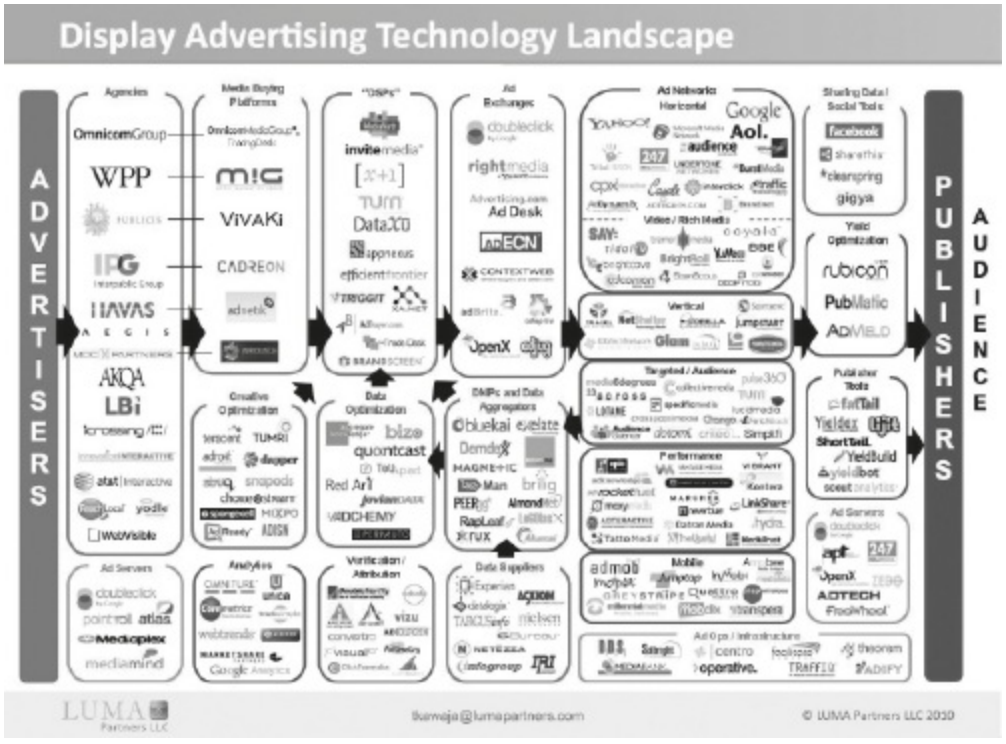


Figura 1. Rede de publicidade direcionada no cenário estadunidense[128].

Figura 2. Rede de publicidade direcionada no cenário brasileiro[129].

O *zero-price advertisement business model* consiste, portanto, em um (novo) modelo de negócio, que esconde uma série de sujeitos para a sua operacionalização. É uma intricada e complexa rede de atores que atua colaborativamente para a entrega de publicidade direcionada (comportamental). Dentre alguns desses atores, inserem-se os chamados *data brokers*, que agregam a maior quantidade possível de dados para ajustes ainda mais finos nas campanhas publicitárias. Como resultado, há um fluxo informacional abundante e difícil de mapear todos os atores nele envolvidos, o que é desafiador para qualquer perspectiva regulatória.

1.2.2.5 O exemplo da aquisição do WhatsApp pelo Facebook

Um bom exemplo para ilustrar tudo o que foi dito acima sobre os modelos de negócios escorados na publicidade comportamental é a aquisição do aplicativo de mensageria WhatsApp pela rede social Facebook, na ordem de U$ 19 bilhões de dólares – uma das maiores transações da história desse ramo[130].

O WhatsApp não só surgiu como um aplicativo para troca de mensagens privadas, mas, também, com a promessa de que os dados pessoais dos seus usuários não seriam revertidos para fins de publicidade comportamental.

Nesse sentido, o próprio criador do aplicativo cogitou que fosse pago o valor de U$ 1,00 dólar ao ano. O discurso era de que seus usuários (entenda-se seus dados pessoais) não seriam o produto a ser comercializado[131].

Essa promessa foi um dos fatores pelos quais tal aplicativo teria alcançado tanta audiência ao redor do mundo. Por isso, a *Eletronic Privacy Information Center*/EPIC e o *Center Digital for*

Democracy ingressaram com um procedimento no órgão regulador americano (*Federal Trade Commission*/FTC) para investigar os propósitos de tal aquisição, a fim de assegurar e questionar se seria mantida a promessa de que os dados pessoais dos usuários não alimentariam ações publicitárias[132].

Em 2015, a (nova) política de privacidade do WhatsApp concretizou a cogitada reversão do seu modelo de negócio. Agora, os dados dos seus usuários são compartilhados entre o grupo de empresas do Facebook[133] para "aprimorar as experiências" dos seus serviços, especialmente com relação aos "anúncios e produtos no Facebook"[134].

O valor de U$19 bilhões teria sido uma "bagatela". A perspectiva de rentabilizar os dados pessoais dos usuários da plataforma via publicidade comportamental elevaria o valor de U$ 1,00 por ano – como antes cogitado pelo próprio fundador do aplicativo – para U$12,00 ao ano por usuário[135].

É por esta razão que é paradigmática a aquisição do WhatsApp pelo Facebook, pois muito explica a respeito da propugnada monetização dos dados pessoais. Em especial, como uma determinada estratégia comercial influencia toda a discussão regulatória sobre proteção de dados pessoais[136].

Acontece que tais atividades somente se tornaram possíveis devido à estruturação de enormes bancos de dados, que organizam todo esse volume de informações (vide subcapítulo 1.1). Cabe, assim, tecer breves considerações a respeito de como se dá esse processo de gestão da informação: a estruturação e a mineração de uma base de dados.

1.3 MINERANDO DADOS

Não se pretende abordar, tecnicamente, os elementos que compõem um banco de dados, seja porque isso demandaria um conhecimento muito especializado de sistemas de informação, seja porque isso fugiria do escopo deste trabalho.

Dessa forma, busca-se compreender a dinâmica de um banco de dados para esclarecer algumas questões terminológicas, tais como a diferença entre dados e informação, e entre banco de dados e cadastro de consumidores. E, ainda, tecer considerações a respeito de *Big Data*, que é, atualmente, a tecnologia de maior destaque para a estruturação e mineração de uma base de dados.

Essas questões são relevantes para a construção das conclusões futuras deste livro.

1.3.1 Sistemas de informação: dados, informação e conhecimento

De início, cabe destacar que dados e informação não se equivalem, ainda que sejam recorrentemente tratados na sinonímia e tenham sido utilizados de maneira intercambiável ao longo deste trabalho. O dado é o estado primitivo da informação[137], pois não é algo *per se* que acresce

conhecimento. Dados são simplesmente *fatos brutos* que, quando processados[138] e organizados[139], se convertem em algo inteligível, podendo ser deles extraída uma informação[140].

Tome-se, novamente, o exemplo citado da multinacional Zara (vide subcapítulo 1.1.2). A simples ação de coletar e acumular os fatos (dados) das vendas e saídas de seus produtos é algo que em si não é dotado de nenhum significado. Somente quando organizados, especialmente para o fim de identificar quais produtos foram os mais vendidos, extrai-se, então, uma informação útil. Especificamente, quais produtos tiveram melhor aceitação pelo mercado consumidor para (re)projetá-los de acordo com tal tendência.

Por isso, a dinâmica de um banco de dados envolve entrada (*input*) e processamento de dados e a saída (*output*)[141] de uma informação. É imprescindível, portanto, o gerenciamento, manual ou automatizado, de um banco de dados, para que dele seja extraído algum conhecimento[142].

A informática e a tecnologia da informação foram cruciais, pois foi com os *softwares*[143] que se automatizou, ainda que parcialmente, a gestão desses bancos de dados, havendo, por conseguinte, uma guinada de ordem qualitativa[144] no processamento de tais informações brutas.

Fala-se em automatização parcial, pois tais *softwares* não eliminaram a etapa prévia, conduzida por um ser humano, de *estruturação* dos dados. Por exemplo, quando se "alimenta" um banco de dados, que gerencia as contas a receber de uma empresa, devem ser inseridos corretamente: **i)** o nome do cliente: o núcleo principal donde derivam todos os demais dados, o que é chamado de *entidade*; **ii)** o valor do serviço, da linha de crédito e o endereço: todos os demais dados que são chamados de *atributos*.

Somente assim é possível emitir faturas de cobrança, relatórios dos clientes inadimplentes, saldos devedores etc.[145] Esse é o chamado banco de dados operacional[146].

Interessam, contudo, os chamados *data warehouses*, que seguem a mesma lógica acima delineada, mas são utilizados para uma tomada de decisão. Tal sistema de gerenciamento permite, por exemplo, identificar um fator que será determinante para adoção ou não de uma ação de *marketing*, como a classificação daqueles clientes que têm maior probabilidade de serem seduzidos por uma "mala direta", ou, por outro tipo de abordagem publicitária[147]. Ou, ainda, no exemplo antes mencionado, se a linha de crédito deverá ser expandida de acordo com a inadimplência acumulada dos clientes-devedores.

É essa dinâmica que possibilita que uma *montanha de fatos*[148] (dados) sobre os usuários da Internet seja gerenciada (informação) para lhes direcionar mensagens publicitárias personalizadas (conhecimento)[149] – vide subcapítulo 1.2.2. Trata-se, portanto, de um fator crítico[150] e viabilizador da publicidade comportamental.

Portanto, que um banco de dados deve ser necessariamente atrelado à ideia de um sistema de informação[151], cuja dinâmica explicita, sequencialmente, um processo que se inicia pela coleta e estruturação dos dados, perpassa a extração de uma informação que, por fim, agrega conhecimento.

Por isso, os bancos de dados não são somente um agrupamento lógico e inter-relacionado do

estado primitivo da informação[152], mas são, também, um ferramental que deve criar uma interface[153] para quem o manipula analisar e descobrir informações para tomada de decisões[154].

Tais decisões vão desde a concepção de um bem de consumo (subcapítulo 1.2.1) ao direcionamento da mensagem publicitária (subcapítulo 1.2.2). Possibilita-se, pois, identificar e precisar o perfil do potencial consumidor, seus hábitos e outras "informações necessárias à tomada de decisões táticas e estratégicas"[155]. É o que se convencionou chamar de mineração de dados[156] ou *data mining*[157].

Em conclusão, não se trata somente de dados ou de bancos de dados, mas, necessariamente, da dinâmica de um sistema de informação, que é o que permite a um manancial de fatos (dados) ser estruturado, organizado e gerenciado para produzir um conhecimento que possa ser revertido para tomada de uma decisão (*e.g.*, direcionamento da ação publicitária).

A tecnologia da informação (dos *bits* ao sistema de informação) permitiu agregar e acumular dados que revelam muitas informações sobre nós. É por tal razão que não se poderia prosseguir sem antes tratar daquilo que pode ser tido como o êxtase e o estado da arte dessa matéria: *Big Data*.

1.3.2 *Big Data*: o êxtase e o estado da arte da mineração dos dados

Com base no que já foi mencionado sobre o progresso quantitativo e qualitativo da gestão da informação (vide subcapítulo 1.1.1), seria possível dizer que o *Big Data* representa o êxtase desse processo. Essa tecnologia permite que um volume descomunal de dados seja estruturado e analisado para uma gama indeterminada de finalidades.

Com base na abordagem de Doug Laney[158], o *Big Data* é comumente associado a 3 (três) "Vs": volume, velocidade e variedade[159]. Volume e variedade, porque ele excede a capacidade das tecnologias "tradicionais" de processamento[160], conseguindo organizar quantidades antes inimagináveis – dos *bits* aos *yottabytes*[161] – e em diversos formatos – *e.g.*, textos, fotos etc. – e, tudo isso, em alta velocidade.

Tal evolução poderia ser imputada a uma diferença crucial entre o *Big Data* e as outras metodologias comuns de processamento de dados (vide subcapítulo 1.3.1), que é o fato da prescindibilidade de os dados estarem previamente estruturados para o seu tratamento[162].

É desnecessário relacionar os dados em entidades e atributos para minerá-los[163]. Há um novo tipo de linguagem para o *Big Data*, que é o NoSQL (*not only structured query language*) em comparação ao SQL[164] (*structured query language*)[165].

A eliminação dessa etapa de estruturação dos dados é o que agrega os três mencionados "Vs" ao *Big Data*. Isso porque tal etapa onera e demanda maiores esforços por parte de quem manuseia uma base de dados. Na medida em que se aumenta o volume, aumenta-se o tempo para estruturar os dados. Da mesma forma, na medida em que se aumentam os tipos (variedade) de dados, demanda-se mais tempo para organizá-los. Diz respeito, enfim, a uma cadeia de fatores interligados que se influenciam reciprocamente, ante a necessidade da etapa prévia de estruturação dos dados, que é

descartada pelo *Big Data*.

Por isso, os dados passaram a ser analisados não mais em pequenas quantidades ou por amostras, mas em toda a sua extensão. Há um salto quanto ao volume de dados processados[166], tornando-se possível correlacionar uma série de fatos (dados), estabelecendo-se entre eles relações para desvendar *padrões* e, por conseguinte, inferir, inclusive, *probabilidades* de acontecimentos futuros.

Por esse motivo, o *Big Data* não é um sistema inteligente. Não se trata de ensinar o computador a pensar como um ser humano, trata-se apenas de uma nova metodologia para que tal ferramental processe e organize dados para inferir a (re)ocorrência de acontecimentos[167].

Torna-se possível, por exemplo, inferir a probabilidade de que uma consumidora esteja grávida, verificando-se que uma determinada lista de produtos é recorrentemente adquirida por tal tipo de cliente. É por meio dessa (cor)relação estabelecida entre fatos que se revela um padrão, ou seja, a recorrência de um evento que permite prever[168] que eles se repetirão no futuro[169].

Em conclusão, *Big Data* não se preocupa com a *causalidade* de um evento, mas, tão somente, com a probabilidade de sua ocorrência. Em vez de questionar por que algo acontece, procura-se diagnosticar o que está acontecendo[170]. Não se está preocupado com a análise das razões que geram uma cadeia de eventos, mas, tão somente, com o seu desencadeamento[171].

1.3.3 Um admirável mundo novo de inferências: da consumidora grávida à iminência do rompimento de um relacionamento afetivo

Um dos exemplos mais citados para ilustrar *Big Data* é o da ação por parte da varejista americana Target para identificar consumidoras grávidas. A gravidez é uma fase da vida na qual tais consumidoras consomem uma infinidade de produtos[172], sendo, por isso, tal informação estratégica.

A equipe de análise da Target conseguiu verificar que tal perfil de consumidoras adquiria uma determinada lista de produtos. Isso permitiu não só prever o estado de gravidez, mas, também, o período de gestação para, daí, lhes direcionar produtos de acordo com a respectiva fase da gravidez[173].

Dessa forma, os algoritmos[174] dos bancos de dados foram programados para estabelecer tal correlação, segmentando, dentre as milhares de consumidoras, aquelas com tal perfil para fins de ação publicitária.

A eficiência da tecnologia em questão foi comprovada quando um pai furioso entrou no estabelecimento comercial de tal empresa, acusando-a de incentivar a sua filha adolescente a engravidar. Passados alguns dias, o gerente da loja, preocupado em perder o cliente, ligou para o furioso pai. Este último, acanhado do outro lado da linha, informou que tinha tomado conhecimento de fatos até então ignorados: a sua filha estava grávida, desculpando-se pelo ocorrido[175].

Sob essa perspectiva, milhares de bases de dados são criadas e, por vezes, agregadas a outras para identificar uma série de padrões de comportamentos e inferir a sua recorrência no futuro, tais como: **i)** um provável surto de gripe, com base nos termos agregados de pesquisa de um buscador[176];

ii) o risco de um tomador de crédito ser inadimplente para calibrar a taxa de juros[177]; **iii)** segurados que tendem a ter maiores riscos de problemas de saúde para daí aumentar o pagamento do prêmio[178].

Uma mesma base de dados pode servir para uma gama de finalidades, podendo ser *reutilizada*[179] para inferir uma série de prováveis acontecimentos e padrões de comportamentos. Deve-se, apenas, *redefinir* o algoritmo para novos usos e correlações[180]. Ela é, portanto, *flexível* para as mais diversas finalidades.

Chegou-se ao ponto de o *Big Data* prever até mesmo crises financeiras[181]. E, ainda, da rede social mais popular do mundo ser capaz de prever quando haverá o rompimento de "um relacionamento sério", com base nos *posts* dos seus usuários[182].

Cada vez mais, os dados dos cidadãos, dispersos na rede, dizem mais sobre eles e quem os manipula sabe até mais sobre eles mesmos. Essa capacidade de identificar os mais diversos padrões de comportamentos e prever a sua recorrência no futuro é uma verdadeira "mina de ouro" para a abordagem publicitária.

Por isso, *Big Data* revolucionou a indústria publicitária[183], criando-se mais do que um rico retrato do consumidor em potencial. A figura translúcida do consumidor de vidro (vide subcapítulo 1.2.2.2) agora perpassa seus passos futuros.

Esclarecida a dinâmica dos bancos de dados, em especial da tecnologia *Big Data*, cabe enfrentar, ainda, uma última questão: a suposta diferença entre bancos de dados e cadastros de consumo – espécies do gênero arquivos de consumo –, questionando-se a utilidade de tal taxonomia.

1.3.4 Bancos de dados e cadastros de consumo: a "promiscuidade" gerada pela economia da informação

Quando se lê o título da Seção VI[184], Capítulo V[185], do Código de Defesa do Consumidor/CDC, é possível afirmar que banco de dados e cadastro de consumo não são figuras equivalentes[186]. Tais termos foram separados pela conjunção aditiva "e" para nomear tal seção, razão pela qual a doutrina passou a tratá-los como espécies do gênero arquivos de consumo[187].

Segundo Antonio Herman Benjamim, coautor do anteprojeto dessa parte específica do CDC, há características que diferenciam bancos de dados de cadastros de consumo.

A primeira é relativa a um aspecto objetivo, o modo pelo qual os dados são coletados. Disso deriva uma segunda característica, de ordem subjetiva, que é quem titulariza tais arquivos de consumo.

Os dados de um cadastro de consumo seriam coletados por quem mantém uma relação comercial com o consumidor, sendo a sua utilização voltada aos interesses do próprio arquivista-fornecedor[188] (por exemplo, os dados cadastrais do cliente para o envio de "malas diretas"), enquanto as informações dos bancos de dados seriam resultado de uma coleta aleatória[189] realizada por terceiros, os quais não mantêm uma relação comercial com o consumidor (por exemplo, as bases de dados dos órgãos de proteção ao crédito).

O terceiro elemento é a transmissibilidade. Quem mantém um banco de dados necessariamente compartilha as suas informações com terceiros (*transmissibilidade extrínseca*). Esse é o caso, por exemplo, dos órgãos de proteção ao crédito, cuja base de dados é acessada por vários atores para fins de análise de crédito. Ao passo que os dados de um cadastro de consumo circulariam apenas em benefício do próprio arquivista e não de terceiros – transmissibilidade intrínseca[190] (por exemplo, os dados dos seus clientes para o envio de correspondência publicitária).

A quarta característica é temporal. A princípio, não faria sentido os cadastros de consumo terem informações armazenadas sobre um cliente que não mais transaciona com o seu arquivista[191]. Por outro lado, os bancos de dados deveriam armazenar permanentemente informações sobre um indivíduo, a fim de viabilizar os mais diversos tipos de consultas por terceiros[192].

A quinta e última característica é relativa à existência e inexistência de autorização do consumidor. Os bancos de dados seriam compostos por informações que não contam com a autorização do seu titular. Por exemplo, os órgãos de proteção ao crédito que, à revelia do consumidor inadimplente, agregam informações sobre seus débitos. Ao passo que no cadastro de consumo há a necessidade da autorização do consumidor, o que, na maioria das vezes, seria coletada no momento da transação comercial entre arquivista e consumidor[193].

Todo esse esforço para diferenciar bancos de dados e cadastros de consumo deriva de uma construção doutrinária, pois, em que pese o título da Seção VI do Código de Defesa do Consumidor enunciar uma possível diferenciação, não se explicitou nos seus artigos correspondentes quais seriam esses elementos de diferenciação[194].

A racional do legislador foi alcançar todas as informações de consumo[195]. Seja qual fosse a espécie do gênero arquivos de consumo, bancos de dados ou cadastros de consumo, elas estariam endereçadas pelo regime jurídico da legislação consumerista.

Contudo, tal taxonomia deixa de fazer sentido na sociedade da informação. Nela, o fluxo de informações é constante, o que acaba por desbancar todos os elementos acima listados que diferenciariam bancos de dados de cadastros de consumo.

Diluiu-se completamente a característica da transmissibilidade (intrínseca) restrita dos cadastros de consumo em comparação à transmissibilidade (extrínseca) mais abrangente dos bancos de dados. Esta última tornou-se praticamente a regra.

A ideia de *prosumer* aponta nessa direção. As opiniões dos consumidores circulam entre vários atores para que a concepção de novos produtos e serviços reflita a tendência do seu público-alvo. Os dados são coletados nas redes sociais, na própria base de dados do fornecedor e de inúmeras outras fontes. Varia-se, apenas, quem os coleta, se o próprio "arquivista" ou terceiros.

Há, ainda, uma complexa rede de atores que circula e compartilha um volume exponencial de dados para tornar mais preciso o perfil do destinatário da mensagem publicitária.

A coleta de dados é, portanto, quase que constantemente, o que fragiliza a diferenciação quanto a uma coleta aleatória ou específica. É nesse contexto que se insere a figura dos *data brokers*[196], que

acumulam e agregam o maior volume possível de dados para fornecer diferentes serviços e produtos, cuja base de sustentação são as informações pessoais dos consumidores.

Ainda, houve um progresso tecnológico que reduziu significativamente os custos para o armazenamento da informação (vide subcapítulo 1.1.1)[197]. Nesse sentido, a diferença de uma base de dados de organização permanente e de um cadastro de consumo de organização temporária também se diluiu.

Por fim, registra-se que a própria ciência da informática não estabeleceu tal taxonomia. Os bancos de dados englobam o conceito de cadastros de consumo. Eles servem tanto para beneficiar decisões do próprio detentor da base de dados – "arquivista" –, como, também, de terceiros (vide subcapítulo 1.3.1).

Talvez fizesse sentido estabelecer tal diferenciação à época da projeção da legislação consumerista, quando os bancos de dados manuais ainda eram os protagonistas – as "fichas de consumo". Atualmente, devido ao seu processo de automatização, uma mesma base de dados tende a acumular, ao mesmo tempo, características de um banco de dados e de um cadastro de consumo[198], havendo uma "promiscuidade" entre tais espécies de arquivos de consumo. Essa ambivalência desnatura tal taxonomia construída pela doutrina consumerista.

Por exemplo, inúmeros fornecedores coletam dados para melhorar o seu próprio serviço ou produto (uma função do cadastro de consumo), mas, também, compartilham tais dados com terceiros, para que direcionem anúncios publicitários (uma característica dos bancos de dados).

Por isso, este trabalho utilizará o termo banco de dados de forma ampla. Essa opção não se afasta do racional do legislador consumerista, já que se faz o uso de tal terminologia de maneira cambiante com cadastro de consumo, englobando, em última análise, todas as situações que se enquadrariam no gênero arquivos de consumo.

1.4 CONCLUSÃO: A FORMATAÇÃO DE UMA ECONOMIA DE VIGILÂNCIA E DE UM VAREJO DOS DADOS PESSOAIS

A incursão realizada neste capítulo inaugural consistiu em um diagnóstico da alocação dos dados pessoais como um ativo econômico. Foi o avanço da tecnologia, propulsor de um salto quantitativo e qualitativo no processamento da informação, que permitiu a introjeção desses dados como um fator crítico da atividade empresarial – a *virtualização* da informação (subcapítulo 1.1).

A começar pelo modelo organizacional das empresas em rede, que permitiu uma flexibilização no processo de produção, a ponto de sincronizar a projeção do bem de consumo instantaneamente às reações do mercado consumidor. Esse sujeito final da cadeia passou a participar mais ativamente durante todo o ciclo de vida de um bem de consumo. Houve a fusão dos atos de consumir

(*consumption*) e de produzir (*production*) na figura do *prosumer* (subcapítulo 1.2.1).

Os dados pessoais dos consumidores revelaram-se igualmente como um elemento crítico para a promoção dos bens de consumo. O caráter estandardizado da abordagem publicitária sofreu um processo de mitigação, pelo qual a publicidade pôde ser direcionada, especialmente no ambiente *on-line*, com base nas preferências do sujeito final da cadeia (subcapítulo 1.2.2.1). E, com o avanço tecnológico, permitiu-se a criação de perfis cada vez mais intrusivos sobre o potencial consumidor (subcapítulo 1.3), monitorando-se constantemente o seu comportamento, a ponto de inferir, até mesmo, o seu estado emocional para correlacioná-lo à mensagem publicitária (subcapítulo 1.2.2.2).

A essa altura, a publicidade já se apresentava como algo altamente rentável que viria a conduzir uma nova estratégia comercial. As receitas publicitárias consolidaram um novo modelo de negócio – *zero-price advertisement business model*. O consumidor não paga diretamente por um bem de consumo mediante uma prestação pecuniária (*zero-price*). A contraprestação consiste no fornecimento de seus dados pessoais para a entrega de publicidade direcionada (*advertisement business model*), fechando a equação econômica dos serviços e produtos "gratuitos" (subcapítulo 1.2.2.3). Essa *monetização* dos dados pessoais formatou uma nova economia.

Uma economia que tem como cerne a *vigilância*[199]. É a observação permanente do comportamento dos indivíduos que a movimenta, sendo as suas informações pessoais a matéria-prima a ser explorada para a geração de riqueza. Mais do que isso, há um "varejo dos dados pessoais"[200]. Para a operacionalização desse modelo de negócio, há uma complexa rede de atores que transaciona as informações pessoais dos consumidores, agindo cooperativamente para agregar mais e mais dados e, em última análise, tornar a mensagem publicitária ainda mais eficiente.

Qualquer perspectiva regulatória para a proteção dos dados pessoais deve levar em consideração o quadro acima descrito, a existência de uma "economia de vigilância"[201]. Tal diagnóstico deságua em estratégias regulatórias complementares que são, por um lado, o empoderamento do indivíduo para exercer um controle significativo sobre seus dados pessoais, e, por outro lado, a consideração de que o próprio fluxo das informações pessoais não se deve submeter, tão somente, à lógica desses interesses econômicos em jogo[202]. Este trabalho pretende ensaiar normativamente uma conciliação entre tais questões.

[1] Esta expressão é utilizada por: SILVA, Daniel Pereira Militão. *Desafios do ensino jurídico na pó modernidade: da sociedade agrícola e industrial para a sociedade da informação*. Dissertação (Mestrado) – Faculdade de Direito da Pontifícia Universidade Católica de São Paulo. São Paulo 2009. p.43.

[2] Ibidem, p.57.

[3] MURRAY, Andrew. *Information, Technology Law*. New York: Oxford University Press, 2010. p "Post-industrial economics emerged in the UK immediately after World War II. With the cost of production of traditional industrial products such as shipbuilding and steel production being cheaper offshore, the UK's industrial capital began to move to places such as India, Malaysia, and Hong Kong. The UK economy started the painful transition from industrial values of 'what can we produce?' to the newly developing service sector and the question 'what can we provide?' With a massive growth in professional services such as banking, insurance, legal services, education, and media, the UK became the archetypal post-industrial or service economy". No mesmo sentido: LEMOS, Cristina. Inovação na era do conhecimento. In: LASTRES, Helena M. M.; ALBAGAJI, Sarita (Org.). *Informação e globalização na era do conhecimento*. Rio de Janeiro: Campus, 1999. p.128.

[4] CASTELLS, Manuel. *A sociedade em rede*. 3.ed. São Paulo: Paz e Terra, 2000. (A era da informação: economia, sociedade e cultura, 1): "Assim, no modo agrário de desenvolvimento, a fonte do incremento de excedente resulta dos aumentos quantitativos da mão de obra e dos recursos naturais (em particular a terra) no processo produtivo, bem como da dotação natural desses recursos. No modo de desenvolvimento industrial, a principal fonte e produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo dos processos produtivo e circulação. *No novo modo informacional de desenvolvimento, a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos*" (grifos). Nesse mesmo sentido, SIQUEIRA JR., Paulo Hamilton. *Teoria do direito*. São Paulo: Saraiva, 2009. p.218: "A 'sociedade da informação' tem como principal valor a informação, o conhecimento. Na era agrícola, a terra se configurava como o fator primordial da geração de riquezas. Na era industrial a riqueza surge da máquina a vapor e da eletricidade. *Na era do conhecimento, a informação e o conhecimento são os atores centrais da produção econômica*" (grifos).

[5] MELODY, William H. Markets and policies in new knowledge economies. In: MANSEL, Robin et al. (Org.). *The Oxford handbook of information and communication technologies*. New York: Oxford University Press, 2007. p.59: "In an agricultural economy, land is the most valuable resource attracting investment capital. In an industrial economy, manufacturing plants, machinery,

and other forms of physical capital are the focal points of investment activity. *In the evolving knowledge economy, the expectation is that skilled and well-trained people, and the information and communication tolls they use, will be central resource attracting investment because knowledge or produced, stored, and applied primarily by humans*" (grifos).

[6] PAESANI, Liliana Minardi (Coord.).*O direito na sociedade da informação*. São Paulo: Atlas, 2007. p.XI (Apresentação): "Vive-se hoje a era da mais importante revolução tecnológica jamais antes experimentada. Revolução pós-industrial, de dimensão planetária. *Novo poder foi criado, o poder tecnológico, que encurta distâncias de tempo e espaço*. São enormes e diferentes as consequências que produz sobre as concepções a respeito das relações entre território, política, economia e cultura e atinge áreas geográficas mais extensas e maior quantidade de pessoas" (grifos).

[7] Ibidem, p.XI: "*Essa revolução produziu o encolhimento do mundo pelo encurtamento do tempo. Assim, o mundo aparece como uma entidade menor, mais integrada e ao mesmo tempo, paradoxalmente, mais fragmentada*. A velocidade e a simultaneidade, produzidas pelo desenvolvimento das indústrias de transporte, de comunicação e informática, são as responsáveis pelo encolhimento do mundo, por meio da compreensão do espaço-tempo" (grifos).

[8] Faz-se referência às manifestações erigidas inicialmente em São Paulo e no Rio de Janeiro contra aumento da tarifa de ônibus, cujo ponto alto deu-se no dia 13 de junho de 2013 – marco que nomina tais protestos – com uma repressão policial violenta contra os manifestantes. A partir de então, tais protestos se expandiram por todo o território nacional com uma série de reivindicações sociais que extrapolavam os 20 (vinte) centavos relativos ao aumento da tarifa. Veja-se, nesse sentido, a historiografia dos protestos por: JUDENSNAIDER, Elena; LIMA Luciana; ORTELLADO, Pablo; POMAR, Marcelo.*Vinte centavos*: a luta contra o aumento. São Paulo: Veneta, 2013.

[9] A sociedade da informação abrange todo e qualquer tipo de acesso facilitado à informação, tal co *fax*. Nesse sentido: LISBOA, Roberto Senise. O consumidor na sociedade da informação. *Revista de Direito do Consumidor*, ano 16, n.61, p.214-215, jan.-mar. 2007. Nesse mesmo sentido, considerando que a transição para a sociedade da informação iniciou-se muito antes do advento do computador, notadamente com o telégrafo elétrico: AMARAL, João Ferreira do. *Economia da informação e do conhecimento*. Coimbra: Almedina, 2009. p.88: "Este é sem dúvida um dos principais factores do progresso da Humanidade e tem ajudado de forma crescente o desenvolvimento econômico desde o século XIX a partir, fundamentalmente da invenção fundamental que foi o telégrafo elétrico".

[10] BARRETO JÚNIOR, Irineu. Atualidades no conceito da sociedade da informação. In: PAESANI Liliana Minardi (Coord.). *O direito na sociedade da informação*. São Paulo: Atlas, 2007. p.69: "O Direito é fato social. Tomando-se como pressuposto o clássico conceito formulado por Émile

Durkheim, o fenômeno jurídico é resultado da realidade social, emanando desta por meio dos instrumentos e instituições destinados a formular o Direito e que refletem a realidade social, sua conformação e os processos de interação e inter-relacionamentos sociais".

[11] MARQUES, Garcia; MARTINS, Lourenço. *Direito da informática*. Coimbra: Almedina, 2006. p.36.

[12] HOUAISS, Antônio; VILLAR, Mauro de Salles. *Dicionário Houaiss da língua portuguesa*. Rio d Janeiro: Objetiva, 2009. p.216: "para os pensadores do atomismo, cada uma das partículas minúsculas, eternas e indivisíveis, que se combinam e desagregam movidas por forças mecânicas da natureza, determinando desta maneira as características de cada objeto".

[13] Ibidem, p.296: "dígito binário. 1. menor parcela de informação processada por um computador. 2. algarismo do sistema binário que somente pode assumir as formas de 0 ou 1".

[14] "*Bit* também é conceituado como a menor unidade de 'informação' armazenável. Porém o bit (0 ou 1), apesar de ser um dado (fato não processado) não pode ser confundido como a menor 'unidade de medida da informação', pois representa apenas valores que, somente em conjunto (octeto ou byte), formarão a informação em si, que é o produto do processamento desse conjunto de dados. Cabe salientar que o bit é usado como unidade de medida sim, mas em transmissão de dados de forma serial. Em comunicação de dados apenas a definição métrica de um kilobyte (1.000 bytes por kilobyte) está correta. A definição binária de um kilobyte (1.024 bytes por kilobyte) é usada em áreas como armazenamento de dados (disco rígido, memória), mas não para expressar a largura de banda e taxa de transferência". Conceito tirado do site Wikipédia. Disponível em: <http://pt.wikipedia.org/wiki/Bit>.

[15] MURRAY, Andrew. Op.cit., p.6: "At the most basic level therefore a bit is simply a 0 or 1, but lik atoms, which on their own are not very impressive either, it is how bits can be used to constructed larger, more complex systems that gives them their economic value and social importance. In the world of computer systems a bit represent a single instruction to the computer. This instruction is either to do (1) or not do (0) a particular function. The instruction is ready by the brain of the computer, the Microprocessor or Central Processing Unit (CPU). The CPU ma be thought of as a superfast calculator which works in binary. Bits of information are fed to the CPU from the computer memory, the CPU does a calculation and based upon the result the personal computer (or PC) carries out a predetermined function".

[16] NEGROPONTE, Nicholas. *A vida digital*. Trad. Sérgio Tellaroli. Supervisão técnica Ricardo Rangel. São Paulo: Companhia das Letras, 1995. p.19: "Os bits sempre foram a partícula subjacente à computação digital, mas, ao longo dos últimos 25 anos, expandimos bastante nosso vocabulário binário, nele incluindo muito mais do que apenas números. *Temos sido capazes de digitalizar diferentes tipos de informação, como áudio e vídeo, reduzindo-os também a uns e zeros*" (grifos).

[17] Tal processo teria se iniciado com a invenção do microprocessador *Intel*, dizendo-se que ele teria sido o *big bang* dessa explosão no processamento de informações: FREEMAN, Chris. Th ICT paradigm. In: MANSEL, Robin et al. (Org.)*The Oxford handbook of information and communication technologies*. New York: Oxford University Press, 2007. p.38. "(...) but frequently in the past history of paradigm change one particular event had been especially significant, designated by her as a 'big bang'. For the ICT paradigm this big bang was the Intel microprocessor".

[18] Teria sido a transição de átomos para bits que concretizou a chamada vida digital. NEGROPONT Nicholas. Op.cit., p.10 e 77.

[19] MURRAY, Andrew. Op.cit., p.36: "The development of information technology allows for a singl record which can be accessed by all careers contemporaneously and which may, instantly, be searched by any keyword".

[20] LÈVY, Pierre. *Cibercultura*. Trad. Carlos Irineu da Costa. São Paulo: Editora 34, 2011. p.54: "A informação digitalizada pode ser processada automaticamente, com grau de precisão quase absoluto, muito rapidamente e em escala quantitativa. Nenhum outro processo a não ser o processamento digital reúne, ao mesmo tempo, essas quatro qualidades. A digitalização permite o controle das informações das mensagens 'bit a bit', número binário a número binário, e isso na velocidade de cálculo de computadores".

[21] Como constará, mais à frente, a menção à virtualização não tem a semântica comum de ser oposto ao que é real.

[22] LASTRES, Helena Maria Martins; FERRAZ, João Carlos. Economia da Informação, conhecimento e do aprendizado. In: LASTRES, Helena M. M.; ALBAGAJI, Sarita (Org *Informação e globalização na era do conhecimento*. Rio de Janeiro: Campus, 1999. p.33.

[23] Ibidem, p.31.

[24] LISBOA, Roberto Senise. Direito na sociedade da informação*Revista dos Tribunais*, ano 95, v.847, p.78, maio 2007.

[25] DRUCKER, Peter. *A sociedade pós-capitalista*. Trad. Nivaldo Montigelli Jr. São Paulo: Pioneira 1993. p.15-20.

[26] CASTELLS, Manuel. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade Tradução Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003. p.58: "entendo por isso a forma organizacional construída em torno de projetos de empresas que resultam da cooperação entre diferentes componentes de diferentes firmas, que se interconectam no tempo de duração de dado projeto empresarial, reconfigurando suas redes para a implementação de um projeto".

[27] CASTELLS, Manuel. *A sociedade*... cit., p.220-233.

[28] KOSKINS, Tasny.*Luxury brands*: higher standards or just a higher mark-up? Disponível em:

<https://www.theguardian.com/sustainable-business/2014/dec/10/luxury-brands-behind-gloss-same-dirt-ethics-production>.

[29] DANTAS, Marcos. Capitalismo na era das redes. In: LASTRES, Helena M. M.; ALBAGAJI, Sari (Org.). *Informação e globalização na era do conhecimento*. Rio de Janeiro: Campus, 1999. p.220: "Em suma, executivos, analistas de mercados, estilistas, desenhistas, fotógrafos, engenheiros de computação, economistas, muitos outros técnicos da Benetton, trabalham obtendo informação, processando informação, registrando informação e comunicando informação".

[30] CASTELLS, Manuel. *A galáxia*... cit., p.64.

[31] Ibidem, p.62.

[32] DANTAS, Marcos. Capitalismo... cit., p.225.

[33] BOULDING, K. E. The economics of knowledge and the knowledge of economics. In: LAMBERTON, D. M. (Ed.)*Economics of information and knowledge, selected readings*. Baltimore: Penguin Books, 1971. p.29.

[34] MELODY, William H. Op.cit., p.59: "One important distinction between the industrial economy and the evolving new knowledge economy is the shift in emphasis from a primary focus on the transformation of material resources, that is, the physical production of goods, to a focus on improving and facilitating transaction capabilities, that is, generating and communicating information to facilitate exchange transactions".

[35] LISBOA, O Direito... cit., p.85.

[36] LÉVY, Pierre. *O que é virtual*. Trad. Paulo Neves. São Paulo: Editora 34, 2011. p.47: "Enfim, e sobretudo, um computador ramificado no hiperespaço pode recorrer às capacidades de memória e de cálculo de outros computadores da rede (que, por sua vez, fazem o mesmo), bem como a diversos aparelhos distantes de captura e de apresentação de informação. Todas as funções da informática (captura, digitalização, memória, tratamento e apresentação) são distribuíveis e, cada vez mais, distribuídas. *O computador não é um centro, mas um pedaço, um fragmento da trama, um componente incompleto da rede calculadora universal*" (grifos).

[37] LÉVY, Pierre. *O que é*... cit., p.17-18: "Mas o que é a virtualização? Não mais o virtual como maneira de ser, mas a virtualização como dinâmica. *A virtualização pode ser definida como o movimento inverso da atualização*. Consiste em uma passagem do atual ao virtual, em uma 'elevação à potência' da entidade considerada. A virtualização não é uma desrealização (a transformação da realidade num conjunto de possíveis), mas uma mutação de identidade, um deslocamento do centro de gravidade ontológica do objeto considerado: em vez de definir principalmente por sua atualidade (uma solução), a entidade passa a encontrar sua consistência essencial num campo problemático" (grifos).

[38] Ibidem, p.18: "Virtualizar uma entidade qualquer consiste em descobrir uma questão geral à qual ela se relaciona, em fazer mutar a entidade em direção a essa interrogação e em redefinir a

atualidade de partida como resposta a uma questão particular".

39 CASTELLS, Manuel. *A galáxia*... cit., p.57: "O que está surgindo não é uma economia ponto.com, mas uma economia interconectada com um sistema nervoso eletrônico".

40 CASSIOLATO, José Eduardo. A economia do conhecimento e as novas políticas industriais e tecnológicas. In: LASTRES, Helena M. M.; ALBAGAJI, Sarita (Org.). *Informação e globalização na era do conhecimento*. Rio de Janeiro: Campus, 1999. p.175: "As tecnologias de informação e comunicações afetam e influenciam significativamente os processos de aprendizado fundamentais para a organização da informação que é, por sua vez, atividade básica para a geração de conhecimento".

41 BOULDING, K. E. Op.cit., p.24.

42 AMARAL, João Ferreira do. *Economia*... cit., p.116: "O que faz a empresa ganhar dinheiro não é receber a informação em si própria. É transformar essa informação em conhecimento que depois é aplicado. Falta-nos por isso introduzir a questão da transformação da informação em conhecimento".

43 DUCKER, Peter. Op.cit., p.149: "A produtividade do conhecimento será o fator determinante da posição competitiva de uma empresa, de uma indústria, de todo um país. Nenhum país, indústria ou empresa tem uma vantagem ou desvantagem 'natural'. A única vantagem possível é a capacidade para explorar o conhecimento universalmente disponível. A única coisa que será cada vez mais importante, tanto na economia nacional como na internacional, é o desempenho gerencial para tornar produtivo o conhecimento".

44 MELODY, William H. Op.cit., p.66; BOULDING, K. E. Op.cit., p.23. No mesmo sentido DUCKER, Peter. Op.cit., p.21: "Os tradicionais 'fatores de produção' – terra (isto é, recursos naturais), mão de obra e capital – não desaparecem, mas tornaram-se secundários, eles podem ser obtidos facilmente, desde que haja conhecimento. E o conhecimento, neste novo sentido, significa o conhecimento como uma coisa útil, como meio para a obtenção de resultados sociais e econômicos". Em sentido análogo, fala-se em capital-informação: DANTAS, Marcos. *A lógica do capital-informação*: a fragmentação dos monopólios e a monopolização dos fragmentos num mundo de comunicações globais. Rio de Janeiro: Contraponto, 2002. p.144.

45 ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Informatio Civilization. *Journal of Information Technology*, 04 abr. 2015, p.77. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754>.

46 ZUBOFF, Shoshana. Big Other... cit., p.79.

47 Ibidem, p.78.

48 TORRES, Claudio. *A bíblia do marketing digital*: tudo o que você queria saber sobre o marketing e a publicidade na internet e não tinha a quem perguntar. São Paulo: Novatec, 2009. p.22-24.

[49] CHEN, Yubo; XIE, Jinhong. Online consumer review: a new element of marketing communication mix. *Management Science*, v.54, n.3, p.1-43, 2008. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=618782>.

[50] Ibidem, p.6.

[51] MATTOS, Karla Cristina da Costa e Silva. *O valor econômico da informação nas relações de consumo*. São Paulo: Almedina, 2012. p.131-149.

[52] CASTELLS, Manuel. *A sociedade*... cit., p.212: "Sistemas flexíveis de produção em grande volume, geralmente ligados a uma situação de demanda crescente de determinado produto, coordenam grande volume de produção, permitindo economias de escalas e sistemas de produção personalizada reprogramável, captando economias de escopo. As novas tecnologias permitem a transformação das linhas de montagem típicas da grande empresa em unidades de produção de fácil programação que podem atender às variações do mercado (flexibilidade do produto) e das transformações tecnológicas (flexibilidade do processo)".

[53] CHEN, Yubo; XIE, Jinhong. Op.cit., p.33.

[54] CASTELLS, 2003, p.65: "A essência do negócio jurídico está na conexão em rede, interativa baseada na internet, entre produtores, consumidores e prestadores de serviços. Aqui mais uma vez, a rede é a mensagem. É a capacidade de interagir, recuperar e distribuir globalmente, de maneira personalizada, que está na fonte da redução do custo, da qualidade, eficiência e satisfação do comprador – a menos que a administração da complexidade derrube o sistema, como tantas as vezes acontece, indignando os consumidores que compreendem que, provavelmente, são as cobaias desse novo modelo de empresa".

[55] TORRES, Claudio. Op.cit., p.24: "Novas tecnologias e aplicações, como os blogs, as ferramentas de busca, os fóruns, as redes sociais e tantas outras aplicações on-line foram utilizadas pelos internautas para, literalmente, assumir o controle, a produção e o consumo da informação, atividades antes restritas aos grandes portais".

[56] LISBOA, Roberto Senise. Prefácio. In: MATTOS, Karla Cristina da Costa e Silva. *O valor econômico da informação nas relações de consumo*. São Paulo: Almedina, 2012. p.16: "O acesso à informação, como direito fundamental e direito básico dos consumidores, transforma-os em *prosumers*, ou seja, participantes ativos na própria confecção, distribuição, aquisição e descarte de produtos e serviços colocados no mercado pelos fornecedores".

[57] Por isso fala-se em marketing digital, que é redimensionado por todo esse fluxo informacional próprio do meio digital. TORRES, Claudio. Op.cit., p.45.

[58] MATTOS, Karla. Op.cit., p.149.

[59] Nesse sentido: FERNANDES NETO, Guilherme. *Direito da comunicação social*. São Paulo: Revista dos Tribunais, 2004. p.118-124; MARQUES, Cláudia Lima. *Contratos no Código de*

Defesa do Consumidor: o novo regime das relações contratuais. São Paulo: Revista dos Tribunais, 2011. p.829; ROCHA, Sílvio Luís Ferreira. O controle da publicidade no CDC. In MORATO, Antonio Carlos; NERI, Paulo de Tarso (Org.)*20 anos do Código de Defesa do Consumidor*: estudos em homenagem ao professor José Geraldo Brito. São Paulo: Atlas, 2010 p.177; JACOBINA, Paulo Vasconcelos *Publicidade no direito do consumidor*. Rio de Janeiro: Forense, 1996. p.15.

60 MARQUES, *Contratos*... cit., p.70. No mesmo sentido: LIMA, Cíntia Rosa Pereira de. *Validade e obrigatoriedade dos contratos de adesão eletrônicos (*shrink-wrap *e* click-wrap*) e dos termos e condições de uso (*browse-wrap*): um estudo comparado entre Brasil e Canadá.* Tese (Doutorado) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2009. p.70.

61 BRAUDRILLARD, Jean. *A sociedade de consumo*. Lisboa: Edições 70, 2011. p.161: "Em tal sentido, a publicidade revela-se talvez como o mais notável meio de comunicação de massas da nossa época. Assim como, ao falar de qualquer objecto, os glorifica virtualmente a todos, referindo-se à totalidade dos objectos e ao universo totalizado pelos objectos e pela marca em virtude da menção de tal objecto ou de tal marca – assim também, por meio de cada consumidor, se dirige a todos os consumidores e vice-versa, fingindo uma totalidade consumidora (...)".

62 PICKER, Randal C. Online advertising, identity and privacy. *Chicago Law & Economics, working papers series*. The Law School of University of Chicago, p.20, June 2009. Disponível em <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1428065>.

63 FISHER, Luciana. Revista propaganda: a publicitária na mídia segmentada (um estudo de caso). In XIV CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO. Campo Grande, Disponível em: <http://www.portcom.intercom.org.br/pdfs/147689473119175129741594975834332170614.pdf> Nesse mesmo sentido, diferenciando publicidade contextual de publicidade comportamental *on-line*: STRANDBURG, Katherine J. Free Fall: The Online Market's Consumer Preference Disconnect. *NYU School of Law, Public Law Research Paper* n.13-62, p.97, Oct. 2013. Disponível em: <http://ssrn.com/abstract=232396>.

64 "A Comunicação Segmentada é um desdobramento do modelo de Comunicação de Massa. Ela ocorre pelos meios de comunicação tradicionais como jornais, rádios, TVs, cinema, cartazes ou internet, porém, diferentemente do modelo de massa, atinge grupos específicos, classificados de acordo com características próprias e preferências similares. A Comunicação Segmentada tem a particularidade de atingir um número menor, porém mais específico, de receptores ao mesmo tempo, partindo de um único emissor". Disponível em: <http://pt.wikipedia.org/wiki/Comunica%C3%A7%C3%A3o_segmentada>.

65 Em sentido análogo, pontuando as diferenças entre publicidade comportamental *on-line*, contextual e segmentada: ARTICLE 29, Data Protection Working Party. *Opinion 02/2010 sobre publicidade*

comportamental em linha. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pt.pdf>.

[66] Reconhece-se que a classificação exposta é equívoca, havendo quem trate na mesma espécie a publicidade segmentada e a comportamental, fazendo uso da terminologia "segmentação comportamental". BORGESIUS, Frederick Zuiderveen. Segmentação comportamental*Do not track* e o desenvolvimento jurídico europeu e holandês. *Revista Politics*: publicação do Núcleo de Pesquisas e Estudo de Formação (Nupef), n.14, p.9, fev.2013.

[67] *Faturamento do e-commerce deve crescer 12% e atingir quase R$ 50 bilhões em 2017*. Disponível em: <http://www.fecomercio.com.br/noticia/faturamento-do-e-commerce-deve-crescer-12-e-atingir-quase-r-50-bilhoes-em-2017>.

[68] Em capítulo próprio serão abordadas especificamente as mais diversas técnicas de rastreamento d comportamento do usuário na internet para fins de reavaliar a autodeterminação informacional, tecendo breves considerações sobre *flash cookies*, *e'tags*, *HTML5*, *evercookie* (subcapítulo 4.1.3.2).

[69] "Trata-se de programas de dados gerados com o objetivo principal de identificação do usuário, rastreamento e obtenção de dados úteis a seu respeito, especialmente, baseada em dados de navegação e de consumo. Tais fichários de dados, normalmente utilizados pelos provedores de Internet, são enviados aos navegadores dos usuários, em cujos computadores restam salvos em diretórios específicos" (MARTINS, Guilherme Magalhães.*Responsabilidade por acidente de consumo na Internet*. São Paulo: Revista dos Tribunais, 2008. p.227-228). No mesmo sentido: HOOFNAGLE, Chris Jay; SOLTANI, Ashkan; GOOD, Nathaniel; WAMBACH, Dietri AYENSON, Mika D. Behavioral advertising: the offer you cannot refuse.*Harvard Law & Policy Review*, v.6, p.276, 2012; ANTONIALLI, Dennys Marcelo. Watch your steps: an empirical stud of the use of online tracking technologies in different regulatory regimes. *Stanford Journal of Civil Rights & Civil Liberties*, p.329, Aug. 2012.

[70] BAROCAS, Solon; NISSENBAUM, Helen. On Notice: The Trouble with Notice and Consent, p.3 Disponível em: <http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf>.

[71] Federal Trade Commission/FTC. Behavioral Advertising: Tracking, Targeting, and Technology, p.18, 2007. Disponível em: <http://www.ftc.gov/news-events/events-calendar/2007/11/ehavioral-advertising-tracking-targeting-technology>.

[72] PICKER, Randal C. Op.cit., p.4. "That information could arise from any number of sources, but th clickstream that we create as we surf the Internet probably presents unrivaled access to information about us".

[73] EVANS, David D. The economics of the online advertising industry.*Journal of Economic Perspectives*, Apr. 2009, p.42. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1376607>.

[74] PICKER, Randal C. Op.cit., p.18.

[75] Há quem divirja se a publicidade baseada nos termos de busca deva ser enquadrada como uma publicidade comportamental, sustentando-se que seria um *mix* entre esta e a publicidade contextual, uma vez que o próprio contexto do *website* (os resultados da busca) estaria correlacionado com a abordagem publicitária (STRANDBURG, Katherine J. Op.cit., p.7). Es trabalho opta por classificá-la como publicidade comportamental *on-line*, já que o seu traço marcante é, justamente, rastrear o comportamento do usuário, especificamente os seus interesses extraídos pela utilização do buscador.

[76] PICKER, Randal C. Op.cit., p.2: "These cloud-service providers will also have available to them rich datastream that arises from their customer's activities. This combination of identity and an ongoing stream of interactions with remote computers make it possible for service providers to know a great deal about me. My direct revelation of information coupled with information revealed during identified use creates a rich information profile about me or at least about my online identity, my avatar me as it were. (...) The advertising that supports much of the content on the Internet is more valuable if it can be matched to my actual interests, and the flexibility of the web in delivering content means that web advertising is increasingly tailored advertising, or so called behavioral advertising".

[77] EVANS, David D. The online advertising industry: economics, evolution, and privacy. *Journal of Economic Perspectives*, Apr. 2009, p.5. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1376607>.

[78] Veja-se, a título de exemplo, o crescimento em 113% (cento e treze por cento) da venda de *smartphones*, comparando-se o primeiro trimestre do ano de 2012 ao de 2013. Nesse sentido, é a reportagem intitulada: Vendas de *smartphones* têm crescimento espetacular no Brasil. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/8-3-milhoes-de-smartphones-sao-vendidos-no-segundo-trimestre>.

[79] Veja-se a pesquisa *TIC Domicílios* do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) do Núcleo de Informação e Coordenação do Ponto BI (NIC.br) do ano de 2015, quando o "celular ultrapassou o computador como dispositivo mais utilizado para o acesso à Internet". Disponível em: <http://cetic.br/noticia/celular-torna-se-o-principal-dispositivo-de-acesso-a-internet-aponta-cetic-br/>. A pesquisa completa pode ser acessada aqui: <http://cetic.br/pesquisa/domicilios/indicadores>.

[80] "O sistema de posicionamento global (do inglês *global positioning system*, GPS) é um sistema de navegação por satélite que fornece a um aparelho receptor móvel a sua posição, assim como informação horária, sob todas condições atmosféricas, a qualquer momento e em qualquer lugar na Terra, desde que o receptor se encontre no campo de visão de quatro satélites GPS". Disponível em: <http://pt.wikipedia.org/wiki/Sistema_de_posicionamento_global>.

[81] "*Smartphone* (telefone inteligente, numa tradução livre do inglês) é um telemóvel com funcionalidades avançadas que podem ser estendidas por meio de programas executados por seu sistema operacional. (...) Geralmente um s*martphone* possui características mínimas de hardware e software, sendo as principais a capacidade de conexão com redes de dados para acesso à Internet, a capacidade de sincronização dos dados do organizador com um computador pessoal, e uma agenda de contatos que pode utilizar toda a memória disponível do celular – não é limitada a um número fixo de contatos". Disponível em: <http://pt.wikipedia.org/wiki/Smartphone>.

[82] EDWARDS, Lilian; HATCHER, Jordan. Consumer privacy law 2: data collection, profiling ar targeting. In: EDWARDS, Lilian; WAELDE, Charlotte (Coord.)*Law and the internet*. Portland: Har Publishing, 2009. p.516-517: "Collecting*location* data as potentially valuable is a newer concept. A marker for mobile e-commerce ('m-commerce') is developing in which location data is crucial. Location data is typically sold by the telco originally collecting the data to third parties who then in their turn use it to sell services to mobile users on a basis location or proximity, eg taxis, nearest fast foods, weather forecasts (...)".

[83] Sobre o valor da compra, veja a reportagem intitulada: Google confirma a compra da Waze. Disponível em: <http://g1.globo.com/tecnologia/noticia/2013/06/google-confirma-compra-da-waze.htm>.

[84] MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth*Big Data*: A revolution will transform how we live, work and think. New York: Houghton Mifflin Publishing, 2013. p.90.

[85] TURBAN, Efraim; MCLEAN, Ephraim; WETHERBE, James*Tecnologia da informação para gestão*. Trad. Renate Schinke. 3.ed. Porto Alegre: Bookman, 2004. p.413.

[86] BANERJEE, Syagnik; DHOLAKIA, Ruby Roy. Mobile Advertising: Does Location Bas Advertising Work? *International Journal of Mobile Marketing*, Dec. 2008, p.5. Disponível em: <http://ssrn.com/abstract=2135087>.

[87] PAESANI, Liliana Minardi. A publicidade móvel e a vulnerabilidade do consumidor. In MORATO, Antonio Carlos; NERI, Paulo de Tarso (Org.)*20 anos do Código de Defesa do Consumidor*: estudos em homenagem ao professor José Geraldo Brito. São Paulo: Atlas, 2010 p.188.

[88] Nesse sentido é a reportagem intitulada: WhatsApp e aplicativos de mensagens ultrapassam SMS em 2012. Disponível em: <http://tecnologia.terra.com.br/internet/whatsapp-e-aplicativos-de-mensagem-ultrapassam-sms-em-2012,48db5334cc55e310VgnVCM4000009bcceb0aRCRD.html>.

[89] "Forma de comunicação paralinguística, um *emoticon*, palavra derivada da junção dos seguintes termos em inglês: *emotion* (emoção) + *icon* (ícone) (em alguns casos chamado *smiley*) é uma sequência de caracteres tipográficos, tais como: :), ou ^-^ e :-); ou, também, uma imagem (usualmente, pequena), que traduz ou quer transmitir o estado psicológico, emotivo, de quem os

emprega, por meio de ícones ilustrativos de uma expressão facial". Disponível em: <http://pt.wikipedia.org/wiki/Emoticon>.

[90] Esse é caso, por exemplo, da rede social Facebook, que permite ao usuário expressar se está se sentindo animado, cansado, infeliz, feliz etc. Disponível em: <http://pt-br.facebook.com/help/www/427780037309149>.

[91] É o caso, por exemplo, do tweetfeel que monitora as conversas do twitter, catalogando os pensamentos positivos e negativos de seus usuários sobre filmes, músicas etc. *Tweetfeel*. Disponível em: <http://www.tweetfeel.com/faq.php>.

[92] Nesse sentido a reportagem intitulada: Veja *sites* que usam e mapeiam emoções: ao dizer estado sentimental, usuário ganha sugestões de músicas e filmes; serviços também monitoram opiniões. Ódios e amores dos que navegam na Internet são organizados por meio de serviços que rastreiam redes sociais. Disponível em: <http://www1.folha.uol.com.br/fsp/tec/tc0405201117.htm>.

[93] MAYER-SCHONEBERGER, Viktor. *Big*... cit., p.92: "Many businesses parse tweets, sometimes using a technique called sentiment analysis, to garner aggregate customer feedback or judge the impact of marketing campaigns".

[94] Nesse sentido: DEMETRIO, Amanda. São tantas emoções: Empresas e pesquisadores buscam maneiras de captar, usar e interpretar os sentimentos dos usuários que navegam na Internet [sem paginação]. Disponível em: <http://www1.folha.uol.com.br/fsp/tec/tc0405201101.htm>.

[95] Nesse sentido: MOROZOV, Evgeny.*O perigo da publicidade baseada em emoções*. Trad. Paulo Migliacci, sem paginação. Disponível em: <http://www1.folha.uol.com.br/colunas/evgenymorozov/2013/12/1381821-o-perigo-da-publicidade-baseada-em-emocoes.shtml>.

[96] Idem.

[97] Nesse sentido: *O que o chip sensor de movimentos m7 da Apple pode fazer*. Disponível em: <http://www.technologyreview.com.br/printer_friendly_article.aspx?id=43921>.

[98] DEMETRIO, Amanda. Op.cit.

[99] Nesse sentido é a afirmação de Carlos Affonso de Souza no quadro Futuro: modo de usar do jornal Globo News, intitulada: Emoções de usuários são monitoradas na internet. Disponível em: <http://globotv.globo.com/globo-news/jornal-globo-news/v/emocoes-de-usuarios-sao-monitoradas-na-internet/3081499/>.

[100] LACE, Susanne.*The glass consumer*: life in a surveillance society. Bristol: Policy Press, 2005. p.1: "We are all 'glass consumers': others know so much about us, they can almost see through us. Our everyday lives are recorded, analysed and monitored in innumerable ways (...)".

[101] Utilizando-se dos ensinamentos da supracitada autora, tal como tecendo conclusão similar: MENDES, Laura Schertel.*Transparência e privacidade: violação e proteção da informação*

pessoal na sociedade de consumo. Dissertação (Mestrado em Direito) – Faculdade de Direito da Universidade de Brasília. Brasília, 2008. p.81-85.

[102] SEBASTIAN, Kent. No Such Thing as a Free Lunch: Consumer Contracts and "Free Services" *Relatório da Public Interest Advocacy Centre's,* p.6. Disponível em: <http://www.piac.ca/privacy/canadian_consumers_need_more_protection_dealing_with_free_ser

[103] No cenário brasileiro, veja-se a afirmação do conselheiro Fernando de Magalhães Furlan ao analisar a parceria firmada entre as sociedades empresárias "Oi", Telefônica e a Phorm no tocante à publicidade comportamental: "A resposta mais simples é que estão sendo vendidas informação e apresentação. Vende-se a informação sobre o histórico de navegação na Internet dos usuários de banda larga na forma de perfis. E vende-se a apresentação de publicidade a usuários com perfis desejados pelo anunciante. Não se trata de uma venda isolada. No sistema da Phorm, esses dois serviços são vendidos de forma conjunta e inseparável: o anunciante compra a apresentação de publicidade aos usuários que pertençam a um determinado perfil. Nesse contexto, o usuário de banda larga não é o cliente, mas o produto. As provedoras vendem dados do usuário e vendem a apresentação de publicidade a este usuário. O real cliente é o anunciante". MATIUZZO, Marcela. Propaganda Online e privacidade: o varejo de dados pessoais na perspectiva antitruste. p.65 Disponível em: <http://www.seae.fazenda.gov.br/premio-seae/edicoes-anteriores/edicao-2014/tema1-3lugar-MM.pdf>.

[104] ANDERSON, Simon P. Advertising on the internet. In: PEITZ, Martin; WALDFOGEL, Joel (Org.) *The Oxford handbook of the digital economy*. New York: Oxford University Press, 2012. p.364.

[105] STRANDBURG, Katherine J. Op.cit., p.107.

[106] CUSUMANO, Michael A.; GOELDI, Andreas. New Businesses and new business models. I DUTTON, William H. (Org.). *The Oxford handbook of internet studies*. United Kingdon: Oxford University Press, 2012. p.252. Nesse mesmo sentido, foi a intervenção realizada por: ANTONIALLI, Dennys*Estado e cidadão: novos desafios jurídicos para a proteção de dados no Brasil*. Evento realizado pela Faculdade de Direito da Fundação Getulio Vargas, jun.2013 Disponível em: <http://www.youtube.com/watch?v=aPSfG_GhoTo>.

[107] A expressão é de STRANDBURG, Katherine J. Op.cit., p.96.

[108] IAB Europe.*Consumers Driving the Digital Uptake*. The economic value of online advertising-based services for consumers, p.7, Sept. 2010. Disponível em: <http://www.iabeurope.eu/files/7113/7000/0832/white_paper_consumers_driving_the_digital_up (IAB Europe Sept. 2010).

[109] NOVOTNY, Alexander; SPIEKERMANN, Sarah. Personal information markets and privacy: new model to solve the controversy, p.1, Aug. 2012. Disponível em: <http://ssrn.com/abstract=2148885>.

[110] CUSUMANO, Michael A. GOELDI, Andreas. Op.cit., p.251. Nesse mesmo sentido: NELSO

Brett. The "Freemium" Model: top flaws and potent fixes. Disponível em <http://www.forbes.com/sites/brettnelson/2013/07/23/the-freemium-model-top-flaws-and-potent-fixes/>.

111 CUSUMANO, Michael A.; GOELDI, Andreas. Op.cit., p.252.

112 A título de exemplo, o serviço de *cloud computing dropbox* tem a mesma política de privacidade para versão básica e *premium* de tal serviço, não estabelecendo diferenças com relação a tais tipos de usuários. Consulte: Dropbox política de privacidade. Disponível em: <https://www.dropbox.com/privacy#privacy>.

113 Em sentido análogo: STRANDBURG, Katherine J. Op.cit., p.150. "Not only are consumers unable to come up with useful estimates of the expected disutility they are incurring by allowing data collection, but the simple picture of a purchase transaction in which consumer data is exchanged for an information product is also misleading. The bulk of data collection does not occur at the time a consumer first accesses a zero-price online product or service. The online behavioral advertising model is 'buy now, pay later'. Or, more accurately, it is a model that involves payments over time for ongoing access to services".

114 Não raras vezes, percebe-se que mensagens publicitárias "perseguem" os usuários durante a sua navegação e com uma certa longevidade temporal. Veja-se, nesse sentido, a bem-humorada reportagem de que uma determinada sapatilha que perseguiu uma usuária durante 8 meses: Sensacionalista. Polícia apreende sapatilha que perseguia mulher há oito meses na internet. Disponível em: <http://sensacionalista.uol.com.br/2015/03/19/policia-apreende-sapatilha-que-perseguia-mulher-ha-seis-meses-na-internet/>.

115 ARTICLE 29, Data Protection Working Party. Opinion 2/2010... Op.cit., p.19. Disponível em <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf>.

116 No contexto brasileiro, veja-se, a título de exemplificação, a rede social de publicidade Interactiv Advertising Bureau/IAB. Disponível em: <www.iabbrasil.net>.

117 BAROCAS, Solon; NISSENMABUM, Helen. On notice... Op.cit., p.2.

118 Por tal razão, estabelece-se a diferenciação entre *third-party* tracking and *first-party tracking*. O rastreamento executado por terceiro é aquele realizado pela rede social que não mantém uma relação direta com o usuário e, portanto, não pode ser tomado como a primeira parte dessa lógica de rastreamento, que seria a aplicação ou *website* acessado pelo usuário. Nesse sentido, veja-se: GOMEZ, Joshua et al.*Know Privacy*: Report of University of California, Berkeley. p.8. Disponível em: <http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf>.

119 BAROCAS, Solon; NISSENMABUM, Helen. On notice... cit., p.2: "Behavioral targeting ste from the ability to track users across the web as they navigate within and between sites, capturing a consistent flow of information about users' behavior, including their interaction with ads themselves. This requires that a third party (not isolated publishers) be able and allowed to

follow users across sites so as to develop user profiles which can then be subject to various data mining techniques, yielding predictive models that serve as the engine for ad decisioning and targeting systems".

120 Ibidem.

121 Primeiramente, a indústria dos *data brokers* focou no setor financeiro. Com o surgimento da Internet e dos modelos de negócios baseados em publicidade comportamental, expandiu-se o espectro de atuação de tal indústria. Veja-se, entre outros: Federal Trade Commission/FTC. Data brokers: a call for transparency, p.i, May 2014. Disponível em: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

122 Veja, *e.g.*, o *podcast* de: GOULART, Guilherme; SERAFIN, Vinicius. Data Brokers, Privacidade Discriminação. Disponível em: <http://www.segurancalegal.com/2014/06/episodio-52-databrokers-privacidade-e.html>.

123 Federal Trade Commission/FTC. Data brokers... cit., p.11-13.

124 Observa-se que a indústria dos *data brokers* não se limita apenas ao segmento do marketing, atuando, também, para fins de minimização de riscos (verificação de identidades e prevenção de fraudes) e para busca de pessoas (*people search*). Para uma abordagem completa dos produtos dos *data brokers*, veja-se: Federal Trade Commission/FTC. Data brokers... cit., p.23-31. Na literatura brasileira, veja-se o recente estudo de: GOULART, Guilherme Goulart: Por uma visão renovada dos arquivos de consumo. *Revista de Direito do Consumidor*, São Paulo, v.107, p.452: "Os *databrokers* são instituições que coletam e mantêm dados de milhões de pessoas para a realização de análise e empacotamento dos dados, podendo ou não processar informações pessoais. Os serviços são usados para verificação de identidade, diferenciação de registros (homônimos, por exemplo), oferecimento de serviços de marketing e prevenção de fraudes. Em geral, as atividades são realizadas sem a permissão e o conhecimento do usuário, o que representa uma flagrante violação da boa-fé e também do princípio da transparência das relações de consumo".

125 Federal Trade Commission/FTC. Data brokers... cit., p.18.

126 No contexto brasileiro, toma-se como exemplo a Serasa Experian que, com o produto Mosaic Brasil, divide os brasileiros em: a) elites brasileiras; b) experientes urbanos com vida confortável; c) juventude trabalhadora urbana; d) jovens da periferia; e) adultos urbanos estabelecidos; f) envelhecendo no século XXI; g) donos de negócio; h) massa trabalhadora urbana; i) moradores de áreas empobrecidas do Sul e Sudeste; j) habitantes de zonas precárias; k) habitantes de áreas rurais. Disponível em: <http://www.serasaexperian.com.br/mosaic/Mosaic_Web.pdf>. Vejam-se, ainda, as considerações de: GOULART, Guilherme. Por uma visão... cit., p.453.

[127] Federal Trade Commission/FTC. Data brokers... cit., p.23-34.

[128] Display advertising technology landscape. Disponível em: <http://www.lumapartners.com/lumascapes/display-ad-tech-lumascape/>.

[129] *On-line display*: mercado brasileiro. Disponível em: <http://pt.slideshare.net/DigiTalks/o-que-so as-adnetworks-como-funcionam-quais-as-vantagens-e-como-esse-mercado-nos-eua-e-no-brasil>.

[130] A respeito dos valores envolvidos, colocando tal transação como uma das maiores na história do ramo dos negócios, veja-se a reportagem intitulada: Facebook anuncia compra do aplicativo WhatsApp por US$ 16 bilhões. Disponível em <http://tecnologia.uol.com.br/noticias/redacao/2014/02/19/facebook-anuncia-compra-do-aplicativo-whatsapp.htm>.

[131] Transcrevendo tal ponto de vista do criador do aplicativo: DIAS, Roberto. Análise: Aquisição do WhatsApp une duas visões de mundo opostas. Disponível em: <http://www1.folha.uol.com.br/tec/2014/02/1414823-analise-aquisicao-do-whatsapp-une-duas-visoes-de-mundo-opostas.shtml>: "Com a palavra, seu fundador: 'As empresas hoje em dia sabem literalmente tudo de você, dos seus amigos, dos seus interesses, e usam isso para vender anúncios', escreveu Koum no blog da companhia, em 2012. 'A publicidade não significa apenas a ruptura da estética, um insulto a sua inteligência e a interrupção do seu treinamento mental. Em cada empresa que vende anúncios, uma parte significativa dos seus engenheiros passa o dia escrevendo códigos para coletar todos os seus dados pessoais'. Koum enfatizava: 'Lembre-se: quando há publicidade envolvida você, usuário, é o produto'. É com base nisso que ele defendia a cobrança pelo serviço do WhatsApp (US$ 1 por ano). E a quem o que questionava sobre esse pagamento, devolvia: 'Já considerou a alternativa?'".

[132] "Facebook's $ 19 billion acquisition of cross-platform mobile messaging company WhatsApp, announced last month, became the target of privacy groups, as the Electronic Privacy Information Center and the Center for Digital Democracy filed a complaint with the Federal Trade Commission, alleging that the privacy of current WhatsApp users will be affected by Facebook's use of their information. The two privacy groups said in the introduction to their complaint, embedded below: This complaint concerns the impact on consumer privacy of the proposed acquisition of WhatsApp Inc. by Facebook Inc. As set forth in detail below, WhatsApp built a user base based on its commitment not to collect user data for advertising revenue. Acting in reliance on WhatsApp representations, Internet users provided detailed personal information to the company, including private text to close friends. Facebook routinely makes use of user information for advertising purposes and has made clear that it intends to incorporate the data of WhatsApp users into the user profiling business model. The proposed acquisition will therefore violate WhatsApp users' understanding of their exposure to online advertising and constitutes an unfair and deceptive trade practice, subject to investigation by the Federal Trade Commission".

Electronic Privacy Information Center/EPIC e Center Digital for Democracy. Privacy Group File FTC Complaint Vs. Facebook-WhatsApp Deal. Disponível em: <http://allfacebook.com/ftc-complaint-whatsapp_b129849?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=Feed%3A+allfacebook+%28Face

133 Após algumas autoridades de proteção de dados pessoais europeias iniciarem procedimentos investigatórios sobre a legalidade de tal compartilhamento de dados, o WhatsApp decidiu suspendê-lo. No entanto, tal medida alcança somente os dados em fluxo no continente europeu. Nesse sentido: Facebook halts WhatsApp data sharing across Europe over privacy concerns Disponível em: <http://arstechnica.co.uk/tech-policy/2016/11/facebook-pauses-whatsapp-data-sharing-uk-ico-threatens-action/>.

134 BIONI, Bruno Ricardo.*WhatsApp e a chance para uma nova discussão*. Disponível em: <http://www.telesintese.com.br/nova-politica-de-privacidade-do-whatsapp-chance-de-se-discutir-modelos-de-negocios-e-praticas-de-tratamento-de-dados-menos-invasivos-privacidade/>.

135 "Facebook is buying WhatsApp for $19 billion. There's no denying that's a big number. But, a big number doesn't necessarily mean it's an expensive number. In fact, it might be a relative bargain, even at $19 billion. This chart from Statista shows that the per-user price Facebook paid for WhatsApp. Compared to all the other major social networks, WhatsApp is fairly cheap. Part of the reason is that WhatsApp hasn't effectively monetized these users. In the long run, though, it's not hard to see WhatsApp getting anywhere from $1-$12 per user annually, which would make it a lucrative business". *The Chart That Shows WhatsApp Was A Bargain At $19 Billion* Disponível em: <http://www.businessinsider.com/price-per-user-for-whatsapp-2014-2#ixzz2vzLK2Kit>.

136 Veja-se, por exemplo, o relatório de: ZANATTA, Rafael A. F. *Consentimento forçado?* Uma avaliação sobre os novos termos de uso do WhatsApp e as colisões com o Marco Civil da Internet. São Paulo: IDEC, 2016. Veja-se, ainda, o ensaio deste autor que endereça esse estudo de caso sob a perspectiva do consentimento do titular dos dados: BIONI, Bruno Ricardo. Nova política de privacidade do WhatsApp: questões a serem debatidas sobre consentimento. *Digital Watch*, n.13, p.5-7, ago. 2016. Disponível em: <http://www.academia.edu/28751735/Nova_Politica_de_Privacidade_do_Whatsapp_questoes_a

137 DONEDA, Danilo.*Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006. p.152.

138 ROB, Peter. *Sistemas de bancos de dados*: projeto e implementação. Trad. All Tasks. São Paulo: Cengage Learning, 2011. p.4: "Para compreender o que deve orientar o projeto de bancos de dados, você deve entender a diferença entre dados e informação. Os dados são fatos brutos. A palavra *bruto* indica que os fatos ainda não foram processados para revelar seu significado. (...)

As informações são o resultado do processamento de dados brutos para revelar o seu significado".

139 STAIR, Ralph; REYNOLDS, George W. *Princípios de sistema de informação*: uma abordagem gerencial. Tradução Flávio Soares Correa. São Paulo: Cengage Learning, 2009. p.4: "Dados são compostos por fatos básicos, como o nome e a quantidade de horas trabalhadas em uma semana de um funcionário, número de peças em estoque ou pedidos. (...) Quando esses fatos são organizados ou arranjados de maneira significativa, eles se transformam em informações. Informação é um conjunto de fatos organizados de modo a terem valor adicional, além de valor propriamente ditos".

140 FINOCCHIARO, Giusella. *Privacy e protezione dei dati personali*. Torino: Zanichelli Editore, Torino, 2012. p.33: "Coincidono, nella defizione del Codice i concetti di dato e di informazione, mentre invece si tratta di concetti differenti. Più precisamente, il dato è la fonte della ´informazione, nel quale questa è contenuta e dal singolo dato o dall'insieme di dati l'informazione può essere estratta o inferita. Ma l'informazione, a rigore, non coincide com il dato stesso. L'informazione è elaborazione del dato".

141 Ibidem, p.12-13.

142 MANNINO, Michael V. *Projeto, desenvolvimento de aplicações e administração de banco de dados*. Trad. Beth Honorato. São Paulo: McGraw-Hill, 2008. p.17-19.

143 ROB, Peter. Op.cit., p.6: "O sistema de gerenciamento de bancos de dados (SGBD) é um conjunto de programas que gerenciam a estrutura dos bancos de dados e controlam o acesso aos dados armazenados. Até certo ponto, o banco de dados se assemelha a um arquivo eletrônico com conteúdo muito bem organizado com a ajuda de um software poderoso, conhecido como sistema de gerenciamento de bancos de dados". E, ainda, explicando o conceito de *software* no contexto de bancos de dados: "Software consiste nos programas de computador que governam a operação de um computador. Esses programas permitem que um computador processe a folha de pagamentos, envie contas aos clientes e proporcione ao gerente informações para ampliar os lucros, reduzir os custos e oferecer melhores serviços aos clientes. Existem dois tipos básicos de softwares: software de sistemas, como Windows XP, que controla as operações básicas do computador, como a inicialização e impressões, e software de aplicação, como o Office XP, que permite a execução de tarefas específicas, como o processamento de textos e tabulação de números".

144 DONEDA, Danilo. Da privacidade. Op.cit., p.172.

145 ROB, Peter. Op.cit., p.33.

146 MANNINO, Michael V. Op.cit., p.555.

147 TURBAN, Efraim et al. Op.cit., p.409.

148 MANNINO, Michael V. Op.cit., p.18.

[149] TURBAN, Efraim et al. Op.cit., p.416-417.

[150] Ibidem, p.396.

[151] STAIR, Ralph; REYNOLDS, George W. Op.cit., p.12: "Um sistema de informação é um tipo d especialização de sistema e pode ser definido de diversas formas distintas. Conforme mencionado, um sistema de informação é um conjunto de elementos ou componentes inter-relacionados que coletam (entrada), manipulam (processo) e disseminam (saída) dados e informações (...)".

[152] TURBAN, Efraim et al. Op.cit., p.490.

[153] STAIR, Ralph; REYNOLDS, George W. Op.cit., p.170.

[154] MANNINO, Michael V. Op.cit., p.3: "Os bancos de dados contêm uma enorme quantidade d dados sobre muitos aspectos da nossa vida: preferências de consumo, uso de telecomunicações, histórico de crédito, hábitos ao assistir à televisão e assim por diante. A tecnologia de banco de dados ajuda a consolidar essa massa de dados e a transformá-la em informação útil para a tomada de decisão. Os gestores usam a informação recolhida nos bancos de dados para tomar decisões de longo prazo como investir em fábricas e equipamentos, escolher a localização de lojas, adicionar novos itens ao estoque e entrar em novos negócios".

[155] Ibidem, p.9.

[156] STAIR, Ralph; REYNOLDS, George W. Op.cit., p.182.

[157] MANNINO, Michael V. Op.cit., p.558.

[158] LANEY, Doug. *3D data management: Controlling data volume, velocity and variety*. Disponíve em: <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>.

[159] *Revista. Br*: publicação do Comitê Gestor da Internet, ano 4, ed. 05, p.36, nov.2013. Nesse mesm sentido: *Revista Veja,* ano 46, n.20, p.74-75, 15 maio 2013: "Entenda o que é Big Data: o megafenômeno digital que transforma em riqueza dados pessoais, posts, tuítes, e-mails e cliques"; O'REALLY MEDIA INC*Big data now*: current perspectives from O'Really Media. Bejing O'Really Media, 2012. Kindle Edition, posição 31-2322.

[160] O'Really Media Inc. Op.cit., posição 32-2322.

[161] "Em números decimais, um Yottabyte equivale a 1.208.925.819.614.629.174.706.176 bytes". Disponível em: <http://pt.wikipedia.org/wiki/Yottabyte>.

[162] O'REALLY MEDIA INC. Op.cit., posição 109-2322. Nesse mesmo sentido é a reportage intitulada "Big data: what is it and how can it help?" Disponível em: <http://www.theguardian.com/news/datablog/2012/oct/26/big-data-what-is-it-examples>.

[163] "Então, qual é a diferença entre dados relacionais e não relacionais – ou SQL e NoSQL (aka NewSQL)? Os dados relacionais são definidos no nível básico por uma série de entidades tabela

que contêm colunas e linhas, ligadas a outras entidades de mesa por atributos comuns. Assim, por exemplo, como o proprietário de um pequeno negócio on-line você pode ter um banco de dados MySQL por trás de seu site com uma mesa de gravação do nome e endereço de e-mail de seus clientes. Outra tabela pode gravar os seus nomes de produtos e seus preços. A terceira tabela pode ligar os dois, registrando os clientes que compraram produtos, com informações adicionais, como a data da compra e se ou não qualquer desconto foi aplicado. (...) Os dados não relacionais, no entanto, não são (em geral) armazenados nas tabelas. Muitas vezes chamados de 'dados não estruturados', esses dados consistem de registros separados com atributos que variam, muitas vezes por registro". SAMPAIO, Luciana.*NoSQL, SQL e Big data* Disponível em: <http://lucianasampaio.wordpress.com/2013/10/03/nosql-sql-e-big-data/>.

[164] O próprio vocábulo induz a essa compreensão quanto à desnecessidade da estruturação prévia dos dados para trabalhá-los. As iniciais No (NoSQL) significam "not only", ou seja, não apenas SQL, fazendo alusão, justamente, à análise de dados não estruturados que o sistema SQL – dos bancos de dados tradicionais – não é capaz de trabalhar. Veja-se: FRANÇA, Guilherme.*Entenda melhor o NoSQL e o Big Data* Disponível em: <http://blog.websolute.com.br/entenda-melhor-o-nosql-e-o-big-data/>.

[165] TAURION, Cezar.*Você sabe realmente o que é Big Data*. Disponível em: <https://www.ibm.com/developerworks/community/blogs/ctaurion/entry/voce_realmente_sabe_o_ lang=en>.

[166] MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. *Big data*... Op.cit., p.12.

[167] MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. *Big data*... Op.cit., p.12.

[168] *Revista. Br*: publicação do Comitê Gestor da Internet, ano 4, ed. 5, p.36, nov.2013. Nesse mesmo sentido: *Revista Veja*, ano 46, n.20, p.74, 15 maio 2013): "Entenda o que é Big Data: o megafenômeno digital que transforma em riqueza dados pessoais, posts, tuítes, e-mails e cliques".

[169] LERMAN, Jonas. Big Data and Its Exclusions*Stanford Law Review Online*, v.66, Sept. 2013. Disponível em: <SSRN:http://ssrn.com/abstract=2293765>. 2014. p.57: "Big data, for all its technical complexity, springs from a simple idea: gather enough details about the past, apply the right analytical tools, and you can find unexpected connections and correlations, which can help you make unusually accurate predictions about the future – how shoppers decide between products, how terrorists operate, how diseases spread. Predictions based on big data already inform public and private-sector decisions every day around the globe".

[170] MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. *Big data*... Op.cit., p.49-52.

[171] Ibidem, p.62.

[172] DUHIGG, Charles.*How companies learn your secrets*. Disponível em: <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0>.

[173] MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. *Big data*... Op.cit., p.57: "The analytics

team reviewed the shopping histories of women signed up for its baby gift-registry. They noticed that these women bought lots of unscented lotion at around the third month of pregnancy, and that a few weeks later they tended to purchase supplements like magnesium, calcium, and zync. The team ultimately uncovered around two dozen products that, used as proxies, enabled the company to calculate a 'pregnancy prediction'".

174 "Um algoritmo é uma sequência finita de instruções bem definidas e não ambíguas, cada uma das quais pode ser executada mecanicamente num período de tempo finito e com uma quantidade de esforço finita. O conceito de algoritmo é frequentemente ilustrado pelo exemplo de uma receita culinária, embora muitos algoritmos sejam mais complexos. Eles podem repetir passos (fazer iterações) ou necessitar de decisões (tais como comparações ou lógica) até que a tarefa seja completada. Um algoritmo corretamente executado não irá resolver um problema se estiver implementado incorretamente ou se não for apropriado ao problema". Disponível em: <http://pt.wikipedia.org/wiki/Algoritmo>.

175 Nesse mesmo sentido: *Revista Veja*. Entenda... Op.cit., p.71. Nesse mesmo sentido: MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. *Big data*... Op.cit., p.57.

176 Trata-se do projeto denominado *Google Flu*. No Brasil ganhou o nome de tendências da gripe e já está monitorando os casos de dengue: Google Flu. Disponível em: <http://www.google.org/flutrends/intl/pt_br/about/how.html>.

177 WORLD ECONOMIC FORUM. *Big data, big impact: new possibilities for international development*. Disponível em: <http://www3.weforum.org/docs/WEF_TC_MFS_BigData-BigImpact_Briefing_2012.pdf>.

178 MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. *Big data*... Op.cit., p.160.

179 Ibidem, p.36.

180 JEROME, Joseph W. Buying and selling privacy: Big Datas's Different burdens and benefits. *Stanford Law Review Online*, v. 66, p.51, Sept. 2013.

181 MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. *Big data*... Op.cit., p.41.

182 Nesse sentido é a reportagem intitulada: *When You Fall in Love, This Is What Facebook Sees*. Disponível em: <http://www.theatlantic.com/technology/archive/2014/02/when-you-fall-in-love-this-is-what-facebook-sees/283865/>. No mesmo sentido: *Algoritmo prevê, no Facebook, quando um namoro vai acabar*. Disponível em: <http://info.abril.com.br/noticias/ciencia/2013/10/algoritmo-preve-no-facebook-quando-um-namoro-vai-acabar.shtml>.

183 Nesse sentido é a reportagem intitulada: *What's the role of data scientists on online advertising?* Disponível em: <http://www.theguardian.com/news/2013/nov/11/data-scientists-impact-online-advertising>.

[184] "Dos bancos de dados e cadastros de consumidores".

[185] "Das práticas comerciais".

[186] BESSA, Leonardo Roscoe. A abrangência da disciplina conferida pelo código de defesa do consumidor aos bancos de proteção ao crédito. In: NERY JÚNIOR, Nelson; NERY, Rosa Maria de Andrade (Org.). *Coleção doutrinas essenciais*: Responsabilidade civil – direito à informação. São Paulo: Revista dos Tribunais, 2010. v.8, p.405.

[187] BENJAMIN, Antônio Herman de Vasconcellos e. *Código brasileiro de defesa do consumidor*: comentado pelos autores do anteprojeto. Direito material (arts. 1º a 80º e 105 a 108). Rio de Janeiro: Forense, 2011. v.1, p.443: "Em estrito rigor terminológico, a expressão *arquivo de consumo* é gênero do qual fazem parte duas grandes famílias de registros: os bancos de dados e os cadastros de consumidores, denominação dobrada utilizada pela seção VI, do Capítulo V ('Das Práticas Comerciais'), do CDC, que alguns preferem chamar, simplesmente, de 'cadastros de inadimplentes'".

[188] EFING, Antônio Carlos. *Bancos de dados e cadastro de consumidores*. São Paulo: Revista dos Tribunais, 2002. p.34.

[189] BENJAMIN, Antônio Herman de Vasconcellos e. *Código*... Op.cit., p.444.

[190] Ibidem, 2011, p.445. Nesse mesmo sentido: EFING, Antônio Carlos. *Bancos*... Op.cit., p.34. Em sentido análogo: BESSA, Leonardo Roscoe. *Cadastro positivo*: comentários à Lei 12.414, de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011. p.27: "De modo simplificado, a distinção entre bancos de dados e cadastros de consumo se faz a partir da fonte e o destino da informação. Os bancos de dados, em regra, coletam informações do mercado para oferecê-las ao próprio mercado (fornecedores). No cadastro, a informação é obtida diretamente do consumidor para uso de um fornecedor específico, a exemplo do que ocorre em diversos estabelecimentos comerciais quando se solicitam dados pessoais (nome, endereço postal e eletrônico, telefone, data de aniversário, entre outros), independentemente de a compra ser à vista ou mediante crediário. No cadastro, objetiva-se estreitar o vínculo com alguns consumidores, intensificando a comunicação sobre ofertas, promoções e outras vantagens, de modo a fidelizá-los a uma marca ou estabelecimento".

[191] EFING, Antônio Carlos. *Bancos*... Op.cit., p.31.

[192] BENJAMIN, Antônio Herman de Vasconcellos e. *Código*... Op.cit., p.444: "(...) b) organização permanente das informações, que ali ficam, de modo latente, à espera da utilização futura, independentemente do número de operações que o consumidor realizar no mercado".

[193] Ibidem, 2011, p.444-445. Nesse mesmo sentido: EFING, Antônio Carlos. *Bancos*... Op.cit., p.32.

[194] BESSA, Leonardo Roscoe. *Cadastro*... Op.cit., p.26.

[195] BENJAMIN, Antônio Herman de Vasconcellos e. *Código*... Op.cit., p.444.

[196] Veja-se por todos a posição de Guilherme Goulart, que se utiliza do estudo de caso dos *data brokers* para concluir que é necessária uma visão renovada dos arquivos de consumo: GOULART, Guilherme. Por uma visão... Op.cit., p.453-458.

[197] MAYER-SCHÖNBERGER, Viktor. *Delete*: The virtue of forgetting in the digital age. United Kingdom: Princeton University Press, 2009. p.79.

[198] EFING, Antônio Carlos. *Bancos*... Op.cit., p.34: "Os cadastros de consumo utilizam-se subsidiariamente das informações, para fins de controle interno acerca das possibilidades de concretização das relações comerciais, que são de interesse precípuo e atividade definitiva para a obtenção de seus recursos. Desta forma, as preocupações estão voltadas para a realização das relações comerciais que lhe são pertinentes, e o interesse econômico destes negócios poderá ser analisado com auxílio de seus arquivos internos, que são auxiliares da atividade principal. b) por outro lado, os bancos de dados de consumidores não apresentam característica de informação subsidiária aos seus arquivos, estes sendo sua própria fonte de renda e atividade comercial. Através da venda das informações constantes nestes arquivos, os bancos de dados conseguem se manter, sendo esta sua verdadeira razão de ser. As informações têm função exclusivamente econômica para os bancos de dados de consumidores. Sinteticamente, pode-se engajar a função dos dados colecionados ou relação às empresas conceituados como bancos de dados e cadastros, respectivamente, no âmbito econômico e informativo".

[199] No cenário brasileiro, veja-se: TEIXEIRA, Lucas. Data brokers e profiling: *vigilância como modelo de negócio*. Disponível em: <https://antivigilancia.org/boletim_antivigilancia/consultas/data-brokers-profiling>.

[200] A expressão é de MATIUZZO, Marcela. Op.cit.

[201] Empresta-se a terminologia de: DE VRIES, Jennifer Valentino. The Economics of Surveillance. Disponível em: <http://blogs.wsj.com/digits/2012/09/28/the-economics-of-surveillance/>.

[202] NISSENBAUM, Helen. *Daedalus*, v.140, n.4, p.41, Fall 2011. Disponível em: <https://ssrn.com/abstract=2567042>.

Capítulo II

DADOS PESSOAIS E DIREITOS DA PERSONALIDADE

2.1 DIREITOS DA PERSONALIDADE: CONSIDERAÇÕES INICIAIS SOBRE A INSERÇÃ DOS DADOS PESSOAIS NESSA CATEGORIA JURÍDICA

A travessia dos direitos da personalidade não apresenta um trajeto histórico linear[1], uma vez que os seus primeiros apontamentos, o seu próprio fundamento e a sua consolidação apresentam intervalos temporais significativos para a sua articulação. Mesmo que brevemente e de forma aleatória, é importante abordá-los para verificar como se deu a diacronia de tal categoria jurídica, o que pavimentará a via de acesso para nela alocar a proteção dos dados pessoais.

O prelúdio dos direitos da personalidade se dá no direito grego (*hybris*)[2] e no direito romano (*actio iniuriarum*)[3]. Diferentemente de outras culturas jurídico-legais anteriores (*e.g.*, Código de Hamurabi) que baseavam a tutela da pessoa humana tão somente na tutela da integridade física[4], passou-se a situá-los também no campo moral (*e.g.*, tutela da honra)[5].

Essa orientação, de uma ciência jurídica focada na pessoa, vem a encontrar sinergia no *jusnaturalismo*, especialmente a partir da concepção empregada por Hugo Grócio[6] no século XVII. É nesse momento que se afasta da ideia de que os direitos provinham de uma força divina, sofrendo a ciência jurídica um processo de laicização[7]: a ideia de que o homem teria direitos que lhe seriam inatos e, mais do que isso, decorrentes da sua própria natureza como ser humano.

Essa passagem é de extrema importância para o fundamento[8] dos direitos da personalidade, os quais são concebidos e projetados de acordo com a perspectiva de promoção do ser humano – uma visão antropocêntrica. Sobressai-se, em última análise, o vetor *extrapatrimonial* da ciência jurídica.

Contudo, com a dessacralização da ciência jurídica, emerge, ao mesmo tempo, o racionalismo na cena jurídica[9]: o *jusracionalismo*[10]. Nessa fase, o direito passa a contar com traços metodológico-sistemáticos[11] bem definidos, dando-se ênfase na elaboração de conceitos abstratos – verdadeiros dogmas[12] – para compor um sistema ordenado lógico-fechado. Os seus enunciados deveriam fornecer premissas com a exatidão da ciência matemática[13]. É, exatamente, quando florescem as noções de negócio jurídico, relação jurídica e declaração de vontade, que são abstrações *pandecistas* que defluem desse movimento *jusracionalista*[14].

Com tamanha abstração, a ciência jurídica acabou por se distanciar de uma visão *antropocêntrica* e extrapatrimonial. Nas codificações civis que se seguiram – *e.g.*, Código Civil Napoleônico[15] – prevaleceu uma excessiva carga patrimonialista apoiada justamente nos conceitos de declaração de vontade, relação e negócio jurídico[16].

Tais aspectos explicam por que os direitos da personalidade não angariaram o espaço que lhes seria devido no direito privado naquela época, não obstante terem sido pensados e sistematizados anteriormente[17].

Aliás, a própria dissidência histórica instaurada por Savigny quanto à recepção dos direitos da personalidade derivava de uma questão única e exclusivamente dogmática[18]. Argumentava-se que o sujeito de uma relação jurídica não poderia ser ao mesmo tempo o seu objeto, sob pena de se legitimar o suicídio.

Ou seja, negava-se reconhecer os direitos da personalidade por faltar uma norma que os positivasse[19]. De acordo com esse raciocínio dogmático, era imprescindível a inserção dos direitos da personalidade na categoria de um direito subjetivo para, daí, serem escoados.

Nesse percurso, a pessoa humana perdeu espaço em detrimento das abstrações do positivismo[20] e da excessiva preocupação do direito com aspectos patrimoniais. Tal período não se mostrou acolhedor para o desenvolvimento dos direitos da personalidade, muito menos para a sua consolidação[21].

Necessário se fez que a história interviesse com experiências terrificantes para se repensar esse caminho até então trilhado. A escravidão e os regimes nazifascistas esfacelaram, todos eles com a chancela da ciência jurídica (direito positivo), a ideia da prometida universalidade de direitos do homem proposta pelo jusnaturalismo.

É, especialmente, após a Segunda Guerra Mundial[22], com a proliferação do princípio da dignidade humana nas constituições[23], tal como a própria declaração de direitos universais da Organização das Nações Unidas[24], que se dá uma guinada para que o direito passasse a assegurar os interesses existenciais da pessoa humana.

No âmbito do direito privado, é o que se convencionou chamar de *despatrimonialização* do direito civil[25]. Altera-se qualitativamente[26] o foco da tutela jurídica[27], reposicionando o ser humano como o seu centro gravitacional.

Nesse sentido, por exemplo, a Constituição Federal alemã passou a prever, ao lado do princípio da dignidade da pessoa humana, o direito ao livre desenvolvimento da personalidade[28]. Era o que faltava para que fosse desenvolvida, efetivamente, a tutela dos direitos da personalidade naquele país[29], passando a ser replicada tal cláusula geral em outras codificações privadas, ou, ainda, a própria enumeração de quais viriam a ser os direitos da personalidade[30].

Nessa conjuntura, no cenário nacional ainda sob a vigência do Código Civil de 1916, a doutrina brasileira já reconhecia os direitos da personalidade de forma implícita, mediante a interpretação de dispositivos que versavam remotamente sobre os aspectos extrapatrimoniais das relações sociais[31].

A matéria somente ganhou ares de sistematização com o projeto de Código Civil de Orlando Gomes, tendo-lhe sido dedicado um capítulo próprio. O jurista baiano deixou claro que o norte da projetada sistematização seria romper com o viés individualista-patrimonialista[32] da codificação anterior, cujas raízes estavam fortemente ancoradas no Código Civil francês.

Seria necessário dispensar maior proteção à pessoa, que foi anteriormente negligenciada pela ênfase dada ao patrimônio. Já em 1955, em sua obra *A crise do Direito*, Orlando Gomes identificava a *despatrimonialização* ou *repersonalização* do direito civil como um necessário processo de *humanização* do direito privado[33].

Por essa razão, o seu projeto de Código Civil enumerou os direitos da personalidade, como, por exemplo, o direito ao nome, à imagem, à liberdade, à honra, à integridade física e, por fim, os direitos autorais[34]. Não seria nenhum exagero registrar que o atual CC fez bom uso do projeto de codificação do jurista baiano[35]. Uma das grandes inovações do direito privado brasileiro foi gestada por Orlando Gomes, o qual iniciou um novo tripé para a teoria geral do direito civil brasileiro: personalidade, negócio jurídico e patrimônio[36].

A ordem cronológica da personalidade como primeiro elemento desse tripé reflete como se deu a sua sistematização no CC atual, sendo um dos capítulos inaugurais (II). E, por essa mesma lógica topográfica, não se deve negligenciar que o princípio constitucional da dignidade da pessoa humana abre, também, o texto constitucional, sendo um dos fundamentos da República Federativa do Brasil – art. 1º, III[37] –, para que dele se possa extrair a sua máxima potencialidade[38].

Essa é uma chave de leitura[39] que confirma a (re)construção do direito privado com foco na proteção da pessoa humana (*despatrimonialização*), sendo este o ponto de atenção de um direito civil *repersonalizado*[40].

Dito de outra forma, os direitos da personalidade não representam somente uma inovação no ordenamento jurídico brasileiro, trata-se, também, de um componente central de uma nova hermenêutica que coloca o ser humano como o "coração do direito civil contemporâneo"[41].

Daí por que os direitos da personalidade fazem parte de uma cláusula geral[42] de proteção de tutela e promoção da pessoa humana[43] ou de um sistema geral de tutela à pessoa humana[44], cuja consequência principal é a sua *elasticidade*[45].

Os direitos da personalidade são uma "noção inacabada" que deve ser "cultivada"[4546], especialmente frente ao abordado manancial de dados produzidos pelas pessoas na sociedade da informação. Por meio dessa premissa, será possível identificar uma nova variante desta categoria jurídica para nela enquadrar a proteção dos dados pessoais.

Nesse sentido, os direitos da personalidade não se limitam àquelas situações previstas no CC, sendo o seu rol *numerus apertus* (rol aberto)[47]. Eles não se exaurem[48] naquelas espécies enumeradas nos arts. 11 a 21 do CC[49], o que abre caminho para o reconhecimento da proteção dos dados pessoais como um *novo direito da personalidade*.

Foge aos limites deste trabalho adentrar na discussão sobre a tutela dos direitos da personalidade como um direito geral de personalidade e/ou a sua inserção por meio de espécies[50], até porque se julga ser a mesma inócua. Pragmaticamente, o que importa é que ambas as orientações geram o mesmo resultado: uma tutela dinâmica e aberta para abraçar novas situações como um ferramental para a promoção da pessoa humana[51].

Anota-se que personalidade aqui, na sua função de adjetivação – direitos da personalidade –, é completamente diferente de personalidade tomada como substantivo – personalidade jurídica. Não se trata da aptidão de um sujeito ser titular de direitos e deveres, mas da proteção jurídica canalizada para o desenvolvimento da pessoa humana. O objetivo é dispor de objetos juridicamente tutelados que conformem tal proteção[52], como o que se pretende traçar no tocante à proteção de dados pessoais.

Por isso, fala-se em *bens da personalidade*[53] que são dirigidos para a satisfação do livre desenvolvimento da personalidade. A sua conotação é essencialmente extrapatrimonial, tratando-se de situações jurídicas[54] distintas daquelas de bem como um conceito estritamente econômico[55]. Diz respeito, portanto, aos bens (objetos) que facilitam a promoção da pessoa humana.

O único problema reside no fato de que o CC não estabeleceu um conceito do que viriam a ser os direitos da personalidade, razão pela qual sua noção jurídica prende-se a duas perspectivas construídas doutrinariamente: **a)** como um atributo, prolongamento ou projeção que é próprio da *ipseidade* da pessoa humana (subcapítulo 2.2 *infra*); **b)** pela percepção de que o ser humano é, por excelência, um ser social, devendo-se assegurar a sua esfera relacional (subcapítulo 2.3 *infra*).

Se na sequência for possível desvendar tais características, então terá sido possível alcançar o objetivo de tornar mais palpável a figura etérea, ao menos conceitualmente, dos direitos da personalidade e, em última análise, alocar os dados pessoais como uma nova espécie de tal categoria jurídica.

A função dos direitos da personalidade é promover e assegurar o valor-fonte[56] do ordenamento jurídico, a pessoa humana que se encontra respaldada por um sistema ou uma cláusula geral de proteção. Essa orientação é energizada pela concepção de um direito privado despatrimonializado ou repersonalizado.

Por isso, necessário se faz revisitar constantemente os direitos da personalidade para se aperfeiçoar a busca incessante e mutável da tutela da pessoa humana[57]. As novas tecnologias trazem novos desafios a esse respeito[58].

2.2 A PROJEÇÃO DA PERSONALIDADE POR MEIO DOS DADOS

2.2.1 Dados pessoais e projeção da personalidade: uma nova identidade

Personalidade significa as "características ou o conjunto de características que distingue uma pessoa"[59] da outra. Com base nessa abordagem semântica, os direitos da personalidade seriam os caracteres incorpóreos e corpóreos[60] que conformam a projeção[61] da pessoa humana. Nome, honra, integridade física e psíquica[62] seriam apenas alguns dentre uma série de outros atributos que dão

forma a esse prolongamento[63].

Dada a *ipseidade* que difere o ser humano dos outros entes e entre seus próprios pares (*distinctum subsistens*)[64], a ciência jurídica o protege das agressões que afetem a sua individualidade[65]. Trata-se de conferir tutela jurídica aos elementos que emprestam conteúdo ao valor-fonte do ordenamento jurídico, aos bens (da personalidade) que individualizam o sujeito perante a sociedade[66].

Sob essa perspectiva, um dado, atrelado à esfera de uma pessoa[67], pode se inserir dentre os direitos da personalidade. Para tanto, ele deve ser adjetivado como pessoal, caracterizando-se como uma projeção, extensão ou dimensão do seu titular[68].

E, nesse sentido, cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas. Hoje vivemos em uma sociedade e uma economia que se orientam e movimentam a partir desses *signos identificadores* do cidadão.

Trata-se de um novo tipo[69] de identidade[70] e, por isso mesmo, tais *dossiês digitais*[71] devem externar informações corretas para que seja fidedignamente *projetada* a identidade[72] do titular daquelas informações.

Isso acaba por justificar *dogmaticamente* a inserção dos dados pessoais na categoria dos direitos da personalidade, assegurando, por exemplo, que uma pessoa exija a retificação de seus dados pessoais para que a sua projeção seja precisa[73].

Por isso, os dados pessoais não estão relacionados somente com a privacidade, transitando dentre mais de uma das espécies dos direitos da personalidade. Tal construção dogmática[74] é útil, pois é tal *ampliação normativa* que assegura o direito à retificação e de acesso aos dados e outras posições jurídicas próprias do direito à proteção dos dados pessoais (*e.g.*, direito de revisão de decisões automatizadas)[75-76].

Seria contraproducente e até mesmo incoerente pensar a proteção de dados pessoais somente sob as lentes do direito à privacidade. O eixo da privacidade está ligado ao controle de informações pessoais do que seja algo íntimo ou privado do sujeito. A proteção dos dados pessoais não se satisfaz com tal técnica normativa, uma vez que a informação pode estar sob a esfera pública, discutindo-se, apenas, a sua exatidão, por exemplo[77].

Ao lado do princípio da qualidade dos dados, o direito de correção é uma construção que deriva da perspectiva da identidade do sujeito e não do direito à privacidade[78]. É o primeiro direito de personalidade que determina a necessidade de haver uma correspondência[79] fidedigna entre a pessoa e seus dados pessoais. A esfera do que é público ou privado revela-se incompleta para dar vazão a esse tipo de dinâmica normativa.

Por isso, os dados que influem na projeção de uma pessoa e na sua esfera relacional adéquam-se conceitualmente como um novo direito da personalidade[80]. Alocar a proteção dos dados pessoais nessa categoria jurídica é uma construção dogmática necessária. Além de dar coerência normativa a uma série de faculdades jurídicas próprias desse direito (*e.g.*, direito de acesso, correção, revisão de

decisões automatizadas etc.), trata-se de um norte que facilita a sua interpretação e aplicação para não empolar a compreensão de seus conceitos basilares.

2.2.2 Conceito de dados pessoais: reducionista *versus* expansionista nas leis setoriais e na lei geral brasileira de proteção de dados pessoais[81]

O conceito de dados pessoais é um elemento central[82] para que se aperfeiçoe a normatização sob análise, na medida em que se estabelecem os limites da própria tutela jurídica em questão. Em outras palavras, um dado que não avoque tal qualidade não poderia ser cogitado como um prolongamento da pessoa por lhe faltar tal centro de imputação.

Mutatis mutandis, seria a mesma lógica do fato jurídico[83]. Não seria qualquer dado que teria repercussão jurídica, mas, somente, aquele que atraísse o qualificador pessoal.

De forma sistemática, o vocabulário para prescrever tal definição é composto por palavras que restringem ou alargam o *gargalo* dessa proteção. Há uma bipartição do seu léxico que ora retrai (reducionista), ora expande (expansionista), a moldura normativa de uma lei de proteção de dados pessoais.

Os quadros a seguir sintetizam qual é esse vocabulário e qual foi a opção adotada na LGPD e nas normas setoriais brasileiras de proteção de dados pessoais para, em seguida, proceder a uma análise ilustrativa das suas repercussões práticas.

Quadro 1 – Vocabulário analítico para a definição do conceito de dados pessoais

Expansionista	**Reducionista**
Pessoa identificável	Pessoa identificada
Pessoa indeterminada	Pessoa específica/determinada
Vínculo mediato, indireto, impreciso ou inexato	Vínculo imediato, direto, preciso ou exato
Alargamento da qualificação do dado como pessoal	**Retração da qualificação do dado como pessoal**

Quadro 2 – Tabela analítica da definição de dados pessoais no ordenamento jurídico brasileiro

LGPD	**Leis Setoriais de PDP**	
	Decreto 8.771/2016	**Lei 12.527/2011**
Art. 5º, inciso I – dado pessoal: dado relacionado à	Art. 14, inciso I – dado pessoal: dado relacionado à pessoa natural **identificada ou identificável**,	Art. 4º, inciso IV – informação pessoal: aquela

pessoa natural **identificada ou identificável**	inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa	relacionada à pessoa natural **identificada ou identificável**
Expansionista (sem rol exemplificativo)	**Expansionista** (com rol exemplificativo)	**Expansionista** (sem rol exemplificativo)

A intelecção do conceito de dado pessoal e, por conseguinte, das estratégias regulatórias possíveis para a sua definição é algo fluido, que pode ser esclarecido a partir da dinâmica de conceitos básicos de sistemas de informação e de banco de dados. Somente, assim, o seu vocabulário ganhará uma análise mais concreta a demonstrar as diferenças e consequências práticas entre tais estratégias regulatórias distintas.

Para fins de ilustração, optou-se pelo exemplo de um banco de dados relacionais. Esse tipo de banco de dados é estruturado por tabelas[84], em que cada uma de suas colunas – que são chamadas de atributos[85] – é a maneira pela qual os dados são organizados. É a correlação entre as colunas e as linhas dessa tabela que empresta valor (significado) aos dados, permitindo que deles seja extraído algo inteligível (informação)[86].

Esse é um exercício didático para entender como os referenciais teóricos reducionista e expansionista distanciam-se completamente um do outro, apesar da proximidade léxica entres eles.

Tabela 1 – Base de dados relacionais

A) Nome	B) CPF	C) CEP	D) Idade	E) Classificação/segmentação
1. Bruno Santos	123.456-77	04055-000	18	Jovem hipster
2. Bruno Santos	234.567-88	04055-111	17	Jovem poupador
3. Bruno Santos	345.678-99	04055-222	17	Jovem consumista
4. Bruno Souza	456.789-10	01201-000	65	Idoso com rentabilidade
5. Bruna Souza	567.891-01	04201-111	66	Idosa sem rentabilidade
6. Bruna Bioni	222.333-44	04201-222	70	Idosa com rentabilidade
7. Maria Silva	157.890-88	09201-000	40	Adulto desempregado
8. Maria Silva	666.666-66	09201-111	38	Adulto perfil executivo
9. Maria da				

Hipótese 1 (reducionistas): a presença de homônimos não permitiria que houvesse a individualização precisa de uma parcela das pessoas inseridas no banco de dados acima, caso não houvesse outros dados – identificadores (únicos) como, por exemplo, o CPF. Somente mediante tal associação identificou-se exatamente o(s) "Bruno(s)" e a(s) "Maria(s)", tornando-os pessoas identificadas, isto é, individualizadas de maneira precisa, exata e inequívoca.

Hipótese 2 (expansionistas): caso houvesse a eliminação da coluna "B", haveria incerteza a respeito de qual dos "Brunos" seria consumista, poupador ou hipster (coluna "E"), já que não haveria outro dado – identificador (único) – para diferenciar cada um dos homônimos. E, o mesmo, com relação a qual Maria seria a desempregada ou a executiva. Tais informações não estariam relacionadas a pessoas identificadas, ainda que elas pudessem vir a ser a partir da sua localização geográfica (coluna "B"), por exemplo. Nesse caso, a incerteza gerada por um grupo de pessoas com o mesmo nome tende a ser eliminada pela agregação dessa outra informação, tornando as pessoas identificáveis. Há, em última análise, o potencial de individualizá-las.

Portanto, verificar se um dado pode ser adjetivado como pessoal é uma *análise contextual* que depende de qual tipo de informação pode ser extraída de uma base de dados. Essa análise circunstanciada pode ser mais dura ou mais flexível. Para os reducionistas, somente na hipótese "A" haveria dados pessoais. Para os expansionistas, as hipóteses "A" e "B" seriam abraçadas pelo conceito de dado pessoal.

2.2.3 Dados "anônimos" como a antítese de dados pessoais: o filtro da razoabilidade

A antítese do conceito de dado pessoal seria um dado anônimo, ou seja, aquele que é incapaz de revelar a identidade de uma pessoa. Diante do próprio significado do termo, anônimo seria aquele que não tem nome nem rosto[87].

Essa inaptidão pode ser fruto de um processo pelo qual é quebrado o vínculo entre o(s) dado(s) e seu(s) respectivo(s) titular(es), o que é chamado de anonimização[88]. Esse processo pode se valer de diferentes técnicas que buscam eliminar tais elementos identificadores de uma base de dados[89], variando entre: **a)** supressão; **b)** generalização; **c)** randomização e; **d)** pseudoanonimização[90].

Foge ao escopo deste trabalho abordar cada uma das citadas técnicas do processo de anonimização. Vale a pena, no entanto, abordar as duas primeiras para ilustrar a sua dinâmica e pavimentar a via de acesso para se debruçar sobre as implicações normativas de uma eventual dicotomia entre dados anônimos (anonimizados) e dados pessoais.

Retomando o exemplo de base de dados relacionais estruturada, deve-se identificar quais

elementos poderiam ser modificados – suprimidos ou generalizados – para que o seu *grau de identificabilidade* seja eliminado ou reduzido:

a) **supressão do CPF**: por ser um identificador capaz de diferenciar até mesmo pessoas homônimas, sendo um identificador único; logo, a sua disponibilização, ainda que parcial – *e.g.*, cinco primeiros dígitos –, não seria prudente;

b) **generalização do nome completo**: constaria apenas o prenome, desde que fosse observado que os nomes da base de dados não são comuns. O objetivo é evitar que um nome possa ser atribuído a um indivíduo em específico;

c) **generalização da localização geográfica**: em vez de disponibilizar o número completo do CEP, seriam divulgados apenas os seus primeiros dígitos. Assim, haveria uma localização menos detalhada, a fim de quebrar o vínculo de identificação desta informação com um sujeito;

d) **generalização da idade**: em vez de divulgar a idade exata, seria divulgada a faixa etária para viabilizar a categorização dos indivíduos como jovens, adultos ou idosos (coluna "E") e, por outro lado, inviabilizar a sua individualização, dado o universo de pessoas que se enquadram naquela mesma faixa etária.

Tabela 2 – Base de dados relacionais anonimizada

A) Nome	B) CPF	C) CEP	D) Faixa etária	E) Classificação/segmentação
1. Bruno dos Santos	~~123.456-77~~	04055-000	18>	Jovem hipster
2. Bruno dos Santos	~~234.567-88~~	04055-111	18>	Jovem poupador
3. Bruno dos Santos	~~345.678-99~~	04055-222	18>	Jovem consumista
4. Bruna Souza	~~456.789-10~~	01201-000	60<	Idoso com rentabilidade
5. Bruna Souza	~~567.891-01~~	04201-111	60<	Idosa sem rentabilidade
6. Bruna Schonber	~~222.333.44-55~~	04201-222	60<	Idosa com rentabilidade

7. Maria Silva	~~157.890.88-66~~	09201-000	18<	Adulto desempregado
8. Maria Silva	~~666.666.66-66~~	09201-111	18<	Adulto perfil executivo
9. Maria Sóstenes	~~987.354.22-99~~	09201-222	18>	Jovem hipster

Com maior ou menor grau de intensidade – *e.g.*, supressão ou generalização – nota-se um método cujo mote é gerenciar circunstancialmente a *identificabilidade* de uma base de dados. As características de cada dado e a percepção de eles estarem inseridos em uma gama de informações devem orientar tal análise.

Por isso, não há um único método ou uma combinação perfeita *ex ante* para parametrizar o processo de anonimização, devendo-se analisar contextualmente como este deve ser empreendido para que os titulares dos dados anonimizados não sejam reidentificados, nem mesmo por quem procedeu à sua anonimização.

Amarrar o conceito teórico de dados anônimos a uma análise contextual, com os olhos voltados para a irreversibilidade do processo de anonimização, joga luz diretamente sobre o fator problemático dessa proposição: o seu caráter elusivo ou mesmo a sua impossibilidade teórica[91].

Torna-se cada vez mais recorrente a publicação de estudos que demonstram ser o processo de anonimização algo falível. A representação simbólica de que os vínculos de identificação de uma base de dados poderiam ser completamente eliminados, garantindo-se, com 100% (cem por cento) de eficiência, o anonimato das pessoas, é um mito[92].

Os pesquisadores Arvind Narayanan e Vitaly Shmatikov têm se destacado nessa área. Eles reidentificaram diversas bases de dados anonimizados, como, por exemplo, a de um famoso provedor de aplicação de Internet – o caso Netflix Prize.

Nesse caso, os referidos pesquisadores desenvolveram um algoritmo que calculava dentre outras coisas: **a)** quantos *bits* de informação seriam necessários para reverter o processo de anonimização; **b)** qual seria o melhor critério para a escolha de uma informação auxiliar – i.e., uma outra base de dados – a ser agregada para reverter o processo de anonimização; **c)** uma métrica sobre a probabilidade de acerto da reidentificação, evitando-se "falsos positivos" – i.e., a vinculação errônea de indivíduos aos dados desanonimizados[93].

À época, a maior provedora de *streaming* de filmes do mundo criou um concurso, cujo desafio era melhorar o seu algoritmo de sugestão de filmes. Então, a Netflix disponibilizou a sua base de dados com todas as avaliações dos filmes de seu catálogo do período de 1998 a 2005, suprimindo os nomes dos usuários avaliadores e deixando somente a data e a nota da avaliação.

A fim de tornar tal processo de reidentificação mais robusto, a Netflix se utilizou da técnica de

randomização. Ela alterou algumas datas e *ratings* das avaliações dos seus consumidores, o que aumentaria o risco de "falsos positivos", a não ser pelo fato de o algoritmo dos pesquisadores ter sido projetado para isso.

Os pesquisadores "rodaram" tal algoritmo na base de dados disponibilizada, descobrindo que seria necessário entre 3 (três) e 19 (dezenove) *bits* de informação para reverter o processo de anonimização. Esse *pool* de informações necessário estava publicamente disponível e acessível na Internet Movies Databases/IMDB[94].

O IMDB é um*website* onde as pessoas compartilham suas impressões sobre filmes, utilizando-se, na maioria das vezes, dos seus nomes reais. Desta forma, os pesquisadores "cruzaram" essas informações com a base de dados da Netflix, correlacionando as datas das avaliações dos filmes e seus respectivos *scorings*. Assim, a peça faltante do quebra-cabeça – a identidade dos usuários da Netflix – foi desvendada com base nos nomes contidos nas avaliações do IMDB[95].

O exemplo em questão é simbólico, pois sublinha o "calcanhar de Aquiles" dos dados anônimos. Sempre existirá a possibilidade de uma base de dados anonimizada ser agregada a outra para a sua reidentificação[96-97].

Por isso, via de regra, prevalece o conceito *expansionista*[98] pelo qual dado pessoal equivale a uma informação que, direta ou indiretamente, identifica um sujeito. Essa definição abraça, portanto, mesmo as informações que têm o potencial de identificar alguém, ainda que de maneira remota[99].

Desde a década de 1980, organismos internacionais, blocos econômicos, países norte-americanos e latino-americanos conceituam dados pessoais como uma informação a respeito de uma pessoa identificada ou identificável[100].

Tabela 3 – Tabela comparativa acerca da definição de dados pessoais no direito comparado

OCDE	CoE	Canadá	Argentina	APEC	UE
"personal data" means any information relating to an identified or identifiable individual (data subject)	"personal data" means any information relating to an identified or identifiable individual ("data subject")	personal information means information about an identifiable individual.	Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.	Personal information means any information about an identified or identifiable individual.	"personal data" means any information relating to an identified or identifiable individual ("data subject");
Expansionista	Expansionista	Expansionista	Expansionista	Expansionista	Expansionista

1980	1981	2000	2000	2005	1995/2016

A proteção dos dados pessoais, como um novo direito da personalidade, dirige-se a todo e qualquer dado em que se denote o *prolongamento* de um sujeito. Dados pessoais não se limitam, portanto, a um tipo de projeção *imediata*, mas, também, a um referencial *mediato* que pode ter *ingerência* na esfera de uma pessoa[101].

Por essa lógica, qualquer dado pessoal anonimizado detém o *risco inerente* de se transmudar em um dado pessoal[102]. A agregação de diversos "pedaços" de informação (dados) pode revelar (identificar) a imagem (sujeito) do quebra-cabeça, a qual era até então desfigurada (anônimo) – o chamado efeito mosaico.

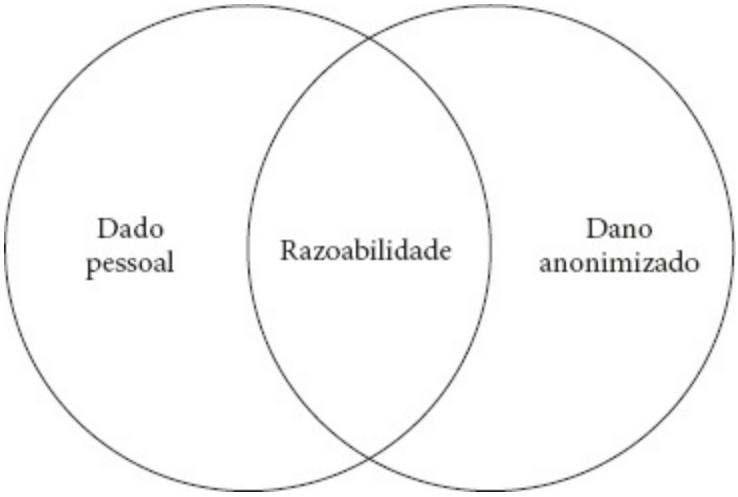
Por isso, em princípio, eventual dicotomia entre dados pessoais e dados anônimos só guardaria coerência junto ao conceito reducionista de dados pessoais. Isso porque dados anônimos não são dados relacionados a uma pessoa identificada, demandando a reversão do processo de anonimização para se chegar aos respectivos titulares, sendo a sua identificabilidade remota (identificável) e não imediata (identificada).

Dessa forma, leis que adotam o conceito expansionista de dados pessoais e, ao mesmo tempo, estabelecem uma dicotomia deste com dados anônimos correriam o risco de ser tautológicas. Isso porque haveria uma *redundância normativa*, já que dados anônimos seriam, em última análise, potencial e provavelmente, dados relacionados a uma pessoa identificável.

Para não gerar tal incoerência, a única saída foi a adoção de um "filtro" que delimitasse a *elasticidade* do conceito expansionista – neste caso o termo identificável –, sob pena de a fronteira entre dados pessoais e dados anônimos ser sempre transponível.

E, nesse sentido, o direito comunitário europeu[103] e a LGPD[104] valeram-se do critério da razoabilidade para delimitar o espectro do conceito expansionista de dados pessoais. Não basta a mera possibilidade de que um dado seja atrelado a uma pessoa para atrair o termo identificável[105]. Essa vinculação deve ser objeto de um "esforço razoável"[106], sendo esse o perímetro de elasticidade do conceito de dado pessoal como aquele relacionado a uma pessoa identificável.

A contrario sensu, se para a correlação entre um dado e uma pessoa demanda-se um esforço fora do razoável, não há que se falar em dados pessoais. Nessa situação, o dado é considerado como anônimo, uma vez que o "filtro da razoabilidade" barra o seu enquadramento como aquele relacionado a uma pessoa identificável[107].



Com isso, há coerência em se estabelecer conceitos diferentes para tais espécies de dados, sobretudo sob o ponto de vista de uma dicotomia mutualmente excludente entre eles, que é delimitada pelo fator da razoabilidade[108]. Do contrário, repita-se, haveria uma redundância normativa, na medida em que dados anônimos – sem o critério da razoabilidade – seriam sempre enquadrados dentro do conceito de dado pessoal, como aquele relacionado a uma pessoa identificável.

2.2.3.1 Calibrando o filtro da razoabilidade: critérios objetivos e subjetivos como fatores de uma análise de risco

O legislador brasileiro procurou talhar uma norma neutra tecnológica[109]. Ao contrário de apontar para uma tecnologia em específico que poderia se tornar obsoleta ao longo do tempo, utilizou-se de um conceito indeterminado – razoabilidade – a ser significado e atualizado pelo próprio desenvolvimento científico. Simultaneamente, contudo, prescreveu balizas para reduzir a discricionariedade de tal exercício interpretativo e, com isso, alcançar um mínimo de previsibilidade quando tal norma viesse a ser colocada em movimento.

O primeiro eixo de análise é objetivo, sendo composto por uma matriz e dois elementos fatoriais respectivamente[110]: a) estado da arte da tecnologia; a.1) custo e; a.2) tempo[111]. Deve-se analisar o quão custoso e moroso seria reverter um processo de anonimização, de acordo com as tecnologias disponíveis para tanto. Trata-se, portanto, de uma análise dinâmica[112], a ser demarcada pelo próprio progresso tecnológico, que aponta qual deve ser o grau de investimento financeiro e temporal para se reidentificar uma base de dados anonimizada.

Por exemplo, há muito tempo se fala e se espera a chegada da computação quântica[113]. Quando isso acontecer, testemunhar-se-á um verdadeiro progresso acerca da capacidade, em termos quantitativos e qualitativos, de processamento de dados. Consequentemente, atualizar-se-á por completo, o custo e o tempo quanto ao emprego das técnicas de anonimização, mas, também, por outro lado, das suas respectivas contra-tecnologias.

Em síntese, o primeiro eixo de análise propõe uma avaliação acerca do grau de *resiliência* de um processo de anonimização frente aos *padrões sociais*. Uma investigação de ordem objetiva cujo

marcador é verificar como o estado da técnica calibra a escala de recursos (custo e tempo) para transmutar um dado anonimizado em dado pessoal.

O segundo eixo de análise é subjetivo. Deve-se levar em consideração quem é o agente de tratamento de dados e se ele dispõe de "meios próprios"[114] para reverter o processo de anonimização. Ao invés de considerar quais são os padrões sociais acerca da reversibilidade de um dado anonimizado, foca-se em analisar qual é a capacidade individual de engenharia reversa de quem processa tais dados. Abrem-se, com isso, dois vetores importantes de análise.

Em primeiro lugar, sob o ponto de vista do fluxo de dados dentro de uma organização. É cada vez mais comum que organizações segmentem as suas bases de dados de acordo com suas respectivas áreas de negócio e, até mesmo em alguns casos, empreguem práticas de anonimização para geração de *business inteligence/BIA*.

Por exemplo, é o caso de uma grande rede de lojas varejistas que decide utilizar a sua base de dados de programa de fidelidade para melhorar o seu sistema de distribuição logística. Uma nova finalidade foi atribuída a um conjunto de dados, não sendo necessário saber quem são seus respetivos consumidores de forma individualizada, mas, tão somente, quais produtos têm mais ou menos entrada e saída de acordo com o perfil de vendas de cada um dos seus estabelecimentos geograficamente espalhados. Dessa forma, é factível a estruturação de uma nova base de dados sem que haja a associação direta ou indireta a indivíduos, podendo ser mantida, inclusive, em separado da outra base de dados (programa de fidelidade) que lhe deu origem.

Nesse cenário, o próprio agente tem informações adicionais, ainda que mantidas separadamente, para reverter o processo de anonimização. Ou seja, ele possui meios próprios para transmutar um dado aparentemente anonimizado em um dado pessoal, o que é revelado com base em uma análise subjetiva focada na sua própria capacidade de entropia de informação[115].

O cenário acima descrito é o que se convencionou chamar de pseudoanonimização, ou seja, uma falsa, superficial, técnica de anonimização, que é quebrável em especial pela própria organização que a empregou.

A primeira reflexão que pode seguir a esse respeito é: por que a organização deveria empregar todo o esforço acima mencionado, se toda a carga regulatória da legislação de proteção de dados ainda assim recairá sobre ela (o dado não deixará de ser pessoal)?

Diferentemente da GDPR, a legislação de proteção de dados pessoais brasileira não sistematizou adequadamente a figura da pseudoanonimização, muito menos desenhou normativamente incentivos expressos para a sua adoção por parte dos agentes de tratamento de dados. Enquanto o regulamento europeu previu até mesmo o relaxamento de algumas obrigações legais[116], a lei geral brasileira de proteção de dados pessoais apenas citou pseudoanonimização de forma assistemática[117].

No entanto, ainda assim, é possível chegar à conclusão de que há sim incentivos, mesmo que indiretos, a serem burilados na lei geral de proteção de dados pessoais. Na medida em que pseudoanonimização é o "meio do caminho"[118] entre um dado pessoal e um dado anonimizado, seria

possível correlacioná-la às diversas menções que a LGPD faz para que os agentes de tratamento "sempre que possível", anonimizem os dados[119]. Isto porque a lógica normativa em questão é encarar o processo de retirada dos identificadores de uma base de dados como algo que minimiza os riscos de uma atividade de tratamento de dados. Esse é exatamente o mote de técnicas de pseudoanonimização, ainda que não retire por completo o caráter pessoal de um dado.

Soma-se, ainda, o fato de que técnicas de pseudoanonimização podem compor o espectro de medidas, políticas e processos de um programa de governança que é referenciado pela LGPD[120]. E, ainda, por ser uma medida tradicional de segurança da informação que pode reduzir significativamente os impactos de um incidente de segurança, a partir da simples constatação de que: a) uma base de dados pseudoanonimizada pode não ser reversível por terceiros-atacantes[121] e; b)certamente, gera menos riscos em relação a uma base de dados comprometida que não tenha havido o emprego de tais medidas.

Por fim, em segundo lugar, ainda quanto ao eixo de análise subjetiva, deve-se considerar o fluxo de dados para fora da organização. Nesse caso, como que terceiros deteriam "meios próprios" para reverter o processo de anonimização dos dados. Trata-se de uma questão particularmente importante no que diz respeito a eventuais parcerias que envolvam o uso compartilhado de dados[122], mesmo que não sejam dados pessoais *a piori*.

Por exemplo, é muito comum que organizações se associem, mediante o compartilhamento e cruzamento de dados, para pesquisas científicas e outras atividades econômicas. Imagine o seguinte cenário:

a) uma pesquisa cujo objetivo é mensurar a eficácia de um determinado tratamento médico;

b) de antemão, reconhece-se ser necessário que a amostra de pessoas deve ser a mais ampl com objetivo de capturar pacientes com características distintas;

c) então, se faz necessária uma análise que envolva um conjunto de hospitais e clínicas médicas que trataram grupos de pacientes com diferentes perfis;

d) também se nota, desde logo, ser desnecessário o compartilhamento das bases de dados brutas (*raw data*), a qual identificaria diretamente cada um dos pacientes;

e) seria necessária apenas a indicação do perfil dos pacientes, os quais seriam agrupados c acordo com características semelhantes sem os tornar identificáveis *a priori*;

f) diversos testes de reidentificação foram executados, a fim de se assegurar e ser certifica a razoabilidade das técnicas de anonimização empregadas que correspondem ao estado atual da arte.

Apesar da situação hipotética descrever um cenário no qual a pesquisa rodaria em cima de uma base de dados anonimizada (critério objetivo – item "e"), isso por si só não encerraria a discussão

acerca dos riscos de reindetificação. Deve-se verificar, ainda, se algum hospital ou clínica participante poderia lançar mão de "meios próprios" capazes de reverter o processo de anonimização da base como um todo. Mais uma vez, entra em cena uma análise subjetiva, que é focada na capacidade de um agente em específico. Pense, por exemplo, que um dos hospitais deteria uma alta capacidade de entropia de informação, em razão de: **a)** deter uma série de informações adicionais por conta sua capilaridade no setor com atendimento à grande parte da população, representada no estudo; **b)** possuir tecnologias de processamento de dados disruptivas, que superam os padrões praticados até então no setor.

Dessa forma, também é relevante observar a capacidade subjetiva de terceiros que ingressem no fluxo informacional de uma organização. Especialmente, quando se tem em vista atividades de enriquecimento de dados que envolvam agentes externos para viabilizar uma atividade de tratamento de dados.

Em síntese, o legislador brasileiro adotou uma estratégia normativa alinhada à premissa de que os dados anonimizados seriam sempre passíveis de reversão. Os dois eixos de análise acima descritos – objetivo e subjetivo – compõem uma matriz de risco[123] em torno de possíveis engenharias reversas de um processo de anonimização. A *resiliência* de tal processo é o que determinará se haverá algum tipo de intersecção entre dados anonimizados e dados pessoais, cujos elementos de análise são de ordem objetiva (razoabilidade) e subjetiva (meios próprios).

2.2.3.2 Exemplificando alguns fatores de risco: os enigmáticos termos "no momento" e "ocasião do tratamento

Em vez de considerar anonimização como algo cujo resultado (*output*) é infalível, foca-se em uma abordagem que considera a aplicação sistemática de técnicas de anonimização com o objetivo de agregar consistência ao processo como um todo[124]. Por essa razão, a análise acerca se um dado deve ser, de fato, considerado como anonimizado é eminentemente *circunstancial*. Os dois critérios de análise – objetivo e subjetivo – acima mencionados ganharão vida somente a partir do contexto no qual está inserida uma atividade de tratamento de dados, sobre a qual se busca retirar, ao máximo, seus respectivos identificadores.

Aliás, não é por outra razão, que a LGPD amarra o conceito de dado anonimizado e anonimização, respectivamente, à "ocasião" e ao "momento" no qual se dá uma atividade de tratamento de dados pessoais. Na medida em que a definição de atividade de tratamento de dados engloba nada mais do que 20 (vinte) ações,[125] tudo o que é feito com um dado, o processo de anonimização deve representar um conjunto de ações contínuo e logicamente ordenado que abrace toda a extensão do ciclo de vida de um dado – da coleta ao descarte.

A título de exemplo, lista-se ao menos 06 (seis) fatores de risco[126] e algumas medidas de mitigação.

a) **Volume dos dados**: quanto maior for a quantidade de dados, maiores são as chances de alguém fazer o caminho inverso de um processo de anonimização. Desta forma, modelos de negócios, produtos ou serviços e, até mesmo, políticas públicas (incluindo de dados abertos) que envolvam grandes massas de dados devem proporcionalmente apresentar técnicas de anonimização correspondentes aos altos riscos de reindentificação em jogo;

b) **Natureza dos dados:** a natureza do dado (e.g., saúde, financeiro, geolocalização etc.) é determinante sobre o quão valiosas são eventuais informações que dele podem ser extraídas. Com isso, o apetite de terceiros e o quão recompensador seria reverter um processo de anonimização impulsionam os seus respectivos riscos de reidentificação;

c) **Cadeia da atividade de tratamento de dados (recipientes, compartilhamento e uso compartilhado)**: em muitas situações, há uma complexa cadeia de atores para viabilizar um modelo de negócio ou mesmo uma política pública. Em regra, quanto maior for o ingresso de entidades para a geração ou mesmo o uso de uma base de dados anonimizada, mais elevado será o rsco de sua reidentificação. Isto porque, não se aumenta apenas o volume do fluxo informacional (item "a"), como, também, a população que dele participa. Por exemplo, no caso acima mencionado relacionado à pesquisa científica, é comum se utilizar dos chamados "recipientes confiáveis". Esses são terceiros no qual organizações, que desejam gerar uma nova base de dados (anonimizado) a partir dos seus bancos de informações, confiam a sua execução. Uma espécie de filtro com relação a quem deteria poder informacional para reverter o processo de anonimização. Nesse caso, o ingresso do terceiro no fluxo informacional se dá justamente para tornar mais resiliente o processo de anonimização.

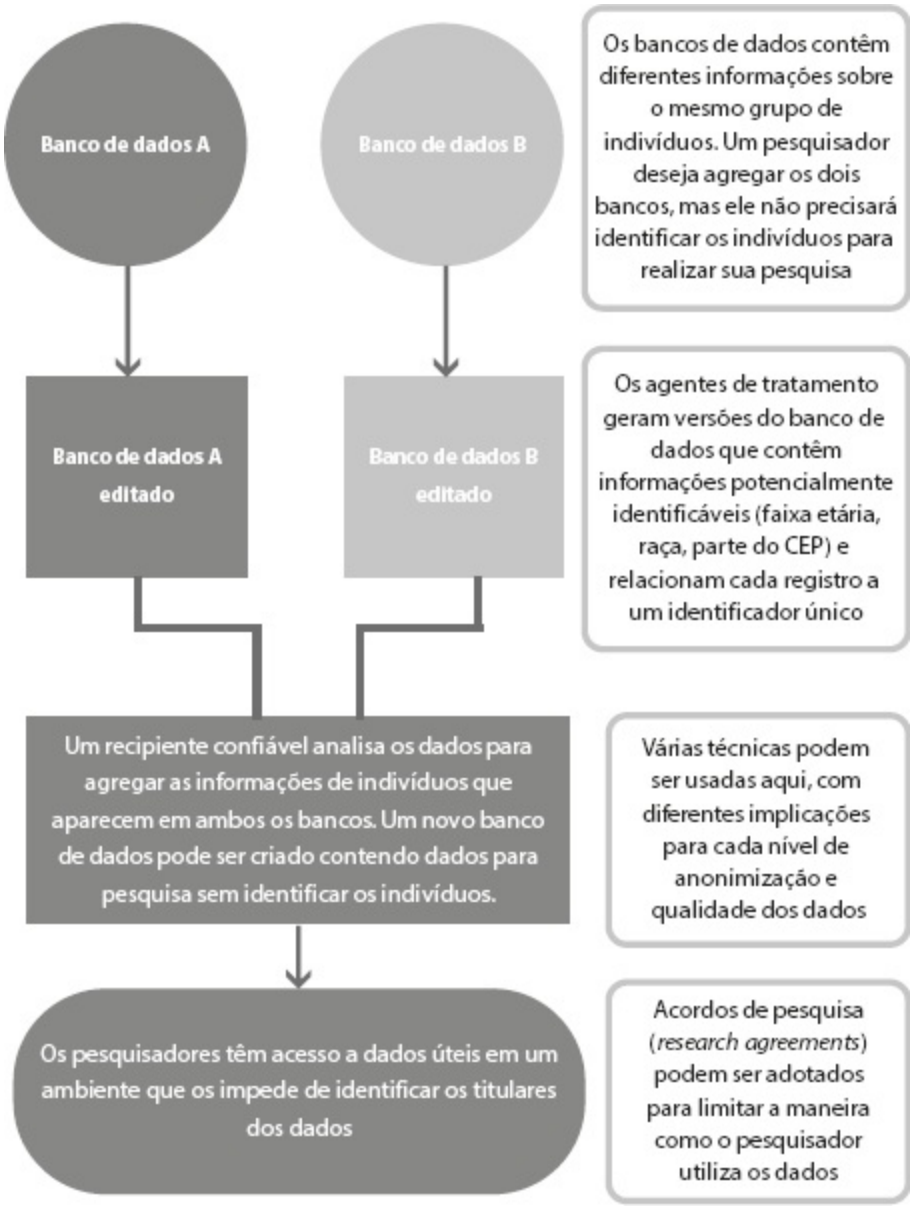


Figura 2
Information Commissioner's Office. Anonymisation: managing data protection risk code of practice. 2012. p.42 (tradução livre). Disponível em: <https://www.dropbox.com/s/alxugfisaocl02u/Anonymisation-managing%20data%20protection%20risk%20code%20of%20practice.pdf?dl=0>.

d) **Gerenciamento de identidades e segmentação**: tão importante quando se colocar em prática processos de pseudoanonimizaçõa, é, também, controlar quem acessa as informações adicionais capazes de revertê-los. Por isso, é o caso de não só segregar fisicamente, mas, também, logicamente as bases de dados de uma organização (vide: exemplo supramencionado sobre uma rede varejista). Dessa forma, os riscos (internos) de reindentificação também passam a ser menores, na medida em que se reduz o número de atores que teria capacidade de juntar as peças do quebra-cabeça para formar a imagem dos titulares da informação. Nesse sentido, é importante destacar que o Decreto do Marco Civil da Internet (Decreto 8.771/2016) já determina a adoção de mecanismos

de gerenciamento de identidade a uma base de dados, inclusive com a previsão de sistemas de autenticação dupla e a individualização do respectivo usuário[127].

e) **Cláusulas contratuais**[128]: na medida em que fluxo informacional envolva cada vez mais agentes, em particular quando há o compartilhamento de dados para extração de informações, com ou sem os chamados "recipientes confiáveis, é cada vez mais comum cláusulas que: **a)** proíbam as partes reverterem o processo de anonimização; **b)** delimitem o papel de cada um dos agentes de tratamento de dados de acordo com o objeto da atividade de tratamento de dados e, adicionalmente, vedando ou o condicionando o repasse a terceiros que executariam tal atividade em nome de uma das partes; **c)** a destruição dos dados tão logo seja concluída a atividade de tratamento de dados ou caso haja a resolução de alguma condição pactuada;

f) **Atualização contínua**: anonimização é algo inacabado e fluído tal como é a própria definição da atividade de tratamento de dados, a qual procura capturar os dados em todos os seus movimentos. Ao expressamente correlacionar o conceito de dado anonimizado e anonimização ao "momento" e de acordo com a "ocasião" na qual um dado está sendo processado, a LGPD procurou deixar claro que as técnicas de anonimização devem considerar toda a jornada de um dado e, sobretudo, ser constantemente atualizadas. Por exemplo, não adiantará um contrato de processamento de dados, que especificou todas as técnicas de anonimização e inclusive a forma pela qual os "recipientes terceiros" as colocariam em prática, se esse contrato foi firmado há bastante tempo e tais medidas já se encontram defasadas. O *continuum* de uma atividade de tratamento de dados, espelhado por nada mais do que 20 (vinte) ações diferentes, também deve nortear a *dinamicidade* com a qual se emprega técnicas de anonimização[129].

Com isso, o legislador convida os agentes de tratamento de dados a conceberem e aplicarem as melhores técnicas de anonimização de acordo com as particularidades das suas respectivas atividades. É uma empreitada multifacetada, de ordem técnica, organizacional e, inclusive, contratual, com o objetivo de controlar os riscos associados à reidentificação de uma determinada atividade de tratamento de dados.

2.2.4 A importância pragmática da alocação dogmática de dados pessoais como um novo direit da personalidade: análise consequencialista

Certa vez, um engenheiro do Google teria dito que eles não coletam informações associadas aos nomes das pessoas, pois isso geraria desinformação – "ruído" nas palavras dele[130]. Em outra oportunidade, o então chefe de assuntos de privacidade do Facebook, Erin Egan, afirmou paradoxalmente que, apesar de a rede social fornecer publicidade com base na identidade dos seus

usuários, isso não significaria que eles sejam pessoas identificáveis[131]. Em uma série de reportagens sobre a técnica de "Privacy Differential" da Apple, a revista *Wired* é provocativa ao dizer, paradoxalmente, que essa técnica "coleta dados sobre você", mas não muito "bem sobre você"[132].

De fato, o modo pelo qual a Internet e outros sistemas funcionam não torna necessário saber-se a identidade do usuário para lhe direcionar um conteúdo, ou, mesmo, sujeitá-lo a um processo de decisão automatizada. Basta lhe atribuir um identificador eletrônico único que permita separá-lo dos milhões de usuários da rede ou do sistema. Por exemplo, em relação ao computador ao qual ele está conectado, o que é feito por meio do número de conexão a ele atribuído (o chamado protocolo de endereço – IP; vide subcapítulo 2.3.2 *infra*)[133]; ou o IMEI de um aparelho celular, também um identificador numérico único atribuído a tal dispositivo[134].

A partir desses identificadores eletrônicos, reconhece-se o dispositivo conectado, o que permite, dentre outras coisas, a memorização dos *logins* e senhas para um acesso mais dinâmico às aplicações da *web, por exemplo*. É dessa maneira que se melhora a experiência do usuário – mantra tão repetido nos diais atuais –, que nada mais é que a formação de um perfil comportamental da sua navegação.

É possível, portanto, compilar um perfil "browsing" (navegação) – vernáculo na língua inglesa que define o ato de "surfar" na Internet –, ainda que não se tenha certeza a respeito do sujeito que pratica tal ação. Pode ser, por exemplo, uma família ou mesmo um conglomerado de funcionários de uma empresa que fazem uso da mesma conexão, o que acaba por tornar difícil o enquadramento de tais dados como aqueles relacionados a uma pessoa identificável.

Se a premissa da causa regulatória da proteção de dados pessoais é tutelar o cidadão, que é cada vez mais exposto a tais tipos de práticas que afetam a sua vida, então, uma compartimentalização "dura" entre dados pessoais e dados anonimizados deixaria de fazer sentido. Em especial, quando está em questão a formação de perfis comportamentais que tem por objetivo precípuo influenciar de alguma forma a vida de uma pessoa, que está atrás de um dispositivo e pouco importa ser ela identificável ou não[135].

Abre-se espaço, assim, para uma escolha normativa *consequencialista*. Não se normatiza apenas pela lente da conceituação mutualmente excludente entre dados pessoais e dados anônimos, mas, também, por meio da relação de causa e efeito que a mera atividade de tratamento de dados pode exercer sobre um indivíduo.

Não se deve perder de vista, portanto, que mesmo o tratamento de dados anonimizados pode repercutir na esfera do livre desenvolvimento da personalidade das pessoas. Algoritmos[136] que mineram dados anonimizados podem esconder práticas discriminatórias em prejuízo de uma coletividade e de pessoas singulares[137].

Esse seria o caso, por exemplo, de uma empresa que considerasse elaborar um processo seletivo de forma anônima dos candidatos[138], mas cujo critério seletivo fosse parametrizado pela mineração dos dados pessoais das características preponderantes daqueles que já integram a sua equipe de colaboradores. Muito provavelmente, o algoritmo de seleção replicaria os vieses já enraizados

naquela organização, tais como questões de gênero e de etnia. Hipoteticamente, mulheres afrodescendentes ou asiáticas com histórico profissional e habilidades semelhantes aos de homens brancos poderiam ter resultados completamente diferentes ao longo do processo seletivo, ainda que uma análise meritória individual dos candidatos sugerisse o contrário.

De maneira bastante sintética, esse é o pano de fundo do debate em torno da agenda de regulação de algoritmos e de inteligência artificial[139]. O desafio está em arquitetar processos de governança[140] que impeçam a ocorrência de efeitos indesejados ao se introjetar tais tecnologias nos circuitos decisórios do nosso cotidiano.

Leis de proteção de dados pessoais compõem necessariamente esse arranjo de governança, na medida em que suas normas abraçam todo e qualquer processamento de dados que sujeite um indivíduo ou uma coletividade a uma decisão automatizada[141]. Pouco importa se tal tratamento se centra em uma informação isolada ou agregada e que não revele uma pessoa direta ou indiretamente (dados anonimizados), desde que ele impacte de forma significativa[142] a sua vida e, portanto, o livre desenvolvimento da sua personalidade.

Daí a importância da alocação da proteção dos dados pessoais como um novo direito da personalidade. Com isso, permite-se um alcance normativo maior, que é capaz de abraçar toda e qualquer atividade de processamento de dados (ainda que não pessoal), mas que impacta a vida de um indivíduo.

Essa é a racionalidade da LGPD ao prever que dados anonimizados podem ser considerados como dados pessoais caso sejam utilizados para a formação de perfis comportamentais (art. 12, § 2º)[143]. O foco está, portanto, nas *consequências* que tal atividade de tratamento de dados pode ter sobre um sujeito.

Muitas vezes, processos de decisões automatizados valem-se desses perfis que não necessariamente identificam uma pessoa em específico, mas um grupo – *grouping*. É pelo fato de ela estar catalogada, inserida, referenciada ou estratificada nesse grupo que uma série de decisões serão tomadas a seu respeito, ainda que sem individualizá-la diretamente *a priori*. Como já apontado no início deste subcapítulo, essa é uma metodologia bastante comum em muitos modelos de negócios que se valem de dados estatísticos de grupos para o direcionamento de conteúdo e publicidade, ainda que não seja possível identificar as pessoas que compõem aquela massa[144].

Por isso, as expressões "determinada pessoa" e "identificada", constantes do referido dispositivo da LGPD, devem ser compreendidas com relação aos desdobramentos que o tratamento de dados pode ter sobre um indivíduo, ao contrário de significá-los com os olhos voltados para a base de dados em si, especificamente se o perfil comportamental pode ser ou não atribuído a uma pessoa em específico. Ou seja, o foco não está no dado, mas no seu uso – para a formação de perfis comportamentais – e sua consequente repercussão na esfera do indivíduo.

Essa é uma interpretação sistemática do artigo supracitado que está em linha com o próprio conceito expansionista de dados pessoais – pessoa identificável e não somente identificada –, bem

como um dos objetivos e fundamentos da própria lei – o livre desenvolvimento da personalidade (arts. 1º e 2º, VII). Não faria sentido, também sob o prisma de uma interpretação teleológica, prever uma exceção pela qual dados anonimizados estariam dentro do escopo da lei, mas que dela não seria possível alcançar situações nas quais um grupo de indivíduos (pessoas identificáveis) tem as suas respectivas liberdades (desenvolvimento da personalidade e direitos fundamentais) afetadas pelo uso de tais dados.

Garante-se, com isso, uma *exegese* que torna o § 2º do art. 12 aplicável e não "letra morta". E, sobretudo, coerente com o conceito de dado pessoal que foi desenhado e é vocacionado para expandir a proteção da pessoa natural com relação às situações nas quais a atividade de tratamento de dados – mesmo anonimizados – afeta o livre desenvolvimento da sua personalidade. Caso contrário, prevalecendo uma interpretação literal do dispositivo em questão, a própria lei e um dos seus fundamentos seriam esvaziados.

Nesse sentido, é importante ressaltar que o dispositivo em específico detinha uma outra redação quando se iniciou o debate no Congresso Nacional. Em vez da expressão "se identificada", constava a locução "ainda que não identificada" no então PLPDP/EXE. Essa investigação histórica do processo legislativo reforça uma interpretação teleológica no sentido de que o parágrafo em questão foi projetado para expandir a proteção da pessoa natural, ainda que o perfil comportamental não a individualize diretamente. Se fosse desejo do legislador não conferir tal proteção, bastaria, em termos de técnica legislativa, suprimir o referido parágrafo.

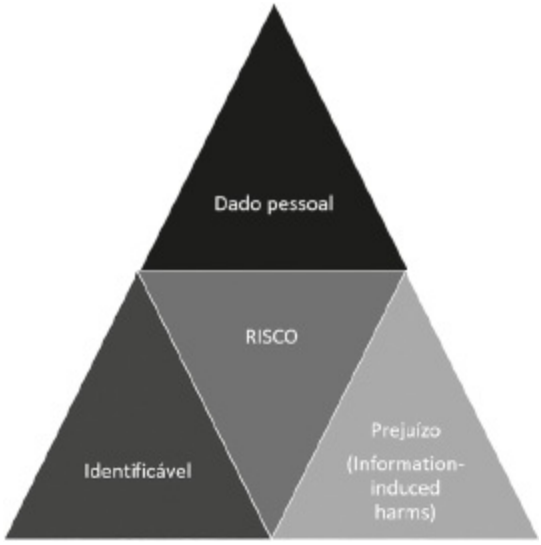
Outro dispositivo que reforça esse tipo de análise é o art. 20 da LGPD[45]. O direito do titular de revisão de decisões automatizadas alcança qualquer tipo de atividade de tratamento automatizado de dados que "afetem seus interesses". Mais uma vez entra em cena uma análise consequencialista que expande o espectro da LGPD. Nesse sentido, não se condiciona o exercício desse direito com base apenas em "perfil" referente a uma "pessoa identificada", mas todos aqueles que se valem de aspectos da sua personalidade *e* que afetem seus interesses. Em síntese, poderia se esquematizar a seguinte disputa interpretativa a esse respeito:

ART. 12 PL/EXE	ART. 12 DA LGPD	ART. 20 DA LGPD	ART. 5, I DA LGPD	ART. 2º, VIII DA LGPD
§ 1º Poderão ser igualmente considerados como dados pessoais para os fins desta Lei os dados utilizados para a formação do perfil comportamental de uma determinada pessoa natural, **ainda que não identificada**.	§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.	O titular dos dados tem direito a solicitar a revisão de **decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses**, incluídas as decisões destinadas a definir o seu **perfil pessoal**, profissional, de consumo e de crédito ou os **aspectos de sua personalidade**.	Dado relacionado à pessoa natural **identificada ou identificável**	VII - os direitos humanos, o **livre desenvolvimento da personalidade**, a dignidade e o exercício da cidadania pelas pessoas naturais.
Expande	**Restringe**	**Expande**	**Expande**	**Expande**
A PROTEÇÃO DA PESSOA NATURAL				

A conjunção aditiva "e" é de extrema importância. O alargamento do espectro da LGPD também não pode torná-la uma esponja que sugue todo e qualquer tipo de dado, bem como toda e qualquer extração de informação para fins de formação de perfil comportamental para dentro do seu escopo de aplicação. Em vez de esvaziá-la, esse tipo de interpretação a inundaria, tornando-a, em última análise, a lei de "tudo"[146] no contexto de uma sociedade e economia movida por dados.

A ensaiada *análise consequencialista* do conceito de dado pessoal tem como gargalo as hipóteses nas quais o tratamento de dados pode ocasionar efeitos negativos sobre uma pessoa ou um grupo de pessoas. Dito de outra forma, a mesma mola que a alarga é a que lhe contrai: o livre desenvolvimento da personalidade e a proteção de liberdades fundamentais.

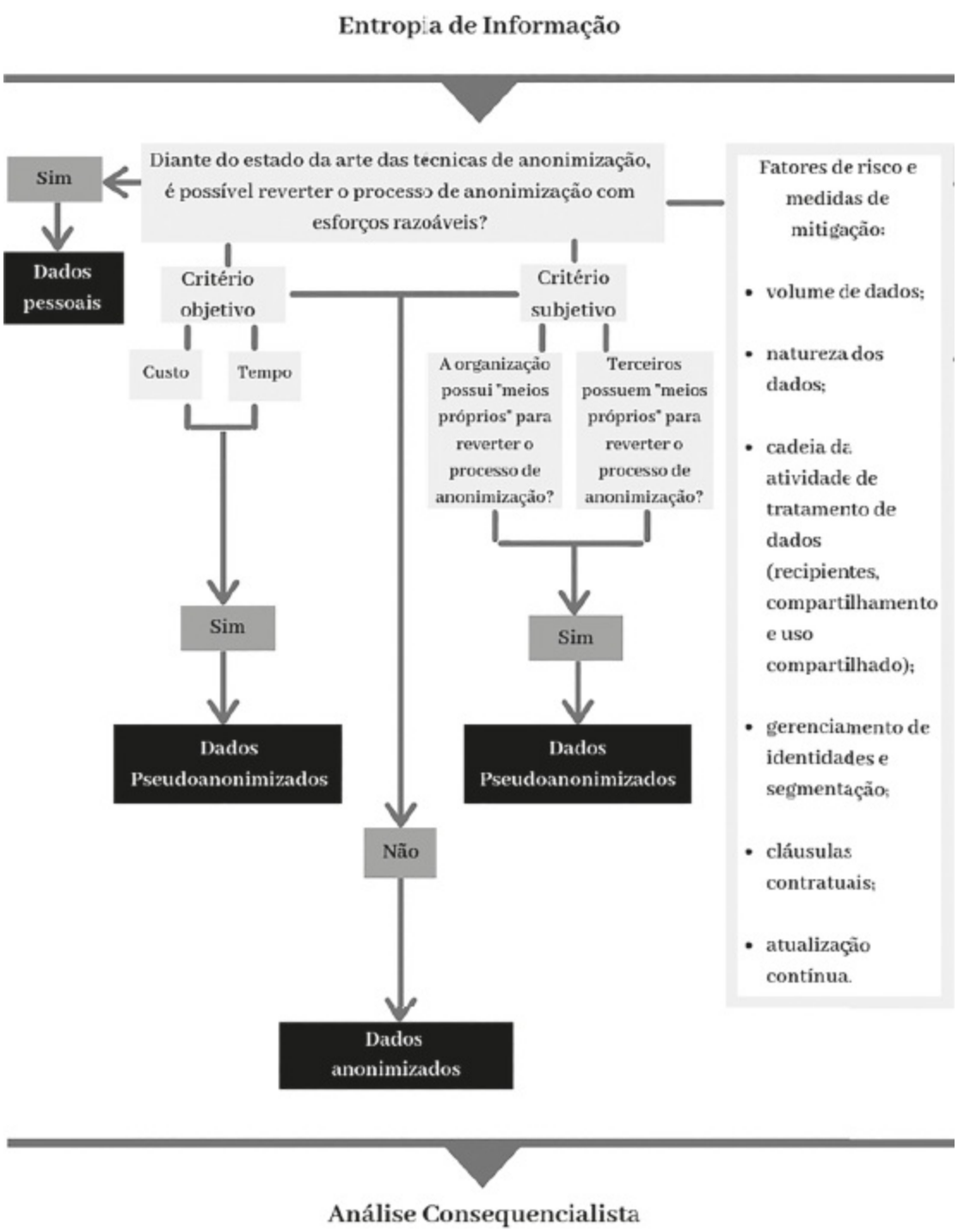
Verifica-se, portanto, que a empreitada normativa da proteção dos dados pessoais passa necessariamente pela *construção dogmática* do seu enlace com os direitos da personalidade. Isso faz que sejam revisitados e atualizados: **i)** o próprio conceito de direitos da personalidade; **ii)** o que pode ser considerado como projeção ou prolongamento da pessoa natural; **iii)** mais especificamente, um conceito de dado pessoal que leva em consideração não apenas os riscos: iiia.) de uma pessoa ser visível (indetificável) em uma base de dados; iii.b), mas, também, os prejuízos decorrentes de uma atividade de tratamento de dados sobre um indivíduo.. Uma matriz de risco que complementa a anterior, focando-se não apenas no grau de identificabilidade de um dado, mas, também, acerca dos efeitos coletareis de uma atividade de tratamento de dados a ser experimentado por um indivíduo[147]:



Com isso, facilita-se, dentre outras coisas, a percepção de que o tratamento de dados – sejam eles anônimos ou pessoais – que submeta uma coletividade ou uma pessoa a processos de decisões automatizadas deve estar dentro do escopo normativo da proteção dos dados pessoais. Essa é uma chave de leitura essencial para a compreensão da matéria na cultura jurídico-legal brasileira e dos desafios regulatórios de uma sociedade e uma economia cada vez mais movidas por dados.

2.2.5 Modelo analítico de dado pessoal

a análise acerca se a natureza de um dado pessoal, submetido a um processo de anonimização, pode ser transmutada envolve uma série de elementos. O teste abaixo agrupa logicamente os 07 (sete) critérios normativos prescritos pela própria LGPD e, ainda, lista, paralelamente, uma série de fatores, com base na literatura revisada, que ajudam na identificação do quão tolerável (razoável) são riscos de reversão das técnicas de anonimização aplicadas.



2.3 O DESENVOLVIMENTO DA PERSONALIDADE POR MEIO DO FLUXO INFORMATIVO

Para além da perspectiva subjetiva de que cada ser humano detém seus prolongamentos – atributos e características próprias que o tornam singular –, encaixam-se os dados pessoais como um elemento que compõe essa singularidade. Não se pode perder de vista que todo esse desenho só tem razão de ser porque a pessoa é um ser eminentemente social. A sua singularidade-subjetividade aperfeiçoa-se na social-intersubjetividade[148].

Em outros termos, se não houvesse o social não se justificaria o singular, pois é no meio coletivo

que se faz possível considerar e identificar o "eu" – individual – frente aos outros – multidão. Portanto, tais ideias são condicionadas transcendentalmente uma pela outra[149].

Daí por que pensar em direitos da personalidade não é uma reflexão sob uma categoria jurídica assentada em uma *solidão ôntica*, mas, sobretudo, uma *concepção ontológica* da pessoa humana. Como bem traçado por Diogo Costa Gonçalves[150], a pessoa se concretiza quando ela se relaciona (intersubjetividade)[151], isto é, quando ela responde ou procura afirmar quem ela é em meio à comunidade[152].

A noção completa dos direitos da personalidade liga-se necessariamente à tutela jurídica para que a pessoa possa se realizar e se relacionar junto à sociedade, completando justamente a locução, antes mencionada, *projeção social*.

Do contrário, haveria uma visão míope do que é tal categoria jurídica que deve compreender as atividades de inter-relacionamento da pessoa[153]. O ser humano não é uma ilha, ele se conforma e se desenvolve quando se relaciona com os demais "no seio da sociedade que o abriga"[154].

Nesse sentido, os dados pessoais não só se caracterizam como um prolongamento da pessoa (subjetividade), mas, também, influenciam essa perspectiva relacional da pessoa (intersubjetividade). A proteção dos dados pessoais é instrumental para que a pessoa possa livremente desenvolver a sua personalidade[155].

Neste capítulo, procurar-se-á, então, discorrer sobre a importância da tutela jurídica dos dados pessoais na dimensão relacional[156] da pessoa, mostrando-se como tal direito de personalidade é crítico para que a pessoa não seja discriminada e não tenha, por fim, a sua própria liberdade afetada.

A proteção de dados pessoais situa-se entre os direitos da personalidade, pois, também, interfere na dimensão relacional e social do ser humano.

2.3.1 Dados sensíveis e o tratamento sensível de dados triviais: a interface com o direito de isonomia e não discriminação

Os dados sensíveis são uma espécie[157] de dados pessoais que compreendem uma tipologia[158] diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação[159].

Quando se pensa em dados que exprimem a orientação sexual, religiosa, política, racial, estado de saúde ou filiação sindical[160], surge a preocupação em haver distinção ou diferenciação de uma pessoa por conta de tais aspectos da sua personalidade[161].

Ainda que, assim como um dado anônimo pode se tornar um dado pessoal, um dado "trivial" pode também se transmudar em um dado sensível[162]; particularmente, quando se têm disponíveis tecnologias (*e.g., Big Data*) que permitem correlacionar uma série de dados para prever comportamentos e acontecimentos, tal como ocorreu com a loja de departamentos que identificou quais consumidoras estariam grávidas, precisando, inclusive, o período gestacional.

É possível, portanto, identificar individualidades mais sensíveis das pessoas, tais como orientação sexual, raça e estado de saúde[163], a partir de informações triviais[164].

A título de exemplo, segundo um estudo da Universidade de Cambridge, as "curtidas" em uma rede social podem criar um retrato fiel dos gostos e preferências dos usuários por meio do qual poderiam ser extraídos diversos tipos de inferências. A pesquisa identificou com exatidão a porcentagem dos usuários homossexuais e heterossexuais, os usuários brancos e negros e, por fim, quais teriam uma ligação partidária republicana ou democrata[165].

O mesmo pode suceder com outros "registros digitais", tais como o histórico de navegação, os termos de pesquisa ou mesmo as compras realizadas por um consumidor. Todos esses dados têm o potencial de revelar muitos atributos da personalidade de um indivíduo, dentre os quais informações sensíveis a seu respeito[166].

Por tal razão, a proteção dos dados pessoais perpassa a própria tutela do princípio da isonomia[167], na medida em que é um instrumento de contenção às práticas discriminatórias.

Exatamente por esse motivo leis de proteção de dados pessoas, incluindo a brasileira, dedicam um regime jurídico mais protetivo em relação a dados sensíveis com o intuito de frear práticas discriminatórias[168].

Tal tutela jurídica procura assegurar que o titular dos dados pessoais possa se relacionar e se realizar perante a sociedade, sem que eventuais práticas frustrem tal projeto.

Com isso, pretende-se garantir a ausência de traços diferenciais nas relações sociais, a fim de possibilitar que o indivíduo desenvolva livremente a sua personalidade. Em última análise, a proteção dos dados pessoais tem um papel de fundamental importância para que o indivíduo *se realize e se relacione* na sociedade, o que é um traço marcante dos direitos da personalidade[169].

2.3.2 "Datificação" das nossas vidas: Internet das coisas e o IPV6

A característica da ubiquidade[170] da Internet já foi apontada quando se teceram considerações a respeito do crescimento exponencial dos *smartphones* (a onipresença do ambiente virtual). É nesse contexto que surge o chamado fenômeno da datificação[171]: o ato de datificar – pôr em dados – praticamente toda a vida de uma pessoa.

Para além do telefone celular, espera-se que os mais diversos objetos estejam conectados à Internet. É a chamada Internet das coisas – Internet of Things/IOT –, que é decorrência, em certa medida, da tecnologia RFID[172] desenvolvida pelo Massachusetts Institute of Technology/MIT, por meio da qual quaisquer aparelhos do dia a dia do indivíduo estariam conectados por um sistema de radiofrequência[173].

Com tal infraestrutura, permitir-se-á, por exemplo: **i)** uma geladeira verificar quais são os alimentos faltantes para encomendá-los, automaticamente, no *site* de compras de um supermercado[174]; **ii)** o despertador avisar a cafeteira para iniciar o preparo do café, fervendo a água para que o sujeito possa ficar mais alguns minutos em sua cama[175]; **iii**) que o seu tênis se conecte com outro dispositivo para registrar suas performances e até elaborar novos treinos, como já se verifica da parceria firmada entre Nike e Apple[176]; **iv)** um marca-passo registrar todo o ritmo cardíaco de um implantado,

o que possibilitará diagnósticos e prognósticos mais precisos; **v)** automóveis transmitirem os dados de seu deslocamento para um melhor gerenciamento das rotas de tráfego.

A chegada do IPV6[177] é o que viabilizará essa conectividade das coisas dado o aumento exponencial nos números de protocolos de comunicação necessários para aperfeiçoar o envio e o recebimento desse oceano de dados através da Internet[178].

A realidade[179] da Internet das coisas consolida, pois, o fenômeno da datificação[180]. Nessa era, tudo ao redor do mundo *off-line* tende a ser *integrado* ao mundo *on-line*, produzindo-se mais dados.

Revitaliza-se, em última análise, a própria ideia de vigilância. Antes tomada e associada neste trabalho a partir do histórico de navegação e dos rastros deixados no mundo *on-line*, agora é transposta para o mundo físico por meio das coisas e objetos presentes no cotidiano do ser humano. Ela se torna mais intrusiva e opaca[181].

Interessa, contudo, para fins do presente trabalho, que esse novo cenário aumentará exponencialmente a coleta de dados pessoais[182], agregando-se mais informações relativas, por exemplo, aos hábitos alimentares, rotinas de exercícios físicos e muitos outros atributos da personalidade dos indivíduos[183]. O ser humano terá um prolongamento e projeção completa no ambiente digital, sendo todas as suas individualidades datificadas. Problematiza-se, mais ainda, o desafio da tutela dos dados pessoais como um novo direito da personalidade, já que muitos aspectos da vida de uma pessoa poderão ser decididos a partir dessa sua extensão eletrônica.

2.3.3 "Ditadura dos dados" e *profiling*: estigmatização do ser humano e os seus reflexos na su esfera relacional e nas liberdades fundamentais

Decorrência do fenômeno da datificação é a existência, na feliz expressão de Daniel J. Solove[184], de uma *biografia digital*, o que não deixa de ser um resultado lógico e esperado do prolongamento da pessoa por meio de seus dados.

Importa considerar, no entanto, que, para além dessa captação em *bits* do ser humano, há a sua classificação e segmentação com base em tais informações. Criam-se, ao final, verdadeiros estereótipos[185] que *estigmatizam* um sujeito perante os seus pares. Esse fator é determinante para calibrar uma série de decisões que influencia o rumo de suas próprias vidas.

Decisões automatizadas com base em tais estereótipos das pessoas já são uma realidade, sendo, inclusive, objeto de abordagem expressa da diretiva da União Europeia de proteção dos dados pessoais[186], tal como da LGPD.

Exemplos não faltam, valendo-se, mais uma vez, do raciocínio dedutivo. Processos seletivos na área de recursos humanos[187-188], para a concessão de crédito[189], para a estipulação de prêmios nos contratos securitários[190] e até mesmo o risco de não embarcar em um avião, porque seus hábitos alimentares podem ser coincidentes com o perfil de um terrorista[191]. Essas são amostras de que a categorização da pessoa, a partir de seus dados pessoais, pode repercutir nas suas *oportunidades sociais*, no contexto de uma sociedade e uma economia movidas por dados.

Por exemplo, o próprio ato de consumo pode ser modelado com base no histórico de compras. Por meio dele, cria-se um perfil do consumidor[192] para direcionar preços de acordo com a sua respectiva capacidade econômica (*price-discrimination*)[193].

É a prática conhecida como *profiling*[194], em que os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões. Tudo é calibrado com base nesses estereótipos; inclusive, o próprio conteúdo acessado na Internet. Na famosa expressão de Eli Pariser, há uma bolha que, como um filtro invisível[195], direciona desde a própria interação do usuário com outras pessoas em uma rede social até o acesso e a busca por informação na rede. Doutrina-se[196] a pessoa com um conteúdo e uma informação que giram em torno dos interesses inferidos por intermédio dos seus dados, formando-se uma bolha que impossibilita o contato com informações diferentes, ocasionais e fortuitas, que escapariam dessa catalogação.

A conjugação dessas diversas variáveis evidencia que a proteção dos dados pessoais tangencia o próprio rumo da vida[197] das pessoas, perpassando, transversalmente, os seus mais variados contatos sociais. Desde a celebração de contratos e o ato do consumo à – até mesmo – busca pelo acesso à informação.

De acordo com Mayer-Schoneberger, há uma espécie de "ditadura" dos dados[198]. Seus titulares – as pessoas datificadas – seriam as potenciais vítimas dessa estrutura em que os dados atropelam a pessoa de carne e osso. No contexto do *Big Data*, são os algoritmos que passam a orquestrar[199] as vidas dessas pessoas, decidindo a respeito das suas oportunidades.

A tutela jurídica dos dados pessoais é um imperativo que impõe uma nova fronteira aos direitos da personalidade, a fim de que o fluxo informacional não seja corrosivo à esfera relacional da pessoa humana[200] e, por tabela, ao livre desenvolvimento de sua personalidade[201]. Por isso, o direito à proteção dos dados pessoais reclama uma normatização própria que não pode ser reduzida a uma mera "evolução" do direito à privacidade, mas encarada como um novo direito da personalidade que percorre, dentre outras liberdades e garantias fundamentais, a liberdade de expressão, de acesso à informação e de não discriminação. Em última análise, trata-se da nossa própria capacidade de autodeterminação.

2.4 A PROTEÇÃO DOS DADOS COMO CATEGORIA AUTÔNOMA DOS DIREITOS DA PERSONALIDADE: ROMPENDO COM A DICOTOMIA DO PÚBLICO E PRIVADO

Neste subcapítulo, complementar-se-ão as considerações traçadas anteriormente sobre a inserção da proteção dos dados pessoais como um novo direito da personalidade, enfrentando-se posições que o alocam como uma evolução do direito à privacidade e não como uma categoria autônoma.

Levar-se-á em consideração principalmente a doutrina de Stefano Rodotà, que foi um dos

percussores na temática em torno da proteção de dados pessoais. O jurista italiano exerceu não só grande influência no continente europeu, mas, igualmente, no cenário nacional, diante do que foi desenvolvido a respeito do tema até os dias de hoje[202].

2.4.1 Estabelecendo um diálogo entre o direito à privacidade (liberdade negativa) e à proteçã dos dados pessoais (liberdade positiva)

O direito à privacidade tem sido historicamente articulado com base na dicotomia entre as esferas pública e privada[203]. Sempre esteve em perspectiva a demarcação de atividades que deveriam ser desempenhadas privativamente ou em público *vis-à-vis*.

A habitação privada (casa) estabeleceria os contornos dessa dicotomia, sendo, por excelência, o espaço para que as pessoas se refugiassem do escrutínio público[204]. Isso é simbolizado a partir da metáfora de que o indivíduo tem a faculdade de se afastar da multidão (espaço público) para se recolher ao seu castelo (espaço privado)[205].

Seria na esfera privada que as pessoas refletiriam e pensariam criticamente para voltar a público e discutir os mais variados assuntos. Esse refúgio evitaria que os indivíduos sofressem um nivelamento[206] social e, em última análise, a instalação[207] de visões totalitárias[208].

Portanto, o direito à privacidade é basilar à própria democracia[209] e, ao mesmo tempo, condição essencial ao livre desenvolvimento da personalidade dos cidadãos. Somente com a fuga da "pressão social", os indivíduos conseguiriam desenvolver cada qual a sua subjetividade[210] para, posteriormente, projetá-la em meio à sociedade.

Como observa Hannah Arendt, lançando luz sobre o prefixo *idion* de indivíduo, a vida em absoluta *privatividade* ou em total escrutínio público seria idiota[211]. Os fatos que contornam a individualidade de cada ser humano devem ser compartilhados de acordo com as suas respectivas opções[212] para que ele revele e desenvolva a sua personalidade[213].

A teoria das esferas[214] sublinha essa *revelação seletiva* de informações por parte de cada indivíduo. Segredo, intimidade ou vida privada são as esferas que, com maior ou menor grau de intensidade[215], procuram delimitar os espaços da vida privada e pública.

Por exemplo, informações que são compartilhadas entre amigos – esfera da vida privada ou mesmo intimidade – não são divulgadas indiscriminadamente ao público. Ainda que fatos da vida privada sejam compartilhados com outrem, eles permanecem na esfera privada ao se considerar que um número maior ou menor de pessoas – mas não o público em geral – saberá de determinadas particularidades.

É nesse sentido que se compreende a privacidade como o direito de ser deixado só[216], estar a salvo de interferências alheias, do segredo ou sigilo que são direitos calibrados pela dicotomia das esferas pública e privada. A pessoa tem o direito de *retrair* aspectos de sua vida do domínio público[217].

O artigo seminal *right to privacy* está inserto nesse contexto. Seus autores, os advogados

Brandeis e Warren, não queriam que fatos das suas vidas fossem retratados pela imprensa americana[218]. Não seria a curiosidade do público que romperia as portas impenetráveis do castelo da privacidade[219].

O comando de que a vida privada é inviolável[220] resulta dessa *rivalização* entre as esferas do público e do privado. A casa, a correspondência e as comunicações dos indivíduos são claras hipóteses de espaços da vida privada que angariaram dispositivos constitucionais autônomos para tutelar a sua inviolabilidade[221].

O que é público e privado[222] é o que normatiza[223] o conteúdo do direito à privacidade, sendo a sua lógica centrada na *liberdade negativa* de o indivíduo não sofrer interferência alheia.

A definição do que venha a ser privado é difícil de ser estabelecida afora os casos supracitados (domicílio, correspondência e comunicação). Por isso, privacidade tem sido considerada uma palavra-camaleão[224] ou um termo guarda-chuva[225] cuja conceituação é obscura[226], de definição improvável ou impossível[227].

Não se pretende (re)elaborar o conceito de privacidade, mas, tão somente, resgatar a *chave de leitura* de que é um direito permeado pela dicotomia entre o público e o privado e encarado como uma liberdade negativa. Um direito *estático* à espera de que o seu titular delimite quais fatos da sua vida deveriam ser excluídos do domínio público[228].

Por outro lado, a "evolução"[229] do direito à privacidade, que englobaria o direito à proteção de dados pessoais, consistiria em uma proteção *dinâmica*[230] e em uma *liberdade positiva*[231] do controle sobre as informações pessoais.

A *esfera privada* não seria algo já posto à espera de uma violação, mas um espaço a ser construído[232] *a posteriori*[233] e dinamicamente mediante o controle das informações pessoais[234]. Haveria, por isso, uma mudança qualitativa[235] representada pela transposição do eixo antes focado no trinômio "pessoa-informação-sigilo" ao eixo agora composto por quatro elementos – "pessoa-informação-circulação-controle"[236].

Com isso, a noção tradicional de privacidade deveria conviver[237] com essa sua nova dimensão[238]. Deveria haver um intercâmbio entre as tutelas estática e dinâmica do direito à privacidade[239], o que, no entanto, não significa que o direito à proteção dos dados pessoais deveria ser reduzido a uma mera evolução do direito à privacidade.

O direito à proteção de dados pessoais angaria autonomia própria. É um novo direito da personalidade que não pode ser amarrado a uma categoria específica, em particular ao direito à privacidade. Pelo contrário, demanda-se uma correspondente *ampliação normativa*[240] que clareie e não empole a sua tutela.

A própria intelecção do objeto jurídico em questão não é conduzida pela dicotomia entre público e privado. Toda a sua construção é balizada pelo conceito de dado pessoal, o que pode ser vis-à-vis uma informação pública ou privada (vide subcapítulo 2.2.2)[241].

Por exemplo, fatos públicos, que *a priori* não gerariam preocupação atinente à vida privada[242],

podem, quando agregados a outros fatos (dados), revelar detalhes precisos sobre a personalidade de um indivíduo. O mesmo com relação à agregação de dados triviais que permite a extração de informações sensíveis e, portanto, mais intrusivas dos indivíduos.

A dinâmica de proteção dos dados pessoais foge à dicotomia do público e do privado, diferenciando-se substancialmente do direito à privacidade. Propugnar que o direito à proteção dos dados pessoais seria uma mera evolução do direito à privacidade é uma *construção dogmática falha* que dificulta a sua compreensão.

É um direito que opera fora da lógica binária do público e do privado[243], bastando que a informação esteja atrelada a uma pessoa – conceito de dado pessoal – para deflagrá-lo.

Nesse sentido, os direitos de acesso e retificação transitam na esfera pública e não na privada, na medida em que se busca apenas tutelar que o dado pessoal projete fidedignamente o seu titular.

Além disso, observa-se que cada vez mais a atividade de tratamento de dados impacta a vida das pessoas, em particular quando elas são submetidas a processos de decisões automatizadas que irão definir seu próprio futuro. Nesse contexto, o direito à proteção de dados pessoais tutela a própria dimensão relacional da pessoa humana, em especial para que tais decisões não ocasionem práticas discriminatórias, o que extrapola e muito o âmbito da tutela do direito à privacidade[244].

Há, portanto, uma série de liberdades individuais, atreladas ao direito à proteção dos dados pessoais, que não são abraçadas pelo direito à privacidade. Além disso, o centro gravitacional[245] da proteção dos dados pessoais é diferente do direito à privacidade – *i.e.*, a percepção de que a sua tutela jurídica opera fora da dicotomia do público e do privado.

O direito à proteção dos dados pessoais deve ser alocado como uma nova espécie do rol aberto dos direitos da personalidade[246], dando elasticidade à cláusula geral da tutela da pessoa humana[247]. Caso contrário, corre-se o risco de ele não se desprender das amarras conceituais e da dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana[248].

A sociedade da informação imprime uma nova dinâmica e novos desafios para a proteção da pessoa humana, a começar pela monetização dos seus dados pessoais. Tais dados, além de consolidar uma nova forma de prolongamento da pessoa, passam a interferir em sua própria esfera relacional, reclamando, por isso, uma normatização específica[249] que justifica dogmaticamente a autonomia do direito à proteção dos dados pessoais e os desdobramentos da sua tutela jurídica (*e.g.*, direito de acesso e retificação dos dados e oposição a decisões automatizadas, em especial de práticas discriminatórias).

2.4.2 A decisão da Corte Constitucional alemã: Lei do Censo de 1983

A Lei do Censo alemã (*Volkszählunsgesetz*) de 1983 determinou que os cidadãos fornecessem uma série de dados pessoais para mensurar estatisticamente a distribuição espacial e geográfica da população[250].

A referida lei previa, contudo, a possibilidade de que os dados coletados fossem cruzados com outros registros públicos para a finalidade genérica de execução de "atividades administrativas"[251].

Tal vagueza e amplitude da lei de recenseamento foi o estopim para uma série de reclamações perante o Tribunal Constitucional alemão, que declarou a sua inconstitucionalidade parcial. A Corte alemã considerou que eventual compartilhamento dos dados coletados deveria se destinar única e exclusivamente para a finalidade de recenseamento (estatística)[252].

A relevância do julgado destaca-se por sua *ratio decidendi* sob dois aspectos: **a)** a proteção dos dados pessoais como um direito de personalidade autônomo e a compreensão do termo autodeterminação informacional para além do consentimento; **b)** a função e os limites do consentimento do titular dos dados.

Pretende-se, na verdade, fazer uma *releitura* de tal julgado paradigmático, constando eventuais pontos da sua fundamentação que nos ajude a responder à pergunta central deste livro.

Na primeira parte do julgado, estabelece-se a importante construção de que o cidadão deve ter o controle sobre os seus dados pessoais, a fim de que ele possa autodeterminar as suas informações pessoais. Cunha-se, então, a expressão "autodeterminação informacional ou autodeterminação informativa"[253].

Para além dessa relevância terminológica, o julgado desenvolveu um direito autônomo[254] e destacado do direito à privacidade para chegar à conclusão de inconstitucionalidade parcial da lei de recenseamento.

Nesse sentido, as considerações iniciais do julgado são de contumaz importância, na medida em que contextualizam como o avanço tecnológico e, principalmente, o progresso qualitativo na organização das informações impactaram significativamente as liberdades individuais[255].

Baseado em tal premissa, o Tribunal Constitucional alemão delineia o direito da autodeterminação informacional, valendo-se do direito geral da personalidade[256]. A capacidade do indivíduo de autodeterminar seus dados pessoais seria parcela fundamental do seu direito em livremente desenvolver sua personalidade.

Por tal razão, o Tribunal Constitucional alemão argumenta recorrentemente que a atividade de processamento dos dados pessoais deve ter limites, impondo-se "precauções organizacionais e processuais que combatam o perigo de uma violação do direito da personalidade"[257]. Portanto, não só considerando o consentimento como desdobramento desse novo direito da personalidade.

Assim, o Tribunal Constitucional não recorre ao discurso do que é público ou privado para criar o direito à autodeterminação informacional (vide subcapítulo 2.4.1 *supra*). Ao revés, a sua fundamentação acaba por transpor tal dicotomia, na medida em que estabelece que o uso das informações pessoais não deve afetar o desenvolvimento da personalidade das pessoas. Para tanto, o controle exercido pelo cidadão sobre seus dados seria de fundamental importância, bem como a prevenção de práticas de discriminação social[258].

Deslocou-se, por exemplo, a discussão sobre se um dado é sensível ou se esconderia algo íntimo

da pessoa[259] para se considerar que qualquer dado pessoal pode angariar um efeito lesivo e, daí, então, dar ênfase na garantia de que os dados pessoais fossem anonimizados[260], bem como que o seu uso fosse restrito às finalidades estatísticas[261].

Portanto, o julgado é paradigmático na construção de um direito autônomo da personalidade relativo à proteção dos dados pessoais, o qual avança na compreensão de que a sua dinâmica se afasta da dicotomia entre público e privado.

Ao atestar tal afirmação, recorre-se à comparação da fundamentação do julgado sob análise (Lei do Recenseamento de 1983) frente a uma decisão pretérita da própria Corte Constitucional alemã (Lei do Microcenso de 1957). Nessa última, a *ratio decidendi* centrou-se, diferentemente, na argumentação de que os dados pessoais coletados não deveriam atingir a esfera íntima dos cidadãos para daí, então, estabelecer a proteção de seus dados pessoais[262].

Por isso, a fundamentação construída pelo julgado sob análise – Lei do Recenseamento de 1983 – é paradigmática ao não tomar a proteção dos dados pessoais como uma evolução do direito à privacidade. Pelo contrário, tratá-lo como um direito de personalidade autônomo que reclama uma técnica de proteção desconectada da dicotomia entre público e privado.

Deriva daí, portanto, o primeiro aspecto relevante da releitura do julgado da Corte Constitucional alemã, em razão da construção dogmática da proteção dos dados pessoais como um direito de personalidade autônomo. Tal aspecto se não é por vezes omitido, não angaria, ao menos, o merecido destaque por parcela da doutrina que estabelece a proteção dos dados pessoais como uma evolução do direito à privacidade.

Outro ponto a ser explorado na releitura do julgado diz respeito à ênfase de que os dados coletados dos cidadãos alemães fossem anonimizados e não utilizados para outra finalidade que não a estatística. Por se tratar de uma lei de recenseamento, era obrigatório o fornecimento de dados, não havendo a opção de recusa.

Por isso, a ressalva de que se deveria garantir que o uso dos dados fosse restrito às finalidades estatísticas independentemente do consentimento dos seus titulares em sentido contrário. E, nesse sentido, tornava-se ainda mais relevante que o Estado coletasse somente o que fosse realmente necessário[263].

Ainda que se reconhecesse que o levantamento de dados estatísticos adquire múltiplas funções (*e.g.*, densidade demográfica, espacial, geográfica etc.), no entanto, não autorizava o seu uso ou transmissão para outra finalidade que não o recenseamento[264].

O que se extrai do julgado não é só a construção do princípio da especificação dos propósitos[265] que orienta e limita a coleta e a utilização dos dados pessoais (finalidade estatística), mas, sobretudo, a sua prevalência em um contexto no qual o consentimento dos titulares de dados pessoais não teve um papel de protagonismo. Caso contrário, a pessoa poderia ser transformada em um "objeto de informação" decorrente da sua relação de assimetria de poder para com o Estado[266].

Não raras vezes a terminologia "autodeterminação informacional" implica a interpretação

equivocada de que o consentimento do titular dos dados pessoais teria primazia e prevalência na proteção dos dados pessoais, a fim de que, justamente, o sujeito autodeterminasse as suas informações pessoais[267].

A título de exemplo, essa parece ser a análise procedida por Viktor Mayer-Schoneberger[268], que não sopesa a terminologia inaugurada com a própria *ratio decidendi* da Corte Constitucional alemã. O referido autor identifica o direito de controle sobre os dados pessoais, mas não considera o limite a ele imposto por tal decisão, qual seja, que a coleta e o uso dos dados deveriam se restringir à finalidade de recenseamento.

Do contrário, como adverte a própria decisão da Corte Constitucional alemã, desproteger-se-iam os dados pessoais provenientes de uma prática pouco ou nada transparente que feriria a confiança[269] dos cidadãos alemães com relação ao *contexto* da coleta dos dados pessoais – *i.e.*, estatística.

A conclusão que se extrai da releitura do julgado é de que o consentimento poderia servir às avessas para a desproteção dos dados pessoais, na medida em que tornaria ilimitada a coleta e o processamento dos dados pessoais, tornando a pessoa, intermediada por seus dados, um objeto a ser ilimitadamente explorado.

A releitura do julgado impõe, portanto, não só reconsiderar a proteção dos dados pessoais como uma evolução do direito à privacidade, como, também, o próprio protagonismo do consentimento do titular dos dados pessoais. Este último aspecto é de suma importância para a exata compreensão do conteúdo da autodeterminação informacional, bem como para a sua própria reavaliação dentro do quadro normativo da proteção dos dados pessoais (Parte II *infra*).

2.5 CONCLUSÃO: AUTODETERMINAÇÃO INFORMACIONAL E A DUPLA FUNÇÃO D LEIS DE PROTEÇÃO DE DADOS PESSOAIS

É comum a afirmação de que os dados pessoais são o petróleo[270], insumo[271] ou uma *commodity*[272], estando para a economia da informação como a destruição do meio ambiente estava para a economia industrial[273]. O primeiro capítulo prestou-se para situar essa questão e identificou que os modelos de negócios são rentabilizados pelo uso de dados pessoais[274].

Ainda que a afirmativa de Zygmunt Bauman[275] tenha se dado em um outro contexto, poder-se-ia tomar emprestado a sua assertiva de que há uma verdadeira transformação das pessoas em mercadorias, considerando-se que os seus dados são o seu prolongamento.

Não é à toa que se fala em "morte da privacidade", crise ou erosão da intimidade[276], pois a realidade que lhe é subjacente demonstra que os dados pessoais são o que alimenta e movimenta tal economia e, mais do que isso, são a base de sustentação e ativo estratégico de uma série de modelos de negócios e para formulação de políticas públicas. Há uma economia[277] e uma sociedade que são

cada vez mais reféns e dependentes desse livre fluxo informativo.

Diante disso, a proteção de dados pessoais permite disciplinar a liberdade, a inovação e o desenvolvimento. E, em um cenário em que dados pessoais projetam a maneira como cada indivíduo é visto no mundo, permite também o exercício de direitos e da cidadania. Trata-se, hoje, do mais importante pilar do nosso contrato social[278].

Nesse contexto, historicamente, normas de proteção de dados pessoais sempre tiveram a *dupla função* de não só garantir a privacidade e outros direitos fundamentais, mas também fomentar o desenvolvimento econômico.

Já na década de 1980, a Organização para o Desenvolvimento e Cooperação Econômica (OCDE emitiu diretrizes a respeito do tema, as quais foram atualizadas e ampliadas mais de três décadas depois. Em ambos os momentos, o fio condutor foi justamente o papel estratégico[279] dos dados pessoais para o progresso socioeconômico.

Ao definir um conjunto de direitos e obrigações para o tratamento de dados pessoais, as *guidelines* da OCDE e, de forma geral, as leis de proteção de dados procuraram conferir segurança jurídica tanto ao cidadão, como, também, ao setor estatal e privado sobre como deve se dar o fluxo desses dados. E, em última análise, assegurar *confiança* entre todos os atores desse ecossistema para que não haja paralisia nessas trocas econômicas.

Até a aprovação da LGPD, o Brasil contava somente com leis setoriais de proteção de dados Era uma verdadeira "colcha de retalhos" que não cobria setores importantes da economia e, dentre aqueles cobertos, não havia uniformidade em seu regramento. Essa assimetria gerava insegurança para: **a)** que os mais diversos setores produtivos trocassem dados entre si com o objetivo de desenvolver novos modelos de negócios; **b)** a formulação de políticas públicas e parcerias público-privadas igualmente dependentes desse intercâmbio de dados; e **c)** o cidadão que não detinha uma proteção integral e universal com relação a todas as atividades do cotidiano em que fornece seus dados, seja para o setor privado ou público[280].

Sendo a proteção do consumidor e a dignidade da pessoa humana erigidas como princípios da ordem econômica pela Constituição Federal (art. 170, *caput* e inciso V, da Constituição Federal) que conformam a livre-iniciativa[281], mostra-se ainda mais pertinente o diagnóstico dessa dupla faceta de leis gerais de proteção de dados pessoais, especialmente para se cumprir com o que foi programado em termos de ordem econômica pelo texto constitucional.

A LGPD internaliza tal orientação constitucional. As suas disposições preliminares enunciam que a disciplina da proteção de dados pessoais tem como objetivo proteger os direitos fundamentais e o livre desenvolvimento da personalidade (art. 1º), repetindo-os como um dos seus fundamentos ao lado do desenvolvimento econômico-tecnológico e da inovação (art. 2º). A LGPD estabelece, portanto, uma *dialética normativa* de conciliação entre todos esses elementos[282].

O principal vetor para alcançar tal objetivo é franquear ao cidadão *controle* sobre seus dados pessoais. Essa estratégia vai além do consentimento do titular dos dados, pelo qual ele autorizaria o

seu uso. Tão importante quanto esse elemento volitivo é assegurar que o fluxo informacional atenda às suas legítimas expectativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade.

É a combinatória desses elementos de que se trata a autodeterminação informacional. Este livro reavaliará tal paradigma normativo, identificando quais são a função e os limites do consentimento e, em última análise, desmitificando[283] os falsos "dilemas"[284] sobre qual é o seu papel no campo da proteção de dados pessoais. Essa é uma investigação necessária como parte da equação de leis de proteção de dados pessoais, cujo produto é a facilitação de trocas econômicas que não sejam lesivas às liberdades dos cidadãos.

[1] Não é o nosso objetivo discorrer, minuciosamente, sobre a história dos direitos da personalidade direito privado. Verificar-se-á que há "saltos" históricos, cujos eventos estão relacionados para discorrer sobre a diacronia dos direitos da personalidade. REALE, Miguel.*Política e direito*: ensaios. São Paulo: Saraiva, 2006. p.91: "Como já disse, cada direito da personalidade se vincula a um *valor fundamental* que se revela através do processo histórico, o qual não se desenvolve de maneira linear, mas de modo diversificado e plural, constituindo aqueles que as denomino invariantes *axiológicas*".

[2] AMARAL, Francisco. Op.cit., p.289: "No direito grego, onde começou a delinear-se a ideia d pessoa, a proteção da personalidade partia da ideia de hybris (excesso, injustiça), que justifica a sanção penal punitiva". Nesse mesmo sentido, trazendo maiores subsídios para a compreensão da hybris: "Já no campo dos institutos jurídicos, podemos destacar a tutela da pessoa em Atenas por meio da ação fundada na ideia de *hybris*. Essa ação tinha inicialmente caráter penal e objetivava a punição de ultrajes ou sevícias sobre uma pessoa. Com o passar do tempo houve o seu aprimoramento, o que permitiu, mediante ações públicas ou privadas, a tutela de outros ilícitos, como as ofensas corporais, a difamação, a violação de mulheres e o uso da força sobre coisa alheia. (...) Seja como for, é por meio da *hybris* que os gregos expressavam seu repúdio ao excesso, à injustiça, ao desequilíbrio, à insolvência e à soberba" (ZANINI, Leonardo Estevam d Assis. *Direitos da personalidade*: aspectos essenciais. São Paulo: Saraiva, 2011. p.24-25).

[3] CORDEIRO, António Menezes de.*Tratado de direito civil*: parte geral, pessoas. Coimbra: Almedina, 2011. v.4, p.49: "Trata-se de uma decorrência da estruturação processual do Direito romano: apenas muito mais tarde surgiria a figura do direito subjetivo. Os acasos históricos da *actio iniuriarium* levaram-na para a área dos delicta, assim se perdendo, logo no início, a hipótese de a sistematizar em torno da própria pessoa: noção essa que, de resto, também tardou em se impor. Todavia, a tutela da personalidade estava já consignada, no Direito Romano. O direito – particularmente o civil – existe para defender as pessoas, sendo sintomático que, desde cedo, os hoje ditos bens de personalidade tivessem obtido proteção. A ideia de que a dignidade das pessoas data do liberalismo não é historicamente exata".

[4] AMARAL, Francisco. Op.cit., p.289.

[5] GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. *Novo curso de direito civil*: parte gera São Paulo: Saraiva, 2006. v.1, p.141.

[6] VILLEY, Michel. *A formação do pensamento jurídico moderno*. Trad. Claudia Berliner. São Pau Martins Fontes, 2006. p.649.

[7] BITTAR, Carlos Eduardo Bianca; ALMEIDA, Guilherme Assis de. *Curso de filosofia de direito*. São Paulo: Atlas, 2008. p.258.

[8] Entre outros, aduzindo o direito natural como fonte e fundamentos dos direitos da personalidade:

LIMONGI FRANÇA, Rubens. *Instituições de direito civil*. São Paulo: Saraiva, 1996. p.1035: "O fundamento próximo da sua sanção é realmente a estratificação no direito consuetudinário ou nas conclusões da Ciência Jurídica. Mas o seu fundamento primeiro são as imposições da natureza das coisas, noutras palavras, o direito natural". Nesse mesmo sentido: DE MATTIA, Fábio Maria. Direitos da personalidade: aspectos gerais. In: CHAVES, Antônio (Coord.) *Estudos de direito civil*. São Paulo: Revista dos Tribunais, 1979. p.100; BITTAR, Carlos Alberto. *Os direitos da personalidade*. Rio de Janeiro: Forense Universitária, 2004. p.7.

[9] BITTAR, Carlos Eduardo Bianca; ALMEIDA, Guilherme Assis de. Op.cit., p.258.

[10] WIEACKER, Franz. *História do direito privado moderno*. Tradução António Manuel Botelho Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004. p.280: "O jusracionalismo não constitu senão um curto capítulo histórico das mais vastas manifestações do jusnaturalismo".

[11] Ibidem, p.306: "Se voltarmos à influência particular sobre a *história do direito*, são os traços metodológico-sistemáticos do jusracionalismo e a sua emancipação em relação à teologia moral que caracterizaram o jusnaturalismo moderno do continente europeu. Como *teoria*, ele liberta finalmente a jurisprudência técnica das autoridades da Idade Média e dá-lhe um sistema interno e um método dogmático específicos – a construção a partir de conceitos gerais".

[12] LOSANO, Mario G. *Sistema e estrutura no direito*: das origens à escola histórica. Trad. Carlo Alberto Dastoli. São Paulo: Martins Fontes, 2008. v.I, p.295.

[13] WIEACKER, Franz. Op.cit., p.310.

[14] Ibidem, p.427: "De forma significativa, os princípios fundamentais da ciência pandectística, que ainda hoje constituem essencialmente o sistema civilista, foram portanto recebidos, no seu conjunto dos sistemas jusracionalistas e não do *usus modernus*, embora só agora tenha sido, na maior parte dos casos, formulados de forma rigorosa: assim, o direito objectivo, o direito subjectivo e a sua divisão, negócio jurídico, a declaração de vontade, o contrato bilateral, o dever de prestação, a impossibilidade de prestação, etc.".

[15] Ibidem, p.386.

[16] VILLEY, Michel. Op.cit., p.675.

[17] SZANIAWSKI, Elimar. *Direitos da personalidade e sua tutela*. São Paulo: Revista dos Tribunai 1993. p.29. Nesse mesmo sentido: DE MATTIA, Fabio Maria. Op.cit., 1979, p.108.

[18] CORDEIRO, António Menezes de. Op.cit., p.52: "No início podemos situar SAVIGN Curiosamente, SAVIGNY é apontado como negativista, em termos de direitos da personalidade, imputando-lhe mesmo o atraso no reconhecimento da figura. Todavia e em rigor, SAVIGNY apenas questionou a possibilidade dogmática de construir um direito decalcado do direito de propriedade, mas dirigido ao próprio 'titular' e que poderia envolver diversos inconvenientes, entre os quais o reconhecimento de um direito ao suicídio. (...) SAVIGNY não era contrário à tutela da pessoa: bem pelo contrário. Ele apenas duvidou da viabilidade dogmática dos direitos

da personalidade, numa dimensão a que, de resto, ainda hoje teremos de atender". Em sentido análogo: BORGES, Roxana Cardoso*Direitos da personalidade e autonomia privada*. São Paulo: Saraiva, 2009. p.20.

[19] SZANIAWSKI, Elimar. Op.cit., p.30: "Com a promulgação do BGB, o Código Civil alemão, e 1.1.1900, o citado tribunal abandonou essa doutrina entendendo que, com o ordenamento positivo civil em vigor, não haveria lugar para reconhecer-se a existência de um direito geral de personalidade devido à incompatibilidade dos dispositivos legais do novo Código com a mencionada doutrina".

[20] Nesse sentido, tecendo considerações a respeito da carga patrimonialista e individualista presente no direito privado, em especial a influência sofrida pelo Código Bevilácqua do Código Civil Francês: TEPEDINO, Gustavo. Op.cit., p.2; ainda sobre a visão patrimonialista prejudicial a desenvolvimento dos direitos da personalidade: "Nos princípios do século XX, a categoria dos direitos da personalidade foi introduzida em França. Surgiu decisiva pressão doutrinária alemã. Atentou-se, então, em que o *Code Civil* apenas se preocupava com o patrimônio e com os aspectos patrimoniais, deixando os direitos da personalidade, entendidos como todos os que não se reportem a bens". (CORDEIRO, António Menezes de. Op.cit., p.57).

[21] Em sentido análogo, após descrever o desenvolvimento da tese dos direitos da personalidade com os consequentes entraves dogmáticos e positivistas, atentando, por fim, que o Código Civil de 1916 não veio a prever os direitos da personalidade diante de tal cenário instável para a sua acolhida dogmática: ZANINI, Leonardo Estevam de Assis. Op.cit., p.42-46.

[22] ZANINI, Leonardo Estevam de Assis. Op.cit., p.48-49.

[23] Mesmo antes da Segunda Guerra Mundial, pondera-se que as Constituições do México e de Weim já haviam previsto o princípio da dignidade da pessoa humana no início do século XIX.

[24] SZANIAWSKI, Elimar. Op.cit., p.26; traçando o mesmo paralelo para o reconhecimento legislativ da dignidade humana entre Constituição e a Declaração da ONU: CHAVES, Antonio.*Tratado de direito civil*: introdução à ciência do direito, sujeito de direito. São Paulo: Revista dos Tribunais, 1982. t. 1, v.1, p.487.

[25] PERLINGIERI, Pietro*Perfis do direito civil*. Trad. Maria Cristina de Cicco. Rio de Janeiro Renovar, 1999. p.33: "Com o termo, certamente não elegante, a 'despatrimonialização', individua-se uma tendência normativa-cultural; se evidencia que no ordenamento se operou uma opção, que, lentamente, se vai concretizando, entre personalismo (superação do individualismo) e patrimonialismo (superação da patrimonialidade fim a si mesma, do produtivismo, antes, do consumismo, depois, como valores). Com isso, não se projeta a 'expulsão' e a 'redução' quantitativa do conteúdo patrimonial no sistema jurídico e naquele civilístico em especial (...) A divergência, não certamente de natureza técnica, concerne à avaliação qualitativa do momento econômico e à disponibilidade de encontrar, na exigência da tutela do homem, um aspecto

idôneo, não a 'humilhar' a aspiração econômica, mas, pelo menos, a atribuir-lhe uma justificativa institucional de suporte ao livre desenvolvimento da pessoa".

[26] Ibidem, p.34: "é preciso predispor-se a reconstruir o Direito Civil não com uma redução ou um aumento de tutela das situações patrimoniais, mas com uma tutela qualitativamente diversa. Desse modo, evitar-se-ia comprimir o livre e digno desenvolvimento da pessoa mediante esquemas inadequados e superados".

[27] ZANINI, Leonardo Estevam de Assis. Op.cit., p.17: "Somente após a Segunda Guerra Mundial particularmente devido ao holocausto nazifascista, é que houve realmente o florescimento dos direitos da personalidade. Isso foi possível pelo fato de a dignidade da pessoa humana ter passado a integrar o frontispício das constituições e de documentos internacionais, o que levou a um movimento de personalização do direito, em especial do direito civil, que até então era o direito do patrimônio".

[28] A Lei Fundamental da República da Alemanha (1949) prevê em seu art. 2º: "Todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral".

[29] SZANIAWSKI, Elimar. Op.cit., p.31-32.

[30] Traçando tal linha evolutiva para daí destacar a reforma no Código Civil francês para fazer constar a locução "danos à personalidade" e, em sentido análogo, no Código Civil suíço: DE MATTIA, Fabio Maria. Op.cit., p.108. Do mesmo ponto de partida até o Código Civil português de 1966: CARVALHO, Orlando de. Op.cit., p.252-253. Registre-se, no entanto, que o Código Civil italiano, promulgado durante a Segunda Guerra Mundial, já dispunha a respeito da sistematização dos direitos da personalidade, ainda que sufocados pelo regime fascista.

[31] Nesse sentido, aduzindo a respeito da proteção implícita e, ainda, enumerando quais viriam a ser tais artigos do CC/1916: MORATO, Antonio Carlos. Quadro geral dos direitos da personalidade. *Revista da Faculdade de Direito da Universidade de São Paulo* v.106-107, p.122, dez. 2011/jan.2012.

[32] GOMES, Orlando.*Memória justificativa do anteprojeto de reforma do código civil*. Rio de Janeiro: Departamento de Imprensa Nacional, 1963. p.35.

[33] GOMES, Orlando. *A crise*... Op.cit., p.25-30.

[34] GOMES, Orlando. *Memória*... Op.cit., p.64-65.

[35] Veja-se, nesse sentido: RAMOS, Luiz Felipe Rosa; SILVA FILHO, Osny. *Orlando Gomes*. Rio de Janeiro: Elsevier, 2015. p.93-95.

[36] AMARAL, Francisco. Evocação a Orlando Gomes*Revista de direito comparado*, n.17. p.7, 2º sem. 1999.

[37] MARTINS-COSTA, Judith. *Pessoa, personalidade, dignidade*: ensaio de uma qualificação. Tese

(Livre-docência) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2003. p.233 "Na introdução a essa tese, eu afirmei que 'a estrutura fala'. Percebemos a importância de, tanto na constituição quando no novo Código Civil, os direitos da personalidade, ao invés de estarem situados quase ao fim do texto constitucional (como ocorria com as Cartas de 67 e 69), proporcionarem, já no inaugurar do texto, a chave de leitura dos demais e princípios e regras atinente ao sistema geral de tutela à pessoa".

[38] Ibidem, p.9.

[39] Ibidem, p.233.

[40] CARVALHO, Orlando. Op.cit., p.73-74: "Neste sentido é que se julga oportuna a 'repersonalização' do direito civil – seja qual for o invólucro em que esse direito se contenha –, isto é, a acentuação da sua raiz antropocêntrica, da sua ligação visceral com a pessoa, e os seus direitos. Sem essa raiz um tal direito é ininteligível, não tanto porque a grosso das instituições civilísticas apela ainda para a autonomia da vontade, pelo menos na forma de liberdade de conclusão, mas principalmente porque o civismo ou civilismo é uma ideia que ou já não tem qualquer nexo ou tem-no justamente por ser o círculo da pessoa". Nesse mesmo sentido: FACHIN, Luiz Edson*Teoria crítica do direito civil*. Rio de Janeiro: Renovar, 2012. p.253-266; LÔBO, Paulo. *Direito Civil*: parte geral. São Paulo: Saraiva, 2012. p.132.

[41] CARVALHO, Orlando. Op.cit., p.228. Em sentido análogo: CORDEIRO, António Menezes. Op.cit. p.99.

[42] Veja-se, nesse sentido, o Enunciado 274 da IV Jornada de Direito Civil: "Os direitos da personalidade, regulados de maneira não exaustiva pelo Código Civil, são expressões da cláusula geral de tutela da pessoa humana, contida no art. 1º, III, da Constituição (princípio da dignidade da pessoa humana). Em casos de colisão entre eles, nenhum pode sobrelevar os demais, deve-se aplicar a técnica da ponderação".

[43] TEPEDINO, Gustavo*Temas*... Op.cit., p.54: "Com efeito, a escolha da dignidade da pessoa humana como fundamento da República, associada ao objetivo fundamental de erradicação da pobreza e da marginalização, e de redução das desigualdades sociais, juntamente com a previsão do § 2º do art. 5º, no sentido da não exclusão de quaisquer direitos e garantias, mesmo que não expressos, desde que decorrentes dos princípios adotados pelo texto maior, configuram uma verdadeira *cláusula geral de tutela e promoção da pessoa humana*, tomada como valor máximo do ordenamento". Nesse mesmo sentido: FACHIN, Luiz Edson. Fundamentos, limites e transmissibilidade: anotações para uma leitura crítica, construtiva e de índole constitucional da disciplina dos direitos da personalidade no Código Civil brasileiro. *Revista da Escola da Magistratura do Estado do Rio de Janeiro*, v.8. n.31, p.69. 2005. Em sentido análogo, também, fazendo alusão à cláusula geral: CAMPOS, Diogo Leite de*Nós*: estudo sobre os direitos das pessoas. Almedina: Coimbra, 2004. p.133: "Os direitos da personalidade constituirão,

praticamente, 'cláusulas gerais' de controlo do ordenamento e de preenchimento de lacunas. Sendo as normas (formais ou substanciais) que os consagram enquanto tais, consumidas pela concorrência de outras normas que utilizam (com justiça) tais direitos como um dos ingredientes da composição dos interesses em jogo".

[44] Para essa parte específica da doutrina, prefere-se tal nomenclatura baseada na percepção de que não se deve esvaziar o discurso da dignidade da pessoa humana, vulnerando-se, em última análise, o próprio princípio constitucional. Acredita-se, por isso, que a disciplina dos direitos da personalidade deve ser o recurso primeiro para a propugnada tutela promocional da pessoa, ainda que seja otimizada pelo postulado normativo constitucional. O seu recurso contínuo prejudica o caráter argumentativo e normativo: MARTINS-COSTA, Judith. Op.cit., p.5-6: "Em primeiro lugar, agora o modelo de incomunicabilidade que, por quase um século, operou entre Constituição e Código Civil, é substituído pelo modelo da conexão e complementaridade intertextual. Constatar esse modelo não significa simplesmente endossar a tese da 'constitucionalização do Direito Civil', fenômeno que – dado como suposto – tem sido abordado tanto por civilistas quanto por constitucionalistas, daqui e d'além mar. Significa tão somente – para os fins deste trabalho – considerar o novo Código Civil Brasileiro como uma estrutura apta a operacionalizar o que chamo de *sistema geral de tutela à pessoa humana* – expandindo nas situações interprivadas os bens da personalidade. Significa não mais considerar o Código como um universo isolado, fechado sobre si mesmo, substancialmente oposto, até, ao universo constitucional". E, em notas conclusivas, fecha-se o raciocínio (p.254): "Não é preciso, frente ao novo Código, esvaziar a força normativa e argumentativa e o imenso valor do princípio da dignidade da pessoa humana, utilizando-se como substitutivo de outros princípios e regras de maior densidade".

[45] TEPEDINO, Gustavo. Op.cit., p.55: "Mais ainda, a tutela da personalidade, como bem se acentuou na doutrina alienígena, é dotada do atributo da elasticidade, não se confundindo, todavia, tal característica com a elasticidade do direito de propriedade. No caso da pessoa humana, elasticidade significa a abrangência de tutela, capaz de incidir a proteção do legislador e, em particular, o ditame constitucional de salvaguarda da dignidade humana a todas as situações, previstas ou não, em que a personalidade, entendida como valor máximo do ordenamento, seja o ponto de referência objetivo".

[46] MARTINS-COSTA, Judith. Op.cit., p.107: "Por isso mesmo, a noção de direitos da personalidade é inacabada, transitiva – em uma palavra, é cultivável".

[47] SCHEREIBER, Anderson.*Os direitos da personalidade*. São Paulo: Altas, 2011. p.14; PEREIRA, Caio Mário da Silva.*Instituições de direito civil*. Atualização Maria Celina Bodin de Moraes. Rio de Janeiro: Forense, 2010. p.205; GONÇALVES, Carlos Roberto*Direito civil*: parte geral. São Paulo: Saraiva, 2010. v.I, p.187.

[48] REALE, Miguel. *Política*... Op.cit., p.90: "Nada mais acrescenta o Código, nem poderia enumerar os direitos da personalidade, que se espraiam por todo o ordenamento jurídico, a começar pela Constituição Federal que, logo no art. 1º, declara serem fundamentos do Estado Democrático do Direito a cidadania, a dignidade da pessoa humana, os valores sociais do trabalho e a livre-iniciativa".

[49] Textualmente, tais dispositivos preveem: a integridade biopsíquica, o nome, a imagem, honra e privacidade como direitos da personalidade.

[50] O direito geral de personalidade guarda suas origens no direito alemão em que é assegurado, constitucionalmente, à pessoa humana, o livre desenvolvimento de sua personalidade, sendo, pois, um "direito-fonte (*Quellrecht*), um direito-mãe (*Muttrrecht*), do qual todos os outros direitos emanariam" (ZANINI, Leonardo Estevam de Assis. Op.cit., p.145). Não haveria portanto, uma enumeração dos direitos da personalidade, sendo um arquétipo, totalmente, fluido e aberto, o que seria para a escola de Coimbra um elemento "imprescindível do patrimônio jurídico" (CAPELO DE SOUSA, Rabindranath V.A*O direito geral de personalidade*. Lisboa: Coimbra Editora, 2011. p.627). Enquanto a escola de Lisboa "seria contrária a tal figura" (MIRANDA, Jorge; RODRIGUES JUNIOR, Otavio Luiz; FRUET, Gustavo Bonato. Princi problemas dos direitos da personalidade e estado da arte da matéria no direito comparado. *Direitos da personalidade*. São Paulo: Atlas, 2012. p.18). Registre-se, no entanto, que a própria figura do direito geral de personalidade perdeu espaço na Alemanha, pois, como visto, foi necessário a ele recorrer para que o direito da personalidade pudesse ser tutelado diante da necessidade de seu enquadramento como um direito subjetivo, estando agora em regressão naquele país (CORDEIRO, António Menezes. Op.cit., p.66). Anota-se, tal divergência, também no Brasil; dentre alguns dos defensores do direito geral: AMARAL, Francisco.*Direito Civil*... Op.cit., p.287; GARCIA, Enéas Costa *Direito geral de personalidade no sistema jurídico brasileiro*. São Paulo: Juarez de Oliveira, 2007. p.230; dentre alguns dos defensores das espécies dos direitos da personalidade: CHINELLATO, Silmara Juny de Abreu. Comentários Parte Geral – artigos 1º a 21 do Código Civil. In: MACHADO, Antonio Cláudio da Costa (Org. CHINELLATO, Silmara Juny (Coord.)*Código Civil interpretado*: artigo por artigo, parágrafo por parágrafo. 5.ed. Barueri: Manole, 2012. p.43; MORATO, Antonio Carlos.*Quadro geral*... Op.cit., p.153.

[51] BORGES, Roxana Cardoso. Op.cit., p.29: "Os efeitos práticos de adotar o direito geral d personalidade ou uma lista exemplificativa de direitos de personalidade são os mesmos, pois ambos têm como fundamento a dignidade da pessoa humana e nenhuma das duas correntes restringe a proteção jurídica aos direitos expressos no direito positivo, o que é imprescindível para a adequada proteção de tais direitos numa sociedade em veloz mutação".

[52] DANTAS, San Tiago.*Programa de direito civil*: parte geral, aulas proferidas na Faculdade de

Direito Civil. Rio de Janeiro, 1979. p.192: "É um ponto de partida e não um ponto de chegada, na construção dos direitos subjetivos. Esse argumento, que ele explana muito bem, pode ser, entretanto, repelido com uma observação capital, é que a palavra *personalidade* está tomada, aí, em dois sentidos. Quando se fala em *direitos de personalidade*, não se está se identificando aí a personalidade como a capacidade de ter direitos e obrigações; estamos então considerando a personalidade como um fato natural, como um conjunto de atributos inerentes à condição humana; estamos pensando num homem vivo e, não, nesse atributo especial do homem vivo, que é a capacidade jurídica, em outras ocasiões identificada como a personalidade". Nesse sentido é a nota da atualizadora: PONTES DE MIRANDA, Francisco Cavalcanti. *Tratado de direito privado*: direito de personalidade. Direito de família: direito matrimonial (Existência e validade do casamento). Atualização Rosa Maria Barreto Borriello de Andrade Nery. São Paulo: Revista dos Tribunais, 2012. p.59. (Coleção Tratado de Direito Privado: parte especial, 7.)

53 CORDEIRO, António Menezes. Op.cit., p.56: "O progressivo domínio dogmático da 'periferia' da personalidade permitiu o esforço de abstração necessária para se alcançar a ideia de 'bem de personalidade', base de qualquer dogmática coerente de direitos da personalidade". No mesmo sentido: ANTUNES, Ana Filipa Morais. *Comentários aos artigos 70.º a 81.º do Código civil*: direitos da personalidade. Lisboa: Universidade Católica, 2012. p.19.

54 O recurso do enquadramento dos direitos da personalidade como sendo bens jurídicos ou situações jurídicas é fruto da percepção de que a veste do direito subjetivo seria inadequada para a proteção da pessoa humana. O direito subjetivo foi algo forjado para a circulação econômica, a enquadrar o ser humano (sujeito de direito) em polos de uma relação jurídica, cujo objeto que os ligava era patrimonial. Daí todo o engodo da divergência de Savigny para o reconhecimento dos direitos da personalidade, já que por esse arquétipo legitimar-se-ia o suicídio – disponibilidade de tal direito que advém da noção de patrimônio –, ou, ainda, a própria noção de que tal relação subjetiva seria limitada não alcançando a proteção difusa e *erga omnes* necessária para a proteção da pessoa humana. Nesse sentido: MARTINS-COSTA, 2003, p.106-107: "O conceito de direito subjetivo é hoje, ao menos do ponto de vista analítico, uma veste inadequada para tratar os direitos da personalidade (...) A categoria deve ser compreendida a partir de pressupostos diversos daqueles que formataram a sua origem, estando inserida na classe, mais abrangente, das situações jurídicas subjetivas". Em sentido análogo: DONEDA, Danilo. O direitos da personalidade no novo Código Civil. In: TEPEDINO, Gustavo (Coord.). *A parte geral do novo Código Civil*: estudos na perspectiva constitucional. Rio de Janeiro: Renovar, 2002. p. 44-45.

55 BORGES, Roxana Cardoso. Op.cit., p.46: "Assim, verifica-se que, se toma um conceito de bem jurídico diferente do conceito de bem econômico, que seja apropriado às inúmeras situações encontradas em nosso ordenamento jurídico atual, os atributos da personalidade, protegidos pelos direitos da personalidade, podem ser considerados bens jurídicos, portanto objetos de

direitos, embora não regulamentados pelo Livro II da Parte Geral do Código Civil de 2002".

[56] Miguel Reale dirá que a pessoa-humana é um valor-fonte. Pondera que os valores não possuem un existência em si ontológica, mas seriam provenientes da experiência humana, especialmente por meio da história a se tornar uma invariante axiológica. Por esse raciocínio, é que se chega ao princípio da dignidade da pessoa humana e aos direitos da personalidade em virtude da travessia aqui projetada, especialmente por conta dos episódios históricos terrificantes que conformam esse horizonte de proteção do ser humano. REALE, Miguel.*Filosofia do direito*. São Paulo: Saraiva, 2002. p.208-214. Em outra obra, o professor cruza tais informações: REALE, Miguel *Política*... Op.cit., p.91: "Como já disse, cada direito da personalidade se vincula a um*valor fundamental* que se revela através do processo histórico, o qual não se desenvolve de maneira linear, mas de modo diversificado e plural, constituindo aqueles que as denomino invariantes *axiológicas*".

[57] CAPELO DE SOUSA, Rabindranath V.A. Op.cit. p.764.

[58] CORDEIRO, António Menezes. Op.cit., p.61: "A dramática experiência do III Reich levou, n República Federal Alemã subsequente a 1949, a um surto no desenvolvimento de direitos fundamentais e de personalidade. Esse movimento intensificou-se com a multiplicação dos meios suscetíveis de agredir ou pôr em causa a esfera mais pessoal de cada um: meios de comunicação e de vigilância, informática e biotecnologia, como exemplos".

[59] HOUAISS, Antônio; VILLAR, Mauro de Salles. Op.cit., p.1.480.

[60] SIMÃO, José Fernando. *Responsabilidade civil do incapaz*. São Paulo: Atlas, 2008. p.14.

[61] BITTAR, Carlos Alberto.*Os direitos*... Op.cit., p.1: "Consideram-se como da personalidade os direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos no homem, como a vida, a higidez física, a intimidade, a honra, a intelectualidade e outros tanto". Em sentido análogo: "Nesta ordem de ideias, há que concluir que a personalidade jurídica é a projecção no Direito (no mundo normativo jurídico) da personalidade humana". (CARVALHO, Orlando de Op.cit., p.190).

[62] Esses são, por exemplo, algumas das espécies de direitos da personalidade listadas pelo CC.

[63] FRANÇA, Rubens Limongi. Direitos da personalidade. In: MENDES, Gilmar Ferreira; STOC Rui (Org.). *Doutrinas essenciais*: direito civil – parte geral – pessoas e domicílio. São Paulo: Revista dos Tribunais, 2011. p.654: "Portanto, Direitos da Personalidade dizem-se as faculdades jurídicas cujo objeto são os diversos aspectos da própria pessoa do sujeito, bem assim seus prolongamentos e projeções. Ao tratarmos dos Direitos da Personalidade em espécie, será elucidada a parte do nosso conceito relativo às palavras 'prolongamentos' e 'projeções'".

[64] GONÇALVES, Diogo Costa*Pessoa e direitos da personalidade*: fundamentação ontológica. Coimbra: Almedina, 2008. p.44: "Mas, sendo *subsistens*, o Homem é *distinctum subsistens*.

Quando afirmamos *distinctum*, porque o acto de ser, no Homem, está marcado pela autopossessão, pela imanência, pela ipseidade... em suma, por uma radical intimidade ontológica que só toda a densidade semântica do 'eu sou' é capaz de expressar. Nesta acepção, que evidencia a realidade da pessoa como ser em si podemos afirmar que o Homem é o único *subsistens* em sentido estrito ou próprio".

65 TEPEDINO, 2008, p.29: "De outro ponto de vista, todavia, tem-se personalidade como conjunto d características e atributos da pessoa humana, considera-se como objeto de proteção por parte do ordenamento jurídico. A pessoa, vista deste ângulo, há de ser tutelada das agressões que afetam a sua personalidade. (...) Dito diversamente, considerada como sujeito de direito, a personalidade não pode ser dele o seu objeto. Considerada, ao revés, como valor, tendo em conta o conjunto de atributos inerentes e indispensáveis ao ser humano (que se irradiam da personalidade), constituem bens jurídicos em si mesmos, dignos de tutela privilegiada".

66 CUPIS, Adriano de. *Os direitos da personalidade*. Tradução Afonso Celso Furtado Rezende. São Paulo: Quorum, 2008. p.180: "O indivíduo como unidade da vida social e jurídica, tem necessidade de afirmar a própria individualidade, distinguindo-se dos outros indivíduos, e, por consequência, ser conhecido por quem é na realidade. O bem que satisfaz essa necessidade é o da identidade, o qual consiste, precisamente, no distinguir-se das outras pessoas nas relações sociais".

67 MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. *Revista de Direit do Consumidor*, ano 20, v.79, p.75, jul./set. 2011: "Tendo em vista tratar-se de direito à personalidade, já que os dados armazenados representam a pessoa na sociedade". Em sentido similar: CATALA, Pierre. Ebauche d'une théorie juridique de l'information, p.20,*apud* DONEDA, Danilo. *Da privacidade*... Op.cit., p.157: "Mesmo que a pessoa em questão não seja a 'autora' da informação, no sentido de sua concepção, ela é titular legítima dos seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um direito da personalidade".

68 RODOTÀ, Stefano.*Il diritto di avere*. Roma: Laterza, 2012. p.148: "Nel discorso giuridico, la registrazione di un dato deve essere compagnata da una riflessione sul senso del passagio nella nuova dimensione, dunque da una attività necessariamente ricostruttiva".

69 TENNIS, Bradley. Privacy and identity in a networked world. In: AKRIVOPOLOUS, Christi PSYGKAS, Athanasious (Org.).*Personal data privacy and protection in a surveillance era*: technologies and practices. New York: Information Science Reference, 2011. p.12-13.

70 RODOTÀ, Stefano.*Il diritto*... Op.cit., p.314: "Tutto questo, oggi, può essere considerato anche nella dimensione de diritti, di uma construzione dell'indetitá che finisce com il coincidere con la costruzione stessa dell'umano (...) costruire liberamente la própria indetità utilizando tutte le oportunità socialmente disponibili. La nuova dimensione dell'umano sige uma diversa misura

giuridica, che dilata l'ambito de diritti fondamentali della persona".

[71] A expressão de Daniel J. Solove, cujo título da obra expressa a atribuição de uma nova identidade provinda dos dados pessoais. SOLOVE, Daniel. J.*The digital person*: technology and privacy in the information age. New York: New York University Press, 2004. p.3.

[72] Enquadrando direito à identidade como um dos direitos da personalidade, veja RIZZARDO Arnaldo. *Parte geral do código civil*. Rio de Janeiro: Forense, 2011. p.157: "O ponto de realce, aqui, restringe-se à identidade como direito da personalidade, para que tenham as pessoas uma presença na sociedade e perante o Estado, e para que não se considerem simples quantidades ou números na ordem do gênero humano. Por isso, decorre do direito da personalidade o tratamento como uma individualidade, dentro de uma performance própria – ou um ser que se destaca, merecedor de respeito e titular de uma posição única".

[73] Como decorrência do princípio da qualidade dos dados, o cidadão tem o direito de exigir a correção de dados incompletos, inexatos ou desatualizados, de acordo com os arts. 6º, V, e 8º, III, ambos da LGPD.

[74] Apesar de discordar com a conclusão final – direito à identidade informacional – concorda-se com o trajeto percorrido pelo jurista português que sublinha a importância do direito à proteção dos dados pessoais sob as lentes do direito da personalidade para fins de uma correta construção dogmática. Como será visto mais à frente, o reconhecimento do direito à proteção dos dados pessoais como um novo direito da personalidade já é suficiente para galgar tal rigor dogmático e, nesse sentido, o que propomos nesse trabalho é reavaliar a sua percepção tradicional – autodeterminação informacional – para uma recepção crítica de acordo com a cultura jurídica legal brasileira. PINHEIRO, Alexandre Sousa*Privacy e proteção de dados pessoais*: a construção dogmática do direito à identidade informacional. Lisboa: AAFDL, 2015. p.827-829.

[75] Toda vez que submetido a um processo de decisão totalmente automatizado, sem que haja qualquer tipo de intervenção humana, o cidadão tem assegurado o direito de solicitar sua revisão, bem como obter explicação a respeito dos critérios que estão sendo utilizados para tal automatização (art. 10, *caput* e § 1º, da LGPD).

[76] RODATÀ, Stefano. Persona, riservatezza, identità.*Rivista Crtica del Diritto Privato*, ano XV, p.583-584, dic. 1997: "Alcuni abituali usi linguistica, e il peso di una lunga vicenda d'origine, inducono a corisiderare la legge sulla protezione dei dati personali come una disciplina della 'libertà informatica' come un insieme di norma sulla 'rivacy informatica'. Ma è sicuramente improprio l´uso sia del sostantivo (privacy) (...)il tratamento dei dati personali si svolga nel rispetto dei diritti, della libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all indetitá personale (...) Una lettura condotta unicamente in termini di privacy non sarebbe soltano riduttiva, ma porterebbe pure ad una impropria risconstruzione di questo stesso concetto(...) entrambe confrmano la dilatazione della

consideraione normativa".

77 ANDRADE, Norberto Nuno Gomes de Andrade. The right to privacy and the right to identity in th Age of ubiquitous computing: Friends or foes? A proposal towards a legal articulation. In: AKRIVOPOLOUS, Christina; PSYGKAS, Athanasious (Orgs.). *Personal data privacy and protection in a surveillance era*: technologies and practices. New York: Information Science Reference, 2011. p.34: "Moreover, this means that rules on the protection of personal data (defined as any information, truthful or not, relating to an identified or identifiable person) go clearly beyond the protection of privacy, covering also the protection (and promotion) of one's identity".

78 *Vide* nota de rodapé 73, *supra*.

79 CAPELO DE SOUSA, Rabindranath V.A. Op.cit. p.245: "O bem da identidade reside, assim, n própria ligação de correspondência ou identidade do homem consigo mesmo e está, pois, ligado a profundas necessidades humanas, a ponto de o teor da convivência humana depender de sua salvaguarda em termos de reciprocidade".

80 FINOCCHIARO, Giusella. *Privacy*... Op.cit., p.5: "Il diritto alla protezione dei dati personali va collocato nell'ambito dei diritti della personalità. Si tratta, como é noto, di una categoria aperta di diritti caratterizzati dall´essere assoluti, indisponibli e imprescritibitibili".

81 Uma parcela deste subcapítulo congrega parte das contribuições de outro trabalho de nossa autoria BIONI, Bruno Ricardo. Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação/GPoPAI da Universidade de São Paulo. 2016. Disponível em <https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_inicia

82 SCHWARTZ Paul; M. SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept Personally Identifiable Information.*Review Law N.Y.U.*, p.1816. Disponível em: <http://scholarship.law.berkeley.edu/facpubs/1638>: "PII is one of the most central concepts in privacy regulation. It defines the scope and boundaries of a large range of privacy statutes and regulations".

83 Fato jurídico é aquele que tem repercussão para o direito, produzindo efeitos jurídicos, criando, modificando e extinguindo relações jurídicas. Um fato sem tal adjetivação não tem repercussão e, portanto, não produz efeitos jurídicos, como é o exemplo da queda de uma folha seca da árvore que em nada tem relevância para a ciência jurídica (AMARAL, Francisco.*Direito*... Op.cit., p.379-380).

84 MANNINO, Michael V.*Projeto*... Op.cit., p.555.

85 ROB, Peter. *Sistemas*... Op.cit., p.4.

86 Ibidem.

[87] HOUAISS, Antônio; VILLAR, Mauro de Salles. Op.cit., p.140-141.

[88] DONEDA, Danilo. *Da privacidade*... Op.cit., p.44-43.

[89] COUNCIL OF EUROPE. *Handbook on European Data Protection Law*. Luxembourg: Publicatio Office of the Europe Union, 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>.

[90] Para muitos, a pseudoanonimização não é considerada uma técnica de anonimização. Isso porque substituem, apenas, os identificadores diretos – *e.g.*, nome, CPF etc. – por pseudônimos – *e.g.*, números aleatórios, de modo que a pessoa permanece sendo identificável em razão de tais pseudônimos serem um retrato detalhado indireto delas (WP 29, 2014, p.20).

[91] TEIXEIRA, Lucas. Teoricamente impossível: problemas com a anonimização de dados pessoais Disponível em: <https://antivigilancia.org/pt/2015/05/anonimizacao-dados-pessoais/>.

[92] NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and Fallacies of "Personally Identifiabl Information". *Communications of the ACM*, v.53, n.06, p.24, June 2010. Disponível em: <www.cs.utexas.edu/~shmat/shmat_cacm10.pdf>.

[93] NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust De-anonymization of Large Spars Datasets, p.6. Disponível em: <https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>.

[94] NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust... Op.cit., p.12.

[95] Ibidem, p.15.

[96] OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymizatio (August 13, 2009). *UCLA Law Review*, v.57, p.1749, 2010; *Colorado Law Legal Studies Research Paper* n.9-12. Disponível em: <http://ssrn.com/abstract=1450006>.

[97] NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust... Op.cit., p.4.

[98] SCHWARTZ Paul M.; SOLOVE, Daniel J. The PII... Op.cit., p.1874.

[99] Vejam-se, no entanto, nossas ressalvas feitas em outro trabalho em que se leva em consideração o critério de razoabilidade para transformar um dado anônimo em dado pessoal (processo de reidentificação). Nele, nós concluímos ser possível a convivência entre um conceito expansionista e o de dado anonimizado: BIONI, Bruno. Xeque-mate... Op.cit., p.30-36.

[100] Art. 5º, I: "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa".

[101] FINOCCHIARO, Giusella*Privacy*... Op.cit., p.55: "Il concetto chiave, tanto nella defizione di dato personale, quanto in quella di dato anonimo, é quello di riferibilità. Se le informazioni possono essere riferite ad un goggetto, i dati non sono anonimi, ma personali e, consequentemente, deve applicarsi la normativa in materia di protezione dei dati personali".

[102] TENE, Omer. Privacy law's midlife crisis: a critical assessment of the second wave of global

privacy laws. *Ohio State Journal*, v.74, 2013, p.1.242.

[103] A Diretiva 95/46 e a sua proposta de regulamentação adotam os conceitos de razoabilidade, respectivamente, nas considerandas 26 (vinte e seis) e 23 (vinte e três).

[104] Na definição de dados anônimos, de anonimização, bem como no dispositivo que prevê em quais hipóteses dado anonimizado pode ser considerado como dado pessoal, a LGPD faz alusão ao termo razoável(is) – respectivamente, arts. 5º, II e III, e 18.

[105] ARTICLE 29, Data Protection Working Party. Opinion 04/2007 on the concept of personal data p.1749. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>. p.15.

[106] Essa é exatamente a terminologia utilizada pelo art. 12, *caput*, da LGPD: "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido".

[107] Ibidem, p.21.

[108] Sobre as disputas interpretativas em torno do conceito jurídico indeterminado de razoabilidade, veja-se: BIONI, Bruno Ricardo. Xeque-mate... Op.cit., p.34-35.

[109] O conceito de "technology-neutral regulation" tem sido evocado para se discutir o desenho de modelos regulatórios capazes de estimular e acompanhar o desenvolvimento tecnológico, sem engessá-lo nem ser permissivo a riscos. Sobre isso: KOOPS, Bert-Jaap. Should ICT Regulation Be Technology-Neutral? In: Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens (eds.). *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, IT & Law Series, v. 9, The Hague: T.M.C. Asser Press 2006, ISBN 90-6704-216-1, pp. 77-108; REED, Chris. Taking Sides on Technology Neutrality.*SCRIPT-ed*, v. 4, issue 3, September, 2007; MOSES, Lyria Bennett. How to think about law, regulation and technology: problems with 'technology' as a regulatory target. *Law, Innovation and Technology*, v. 5, p. 1-20, 2013. Para a discussão no cenário nacional, ver: BAPTISTA, Patrícia; KELLER, Clara. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. *Revista de Direito Administrativo*, n. 273, p. 123-163, set./dez. 2016.

[110] A GDPR, em sua Consideranda 26, também utiliza esses três fatores objetivos como delimitação à razoabilidade.

[111] Artigo 12 da LGPD. Art. 12. § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

[112] A LGPD, em seu art. 5º, III e XI, define dado anonimizado a partir do emprego dos meios técnicos

razoáveis disponíveis na ocasião (III) e no momento (XI) de seu tratamento. Esse tipo de avaliação torna-se, assim, contextual. Se, por um lado, essa análise contextual incentiva estudos sobre o tema, por outro, traz complicações à avaliação de seu cumprimento tendo em vista, por exemplo, diferenças quanto ao acesso à informação e recursos econômicos disponíveis entre os diferentes atores.

[113] Em 08.01.2019, foi lançado o primeiro computador quântico de uso comercial do mundo. Contudo estima-se um período entre cinco e dez anos para que a computação quântica passe a ser adotada nos negócios. Assim, apesar de existente, essa tecnologia não compreenderia o estado da arte da tecnologia (ou meio técnico razoável disponível, nos termos da LGPD), tornando um encargo demasiado excessivo à expectativa de sua adoção. Disponível em <https://epocanegocios.globo.com/Tecnologia/noticia/2019/02/como-computacao-quantica-vai-abalar-os-negocios-para-sempre.html>.

[114] Artigo 12 da LGPD. Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

[115] Entropia da informação é o uso de uma informação auxiliar para a reversão do processo de anonimização. No caso em análise, as informações adicionais estão em posse do agente de tratamento.

[116] O artigo 11 da GDPR estabelece que, se o propósito do tratamento dos dados pessoais não exige (ou não exige mais) que o agente seja capaz de identificar o titular, o agente não será obrigado a manter informações adicionais para identificá-lo. E, por não sê-lo, estará escusado de garantir os direitos de acesso, retificação, exclusão e portabilidade do titular - a menos que o próprio titular, buscando exercer esses direitos, forneça as informações adicionais para sua identificação. Disponível em <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/>.

[117] Artigo 13 da LGPD. Art. 13. “Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. (...) § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro”.O tema foi uma das últimas inclusões na Lei, tendo sido inserido pela primeira vez em 24.05.2018, pelo

relator, deputado Orlando Silva, no substitutivo 1 ao PL 4.060/2012 apresentado à Câmara dos Deputados.

118 Na pseudoanonimização, as informações adicionais que permitiriam a identificação do titular são mantidas em separado pelos agentes de tratamento, que podem, assim, reidentificar os dados se fizerem uso dessa informação. Contudo, caso excluam essas informações adicionais, os agentes não mais poderão efetuar a reidentificação "por meios próprios", caracterizando, assim, uma técnica de anonimização. É nesse sentido que a pseudoanonimização seria "o meio do caminho" para a anonimização.

119 A LGPD estabelece a necessidade de que, sempre que possível, haja a anonimização dos dados utilizados em pesquisas (arts. 7º, IV; 11, II, "c", 13 e 16, II), assim como determina que, embora uma das exceções à eliminação dos dados após o término do tratamento seja o uso exclusivo do controlador, ela está condicionada à vedação do acesso aos dados por terceiro e à anonimização dos dados (art. 16, IV).

120 Artigo 50 da LGPD. Art. 50. Os controladores e operadores, no âmbito de suas competências, pel tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (...) § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do*caput* do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I - implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; (...).

121 Como as informações adicionais que permitiriam a identificação do titular são mantidas separadamente e em posse dos agentes de tratamento, terceiros terão maior dificuldade em reverter a anonimização.

122 Artigo 5º da LGPD. Art. 5º Para os fins desta Lei, considera-se: (...) XVI - uso compartilhado d dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; (...).

[123] Sobre a estratégia regulatória baseada no risco e, em particular, relacionada ao conceito de dado pessoal e dado anonimizado, veja-se: RUBINSTEIN, Ira; HARTZOG, Woodrow. Anonymizatio and Risk (August 17, 2015). *91 Washington Law Review*, 703, 2016; *NYU School of Law, Public Law Research Paper* n.15-36. Disponível em: <https://ssrn.com/abstract=2646185>.

[124] Ao se considerar todo o ciclo de vida dos dados em sua divulgação, a análise (e preocupação) se desloca *do dado* - i.e. seus atributos, qualidades e riscos em determinado momento - para *o processo* - i.e. a realização de um conjunto de ações voltado à proteção da informação durante toda o seu processamento.

[125] Artigo 5º da LGPD: "Art. 5º Para os fins desta Lei, considera-se: (...) X - tratamento: tod operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (...)".

[126] RUBINSTEIN, Ira S. e HARTZOG, Woodrow. Anonymization... *op. cit.*, 2015.

[127] Artigo 13 do Decreto 8.771/2016. Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes. (...).

[128] FTC. Protecting consumer privacy in an era of rapid change: recommendations for businesses and policymakers, 2012; ROSENFELD, Dana B.; HUTNIK, Alysa Zeltzer. Data security contra clauses for service provider arrangements (pro-customer). *Practical Law Company*, 2011.

[129] Nesse sentido, uma das práticas previstas para se avaliar condutas pelo Modelo de Maturidade de Privacidade (*Privacy Maturity Model*), criado pelo Instituto Americano dos Contadores Públicos Certificados e pelo Instituto Canadense de Contadores (AICPA/CICA), é a otimização i.e. "a revisão e a avaliação periódicas são utilizadas para garantir a melhoria contínua de determinado processo". Disponível em <https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-

2011.pdf>. A aplicação desse modelo de análise (e a conformidade especificamente a essa prática) foi observada no tratamento de dados pessoais efetuado pela municipalidade de Seattle. Ver: Future of Privacy. City of Seattle: Open data risk assessment, 2018. Disponível em <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf>.

130 HARDY, Quentin. *Rethinking Privacy in an Era of Big Data*. Disponível em: <http://bits.blogs.nytimes.com/2012/06/04/rethinking-privacy-in-an-era-of-big-data/?_r=0>.

131 DEVRIES, Jennifer Valentino; VINE, Jeremy Singer. *They Know What You're Shopping For*. Disponível em: <http://www.wsj.com/articles/SB10001424127887324784404578143144132736214>.

132 Disponível em: <https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/>.

133 O Marco Civil acabou por definir o conceito de protocolo IP em seu art. 5º, III: "III – endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais".

134 Para caso de uso de IMEI para publicidade, ver <https://canaltech.com.br/publicidade/como-empresas-estao-usando-sua-geolocalizacao-para-campanhas-de-marketing-48533/>.

135 POULLET, Yves; DINANT, Jean-Marc. Informational self-determination in the internet era. Strasbourg: Conselho da Europa, 2004. p.33.

136 BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. *California Law Review*, v.104, p.2-6, 2016. Disponível em: <http://ssrn.com/abstract=2477899>.

137 BAROCAS, Solon; SELBST, Andrew D. *Big*... Op.cit., p.20-23.

138 Veja, *e.g.*, IZA WORLD OF LABOR. Anonymous job applications and hiring discrimination. Disponível em: <http://wol.iza.org/articles/anonymous-job-applications-and-hiring-discrimination-1.pdf>.

139 Vejam-se, entre outros, os projetos do Artificial Inteligence Institute (<https://ainowinstitute.org/>) e o projeto Fairness, Accountability and Transparency in Machine Learning (<https://www.fatml.org/>).

140 DONEDA, Danilo; ALMEIDA, Virgílio A. F. O que é governança de algoritmos. *Revista Politics*, publicação do Núcleo de Pesquisas e Estudo de Formação/NUPEF, n.24, out. 2016.

141 BIONI, Bruno Ricardo et al. Contribuição do Grupo... Op.cit., p.8. "Na seara da proteção de dados pessoais, outra dificuldade é delimitar o que poderia ser considerado um dado relacionado a uma pessoa identificável, quando por muitas vezes, devido justamente ao atual estado das tecnologias de tratamento de dados, é desnecessário identificar uma pessoa natural para sujeitá-la a uma decisão automatizada que possa influenciar o seu comportamento e, eventualmente, mitigar a sua privacidade (...) Por isso, a importância do texto normativo em alargar o seu espectro para cobrir

toda e qualquer informação isolada ou agregada que sujeite um determinado indivíduo a um processo de decisão automatizada". (Agradeço ao colega Renato Leite Monteiro pelas reflexões e troca de ideias sobre este tópico em específico, seja na contribuição do GPoPAI, seja pelas conclusões delineadas nesse trabalho).

142 Mesmo que a decisão não afete direitos e obrigações do titular, este ainda pode ser impactado de maneira a exigir certa proteção. É o caso de decisões que: (i) afetam as circunstâncias, os comportamentos e as escolhas dos indivíduos envolvidos; (ii) possuem efeito prolongado ou permanente no titular; e (iii) excluem ou discriminam indivíduos. Ver: ARTICLE 29, Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 21. Disponível em: <https://iapp.org/media/pdf/resource_center/W29-auto-decision_profiling_02-2018.pdf>.

143 Art. 12, § 2º: "Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada".

144 Veja a definição, por exemplo, de *differential privacy*: "Differential privacy, translated from Apple-speak, is the statistical science of trying to learn as much as possible about a group while learning as little as possible about any individual in it. With differential privacy, Apple can collect and store its users' data in a format that lets it glean useful notions about what people do, say, like and want. But it can't extract anything about a single, specific one of those people that might represent a privacy violation. And neither, in theory, could hackers or intelligence agencies (...)" (*Differential privacy lets you gain insights from large datasets, but with a mathematical proof that no one can learn about a single individual*. Disponível em: <https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/>).

145 Artigo 20 da LGPD: Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

146 Em conclusão similar, mas no contexto da GDPR: PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, jan. 2018, p. 40-81.

147 PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, jan. 2018, p. 80: "I believe that there is a third option which too deserves careful consideration, namely, to abandon the concept of personal data as a cornerstone of data protection altogether, and seek remedies for 'information-induced harms' – understood broadly as any individual or public negative consequences of information processing – without a sentimental attachment to this familiar proxy.

To preserve this formal distinction will always imply that there is also data that is not personal, and while the former triggers legal protection, the latter should not. This duality is at odds with the world where any information has the potential to affect people".

148 REALE, Miguel.*O estado democrático de direito e o conflito das ideologias*. São Paulo: Saraiva, 2005. p.104-105: "Nenhum conteúdo existencial é possível como ato singular isolado, o que decorre, aliás, do conceito mesmo de circunstância, que abrange, como vimos, também a *condicionalidade corpórea social do eu*. (...), o que demonstra que nenhum eu é real a não ser em relação com outros eus, nenhuma subjetividade é tal senão com a *intersubjetividade*, ou *socialidade*, determinando e legitimando a pluralidade das ideologias".

149 Ibidem, p. 105: "A pessoa do outro não é apenas um elemento circunstancial constitutivo do meu eu, pois ambos, o *eu* e o *outro eu*, acham-se condicionados transcendentalmente por algo que os torna histórica e realmente possíveis: esse algo que põe a subjetividade como intersubjetividade é, a meu ver, o valor da pessoa humana, qual, como tal, pode ser considerado o valor-fonte de todos os valores, e, por conseguinte, dos direitos humanos fundamentais".

150 GONÇALVES, Diogo Costa. Op.cit., p.40-60.

151 Ibidem, p.45-47: "A radical intimidade ontológica do Homem, que atrás consideramos, levou-nos a evidenciar notas de unicidade, irrepetibilidade, incomunicabilidade da sua estrutura ôntica. (...) A pergunta assim formulada pode parecer um pouco absurda... acaso não é evidente que o Homem vive em sociedade e sem vida social jamais realizaria os seus fins? (...) A relação, no Homem, é constitutiva da sua realidade ontológica. O Homem não é só *distinctum subsistens*, não é só imanência. Está aberto à relação, à transcendência... é um *distinctum subsistens*, mas um *distinctum subsistens respectivum*".

152 Ibidem, p.64: "Face à realidade do Homem, a primeira pergunta que fazemos é esta: *o que é Homem*? A esta questão responde-se com o conceito de pessoa: O homem é pessoa. Mas esta interrogação não esgota a problemática humana. Pelo contrário, lança-nos directamente numa outra pergunta distinta: se o Homem é pessoa, então *quem* é o Homem? E a esta pergunta – *quem*? – responde o conceito de personalidade".

153 CAMPOS, Diogo Lei de. Op.cit., p. 15: "Mas, além destes, existem outros só impropriament chamados direitos da personalidade (em sentido lato), que compreendem a actividade de inter-relacionamento da pessoa, a sua dimensão social, a pessoa-ser-social".

154 ALMEIDA, Kellyne Laís Laburú Alencar de. O direito ao livre desenvolvimento d personalidade: perspectiva do direito português. In: MIRANDA, Jorge; RODRIGUES JUNIC Otavio Luiz; FRUET, Gustavo Bonato (Org.)*Direitos da personalidade*. São Paulo: Atlas, 2012. p.69: "Mas não é só. Nenhum homem é uma ilha, nenhuma pessoa encerra-se em si mesma. O ser humano forma-se e conforma-se em seu relacionamento com os demais, no seio da sociedade que o abriga. A alteridade é parte da realidade humana, já que o homem só alcança a

plenitude de sua existência por meio das relações que estabelece".

155 TEPEDINO, Gustavo*Temas*... Op.cit., p.26-27: "Em síntese feliz, observou-se que o homem, como pessoa, manifesta dois interesses fundamentais: como indivíduo, o interesse a uma existência livre, como partícipe do consórcio humano, o interesse ao livre desenvolvimento da 'vida em relações'. A esses dois aspectos essenciais do ser humano podem substancialmente ser reconduzidas todas as instâncias específicas da personalidade".

156 O termo é de CAPELO DE SOUSA, Rabindranath V.A. Op.cit., p.243.

157 DONEDA, Danilo. *Da privacidade*... Op.cit., p.160.

158 FICI, Antonio; PELLECCHIA, Enza. Il consenso al tratamento. In: PARDOLESI, Roberto (Or *Diritto alla riservatezza e circolazione dei dati personali*. Giuffrè: Milano, 2003. p.513.

159 MARQUES, Garcia. MARTINS, Lourenço. Op.cit., p.336.

160 A LGPD assim define dado sensível em seu art. 5º, II: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual, genética ou biometria, quando vinculado a pessoa natural".

161 MENDES, Laura Schertel. *Transparência*... Op.cit., p.64.

162 DONEDA, Danilo. *Da privacidade*... Op.cit., p.162.

163 BRILL, Julie. Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions, p. Disponível em: <http://www.ftc.gov/system/files/documents/public_statements/202151/140220princetonbigdata_ "As we further examine the privacy implications of big data analytics, I believe one of the most troubling practices that we need to address is the collection and use of data — whether generated online or offline — to make sensitive predictions about consumers, such as those involving their sexual orientation, health conditions, financial condition, and race".

164 A LGPD considera essa possibilidade ao estabelecer que o regime dispensado à proteção de dados sensíveis "aplica-se a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica" (art. 17, § 1º).

165 KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes predictable from digital records of human behavior, p.1. Disponível em: <http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html>.

166 Ibidem, p.4.

167 DONEDA, Danilo. *Da privacidade*... Op.cit., p.161.

168 Veja, nesse sentido, a seção II da LGPD.

169 BANDEIRA DE MELLO, Celso Antônio*O conteúdo do princípio da igualdade*. São Paulo:

Malheiros, 2009. p.18.

[170] ANDRADE, Norberto Nuno Gomes de Andrade. Op.cit., p.20.

[171] O termo foi cunhado e trazido no contexto da era digital e correlacionado ao *Big Data* por MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. Op.cit., p.91.

[172] Veja, *e.g.*, TAVEIRA JÚNIOR, Fernando Tenório. A utilização da tecnologia RFID no mundo d computação ubíqua: algumas sugestões para a manutenção da privacidade, em um cenário futuro. In: ROVER, Aires José; CELLA, José Renato Gaziero; AYUDA, Fernando Galindo (Org *Direito e novas tecnologias*: XXIII Encontro Nacional do CONPEDI. Florianópolis: Conpec s.d. p.109-136.

[173] WEBER, Rof H. Internet of Things – New security and privacy challenges, p.23. Disponível en <https://www.academia.edu/>.

[174] *O que é internet das coisas*. Disponível em: <http://www.futurecom.com.br/blog/o-que-e-a-internet-das-coisas/>.

[175] STUART, Heritage.*Beware the internet of things*. Disponível em: <http://www.theguardian.com/commentisfree/2014/jan/26/beware-internet-of-things-fridges>.

[176] Saiba como a "internet das coisas" vai mudar seu cotidiano em breve. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/05/saiba-como-internet-das-coisas-vai-mudar-seu-cotidiano-em-breve.html>.

[177] Como já explicado em nota de rodapé, a Internet funciona por meio de protocolos de comunicações. Toda vez que um computador se conecta à Internet gera-se uma identificação para que os computadores possam se comunicar na rede, aperfeiçoando, assim, a transmissão e a troca de pacote de dados. Esse protocolo identifica, portanto, o computador conectado, sendo gerado um número pelo provedor de acesso durante aquela conexão. O IPV4 é o que estabelece tais endereços de comunicação, tendo um valor de 32 bits, o que equivale a 4.294.967.296 valores únicos. Dada a limitação de tais endereços, o provedor de acesso vale-se muitas das vezes de um endereço de IP dinâmico, isto é, que não é fixo para cada usuário – disperso entre vários usuários pelos respectivos tempos de conexão. Com a chegada do IPV6 ter-se-á um valor de 128 bits, c equivalente a 340 mil decilhões de números. Assim, será possível que cada usuário tenha o seu endereço de IP fixo, tal como cada objeto da Internet das coisas. Para uma comparação e os problemas em torno da transição entre o IPV4 e o IPV6, consultou-se: HUSTON, Geoff. C desafios da transição ao IPV6.*Revista Politcs*: publicação do Núcleo de Pesquisa e Formações/NUPEF, n.15, p.16-27, jun.2013.

[178] DONEDA, Danilo. O IPv6 e a internet das coisas (05 jan.2011). Disponível em <http://observatoriodainternet.br/o-ipv6-e-a-internet-das-coisas>.

[179] Apenas a título de ilustração, registra-se a realização de dois congressos sobre o tema no Brasil. Disponível em: <http://www.congressorfid.com.br/congresso/>.

[180] MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. Op.cit., p.96.

[181] DONEDA, Danilo. O IPV6... Op.cit.: "Vários dos sensores com seus próprios endereços IPv serão utilizados para fornecer informações pessoais a terceiros. Sensores com alto potencial neste sentido vão desde chips RFId a câmeras de vídeo (que poderão operar com maior eficiência), porém chegam até dispositivos com alto grau de intrusividade e opacidade que estão, hoje, em diversos graus de desenvolvimento, como a chamada *smart dust*".

[182] Ibidem: "As novas possibilidades abertas pelo IPv6 e pela sofisticação de diversos tipos de sensores são, portanto, mais um dos temas que devem ser abordados por um moderno sistema de proteção de dados pessoais".

[183] ANDRADE, Norberto Nuno Gomes de Andrade. Op.cit., p.20.

[184] SOLOVE, Daniel J. *The digital*... Op.cit., p.44.

[185] SOLOVE, Daniel J.*The digital*... Op.cit., p.46: "Our digital biography is revealing of ourselves but in a rather standardized way. It consists of bits of information pre-defined based on the judgment of some entity about what categories of information are relevant or important. We are partially captured by details such as our age, race, gender, net worth, property owned, and so on, but only in a manner that standardizes us into types or categories. Indeed, database marketers frequently classify consumers into certain categories based on stereotypes about their values, lifestyle, and purchasing habits".

[186] Art. 12: "conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito, pelo menos no que se refere às decisões automatizadas referidas no nº 1 do artigo 15º"; Art. 15: 1. "Os Estados-membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento. 2. Os Estados-membros estabelecerão, sob reserva das restantes disposições da presente directiva, que uma pessoa pode ficar sujeita a uma decisão do tipo referido no nº 1 se a mesma: a) For tomada no âmbito da celebração ou da execução de um contrato, na condição de o pedido de celebração ou execução do contrato apresentado pela pessoa em causa ter sido satisfeito, ou de existirem medidas adequadas, tais como a possibilidade de apresentar o seu ponto de vista, que garantam a defesa dos seus interesses legítimos; ou b) For autorizada por uma lei que estabeleça medidas que garantam a defesa dos interesses legítimos da pessoa em causa".

[187] Veja, nesse sentido, o já citado art. 10 da LGPD.

[188] SOLOVE, Daniel J. *The digital*... Op.cit., p.46.

[189] MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. Op.cit., p.176.

[190] Ibidem, p.57.

[191] Referimo-nos à troca de dados pessoais de passageiros aéreos entre União Europeia e Estados Unidos sob o fundamento de que se combateria o terrorismo (*Passager Name Record*). Disponível em: <http://www.migalhas.com/mostra_noticia.aspx?op=true&cod=154037>.

[192] ODLYZKO, Andrew. Privacy, Economics, and Price Discrimination on the Internet (July 27 2003). In: ICEC2003: FIFTH INTERNATIONAL CONFERENCE ON ELECTRO COMMERCE, N. Sadeh, ed., ACM, 2003. Disponível em: <http://ssrn.com/abstract=429762> ou <http://dx.doi.org/10.2139/ssrn.429762>. p.14-15.

[193] RAMASASTRY, Anita.*Web sites change prices based on customers' habits*. Disponível em: <http://www.cnn.com/2005/LAW/06/24/ramasastry.website.prices/>: "The Internet allows shoppers to easily compare prices across thousands of stores. But it also enables businesses to collect detailed information about a customer's purchasing history, preferences, and financial resources – and to set prices accordingly (...) In September 2000, Amazon.com outraged some customers when its own price discrimination was revealed. One buyer reportedly deleted the cookies on his computer that identified him as a regular Amazon customer. The result? He watched the price of a DVD offered to him for sale drop from $26.24 to $22.74".

[194] Veja, *e.g.*, RUBINSTEIN, Ira; LEE, Ronald D.; SCHWARTZ, Paul M. Data Mining and Inter Profiling: Emerging Regulatory and Technological Approaches. *University of Chicago Law Review*, v.75, p.261, 2008.

[195] PARISER, Eli. *O filtro invisível*: o que a internet está escondendo de você. Rio de Janeiro: Zahar 2012. Kindle Edition, posição 132.

[196] Ibidem, posição 213.

[197] Há uma passagem do supracitado autor que se aplica bem ao cenário descrito de como os dados pessoais influem na própria tomada de decisão na vida das pessoas datificadas: PARISER, Eli Op.cit., posição 237. "A personalização se baseia numa barganha. Em troca do serviço de filtragem, damos às grandes empresas uma enorme quantidade de dados sobre nossa vida diária – dados que muitas vezes não dividiríamos com nossos amigos. Essas empresas estão ficando cada vez melhores no uso desses dados para traçar estratégias. No entanto, muitas vezes acreditamos excessivamente que essas empresas irão cuidar bem dessas informações e, quando nossos dados são usados para tomar decisões que nos afetam negativamente, em geral não ficamos sabendo. Em última análise, a bolha dos filtros pode afetar a nossa capacidade de decidir como queremos viver".

[198] MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. Op.cit., p.151. "In addition to priva and propensity, there is a third danger. We risk falling victim to a dictatorship of data, whereby we fetishize the information, the output of our analyses, and end up misusing it. (...) The stakes are higher than is typically acknowledge. The dangers of failing to govern big data in respect to

privacy and predictions, or of being deluded about the data´s meaning, go far beyond trifles like targeted online ads".

[199] PARISER, Eli. Op.cit., posição 132: "Os algoritmos que orquestram a nossa publicidade estão começando a orquestrar nossa vida".

[200] BIONI, Bruno R.; MONTEIRO, Renato Leite. *Que tal uma pizza de tofu com rabanetes: você vai adorar*. Disponível em: <http://www.brasilpost.com.br/renato-leite-monteiro/que-tal-uma-pizza-de-tofu_b_7561906.htm>.

[201] RODATÀ, Stefano.*A vida na sociedade da vigilância*. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.17: "Estamos diante da verdadeira reinvenção da proteção de dados – não somente porque ela é expressamente considerada como um direito fundamental autônomo, mas também porque se tornou uma ferramenta essencial para o livre desenvolvimento da personalidade. A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio". E, mais à frente, arremata o citado autor (p.105-106): "A difusão do recurso aos perfis pode ocasionar a discriminação das pessoas que não correspondem ao modo geral, acentuando a estigmatização dos comportamentos desviantes e a penalização das minorias. Pode-se identificar aqui um obstáculo ao pleno desenvolvimento da personalidade individual".

[202] A lista a seguir não é exaustiva, consistindo, apenas, na revisão bibliográfica parcial realizada pelo autor. Citando Stefano Rodotà e acolhendo a inserção da proteção dos dados pessoais como uma linha evolutiva do direito à privacidade: DONEDA, Danilo.*Da privacidade*... Op.cit., p.101-147; SCHEREIBER, Anderson.*Direitos da*... Op.cit., p.130-134; MENDES, Laura Schertel. *Transparência*... Op.cit., p.14-24; LEONARDI, Marcel.*Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2012. p.67-78; TADEU, Silney Alves. Um novo direito fundamental: algumas reflexões sobre a proteção da pessoa e o uso informatizado de seus dados pessoais. *Revista de Direito do Consumidor*, ano 20, v.79, p.97, jul./set. 2011; LORENZETTI, Ricardo Luis. Informática, Cyberlaw e e-commerce. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (Org.). *Coleção doutrinas essenciais*: direito do consumidor – proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v.3, p.1.329-1.364. Tratando da proteção de dados, alocando-a como um direito à privacidade, deixando, no entanto, de traçar a linha evolutiva de Rodotà e sem a ele fazer alusão: GAMBOGI, Ana Paula. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (Org.).*Coleção doutrinas essenciais*: direito do consumidor – proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v.3, p.915-954; RAMOS, André de Carvalho. O pequeno irmão que nos observa: os direitos dos consumidores e os bancos de dados no Brasil. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (Org.)*Coleção doutrinas essenciais*: direito do consumidor – proteção da

confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v.3, p.957-974.

[203] LAFER, Celso.*A reconstrução dos direitos humanos*: um diálogo com o pensamento de Hannah Arendt. São Paulo: Companhia das Letras, 1988. p.258.

[204] DONEDA, Danilo. *Da privacidade*... Op.cit., p.126-127.

[205] COSTA JÚNIOR, Paulo José*O Direito de estar só*: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 2007. p.11.

[206] LAFER, Celso. Op.cit., p.263: "Com o advento da modernidade, a intimidade se colocou de maneira distinta, como resposta à emergência do social, ou seja, como reação ao conformismo nivelador da sociedade, que exige que seus membros se comportem como se fossem membros de uma grande família, com uma só opinião e um único interesse".

[207] ARENDT, Hannah. Op.cit., p.72.

[208] Ibidem, p.77.

[209] Ibidem, p.263.

[210] Ibidem, p.85

[211] ARENDT, Hannah. Op.cit., p.46.

[212] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: O direito à privacidade e os limites d função fiscalizadora do estado. *Revista da Faculdade de Direito da Universidade de São Paulo* v.88, p.441, 1993: "Este último, expresso por Hannah Arendt com base em Kant (cf. Celso Lafer, p.267), visa assegurar ao indivíduo a sua identidade diante dos riscos proporcionados pela niveladora pressão social e pela incontrastável impositividade do poder político. Aqui que é exclusivo é o que passa pelas opções pessoais, afetadas pela subjetividade do indivíduo e que não é dominada nem por normas nem por padrões objetivos. O princípio da exclusividade comporta três principais: a solidão (donde o desejo de estar só), o segredo (donde a exigência do sigilo) e autonomia (donde a liberdade de decidir sobre si mesmo como centro emanador de informações)".

[213] LAFER, Celso. Op.cit., p.268.

[214] CHINELATO, Silmara Juny. Op.cit., p.51: "Vida privada e intimidade são sinônimos. Aquela tem âmbito maior, que contém a intimidade, ou seja, vida privada e intimidade podem ser consideradas círculos concêntricos. O Código também foi omisso quanto ao segredo, círculo menor dentro do relativo à intimidade".

[215] FERRAZ JÚNIOR, Tércio Sampaio. Op.cit., p.442.

[216] BULOS, Uadi Lammêgo.*Curso de Direito Constitucional.* São Paulo: Saraiva, 2008. p.431: "A vida privada e a intimidade são os outros nomes do direito de estar só, porque salvaguardam a esfera do ser humano, insuscetível de intromissões externas (aquilo que os italianos chamam de rizervatezza e os americanos, privacy)".

[217] DOTTI, René Ariel.*Proteção da vida privada e liberdade de informação*. São Paulo: Revista dos Tribunais, 1980. p.71: "Genericamente, a vida privada abrange todos os aspectos que por qualquer razão não gostaríamos de ver cair no domínio público; é tudo aquilo que não deve ser objeto do direito à informação nem da curiosidade da sociedade moderna que, para tanto, conta com aparelhos altamente sofisticados".

[218] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Op.cit., p.282.

[219] BRANDELS, Louis. WARREN, Samuel. The right to privacy. Disponível em <http://civilistica.com/the-right-to-privacy/>.

[220] Art. 5º, X, da CF: "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"; Art. 21 do Código Civil: "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".

[221] Art. 5º, XI, da CF: "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial"; inciso XII: "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

[222] Propugnando tal dicotomia para tecer considerações sobre o direito à privacidade na sua "tradicional" vertente: CORDEIRO, António Menezes. Op.cit., p.259; PARDOLESI, Roberto. Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità. In: PARDOLESI, Roberto (Org.)*Diritto alla riservatezza e circolazione dei dati personali*. Milano: Giuffrè, 2003. p.1; FERRAZ JÚNIOR, Tércio Sampaio. Op.cit., p.440-441.

[223] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Op.cit., p.281.

[224] LEONARDI, Marcel. *Tutela*... Op.cit., p.46.

[225] SOLOVE, Daniel. *Understanding privacy*. Cambridge: Harvard University Press, 2008. p.44.

[226] Ibidem, p.45.

[227] Citando as respectivas expressões de André Vitalis e François Rigaux: DONEDA, Danilo*Da privacidade*... Op.cit., p.104.

[228] RODOTÀ, Stefano*Il diritto*... Op.cit., p.320: "La privacy, infatti, è estata construita come un dispositivo 'escludente', come uno strumento per allontanare lo sguardo indesiderato (...)".

[229] BODIN, Maria Celina. Apresentação do autor e da obra. In: RODATÀ, Stefano*A vida na sociedade da vigilância*. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro Renovar, 2008. p.7: "O notório conceito do 'direito a ficar só', o direito à vida privada atribuído

à elaboração de Warren e Brandeis (mas na verdade, adverte o autor, concebido por Robert Kerr quarenta anos antes), é qualitativamente diferente da privacidade como 'direito à autodeterminação informativa', o qual concede a cada um de nós um real poder sobre nossas próprias informações, nossos próprios dados. Percebe-se aqui, segundo Rodotà, um ponto de chegada na longa evolução do conceito de privacidade, da originária definição – *the right to be let alone* – ao direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada".

230 RODOTÀ, Stefano. *A vida*... Op.cit., p.17.

231 ANTONIALLI, Dennys*Privacy and International Compliance: When Differences Become an Issue*. p.14. Disponível em: <https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/viewFile/1165/1470>.

232 RODOTÀ, Stefano. *A vida*... Op.cit., p.17.

233 NIGER, Sergio.*Le nuove dimensioni della privacy*: dal diritto alla riservatezza alla protezione dei dati personalli. Padova: Cedam, 2006. p.70: "Le nuove dimensioni della privacy investono non solo l'aspetto del controllo sul flusso delle informazioni in uscita dall'interno della sfera privata verso l'esterno, ma anche l´ulteriore, e non secondario, aspetto delle informazioni in entrata".

234 RODOTÀ, Stefano.*Il diritto*... Op.cit., p.321: "la privacy viene inoltre definita come 'diritto di mantenere il controllo sulle proprie informazioni e di determinare le modalità di construzione della propriea sfera privata' e, in definitiva, come 'il diritto di scegliere liberamente il proprio modo di vivere'".

235 Ibidem, 2008, p.24.

236 RODOTÀ, Stefano. *A vida*... Op.cit., p.93.

237 RODOTÀ, Stefano.*Il diritto*... Op.cit., p.320: "L'originaria definizione della privacy come 'diritto a essere lasciato solo' non è estata cancellata, ma parte di un contesto via via arrichito da diversi punti di vista".

238 Nova dimensão é, por exemplo, a terminologia utilizada por: NIGER, Sergio. Op.cit., p.62-79.

239 Ponderando tal aspecto para fundamentar uma posição crítica à proteção dos dados pessoais como uma evolução do direito à privacidade: ZANON, João Carlos.*Direito à proteção dos dados pessoais*. São Paulo: Revista dos Tribunais, 2013. p.63: "Esse quadro traduz uma reflexão: seria essa forma de redefinição do direito à privacidade a melhor maneira do Direito nacional lidar com o advento das necessidades da contemporânea sociedade da informação? O ponto de partida para responder essa indagação, em nosso sentir, parece estar em considerar que essa evolução do direito à privacidade não significa – nem pode significar – uma *superação* dos velhos problemas de intromissão indevida na esfera íntima e na vida privada dos indivíduos. Estes antigos conflitos, a que poderíamos denominar de clássicas violações à privacidade, continuam

existindo, sendo, aliás, cada vez mais recorrentes".

240 RODOTÀ, Stefano. *Persona*... Op.cit., p.583-584.

241 TENNIS, Bradley. Op.cit., p.7.

242 ZANON, João Carlos. Op.cit., p.147: "Significa dizer que mesmo os cadastros e bancos de dados formados com dados pessoais que não envolvam aspectos da intimidade e vida privada do indivíduo submetem-se às regras do direito à proteção dos dados pessoais. Essa concepção depende, sobretudo, da percepção de que até as informações aparentemente mais inócuas podem ser integradas a outras e provocar danos ao seu titular".

243 Vejam-se, por exemplo, as discussões travadas sobre a legalidade das plataformas "Tudo sobre todos" e "Nomes Brasil" que foram orientadas em torno dessa dicotomia entre o público e privado. BIONI, Bruno Ricardo; RIBEIRO, Márcio Moretto*A transposição da dicotomia entre o público e o privado*. Disponível em: <http://jota.info/a-transposicao-da-dicotomia-entre-o-publico-e-o-privado>.

244 Parte dessa equívoca construção dogmática – do direito à proteção de dados pessoais como mera evolução do direito à privacidade – pode ser imputada ao fato de que parte da doutrina segue a experiência norte-americana que conecta a proteção dos dados pessoais à privacidade. Acontece que a *privacy* no sistema norte-americano ganhou tal alargamento, pois naquele sistema inexistem justamente os direitos da personalidade para tutelar de forma ampla a pessoa humana. Tal espécie de direito da personalidade faz as vezes de uma categoria jurídica geral para a defesa do livre desenvolvimento da personalidade, o que não é compatível com o ordenamento jurídico brasileiro. Veja-se por todos: ROOPO, Enzo. I diritti della personalità. In: ALPA, Guido BESSONE, Mario (Org.)*Banche dati telematica e diritti della personalità*. Padova: Cedam, 1984. p.52.

245 A expressão é de ZANON, João Carlos. Op.cit. p.67.

246 Compartilha-se, assim, do mesmo posicionamento de: ZANON, João Carlos. Op.cit. p.146-151. E arremata o citado autor (p.156): "À vista do exposto, voltamos a considerar que o direito à proteção dos dados pessoais volta-se à proteção da pessoa, assegurando-lhe e promovendo-lhe a dignidade, a paridade, a não discriminação e a liberdade. Correta, pois, a sua inserção entre os direitos da personalidade (...)".

247 HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales en la sociedad de la información*. Bilbao: Universidad de Deusto, 2003. p.16: "recapitulando se pude proclamar que el derecho a la protección de datos personales es un derecho de la personalidad por su condición de derecho inherente a la persona, esto es, el bien jurídico tutelado es proprio de la persona, y necesario para el pleno desarrollo da de su personalidad, en tanto que su vulneración priva a la persona del desfrute y goce de los más significativos derechos y libertades".

248 Registre-se que Danilo Doneda pode ter mudado de posicionamento tecido anteriormente em sua

obra monográfica sobre o tema (DONEDA, Danilo.*Da privacidade*... Op.cit.), diante da seguinte consideração em prefácio de sua autoria: DONEDA, Danilo. Prefácio. In: BESSA, Leonardo Roscoe. *Cadastro positivo*: comentários à Lei 12.414, de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011. p.10: "De fato, quando os cidadãos passam a ser cada vez mais avaliados e classificados apenas a partir de informações a seu respeito, a proteção e o cuidado com estas informações deixa de ser um aspecto que somente diga respeito às esferas do sigilo ou da privacidade, passando a figurar um componente essencial para determinar o grau de liberdade de autodeterminação individual de cada pessoa". E, ainda, em outra obra, o referido autor ressalva a "autonomia da temática da proteção dos dados pessoais": DONEDA, Danilo. Princípios e proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.).*Direito & Internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. p.370.

249 DONEDA, Danilo.*Da privacidade*... Op.cit., p.100: "Algumas normativas específicas para a proteção da pessoa surgem então em torno de necessidades específicas – seja no caso da problemática pesquisa genética ou, no nosso caso, em torno da proteção dos dados pessoais".

250 MARTINS, Leonardo. *Introdução à jurisprudência do Tribunal Constitucional Federal Alemão*: Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leonardo Martins. Prefácio: Jan Woischnik. Trad. Beatriz Hennig et al. Montevidéu: Fundação Konrad Adenauer, 2005. p.233-234.

251 Ibidem, p.234: "O § 9 da Lei previa, entre outras, a possibilidade de uma comparação dos dados levantados com os registros públicos e também a transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais para determinados fins de execução administrativa".

252 Ibidem, p.244.

253 Nesse sentido são as considerações de: MENDES, Laura Schertel.*O direito*... Op.cit., p.52; DONEDA, Danilo.*Da privacidade*... Op.cit., p.196-197; GAMBOGI, Ana Paula. Op.cit., p.925; WALZ, Stefan. Protezione dei dati: L'esperienza tedesca. In: ALPA, Guido; BESSONE, Mario (Org.). *Banche dati telematica e diritti della personalità*. Padova: Cedam, 1984. p.101. Anota-se que na tradução do julgado utilizou-se a expressão "autodeterminação sobre a informação": MARTINS, Leonardo. Op.cit., p.235.

254 MARTINS, Leonardo. Op.cit., p.187: "O Art. 2 I GG tem uma importância prática ímpar. Se sempre destacado caráter subsidiário em face das outorgas específicas não afasta seu significado. Pelo contrário: como último limite à ação estatal cerceadora da liberdade individual, ele precisou ser dogmática e minuciosamente concretizado. Também aqui o TCF não foi omisso, mas, pelo contrário, em um número de decisões muito relevantes que chega à casa das dezenas, concretizou vários aspectos, chegando a criar verdadeiros 'direitos', a partir da derivação do

conceito de livre desenvolvimento encontrado no Art. 2 I GG, como foi o caso do direito à autodeterminação sobre informações (ou dados) pessoais (*informationelles Selbstbestimmungsrecht*) na decisão *Volkszählung* (BVerfGE 65, 1 – cf. abaixo: decisão 20)".

255 MARTINS, Leonardo. Op.cit., p.237: "Esse poder necessita, sob as condições atuais e futuras d processamento automático de dados, de uma proteção especialmente intensa. Ele está ameaçado, sobretudo porque em processos decisórios não se precisa mais lançar mão, como antigamente, de fichas e pastas compostos manualmente. Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (dados relativos à pessoa [cf. § 2 I BDSG – Lei Federal sobre a Proteção de Dado Pessoais]) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. Com isso, ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas".

256 Ibidem, p.236-238: "Quem não consegue determinar com suficiente segurança quais informações sobre sua pessoa são conhecidas em certas áreas de seu meio social, e quem não consegue avaliar mais ou menos o conhecimento de possíveis parceiros na comunicação, pode ser inibido substancialmente em sua liberdade de planejar ou decidir com autodeterminação. (...) Daí resulta: O livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. Esta proteção, portanto, é abrangida pelo direito fundamental do Art. 2 I c. c. Art. 1 I GG. O direito fundamental garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais".

257 MARTINS, Leonardo. Op.cit., p.239.

258 Essa é terminologia usada, mais de uma vez, ao longo do julgado. Ibidem, p.242.

259 Ibidem, 239: "Com isso, um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados 'insignificantes' no contexto do processamento eletrônico de dados. O fato de informações dizerem respeito a processos íntimos não decide por si só se elas são sensíveis ou não. É muito mais necessário o conhecimento do contexto de utilização, para que se constate a importância do dado em termos de direito da personalidade".

260 Ibidem, p.243: "De especial importância para os levantamentos estatísticos são as eficazes regras de bloqueio em face do mundo exterior. Para a proteção do direito de autodeterminação sobre a informação é imprescindível a manutenção em sigilo absoluto dos dados individuais obtidos para

fins estatísticos – e já desde o processo de levantamento – enquanto existir uma referência pessoal ou esta puder ser produzida (segredo estatístico); o mesmo vale para a obrigação de tornar, o mais cedo possível, anônimos (de fato) os dados, associada a precauções contra a quebra do anonimato".

261 Ibidem, p.244: "Uma eventual transmissão (entrega) dos dados que não sejam anônimos nem tenham sido processados estatisticamente – portanto, que sejam ainda pessoais – encerra problemas especiais".

262 MARTINS, Leonardo. Op.cit., p.215: "O TCF julgou presentes as condições processuais d apresentação judicial e no mérito confirmou a constitucionalidade dos dispositivos da lei do microcenso, que havia sido questionada pelo juízo representante. Na fundamentação, o TCF considerou, em suma, que os dados levantados não atingiam a esfera íntima intocável do indivíduo e que a intervenção estava justificada por ser formalmente permitida pelo Art. 2 I GG e materialmente proporcional em face do propósito de abastecer o Estado com dados necessários ao planejamento da ação estatal".

263 MARTINS, Leonardo. Op.cit., p.240: "A obrigação de fornecer dados pessoais pressupõe que o legislador defina a finalidade de uso por área e de forma precisa, e que os dados sejam adequados e necessários para essa finalidade. Com isso não seria compatível a armazenagem de dados reunidos, não anônimos, para fins indeterminados ou ainda indetermináveis. Todas as autoridades que reúnem dados pessoais para cumprir suas tarefas devem se restringir ao mínimo indispensável para alcançar seu objetivo definido".

264 Ibidem, p.241: "No levantamento de dados para fins estatísticos não se pode exigir uma vinculação estrita e concreta dos dados à finalidade. Segundo a essência da estatística, os dados devem ser utilizados para as tarefas mais diversas, não determináveis de antemão; consequentemente, existe também uma necessidade de armazenagem de dados. (...) O recenseamento deve ser levantamento e manipulação com múltiplas finalidades, portanto reunião e armazenagem de dados, para que o Estado possa enfrentar, estando para tanto preparado, o desenvolvimento da sociedade industrial. Também as proibições de transmissão e uso de dados preparados estatisticamente seriam contrárias à sua finalidade".

265 DONEDA, Danilo. *Da privacidade*... Op.cit., p.195; MENDES, Laura Schertel*Transparência*... Op.cit., p.47.

266 MARTINS, Leonardo. Op.cit., p.241: "Se a diversidade das possibilidades de uso e associação d dados não é determinável antecipadamente, pela natureza da estatística, são necessários limites compensatórios no levantamento e no uso da informação dentro do sistema de informação. É necessário criar condições de manipulação claramente definidas que garantam que o indivíduo não se torne um simples objeto de informação, no contexto de um levantamento e manipulação automáticos dos dados relativos à sua pessoa".

[267] Nesse sentido é a advertência de DONEDA, Danilo. *Da privacidade*... Op.cit., p.198: "(...) já em uma leitura em chave liberal a autodeterminação concentrar-se-ia no ato do consentimento da pessoa para o tratamento dos dados pessoais e assumiria contornos negociais, e assim prestar-se-ia ao afastamento da matéria do âmbito dos direitos da personalidade".

[268] MAYER-SCHONEBERGER, Viktor. Generational development of data protection in Europe. I AGRE, Phillip E.; ROTENBERG, Marc (Org.). *Technology and Privacy*: The New Landscape. Cambridge: The MIT Press, 1997, p. 229-230.

[269] MARTINS, Leonardo. Op.cit., p.243: "Esse objetivo somente será atingido se for criada n cidadão, que é obrigado a fornecer informações, a confiança necessária na proteção de seus dados coletados para fins estatísticos, sem a qual não se pode contar com sua prontidão em fornecer dados verdadeiros (correta a fundamentação do governo federal sobre o projeto da Lei do Recenseamento de 1950, cf. BTDrucks 1/1982, p.20 sobre o § 10). Uma ação governamental que não se esforçasse pela formação de tal confiança, por meio da transparência do processo de processamento de dados e de sua estrita proteção, levaria a longo prazo à decrescente prontidão para cooperação, porque surgiria a desconfiança [sobre o modo de processamento e o próprio destino dos dados]".

[270] LEMOS, Ronaldo.*Ou a sociedade acompanha internet ou a democracia começa a ficar em xeque*. Disponível em: <http://blogdomorris.blogfolha.uol.com.br/2014/04/08/ou-sociedade-acompanha-internet-ou-democracia-comeca-a-ficar-em-xeque/>.

[271] MENDES, Laura Schertel. *O direito*... Op.cit., p.76.

[272] DONEDA, Danilo. *Da privacidade*... Op.cit., p.372.

[273] BELLEIL, Arnaud.*@privacidade*: o mercado dos dados pessoais: protecção da vida privada na idade da internet. Lisboa: Piaget, 2001. p.7.

[274] Ibidem, p.39.

[275] A alusão é ao título de sua obra: BAUMAN, Zygmunt.*Vida para consumo*: a transformação das pessoas em mercadoria. Rio de Janeiro: Zahar, 2008.

[276] Vide: todas as considerações sobre a proteção dos dados pessoais como espécie autônoma dos direitos da personalidade.

[277] O poder econômico e o progresso tecnológico historicamente têm se colocado como adversários na luta pelos direitos do homem: "A luta pelos direitos teve como primeiro adversário o poder religioso; depois, o poder político; e, por fim, o poder econômico. Hoje, as ameaças à vida, à liberdade e à segurança podem vir do poder sempre maior que as conquistas da ciência e das aplicações dela derivadas dão a quem está em condição de usá-las. Entramos na era que é chamada de pós-moderna e é caracterizada pelo enorme progresso, vertiginoso e irreversível, da transformação tecnológica, e, consequentemente, também tecnocrática do mundo. Desde o dia em

que Bacon disse que ciência é poder, o homem percorreu um longo caminho! O crescimento do saber só fez aumentar a possibilidade do homem dominar a natureza e os outros homens" (BOBBIO, Norberto. *A era*... Op.cit., p.209).

278 BIONI, Bruno R. Por que proteção de dados importa? TEDxPinheiros, 2018. Disponível e <https://www.youtube.com/watch?v=TzI5VfvQA6I>.

279 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Elaboração: André-Pascal. França: OECD Publications Service, 2011. p. 32. *The OECD Privacy Framework 2013*. p. 3-5 (prefácio). Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

280 BIONI, Bruno Ricardo. Brasil precisa ser competitivo em uma economia de dados.*Jornal Valor Econômico*, jul. 2018. Disponível em: <https://www.valor.com.br/opiniao/5669703/pais-precisa-ser-competitivo-em-uma-economia-de-dados>.

281 GRAU, Eros Roberto. *A ordem econômica na Constituição de 1988*. São Paulo: Malheiros, 2005 p. 193-195: "É que, de um lado, não se pode visualizar a ordem econômica constitucional como produto de imposições circunstanciais ou meros caprichos dos constituintes, porém como resultado do confronto de posturas e texturas ideológicas e de interesses que, de uma ou outra forma, foram compostos, para como peculiar estrutura ideológica, aninhar-se no texto constitucional. (...) Todo esse conjunto de princípios, portanto, há de ser ponderado, na sua globalidade, se pretendemos discernir, no texto constitucional, a definição de um sistema e de um modelo econômicos. A constituição não é um mero agregado de normas; e nem se pode interpretar em tirar, aos pedaços. Será de todo conveniente, destarte, deitarmos atenção a esse conjunto, o que, não obstante, importará o exame de cada qual de tais princípios, separadamente". Em sentido análogo: COMPARATO, Fábio Konder. A proteção do consumidor na Constituição brasileira de 1988. In: MARQUES, Claudia Lima; MIRAGEM, Bruno (orgs *Direito do consumidor*: vulnerabilidade do consumidor e modelos de proteção. São Paulo: Revista dos Tribunais, 2011. v. 2, p. 182 (Coleção Doutrinas Essenciais do Direito do Consumidor): "Não há, pois, como se negar que o princípio constitucional de proteção ao consumidor tem, pelo menos, a mesma importância hierárquica que o da livre-iniciativa e atuação empresarial".

282 RODOTÀ, Stefano. A vida... op. cit., p. 46: "Logo, não podemos nos limitar a falar da informação como 'recurso', ou o 'bem' fundamental da sociedade que está se delineando diante dos nossos olhos. As tecnologias interativas criam uma nova 'mercadoria' da qual a legislação tende a se ocupar nas novas disciplinas relativas à 'cable privacy' ou nos sistemas de videotexto".

283 A expressão foi citada por NIGER, Sergio. Op.cit., p. 150 e DONEDA, Danilo. *Da privacidade*... Op.cit., p. 131.

284 A expressão foi citada por SOLOVE, Daniel. Introduction: privacy self-management and th

consent dilemma. *Harvard Law Review*, v. 126, 2013, p. 1.884. Disponível em: <http://www.harvardlawreview.org/media/pdf/vol126_solove.pdf>.

Parte II

CONSENTIMENTO E A (RE)AVALIAÇÃO DO SEU PAPEL NORMATIVO NA PROTEÇÃO DOS DADOS PESSOAIS

Capítulo III

A TRAVESSIA DO PROTAGONISMO DO CONSENTIMENTO

3.1 O CONTEXTO INICIAL EM TORNO DA DEMANDA REGULATÓRIA DA PROTEÇÃ DOS DADOS PESSOAIS E A PRIMEIRA GERAÇÃO[1] DE LEIS[2]

A demanda regulatória subjacente à proteção dos dados pessoais surge, basicamente, com a formação do Estado Moderno[3]. Após a Segunda Guerra Mundial, a máquina administrativa percebe que as informações pessoais dos seus cidadãos são úteis para planejar e coordenar as suas ações para um crescimento ordenado[4].

A tecnologia foi o que viabilizou essa nova faceta do Estado, especialmente a ciência computacional que revolucionou quantitativa e qualitativamente a capacidade de processamento de tais informações (vide subcapítulo 1.1.1 *supra*). É justamente nesse contexto que alguns países começaram a cogitar a criação de bancos de dados unificados (*National Data Centers*), enxergando-os como parte do ferramental necessário para a expansão orgânica da população[5].

A *primeira geração* de leis de proteção de dados pessoais decorre, assim, da preocupação com o processamento massivo dos dados pessoais dos cidadãos na conjuntura da formação do Estado Moderno[6]. Naquela época, a saída regulatória foi focar na própria tecnologia[7] que deveria ser domesticada[8] e orientada pelos valores democráticos. Temia-se a emergência da figura *orwelliana* do Grande Irmão, que poderia sufocar a liberdade do cidadão com uma vigilância ostensiva[9]. Optou-se, então, por controlar a criação desses bancos de dados por meio da concessão de autorizações para o seu funcionamento[10].

Em suma, o que marca a primeira geração de proteção dos dados pessoais é o seu foco na esfera governamental, bem como na premissa em se estabelecer normas rígidas que domassem o uso da tecnologia[11]. Todavia, o processamento de dados transcendeu a esfera governamental, o que aumentou a quantidade de atores e, simetricamente, o número de bancos de dados a serem regulados-autorizados. Esse novo cenário exigiu uma nova estrutura normativa.

3.2 AS SUBSEQUENTES GERAÇÕES DE LEIS DE PROTEÇÃO DE DADOS PESSOAIS: EMERGÊNCIA, QUESTIONAMENTO E A REAFIRMAÇÃO DO PAPEL DE PROTAGONISMO DO CONSENTIMENTO

A *segunda geração* de leis de proteção de dados pessoais é caracterizada por uma mudança do âmago regulatório. Preocupa-se não somente com as bases de dados estatais, mas, também, com as da esfera privada[12]. A figura do Grande Irmão (uma única e centralizada base de dados) é diluída pela de Pequenos Irmãos (bancos de dados dispersos no plano estatal e privado)[13].

Com isso, percebe-se que seria inviável a estratégia regulatória anterior em que incumbia ao Estado licenciar a criação e o funcionamento de todos os bancos de dados. A segunda geração de leis transfere para o próprio titular dos dados a responsabilidade de protegê-los. Se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais[14].

Destaca-se, nesse sentido, o referencial teórico de Alan Westin que compreendia a privacidade como a "reivindicação dos indivíduos, grupos e instituições de determinar, por eles mesmos, quando, como e em qual extensão suas informações pessoais seriam comunicadas aos outros"[15]. Dá-se ênfase à autonomia do indivíduo em controlar o fluxo de suas informações pessoais[16].

A amplitude desse papel de protagonismo[17] do indivíduo na proteção dos dados pessoais é o divisor de águas para a *terceira geração* de leis. Nesse estágio, as normas de proteção de dados pessoais procuraram assegurar a participação do indivíduo sobre todos os movimentos dos seus dados pessoais: da coleta ao compartilhamento[18]. Alcançar-se-ia, assim, o êxtase da própria terminologia da "autodeterminação informacional", pois, com tal participação, possibilitar-se-ia que o sujeito tivesse um controle mais extensivo sobre as suas informações pessoais.

Não por outra razão, Viktor Mayer-Schoneberger elege a analisada decisão da Corte Constitucional alemã como emblemática para a terceira geração das leis de proteção de dados pessoais[19], em que pese, como já destacado, tal julgado ter focado também na criação de deveres para quem coleta e processa dados pessoais, cuja abordagem é complementar e, em certa medida, minimiza o protagonismo do titular das informações pessoais.

Fato é, contudo, que a própria emergência do consentimento como vetor central para a proteção dos dados pessoais carregou consigo seus complicadores. Desde a segunda geração das leis de proteção de dados pessoais já se questionava a efetividade de um quadro normativo focado no poder de escolha dos indivíduos. Já naquela época, diversas relações sociais tinham como condição a entrega dos dados pessoais para o seu aperfeiçoamento. Entre as burocracias governamentais, o exercício da cidadania pelo voto e o acesso a bens de consumo (*e.g.*, os bancários) exigiam o fornecimento dos dados pessoais como a chave para a porta de entrada dessas relações sociais[20]. Na feliz expressão de Mayer-Schoneberger, somente os eremitas alcançariam a proteção plena de seus dados, já que, como decorrência da sua recusa em fornecê-los, amargariam o custo social[21] decorrente da exclusão de tais atividades[22].

A *quarta geração* veio para cobrir essa deficiência das gerações de leis anteriores. A disseminação de autoridades independentes para a aplicação das leis de proteção de dados

pessoais[23], bem como de proposições normativas, que não deixavam ao reino do indivíduo a escolha sobre o processamento de certos tipos de dados pessoais (*e.g.*, sensíveis)[24], relativizaram a referenciada centralidade do consentimento[25].

Ao mesmo tempo, contudo, esse progresso geracional não eliminou o protagonismo do consentimento. A sua centralidade permaneceu sendo o traço marcante da abordagem regulatória. Tanto é verdade que, em meio a esse processo evolutivo, o consentimento passou a ser adjetivado[26], como devendo ser livre, informado, inequívoco, explícito e/ou específico, tal como ocorreu no direito comunitário europeu[27]. Essa distribuição de qualificadores acaba, portanto, por desenhar um movimento refratário em torno do papel de destaque do consentimento quase como sendo sinônimo de autodeterminação informacional.

O progresso geracional normativo da proteção dos dados pessoais assinala, destarte, um percurso no qual o consentimento emerge, é questionado e se reafirma como sendo o seu vetor central. Com isso, o titular dos dados pessoais permanece sendo o seu ponto focal[28], o que é replicado até os dias de hoje. A construção e a própria interpretação das normas a respeito da proteção dos dados pessoais têm seguido esse norte regulatório.

3.3 A REDOMA DO CONSENTIMENTO NA NORMATIZAÇÃO DA PROTEÇÃO DOS DADOS PESSOAIS

3.3.1 *Fair Information Practice Principles/FIPPs* e as *guidelines* da Organização para a Cooperação e Desenvolvimento Econômico

As *guidelines* da OCDE são de sobremaneira importância para a compreensão do arranjo normativo acima descrito.

A OCDE é um organismo internacional multilateral[29] criado após a Segunda Guerra Mundial, em 1948, cuja missão é promover o bem-estar econômico e social global[30]. Nesse sentido, tal organismo tem como objetivo estabelecer uma relação de cooperação entre seus países-membros para a solução de problemas comuns que os afligem. Visa, em última análise, estabelecer padrões que desencadeiam respostas uniformes para tanto[31].

Dentre tais questões, em 1980, percebeu-se que o desenvolvimento econômico e social havia sido redimensionado pela tecnologia da informação[32] e era, especialmente, dependente do processamento dos dados pessoais dos cidadãos. Fazia-se necessário conciliar o desenvolvimento econômico e a proteção da privacidade das pessoas[33].

Nesse contexto, a OCDE emitiu dois importantes documentos (*privacy guidelines* em 1980 e *declaration on transborder data flows* em 1985), que vieram a influenciar mundialmente o desenvolvimento da proteção dos dados pessoais; aliás, não poderia ser diferente, haja vista ser esta

a finalidade intrínseca da OCDE como um organismo internacional multilateral.

Tais *guidelines* estabeleciam padrões normativos para a proteção dos dados pessoais, a fim de assegurar o livre fluxo de informações entre seus países-membros[34]. Por isso, além de haver uma parte geral conceitual sobre, por exemplo, a definição de dados pessoais[35], havia uma segunda parte que vinculava[36] os seus países-membros a incorporar os princípios previstos em tal documento. O resultado desejado era criar um *ambiente regulatório uniforme* entre os países-membros e, ante a inexistência de disparidades regulatórias, garantir o livre trânsito de informações.

Dos oito princípios elencados[37], verifica-se que a metade[38] deles faz alusão expressa ao titular dos dados. Um deles é inclusive nomeado como princípio da *participação individual*.

Nesse sentido, o princípio da "limitação da coleta"[39], seguido pelo princípio da especificação dos propósitos[40], estabelece a *técnica normativa* pela qual o titular dos dados deve ser informado sobre as finalidades do seu processamento[41] para, então, autorizá-lo, consolidando-se, por fim, a sua participação ao longo de todo o fluxo informacional.

Destas normas fundacionais decorrem outros direitos que complementam essa ideia da autodeterminação informacional, como, por exemplo, o poder de o indivíduo retificar, emendar, apagar e/ou completar seus dados pessoais[42].

Trata-se de normas que elevam o próprio titular dos dados pessoais como o seu grande protagonista. A própria noção do que seja um tratamento de dados pessoais justo e lícito é vinculada ao consentimento do indivíduo.

Essa orientação normativa acabou por ser denominada *Fair Information Practice Principles/FIPPs*[43-44], de modo que o que determina ser (i)lícita qualquer atividade de tratamento de dados pessoais é a carga participativa do cidadão ao longo do fluxo informacional.

Com isso, estabelece-se uma diretriz normativa, que é o cidadão ter controle sobre seus dados pessoais, como sinônimo de autodeterminação informacional. Daí por que as *guidelines* da OCDE situam-se entre a terceira e a quarta geração de leis de proteção de dados pessoais.

O segundo documento, a declaração sobre o fluxo transfronteiriço de dados (*declaration on transborder data flows*, de 1985), é elucidativo sobre a disseminação dessa orientação normativa ao redor do mundo. A OCDE havia constatado a necessidade de harmonizar os mais diversos ambientes regulatórios dos seus países-membros para que não houvesse disparidades regulatórias que obstaculizassem o livre fluxo informacional entre eles[45].

Em 2013, ambas as *guidelines* sofreram um processo de revisão[46], tendo sido mantida, no entanto, a sua espinha dorsal. Após 30 (trinta) anos[47], havia maior preocupação com questões procedimentais pertinentes à sua implementação.

De um lado, a diretriz normativa da autodeterminação informacional permaneceu intacta, mas com a ressalva de que novas tecnologias emergiram e, com isso, a coleta e o uso dos dados estavam cada vez mais complexos e menos transparentes. Seria necessário investigar meios que reduzissem essa opacidade e, por conseguinte, garantissem aos indivíduos controle sobre suas informações[48].

Nota-se, portanto, que as *guidelines* da OCDE também experimentaram um movimento pendular do consentimento: a sua emergência, o questionamento e a reafirmação como ponto focal da dinâmica regulatória.

De outro lado, ainda se buscava fazer ajustes em termos de interoperabilidade legal[49] entre os países-membros. E, nesse sentido, mais do que haver uniformidade normativa, o processo de revisão aponta para a necessidade de ações coordenadas para a aplicação e a fiscalização das leis de proteção de dados pessoais, por ser isto também um elemento crucial para o livre fluxo informacional transfronteiriço[50].

Resulta, portanto, de mais de 3 (três) décadas a proeminência[51] das *guidelines* da OCDE, as quais vieram a influenciar[52] as mais diversas legislações sobre proteção de dados pessoais ao redor do mundo[53]. Esse processo teve como fio condutor a elevação do titular dos dados pessoais como principal ator da dinâmica normativa sobre proteção de dados pessoais. A replicação de muitos dos direitos acima elencados nas mais diversas legislações, que convergem para o papel de destaque que o consentimento do titular dos dados desempenha nesse arranjo normativo, é elucidativa para a compreensão de como até hoje foram estruturadas as normas sob tal temática ao redor do mundo.

3.3.2 O direito comunitário europeu (Conselho da Europa e União Europeia): da Convenção 1 à GDPR[54]

O direito comunitário europeu exprime bem a travessia do consentimento no percurso geracional das leis de proteção de dados pessoais, cuja linha evolutiva permanece em curso até hoje; a começar pela influência das *guidelines* da OCDE que se sente na primeira normatização sobre o tema no direito comunitário europeu. A Convenção 108, da década de 1980, de *Strasbourg*[55], do Conselho da Europa, é resultado do movimento promovido pela OCDE para facilitar a harmonização das legislações de proteção de dados pessoais[56].

Nesse sentido, o próprio preâmbulo dessa norma de direito internacional correlacionou a proteção dos dados pessoais ao livre fluxo informacional[57], dedicando, inclusive, um capítulo inteiro sobre o "Fluxo Transfronteiriço dos Dados"[58]. Para além da coincidência terminológica, há, sobretudo, uma carga ideológica que foi posta em curso não só pelo organismo internacional multilateral, mas, também, pelo bloco continental europeu, o que rege, até hoje, o seu quadro normativo de proteção de dados pessoais[59].

Veja-se, por exemplo, que 02 (duas) décadas depois, a Diretiva Europeia de Proteção de Dados Pessoais (95/46/EC) da União Europeia irá transpor a mesma correlação em suas considerandas[60] e, principalmente, irá traduzir[61], em normas mais específicas, a promessa antes firmada na Convenção de *Strasbourg* de assegurar aos indivíduos o controle sobre as suas informações pessoais[62]. Dito de outra forma, irá adotar as FIPPs como a sua espinha dorsal, de modo que a autodeterminação do indivíduo é o que parametriza a (i)licitude de qualquer atividade de tratamento dos dados pessoais.

Nesse sentido, como já dito anteriormente, a diretiva europeia irá adjetivar o consentimento na

tentativa de operacionalizá-lo. A sua qualificação como devendo ser livre, informado, inequívoco, explícito e/ou específico[63] é uma das características marcantes do progresso geracional das leis de proteção de dados pessoais, na medida em que procura resolver a problemática em torno de um controle ilusório ou pouco efetivo das informações pessoais por parte do seu titular (vide subcapítulo 3.2 *supra*).

Nesse sentido, aliás, a diretiva irá impor não só o direito de o titular dos dados pessoais controlá-los, mas, simetricamente, deveres aos *data controllers* – quem processa os dados pessoais – para aperfeiçoar tal estratégia regulatória.

Por exemplo, o princípio da proporcionalidade[64] cria a obrigação de o *data controller* não coletar dados excessivos frente ao propósito especificado para o tratamento dos dados pessoais. Trata-se da ideia da minimização[65] dos dados (*data minimization*) que permitirá, em última análise, que o titular dos dados pessoais maximize a sua esfera de controle sobre as suas informações pessoais. Quanto menos dados em fluxo, mais fácil é exercer controle sobre eles.

Trata-se, enfim, de uma abordagem regulatória que se centra nesses dois atores[66] – o titular das informações pessoais e quem as processa – para, por meio de direitos e obrigações simétricas, ser garantido o prometido controle dos dados pessoais.

É importante destacar que a diretiva posiciona o princípio da minimização como sendo um dever de quem é o responsável pela atividade de tratamento de dados. Diferentemente, as *guidelines* da OCDE imputavam[67] a referida limitação apenas ao titular dos dados pessoais (vide subcapítulo 3.3.1), não havendo o dever de cooperação dos outros atores envolvidos nessa relação jurídica. Essa diferença é o que situa as *guidelines* na terceira geração das leis de proteção dos dados pessoais e, por seu turno, a diretiva na quarta geração. Essa última etapa evolutiva é marcada pela promulgação de normas que procuram empoderar o titular com o controle de suas informações pessoais e, por isso, expandem o seu espectro para todos os sujeitos inseridos ao longo da cadeia do fluxo informacional (vide subcapítulo 3.2).

Nesse sentido, a Diretiva Europeia (2002/58) sobre o tratamento e a proteção da privacidade nas comunicações eletrônicas veio para conformar tal capacitação no ambiente eletrônico[68]. As suas considerandas são um rico retrato de tal objetivo.

Por um lado, verificam-se proposições genéricas a esse respeito, reafirmando que o consentimento deve ser livre, específico e informado para corresponder aos anseios do titular no tocante ao controle dos seus dados pessoais[69]. Tal controle deve ser, aliás, realizado preferencialmente de forma prévia à coleta e ao processamento de seus dados pessoais[70].

Acumulam-se, ainda, proposições bem específicas, indicando-se os meios pelos quais seria operacionalizado tal controle. Propõe-se a utilização de "caixas de diálogo", a serem exibidas pelo *website*, para que o usuário as assinale como uma forma de externar o seu consentimento[71]; ou outros métodos capazes de informar o usuário para que ele exerça, de forma "amistosa", o controle sobre seus dados pessoais[72]; e, ainda, listando, de forma não exaustiva, quais seriam as ferramentas de

coleta de dados pessoais, como *cookies*[73], *web bugs* e *spywares*[74].

Essa mesma matriz foi adotada na reforma (regulação) da diretiva de proteção de dados no direito comunitário europeu (GDPR –*General Data Protection Regulation*)[75]. Na proposta apresentada e aprovada pelo *Trialogue* da União Europeia em dezembro de 2015[76], verifica-se, mais uma vez, a preocupação nuclear em torno do consentimento. Em suas definições elenca-se, novamente, uma série de qualificadores para o consentimento, sendo que, desta vez, deixa-se claro que tais qualificadores são cumulativos em razão do uso da partícula aditiva "e". Por fim, o mais relevante é que a própria norma em questão dispõe sobre qual deve ser o resultado esperado: o consentimento deve corresponder aos anseios do titular dos dados pessoais, seja por meio de uma declaração ou de uma ação afirmativa representativa[77].

É importante enaltecer que essa disposição já havia sido, de maneira similar, delineada em uma das considerandas da Diretiva 2002/58. Desta vez, contudo, ela é transportada para um dispositivo da regulação e, por fim, complementada pela ressalva de que o prometido controle dos dados pessoais deve ser resultante de uma ação afirmativa ou declaração nesse sentido.

Desce-se, inclusive, às minúcias de se elaborar um artigo específico para tratar das condições do consentimento[78]. Dentre as suas disposições, destaca-se, por exemplo, a preocupação de que o processo de tomada de decisão do titular dos dados pessoais deve partir de uma informação inteligível, facilmente acessível, clara e de simples linguagem[79].

Mais uma vez, portanto, o consentimento avoca para si o papel de protagonista, sendo, inclusive, um dos fios condutores da recente reforma (regulação) da diretiva europeia de proteção de dados pessoais.

O cenário acima descrito é apenas uma amostra de como o progresso geracional das leis de proteção de dados pessoais teve curso no direito comunitário europeu. Nesse retrato reducionista, focou-se, especialmente, no consentimento que tem sido constantemente revisitado ao longo dessa travessia. Tal trajeto esclarece que ele tem sido revigorado ao longo dessa jornada, permanecendo como o seu elemento fundante. A sua proeminência alcança desde os primeiros passos dessa normatização até os seus mais recentes movimentos.

3.3.3 Leis setoriais e a Lei Geral de Proteção de Dados Pessoais[80]

3.3.3.1 Código de Defesa do Consumidor

O Código de Defesa do Consumidor disciplinou, em seu art. 43, os bancos de dados e cadastros de consumidores[81]. Note-se a amplitude do dispositivo em questão, que alcança todo e qualquer dado pessoal do consumidor, indo muito além, portanto, dos bancos de dados de informações negativas para fins de concessão de crédito[82]. A racional do legislador foi alcançar todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidade do consumidor[83].

Nessa esteira, a legislação consumerista optou por conferir ao consumidor o direito de controlar

as suas informações pessoais, seguindo o padrão regulatório acima referenciado das FIPPs. Com efeito, toda normatização ali desenhada desemboca para que o consumidor seja capacitado para autodeterminar as suas informações pessoais.

A começar pela exigência de que o consumidor deve ser notificado da abertura de um banco de dados pessoais por ele não solicitado (art. 43, § 2º, do CDC). Esse dever de comunicação prévia[84] permite que o consumidor acompanhe o fluxo de seus dados pessoais, já que tal atividade deve ser a ele comunicada e, em última análise, ser *transparente*[85]. Por meio de uma interpretação extensiva de tal dispositivo, como propõe Antônio Herman Benjamin[86], o termo abertura cingir-se-ia a toda e qualquer movimentação dos dados pessoais, possibilitando ao consumidor acompanhar de *forma dinâmica* a circulação de suas informações pessoais.

A referida transparência só tem razão de ser porque o operador dos bancos de dados terá, simetricamente, os deveres de: i) garantir o seu *acesso* pelo consumidor (art. 43, *caput*, do CDC); ii) *exatidão* de tais informações; iii) que o banco de dados se restrinja para *finalidades claras e verdadeiras* e, por fim; iv) que seja observado o *limite temporal* de cinco anos para o armazenamento de informações negativas (art. 43, § 1º, do CDC). Por esse arranjo, o consumidor poderá demandar a imediata *correção-cancelamento* de uma informação errônea ou que tenha superado tal limite temporal (art. 43, § 3º, do CDC).

Tais direitos (acesso, retificação e cancelamento) e princípios (transparência, qualidade [exatidão] e limitação temporal)[87] gravitam em torno da figura do consumidor, para que ele, na condição de titular dos dados pessoais, exerça controle sobre suas informações pessoais. Em suma, o Código de Defesa de Consumidor buscou conferir a autodeterminação informacional[88], o que perpassa desde regras para garantir a exatidão dos dados até limitações temporais para o seu armazenamento.

3.3.3.2 Lei do Cadastro Positivo

A Lei 12.414/2011 veio a disciplinar a formação de banco de dados sob um conjunto de dados relativos às operações financeiras e de adimplemento para fins de concessão de crédito[89]. Com isso, a situação econômica do postulante ao crédito não é mais, somente, analisada a partir de dados relativos a dívidas não pagas, mas, também, a partir de outras informações que possam exprimir dados positivos sobre a sua capacidade financeira e o seu histórico de adimplemento[90]. Daí por que tal legislação foi apelidada de "Cadastro Positivo", já que a avaliação do crédito terá uma amplitude[91] maior do que apenas o exame de informações a respeito de dívidas inadimplidas, cuja conotação seria negativa[92].

Essa nova peça legislativa setorial acabou por trazer, de uma forma original e mais sistematizada[93], a orientação de que o titular dos dados pessoais deve ter o direito de gerenciá-los. Nesse sentido, requer-se mais do que a simples comunicação da abertura do banco de dados, tal como fez a legislação consumerista.

Antes da Lei Complementar nº 166/2019, a inclusão de nomes de consumidores só ocorria mediante o consentimento do titular dos dados pessoais. Agora, com a nova lei, a inclusão de consumidores no banco de dados tornou-se automática, tendo os titulares dos dados pessoais a possibilidade de solicitarem a retirada dos seus nomes do banco de dados. Passou, assim, de um sistema de opt-in para um sistema opt-out. Nos casos de compartilhamento da base de dados com terceiros, a Lei Complementar nº 166/2019 alterou a Lei 12.414/2011 para permitir ao gestor o compartilhamento de informações cadastrais e de adimplemento de outros bancos de dados[94], transferindo aos terceiros as obrigações e responsabilidades do agente de tratamento originário[95].

Esse arranjo é complementado, ainda, pelo dever de o gestor da base de dados não coletar informações excessivas[96] e sensíveis[97] para fins de análise de crédito, bem como de não as utilizar para outra finalidade que não a creditícia[98]. Com tais limitações, tal quadro normativo limita a coleta e as finalidades de tratamento dos dados pessoais com o intuito de capacitar o consumidor com o controle de suas informações pessoais. Mais uma vez, portanto, a técnica legislativa deita-se sobre o referencial normativo da autodeterminação informacional[99].

3.3.3.3 Marco Civil da Internet

A Lei 12.965/2014, conhecida como Marco Civil da Internet/MCI, inaugurou uma normativa específica para os direitos e garantias do cidadão nas relações travadas na Internet. O MCI foi, aliás, uma reação da sociedade civil contra um movimento legislativo que pretendia regulamentar a Internet no Brasil por meio de leis penais. Nesse sentido, o MCI procurou, de forma principiológica, assegurar os direitos e garantias do cidadão no ambiente eletrônico, sendo o seu traço marcante a distância de uma técnica normativa prescritiva e restritiva das liberdades individuais, própria do âmbito criminal[100], que poderia ter efeitos inibitórios para a inovação e a dinamicidade da Internet[101].

Dentre os direitos previstos, encontra-se a proteção da privacidade e dos dados pessoais[102]. Tidos como um dos pilares do MCI, ao lado da neutralidade de rede e da liberdade de expressão[103], a sua proeminência consolidou-se com o episódio do escândalo de espionagem revelado pelo ex-analista Edward Snowden, da Agência Nacional de Segurança dos Estados Unidos. Tais revelações repercutiram no MCI, que teve mudanças substanciais em seu texto para "endurecer"[104] a proteção ao direito à privacidade e aos dados pessoais, bem como na própria aceleração de seu trâmite legislativo que, com a adoção do regimento de urgência[105], culminou em sua aprovação no Congresso brasileiro em 2014[106].

Apenas a título de ilustração, o art. 7º detinha, apenas, cinco incisos[107], passando a ter, no cenário "pós-Snowden", oito incisos, sendo que todos eles foram direcionados para a proteção dos dados pessoais[108]. Com o acréscimo de tais dispositivos, houve uma alteração de ordem qualitativa no arranjo normativo do MCI, tendo sido o usuário eleito como o grande protagonista para desempenhar a proteção de seus dados pessoais[109].

Com efeito, verifica-se ao todo que três dispositivos fazem menção expressa à necessidade do

consentimento do usuário para a coleta, o uso, o armazenamento e o tratamento de seus dados pessoais, tal como para a sua transferência a terceiros[110]. Nesse sentido, o MCI irá, ainda, qualificar o consentimento como devendo ser livre, expresso e informado[111]. E, com relação aos dois últimos adjetivos, o MCI dedicou mais quatro dispositivos pelos quais se procurou estabelecer uma orientação do que venha a ser um consentimento expresso e informado. Aquele que exerce tal atividade de tratamento de dados pessoais deve prestar informações claras e completas, utilizando-se de cláusulas contratuais destacadas e dando publicidade às suas políticas de uso para o preenchimento dos adjetivos em questão.

É com base, justamente, em tais informações, que são especificados os propósitos[112] que justificam a coleta dos dados pessoais para que o seu titular possa fazer as suas escolhas a esse respeito.

Para conformar essa esfera de controle dos usuários sobre seus dados pessoais, o MCI dispõe ainda, que o usuário poderá requerer a exclusão definitiva de seus dados pessoais fornecidos a uma determinada aplicação de Internet, uma vez encerrada a relação entre eles[113].

Pela combinatória de tais dispositivos, verifica-se ser a autodeterminação informacional o parâmetro normativo eleito pelo MCI para a proteção de dados pessoais. Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento. Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento dos dados com terceiros até o direito de deletá-los junto ao prestador de serviços e produtos de Internet ao término da relação.

3.3.3.4 Lei Geral de Proteção de Dados Pessoais: o percurso do consentimento entre 2010 e 201

Após quase uma década de debates, o Brasil finalmente aprovou uma Lei Geral de Proteção de Dados Pessoais. Pelo menos desde 2010, é possível colher registros de debates públicos sobre o tema, como é o caso: **a)** do I Seminário de Proteção à Privacidade e aos Dados Pessoais, realizado em setembro pelo Comitê Gestor da Internet/CGI.br e o Núcleo de Informação e Coordenação do Ponto BR/NIC.br[114]; e **b)** da primeira consulta pública de um anteprojeto de lei que foi conduzida pelo Ministério da Justiça em novembro daquele ano[115].

Não é o objetivo deste subcapítulo remontar toda a linha do tempo dessa discussão[116], mas tão somente observar como o consentimento percorreu essa trajetória e permanece sendo um dos elementos cardeais da LGPD.

É interessante notar que, na primeira versão do anteprojeto de lei colocada sob consulta pública em 2010[117], o consentimento era, em termos topográficos, a única base legal[118] para o tratamento de dados pessoais. Isso se repetiu na segunda consulta pública em 2015[119], quando o que hoje são as demais bases legais da LGPD eram hipóteses nas quais o consentimento poderia ser dispensado.

Após tais consultas públicas, o texto enviado[120] ao Congresso Nacional, que depois veio a ser aprovado e sancionado, acabou por posicionar o consentimento como sendo uma das hipóteses legais

e não na cabeça do dispositivo. Isso significa que, em termos de técnica legislativa, o consentimento não só deixou de ser a única base legal para o tratamento de dados, como também foi alocado topograficamente sem ser hierarquicamente superior às demais bases legais por estarem todas elas horizontalmente elencadas em incisos do art. 7º da LGPD.

Por outro lado, também é possível dizer que o consentimento não deixou de ser o seu vetor principal. Isso porque uma análise detida dos princípios e a maneira pela qual a LGPD disseca tal elemento ao longo do seu corpo normativo acabam por revelar uma forte preocupação, mais uma vez, sobre qual deve ser a carga participativa do indivíduo no fluxo de suas informações pessoais.

Primeiro, por adjetivar extensivamente o consentimento seguindo a linha evolutiva do direito comunitário europeu e da quarta geração de leis de proteção de dados pessoais. O consentimento deve ser livre, informado, inequívoco e dizer respeito a uma finalidade determinada de forma geral[121] e, em alguns casos, deve ser, ainda, específico[122].

Segundo, porque grande parte dos princípios[123] tem todo o seu centro gravitacional no indivíduo: **a)** de um lado, princípios clássicos, como a transparência, a especificação de propósitos, de acesso e qualidade de dados por meio dos quais o titular do dado deve ser munido com informações claras e completas sobre o tratamento de seus dados e, ainda, ter acesso a eles para, eventualmente, corrigi-los; **b)** de outro lado, princípios mais "modernos", como adequação e necessidade, em que o tratamento dos dados deve corresponder às legítimas expectativas do seu titular. Isso deve ser perquirido de acordo com a finalidade especificada para o tratamento dos dados, assegurando-se que os dados sejam pertinentes, proporcionais e não excessivos (*minimização dos dados*).

É uma carga principiológica que procura conformar, justamente, a ideia de que o titular dos dados pessoais deve ser empoderado com o *controle* de suas informações pessoais e, sobretudo, na sua autonomia da vontade.

Terceiro, porque há uma série de disposições que dão um regramento específico para concretizar, orientar e, em última análise, reforçar o controle dos dados pessoais por meio do consentimento. Por exemplo: **a)** consentimento deveria ser extraído por meio de "cláusulas contratuais destacadas"[124]; **b)** autorizações genéricas (sem uma finalidade determinada) seriam nulas[125]; e, principalmente, **c)** nas hipóteses em que não há consentimento se deveriam observar os direitos e princípios da LGPD[126], de modo que haja a possibilidade de o titular dos dados pessoais se opor ao tratamento de seus dados[127].

Esses são alguns exemplos das 35 vezes em que aparece o termo "consentimento" no texto da LGPD. Uma análise não só quantitativa, mas também qualitativa, que diagnostica um arranjo normativo *circular* à figura do consentimento e que o canaliza como seu elemento cardeal.

Uma das possíveis disputas interpretativas da LGPD será verificar se: **a)** as demais hipóteses que legitimam o tratamento dos dados pessoais – os outros nove incisos do art. 7º[128] – são situações taxativas nas quais o tratamento dos dados pessoais ocorre sem o consentimento do seu titular; e, **b)** havendo a aplicação dessas hipóteses de "dispensa do consentimento", verificar como será

assegurada *transparência* ao cidadão para fazer valer a sua vontade por meio do consentimento, mesmo que *a posteriori*.

Trata-se, em última análise, de checar qual será o espaço ocupado pelo consentimento na malha normativa da LGPD. Para isso, é necessário não apenas uma leitura topográfica das outras nove bases legais que legitimam o tratamento de dados, mas também perquirir quais são a função e os limites do consentimento no sistema. Um dos caminhos para essa reflexão é a ensaiada reconstrução de como se deu a sua travessia durante a longa gestação da LGPD, a exemplo do progresso geracional das leis de proteção de dados pessoais.

3.4 CONCLUSÃO: A REDOMA DO CONSENTIMENTO E O REFRATÁRIO PROTAGONISMO DO CONSENTIMENTO

O titular dos dados pessoais alçou papel de protagonista a partir da segunda geração de leis de proteção de dados pessoais. Naquele momento, optou-se por uma estratégia regulatória que nele depositava a responsabilidade de autoproteger as suas informações pessoais. Essa diretriz normativa foi fundada a partir do direito de o indivíduo controlar os seus dados pessoais, socorrendo-se, por isso, à técnica legislativa de exigir o consentimento[129] do titular dos dados pessoais para que eles fossem coletados, utilizados, compartilhados, enfim, para toda e qualquer etapa de tratamento de tais informações.

A proeminência de tal estratégia regulatória consistiu no fator determinante para a (i)legalidade de toda e qualquer atividade de tratamento dos dados pessoais. Nesse sentido, as FIPPs desenharam um arquétipo cujo centro gravitacional[130] girava em torno de princípios e direitos para conformar essa diretriz normativa de que o indivíduo deveria autodeterminar as suas informações pessoais (subcapítulo 3.3.1 *supra*) – chamado até de participação individual.

A própria intelecção da proteção de dados pessoais foi forjada sob a alcunha de autodeterminação informacional. Da decisão da Corte Constitucional alemã ao referencial teórico de Alan Westin consolidou-se a crença reducionista de que autodeterminação informacional corresponderia ao elemento volitivo – autonomia da vontade – do titular do dado. Com ela, o consentimento atingiu um *status* canônico[131], cujo reverência se fez sentir ao longo de todo o percurso geracional das leis de proteção de dados pessoais (subcapítulo 3.2 *supra*).

Em que pese ter sempre havido dúvidas em torno da racionalidade e do poder de barganha dos titulares dos dados pessoais para que eles empreendessem um controle efetivo sobre seus dados pessoais, o consentimento permaneceu sendo o elemento nuclear da estratégia regulatória da privacidade informacional. A sua adoração pode ser traduzida pelo ciclo de adjetivações recebido ao longo desse trajeto. Seja no direito comunitário europeu (subcapítulo 3.3.2 *supra*), seja no que diz

respeito às leis setoriais[132] e geral de proteção de dados pessoais no Brasil (subcapítulo 3.3.3 *supra*), o consentimento tido como informado, livre, expresso, específico ou inequívoco confirma esse processo de veneração.

Trata-se, sobretudo, de um processo de revigoramento dessa estratégia regulatória que, forjada nos anos 1980, conduz a um refratário protagonismo do consentimento. O saldo desse percurso é apostar no indivíduo como um ser capaz, racional e hábil para controlar as suas informações pessoais. Tem-se, assim, um quadro regulatório encapsulado por uma compreensão reducionista do conteúdo a que se deve referir autodeterminação informacional que, passadas mais de duas décadas, não mais se ajusta ao contexto subjacente dos dados pessoais como ativo econômico em constante circulação (Capítulo 1) e que modula o livre desenvolvimento da personalidade dos cidadãos (Capítulo 2 *supra*).

Nessa conjuntura, faz-se necessário reavaliar tal estratégia regulatória e a própria compreensão do conteúdo do que é autodeterminação informacional. Devem-se canalizar esforços para identificar a problemática em torno de uma estratégia regulatória e dogmática anacrônica pensada nos anos 1980, que enfrente uma demanda social dos anos 2000 (Capítulo 3). E, assim, verificar como deve ser encarado esse descompasso, balanceando soluções que, por um lado, empoderem o titular dos dados pessoais (Capítulo 4), e, por outro lado, não deixem apenas sobre seus ombros a proteção de suas informações pessoais (Capítulo 5).

[1] Optou-se por seguir, em parte, a *taxonomia* desenhada por MAYER-SCHONEBERGER, Viktc Generational... Op.cit., que estabeleceu quatro divisões para as gerações das leis de proteção de dados pessoais. Verifica-se, contudo, outro referencial teórico que estabelece apenas três ondas geracionais: POULLET, Yves. About the E-Privacy Directive: Towards a Third Generation o Data Protection Legislation? In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul de (Org *Data Protection in a Profiled World*. New York: Springer, 2010, p.3-30. Nossa abordagem seguirá uma análise mais descritiva – descrevendo o progresso geracional, mas sem, necessariamente, compartimentalizar as gerações. O foco é identificar como o consentimento está inserido nesse processo.

[2] A nacionalização do referencial teórico a respeito das gerações das leis de proteção de dados pessoais já foi abordada por: DONEDA, Danilo.*Da privacidade*... Op.cit., p.203-217. MENDES, Laura Schertel.*Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p.37-44; E, anteriormente, em sua dissertação de mestrado: MENDES, Laura Schertel. *Transparência*... Op.cit., p.33-40.

[3] Atentando-se para o surgimento dessa demanda regulatória e, em paralelo, com os primórdios de uma sociedade de vigilância, veja-se, *e.g.*, RIBEIRO, Márcio Moretto. Criptografia com resistência à sociedade da vigilância. III SIMPÓSIO INTERNACIONAL LAVITS (Rede Lati Americana de Estudos sobre Vigilância, Tecnologia e Sociedade). Disponível em: <https://www.youtube.com/watch?v=kyIX1na65DM>.

[4] LYON, David. *The Electronic Eye*: The rise of surveillance society. Minneapolis: University of Minnesota Press, 1994. p.31-37.

[5] MILLER, Arthur. *The assault privacy*: computers, data banks, and dossiers. Michigan: University Michigan Press, 1971. p.71-73.

[6] MILLER, Arthur. Op.cit., p.221-222.

[7] MAYER-SCHONEBERGER, Viktor. Generational... Op.cit., p.223: "The computer is the problen it seems, and its application must be regulated and controlled. Consequently, the first-generation data protection norms take a functional look at the phenomenon of data processing. If the act of processing is the actual problem, then legislation should target the working of the computer. Data-protection norms were seen as part of a larger attempt to tame technology".

[8] Ibidem, p.223.

[9] Ibidem, p.225. A menção é feita pelo próprio autor em alusão ao famoso romance intitulado *1984*, de George Orwell, pseudônimo de Eric Arthur Blair, no qual o Estado (a figura do Grande Irmão) monitora tudo e todos, retratando-se, então, como se desenrola a vida do cidadão Winston.ORWELL, George.*1984*. Tradução Alexandre Hubner e Heloisa Jahn.São Paulo Companhia das Letras, 2009.

[10] DONEDA, Danilo. *Da proteção*... Op.cit., p.208.

[11] Ibidem, p.22.

[12] DONEDA, Danilo.*Da proteção*... Op.cit., p.24. Em sentido análogo, verificando-se que na primeira geração o setor privado não era afetado por tal normatização: MILLER, Arthur. Op.cit. p.221.

[13] Toma-se emprestada a analogia de: RAMOS, André Carvalho. Op.cit., p.957: "Chamaram esse bancos de dados de "Pequeno Irmão", alusão ao Grande Irmão orwelliano. Apontaram o perigo de violação da intimidade do consumidor e de discriminação odiosa pela existência dos 'credit bureaus'". E, arremata, p.959: "Como veremos, necessitamos de amarras ao "Pequeno Irmão" que possui mais dados sobre os brasileiros que o próprio Poder Público".

[14] MAYER-SCHONEBERGER, Viktor. Generational... Op.cit., p.226-227.

[15] WESTIN, Alan F.*Privacy and Freedom*. New York: Atheneum, 1970. p.7: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".

[16] RODOTÁ, Stefano. *Il diritto*... Op.cit., p.320.

[17] MENDES, Lara Schertel. *Privacidade*... Op.cit., p.42: "A principal diferença em relação à segund geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, armazenamento e a transmissão e não apenas como a opção entre tudo ou nada".

[18] MAYER-SCHONEBERGER, Viktor. Generational... Op.cit., p.231.

[19] MAYER-SCHONEBERGER, Viktor. Generational... Op.cit., p.229.

[20] Ibidem, p.228.

[21] Comentando tal geração de leis de proteção de dados pessoais, veja-se: DONEDA, Danilo *Princípios*... Op.cit., p.372: "Estas leis apresentavam seus problemas, que motivaram uma subsequente mudança de paradigma: percebeu-se que o fornecimento de dados pessoais pelos cidadãos vinha se tornando um requisito indispensável para a sua efetiva participação social".

[22] MAYER-SCHONEBERGER, Viktor. Generational... Op.cit., p.229: "But what price does one hav to pay for that? Is it acceptable that such data-protection liberties can be exerciced only by hermits? Have we reached an optimum of data protection if we guarantee privacy rights that, when exercised, will essentially expel the individual citizen from society?".

[23] DONEDA, Danilo. *Da privacidade*... Op.cit., p.213.

[24] Ibidem, p.233. O autor estabelece uma clara alusão à diretiva da União Europeia que limita o tratamento e o processamento de dados sensíveis. Tal ponto já foi abordado nesta obra no subcapítulo *supra* 3.3.1.

[25] DONEDA, Danilo. *Princípios*... Op.cit., p.373: "A proteção de dados é vista, por tais leis, como

um processo mais complexo, que envolve a participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que a sua liberdade de decidir livremente é cerceada por eventuais condicionantes – proporcionando o efetivo exercício da autodeterminação informativa".

[26] MAYER-SCHONEBERGER, Viktor. Generational... Op.cit., p.234.

[27] Vejam-se, por exemplo, os arts. 2 (a), 7(a), 8(a).

[28] MAYER-SCHONEBERGER, Viktor. Generational... Op.cit., p.235.

[29] Trata-se de um organismo internacional multilateral que, atualmente, conta com 34 países-membro Disponível em: <http://www.oecd.org/about/membersandpartners/>.

[30] A missão do organismo está descrita com maiores detalhes em: <http://www.oecd.org/about/>.

[31] Ibidem: "The OECD provides a forum in which governments can work together to share experiences and seek solutions to common problems. We work with governments to understand what drives economic, social and environmental change. We measure productivity and global flows of trade and investment. We analyse and compare data to predict future trends".

[32] OECD Guidelines... Op.cit., p.7.

[33] Ibidem, p.7.

[34] Ibidem, p.11: "Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries; (...)".

[35] As *guidelines* definem, em seu item 1, alínea *b*, dados pessoais como: "personal data" means any information relating to an identified or identifiable individual (data subject)".

[36] OECD Guidelines... Op.cit., p.7: "The Guidelines on the Protection of Privacy and Transborde Flows of Personal Data (the "Privacy Guidelines") were adopted as a Recommendation of the OECD Council in support of the three principles that bind OECD Member countries".

[37] Os oito princípios são: a) Limitação de Coleta (Collection Limitation Principle); b) Qualidade do Dados (Data Quality Principle); c) Especificação dos Propósitos (Purpose Specificatio Principle); d) Limitação do Uso (Use Limitation Principle); e) Padrões de Mecanismos d Segurança (Security Safeguards Principle); f) Abertura (Openness Principle); g) Participaçã individual (Individual Participation Principle); h) Responsabilidade (Accountability Principle).

[38] São os princípios "a", "c", "d" e "g" supracitados.

[39] OECD Guidelines... Op.cit., p.14: "Collection Limitation Principle: 7. There should be limits to th collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject".

[40] Ibidem, p.15: "Purpose Specification Principle: 9 The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use

limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose".

41 Ibidem, p.15: "Use Limitation Principle: 10. Personal data should not be disclosed, made availabl or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law".

42 Ibidem, p.16: "Individual Participation Principle: 13. An individual should have the right: (...) d) t challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended".

43 Contextualizando as FIPPS com as *guidelines* da OECD e, por fim, conceituando-as: CATE, Fred H. The Failure of Fair Information Practice Principles. In: WINN, Jane K. (Ed.). *Consumer Protection in the Age of the 'Information Economy'* (markets and the law). Hampshire: Ashgate Publish, 2006. p.356.

44 Não se ignora que as FIIPS datam de 1973, como resultado do trabalho do Comitê d Aconselhamento sobre Sistemas de Dados Automatizados no âmbito do Departamento da Saúde Educação e bem-estar do governo estadunidense. Contudo, tais princípios ensaiados somente ganharam escala ao serem transpostos pela OCDE e, por isso, centramos nossa análise nesse documento.

45 Tal conclusão é extraída dos quatro objetivos listados na declaração. OECD Guidelines... Op.cit., p.34: "a) achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data; b) reducing differences between relevant domestic rules and practices of Member countries to a minimum; c) ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and d) eliminating, as far as possible, reasons which might induce Member countries to restrict transborder flows of personal data because of the possible risks associated with such flows".

46 The OECD Privacy Framework 2013, p.148. Disponível em <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

47 Veja-se, em especial, o capítulo 4 denominado "The evolving privacy landscape: 30 years after th OECD Privacy Guidelines (2011)". Ibidem, p.65-127.

48 Nesse sentido, veja-se o subitem 4 do capítulo 2 denominado "It is increasingly difficult for individuals to understand and make choices related to the uses of their personal data". Ibidem, p.67-68.

49 O documento utiliza várias vezes o termo interoperabilidade, como, por exemplo, "interoperable privacy frameworks". Ibidem, p.33.

50 Vejam-se, por exemplo, os subitens denominados "Bilateral co-operation on cross-border cases" "Multilateral enforcement co-operation". Ibidem, p.148.

[51] KUNER, Christopher. Regulation of Transborder Data Flows under Data Protection and Privac L a w . *OECD Digital economic papers*, Paris, n.187. Disponível em: <http://dx.doi.org/10.1787/5kg0s2fk315f-en>. p.6: "The first examples of regulation of transborder data flows under data protection and privacy law can be found in data protection laws passed in various European countries in the 1970s. In the 1980s various international organisations enacted instruments dealing with the subject, most prominently the OECD Guidelines".

[52] Essa é a conclusão de tópico da obra de: SOLVE, Daniel J.; SCHWARTZ, Paul L*Information privacy*. New York: Wolters Kluwer Law, 2011. p.1064.

[53] Veja-se, por exemplo, o subcapítulo denominado "The influence of the Guidelines". The privacy framework... Op.cit., p.76.

[54] Ressalva-se que tal abordagem é reducionista. O objetivo é, apenas, pinçar alguns exemplos de como o consentimento alocou-se em meio a esse progresso geracional no direito comunitário europeu.

[55] Disponível em: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

[56] Nesse sentido, consulte-se o *Relatório Explanatório* sobre a Convenção de Strasbourg que tem ur tópico dedicado e nomeado "Cooperação com a OECD". Disponível em <http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm>.

[57] Trata-se da última consideranda do preâmbulo: "Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples".

[58] Capítulo III – "Transborder data flows".

[59] Em 18.05.2018, o Conselho Europeu atualizou a referida Convenção. Iniciada em janeiro de 2011 a iniciativa visava a reforçar os direitos dos indivíduos diante dos novos desafios colocados pelas novas tecnologias, bem como reforçar sua própria implementação – preservando seu caráter flexível, pragmático e coerente e convergente com outros sistemas jurídicos. Dentre os principais pontos trazidos pela modernização estão: (i) a legitimidade e qualidade do processamento de dados; (ii) reforço dos princípios da accountability, transparência, privacy by design e default, e impact assessment; (iii) exceções à sua aplicação, que deverão se dar por lei e serem justificáveis e proporcionais no contexto de sociedades democráticas; (iv) direito dos titulares de serem ouvidos e de terem conhecimento da racionalidade de decisões automatizadas que lhes impacte. A emenda à Convenção 108 está disponível em <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e>. Sobre isso, ver também: KWASNY, Sophie. Convenção 108+. Apresentação no IX Seminário de Privacidade do Comitê Gestor da Internet no Brasil, 2018. Disponível em <https://www.youtube.com/watch?v=X3zdwB2xi_E&list=PLQq8-9yVHyOZVGYJeegT8I-mHrWOPIiYh&index=6&t=0s>.

[60] Veja-se, a título de exemplificação, que a primeira consideranda já exprime a tensão regulatória entre a proteção dos dados pessoais e o desenvolvimento econômico tomado por ações que eliminem as barreiras que dividem o continente europeu. Ainda na quinta consideranda retoma-se essa perspectiva de integração econômica para que seja posta em curso por um aumento substancial do fluxo "transfronteiriço" dos dados pessoais.

[61] POULLET, Yves. About... Op.cit., p.3.

[62] Veja-se, mais uma vez, o "Relatório Explanatório" sobre a Convenção de Strasbourg (nota de rodapé 55 *supra*), p.1-2: "However, there is a lack of general rules on the storage and use of personal information and in particular, on the question of how individuals can be enabled to exercise control over information relating to themselves which is collected and used by others".

[63] Veja-se, por exemplo, os arts. 2 (a), 7(a), 8(a)

[64] Art. 6(1), alínea *c*: "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Em tradução livre, leia-se: adequado, relevante e não excessivo em relação ao propósito para o qual eles [dados pessoais] são coletados e/ou para processamento adicional).

[65] Veja-se, *e.g.*, KUNER, Christopher. *European Data Protection Law*. New York: Oxford University Express, 2007. p.74.

[66] POULLET, Yves. About... Op.cit., p.5.

[67] Atenta-se que, durante a revisão das guidelines da OECD, procedeu-se a tal evolução balizada pela essa perspectiva da minimização dos dados pessoais, notadamente pelo dever de o *data controller* processar a menor quantidade possível de dados pessoais. The OECD Privacy Framework 2013, p.148. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

[68] Atualmente, já está em discussão uma proposta de reforma dessa diretiva. Disponível em: <http://europa.eu/rapid/press-release_IP-17-16_en.htm>.

[69] Veja-se, *e.g.*, a consideranda 17: "(...) Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking box when visiting an Internet website".

[70] Recorrentemente, a diretiva utiliza o termo "*prior consent*" para delinear, como regra, que tal controle deve ser exercido, previamente, ao tratamento dos dados pessoais e não *a posteriori*. Vejam-se, *e.g.*, arts. 6(4), art. 8(3), 9(1), 13(1).

[71] Veja-se, *e.g.*, a consideranda 17 da Diretiva.

[72] Veja-se, *e.g.*, consideranda 25 da Diretiva.

[73] Veja-se, *e.g.*, consideranda 25 da Diretiva.

[74] Veja-se, *e.g.*, consideranda 24 da Diretiva.

[75] A primeira versão da Proposta de Reforma (Regulação) foi apresentada no ano de 2012. Disponível em: <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011>.

[76] O triálogo europeu é composto pelo Parlamento, Conselho e Comissão da União Europeia. Em dezembro de 2015, eles entraram em acordo sobre o texto da regulação geral de proteção de dados pessoais: Agreement on Commission's EU data protection reform will boost Digital Single Market. Disponível em: <http://europa.eu/rapid/press-release_IP-15-6321_en.htm>. A versão aprovada pelo triálogo: General Data Protection Regulation EU. Disponível em <http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf>.

[77] Art. 4(8): "'the data subject's consent' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed".

[78] Trata-se do art. 7º nomeado como Condições para o Consentimento.

[79] Art. 7(2): "If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of the declaration which constitutes an infringement of this Regulation that the data subject has given consent to shall not be binding".

[80] Optou-se por fazer uma revisão da legislação infraconstitucional, que dispõe sobre normas específicas (setoriais) sobre a proteção de dados pessoais. Isso não significa, contudo, que as normas constitucionais não tenham relevância, complementando a normatização em torno da matéria. Para tal perspectiva, veja-se, *e.g.*, MENDES, Laura Schertel*Privacidade*... Op.cit., p.161-190. Ressalva-se, ainda, a opção por não analisar: i) Código Civil – i.e., seus dispositivos "soltos", já que iremos proceder e já procedemos a sua análise de acordo com a matriz dos direitos da personalidade; ii) a Lei de Acesso à Informação e iii) *Habeas Data*. No tocante ao Código Civil, verifica-se, por exemplo, o Enunciado 404 da V Jornada de Direito Civil do Conselho da Justiça Federal: "A tutela da privacidade da pessoa humana compreende os controles espacial, contextual e temporal dos próprios dados, sendo necessário seu expresso consentimento para tratamento de informações que versem especialmente o estado de saúde, a condição sexual, a origem racial ou étnica, as convicções religiosas, filosóficas e políticas". E, com relação à Lei de Acesso à Informação, veja-se: MENDES, Laura Schertel*Privacidade*... Op.cit., p.148-154.

[81] A respeito da diferenciação dogmática entre bancos de dados e cadastros de consumo, e, por fim, posicionamento desse autor conquanto a sua inaplicabilidade prática, veja-se o subcapítulo 1.3.3.

[82] BESSA, Leonardo Roscoe. A abrangência... Op.cit., p.401: "O delineamento dos limites jurídicos da atuação dos bancos de dados de proteção ao crédito no Brasil exige do intérprete análise

sistemática do ordenamento jurídico. Ao lado do exame da disciplina constante na Lei de 8.078/90 (Código de Defesa do Consumidor), é fundamental uma compreensão dos *direitos da personalidade,* especialmente do *direito à privacidade* – em seu aspecto de proteção de informações pessoais – e do *direito à honra*".

[83] BENJAMIN, Antônio Herman de Vasconcellos e. *Código*... Op.cit., p.421: "De modo direto, o ma funcionamento dos arquivos de consumo ameaça, primeiramente, o direito à privacidade, por que cada indivíduo pode clamar, na esteira da elaboração mais ampla dos direitos da personalidade".

[84] Ibidem, p.927.

[85] MENDES, Laura Schertel. *Privacidade*... Op.cit., p.142.

[86] BENJAMIN, Antônio Herman de Vasconcellos e. *Código*... Op.cit., p.476: "Daí que, cada vez que o arquivo de consumo recebe dado que significa inovação, se se quer incorporá-la precisa informar o consumidor. Vale dizer, o direito à comunicação não se exaure num momento específico e inicial da vida do arquivo de consumo, mas se protrai no tempo, enquanto este permanecer".

[87] Identificando-se os mesmos princípios, veja-se, *e.g.*, MENDES, Laura Schertel.*Privacidade*... Op.cit., p.142-143; GAMBOGI, Ana Paula. Op.cit., p.953.

[88] GAMBOGI, Ana Paula. Op.cit., p.930: "A preocupação do legislador em assegurar ao consumido o controle da manipulação de dados seus armazenados em arquivos de consumo denota a busca pela chamada autodeterminação informacional".

[89] Tal definição pode ser extraída da interpretação conjunta dos arts. 1º, *caput*, 2º, III, e 3º, § 1º.

[90] BESSA, Leonardo Roscoe.*Cadastro*... Op.cit., p.38: "Nesse contexto as informações positivas devem ser compreendidas em contraste com os dados caracterizadores de dívidas vencidas e não pagas: qualquer dado além das informações necessárias para identificar um débito vencido e não pago pode ser classificado como informação positiva".

[91] COSTA, Carlos Cleso Orcesi. *Cadastro Positivo*: Lei nº 12.414/2011. São Paulo: Saraiva, 2012. p.72.

[92] Em 09.04.2019, foi sancionada a Lei Complementar nº 166/2019, que tornou automática a inclusã de consumidores no Cadastro Positivo.

[93] DONEDA, Danilo. Princípios... Op.cit., p.381: "A Lei 12.414 de 2011, geralmente referida como Lei do Cadastro Positivo, é igualmente responsável por estabelecer em nosso ordenamento alguns dos princípios de proteção de dados pessoais (...) fez com que se tornasse a normativa que refletisse com maior intensidade, em seu tempo, um modelo de proteção de dados pessoais – ainda que restrita ao seu âmbito, referente aos históricos de crédito".

[94] Art. 4º: "Art. 4º O gestor está autorizado, nas condições estabelecidas nesta Lei, a: (...) III compartilhar as informações cadastrais e de adimplemento armazenadas com outros bancos de

dados; (...)".

[95] Art. 9º: "Art. 9º O compartilhamento de informações de adimplemento entre gestores é permitido na forma do inciso III do *caput* do art. 4º desta Lei.§ 1º O gestor que receber informação por meio de compartilhamento equipara-se, para todos os efeitos desta Lei, ao gestor que anotou originariamente a informação, inclusive quanto à responsabilidade por eventuais prejuízos a que der causa e ao dever de receber e processar impugnações ou cancelamentos e realizar retificações".

[96] Art. 3º, § 3º, I: "Ficam proibidas as anotações de: informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor".

[97] Art. 3º, § 3º, II: "Ficam proibidas as anotações de: sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".

[98] Art. 5º, VII: "ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados".

[99] Veja-se, *e.g.*, MENDES, Laura Schertel.*Privacidade*... Op.cit., p.146: "É de se destacar também que a referida lei consolida a evolução de um conceito de autodeterminação informativa no nosso ordenamento, ao estabelecer mecanismos de controle do indivíduo sobre os seus dados, atribuindo a ele o poder de decidir se tem interesse ou não em formar esse histórico e de decidir quando deseja cancelá-lo". Em sentido similar: BESSA, Leonardo Roscoe.*Cadastro*... Op.cit., p.97-104.

[100] Para uma visão aprofundada sobre tal cenário político ("Mega Não" dessa atividade legiferante de cunho penal), bem como o processo de construção do MCI, veja-se, especialmente, o capítulo II de: BRITO CRUZ, Francisco.*Direito, democracia e cultura digital*: a experiência de elaboração legislativa do marco civil da internet. Dissertação (Mestrado) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2009. p.29-53.

[101] Veja-se, ainda: BIONI, Bruno Ricardo. Projeto de Lei 215/2015, infanticídio aos recém-nascidos direitos digitais no Brasil. *Digital Rights* n.28, out. 2015. Disponível em: <http://www.digitalrightslac.net/pt/proyecto-de-ley-2152015-infanticidio-contra-los-recien-nacidos-derechos-digitales-en-brasil/>.

[102] Art. 3º, II e III, do MCI: "A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) II – proteção da privacidade; III – proteção dos dados pessoais, na forma da lei".

[103] Nesse sentido foram as considerações tecidas pelo Deputado Alessandro Molon em evento da Universidade de São Paulo: MOLON, Alessandro.*Marco civil da internet e neutralidade da rede*. Organização Centro Acadêmico XI de Agosto da Faculdade de Direito da Universidade de São Paulo. 20 de mar. 2014.

[104] Esse foi o verbo utilizado na relatoria final pelo Deputado Alessandro Molon à época em que o

projeto de lei foi submetido à votação: MOLON, Alessandro. Apresentação do relatório do projeto de lei do marco civil da internet. Disponível em: <https://www.youtube.com/watch?v=YE7wrCHqWFI>: "(...) em especial os dispositivos que tratam sobre privacidade (...) nós tornamos as regras ainda mais duras, após os escândalos de espionagem revelados em junho passado".

105 O regimento de urgência determina que a votação de projeto de lei deve ser realizada no período de 45 dias, sob pena de trancamento da pauta de votações. Cf. a reportagem: Após espionagem, Dilma pede urgência de votação do Marco Civil da Internet. Disponível em <http://oglobo.globo.com/sociedade/tecnologia/apos-espionagem-dilma-pede-urgencia-de-votacao-do-marco-civil-da-internet-9912712>.

106 Vale lembrar que a sanção do Marco Civil da Internet ocorreu no evento de governança multissetorial da internet (NetMundial). ARAGÃO, Alexandre. Dilma sanciona Marco Civil na abertura do NETMundial. Disponível em: <http://www1.folha.uol.com.br/tec/2014/04/1444200-dilma-sanciona-marco-civil-na-abertura-do-netmundial.shtml>.

107 A versão "pré-Snowden" está disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=912989&filename=PL+2126/2011>.

108 Para fins de uma melhor visualização e compreensão das modificações ocorridas em decorrência do escândalo de espionagem, veja-se: LIMA, Cíntia Rosa Pereira de. BIONI, Bruno Ricardo. A proteção dos dados pessoais na fase de coleta: apontamentos sobre a adjetivação do consentimento implementada pelo art. 7, incisos VIII e IX do Marco Civil da Internet a partir da *human computer interaction* e da *privacy by default*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.)*Direito & Internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. t. I, p.266.

109 Ibidem, p.267: "Para além dessa guinada quantitativa, constata-se, sobretudo, uma alteração de conteúdo do próprio texto da lei, tendo o legislador eleito um parâmetro normativo muito claro a respeito da proteção dos dados pessoais. Trata-se da autodeterminação informacional fundada na perspectiva de que o próprio usuário deve ter controle sobre as suas informações pessoais, autodeterminando-se. Socorrer-se, por isso, a técnica de se exigir o consentimento do titular dos dados pessoais para que eles sejam coletados, processados e compartilhados (...)".

110 Art. 7º, VII, IX e art. 16, II.

111 Art. 7º, VI, VIII, IX e XI.

112 Art. 7º, VIII.

113 Art. 7º, X.

114 As palestras estão disponíveis em: <https://seminarioprivacidade.cgi.br/2010/index.htm>.

[115] A plataforma do debate público ainda permanece acessível em: <http://culturadigital.br/dadospessoais/>.

[116] Já realizamos essa análise em artigo de opinião: BIONI, Bruno.*De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados pessoais*. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018>.

[117] "Art. 9º O tratamento de dados pessoais somente pode ocorrer após o consentimento livre, expresso e informado do titular, que poderá ser dado por escrito ou por outro meio que o certifique, após a notificação prévia ao titular das informações constantes no art. 11" (Disponível em: <http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf>).

[118] Não se ignora que grande parte das atuais bases legais constantes da LGPD aparecia no art. 13 do então anteprojeto de lei, mas justamente em um dispositivo autônomo e que expressamente as considerava como exceções ao consentimento.

[119] Arts. 9º e 11 do anteprojeto. Disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>.

[120] Arts. 7º e 11 do anteprojeto de lei. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=62B6CCB8D15F0
codteor=1457971&filename=Avulso+-PL+5276/2016>.

[121] Art. 5º, XII, da LGPD: "consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

[122] Esse é o caso constante dos arts. 7º, § 5º, 14, § 1º, e 33, VIII, da LGPD.

[123] Art. 6º, I, II, III, IV, V e VI: "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

[124] Art. 8º, § 1º, da LGPD: "Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais".

[125] Art. 8º, § 4º, da LGPD: "O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas".

[126] Art. 7º, § 6º: "A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular".

[127] Art. 18, § 2º, da LGPD: "O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei".

[128] "II – para o cumprimento de obrigação legal ou regulatória pelo controlador; III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente".

[129] MONTELEONE, Shara. LE MÉTAYER, Daniel. Automated consent through privacy agents: Legal requirements and technical architecture. *Computer Law & Security Review*, 25, p.138, 2009.

[130] SCHWARTZ, Paul M. Privacy and democracy in cyberspace.*Vanderbilt Law Review*, v.52, p.1658, 1999.

[131] A expressão eloquente é de: BELLAMY, Bojana; HEYDER, Markus*Empowering Individuals Beyond Consent.* Disponível em: <https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Centre_Bellamy_He

[132] A alteração da Lei do Cadastro Positivo pela Lei Complementar nº 166/2019, contudo, parece fazer parte de um movimento pendular da centralidade do consentimento, ao retirar a necessidade de consentimento dos titulares dos dados para sua inclusão.

Capítulo IV

REAVALIAÇÃO PROCEDIMENTAL (FORMA) DO CONSENTIMENTO COMO PROTAGONISTA DA PROTEÇÃO DE DADOS PESSOAIS

4.1 CONSENTIMENTO E A DEMANDA SUBJACENTE CONTEMPORÂNEA DA PROTEÇÃO DE DADOS PESSOAIS

4.1.1 Da teletela orwelliana à vigilância distribuída e líquida: entre a percepção romancista-ficcional e a análise sociológica crítica do controle dos dados

Não são raras as associações entre o romance intitulado *1984* e o desafio contemporâneo da privacidade informacional. Fala-se, recorrentemente, que o acesso indiscriminado aos nossos dados pessoais guardaria correspondência com a vigilância operada pela *teletela orwelliana*. Se, por um lado, tal analogia é válida para identificar um cenário similar de vigilância constante, por outro lado, essa relação de semelhança esvai-se quando esses cenários são contrastados sob a perspectiva de uma esfera, mais ou menos reduzida, do controle das nossas informações sujeitas a tal escrutínio. Por tal razão, ainda que paradoxal, o romance de George Orwell é um bom início de conversa. Isto porque, mesmo na distopia de *1984*, o protagonista Winston conseguia escapar, em certos momentos, da vigilância operada pelo Grande Irmão[1].

Na ficção de Erick Arthur Blair[2], a teletela era um tipo de tecnologia bidimensional. Fazia as vezes de uma televisão para transmitir as mensagens do programa oficial do governo e, às vezes, de uma câmera de vigilância para observar os cidadãos em suas residências[3]. Tal aparelho de vigilância tinha suas limitações. Ele captava somente sons que ultrapassassem o nível de um sussurro[4] e, principalmente, no caso específico de Winston, ele tinha um campo de visão restrito.

A câmera de vigilância ocupava uma posição atípica. Em vez de estar posicionada em uma parede ao fundo da sala para ter um campo de observação mais amplo, a teletela estava instalada em uma parede que lhe impedia vigiar o cômodo inteiro[5]. Com isso, Winston conseguia ficar em um determinado espaço na sala fora do alcance da teletela, sendo este o local onde ele começou a escrever o seu diário[6] e, em última análise, exercer controle sobre as suas informações pessoais. Naquele espaço e naquele caderno, Winston produzia registros (dados) que estavam a salvo da vigília do Grande Irmão.

Essa esfera de controle se fez possível porque a vigilância em questão era ostensiva. Tal como os cartazes expostos ao longo de todo o território da Oceania[7], a teletela era em si mesma um alerta

de que o Grande Irmão "estava de olho em você"[8], naquele espaço e naquele momento. E, nesse sentido, o romance não encontra semelhança com a realidade.

Atualmente, o próprio conceito de vigilância sofreu um desgaste conceitual, ao menos sob o ponto de vista de sua definição clássica. Já não mais existe uma relação estanque e delimitada, ora compreendida pela existência de polos bem definidos entre as figuras do observador e do observado[9].

Nesse sentido, a *figura sólida* do Grande Irmão dilui-se pela multiplicação de Pequenos Irmãos[10], haja vista uma economia em que seus atores têm como modelo de negócio vigiar os cidadãos-potenciais consumidores (vide subcapítulo 1.4). A vigilância não é mais centralizada, mas descentralizada, estando dispersa[11] pelos "tiny brothers"[12]. Trata-se, pois, de uma atividade que não tem mais uma única face. A sua multifacetação é resultado desse complexo ambiente da economia dos dados pessoais em que, por exemplo, a sede pelas informações pessoais estrutura uma indústria própria, como os *data brokers* (subcapítulo 1.2.2.4).

Complementarmente, a teletela é substituída por inúmeras "microtelas". Dos aparelhos celulares *smartphones* aos *trackers* (subcapítulo 1.2.2.2 *supra*)[13], desenha-se uma *arquitetura de vigilância* que mapeia todos os hábitos dos cidadãos. Com a *Internet* das coisas há, por exemplo, o estreitamento dos mundos *off-line* e *on-line* e, por conseguinte, a difusão dessa vigília. Há, em suma, a *datificação* das vidas dos cidadãos, que é o pressuposto de uma *vigilância ubíqua* a movimentar a roda da economia de dados.

A vigilância está *distribuída*[14]. Das figuras homogêneas[15] e centrais do Big Brother e da teletela, expande-se o ato de vigiar – em um movimento descentralizador e mais plural – pela presença de múltiplos observadores e pela penetração de inúmeras e novas tecnologias para tal propósito[16].

Em suma, a vigilância não é mais ostensiva como no romance *1984*. Ela passa a ser mais *opaca* como decorrência lógica dessa dispersão. As suas características sólidas e bem delimitadas derretem-se nesse processo de distribuição em que o vigia e a sua atividade tornam-se mais voláteis[17]. Diferentemente de Winston, os cidadãos da atualidade já não têm mais um espaço delimitado e certo para se colocar a salvo da vigilância. Ela vem de todos os lados e de inúmeros dispositivos, havendo um permanente estado de visibilidade[18] da pessoa de carne e osso do século XXI[19].

A vigilância[20] é *líquida*[21], tal como propõem os sociólogos Zygmunt Bauman e David Lyon. Ela não tem mais as características de firmeza e solidez, tal como se propunha a figura de um único observador e a sua atividade ostensiva de vigiar. Ela está diluída no arranjo socioeconômico contemporâneo no qual os dados fluem por inúmeros atores e sensores, os quais, como uma esponja[22], absorvem-nos para sua exploração econômica.

Por isso, o fluxo dos dados pessoais não mantém mais traços consistentes e compactos, tal como era de se supor nos anos de 1980. Passadas mais de três décadas, repita-se, há uma economia e modelos de negócios que encontram nas informações pessoais a sua matéria-prima. A sua fluidez é

um pressuposto do movimento cíclico dessa nova economia.

Daí por que se afirmar que há um *anacronismo* entre o arranjo normativo forjado na década de 1980 e a demanda subjacente atual pela proteção dos dados pessoais. Qualquer perspectiva de controle dos dados pessoais se não é prejudicada, é, ao menos, problematizada por essa contínua *fluidez* dos dados pessoais. A própria expressão em questão – liquidez – é *per se* contrária a uma perspectiva de controle. Diferentemente do estado da matéria sólida, o líquido não pode ser manipulado pelas mãos, sendo, por conseguinte, de difícil manuseio e controle[23].

Esse relato sociológico é muito importante para clarear os desafios atuais à proteção dos dados pessoais. Diferentemente do romance *1984*, a pessoa de carne e osso está em contínuo estado de visibilidade e sujeita a uma vigilância mais opaca, dispersa, intensiva e extensiva[24]. Nesse contraste de maior transparência do cidadão e menor visibilidade da atividade de vigilância[25], nem mesmo a ficção orwelliana foi capaz de se igualar à realidade contemporânea.

O Grande Irmão, a teletela e o espaço reservado na sala de Winston para que ele escrevesse seu diário consistiam em um cenário mais favorável para o controle das informações pessoais. Os Pequenos Irmãos, as microtelas e a vigilância onipresente da vida real acabam por minar essa perspectiva. A realidade esconde um quadro mais problemático do que a ficção. A fluidez dos dados pessoais resulta em um complexo fluxo informacional, tornando-se necessário reavaliar a estratégia regulatória focada na capacidade de o titular dos dados pessoais controlá-los. A anotada fluidez das informações pessoais deixa para trás os seus titulares, mistificando, ainda mais, a crença da autodeterminação informacional, pelo menos como sinônimo do mero consentimento do cidadão.

4.1.2 A complexidade do fluxo informacional e as limitações cognitivas[26] para um genuíno processo de tomada de decisão sobre os dados pessoais

Um exemplo categórico dessa fluidez das informações pessoais é a própria rede dos atores envolvidos para operacionalizar os modelos de negócios baseados na publicidade direcionada. As imagens representativas dessa *network* (vide subcapítulo 1.2.2.4) revelam uma plêiade de atores pelos quais os dados pessoais trafegam para que, ao final, seja customizada a abordagem publicitária. São esses os famigerados "parceiros comerciais" constantes das políticas de privacidade que viabilizam e monetizam o *zero-price-advertisement business model* (subcapítulo 1.2.2.3).

A estruturação dessa indústria desaguará na prática comum de agregação de dados (itens 1.2.2.2 e 1.2.2.3). Aliás, o próprio conceito de uma rede implica ações cooperativas, notadamente por meio do compartilhamento de informações para que seja alcançada uma finalidade comum. Daí por que, no caso específico, os seus integrantes fazem um uso comum dos dados pessoais coletados entre eles para que, ao final, a publicidade – e também o conteúdo dirigido – seja a mais personalizada possível.

Em suma, os pequenos pedaços[27] de informações são agregados pelos integrantes dessa rede, a

fim de compilar um perfil mais preciso dos hábitos do potencial consumidor[28]. De modo que, em última análise, esse fluxo informacional passa a ser de difícil determinação, interminável e imprevisível[29].

Há, pois, um complexo ecossistema formado por uma miríade de sujeitos em que todos põem "as mãos" sobre os dados pessoais, tornando o fluxo informacional completamente volátil. Como consequência, o titular dos dados pessoais deveria ter consciência a respeito de todos esses atores e das suas respectivas práticas de mineração de dados (subcapítulo 1.3.1) para que, ao final, pudesse gerenciar as suas informações pessoais[30].

Dada a *racionalidade limitada* do ser humano, é pouco provável que ele esteja capacitado para tanto. Com efeito, a *bounded rationality* prescreve justamente que as habilidades cognitivas do ser humano são limitadas[31], minando a sua capacidade de absorver, memorizar e processar todas as informações relevantes para um processo de tomada de decisão[32]. Já se faz impossível memorizar os inúmeros atores que compõem a referenciada rede social de publicidade, quanto mais compreender como os dados pessoais serão por eles tratados, já que cada um deles tem as suas respectivas políticas de privacidade. Soma-se, ainda, o complicador da compreensão de como a agregação dos dados pessoais desenrolar-se-á a ponto de extrair informações mais detalhadas sobre seus titulares[33].

A complementar tal quadro problemático, há barreiras psicológicas que mistificam por completo a capacidade de o indivíduo controlar as suas informações pessoais.

A primeira delas é a chamada teoria da decisão da utilidade subjetiva[34]. O ser humano tem a tendência de focar nos *benefícios imediatos*, o que, de acordo com o arranjo e os modelos de negócios da economia informacional, é representado pelo acesso a um produto ou serviço *on-line*. Por tal razão, deixa-se de sopesar os possíveis prejuízos à privacidade, que são temporariamente distantes. De fato, os possíveis danos com relação à perda do controle sobre as informações pessoais só podem ser experimentados no futuro.

Esse é o caso justamente da agregação de dados que, a partir do tratamento de dados triviais, pode revelar informações sensíveis sobre uma pessoa (vide subcapítulo 2.3.1). Ou, ainda, de um eventual uso inadequado que pode gerar danos na esfera patrimonial e extrapatrimonial. Ou, mesmo, o compartilhamento dos dados pessoais com terceiros que, dada a volatilidade do trânsito de tais informações, mina a perspectiva de controle sobre tal fluxo informacional. Em todas essas situações, a pessoa em causa experimentará danos à sua privacidade somente após o ganho imediato pertinente aos bens de consumo digital. Por tal razão, o titular dos dados pessoais tende a, subjetivamente, valorizar mais tais benefícios imediatos, minimizando-se os possíveis prejuízos representados pela perda do controle de seus dados pessoais.

E, uma vez feita tal escolha, é pouco provável que o sujeito volte atrás, revogando o consentimento para o tratamento dos dados pessoais. A "teoria prospectiva" assinala que o processo de tomada de decisão tende a se levar pelo contexto de que as perdas são maiores do que os ganhos[35]. Assim, o usuário que teve acesso a um produto ou serviço sopesará mais essa perda do que

o ganho em retomar, em tese, o controle de seus dados pessoais. Sobressai[36], em última análise, que o serviço ou produto "gratuito" é mais valorizado nesse processo de tomada de decisão[37].

Nesse jogo de ganhos e perdas, o ser humano tende a procurar uma "zona de conforto" para não se culpar em torno do prejuízo por ele suportado[38]. Trata-se das chamadas *dissonâncias cognitivas* em que o sujeito procura um alívio para simetricamente compensar um desconforto. É nesse contexto que se insere o denominado "paradoxo da privacidade"[39]. Em que pese as pessoas valorarem a proteção de seus dados pessoais, elas empreendem ações dissonantes a tal apreço. As suas condutas contradizem o que elas estimam, surgindo-se uma relação de incoerência entre o que elas praticam e o que elas enxergam como ideal[40].

A própria lógica do *trade-off* da economia dos dados pessoais é traiçoeira, portanto, frente a tal *arquitetura de escolha de decisões*, notadamente por essa *idiossincrasia* entre *gratificações imediatas e prejuízos mediatos/distantes*[41]. A crença de que o cidadão é um sujeito racional e capaz de desempenhar um processo genuíno de tomada de decisão para controlar seus dados pessoais é posta em xeque por toda essa complexidade envolta ao fluxo das informações pessoais[42]. Ele está em uma situação de *vulnerabilidade específica* em meio a uma *relação assimétrica* que salta aos olhos, havendo uma série de evidências empíricas a esse respeito.

4.1.3 Estudos empíricos a confirmar a sobrecarga e evasão ao consentimento

4.1.3.1 Mental models *(Universidades de Stanford e Carnegie Mellon)*

A primeira pesquisa empírica foi desenhada para investigar os modelos mentais dos usuários a respeito do funcionamento da publicidade comportamental no ambiente *on-line*[43]. Por isso, o título da pesquisa estabelece uma correlação entre as crenças e os comportamentos dos usuários[44] nesse contexto, a fim de verificar qual seria a compreensão dos titulares dos dados pessoais quanto ao fluxo de suas informações pessoais.

As pesquisadoras, Lorrie Cranor e Aleecia McDonald, procederam a entrevistas com usuários em duas etapas[45]: **i)** na primeira fase, mediante um questionário de formato semiestruturado[46], elas procederam a entrevistas mais complexas com um número reduzido de entrevistados[47]; **ii)** na segunda fase, os resultados da primeira etapa foram testados e validados por meio de um formulário de perguntas[48], sendo, desta vez, totalmente estruturado para alcançar um número maior de entrevistados, aumentando-se a amostra do estudo empírico[49].

As primeiras constatações revelaram que os usuários não têm um conhecimento técnico para autodeterminar os seus dados pessoais no plano da sua coleta. Apenas 23% dos usuários usam o modo de navegação privada – aquele que bloqueia a coleta dos dados pessoais –, enquanto 50% dos usuários não usam tal ferramenta e 27% não têm certeza. Além disso, somente 17% deletam *cookies*, 23% não têm certeza, e, por fim, 60% não deletam essa ferramenta de coleta de dados pessoais[50].

A situação torna-se, ainda, mais esclarecedora, quando se analisam as razões pelas quais aquela

parcela reduzida de usuários deleta os *cookies*[51]. Nesse pequeno universo, encontram-se respostas curiosas, tais como: **i)** "alguém recomendou que eu fizesse e, assim, eu tenho feito desde então" ou; **ii)** "minha mãe, minha filha ou meu pai me disseram"[52]. Em termos percentuais, apenas 30% esclareceram que a "limpeza" de seus *cookies* estaria relacionada às questões de segurança e privacidade[53], o que reduz, mais ainda, aqueles que, em tese, seriam realmente hábeis para gerenciar os seus dados pessoais.

Em linhas gerais, a pequena parcela que estaria exercendo um controle sobre as suas informações coletadas é encolhida por conta da significativa "confusão" em torno da motivação que lhe é subjacente[54]. Assim, um *genuíno processo de tomada de decisão* referente ao controle dos dados pessoais desmorona-se, já que a sua causa é viciada com relação ao seu propósito idealizador.

Essa percepção se tornou mais clara quando a pesquisa realizada questionou os entrevistados – por meio de quatro figuras ilustrativas – a respeito de *cookies* de terceiros para perquirir a compreensão[55] de como seus dados pessoais são coletados e fluem no contexto de uma rede de publicidade comportamental (vide subcapítulo 1.2.2.4). Apenas metade dos entrevistados assinalou o melhor gráfico representativo de tal situação, o que mistifica, mais ainda, a capacidade de o titular dos dados pessoais tomar uma decisão significativa sobre o trânsito de seus dados[56].

No entanto, 70% dos entrevistados afirmam que, ao efetuar compras *on-line*, levariam em consideração se o *website* compartilharia os seus dados pessoais com parceiros, cujas atividades estariam relacionadas à atividade publicitária[57]. Veja-se, pois, que, apesar de os usuários não terem um completo entendimento do fluxo de seus dados pessoais com tais parceiros comerciais, eles valoram o trânsito de suas informações pessoais nesse contexto.

Essa preocupação com a proteção dos dados pessoais é coerente com o alto percentual de 64% dos entrevistados que consideraram ser invasiva a vigilância sobre as suas atividades *on-line*[58]. Desenha-se, assim, uma incompatibilidade entre o modelo de negócios predominante na Internet e as perspectivas dos usuários, já que tais percentuais acentuam a intenção de eles manterem seus dados pessoais sob a sua esfera de controle, seja limitando os seus recipientes, seja restringindo o próprio acesso dos seus hábitos *on-line*.

Essa contradição é sublinhada na última parte da pesquisa empírica, quando os entrevistados são questionados, respectivamente, em dois grupos: **i)** se pagariam o valor de U$ 1,00 (um dólar) para evitar que os provedores de Internet coletassem suas informações pessoais, ou, alternativamente; **ii)** se aceitariam o desconto de U$ 1,00 (um dólar) em troca da permissão para que os provedores de Internet coletassem seus dados pessoais[59].

No primeiro grupo, 11% afirmam estar dispostos a pagar o valor de U$ 1,00 (um dólar). Ao passo que, no segundo grupo, 69% concordariam com o desconto ofertado em troca de suas informações pessoais. Tais percentuais confirmam as limitações cognitivas já abordadas neste trabalho (subcapítulo 4.1.2). Isso porque aqueles que têm o controle sobre as suas informações pessoais, enxergando a privacidade como uma perda imediata, tendem a valorá-la mais, como é o

caso do segundo grupo (69%). Enquanto aqueles que, em tese, já têm uma reduzida esfera de controle sobre os dados pessoais, tendem a valorizar menos tal benefício, até como consequência de estarem situados em uma zona de conforto com tal situação (11%). Trata-se de um exemplo concreto da chamada teoria prospectiva e das dissonâncias cognitivas (subcapítulo 4.1.2) referidas anteriormente.

Relevante é, contudo, a opinião dos entrevistados com relação ao *trade-off* (troca) acima cogitado. Juntando-se os dois subgrupos, houve o consenso de 69% dos entrevistados de que a privacidade é um direito, de modo que eles não deveriam ser obrigados a pagar uma quantia monetária para evitar que as empresas a violassem[60]. Nesse sentido, 61% dos entrevistados afirmaram, categoricamente, que tal tipo de pagamento consistiria em uma extorsão[61].

As conclusões dessa pesquisa empírica trazem uma série de argumentos que convergem para a conclusão de que os usuários não estão capacitados para tomar decisões informadas no tocante ao controle de seus dados pessoais[62], como: **i)** falta de conhecimento no que diz respeito ao funcionamento das tecnologias de coleta dos dados pessoais e da sua inserção no contexto da publicidade comportamental, que determina o fluxo de suas informações em meio aos diversos atores que operam esse mercado; **ii)** idiossincrasia do *trade-off* da economia informacional, uma vez que o controle aos dados pessoais é visto, respectivamente, como um benefício imediato e uma perda mediata, o que o desvaloriza nesse processo de tomada de decisão; **iii)** em último lugar, porque os próprios usuários discordam da lógica econômica pela qual eles teriam que despender uma quantia para assegurar o seu direito à privacidade, enxergando tal dinâmica como uma extorsão.

Em poucas palavras, tal estudo empírico sublinha a posição de vulnerabilidade dos cidadãos em exercer o controle de seus dados pessoais, o que perpassa desde uma assimetria informacional até a própria estruturação dos modelos de negócio que se divorciam das expectativas de privacidade dos usuários.

4.1.3.2 Trackers *e a corrida armamentista tecnológica como elemento neutralizador da capacidade do usuário em controlar as suas informações pessoais (Universidade de Berkeley)*

Um segundo estudo empírico foi realizado pelos pesquisadores da Universidade de Berkeley da Califórnia[63]. Procurou-se investigar como o estado da arte das tecnologias de coleta de dados, permeado por sua contínua evolução, mistifica o poder e a própria escolha dos consumidores quanto ao controle da coleta de seus dados pessoais[64]. Por meio de simulações, navegando-se por *sites*, ativando e desativando *trackers*, bem como investigando o próprio funcionamento dessas novas tecnologias[65], ponderou-se se as escolhas dos titulares dos dados pessoais seriam efetivamente respeitadas[66].

O estudo atenta para o surgimento de novas tecnologias de rastreamento que convivem com, e, por vezes, substituem, os tradicionais *cookies*, dificultando que os usuários as deletem ou as bloqueiem[67]. Perpassando *E-tags*[68], *flash cookies*[69], *HTML5 Web Storage*[70], *evercookie*[71],

fingerpriting[72], realizou-se uma revisão da literatura dos *trackers*, testando-os em navegações simuladas nos 100 (cem) *websites* mais acessados nos Estados Unidos[73].

Para além do número expressivo e "campeão" de utilização dos tradicionais *cookies*[74] e, em especial, de terceiros[75], o estudo registrou a presença de *flash cookies* e *HTML5 Web Storage*. A utilização de tais *trackers*, ilustrada em um estudo de caso[76], é conclusiva de que essas novas tecnologias tornam a coleta de dados ubíqua, robusta e redundante[77].

Por exemplo, as duas novas tecnologias citadas são mais persistentes[78] que os tradicionais *cookies*, já que: **i)** elas são mais difíceis de ser bloqueadas, pois são armazenadas de forma incomum em pastas locais do sistema computacional[79] e por não ter uma expiração por padrão (*by default*) a cada término da sessão de navegação[80]; **ii)** elas têm a capacidade de reviver[81], isto porque, mesmo que sejam deletadas, a execução de um programa pode reativá-las automaticamente, sem o conhecimento do usuário.

O êxtase dessa prática é a própria tecnologia *evercookie* que é apelidada de *tracker* zumbi[82]. Por ser o resultado da combinação de inúmeros *trackers*, a coleta dos dados pessoais é quase que perene. Dada essa metamorfose e sobreposição de rastreadores, eles continuam a "perambular" se não há o "extermínio" de todos eles pelo titular dos dados pessoais. Por exemplo, se o usuário deleta *cookies*, ele ainda poderá ser rastreado por outros inúmeros *trackers – flash cookies*, *E-tags* e assim por diante.

Essas novas tecnologias tornam, portanto, a vigilância mais *opaca*. Ela não só flui a cada passo e rastro da navegação do usuário, como, também, *dribla* as escolhas destes com relação à coleta de seus dados pessoais[83]. Tais tecnologias empregam liquidez a um monitoramento contínuo e permanente dos usuários, acuando-os em meio a uma "corrida armamentista tecnológica" que invalida as suas escolhas para que as suas informações pessoais não sejam coletadas[84]. Esses dispositivos são as microtelas do século XXI que criam um estado de visibilidade constante do cidadão, colocando em xeque a sua capacidade de controlar seus dados pessoais.

Por isso, esse segundo estudo empírico é complementar ao primeiro. Desenvolvem-se outras evidências que demonstram ser o fosso da assimetria informacional e da vulnerabilidade maior do que se aparentava ser naquela pesquisa anterior. Mesmo que os consumidores se capacitem para o controle de seus dados pessoais, o próprio mercado acaba por criar novas tecnologias para neutralizá-lo. Tal fator é determinante para se (re)pensar e (re)avaliar um quadro regulatório que eleva o consentimento como seu elemento normativo central e, por essa lógica, o seu titular como sujeito autônomo[85] e capaz para exercer tal esfera de controle e, em última análise, desempenhar por si próprio a proteção de suas informações pessoais.

*4.1.3.3 Resignação pela assimetria de poder no fluxo das informações pessoais: o problema estrutural do câmbio-troca (*trade-off*) da economia dos dados pessoais (Universidade da Pensilvânia)*

A terceira pesquisa empírica é da Faculdade de Comunicação Annenberg[86] da Universidade da Pensilvânia. O estudo reverte a suposição e as conclusões de estudos anteriores, bem como o discurso da indústria publicitária de que os consumidores estariam confortáveis e conscientes da troca de seus dados pessoais por serviços e produtos "gratuitos": o abordado câmbio-troca (*trade-off*) da economia dos dados (vide subcapítulo 1.2).

Ao todo, a pesquisa entrevistou 1.506 (um mil e quinhentos e seis) pessoas adultas de diferentes faixas etárias, classes socioeconômicas e etnias, a fim de ser a mais representativa possível da população americana[87]. Com um questionário estruturado, a referida população do estudo foi instada a: **i)** na primeira parte da pesquisa: tecer considerações gerais sobre essa lógica da economia de dados pessoais e; **ii)** em um segundo momento: externar reflexões mais detalhadas de como se aperfeiçoaria o fluxo de suas informações pessoais nesse contexto.

Na parte mais genérica, constatou-se que 91% considerariam "injusta"[88] a coleta de suas informações sem o seu respectivo conhecimento. Questionados se estariam de acordo se: **i)** uma loja *on-line* ou *off-line* fornecesse Wi-Fi gratuita em troca de seus dados pessoais e; **ii)** fossem criados perfis para melhorar os serviços a eles fornecidos; mais uma vez a resposta foi negativa, alcançando os percentuais de 71% e 55%, respectivamente[89].

Tais percentuais por si só já seriam suficientes para sublinhar esse descompasso entre o mencionado câmbio-troca e a vontade dos titulares dos dados pessoais. Contudo, os pesquisadores estavam motivados em produzir dados mais significativos a esse respeito. Para tanto, eles criaram uma valoração diferente das respostas favoráveis a tal crença do *trade-off* da economia dos dados pessoais, chegando-se ao percentual agregado de 21%[90]. Esse índice foi o que justificou e embasou a segunda parte da pesquisa.

Iniciou-se com o seguinte exercício de reflexão: "Por favor, pense a respeito de um supermercado que você frequenta. Vamos supor que esse supermercado proponha lhe dar descontos em troca das suas informações pessoais que ele coleta a respeito de todas as suas compras. Você aceitaria isso ou não?"[91].

Desse exemplo mais concreto, extraiu-se o percentual de que 43% concordariam com tal prática. Por um lado, ele é muito maior que o valor agregado de 21% dos entrevistados que subscreveriam essa troca. Por outro lado, ele é bem similar ao citado percentual de 45% de entrevistados que aquiesceriam com a criação de seus perfis para aprimorar serviços a eles prestados. Essa ausência de correspondência reforçou a importância em se investigar as *razões subjacentes* dessa parcela dos entrevistados simpáticos ao *trade-off* da economia digital[92].

Então, os pesquisadores passaram a questionar aquela população específica sobre possíveis usos de seus dados pessoais, a fim de tornar mais concreta a abstrata operação econômica consubstanciada pela troca de suas informações pessoais por serviços e produtos "gratuitos", ou, nesse caso, representada por uma vantagem econômica – os cupons de descontos de supermercado[93].

Há um *declínio eloquente* daqueles que seriam aquiescentes com o *trade-off* em questão. Os

entrevistados acabaram por enxergar com outros olhos o trânsito de seus dados, quando é levantada uma série de possibilidades a respeito da gama de informações que podem ser extraídas da mineração de seus dados, como, por exemplo: **a)** se eles teriam tendência à compra de alimentos com baixo índice de gordura (33%); **b)** se eles teriam crianças e quais as suas respectivas faixas etárias (27%); **c)** as suas atividades fora do trabalho (25%); **d**) se gozariam seus períodos de férias (22%); **e)** seu respectivo estado de saúde e de alguém de sua família (21%); **f)** sua capacidade financeira (21%); **g)** se estariam em vias de atingir um momento importante na trajetória de suas vidas (19%) e; **h)** suas origens raciais ou étnicas (19%)[94].

Há uma redução média de 20%[95], que é muito significativa, já que cai mais que pela metade o índice anterior (45%). Tal constatação embasa uma nova explicação do porquê de as pessoas, em sua grande maioria e na prática, serem coniventes com essa lógica da economia dos dados pessoais. Elas estariam *resignadas*. Ou seja, elas teriam simplesmente acatado algo que é indesejável, mas que é, ao mesmo tempo, inevitável.

Essa é a hipótese[96] levantada pela pesquisa que acaba por dar uma nova explanação de por quê, apesar de as pessoas valorarem a sua privacidade, elas acabariam por tomar atitudes contraditórias frente a tal bem apreciado. Trata-se do denominado *paradoxo da privacidade*[97] que, no caso da proteção dos dados pessoais, residiria na incoerência de os seus titulares anuírem com um trânsito contínuo de suas informações pessoais, ainda que eles estimassem a sua proteção[98].

O estudo associou essa reduzidíssima parcela da população, resistente em favor do câmbio-troca da economia dos dados pessoais, com os seguintes questionamentos: **i)** você gostaria de ter controle sobre o que é feito com os seus dados? (84%) e; **ii)** você reconhece que tem pouco controle sobre o que pode ser feito com as suas informações pessoais? (65%)[99]

Por tal combinação, o estudo concluiu que os consumidores estão *resignados* com essa dinâmica. No fundo, eles desejam ter um maior controle sobre o uso de seus dados pessoais, reconhecendo, ao mesmo tempo, que têm pouca gerência sobre tal situação.

Em síntese, não haveria um paradoxo da privacidade, já que não haveria uma *ambivalência* de escolhas conflitantes. Isso porque se, de fato, houvesse mais de uma opção, prevaleceria a vontade massiva em exercer um melhor controle sobre os dados pessoais. Ausente, pois, um genuíno processo de tomada de decisão composto por mais de uma escolha, pelo contrário, haveria, tão somente, a submissão a tal lógica do *trade-off* da economia dos dados pessoais que é, em última análise, o próprio significado de resignação[100].

O estudo prossegue, ainda, com outras perguntas para aferir o nível de conhecimento da população (resignados) sobre as práticas recorrentes do mercado informacional[101]. A pesquisa identifica que o percentual de resignação cresce, proporcionalmente, de acordo com tal competência. Assim, aqueles que, em tese, teriam mais habilidade para tomar decisões informadas e genuínas quanto ao fluxo de seus dados pessoais, acabam por compor o *núcleo duro* dos resignados[102].

O estudo coloca em xeque, portanto, os consumidores como sujeitos capazes de controlar as suas

informações pessoais. Trata-se, aliás, de uma evidência contrária a essa suposição, já que a resignação em questão é fruto da própria descrença dessa habilidade[103]. Isso porque no pano de fundo dessa constatação encontra-se o diagnóstico de que a prometida autodeterminação informacional é estrangulada em meio a uma relação assimétrica[104].

Com efeito, a programada autonomia dos consumidores para controlar seus dados pessoais é sufocada por todo um mercado sedento por tal ativo econômico. A lógica da economia dos dados pessoais prevalece e impõe as suas forças sobre a parte mais vulnerável dessa relação. Os consumidores mostram-se impotentes[105] para fazer valer o seu desejo de controlar seus dados pessoais, sendo tal *assimetria de poder* a mola propulsora de tal resignação.

Em suma, o problema é *estrutural*[106]. Parafraseando o título da pesquisa sob análise, trata-se de uma *falácia* imposta pelo *trade-off* da economia dos dados pessoais. Mistifica-se a capacidade dos cidadãos de autoproteção de seus dados pessoais, notadamente por sua pseudoautonomia em controlar as suas informações.

Em conclusão, esse terceiro estudo empírico é complementar aos anteriores, uma vez que ele situa, de forma estrutural, o problema da autodeterminação informacional frente à própria dinâmica da economia dos dados pessoais. A suscitada assimetria informacional, decorrente do uso da tecnologia para um melhor controle dos dados pessoais – primeiro e segundo estudos empíricos –, acaba por encontrar abrigo e, talvez, até como a sua causa, o relato mais abrangente de uma relação assimétrica e própria desse cabo de forças do mercado informacional – último estudo empírico. Daí por que a racionalidade regulatória deve identificar a parte vulnerável dessa relação assimétrica e empoderá-la para reequilibrar tal relação desigual.

4.1.3.4 Avisos de Cookies: o cenário pós-GDPR e a contínua evasão das escolhas do titular dos dados (Universidade de Bochum)

A quarta pesquisa empírica e a mais recente foi conduzida pela Universidade de Bochum (Alemanha)[107]. Ao notar um aumento exponencial, na casa de 45%, na adoção dos chamados avisos de *cookies*[108] por parte de *websites* no cenário pós-GDPR, os pesquisadores analisaram se tais notificações promoviam, de fato, transparência acerca das práticas de tratamento de dados pessoais pelas plataformas e se, em última análise, auxiliariam na obtenção de um consentimento válido por parte dos usuários.

Partindo de um estudo anterior em que pré-selecionarem 6.000 (seis mil) *websites* e coletarem 5.087 (cinco mil e oitenta e sete) avisos de cookies, selecionou-se uma amostra aleatória de 1.000 (um mil) notificações que foram analisadas manualmente para se estabelecer as diferenças de interface em cada uma. Os pesquisadores chegaram então a oito variáveis para a análise: posição (na tela), escolhas oferecidas para o usuário responder, o uso de cores escuras visando a influenciar a resposta do usuário, link para informações adicionais, o texto contido nas notificações, layout (cores e fonte), bloqueio de conteúdo até a resposta do usuário e tamanho. As quatro primeiras variáveis

foram observadas em uma pesquisa de campo, com os usuários de um site de e-commerce alemão – sem que estes soubessem que estavam sendo estudados. Além disso, visando a validar os critérios de análise, foram realizadas entrevistas (*survey*) com 100 participantes, nas quais os usuários foram inquiridos a reportar as motivações para suas escolhas, o que eles achavam dos avisos e como eles achavam que esses avisos funcionavam em geral.

Ao todo foram realizados três experimentos que consideraram respectivamente: a) a posição na qual o aviso era exibido na plataforma; b) se aos usuários eram franqueadas opções para decidir como seus dados poderiam ser utilizados pela plataforma e, ainda, como tais preferências poderiam ser exercidas; c) por fim, a linguagem de tais avisos. O estudo aponta para uma falha no *design* da tecnologia em questão, a qual além de não informar adequadamente os usuários, também, em sua grande maioria, não despertava neles uma interação adequada.

Com relação ao primeiro experimento, notou-se que o posicionamento do aviso em mais de 91,8% das vezes era alocado no topo ou ao final da plataforma, não sendo de fácil visualização. Na medida em que tais notificações não bloqueavam o conteúdo do site, consequentemente havia uma baixa da taxa de cliques. Ainda, uma boa parte era colorida de forma a prejudicar a sua visibilidade, como, por exemplo, tonalidades escuras[109].

O segundo teste constatou que tal tecnologia não causava interação no usuário, porque: i) na grande maioria das vezes, não lhe franqueava qualquer tipo opção senão a aceitação do uso dos seus dados; ii) quando havia opções, essas eram limitadas a ele aceitar ou não o uso de *cookies*. Uma lógica binária que não lhe informava os vários usos possíveis com os seus dados; iii) quando havia várias opções (e.g., analytics, marketing[110]), os avisos dificultavam o exercício de uma escolha genuína de sua parte, sendo: iii.a) as opções pré-marcadas, de modo que, por padrão, o usuário autorizava o processamento de seus dados; iii.b) as opções em não aceitar o uso de *cookies* ou aceitá-los com restrições não eram destacadas com cores que as realçavam; iii.c) a aceitação do uso de *cookies* com restrições demandavam uma série de cliques, não sendo, muitas vezes, tais opções apresentadas na primeira tela da notificação.

O terceiro teste considerou a linguagem dos avisos de notificação. Os usuários entrevistados mostraram o quão desafiador é a construção de um vocabulário que seja de fácil compreensão: a) o próprio termo "cookies", apesar de ser empregado em boa parte das notificações, é técnico e seu significado não é tão difundido; b) alguns dos entrevistados não compreendem as implicações das suas escolhas, como, por exemplo, acreditando que recusar um cookie os impediria de acessar o site ou significaria o aparecimento de menos anúncios.

Em síntese, tão importante quanto criar uma tecnologia voltada a reduzir a assimetria de informação e de poder é verificar se a sua arquitetura é responsiva a tais objetivos. As variáveis consideradas por esse último estudo empírico evidenciam o quão traiçoeiro pode ser o seu design a ponto de manipular a decisão tomada pelo cidadão com relação aos seus dados.

4.1.4 Conclusão: assimetria e (hiper)vulnerabilidade próprias no âmbito da proteção dos dados pessoais e o debate normativo da proteção dos dados pessoais

Não é de hoje que a ciência jurídica volta os seus olhos para relações assimétricas. Esse é o caso do direito do trabalho, em que o poder econômico do empregador ocasiona uma discrepância de forças em relação ao trabalhador. Para a própria caracterização do vínculo empregatício, exige-se, aliás, que o empregado esteja subordinado ao empregador[111]. Cabe a este exercer um poder diretivo[112] sobre aquele para determinar os rumos da prestação de seus serviços, o que sublinha essa posição de dependência entre assalariado e assalariador. A própria vigilância do ambiente do trabalho cumpre essa finalidade, clarividenciando essa *relação assimétrica* de poder[113]. Esse ramo específico do direito tem, portanto, a função de tutelar[114] o trabalhador, como sendo a parte mais fraca dessa relação.

O mesmo sucede com o direito do consumidor. Ideologicamente[115], esse ramo do direito emerge para corrigir a desigualdade[116] daquele frente aos prestadores e fornecedores de produtos e serviços. O precursor discurso de 1962 do ex-presidente americano John Kennedy, que para muitos marca o nascimento do direito consumerista[117], é elucidativo nesse sentido[118]. Ao elencar o direito à segurança, à informação, à escolha de bens alternativos e com preços justos e o direito de ser ouvido na formulação de políticas públicas, procura corrigir falhas de um mercado capazes de lesar essa parte mais frágil. Desde a (in)existência de padrões de qualidade dos bens de consumo até a debilidade lobística do consumidor, o discurso ataca, prioritariamente, a *equalização* das forças desse mercado. O direito do consumidor cumpre, portanto, essa missão protetiva em favor do elo mais frágil da cadeia econômica que tende a se submeter ao poder de controle dos titulares dos bens de produção[119].

Em cena, portanto, o paradigma protetivo[120] que reconhece a posição de *vulnerabilidade* de certos grupos, dedicando-lhes normas especiais para tutelá-los na exata medida de suas fraquezas[121]. A etimologia da palavra vulnerabilidade – em latim: *vulnus* (machucado ou ferida)[122] – significa a potencialidade de o sujeito, ora identificado como vulnerável, ser mais suscetível de sofrer danos. Decorre daí, portanto, a noção de *instrumentalidade*[123] do direito na emissão de normas protetivas para dispensar um tratamento desigual aos sujeitos desiguais[124].

E o cidadão, em meio ao mercado informacional, deve ser identificado como um sujeito vulnerável. Os tópicos anteriores revelaram que ele avoca fraquezas próprias desse contexto. Retomam-se, brevemente, algumas das conclusões já tecidas neste trabalho.

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.

Outra especificidade diz respeito à própria operação econômica em causa (subcapítulo 1.2.2.3). Como já dito, não há um deslocamento patrimonial, cuja contraprestação pelo bem de consumo seja fixada pecuniariamente. Na lógica da economia digital, os dados pessoais são a moeda de troca pelo bem de consumo. Em um contexto de agregação de dados e de complexidade do fluxo informacional (subcapítulo 4.1.2), o consumidor não sabe, ao certo, os custos efetivos de tal transação econômica, já que é incerto o alcance do fluxo de seus dados pessoais e, por conseguinte, o que deles se pode extrair.

O consumidor "compra agora para pagar depois"[125]. Esse quadro de incertezas é a *eloquência* de uma *nova vulnerabilidade*[126], na medida em que o titular dos dados pessoais pode ser "machucado" pela má utilização de seus dados pessoais, cuja potência da "ferida" não pode ser nem mesmo antevista.

Somam-se, ainda, as citadas limitações cognitivas do ser humano, que o impedem de calibrar as gratificações e as perdas mediatas e imediatas necessárias para racionalizar um processo de tomada de decisão genuíno a respeito do fluxo de seus dados pessoais. A sua situação de vulnerabilidade é *maximizada* por essa idiossincrasia traiçoeira do *trade-off* da economia informacional (subcapítulo 4.1.2).

O primeiro estudo empírico (subcapítulo 4.1.3.1) é clarividente sobre tal situação, evidenciando como funcionam tais *modelos mentais vulneradores*. Mais do que isso, ele denota o quão fundo é o buraco da *assimetria informacional* a ser escalado para que haja um efetivo controle das informações pessoais por seus titulares.

O segundo estudo empírico (subcapítulo 4.1.3.2) expande esse déficit (informacional), coligando-o ao funcionamento e à inovação da tecnologia. A debilidade informacional do consumidor respinga na ausência de um *conhecimento técnico* que poderia tornar a tecnologia um instrumento de melhora do gerenciamento do fluxo informacional. No entanto, o que tais evidências empíricas assinalam é, justamente, o contrário. A tecnologia tem sido utilizada para *neutralizar* essa possível habilidade, fragilizando, ainda mais, o elo mais fraco do mercado informacional.

O terceiro estudo empírico (subcapítulo 4.1.3.1) sedimenta essas discrepâncias sob um olhar mais amplo: a assimetria é estrutural e é decorrente da própria dinâmica da economia dos dados pessoais. O diagnóstico de que os consumidores estão resignados com a perda do controle de suas informações é o efeito colateral – e por que não a própria ferida aberta – dessa nova vulnerabilidade, na qual o elo mais fraco rende-se (resigna-se) às forças do mercado informacional.

Nesse sentido, as diversas oportunidades na sociedade atual estão condicionadas ao fornecimento dos dados pessoais. Cada vez mais, a *participação social*[127] é dependente desse trânsito informacional. Na verdade, a lógica do mercado e da sociedade da informação arquitetam essa (falsa) escolha, já que, para fazer parte do jogo, deve-se aceitar o convite mediante o "concordo" em compartilhar os "meus" dados pessoais. Daí por que a proteção dos dados pessoais geraria um *custo social*[128], qual seja, a não fruição dessas oportunidades que resultaria em uma

eremitania na sociedade da informação[129].

Em suma, percebe-se, pois, um *traço vulnerante peculiar* sob diversas perspectivas: informacional, técnica e econômica[130]. Isso é o saldo de uma assimetria, igualmente própria do mercado informacional, que *agrava* a condição de vulnerável do cidadão. Há uma *sobreposição de fraquezas*, na medida em que aquele sujeito vulnerável é inserido em um novo contexto: o do mercado informacional[131].

Por isso, aponta-se que o consumidor é (hiper)vulnerável[132] em meio a esse mercado informacional. Esse agravamento decorre da situação objetiva[133] pertinente a sua inserção no mercado informacional, cujos traços de vulneração são peculiares e se sobrepõem ao ordinário das tradicionais relações de consumo.

Nota-se que essa nova camada de vulnerabilidade não é alicerçada sobre o estado subjetivo ou mesmo a condição pessoal do consumidor[134], tal como ocorre com os consumidores crianças e adolescentes, idosos e pessoas portadoras de deficiência. Ela é, repita-se, fruto de um aspecto objetivo: a emergência de uma nova economia que vulnera o consumidor, especialmente os seus dados pessoais, com o desenrolar de uma dinâmica própria.

Contudo, assim como aqueles grupos sociais de hipervulneráveis[135], o consumidor, inserto no mercado informacional, irá avocar leis especiais para normatizar tal situação em específico. É por isso que, mundialmente, existem leis específicas de proteção de dados pessoais e, nacionalmente, a existência de leis setoriais e geral sobre o tema, sem prejuízo de se projetar outros diplomas específicos – a atualização do CDC[136].

A sobreposição de vulnerabilidades tem reclamado a sobreposição de regimes legais. É o que, exatamente, sucede com o consumidor no tocante à proteção de seus dados pessoais, notando-se uma multiplicidade de fontes do direito[137] que dialogarão para tutelar esse sujeito hipervulnerável na exata medida de suas fraquezas acumuladas.

É curioso notar, no entanto, que a estratégia regulatória dessa explosão normativa de proteção de dados pessoais segue uma lógica contrária à constatação da (hiper)vulnerabilidade do titular dos dados pessoais. Muito embora se dedique um diploma próprio para tratar dessa situação específica de vulnerabilidade, apostam-se todas as fichas normativas como se a parte mais fraca desse arranjo regulatório fosse um sujeito racional, livre e capaz para fazer valer a proteção de seus dados pessoais. O protagonismo do consentimento encerra, portanto, uma *contradição* (intrínseca) desse ambiente ou estratégia regulatória.

É desse descompasso que emerge um *debate normativo*[138] da proteção de dados pessoais. O consentimento tem sido visto como o pilar dessa estratégia regulatória, mais como um meio para legitimar os modelos de negócios da economia digital, do que como um meio eficiente para desempenhar a proteção dos dados pessoais[139]. Ele tem sido encarado como uma verdadeira ficção legal[140] deformadora e voraz do teorizado regime legal de proteção de dados pessoais e da sua aplicação na prática[141]. Não seria mais do que uma mistificação, na medida em que não é confrontado

com o anotado contexto socioeconômico que estrangula a prometida liberdade da autodeterminação informacional[142].

Por tal motivo, é de suma importância frisar essa *incompatibilidade* do desenho normativo de proteção de dados pessoais[143] e, por conseguinte, pensar como isso pode ser absorvido para fins de reflexão e reajustes do ponto de vista de uma (nova) estratégia regulatória.

Mais do que garantir, *artificialmente*, diversos qualificadores para o consentimento (vide subcapítulo 3.4), devem-se buscar, sobretudo, outras ferramentas regulatórias para *equalizar* a referenciada assimetria do mercado informacional, redesenhando a sua dinâmica de poder[144]. Esse é o maior desafio para se propiciar ao cidadão um melhor controle de seus dados – uma verdadeira autonomia para, com o perdão de ser prolixo, autodeterminar as suas informações pessoais.

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[145]. 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.

Os dois itens seguintes irão sequencialmente escorar-se nessa premissa. Em relações de assimetria e cuja causa regulatória é a proteção de um vulnerável, necessário se faz uma *pitada de paternalismo*[146] para que efetivamente seja alcançada uma autonomia por parte do elo mais fraco no processo de tomada de decisão[147] (subcapítulo 4.2 *infra*) e, complementar e subsidiariamente, tomadas mais intervencionistas para a sua proteção (Capítulo 5).

Antes de concluir, ressalva-se que não se desconhece a bipartição entre paternalismo e paternalismo libertário (ou *soft paternalism*)[148]. Basicamente, o último enseja intervenções mais sutis que não usurpam a autonomia do sujeito. A ideia é arquitetar sistemas (estratégias regulatórias) que facilitem o processo de tomada de decisão para que o sujeito, tido como vulnerável, supere a sua debilidade para empreender decisões genuínas.

Essa é a ideia do presente texto, que procura trabalhar *ambivalentemente* com intervenções normativas mais ou menos sutis, mas cuja prioridade é garantir a prometida autonomia. Mesmo que para isso sejam estabelecidos *pisos mínimos* ao longo do desenho normativo em questão, que suavizem o protagonismo do consentimento e implique em uma compreensão mais alargada do que é a autodeterminação informacional.

Por isso, o traço estruturante deste trabalho funda-se no reconhecimento e na absorção da

demonstrada (hiper)vulnerabilidade do cidadão em meio a uma economia de dados. A partir dessa orientação, pretende-se não só verificar como se poderia (re)pensar a estrutura normativa de proteção de dados pessoais, mas, igualmente, projetar a sua aplicação-interpretação[149] – seja das leis setoriais ou geral de proteção de dados pessoais no Brasil.

4.2 EQUALIZANDO AS ASSIMETRIAS PARA UM CONTROLE MAIS EFETIVO DOS DADOS PESSOAIS: TANGIBILIZANDO A ADJETIVAÇÃO DO CONSENTIMENTO

4.2.1 As políticas de privacidade: uma forma sólida e ineficiente para controlar o fluxo líquido dos dados pessoais

É curioso notar que o progresso geracional das leis de proteção de dados pessoais é marcado pela gradual adjetivação empregada ao consentimento, como sendo inequívoco, expresso, informado, específico ou livre (Capítulo 3). Mas, ao mesmo tempo, verifica-se que há um certo *descaso normativo* com relação à(s) forma(s) pela(s) qual(is) ele deveria ser operacionalizado.

Trata-se, assim, de uma espécie de *hipertrofia do consentimento* junto ao restante do corpo normativo de proteção de dados pessoais, o que é diagnosticado por um *desenvolvimento incompleto* dos seus outros "membros" que preencheriam a citada adjetivação e dariam concretude à prometida esfera de controle dos dados pessoais.

Em meio a esse descompasso, o próprio mercado se autorregulou. O surgimento das políticas de privacidade[150] é uma resposta a essa demanda regulatória. Por meio de tal técnica contratual, colher-se-ia o prescrito e necessário consentimento para legitimar toda e qualquer operação de tratamento dos dados pessoais.

Ocorre que tal mecanismo tem se mostrado falho por inúmeras razões, seja porque ele reforça a aventada assimetria do mercado informacional, seja porque se trata de uma ferramenta que não capacita, efetivamente, o cidadão para exercer controle sobre as suas informações pessoais.

Sob a primeira perspectiva, nota-se que as políticas de privacidade são, por excelência, um contrato[151] de adesão[148]. A massificação[149] das relações contratuais ordinárias de consumo é também característica marcante no mercado informacional. Há, igualmente, uma *estandardização* dos instrumentos contratuais, que é conduzida pela predisposição[154] do seu conteúdo pelo fornecedor e, em alguns casos, pela própria Administração Pública. Ao cidadão-consumidor, cabe aderir (concordo) ou não (discordo)[155], sobrevindo daí a própria terminologia em questão – adesão – que exprime tal técnica de contratação[156].

Essa dinâmica dos contratos de adesão assinala, sobretudo, a assimetria de forças das relações de consumo, na medida em que o seu elo mais forte fixa unilateralmente o programa contratual[157]. Isso significa, em termos de proteção de dados pessoais, que será o fornecedor quem determinará os

rumos do fluxo informacional dos seus usuários, eliminando, praticamente, qualquer faixa de controle a ser por eles operada.

Dada essa dinâmica contratual, os usuários não têm poder de barganha[158] para colocar em curso as suas preferências de privacidade. Isso, somado à proeminência de uma série de plataformas que condicionam a própria participação social do cidadão, acaba por tornar falaciosa a prometida esfera de controle dos dados pessoais. É nesse contexto que a lógica do "tudo" ou "nada"[159] das políticas de privacidade acaba por mistificar a autodeterminação informacional[160]. As políticas de privacidade, ora escoradas nessa dinâmica dos contratos de adesão, têm sido uma ferramenta inapropriada para garantir ao consumidor o controle dos seus dados pessoais.

Veja-se, a título de ilustração, o estudo empírico da *Global Privacy Enforcement Network*/GPEN que, por meio das suas 26 autoridades de garantia de proteção de dados pessoais[161], constatou que, das políticas de privacidade de aplicativos móveis/*mobile apps* analisadas: **i)** 85% falham em prestar uma informação adequada sobre a coleta, o uso e o compartilhamento dos dados pessoais; **ii)** 59% são de difícil compreensão para extração de informações básicas a respeito de privacidade; **iii)** 1/3 está coletando dados pessoais excessivos e; **iv)** 43% têm uma interface inadequada, seja porque a tela ou as letras são muito pequenas, seja porque se trata de longos textos que demandam a leitura de inúmeras páginas[162].

Soma-se, ainda, a atualização contínua dos termos de uso cuja instabilidade[163] retira qualquer perspectiva de controle, já que, na maioria das vezes, eles se tornam mais invasivos em relação às suas versões anteriores. Nesse sentido, é elucidativo o estudo da *Electronic Frontier Foundation/EFF* que criou uma *timeline* – para usar o próprio termo da rede social em questão – das políticas de privacidade do Facebook, constatando-se que houve uma *erosão* de uma série de funcionalidades da plataforma e das garantias contratuais contidas nas antigas políticas de privacidade, que possibilitavam aos seus usuários um maior controle sobre seus dados pessoais[164].

Esses exemplos demonstram que essa ferramenta contratual tem sido utilizada para o esvaziamento de qualquer esfera de controle dos dados pessoais. Tais termos contratuais impõem, às vezes, um "cheque em branco", cujo preenchimento – a utilização dos dados pessoais – fica a bel-prazer daquele que estipulou unilateralmente as suas cláusulas contratuais.

Poder-se-ia questionar, nesse contexto: seria possível que tal controle fosse viabilizado por meio da tradicional proteção contratual do consumidor? A resposta é negativa.

Isso porque a proteção contratual do consumidor tem sido, por excelência, um controle *ex post*, mediante a declaração de nulidade das cláusulas contratuais abusivas[165]. No mais das vezes, é em juízo[166] que tal relação assimétrica é, por assim dizer, equalizada. Ao passo que a proteção dos dados pessoais tem sido forjada sob uma racionalidade regulatória *ex ante*. A extensa adjetivação empregada ao consentimento visa a garantir previamente ao cidadão o controle dos seus dados pessoais. Por isso, ainda que válida, a proteção contratual do consumidor no âmbito das políticas de privacidade seria frustrante, já que, na melhor das hipóteses, a prometida esfera de controle seria *a*

posteriori.

Por isso, a proteção contratual do consumidor no âmbito das políticas de privacidade não deve ser vista como o mecanismo ideal para a proteção dos dados pessoais. Deve ser encarada como uma *ação paliativa* se a causa regulatória primária falhar, qual seja, o empoderamento *ex ante* do cidadão para exercer um controle genuíno sobre seus dados pessoais.

E, nesse sentido, tal ferramenta contratual está longe de ocasionar o empoderamento. Na verdade, os seus textos longos e de difícil compreensão são incapazes de sequer estabelecer uma comunicação adequada[167] para que o titular dos dados pessoais possa racionalizar um processo de tomada de decisão.

É famoso, por exemplo, um estudo das pesquisadoras da *Carnegie Mellon University*[168] que avaliaram que os usuários despenderiam, ao menos, 201 horas por ano – o equivalente a U$ 3,354[169] – para que procedessem à leitura de todos os termos de uso dos *websites* que são em média acessados por um usuário americano.

Esse custo torna-se exponencial se for levado em consideração que a metodologia dessa pesquisa não incluiu as políticas de privacidade dos aplicativos móveis, nem mesmo dos famigerados "parceiros comerciais"[170] da rede (*network*) da publicidade comportamental. Isto porque, em tese, demandar-se-ia do usuário a leitura de todos esses termos de uso para tomar conhecimento de todas as práticas comerciais com relação aos seus dados pessoais para, então, decidir aceitá-los ou não. Tem-se, assim, tal como sugere a própria pesquisa, uma *externalidade social negativa* em que a relação custo-tempo da leitura das políticas de privacidade acaba por tornar tal prática inviável[171].

Ao fornecedor e prestador de produtos e serviços não cabe analisar singularmente cada instrumento contratual, já que ele é o mesmo para toda a sua base de consumidores. Diversamente, o consumidor precisa analisar todos os instrumentos contratuais das suas relações, uma vez que eles variam de acordo com cada fornecedor. A massificação dos instrumentos contratuais é, portanto, unilateral, sendo esta a razão pela qual a suscitada externalidade negativa do seu custo de leitura atinge somente os consumidores.

Nesse contexto, seria o caso de se pensar como a massificação de tais relações poderia ser inversa, ou, ao menos, uma via dupla. Seria o caso de investigar como a tecnologia poderia *massificar as escolhas dos consumidores* sobre o trânsito de seus dados pessoais para toda a miríade de atores do mercado informacional. Isso faz total sentido, pois, diferentemente, das relações ordinárias de consumo, essas (novas) relações são estruturadas *universalmente* sobre um mesmo "objeto de troca": os dados pessoais, que são o *trade-off* desses novos modelos de negócios (subcapítulo 1.2.2.3); ao contrário das relações *off-line*, em que a contrapartida de um bem de consumo é fixada, individual e pecuniariamente, para cada relação de consumo.

Trata-se, pois, de perquirir se há novas formas de concretizar a prometida esfera de controle sobre os dados pessoais, se há novas ferramentas que sejam tão *líquidas* e *fluidas* quanto é o fluxo dos dados pessoais, e que percorram universalmente todo o ambiente *on-line*. Isso porque a técnica

contratual *off-line* das políticas de privacidade é uma ferramenta *sólida* que se presta para *estaticamente* exercer um controle dos dados para cada espaço e relação singular do ambiente eletrônico[172]. É por tal razão, que esse ferramental não se ajusta à mencionada complexidade do fluxo informacional das renovadas relações de consumo, sobrecarregando o cidadão do século XXI.

Com base nessa perspectiva, os próximos itens verificarão qual seria um novo ferramental à disposição dos consumidores. O objetivo é contrabalancear a atrofiada estratégia regulatória encampada por uma extensa adjetivação do consentimento que tem sido *artificial* até o momento. Necessário se faz encontrar, portanto, uma correspondência entre a larga qualificação do consentimento e uma pluralidade de formas que o instrumentalize para a desmistificação da autodeterminação informacional.

4.2.2 Tecnologias de Facilitação da Privacidade (*Privacy Enhancing Technologies*/PETs): uma parcela do conceito de privacidade por concepção (*Privacy by Design*/PbD)

Se, por um lado, a tecnologia pode ser invasiva à privacidade informacional, como se verificou no caso dos *trackers* (subcapítulo 4.1.3.2). Por outro lado, ela pode ser uma ferramenta para a proteção dos dados pessoais[173], tal como propõem as denominadas *Privacy Enhancing Technologies*/PETs.

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.

Não é o objetivo deste trabalho estabelecer uma conceituação[174], ou mesmo uma taxonomia das PETs[175], que têm se mostrado como questões equívocas, mas, tão somente, sublinhar que a tecnologia pode ter como dinâmica prioritária a proteção da privacidade. Isso faz parte da metodologia conhecida como *Privacy by Design*. 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[176].

Veja-se, por exemplo, a criptografia que assegura a confidencialidade das comunicações. Ou, ainda, a anonimização dos dados pessoais que quebra ou pelo menos dificulta o vínculo de identificação entre um dado e o sujeito ao qual ele está atrelado (subcapítulo 2.2.2)[177], bem como mecanismos de navegação anônima que impedem o rastreamento do usuário[178]. Em todos esses exemplos, a arquitetura dos sistemas de informação é um instrumento hábil para proteger os dados pessoais do cidadão[179].

Em razão dessa conotação instrumental, as PETs apresentam-se como uma possível solução para a equalização das mencionadas assimetrias do mercado informacional[180], uma vez que são ferramentas capazes de empoderar os cidadãos com um melhor controle sobre os seus dados. E, para além do plano da confidencialidade e do anonimato – exemplos supramencionados –, as PETs podem desempenhar um *papel multifacetado* e *emancipador* para que o cidadão esteja, devidamente,

municiado em meio à corrida tecnológica armamentista de vigilância, captação e mineração de seus dados (subcapítulo 4.1.3.2)[181].

Trata-se de um caminho promissor a ser percorrido para se operacionalizar a prometida esfera de controle dos dados pessoais, notadamente para que o consentimento do titular dos dados pessoais encontre novas formas de operacionalização que não somente as estéreis políticas de privacidade.

Como um catálogo aberto, as PETs podem regenerar a atrofiada estratégia regulatória encampada por uma extensa adjetivação do consentimento que não encontra simetricamente meios a lhe dar vazão. Os dois itens seguintes endereçam, sem qualquer pretensão de esgotar a matéria, duas iniciativas em específico das PETs, a fim de demonstrar que essa é uma agenda que necessita ir além do plano teórico[182], devendo ser objeto de qualquer estratégia regulatória que pretenda colocar em curso uma proteção de dados pessoais mais efetiva.

4.2.2.1 Do Not Track/DNT*: revisitando a ótica binária do* opt-in *e* opt-out *e a qualificação artificial do consentimento no plano da coleta dos dados pessoais*

Como já abordado anteriormente, há inúmeras ferramentas de rastreamento da navegação do usuário (subcapítulo 4.1.3.2). Nesse contexto, dada a perspectiva de que caberia ao usuário consentir para a coleta dos seus dados pessoais, emergiram disputas regulatórias acirradas a respeito de como tal controle deveria ser exercido.

Especialmente na Europa, houve uma divergência entre os países-membros da União Europeia a esse respeito[183]: **i)** se o titular dos dados pessoais deveria consentir de maneira prévia e expressa, aceitando, por exemplo, cada *cookie* a ser instalado para a coleta dos seus dados de navegação (*opt-in*); ou, **ii)** se essa seria uma escolha *a posteriori* e que poderia ser extraída implicitamente por meio das configurações dos *browsers* (*opt-out*)[184].

Essa discussão binária entre os sistemas *opt-in* e *opt-out*, ora conduzida pelos qualificadores expresso e implícito do consentimento, mostra-se útil para a pretensão deste subcapítulo, que é o posicionamento das PETs em meio a tal tensão regulatória.

É interessante notar que a primeira estratégia regulatória mais rígida teve um efeito adverso (in)esperado. Na medida em que se exigia o consentimento prévio e expresso, os usuários foram "bombardeados"[185] com uma avalanche de avisos sobre a instalação de *cookies*. Esses *disclaimers* acabaram por tornar a experiência de navegação dos usuários maçante[186], de modo que eles aceitavam ou os recusavam independentemente de compreender em que resultava tal ação.

Veja-se, portanto, que uma qualificação rígida do consentimento não é garantia de que seja incutida uma habilidade concreta no cidadão para o controle de seus dados pessoais. Tal aptidão é necessariamente condicionada pelos mecanismos disponíveis que a ela deem vazão.

Da mesma forma, o segundo arranjo regulatório, menos rígido, patinou sobre o mesmo problema. Nesse segundo tipo de abordagem, discutiu-se, por exemplo: **i)** de que forma as configurações dos navegadores seriam disponibilizadas aos usuários[187]; **ii)** se a configuração pelo não rastreamento

deveria ser padrão[188]; **iii)** se deveria haver uma padronização dessa ferramenta entre navegadores e aplicações[189]. Mais uma vez, portanto, a questão de fundo gravita em torno da forma pela qual a prometida esfera de controle dos dados pessoais deveria ser operacionalizada.

É justamente disso que se trata o *Do Not Track*/DNT – Não me Rastreie –, que é uma PET arquitetada para executar as escolhas dos titulares dos dados pessoais no plano da coleta. Mesmo que haja divergências conceituais que delimitem o alcance dessa objeção ao rastreamento[190], o DNT surge dentro dessa perspectiva de se pensar em novas ferramentas que facilitem o controle dos dados[191].

Ao contrário de fechar, rejeitar e/ou aceitar inúmeros *pop-ups* de *cookies*, ou, ainda, travar uma saga constante para deletar inúmeros *trackers*, bastaria ao consumidor acionar o botão "DNT" para que, automaticamente, fosse exteriorizada a sua escolha em barrar ou não a coleta de seus dados. Essa funcionalidade seria ativada pelo próprio navegador do usuário que sinalizaria tal opção do usuário a todas as aplicações por ele acessadas[192]. O *browser* seria, assim, a forma pela qual o consentimento do titular dos dados pessoais seria externalizado e, em última análise, o veículo da autodeterminação informacional.

Veja-se, portanto, que tal tecnologia simplifica substancialmente o controle dos dados pessoais na fase da coleta, capacitando o cidadão para fazer valer a sua escolha, mesmo que sem maiores conhecimentos técnicos e sem ser algo penoso[193]. De um lado, o consumidor não necessitaria ser um *expert* para deletar os vários *trackers*, a fim de vencer a corrida armamentista tecnológica de um rastreamento persistente. De outro lado, a sua experiência de navegação não seria prejudicada, já que tal tecnologia *universalizaria* a sua opção em não ter seus dados coletados por toda a *web*[194].

Apesar de promissora, essa tecnologia esbarrou em um impasse em sua implementação, notadamente por um cabo de forças travado entre diferentes atores que avocaram para si a padronização do DNT.

De início, a *World Wide Web Consortium*/W3C foi o fórum primário de discussão do DNT[195]. Em razão de o W3C ser a organização de padronização da *web*, ela chamaria naturalmente essa tarefa, uma vez que o DNT é implementado por um protocolo na *web*[196]. Em um segundo momento, entidades da indústria de publicidade comportamental atribuíram para si tal tarefa, já que, por serem os órgãos representativos do setor empresarial, seriam capazes de garantir que tal protocolo fosse observado pelas corporações[197].

Em meio a esse cabo de forças, o movimento do DNT enfraqueceu-se. Não havia consenso de quem o implementaria, nem mesmo sobre a sua própria concepção. Por exemplo, para o setor da indústria comportamental, o DNT deveria ser apenas um *opt-out* para não receber publicidade comportamental, distorcendo-se o sentido etimológico do que significaria não rastreamento[198].

Soma-se, ainda, em meio a essa batalha, que alguns navegadores anunciaram que adotariam o DNT como configuração padrão, de modo que o usuário precisaria anuir expressamente para ter seus dados coletados[199]. De um lado, ativistas comemoram, mas, do outro lado, o setor industrial

endureceu mais ainda o embate em torno do DNT. A contranarrativa era de que o DNT destruiria a indústria da publicidade comportamental e, por tabela, a camada de aplicações da Internet[200].

Em meio a essa queda de braço, os consumidores continuam amargando a ausência dessa PET. Na medida em que não houve consenso de como essa ferramenta seria implementada e padronizada, ela acabou por não ser *executável*. Ainda que diversos navegadores disponibilizem tal funcionalidade, não há a garantia de que os provedores de aplicações irão respeitar a opção de não rastreamento. Dito de outra forma, o DNT não é cogente, ficando a bel-prazer da indústria cumpri-lo de forma voluntária[201], caindo por terra o seu atrativo maior de universalizar o consentimento do titular dos dados pessoais por toda a *web*.

Esse resumido percurso histórico do DNT demonstra que o cidadão é dependente de uma intervenção regulatória que não somente prescreva o seu direito à autodeterminação informacional, mas que, sobretudo, interfira para a sua operacionalização. De nada adianta preceituar uma gama ampla de qualificadores para o consentimento, acompanhada de um debate binário se ele deve ser prévio (*opt-in*) ou *a posteriori* (*opt-out*), se não há um movimento de regulação para efetivar esse direito[202].

Em conclusão, se a própria autorregulação mostrou-se frustrante para tal desiderato, necessária se faz, então, uma *intervenção regulatória paternalista (libertária)* para corrigir essa distorção do mercado informacional. Deve haver mecanismos que empoderem o cidadão com um controle efetivo de seus dados pessoais. Caso contrário, ter-se-á um direito que não encontra vivência no mundo real, como parece ser o caso da autodeterminação informacional. O DNT parece ser uma ferramenta promissora para que se exerça tal controle no plano da coleta dos dados, faltando-lhe, no entanto, cogência – ser plenamente executável –, o que pode lhe ser atribuído por meio de uma tomada regulatória mais intervencionista[203].

4.2.2.2 Platform for Privacy Preferences/P3P*: massificação das preferências de privacidade e o consentimento granular*

Para além do controle dos dados pessoais no plano da coleta, a tecnologia pode ser também uma nova forma de gerenciamento com relação ao uso e ao compartilhamento das informações pessoais. Não raramente, há o interesse em receber conteúdo e publicidade direcionada, o que demanda necessariamente a coleta e o tratamento dos dados pessoais, razão pela qual uma autodeterminação informacional genuína deve ir além da fase de captura dos dados.

Nesse contexto, a *Platform for Privacy Preferences*/P3P – Plataforma para Preferência de Privacidades – poderia ser esse mecanismo capacitador[204]. Desenvolvida e recomendada desde os idos de 2002 pela W3C[205], o usuário poderia, por intermédio de seu navegador, configurar as suas mais variadas preferências de privacidade, incluindo, por exemplo, quais tipos de dados pessoais poderiam ser coletados (geolocacionais, sensíveis ou não sensíveis etc.) e, até mesmo, se ele assentiria o seu compartilhamento com terceiros. Portanto, o próprio *browser* procederia a uma

análise automatizada das políticas de privacidade das aplicações acessadas, verificando-se a sua (in)compatibilidade com as preferências de privacidade pré-configuradas.

Acontece que para o sucesso de tal ferramenta, além de os navegadores adotarem a funcionalidade da P3P[206], tornar-se-ia necessário que todas as aplicações padronizassem as suas políticas de privacidade em um formato[207] legível (*machine readable formats*)[208] para ser executado um protocolo semântico e de sintaxe que automatizaria a leitura dos termos de uso[209].

Tal como na experiência do DNT, a P3P esbarrou no mesmo problema de não ser executável. A ausência de uma ação regulatória que a tornasse cogente para os navegadores e as aplicações de Internet foi determinante para o seu insucesso[210]. Assim, mais uma vez, o consumidor restou vulnerado nesse impasse regulatório, relegando-se uma promissora ferramenta que poderia executar eficientemente a sua autodeterminação informacional.

Com efeito, a P3P teria o potencial de tornar o fluxo informacional massificado para ambos os lados da relação de consumo do mercado informacional, já que tal tecnologia permitiria aos consumidores *universalizar* as suas preferências de privacidade e, consequentemente, controlar seus dados pessoais sem que fosse necessária a leitura singular e impraticável de cada política de privacidade (subcapítulo 5.3.1). Dito de outra forma, a PET em questão empregaria *fluidez* à autodeterminação informacional, capilarizando-a frente à massa de relações travadas na economia digital pelo titular das informações.

Mais do que isso, afastar-se-ia a lógica do "tudo" ou "nada" das políticas de privacidade, na medida em que o "concordo" ou "discordo" poderiam ser substituídos pela *granularidade*[211] das autorizações especificadas nas preferências de privacidade[212]. Assegurando-se tal poder de barganha[213] na troca econômica (*trade-off*) da economia de dados, a P3P empoderaria o cidadão com uma autonomia genuína sobre o fluxo de suas informações pessoais. O leque de opções do processo de tomada de decisão avançaria para além da lógica binária do *take-it* ou *leave-it*.

Nesse sentido, inclusive, vencer-se-ia a própria idiossincrasia traiçoeira da economia de dados. Na medida em que os seus titulares delimitariam a sua esfera de controle antes do acesso ao bem de consumo, o processo de tomada de decisão não seria enviesado pelas limitações cognitivas da teoria da decisão da utilidade subjetiva: a valoração entre uma perda mediata (o controle dos dados pessoais) e o benefício imediato (o bem de consumo) – subcapítulo 4.1.2.

Em suma, a P3P possibilitaria que o titular dos dados pessoais exercesse sobre eles uma controle significativo, na medida em que tal tecnologia: **i)** universalizaria o processo de tomada de decisão do titular dos dados pessoais por toda a *web*; **ii)** empoderaria o titular dos dados pessoais com um poder de barganha em meio ao *trade-off* da economia digital, já que as preferências de privacidade seriam capazes de aumentar o leque de opções do processo de tomada de decisão sobre o fluxo informacional – consentimento granular em contraposição à lógica do tudo ou nada; **iii)** propiciaria que, ante a automatização das escolhas dos consumidores, a autodeterminação informacional seja tão fluida quanto é o trânsito dos dados pessoais; **iv)** possibilitaria a superação das limitações

cognitivas, especialmente da idiossincrasia das gratificações imediatas e perdas mediatas, já que o controle dos dados pessoais seria *ex ante* à troca pelo bem de consumo.

Enfim, a P3P seria um novo veículo para autodeterminação informacional em substituição à sua falaciosa faceta contratualizada, ora escorada nas políticas de privacidade (subcapítulo 4.2.1). Passados mais de 10 (dez) anos desde a sua concepção, essa ideia, que parece estar "morta", poderia ser revisitada e retomada por uma ação regulatória que a tornasse executável[214].

4.2.2.3 Internet das Coisas/IoT: interoperabilidade e PETs

A Internet das Coisas/IoT (vide subcapítulo 2.3.2) tem sido vista como um cenário ainda mais desafiador para a proteção de dados pessoais. Qualquer perspectiva de controle dos dados pessoais seria esfacelada com a chegada de inúmeros dispositivos que tornariam a coleta de dados ainda mais permanente, massiva, intrusiva e opaca[215]. Questiona-se, por isso mesmo, se seria o momento de migrar para uma abordagem regulatória menos focada no titular dos dados pessoais[216].

Parece-nos que, mais uma vez, a questão central gira em torno de como "pegar carona" nessas novas tecnologias para nelas embarcar soluções que empoderem o cidadão com um controle mais efetivo sobre seus dados.

Uma das questões principais para destravar a agenda de IoT é a necessária *interoperabilidade*[217] entre os diferentes e diversos dispositivos[218]. Como assegurar que coisas projetadas e desenvolvidas por diferentes fornecedores troquem dados entre si para gerar mais conveniência na vida do consumidor. No cenário de uma casa inteligente, por exemplo, os seus respectivos objetos terão que conversar entre si para extrair as informações necessárias para automatizar e otimizar a vida dos seus moradores (da compra de alimentos e outras atividades domésticas até um consumo energético mais eficiente).

Haverá necessariamente a adoção de padrões técnicos que possibilitem essa interoperabilidade. Essa *agenda de padronização* parece ser uma janela de oportunidade para as PETs. Como visto, um dos motivos pelos quais não foi possível escalá-las até hoje foi a resistência de parte da cadeia de agentes em internalizar a sua *linguagem comum*, como no caso do DNT e P3P, por exemplo.

Na medida em que tais dispositivos terão que adotar um *vocabulário comum* para trocarem dados entre si, abre-se a possibilidade para que os seus donos emitam comandos comuns em torno das suas preferências de privacidade.

Da mesma forma que esses dispositivos podem tornar ainda mais opaca a coleta e o processamento de dados, eles também podem representar um passo importante na criação de novos mecanismos para um melhor controle dos dados pessoais. Ao final, o cenário de IoT parece ser mais uma fronteira da velha tensão em como a tecnologia pode ser concebida tendo a privacidade como um dos seus valores de concepção.

4.2.3 Emprestando densidade legal às PETs e dissecando os adjetivos do consentimento

4.2.3.1 *Relação obrigacional e o processo de controle dos dados: PETS[219] de acordo com a concepção dinâmica do vínculo obrigacional*

Ao se falar das PETs, poder-se-ia questionar qual seria o seu fundamento jurídico para lhe dar vazão junto às relações jurídicas em uma economia de dados. Por isso, para além das possíveis ações regulatórias que as destravariam, torna-se imprescindível investigar qual é o seu *substrato legal* no ordenamento jurídico nacional, a fim de que tal proposição não escape ao discurso normativo aqui pretendido.

Procurar-se-á, assim, enquadrar as PETs no seio da relação jurídica obrigacional travada entre o titular dos dados e quem os processa. Pretende-se responder, portanto, como as PETs devem ser posicionadas entre o plexo de direitos e obrigações dessas relações jurídicas sob análise, a fim de emprestar *densidade legal* às PETs.

Ao se falar em uma plêiade de direitos e obrigações, afasta-se, de antemão, do conceito clássico de obrigação[220], qual seja, uma concepção estática do direito obrigacional que se orienta por uma análise meramente dual[221] em que caberia ao credor receber o pagamento e, por outro lado, ao devedor prestá-lo[222]. Isso seria, *mutatis mutandis*, o que se sucede com as práticas correntes das políticas de privacidade em que o titular dos dados pessoais – na condição de consumidor/devedor – "paga" com seus dados pessoais pelo bem de consumo ao seu fornecedor – credor –, deixando-se de lado outros direitos e deveres dessa relação para que o titular dos dados controle-os e, em última análise, desencadeie uma proteção efetiva de suas informações pessoais.

Advoga-se, pelo contrário, em favor da denominada estrutura dinâmica[223] do complexo obrigacional em que as partes cooperam para a consecução de interesses contrapostos. Como, por exemplo, acomodar a tensão entre quem, por um lado, quer explorar os dados pessoais e quem, de outro lado, quer exercer um controle sobre tal manipulação.

Trata-se, portanto, de uma visão solidarista[224] do direito das obrigações que encontra a sua gênese no princípio da boa-fé[225] e que é também um dos princípios da LGPD[226]. É por meio dessa evolução dogmática que surgem os denominados deveres acessórios, secundários, gravitacionais ou satelitários que redimensionam o vínculo obrigacional para conformar uma plêiade de direitos e deveres, de forma cruzada, entre credor e devedor. Assim como os deveres de sigilo, advertência, proteção, cooperação, lealdade e informação que incidem *ex lege* tanto para o credor quanto para o devedor, superando-se a visão estática do direito obrigacional e que neles incute uma ligação de *cumplicidade*[227].

Deve haver uma coordenação recíproca entre os sujeitos do vínculo obrigacional, em razão dessa concomitância de direitos e deveres que devem ser canalizados para um fim comum. É a perspectiva da obrigação como um *processo* em que, por meio de uma prática de atos coordenados, o vínculo obrigacional nasce, desenvolve-se e alcança seu desiderato de acordo com o programa contratual, contribuindo, solidariamente, os dois polos da relação obrigacional para todo esse desfecho[228].

E, por essa visão solidarista, ínsita está a perspectiva de não se causar danos a outrem[229], o que,

no contexto de uma sociedade e economia de dados, está também ligado ao (des)controle dos dados pessoais. Logo, a ideia de obrigação como processo deve ter como fim não só o aperfeiçoamento da sua operação econômica – o já abordado *tradeoff* entre dados pessoais e um determinado bem de consumo ou até mesmo o acesso a uma política pública –, mas, sobretudo, a própria autodeterminação informacional. Esse é o dever de cooperação desejado nessa relação jurídica obrigacional abrigada por um traço de *alteridade* e que percorrerá toda a adjetivação do consentimento.

4.2.3.2 Adjetivação do consentimento

Historicamente, no direito privado brasileiro, a figura do consentimento sempre esteve incubada no tema dos defeitos do negócio jurídico. Do erro à lesão[230], o bem jurídico tutelado é justamente assegurar que a declaração de vontade da pessoa seja "livre e consciente"[231]. A formação imperfeita desse elemento volitivo[232] é considerada como "vício do consentimento"[233], sendo o negócio jurídico decorrente anulável[234].

Dada a remissão expressa da LGPD no tocante à vedação do "tratamento de dados pessoais mediante vício do consentimento"[235], é muito provável que haja um diálogo com o Código Civil brasileiro para se interpretar toda a adjetivação do consentimento à luz dos defeitos do negócio jurídico.

Este livro não analisará cada um dos defeitos do negócio jurídico, muito menos a sua possível releitura dogmática para colá-los a cada um dos qualificadores do consentimento. Nosso objetivo é, no entanto, fornecer outros vetores que auxiliam na compreensão do que será considerado um consentimento válido, diferenciando-se, inclusive, adjetivações empregadas pela LGPD e pelas setoriais brasileiras de proteção de dados.

4.2.3.2.1 Informado: dever-direito de informar e transparência

O dever-direito de informação é o primeiro instrumento para desencadear a referida perspectiva solidária das relações obrigacionais. Isso porque apenas com uma informação adequada o cidadão estará capacitado para controlar seus dados. O fluxo dos seus dados precisa tomar forma (ser informado), sendo *pressuposto* para que haja qualquer tipo de processo de tomada de decisão por parte do titular dos dados.

Por isso, antes de qualquer coisa, é necessário transportar a normatividade do dever-direito de informação, em especial pelo que é fornecido pela legislação e doutrina consumerista que podem inspirar a interpretação da LGPD.

Perquirindo-se a etimologia da palavra informação, poder-se-ia dizer, na sinonímia, que informação é noticiar, fazer, dar conhecimento e/ou instruir[236]. Ou, como prefere Cláudia Lima Marques, decompondo a palavra, informar é "dar" forma, é colocar (in) em uma "forma", aquilo que um sabe ou deveria saber (o *expert*) e que o outro (leigo) ainda não sabe.

Dessa explicação inaugural, constatam-se dois substratos iniciais para dissecar a informação[237] e, com isso, a própria adjetivação do consentimento como informado do ponto de vista *formal* – primeiro elemento.

Se informar é "dar" forma, deve o ato de comunicação ser ostensivo, isto é, ser *perceptível*. Ou seja, a forma como se inicia tal prática é de extrema relevância por ser o antecedente natural para a sua própria compreensão.

Por exemplo, de nada adiantará a implementação do DNT se ele não detiver um símbolo *ostensivo* para alertar os cidadãos sobre a opção de não rastreamento. Ou, sendo tal funcionalidade por padrão (*by default*), que haja, igualmente, um signo de fácil aparência[238] para quem deseja autorizar a coleta de seus dados.

O *segundo elemento* é a utilidade da informação. Sob tal aspecto, a informação deve se mostrar imprevisível e original[239] para colmatar o déficit informacional. Ela deve acrescer, portanto, conhecimento ao dispensar novos elementos para se racionalizar decisões[240].

Exemplificando-se, novamente, com o DNT, tal ferramenta permite que os cidadãos possam exercer (racionalizar) um controle, de forma facilitada, sobre seus dados na fase de coleta, o que seria pouco provável se eles tivessem que aderir à corrida armamentista tecnológica dos *trackers* (subcapítulo 4.1.3.2).

Por isso, a informação não é apenas aproximação, mas, mediante tal perspectiva, ela possibilita ao leigo uma *autoproteção*[241]. Assim, sob o ponto de vista substancial (*qualitativo*), a informação deve somar, deve acrescer, deve preencher o vazio da assimetria informacional, equalizando-a.

É óbvio, no entanto, que ao consumidor é impossível alcançar o mesmo patamar informativo do fornecedor. Até porque, para ele, é desnecessário saber todas as minúcias da atividade de tratamento de dados pessoais.

Pense-se nos diversos padrões de segurança da informação, de como algoritmos são desenvolvidos e assim por diante. Ao cidadão cabe compreender os riscos e as implicações que tal atividade trará sobre a sua esfera pessoal, a fim de racionalizar alguma decisão sobre o fluxo de seus dados. Ao contrário de ser sobrecarregado com uma avalanche de informações sobre a lógica dos protocolos de segurança e as fórmulas dos algoritmos para desvendar, respectivamente, quais seriam os tipos de vulnerabilidades de cada um dos padrões de segurança da informação e qual seria a correlação a ser descoberta por tal algoritmo.

Isso porque, como já abordado, dada a racionalidade limitada (*bounded rationality*) do ser humano[242], o excesso de informação também desinforma (*overloaded information*) – subcapítulo 4.1.2[243]. Ela deve ser prestada em uma *quantidade* suficiente para permitir que o consumidor saiba das qualidades e características do bem de consumo e, ainda, a sua utilização atenta aos riscos que lhe podem sobrevir.

Ou seja, a quantidade de informações pode prejudicar a sua qualidade, ainda que tais critérios não se confundam. O critério qualitativo liga-se à ideia de uma informação original e imprevisível

que equaliza a disparidade informacional entre consumidor e fornecedor. Ao passo que a quantidade de informações é o seu plano consequente, verificando-se se tais informações originais e imprevisíveis são *suficientes*[244] para despertar no consumidor uma compreensão adequada.

Em outras palavras, pouco adianta atentar o destinatário da informação sobre algo que lhe é útil, se o conteúdo informativo não é completo o suficiente para nele desencadear um entendimento completo que coloque em curso um processo genuíno de tomada de decisão.

Veja-se, nesse sentido, que a LGPD segue tal lógica ao: **a)** prescrever que a informação deve ser clara, adequada e ostensiva (*aspecto qualitativo*); e[245] **b)** elencar quais seriam os tipos de informação que deveriam constar do processo comunicativo (*aspecto quantitativo*)[246].

Um bom exemplo prático de toda essa teorização do dever-direito informacional são as "tabelas nutricionais" de privacidade. Por meio de símbolos e/ou categorizações, resume-se aos usuários como que se dariam a coleta, os usos e o compartilhamento dos seus dados e as suas respectivas opões de controle. Por meio de uma interface cheia de signos, a informação transmitida ganha um veículo eficiente para, a um só tempo, ser original, imprevisível e suficiente, despertando no consumidor uma percepção facilitada do fluxo de suas informações pessoais[247].

Nesse mesmo sentido, veja-se o exemplo do *Lightbeam* que, por meio de uma interface gráfica[248], revela aos usuários quais são os atores envolvidos nas atividades de tratamento dos seus dados. Por exemplo, ao acessar um determinado *website*, tal PET demonstrará, por meio de uma animação gráfica, como seus dados pessoais fluem para além da aplicação acessada (*trackers de terceiros* – subcapítulo 4.1.3.2)[249].

Outro bom exemplo é a aplicação de inteligência artificial que automatiza a leitura de políticas de privacidade. Em vez de uma compreensão manual e pouco escalável em meio aos mais diversos *websites* acessados por nós no dia a dia, um *plug-in* não só faz essa leitura, como também sumariza os seus pontos mais importantes[250].

Outra série de tecnologias poderia ser aqui mencionada. No entanto, o que deve ser absorvido é que o próprio dever-direito informacional deve balizar o desenvolvimento das PETs. Deve-se verificar se tais tecnologias são realmente capazes de despertar nos usuários, a um só tempo, a intelecção e o controle do seu fluxo informacional.

Por isso, a agenda das PETs deve canalizar esforços para torná-las cada vez mais amigáveis – *user friendly* –[251], o que é, em última análise, a própria observância do dever-direito de informação para que tais tecnologias despertem de forma original, imprevisível e eficiente a autodeterminação informacional[252].

O dever-direito de informação deve propiciar, portanto, ao usuário os elementos necessários para o *início* de um processo de tomada de decisão no que tange ao fluxo de seus dados[253]. A prestação de uma informação clara, adequada e suficiente é o *portal de entrada* para capacitar o cidadão com o controle dos seus dados, sendo o próprio *adimplemento (satisfatório)* do dever-direito de informação[254].

O pagamento da obrigação de informar deve estar, assim, vinculado a um resultado ótimo: a transparência do fluxo dos dados pessoais. Se, ao final, o titular for empoderado com o controle de seus dados pessoais, ter-se-á, então, o seu adimplemento perfeito.

Não é por outro motivo, aliás, que a LGPD:**a)** ao dispor a respeito do princípio da transparência, correlaciona-o diretamente à prestação de "informações claras, precisas e facilmente acessíveis"[255]; e **b)** prevê ser o consentimento *nulo* caso não haja esse resultado ótimo esperado: a transparência[256]. Portanto, informação e transparência são elementos normativos imbricados em virtude da tamanha correspondência entre eles, havendo um teste de eficiência do primeiro – informação – para com o segundo – transparência –, como o resultado ótimo do dever-direito de informar.

O objetivo final é a redução da assimetria[257] de informação e técnica que circunda todo o fluxo informacional. Visa-se estabelecer uma relação mais sincera e menos danosa, eliminando-se qualquer tipo de opacidade e obscuridade com relação ao trânsito dos dados pessoais.

Vale repetir, a prestação de uma informação só tem razão de ser se ela ocasionar transparência no fluxo dos dados pessoais. Esse é o resultado ótimo esperado decorrente do adimplemento satisfatório do dever de informar e, em última análise, do que se espera ao adjetivar como informado o consentimento.

Quem processa dados deve não só implementar e tornar executáveis PETs, como, também, informar efetivamente o titular dos dados a esse respeito. Não basta apenas assegurar, tecnicamente, o controle dos dados pessoais, sem antes pensar e compreender como a informação será entregue aos cidadãos para que eles possam efetivamente autodeterminar as suas informações pessoais[258].

Do contrário, ter-se-á uma adjetivação artificial do consentimento como informado. Tal baliza jurídica do dever-direito de informação é, portanto, crucial para se garantir eficiência ao discurso normativo da autodeterminação informacional.

4.2.3.2.2 Livre: "poder de barganha"

O adjetivo livre nos remete à ideia de uma ação espontânea que não é objeto de pressão, mas, pelo contrário, de livre-arbítrio caracterizado pela tomada de uma escolha em meio a tantas outras que poderiam ser feitas por alguém.

Por isso, o ponto central do qualificador livre é investigar qual é o nível de assimetria de poder em jogo[259]. Deve-se verificar qual é o "poder de barganha" do cidadão com relação ao tratamento de seus dados pessoais, o que implica considerar quais são as opções do titular com relação ao tipo de dado coletado até os seus possíveis usos. Em síntese, o "cardápio de opções" à disposição do cidadão calibrará o quão livre é o seu consentimento, na exata medida em que esse "menu" equaliza tal relação assimétrica.

Um exemplo claro dessa abordagem é a emergência dos chamados painéis de privacidade que procuram fugir da lógica do "tudo" ou "nada" das políticas de privacidade e, em última análise, da

dinâmica dos contratos de adesão. O leque de opções dessas ferramentas oxigena processos de tomadas de decisões antes sufocados pela lógica binária do *take-it* ou *leave-it*.

O consentimento se torna *granular*[260], por meio do qual o cidadão pode emitir autorizações fragmentadas no tocante ao fluxo de seus dados. Abre-se espaço, assim, para que o controle dos dados seja *fatiado* de acordo com cada uma das funcionalidades que são ofertadas e se deseja ter e que demandam, respectivamente, tipos diferentes de dados.

Nesse sentido, a LGPD considera que, quando o fornecimento de dados pessoais for condição para o acesso a algum tipo de produto ou serviço, o cidadão deve ser informado a esse respeito e sobre os meios pelos quais ele pode exercer seus direitos[261], dentre os quais a revogação do consentimento. Essa disposição, interpretada em conjunto com o adjetivo livre, pode dar normatividade ao consentimento granular.

A questão central é sempre checar a existência de algum tipo de subordinação – assimetria de poder – que possa minar a voluntariedade do consentimento, devendo haver uma análise casuística para se concluir se o consentimento pode ser adjetivado ou não como livre.

4.2.3.2.3 Inequívoco e finalidades determinadas: "não manipulação"

O princípio da finalidade[262] determina que toda atividade de tratamento de dados deve se basear em um propósito "específico e explícito", mesmo nos casos em que a base legal seja uma das outras noves hipóteses autorizativas. Faz parte de toda a lógica do sistema da LGPD especificar a razão pela qual se faz uso de um dado.

No caso do consentimento, esse princípio se torna ainda mais relevante. Qualquer declaração de vontade deve ter um direcionamento, já que não se consente no vazio e de forma genérica. Seria o equivalente a emitir uma espécie de "cheque em branco" que esvaziaria qualquer esfera de controle do cidadão sobre seus dados[263]. Em termos práticos, o famoso "para fins de melhorar a sua experiência", constante de inúmeras políticas de privacidade, deve ser abandonado.

Além disso, a definição de uma finalidade é o que permitirá *analisar regressivamente* se o cidadão foi adequadamente informado para iniciar um processo de tomada de uma decisão livre. Dito de outra forma, os adjetivos informado e livre são calibrados pela locução "finalidades determinadas", ainda que sejam a ela antecedentes.

Trata-se de um *processo* que deve desembocar em uma declaração de vontade *inequívoca* por parte do titular. As suas diferentes fases revelarão se há um comportamento concludente[264], isto é, uma ação afirmativa que não deixe dúvidas sobre a intenção do cidadão.

O termo "ação afirmativa" é uma das diferenças entre a GDPR e a antiga diretiva de proteção de dados pessoais na União Europeia[265]. Ao longo do processo de modernização, o legislador europeu notou a necessidade de traçar parâmetros bastante descritivos para auxiliar na compreensão do que seria um consentimento inequívoco – *unambiguous consent*[266].

Chegou-se até mesmo a prescrever que caixas pré-selecionadas não configurariam um

consentimento inequívoco, na medida em que isso representaria inação ou silêncio por parte do titular do dado. Ao contrário, da situação em que ele de forma proativa sinaliza o seu consentimento por meio das configurações do serviço acessado[267].

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

Apesar de a LGPD não dispor expressamente sobre esse conceito de*privacy by default* em comparação à GDPR[268], é possível extraí-lo do princípio da necessidade[269] ao lado do da responsabilização e prestação de contas. Esta é, aliás, uma interpretação que já se fazia possível pela inteleção do que deve ser um processo genuíno de tomada de *decisão* desde o Marco Civil da Internet[270].

Ao final e o cabo, o grau e a qualidade da *interação* do usuário serão determinantes para qualificar o consentimento como sendo inequívoco. Será necessário, sobretudo, checar a maneira pela qual o *design*[271] de um ambiente (*on-line* e *off-line*) deve incutir no cidadão um controle *visceral*[272] sobre seus dados, em vez de manipular as suas escolhas. Algo que está intrinsecamente ligado ao princípio da boa-fé.

Esse não é um achado tão diferente do que já vem sendo trabalhado há muito tempo no campo da contratação eletrônica acerca dos comportamentos concludentes[273], mas que exige a sua releitura interdisciplinar (da ciência comportamental econômica ao *design*).

Por fim, é importante apontar que o adjetivo inequívoco deve ser visto de forma integrada com outras bases legais, como é o caso do legítimo interesse (Capítulo 5). Dentro de uma perspectiva sistêmica, se fez necessário esculpir um qualificador que não fosse contraditório em relação a situações nas quais se poderiam extrair possíveis usos dos dados, mas sem recorrer à nova autorização do titular dos dados.

Nesse sentido, é importante resgatar os debates travados especificamente ao longo da segunda consulta pública do então anteprojeto de lei de proteção de dados pessoais. A inclusão da base legal do interesse legítimo foi casada como uma adjetivação do consentimento que permitisse tais usos tácitos e implícitos[274]. Esse denominador comum é o que dá organicidade e coerência ao texto como um todo da LGPD.

4.2.3.2.4 Específico e expresso: carga participativa máxima do titular

O adjetivo específico aparece taxativamente nas seguintes situações na LGPD:**a)** quando há envolvimento de terceiros que não mantêm relação direta com o titular para o tratamento de seus dados[275]; **b)** por conta da natureza do dado coletado: dados sensíveis[276]; **c)** em razão da condição de vulnerabilidade do titular do dado: crianças e adolescentes[277]; e **d)** na transferência internacional para um país sem o mesmo nível de proteção de dados que o Brasil[278].

Tal como a GDPR[279], a racional da LGPD é estabelecer uma "camada adicional"[280] de proteção por entender que tais cenários apresentam um risco anormal. O fiel dessa balança é a obtenção de um consentimento especial por parte do cidadão em que ele assente deliberadamente com tais riscos elevados.

Contudo, diferentemente da GDPR, a LGPD utilizou o qualificador específico em vez d expresso. Essa mudança se consolidou no substitutivo apresentado na Câmara dos Deputados em comparação à versão do PLPDP/EXE. Do ponto de vista de técnica legislativa, o termo específico redundante se for considerado que o consentimento já deve ser necessariamente direcionado para propósitos "específicos e explícitos" na linha do que dispõe o princípio da finalidade. Essa significação já está contida na própria definição de uma declaração de vontade que deve ser dirigida para "finalidades determinadas".

Diante desse cenário, o desafio interpretativo é extrair qual seria a "camada adicional de proteção" conferida por esse consentimento especial, ainda que o seu qualificador não seja singular sob o ponto de vista de uma interpretação sistemática da LGPD. Parece-nos que a saída é enxergá-lo como um vetor para que haja mais *assertividade* do titular com relação a esses movimentos "específicos" de seus dados.

Uma das maneiras de extrair essa *carga participativa maior* do titular dos dados seria adotar mecanismos que chamassem mais a sua atenção. Deve haver um alerta que *isole* não só o dever-direito de informação, como, também, a declaração de vontade, colando-a à situação na qual é exigido o consentimento específico.

Isso vai muito além de cláusulas contratuais destacadas que já são mencionadas como uma forma de obter o consentimento trivial e não específico[281]. Todo o processo de tomada de decisão é (com o perdão de ser prolixo) específico e deve ser *pontual*. Da informação até o aceite do titular do dado.

Mais uma vez, será necessário analisar o grau e a qualidade de interação de todo o processo que desengatilha a declaração de vontade. Isso pode variar de mensagens textuais, imagens até um sistema que combine ambos e seja de dupla verificação do consentimento, como seria o caso em que o titular dos dados dá o "concordo" em um *website* e, posteriormente, o confirma por *e-mail*[282].

Não há uma fórmula mágica e, muito provavelmente, haverá variações de acordo com a particularidade dos riscos envolvidos em cada uma das situações em que se exige o consentimento específico[283]. O vetor principal é assegurar que esse processo de deliberação seja gritante (não apenas inequívoco).

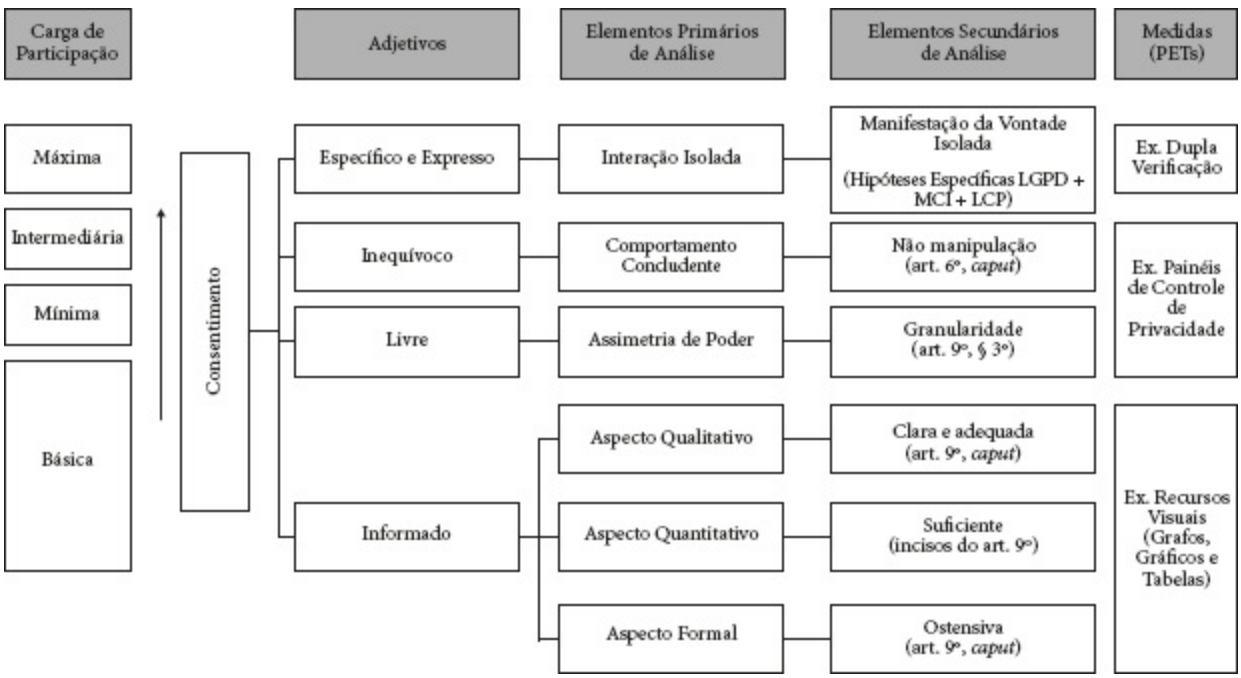
Por isso, sob o ponto de vista de técnica legislativa, teria sido melhor que a LGPD tivesse adotado o adjetivo *expresso*, tal como fez a GDPR, bem como o Marco Civil da Internet e[284], quando se quis prever um tipo de consentimento especial. Esse qualificador é o que semanticamente representaria melhor esse nível de participação mais intenso do cidadão no fluxo dos dados.

Apesar dessa diferença semântica entre os qualificadores expresso e específico, a consequência normativa tende a ser a mesma. Isso porque o que está em jogo é reservar um tipo de autorização

singular em situações igualmente singulares no que tange ao tratamento de dados, sendo esta a racionalidade que percorre a LGPD, a GDPR e parte das leis setoriais brasileiras de proteção d dados pessoais.

Como já defendemos anteriormente, essa adjetivação mais extensa – expresso e específico – desemboca para o mesmo lugar: a carga máxima de participação do cidadão dentro da dinâmica da proteção dos dados pessoais baseada, a partir da acepção de que ele deveria seguir seus dados em todos os seus movimentos[285].

Nesse sentido, o que está por trás de toda adjetivação do consentimento é fornecer pistas sob qual deve ser a carga participativa exigida do cidadão para a circulação de seus dados pessoais. Para fins de sistematização, chegou-se à seguinte abordagem escalável do consentimento que busca estabelecer uma análise progressiva do adjetivo informado ao expresso ou específico.



4.3 CONCLUSÃO: EMPODERANDO O TITULAR DOS DADOS PESSOAIS POR MEIO D UMA AGENDA CRÍTICA DA ARQUITETURA DA REDE E DE ESCOLHAS

Na passagem inaugural deste capítulo, sublinhou-se como a diretriz normativa da autodeterminação informacional se perdeu em meio às assimetrias do mercado informacional, concluindo-se que o cidadão-consumidor está exposto a uma (hiper)vulnerabilidade que mistifica a sua prometida capacidade de controle dos seus dados pessoais.

Logo em seguida, tal diagnóstico realista e pessimista foi contrastado com a perspectiva positiva de que a própria tecnologia pode remendar as fissuras entre o arranjo normativo teorizado e a realidade que lhe é subjacente.

Ao final, problematizou-se que tal horizonte animador poderia consistir, mais uma vez, em uma

solução teoricamente perfeita que pode não encontrar abrigo na vida real. Este subcapítulo visa, assim, fechar tais articulações retóricas, a fim de clarificar as suas proposições.

A tecnologia revelou ser um elemento onipresente do exercício de reflexão proposto até aqui. A arquitetura da rede[286] pode ser, paradoxalmente, um elemento neutralizador – *Privacy Invasive Technologies* – ou capacitatório – *Privacy Enhancing Technologies/PETs* – da habilidade do cidadão em controlar seus dados.

Até o momento, no entanto, essa referenciada dualidade tem escapado ao ambiente regulatório da proteção dos dados pessoais. Por conta da ausência de uma intervenção regulatória, as PETs não têm se mostrado plenamente executáveis aos usuários, tal como foi analisado, de forma mais detida, com as iniciativas do DNT e da P3P. A aposta de que o mercado se autorregularia fracassou, mostrando-se que a mão invisível do mercado foi, de fato, invisível[287] para que a tecnologia se mostrasse, ambivalentemente, como um instrumento para a proteção dos dados pessoais e não só para a sua exploração.

O primeiro passo seria, portanto, viabilizar essa combinação entre direito e tecnologia[288], o que demanda necessariamente uma tomada regulatória[289] para tornar tais tipos de tecnologia cogentes, ou, pelo menos estimulá-los. Somente assim tais tecnologias serão executáveis.

Para além, contudo, dessa agenda regulatória das PETs, necessário se faz absorvê-la sob uma perspectiva crítica. A sua implementação deve observar certas balizas, a fim de que o seu saldo final seja aquele programado pelo discurso normativo da proteção dos dados pessoais, qual seja, a autodeterminação informacional.

Ter em mente que tais tecnologias devem ser de uso fácil e amigáveis (*usable-friendly*), a fim de despertar no usuário uma real capacidade de gerenciamento de suas informações. Trata-se de uma questão substancial para que a abordagem regulatória proposta não seja estéril. Do contrário, o esperado empoderamento do usuário, alavancado pela transparência do fluxo informacional e a redução das assimetrias da relação jurídica sob análise, será apenas uma promessa não cumprida.

A juridicidade desse discurso encontra lugar no dever-direito de informação que, associado à concepção da relação obrigacional como um processo, deve dirigir a implementação das PETs. Trata-se de verificar se essa parcela da PbD é capaz de prestar uma informação adequada, clara e suficiente a respeito do fluxo informacional, a fim de que os cidadãos possam racionalizar um processo de tomada de decisão a seu respeito.

Portanto, o segundo passo, ou mesmo concomitante ao primeiro, é canalizar esforços para que as PETs sejam, utilizando-se uma tradução literal do termo, um instrumento real de melhoria da privacidade. Isso significa, em termos de proteção dos dados pessoais, que o seu resultado ótimo deve despertar no cidadão a capacidade genuína de gerenciamento de suas informações pessoais.

Somente assim o sujeito (hiper)vulnerável poderá cicatrizar a ferida do (des)controle dos seus dados pessoais. A tecnologia pode e deve empoderá-lo, energizando-o para que sejam superadas as fraquezas impostas pela dinâmica de uma economia de dados. Dito de outra forma, uma relação de

interdependência deve ser estabelecida entre a programada autodeterminação informacional e a tecnologia, sendo esta última o seu instrumento de operacionalização[290].

Por isso, as PETs assumem, sobretudo, uma dimensão normativa[291]. As PETs podem, enfim, ser o aparato para um controle genuíno dos dados pessoais, pondo de lado a artificialidade de toda uma adjetivação extensa do consentimento. Os consumidores poderão manipular seus dados pessoais, em vez de terem as suas preferências de privacidade informacional manipuladas[292].

A arquitetura da rede deve, assim, funcionalizar tal habilidade, tomando-se como ponto de partida que o titular dos dados pessoais é um sujeito vulnerável para tanto. É o que chamamos em outra oportunidade de *arquitetura de vulnerabilidade*[293], pela qual se deve aparelhá-lo com mecanismos que lhe permitam superar a sua debilidade com relação ao fluxo de suas informações pessoais.

Esse é o mesmo raciocínio contido na literatura tradicional do "paternalismo libertário"[294] que tem diversos casos *off-line* de sucesso. Por exemplo: **i)** ao se deixarem mais visíveis os alimentos mais nutritivos e menos expostos os alimentos industrializados e mais calóricos nas cantinas das escolas, os alunos passaram a ter hábitos alimentares mais saudáveis; **ii)** ao se estabelecer que a renovação dos contratos de previdência se daria com base no valor escolhido no momento da contratação e não com base no valor mínimo de contribuição estipulado, as pessoas passaram a poupar mais e, ao final, aposentaram-se com uma renda maior.

Ao final e ao cabo, trata-se também da projeção de ambientes[295] que favoreçam a tomada de decisões mais benéficas às pessoas[296]. Na criação de uma arquitetura que "cutuque"[297] o sujeito a fazer escolhas que mitiguem riscos e danos. Por exemplo, ao se alimentar melhor e poupar mais, a pessoa tende a não ter problemas de saúde nem financeiros. E, em uma sociedade em que as suas oportunidades são decididas com base em seus dados pessoais, que o cidadão possa controlá-los.

Somente desta forma se superará parte do drama da proteção dos dados pessoais, que é a sublinhada falta de correspondência entre o programado direito da autodeterminação informacional e uma arquitetura que lhe dê vazão[298]. Trata-se, portanto, de promover o encontro entre o arranjo jurídico-normativo da privacidade informacional com a realidade que lhe é subjacente, buscando-se novas formas para o venerado consentimento do titular dos dados pessoais, nutrindo-se[299], em última análise, a sua capacidade (autonomia) em controlá-los.

[1] O Grande Irmão (Big Brother) era o líder simbólico do partido (figura estatal) que controlava tud todos.

[2] Esse era o verdadeiro nome do romancista; George Orwell era seu pseudônimo.

[3] ORWELL, George. Op.cit., p. 13: "Por trás de Winston, a voz da teletela continuava sua lenga-len infinita sobre ferro-gusa e o total cumprimento – com folga – das metas do Nono Plano Trienal. A teletela recebia e transmitia simultaneamente. Todo som produzido por Winston que ultrapassasse o nível de um sussurro muito discreto seria captado por ela; mais: enquanto Winston permanecesse no campo de visão enquadrado pela placa de metal, além de ouvido também poderia ser visto. Claro, não havia como saber se você estava sendo observado num momento específico".

[4] Idem.

[5] ORWELL, George. Op.cit., p. 16: "Por alguma razão, a teletela da sala de estar ocupava um posição atípica. Em vez de estar instalada, como de hábito, na parede ao fundo, de onde podia controlar a sala inteira, ficava na parede mais longa, oposta à janela. Em um de seus lados havia uma reentrância pouco profunda na qual Winston estava agora instalado e que na época da construção dos apartamentos provavelmente se destinava a abrigar uma estante de livros. Sentando-se na reentrância e permanecendo bem ao fundo, Winston conseguia ficar fora do alcance da teletela, pelo menos no que dizia respeito à visão. Podia ser ouvido, claro, mas enquanto se mantivesse naquela posição não podia ser visto".

[6] Ibidem, p. 16-17.

[7] Oceania é onde se passa o romance *1984*.

[8] ORWELL, George. Op.cit., p. 12: "Em todos os patamares, diante da porta do elevador, o pôste com o rosto enorme fitava-o da parede. Era uma dessas pinturas realizadas de modo a que os olhos o acompanhem sempre que você se move, O GRANDE IRMÃO ESTÁ DE OLHO E VOCÊ, dizia o letreiro, embaixo (...). Não havia lugar de destaque que não ostentasse aquele rosto de bigode negro a olhar para baixo. O GRANDE IRMÃO ESTÁ DE OLHO EM VO dizia o letreiro, enquanto os olhos escuros pareciam perfurar os de Winston".

[9] Essa abordagem foi estabelecida com base na diferença semântica e polissêmica entre os termos *surveillance* e vigilância. O termo em inglês guardaria um sentido maior a cobrir, mais satisfatoriamente, o fenômeno contemporâneo. Veja-se, nesse sentido, a abordagem de: JACOB NETO, Elias; BOLZAN DE MORAIS, Jose Luis. *Surveillance* e Estado-Nação: as inadequadas tentativas de controlar os fluxos de dados através do Marco Civil da Internet e da CPI da espionagem. In: CONPEDI/UFPB (Org.). *Direito e novas tecnologias I*. Florianópolis: Conpedi, 2014. p. 237-238: "Embora a tradução literal – vigilância – seja linguisticamente adequada, a palavra em língua inglesa – bem como na francesa – possui uma polissemia que não é alcançada

pelo termo em português. Isso fica nítido quando os teóricos dos estudos sobre a surveillance fazem a distinção entre 'surveillance' e 'new surveillance', respectivamente associadas à modernidade tradicional e à modernidade líquida. A maturidade do debate no exterior, contudo, permite que os autores anglófonos ressignifiquem a palavra em inglês. Como a carga semântica do vocábulo 'vigilância' é demasiadamente forte no Brasil – por vários motivos, inclusive por estar muito mais ligada, etimologicamente, à palavra 'vigilance' (inglês e francês) –, na ausência de tradução que compartilhe o mesmo sentido, preferimos utilizar o termo diretamente do inglês".

[10] Sobre esse relato ilustrativo da transição da vigilância operada pelo Grande Irmão (Estado) e pel Pequenos Irmãos (setor privado), veja-se, *e.g.*, RAMOS, André de Carvalho. Op.cit., p. 957.

[11] LYON, David. *The Electronic*... Op.cit., p. 51: "Today, networking makes that comprehensivity o reach even more sophisticated, but as the databases are more dispersed, perhaps 'centralization' is not the single best term for this dimension of surveillance capacity. What seems to be happening in many countries is that both greater centralization and increased decentralization is occurring. Surveillance is indeed more dispersed, but the same technical systems make it easier for individuals to be traced by central institutions such as government administrative departments or the police".

[12] Fazendo, também, alusão aos pequenos irmãos: STAPLES, Willliam G.*Everyday Surveillance*. Maryland: Rowman & Littlefield, 2014. p. xii: "What I have been doing for the past two decades is documenting the appearance of what I call postmodern surveillance practices: These relatively mundane, microtechniques of social monitoring and control – the 'tiny brothers' – include the activities of large commercial enterprises that specialize in collecting, processing, aggregating, and storing comprehensive and detailed information about us".

[13] Faz-se referência a todas as ferramentas de rastreamento dos hábitos dos consumidores ao longo d sua navegação na Internet, como, por exemplo, os *cookies, web beacons* etc.

[14] A expressão é de: BRUNO, Fernanda.*Máquinas de ver, modos de ser*: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. p. 24-26: "Propor uma noção que designe as redes de vigilância contemporânea tem aqui duas motivações principais. Inicialmente, a de propor um termo capaz de designar um fenômeno que é complexo, difuso e heterogêneo. Em seguida, a de contestar um diagnóstico corrente tanto em parte dos estudos de vigilância quando nos meios de comunicação. A saber, o da caracterização da ampliação das práticas e dispositivos de vigilância como hipertrofia do panóptico (Jeremy Bentham, 1787), ou do Big Brother (Orwell 1948/1949), dois modelos recorrentes de caracterização de vigilância. (...) A noção de vigilância distribuída aponta, assim, para essa dupla face de escape e captura e marca alguns dos seus ambientes, processos e tecnologias, sobretudo aqueles articulados às redes digitais de informação e comunicação".

[15] Ibidem, p. 25: "A noção de distribuição busca designar um processo reticular, espraiado e

diversificado, pleno de ambiguidades, que não se confunde com a ideia de vigilância homogênea, sem arestas nem conflito".

[16] Ibidem, p. 24-25: "Tendo em vista a crescente penetração das tecnologias de vigilância no cotidiano e a retórica de segurança e do terror após o 11 de setembro de 2001, inúmeros autores têm identificado uma ampliação de dispositivos panópticos nas sociedades atuais (...)".

[17] BAUMAN, Zygmunt; LYON, David. *Vigilância líquida*. Rio de Janeiro: Zahar, 2014. p. 73.

[18] A expressão é de STAPLES, Willliam G. Op.cit., p. 5.

[19] Utilizando-se do mesmo referencial teórico para tecer conclusões similares: BARRETO JUNIOR, Irineu Francisco. Proteção da privacidade e de dados pessoais na internet: o marco civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. t. I, p. 419: "Em suma, para Bauman, vivemos em tempos nos quais as novas práticas de vigilância, baseadas no processamento de informações, permitem tal grau de exposição da vida dos cidadãos, do espectro de papéis que estes desempenham na vida, e faz com que sejamos 'permanentemente checados, monitorados, testados, avaliados, apreciados e julgados".

[20] LYON, David. Introdução. In: BAUMAN, Zygmunt; LYON, David. *Vigilância líquida*. Rio de Janeiro, 2014. p. 10: "'Vigilância Líquida' é menos uma forma completa de especificar a vigilância e mais uma orientação, um modo de situar as mudanças nessa área de modernidade fluida e perturbadora da atualidade. A vigilância suaviza-se especialmente no reino do consumo. Velhas amarras se afrouxam à medida que fragmentos de dados pessoais obtidos para um objetivo são facilmente usados como outro fim. A vigilância se espalha de formas até então inimagináveis, reagindo à liquidez e reproduzindo-a. Sem um contêiner fixo, mas sacudida pelas demandas de 'segurança' e aconselhada pelo marketing insistente de empresas de tecnologia, a segurança se esparrama por toda a parte".

[21] O termo líquido é empregado como um guarda-chuva para explicar todos os fenômenos da modernidade. Segundo Bauman, essa modernidade seria líquida, cujo acontecimentos não seriam formas firmes e sólidas. A metáfora do líquido atenta, assim, que esses fenômenos conservam certas características, ainda que presos não sob uma única forma. É a partir desse paradoxo que o sociólogo polonês emitirá um diagnóstico para os fenômenos do consumo, das relações afetivas e para a própria vigilância. Como está sendo abordado, a vigilância continua a existir na modernidade, mas ela assume outras características que são muito mais fluidas em contraposição a uma percepção clássica e estática, tal como a relação bem delimitada entre vigia e vigiado e tomada por uma atividade ostensiva e específica de observação. Atualmente, já não mais existe um único observador e a atividade de vigilância penetra, cotidianamente, nas vidas dos cidadãos, seja para fins de segurança, seja porque uma nova economia está estruturada pela observância

constante dos potenciais consumidores. Vejam-se, respectivamente, os seguintes referenciais teóricos: BAUMAN, Zygmunt.*Modernidade líquida.* Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2011; BAUMAN, Zygmunt.*Tempos líquidos*. Rio de Janeiro: 2007; BAUMAN Zygmunt. *Amor líquido*. Rio de Janeiro: Zahar, 2004.

22 A expressão "esponja de dados" é utilizada por STAPLES, Willliam G. Op.cit., p. 5.

23 JACOB NETO, Elias; BOLZAN DE MORAIS, Jose Luis. Op.cit., p. 234: "Logo, o eleme 'líquido' (BAUMAN; LYON, 2012), e, por consequência, de difícil controle que caracteriza o fluxo de dados por sistemas de computadores é um traço essencial do que se quer, aqui, denominar 'surveillance'".

24 LYON, David. *The Electronic*... Op.cit., p. 53.

25 BAUMAN, Zygmunt; LYON, David. *Vigilância*... Op.cit., p. 19: "São enormes os desafios que iss apresenta. Expressando de uma forma muito simples, as novas práticas de vigilância, baseadas no processamento de informações e não nos discursos que Focault tinha em mente, permitem uma nova transparência, em que não somente os cidadãos, mas todos nós, por todo o espectro dos papéis que desempenhamos na vida cotidiana, somos permanentemente checados, monitorados, testados, avaliados, apreciados e julgados. Mas, claramente, o inverso não é verdadeiro. À medida que os detalhes de nossa vida diária se tornam mais transparentes às organizações de vigilância, suas próprias atividades são cada vez mais difíceis de discernir. À proporção que o poder se move à velocidade de sinais eletrônicos na fluidez da modernidade líquida, a transparência simultaneamente aumenta para uns e diminui para outros".

26 Não se pretende analisar, profundamente, as limitações cognitivas do ser humano, já que isso desviaria o foco dessa pesquisa que se prende a uma perspectiva normativa. No entanto, é oportuno, ainda que superficialmente, relatar parte dessas limitações cognitivas para fins de problematização da autodeterminação informacional.

27 SOLOVE, Daniel J. Introduction... Op.cit., p. 1889.

28 BAROCAS, Solon; NISSENBAUM, Helen. On Notice... Op.cit., p. 3: "The selective targeting ads based on past behaviors and, possibly, other personal information, raises concerns over an insidious form of discrimination that Oscar Gandy has called the 'panoptic sort'. Aggregating information drawn from diverse sources and different contexts, individuals are profiled and assigned to categories of treatment".

29 A sequência de adjetivos citados (*indeterminate, unending and unpredictable*) compõe um dos subcapítulos de: BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run Around Consent and Anonymity. In: Lane, J.; STODDEN, V.; BENDER, S.; NISSENBAUM, H. (Ed.). *Privacy, Big Data and the Public Good*. Cambridge: Cambridge University Press, 2014. p. 59.

30 BAROCAS, Solon; NISSENBAUM, Helen. On notice... Op.cit., p. 5: "After investigating subject of behavioral targeting intensively and extensively, our own ongoing uncertainty over

what really is happening with information about our online activities suggests that notice, as yet, may not be sufficient for meaningful consent. Users who are subject to OBA confront not only significant hurdles but full-on barriers to achieving meaningful understanding of the practice and uses to which they are expected to be able to consent. This stems from various types of complexity and volatility in the ecology and dynamics of the industry, its policies, and its information flows".

[31] JOLLS, Christine; SUNSTEIN, Cass R.; THALER, Richard. A behavioral approach to law a economics. *Stanford Law Review*, v. 50, p. 1.477, 2004.

[32] ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and rationality in individual decisi making. *IEEE Security & Privacy Review* p. 27, Jan./Feb. 2005. p. 27: "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".

[33] Ibidem, p. 30: "Even if individuals have access to complete information about their privacy risks and modes of protection, they might not be able to process vast amounts of data to formulate a rational privacy-sensitive decision. Human beings' rationality is bounded, which limits our ability to acquire and then apply information".

[34] KERR, Ian; BARRIGAR, Jennifer; BURKELL, Jacqelyn; BLACK, Katie. Soft surveillance, h consent. In: KERR, Ian (Ed.).*Lessons from the identity trail*: anonymity, privacy and identity in a networked society. New York: Oxford University Press, 2009. p. 17: "It is well known in decision theory that subjective utility – that is, the personal value of an outcome – changes depending on when the outcome will be experienced. In particular, the subjective value of a benefit or loss that will be experienced today is greater than the subjective value of that same benefit or loss if we know that it will be experienced some time in the future".

[35] KERR Ian et al., Soft surveillance... Op.cit., p. 18: "(...) decisions against withdrawing consent Bias arises from what is, essentially, a re-weighting of the gains and losses associated with consent after the initial decision has been made. It is a direct result of the decision itself. According to prospect theory, decisions are made in a context where losses loom larger than gains, and outcomes are evaluated against an anchor point or implicit comparator. If the decision under consideration is whether to offer consent in the first place (...)".

[36] Buscando-se a linguística do verbo "prospectar" associada ao adjetivo "prospectiva": HOUAISS Antônio; VILLAR, Mauro de Salles. Op.cit., p. 1.564: "ser mais visível ou mais importante sobressair, salientar-se".

[37] KERR Ian et al., Soft surveillance... Op.cit., p. 18.

[38] Ibidem, p. 19.

[39] Essa foi a expressão utilizada na palestra de: ROSSOGLOU, Kostas. Do-it yourself privac protection. In: COMPUTERS, PRIVACY & DATA PROTECTION INTERNATION CONFERENCE, Jan. 2015. Disponível em: <https://www.youtube.com/watch?v=M_o_uaZwB2Y>.

[40] KERR Ian et al., Soft surveillance... Op.cit., p. 19.

[41] ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and rationality... Op.cit., p. 27.

[42] PURTOVA, Nadezhda. *Property rights in personal data*: An European Perspective. Tese (Doutorado) – Faculdade de Direito da Universidade de Tilburg. Tilburg, 2011. Disponível em: <https://www.academia.edu/4373515/Property_rights_in_personal_data_A_European_perspectiv

[43] CRANOR, Lorrie Faith; MCDONALD, Aleecia M. Beliefs and Behaviors: Internet Use Understanding of Behavioral Advertising, p. 1. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092>.

[44] Idem. Em tradução livre do título da pesquisa, leia-se: 'Crenças e comportamentos: a compreensã dos usuários de Internet a respeito da publicidade comportamental'.

[45] A respeito da metodologia e considerações demográfica da pesquisa: Ibidem, p. 5-6.

[46] Ibidem, p. 4.

[47] Na primeira fase alcançou-se o número de 14 entrevistados. Ibidem, p. 4.

[48] Ibidem, p. 4.

[49] Na segunda fase alcançou-se o número de 314 entrevistados. Ibidem, p. 4-5.

[50] Ibidem, p. 11.

[51] Ibidem, p. 11.

[52] Ibidem, p. 12.

[53] Ibidem, p. 12.

[54] Ibidem, p. 12.

[55] Ibidem, p. 15: "In particular, behavioral advertising based on third-party cookies works in large part because advertising companies can set and read cookies due to ads hosted on a multitude of websites. If people do not understand these basic mechanics, they will not be able to make informed decisions about accepting, blocking, or deleting third-party cookies".

[56] Ibidem, p. 16: "Participants were most likely to select the graphic that reflects the state of modern third-party cookie use, but not even half gave the best answer. Especially when combined with the majority of respondents confused on what is impossible, it seems people do not understand how cookies work and where data flows. Incorrect mental models of how the web works will make it exceedingly difficult for people to understand what options are available to them, and how to enact their privacy preferences online".

[57] Ibidem, p. 25.

[58] Ibidem, p. 23.

[59] Ibidem, p. 25.

[60] Ibidem, p. 26.

[61] Ibidem, p. 28.

[62] Ibidem, p. 29: "First and foremost, consumers cannot protect themselves from risks they do not understand. We find a gap between the knowledge users currently have and the knowledge they would need to possess in order to make effective decisions about their online privacy. (...) Ideally, users could choose for themselves but at present they lack the knowledge to be able to make informed decisions".

[63] Optamos por proceder à leitura do relatório da pesquisa empírica e sua versão em formato de artigo acadêmico, respectivamente: HOOFNAGLE, Chris Jay; URBAN, Jennifer M.; LI, S Privacy and modern advertising: most US internet users want 'do not track' to stop collection of data about their online activities. In: AMSTERDAM PRIVACY CONFERENCE, 20 Disponível em: <http://ssrn.com/abstract=2152135>; HOOFNAGLE, Chris Jay; SOLTAN Ashkan; GOOD, Nathan; WAMBACH, Dietrich James; AYENSON, Mika. Behavior advertising: the offer you cannot refuse. *Harvard Law & Policy Review*, v. 6, p. 273, Aug. 2012); *UC Berkeley Public Law Research Paper* n. 2137601, p. 273-296. Disponível em: <http://ssrn.com/abstract=2137601>.

[64] HOOFNAGLE, Chris Jay et al. Behavioral advertising... Op.cit., p. 273: "Our work demonstrate that advertisers use new, relatively unknown technologies to track people, specifically because consumers have not heard of these techniques. Furthermore, these technologies obviate choice mechanisms that consumers exercise".

[65] Veja-se, especialmente, o tópico atinente à metodologia da pesquisa empírica: HOOFNAGLE Chris Jay et al. Behavioral advertising... Op.cit., p. 285.

[66] Ibidem, p. 277: "Users may be able to avoid some tracking by blocking cookies, but that approach assumes that advertisers will respect individuals' choices, and that advertisers will not employ alternative methods for tracking".

[67] Ibidem, p. 281: "Cookies have been the standard technology for uniquely enumerating Internet user But in recent years, advertisers have adopted new methods that are more difficult for users to detect and block. At the same time, researchers have identified these technologies and explained how they implicate privacy".

[68] São identificadores armazenados no navegador do usuário, criando uma espécie de "impressão digital" que rastreia a sua navegação. Disponível em: <https://en.wikipedia.org/wiki/HTTP_ETag>.

[69] Como o próprio nome induz, trata-se de um *tracker* atrelado ao "Adobe Flash", razão pela qual ta rastreadores têm a capacidade de guardar informações sobre vídeos, músicas e outras aplicações dependentes da execução desse programa, além das páginas visitadas, o que é próprio do rastreamento tradicional. Uma outra peculiaridade diz respeito à dificuldade de deletá-lo, já que ele é armazenado em pastas locais do sistema e não na lista de *cookies* e do histórico da Internet. E, o mais problemático: ele pode reaparecer sempre que for executado o programa da Adobe. Veja-se: FERREIRA, Ana Paula. O que são flash cookies? Por que é importante removê-los Disponível em: <http://www.tecmundo.com.br/seguranca/3046-o-que-sao-flash-cookies-por-que-e-importante-remove-los-.htm>. E, ainda, veja-se a definição disponível em: <https://en.wikipedia.org/wiki/Local_shared_object>.

[70] É como se fosse uma evolução do *cookie* que não expira automaticamente ao terminar a sessão do navegador, tendo, ainda, uma maior capacidade de armazenamento. Veja-se: HOOFNAGLE Chris Jay et al. Behavioral advertising... Op.cit., p. 284.

[71] Apelidado de "*cookies* zumbis", trata-se de um rastreador que combina várias técnicas de rastreamento para se tornar resistente à tentativa de o usuário obstar a coleta de seus dados. Disponível em: <https://en.wikipedia.org/wiki/Evercookie>.

[72] Agrega e combina diversos atributos do computador do usuário, tal como o tipo de navegador, os *plug-ins* para identificá-lo e rastreá-lo. HOOFNAGLE, Chris Jay et al. Privacy and modern. Op.cit., p. 285.

[73] HOOFNAGLE, Chris Jay et al. Behavioral advertising... Op.cit., p. 285.

[74] Ao todo, verificou-se a presença de 5.675 *cookies*, o que representa um crescimento significativo em comparação aos 3.602 de uma pesquisa anterior de 2009. Ressalta-se que todos os 100 *websites* anotaram a instalação de *cookies*. Ibidem, p. 286.

[75] Dos 5.675 *cookies*, 4.915 eram de terceiros. Ibidem, p. 286.

[76] Verificou-se como o *site* Hulu.com manejava as tecnologias *flash cookies* e HTML5 *Web Storage* para fins de uma coleta persistente dos dados pessoais de seus usuários.

[77] HOOFNAGLE, Chris Jay et al. Privacy modern... Op.cit., p. 5: "As consumers have learned about blocking TPCs, some companies have adjusted their tracking mechanisms to make it more difficult for users to avoid tracking. The techniques used to track consumers online now are centralized, ubiquitous, robust, and often redundant".

[78] Esse é o adjetivo usado várias vezes pelos pesquisadores. Exemplificativamente: HOOFNAGLE Chris Jay et al. Behavioral advertising... Op.cit., p. 273, 277, 283, 284, 291 etc.

[79] Notas de rodapé 69 e 70 *supra*.

[80] Idem.

[81] Idem.

[82] Idem.

[83] HOOFNAGLE, Chris Jay et al. Behavioral advertising... Op.cit., p. 285: "The industry has use obscure technologies to circumvent user choices, and they have developed other techniques to undermine consumers' key tool for protecting privacy – the ability to withhold information from sites".

[84] Ibidem, p. 291: "Second, because these vectors are resistant to blocking, they rob consumers of choice. This undermines the advertising industry's representations about respecting individuals' choices and leaves consumers in a technical arms race with advertisers".

[85] Ibidem, p. 294: "The use of obscure tracking methods, data enhancement, cookie respawning, and the zip code re-identification schemes discussed above circumvent user choice. These techniques are often adopted explicitly to make the consumers think they are not being tracked or identified. This combination of disguised tracking technologies, choice-invalidating techniques, and models to trick the consumers into revealing data suggests that advertisers do not see individuals as autonomous beings".

[86] TUROW, Joseph; HENESSY, Michael; DRAPER, Nora. The tradeoff fallacy: how marketers a misrepresenting and opening them up to exploitation. Disponível em: <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf>.

[87] Para maiores detalhes sobre a "população do estudo", veja-se: Ibidem, p. 9-10.

[88] Na pesquisa foram usados os termos "fair" e "ok". Ibidem, p. 11.

[89] Veja-se o quadro representativo donde foram extraídos tais percentuais. Ibidem, p. 12.

[90] As opções do questionário eram: a) concordo definitivamente; b) concordo; c) discordo; d) discordo definitivamente; e) tanto faz. Em números gerais, envolvendo os três questionamentos, apenas 4% responderam as alternativas "a" e "b". Contudo, criando-se um índice de aceitação geral, até para permitir uma interpretação ampla do mencionado *trade-off*, computando-se a alternativa "e" chegou-se ao percentual de 21% em média. Ibidem, p. 12: "To allow for a broader interpretation of a belief in tradeoffs we created a tradeoff acceptance index that gave a value to each answer – 5 to strongly agree, 4 to agree, 3 to neither agree nor disagree, 2 to disagree and 1 to strongly disagree. We then calculated the average scores respondents had on the three statements to see how many averaged disagreement or agreement with the statements. We found that even using from this broader measure a small proportion – 21% – believes common tradeoffs with marketers amount to a fair deal. We then calculated the average scores respondents had on the three statements to see how many averaged disagreement or agreement with the statements. We found that even using from this broader measure a small proportion – 21% – believes common tradeoffs with marketers amount to a fair deal".

[91] Ibidem, p. 12: "please think about the supermarket you go to most often. Let's say this supermarket says it will give you discounts in exchange for its collecting information about all your grocery

purchases. Would you accept the offer or not?".

92 Ibidem, p. 13.

93 Ibidem, p. 13.

94 Ibidem, p. 14.

95 Ibidem, p. 13.

96 Ibidem, p. 13: "Here is where we begin to explore an alternative view, our resignation hypothesis The meaning of resignation we intend is, to quote a Google dictionary entry, "the acceptance of something undesirable but inevitable".

97 Esse é um diagnóstico recorrente na literatura para apontar que, apesar de as pessoas valorarem a sua privacidade, empreendem ações que com ela são conflitantes. Veja-se, entre outros: HOLLAND, H. Brian. Privacy Paradox 2.0 (April 4, 2010). Disponível en <http://ssrn.com/abstract=1584443>.

98 STONE, Brad. Our Paradoxical Attitudes towards Privacy.*New York Times*, 2 de julho de 2008. Disponível em: <http://bits.blogs.nytimes.com/2008/07/02/our-paradoxical-attitudes-towards-privacy/.>.

99 TUROW, Joseph et al., The tradeoff... Op.cit., p. 14.

100 Resignação é compreendida como ato de submissão à vontade de alguém: HOUAISS, Antônic VILLAR, Mauro de Salles. Op.cit., p. 1651.

101 Uma série de perguntas foi feita, envolvendo desde *price discrimination* até o compartilhamento dos dados pessoais com terceiro. Ibidem, p. 16.

102 Ibidem, p. 17.

103 Ibidem, p. 19: "One issue raised by the findings is that Americans' are resigned regarding their ability to control the information marketers can collect and use about them. Resigned individuals may behave in ways that allow marketers to claim they are unconcerned or accept the economic logic (...)".

104 Ibidem, p. 21.

105 Ibidem, p. 19: "Americans surely sense the changes that are happening and feel powerless to do anything about them. Our finding that 58% of Americans are resigned to not having a say in these activities – that they do not want to lose control over their information but also believe their loss of control has already happened – suggests the population feels a lack of autonomy".

106 O pesquisador Jospeh Turow concedeu uma entrevista ao Grupo de Políticas Públicas para Acess à Informação/GPoPAI da Universidade de São Paulo, oportunidade na qual ele assinala que esse problema estrutural está, sobretudo, correlacionado ao custo social de uma vida dependente desses novos bens de consumo: Você trocaria sua privacidade por descontos em produtos? Disponível em: <http://www.privacidade.net/?p=62> ou

<http://www.cartacapital.com.br/sociedade/voce-trocaria-sua-privacidade-por-descontos-em-produtos-4348.html>: “As pessoas sabem que estão sendo vigiadas”, explica Turow, “mas não enxergam nenhuma maneira de impedir isso”. Para ele os consumidores americanos se sentem acuados. Por um lado, não compreendem como seus dados pessoais são utilizados pelas empresas e pelos publicitários; por outro, temem sofrer perdas sociais e econômicas caso escolham não tomar parte nas relações e serviços de uma economia baseada na troca de dados. “Quando você vive num mundo em que todos os seus amigos estão numa rede social que coleta seus dados, como Facebook, ou acredita que o Google fornece o melhor serviço de buscas da Internet, é muito difícil se imaginar fora deste mundo”, explica ele.

[107] UTZ, Christine; DEGELING, Martin; FAHL, Sascha; SCHAUB, Florian; HOLZ, Thors (Un)informed consent: studying GDPR consent notices in the field. In: 2019 ACM SIGSA Conference on Computer and Communications Security (CCS ’19), November 11–15, 2019 London, United Kingdom. ACM, New York, NY, USA. Disponível em <https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2019/09/05/uninformed-consent_Yl7FPEh.pdf>.

[108] Aviso de cookie ou cookie notice é o banner que aparece na tela do usuário ao entrar em um site, indicando que este está coletando cookies.

[109] UTZ, Christine; DEGELING, Martin; FAHL, Sascha; SCHAUB, Florian; HOLZ, Thors (Un)informed consente... Op cit., p. 04: “Typical techniques include color highlighting of the button to accept privacy-unfriendly defaults, hiding advanced settings behind hard to see links, and pre-selecting checkboxes that activate data collection”.

[110] Dentre os diferentes tipos de notificações usadas pelos pesquisadores para observar as interações dos usuários, utilizou-se um aviso que dizia “[Este site] utilizada cookies para analisar a experiência de seus usuários, para fixar vídeos e links para redes sociais, e para personalizar os anúncios que você vê. Por favor, selecione os tipos de cookies que estamos autorizados a usar. Você pode encontrar mais informações em nossa política de privacidade. [] Necessários; [] Personalização e Design; [] Analytics; [] Social Media; [] Marketing”. Este aviso foi apresentado de duas formas: com todas as opções selecionadas e com apenas a primeira opção selecionada e sem possibilidade de ser “desmarcada”.

[111] É o que se depreende do art. 2º, *caput*, em conjunto com o art. 3º, *caput*, ambos da Consolidação das Leis do Trabalho. Respectivamente: “Considera-se empregador a empresa, individual ou coletiva, que, assumindo os riscos da atividade econômica, admite, assalaria e *dirige* a prestação pessoal de serviço”; “Considera-se empregado toda pessoa física que prestar serviços de natureza não eventual a empregador, sob a *dependência* deste e mediante salário” (grifos).

[112] NASCIMENTO, Amauri Mascaro*Iniciação ao direito do trabalho*. São Paulo: LTR, 2009. p. 163-164: “Empregado é um trabalhador cuja atividade é exercida sob dependência de outrem

para quem ela é dirigida. Nossa lei usa a palavra 'dependência'. No entanto, em lugar dela, generalizou-se hoje outra expressão, a palavra 'subordinação', de maior importância, uma vez que permite dividir dois grandes campos de trabalho humano: o trabalho subordinado e o trabalho autônomo".

113 LYON, David. *The Electronic*... Op.cit., p. 34.

114 Fala-se, nesse sentido, em "função tutelar" para que o trabalhador não seja "absorvido" pelo pode econômico do trabalhador: NASCIMENTO, Amauri Mascaro. Op.cit., p. 161.

115 MORATO, Antonio Carlos. *Pessoa jurídica*... Op.cit., p. 138.

116 MIRAGEM, Bruno. *Direito do*... Op.cit., p. 23.

117 Ibidem, p. 24.

118 Tal mensagem ao congresso americano está disponível em: <http://www.presidency.ucsb.edu/ws/pid=9108>.

119 COMPARATO, Fábio Konder. Op.cit., p. 170.

120 LORENZETTI, Ricardo Luis. *Teoria da*... Op.cit., p. 251.

121 Não é o objetivo deste trabalho esgotar o tema da vulnerabilidade, mas, tão somente, apontar a existência de uma vulnerabilidade própria do consumidor no mercado informacional para, daí, serem tecidas algumas conclusões do ponto de vista de estratégia regulatória para a proteção de seus dados pessoais. Anota-se, por isso, a existência de obra monográfica sobre o tema que situa historicamente tal transformação "solidária" do direito na tutela dos vulneráveis, discorrendo sobre seus fundamentos éticos e jurídicos e suas projeções futuras. MARQUES, Cláudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis*. São Paulo: Revista dos Tribunais, 2012.

122 Ibidem, p. 190.

123 MARQUES, Cláudia Lima; BENJAMIN, Antônio Herman V.; MIRAGEM, Bruno. *Comentários*... Op.cit., p. 198.

124 MIRAGEM, Bruno. *Direito*... Op.cit., p. 23: "(...) intervenção em favor do sujeito reconhecido como vulnerável tem por objetivo a recomposição da igualdade jurídica, corrigindo os elementos fáticos de desigualdade".

125 Nota de rodapé 118 do Capítulo 1 *supra* (STRANDBURG, Katherine J. Op.cit., p. 150).

126 DONEDA, Danilo. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia/Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 9-10: "A abundância da informação passível de ser obtida sobre o consumidor pode caracterizar *uma nova vulnerabilidade do consumidor* em relação àqueles que detêm a informação pessoal. O acesso do fornecedor a estas informações é capaz de desequilibrar a relação de consumo em várias de suas fases, ao consolidar uma nova modalidade de assimetria informacional. Esta nova

assimetria informacional não se revela somente no poder a que o fornecedor pode ascender em relação ao consumidor ao tratar suas informações pessoais, porém também em *uma nova modalidade de modelo de negócio na qual a própria informação pessoal se objetiva como commodity*, como um ativo que pode chegar a ser o eixo de um determinado modelo de negócios" (grifos).

127 Essa terminologia é emprestada de LYON, David. *The Electronic*... Op.cit., p. 31. É importante notar, contudo, que o sociólogo canadense tem um olhar mais amplo, que não o circunscrito neste trabalho jungido ao mercado consumidor informacional. Ele denota que a vigilância, seja nas relações com o estado ou com os particulares, tem uma dupla faceta: a de controle e a de participação social.

128 Ibidem, p. 232: "Consequently, data protection, despite deliberate attempts to broaden access and streamline enforcement, remained largely a privilege of minorities, who could economically and socially afford to exercise their rights, while the intended large-scale self-determined shaping of one´s own informational image remained political rhetoric".

129 Ibidem, p. 229: "But what price does one have to pay for that? Is it acceptable that such data-protection liberties can be exercised only by hermits? Have we reached an optimum of data protection if we guarantee privacy rights that, when exercised, will essentially expel the individual citizen from society?".

130 Sabe-se que a vulnerabilidade tem sido fragmentada em técnica, informacional, jurídica e econômica (MARQUES, Cláudia Lima; BENJAMIN, Antônio Herman V.; MIRAGEM, Bru *Comentários*... Op.cit., p. 198-199; MIRAGEM, Bruno *Direito*... Op.cit., p. 63-64). Em nosso trabalho, não recorremos a tal compartimentalização, ainda que isso fosse possível. Isto porque, sob nosso ponto de vista, perder-se-ia coesão na sua construção, já que suas subdivisões se apresentam, intimamente, entrelaçadas no mercado informacional.

131 Nossa pretensão é identificar uma (hiper)vulnerabilidade do consumidor no mercado informacional, ora caracterizada no âmbito da proteção de seus dados pessoais. Difere-se em parte, portanto, de outros estudos que similarmente identificam uma vulnerabilidade agravada do consumidor no âmbito do comércio eletrônico, mas que não têm esse mesmo recorte epistemológico. Veja-se, por exemplo: CANTO, Rodrigo Eidelvein do. *A vulnerabilidade dos consumidores no comércio eletrônico*: a reconstrução da confiança na atualização do Código de Defesa do Consumidor. São Paulo: Revista dos Tribunais, 2015. p. 78-95; MARQUES, Cláudi Lima; BENJAMIN, Antônio Herman V.; MIRAGEM, Bruno *Comentários*... Op.cit., p. 71; MIRAGEM, Bruno. Responsabilidade por... Op.cit., p. 1035: "Neste sentido ocorr especialmente em relação às normas de proteção do consumidor, cuja aplicação no ambiente da Internet guarda correspondência com as relações de consumo estabelecidas no mercado, devendo ser observada inclusive maior nível de proteção, em face da vulnerabilidade agravada dos

consumidores em relação às inovações tecnológicas da informática de um modo geral".

[132] MARQUES, Cláudia Lima; MIRAGEM, Bruno. *O novo direito*... Op.cit., p. 189: "Já hyper é prefixo grego para designar o aumento, agravamento, aquilo que é 'além' do ordinário, normal ou típico, que está em outra dimensão, que abre um espaço especial (no caso, de proteção do mais fraco)".

[133] Similar raciocínio para concluir pela (hiper)vulnerabilidade do consumidor no comércio eletrônico: CANTO, 2015. p. 91: "Sobre essa vulnerabilidade basilar alicerçar-se-á a transposição das relações de consumo para o mundo *on-line* – também denominada de virtualização do real – que, passará a compor a segunda camada de vulnerabilidade. Essa sobreposição de vulnerabilidades afetará todos os consumidores que utilizam o comércio eletrônico indiscriminadamente, tornando-os mais frágeis e suscetíveis de serem sistematicamente lesionados pelos fornecedores, sendo isso resultado da despersonalização, desmaterialização, desterritorialização, a atemporalidade da contratação eletrônica".

[134] Destoa-se, assim, da parcela doutrinária que condicionaria a (hiper)vulnerabilidade a uma condição subjetiva do consumidor. Em nosso trabalho estamos a falar de uma situação objetiva, que é a inserção do consumidor no mercado informacional e, especialmente, no tocante à proteção de seus dados pessoais. Em sentido contrário, parece ser o posicionamento de: MARQUES, Cláudia Lima; MIRAGEM, Bruno. *O novo direito*... Op.cit., p. 189: "Em outras palavras, enquanto a vulnerabilidade 'geral' do art. 4.º, I se presume e é inerente a todos os consumidores (em especial tendo em vista a sua posição nos contratos, tema desta obra), a hipervulnerabilidade seria inerente e 'especial' à situação pessoal de um consumidor, seja permanente (prodigalidade, incapacidade, deficiência física ou mental) ou temporária (doença, gravidez, analfabetismo, idade) (...) Parece-me, porém, que a vulnerabilidade agravada é assim como a vulnerabilidade um estado subjetivo multiforme e pluridimensional, e que, com base no princípio da igualdade (*aequitas*) e da equidade, pode se incluir outros 'fracos', como as minorias mais frágeis e os doentes, por exemplo".

[135] Respectivamente, nós temos o Estatuto da Criança e do Adolescente (Lei 8.069/90), o Estatuto do Idoso (Lei 10.741/2003), as Leis 7.853/1989 (Política Nacional de Integração da Pessoa Portadora de Deficiência) e os Decretos 3.956/2001 (Convenção Interamericana para a Eliminação de Todas as Formas de Discriminação contra as Pessoas Portadoras de Deficiência) e 6.949/2009 (Convenção Internacional sobre os Direitos das Pessoas com Deficiência).

[136] Atenta-se que o PL 281/2012 do Senado, que tem o foco de regulamentar o comércio eletrônico, conta com dois dispositivos dedicados à proteção de dados pessoais, sendo que um deles ressalta essa nova assimetria e o direito do consumidor de autodeterminar as suas informações pessoais: "Art. 45-A. Esta seção dispõe sobre normas gerais de proteção do consumidor no comércio eletrônico, visando a fortalecer a sua confiança e assegurar tutela efetiva, com a

diminuição da *assimetria de informações*, a preservação da segurança nas transações, a *proteção da autodeterminação e da privacidade dos dados pessoais*" (grifos).

137 AZEVEDO, Antônio Junqueira de. O direito pós-moderno e a codificação. In: MARQUE Cláudia Lima; MIRAGEM, Bruno (Org.). *Coleção doutrinas essenciais*: direito do consumidor – fundamentos do direito do consumidor. São Paulo: Revista dos Tribunais, 2011. v. 1, p. 555-564.

138 Vejam-se, a título de exemplo, os seguintes textos que situam bem esse debate normativo: CATE, Fred H. The failure... Op.cit.; AUSTIN, Lisa M. Reviewing PIPEDA: control, privacy and t limits of fair information practices. *The Canadian Business Law Journal*, v. 44, n. 1, p. 21-53, Oct. 2006. E, ainda, a nota de rodapé 46 do Capítulo 5 *infra*.

139 BLUME, Peter. The inherent contradictions in data protection law.*International Data Privacy Law*, v. 2, n. 1, p. 27, 2012: "Seen from the perspective of the controllers, it is implied that data protection aims to make it legitimate to process personal data. (...) The fundamental observation is that data protection law is viewed as a societal necessity in order to make it possible for controllers to process personal data and to benefit from the information and knowledge processing entails".

140 Utiliza-se o termo "ficção legal do consentimento" para descrever essa disparidade entre a teoria a realidade prática da proteção de dados pessoais: SCHWARTZ, Paul M. Internet privacy an state. *Connecticut Law Review*, v. 32, p. 825, 2000.

141 Veja-se, por exemplo, o instigante estudo, cujo título fala por si mesmo: BAMBERGER, Kenneth, et al. Privacy on the books and on the ground. *Stanford Law Review*, v. 63, p. 247, Jan. 2011.

142 SMITIS, Spiros. Reviewing Privacy in an Information Society*University of Pensilvania Law Review*, v. 135, p. 736, 1987: "the chimerical nature of the assumption that effective protection of privacy can be accomplished by simply entrusting the processing decision to the persons concerned (...) process of consent is no more than a 'mystification' that ignores the long-standing experience that the value of a regulatory doctrine such as 'informed consent' depends entirely on the social and economic context of the individual activity".

143 ACQUISTI, Alessandro. Nudging privacy: behavioral economics of personal information*IEEE Security & Privacy*, p. 83, Nov./Dec. 2009.

144 A expressão "dinâmica de poder" é de: CALO, Ryan. Consumer subject review boards: a though experiment. *Stanford Law Review Online*, v. 97, p. 97-102, Sept. 2013.

145 BLUME, Peter. Op.cit., p. 30.

146 HOOFNAGLE, Chris Jay et al. Behavioral advertising... Op.cit., p. 285: "In the political debat "paternalism" is a frequently invoked objection to privacy rules. Our work inverts the assumption that privacy interventions are paternalistic while market approaches promote freedom. (...) We argue that 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".

147 Kerr, Ian et al. Soft surveillance... Op.cit., p. 5-7; ACQUISTI, Alessandro. Nudging... Op.cit., p 84.

148 O escopo deste trabalho não permite um exame profundo das diferenças entre *paternalism* e *soft paternalism*. Anotam-se, por isso, as referências bibliográficas em termos gerais e em termos específicos sobre privacidade, respectivamente: REBONATO, Riccardo.*Taking liberties*: a critical examination of Libertarian paternalism. London: Palgrave, 2012. Para um referencial em língua portuguesa, veja-se: SUNSTEIN, Cass. THALER, Richard H. O paternalismo libertár não é uma contradição em termos. Tradução Fernanda Cohen. *Revista Civilística*, n. 2, p. 1-47, 2015. Disponível em: <http://civilistica.com/wp-content/uploads/2015/12/Sunstein-e-Thaler-trad.-Cohen-civilistica.com-a.4.n.2.20151.pdf>. E também o livro: SUNSTEIN, Cass. THALE Richard H. *Nudge*: improving decisions about health, wealth, and happiness. New Haven & London: Yale University Press, 2008.

149 Em sentido mais abrangente, cobrindo a chamada proteção dos vulneráveis: MARQUES, Cláudi Lima; MIRAGEM, Bruno*O novo direito*... Op.cit., p. 124: "São essas as bases do pensamento filosófico, ético-jurídico, as quais permitem que se identifique no direito privado a ressignificação da igualdade e reconhecimento da necessidade de proteção dos vulneráveis mediante produção normativa nova, mas especialmente a partir de uma nova perspectiva dos juristas na construção das soluções jurídicas concretas, mediante interpretação e aplicação das normas jurídicas".

150 Correlacionando a autorregulação, por meio do surgimento das políticas de privacidade, no mercado americano com o padrão normativo da autodeterminação informacional advindo das FIPPs: SOLOVE, Daniel J.; HARTZOG, Woodrow. The FTC... Op.cit., p. 593: "Another of most prominent FIPPs is the individual's right to consent to the collection and use of her personal data. These two FIPPs became the backbone of the U.S. self-regulatory approach, with privacy policies seeking to satisfy the right to notice, and with user choice seeking to satisfy the right to consent".

151 Neste trabalho, reconhece-se não ter uma opinião formada se as políticas de privacidade seriam consideradas contratos de adesão ou condições gerais de contratação. Isto porque os termos de uso acabam por disciplinar um número indeterminado de relações contratuais do consumidor, na medida em que, por exemplo, seria capaz de regulamentar o fluxo dos dados pessoais dos consumidores com outras aplicações e com os famigerados "parceiros comerciais". Por esse viés, as políticas de privacidade enquadrar-se-iam nessa última espécie do fenômeno da massificação contratual. A nossa indecisão é decorrente do próprio impasse na doutrina no que diz respeito à utilidade de tal diferenciação entre contratos de adesão e condições gerais de contratação. A favor: MARQUES, Cláudia Lima. *Contratos no código de defesa do consumidor*:

o novo regime das relações contratuais. São Paulo: Revista dos Tribunais, 2011. p. 74-75; 86-87. Em sentido contrário: GOMES, Orlando.*Contratos de adesão*: condições gerais dos contratos. São Paulo: Revista dos Tribunais, 1972. p. 5-9.

[152] Para um estudo completo sobre os contratos eletrônicos de adesão, veja-se por todos: LIMA Cíntia Rosa Pereira de.*Validade e obrigatoriedade dos contratos de adesão eletrônicos (shrink-wrap e click-wrap) e dos termos e condições de uso (browse-wrap)*: um estudo comparado entre Brasil e Canadá. Tese (Doutorado) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2009.

[153] Essa é, em síntese, a "gênese" dos contratos de adesão que é marcada pela transição de uma economia artesanal e familiar por uma economia industrial em massa. Nesse sentido: MIRANDA, Custódio da Piedade Ubaldino. *Contrato de Adesão*. São Paulo: Atlas, 2002. p. 13-16.

[154] GOMES, Orlando. *Contratos de adesão*... Op.cit., p. 5.

[155] Veja-se, nesse sentido, a própria ressalva terminológica de que os contratos seriam por adesão e não de adesão. GOMES, Orlando.*Contratos de adesão.* Op.cit., p. 5: "Afinal, a aceitação em bloco de cláusulas preestabelecidas significa que o consentimento sucede por adesão, prevalecendo a vontade do predisponente (...)".

[156] MIRANDA, Custódio da Piedade Ubaldino*Contratos*... Op.cit., p. 20: "A expressão contrato de adesão resulta inicialmente do fato de que o que impressiona nessa figura, em relação à estrutura normal de um contrato, é a posição do aderente que não tem a possibilidade de discutir as cláusulas, até mesmo as que lhe sejam desfavoráveis, quer sejam ilegais, quer não, sob pena de ser excluído o círculo dos possíveis contratantes".

[157] MARQUES, Cláudia Lima. *Contratos*... Op.cit., p. 77.

[158] DOCTOROW, Cory. The Curious Case of Internet Privacy*MIT Technology Review*, 2012. Disponível em: <http://www.technologyreview.com/news/428045/the-curious-case-of-internet-privacy>. Veja-se, ainda, o estudo empírico que analisou as políticas de privacidade sob as jurisdições americana e alemã de: ANTONIALLI, Dennys Marcelo. Watch your steps: a empirical study of the use of online tracking tecnologies in different regulatory regimes. *Stanford Journal of Civil Rights & Civil Liberties*, p. 348, Aug. 2012.

[159] MARQUES, Cláudia Lima. *Contratos*... Op.cit., p. 79: "Realmente, no contrato de adesão, não há liberdade contratual de definir conjuntamente os termos do contrato, podendo o consumidor somente aceitá-lo ou recusá-lo. É o que os doutrinadores anglo-americanos denominam em uma take-it-or-leave-it".

[160] SCHWARTZ, Paul. Privacy in... Op.cit., p. 825: "In this fashion, privacy-consent neglects th actual conditions of choice regarding the processing of personal information, and permits notice to become an alibi for 'take-it-or-leave-it' data processing".

[161] Ressalva-se a multiplicidade de reguladores associados a tal órgão de cooperação, sendo que nem

todos enquadram-se, formalmente, no conceito de autoridade de garantia. Esse é, por exemplo, o caso do Privacy Commissioner do Canadá que não tem os mesmos poderes de uma autoridade de garantia, tal como de "poder de polícia", para a imposição de penalidades monetárias. Veja-se a lista completa dos órgãos associados em: <https://www.privacyenforcement.net/public/members>.

[162] Informational Commissioner's Office. Global survey finds 85% of mobile apps fail to provide basic privacy information. Disponível em: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/09/global-survey-finds-85-of-mobile-apps-fail-to-provide-basic-privacy-information>.

[163] BAROCAS, Solon; NISSENBAUM, Helen. On notice... Op.cit., p. 1.

[164] OPSAHL, Kurt. Facebook's Eroding Privacy Policy: a timeline. Disponível em: <https://www.eff.org/deeplinks/2010/04/facebook-timeline>.

[165] Veja-se, nesse sentido, o rol exemplificativo de cláusulas abusivas contido no art. 51 do CDC.

[166] Ressalva-se, contudo, que a proteção do consumidor pode ser realizada no âmbito das esferas dos interesses difusos e coletivos, o que suavizaria esse controle *ex post*, já que, em tese, (novos) consumidores beneficiar-se-iam desse controle ao contratar sob essas novas bases contratuais – após ações coletivas para reequilibrar esses instrumentos contratuais abusivos. Mas, mesmo assim, o controle dessa abusividade é, necessariamente, exercido em um momento posterior à adoção dessas práticas contratuais pelo mercado, sendo sempre repressivo (*ex post*) e não preventivo (*ex ante*).

[167] Já tivemos a oportunidade de tratar sobre o dever-direito de informar e a sua (in)aplicabilidade por meio das políticas de privacidade: BIONI, Bruno Ricardo. O dever... Op.cit., p. 306 "Políticas de privacidade e termos de uso com textos longos e pouco claros não transmitem, na maioria das vezes, uma mensagem adequada para que o consumidor seja cientificado a respeito do fluxo dos seus dados pessoais. Ao revés, acaba por desinformá-lo, trazendo ainda maior opacidade e assimetria de informações, desconsiderando, pois, o resultado ótimo/esperado de transparência que tal canal de comunicação deveria propiciar".

[168] MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The Cost of Reading Privacy Polici *Journal of Law and Policy for Information Society*, v. 4, p. 565, 2008: "We estimate that reading privacy policies carries costs in time of approximately 201 hours a year, worth about $3,534 annually per American Internet user".

[169] Ibidem, p. 564.

[170] BAROCAS, Solon; NISSENBAUM, Helen. On notice... Op.cit., p. 4.

[171] MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The Cost... Op.cit., p. 544.

[172] Esse raciocínio já foi estabelecido, anteriormente, para tratar da proteção de dados pessoais na

fase da coleta. LIMA, Cíntia Rosa Pereira de; BIONI, Bruno Ricardo. Op.cit., p. 274-275: "D por que, propugnar que o consentimento expresso decorreria da leitura de termos e políticas de privacidade que contivesse uma cláusula com destaque é, totalmente, criticado e desafiado por esse artigo. Isto porque, utilizar-se-ia um canal de comunicação que é próprio das relações *off-line*, quando, na verdade, as relações *on-line* demandam um tipo de abordagem particularizada, tal como se evidenciar pela HCI [Human Computer Interaction] em que a interação entre o usuário e a aplicação tem, certamente, maior efetividade para divulgar qualquer tipo de informação, estabelecendo, portanto, uma *comunicação sem ruídos*".

173 Veja-se, nesse sentido, a diferenciação estabelecida entre *Privacy Invasive Technologies (PITs)* e *Privacy Enhancing Technologies (PETs)*. PARAMAGURU, Abi; VAILE, David; WATERS Nigel; GREENLEAF, Graham. Distinguishing PETs from PITs: developing technology wit privacy in mind. *UNSW Law Research Paper* n. 35, p. 1-26, May 2008. Disponível em: <http://ssrn.com/abstract=1397402>.

174 Reconhecendo-se as múltiplas conceituações, ao procurar responder o que são PETs, veja-se: Commission of the European Communities. Promoting data protection by privacy enhancing technologies (pets)', p. 3, 2007. Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0228&from=EN>.

175 Veja-se, entre outras tentativas de categorização: HEURIX, Johannes; ZIMMERMANN, Pete NEUBAUER, Thomas; FENZ Stefan. A taxonomy for privacy enhancing technologies *Computers & Security*, v. 53, p. 1-17, 2015.

176 MULLIGAN, Deirdre K; KING, Jennifer, Bridging the Gap between Privacy and Desig *University of Pennsylvania Journal of Constitutional Law*, v. 14, n. 4, p. 989, 2012. Disponível em: <http://ssrn.com/abstract=2070401>; RUBINSTEIN, Ira; GOOD, Nathan. Privacy by Desig A Counterfactual Analysis of Google and Facebook Privacy Incidents. *Berkeley Technology Law Journal* n. 28, 2013; *NYU School of Law, Public Law Research Paper* n. 12-43. p. 1342. Disponível em: <http://ssrn.com/abstract=2128146 or http://dx.doi.org/10.2139/ssrn.2128146>.

177 Esses exemplos foram citados por: COMMISSION OF THE EUROPEAN COMMUNIT Promoting... Op.cit., p. 3.

178 Diversos navegadores já dispõem da ferramenta de navegação anônima que impedem o seu rastreamento e, por consequência, dos dados pessoais dos usuários. Por exemplo, os browsers do Google Chrome e Firefox (Mozilla), respectivamente: i) <https://support.google.com/chrome/answer/95464?hl=pt-BR>; ii) <https://support.mozilla.org/pt-PT/kb/Navega%C3%A7%C3%A3o%20Privada>.

179 COMMISSION OF THE EUROPEAN COMMUNITIES. Promoting... Op.cit., p. 3.

180 KOOPS, Bert-Jaap; LEENES, Ronald E. 'Code' and the slow erosion of privacy. Michiga Telecommunications and Technology Law Review, v. 12, n. 1, p. 139, 2005. Disponível em:

<http://ssrn.com/abstract=1645532>.

[181] GÜRSES, Seda. PETs and their users: a critical review of the potentials and limitations of th privacy as confidentiality paradigm. *Identity in the Information Society*, v. 3, n. 3, p. 546, Dec. 2010.

[182] KOOPS, Bert-Jaap; LEENES, Ronald E. Op.cit., p. 187.

[183] Listando a posição adotada por cada país-membro da União Europeia, veja-se: DE LIMA Desiree; LEGGE, Adam. The European Union's approach to online behavioural advertising Protecting individuals or restricting business? *Computer Law & Security Review*, v. 30, p. 69, 2014.

[184] Diferenciando os sistemas *opt-in* e *opt-out*, veja-se: TENE, Omer; POLONETSKY, Jules. Privac in the... Op.cit., p. 68. Identificando tal tensão regulatória no contexto europeu, veja-se: SMIT Edith G.; NOORT, Guda Van; VOORVELD, Hilde A.M. Understanding online behaviour advertising: User knowledge, privacy concerns and online coping behavior in Europe. *Computers in Human Behavior*, v. 32, p. 15, 2014.

[185] A expressão é de: DE LIMA, Desiree; LEGGE, Adam. Op.cit., p. 71.

[186] Ibidem, p. 68.

[187] BORGESIUS, Frederick Zuiderveen. Segmentação... Op.cit., p. 8.

[188] Ibidem, p. 9.

[189] Veja-se, nesse sentido, o discurso da Vice-Presidente da Comissão Europeia: KROES, Neelie Speech – Online privacy: reinforcing trust and confidence. Disponível em: <http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm>.

[190] Verifica-se, por exemplo, a equívoca conceituação se o DNT barraria o rastreamento apenas de terceiros (*third party tracking*) ou também com relação à própria aplicação acessada (*first party tracking*). E, mesmo para alguns que entendem ser possível o *first party tracking*, entende-se que estaria limitado a ações para prevenção de fraudes, incidentes de segurança ou para conclusão de transações eletrônicas. Veja-se, *e.g.*, tais ressalvas conceituais feitas por: MCDONALD Aleecia; PEHA, Jon M. Track gap: policy implications of user expectations for the 'do not track internet privacy feature. In: TPRC CONFERENCE (September 25, 2011). Disponível em <http://ssrn.com/abstract=1993133>. Como exemplo do que viria a ser o conceito de não rastreamento do DNT, veja-se a proposta da EFF: ECKERSLEY, Peter. What Does the "Track in "Do Not Track" Mean? Disponível em: <https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean>.

[191] A terminologia "escolha simplificada" é correlacionada ao DNT no Relatório da: Federal Trade Commission/FTC. Protecting consumer privacy in an era of rapid change, p. I, Mar. 2012 Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-

commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

192 Por meio do cabeçalho do htpp constaria a opção do usuário em ser rastreado ou não, cabendo aos provedores de aplicação observarem tal opção externada pelo titular dos dados pessoais. Veja-se, por exemplo, a explicação dada pelo Consórcio da World Wide Web/W3C: W3C. Tracking Protection Working Group Charter. Disponível em: <http://www.w3.org/2011/tracking-protection/charter-draft.html>.

193 MCDONALD, Aleecia; PEHA, Jon M. Op.cit., p. 2.

194 MAYER, Jonathan; NARAYANAN, Arvind. Do not track: universal web tracking opt-out*IAB Internet Privacy Workshop Position Paper,* p. 2, Nov. 2010.

195 Vide nota de rodapé 189 *supra*.

196 Idem.

197 Contextualizando esse cabo de forças à chamada da FTC para que o mercado se autorregulasse e, posteriormente, às ações tomadas pela Network Advertising Initiative (NAI), veja-se: TENE Omer; POLONETSKY, Jules. To track... Op.cit., p. 24-28.

198 NARAYANAN, Arvind. MAYER, Jonathan. The trouble with ID cookies: why do not track mu means do not collect. Disponível em: <http://cyberlaw.stanford.edu/blog/2012/08/trouble-id-cookies-why-do-not-track-must-mean-do-not-collect>.

199 Esse foi o caso do Internet Explorer, mas que, recentemente, voltou atrás com relação ao DNT como sua configuração padrão. Veja-se: LARDINOIS, Frederic. Microsoft will remove "do nc track" as the default setting in its new browsers. Disponível em: <http://techcrunch.com/2015/04/03/microsoft-disables-do-not-track-as-the-default-setting-in-internet-explorer/#.wko2bl:vxwq>.

200 Veja-se, por exemplo: MCENTEGART, Jane. Proposed 'do not track' specs would kill ie10's default dnt. Disponível em: <http://www.tomshardware.com/news/Microsoft-Internet-Explorer-IE-10-Do-Not-Track-DNT-Specifications,15920.html>.

201 Por exemplo, até o momento, há uma pequena lista de corporações que honram com o DNT nc cenário americano. Disponível em: <http://donottrack.us/implementations>. Acesso de 14 de outubro de 2015.

202 Nesse mesmo sentido, já se advogou por uma interpretação similar dos dispositivos sobre proteção de dados pessoais no MCI: BIONI, Bruno R; LIMA, Cíntia Rosa Pereira. Op.cit., 270-271.

203 Veja-se, *e.g.* o citado discurso da Vice-Presidente da Comissão Europeia, Neelie Kroes, que estabelece esse mesmo paralelo entre autorregulação e regulação para o DNT – nota de rodapé 186 *supra* (sem paginação).

[204] A P3P já vem sendo desenvolvida desde a década passada, principalmente por: LESSIG Lawrence. *Code and other laws of cyberspace*: version 2.0. Nova York, Basic Books, 2006. p. 226 e ss.

[205] Para o detalhamento de todo o histórico da P3P, veja-se: <http://www.w3.org/P3P/>.

[206] Dos mais populares navegadores, somente o *Internet Explorer* adotou a P3P. Disponível em: <https://en.wikipedia.org/wiki/P3P>.

[207] REAGLE, Joseph; CRANOR, Lorrie Faith. The platform for privacy preferences: world-wide we consortium's platform for privacy preferences project, web site privacy. *Communications of the ACM*, v. 42, n. 2, p. 49, Feb. 1999.

[208] Veja-se o relatório final da W3C sobre a P3P: W3C. The Platform for Privacy Preferences 1. (P3P1.1) Specification. p. 3. Disponível em: <http://www.w3.org/TR/P3P11/>.

[209] Esse formato legível para máquina dar-se-ia na linguagem XML. Ibidem, p. 25 e ss.

[210] Atentando-se que o sucesso da P3P seria dependente de *enforcement mechanisms*: REAGLE Joseph; CRANOR, Lorrie Faith. Op.cit., p. 49. No mesmo sentido: LESSIG. Op.cit., p. 228.

[211] Para o conceito de consentimento granular, veja-se, entre outros: Article 29 Data Protection Working Party. Opinion 02/2013 on apps on smart devices, p. 15, Feb. 2013. p. 15 (nota de rodapé 34). Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>. BIONI, Bruno Ricardo e al. Contribuição... Op.cit., p. 15: "O consentimento granular estabelece, portanto, limites à microeconomia dos dados pessoais, na medida em que resguarda a opção do titular em emitir autorizações, de forma fragmentada, no tocante ao fluxo de seus dados pessoais. Por exemplo, uma aplicação pode oferecer inúmeras funcionalidades cujo funcionamento demanda, indispensavelmente, uma gama de dados pessoais para a sua operacionalização. Com a ressalva do consentimento granular, o titular poderá fazer o uso de tal aplicação, determinando, de forma correlacionada, quais dados pessoais seus serão tratados de acordo com as funcionalidades que pretende fazer uso. O titular possuiria, assim, um controle sobre seus dados pessoais em face do próprio produto e/ou serviço, na medida em que pode, de forma compartimentalizada, escolher como se dará o tratamento de suas informações pessoais".

[212] Estabelecendo o mesmo paralelo entre consentimento granular e P3P, veja-se: SCHUNTER Matthias; VAN HERREWEGHEN, Els; WAIDNER, Michael. Expressive privacy promises: ho to improve the platform for privacy preferences (P3P), p. 2. Disponível em: <http://www.w3.org/2002/p3p-ws/pp/ibm-zuerich.pdf>.

[213] Fala-se em ícones e interações com os usuários, quando uma determinada política de privacidade seria incompatível, gerando-se uma rodada de negociações. Propõe-se, no entanto, que essa rodada de negociações seja vista cum *grano salis* para que, ao final, não se volte a uma falsa escolha do *take-it* ou *leave-it*. A respeito do processo de rodada de negociações na P3P, veja-se:

REAGLE, Joseph; CRANOR, Lorrie Faith. Op.cit., p. 49. Veja-se, ainda: SPIEKERMAN Sarah; Cranor, Lorrie Faith. Engineering Privacy.*IEEE transactions on software engineering*, v. 35, n. 1, p. 79, Jan./Feb. 2009.

214 CRANOR, Lorrie. P3P is dead, long live P3P! Disponível en <http://lorrie.cranor.org/blog/2012/12/03/p3p-is-dead-long-live-p3p/>.

215 EDWARDS, Lilian. Privacy, Security and Data Protection in Smart Cities: A Critical EU La Perspective (January 5, 2016). *European Data Protection Law Review* (Lexxion), 2016. Available at SSRN: <https://ssrn.com/abstract=2711290> or <http://dx.doi.org/10.2139/ssrn.2711290>.

216 Veja-se, por exemplo, o workshop promovido pela Federal Trade Commission. *Internet of things* privacy and security in a connected world. Washington: Federal Trade Commission/FTC, 2017 Disponível em: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

217 Não é nosso objetivo destrinchar o tema da interoperabilidade, mas apenas resgatá-lo como uma janela de oportunidade para as PETs. Um detalhamento melhor do tema e da sua taxonomia pode ser encontrado no estudo adotado pela Aliança da Internet das Coisas e Inovação, lançado pela Comissão da União Europeia em: Building the hyperconnected society: IoT research and innovation value chains ecosystems and markets. Disponível em: <https://ec.europa.eu/digital-single-market/en/reports-and-studies/76003/74243>.

218 A interoperabilidade é uma das questões transversais eleitas pelo Plano Nacional de Internet das Coisas no Brasil: Relatório do Plano de Ação (Produto 8). Disponível em <https://www.bndes.gov.br/wps/portal/site/home/conhecimento/estudos/chamada-publica-internet-coisas/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil>.

219 Este subcapítulo é uma exposição do fundamento jurídico das PETs sob a perspectiva do direito obrigacional. Em outro ensaio, nós já tivemos a oportunidade de tratar da evolução dogmática do direito das obrigações e do dever informacional para a autodeterminação informacional, faltando, contudo, essa correlação com as PETs. Naquela oportunidade, focou-se mais na teoria do diálogo das fontes e em um estudo de caso, razão pela qual tais leituras podem ser complementares: BIONI, Bruno. O dever de informar... Op.cit., p. 285-309.

220 Veja-se, por todos: BEVILAQUA, Clovis*Direito das obrigações*. Rio de Janeiro: Livraria Francisco Alves, 1945. p. 14: “é a relação transitória de direito, que nos constrange a dar, fazer ou não fazer uma coisa, em regra economicamente apreciável, em proveito de alguém conosco juridicamente relacionado”.

221 TEPEDINO, Gustavo; SCHREIBER, Anderson. *Código civil comentado*: direito das obrigações - artigos 233 a 420. São Paulo: Atlas, 2008. v. IV, p. 5: “A cláusula geral da boa-fé objetiva impõe deveres anexos às convenções, como o dever de informação e o dever de colaboração, que

recaem também sobre o credor, fazendo-o a um só tempo titular de direitos e deveres frente à contraparte e mesmo a centros de interesses que não integram diretamente o vínculo obrigacional".

222 A tradicional classificação de obrigações em simples e complexas é um exemplo da mencionada concepção estática da relação jurídica obrigacional. Por tal categorização, a complexidade da obrigação era erigida, tão somente, em razão da conjunção de um dar ou fazer (elemento objetivo da obrigação), desconsiderando-se que o próprio credor poderia ser, também, sujeito passivo de obrigações junto ao devedor. Por isso, essa dicotomia é falha em razão de a complexidade do vínculo obrigacional ser uma via única para quem irá receber um dar e/ou fazer. Nesse sentido, veja-se: MENEZES CORDEIRO, António Manuel da Rocha e. *Da boa fé no direito civil*. Coimbra: Almedina, 2011. p. 586: "A complexidade intraobrigacional traduz a ideia de que o vínculo obrigacional abriga, no seu seio, não um simples dever de prestar, simétrico a uma prestação creditícia, mas antes vários elementos jurídicos dotados de autonomia bastante para, de um conteúdo unitário, fazerem de uma realidade composta".

223 MARTINS-COSTA, Judith. *A boa-fé no direito privado*: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 1999. p. 394: "Ora, como efeito da apreensão da totalidade concreta da relação obrigacional, percebe-se ser a mesma um vínculo dinâmico – porque passa a englobar, num permanente fluir, todas as vicissitudes, 'casos' e problemas que a ela possam ser reconduzidas – que se movimenta processualmente, posto criado e desenvolvido à vista de uma finalidade, desenvolvendo-se em fases distintas, a do nascimento do vínculo, do seu desenvolvimento e adimplemento".

224 EHRHARDT JÚNIOR, Marcos. Relação obrigacional como processo na construção do paradigma dos deveres gerais de conduta e suas consequências. *Revista da Faculdade de Direito da Universidade Federal do Paraná*, Curitiba, n. 47, 2008, p. 144-45: "Considerando o disposto nos parágrafos anteriores, pode-se concluir que o conceito clássico de relação obrigacional se revelou inadequado e insuficiente para tutelar todas as vicissitudes inerentes à visão solidarista da relação obrigacional, que não mais se limita ao resultado da soma de débito e crédito, devendo abandonar tal posição estática para que o vínculo obrigacional seja visto como um processo de cooperação voltado para determinado fim".

225 MENEZES CORDEIRO, António Manuel da Rocha e. *Tratado de direito civil português*. Direito das obrigações: introdução, sistemas e direito europeu, dogmática geral. Coimbra: Almedina, 2009. t. 1, v. 2, p. 467: "Em síntese, podemos dizer que, através da *bona fides*, o Direito romano aperfeiçoou o sistema geral das obrigações, de modo a permitir que o juiz, em vez de se ater a formalismos estritos, pudesse, através de certos expedientes, descer à substância das questões".

226 Art. 6º, *caput*, da LGPD.

227 Há quem avance nesse teor de cumplicidade do vínculo obrigacional, assinalando que credor e

devedor estariam ligados por um *laço de irmandade* (RIPERT, Georges. *A regra moral nas obrigações civis*. Campinas: Bookseller, 2009. p. 23): "Até que ponto o mundo jurídico se poderá organizar fora de toda a preocupação moral, sobre os dados práticos e irracionais? Quando se trata de regrar os efeitos legais das vontades e das atividades, de organizar a troca de capitais e de serviços, poder-se-á sobre um ideal bastante vago ou necessidade econômica fazer construções abstratas, e depois divertir-se a escrever equações de relações jurídicas e a transformá-las? Não é, pelo contrário, preciso ter presente que o credor e o devedor, ligados um ao outro pela relação de direito, são homens que fazem parte da mesma comunidade, que uma moral sublime chama irmãos e que não podem ter, um os direitos, outro as obrigações senão na medida em que a lei moral permite tirar de alguém proveito e serviços, ou não o impede em todo o caso de o prejudicar".

228 SILVA, Clóvis do Couto e. *A obrigação como processo*. Rio de janeiro: Editora FGV, 2006. p. 20: "Os atos praticados pelo devedor, assim como os realizados pelo credor, repercutem no mundo jurídico, nele ingressam e são dispostos e classificados segundo uma ordem, atendendo-se aos conceitos elaborados pela teoria do direito. Esses atos, evidentemente, tendem a um fim. E é precisamente a finalidade que determina a concepção da obrigação como processo".

229 SILVA, Clóvis do Couto e. Op.cit., p. 40: "Há, no contrato, o dever bilateral de proteção, que impede que uma das partes cause à outra algum dano, em razão de sua atividade. Existem, assim, deveres do credor, que não são deveres para consigo mesmo, mas sim deveres jurídicos. Muitos deles consistem em conduta determinada, em comunicar algo, em indicar alguma circunstância, em fornecer informações, cuja omissão pode causar dano ao outro figurante".

230 Veja as cinco seções do Capítulo IV do Livro III do Código Civil correspondentes a: a) erro ou ignorância; b) dolo; c) coação; d) estado de perigo; e e) lesão.

231 THEODORO JUNIOR, Humberto. *Comentários ao novo Código Civil*: dos defeitos do negócio jurídico ao final do livro III. Rio de Janeiro, 2003. t. 1, v. 3, p. 4.

232 RIZZARDO, Arnaldo. *Parte geral do Código Civil*. Rio de Janeiro: Forense, 2011. p. 437.

233 MONTEIRO, Washington de Barros. *Curso de direito civil*: parte geral. São Paulo: Saraiva, 2012 v. 1, p. 242.

234 É importante observar que a LGPD prevê algumas hipóteses de nulidade e não anulabilidade. Por isso, é necessário ter o regime de defeitos do negócio jurídico como um dos vetores para se interpretar o consentimento previsto na LGPD, mas não o único.

235 Art. 8º, § 3º, da LGPD.

236 HOUAISS, Antônio; VILLAR, Mauro de Salles. Op.cit., p. 1.082.

237 MARQUES, Cláudia Lima et al. Comentários... Op.cit., p. 249.

238 LÔBO, Paulo Luiz Netto. A informação como direito fundamental do consumidor. In: MARQUES,

Claudia Lima; MIRAGEM, Bruno (orgs.)*Direito do consumidor*: proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 603: "A adequação diz com os meios de informação utilizados e com o respectivo conteúdo. Os meios devem ser compatíveis com o produto ou o serviço determinado e com o consumidor destinatário típico. Os signos empregados (imagens, palavras, sons) devem ser claros e precisos, estimulantes do conhecimento e da compreensão. No caso de produtos, a informação deve referir à composição, aos riscos, à periculosidade".

239 LISBOA, Roberto Senise*A obrigação de informar*. São Paulo: Almedina, 2012. p. 28: "O emitente deve buscar o equilíbrio ideal entre os elementos da mensagem, transmitindo a informação em um grau de originalidade e imprevisibilidade que, ao mesmo tempo, desperte a atenção do receptor e possibilite a sua compreensão. Agindo desta maneira, o emitente da informação terá maior êxito no processo comunicativo, podendo inclusive exercer legitimamente o convencimento necessário para que o destinatário adote a conduta dele esperada. A comunicação adequada e eficiente provoca a reação no destinatário da mensagem".

240 TOMASETTI JÚNIOR, Alcides. O objetivo da transparência e o regime jurídico dos deveres riscos da informação nas declarações negociais para consumo. *Revista de Direito do Consumidor*, São Paulo: Revista dos Tribunais, n. 4, p. 52-90, 1992. p. 52-58: "O instrumento teorético denominado modelo supõe entretanto uma racionalização dos comportamentos, o que equivale a entender que exista uma certa possibilidade de previsão da realidade, mediante a apreensão crítica das constâncias de seus fenômenos e da repetição das relações estruturais correspondentes, de modo que, para além da previsão, haja também, embora ilimitadamente, possibilidade de interferência sobre a realidade mesma, com o objetivo de modificá-la".

241 BARBOSA, Fernanda Nunes*Informação*: direito e dever nas relações de consumo. São Paulo: Revista dos Tribunais, 2008. p. 35: "Assim, poderíamos dizer, com os autores argentinos e a doutrinadora brasileira, que comunicar, no sentido que para nós interessará, significa uma aproximação, ao passo que informar, uma forma de proteção".

242 MARZAGÃO, Nelcina C. de O. Tropardi. *Da informação e dos efeitos do excesso de informação no direito do consumidor.* São Paulo: USP-SP, 2005. Tese (Doutorado em Direito) Universidade de São Paulo Faculdade de Direito. p. 198: "Para responder tais questões precisamos analisar a capacidade humana de armazenar e processar informações. Para tanto, diversos autores utilizam o conceito de *bounded rationality*, que traduz a noção de racionalidade limitada e postula que os indivíduos não têm capacidade para receber, armazenar e processar grande volume de informações".

243 MACEDO JÚNIOR, Ronaldo Porto. Privacidade, mercado e informação. In: NERY JR., Nelson NERY, Rosa Maria de Andrade (orgs.). *Responsabilidade civil*: direito à informação. São Paulo: Revista dos Tribunais, 2010. v. 8, p. 27: "Estudos sobre o conceito de racionalidade

limitada (*bounded rationality*) e sobrecarga de informação (*overloaded information*), têm evidenciado que a equação: maior informação = maior capacidade de decisão consciente (e, portanto, livre) frequentemente não corresponde à realidade".

244 LÔBO, Paulo Luiz Netto. A informação... Op.cit., p. 604: "A suficiência relaciona-se com a completude e integralidade da informação. Antes do advento do direito do consumidor, era comum a omissão, a precariedade, a lacuna, quase sempre intencionais, relativamente a dados ou referências não vantajosas ao produto ou serviço. A ausência de informação sobre prazo de validade de um produto alimentício, por exemplo, gera confiança no consumidor de que possa ainda ser consumido, enquanto a informação suficiente permite-lhe escolher aquele que seja de fabricação mais recente. Situação amplamente divulgada pela imprensa mundial foi a das indústrias de tabaco que sonegaram informação, de seu domínio, acerca dos danos à saúde dos consumidores. Insuficiente é, também, a informação que reduz, de modo proposital".

245 Art. 9º, *caput*, da LGPD: "O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso".

246 Ressalta-se, no entanto, que tal rol é exemplificativo, sendo apenas uma quantidade mínima de informações para que o cidadão possa ter uma noção básica de como seus dados pessoais são tratados. Vejam-se os incisos do referido art. 9º da LGPD: "I – finalidade específica do tratamento; II – forma e duração do tratamento, observados os segredos comercial e industrial; III – identificação do controlador; IV – informações de contato do controlador; V – informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI – responsabilidades dos agentes que realizarão o tratamento; e VII – direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei".

247 Veja-se, por todos: KELLEY, Patrick Gage; BRESEE, Joanna; CRANOR, Lorrie Faith; REEDER Robert W. *A "Nutrition Label" for Privacy*. Disponível em: <https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf>.

248 Tal PET foi objeto das considerações de: ROSINA, Mônica Guine; SILVA, Alexandre Pacheco da et al. *Contribuição Grupo de Pesquisa em Inovação da Faculdade de Direito da Fundação Getulio Vargas ao anteprojeto de dados pessoais*. Disponível em: <http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/07/ef64f4d964b58ecf1a9a5040efc25464.pdf>.

249 O *lightbeam* é uma extensão da Mozila para o navegador Firefox. Disponível em: <https://addons.mozilla.org/en-us/firefox/addon/lightbeam/>.

250 Trata-se do Polisis (<https://pribot.org/>) que foi reportado pelo jornal Nexo (<https://www.nexojornal.com.br/expresso/2018/02/25/Este-site-desenha-as-pol%C3%ADticas-

de-privacidade-de-aplicativos-para-voc%C3%AA>) e pela Wired (<https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/>).

[251] Nesse sentido foram as conclusões de: HANSEN Marit et al. Assessing PET Maturity*IFIP Summer School* (Universidade de Edimburgo). Workshop, Edimburgo (19 de agosto de 2015).

[252] Veja-se, nesse sentido, que *a privacy nutritional labels* tem sido associada à P3P, a fim de que não falte a essa PET "usability": KELLEY, Patrick Gage et al. Op.cit., p. 4-7.

[253] BIONI, Bruno Ricardo. O dever... Op.cit., p. 295.

[254] Ibidem, p. 305.

[255] Art. 6º, VI, da LGPD.

[256] Art. 9º, § 1º, da LGPD.

[257] TOMASEVICIUS FILHO, Eduardo*Informação assimétrica, custos de transação, princípio da boa-fé*. São Paulo: USP-SP, 2007. Tese (Doutorado), Faculdade de Direito da Universidade d São Paulo. p. 308: "A doutrina em geral reconhece que uma das condições para que surja o dever de informar é a existência de informação assimétrica. Fabre-Magnan sustenta que o fundamento do dever de informar está na desigualdade entre as partes. Para Llobet, a obrigação de informação encontra sua razão de ser no desequilíbrio de conhecimentos entre os contratantes, que pode ter duas causas: a própria técnica da formação de contrato, ou pelas circunstâncias".

[258] BIONI, Bruno Ricardo. O dever... Op.cit., p. 305.

[259] Esse vetor está previsto na consideranda 43 da GDPR ao se fazer menção sobre "a clea imbalance between data subject and the controller". E, também, nesse sentido: Article 29 Data Protection Working Party. Guidelines on consent under Regulation 2016/679. p. 5. Disponível em: <http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030>.

[260] Article 29 Data Protection Working Party. Opinion 8/2014 on the on Recent Developments on the Internet of Things. p. 22. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>. E, também: Article 29 Data Protection Working Party. Opinion 02/2013 on apps and smart devices. Fevereiro, 2013. p. 15 (nota de rodapé 34). Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>.

[261] Art. 9º, § 3º, da LGPD. Article 29 Data Protection Working Party. Guidelines on consent... Op.cit. p. 10.

[262] Art. 6º, I, da LGPD.

[263] Article 29 Data Protection Working Party. *Guidelines on consent under Regulation 2016/679*. Disponível em: <https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publis

[264] PASQUALOTTO, Alberto.*Os efeitos obrigacionais da publicidade no Código de Defesa do*

Consumidor. São Paulo: Revista dos Tribunais, 1997. p. 43: A declaração de vontade é vista como ato de autodeterminação privada, capaz de produzir efeitos jurídicos. Esses efeitos, porém, podem ser atingidos igualmente por comportamentos concludentes segundo as concepções gerais, destituídos de consciência da declaração, mas animados por uma vontade natural. Tais comportamentos, objetivamente considerados, suscitam a proteção da confiança que para o declarante gera a sua própria declaração, correspondendo a uma vontade negocial.

265 Veja, nesse sentido, a análise comparativa feita pelo: Article 29 Data Protection Working Party. *Guidelines on consent*... Op.cit., p. 15-17.

266 Veja, nesse sentido, a consideranda 32 da GDPR: "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided".

267 Painéis de privacidade ou mesmo a configuração de navegador, como é o caso das ferramentas do DNT e P3P antes analisadas, seriam ferramentas a operacionalizar esse processo de tomada de decisão.

268 Art. 25 (2): "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".

269 Art. 6º, III e X, da LGPD, respectivamente: "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"; e "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 LIMA, Cíntia Rosa Pereira de; BIONI, Bruno Ricardo. A proteção dos dados pessoais na fase d

coleta... Op.cit., p. 270-274.

271 Essa é uma das principais conclusões do recente livro de: Woodrow Hartzog.

272 Esse é a conclusão do artigo de: CALO, Ryan. Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review*, vol. 87:3, march 2011. p. 1.027-1.072.

273 MARQUES, Claudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor*: um estudo dos negócios jurídicos do consumo no comércio eletrônico. São Paulo: Revista dos Tribunais, 2004. p. 71.

274 Veja o mapeamento feito pelo Centro de Pesquisa InternetLab do qual esse autor foi um dos coautores: ANTONIALLI, Dennys et al. *InternetLab reporta: consultas públicas nº 4*. Disponível em: <http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-consultas-publicas-no-04/>.

275 Art. 7º, § 5º, da LGPD.

276 Art. 11, I, da LGPD.

277 Art. 14, § 1º, da LGPD.

278 Art. 33, VIII, da LGPD.

279 Veja, nesse sentido, a análise comparativa feita pelo: Article 29 Data Protection Working Party. *Guidelines on consent*... Op.cit., p. 18-21.

280 Veja, nesse sentido, o relatório do substitutivo apresentado pelo Deputado Orlando Silva (PCdoB/SP). Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=SBT+1+PL406012+%3D%3E+PL+4060/2012>. p. 35.

281 Art. 8º, § 1º, da LGPD.

282 Veja, nesse sentido, a análise comparativa feita pelo: Article 29 Data Protection Working Party. *Guidelines on consent*... Op.cit., p. 19.

283 Por exemplo, a princípio, o mero compartilhamento de dados não implica o mesmo risco que a transferência internacional para um país sem um nível adequado de proteção. Parece-nos que eventual regulação por parte do órgão fiscalizador será de extrema relevância para fins de segurança jurídica e não vulgarização desse consentimento especial.

284 Art. 7º, VII, do MCI e.

285 RODOTÁ, Stefano. Sociedade de vigilância... Op.cit., p. 17.

286 Faz-se uma clara alusão ao referencial teórico de Lawrence Lessig para quem o direito e a tecnologia (arquitetura da rede) podem ser combinados, não excluindo um ao outro para a regulação da internet. LESSIG, Lawrence. *Code*... Op.cit.

287 Ibidem, p. 232.

288 Ibidem, p. 215.

[289] KOOPS, Bert-Jaap; LEENES, Ronald E. 'Code'... Op.cit., p.56: "Therefore, if PETs are to ke privacy alive, a conscious and concerted effort is needed. The market will not stimulate and use PETs by itself; it is clear that government intervention is needed if privacy enhancing "code" is really to carry weight to stem and stop the gradual erosion of privacy".

[290] Veja-se, *e.g.*, o "manifesto" dos acadêmicos: FISCHER-HÜBNER, Simone; HOOFNAGLE, Chris Jay; KRONTIRIS, Ioannis; RANNENBERG, Kai; WAIDNER, Michael; BOWDEN, Cas Online Privacy – Towards Informational Self-Determination on the Internet. In: HILDEBRANDT M.; O'HARA, K.; WAIDNER, M. (Ed.). *Digital Enlightenment Yearbook*. Amsterdam: ISO Press, 2013. p. 136.

[291] RAAB, Charles D. DE HERT, Paul. The regulation of technology: policy tools and policy actor (November 1, 2007). *TILT Law & Technology Working Paper Series*, n. 3, p. 18, 2007.

[292] Veja-se, *e.g.*, CALO, Ryan. Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review*, v. 87, n. 3, p. 1.046, Mar. 2011. "The goal of visceral privacy notice (...) should be to create awareness of data collection and other relevant issues and realities (...) In other words, the goal of notice is not to manipulate preferences but to give consumers the information they need to act (...)".

[293] BIONI, Bruno Ricardo. Op.cit. p. 306: "Deve-se reconhecer, como já exposto em todo o trabalho, a vulnerabilidade (informacional) do consumidor e, com isso, com base nas ideias de Daniel J. Solove, dispor a rede de modo tal que permita ao usuário ter acesso a todas essas funcionalidades propostas para o controle de seus dados (*arquitetura de vulnerabilidade*)".

[294] Das obras já citadas, veja-se em especial: SUNSTEIN, Cass. THALER, Richard H. *Nudge*... Op.cit.

[295] Fala-se em ambientes de escolhas amigáveis. Ibidem, p. 11.

[296] Ibidem, p. 5.

[297] Essa é uma tradução literal do termo *nudge*. Ibidem, p. 4.

[298] Sobre a arquitetura da privacidade na Internet, veja-se, por todos, o Capítulo 6 da obra de SOLOVE, Daniel J. *The digital*... Op.cit., p. 93-126.

[299] A expressão de que a autonomia precisa ser nutrida, especialmente no que tange à autodeterminação informacional é de: COHEN, Julie. Examined lives: informational privacy and subject as object. *Stanford Law Review*, n. 52, p. 1.424, 1999-2000.

Capítulo V

A REAVALIAÇÃO SUBSTANTIVA (CONTEÚDO) DO CONSENTIMENTO COMO PROTAGONISTA DA PROTEÇÃO DE DADOS PESSOAIS

5.1 EM DIREÇÃO A UMA NORMATIZAÇÃO SUBSTANTIVA E MENOS PROCEDIMENTAL DA PROTEÇÃO DOS DADOS PESSOAIS

As considerações do capítulo anterior procuraram sublinhar a dissonância entre o *paradigma* normativo da proteção dos dados pessoais – a autodeterminação informacional – e o mercado informacional, especialmente frente à arquitetura da Internet. Nele, nós assinalamos como tal discurso normativo poderia ser completado, paradoxalmente, pela própria realidade que lhe é problemática: a tecnologia por meio de uma arquitetura de empoderamento do (hiper)vulnerável.

Mesmo assim, a nossa abordagem correria o risco de ser inconclusa, pois estaríamos a apostar, única e exclusivamente, no consentimento como a panaceia normativa para a proteção dos dados pessoais. Isto porque a referida abordagem seria meramente *procedimental,* instrumentalizando, tão somente, o cidadão com o direito em autodeterminar as suas informações.

Daí por que as próximas linhas cercar-se-ão de outro relato normativo que não deixa ao reino do indivíduo[1] toda a carga da proteção dos dados pessoais. Uma *normatização substantiva* será endereçada, pela qual devem ser impostos limites ao consentimento do indivíduo para se alcançar um fluxo informacional apropriado.

Do que se trata esse relato normativo e em qual referencial teórico ele está apoiado? Já há traços dessa proposta na cultura jurídico-legal brasileira? Como se daria a sua aplicação na prática, a partir de alguns casos concretos? Como o próprio consentimento está interligado com essa proposta? Ela pode ser uma saída para os desafios decorrentes da tecnologia do *Big Data*?

Essas são as perguntas a serem investigadas, que delinearão a conclusão deste trabalho que pretende responder à seguinte pergunta: autodeterminação informacional está centrada única e exclusivamente no consentimento?

5.2 FUNDAÇÕES TEÓRICAS PARA A NORMATIZAÇÃO SUBSTANCIAL DA PROTEÇÃ DOS DADOS PESSOAIS

5.2.1 Um diálogo com Helen Nissenbaum sobre privacidade contextual: a equação contexto + integridade = normas informacionais

Há, sem dúvidas, a produção de uma literatura crítica teórica[2] e empírica[3] do consentimento como sendo a estratégia regulatória central para a proteção dos dados pessoais. Todavia, com exceção de Helen Nissenbaum[4], pouco se avançou com a proposição de soluções alternativas[5]. Por isso, escolheu-se tal referencial teórico[6] para endereçar outro relato que não seja apenas o da autodeterminação informacional, centrada única e exclusivamente no consentimento, para a proteção dos dados pessoais.

Provocada pelo "desnorteamento"[7] do fluxo informacional decorrente das novas tecnologias[8], Nissenbaum traça uma abordagem crítica dos diversos tipos de relatos e conceitos da privacidade, em especial daquele que a condensa como o direito de o indivíduo consentir para o fluxo de suas informações:

(...) [muitos] argumentam que proteger a privacidade significa estritamente limitar o acesso à informação pessoal ou assegurar o direito das pessoas em controlar as informações sobre elas mesmas. Eu discordo. O que as pessoas se preocupam não é simplesmente restringir o fluxo de informações, mas assegurar que ele flua apropriadamente (...)[9].

A professora da *Cornell University*[10] propõe que o trânsito das informações pessoais tem um valor social[11], guiado por considerações políticas e morais[12], que é o que determina ser ele (in)apropriado. A intelecção do que venha a ser (in)apropriado decorre do *contexto*[13] de cada relação subjacente na qual as informações pessoais fluem. É dessa análise heurística[14] que deve ser extraída uma linguagem – por ela denominada de linguagem informacional[15] – que sinaliza a (des)*integridade* do tráfego dos dados pessoais.

Estabelece-se, assim, a locução *privacidade como integridade contextual*[16]. Dessa conjunção (contexto + integridade) é que se arquiteta uma alternativa normativa em que a proteção dos dados pessoais não se baseia única e exclusivamente nos desígnios do próprio titular dos dados pessoais. Pelo contrário, as chamadas *normas informacionais* impõem restrições ao fluxo informacional que independem do controle (consentimento) exercido pelo indivíduo.

Nessa nova equação normativa, o consentimento não está presente *a priori*. A sua fórmula é composta da seguinte maneira: contexto + integridade = normas informacionais[17].

É o produto (normas informacionais) dos citados elementos (contexto e integridade) dessa equação que deve governar o trânsito dos dados. Invertendo-se a ordem dos fatores, mas não do seu resultado: as normas informacionais restringem o fluxo dos dados, verificando-se a sua integridade de acordo com o contexto em que eles estão inseridos.

Esse relato abstrato pode e deve ser dissecado com exemplos trazidos pela própria Nissenbaum, a fim de compreender, sobretudo, como se dá a aplicação dessa proposta normativa.

5.2.1.1 Normas informacionais: entre um fluxo interno e externo apropriado dos dados pessoais

o saldo das legítimas expectativas de privacidade

Ao partir da premissa de que o fluxo das informações pessoais cumpre um valor social e político, a referida autora considera que os indivíduos se desenvolvem de acordo com as suas esferas[18] sociais[19]. A informação que é compartilhada na relação médico-paciente, no ambiente educacional e de trabalho, na cena política e religiosa cumpre, respectivamente, um papel de inserção do seu titular em cada um desses contextos.

Por exemplo, a opinião religiosa de um cidadão pouco ou nada tem a acrescentar nas suas relações de cunho profissional. Se a sua crença religiosa influenciar as suas aspirações profissionais, esse fluxo informacional será, muito provavelmente, inapropriado. Daí por que a capacidade de se relacionar[20] é condicionada pelo *fluxo contextual* das informações pessoais, atraindo, portanto, uma importância social.

Os atores, os atributos (tipo) do dado pessoal e como ele é disseminado são os elementos eleitos por Nissenbaum para dissecar essa análise contextual[21]. Nós propomos, no entanto, uma leitura (subdivisão) progressiva desses elementos com relação ao fluxo informacional interno (atores e atributos) e externo (disseminação)[22].

O foco é, portanto, analisar como se dá a dinâmica do tráfego informacional sob a perspectiva da relação que lhe dá origem – que é a causa primária da coleta e do tratamento dos dados pessoais – e, posteriormente, como terceiros podem nele ingressar. Isso porque, de acordo com o recorte dessa pesquisa, faz mais sentido analisar como a dinâmica do fluxo dos dados pessoais no mercado informacional, que envolve rastreamento e compartilhamento com terceiros, pode ser afetada por esse novo relato normativo (vide, em especial, subcapítulo 1.2.2.4).

A partir dessa abordagem, será possível não só investigar a operação inicial da coleta e processamento de dados – momento em que se dá a troca (*trade-off)* dos dados pessoais para se acessar um produto ou serviço (fluxo interno) –, mas, também, o compartilhamento desses dados com terceiros (fluxo externo).

Fluxo interno

O primeiro elemento é o mais basilar de todos eles. Identificar quem são os *atores* envolvidos em meio ao fluxo informacional implica, por consequência lógica, investigar qual é o vínculo existente entre eles e, em última análise, qual é a *esfera social* em que eles estão inseridos. Trata-se, portanto, de um diagnóstico preciso sobre o contexto em que se instaura o fluxo informacional, o que vai balizar toda a análise da privacidade contextual.

É com base na conexão estabelecida entre emissário e recipiente da informação que se parametrizará todo o fluxo informacional, tal como o segundo elemento de análise: os atributos – i.e., quais tipos de informações devem ser transmitidos.

Como exemplos: em uma relação médico-paciente, os dados a respeito do estado de saúde do paciente; em uma relação de trabalho, as informações sobre como uma tarefa deve ser executada; em

uma igreja, a crença e os rituais dos seus fiéis; na relação de um casal, as confidências dos pares; entre pais e filhos, toda a miríade de informações necessárias para o afeto e o processo educacional que, por seu turno, também é desempenhado no ambiente escolar, mas com uma carga mais restrita em comparação à primeira relação. Em todos esses contextos, o fluxo das informações é determinante para que seus atores desempenhem seus respectivos papéis[23] em cada uma dessas esferas sociais.

A contrario sensu, ao médico é desnecessário saber as atribuições profissionais de seu paciente; ao empregador, as confidências amorosas de seu empregado; ao professor, qual é o gesto carinhoso predileto entre pais e filhos; ao padre, qual é o desempenho escolar de seus fiéis, e assim por diante. Nesses casos, o fluxo informacional seria inapropriado, na medida em que se desvirtua do contexto que lhe é subjacente.

Fluxo externo

Prosseguindo com essa dinâmica de exemplos, foca-se, desta vez, na disseminação da informação (fluxo externo). Pode-se dizer que seria inapropriado que o médico dissesse o estado de saúde de seu paciente ao empregador deste; que o padre compartilhasse os detalhes dos rituais praticados por seu fiel ao professor deste; que o professor divulgasse o desempenho escolar do seu aluno ao médico deste.

No entanto, seria adequado que o médico disseminasse informações do estado de saúde do seu paciente à sua respectiva equipe médica; que o professor alertasse os pais de um aluno sobre seu desempenho deficitário, e assim por diante.

Cada contexto tem, portanto, uma linguagem (informacional) que determina a lógica do fluxo informacional interna e externamente: internamente, *quais* são os tipos de informações a serem trocados entre emissário e recipiente; externamente, *quem* são os terceiros que podem ingressar no fluxo informacional.

Ao final, cada contexto exprime as expectativas de privacidade[24] que o titular das informações deposita, na condição de emissor, no recipiente, e de como esse fluxo informacional fluirá interna e externamente.

Por exemplo, o paciente não espera que seu médico vá trocar informações com o seu empregador (fluxo externo) e, nesse sentido, que ele deva informar seus rendimentos e atribuições profissionais para fins de atendimento médico (fluxo interno). Da mesma forma, o aluno não compartilha as suas confidências amorosas com seu professor (fluxo interno), bem como não espera que a sua advertência, por indisciplina no ano primário, seja levada em consideração por seu empregador para a sua promoção (fluxo externo).

Tais exemplos são ilustrações de como a teoria da privacidade contextual tem uma aderência cotidiana. A todo momento, os indivíduos estão transmitindo informações em múltiplos contextos[25]. E, nesse sentido, o desenvolvimento da personalidade deles está condicionado por tal trânsito

informacional, a fim de que seus *papéis sociais* sejam executados em suas respectivas esferas.

O saldo final da teoria (equação) da privacidade contextual consiste, portanto, na consideração de que em cada contexto o titular dos dados pessoais tem legítimas expectativas (de privacidade) de como eles irão fluir de forma apropriada. O tráfego dos dados pessoais não se dá, portanto, no vácuo, mas sob um conjunto de circunstâncias que determinam a sua integridade.

Os atores, os atributos da informação transmitida e para quem elas são disseminadas são fatores que só adquirem significado mediante essa análise contextual. São esses fatores contextuais que devem governar o fluxo informacional para que os sujeitos possam desempenhar apropriadamente seus respectivos papéis sociais.

5.2.1.2 O valor social da proteção dos dados pessoais e a negociabilidade limitada dos direitos d personalidade: titularidade versus *propriedade dos dados*

Propugnar que a privacidade é uma condicionante aos papéis sociais desempenhados pelos cidadãos nos reconduz a um relato de que a privacidade tem um valor social a cumprir que supera a sua perspectiva meramente individualista.

Como já citado neste trabalho, Hannah Arendt já alertava que a privacidade protege o indivíduo da pressão social. Ele pode se colocar a salvo do olhar público, sendo capaz de desenvolver uma subjetividade crítica para voltar à cena social e contribuir para um debate reflexivo das ideias. Evita-se, com isso, o nivelamento social e visões homogêneas, caso os cidadãos estivessem sob um escrutínio público constante (subcapítulo 2.4.1).

Por isso, a privacidade é encarada como um *bem comum*[26], que detém particular importância para o estado democrático de direito, por garantir uma participação deliberativa[27] e heterogênea entre os cidadãos em contraste às sociedades totalitárias[28]. A privacidade não beneficia, portanto, somente o indivíduo, mas, colateralmente, a sociedade, revelando-se como um elemento constitutivo da própria vida em sociedade[29].

O relato normativo da privacidade contextual capta essa mensagem e a verticaliza para a proteção dos dados pessoais, na medida em que se propõe a investigar quais são as implicações do fluxo informacional para as interações sociais. Esse discurso está alinhado com a proposição deste trabalho de que a proteção dos dados pessoais se insere como um novo direito da personalidade.

Os indivíduos têm cada vez mais condicionada a sua *participação social*[30] pela exponencial datificação das suas vidas, sendo estigmatizados e submetidos a uma série de decisões automatizadas e, por vezes, a práticas discriminatórias que afetam o livre desenvolvimento da sua personalidade (subcapítulo 2.3.3).

Por isso, os dados pessoais não podem ser passíveis de uma mercantilização total[31]. Eles detêm um valor social a cumprir que impõe barreiras[32] para sua negociabilidade limitada. O relato da privacidade contextual deve ser encarado como uma *vertente normativa complementar* à autodeterminação informacional para restringi-la aos espaços que não esvaziem a importância do

papel social desempenhado pela proteção dos dados pessoais.

A compreensão de que o fluxo informacional é (in)apropriado envolve, portanto, a limitação do consentimento, verificando-se qual é o impacto do trânsito das informações pessoais nas relações sociais do seu titular, em particular para o livre desenvolvimento da sua personalidade[33]. Daí por que o consentimento do titular dos dados pessoais não deve ser um recurso para legitimar os mais abusivos e invasivos tipos de tratamentos de dados pessoais, coisificando-o[34].

Essa interpretação está de acordo com a matriz normativa do CC[35] que impõe limites à autonomia privada[36], em especial, na seara dos direitos da personalidade.

O art. 11 do CC[37] teria sido, inclusive, demasiadamente intervencionista[38] ao dispor que os direitos da personalidade seriam irrenunciáveis e intransmissíveis, não podendo sofrer limitação voluntária afora os casos previstos em lei.

Uma interpretação dura de tal dispositivo acabaria por esvaziar qualquer esfera de disponibilidade sobre os direitos da personalidade[39], na medida em que tal poder de disposição deveria vir acompanhado de uma permissão legal[40]. Isso acabaria por se contrapor à realidade[41] em que diuturnamente são praticados negócios jurídicos que têm como objeto os direitos da personalidade, como a cessão de imagem e nome, a limitação à integridade física em atividades esportivas etc.[42]

Por outro lado, essa interpretação *cum grano salis* do art. 11 do CC não pode autorizar uma disponibilidade total dos direitos da personalidade, sob pena de contrariar a sua matriz paternalista que procura assegurar os interesses extrapatrimoniais em jogo para a tutela da pessoa humana[43]. Compreender o alcance de tal dispositivo ajudará a balizar os fundamentos (jurídicos) para se investigar quais são os contornos e limitações da autonomia da vontade no campo da proteção dos dados pessoais.

De início, cumpre observar que as proibições dos adjetivos "irrenunciáveis" e "intransmissíveis" dizem respeito ao poder de disposição sobre o bem jurídico em si. A pessoa não é autorizada a transmitir permanentemente[44] o seu direito à imagem ou a renunciar o seu direito ao nome. Nos negócios jurídicos praticados que envolvam tais bens da personalidade, o que está na esfera de autonomia do seu titular é o seu poder de fruição (exercício)[45], como, por exemplo, a limitação temporária do direito de imagem e ao nome para uma campanha publicitária. Em tais casos, a pessoa não renuncia ou mesmo transmite seus direitos da personalidade para outrem, mas, tão somente, limita o seu direito de uso e gozo[46].

Por isso, o debate a respeito da propriedade[47] dos dados pessoais não se aplica ao ordenamento jurídico brasileiro[48]. A negociabilidade dos direitos da personalidade cinge-se à fruição de tais bens (*lato sensu*) e, não, propriamente, à sua titularidade (*stricto sensu*), de acordo com a intelecção dos vocábulos "intransmissibilidade" e "irrenunciabilidade" contidos no art. 11 do Código Civil[49].

A *limitação voluntária* dos direitos da personalidade é admitida em uma perspectiva de *disponibilidade relativa*[50] por seu titular[51]. No entanto, o grande desafio é parametrizar qual deve ser

o sentido dessa liberdade[52], notadamente, quais são os limites impostos a tal esfera de autonomia relativa.

Do seminal caso de arremesso de anão[53], passando-se pelos contratos vitalícios de patrocínio[54], do direito sobre o próprio corpo (*body-art*)[54], da convicção religiosa em conflito com o direito à vida (testemunhas de jeová)[56], dos programas de *reality show*[57], verifica-se que há uma tensão permanente em preencher o significado da referenciada disponibilidade relativa dos direitos da personalidade e, em especial, na maioria dos casos, dos limites da *natureza negocial* do consentimento[58] dos seus titulares sobre a circulação comercial dos seus bens da personalidade.

Essa mesma tensão está presente na proteção dos dados pessoais[59]. Até que ponto o seu titular pode deles dispor por meio da sua vontade negocial?[60] Quais são os limites a serem impostos às mais variadas práticas de tratamentos dos dados pessoais, cujos parâmetros são estabelecidos pelos termos de uso das aplicações a que seus usuários aderem?

Tais reflexões trazem à tona, novamente, uma perspectiva crítica da autodeterminação informacional como algo único e exclusivamente centrado no consentimento. Tal paradigma normativo não deve ser absoluto, mas, como dito, complementado por outro relato que lhe imponha restrições. A autonomia do titular dos dados pessoais não deve ser uma armadilha[61] a esconder um território informacional que lhe seja destrutivo[62].

Zonas de autonomia[63] devem ser esculpidas, levando-se em conta parâmetros[64] que não esvaziem o valor social que a proteção dos dados pessoais tem a cumprir. Deve-se verificar em que medida o fluxo informacional é (in)apropriado para garantir o engajamento social, notadamente se ele estabelece uma excessiva interferência ao livre desenvolvimento da personalidade do titular das informações pessoais em circulação.

Por isso, a importância do relato normativo complementar da privacidade contextual que investiga em que medida o fluxo informacional (in)viabiliza que os titulares das informações pessoais cumpram seus respectivos papéis sociais e, com isso, projetem e desenvolvam a sua personalidade.

Tal análise deve ser casuística, levando-se em conta os contextos subjacentes ao fluxo informacional, a fim de verificar a sua integridade. Resta claro que limites devem ser impostos, evitando-se que haja uma fricção social[65] por meio de práticas disruptivas a esse bem comum: a privacidade informacional. Esse é o sentido que deve ser extraído da proteção dos dados pessoais como um novo direito da personalidade, cujo poder de disposição é relativo em consonância com o que prescreve o art. 11 do CC.

5.3 PERSPECTIVAS NORMATIVAS-PRÁTICAS DA LIMITAÇÃO DO CONSENTIMENTO

5.3.1 Os núcleos duros impostos em leis setoriais de proteção de dados pessoais

5.3.1.1 Sigilo e inviolabilidade das comunicações privadas na Internet (Marco Civil da Internet)

Como já dito, o MCI elegeu como um dos seus pilares regulatórios o direito à privacidade e à proteção dos dados pessoais, dedicando uma série de dispositivos para regular a matéria. Trata-se de um verdadeiro *miniestatuto-microssistema*[66] que estabelece, por vezes de maneira detalhada, regras que governam o fluxo das informações pessoais no ambiente eletrônico.

Veja-se, por exemplo, a maneira detida como foram tratados o sigilo e a inviolabilidade das comunicações privadas[67]. Seguindo a dinâmica constitucional[68], há dispositivos específicos para reafirmar tal desdobramento do direito à privacidade, o qual encontra abrigo, por excelência, no recôndito das comunicações[69].

Tal garantia é vital para que os cidadãos possam se relacionar uns com os outros, trocando confidências e expressando as suas opiniões sobre os mais variados assuntos, quer sejam fúteis ou não, sem que seus posicionamentos se voltem contra eles. Por essa razão, o sigilo das comunicações é tido como um direito fundamental, tamanha a sua importância para tal tipo de interação social[70].

Isto porque, ao assegurar que todo e qualquer tipo de interferência à confidencialidade das comunicações será excepcional – somente mediante ordem judicial[71] –, encoraja-se o engajamento social[72], em vez de sufocar e inibir o processo comunicacional. Note-se, pois, novamente, o valor social que está por trás da privacidade, sendo, nesse caso específico, a confidencialidade e o sigilo das comunicações.

Por tal razão, o MCI não admite que os usuários transacionem a seu respeito. O art. 8º, parágrafo único, I[73], estabelece que são nulas de pleno direito as cláusulas contratuais que ofendam a inviolabilidade e o sigilo das comunicações privadas. Não há, pois, uma zona de autonomia que permita ao usuário autorizar o tratamento dos seus dados pessoais de suas comunicações privadas. Tal fluxo informacional somente é apropriado se ocorrer entre os atores que encabeçam as pontas do processo comunicacional[74], vedando-se a interferência de terceiros.

Sedimenta-se[75], assim, a ilegalidade de uma série de modelos de negócios, tais como serviços de *e-mail* e aplicativos de mensagens que inspecionam o conteúdo da comunicação de seus usuários, a fim de lhes direcionar conteúdo – em especial publicidade comportamental.

O MCI impõe, portanto, um *núcleo duro* para preservar a integridade do fluxo informacional, restringindo o poder de disposição dos titulares dos dados pessoais. Prevalece, nesse caso, o valor social da inviolabilidade e do sigilo das comunicações, pelo qual os dados pessoais de tal processo comunicacional não estão dentro da esfera de autonomia dos seus titulares, limitando-se significativamente, em última análise, a autodeterminação informacional.

5.3.1.2 A proibição da guarda combinada de logs de acesso e de aplicação pelos provedores de conexão (Marco Civil da Internet)

O MCI estabeleceu o dever legal de retenção dos registros de conexão e de acesso às aplicações na Internet, de acordo, respectivamente, com os arts. 13, *caput*[76], e 15, *caput*[77]. Não se trata, portanto, de uma faculdade, mas de uma obrigação legal o armazenamento de tais dados, imposta aos provedores de conexão e aplicação, respectivamente, pelos períodos de 1 (um) ano e 6 (seis) meses.

Registro de conexão é o conjunto de informações sobre o início e o término da conexão de um determinado terminal (computador) por meio do seu número IP[78], sendo os rastros – horário e data – deixados na porta de entrada (*log-in*) e de saída (*log-out*) da Internet[79].

Por isso, os provedores de conexão poderiam ser considerados como o portal da Internet – *gateways* –, pois eles atuam nas camadas física e lógica[80] da rede para que os cabos e as fibras (óticas, de rádio ou de linhas de telefone) transmitam os pacotes de dados necessários – por meio do protocolo IP – para prover conexão aos usuários.

O registro de aplicação é o conjunto de informações referente ao início e término de acesso a uma determinada aplicação na Internet, o que é, também, extraído a partir de um número IP[81]. Trata-se, portanto, dos rastros – horário e data – de tudo aquilo que é transmitido na Internet, isto é, do seu conteúdo (camada de conteúdo)[82], como um *e-mail*, um *post* em uma rede social, o *upload* de um texto em um *blog*, o *download* de um *software* etc.

Com tais dados, obtém-se possivelmente a posição única e inequívoca de um computador conectado à Internet e, em tese, do seu usuário[83]. Essa é a razão para o regime legal de retenção dos chamados *logs* de conexão e aplicação, a fim de identificar a autoria dos atos praticados na Internet por seus usuários.

Por exemplo, se alguém utilizou um perfil *fake* em uma rede social para difamar outrem, ter-se-ia a seguinte cadeia de acontecimentos para identificar o usuário: **i)** o provedor de aplicação fornece, mediante ordem judicial, o endereço IP que postou tal conteúdo ofensivo; **ii)** com base nessas informações, torna-se possível requerer ao provedor de conexão, mediante ordem judicial, os dados cadastrais[84] do usuário e/ou a localização exata do terminal do computador que se conectou à Internet, utilizando-se o número IP previamente individualizado pelo provedor de aplicação; **iii)** assim, com a combinatória de tais dados, tornar-se-ia possível identificar o autor de tal delito contra a honra[85] e, por conseguinte, a persecução criminal e civil dos mais diversos ilícitos praticados na rede.

Afora a discussão se tal dever legal de retenção de dados é uma interferência excessiva ao direito à privacidade a atrair a sua inconstitucionalidade[86], fato é que o MCI adotou tal política legislativa. Nesse contexto, importa verificar como tal escolha foi arquitetada, levando-se em conta os limites impostos pelo MCI ao fluxo informacional dos registros de conexão e navegação dos usuários.

Em seu art. 14, *caput*[87], o MCI proíbe que os provedores de conexão armazenem *logs* de acesso à aplicação, além dos *logs* de conexão a que estão obrigados legalmente. Por parte do legislador[88], houve a preocupação de que a ausência de tal proibição implicaria sério prejuízo à privacidade dos

usuários. Isto porque os provedores de conexão poderiam rastrear toda a navegação do usuário, na medida em que eles são a porta de entrada e de saída da Internet para os usuários. Por estarem situados nas camadas física e lógica da rede, eles poderiam mapear todo o conteúdo acessado por seus consumidores, o que seria extremamente invasivo[89].

Há, assim, mais um *núcleo duro* sob o qual não há espaço para a autonomia da vontade dos titulares dos dados pessoais. Isso porque eventual negócio jurídico que procurasse autorizar tal coleta combinada de dados – *logs* de acesso e aplicação – teria por objetivo fraudar tal imperativo legal constante no MCI, atraindo a nulidade prevista no art. 166, VI, do Código Civil[90]. Dito de outra forma, o titular dos dados pessoais não tem poder de gerência para que toda a sua navegação seja rastreada, de acordo com a *ratio* do art. 14, *caput*, do MCI.

De fato, permitir que houvesse tal devassa do fluxo informacional seria inapropriado, possibilitando-se que toda a "vida digital" dos usuários fosse mapeada. Tal prática contraria a perspectiva da privacidade contextual, pela qual o fluxo das nossas informações pessoais deve respeitar os contextos das múltiplas relações sociais travadas pelo cidadão – seja no ambiente *on-line* ou *off-line*. O relato normativo da privacidade contextual passa a encontrar abrigo, portanto, na *mens legis* do MCI, limitando-se, mais uma vez, o paradigma normativo da autodeterminação informacional.

5.3.1.3 Limitação do uso de dados pessoais para fins de avaliação de crédito (Lei do Cadastro Positivo e Superior Tribunal de Justiça)

"Se pode ser verdadeiro que, sob a ótica econômica, quanto mais informações melhor é a avaliação de crédito (*more is better*), para o direito, para a proteção da privacidade, é fundamental restringir, tanto no tempo, como na qualidade e quantidade as informações que circulam pelos bancos de dados de proteção ao crédito".[91] Foi, a partir dessa linha de argumentação, que o Superior Tribunal de Justiça/STJ reconheceu a legalidade do sistema de *credit score*, estabelecendo, ao mesmo tempo, uma série de salvaguardas para a governança de tais bancos de dados.[92] Em grande parte, o precedente reafirma limitações previstas na então Lei do Cadastro Positivo, as quais foram, em sua essência, mantidas pela modificações decorrentes da Lei Complementar nº 166/2019.

Nesse sentido, é importante destacar dois tipos de previsões constantes em tal lei setorial: a) uma proibição de ordem genérica: que veda, em clara alusão ao princípio da necessidade, o uso de informações excessivas, "assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor"; b) outras três proibições mais específicas que vedam: b.1) o uso de dados sensíveis; b.2) informações de pessoas que não tenham relação de parentesco de primeiro grau ou de dependência econômica com o avaliado; e b.3) relacionadas ao exercício regular de direito pelo avaliado, especialmente aquelas previstas na própria lei do Cadastro Positivo.

Dessa forma, o legislador além de traçar uma norma ampla e geral acerca do que considera uma interferência excessiva[93] à proteção de dados pessoais frente à proteção do crédito (item "a"), optou,

ainda, por dissecá-la exemplificativamente (item "b"). Trata-se de uma arquitetura normativa que aponta, de saída, o que considera ser um fluxo informacional interno (itens b.1 e b.3) e externo (in)apropriado (item b.2), cujos contornos independem do consentimento do próprio titular da informação.

Sob o ponto de vista de um fluxo informacional interno, tal política legislativa considerou que a utilização de certos atributos de informação:

i) não guardariam pertinência para compor a análise da vida financeira de uma pessoa, com por exemplo, dados a respeito da sua saúde, etnia e condizentes a sua orientação religiosa, filosófica ou política. Ou seja, eventual correlação desse tipo seria incongruente à própria lógica de tomada de decisão de concessão crédito;

ii) desvirtuariam a própria dinâmica de acesso ao mercado de crédito, na medida em que o exercício de um conjunto de direitos como de acesso, retificação, impugnação de um banco de dados, entre outros, servem para que os indivíduos desempenhem seus respectivos papéis sociais nessa seara. Nesse sentido, tais direitos servem, por exemplo, para que o próprio titular da informação oxigene bancos de dados com informações de maior qualidade e, por conseguinte, sejam tornadas mais precisas e eficientes. Eventual cômputo dessas informações prejudicaria não apenas o cidadão, mas, também, o próprio sistema de crédito.

Sob o ponto de vista de um fluxo informacional externo, tal política legislativa considerou que informações de terceiros, via de regra, não deveriam parametrizar a análise da vida financeira de um indivíduo:

i) excepciona-se, contudo, o caso de terceiros que com ele mantenha relação de parentesco de primeiro grau ou dependência econômica, hipótese na qual a disseminação de tais informações externas, não diretamente vinculadas à pessoa avaliada, poderia agregar na análise de seu crédito. Ainda assim, há o ônus argumentativo do porquê tais exceções seriam aplicáveis por parte de quem processará tais informações excepcionadas por tal regra proibitiva.

ii) com isso, por exemplo, de nada adiantará argumentar pura e simplesmente que a informação utilizada é do genitor ou do filho do avaliado, senão for demonstrada qual é a sua pertinência com a análise de crédito realizada. Caso contrário, uma pessoa com um histórico de crédito extremamente positivo poderia ser prejudicada pelo único fato de um terceiro, com qual mantém primeiro grau de parentesco, ser um devedor contumaz.

Há, assim, mais um núcleo duro pelo qual se limita, de antemão, o fluxo informacional, desta vez tanto no seu aspecto interno quanto externo. Ao prescrever, de forma expressa, tais regras proibitivas, a Lei do Castro Positivo segue uma lógica de governança dos dados pessoais que não só independe, como, também, limita o consentimento do titular da informação.

5.3.2 Proteção de dados pessoais e discriminação: agenda em construção sobre os limites da autodeterminação informacional no cenário de decisões automatizadas

A correlação entre proteção de dados pessoais e discriminação foi captada desde muito cedo com a criação de uma categoria especial de dados pessoais: os denominados dados sensíveis. Informações sobre raça, credo, opção sexual, convicções políticas e filosóficas, filiações partidárias e sobre o estado de saúde têm o potencial de ocasionar, isoladamente ou em conjunto, práticas discriminatórias ao seu titular e, por isso, têm sido historicamente tratadas como uma categoria especial (vide subcapítulo 2.3.1).

Tal particularidade deságua, como faz a LGPD, seguindo a matriz da GDPR, em um catálogo mais fechado das hipóteses em que se autoriza o tratamento de dados sensíveis. Dentre algumas dessas previsões mais restritas, está um consentimento especial – ainda mais adjetivado – do titular dos dados pessoais, como contrapeso desse risco inerente ao tratamento de tal categoria de dados pessoais (vide subcapítulo 4.2.3.2.4).

Com o advento de técnicas de tratamento de dados pessoais preditivas – *e.g.*, *Big Data* (vide subcapítulo 1.3.2) –, essa agenda entre proteção de dados pessoais e discriminação ganhou novos compromissos. Levar em consideração que a mineração de dados pessoais pode ser capaz de antever e prever comportamentos de seus titulares para, daí, sujeitá-los a decisões automatizadas, traz à tona, novamente, e com muito mais força, o debate da discriminação.

Coletam-se, cada vez mais, informações sobre um indivíduo, a fim de compor um perfil detalhado para alimentar análises preditivas a seu respeito. Isso equivale a classificá-lo[94] e, até mesmo, segregá-lo (vide subcapítulo 3.3.3). Da análise de crédito[95], do prêmio fixado na apólice de seguro[96] ao anúncio publicitário na rede social[97], tais práticas estão se tornando corriqueiras, parametrizando as oportunidades de nossas vidas[98].

Não é o objetivo deste trabalho esgotar o tema, adentrando-se em todas as nuances e profundidades que o tema exige, mas, tão somente, invocá-lo como uma outra repercussão concreta da limitação do paradigma normativo da autodeterminação informacional.

Para tanto, pincelar-se-á um único exemplo: o tratamento preditivo de dados genéticos para fins securitários, recorrendo-se, prioritariamente, ao processo de revisão de uma recomendação do Conselho da Europa/CoE a esse respeito[99]. Além de possuir convenções sobre o tratamento automatizado de dados pessoais – Convenção de Strasbourg[100] –, sobre Direitos Humanos e Biomedicina – Convenção de Oviedo[101] –, o CoE tem convenções e recomendações específicas sobre dados genéticos.

Há, primeiro, um protocolo adicional à Convenção de Oviedo para tratar, especificamente, de dados genéticos. Nele, retoma-se a limitação de que o tratamento de dados genéticos para fins preditivos deve-se limitar unicamente à proteção da saúde e para fins de pesquisa, a fim de que os indivíduos não sejam "discriminados e estigmatizados" de acordo, respectivamente, com o art. 12 da Convenção[102] e o art. 4 (1) (2) do seu Protocolo Adicional[103].

Uma dessas possíveis estigmatizações e discriminações se daria na área dos contratos securitários. Na medida em que é a ciência atuarial e estatística que[104] – por meio de cálculos que identificam a probabilidade de um acontecimento – decide se o risco é assegurável ou não (cobertura)[105] e, em caso afirmativo, o prêmio a ser pago pelo segurado, testes genéticos teriam um grande impacto nesse arranjo contratual, segregando-se a sociedade entre aqueles com características genéticas mais ou menos propensas a desenvolver certos tipos de doenças[106]. Da recusa em contratar à fixação de prêmios fixados em patamares mais elevados, uma *seleção eugênica* poderia prosperar.

Por isso, a Recomendação (92) 3 do CoE[107] sobre testes genéticos proíbe, em seu art. 7[108], que seguradoras exijam testes genéticos como pré-condição contratual ou para modificação de contrato em vigor. Tal regra geral visa, justamente, parametrizar o fluxo informacional para que não haja discriminações nessa esfera social. Fronteiras são erguidas para que os titulares dos dados pessoais possam livremente desenvolver seus respectivos papéis sociais na condição de consumidores na área de seguros.

Não é nenhum exagero, aliás, falar em papel social, quiçá livre desenvolvimento da personalidade, em vista da irrefutável precarização dos sistemas universais de saúde que coagem os cidadãos a se socorrerem ao sistema de assistência suplementar[109] à saúde, colocando-se em xeque, até mesmo, o seu caráter subsidiário.

Há, portanto, uma tensão com relação ao tratamento de dados pessoais para fins securitários, notadamente no que diz respeito a quais tipos de informação (atributos) deveriam fluir nesse contexto (fluxo interno). *A priori*, verifica-se a tendência de considerar inapropriado o fluxo de dados genéticos nesse contexto[110].

O tratamento de dados genéticos é, apenas, uma das tensões postas à mineração de dados para fins preditivos que se chocam e reforçam possíveis práticas discriminatórias. Essa é uma agenda ainda em construção que promete ser informativa sobre quais barreiras serão impostas ao fluxo informacional e, por conseguinte, sobre o paradigma normativo da autodeterminação informacional colado à privacidade contextual.

5.3.3 Reflexões sobre casos midiáticos: unificação de políticas de privacidade, pesquisas emocionais, termos de uso "absurdos" e a "teletela orwelliana" do século XXI

Uma última maneira de abordar exemplos práticos da teoria da privacidade contextual é correlacioná-la a alguns casos de grande repercussão, os quais geraram debates assíduos sobre os limites do consentimento do titular dos dados pessoais. Não se pretende propor uma solução, mas,

tão somente, analisá-los sob a lente de tal relato normativo complementar à autodeterminação informacional para fins de reflexão.

a) **Unificação das Políticas de Privacidade do Google**: em março de 2012, a Google consolidou as 70 (setenta) políticas de privacidade das suas aplicações em um único termo de uso. Por um lado, facilitar-se-ia a compreensão dos termos de uso até então dispersos em 70 (setenta) arranjos contratuais diferentes e, por outo lado, possibilitar-se-ia uma "melhor experiência" dos usuários, na medida em que a empresa poderia cruzar os dados das suas diferentes plataformas para personalizá-los de maneira mais eficiente[111].

Tal justificativa não convenceu diversos reguladores ao redor do mundo[112], inclusive no Brasil[113]. O problema residia na agregação desproporcional das informações pessoais dos consumidores. Dada a posição dominante da empresa do Vale do Silício, os consumidores seriam monitorados constantemente[114], possibilitando-se uma reunião descomunal de suas informações pessoais provindas de diferentes contextos. A questão em jogo seria, portanto, verificar os efeitos colaterais dessa agregação de dados dos consumidores[115] e, em última análise, os limites a serem impostos ao consentimento do consumidor escorado nessa nova política de privacidade.

b) **Pesquisa emocional no Facebook**: no ano de 2014 veio a público um artigo científico[116], do qual um dos seus coautores era membro da equipe de dados científicos do Facebook, de que a referida rede social realizou uma pesquisa de cunho emocional com seus usuários. Tal pesquisa verificou que os usuários da rede social eram passíveis de ser contagiados emocionalmente pelo conteúdo de suas *timelines*. Na medida em que suas páginas eram alimentadas por notícias de cunho negativo ou positivo, os usuários refletiam tal carga emocional em seus *posts*. Eles produziam um tipo de conteúdo que espelhava os padrões exibidos e manipulados pelos pesquisadores, de cunho negativo ou positivo[117].

No próprio artigo publicado, os pesquisadores preocuparam-se em justificar a legalidade da pesquisa desenvolvida. Em uma afirmação estampada pelo editorial do periódico, vinha a ressalva de que tal pesquisa foi executada com o consentimento informado dos envolvidos, uma vez que os termos de uso do Facebook previam o uso das informações de seus usuários para propósitos científicos[118].

Dito de outra forma, tal tratamento dos dados pessoais dos 689.003 usuários envolvidos na pesquisa emocional seria lícito, já que eles o teriam autorizado ao aderir às políticas de privacidade da rede social[119]. Procurou-se, assim, conduzir a questão da proteção dos dados pessoais sob o relato normativo único da autodeterminação informacional.

c) **Termos de uso do Facebook Messenger**: no mesmo ano de 2014, o Facebook lançou o aplicativo Facebook Messenger e, ao mesmo tempo, tornou indisponível a funcionalidade de troca de mensagens privadas (*inbox*) na versão "mãe" da rede social[120]. Se os usuários pretendessem continuar trocando mensagens privadas, eles teriam que baixar um novo aplicativo que, de acordo com o criador da rede social, teria o objetivo de melhorar a experiência do seu público: o Facebook

Messenger[121]. Em vez de acessar o aplicativo "antigo" e a partir dele buscar a "aba" de tal funcionalidade, o que demandaria tempo e tornaria maçante a experiência dos usuários, eles poderiam usar tal funcionalidade diretamente, a partir desse novo aplicativo, sem tais tipos de contratempos.

No entanto, esse novo aplicativo continha a sua própria política de privacidade que redimensionava, por completo, o fluxo informacional dos seus usuários em comparação àquela do aplicativo "antigo". De acordo com os termos dessa nova política de privacidade, o novo aplicativo poderia ler e editar mensagens de texto, gravar áudio e vídeos, fazer ligações e tirar fotos, sendo que em todas essas ocasiões não haveria a necessidade de ("nova") autorização (intervenção ou confirmação) do usuário para tais práticas[122].

Poucas vezes, percebeu-se uma reação tão negativa a uma política de privacidade que foi chamada de "insidiosa"[123] e cujos termos de uso seriam um "absurdo"[124]. Por trás dessa qualificação negativa, o que está em jogo, novamente, é a validade do instrumento contratual que dá roupagem ao consentimento dos usuários-aderentes quanto ao uso de suas informações pessoais.

d) **Termos de uso da Samsung Smart TV**: no início de 2015, os holofotes estavam sob a cláusula de política de privacidade da Samsung Smart TV, que alertava seus consumidores de que suas palavras e outras informações sensíveis, captadas pelo microfone do televisor, poderiam ser armazenadas e transmitidas a terceiros[125].

Da maneira vaga como tal cláusula foi descrita, compreendia-se que os consumidores estariam sendo constantemente vigiados em suas salas, quartos e outros ambientes habitados pelo aparelho televisivo, de modo que não demorou muito para que fosse estabelecida uma analogia à *teletela orwelliana*[126]. Em meio a tal alvoroço, a empresa sul-coreana prestou um esclarecimento público[127] e, ainda, redigiu novamente tal cláusula contratual[128].

Nota-se, mais uma vez, uma tensão sobre os limites de tais arranjos contratuais e a (des)proteção dos dados pessoais, e, por conseguinte, quais devem ser as fronteiras impostas ao poder de disposição dos titulares dos dados pessoais. Nos Estados Unidos, por exemplo, a *Electronic Privacy Information Center/EPIC* moveu uma reclamação perante a *Federal Trade Commission/FTC*, sustentando que tal cláusula contratual seria deceptiva e injusta, não podendo legitimar uma vigilância intrusiva a ponto de esvaziar, por completo, a proteção dos consumidores[129].

5.3.3.1 Síntese da privacidade contextual na prática

Em todos os casos mencionados, o relato normativo da autodeterminação informacional, centrado única e exclusivamente no consentimento, *per se* não indica uma solução para tais conflitos. Isso porque o que está em jogo não é somente se houve o consentimento dos titulares dos dados pessoais, mas se o fluxo informacional que lhes é subjacente é íntegro.

No caso "a", o que se discute é se o cruzamento das informações pessoais dos consumidores não seria altamente intrusivo. Poder-se-ia fazer uma analogia de que cada plataforma representaria uma

esfera social em que os consumidores buscam diferentes funcionalidades e interesses, quiçá tipos de relacionamentos díspares. Seriam os casos, respectivamente, dos mecanismos de busca, das plataformas de *e-mail*, vídeos e rede social. Cada plataforma poderia ser considerada como um contexto diferente, questionando-se se a promiscuidade do fluxo informacional entre elas seria (in)apropriada.

De forma similar, no caso "b", a tensão está voltada a uma análise contextual do fluxo informacional. Ainda que prolixo, uma rede social tem por objetivo promover o relacionamento de seus usuários, em que o conteúdo por eles produzido e compartilhado é o que facilita tal tipo de interação social. Daí por que refletir se em tal cenário seria admitido que os usuários da rede social pudessem expandir seus papéis sociais para o âmbito da pesquisa com seres humanos.

Nos casos "c" e "d", o que está em questão é se os atributos das informações em trânsito seriam adequados, investigando-se em que medida o acesso a uma série de informações conforma-se, respectivamente, a uma plataforma que visa facilitar a comunicação privada de seus usuários e de um aparelho de entretenimento. A integridade do fluxo informacional está, diretamente, ligada com as funcionalidades por ele desempenhadas, a justificar as suas respectivas intrusões na vida dos seus usuários.

Veja-se, portanto, que o relato da privacidade contextual complementa a autodeterminação informacional. Ele mostra outros horizontes para a solução dos casos apontados que não apenas o consentimento dos usuários para governar o fluxo de seus dados pessoais. Nos casos "a" e "b", torna-se possível uma análise do fluxo informacional sob a perspectiva de que ele transcende diferentes esferas e contextos (*fluxo externo*); nos casos "c" e "d", se o conjunto dos dados pessoais está apropriado dentro da lógica interna da relação que lhe é subjacente (*fluxo interno*).

Tais análises não são, repita-se, uma proposta de solução para tais casos. Trata-se, tão somente, de provocações que procuram elucidar a importância da análise da proteção dos dados pessoais não apenas sob uma lente tradicional do paradigma normativo da autodeterminação informacional.

Nesse arranjo *ambivalente*, devem-se esgotar os elementos contextuais da relação sob análise, verificando-se, dentre outros aspectos: **i)** quais são os propósitos do tratamento dos dados pessoais, levando-se em consideração o contexto da relação subjacente ao fluxo informacional; **ii)** como terceiros podem estar inseridos no fluxo informacional e sob quais condições; **iii)** quais são as implicações do tratamento dos dados pessoais sobre seu titular: **iii.a)** no que diz respeito ao desenvolvimento da sua personalidade; **iii.b)** para que ele se relacione livremente em outras e nas diversas esferas sociais.

Deve-se reunir, pois, todo um conjunto de informações necessárias – fatores contextuais – para verificar a integridade do fluxo informacional, observando-se o valor social da privacidade informacional e a negociabilidade limitada dos direitos da personalidade.

5.4 *BIG DATA* E USOS SECUNDÁRIOS DOS DADOS PESSOAIS: DESAFIOS PARA UM OUTRO RELATO NORMATIVO COMPLEMENTAR DA PRIVACIDADE CONTEXTUAL

Verificou-se que um dos princípios cardeais à autodeterminação informacional é o princípio da especificação dos propósitos (subcapítulo 3.3.1). Caso a caso, caberia ao cidadão emitir autorizações para o uso de seus dados pessoais de acordo com um propósito especificado. Essa sinergia entre a especificação de uma finalidade e o consentimento é o que se chama de princípio da limitação dos propósitos[130] (*purpose limitation principle*)[131]: o uso dos dados pessoais deve-se limitar àquela finalidade autorizada[132], sendo que qualquer outro uso demandaria um novo consentimento[133].

O problema com essa dinâmica normativa surge com a própria delimitação do que venha a ser a especificação de uma finalidade: **a)** deveria ela ser rígida a ponto de angariar uma hipótese singular de tratamento de dados pessoais? **b)** deveria ser ela individualizada, mas não tão rígida a ponto de viabilizar um conjunto de hipóteses de tratamento voltado para uma finalidade comum? **b.1)** como nesse último caso, garantir-se-ia que a flexibilidade desse propósito não seja tão genérica, a ponto de distorcer o princípio da especificação dos propósitos?[134]

Essas nuances revelam a dificuldade da autodeterminação como o único relato normativo da proteção de dados pessoais, em especial na sua acepção genuína – a hipótese "a" mais restritiva – em que caberia ao titular seguir seus dados em todos os seus movimentos[135]. Diversas críticas são tecidas a seu respeito, o que, ao final, será acomodado por algumas leis de proteção de dados pessoais, incluindo a brasileira.

Sem exaurir a lista de argumentos, destaca-se que: **a)** construir-se-ia um regime problemático para a dinamicidade das relações sociais, na medida em que a "trava" do consentimento estaria a todo momento bloqueando o fluxo dos dados pessoais; **b)** em meio a essa "burocratização", os cidadãos seriam sobrecarregados com tal estratégia normativa, já que exigir, a todo momento, o seu consentimento, o levaria à exaustão – a chamada fadiga do consentimento –, o que encontra ressonância nas limitações cognitivas do ser humano (subcapítulo 4.1.2); **c)** a inovação seria prejudicada. Toda e qualquer atividade precisaria de um espaço não previamente definido para criação, de modo que exigir um escopo inventivo pré-definido na economia dos dados seria inviabilizá-lo[136].

Esse discurso encontrou seu ápice na tecnologia do *Big Data*, por ser uma tecnologia que permite reutilizar uma mesma base de dados para propósitos diferentes (subcapítulo 1.3.2). Ela é incompatível com a dinâmica normativa tradicional da autodeterminação informacional, ora tangenciada pelos princípios da especificação e limitação dos propósitos[137]. Como delimitar um único uso para os dados pessoais, se a própria tecnologia visa alargá-los[138], tornando-os indetermináveis *a priori*?[139]

Nessa conjuntura, uma abordagem normativa mais flexível seria necessária, o que foi endereçado

por algumas legislações ao redor do mundo por meio da criação de outras bases legais para o tratamento de dados pessoais que não só o consentimento, o que foi articulado com uma adjetivação deste mais relaxada (subcapítulo 4.2.3.2.4)[140]. Previsões legais para o tratamento adicional dos dados pessoais sem consentimento ulterior do titular – *e.g.*, interesses legítimos na antiga Diretiva da União Europeia e replicada na GDPR[141] – ou a possibilidade do chamado consentimento implícito – *e.g.*, *implicit consent* na legislação canadense[142] –, são alguns exemplos de flexibilizações da técnica normativa tradicional da autodeterminação informacional, reduzindo-se o protagonismo do titular dos dados pessoais[143]. Dito de outra forma, a carga participativa máxima do cidadão no fluxo dos seus dados é reservada para momentos bastante específicos – consentimento expresso e específico (vide subcapítulo 4.2.3.2.4).

Afora a hipótese prevista no direito comunitário europeu e brasileiro, não é objetivo deste trabalho fazer uma análise detida dessas variações normativas, mas, tão somente, considerá-las para chamar a atenção como o conteúdo da autodeterminação informacional é circular ao consentimento, mas a ele não se resume pelo menos em sua acepção máxima.

Trata-se, em última análise, de compreender qual é a dinâmica normativa como um todo de leis gerais de proteção de dados pessoais, especialmente acerca do conceito que as orientou historicamente e, em particular, é um dos fundamentos da lei brasileira: a autodeterminação informacional.

Mais especificamente, deve haver uma esfera mínima de controle por parte do titular dos dados, mesmo nos casos em que não há a aplicação da base legal do consentimento? Se sim, haveria nesses casos, ainda que possa parecer, a princípio, paradoxal, a figura de um *consentimento contextual*? Isso está presente na LGPD à luz da influência advinda do direito comunitário europeu? Ou mesmo de elementos que não encontram simetria na GDPR.

5.4.1 Aplicação da privacidade (consentimento) contextual a partir de vetores tradicionais da cultura jurídica brasileira

A teoria da privacidade contextual estrutura-se sob a premissa de que o fluxo informacional deve ser apropriado de acordo com as suas respectivas esferas sociais. Por meio dessa análise contextual, o titular dos dados pessoais detém legítimas expectativas de como eles fluirão, o que determina, então, a sua integridade. Falar em legítimas expectativas de privacidade nos reconduz em considerar quais são os desígnios do titular dos dados, mesmo que não sob uma perspectiva subjetiva de cada indivíduo, mas sob uma faceta objetiva pertinente a um padrão social[144].

Reconhece-se, por isso, que a privacidade contextual é inerentemente conservadora, na medida em que ela repele *a priori* práticas disruptivas de condutas arraigadas da sociedade[145]. Para que novos padrões emerjam, eles têm que ser "moralmente superiores"[146], submetendo-se ao escrutínio do valor social da privacidade e da negociabilidade limitada dos direitos da personalidade. Tal como proposto na análise de casos midiáticos, deve-se identificar se o fluxo informacional

promove[147] a participação social e o livre desenvolvimento da personalidade do titular dos dados pessoais.

Por isso, afora os casos em que a lei prevê expressamente restrições ao fluxo informacional, retoma-se em parte o discurso normativo da autodeterminação informacional. Na medida em que se deve considerar qual seria a legítima expectativa do titular dos dados pessoais, procura-se entender de que forma ele consentiria para o fluxo de suas informações pessoais, ainda que com base nas práticas comuns da sociedade.

Para limitar e se revelar como um relato normativo complementar à autodeterminação informacional centrada no consentimento, a privacidade contextual dela se aproxima ao propugnar que o controle dos dados pessoais deve ser visto sob as lentes das práticas sociais e não meramente individual. Ao fazê-lo, amplia-se, consequentemente, a esfera de controle dos dados pessoais, que toma lugar sob um conjunto de ações possíveis dentro de um determinado contexto.

O consentimento passa a ser contextual. Ele não é delimitado por um propósito específico e duro – em linha com o que dispõe a expressão finalidades determinadas (subcapítulo 4.2.3.2.3) –, mas direcionado a uma gama de ações passíveis de serem executadas no contexto de uma relação. Com isso, a privacidade contextual mostra-se útil, já que ela é *elástica* o suficiente para governar o uso secundário dos dados pessoais que não podem ser previamente especificados e controlados de maneira rígida.

5.4.1.1 Consentimento contextual em uma relação contínua e cativa de longa duração

A ideia do consentimento contextual em si não é nova. No âmbito do direito contratual, ela tem tido uma particular importância nos denominados contratos relacionais[148] ou cativos de longa duração[149]. Diferentemente dos contratos descontínuos[150], tais relações contratuais são marcadas por seu *prolongamento temporal* que supera uma mera troca isolada ou pontual de interesses ou promessas[151], o que inviabiliza prever todos os seus desdobramentos.

Vejam-se, por exemplo, os contratos de seguro-saúde. A relação contratual protrai-se no tempo, não sendo possível prever todo o complexo obrigacional que tende a se modificar de acordo com a evolução da medicina e as características do segurado. Assim, o rol dos serviços que engloba tal assistência suplementar variará com o passar do tempo, na medida em que serão descobertas novas técnicas. Mostra-se, assim, impossível, listar qual seria o alcance da cobertura do contrato securitário no momento da contratação, já que o vínculo obrigacional não se prende a uma "análise estática e unitemporal"[152].

Por isso, como bem explica Ronaldo Porto Macedo Júnior, nos contratos relacionais se faz impossível *presentificar* o futuro da relação contratual, isto é, determinar com precisão todo o seu programa no momento da contratação[153]. O *continuum*[154] dessa relação joga para o futuro a completude do conteúdo obrigacional e, com ele, o seu próprio adimplemento[155].

Daí por que impossível haver um consenso – "consentimento expresso"[156] – acerca de todos os

termos contratuais. Os elementos contextuais[157] da relação é que devem ser levados em consideração para a execução do programa contratual, já que seus termos são ajustados no curso da sua *performance*[158].

Há, assim, uma consequente busca por segurança[159], que é consequência lógica dessas incertezas criadas pela ausência de uma engenharia contratual completa. Simetricamente, há uma maior confiança[160] entre os parceiros contratuais e, em especial, nas relações de consumo por parte do consumidor que passa a ser cativado[161] por essa situação de maior dependência e cumplicidade.

Esses mesmos traços são notados em uma economia de dados, e até com maior intensidade, em decorrência da sua lógica circundada pela atividade de tratamento de dados pessoais.

Diversas aplicações mantêm não só uma relação contínua com seus consumidores, mas, sobretudo, de alta intensidade. E, com isso, o fluxo informacional torna-se de longa duração e exponencial. Não só o volume, mas a própria atividade de tratamento dos dados pessoais passa a ser esculpida pelo progresso de tal ação temporal.

É só pensar que tal fluxo informacional progride e evolui com a própria inovação e novas funcionalidades que são oferecidas por tais plataformas. Todos esses elementos são ajustados com o desenrolar dessas relações, havendo uma dinamicidade que inviabiliza cravar, pelo menos de forma rígida, todas as variantes desse *continuum*.

Mostra-se inviável *presentificar* todas as nuances da atividade de tratamento dos dados pessoais para que seu titular consinta especificamente. Consente-se, por isso, acerca da relação[162] que se protrairá no tempo e, com ela, as variantes de tratamento dos dados pessoais que devem estar adequadas ao contexto da relação.

Não se trata, assim, de uma análise fechada das atividades de tratamento dos dados pessoais – propósito específico –, mas de uma análise mais aberta que perquire a respeito das suas *características*[163]; se tais características estão de acordo com o contexto da relação subjacente ao fluxo informacional, para que as suas partes executem seus respetivos papéis de maneira íntegra[164]. Esse é o elemento que dá um mínimo de previsibilidade (segurança) frente a tais espaços de incertezas do fluxo informacional.

Por isso, o uso secundário dos dados não é um "cheque em branco". Por exemplo, ao se valer da tecnologia do *Big Data*, não se devem estabelecer correlações ou análises preditivas que fogem às legítimas expectativas de privacidade do titular dos dados pessoais.

Paradoxalmente, a privacidade contextual que não tem como gatilho o consentimento é a mesma que alarga seu espectro. Mesmo nas situações em que não se recorre a uma declaração de vontade do titular para usos ulteriores das suas informações, não se perde de vista lhe assegurar controle sobre o fluxo informacional.

Ausência de consentimento não equivale à ausência de controle. O cidadão também exerce domínio sobre seus dados, se estes forem tratados de acordo com as suas *legítimas expectativas*. Em poucas palavras, a rota proposta pela privacidade contextual desemboca na compreensão de que

autodeterminação informacional vai além de consentimento. Trata-se, também, de garantir *previsibilidade* ao fluxo das informações pessoais do cidadão.

5.4.1.2 Boa-fé e tutela da confiança como vetores da privacidade contextual

A expressão "legítima expectativa" traz consigo dois elementos bastante adensados na cultura jurídico-nacional[165]: o princípio da boa-fé (objetiva)[166] e da confiança, sendo o primeiro expressamente previsto na LGPD (art. 6º,*caput*). Diversos trabalhos já exploraram os temas monograficamente[167], sendo que o que se busca é apenas demonstrar como eles são possíveis veículos para a aplicação da privacidade contextual no ordenamento jurídico brasileiro, somando-se à teoria dos contratos relacionais.

Os princípios da boa-fé e da confiança estão entrelaçados e detêm uma relação de complementaridade um para com o outro[168]. É do dever de cooperação, lealdade, enfim, de uma conduta proba (boa-fé)[169], que se extraem situações de confiança que devem ser tuteladas.

Do já referido dever-direito de informação às conhecidas figuras parcelares da boa-fé[170], a confiança é como se fosse a aceitação e a internalização de uma conduta correta e adequada[171]: a crença de que os outros – parceiro (contratual) e terceiros – não se comportarão contraditoriamente ao longo da relação obrigacional e cooperarão para o seu adimplemento.

A privacidade contextual reside justamente na fidelidade depositada pelo emissor de uma informação ao(s) seu(s) recipiente(s), na legítima expectativa de que seus dados pessoais serão usados e compartilhados de acordo com o contexto de uma relação preestabelecida ou a razão pela qual foi publicizado um dado; particularmente, na esperança de que o trânsito das suas informações pessoais não minará e trairá a sua capacidade de livre desenvolvimento da personalidade e de participação social.

É exatamente essa confiança que é capaz de reduzir a complexidade[172] do fluxo informacional em substituição à abordagem tradicional da autodeterminação informacional (consentimento específico). A privacidade (consentimento) contextual é como se fosse o óleo das engrenagens de um mercado e de uma série de relações sociais movimentadas e altamente dependentes da troca intensa e dinâmica de dados.

5.4.1.3 Abuso de direito e a posição jurídica de quem se vale da privacidade contextual para legitimar uma atividade de tratamento de dados

A privacidade contextual é um relato normativo pelo qual emergem dois tipos de direitos, que são, por assim dizer, duas faces da mesma moeda. De um lado, o direito do titular de exercer controle sobre seus dados, ainda que não o consinta para tanto, desde eles sejam tratados de acordo com a sua legítima expectativa. De outro lado, o direito de quem deseja processar dados pessoais sem que haja manifestação de vontade por parte do seu titular. Com isso, cria-se uma dinâmica obrigacional pela qual não só o cidadão titulariza o direito em circular a sua informação pessoal,

mas, também, outras entidades o fazem, sem que devam necessariamente consultá-lo para tanto.

Dito de outra forma, terceiros, que não o próprio titular da informação, detêm a liberdade jurídica[173] para destravar o fluxo informacional. Para além do contrapeso específico da legítima expectativa, tal posição jurídica tende a ser ponderada pela aplicação de um instituto relativamente tradicional na cultura jurídica brasileira: o abuso de direito.[174]

A esse respeito, a cláusula geral contida no Código Civil brasileiro será de particular importância, pois delimitará quem pode cometer ato ilícito ao se valer dessa prerrogativa em circular uma informação pessoal, caso "exceda manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé e pelos bons costumes"[175].

Ao todo, se acumulam quatro elementos delineadores acerca da (anti)licitude de quem deseja se valer de tal prerrogativa – boa-fé, fins econômico e social, e bons costumes –, o que fez com que, dado justamente à indeterminação de tais conceitos, fossem chamados de uma espécie de "superlegalidade"[176]. Nesse sentido, o instituto do abuso de direito seria o portal de entrada para os "limites éticos e sociais impostos a uma atividade"[177], justamente em um momento em que se verifica uma guinada da ética[178] em meio aos debates regulatórios[179] sobre as tecnologias de informação e comunicação[180].

Para além de pura e simplesmente apontar que o instituto do abuso de direito pode ser uma ferramenta de delimitação de juridicidade da privacidade contextual no cenário brasileiro, importa verificar em que a lei geral de proteção de dados agrega teleologicamente a essa análise.

Como já apontado anteriormente, o novo marco regulatório estabelece uma dialética normativa de conciliação entre a proteção de direitos e liberdades fundamentais do titular do dado e o livre desenvolvimento econômico e tecnológico (subcapítulo 2.5). Ao fazê-lo, contudo, expressamente eleva a proteção de dados como um novo direito da personalidade[181] (subcapítulo 2.2) e que tem como fundamento a autodeterminação informacional[182].

Dessa forma, o fim econômico e social em torno da circulação de dados pessoais deve necessariamente ser recortado pelo grau de empoderamento do seu titular em visualizá-lo e controlá-lo. Quem se vale da posição jurídica em tratar dados pessoais, sem o consentimento prévio do seu respectivo titular, não pode dela *abusar* a ponto de gerar ou agravar a assimetria de informação e de poder frente a quem tem o livre desenvolvimento da sua personalidade condicionado pelo uso de suas informações pessoais. Se isso ocorre, descamba-se para a *ilegitimidade*, que é o problema de qualificação acerca do exercício de uma prerrogativa, que o instituto do abuso de direito endereça.

Todo esse substrato teórico acerca da privacidade contextual pode e deve ir além do plano teórico e dogmático, cujo enraizamento se dá em elementos tradicionais da cultura jurídica brasileira – os princípios da boa-fé e da confiança, a teoria dos contratos relacionais e cativos de longa duração e o instituto do abuso de direito. Como se notará a seguir, todo o vocabulário até aqui talhado está espelhado no regulamento europeu de proteção de dados pessoais/GDPR, na lei geral brasileira de proteção de dados/LGPD e, por fim, em alguns casos hipotéticos, onde se considera a

aplicação e interpretação da base legal do legítimo interesse.

5.4.2 Base legal do legítimo interesse: aplicação da privacidade contextual

5.4.2.1 O "denominador comum" do legítimo interesse no direito comunitário europeu: da direti à GDPR

Historicamente,[183] o legítimo interesse tem sido encarado como a mais flexível[184] das bases legais de tratamento de dados no regime do direito comunitário europeu. Ainda que sob o mesmo nível hierárquico, o legítimo interesse serviria como uma válvula de escape para que as demais bases legais não fossem "sobrecarregadas"[185].

De um lado, sob o ponto de vista de que quatro das bases legais[186] seriam aplicáveis em situações específicas, como a execução de um contrato, de uma obrigação legal e de um interesse público, bem como para a proteção de interesses vitais do titular dos dados. De outro lado, porque, em muitas situações, seria: **a)** desnecessário coletar novo consentimento para outros usos (implícitos) dentro de uma relação já preestabelecida com o titular; ou **b)** quando terceiros: **b.1)** não tivessem meios para obter tal tipo de autorização; ou **b.2)** esse tipo de interação inviabilizaria o próprio tratamento dos dados.

Como já adiantado, essa base legal ganhou ainda mais relevância diante da emergência de tecnologias e no contexto de uma economia baseada no uso intensivo de dados (subcapítulo 5.4). Tal como o consentimento no início do progresso geracional das leis de proteção de dados pessoais (subcapítulo 2.5), o legítimo interesse ganhou o *status* de uma nova "carta coringa regulatória" para abraçar uma miríade de possíveis usos dos dados.

Ao prever o legítimo interesse, a antiga diretiva europeia de proteção de dados não detalhava os critérios para a sua aplicação. Até porque se tratava de um instrumento normativo que estabelecia objetivos gerais, a serem internalizados no direito doméstico de cada um dos seus países-membros do bloco europeu. Diferentemente do Regulamento Europeu de Proteção de Dados Pessoais – GDPR que se vale de uma técnica normativa mais prescritiva e que tem eficácia imediata por todo o bloco econômico europeu, sem a necessidade de internalização dos seus países-membros[187].

Como resultado, ao longo da vigência da diretiva, notou-se, negativamente: **a)** a ausência de uma aplicação harmônica e consistente de tal base legal entre os países do bloco econômico europeu. Isso porque cada um deles estabeleceu regras e leituras distintas do legítimo interesse; e **b)** o risco de o âmbito de aplicação das outras bases legais ser esvaziado, na medida em que o legítimo interesse poderia ser visto como aquela menos restritiva que as demais.

Nessa conjuntura, o Grupo de Trabalho do Artigo 29[188] acabou por formular uma opinião sobre legítimo interesse que, ao estabelecer critérios para a sua aplicação, tinha por objetivos: **a)** trazer previsibilidade e segurança jurídica na aplicação dessa base legal em todo o bloco econômico europeu; e **b)** evitar que o legítimo interesse fosse uma "porta aberta"[189] para contornar os direitos e

princípios da diretiva, em especial as outras bases legais para o tratamento de dados.

O achado mais importante desse documento é a elaboração de um teste "multifatorial"[190] a ser considerado pelos reguladores e pelos próprios agentes da cadeia de processamento de dados (os controladores), respectivamente, ao interpretarem e se valerem dessa base legal.

O novo regulamento europeu de proteção de dados Pessoais/GDPR bebeu diretamente dessa fonte. As considerandas 47 a 50 internalizaram todo o vocabulário prescrito na referida opinião sobre legítimo interesse. Basta uma simples leitura entre esses documentos para tal diagnóstico.

Em suma, houve a necessidade de *estabilizar* a aplicação de tal conceito jurídico indeterminado. Trata-se de um denominador comum entre os titulares dos dados e os agentes reguladores e da cadeia de tratamento de dados diante da necessidade em assegurar *previsibilidade* à aplicação da base legal do legítimo interesse.

5.4.2.2 O "denominador comum" do legítimo interesse no Brasil: do anteprojeto à LGPD

Mutatis mutandis foi o que se sucedeu no Brasil. Ao longo das consultas públicas e do debate legislativo da lei geral brasileira de proteção de dados, chegou-se ao denominador comum em torno da necessidade de se prever critérios para a aplicação do legítimo interesse.

A segunda consulta pública do então anteprojeto de lei de proteção de dados foi decisiva para tanto. Na primeira versão do anteprojeto de lei, o legítimo interesse sequer constava no rol das hipóteses legais para o tratamento de dados pessoais[191], tendo havido um debate frutífero:

a) de um lado, uma série de atores, principalmente parte do setor empresarial, sustentou ser necessário transpor tal hipótese do direito comunitário europeu para a futura lei brasileira. O principal argumento seria que tal hipótese seria mais *flexível* e extremamente pertinente em um cenário de uso intensivo dos dados, já que seria contraproducente e inviável recorrer a todo o momento ao consentimento para legitimar tais tratamentos de dados;
b) de outro lado, uma série de atores, principalmente parte da academia e sociedade civil, puxou um cabo de força para que a inclusão do legítimo interesse viesse acompanhada de requisitos para a sua aplicação. O principal argumento era que a futura lei brasileira não repetisse o equívoco da diretiva, de modo que fossem asseguradas previsibilidade e segurança jurídica na interpretação desse conceito equivocado[192-193].

Ao ser enviado o PLDPD/EXE ao Congresso Nacional[194], já constava um teste de aplicação do interesse legítimo. Ainda que parte do texto tenha sido modificada, a sua redação não perdeu a essência em balancear os interesses do titular dos dados e dos agentes de tratamento de dados pessoais. Esse teste, por nós chamado anteriormente de teste de proporcionalidade[195], foi o que prevaleceu na LGPD, à semelhança do que consta na GDPR.

5.4.2.3 Teste de proporcionalidade do legítimo interesse: balanceando direitos na LGPD em quatro etapas

Com base na opinião do Grupo de Trabalho do artigo 29[196], popularizou-se um teste composto de quatro fases para a aplicação do legítimo interesse para o tratamento de dados: *legitimate interests assessment* (LIA)[197].

O fio condutor de toda essa avaliação é "balancear"[198] os direitos em jogo. De um lado, do titular dos dados e, de outro lado, de quem faz uso das suas informações. Tão importante quanto aferir se há um *interesse legítimo* é verificar se as *legítimas expectativas* e os direitos e liberdades fundamentais do cidadão serão respeitados.

Ou seja, parte dos dois principais componentes dessa difícil equação são conceitos jurídicos indeterminados (legítimo interesse e legítima expectativa), o que a torna ainda mais complexa. Daí por que a importância em sistematizar um teste, que oriente a sua solução, a seguir:

a) Verificação da legitimidade do interesse: situação concreta e finalidade legítima (art. 10, *caput* e I, da LGPD)

O primeiro passo é verificar se **a.1)** o interesse do controlador é contornado por uma **finalidade legítima**, isto é, senão contraria, por exemplo, outros comandos legais (leis esparsas e legislação infralegal)[199]. Note-se, entretanto, que essa é somente a primeira parte da aferição da legitimidade do interesse do agente de tratamento de dados, a qual será intensificada principalmente na terceira fase quando se verificará a compatibilidade do uso dos dados frente à legítima expectativa do titular.

Nesse pontapé dessa primeira fase de análise, o que importa é observar se está presente algum benefício ou vantagem com o uso dos dados por parte do controlador e não do titular dos dados – **apoio e promoção das atividades do controlador**. A partir disso, verificar se tal interesse está claramente **a.2)** articulado[200], para que não seja um cheque em branco[201]. Deve-se perquirir se há uma "**situação em concreto**" que lhe dê suporte. Quanto mais bem definida e articulada tal situação, mais fácil será analisar o legítimo interesse diante dos próximos três passos, diminuindo os riscos de ser considerado como algo meramente especulativo[202].

b) Necessidade: minimização e outras bases legais (art. 10, § 1º, da LGPD)

Uma vez bem articulado e identificado o interesse do controlador ou do terceiro, é necessário verificar se: **b.1)** os dados coletados são realmente aqueles **necessários** (**minimização**) para se atingir a finalidade pretendida. A reflexão a ser feita é se seria possível atingir o mesmo resultado por meio de uma quantidade menor de dados, sendo, em última análise, menos intrusivo[203] e impactando menos o indivíduo; e **b.2)** se o tratamento dos dados não seria coberto por **outras bases legais**, que não a do interesse legítimo. Uma das questões mais difíceis será analisar quando a base legal do consentimento seria mais adequada que a do legítimo interesse, e vice-versa.

c) Balanceamento: impactos sobre o titular dos dados e legítimas expectativas (art. 10, II, da LGPD)

Essa é a principal fase do teste de proporcionalidade na qual efetivamente sopesam-se os interesses do controlador e de terceiros diante dos do titular dos dados. Deve-se perquirir: **c.1)** se o novo uso atribuído ao dado está dentro das **legítimas expectativas** do titular dos dados. Isso é parametrizado pela noção de *compatibilidade*[204-205] entre o uso adicional e aquele que originou a coleta dos dados pessoais[206]. Eles devem ser próximos[207] um do outro[208], demandando-se uma análise *contextual* para verificar se esse uso secundário seria esperado pelo titular dos dados.[209] Aliás, não foi por outra razão a escolha do termo "legítimo", o qual qualifica não só a base legal em questão, como, também, o princípio da finalidade; e **c.2)** de que forma os titulares dos dados serão impactados, especialmente repercussões negativas em termos de discriminação e sobre a sua autonomia (**liberdades e direitos fundamentais**)[210]. Caso, mas não necessariamente, o tratamento de dados também os "beneficie", a balança tende a estar equilibrada.

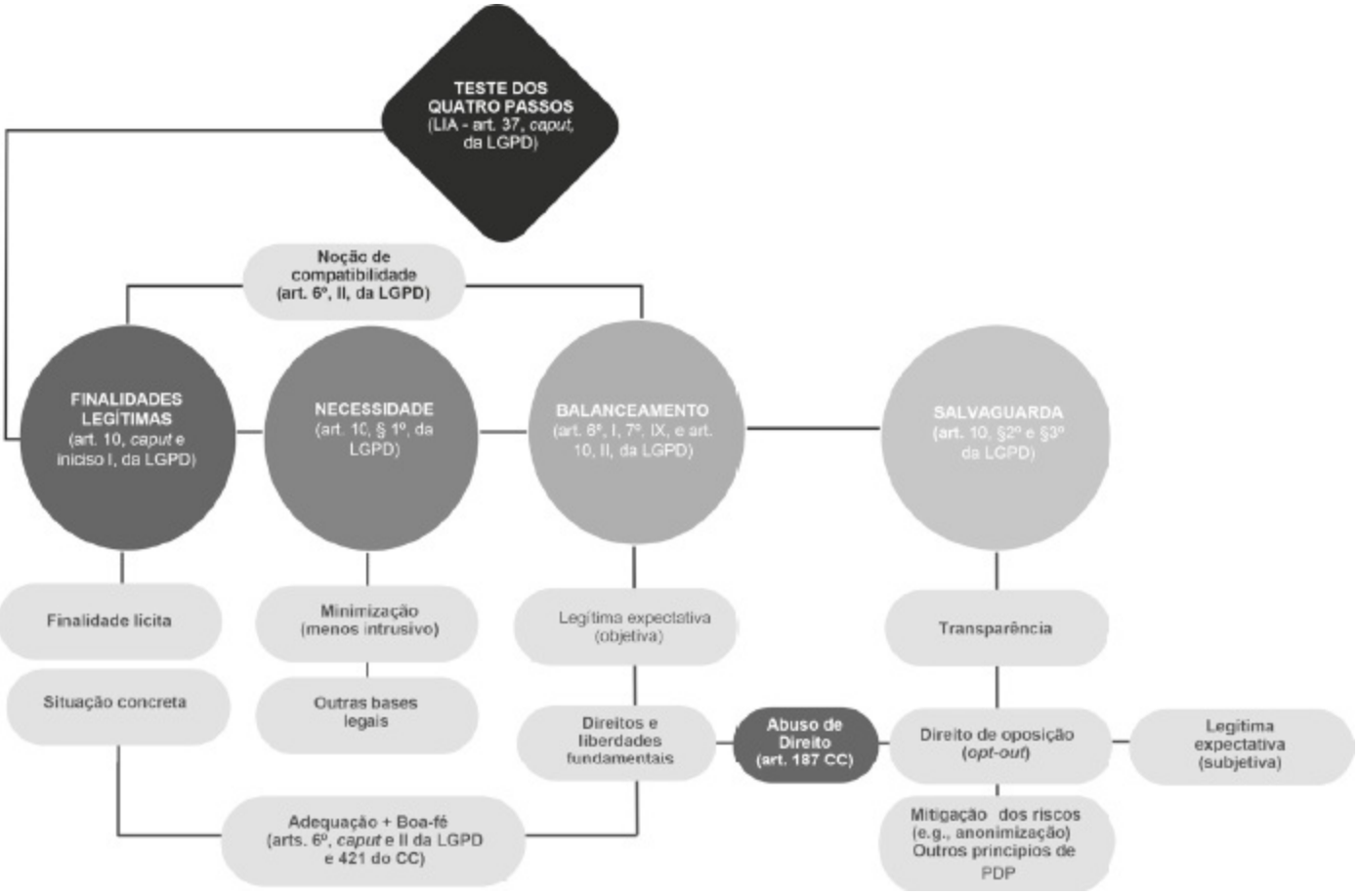
Em síntese, do início ao fim, essa fase do teste é calibrada pelo vocabulário da teoria da privacidade contextual, devendo-se analisar as legítimas expectativas em jogo e, principalmente, se o fluxo informacional é apropriado-íntegro para o livre desenvolvimento da personalidade do titular.

Nesse sentido, uma das questões mais tormentosas será a aplicação do legítimo interesse de terceiros, isto é, de alguém que não mantém uma relação já preestabelecida com o titular dos dados. Nesses casos, a noção de legítima expectativa mostra-se mais difícil de ser demonstrada e o risco da aplicação dessa base legal é ainda maior, como veremos nos casos a seguir.

d) Salvaguardas: transparência e minimização dos riscos ao titular do dado (art. 10, §§ 2º e 3º, da LGPD)

Não é porque o legítimo interesse prescinde do consentimento do titular que a atividade de tratamento de dados deve ser opaca. Pelo contrário, reforça-se **d.1)** o dever de **transparência**. Objetiva-se, com isso, franquear ao cidadão **d.2)** poder de tomada de decisão para se opor a tal atividade de tratamento de dados (*opt-out*), podendo optar por estar fora do que considera ser incompatível com as suas legítimas expectativas. E, por fim. Isso porque a legítima expectativa é também dele titular e é nesse momento que pode levantar a sua voz para controlar seus dados *a posteriori*, **d.3)** o controlador deve adotar **ações que mitiguem os riscos** do titular dos dados (*v.g.*, anonimização dos dados), sendo este o sentido da previsão da eventual necessidade elaboração de relatório de impacto à privacidade na LGPD.

Em termos de sumarização, o teste de proporcionalidade, dividido em quatro estágios, para a aplicação e interpretação do legítimo interesse teria a seguinte ilustração[211]:



5.4.2.4 Casos

A aplicação do referido teste de proporcionalidade do legítimo interesse pode ser ilustrada por meio de alguns casos[212], de modo a tangibilizar a sua dinâmica normativa:

a) Monitoramento de ambientes de trabalho

Não é de hoje a existência de uma série de tecnologias de monitoramento e coleta de dados para medir ou modular a produtividade do empregado. Até como decorrência da sua subordinação, que é um dos pressupostos da relação de emprego, ao empregador.

i) Legitimidade: o monitoramento do ambiente de trabalho é uma das formas do empregador exercer o seu poder diretivo sobre seus colaboradores, consistindo em uma finalidade legítima que decorre das próprias normas da legislação trabalhista. E, nesse sentido, há o legítimo interesse da sua parte em processar tais dados para melhorar a performance dos seus empregados.

ii) Necessidade: nesses casos de relação de trabalho em que há total assimetria entre empregado e empregador, o consentimento do titular dos dados tende a não ser livre. Por isso, no contexto europeu, a base legal do legítimo interesse tem sido a mais utilizada diante do alto risco de o consentimento obtido ser inválido[213]. As maiores controvérsias dizem respeito ao quão intrusivas e necessárias são tais técnicas de monitoramento do ambiente de trabalho. Por exemplo: **ii.a) monitoramento do tráfego da rede corporativa:** em vez de analisar todo o tráfego de navegação dos empregados, uma medida tão ou mais efetiva não seria a adoção de filtros de determinados *websites* que prejudicariam a produtividade do trabalhador?[214]; **ii.b) key-logger e screenshots**: a adoção de *softwares* que registram tudo o que é digitado pelo empregado, bem como fotografam, em

um certo intervalo de tempo, as páginas visitadas não seria uma medida desnecessária para garantir a produtividade dos empregados?

As duas situações acima conduzem à reflexão se é possível a adoção de uma arquitetura pela qual o empregador possa atingir o seu legítimo interesse de zelar pela produtividade do ambiente de trabalho, mas sem que isso implique em práticas extremamente intrusivas.

iii) Balanceamento: no ambiente de trabalho, é esperado que o empregador exerça algum tipo de monitoramento das atividades dos seus empregados. Está dentro das legítimas expectativas destes que haja eventual coleta de seus dados para verificar a sua produtividade e desempenho. Isso não significa, no entanto, que tal vigilância possa ser massiva, a ponto de desequilibrar totalmente a balança, como é reflexão contida nos itens "ii.a" e "ii.b".

iv) Salvaguardas: uma das questões centrais é informar ao empregado a que tipo de monitoramento está sujeito. Esse informe deve ocorrer antes do início da coleta dos dados, de modo a possibilitar eventuais questionamentos que podem ser feitos perante o próprio empregador ou por meio das entidades sindicais. Outra questão é verificar quais são as possíveis providências para minimizar os riscos ao titular dos dados. Por exemplo, se o empregador está em dúvidas se irá ou não filtrar determinados *websites*, decidindo, por isso, verificar com que frequência seus funcionários acessam redes sociais e outras aplicações para fins pessoais. Essa análise precisaria ser individualizada com relação a cada um dos empregados, ou se poderia fazer uma análise geral do tráfego de rede?

b) Operações societárias e processos de troca de informações (*due dilligence*)

Via de regra, em operações societárias há um processo de troca de informações (*due dilligence*) como parte do processo de fusão, aquisição e cisão coorporativa. Da análise financeira, fiscal, contábil ao do quadro de funcionários e da base de consumidores da organização, em muitos casos é necessário o processamento de dados pessoais.

i) Legitimidade: esse é um dos casos em que terceiros, que não mantêm uma relação já preestabelecida com o titular dos dados, têm o legítimo interesse em processar as suas informações. A finalidade se legitima porque toda a operação societária deve ser necessariamente lastreada pela troca dessas informações, sem a qual se faz impossível concretizá-la. Além disso, é uma situação concreta em que se faz um uso bastante pontual dos dados para o apoio das atividades do controlador.

ii) Necessidade: não é simples aferir qual é o volume necessário de dados para informar tal processo, sobretudo no que diz respeito aos dados pessoais de consumidores, fornecedores e funcionários de uma organização. Profissionais do campo societário e de privacidade e proteção de dados pessoais terão o desafio de encontrar soluções que minimizem a coleta de tais dados, mas sem prejudicar a formação de um inventário útil para o processo de *due dilligence*. Ao mesmo tempo, esse tipo de exercício pode gerar eficiência no processo, já que dados, que gerariam algum tipo de "ruído", seriam descartados.

iii) Balanceamento: a princípio, essa atividade de tratamento de dados não gera qualquer tipo de repercussão negativa para o titular. Ao final do processo, o que se busca é concluir como se dará a reorganização societária de empresas, o que em si não impacta as liberdades e os direitos fundamentais de consumidores e funcionários da corporação. Além disso, está dentro das legítimas expectativas do titular dos dados que tais reestruturações societárias ocorram.

Algo a ser considerado, no entanto, é se tal reorganização implicará agregação e concentração de mais dados sobre um indivíduo. Em casos de fusão e aquisição, por exemplo, o titular do dado mantinha relações distintas com tais organizações e em contextos diferentes para produtos ou serviços igualmente díspares. Eventual cruzamento dessas bases de dados pode impactar negativamente as suas liberdades e direitos fundamentais, a depender do quão intrusivo seja tal combinação de dados e do próprio modelo de negócio em si.

iv) Salvaguardas: o processo de troca de informações (*due dilligence*) se faz regularmente por meio de ambientes controlados, até para que não haja o armazenamento e o uso de informações estratégicas de uma das organizações pela outra. Para além de obrigações contratuais, há muitas vezes a adoção de uma arquitetura tecnológica que minimiza a exposição dos dados da organização, bem como dos seus consumidores e funcionários. Além disso, é recomendável que tais relatórios finais tragam análises estatísticas (dados agregados e não individualizados), o que, igualmente, pode ser encarado como uma salvaguarda.

c) Fraudes e incidentes de segurança[215]

Algo bastante comum é a criação de perfis comportamentais dos consumidores para combater fraudes e incidentes de segurança, pelos quais se diagnosticam atividades que fogem do padrão para tratá-las como suspeitas. É por esse motivo que serviços de e-mail, rede social e instituições financeiras alertam seus clientes e, em muitos casos, bloqueiam automaticamente acessos e transações financeiras. Por exemplo, se o acesso a uma conta parte de um dispositivo diferente, se a compra supera valores e é realizada em locais que não aqueles usuais. Todos esses dados informam ações de combate a fraudes e incidentes de segurança.

i) Legitimidade: há pouca discussão acerca da legitimidade do interesse em se combater fraudes e incidentes de segurança. Trata-se de uma questão reputacional e econômica por parte da organização, sendo inquestionável como o controlador é beneficiado por tal tipo de tratamento dos dados e é um apoio às suas atividades. Ao mesmo tempo, contudo, deve-se ter em mente qual é o tipo de fraude que se pretende combater, o que variará de acordo com cada modelo de negócio. Essa justificativa não pode se tornar um cheque em branco.

ii) Necessidade: o mais difícil é precisar a quantidade de dados para traçar tais perfis e, com isso, ser mais assertivo em ações suspeitas. Está longe de ser simples a conciliação entre o princípio da minimização e a perspectiva de maximização de dados para a formação de perfis mais precisos e, a princípio, mais refinados para o diagnóstico do que estaria fora do padrão do cliente. Por isso, é muito importante estar claro qual é o tipo de fraude e incidente de segurança que se pretende

combater.

iii) Balanceamento: a oferta de serviços e produtos mais seguros não beneficia apenas o controlador, mas, também, o titular do dado. É algo que reforça a proteção das suas liberdades e direitos fundamentais e está dentro das suas legítimas expectativas. Nesses casos, em que há, também, um benefício por parte do titular do dado, a balança tende a estar equilibrada.

No entanto, esse também seria um caso em que poderia não existir um benefício para outros titulares dos dados. Caso este seja um fraudador, o tratamento dos seus dados pode implicar no cerceamento dos seus direitos e liberdades fundamentais. Nessa situação, percebe-se que nem sempre haverá um real beneficiamento em prol do titular ao se aplicar o legítimo interesse de terceiro, mas porque, especificamente, há um benefício até mesmo difuso e coletivo de outros indivíduos.

iii.a) CERTs:[216] uma outra hipótese relacionada ao uso de dados para fins de combate a incidentes de segurança está relacionada à atuação dos Centros de Respostas a Incidentes de Segurança – CERTs[217]. Por funcionar como um ponto central para notificações de incidentes de segurança, não raramente são transmitidas e compartilhadas informações sobre ataques à rede que contêm dados pessoais. Nesses casos, haveria o legítimo interesse desses terceiros na troca de tais informações, cujo objetivo é fortalecer a segurança da rede e, em última análise, os direitos e liberdades de toda a sua coletividade de usuários. Por beneficiar os próprios titulares dos dados, esse seria mais um dos casos em que a balança tende a estar equilibrada e há um legítimo interesse de terceiro.

iv) Salvaguardas: possíveis ações para mitigação de riscos seriam: **a)** a pseudoanonimização de tais bases de dados, de modo que não houvesse a identificação direta da pessoa. Por exemplo, a substituição do seu nome, entre outros dados, por signos alfanuméricos; **b)** o agrupamento dos consumidores-usuários com padrões semelhantes, de modo que tal perfilhamento não fosse individualizado; **c)** no caso de CERTs, a "sanitização" das informações reportadas com o repasse dos dados estritamente necessários para que o "atacado" ou o próprio CERT possam reagir ao ataque. Isso pode variar da pseudoanonimização de "logs" à eliminação de dados como CPF, senha, entre outros, de uma base de dados comprometida.

Com uma dinâmica muito próxima à segunda fase do teste de proporcionalidade, trata-se de checar até que ponto é possível conciliar a abstração e a utilidade dessas informações para uma engenharia de combate a fraudes e incidentes de segurança.

d) *Background-check*: reunião de informações sobre o candidato em processos seletivos

É cada vez mais comum a reunião de informações (*background-check*) sobre o histórico de um candidato em um processo seletivo, como uma forma de checar as competências declaradas em seu currículo e a adequação de seu perfil para a vaga.

i) Legitimidade: ao proceder com tal investigação, o empregador (ou terceiro contratado) tem um interesse legítimo em acumular mais elementos para auxiliar e respaldar o seu processo de decisão.

A vantagem em questão é atribuir mais eficiência e precisão ao processo seletivo, sendo, portanto, um apoio às suas atividades.

ii) Necessidade: **ii.a)** ainda que o consentimento seja uma das possíveis bases legais para esse tipo de tratamento de dados, este pode ser considerado inválido dada a assimetria da relação em questão. Um raciocínio muito próximo ao que foi descrito no item "a", razão pela qual o legítimo interesse também se apresentaria como uma das possíveis bases legais; **ii.b)** uma vez eleita a base legal, a questão mais controvérsia diz respeito a quais são os dados necessários para avaliar o candidato. Especialmente o que poderia ser enquadrado como uma informação útil para compor o quadro analítico das habilidades e técnicas do candidato ao exigido pela vaga. Por exemplo, mesmo que o Tribunal Superior do Trabalho – TST tenha se posicionado sobre a excepcionalidade da utilização de antecedentes criminais, acabou por trazer um rol bastante amplo de situações nas quais seria justificável o uso de tais informações[218]. Com a LGPD, é muito provável que tais questões voltem à tona, oxigenadas pela aplicação desse teste de proporcionalidade.

iii) Balanceamento: **iii.a)** no contexto de um processo seletivo, é esperado que haja algum tipo de confirmação ou investigação das informações, habilidades e técnicas declaradas pelo candidato. Ou seja, está dentro das suas legítimas expectativas que haja tal tipo de tratamento de dados; **iii.b)** o ponto ótimo do balanceamento em questão parece ser a prevenção de práticas discriminatórias injustificadas, como o TST alerta sobre o uso de antecedentes criminais. Além de ser um dos direitos sociais, o trabalho é também um dos princípios fundamentais do texto constitucional brasileiro, de modo que esse tipo de tratamento de dados pessoais deve ser cauteloso para não impor barreiras infundadas ao mercado de trabalho. Uma reflexão, nesse sentido, seria a utilidade do histórico de crédito e até patrimonial de um candidato como um dos elementos considerados para tal processo de tomada de decisão[219]. Nesse aspecto, os itens "ii" e "iii" do teste de proporcionalidade são complementares um ao outro, havendo uma intersecção entre eles.

iv) Salvaguardas: uma das questões centrais é informar o candidato sobre tal prática na primeira oportunidade durante o processo seletivo, de modo que tal atividade de tratamento de dados seja transparente.

e) Outros exemplos mais prescritivos

Por fim, é válido ainda aprofundar o teste de proporcionalidade de aplicação do legítimo interesse com base em exemplos mais prescritivos. Esse tipo de dinâmica torna ainda mais tangível perceber como o referencial teórico da privacidade contextual oxigena a aplicação dessa base legal em específico para o tratamento de dados:

e.1) sendo o consumidor paciente de um profissional liberal da saúde, ele não espera que seu histórico de saúde seja transmitido a terceiros para fins de publicidade direcionada, tal como para uma agência de turismo que fornece pacotes turísticos para pessoas com estado de saúde debilitado[220]. Pense-se, ainda, na transmissão de tais dados para empresas farmacêuticas que poderiam personalizar a sua abordagem publicitária. O ingresso desses terceiros no fluxo (externo)

informacional foge completamente ao *contexto da relação* entre médico e paciente, violando-se as *legítimas expectativas* do titular dos dados pessoais.

e.2) uma rede de supermercado cria seu programa de fidelidade, informando que os consumidores, que adquirirem seu cartão fidelidade, terão acesso a uma série de benefícios. Além do tradicional sistema de pontuação, o histórico de compras será utilizado para fins de publicidade direcionada. Com o avanço tecnológico, tornam-se possíveis os seguintes tipos de abordagem:

e.2.1) ofertas por meio de um algoritmo que correlaciona a flutuação do estoque com os hábitos de seus consumidores a fim de alertá-los sobre as chamadas "queimas de estoque"[221];

e.2.2) um algoritmo que permite estabelecer análises preditivas de seus consumidores, em especial daquelas consumidoras que estão grávidas para lhes direcionarem produtos e ofertas para cada fase da gestação[222];

e.2.3) o supermercado acaba por aderir a uma política pública governamental para melhorar os hábitos alimentares da população[223], compartilhando a sua base de dados com uma determinada entidade governamental. Ela reutiliza tal base de dados para fins de análise preditiva daqueles cidadãos com maior propensão de desenvolver doenças por maus hábitos alimentares. Uma vez feita tal classificação, contata-os para lhes oferecer um acompanhamento nutricional gratuito pela rede pública de saúde, bem como alertá-los de que terão o desconto de 5% na compra dos alimentos da lista "bem-estar é viver" que será subsidiado pelo próprio governo por meio da redução da carga tributária de tais produtos.

A hipótese "e.2.1" está dentro das legítimas expectativas, sendo, inclusive, uma prática arraigada na sociedade, mas que agora se torna possível de ser personalizada para um grupo restrito de consumidores ou mesmo de forma individual, ao passo que as hipóteses "c.2.2" e "c.2.3" são práticas desleais, pois consumidores não *esperam* que seja obtida uma informação sensível, própria do contexto familiar (gravidez), muito menos no que diz respeito à propensão de doenças por hábitos alimentares, sendo que, nesse último caso, um terceiro totalmente estranho ao *contexto da relação* ingressará de forma *inapropriada no fluxo informacional*;

e.2.4) uma grande montadora do mercado automobilístico verifica um grave vício de fabricação dos seus veículos. Por obrigação legal, ela deve contatar os consumidores para sanar tais vícios. No entanto, ela não comercializa tais bens de consumo, de modo que ela deve ter acesso aos dados pessoais dos consumidores por meio das agências de veículos para haver um *recall* efetivo. Nos contratos de compra e venda de veículos não há a previsão do compartilhamento de dados pessoais dos consumidores para tal finalidade, de modo que isso consiste em um *uso secundário*[224]. *Nessa hipótese, o fluxo informacional é apropriado*, estando dentro das *legítimas expectativas* do consumidor de que seus dados pessoais sejam compartilhados para fins de prevenção de um acidente de consumo.

5.4.2.4.1 Questões controvertidas sobre a aplicação do legítimo interesse

5.4.2.4.1.1 É obrigatório documentar o teste do legítimo interesse (LIA) na LGPD?

No âmbito da GDPR, ainda há discussão se os agentes de tratamento de dados deverian documentar o teste de ponderação do legítimo interesse sempre que as suas atividades de tratamento de dados estivessem apoiadas em tal base legal. Isto porque a própria estrutura do LIA não está esquematizada no "texto duro" da lei[225], mas, tão somente, nas diretrizes para a sua interpretação. E, além disso, o regulamento europeu apenas reforçou o dever de informação junto aos titulares dos dados (artigos 13 e 14 da GDPR), mas não o dever de documentação acerca das atividades de tratamento de dados, lastreadas no legítimo interesse.

No entanto, doutrinariamente[226] e uma parcela dos órgãos reguladores já têm se posicionado acerca da obrigatoriedade do LIA. A partir do princípio da *accountability*, argumenta-se que os controladores de dados deveriam demonstrar a sua responsabilidade em balancear seus interesses frente aos dos titulares através dessa documentação em específico.

No âmbito da LGPD, o desenho normativo é substancialmente distinto:

a) Primeiro, porque as fases do LIA estão talhadas no próprio texto duro da lei, estando distribuídas ao longo dos incisos e parágrafos do artigo 10º. Ou seja, não se trata de uma diretriz interpretativa, mas, efetivamente, do próprio conteúdo normativo em torno da licitude de tal base legal;
b) Segundo, porque não apenas o dever de informação é reforçado como corolário do princípio da transparência[227], mas, também e principalmente, o dever de registro das atividades de tratamento de dados[228]. Com isso, a racionalidade da LGPD aponta para uma documentação especial, que nos parece ser justamente o LIA.

Com isso, a peculiaridade do desenho normativo acima descrito da LGPD, somado ao princípio da *accountability*, deságua necessariamente na obrigação de execução e de documentação do LIA. Uma interpretação sistemática dos arts. 6º, X, 10 e 37[229] da lei condiciona o uso responsável da base legal do legítimo interesse ao referido teste, sob pena dos agentes de tratamento de dados não demonstrarem a adoção de medidas eficazes para tanto.

Por essa razão, em comparação à GDPR, a LGPD possivelmente desengatilhará senão uma aplicação mais restritiva em torno do legítimo interesse, ao menos em um cenário no qual se demanda um maior esforço argumentativo por parte dos agentes de tratamento de dados. Em poucas palavras, sob o ponto de vista teórico-normativo, o uso de tal base legal carrega consigo uma série de obrigações. O "bônus" do legítimo interesse deve estar sincronizado com o "ônus" decorrente da aplicação e documentação do referido teste de avaliação.

5.4.2.4.1.2 Direito de oposição: possibilidades e limites a partir das lentes do abuso de direito e aspectos objetivos e subjetivos da legítima expectativa

À semelhança da hipótese de revogação do consentimento[230], a LGPD também previu o chamado direito de oposição frente às outras (nove) bases legais como uma maneira do titular obstruir o tratamento de seus dados[231]. Com isso, procurou-se reforçar o direito do indivíduo controlar seus dados independentemente da base legal utilizada para processá-los.

Contudo, diferentemente da revogação do consentimento, que se apresenta como um direito potestativo[232] e sem limitações, *a priori* estabelecidas, a LGPD condicionou o exercício do direito de oposição desde que haja uma violação a uma das suas normas. Uma primeira interpretação mais apressada levaria à conclusão de que o exercício desses dois direitos de objeção teria alcances distintos, já que o último não dependeria única e exclusivamente da vontade do titular em exercê-lo.

Se assim fosse, como resultado haveria uma indesejada assimetria normativa entre tais bases legais, a qual, como visto, procurou ser equalizada pelo legislador ao alocar sob o mesmo nível hierárquico todas as bases legais. Ao fim e ao cabo, deve-se buscar, sempre que possível, uma interpretação que busque colocar em pé de igualdade as hipóteses de legitimação para o tratamento de dados pessoais. Especialmente, o consentimento frente ao legítimo interesse, que é o objeto deste trabalho.

Como visto anteriormente, o legítimo interesse deve ser balanceado frente às legítimas expectativas do titular dos dados. Em um primeiro plano, tal análise é feita objetivamente de acordo com os padrões sociais e pelo próprio agente de tratamento de dados, o qual se coloca na posição do titular para avaliar se a sua conduta não frustraria a confiança nele depositada. Ao final, contudo, a última fase do teste tem como um dos seus pilares a adoção de medidas de transparência, de modo que o cidadão possa, também, ter voz sobre o que considera ser um uso (in)adequado das suas informações pessoais.

Portanto, a forma pela qual foi costurado o legítimo interesse na LGPD também confere uma posição jurídica ao titular de objeção ao tratamento de seus dados, lastreado em tal base legal. Nesse sentido, a expressão "legítima expectativa" tem igualmente uma *conotação subjetiva*, vinculada ao que o próprio titular deseja e espera que seja feito com seus dados. Caso contrário, a última fase do LIA, relativa ao dever de transparência, não funcionalizaria um dos fundamentos da lei que é a autodeterminação informacional.

Em poucas palavras, se na medida em que é dada transparência acerca do tratamento de dados com base no legítimo interesse e o titular a ele se opõe, caso o agente de tratamento de dados não o acate estará violando uma das normas da lei geral de proteção de dados pessoais. Trata-se de uma interpretação sistemática entre os arts. 10, II e § 2º, combinado com o art. 18, § 2º.

No entanto, deve-se observar que esse direito não é absoluto. Se por um lado, a posição jurídica de processar dados sem o consentimento prévio não pode ser abusada a ponto de lhe retirar por completo a sua capacidade de autodeterminação informacional, por outro lado tal direito de objeção também deve ser contornado pela figura do abuso de direito (subcapítulo 5.4.1.3).

Nesse sentido, por exemplo, a hipótese na qual o tratamento de dados pessoais serve ao

propósito de combate a incidentes de segurança na rede e processos de *due diligence* em operações societárias, são cenários nos quais há uma finalidade econômica-social que suplanta o direito individual do próprio titular. Se tais atividades de tratamento de dados estão em linha com os princípios e demais normas de proteção de dados, em especial com aqueles que são reforçados nas quatro fases do teste de aplicação do legítimo interesse (necessidade, transparência e prevenção), o direito de oposição tende a ser relativizado frente a um interesse coletivo. É uma dialética normativa que coteja a autodeterminação informacional frente aos demais fundamentos da LGPD[233].

Em conclusão, diferentemente da GDPR[234], a LGPD não procedimentalizou minimamente o direito de oposição especialmente frente à base legal do legítimo interesse. Com isso, abrem-se margens para disputas interpretativas. As considerações acima apontam que a aplicação e interpretação do direito de posição não deve ter como resultado um regime jurídico assimétrico, especialmente frente ao direito correspondente de revogação do consentimento. E, por fim, deve-se considerar que o direito de oposição não é absoluto e o seu exercício deve se amoldar à cláusula geral do abuso de direito.

5.4.2.4.1.3 Uma lógica de risco: pontos de atenção em torno do uso da base legal do legítimo interesse a partir do exemplo do campo da publicidade direcionada

Ao longo de tudo o que foi exposto, nota-se que a base legal do legítimo interesse é, em sua essência, recheada de incertezas. Para dela se valer, há a necessidade de se desvencilhar de um ônus argumentativo complexo, o qual ainda deve ser documentado. É, nesse cenário, que o LIA se apresenta e é capaz de fornecer algumas pistas sobre quais são os principais pontos de atenção para a mitigação dos riscos de eventual não conformidade acerca do uso dessa base legal.

Além de repisar parte do LIA, esse subcapítulo se valerá das discussões travadas por alguns órgãos reguladores no campo da publicidade comportamental e marketing a fim de agregar maior pragmatismo em nossa análise. Até porque, atualmente, a principal engrenagem do formato atual da economia são os dados pessoais para personalizar a oferta e o próprio bem de consumo. E, em muitos casos, a receita publicitária é a própria base de sustentação de muitos modelos de negócios.

Dessa forma, seja quem já mantém uma relação previamente estabelecida com o titular dos dados, seja no caso de terceiros que compõem uma rede de publicidade comportamental (subcapítulo 1.2.2.4), ambos têm, em princípio, o legítimo interesse em processar tais dados para otimizar e viabilizar as suas atividades comerciais. Não há dúvida em torno do benefício e da vantagem decorrente de tal atividade de tratamento de dados, ainda que puramente comercial. As três demais fases do teste do legítimo interesse é que atraem maiores controvérsias, sendo que, ao todo, listamos 4 variáveis para a composição de uma matriz de risco:

a) **relação preestabelecida e contexto na abordagem publicitária:** a ideia de legítima expectativa é muito mais aderente quando já há uma relação preestabelecida entre o

titular do dado e o agente de tratamento de dados. E, nesse ponto, o tipo de abordagem e reunião de informações pode trazer mais ou menos riscos no uso da base legal do legítimo interesse **a.1) *marketing* direto**[235]: há situações nas quais o titular do dado já mantém uma relação com o controlador, como no caso dele já ter adquirido seus produtos e serviços. A partir desse histórico de compras, é possível lhe direcionar anúncios publicitários condizentes com o seu padrão de consumo. Por exemplo, é o que uma loja de vinhos faria com consumidores que gostassem mais de uma determinada uva, ou o que livrarias fariam com clientes que gostassem mais de um determinado autor, e assim por diante; **a.1.1) *first-party tracking***[236]: esse perfil poderia ser construído não só através das compras efetivadas pelo consumidor, mas, também, do que lhe despertou interesse em sentido amplo. Por exemplo, quais produtos foram por ele pesquisados, quais deles se buscou saber mais a seu respeito através da quantidade de cliques e, assim por diante, em um cenário no qual a própria plataforma monitoraria o comportamento dos seus usuários; **a.1.2) síntese:** nesses casos, há um contexto que favorece a aplicação do legítimo interesse, na medida em que essa relação preestabelecida é um indicativo de que tal uso de dados é compatível com o que originou a sua coleta e, em última análise, com a legítima expectativa do seu titular; **a.2) *marketing* indireto e *targeted advertisement*:** há uma rede de publicidade comportamental composta por uma série de atores que trocam dados entre si e exibem tais anúncios em diferentes plataformas (subcapítulo 1.2.2.4). Essa é a razão pela qual, por exemplo, o mesmo anúncio publicitário percorre diferentes *websites* visitados ou aplicativos acessados. A dinâmica desse tipo de abordagem publicitária envolve: **a.2.1) terceiros:** uma multidão de atores que não mantêm nenhum tipo de relação com o titular dos dados, sendo na maiorias das vezes desconhecidos; e **a.2.2) *third-party tracking***[237]*:* a agregação de dados sobre o titular relativa a diferentes contextos nos quais tal rede opera cooperativamente para monitorá-lo (*cross-tracking*) ; **a.2.3) síntese:** nesses casos, há não só o ingresso de terceiros no fluxo informacional, mas também o acúmulo de dados de diferentes esferas da vida do titular do dado. É por esse motivo que o Grupo de Trabalho do Artigo 29 reafirmou o seu posicionamento de que o legítimo interesse não seria aplicável nesses casos[238], retomando a sua conclusão de que não estaria dentro das legítimas expectativas do titular dos dados e seria necessário recorrer à base legal do consentimento[239]. Por outro lado, alguns órgãos reguladores não têm fechado a porta de forma definitiva para a aplicação da base legal do legítimo interesse, devendo ser feita uma avaliação acerca do *grau de intrusão de perfilamento*, entre outros elementos[240];

b) **nível de intrusão (minimização)**: a lógica da publicidade comportamental é reunir ao máximo informações sobre o consumidor em potencial, mediante a criação do retrato

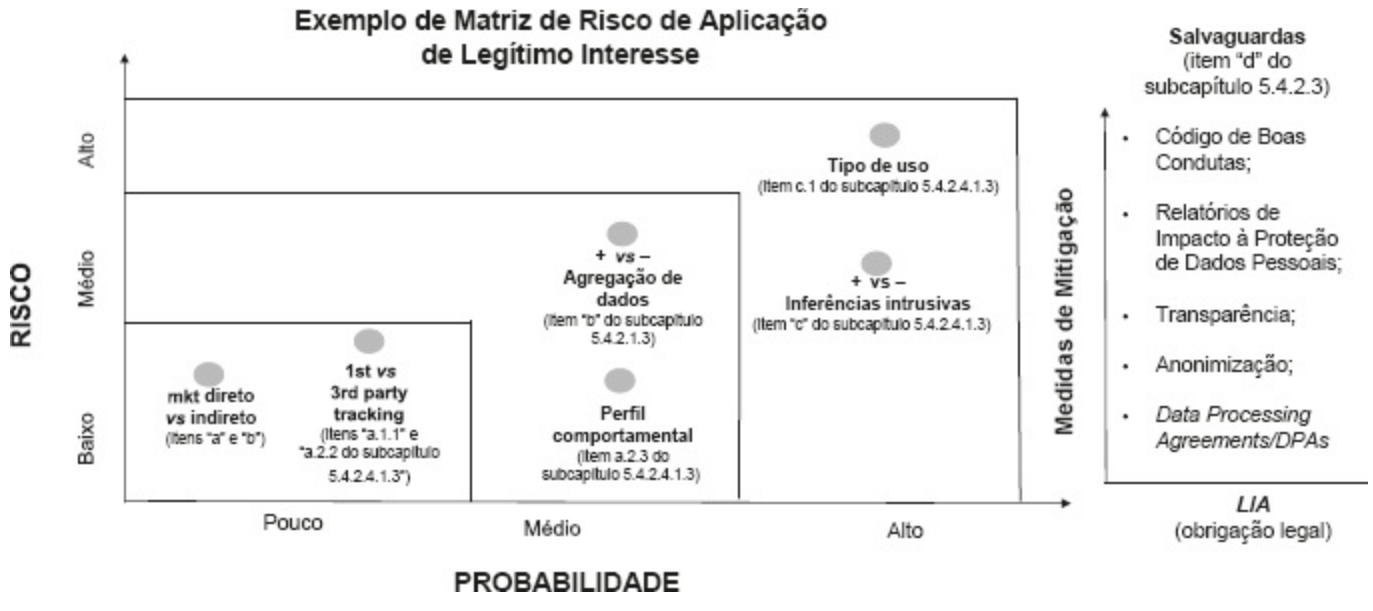
mais completo possível da sua personalidade. É o que tem prevalecido e a razão pela qual a publicidade comportamental tem se tornado mais efetiva do que outros tipos de publicidade direcionada, em especial no ambiente *on-line* (subcapítulo 1.3.2). Nesse contexto, há diferentes vetores de análise, que levam a destinos completamente distintos para calibrar a aplicação do princípio da minimização: **b.1)** se a finalidade é a simples personalização da abordagem publicitária, que pode se dar com um maior ou menor nível, então a lógica de maximização não se chocaria com tanta força com o princípio da minimização. Em outros termos, é possível viabilizá-la sem que para isso seja necessário formar um perfil bastante intrusivo e intimista do titular do dado (e.g., publicidade contextual e segmentada); **b.2)** se, por outro lado, a finalidade leva em consideração o grau de eficiência que se espera alcançar com o direcionamento da publicidade, então o que poderia ser considerado como dados necessários teria um espectro muito mais alargado (e.g., publicidade comportamental); **b.3)** a esse respeito é importante levar em consideração um dos "núcleos duros" da privacidade previstos no Marco Civil da Internet, qual seja, a proibição de que provedores de conexão pudessem armazenar *logs* de aplicação (subcapítulo 5.3.1.2). Como visto, a racionalidade do legislador foi impedir um mapeamento completo da vida digital das pessoas, o que seria tecnicamente possível por quem é a porta de entrada e de saída da internet. Ainda que tal dispositivo não seja direcionado aos provedores de aplicação, tal previsão poderia orientar quais limites deveriam ser impostos a tais atores da camada de conteúdo da Internet a respeito de como eles se organizam e cooperaram para direcionar publicidade. Uma interpretação que busca, acima de tudo, não gerar assimetrias frente à multiplicidade de agentes econômicos regulados e, com isso, verificar qual grau de capilaridade e pervasividade seria aceitável na agregação de informações para o direcionamento de publicidade[241];

c) **inferências e usos:** outro fato a ser considerado como fiel dessa balança são os tipos de inferência e usos desses dados. Como visto anteriormente (subcapítulo 1.2.2.2), tornou-se possível mapear as emoções do consumidor em potencial e até mesmo precificá-lo de acordo com o seu perfil. Nesses casos, a balança tende a estar em desequilíbrio por ser algo que: **c.1)** foge das legítimas expectativas do titular dos dados, como no caso de uma precificação dinâmica; e, principalmente, **c.2)** impacta negativamente a sua própria autodeterminação de forma ampla. Nessa situação, por exemplo, o seu poder de tomada de decisão para a aquisição de um bem de consumo em termos volitivos e econômicos é impactado negativamente[242]. Nesse sentido, será útil estabelecer um diálogo entre a LGPD e o Código de Defesa do Consumidor,[243] a fim de se verificar se tal tipo de prática também não seria abusiva;[244]

d) **Salvaguardas**: **d.1)** a principal salvaguarda nesses casos é a adoção de mecanismos de

transparência que permitam ao titular dos dados se opor a tal tipo de tratamento (*opt-out*). Quanto mais visível for tal prática e mais fácil for o exercício do *opt-out*, maiores serão as chances de a aplicação do legítimo interesse ser considerada como uma base legal válida; **d.2.)** a aplicação de PETs é um fator-chave, principalmente as que facilitam que o titular do dado barre ou personalize o seu monitoramento diante da multidão de atores que compõem uma rede de publicidade comportamental (caso essa prática passasse pela fase anterior do teste); **d.3)** havendo uma série de atores que cooperam para a entrega da publicidade comportamental, é importante verificar qual é o seu nível de cooperação para proteção de dados pessoais. Nesse sentido, além do estabelecimento de contratos que definam a responsabilidade e os deveres de um dos agentes da cadeia de tratamento de dados pessoais é algo básico, o qual pode e deve ser complementado pela elaboração de relatórios de impacto à proteção de dados pessoais, códigos de boas condutas e outras iniciativas que reforcem o seu comprometimento a esse respeito.[245]

Em conclusão, ainda será testado e validado, especialmente no cenário brasileiro, quais os limites de aplicação da base legal do legítimo interesse como medida de apoio e promoção das atividades no campo da publicidade. Contudo, de antemão, já é possível diagnosticar quais serão as hipóteses mais controversas e mais arriscadas e, por outro lado, as respectivas medidas de contenção dos riscos em questão. Toda a jornada percorrida pode ser sumarizada a partir da seguinte matriz de análise:



5.4.2.5 Síntese da aplicação da privacidade contextual na LGPD através do legítimo interesse

A aplicação da base legal do legítimo interesse não se dá no vazio, demandando-se uma análise *contextual* para verificar se o tratamento dos dados está de acordo com as "legítimas expectativas" do seu titular[246]. Seja no caso de quem já mantém uma relação preestabelecida com o titular do dado,

seja no caso de terceiros, deve-se verificar se o novo uso atribuído é *compatível*[247] *e está bem articulado dentro de uma situação concreta.*

Retoma-se, com isso, o vocabulário próprio da privacidade contextual que ganha gatilhos no próprio desenho normativo da LGPD. Como seu saldo final: **a)** deve haver um fluxo informacional que seja íntegro-apropriado para o livre desenvolvimento da personalidade do titular do dado (proteção dos seus direitos e liberdades fundamentais); **b)** que esteja dentro da sua esfera de controle (legítimas expectativas), garantindo-se, inclusive, medidas de transparência que reforcem a sua carga participativa no fluxo das suas informações, ainda que *a posteriori*.

A combinação entre legítimo interesse e privacidade contextual confirma a tese de que autodeterminação informacional vai além do consentimento. O cidadão também exerce domínio sobre seus dados, se estes forem tratados de forma previsível de acordo com suas legítimas expectativas.

5.5 DADOS PÚBLICOS E MANIFESTAMENTE PÚBLICOS NA LGPD

Uma leitura apressada dos §§ 3º e 4º do art. 7º[248] poderia sugerir que a LGPD não teria rompido com a dicotomia entre público e privado ao prever as categorias de dados de "acesso público" e "manifestamente públicos" (subcapítulo 2.4). Na verdade, trata-se justamente do contrário. A lei procurou estancar qualquer tipo de dúvida em torno da sua aplicabilidade sobre esse tipo de dado e, ao fazê-lo, é mais um desdobramento da aplicação da privacidade contextual.

A cultura jurídico-legal brasileira ainda associa muito a proteção de dados pessoais ao direito à privacidade, tratando-os quase como sinonímia (subcapítulo 2.4.1). Tanto é verdade que durante a consulta pública do então anteprojeto de lei de proteção de dados pessoais notaram-se debates acirrados[249] sobre tal aspecto dogmático e, mais especificamente, a sua adoção em alguns julgados nos tribunais brasileiros.

Apenas a título de exemplo, pode ser citada a ação civil pública julgada pelo Tribunal de Justiça do Rio Grande do Sul – TJRS envolvendo o Ministério Público gaúcho e a Confederação Nacional de Dirigentes Lojistas – Serviço de Proteção ao Crédito – SCP do Brasil[250]. Ao reformar a decisão de primeira instância, a racionalidade do julgado aponta que dados pessoais, como nome, endereço, profissão, idade, estado civil e filiação – os chamados "dados cadastrais" –, seriam dados de caráter público[251], dados que "quase todos os cidadãos comuns, quase que diariamente, são compelidos a fornecer ao praticar atos da vida civil (...), não sendo, portanto, sigilosos". Por serem de "domínio público", "nada de ilícito" existiria na "comercialização" desses dados, especialmente para fins de "*marketing* e *telemarketing*", mesmo que sem a autorização por parte do cidadão.

Todo o esforço argumentativo em associar tal categoria de dados como não passíveis de proteção remonta justamente ao pensamento dicotômico entre público e privado, isto é, em conferir um maior

ou menor grau de proteção de acordo com o caráter confidencial da informação. Essa racionalidade não permite avançar na reflexão sobre a finalidade para quais dados estão em circulação e, em última análise, o que justifica a sua disponibilização.

Nesse sentido, o § 3º do art. 7º da LGPD ressalva expressamente que o tratamento de "dados pessoais cujo acesso é público deve considerar a finalidade, boa-fé e o interesse público que justificaram sua disponibilização". Ademais, o § 3º do mesmo artigo limita o tratamento posterior (i.e., para "novas finalidades") dos dados pessoais manifestamente públicos e os de acesso público desde que observados os "propósitos legítimos e específicos" para o novo tratamento e a preservação dos direitos do titular[252]. Com isso, a norma propõe justamente romper com esse pensamento binário entre o público e privado ao ressalvar que se deve levar em consideração o *contexto* pelo qual tais dados são publicamente acessíveis.

Por exemplo:

a) se, para fins de transparência, o Poder Público divulga os nomes, os cargos e a renda dos servidores, tal base de dados dificilmente poderia ser reutilizada para fins de *marketing*. Por outro lado, seria possível o seu uso para diagnosticar eventual nepotismo na Administração Pública[253];
b) se o Poder Judiciário disponibiliza certidões sobre processos judiciais para, dentre outras coisas, aferir a capacidade de (in)solvência dos cidadãos, muito provavelmente, essa informação poderia ser utilizada para a análise de crédito. Por outro lado, seria questionável o seu uso para desclassificar o devedor-candidato em um processo de contratação.

Em todos esses casos, o que define a (i)legalidade do tratamento dos dados é a sua *compatibilidade* com a finalidade e o interesse público pelo qual tais dados são de acesso público. É necessária, portanto, uma *análise contextual* para saber por que houve publicização da informação, o que calibrará os possíveis (re)usos que dela podem ser feitos. Veja-se, portanto, que mais uma vez retoma-se o vocabulário para privacidade contextual.

A mesma lógica pode ser transposta no que diz respeito aos chamados "dados manifestamente públicos". Da mesma forma que dados de acesso público[254], deve ser levado em consideração o contexto em que tal informação foi disponibilizada. Ao ressalvar que os direitos do titular e os princípios[255] previstos na lei estariam resguardados, o § 4º[256] do art. 7º da LGPD não autoriza o uso indiscriminado dessas informações. Pelo contrário, retoma-se justamente a ideia de que deve haver *compatibilidade* entre o seu uso e as circunstâncias pelas quais tal dado foi tornado público.

Por exemplo, a princípio, terceiros não poderiam usar dados de uma rede social, mesmo que de perfis públicos, para fins de *marketing*. As circunstâncias pelas quais tais dados foram tornados públicos pelo seu próprio titular deram-se para uma outra finalidade, que é a de se relacionar com

quem integra o seu círculo social.

Por outro lado, a princípio, seria compatível o uso de dados de perfis públicos de uma rede profissional (*e.g.*, LinkedIn) por terceiros, como *headhunters*, para aproximar seus usuários às vagas profissionais de seu eventual interesse. Esse uso é compatível com a finalidade não só da plataforma em si, como, principalmente, a razão pela qual tais dados são públicos[257].

Portanto, as figuras de dados de acesso público e manifestamente público, além de estarem dentro do escopo de aplicação da LGPD, também estão sujeitas a um regime que impõe uma série de requisitos para o seu tratamento à luz do referencial da privacidade contextual. O *caráter pedagógico* dessa taxonomia é não deixar dúvidas de que tais tipos de dados não deixam de ser pessoais[258], rompendo com a chave binária do público-privado. E, por fim, assegurar uma esfera de controle por parte dos titulares dos dados, ainda que não haja o seu consentimento para tanto.

5.6 DIÁLOGO DAS FONTES: LGPD EM COORDENAÇÃO COM O RESTANTE DO ORDENAMENTO JURÍDICO BRASILEIRO

Uma lei que terá um impacto econômico-social e regulatório como poucas outras tiveram na história do país, suplantável ao que foi o Código de Defesa do Consumidor e a Consolidação das Leis Trabalhistas. Empresas, governos, cidadãos, consumidores, enfim, todos nós estamos, a todo o momento, trocando dados. Uma sociedade e economia que é cada vez mais movida por dados (*data-driven economy and society*) – (subcapítulo 1.2), estando todo o tecido social "datificado". Um "dataísmo", nas palavras de Yuval Harari[259], que orienta toda a lógica de geração de riqueza e conhecimento dos mais diversos setores produtivos (das empresas nascentes de tecnologias à indústria mais tradicional) e na formulação e implementação das mais distintas políticas públicas (do acesso à saúde a programas de transferência de renda). Em razão desse contexto, leis gerais de proteção de dados pessoais, como a Lei 13.709/2018, são elevadas, por vezes, ao patamar de um novo contrato social. Nelas se encontram as "regras do jogo" para o próprio funcionamento pacífico e democrático da sociedade.

Nesse cenário, mostra-se desafiadora a acomodação da LGPD no sistema jurídico brasileiro por ser uma peça que o atravessará quase que por completo. Será necessário encontrar um método ancorado em uma perspectiva de integração e sincronização dessa nova lei com o restante do ordenamento, que é exatamente o que se busca com a teoria do diálogo das fontes.

Diferentemente dos métodos tradicionais de hermenêutica[260], que rogam pela prevalência de uma norma sobre a outra[261], a teoria do diálogo das fontes propõe uma nova teoria geral do direito visando à intersecção e complementação das normas. Em vez de uma monossolução[262], passa-se a adotar uma lógica de coordenação[263] pela qual deve haver aproximação e não afastamento em um

ambiente normativo plúrimo. Pavimenta-se, com isso, uma via para que haja influência recíproca entre as normas[264], isto é, um verdadeiro diálogo[265].

A esse respeito, é importante destacar que a própria LGPD acenou para tal intersecção ao pontuar que não estão excluídos outros direitos e princípios relacionados à matéria previstos no ordenamento jurídico brasileiro[266]. Com isso, o texto da lei, reforçando o seu próprio *nomen juris*, coloca-se como uma *fonte normativa materialmente geral* que deve conversar com as demais para governar o uso de dados pessoais. Há, portanto, uma orientação hermenêutica embutida no desenho da LGPD, que preza pela unicidade de todo o conjunto de normas afeto à matéria.

A partir dessa perspectiva, três são as vertentes da teoria do diálogo das fontes a serem consideradas:

a) **coerência-sistemática**: a LGPD e outras leis podem servir de *base conceitual* uma para outra, fornecendo-se *vis-a-vis* critérios e elementos interpretativos. Essa influência recíproca teria o potencial de garantir unicidade ao sistema jurídico brasileiro de proteção de dados pessoais, a partir de uma lógica de coerência interna da LGPD e externa de outras normas de proteção de dados;

b) **complementariedade-subsidiariedade**: a LGPD agregou novos parâmetros de governan para o uso de dados pessoais, os quais devem *complementar e ser aplicados de forma coordenada com os anteriores*. Em especial a LGPD terá que ser sincronizada, por exemplo, com a Lei do Cadastro Positivo, o Código de Defesa do Consumidor, o Marco Civil da Internet, os quais já dispõem de normas de proteção de dados pessoais.

c) **coordenação-adaptação sistêmica**: a LGPD define conceitos e princípios que, quando aplicados a outras leis, *redefinem o escopo de aplicação e os parâmetros delas – e vice-versa*. Trata-se da influência do sistema especial no geral e do geral no especial.

O quadro abaixo lista exemplificativamente possíveis aplicações da teoria do diálogo das fontes, a partir do que já foi analisado ao longo deste trabalho. Ao final e ao cabo, será necessário decantar a LGPD frente não só às demais normas já existentes sobre proteção de dados pessoais, mas, também e principalmente, frente a elementos bastante tradicionais e adensados da cultura jurídica brasileira:

Temas de Diálogo	Leis e Dispositivos em Diálogo	Categorização do Diálogo	Ganho Interpretativo
	LGPD (art. 5º, I)		A LGPD adota a orientação de um conceito de dados pessoais expansionista – i. e. com o uso do
	Decreto do MCI (art. 14, I)		

Conceito de Dado Pessoal – Expansionista	LAI (art. 4º, I)	**Complementariedade –subsidiariedade** (suplementação do conceito de dado pessoal com exemplos)	qualificativo "identificável" –, mas é o Decreto do Marco Civil da Internet que traz um rol exemplificativo do que pode ser considerado dado pessoal. A LAI, por sua vez, define o que seja "informação", fornecendo, assim, elemento interpretativo para a definição trazida pela LGPD. (subcapítulo 2.2)
Conceito de Dado Pessoal – Análise Consequencialista	LGPD (arts. 1º, caput; 2º, VII, 5º, I; 12, § 1º, e 20) CC (art. 21)	**Coordenação-adaptação sistêmica** (redefinição do escopo de direitos da personalidade e da compreensão de livre desenvolvimento da personalidade)	O compromisso do ordenamento jurídico pátrio com a proteção à vida privada, aos direitos fundamentais e ao livre desenvolvimento da personalidade, indicados na LGPD e no CC, consubstanciam a adoção do que chamamos de "análise consequencialista" de dados pessoais. (subcapítulo 2.2.4)
	LGPD (art. 7º) MCI (art. 7º, VII) LCP (art. 4º) LAI (art. 8º, caput)	**Complementariedade –subsidiariedade & Coordenação-adaptação sistêmica** (suplementação das	A LGPD traz, ao todo, 10 (dez) hipóteses para a legitimação das atividades de tratamento de dados pessoais. Suplementa-

Bases Legais para o Tratamento de Dados	CDC (art. 44)	bases legais para o tratamento de dados pessoais com a redefinição do escopo de aplicação das bases legais constantes em leis setoriais de dados pessoais pela LGPD)	se, com isso, as demais normas setoriais de proteção de dados, as quais, em sua grande maioria, gravitavam em torno do consentimento. (subcapítulo 3.3.3)
Dever de Informação e Transparência & Consentimento Informado	LGPD (art. 9º) MCI (art. 7º, VI e VIII) LCP (arts. 3º, § 2º; 7-A, § 2º) CDC (art. 6º, III) LAI (Art. 6º, I)	**Complementariedade–subsidiariedade** (suplementação do dever de informação geral previsto pelo CDC, pelas LGPD e leis setoriais no campo de proteção de dados pessoais)	O CDC já havia estabelecido o dever de informação de forma ampla e aberta. Foram as leis posteriores, contudo, que estabeleceram os critérios e parâmetros interpretativos da forma como e quais informações deveriam ser fornecidas na seara de proteção de dados pessoais. O diálogo de fontes tornou mais prescritivo o dever de informação a esse respeito. (subcapítulo 4.2.3)
Meios de Obtenção	LGPD (art. 8º, caput) MCI (art. 7º, IX) LCP (art. 4º, IV, "b")	**Complementariedade–subsidiariedade** (suplementação dos	A exigência de "autorização" prévia e específica do consumidor estabelecida pelo CDC é seguida por leis que estabelecem a exigência de "consentimento" de

do Consentimento	CDC (art. 6º, III)	meios pelos quais se pode obter o consentimento)	maneira cada vez mais contratualizada. Finalmente, a LGPD previu a coleta do consentimento "por outro meio" que não o escrito. (subcapítulo 4.1)
Consentimento Livre	LGPD (art. 9º, § 3º) MCI (art. 8º) LCP (arts. 7º-A; 4º, IV, "b") CDC (art. 39) CC (art. 423)	**Coerência-sistemática & Complementariedade–subsidiariedade** (base conceitual da autonomia da vontade prevista em leis gerais, cujos desdobramentos são suplementados por leis de proteção de dados)	O CDC e o CC já traziam dispositivos acerca de relações em que há assimetria de poder e informação, com vistas a proteger a parte mais vulnerável e equalizar os direitos e deveres entre partes. Com as leis posteriores, em especial o MCI e a LGPD, essa lógica continua sendo utilizada para se apurar o quão livre é o consentimento no tratamento de dados pessoais. (subcapítulo 4.2.3)
Consentimento Expresso e Específico	LGPD (arts. 5º, XII; 7º, §5º; 8º, § 4º; 14, §1º; 33, VIII) MCI (arts. 7º, VII e IX; 16, II)	**Coordenação-adaptação sistêmica** (definição do escopo de aplicação de um consentimento mais reforçado a partir das exigências específicas	A exigência de um consentimento mais reforçado (adjetivos "expresso" e "específico") variará de acordo com a natureza do dado e de acordo com o respectivo

	LCP (art. 4º, IV, "b")	de cada uma das leis de proteção de dados pessoais)	regime jurídico atribuído pela lei aplicável. (Subcapítulo 4.2.1)
Legítima Expectativa & Legítimo Interesse	LGPD (arts. 6º, I e II; 7º, IX e 10) CC (arts. 187 e 422) CDC (arts. 4º, III e 51)	**Coerência-sistemática** (base conceitual de conceitos jurídicos indeterminados constantes da LGPD, a partir do CC e CDC)	As expressões "legítima expectativa" e "legítimo interesse" trazidas pela LGPD são conceitos jurídicos indeterminados. Assim, para sua aplicação, sem que se tornem "carta-branca" para abusos, devem ser correlacionados com outros parâmetros interpretativos mais adensados na cultura jurídico-brasileira, de maneira coordenada. (subcapítulo 5.4.2)
Dados Públicos	LGPD (art. 7º, § 3º)	**Coerência-sistemática** (base conceitual do porquê uma informação deve ser publicizada e qual a racionalidade para se legitimar novos usos desse dado público)	A LAI define o que seja acesso público a contrario sensu, de maneira ampla e sem parâmetros para o tratamento de dados que sejam de acesso público. A LGPD, por sua vez, visando à proteção e à autodeterminação informacional do titular, estabelece os parâmetros para o tratamento desse tipo

			de dado. (subcapítulo 5.5)

5.7 CONCLUSÃO: AUTODETERMINAÇÃO INFORMACIONAL VAI MUITO ALÉM DO CONSENTIMENTO

Após uma abordagem analítica dos dados pessoais como um novo ativo econômico, como um novo direito da personalidade e de como isso foi acomodado pelas legislações de proteção de dados pessoais, reavaliou-se, em duas frentes, o produto desse diagnóstico: a função e os limites do consentimento para compreender o que é autodeterminação informacional, que é um dos fundamentos da LGPD.

A primeira demonstra que a falácia do consentimento pode ter como causa a ausência de uma tomada regulatória que disponibilize formas efetivas ao cidadão para autodeterminar as suas informações pessoais. Atacou-se, prioritariamente, a *contratualização* da autodeterminação informacional – políticas de privacidade –, que tem se mostrado como um mecanismo ineficiente para capacitar o cidadão a controlar seus dados pessoais. Isso, associado ao próprio desenvolvimento tecnológico que tem sido invasivo à privacidade (PETs), tem mistificado por completo a autodeterminação informacional com base no consentimento.

Contudo, a tecnologia pode ser, diferentemente, uma ferramenta de empoderamento do titular dos dados pessoais. Sob o guarda-chuva das PETs, verificou-se que a tecnologia pode funcionalizar a autodeterminação informacional, remendando-se as fissuras entre o arranjo normativo teorizado e a realidade que lhe é subjacente.

Nossa releitura propõe, basicamente, que a condição de (hiper)vulnerável do cidadão, posto em uma relação assimétrica em uma economia de dados, seja absorvida pela arquitetura da rede. A partir de uma análise detida de duas PETs em específico – DNT e P3P –, demonstrou-se que falta torná-las executáveis. Elas podem representar uma multiplicidade de formas diante dos múltiplos adjetivos – expresso, informado, inequívoco, específico e livre – dados ao consentimento do titular dos dados pessoais, garantindo-se que tal qualificação não seja artificial e desemboque em um controle mais significativo dos dados pessoais.

Não falta, contudo, uma percepção crítica à releitura proposta. Ressalva-se a importância de que tais tecnologias sejam amigáveis (*usable-friendly*). O dever-direito de informação deve oxigenar a implementação das PETs, a fim de que elas sejam o veículo para que seja prestada uma informação adequada, clara e suficiente aos cidadãos sobre o fluxo de seus dados pessoais. Somente assim eles poderão racionalizar um processo de tomada de decisão genuíno a seu respeito.

Com isso, empresta-se, ainda, densidade legal às PETs. O dever-direito da informação,

associado à concepção da relação obrigacional como um processo, revela que o empoderamento do cidadão com o controle das suas informações pessoais situa-se dentro do plexo de direitos e obrigações das relações do mercado informacional, mostrando-se as PETs como o meio adequado para efetuar o seu pagamento. Em outras palavras, as PETs passam a ter uma dimensão normativa no seio obrigacional das relações de uma economia de dados, traduzindo-se como o adimplemento satisfatório de tal dever obrigacional.

Em suma, propõe-se, sob uma primeira lente de análise, a reavaliação *procedimental* da autodeterminação informacional. Investiga-se como novas formas podem operacionalizar de forma mais eficiente o consentimento do titular dos dados pessoais, a fim de nutrir a sua capacidade em controlá-los.

Sob uma segunda lente, sugere-se uma análise que é contingente à primeira, mas que a complementa. Procura-se compreender a autodeterminação informacional para além do consentimento, investigando-se quais são a função e os limites da autonomia da vontade do titular dos dados. Com isso, reavalia-se *substantivamente* o paradigma normativo da autodeterminação informacional.

Retrocede-se ao discurso da proteção dos dados pessoais como um direito da personalidade, ressaltando-se o seu valor social para traçar um *relativo normativo complementar* – privacidade contextual, elaborado por Helen Nissenbaum – que não deixa somente sob os ombros do indivíduo a carga da proteção dos dados pessoais. Propõe-se que a proteção dos dados pessoais não deve ser compreendida sob uma lente egoística e individualista, reforçando a sua alocação dogmática junto aos direitos da personalidade em oposição ao direito de propriedade. Sublinha-se, com isso, a negociabilidade limitada dos direitos da personalidade, o que impede que o consentimento coisifique o próprio titular dos dados pessoais.

A autonomia da vontade deve ser, portanto, limitada, assegurando-se que o fluxo informacional seja apropriado para o livre desenvolvimento da personalidade. Para além das hipóteses já previstas no ordenamento jurídico que estabelecem núcleos duros ao consentimento do titular, verificou-se que a privacidade contextual amplia o horizonte normativo para a solução de casos em que o consentimento ocasionaria distorções ao valor social da proteção dos dados pessoais.

Por fim, notou-se, paradoxalmente, que a limitação da carga participativa do indivíduo dá fôlego ao consentimento para que ele opere em cenários nos quais ele não seria a base legal para o tratamento dos dados pessoais. Ao se analisar o regime jurídico da LGPD dispensado ao legítimo interesse e aos dados públicos e manifestamente públicos, há uma espécie de *consentimento contextual* em que o cidadão também exerce domínio sobre seus dados, ainda que sem declarar a sua vontade, se estes forem tratados de forma previsível – *i.e.*, de acordo com as suas legítimas expectativas.

Em um solo epistemológico – *v.g.*, *Big Data* –, que torna exponencial os diversos usos possíveis com dados, a privacidade (consentimento) contextual mostra-se útil. Há uma nova roupagem para que

a autodeterminação informacional seja elástica o suficiente para governar tais usos dos dados pessoais, os quais não podem ser previamente especificados (*presentificados*) de maneira rígida. É uma bagagem normativa-teórica que tem como vetores de aplicação os princípios da boa-fé e da confiança, já altamente adensados na cultura jurídica brasileira.

Há, assim, um discurso de *ambivalência*. Ora se aposta na capacidade do cidadão em controlar seus dados pessoais. Ora dela se desconfia, mas com o intuito de que, com a criação de uma zona de interferência, seja assegurada uma zona de autonomia genuína e coerente com o valor social da proteção dos dados pessoais. Essa dualidade tem, no entanto, um traço marcante comum, que é a percepção de que o titular dos dados pessoais amarga uma (hiper)vulnerabilidade, o que demanda, respectivamente, o seu empoderamento para emancipá-lo e a sua intervenção para assisti-lo[267].

Por conta dessa racionalidade comum, tais caminhos bifurcados confluem para o mesmo destino: a reavaliação do paradigma da autodeterminação informacional e o papel do consentimento na proteção de dados pessoais. Ao longo desse percurso, verificou-se que *o consentimento* do titular dos dados *continua a exercer um papel normativo de protagonismo, mas sob um novo roteiro que inclui a atuação de atores coadjuvantes importantes*: **i)** novas formas para operacionalizá-lo, levando-se em conta a arquitetura (de vulnerabilidade) da rede; **ii)** o relato normativo complementar da privacidade contextual que o limita e o readapta diante de um solo epistemológico que esfacela a técnica tradicional da autodeterminação baseada de declaração de vontade do titular dos dados; e **iii)** o cidadão também exerce domínio sobre seus dados, se estes forem tratados de forma previsível de acordo com suas legítimas expectativas. Portanto, o conteúdo jurídico-normativo de autodeterminação informacional vai além do consentimento.

O final desse enredo proposto é a tese de que haja uma maior intervenção na economia da informação, seja para reduzir a assimetria existente entre seus agentes econômicos, seja para limitar a autonomia da vontade de quem é a sua parte (hiper)vulnerável – o titular dos dados pessoais. Propõe-se, assim, um *dirigismo* dessa relação de consumo do século XXI, mas que não se confunde com aquele carreado no século passado.

O foco não é uma intervenção dos arranjos contratuais de tais relações de consumo (dirigismo contratual)[268], mas do seu fluxo informacional (*dirigismo informacional*). Isso porque, por exemplo, a proteção contratual do consumidor tem pouco a agregar por ser um remédio *ex post* mediante a invalidação de cláusulas contratuais abusivas. Foca-se, ao contrário, em uma racionalidade regulatória e normativa *ex ante* que procura empoderar o cidadão com o controle dos seus dados pessoais, o que extrapola o momento de quando essa questão ganha roupagem contratual.

Para tal propósito, deve-se ter em mente a referenciada *normatização ambivalente*. Ora *procedimental* à autonomia do cidadão, para capacitá-lo com o controle de seus dados pessoais, uma vez que está inserto em uma relação assimétrica que amordaça a sua liberdade, ora *substantiva*, para garantir um fluxo informacional íntegro ao valor social da privacidade informacional, sublinhando-se a importância de que o trânsito dos dados pessoais promova o livre desenvolvimento da

personalidade de seus titulares.

Essa dualidade pode representar um horizonte de possibilidades para lidar com os inúmeros desafios da proteção de dados pessoais, a começar pela simples proposição de que a proteção dos dados pessoais não comporta uma única lente normativa, bem como que essas novas relações de consumo demandam um novo tipo de dirigismo.

[1] Essa expressão crítica – ao reino do indivíduo – já foi utilizada, anteriormente, por: MAYER-SCHONEBERGER. Op.cit., p. 223.

[2] Veja-se, entre outros, citando-se de forma completa tais bibliografias: CATE, Fred H. The Failure of Fair Information Practice Principles. In: WINN, Jane K. (Ed.)*Consumer Protection in the Age of the 'Information Economy'* (markets and the law). Hampshire: Ashgate Publish, 2006; AUSTIN, Lisa M. Is consent the foundation of fair information practices? Canada's experienc under PIPEDA. Research paper n. 11-05.*University of Toronto Law Journal*, p. 1-54, 2006; SOLOVE, Daniel. Introduction: Privacy self-management and the consent dilemma*Harvard Law Review*, v. 126, p. 1880-1993, 2013; STRANDBURG, Katherine J. Free Fall: The Onlir Market's Consumer Preference Disconnect.*NYU School of Law, Public Law Research Paper*, n. 13-62; *NYU Law and Economics Research Paper*, n. 13-34, p. 94-172, Oct. 2013. Disponível em: <http://ssrn.com/abstract=232396>; KERR Ian; BARRIGAR, Jennifer; BURKELL, Jacqel BLACK, Katie, Soft surveillance, hard consent. In: KERR, Ian (Ed.)*Lessons from the identity trail*: anonymity, privacy and identity in a networked society. New York: Oxford University Press, 2009. p. 5-22; LAWSON, Philippa; O'DONOGHE, Mary. Approaches to Consent Canadian Data Protection Law. In: KERR, Ian (Ed.)*Lessons from the identity trail*: anonymity, privacy and identity in a networked society. New York: Oxford University Press, 2009. p. 23-42; COHEN, Julie. Examined lives: informational privacy and subject as object.*Stanford Law Review*, n. 52, p. 1373-1438, 1999-2000.

[3] Veja-se, especialmente: BAMBERGER, Kenneth A.; MULLIGAN, Deirdre K. Privacy on the boo and on the ground. *Stanford Law Review*, v. 63, p. 247, Jan. 2011. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568385> (O título é autoexplicativo analisando as críticas recorrentes a respeito de um modelo regulatório focado na premissa de empoderar os indivíduos para que eles controlem as suas informações, como assim discorrem os livros, em comparação a sua (in)efetividade na prática (*on the ground*), cuja metodologia de pesquisa valeu-se de entrevistas com *privacy officers*).

[4] É uma professora lotada na Universidade de Nova Iorque, diretora do *Law Information Institute*. sua biografia pode ser encontrada em sua página pessoal: <http://www.nyu.edu/projects/nissenbaum/main_bio.html>.

[5] De forma alguma a pretensão é esgotar o rico referencial teórico a ser analisado que dá uma visão ampla sobre todos os desafios da privacidade. Nosso objetivo é fazer um recorte preciso e breve de como esse referencial se encaixa como uma alternativa a complementar o paradigma normativo da autodeterminação informacional. Por isso, alerta-se o leitor de que as próximas páginas consistem em uma visão seletiva e, de certo modo, arbitrária do referencial teórico de Helen Nissenbaum.

[6] Valeu-se, basicamente, de um livro e de um artigo da mencionada autora, respectivamente: NISSENBAUM, Helen*Privacy in Context*: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010; NISSENBAUM, Helen. Privacy as contextu integrity. *Washington Law Review,* v. 79, p. 119, 2004.

[7] Essa é a terminologia utilizada: NISSENBAUM, *Privacy*... Op.cit., p. 3.

[8] Veja-se, em especial, a parte do livro sob análise: Ibidem, p. 7.

[9] Ibidem, p. 2: "Many them Protecting privacy means strictly limiting access to personal informatior or assuring people's right to control information about themselves. I disagree. What people care most about is not simply restricting the flow of information but ensuring that is flow appropriately (...)".

[10] À época do desenvolvimento da pesquisa, que resultou na primeira edição desse livro, a Prof. Helen Nissenbaum lecionava na New York University a frente, por exemplo, do grupo de Pesquisa em Privacidade. Para mais informações: <https://nissenbaum.tech.cornell.edu/>.

[11] Ibidem, p. 6.

[12] Veja-se, por exemplo, o tópico intitulado "Moralidade Política dos Contextos". Ibidem, p. 165-16 e, especialmente, o valor da privacidade que navega entre os danos causados por um fluxo informacional inapropriado até a própria autonomia do indivíduo. Ibidem p. 74-81.

[13] Ibidem, p. 140.

[14] Utiliza-se o termo "privacidade contextual" como um processo de decisão heurística, cujo centro análise não está focado em capturar significado completo da privacidade, mas identificar como sucedem violações a tal direito. Ibidem, p. 148.

[15] Ibidem, p. 4.

[16] Esse é o título, por exemplo, do mencionado artigo "Privacy as contextual integrity".

[17] Essa é uma interpretação (didática) que se faz do que a autora denomina relação "coconstitutiva" entre normas informacionais e contexto, cunhada por ela de normas informacionais relativas-contextuais, o que é abreviado como normas informacionais. Ibidem, p. 141.

[18] A própria autora alerta que toma emprestada essa teoria (das esferas sociais) de diversos autores, tal como de Talcott Parsons, Erving Golfmman e Max Weber. Ibidem, p. 130.

[19] A teoria de Helen Nissenbaum muito se aproxima da teoria dos círculos concêntricos da privacidade, na medida em que ambas fazem alusão semiótica às esferas em que as informações pessoais circulam. Contudo, elas se distanciam, substancialmente, porque a primeira não trabalha com a dicotomia do público e privado que é uma chave de leitura essencial para diferenciar dinâmica do direito à privacidade do direito de proteção aos dados pessoais (vide subcapítulo 2.4.1). Por isso, a escolha em "nacionalizar" esse referencial teórico em vez da difundida teoria das esferas do direito à privacidade.

[20] Ibidem, p. 129.

[21] Nota-se aqui que houve uma mudança sutil entre o artigo e o livro analisados. No primeiro, a auto elegeu dois elementos para dissecar as normas informacionais: adequação (*appropriateness*) e normas de distribuição (NISSENBAUM, Helen. Privacy as... Op.cit., p. 138-143. Enquanto n livro, os critérios eleitos foram contexto, autores, atributos da informação e princípios de transmissão (NISSENBAUM, Helen. *Privacy in*... Op.cit., p. 140-146).

[22] Essa parecia ser a proposta original contida no artigo citado, já que o segundo elemento focava na análise da "movimentação ou transferência das informações de uma parte para outra". Privacy as... Op.cit., p. 140.

[23] NISSENBAUM, Helen. *Privacy in*... Op.cit., p. 141.

[24] NISSENBAUM, Helen. *Privacy in*... Op.cit., p. 130.

[25] Ibidem, p. 136.

[26] SOLOVE, Daniel. Understanding... Op.cit., p. 89. Vejam-se, ainda, as reflexões de: PARRA Henrique. *Privacidade como um bem comum:* privacy as a commons. Disponível em: <http://lavits.org/?p=1038&lang=pt>.

[27] SCHWARTZ, Paul. Privacy and... Op.cit., p. 1613.

[28] NISSEMBAUM, Helen. Op.cit., p. 76.

[29] Nesse sentido, utiliza-se o termo privacidade como "elemento constitutivo da sociedade civil". Cohen, Julie. Examined... Op.cit., p. 1428.

[30] SCHWARTZ, Paul. Privacy and... Op.cit., p. 1663.

[31] Veja-se o item "Commodification, identity and agency" da obra de: ROESSLER, Beate. Shoul personal data be a tradable good? On the moral limits of markets in privacy. In: ROESSLER Beate; MOKROSINSKA, Dorota (Org.)*Social Dimensions of Privacy*. Cambridge: Cambridge University Press, 2015. p. 146-150.

[32] SCHWARTZ, Paul. Privacy and... Op.cit., p. 1664.

[33] Veja-se a afirmação contumaz de que a "*commodifitcation* dos dados pessoais pode afetar a constituição da personalidade e da identidade das pessoas" de: ROESSLER, Beate. Should. Op.cit., p. 150. Na doutrina brasileira, veja-se, ainda, a consideração de que os direitos da personalidade não são um valor "exclusivamente individual", mas que nele "há um mínimo intangível, que é igual para todas as pessoas". LÔBO, Paulo Luiz Neto. Direito civil... Op.cit., p 154.

[34] Ibidem, p. 154.

[35] GAMA, Guilherme Calmon Nogueira da; PEREIRA, Daniel Queiroz. Direitos da personalidade Código Civil de 2002. In: MENDES, Gilmar Ferreira; STOCO, Rui (Org.)*Doutrinas essenciais*: direito civil – parte geral – pessoas e domicílio. São Paulo: Revista dos Tribunais,

2011. v. 3, p. 321.

[36] O próprio uso da terminologia "autonomia privada", em substituição ao termo "autonomia da vontade", sinaliza a evolução de um direito privado mais intervencionista em contraposição a uma matriz individualista, própria dos códigos oitocentistas em que a autonomia do indivíduo era tratada como um dogma. Veja-se, entre outros: AMARAL, Francisco. Introdução... Op.cit., p 156; TEPEDINO, Gustavo. *Temas de Direito Civil*. Rio de Janeiro: Renovar, 2004. p. 2.

[37] "Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária".

[38] Para uma análise completa e crítica das limitações impostas pelo Código Civil à autonomia privad na seara dos direitos da personalidade, suscitando-se, inclusive, a inconstitucionalidade desse dirigismo jurídico da vida das pessoas, veja-se a obra de: BORGES, Roxana Cardos Brasileiro. Op.cit., p. 134-135.

[39] Ibidem, p. 114-127.

[40] SCHREIBER, Anderson. *Direitos da Personalidade*. São Paulo: Atlas, 2011. p. 26: "O art. 11 do Código Civil opta por uma resposta radical. Tomado em sua literatura, o dispositivo negaria qualquer efeito ao consentimento no campo dos direitos da personalidade (...) Daí a linguagem forte do Código Civil, que não pretendeu prejudicar a pessoa com um excessivo paternalismo estatal, mas protegê-la dos efeitos da sua própria vontade". E, arremata mais à frente (p. 29): "Por ora basta constatar que o art. 11 do Código Civil não deve ser interpretado de modo literal. A limitação voluntária ao exercício dos direitos da personalidade tem sido admitida pela comunidade jurídica em numerosas situações. Melhor seria, nesse sentido, que o legislador tivesse cuidado de especificar os parâmetros que devem seguir o controle da legitimidade de tais limitações, em especial: (i) o alcance, (ii) a duração, (iii) a intensidade e (iv) a finalidade da autolimitação".

[41] O grau da (i)licitude da limitação voluntária dos direitos da personalidade deveria ser encarado à luz das práticas socialmente admitidas: SCHREIBER, Anderson. *Direitos da*... Op.cit., p. 26.

[42] Alguns desses exemplos e outros, tais como a transfusão de sangue e pesquisa com seres humanos são citados por: CAPELO DE SOUSA, Rabindranath V. A. Op.cit., p. 408.

[43] A autonomia privada não deve ser equivalente ("unitária") para a tutela de interesses patrimoniais extrapatrimoniais. Tratando-se de situações "existenciais" – *v.g.*, direitos da personalidade, com maior rigor ser verificada a correspondência entre a autonomia privada e a unidade axiológica do ordenamento – a tutela da pessoa humana: PERLINGIERI, Pietro. Op.cit., p. 276-277: "Não possível um discurso unitário sobre a autonomia privada: a unidade é axiológica, porque unitário é o ordenamento centrado no valor da pessoa, mas é justamente essa conformação do ordenamento que impõe um tratamento diversificado para atos e atividades que em modo diferenciado tocam esse valor e regulamentam situações ora existenciais, ora patrimoniais, ora

umas e outras".

[44] ZANINI, Leonardo Estevam de Assis. Op.cit., p. 231-232. Veja-se, ainda, o Enunciado 4 da Jornada de Direito Civil: "Art. 11: O exercício dos direitos da personalidade pode sofrer limitação voluntária, desde que não seja permanente nem geral".

[45] LÔBO, Paulo Luiz Neto. Direitos da... Op.cit., p. 158.

[46] A noção de fruição já havia sido desenvolvida antes mesmo do Código Civil de 2002, pela qual o titular dos dados pessoais tinha o direito de usar e gozar dos direitos de personalidade: DE MATTIA, Fabio Maria. Direitos da personalidade. In: MENDES, Gilmar Ferreira; STOCO, Rui (Org.). *Coleção doutrinas essenciais*: direito civil – parte geral – pessoas e domicílio. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 258.

[47] MENDES, Laura Schertel. *Privacidade*... Op.cit., p. 124: "Dessa forma, percebe-se que a pergunt 'a quem pertencem os dados pessoais' é uma falsa questão. A natureza do bem protegido, a própria personalidade a que os dados pessoais se referem, exige que a proteção de dados pessoais seja compreendida não como um direito à propriedade, mas como uma espécie de direitos da personalidade (...) contra os riscos ocasionados pela coleta, processamento e circulação dos dados pessoais".

[48] Para tal debate travado no direito estadunidense e no direito europeu, veja-se, respectivamente: Schwartz. Paul M. Property, privacy, and personal data. *Harvard Law Review*, v. 117, n. 7, p. 2055-2128, May 2004; PURTOVA, Property in... Op.cit., p. 185-210.

[49] BORGES, Roxana. *Direitos da*... Op.cit., p. 120: "Na verdade, o direito de personalidade, em si, não é disponível *stricto sensu*, ou seja: não é transmissível nem renunciável. A titularidade do direito não é objeto de transmissão. Ou seja: a imagem não se separa do seu titular original, assim como a sua intimidade. A imagem não se separa do seu titular original, assim como a sua intimidade. A imagem continuará sendo daquele sujeito, sendo impossível juridicamente – e até fisicamente – sua transmissão a outrem ou, mesmo, sua renúncia. Mas expressões do uso de direito da personalidade podem ser cedidas, de forma limitada, com especificações quanto à duração da cessão e quanto à finalidade do uso. Há, portanto, certa esfera de disponibilidade em alguns direitos da personalidade. O exercício de alguns direitos da personalidade pode, sim, sofrer limitação voluntária, mas essa limitação também é relativa".

[50] Usando tal expressão: DINIZ, Maria Helena. Comentários à Parte Geral – artigos 1º ao 232 d Código Civil. In: SILVA, Regina Beatriz Tavares da (Coord.).*Código Civil comentado*. São Paulo: Saraiva, 2012. p. 102.

[51] Ibidem, p. 120. No mesmo sentido: ZANINI, Leonardo Estevam de Assis. Op.cit., p. 235.

[52] GARCIA, Maria. Os sentidos da liberdade. In: MENDES, Gilmar Ferreira; STOCO, Rui (Org *Doutrinas essenciais*: direito civil – parte geral – pessoas e domicílio. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 559.

[53] Na década de 1990 na região metropolitana de Paris, casas noturnas e de entretenimento ofertavam aos seus clientes, como prática de lazer, o arremesso de anões. Após a proibição de tal prática pelo prefeito da cidade sob o argumento de violação à dignidade da pessoa humana, um dos donos dessas casas de entretenimento e um dos próprios anões recorreram ao Tribunal Administrativo para garantir tal prática sob o argumento de que ela não violava a dignidade da pessoa humana. Ao revés, garantiria a dignidade dos anões por lhes prover o seu sustento. O caso chegou à Corte de Direitos Humanos da Organização das Nações Unidas, tendo sido mantida a proibição da prática de arremesso de anões. Veja-se, entre outros, a correlação desse caso com os direitos da personalidade por: SCHREIBER, Anderson*Direitos*... Op.cit., p. 1-2. A decisão da Corte de Direitos Humanos da ONU pode ser encontrada em <http://www.equalrightstrust.org/ertdocumentbank/Microsoft%20Word%20-%20Manuel%20Wackenheim%20v.%20Fr.pdf>.

[54] Noticia-se, regularmente, que alguns atletas e demais celebridades têm contrato vitalício de cessão de imagem e nome com determinadas marcas. Por impor uma limitação permanente aos direitos da personalidade, tal prática seria um exemplo de extrapolação ao poder de disponibilidade relativo aos direitos da personalidade. TARTUCE, Flávio.*Direito civil*: lei de introdução e parte geral. Rio de Janeiro: Forense, 2012. p. 154-155.

[55] Por uma tradução literal do termo, trata-se da prática de utilizar o corpo como um espaço/plataforma para a exposição de uma arte. Desde tatuagens espalhadas por toda a extensão corporal até os casos em que pessoas, motivadas pelo desejo de ter uma aparência animal, procedem com intervenções cirúrgicas para alcançar tal transfiguração artística. Veja-se, entre outros: SCHEREIBER, Anderson*Direitos*... Op.cit., p. 35-37. E a obra de: TEIXEIRA, Ana Carolina Brochado. *Saúde, corpo e autonomia privada*. Rio de Janeiro: Renovar, 2010.

[56] Recorrentes são os casos em que testemunhas de jeová não aceitam, por suas convicções religiosas receber transfusão de sangue. Contudo, em muitos casos, esse é o único tipo de intervenção médica eficaz. Dá-se, então, o conflito entre a autodeterminação do titular dos direitos da personalidade e a sua disponibilidade relativa, estando em jogo o próprio direito à vida. Nos casos em que há iminente perigo de morte, o Conselho Regional Federal de Medicina – Resolução 1.021/1980 – orienta os médicos a proceder com a intervenção independentemente do consentimento do interessado: "CONCLUSÃO. Em caso de haver recusa em permitir a transfusão de sangue, o médico, obedecendo a seu Código de Ética Médica, deverá observar a seguinte conduta: 1º – Se não houver iminente perigo de vida, o médico respeitará a vontade do paciente ou de seus responsáveis. 2º – Se houver iminente perigo de vida, o médico praticará a transfusão de sangue, independentemente de consentimento do paciente ou de seus responsáveis". Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/1980/1021_1980.htm>.

[57] Veja-se, por exemplo, a divergência doutrinária sobre a legalidade da limitação ao direito à

privacidade nos programas de *reality show*: MORATO, Antonio Carlos; CASSEB, Paulo Adib REBELLO, Deise Carolina Muniz. A sociedade da informação e os "reality shows". In PAESANI, Liliana Minardi (Coord.).*O Direito na Sociedade da Informação II*. São Paulo: Atlas, 2009. p. 167-190; BORGES, Roxana. *Direitos da*... Op.cit., p. 166-167.

58 VASCONCELOS, Pedro de Pais. *Direitos da*... Op.cit., p. 153.

59 A mesma retórica foi utilizada por: LÔBO, Paulo Luiz Neto... Op.cit., p. 156: "As empresa utilizam-se de programas invasores, que coletam informações sobre as pessoas, para induzi-las ao consumo de seus produtos e serviços, muitas vezes com a colaboração dos indivíduos que prestem informações aparentemente inofensivas sobre dados que integram a intimidade e vida privada. Até que ponto a proteção jurídica da privacidade, máxime o estímulo de autolimitação, pode ser exequível na sociedade da informação".

60 DONEDA, Danilo. *Da privacidade*... Op.cit. p. 372: "Em um sistema de índole patrimonialista, o consentimento assumirá uma função predominantemente legitimadora, ao servir como instrumento para colocar os dados pessoais no mercado e proporcionar, se levarmos ao extremo, a chamada *commodification* dos dados pessoais". E, arremata mais à frente (p. 378): "Este exercício manifesta-se, menos no momento do consentimento em si – se assim fosse, ele teria o feito de transmudar a informação pessoal em um bem jurídico –, do que na possibilidade de concedê-lo ou negá-lo, e reside exatamente nesse porque que, caso limitado pela estrutura negocial, perderia a sua razão de ser".

61 A expressão "armadilha da autonomia", ao abordar criticamente a privacidade informacional com o relato singular do indivíduo controlar seus dados pessoais, é de: SCHWARTZ, Paul. Privacy and... Op.cit., p. 1660.

62 A expressão território informacional destrutivo é do mesmo autor: Ibidem, p. 1655.

63 COHEN, Julie. Examined... Op.cit., p. 1377.

64 Ibidem, p. 1394.

65 SOLOVE. Understanding... Op.cit., p. 98.

66 DONEDA, Danilo. Internet e legislação. In: IV FÓRUM DA INTERNET DO BRA REALIZADO PELO COMITÊ GESTOR DA INTERNET/CGI. São Paulo, 25 abr. 2014.

67 Art. 7º, II e III: "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...) II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial".

68 Art. 5º, XII: "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

[69] Anota-se a controvérsia se a proteção constitucional alcançaria somente os dados em fluxo ou também os dados armazenados. Até o momento, tem prevalecido – jurisprudencialmente – a interpretação mais restritiva – dados em fluxo –, ainda que o texto constitucional não tenha estabelecido tal distinção. As novas disposições do MCI podem reabrir tal discussão, a fim de que o mandamento constitucional cumpra o objetivo de garantir o sigilo das comunicações, estejam elas armazenadas ou em fluxo. AZEREDO, João Fábio A. Sigilo das comunicaçõe eletrônicas diante do marco civil da internet. In: DE LUCCA, Newton; SIMÃO FILH Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.)*Direito & Internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. t. II, p. 230: "Nos parece claro, portanto, que a promulgação do Marco Civil da Internet reforça a necessidade de se reabrir o debate nos tribunais sobre a interpretação do inciso XII, do art. 5º, da Constituição Federal, reconhecendo-se a proteção que esse confere às comunicações privadas armazenadas (*sic*)".

[70] FERRAZ JÚNIOR, Tércio Sampaio. Op.cit., p. 446: "Obviamente o que se regula é comunicaçã por correspondência e telegrafia, comunicação de dados e telefonia. O que fere a liberdade de omitir pensamento é, pois, entrar na comunicação alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro".

[71] Vide os supracitados dispositivos constitucional e infraconstitucional.

[72] SEM, A. Fulya. Communication and human rights. *Social and Behavioral Sciences Review*, n. 174 p. 2815, 2015.

[73] "Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que: I – impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet".

[74] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Op.cit. p. 293: "A quebra confidencialidade da comunicação significa frustrar o direito do emissário de escolher o destinatário do conteúdo da sua comunicação".

[75] Utiliza-se o verbo "sedimentar", pois já havia essa discussão com base na aplicação dos dispositivos constitucionais acima mencionados.

[76] Art. 13, *caput*, do MCI: "Art. 13 Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento".

[77] Art. 15, *caput*, do MCI: "O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento".

[78] Art. 5, VI, do MCI: "registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados".

[79] AMADEU, Sérgio. Marco civil e a proteção da privacidade: após polêmica sobre espionagem proteção virtual se tornou um dos três pilares do marco civil. Disponível em: <http://www.dicyt.com/noticia/marco-civil-e-a-protecao-da-privacidade> (sem paginação): "Para abrir uma página da web ou para receber nossos e-mails, para baixar um arquivo, os dados são enviados para o endereço IP que nossa máquina está utilizando ao se conectar na internet. Quando fazemos o login na rede, pegamos um número IP, e quando saímos da conexão, fazemos o logout. O registro de conexão é o 'conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados'".

[80] LEMOS, Ronaldo.*Direito, tecnologia e cultura*. Rio de Janeiro: Editora FGV, 2005. p. 16: "A estrutura física da internet é constituída pelo conjunto de computadores que a compõem e pelos meios físicos que os interconectam, como fibras óticas, linhas telefônicas, ondas de rádio etc. A estrutura lógica da internet ou o seu 'código' são as inúmeras linguagens que fazem com que as partes físicas possam comunicar-se entre si. Nesta camada, estão incluídos não só os programas de computador, como também protocolos e linguagens compartilhadas entre eles (como o protocolo TCP/IP, base da inter net). Aqui se incluem também os sistemas operacionais, como o sistema Microsoft Windows ou o Linux".

[81] Art. 5º, VIII, do MCI: "registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP".

[82] LEMOS, Direito... Op.cit., p. 16: "A estrutura de conteúdo corresponde a tudo aquilo que é transmitido sobre as camadas física e lógica, como um texto, um e-mail, uma música, um filme, uma mensagem, uma fotografia etc.".

[83] AMADEU, Sérgio. Op.cit., sem paginação.

[84] Dados cadastrais dizem respeito à qualificação pessoal, filiação e endereço de acordo com art. 10 § 3º, do MCI.

[85] Para uma análise detida dos ditames processuais a respeito do acesso aos logs de conexão e aplicação, veja-se: LEONARDI, Marcel. Responsabilidade... Op.cit., p. 206-211. E, ainda, intervenção de: CRUZ, Francisco Brito. In: SEMINÁRIO MARCO CIVIL DA INTERN obrigatoriedade de Guarda de Registros, Medidas de Segurança e Encriptação. Evento realizado pela Protest. Disponível em: <https://www.youtube.com/watch?v=cwQD0QpLSW4>.

[86] Juntamente com o direito à privacidade, invoca-se o princípio constitucional da presunção de inocência. Na medida em que se retêm dados de forma indiscriminada para posterior persecução

criminal, presume-se que todos são, *a priori*, potenciais criminosos, violando-se, assim, tais preceitos constitucionais. Veja-se, ainda, a discussão travada no direito europeu em que a Corte de Justiça da União Europeia declarou a invalidade da diretiva da retenção de dados por ser uma "*serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary*". Disponível em: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>.

87 "Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet".

88 Veja-se, nesse sentido, o relatório final do então projeto de lei do MCI por seu deputado-relator: MOLON, Alessandro. Relatório ao projeto de Lei n. 2.126/2011, p. 41. Disponível em <http://www.camara.gov.br/internet/agencia/pdf/MCI_2014_02_12_Relatorio.doc>: "No atual artigo 15 (antigo artigo 12), optamos por deixar claro que esta Subseção II trata da guarda de registros de acesso a aplicações de Internet 'na provisão de conexão', tornando claro que aos provedores de conexão é vedada a guarda dos registros de acesso a aplicações de Internet. Essa vedação é justificável pelo fato de os provedores de conexão possuírem o cadastro completo de seus usuários, tais como identidade, filiação, endereço, registro de pessoa física (RG) e cadastro de pessoa física (CPF), *além de os mesmos provedores de conexão terem acesso à integralidade da navegação dos usuários da Internet*, em todas as aplicações que rodam em seus cabos, tais como e-mails, chat, redes sociais (como Facebook), micro blogs (como Twitter), aplicativos de Voz sobre IP (como Skype), e assim por diante, *o que potencializa ao máximo a invasão da privacidade dos usuários*. (...) *Portanto, a guarda dos registros de acesso a aplicações de Internet, se realizada pelos provedores de conexão, colocaria em risco a privacidade dos usuários, vez que o monitoramento seria completo e da integralidade da navegação dos usuários*" (grifos).

89 AMADEU, Sérgio. Marco civil... Op.cit., sem paginação: "O Marco Civil, no seu artigo 14, proíb que um provedor de conexão, em geral, uma empresa de telefonia, guarde as informações sobre a navegação dos seus clientes. Com isso, a lei quer evitar uma situação de completa quebra de privacidade, pois só podemos navegar na rede a partir de uma conexão fornecida por uma operadora de telecomunicações. Todos os cliques que damos, todo site que visitamos, todo e-mail que enviamos ou recebemos, todas as buscas que fazemos, todas as compras e conversas que realizamos passam pelos cabos e fibras das empresas de telecom, provedoras de nossa conexão à internet. Para evitar que elas tenham todas as informações sobre nossa vida digital, o Marco Civil proibiu que o provedor de conexão armazene nossos dados de navegação".

90 "Art. 166. É nulo o negócio jurídico quando: (...) VI – tiver por objetivo fraudar lei imperativa".

91 Vale ressaltar que essa passagem do voto do Min. Rel. Paulo Sanseverino na ARE 867.326 RG/S

é uma citação da obra de BESSA, Leonardo Roscoe. Op.cit., p. 93.

[92] Nesse sentido, a Súmula 550 procurou assegurar que houvesse transparência no uso de informaçõe pessoais para fins de avaliação de crédito: "A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo".

[93] BESSA, Leonardo Roscoe. Op.cit., p. 97.

[94] Veja-se, entre outros a obra organizada por: LYON, David. *Surveillance as Social Sorting*: Privacy, risk, and digital discrimination. London: Routledge, 2003.

[95] Veja-se o sistema de *credit scoring* que foi analisado pelo STJ (Recurso Especial n. 1.419.697 - Relator Paulo de Tarso Sanseverino).

[96] Veja-se o caso da companhia de seguros que pode prever quando seu cliente ficará doente: Disponível em: <http://khn.org/news/insurer-uses-patients-personal-data-to-predict-who-will-get-sick/>.

[97] Veja-se a suposta parceria firmada entre Facebook e Serasa que possibilita a segmentação de anúncios publicitários de acordo com a renda de seus usuários: JÚNIOR, Hilário. Facebook Serasa fecham parceria para anúncios segmentados por renda. Disponível em: <https://www.linkedin.com/pulse/facebook-e-serasa-fecham-parceria-para-anuncios-por-renda-junior>.

[98] BIONI, Bruno R.; MONTEIRO, Renato Leite. Que tal... Op.cit. (sem paginação): "Todavia, est decisões e conclusões podem afetar inadvertidamente a vida das pessoas. Imagine ser negado um plano de saúde devido a mera possibilidade de ficar doente; ou um financiamento devido a sua classe social; ser ofertado um preço superior em razão da sua capacidade financeira de pagar mais pelo mesmo serviço (prática conhecida como '*price discrimination*'); um emprego devido às suas preferências e notícias que compartilha na sua rede social; ou até mesmo ser suspeito de práticas criminosas simplesmente porque existe uma maior chance das pessoas que residem no seu bairro praticarem ilícitos. *Os nossos dados pessoais redimensionam, portanto, a autonomia e o livre desenvolvimento da personalidade de cada um de nós. Não se trata de um elemento fantasmagórico de um futuro cinematográfico, trata-se de uma situação real que perfilha nossas vidas*" (grifos).

[99] Tal escolha justifica-se em razão do papel de liderança continental que o Conselho da Europa/Co exerce na agenda de direitos humanos. Além de ter uma composição de maior abrangência do que a União Europeia, o CoE tem como seu objetivo central a promoção dos direitos fundamentais cobrindo-se as suas mais variadas frentes. Nesse sentido, além de conter um comitê de proteção de dados pessoais, o CoE conta com um comitê sobre bioética, o que permitiu um avanço consistente na emissão de recomendações e convenções sobre a proteção de dados pessoais na

área de saúde, especialmente no que diz respeito a dados genéticos. Vejam-se os portais do CoE e do Comitê de Proteção de Dados Pessoais e de Bioética, respectivamente <http://www.coe.int/en/web/portal/home>; <http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp>; <http://www.coe.int/en/web/bioethics/home>.

[100] Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent documentId=0900001680078b37>.

[101] Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent documentId=090000168007cf98>.

[102] "Tests which are predictive of genetic diseases or which serve either to identify the subject as a carrier of a gene responsible for a disease or to detect a genetic predisposition or susceptibility to a disease may be performed only for health purposes or for scientific research linked to health purposes, and subject to appropriate genetic counselling".

[103] "(1) Any form of discrimination against a person, either as an individual or as a member of a grou on grounds of his or her genetic heritage is prohibited; (2) Appropriate measures shall be taken in order to prevent stigmatisation of persons or groups in relation to genetic characteristics".

[104] FRANCO, Vera Helena de Melo. Citar Vela Helena Mero de Franco*Contratos*: direito civil e empresarial. São Paulo: Revista dos Tribunais, 2012. p. 292-293.

[105] Ibidem, p. 294.

[106] CUNHA, Mario Viola de Azevedo. Data Protection and Insurance: The Limits on the Collectic and Use of Personal Data on Insurance Contracts in EU Law. *Global Jurist*, v. 10, p. 1, 2010.

[107] Disponível em: <https://wcd.coe.int/com.instranet.InstraServlet? command=com.instranet.CmdBlobGet&InstranetImage=573883&SecMode=1&DocId=601492&U

[108] "Insurers should not have the right to require genetic testing or to enquire about results of previously performed tests, as a pre-condition for the conclusion or modification of an insurance contract".

[109] É, justamente, por conta de tal precarização, que o adjetivo "suplementar" é colocado em xeque por tal realidade social.

[110] Veja-se, por exemplo, que o próprio CoE está redigindo uma nova recomendação sobre o tratamento de dados genéticos para fins securitários. Não há, portanto, posições claras e sedimentadas, o que, no entanto, não é prejudicial, mas, pelo contrário, fomenta o debate sobre a investigação dos limites do fluxo das informações pessoais, esbarrando-se ou não em proibições para certos tipos de tratamento de dados pessoais. Veja-se a recomendação sob consulta disponível em: <http://www.coe.int/t/dg3/healthbioethic/Source/Final%20E%20consult%20doc.pdf>.

[111] Veja-se a nota de esclarecimento da empresa, disponível em: <https://googleblog.blogspot.fr/2012/01/updating-our-privacy-policies-and-terms.html>.

[112] Por exemplo, na Europa ainda está em curso uma ação coordenada de diversas autoridades de garantia de proteção de dados pessoais que multaram e estão a multar, sistematicamente, a Google: EU privacy watchdogs give Google guidelines to change privacy practices. Disponível em: <http://www.euractiv.com/sections/infosociety/eu-privacy-watchdogs-give-google-guidelines-change-privacy-practices-308740>.

[113] Na época, o então Departamento de Proteção e Defesa do Consumidor do Ministério da Justiça notificou a Google a prestar esclarecimentos: Disponível em: <http://economia.estadao.com.br/noticias/negocios,google-diz-que-respondera-formalmente-a-justica-e-que-nao-vendera-dados,105421>.

[114] Veja-se a afirmação do advogado do Instituto de Defesa do Consumidor/IDEC em audiência pública realizada na Câmara dos Deputados: "Na audiência, o advogado do Instituto de Defesa do Consumidor (Idec), Guilherme Varella, afirmou que, com essa política, o Google pode estar criando sistema de monitoramento constante da navegação dos consumidores, identificando o seu comportamento, preferências e atitudes na internet (...). A unificação das políticas de privacidade dos mais de 60 serviços da empresa significa a possibilidade de cruzamento dos dados do consumidor", disse. Disponível em: <http://www2.camara.leg.br/camaranoticias/noticias/CONSUMIDOR/414412-DEBATEDORES-CRITICAM-NOVA-POLITICA-DE-PRIVACIDADE-DO-GOOGLE.html>.

[115] Vejam-se, por exemplo, as preocupações externadas pelo Privacy Commissioner do Reino Unido: Google's privacy policy 'too vague'. Disponível em: <http://www.theguardian.com/technology/2012/mar/08/google-privacy-policy-too-vague>.

[116] KRAMERA, Adam D. I.; GUILLORYB, Jamie E.; HANCOCKB, Jeffrey T. Experimental evidence of massive-scale emotional contagion through social networks. *PNAS Review*, v. 111, n. 29. p. 8788-8790, July 2014, Disponível em: <http://www.pnas.org/content/111/24/8788.full.pdf>.

[117] Ibidem, p. 8788: "we test whether emotional contagion occurs outside of in-person interaction between individuals by reducing the amount of emotional content in the News Feed. When positive expressions were reduced, people produced fewer positive posts and more negative posts; when negative expressions were reduced, the opposite pattern occurred. These results indicate that emotions expressed by others on Facebook influence our own emotions, constituting experimental evidence for massive-scale contagion via social networks".

[118] Ibidem, p. 10779: "Questions have been raised about the principles of informed consent and opportunity to opt out in connection with the research in this paper. The authors noted in their paper, "[The work] was consistent with Facebook's Data Use Policy, to which all users agree prior to creating an account on Facebook, constituting informed consent for this research".

[119] DEWEY, Caitlin. 9 answers about Facebook's creepy emotional-manipulation experiment. Disponível em: <https://www.washingtonpost.com/news/the-intersect/wp/2014/07/01/9-answers-about-facebooks-creepy-emotional-manipulation-experiment/>.

[120] CONSTINE, Josh. Facebook is forcing all users to download messenger by ripping chat out of it main apps. Disponível em: <http://techcrunch.com/2014/04/09/facebook-messenger-or-the-highway/>.

[121] CHOWDHRY, See Amit. Why Facebook forced users to download a separate messenger app Disponível em: <http://www.forbes.com/sites/amitchowdhry/2014/11/11/why-facebook-forced-users-to-download-a-separate-messenger-app/>.

[122] Veja-se: HAYASHI, Eduardo Issao. 10 termos de uso do Facebook Messenger que vão deixa você boquiaberto. Disponível em: <http://www.tecmundo.com.br/facebook/60271-10-termos-uso-facebook-messenger-deixar-voce-boquiaberto.htm>.

[123] FIORELLA, Sam. The insidiousness of Facebook Messenger's android mobile app permission Disponível em: <http://www.huffingtonpost.com/sam-fiorella/the-insidiousness-of-face_b_4365645.html?utm_hp_ref=tw>.

[124] FILOMENO, Leonardo. 10 termos absurdos de uso do Messenger do Facebook. Disponível en <http://manualdohomemmoderno.com.br/tecnologia/10-absurdos-termos-de-uso-messenger-facebook>.

[125] Disponível em: <http://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy>.

[126] LOMAS, Natasha. Samsung Edits Orwellian Clause Out Of TV Privacy Policy. Disponível en <http://techcrunch.com/2015/02/10/smarttv-privacy/#.bbciupd:yfMB>.

[127] Disponível em: <http://news.samsung.com/global/samsung-smart-tvs-do-not-monitor-living-room-conversations>.

[128] Veja-se que não há mais cláusula com tal redação: <https://www.samsung.com/uk/info/privacy-SmartTV.html>. A versão em português está disponível em: <http://www.samsung.com/br/info/privacy.html>.

[129] Disponível em: <https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf>.

[130] COUNCIL OF EUROPE, *Handbook*... Op.cit., p. 68: "The processing of personal data for undefined and/or unlimited purposes is unlawful. Every new purpose for processing data must have its own particular legal basis and cannot rely on the fact that the data were initially acquired or processed for another legitimate purpose. In turn, legitimate processing is limited to its initially specified purpose and any new purpose of processing will require a separate new legal basis". Nesse mesmo sentido: KUNER, Cristopher. *European*... Op.cit., p. 99-100.

[131] CATE, Fred. The failure... Op.cit. p. 348.

[132] DONEDA, Danilo. Princípios... Op.cit., p. 378: "De acordo com o princípio da finalidade, motivo da coleta ou fornecimento de um dado deve ser compatível com o objetivo final do tratamento ao qual este dado será submetido (...) Cria-se, desta forma, uma ligação entre a informação e a sua origem, vinculando-a ao fim de sua coleta, o modo que esta deverá ser levada em consideração em qualquer tratamento ulterior (...) Antes de ser meramente abstrata sujeita à livre disposição, esta informação, à medida que identifica alguma característica de uma pessoa, permanece sempre vinculada a ela, e sua utilização, pode refletir diretamente para o seu titular (...) No caso específico, através do princípio da finalidade, é possível estabelecer um mecanismo que evite a chamada utilização secundária da informação ? pessoa à revelia de seu titular. Este princípio é tanto mais importante ao se levar em conta que, quebrando-se o vínculo entre o consentimento de uso dos dados pessoais para um fim específico, estar-se-ia abrindo a possibilidade para qualquer uso secundário da informação pessoal e, por consequência, tornando inócuos outros meios secundários de proteção e controle desta informação por parte de seu titular".

[133] Essa é inclusive a interpretação extraída dos princípios da Especificação dos propósitos (*Purpos Specification Principle*) e Limitação do uso (*Use Limitation Principle*) das *guidelines* da OECD.

[134] Article 29 Data Protection Working Party. *Opinion 3/2013 on Purpose Limitation*. Disponível en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. p. 3: "Further, to provide more legal certainty, the WP29 recommends that legislators adopt the above list of relevant factors in order to assess compatibility. Although this presentation of key factors is not fully exhaustive, it attempts to highlight the most typical factors that may be considered in a balanced approach: neither too general so as to be meaningless, nor too specific so as to be overly rigid".

[135] RODOTÁ, Stefano. Op.cit. p. 17: "um tipo de proteção dinâmica, que segue o dado em todos os seus movimentos".

[136] Essa foi uma tensão presente na consulta pública do PL 5.276/2016, principalmente pelo lado do setor empresarial. Vejam-se, por exemplo, aquelas contribuições que advogaram pela substituição do adjetivo "expresso" por "inequívoco" para abrir espaço para uma espécie de consentimento tácito que cobriria a hipótese de tratamento para fins secundários, evitando-se a fadiga do consumidor. De acordo com nosso mapeamento, verificamos os seguintes atores sustentando tal tese: Mariana Cunha e Melo, Claro, Centre for Information Policy Leadership, ITI, Febraban, CNI, Marlon, BSA The Software Alliance, ITS, US Business Council, FIESP, Ia Associação Brasileira de Internet, Boa Vista Serviços. Esse mapeamento foi feito pelo Centro d Pesquisa Independente InternetLab: ANTONIALLI, Dennys Marcelo; BIONI, Bruno Ricar CRUZ, Francisco Brito; KIRA, Beatriz; MARCHEZAN, Jonas Coelho; SANTOS, Maike W

NAKAGAWA, Fabiane Midori S.*O que está em jogo no Debate Público Proteção de Dados Pessoais?* São Paulo: [s.n.], 2016.

137 Veja-se, por todos, o ensaio reflexivo crítico da dinâmica normativa da autodeterminação informacional frente aos desafios do Big Data: CATE, Fred H.; MAYER-SCHONBERGE, Viktor Notice and consent in a world of Big Data. *International Data Privacy Law*, v. 3, n. 2, p. 71-73, 2013.

138 MAYER-SCHONEBERGER, *Big Data*... Op.cit., p. 153: "Strikingly, in a big-data age, most innovative secondary uses haven't been imagined when the data is first collected. How can companies provide notice for a purpose that has yet to exist? How can individuals give informed to an unknown? (...)".

139 NISSENBAUM; BAROCAS. Big data... Op.cit., p. 60.

140 Registre-se que, via de regra, há uma série de exceções à regra do consentimento, tal como para procedimentos contratuais, para tutela da vida, fins estatísticos e de pesquisa, interesse público etc. (vide *e.g.*, as alíneas do art. 7 da Diretiva da União Europeia). Tais exceções não são, contudo, tão vagas, a fim de ser uma hipótese guarda-chuva que pode tornar a regra do consentimento em exceção, tal como são os interesses legítimos ou consentimento tácito. Daí por que a sua importância frente à autodeterminação informacional, pois ela pode esvaziar a regra do consentimento.

141 Veja-se o art. 6(f) da GDPR, que corresponde ao art. 7(a) da antiga Diretiva da União Europeia, c quais serão analisados mais à frente.

142 Art. 4.3.6: "The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney)".

143 Veja-se, entre outros, o resumo dessa tensão normativa por: BELLAMY, Bojana; HEYDER Markus. Empowering... Op.cit., sem paginação: "Third, and perhaps most importantly, are other mechanisms in our ever-growing privacy toolkit and existing legal regimes that, in the appropriate contexts, are able to deliver privacy protection and meaningful control more effectively than consent. However, while these alternative mechanisms already exist, they must be better understood, further developed and more broadly accepted. Policy-makers and lawmakers, as well as privacy regulators, should be shifting a significant portion of their attention from consent to these other mechanisms and safeguards. And organizations, in turn, must be prepared to embrace such alternative and innovative ways to deliver privacy and empowerment to individuals. Of course, there will always be situations where freely given and specific consent will be appropriate and the only way to use people's information".

[144] NISSENBAUM, Helen. *Privacy in*... Op.cit. p. 164.

[145] Ibidem, p. 161: "Contextual integrity, as it has been described thus far, is inherently conservative, flagging as problematic any departure from entrenched practice".

[146] Ibidem, p. 164: "In recognition of this presumption, if a new practice breaches entrenched informational norms, I will say that there has been a prima facie violation of contextual integrity. At the same time, if a way can be found to demonstrate the moral superiority of new practices, this presumption could be overcome and what was recognized as a prima facie violation may be accepted as morally legitimate".

[147] Ibidem, p. 166: "The challenge to contextual integrity, as it is to any conservative theory for which moral legitimacy is important, is how show to allow for at least some departures from entrenched normative practice. The approach I recommend here is to compare entrenched normative practices against novel alternatives or competing practices on the basis of how effective each is in supporting, achieving, or promoting relevant contextual values".

[148] MACEDO JÚNIOR, Ronaldo Porto. Interpretação da boa-fé nos contratos brasileiros: princípios jurídicos em uma abordagem relacional (contra a euforia principiológica). In: MACEDO JÚNIOR, Ronaldo Porto; BARBIERI, Catarina Helena Cortada (Org.). *Direito e interpretação*: racionalidades e instituições. São Paulo: Saraiva, 2011. p. 314.

[149] MARQUES. *Contratos*... Op.cit., p. 96-103.

[150] Ibidem, p. 315.

[151] MACEDO JÚNIOR, Ronaldo Porto. Interpretação... Op.cit., p. 314.

[152] MARQUES, Cláudia Lima. *Contratos*... Op.cit., p. 107.

[153] MACEDO JÚNIOR, Ronaldo Porto. *Contratos relacionais e defesa do consumidor*. São Paulo: Revista dos Tribunais, 2007. p. 168: "No limite ideal, tornar presente o futuro cem por cento predeterminado no presente (...) Nesse sentido, nos contratos relacionais as partes reconhecem os limites para se presentificar o futuro e deixam de pretender tão intensamente fazer isto, tal como se configurava o ideal do pensamento contratual clássico".

[154] MARQUES, Cláudia Lima. *Contratos*... Op.cit., p. 100.

[155] Ibidem, p. 105: "O objeto principal desses contratos muitas vezes é um evento futuro".

[156] MACEDO JÚNIOR, Ronaldo Porto. *Contratos*... Op.cit., p. 100: "Esta alteração restringe muito a extensão que a teoria clássica conferia ao princípio do mútuo consentimento relativizando-o e diminuindo-lhe a importância. Isto porque agora, ante o enfraquecimento do formalismo, o consentimento expresso e inequívoco não mais precisa ser dado a todas as cláusulas, inclusive alguns termos adicionais, mas tão somente aos elementos essenciais do contrato".

[157] Ibidem, p. 313: "Contratos relacionais, numa breve e provisória definição, são contratos que se aperfeiçoam em uma relação complexa, onde elementos contratuais não vinculantes relacionados

com o contexto são levados em consideração para os motivos de sua constituição".

158 MACEDO JÚNIOR, Ronaldo Porto. *Contratos*... Op.cit., p. 103: "Em terceiro lugar, em substituição aos termos de ajustamento, os contratos relacionais incluem termos estabelecendo processos institucionais pelos quais os termos de troca e ajuste serão especificados no curso da performance ou cumprimento contratual".

159 MARQUES, Cláudia Lima. *Contratos*... Op.cit., p. 105.

160 Ibidem, p. 99.

161 Ibidem, p. 105.

162 Ibidem, p. 326: "(...) considera a questão do consentimento em uma relação como 'consenso acerc da relação', o que não é o mesmo que o consenso acerca de todos os termos do contrato (na medida em que é impossível pontuar todos os elementos no presente)".

163 Veja-se que o PL/EXE usa a terminologia "características" para impor a obrigação de informaçã aos titulares dos dados pessoais, quando o tratamento de seus dados for contínuo (art. 8, § 3º): "Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado periodicamente sobre as principais características do tratamento, nos termos definidos pelo órgão competente".

164 Ibidem 321: "Macneil, ao descrever estes fundamentos, descreve a existência de dez normas: (1) papel da integridade (comportar-se de acordo com seu papel dentro de uma relação contratual e administrar os conflitos) (...)".

165 Estabelecendo tal correlação de forma expressa, veja-se: MARQUES, Cláudia Lima. *Contratos*... Op.cit., p. 282.

166 Apesar de confiança ter correlação com a faceta objetiva e subjetiva do princípio da boa-fé, já tendo sido dito que ela exerceria uma "ponte" entre eles (MENEZES CORDEIRO, António. *Da boa fé*... Op.cit., p. 1238), a boa-fé objetiva tem uma conexão histórica e etimológica maior (LISBOA, Roberto Senise. *Confiança contratual*. São Paulo: Atlas, 2012. p. 143), de modo que as considerações a serem tecidas focarão na correlação entre os princípios da boa-fé objetiva e da confiança.

167 Veja-se, por exemplo, o trabalho já citado de MARTINS-COSTA, Judith. *A boa-fé*... Op.cit. Em termos de direito comparado, a obra seminal de MENEZES CORDEIRO, António. *Da boa fé*... Op.cit.

168 Essa é a conclusão da obra de: LISBOA, Roberto Senise. *Confiança contratual*. São Paulo: Atlas 2012. p. 151.

169 Nesse sentido, o art. 422 do Código Civil coloca ao lado da boa-fé a probidade: "Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé".

[170] Veja-se, por exemplo, a correlação das figuras parcelares da boa-fé (*supressio, surrectio, excpetio doli, tu toque*) à tutela da confiança feita por: SCHEREIBER, Anderson. A proibição de comportamento contraditório: tutela da confiança e *venire contra factum proprium*. Rio de Janeiro: Renovar, 2015. p. 123-187.

[171] LISBOA, Roberto Senise. *Confiança*... Op.cit., p. 149.

[172] MENEZES CORDEIRO, António. *Da boa fé*... Op.cit., p. 1242.

[173] Ao analisar o instituto do abuso de direito, considerando como algo que limita um direito subjetiv (i.e. uma posição jurídica), veja-se por todos: CORDEIRO, Antonio Menezes de. Da boa-fé. Op.cit., p. 662-670.

[174] O instituto do abuso de direito tem rendido amplas e complexas análises, de modo que esse subcapítulo está longe de estudá-lo de forma detida. Nesse sentido, mesmo para aqueles que, monograficamente, fizeram uma radiografia a seu respeito em mais de 600 (seiscentas) páginas, o estudo não passou de uma "mera tentativa de reflexão". Essas são as palavras de: CUNHA DE SÁ, Fernando Augusto. *Abuso de Direito.* Almedina: Lisboa, 2005, p. 15.

[175] Artigo 187 do Código Civil: "Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes".

[176] Assim se referiu o. jurista Josserand apud THEODORO JUNIOR, Humberto. *Comentários ao novo código civil*. Rio de Janeiro: Forense, 2003. p. 112.

[177] THEODORO JUNIOR, Humberto. *Comentários ao novo Código Civil*. Rio de Janeiro: Forense, 2003. p. 112.

[178] MANTELERO, Alessandro. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. Computer Law & Security Review 34 (2018), p. 756: "In this scenario, there is a clear tension between the increasing demand for ethically and socially oriented data use from citizens, companies, developers and computer scientists, on the one hand, and the lack of a regulatory framework to address these issues, on the other. Although this gap is partially filled by a variety of bottom-up initiatives, corporate guidance or ongoing public investigations, the main limitations of these initiatives concern the variety of values, approaches and models adopted".

[179] Essa virada no debate regulatório tem ressoado, inclusive, no Conselho da Europa. Tem-se defendido a adoção de abordagens regulatórias baseadas em valores (values-based approach) sociais e éticos, pois, ao contrário da adoção de normas rígidas e específicas, levam em consideração as peculiaridades locais nas discussões regulatórias – algo especialmente importante no caso de tecnologias cuja adoção impacta valores jurídicos, éticos e sociais. Sobre isso, ver: COUNCIL OF EUROPE. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) – Report on Artificial Intelligence "Artificial Intelligence and Data Protection: Challenges and Possible

Remedies", 2019. Disponível em: <https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6>.

180 Sobre isso, ver: FLORIDI, Luciano. Information ethics: its nature and scope. Pre-print, 2005. p. 1-30. Disponível em: <http://uhra.herts.ac.uk/bitstream/handle/2299/3001/903256.pdf;jsessionid=ACF1CD18C9A752A sequence=1>.

181 Artigo 1º, *caput*, da LGPD: "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

182 Artigo 2º, II, da LGPD: "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: (...) II - a autodeterminação informativa; (...)".

183 Veja-se, por exemplo, a opinião da Article 29 Working Group ainda no contexto da diretiva que faz diversas menções ao termo flexível para enquadrar a base legal do legítimo interesse: ARTICLE 29, Data Protection Working Party. Opinion on 06/24 on the notion of legitimat interests of the data controller under Article 7 of Directive 95/46/EC. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>.

184 UK Information Commissioner Office. Guide to the general data protection (GDPR). Disponíve em: <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>.

185 ARTICLE 29, Data Protection Working Party. Opinion on 06/24... Op.cit., p. 5-6.

186 Art. 7º da antiga Diretiva 95/56, o qual corresponde ao artigo 6º do Regulamento Europeu de Proteção de Dados.

187 Sobre tais técnicas normativas, veja-se: POLIDO, Frabricio Pasquot*GDPR e suas repercussões no direito brasileiro*: primeiras impressões de análise comparativa. Belo Horizonte: Instituto de Referência em Internet e Sociedade – IRIS, 2018. p. 5-11. E, também, as definições constantes no site da própria União Europeia em: <https://europa.eu/european-union/eu-law/legal-acts_en>.

188 Article 29 Working Party era o órgão de aconselhamento criado pela própria diretiva para a sua aplicação que congrega representantes de todas as autoridades de proteção de dados pessoais dos países-membros da União Europeia. Na GDPR, foi substituído pelo*European Data Protection Board*.

189 ARTICLE 29, Data Protection Working Party. Opinion on 06/24... Op.cit., p. 10.

190 ARTICLE 29, Data Protection Working Party. Opinion on 06/24... Op.cit., p. 11.

191 Veja que o legítimo interesse não constava do art. 9º do anteprojeto da lei. Disponível em:

<http://culturadigital.br/dadospessoais/files/2010/11/PL-Protecao-de-Dados.pdf>.

192 De acordo com o mapeamento do InternetLab, verificaram-se os seguintes atores nos seguintes espectros do debate público: a) ITI, Centre for Information Policy Leadership, GSMA, Fiesp, Iab, Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações, Associação Brasileira da Indústria Elétrica e Eletrônica, Associação Brasileira de Internet, BSA The Software Alliance, Sky, US Business Council e CNseg, Febraban, RELX Group, Cisco, Brasscom, Camara BR, Claro e VIVO; b) Grupo de Políticas Públicas para o Acesso à Informação da Universidade de São Paulo e Instituto de Tecnologia e Sociedade do Rio de Janeiro. Disponível em: <http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-no-17-debate-publico-de-protecao-de-dados-pessoais//>.

193 Veja-se, especificamente, a contribuição do GPoPAI/USP: "Por um lado, tais requisitos consistirão em um teste para assegurar que, mesmo não havendo um consentimento expresso, os dados pessoais estarão dentro de uma esfera de controle do cidadão (alíneas 'a', 'b' e 'c' do dispositivo sugerido). A exceção baseada no interesse legítimo está mais atrelada à desqualificação do consentimento como sendo expresso, do que, propriamente, à dispensa completa do consentimento (específico, livre e informado). Nesse sentido, o teste proposto visa garantir que o tratamento dos dados pessoais, lastreado nessa exceção, não seja desarrazoado, ferindo as legítimas expectativas de privacidade do seu titular. E, sob outra vertente, um dos requisitos do teste proposto consistirá em um dever do operador de prevenção de danos à privacidade dos cidadãos, como a adoção do processo de anonimização e outras medidas adequadas de segurança que minimizem tais riscos (alínea 'd')".

194 "Art. 10. O legítimo interesse do responsável somente poderá fundamentar um tratamento de dados pessoais, respeitados os direitos e liberdades fundamentais do titular, devendo ser necessário e baseado em uma situação concreta. § 1º O legítimo interesse deverá contemplar as legítimas expectativas do titular quanto ao tratamento de seus dados, de acordo com o disposto no art. 6º, II. § 2º O responsável deverá adotar medidas para garantir a transparência do tratamento de dados baseado no seu legítimo interesse, devendo fornecer aos titulares mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais. § 3º Quando o tratamento for baseado no legítimo interesse do responsável, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo ser anonimizados sempre que compatível com a finalidade do tratamento". Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=62B6CCB8D15F0 codteor=1457971&filename=Avulso+-PL+5276/2016>.

195 BIONI, Bruno Ricardo. Xeque-mate... Op.cit., p. 50-53.

196 Nela havia a previsão de um teste multifatorial composto por quatro passos: a) avalição do legítimo interesse; b) impacto sobre o titular do dado; c) equilíbrio entre "a" e "b"; e d)

salvaguardas a cargo de quem processa dados para prevenir consequências negativas sobre o titular do dado (ARTICLE 29, Data Protection Working Party. Opinion on 06/24... Op.cit., p. 33).

197 Há variações desse teste, ora composto por quatro fases, ora composto por três fases, como é o caso: UK Information Commissioner Office. Guide to the general... Op.cit., p. 82.

198 ARTICLE 29, Data Protection Working Party. Opinion on 06/24... Op.cit., p. 12.

199 É o caso, por exemplo, da vedação de coleta de dados, mesmo com o consentimento do seu titular em relações de trabalho, relacionados a gravidez, AIDS/HIV e toxicológico (Portarias 1.246/2010 e 41/2007).

200 ZANFIR-FORTUNA, Gabriela et al. Processing personal data on the basis of legitimate interes under the GDPR: practical cases. Future of Privacy Forum, 2018. p. 5.

201 ARTICLE 29, Data Protection Working Party. Opinion on 06/24... Op.cit., p. 5-6.

202 ARTICLE 29, Data Protection Working Party. Opinion on 06/24... Op.cit., p. 24.

203 Ibidem, p. 39.

204 Article 29 Data Protection Working Party. Opinion 3... Op.cit., p. 21: "Rather than imposing a requirement of compatibility, the legislator chose a double negation: it prohibited incompatibility. By providing that any further processing is authorised as long as it is not incompatible (and if the requirements of lawfulness are simultaneously also fulfilled), it would appear that the legislators intended to give some flexibility with regard to further use. Such further use may fit closely with the initial purpose or be different. The fact that the further processing is for a different purpose does not necessarily mean that it is automatically incompatible: this needs to be assessed on a case-by-case basis, as will be shown below".

205 Art. 6º, I, da LGPD: "finalidade: realização do tratamento para propósitos legítimos, específicos explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

206 KUNER, Cristopher. European... Op.cit., p. 100.

207 Idem.

208 Article 29 Data Protection Working Party. Opinion 3... Op.cit., p. 24: "This may cover situations where the further processing was already more or less implied in the initial purposes, or assumed as a logical next step in the processing according to those purposes, as well as situations where there is only a partial or even non-existent link with the original purposes. In any case, the greater the distance between the purposes of collection and the purposes of further processing, the more problematic this would be for the compatibility assessment".

209 Ibidem, p. 24: "The second factor focuses on the *specific context* in which the data were collected and the reasonable expectations of the data subjects as to their further use based on that context. In other words, the issue here is what a reasonable person in the data subject's situation would

expect his or her data to be used for based on the context of the collection".

210 ARTICLE 29, Data Protection Working Party. Opinion on 06/24... Op.cit., p. 36-37.

211 Essa sistematização foi elaborada para os cursos do Data Privacy Brasil. A primeira versão, que deu origem a essa última, foi elaborada em conjunto com Renato Leite Monteiro. Os acréscimos e eventuais inconsistência dessa segunda versão são de única e exclusiva responsabilidade do autor.

212 Os casos a seguir foram adaptados de três documentos diferentes, a fim de que fossem mais aderentes ao contexto brasileiro: a) casos julgados pela Corte Europeia de Justiça, mapeados por ZANFIR-FORTUNA, Gabriela et al. Processing... Op.cit.; b) casos hipotéticos tirados d ARTICLE 29, Data Protection Working Party. Opinion on 06/24... Op.cit.; e c) casos levantado pela própria indústria: Data Protection Network. Guidance on the use of legitimate interests under the EU General Data Protection Regulation. Disponível em <https://iapp.org/media/pdf/resource_center/DPN-Guidance-A4-Publication.pdf>.

213 Article 29 Working Party. Opinion 2/2017: on data processing at work. p. 23: "Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer. The legitimate interest of employers can sometimes be invoked as a legal ground, but only if the processing is strictly necessary for a legitimate purpose and the processing complies with the principles of proportionality and subsidiarity" (Disponível em: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiX5vyP5JTdAhULHZAKHapgBBs

214 Ibidem, p. 23.

215 Na consideranda 47 da GDPR, fraudes e incidentes de segurança foram listados como uma das possíveis aplicações do legítimo interesse: "The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned".

216 Esse foi um dos casos que ganhou previsão expressa na consideranda 49 da GDPR: "The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a

legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems".

217 Sobre o CERT brasileiro, consulte: <https://www.cert.br/sobre/>.

218 "A exigência de certidão de candidatos a emprego é legítima e não caracteriza lesão moral quando amparada em expressa previsão legal ou justificar-se em razão da natureza do ofício ou do grau especial de fidúcia exigido, a exemplo de empregados domésticos, cuidadores de menores, idosos e pessoas com deficiência, em creches, asilos ou instituições afins, motoristas rodoviários de carga, empregados que laboram no setor da agroindústria no manejo de ferramentas de trabalho perfurocortantes, bancários e afins, trabalhadores que atuam com substâncias tóxicas e entorpecentes e armas, trabalhadores que atuam com informações sigilosas" (Disponível em: <http://www.tst.jus.br/noticia-destaque/-/asset_publisher/NGo1/content/id/24287126>).

219 Veja, nesse sentido, a reportagem: *Agora as empresas sabem o que você fez no seu trabalho anterior*. Disponível em: <https://exame.abril.com.br/carreira/agora-as-empresas-sabem-o-que-voce-fez-no-seu-trabalho-anterior/>.

220 Exemplo adaptado de: Article 29 Data Protection Working Party. Opinion 3/2013 purpose... Op.cit., p. 58.

221 Ibidem, p. 61-63

222 Ibidem, p. 61.

223 Ibidem, p. 58.

224 Ibidem, p. 63-64.

225 O Regulamento contém 99 artigos e 173 considerandas. Estas são definidas na GDPR como as razões para a adoção dos artigos da GDPR propriamente ditos – "considering the following reasons the articles of the GDPR have been adopted. These are the latest and final recitals of April 27th 2016". Assim, as consideradas apresentam a racionalidade do regulamento, mas não se confundem com ele.

226 FERRETTI, Frederico. Data Protection and the Legitimate Interest of Data Controllers: Much Ado or About Nothing or the Winter of Rights? Common Market Law Review, n. 51, p. 858: "The other novelty is that, following the introduction of an accountability principle, it appears that the data controller will be left with the determination of whether it has a legitimate interest to justify the processing, and whether its interest overrides the fundamental rights and freedoms of the data subject. This will correct the uncertainty of the current framework and the different provisions or practices in the Member States. The processing will be subject to supervision, enforcement and, generally, judiciary control". Sobre isso, ver também: CUIJPERS, Colette. PURTOVA Nadezhda. KOSTA, Eleni. Data Protection Reform and the Internet: the Draft Data Protectio

Regulation. Tilburg Law School Legal Studies Research Paper Series n. 03/2014; KAMARA Irene. DE HERT, Paul. Understanding the Balancing Act Behind the Legitimate Interest of th Controller Ground: a Pragmatic Approach. Brussels Privacy Hub, Working Paper, vol. 4, n. 12 2018; INFORMATION COMMISSIONER'S OFFICE. Update report into adtech and real t bidding, 2019.

227 Artigo 6º, VI, da LGPD: "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; (...)".

228 Artigo 37 da LGPD: "Art. 37. O controlador e o operador devem manter registro das operações d tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse".

229 Em sentido contrário, defendendo que a obrigatoriedade do LIA derivaria do princípio da accountability e, por analogia, do ônus da prova por parte do controlador em comprovar a obtenção do consentimento: BUCAR, Daniel. VIOLA, Mario. Tratamento de Dados Pessoais p "legítimo interesse do controlador": primeiras questões e apontamentos. In *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro.* São Paulo: Thomson Reuters 2019. p. 477.

230 Artigo 8º, §§ 5º e 6º, da LGPD. "Art. 8º O consentimento previsto no inciso I do art. 7º desta Le deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. (...) § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do *caput* do art. 18 desta Lei. § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informa ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração".

231 Artigo 18, § 2º da LGPD: "Art. 18. O titular dos dados pessoais tem direito a obter do controlado em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei". Neste ponto, houve atecnidade na redação da lei, haja vista que as outras bases legais não são exceções ("dispensa") ao consentimento. Provavelmente, isso se deve em razão do fato de que, ao longo das diversas versões do anteprojeto da lei, o consentimento foi tratado como regra.

232 Trata-se de um direito subjetivo que confere ao titular a possibilidade de constituir, modificar ou extinguir uma situação subjetiva com uma declaração de vontade, sem que a outra parte possa se

opor. Ver: CHIOVENDA, Giuseppe. Instituições de direito processual civil. Campinas Bookseller, 2000.

233 Artigo 2º da LGPD: "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre-iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais".

234 O artigo 21 da GDPR estabelece o direito à objeção do titular dos dados nos casos em que o processamento ocorra para a execução de uma tarefa de interesse público, no exercício de uma autoridade oficial investida ao controlador, ou para os propósitos de legítimo interesse do controlador ou de terceiros – incluindo casos de perfilamento. Neste caso, o controlador deverá cessar o processamento a menos que demonstre justificativa legítima para continuá-lo ou o faça para o estabelecimento, exercício ou defesa de uma demanda jurídica. No caso de tratamento de dados para fins de publicidade direta, contudo, esse direito é absoluto (artigo 21 (3)).

235 A GDPR apontou o *marketing* direto como uma das possíveis aplicações do legítimo interesse na consideranda 27: "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest".

236 Para uma definição do que é first-party tracking, veja o subcapítulo 1.2.2.4 no sentido do rastreamento realizado pela própria aplicação ou *website* acessado pelo usuário.

237 Para uma definição do que é third-party tracking, veja o subcapítulo 1.2.2.4 no sentido de que o rastreamento é realizado por terceiros, que não a própria aplicação acessada pelo usuário.

238 Article 29 Working Party. Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679. p. 14.

239 É o primeiro exemplo de uma série da referida opinião do WP sobre legítimo interesse, cuja consumidora fictícia tem o nome de Cláudia – o teste "Cláudia". ARTICLE 29, Data Protectio Working Party. Opinion on 06/24... Op.cit., p. 31.

240 Em junho de 2019, a autoridade de proteção de dados francesa <https://www.cnil.fr/en/cookies-and-other-tracking-devices-cnil-publishes-new-guidelines> e a autoridade do Reino Unido <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> publicaram guidelines a respeito do tema. Ambas indicam que a utilização de termos de uso para coletar o consentimento do titular viola a exigência da GDPR de consentimento específico para cada tipo de tratamento e de dado coletado – recomendando o uso de uma segunda camada, além da coleta de um consentimento geral, permitindo o consentimento individual a cada propósito de tratamento separadamente. Além disso, as autoridades defendem

que para que o consentimento seja informado, o titular deve conseguir identificar todos os agentes que irão processar seus dados. A autoridade francesa, contudo, admite outras bases legais para além do consentimento para tratamentos posteriores, com base no cumprimento de obrigações contratuais e no teste de proporcionalidade (artigo 6(1) da GDPR). Veja, também, o comparativo realizado pela International Association Privacy Professionals/IAPP <https://iapp.org/resources/article/ico-and-cnil-revised-cookie-guidelines-convergence-and-divergence/>. Acesso em: 15 de out. 2019.

241 INFORMATION COMMISSIONER'S OFFICE. Update report into adtech and real time bidd 2019, p. 18: "Reliance on legitimate interests for marketing activities is possible only if organizations don't need consent under PECR and are also able to show that their use of personal data is proportionate, has a minimal privacy impact, and individuals would not be surprised or likely to object".

242 Esse foi um dos aspectos porque o teste acima considerou ser inadequado o legítimo interesse como uma base legal para *cross-tracking*, já que Cláudia teria sido precificada diferentemente na compra de uma pizza com base em sua localização. Ibidem, p. 32: "Lack of transparency about the logic of the company's data processing that may have led to de facto price discrimination based on the location where an order is placed, and the significant potential financial impact on the customers ultimately tip the balance even in the relatively innocent context of take – away foods and grocery shopping".

243 Além desse diálogo entre leis ordinárias, também será útil verificar uma combinação com normas infralegais. Por exemplo, o Decreto 6.523/2008 que regulamenta o Serviço de Atendimento ao Consumidor – SAC.

244 Artigo 39 do CDC: "Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: I – condicionar o fornecimento de produto ou de serviço ao fornecimento de outro produto ou serviço, bem como, sem justa causa, a limites quantitativos; II – recusar atendimento às demandas dos consumidores, na exata medida de suas disponibilidades de estoque, e, ainda, de conformidade com os usos e costumes; III – enviar ou entregar ao consumidor, sem solicitação prévia, qualquer produto, ou fornecer qualquer serviço; IV – prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços; V – exigir do consumidor vantagem manifestamente excessiva; VI – executar serviços sem a prévia elaboração de orçamento e autorização expressa do consumidor, ressalvadas as decorrentes de práticas anteriores entre as partes; VII – repassar informação depreciativa, referente a ato praticado pelo consumidor no exercício de seus direitos; VIII – colocar, no mercado de consumo, qualquer produto ou serviço em desacordo com as normas expedidas pelos órgãos oficiais competentes ou, se normas específicas não existirem, pela Associação Brasileira de Normas Técnicas ou outra

entidade credenciada pelo Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (Conmetro); IX – recusar a venda de bens ou a prestação de serviços, diretamente a quem se disponha a adquiri-los mediante pronto pagamento, ressalvados os casos de intermediação regulados em leis especiais;X – elevar sem justa causa o preço de produtos ou serviços; XI – Dispositivo incluído pela MPV nº 1.890-67, de 22.10.1999, transformado em inciso XIII, quando da conversão na Lei nº 9.870, de 23.11.1999; XII – deixar de estipular prazo para o cumprimento de sua obrigação ou deixar a fixação de seu termo inicial a seu exclusivo critério; XIII – aplicar fórmula ou índice de reajuste diverso do legal ou contratualmente estabelecido; XIV – permitir o ingresso em estabelecimentos comerciais ou de serviços de um número maior de consumidores que o fixado pela autoridade administrativa como máximo".

245 A autoridade de proteção de dados do Reino Unido (Information Commissioner's Office – ICO) posiciona-se nesse exato sentido ao observar a insuficiência de salvaguardas baseada apenas em contratos e cláusulas contratuais. Essa abordagem deveria ser acompanhada por outras medidas como relatórios de impacto, códigos de boas condutas e outros tipos de ferramentas para demonstrar *compliance* à legislação e promover *accountability*. INFORMATION COMMISSIONER'S OFFICE. Update ..., Op.cit., p. 21: "Industry has looked to use contract controls to provide a level of guarantees about data protection-compliant processing of personal data. In fact, some parties have asserted that they go 'beyond' contractual controls, a claim that has yet to be validated. However, this contract-only approach does not satisfy the requirements of data protection legislation. Organisations cannot rely on standard terms and conditions by themselves, without undertaking appropriate monitoring and ensuring technical and organisational controls back up those terms. For example, ICO guidance on controller/processor and contracts and liabilities states that controllers must: assess the processor is competent to process personal data in line with the GDPR; put in place a contract or other legal act meeting the requirements in Article 28(3); and ensure a processor's compliance on an ongoing basis, in order for the controller to comply with the accountability principle and demonstrate due diligence (such as audits and inspections)".

246 Ibidem, p. 24: "The second factor focuses on the *specific context* in which the data were collected and the reasonable expectations of the data subjects as to their further use based on that context. In other words, the issue here is what a reasonable person in the data subject's situation would *expect his or her data to be used for based on the context of the collection*".

247 Art. 6º, I, da LGPD: "finalidade: realização do tratamento para propósitos legítimos, específicos explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

248 "§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. § 4º É dispensada a exigência do

consentimento previsto no *caput* deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei".

249 Veja, por exemplo, as contribuições no sentido da necessidade em se definir o que eram "dados cadastrais" (p. 49) e "acesso público irrestrito" (p. 127): ANTONIALLI, Dennys et al. InternetLab reporta: consultas públicas nº 4. Disponível em: <http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-consultas-publicas-no-04/>.

250 Processo 70069420503 (CNJ: 0152244-45.2016.8.21.7000). O portal Migalhas disponibilizou um resumo do acórdão: <http://www.migalhas.com.br/arquivos/2016/11/art20161104-10.pdf>.

251 O julgado transcreve o seguinte trecho do artigo do Prof. Tércio Sampaio Ferraz Júnior como parte da sua fundamentação: "(...) São dados que, embora privativos – como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial, etc. –, condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido. Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores usados nas relações de convivência, as quais só dizem respeito aos que convivem" (FERRAZ JÚNIOR, Tércio Sampaio. Op.cit., p. 447).

252 Redação incluída da Lei nº 13.853/2019, a partir da MPV 869/2018.

253 Veja, por exemplo, o robô Rosie do Serenata de Amor que analisa os dados abertos dos gastos de despesas parlamentares para identificar transações suspeitas e, com isso, facilitar o controle social da administração pública. Disponível em: <https://serenata.ai/>. Esse é um dos exemplos elaborado em conjunto com Renato Leite para os cursos do Data Privacy Brasil.

254 Em termos conceituais, dados de acesso público são distintos dos manifestamente públicos. Neste último, a disponibilização da informação se daria por iniciativa do próprio titular e não por terceiros e, por fim, o seu acesso não teria qualquer tipo de restrição. Por exemplo, a informação do item "b" não é manifestamente pública nem divulgada por quem a ela está vinculada. Para acessá-la, é necessário fazer uma consulta à base de dados do Poder Judiciário – uma espécie de "filtro" –, que é quem disponibiliza tal informação sobre o possível devedor (réu de uma ação), enquanto os dados de um perfil público de uma rede social são divulgados pelo seu próprio titular, sendo plenamente acessível por quem quer que seja.

255 O princípio mais relevante para tanto seria o da finalidade contido no art. 6º, I, da LGPD: "finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

256 "§ 4º É dispensada a exigência do consentimento previsto no *caput* deste artigo para os dados

tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei".

[257] Esse é mais um dos exemplos elaborado em conjunto com Renato Leite para os cursos do Data Privacy Brasil.

[258] BIONI, Bruno Ricardo; RIBEIRO, Márcio Moretto. A transposição... Op.cit.; MONTEIRO, Renato Leite; BIONI, Bruno Ricardo. Dados públicos são dados pessoais. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/dados-publicos-sao-dados-pessoais-25062016>.

[259] HARARI, Y. N. *Homo Deus*: A Brief History of Tomorrow. Harper Collins, 2016.

[260] Diante de um "conflito de leis no tempo" a "solução" se daria através da prevalência de uma lei sobre a outra, com a consequente exclusão de uma delas do sistema jurídico (revogação, ab-rogação e derrogação). Três são os critérios tradicionais para decidir-se qual lei prevalecerá: (i) especialidade, caso em que lei especial afasta a aplicação da lei geral; (ii) anterioridade, de modo que a lei posterior afasta a anterior; e (iii) hierarquia, fazendo com que uma lei hierarquicamente superior, no sistema jurídico, afaste a aplicação daquela inferior.

[261] V. BOBBIO, Norberto. Teoria do Ordenamento Jurídico. São Paulo/Brasília: Pollis/Universidade de Brasília, 1990.

[262] MARQUES, Cláudia Lima. O "diálogo das fontes" como método da nova teoria geral do direito um tributo a Erik Jayme. In: MARQUES, Cláudia Lima (coord.)*Diálogo das Fontes*. São Paulo: Revista dos Tribunais, 2012. p. 25.

[263] *Ibidem*, p. 26-27: "A bela expressão do mestre Heidelberg é semiótica e autoexplicativa: direito-a-logos, duas "lógicas", duas 'leis' a seguir e coordenar um só encontro no "a", uma "coerência" necessariamente 'a restaurar' os valores deste sistema desta "nova" ordem de fontes, em que uma não mais 'revoga' a outra (o que seria um monólogo, pois só uma lei fala), e, sim, dialogam ambas as fontes, em uma aplicação conjunta e harmoniosa guiada pelos valores constitucionais e, hoje, em especial, pela luz dos direitos humanos. (...) Erik Jayme alerta, porém, que os tempos pós-modernos não mais permitem este tipo de clareza e 'monossolução', sequer a hierarquia dessas leis é clara, mas apenas dos valores constitucionais".

[264] Faz-se alusão ao movimento de descodificação em que diversas leis esparsas passaram a reger relações jurídicas específicas, estabelecendo-se verdadeiros microssistemas jurídicos: LORENZETTI, Ricardo Luis*Fundamento do Direito Privado*. São Paulo: Revista dos Tribunais, p. 1998: "A explosão do Código produziu um fracionamento da ordem jurídica, semelhante ao sistema planetário. Criam-se microssistemas jurídicos que, da mesma forma como os planetas, giram com autonomia própria, sua vida é independente; o Código é como o sol, ilumina-os, colabora em suas vidas, mas já não pode incidir diretamente sobre eles. Pode-se, também, referir a famosa imagem empregada por Wittgenstein aplicada ao Direito, segundo a

qual, o Código é o centro antigo da cidade, a que se acrescentam novos subúrbios, com seus próprios centros e características de bairro. Poucos são os que se visitam uns aos outros; vai-se ao centro de quando em quando para contemplar relíquias históricas".

265 *Idem*, p. 61: "Nesse sentido, alerte-se que o método do diálogo das fontes, por respeito aos valore constitucionais e direitos humanos que lhe servem de base, não deve, por exemplo, ser usado para retirar os direitos consumidor: o diálogo só pode ser usado em favor do sujeito vulnerável (....) Em outras palavras, o diálogo já tem a lógica/racionalidade preponderante: é a promoção pelo julgador dos direitos do consumidor, como impõe o art. 5°, XXXII, da CF/1988, incluída nas cláusulas gerais pétreas brasileiras: promover os direitos do consumidor 'na forma da lei' mais favorável ao sujeito de direitos vulnerável".

266 Artigo 64 da LGPD: Art. 64. "Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria (...)". É algo bastante próximo do art. 7º do CDC, no qual a teoria do diálogo das fontes ganhou tração no direito brasileiro.

267 Ressalva-se que o uso de tais terminologias é no sentido figurado, não sendo uma referência àquelas referidas nos arts. 2º a 5º do Código Civil.

268 Como já dito (subcapítulo 4.2.1), a proteção contratual do consumidor deve ser uma ação paliativa, seja no atual ou no projetado cenário nacional de proteção de dados pessoais. Ela deve ocorrer quando a causa normativa primária falhar: a capacitação do consumidor com o controle dos seus dados, garantindo-se um fluxo informacional apropriado para a pessoa de carne e osso por ele afetada.

Livros

AMARAL, Francisco. *Direito civil*: introdução. Rio de Janeiro: Renovar, 2008.

AMARAL, João Ferreira do. *Economia da informação e do conhecimento*. Coimbra: Almedina, 2009.

ANTUNES, Ana Filipa Morais. *Comentários aos artigos 70.º a 81.º do Código civil*: direitos da personalidade. Lisboa: Universidade Católica, 2012.

ARENDT, Hannah. *A condição humana*. Trad. Roberto Raposo. Rio de Janeiro: Forense Universitária, 2010.

BANDEIRA DE MELLO, Celso Antônio. *O conteúdo do princípio da igualdade*. São Paulo: Malheiros, 2009.

BARBOSA, Fernanda Nunes. *Informação*: direito e dever nas relações de consumo. São Paulo: Revista dos Tribunais, 2008.

BAUMAN, Zygmunt. *Modernidade líquida*. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar 2011.

_____. *Vida para consumo*: a transformação das pessoas em mercadoria. Rio de Janeiro: Zahar, 2008.

_____; LYON, David. *Vigilância líquida*. Rio de Janeiro: Zahar, 2014.

BELLEIL, Arnaud. *@privacidade*: o mercado dos dados pessoais: protecção da vida privada na idade da internet. Lisboa: Piaget, 2001.

BENJAMIN, Antônio Herman de Vasconcellos e. *Código brasileiro de defesa do consumidor*: comentado pelos autores do anteprojeto. Direito material (arts. 1º a 80º e 105 a 108). Rio de janeiro: Forense, 2011. v. 1.

BESSA, Leonardo Roscoe. *Cadastro positivo*: comentários à Lei 12.414, de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011.

_____. *Relação de consumo e aplicação do Código de Defesa do Consumidor*. São Paulo: Revista dos Tribunais, 2009.

BEVILAQUA, Clovis. *Direito das obrigações*. Rio de Janeiro: Livraria Francisco Alves, 1945.

BITTAR, Calos Alberto. *Os direitos da personalidade*. Rio de Janeiro: Forense Universitária, 2004.

BITTAR, Carlos Eduardo Bianca; ALMEIDA, Guilherme Assis de. *Curso de filosofia de direito*. São Paulo: Atlas, 2008.

BOBBIO, Norberto. *A era dos direitos*. Trad. Carlos Nelson Coutinho. Rio de Janeiro: Elsevier 2004.

_____. *O positivismo jurídico*: lições de direito. Trad. Márcio Pugliesi. São Paulo: Ícone, 2006.

_____. *Teoria do ordenamento jurídico*. São Paulo/Brasília: Pollis/Universidade de Brasília

1990.

BORGES, Roxana Cardoso. *Direitos da personalidade e autonomia privada*. São Paulo: Saraiva, 2009.

BRAUDRILLARD, Jean. *A sociedade de consumo*. Lisboa: Edições 70, 2011.

BRUNO, Fernanda. *Máquinas de ver, modos de ser*: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

BULOS, Uadi Lammêgo. *Curso de direito constitucional*. São Paulo: Saraiva, 2008.

CAMPOS, Diogo Leite de. *Nós*: estudo sobre os direitos das pessoas. Coimbra: Almedina, 2004.

CANTO, Rodrigo Eidelvein do. *A vulnerabilidade dos consumidores no comércio eletrônico*: a reconstrução da confiança na atualização do Código de Defesa do Consumidor. São Paulo: Revista dos Tribunais, 2015.

CAPELO DE SOUSA, Rabindranath V. A. *O direito geral de personalidade*. Coimbra: Coimbra Editora, 2011.

CARVALHO, Orlando de. *Teoria geral do direito civil*. Coimbra: Coimbra Editora, 2012.

CASTELLS, Manuel. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Tradução Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003.

_____. *A sociedade em rede.* 3. ed. São Paulo: Paz e Terra, 2000. (A era da informação: economia, sociedade e cultura, 1.)

CETIC.BR. *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros* [livro eletrônico]: TIC domicílios 2015. Núcleo de Informação e Coordenação do Ponto BR [editor]. São Paulo: Comitê Gestor da Internet no Brasil, 2016.

CHAVES, Antonio. *Tratado de direito civil*: introdução à ciência do direito, sujeito de direito. São Paulo: Revista dos Tribunais, 1982. t. 1, v. 1.

CHIOVENDA, Giuseppe. *Instituições de direito processual civil*. Campinas: Bookseller, 2000.

CORDEIRO, António Menezes de. *Tratado de direito civil*: parte geral, pessoas. Coimbra: Almedina, 2011. v. 4.

COSTA, Carlos Cleso Orcesi. *Cadastro positivo*: Lei nº 12.414/2011. São Paulo: Saraiva, 2012.

COSTA JÚNIOR, Paulo José. *O direito de estar só*: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 2007.

COUNCIL OF EUROPE. *Handbook on European Data Protection Law.* Luxembourg: Publications Office of the Europe Union, 2014.

CUPIS, Adriano de. *Os direitos da personalidade*. Trad. Afonso Celso Furtado Rezende. São Paulo: Quorum, 2008.

CUNHA DE SÁ, Fernando Augusto. *Abuso de Direito*. Almedina: Lisboa, 2005.

DANTAS, Marcos. *A lógica do capital-informação*: a fragmentação dos monopólios e a monopolização dos fragmentos num mundo de comunicações globais. Rio de Janeiro: Contraponto, 2002.

DANTAS, San Tiago. *Programa de direito civil*: parte geral, aulas proferidas na faculdade de direito civil. Rio de Janeiro, 1979.

DE LUCCA, Newton. *Direito do consumidor*: teoria geral da relação jurídica de consumo. 2. ed. São Paulo: Quartier Latin, 2008.

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

DOTTI, René Ariel. *Proteção da vida privada e liberdade de informação*. São Paulo: Revista dos Tribunais, 1980.

DRUCKER, Peter. *A sociedade pós-capitalista*. Trad. Nivaldo Montigelli Jr. São Paulo: Pioneira 1993.

EFING, Antônio Carlos. *Bancos de dados e cadastro de consumidores*. São Paulo: Revista dos Tribunais, 2002.

_____. *Contratos e procedimentos bancários à luz do Código de Defesa do Consumidor*. São Paulo: Revista dos Tribunais, 2012.

FACHIN, Luiz Edson. *Teoria crítica do direito civil*. Rio de Janeiro: Renovar, 2012.

FERNANDES NETO, Guilherme. *Direito da comunicação social*. São Paulo: Revista dos Tribunais, 2004.

FILOMENO, José Geraldo Brito. *Código brasileiro de defesa do consumidor*: comentado pelos autores do anteprojeto. Direito material (arts. 1º a 80º e 105 a 108). Rio de Janeiro: Forense 2011. v. 1.

FINOCCHIARO, Giusella. *Privacy e protezione dei dati personali*. Torino: Zanichelli Editore, 2012.

FRANCO, Vera Helena de Mello. *Contratos*: direito civil e empresarial. São Paulo: Revista dos Tribunais, 2012.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. *Novo curso de direito civil*: parte geral. São Paulo: Saraiva, 2006. v. I.

GARCIA, Enéas Costa. *Direito geral de personalidade no sistema jurídico brasileiro*. São Paulo: Juarez de Oliveira, 2007.

GOMES, Orlando. *A crise do direito*. São Paulo: Max Limonad, 1955.

_____. *Contratos de adesão*: condições gerais dos contratos. São Paulo: Revista dos Tribunais, 1972.

_____. *Memória justificativa do anteprojeto de reforma do Código Civil*. Rio de Janeiro: Departamento de Imprensa Nacional, 1963.

GONÇALVES, Carlos Roberto. *Direito civil*: parte geral. São Paulo: Saraiva, 2010. v. I.

GONÇALVES, Diogo Costa. *Pessoa e direitos da personalidade*: fundamentação ontológica. Coimbra: Almedina, 2008.

GONÇALVES, Maria Eduarda. *Direito da informação*: novos direitos e formas de regulação na sociedade da informação. Coimbra: Almedina, 2003.

GRAU, Eros Roberto. *A ordem econômica na Constituição de 1988*. São Paulo: Malheiros, 2005.
HARARI, Yuval Noah. *Homo Deus:* a brief history of tomorrow. HarperCollins, 2016.
HERRÁN ORTIZ, Ana Isabel*El derecho a la protección de datos personales en la sociedad de la información.* Bilbao: Universidad de Deusto, 2003.
HOUAISS, Antônio; VILLAR, Mauro de Salles*Dicionário Houaiss da língua portuguesa*. Rio de Janeiro: Objetiva, 2009.
JACOBINA, Paulo Vasconcelos*Publicidade no direito do consumidor*. Rio de Janeiro: Forense, 1996.
JUDENSNAIDER, Elena; LIMA, Luciana; ORTELLADO, Pablo; POMAR, Marcelo. *Vinte centavos*: a luta contra o aumento. São Paulo: Veneta, 2013.
KUNER, Christopher. *European Data Protection Law*. New York: Oxford University Express, 2007.
LACE, Susanne. *The glass consumer*: life in a surveillance society. Bristol: Policy Press, 2005.
LAFER, Celso.*A reconstrução dos direitos humanos*: um diálogo com o pensamento de Hannah Arendt. São Paulo: Companhia das Letras, 1988.
LEMOS, Ronaldo. *Direito, tecnologia e cultura*. Rio de Janeiro: Editora FGV, 2005.
LEONARDI, Marcel*Responsabilidade civil dos provedores de serviços de internet*. Juarez de Oliveira: São Paulo, 2005.
_____. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2012.
LESSIG, Lawrence.*Code and other laws of cyberspace*: version 2.0. New York: Basic Books, 2006.
LÈVY, Pierre. *Cibercultura*. Trad. Carlos Irineu da Costa. São Paulo: Editora 34, 2011.
_____. *O que é virtual*. Trad. Paulo Neves. São Paulo: Editora 34, 2011.
LIMONGI FRANÇA, Rubens. *Instituições de direito civil*. São Paulo: Saraiva, 1996.
LISBOA, Roberto Senise. *A obrigação de informar*. São Paulo: Almedina, 2012.
_____. *Confiança contratual*. São Paulo: Atlas, 2012.
_____. *Relação de consumo e proteção jurídica do consumidor no direito brasileiro*. São Paulo: Juarez de Oliveira, 1999.
_____. *Responsabilidade civil nas relações de consumo*. São Paulo: Revista dos Tribunais, 2006.
LÔBO, Paulo. *Direito Civil*: parte geral. São Paulo: Saraiva, 2012.
LORENZETTI, Ricardo Luis*Fundamento do direito privado*. São Paulo: Revista dos Tribunais, 1998.
_____. *Teoria da decisão judicial*. Trad. Bruno Miragem. São Paulo: Revista dos Tribunais, 2010.
LOSANO, Mario G.*Sistema e estrutura no direito*: das origens à escola histórica. Trad. Carlo Alberto Dastoli. São Paulo: Martins Fontes, 2008. v. I.
LYON, David.*Surveillance as Social Sorting*: Privacy, risk, and digital discrimination. London: Routledge, 2003.
_____. *The Electronic Eye*: The rise of surveillance society. Minneapolis: University of Minnesota

Press, 1994.

MACEDO JÚNIOR, Ronaldo Porto. *Contratos relacionais e defesa do consumidor*. São Paulo: Revista dos Tribunais, 2007.

MANCUSO, Rodolfo de Camargo. *Interesses difusos*: conceito e legitimação para agir. 4. ed. São Paulo: Revista dos Tribunais, 1997.

MANNINO, Michael V. *Projeto, desenvolvimento de aplicações e administração de banco de dados*. Trad. Beth Honorato. São Paulo: McGraw-Hill, 2008.

MARQUES, Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor*: um estudo dos negócios jurídicos do consumo no comércio eletrônico. São Paulo: Revista dos Tribunais, 2004.

_____. *Contratos no Código de Defesa do Consumidor*: o novo regime das relações contratuais. São Paulo: Revista dos Tribunais, 2011.

_____; BENJAMIN, Antônio Herman V.; MIRAGEM, Bruno. *Comentários ao Código de Defesa do Consumidor*. 3. ed. São Paulo: Revista dos Tribunais, 2010.

_____; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis*. São Paulo: Revista dos Tribunais, 2012.

MARQUES, Garcia; MARTINS, Lourenço. *Direito da informática*. Coimbra: Almedina, 2006.

MARTINS, Guilherme Magalhães. *Responsabilidade por acidente de consumo na Internet*. São Paulo: Revista dos Tribunais, 2008.

MARTINS, Leonardo. *Introdução à jurisprudência do Tribunal Constitucional Federal Alemão*. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leonardo Martins. Prefácio: Jan Woischnik. Trad. Beatriz Hennig et al. Montevidéu: Fundação Konrad Adenauer, 2005.

MARTINS-COSTA, Judith. *A boa-fé no direito privado*: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 1999.

MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. *Big Data*: A revolution will transform how we live, work and think. New York: Houghton Mifflin Publishing, 2013.

_____; _____. *Delete*: The virtue of forgetting in the digital age. United Kingdom: Princeton University Press, 2009.

MAZZILI, Hugo Nigro. *A defesa dos interesses difusos em juízo*: meio ambiente, consumidor, patrimônio cultural e patrimônio público e outros interesses. São Paulo: Saraiva, 2011.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. São Paulo: Saraiva, 2012.

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

MENEZES CORDEIRO, António Manuel da Rocha e. *Da boa fé no direito civil*. Coimbra: Almedina, 2011.

_____. *Tratado de direito civil*: parte geral, pessoas. Coimbra: Almedina, 2011. v. 4.

_____. *Tratado de direito civil português*. Direito das obrigações: introdução, sistemas e direito europeu, dogmática geral. Coimbra: Almedina, 2009. t. 1, v. 2.

MILLER, Arthur. *The assault privacy*: computers, data banks, and dossiers. Michigan: University of Michigan Press, 1971.

MIRAGEM, Bruno. *Direito do consumidor*: fundamentos do direito do consumidor: direito material e processual do consumidor; proteção administrativa do consumidor; direito penal do consumidor. São Paulo: Revista dos Tribunais, 2008.

MIRANDA, Custódio da Piedade Ubaldino. *Contrato de adesão*. São Paulo: Atlas, 2002.

MONTEIRO, Washington de Barros. *Curso de direito civil*: parte geral. São Paulo: Saraiva, 2012. v. 1.

MORATO, Antonio Carlos. *Pessoa jurídica consumidora*. São Paulo: Revista dos Tribunais, 2008.

MURILLO DE LA CUEVA, Pablo Lucas. *El derecho a la autodeterminación informativa*. Madrid: Tecnos, 1990.

MURRAY, Andrew. *Information, Technology Law*. New York: Oxford University Press, 2010.

NASCIMENTO, Amauri Mascaro. *Iniciação ao direito do trabalho*. São Paulo: LTr, 2009.

NEGROPONTE, Nicholas. *A vida digital*. Trad. Sérgio Tellaroli. Supervisão técnica Ricardo Rangel. São Paulo: Companhia das Letras, 1995.

NIGER, Sergio. *Le nuove dimensioni della privacy*: dal diritto alla riservatezza alla protezione dei dati personalli. Padova: Cedam, 2006.

NISSENBAUM, Helen. *Privacy in context*: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

NUNES, Luiz Antonio Rizzatto. *Curso de direito do consumidor*: com exercícios. São Paulo: Saraiva, 2004.

O'REALLY MEDIA INC. *Big data now*: current perspectives from O'Really Media. Bejing: O'Really Media, 2012. (Kindle Edition.)

ORWELL, George. *1984*. Trad. Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

PARISER, Eli. *O filtro invisível*: o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012. (Kindle Edition.)

PASQUALOTTO, Alberto. *Os efeitos obrigacionais da publicidade no Código de Defesa do Consumidor*. São Paulo: Revista dos Tribunais, 1997.

PEREIRA, Caio Mário da Silva. *Instituições de direito civil*. Atualização Maria Celina Bodin de Moraes. Rio de Janeiro: Forense, 2010.

PERLINGIERI, Pietro. *Perfis de direito civil*: introdução ao direito civil constitucional. Rio de Janeiro: Renovar, 1999.

PINHEIRO, Alexandre Sousa. *Privacy e proteção de dados pessoais*: a construção dogmática do

direito à identidade informacional. Lisboa: AAFDL, 2015.
PINHEIRO, Patrícia Peck. *Direito digital*. São Paulo: Saraiva, 2009.
POLIDO, Frabricio Pasquot. *GDPR e suas repercussões no direito brasileiro*: primeiras impressões de análise comparativa. Belo Horizonte: Instituto de Referência em Internet e Sociedade – IRIS 2018.
PONTES DE MIRANDA, Francisco Cavalcanti. *Tratado de direito privado*: direito de personalidade. Direito de família: direito matrimonial (Existência e validade do casamento). Atualização Rosa Maria Barreto Borriello de Andrade Nery. São Paulo: Revista dos Tribunais 2012. (Coleção Tratado de Direito Privado: parte especial, 7.)
REALE, Miguel. *Filosofia do direito*. São Paulo: Saraiva, 2002.
_____. *Lições preliminares de direito*. São Paulo: Saraiva, 2002.
_____. *O Estado Democrático de Direito e o conflito das ideologias*. São Paulo: Saraiva, 2005.
_____. *Política e direito*: ensaios. São Paulo: Saraiva, 2006.
REBONATO, Riccardo. *Taking liberties*: a critical examination of Libertarian paternalism. London: Palgrave, 2012.
RIPERT, Georges. *A regra moral nas obrigações civis*. Campinas: Bookseller, 2009.
RIZZARDO, Arnaldo. *Parte geral do Código Civil*. Rio de Janeiro: Forense, 2011.
ROB, Peter. *Sistemas de bancos de dados*: projeto e implementação. Trad. All Tasks. São Paulo: Cengage Learning, 2011.
RODATÀ, Stefano. *A vida na sociedade da vigilância*. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.
_____. *Il diritto di avere*. Roma: Laterza, 2012.
SCHREIBER, Anderson. *A proibição de comportamento contraditório*: tutela da confiança e *venire contra factum proprium*. Rio de Janeiro: Renovar, 2015.
_____. *Direitos da personalidade*. São Paulo: Atlas, 2011.
SILVA, Clóvis do Couto e. *A obrigação como processo*. Rio de Janeiro: Editora FGV, 2006.
SIMÃO, José Fernando. *Responsabilidade civil do incapaz*. São Paulo: Atlas, 2008.
SIQUEIRA JR., Paulo Hamilton. *Teoria do direito*. São Paulo: Saraiva, 2009.
SOLOVE, Daniel J. *The digital person*: technology and privacy in the information age. New York: New York University Press, 2004.
_____. *Understand privacy*. Cambridge: Harvard University Press, 2008.
_____; SCHWARTZ, Paul L. *Information privacy*. New York: Wolters Kluwer Law, 2011.
STAIR, Ralph; REYNOLDS, George W. *Princípios de sistema de informação*: uma abordagem gerencial. Trad. Flávio Soares Correa. São Paulo: Cengage Learning, 2009.
STAPLES, Willliam G. *Everyday Surveillance*. Maryland: Rowman & Littlefield, 2014.
SUNSTEIN, Cass; THALER, Richard H. *Nudge*: improving decisions about health, wealth, and happiness. New Haven & London: Yale University Press, 2008.

SZANIAWSKI, Elimar. *Direitos da personalidade e sua tutela*. São Paulo: Revista dos Tribunais, 1993.

TARTUCE, Flávio. *Direito civil*: lei de introdução e parte geral. Rio de Janeiro: Forense, 2012.

TEIXEIRA, Ana Carolina Brochado. *Saúde, corpo e autonomia privada*. Rio de Janeiro: Renovar, 2010.

TEPEDINO, Gustavo. *Temas de direito civil*. 4. ed. Rio de Janeiro: Renovar, 2008.

_____; SCHREIBER, Anderson. *Código Civil comentado*: direito das obrigações – artigos 233 a 420. São Paulo: Atlas, 2008. v. IV.

THEODORO JUNIOR, Humberto. *Comentários ao novo Código Civil*: dos defeitos do negócio jurídico ao final do livro III. Rio de Janeiro, 2003. t. 1, v. 3.

TORRES, Claudio. *A bíblia do marketing digital*: tudo o que você queria saber sobre o marketing e a publicidade na internet e não tinha a quem perguntar. São Paulo: Novatec, 2009.

TURBAN, Efraim; MCLEAN, Ephraim; WETHERBE, James. *Tecnologia da informação para gestão*. Trad. Renate Schinke. 3. ed. Porto Alegre: Bookman, 2004.

VASCONCELOS, Pedro Pais de. *Direitos da personalidade*. Coimbra: Almedina, 2006.

VILLEY, Michel. *A formação do pensamento jurídico moderno*. Trad. Claudia Berliner. São Paulo: Martins Fontes, 2006.

WESTIN, Alan F. *Privacy and Freedom*. New York: Atheneum, 1970.

WIEACKER, Franz. *História do direito privado moderno*. Trad. António Manuel Botelho Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

ZANINI, Leonardo Estevam de Assis. *Direitos da personalidade*: aspectos essenciais. São Paulo: Saraiva, 2011.

ZANON, João Carlos. *Direito à proteção dos dados pessoais*. São Paulo: Revista dos Tribunais, 2013.

Capítulos de livros

ALMEIDA, Kellyne Laís Laburú Alencar de. O direito ao livre desenvolvimento da personalidade perspectiva do direito português. In: MIRANDA, Jorge; RODRIGUES JUNIOR, Otavio Lu FRUET, Gustavo Bonato (Org.). *Direitos da personalidade*. São Paulo: Atlas, 2012. p. 65-107.

ANDERSON, Simon P. Advertising on the internet. In: PEITZ, Martin; WALDFOGEL, Joel (Org *The Oxford handbook of the digital economy*. New York: Oxford University Press, 2012. p. 355-396.

ANDRADE, Norberto Nuno Gomes de Andrade. The right privacy and the right to identity in the Ag of ubiquitous computing: Friends or foes? A proposal towards a legal articulation. In: AKRIVOPOLOUS, Christina; PSYGKAS, Athanasious (Org.). *Personal data privacy and protection in a surveillance era*: technologies and practices. New York: Information Science Reference, 2011. p. 19-43.

AZEREDO, João Fábio A. Sigilo das comunicações eletrônica diante do marco civil da internet. In DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. t. II, p. 211-233.

AZEVEDO, Antônio Junqueira de. O direito pós-moderno e a codificação. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (Org.). *Coleção doutrinas essenciais*: *direito do consumidor* – fundamentos do direito do consumidor. São Paulo: Revista dos Tribunais, 2011. v. 1, p. 555-565.

BARBOSA, Marco Antonio. Marco civil da internet: mercado e estado de vigilância. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. t. II, p. 233-252.

BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run Around Consent and Anonymity. In: Lane, J.; STODDEN, V.; BENDER, S.; NISSENBAUM, H. (Ed.). *Privacy, Big Data and the Public Good*. Cambridge: Cambridge University Press, 2014. p. 44-75.

BARRETO JÚNIOR, Irineu. Atualidades no conceito da sociedade da informação. In: PAESANI, Liliana Minardi (Coord.). *O direito na sociedade da informação*. São Paulo: Atlas, 2007. p. 61-77.

_____. Proteção da privacidade e de dados pessoais na internet: o marco civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. t. I, p. 405-430.

BESSA, Leonardo Roscoe. A abrangência da disciplina conferida pelo código de defesa do consumidor aos bancos de proteção ao crédito. In: NERY JÚNIOR, Nelson; NERY, Rosa Maria de Andrade (Org.). *Coleção doutrinas essenciais*: Responsabilidade civil – direito à informação. São Paulo: Revista dos Tribunais, 2010. v. 8, p. 393-438.

_____. Limites Fornecedor equiparado. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (Org.). *Coleção doutrinas essenciais*: direito do consumidor – fundamentos do direito do consumidor. São Paulo: Revista dos Tribunais, 2011. v. 1, p. 1011-1030.

BOULDING, K. E. The economics of knowledge and the knowledge of economics. In: LAMBERTON, D. M. (Ed.). *Economics of information and knowledge, selected readings*. Baltimore: Penguin Books, 1971. p. 21-36.

BUCAR, Daniel; VIOLA, Mario. Tratamento de Dados Pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. Thomson Reuters, 2019.

CABRAL, Marcelo Malizia. A colisão entre os direitos de personalidade e o direito de informação. In: MIRANDA, Jorge; RODRIGUES JUNIOR, Otavio Luiz; FRUET, Gustavo Bonato (Org.). *Direitos da personalidade*. São Paulo: Atlas, 2012. p. 108-154.

CASSIOLATO, José Eduardo. A economia do conhecimento e as novas políticas industriais e tecnológicas. In: LASTRES, Helena M. M.; ALBAGAJI, Sarita (Org.). *Informação e globalização na era do conhecimento*. Rio de Janeiro: Campus, 1999. p. 164-190.

CATE, Fred H. The Failure of Fair Information Practice Principles. In: WINN, Jane K. (Ed *Consumer Protection in the Age of the 'Information Economy'* (markets and the law). Hampshire: Ashgate Publish, 2006. p. 343-379.

CHINELLATO, Silmara Juny de Abreu. Comentários à Parte Geral – artigos 1º a 21 do Códig Civil. In: MACHADO, Antonio Cláudio da Costa (Org.); CHINELLATO, Silmara Ju (Coord.). *Código Civil Interpretado*: artigo por artigo, parágrafo por parágrafo. 5. ed. Barueri: Manole, 2012. p. 30-54.

COMPARATO, Fábio Konder. A proteção do consumidor na constituição brasileira de 1988. In MARQUES, Cláudia Lima; MIRAGEM, Bruno (Org.). *Direito do consumidor*: vulnerabilidade do consumidor e modelos de proteção. São Paulo: Revista dos Tribunais, 2011. v. 2, p. 175-188.

_____. A proteção do consumidor: importante capítulo do Direito Econômico. In: MARQUES Cláudia Lima; MIRAGEM, Bruno (Org.) *Coleção doutrinas essenciais*: direito do consumidor – fundamentos do direito do consumidor. São Paulo: Revista dos Tribunais, 2011. v. 1, p. 167-186.

CUSUMANO, Michael A.; GOELDI, Andreas. New Businesses and new business models. I DUTTON, William H. (Org.).*The Oxford handbook of internet studies*. United Kingdon: Oxford University Press, 2012. p. 239-261.

DANTAS, Marcos. Capitalismo na era das redes. In: LASTRES, Helena M. M.; ALBAGAJI, Sa (Org.). *Informação e globalização na era do conhecimento*. Rio de Janeiro: Campus, 1999. p. 216-261.

DE MATTIA, Fábio Maria. Direitos da personalidade: aspectos gerais. In: CHAVES, Antôni (Coord.). *Estudos de direito civil*. São Paulo: Revista dos Tribunais, 1979. p. 99- 124.

_____. Direitos da personalidade. In: MENDES, Gilmar Ferreira; STOCO, Rui (Org.). *Coleção doutrinas essenciais*: direito civil – parte geral – pessoas e domicílio. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 245-259.

DONEDA, Danilo. Os direitos da personalidade no novo Código Civil. In: TEPEDINO, Gusta (Coord.). *A parte geral do novo Código Civil*: estudos na perspectiva constitucional. Rio de Janeiro: Renovar, 2002. p. 35-58.

_____. Princípios e proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILH Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.) *Direito & Internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. t. I, p. 369-384.

EDWARDS, Lilian; HATCHER, Jordan. Consumer privacy law 2: data collection, profiling ar targeting. In: EDWARDS, Lilian; WAELDE, Charlotte (Coord.). *Law and the internet.*

Portland: Har Publishing, 2009. p. 511-545.

FICI, Antonio; PELLECCHIA, Enza. Il consenso al tratamento. In: PARDOLESI, Roberto (Or *Diritto alla riservatezza e circolazione dei dati personali*. Milano: Giuffrè, 2003. p. 469-616.

FISCHER-HÜBNER, Simone; HOOFNAGLE, Chris Jay; KRONTIRIS, Ioannis; RANNENB Kai; WAIDNER, Michael; BOWDEN, Caspar. Online Privacy – Towards Informational Sel Determination on the Internet. In: HILDEBRANDT, M.; O'HARA, K.; WAIDNER, M. (E *Digital Enlightenment Yearbook*. Amsterdam: ISO Press, 2013. p. 123-138.

FRANÇA, Rubens Limongi. Direitos da personalidade. In: MENDES, Gilmar Ferreira; STOCO, F (Org.). *Doutrinas essenciais*: direito civil – parte geral – pessoas e domicílio. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 653-668.

FREEMAN, Chris. The ICT paradigm. In: MANSEL, Robin et al. (Org.). *The Oxford handbook of information and communication technologies*. New York: Oxford University Press, 2007. p. 34-54.

GAMA, Guilherme Calmon Nogueira da; PEREIRA, Daniel Queiroz. Direitos da personalidade Código Civil de 2002. In: MENDES, Gilmar Ferreira; STOCO, Rui (Org.). *Doutrinas essenciais*: direito civil – parte geral – pessoas e domicílio. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 303-330.

GAMBOGI, Ana Paula. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (Org.). *Coleção doutrinas essenciais*: direito do consumidor – proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 907-956.

GARCIA, Maria. Os sentidos da liberdade. In: MENDES, Gilmar Ferreira; STOCO, Rui (Org *Doutrinas essenciais*: direito civil – parte geral – pessoas e domicílio. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 553-560.

JACOB NETO, Elias; BOLZAN DE MORAIS, Jose Luis. *Surveillance* e Estado-Nação: as inadequadas tentativas de controlar os fluxos de dados através do Marco Civil da Internet e da CPI da espionagem. In: CONPEDI/UFPB (Org.). *Direito e novas tecnologias I*. Florianópolis: Conpedi, 2014. p. 232-258.

KERR Ian; BARRIGAR, Jennifer; BURKELL, Jacqelyn; BLACK, Katie, Soft surveillance, h consent. In: KERR, Ian (Ed.). *Lessons from the identity trail*: anonymity, privacy and identity in a networked society. New York: Oxford University Press, 2009. p. 5-22.

LASTRES, Helena Maria Martins; FERRAZ, João Carlos. Economia da Informação, conhecimento e do aprendizado. In: LASTRES, Helena M. M.; ALBAGAJI, Sarita (Org *Informação e globalização na era do conhecimento*. Rio de Janeiro: Campus, 1999. p. 27-57.

LAWSON, Philippa; O'DONOGHE, Mary. Approaches to Consent in Canadian Data Protection Law. In: KERR, Ian (Ed.). *Lessons from the identity trail*: anonymity, privacy and identity in a networked society. New York: Oxford University Press, 2009. p. 23-42.

LEMOS, Cristina. Inovação na era do conhecimento. In: LASTRES, Helena M. M.; ALBAGA Sarita (Org.). *Informação e globalização na era do conhecimento*. Rio de Janeiro: Campus, 1999. p. 122-144.

LIMA, Cíntia Rosa Pereira de; BIONI, Bruno Ricardo. A proteção dos dados pessoais na fase d coleta: apontamentos sobre a adjetivação do consentimento implementada pelo artigo 7, incisos VIII e IX do Marco Civil da Internet a partir da *human computer interaction* e da *privacy by default*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Coord.). *Direito & Internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. t. I, p 263-290.

LÔBO, Paulo Luiz Netto. A informação como direito fundamental do consumidor. In: MARQUES Cláudia Lima; MIRAGEM, Bruno (Org.) *Coleção doutrinas essenciais*: direito do consumidor – proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 593-612.

LORENZETTI, Ricardo Luis. Informática, Cyberlaw e e-commerce. In: MARQUES, Cláudia Lir MIRAGEM, Bruno (Org.) *Coleção doutrinas essenciais*: direito do consumidor – proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 1339-1372.

MACEDO JÚNIOR, Ronaldo Porto. Interpretação da boa-fé nos contratos brasileiros: os princípi jurídicos em uma abordagem relacional (contra a euforia principiológica). In: MACEDO JÚNIOR, Ronaldo Porto; BARBIERI, Catarina Helena Cortada (Org.) *Direito e interpretação*: racionalidades e instituições. São Paulo: Saraiva, 2011. p. 307-335.

_____. Privacidade, mercado e informação. In: NERY JÚNIOR, Nelson; NERY, Rosa Maria d Andrade (Org.). *Coleção doutrinas essenciais*: responsabilidade civil – direito à informação. São Paulo: Revista dos Tribunais, 2010. v. 8, p. 27-40.

MARQUES, Cláudia Lima. O "diálogo das fontes" como método da nova teoria geral do direito: u tributo a Erik Jayme. In: MARQUES, Cláudia Lima (Coord.) *Diálogo das Fontes*. São Paulo: Revista dos Tribunais, 2012. p. 17-66.

MAYER-SCHONEBERGER, Viktor. Generational development of data protection in Europe. I AGRE, Phillip E.; ROTENBERG, Marc (Org.) *Technology and Privacy*: The New Landscape. Cambridge: The MIT Press, 1997. p. 219-242.

MELODY, William H. Markets and policies in new knowledge economies. In: MANSEL, Robin al. (Org.). *The Oxford handbook of information and communication technologies*. New York: Oxford University Press, 2007. p. 55-74.

MIGUEL, Carlos Ruiz. El derecho a la protección de los datos personales en la Carta de Derecho Fundamentales de la Unión Europea. In: ORDEM DOS ADVOGADOS DO CONSEL DISTRITAL DE PORTO (Org.) *Temas de direito da informática*. Coimbra: Coimbra Editora, 2004. p. 17-72.

MIRAGEM, Bruno. *Eppur si muove*: diálogo das fontes como método de interpretação sistemática no

direito brasileiro. In: MARQUES, Cláudia Lima (Coord.)*Diálogo das fontes*. São Paulo: Revista dos Tribunais, 2012. p. 67-110.

MIRANDA, Jorge; RODRIGUES JUNIOR, Otavio Luiz; FRUET, Gustavo Bonato. Princi problemas dos direitos da personalidade e estado da arte da matéria no direito comparado. In: MIRANDA, Jorge; RODRIGUES JUNIOR, Otavio Luiz; FRUET, Gustavo Bonato (O *Direitos da personalidade*. São Paulo: Atlas, 2012. p. 1-18.

MORATO, Antonio Carlos; CASSEB, Paulo Adib; REBELLO, Deise Carolina Muniz. A socieda da informação e os "reality shows". In: PAESANI, Liliana Minardi (Coord.).*O direito na sociedade da informação II.* São Paulo: Atlas, 2009. p. 167-195.

PAESANI, Liliana Minardi. A publicidade móvel e a vulnerabilidade do consumidor. In: MORATC Antonio Carlos; NERI, Paulo de Tarso (Org.).*20 anos do Código de Defesa do Consumidor:* estudos em homenagem ao professor José Geraldo Brito. São Paulo: Atlas, 2010. p. 183-188.

PARDOLESI, Roberto. Dalla riservatezza alla protezione dei dati personali: una storia di evoluzion e discontinuità. In: PARDOLESI, Roberto (Org.)*Diritto alla riservatezza e circolazione dei dati personali*. Milano: Giuffrè, 2003. p. 1-58.

POULLET, Yves. About the E-Privacy Directive: Towards a Third Generation of Data Protectio Legislation? In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul de (Org.)*Data Protection in a Profiled World*. New York: Springer, 2010. p. 3-30.

RAMOS, André de Carvalho. O pequeno irmão que nos observa: os direitos dos consumidores e o bancos de dados no Brasil. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (Org.).*Coleção doutrinas essenciais*: direito do consumidor – proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 957-974.

ROCHA, Sílvio Luís Ferreira. O controle da publicidade no CDC. In: MORATO, Antonio Carlo NERI, Paulo de Tarso (Org.).*20 anos do Código de Defesa do Consumidor:* estudos em homenagem ao professor José Geraldo Brito. São Paulo: Atlas, 2010. p. 176-182.

ROESSLER, Beate. Should personal data be a tradable good? On the moral limits of markets i privacy. In: ROESSLER, Beate; MOKROSINSKA, Dorota (Org.)*Social Dimensions of Privacy.* Cambridge: Cambridge University Press, 2015. p. 141-161.

ROOPO, Enzo. I diritti della personalità. In: ALPA, Guido; BESSONE, Mario (Org.)*Banche dati telematica e diritti della personalità*. Padova: Cedam, 1984. p. 61-88.

TAVEIRA JÚNIOR, Fernando Tenório. A utilização da tecnologia RFID no mundo da computaçã ubíqua: algumas sugestões para a manutenção da privacidade, em um cenário futuro. In: ROVER, Aires José; CELLA, José Renato Gaziero; AYUDA, Fernando Galindo (Org.)*Direito e novas tecnologias*: XXIII Encontro Nacional do CONPEDI. Florianópolis: Conpedi, s.d. 109-136.

TENNIS, Bradley. Privacy and identity in a networked world. In: AKRIVOPOLOUS, Christi PSYGKAS, Athanasious (Org.).*Personal data privacy and protection in a surveillance era*:

technologies and practices. New York: Information Science Reference, 2011. p. 1-18.

TOMASEVICIUS FILHO, Eduardo. O marco civil da internet e as liberdades de mercado. In: I LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III*: marco civil da internet. São Paulo: Quartier Latin, 2015. t. II, p. 49-64.

ZANELATTO, Marco Antônio. Considerações sobre o conceito jurídico de consumidor. In MARQUES, Cláudia Lima; MIRAGEM, Bruno (Org.). *Coleção doutrinas essenciais*: direito do consumidor – fundamentos do direito do consumidor. São Paulo: Revista dos Tribunais, 2011. v. 1, p. 1031-1054.

Artigos

ACQUISTI, Alessandro. Nudging privacy: behavioral economics of personal information. *IEEE Security & Privacy*, p. 82-85, Nov./Dec. 2009.

_____; GROSSKLAGS, Jens. Privacy and rationality in individual decision making. *IEEE Security & Privacy Review*, p. 26-33, Jan./Feb. 2005.

AMARAL, Francisco. Evocação a Orlando Gomes. *Revista de direito comparado*, n. 17. p. 6-13, 2º semestre de 1999.

ANTONIALLI, Dennys Marcelo. Watch your steps: an empirical study of the use of online trackin technologies in different regulatory regimes. *Stanford Journal of Civil Rights & Civil Liberties*, p. 323-368, Aug. 2012.

AUSTIN, Lisa M. Is consent the foundation of fair information practices? Canada's experience unde PIPEDA. Research paper nº 11-05. *University of Toronto Law Journal*, p. 1-54, 2006.

_____. Reviewing PIPEDA: control, privacy and the limits of fair information practices. *The Canadian Business Law Journal*, v. 44, n. 1, p. 21-53, Oct. 2006.

BAMBERGER, Kenneth; MULLIGAN, Deirdre K. Privacy on the books and on the ground. *Stanford Law Review*, v. 63, p. 247-315, jan. 2011.

BAPTISTA, Patrícia; KELLER, Clara. Por que, quando e como regular as novas tecnologias? O desafios trazidos pelas inovações disruptivas. *Revista de Direito Administrativo*, n. 273, p. 123-163, set./dez. 2016.

BAROCAS, Solon; NISSENBAUM, Helen. On Notice. The Trouble with Notice and Consent. p. Disponível em: <http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf>. Acesso em: 14 jan. 2014.

_____; SELBST, Andrew D. Big Data's Disparate Impact. *California Law Review*, v. 104, p. 2-6. 2016. Disponível em: <http://ssrn.com/abstract=2477899>. Acesso em: 8 jul. 2015.

BANERJEE, Syagnik; DHOLAKIA, Ruby Roy. Mobile Advertising: Does Location Bas Advertising Work? *International Journal of Mobile Marketing*, Dec. 2008, p. 1-23. Disponível em: <http://ssrn.com/abstract=2135087>. Acesso em: 18 fev. 2014.

BIONI, Bruno Ricardo. O dever de informar e a teoria do diálogo das fontes para a aplicação d

autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergências e divergências a partir da análise da ação coletiva promovida contra o *Facebook* e o aplicativo 'Lulu'. *Revista de Direito do Consumidor*, v. 94, p. 283-326, 2014.

_____. Projeto de Lei 215/2015, infanticídio aos recém-nascidos direitos digitais no Brasil. *Digital Rights*, n. 28, out. 2015. Disponível em: <http://www.digitalrightslac.net/pt/proyecto-de-ley-2152015-infanticidio-contra-los-recien-nacidos-derechos-digitales-en-brasil/>. Acesso em: 15 nov. 2015.

BLUME, Peter. The inherent contradictions in data protection law. *International Data Privacy Law*, v. 2, n. 1, p. 26-34, 2012.

BORGESIUS, Frederick Zuiderveen. Segmentação comportamental *Do not track* e o desenvolvimento jurídico europeu e holandês. *Revista Politics*: publicação do Núcleo de Pesquisas e Estudo de Formação (Nupef), n. 14, fev. 2013.

BRANDELS, Louis; WARREN, Samuel. The right to privacy. *Civilistica.com*, Rio de Janeiro, ano 2, n. 3, jul.-set. 2013. Disponível em: <http://civilistica.com/the-right-to-privacy/>. Acesso em: 10 dez. 2013.

CALO, Ryan. Against notice skepticism in privacy (and elsewhere). *Notre Dame law review*, v. 87, n. 3, p. 1027-1072, Mar. 2011.

_____. Consumer subject review boards: a thought experiment. *Stanford Law Review Online*, v. 97, p. 97-102, Sept. 2013.

CATE, Fred H.; MAYER-SCHONBERGE, Viktor. Notice and consent in a world of Big Da *International Data Privacy Law*, v. 3, n. 2, p. 67-73, 2013.

CHEN, Yubo; XIE, Jinhong. Online consumer review: a new element of marketing communication mix. *Management Science*, v. 54, n. 3, p. 1-43, 2008. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=618782>. Acesso em: 5 fev. 2014.

COHEN, Julie. Examined lives: informational privacy and subject as object. *Stanford Law Review*, n. 52, p. 1373-1438, 1999-2000.

CUNHA, Mario Viola de Azevedo. Data Protection and Insurance: The Limits on the Collection an Use of Personal Data on Insurance Contracts in EU Law. *Global Jurist*, v. 10, p. 1-29, 2010.

CUIJPERS, Colette; PURTOVA, Nadezhda; KOSTA, Eleni. Data Protection Reform and the Intern the Draft Data Protection Regulation. *Tilburg Law School Legal Studies Research Paper Series*, n. 03/2014.

DE LIMA, Desiree; LEGGE, Adam. The european union's approach to online behaviour advertising: Protecting individuals or restricting business? *Computer Law & Security Review*, v. 30, p. 69-74, 2014.

DOCTOROW, Cory. Proteção de dado na UE: a certeza da incerteza. *Revista Politics*: publicação do Núcleo de Pesquisas e Estudo de Formação (NUPEF), n. 16, p. 9-22, nov. 2013.

_____. The Curious Case of Internet Privacy. *MIT Technology Review*, 2012. Disponível em: <http://www.technologyreview.com/news/428045/the-curious-case-of-internet-privacy>. Acesso em: 12 fev. 2015.

DONEDA, Danilo; ALMEIDA, Virgílio A. F. O que é governança de algoritmos. *Revista Politics*: publicação do Núcleo de Pesquisas e Estudo de Formação (Nupef), n. 24, out. 2016.

EHRHARDT JÚNIOR, Marcos. Relação obrigacional como processo na construção do paradigm dos deveres gerais de conduta e suas consequências. *Revista da Faculdade de Direito da Universidade Federal do Paraná*, Curitiba, n. 47, p. 141-155, 2008.

EVANS, David D. The economics of the online advertising industry. *Journal of Economic Perspectives*, Apr. 2009, p. 42. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1376607>. Acesso em: 14 fev. 2014. p. 1-46.

_____. The online advertising industry: economics, evolution, and privacy. *Journal of Economic Perspectives*, Apr. 2009, p. 1-41. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1376607>. Acesso em: 14 fev. 2014.

FACHIN, Luiz Edson. Fundamentos, limites e transmissibilidade: anotações para uma leitura crítica construtiva e de índole constitucional da disciplina dos direitos da personalidade no código civil brasileiro. *Revista da Escola da Magistratura do Estado do Rio de Janeiro*, v. 8, n. 31, p. 51-69, 2005.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: O direito à privacidade e os limites da função fiscalizadora do estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 88, p. 430-459, 1993.

FERRETTI, Frederico. Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights? *Common Market Law Review*, n. 51 (3):843-868, jun. 2014.

FLORIDI, Luciano. Information ethics: its nature and scope. Pre-print, 2005. p. 1-30. Disponível em: <http://uhra.herts.ac.uk/bitstream/handle/2299/3001/903256.pdf;jsessionid=ACF1CD18C9A752 sequence=1>. Acesso em: 16 out. 2019.

GOULART, Guilherme Goulart: Por uma visão renovada dos arquivos de consumo. *Revista de Direito do Consumidor*, São Paulo, v. 107, p. 452, 2016.

GÜRSES, Seda. PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm. *Identity in the Information Society*, v. 3, n. 3, p. 539-563, Dec. 2010.

HEURIX, Johannes; ZIMMERMANN, Peter; NEUBAUER, Thomas; FENZ Stefan. A taxonomy privacy enhancing technologies. *Computers & Security*, v. 53, p. 1-17, 2015.

HOOFNAGLE, Chris Jay; SOLTANI, Ashkan; GOOD, Nathaniel; WAMBACH, Dietri AYENSON, Mika D. Behavioral advertising: the offer you cannot refuse. *Harvard Law & Policy Review*, v. 6, p. 273-296, 2012.

JEROME, Joseph W. Buying and selling privacy: Big Datas's Different burdens and benefits *Stanford Law Review Online*, v. 66, p. 47-53, Sept. 2013.

JOLLS, Christine; SUNSTEIN, Cass R.; THALER, Richard. A behavioral approach to law a economics. *Stanford Law Review*, v. 50, p. 1470-1450, 2004.

KAMARA, Irene; DE HERT, Paul. Understanding the Balancing Act Behind the Legitimate Interest the Controller Ground: a Pragmatic Approach. *Brussels Privacy Hub Working Paper*, vol. 4, n. 12, 2018.

KLOZA, Darius; GALETTA, Antonella. Towards efficient cooperation between supervisor authorities in the era of data privacy law. *Brussels privacy working papers*, v. 1, n. 03, p. 1-25, Oct. 2015. Disponível em: <http://www.brusselsprivacyhub.org/Resources/BPH-Working-Paper-VOL1-N3.pdf>. Acesso em: 25 nov. 2015.

KOOPS, Bert-Jaap. Should ICT Regulation Be Technology-Neutral? In: KOOPS, Bert-Jaap; LII Miriam; PRINS, Corien; SCHELLEKENS, Maurice (eds.). Starting Points for ICT Regulati Deconstructing Prevalent Policy One-Liners,*IT & Law Series*, v. 9, The Hague: T.M.C. Asser Press, 2006, p. 77-108.

_____; LEENES, Ronald E. 'Code' and the slow erosion of privacy.*Michigan Telecommunications and Technology Law Review*, v. 12, n. 1, p. 139, 2005. Disponível em: <http://ssrn.com/abstract=1645532>. Acesso em: 13 out. 2015.

KRAMERA, Adam D. I.; GUILLORYB, Jamie E.; HANCOCKB, Jeffrey T. Experimental evidence of massive-scale emotional contagion through social networks. *PNAS Review*, v. 111, n. 29, p. 8788-8790, July 22, 2014. Disponível em: <http://www.pnas.org/content/111/24/8788.full.pdf>. Acesso em: 26 nov. 2015.

KUNER, Christopher. Regulation of Transborder Data Flows under Data Protection and Privac Law. *OECD Digital economic papers*, Paris, n. 187, p. 1-40. Disponível em: <http://dx.doi.org/10.1787/5kg0s2fk315f-en>. Acesso em: 8 jul. 2014.

LERMAN, Jonas. Big data and its exclusions.*Stanford Law Review Online*, v. 66, p. 55-63, Sept. 2013. Disponível em: <http://ssrn.com/abstract=2293765>. Acesso em: 8 mar. 2014.

LISBOA, Roberto Senise. Direito na sociedade da informação*Revista dos Tribunais*, ano 95, v. 847, p. 78-95, maio 2007.

_____. O consumidor na sociedade da informação. *Revista de Direito do Consumidor*, ano 16, n. 61, p. 203-229, jan./mar. 2007.

MANTELERO, Alessandro. AI and Big Data: A blueprint for a human rights, social and ethica impact assessment. *Computer Law & Security Review*, 34 (4), 2018, p. 754-772. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3225749>. Acesso em: 16 out. 2019.

_____. Competitive value of data protection: the impact of data protection regulation on online behaviour. *International Data Privacy Law*, v. 3, n. 4. p. 229-238, 2013.

MAYER, Jonathan; NARAYANAN, Arvind. Do not track: universal web tracking opt-out*IAB*

Internet Privacy Workshop Position Paper, p. 1-2, Nov. 2010.

MCDONALD, Aleecia M; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. *Journal of Law and Policy for Information Society*, v. 4, p. 543-570, 2008.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. *Revista de Direito do Consumidor*, ano 20, v. 79, p. 45-80, jul./set. 2011.

MIRAGEM, Bruno. Responsabilidade por dano na sociedade de informação e proteção d consumidor: desafios atuais da regulação jurídica da internet. *Revista de Direito do Consumidor*, ano 18, n. 70, p. 41-91, abr./jun. 2009.

MONTELEONE, Shara; LE MÉTAYER, Daniel. Automated consent through privacy agents: Legal requirements and technical architecture. *Computer law & security review*, 25, p. 136-143, 2009.

MORATO, Antonio Carlos. Quadro geral dos direitos da personalidade. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 106-107, p. 121-158, dez. 2011/jan. 2012.

MOSES, Lyria Bennett. How to think about law, regulation and technology: problems witl 'technology' as a regulatory target. *Law, Innovation and Technology*, v. 5, p. 1-20, 2013.

MULLIGAN, Deirdre K; KING, Jennifer. Bridging the Gap between Privacy and Design. *University of Pennsylvania Journal of Constitutional Law*, v. 14, n. 4, p. 989-1034, 2012. Disponível em: <http://ssrn.com/abstract=2070401>. Acesso em: 19 ago. 2014.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and Fallacies of "Personally Identifiabl Information". *Communications of the ACM*, v. 53, n. 06, p. 24-26, June 2010. Disponível em: <www.cs.utexas.edu/~shmat/shmat_cacm10.pdfý>. Acesso em: 2 abr. 2014.

NISSENBAUM, Helen. Privacy as contextual integrity. *Washington Law Review*, v. 79, p. 119-157, 2004.

NOVOTNY, Alexander; SPIEKERMANN, Sarah. Personal information markets and privacy: a ne model to solve the controversy, p. 1-16, Aug. 2012. Disponível em: <http://ssrn.com/abstract=2148885>. Acesso em: 14 mar. 2014.

OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymizatio (August 13, 2009). *UCLA Law Review*, v. 57, p. 1701-1777, 2010; *Colorado Law Legal Studies Research Paper*, n. 9-12. Disponível em: <http://ssrn.com/abstract=1450006>. Acesso em: 2 abr. 2014.

PARAMAGURU, Abi; VAILE, David; WATERS, Nigel; GREENLEAF, Graham. Distinguish PETs from PITs: developing technology with privacy in mind (May 12, 2008). *UNSW Law Research Paper*, n. 35, p. 1-26. Disponível em: <http://ssrn.com/abstract=1397402>. Acesso em: 13 out. 2015.

PICKER, Randal C. Online advertising, identity and privacy. *Chicago Law & Economics, working papers series*, The Law School of University of Chicago, p. 1-49, June 2009. Disponível em <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1428065>. Acesso em: 12 fev. 2014.

RAAB, Charles D.; DE HERT, Paul. The regulation of technology: policy tools and policy actor (November 1, 2007). *TILT Law & Technology Working Paper Series*, n. 3, p. 1-25, 2007.

REAGLE, Joseph; CRANOR, Lorrie Faith. The platform for privacy preferences: world-wide we consortium's platform for privacy preferences project, web site privacy. *Communications of the ACM*, v. 42, n. 2, p. 48-55, Feb. 1999.

REED, Chris. Taking Sides on Technology Neutrality. *SCRIPT-ed*, v. 4, n. 3, set. 2007.

RODATÀ, Stefano. Persona, riservatezza, identità.*Rivista Crtica del Diritto Privato*, ano XV, n. 4, p. 583-609, dic. 1997.

RUBINSTEIN, Ira; GOOD, Nathan. Privacy by Design: A Counterfactual Analysis of Google a Facebook Privacy Incidents. *Berkeley Technology Law Journal*, n. 28, 2013; *NYU School of Law*, *Public Law Research Paper*, n. 12-43. p. 1333-1413. Disponível em: <http://dx.doi.org/10.2139/ssrn.2128146>. Acesso em: 19 ago. 2014.

_____; HARTZOG, Woodrow. Anonymization and Risk (August 17, 2015),*91 Washington Law Review* 703, 2016; *NYU School of Law, Public Law Research Paper n. 15-36* Disponível em: <https://ssrn.com/abstract=2646185>.

_____; LEE, Ronald D.; SCHWARTZ, Paul M. Data Mining and Internet Profiling: Emergi Regulatory and Technological Approaches. *University of Chicago Law Review*, v. 75, p. 261, 2008.

SCHWARTZ, Paul M. Internet privacy and state. *Connecticut Law Review*, v. 32, p. 815-859, 2000.

_____. Privacy and democracy in cyberspace. *Vanderbilt law review*, v. 52, p. 1609-1701, 1999.

_____. Property, privacy, and personal data. *Harvard Law Review*, v. 117, n. 7, p. 2055-2128, May 2004.

_____; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiab Information. *Review Law N.Y.U.*, p. 1814-1894, 2011. Disponível em: <http://scholarship.law.berkeley.edu/facpubs/1638>. Acesso em: 7 abr. 2014.

SEM, A. Fulya. Communication and human rights.*Social and Behavioral Sciences Review*, n. 174, p. 2813-2817, 2015.

SMIT, Edith G.; NOORT, Guda Van; VOORVELD, Hilde A.M. Understanding online behaviour advertising: User knowledge, privacy concerns and online coping behavior in Europe. *Computers in Human Behavior*, v. 32, p. 16-22, 2014.

SMITIS, Spiros. Reviewing Privacy in an Information Society*University of Pensilvania Law Review*, v. 135, p. 707-747, 1987.

SOLOVE, Daniel. Introduction: Privacy self-management and the consent dilemma*Harvard law review*, v. 126, p. 1880-1903, 2013. Disponível em: <http://www.harvardlawreview.org/media/pdf/vol126_solove.pdf>. Acesso em: 5 jan. 2014.

_____; HARTZOG, Woodrow. The FTC and the New Common Law of Privacy*Columbia Law Review*, 114, p. 583-676, 2014. Disponível em: <http://ssrn.com/abstract=2312913> ou

<http://dx.doi.org/10.2139/ssrn.2312913>. Acesso em: 27 jul. 2015.

SPIEKERMANN, Sarah; Cranor, Lorrie Faith. Engineering Privacy. *IEEE transactions on software engineering*, v. 35, n. 1, p. 67-82, Jan./Feb. 2009.

STRANDBURG, Katherine J. Free Fall: The Online Market's Consumer Preference Disconnect. *NYU School of Law, Public Law Research Paper*, n. 13-62; *NYU Law and Economics Research Paper*, n. 13-34, p. 94-172, Oct. 2013. Disponível em: <http://ssrn.com/abstract=232396>.

SUNSTEIN, Cass S.; THALER, Richard H. O paternalismo libertário não é uma contradição e termos. Trad. Fernanda Cohen. *Civilistica.com*: revista eletrônica de direito civil. Rio de Janeiro: ano 4, n. 2, 2015. Disponível em: <http://civilistica.com/wp-content/uploads/2015/12/Sunstein-e-Thaler-trad.-Cohen-civilistica.com-a.4.n.2.20151.pdf>. Acesso em: 4 jan. 2016.

TADEU, Silney Alves. Um novo direito fundamental: algumas reflexões sobre a proteção da pessoa e o uso informatizado de seus dados pessoais. *Revista de Direito do Consumidor*, ano 20, v. 79, p. 83-100, jul./set. 2011.

TENE, Omer. Privacy law's midlife crisis: a critical assessment of the second wave of global privacy laws. *Ohio State Journal*, v. 74, p. 1217-1261, 2013.

_____; POLONETSKY, Jules. Privacy in the age of big data: a time for big decisions. *Rev. Online Stanford*, v. 63, p. 63-69, Feb. 2012.

_____; _____. To track or 'do not track': Advancing Transparency and Individual Control in Online Behavioral Advertising (August 31, 2011). *Minnesota Journal of Law, Science & Technology*, v. 13, n. 1, p. 1-55, 2012.

TOMASETTI JÚNIOR, Alcides. O objetivo da transparência e o regime jurídico dos deveres riscos da informação nas declarações negociais para consumo. *Revista de Direito do Consumidor*, São Paulo, n. 4, p. 52-90.

UTZ, Christine; DEGELING, Martin; FAHL, Sascha; SCHAUB, Florian; HOLZ, Thors (Un)informed consent: studying GDPR consent notices in the field. *2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*, Novembro 11–15, 2019, London, United Kingdom. ACM, New York, NY, USA. Disponível em <https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2019/09/05/uninformed-consent_Yl7FPEh.pdf>. Acesso em: 3 out. 2019.

ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Informatio Civilization. *Journal of Information Technology*, 4 abr. 2015, p. 77. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754>.

Teses, dissertações e monografias

BRITO CRUZ, Francisco. *Direito, democracia e cultura digital: a experiência de elaboração*

legislativa do marco civil da internet. Dissertação (Mestrado) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2009.

LIMA, Cíntia Rosa Pereira de.*Validade e obrigatoriedade dos contratos de adesão eletrônicos (*shrink-wrap *e* click-wrap*) e dos termos e condições de uso (*browse-wrap*)*: um estudo comparado entre Brasil e Canadá. Tese (Doutorado) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2009.

MARTINS-COSTA, Judith*Pessoa, personalidade, dignidade: ensaio de uma qualificação*. Tese (Livre-docência) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2003.

MARZAGÃO, Nelcina C. de O. Tropardi*Da informação e dos efeitos do excesso de informação no direito do consumidor*. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2005.

MATIUZZO, Marcela. Propaganda Online e privacidade: o varejo de dados pessoais na perspectiv antitruste, p. 65 Disponível em: <http://www.seae.fazenda.gov.br/premio-seae/edicoes-anteriores/edicao-2014/tema1-3lugar-MM.pdf>. Acesso em: 20 jun. 2015.

MENDES, Laura Schertel.*Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. Dissertação (Mestrado em Direito) – Faculdade de Direito da Universidade de Brasília. Brasília, 2008.

PURTOVA, Nadezhda.*Property rights in personal data: an european perspective*. Tese (Doutorado) – Faculdade de Direito da Universidade de Tilburg. Tilburg, 2011. Disponível em: <https://www.academia.edu/4373515/Property_rights_in_personal_data_A_European_perspecti Acesso em: 10 ago. 2015.

SILVA, Daniel Pereira Militão.*Desafios do ensino jurídico na pós-modernidade: da sociedade agrícola e industrial para a sociedade da informação*. Dissertação (Mestrado) – Faculdade de Direito da Pontifícia Universidade Católica de São Paulo. São Paulo, 2009.

TOMASEVICIUS FILHO, Eduardo*Informação assimétrica, custos de transação, princípio da boa-fé*. Tese (Doutorado) – Faculdade de Direito da Universidade de São Paulo. São Paulo 2007.

Documentos jurídicos, relatórios científicos e contribuições a consultas públicas legislativas

ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 02/2010 sobre publicida comportamental em linha. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pt.pdf>. Acesso em: 14 fev. 2014.

_____. Opinion 02/2013 on apps on smart *devices*. Fevereiro, 2013. p. 15 (nota de rodapé 34). Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>. Acesso em: 15 out. 2015.

_____. Opinion 3/2013 on Purpose Limitation. Disponível em: <http://ec.europa.eu/justice/data-

protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. Acesso em: 2 dez. 2015.

BIONI, Bruno Ricardo et al. Contribuição do grupo de políticas públicas em acesso à informação d universidade de São Paulo (GPOPAI/USP) à consulta pública do anteprojeto de lei de proteçã de dados pessoais. São Paulo, p. 9-13, 2015. Disponível em: <https://gpopai.usp.br/wordpress/wp-content/uploads/2015/08/Contribuicao-GPoPAI-Dados-Pessoais_Diagramada.pdf>.

COMMISSION OF THE EUROPEAN COMMUNITIES. Promoting data protection by pri enhancing technologies (pets)', p. 3, 2007. Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0228&from=EN>. Acesso em: 13 out. 2015.

COUNCIL OF EUROPE. Consultative Committee of the Convention for the Protection of Individua with Regard to Automatic Processing of Personal Data (Convention 108) –*Report on Artificial Intelligence "Artificial Intelligence and Data Protection: Challenges and Possible Remedies"*, 2019. Disponível em: <https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6>. Acesso em: 16 out. 2019.

DONEDA, Danilo.*A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia/Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010.

ELETRONIC PRIVACY INFORMATION CENTER/EPIC; CENTER DIGITAL DEMOCRACY. Privacy Groups File FTC Complaint Vs. Facebook-WhatsApp Dea Disponível em: <http://allfacebook.com/ftc-complaint-whatsapp_b129849?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=Feed%3A+allfacebook+%28Fac Acesso em: 14 mar. 2014.

EXECUTIVE OFFICE OF THE PRESIDENT PRESIDENT'S COUNCIL OF ADVISOR SCIENCE AND TECHNOLOGY. Report to the president big data and privacy: a technologic perspective. p. 17-18. Disponível em: <https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_pr_may_2014.pdf>. Acesso em: 4 jan. 2016.

FEDERAL TRADE COMMISSION/FTC. Data brokers: a call for transparency, p. i, May 20 Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em: 11 jun. 2015.

_____. Ehavioral Advertising: Tracking, Targeting, and Technology, 2007. Disponível em: <http://www.ftc.gov/news-events/events-calendar/2007/11/ehavioral-advertising-tracking-targeting-technology>. Acesso em: 10 fev. 2014.

_____. Protecting consumer privacy in an era of rapid change, Mar. 2012. Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

Acesso em: 13 out. 2015.

FUTURE OF PRIVACY. *City of Seattle: Open data risk assessment*, 2018. Disponível em: <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf>. Acesso em: 4 out. 2019.

GENERAL DATA PROTECTION REGULATION EU. Disponível e <http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf>. Acesso em: 16 dez. 2015.

GOMEZ, Joshua, et al. Know Privacy: Report of University of California, Berkeley, p. 8. Disponíve em: <http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf>. Acesso em: 11 jun. 2015.

INFORMATION COMMISSIONER'S OFFICE (ICO). *Anonymisation: managing data protection risk code of practice*, 2012. Disponível em: <https://ico.org.uk/media/1061/anonymisation-code.pdf>. Acesso em: 4 out. 2019.

_____. *Update report into adtech and real time bidding*, 2019. Disponível em: <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>. Acesso em: 20 out. 2019.

MOLON, Alessandro. Relatório ao projeto de Lei nº 2.126/2011. Disponível em <http://www.camara.gov.br/internet/agencia/pdf/MCI_2014_02_12_Relatorio.doc>. Acesso em: 24 nov. 2015.

OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOW PERSONAL DATA. Elaboração André-Pascal. França: OECD Publications Service, 2011. 32.

ROSENFELD, Dana B.; HUTNIK, Alysa Zeltzer. Data security contract clauses for service provid arrangements (pro-customer). *Practical Law Company*, 2011. Disponível em: <https://iapp.org/media/pdf/resource_center/Rosenfeld_Hutnik_Contract-clauses_Service-provider.pdf>. Acesso em: 20 out. 2019.

ROSINA, Mônica Guine. SILVA, Alexandre Pacheco da et al. Contribuição do grupo de pesquisa em inovação da Faculdade de Direito da Fundação Getúlio Vargas ao anteprojeto de lei de proteção de dados pessoais. Disponível em: <http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/07/ef64f4d964b58ecf1a9a5040efc25464.pdf>. Acesso em: 25 out. 2015.

SEBASTIAN, Kent. No Such Thing as a Free Lunch: Consumer Contracts and "Free Services Relatório da Public Interest Advocacy Centre's, p. 6. Disponível em <http://www.piac.ca/privacy/canadian_consumers_need_more_protection_dealing_with_free_se Acesso em: 11 jun. 2015.

THE OECD PRIVACY FRAMEWORK 2013. Disponível e <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 25 jul. 2015.

TUROW, Joseph; HENESSY, Michael; DRAPER, Nora. *The tradeoff fallacy*: how marketers are

misrepresenting and opening them up to exploitation. Disponível em: <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf>. Acesso em: 8 set. 2015.

ZANATTA, Rafael A. F. *Consentimento forçado?* Uma avaliação sobre os novos termos de uso do WhatsApp e as colisões com o Marco Civil da Internet. São Paulo: IDEC, 2016.

Revistas

Entenda o que é *Big Data*: o megafenômeno digital que transforma em riqueza dados pessoais, posts, tuítes, e-mails e cliques. *Revista Veja*, ano 46, n. 20, p. 71-81, 15 maio 2013.

Revista.Br: publicação do Comitê Gestor da Internet, ano 4, n. 5, nov. 2013.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, jan. 2018.

Palestras e congressos

ANTONIALLI, Dennys*Estado e cidadão: novos desafios jurídicos para a proteção de dados no Brasil*. Evento realizado pela Faculdade de Direito da Fundação Getulio Vargas, Junho 2013 Disponível em: <http://www.youtube.com/watch?v=aPSfG_GhoTo>. Acesso em: 13 mar. 2014.

CRUZ, Fransico Brito. *Seminário Marco Civil da Internet*: obrigatoriedade de Guarda de Registros, Medidas de Segurança e Encriptação. Evento realizado pela Protest. Disponível em <https://www.youtube.com/watch?v=cwQD0QpLSW4>. Acesso em: 6 set. 2015.

DONEDA, Danilo. Internet e legislação. In: IV FÓRUM DA INTERNET DO BRASIL REALIZA PELO COMITÊ GESTOR DA INTERNET/CGI. São Paulo, 25 abr. 2014.

FISHER, Luciana. Revista propaganda: a publicitária na mídia segmentada (um estudo de caso). In XIV CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO. Campo Gr 2001. Disponível em: <http://www.portcom.intercom.org.br/pdfs/147689473119175129741594975834332170614.pdf Acesso em: 12 fev. 2014.

HANSEN Marit et al. Assessing PET Maturity. In: IFIP SUMMER SCHOOL (Universidade Edimburgo). Workshop, Edimburgo (19 de agosto de 2015).

HOOFNAGLE, Chris Jay. URBAN, Jennifer M. Li, Su. Privacy and modern advertising: most U internet users want 'do not track' to stop collection of data about their online activities. In: AMSTERDAM PRIVACY CONFERENCE, 2012. Disponível e <http://ssrn.com/abstract=2152135>. Acesso em: 4 set. 2015.

MCDONALD, Aleecia; PEHA, Jon M. Track gap: policy implications of user expectations for th 'do not track' internet privacy feature. In: TPRC CONFERENCE (September 25, 2011 Disponível em: <http://ssrn.com/abstract=1993133>.

MOLON, Alessandro.*Marco civil da internet e neutralidade da rede*. Organização Centro

Acadêmico XI de Agosto da Faculdade de Direito da Universidade de São Paulo. 20 mar. 2014.

ODLYZKO, Andrew. Privacy, Economics, and Price Discrimination on the Internet (July 27, 2003) In: ICEC2003: FIFTH INTERNATIONAL CONFERENCE ON ELECTRONIC COMME N. Sadeh, ed., ACM, 2003. Disponível em: <http://ssrn.com/abstract=429762> ou <http://dx.doi.org/10.2139/ssrn.429762> Acesso em: 15 abr. 2014.

ROSSOGLOU, Kostas. Do-it yourself privacy protection. In: COMPUTERS, PRIVACY & DA PROTECTION INTERNATIONAL CONFERENCE, Jan. 2015. Disponível <https://www.youtube.com/watch?v=M_o_uaZwB2Y>. Acesso em: 7 ago. 2015.

Prefácios, apresentações e introdução de obras

BODIN, Maria Celina. Apresentação do autor e da obra. In: RODATÀ, Stefano. *A vida na sociedade da vigilância.* Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008 p. 1-12.

DONEDA, Danilo. Prefácio. In: BESSA, Leonardo Roscoe. *Cadastro positivo*: comentários à Lei 12.414, de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011. p. 9-11.

LAFER, Celso. Apresentação. In: BOBBIO, Norberto. *A era dos direitos*. Rio de Janeiro: Elsevier, 2004. p. I-XXIX.

LISBOA, Roberto Senise. Prefácio. In: MATTOS, Karla Cristina da Costa e Silva. *O valor econômico da informação nas relações de consumo*. São Paulo: Almedina, 2012. p. 13-19.

LYON, David. Introdução. In: BAUMAN, Zygmunt; LYON, David. *Vigilância líquida*. Rio de Janeiro, Zahar, 2014. p. 9-24.

Outros textos em meios eletrônicos

Agreement on Commission's EU data protection reform will boost Digital Single Market. Disponível em: <http://europa.eu/rapid/press-release_IP-15-6321_en.htm>. Acesso em: 15 dez. 2015.

Air passager data. Disponível em: <http://www.migalhas.com/mostra_noticia.aspx?op=true&cod=154037>. Acesso em: 15 abr. 2013.

Algoritmo prevê, no Facebook, quando um namoro vai acabar. Disponível em: <http://info.abril.com.br/noticias/ciencia/2013/10/algoritmo-preve-no-facebook-quando-um-namoro-vai-acabar.shtml>. Acesso em: 8 fev. 2014.

AMADEU, Sérgio. *Marco civil e a proteção da privacidade: após polêmica sobre espionagem, proteção virtual se tornou um dos três pilares do marco civil*. Disponível em: <http://www.dicyt.com/noticia/marco-civil-e-a-protecao-da-privacidade>. Acesso em: 24 nov. 2015.

ANDERAÓS, Ricardo. *Internet supera TV em faturamento publicitário nos EUA pela primeira vez*. Disponível em: <http://www.brasilpost.com.br/2014/04/11/internet-tv-

faturamento_n_5134262.html>. Acesso em: 20 dez. 2014.

ANTONIALLI, Dennys Marcelo. *Privacy and International Compliance: When Differences Become an Issue*. p. 13-16. Disponível em: <https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/viewFile/1165/1470>. Acesso em: 13 dez. 2013.

_____ et al. *InternetLab reporta: consultas públicas nº 4*. Disponível em: <http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-consultas-publicas-no-04/>. Acesso em: 5 maio 2015.

Após espionagem, Dilma pede urgência de votação do Marco Civil da Internet. Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/apos-espionagem-dilma-pede-urgencia-de-votacao-do-marco-civil-da-internet-9912712>. Acesso em: 3 jun. 2015.

ARAGÃO, Alexandre. *Dilma sanciona Marco Civil na abertura do NETMundial* Disponível em: <http://www1.folha.uol.com.br/tec/2014/04/1444200-dilma-sanciona-marco-civil-na-abertura-do-netmundial.shtml>. Acesso em: 9 jun. 2015.

BANISAR, David. *National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map* Disponível em: <http://ssrn.com/abstract=1951416>. Acesso em: mar. 2015.

BARBARO, Michael; ZELLER JR, Tom. *A Face is Exposed for AOL Searcher No. 4417749*. Disponível em: <http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=0>. Acesso em: 2 abr. 2014.

BELLAMY, Bojana; HEYDER, Markus. *Empowering Individuals Beyond Consent*. Disponível em: <https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Centre_Bellamy_H Acesso em: 30 jul. 2015.

Big data: what is it and how can it help? Disponível em: <http://www.theguardian.com/news/datablog/2012/oct/26/big-data-what-is-it-examples>. Acesso em: 8 mar. 2014.

BIONI, Bruno Ricardo. Brasil precisa ser competitivo em uma economia de dados. *Jornal Valor Econômico*, jul. 2018. Disponível em: <https://www.valor.com.br/opiniao/5669703/pais-precisa-ser-competitivo-em-uma-economia-de-dados>.

_____. *De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados pessoais*. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018>.

_____. Nova política de privacidade do WhatsApp: questões a serem debatidas sobre consentimento. *Digital Watch*, n. 13, p. 5-7, Ago. 2016. Disponível em: <http://www.academia.edu/28751735/Nova_Politica_de_Privacidade_do_Whatsapp_questoes_ Acesso em: 12 jan. 2017.

_____. *Por que proteção de dados importa?* TEDxPinheiros, 2018. Disponível en

<https://www.youtube.com/watch?v=TzI5VfvQA6I>.

_____. *WhatsApp e a chance para uma nova discussão*. Disponível em: <http://www.telesintese.com.br/nova-politica-de-privacidade-do-whatsapp-chance-de-se-discutir-modelos-de-negocios-e-praticas-de-tratamento-de-dados-menos-invasivos-privacidade/>. Acesso em: 12 jan. 2017.

_____; MONTEIRO, Renato Leite*Principais inovações da nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais/APLPDP*. Disponível em: <https://gpopai.usp.br/?page_id=319>. Acesso em: 3 jan. 2016.

_____; _____. *Que tal uma pizza de tofu com rabanetes: você vai adorar*. Disponível em: <http://www.brasilpost.com.br/renato-leite-monteiro/que-tal-uma-pizza-de-tofu_b_7561906.htm>. Acesso em: 24 nov. 2015.

_____; RIBEIRO, Márcio Moretto*A transposição da dicotomia entre o público e o privado*. Disponível em: <http://jota.info/a-transposicao-da-dicotomia-entre-o-publico-e-o-privado>. Acesso em: 25 out. 2015.

BRILL, Julie.*Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions* Disponível em: <http://www.ftc.gov/system/files/documents/public_statements/202151/140220princetonbigdata_ Acesso em: 11 abr. 2014.

Celular torna-se o principal dispositivo de acesso à Internet, aponta Cetic.br. Disponível em: <http://cetic.br/noticia/celular-torna-se-o-principal-dispositivo-de-acesso-a-internet-aponta-cetic-br/>.

CAMPOS, Elisa; CANDIDO, Fabiano*Como a computação quântica vai abalar os negócios para sempre*. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2019/02/como-computacao-quantica-vai-abalar-os-negocios-para-sempre.html>. Acesso em: 4 out. 2019.

CHOWDHRY, See Amit.*Why facebook forced users to download a separate messenger app*. Disponível em: <http://www.forbes.com/sites/amitchowdhry/2014/11/11/why-facebook-forced-users-to-download-a-separate-messenger-app/>. Acesso em: 25 jan. 2015.

Comércio eletrônico no Brasil. Disponível em: <http://www.b2wdigital.com/institucional/comercio-eletronico-no-brasil>. Acesso em: 30 dez. 2015.

CONSTINE, Josh*Facebook is forcing all users to download messenger by ripping chat out of its main apps*. Disponível em: <http://techcrunch.com/2014/04/09/facebook-messenger-or-the-highway/>. Acesso em: 26 nov. 2015.

CRANOR, Lorrie.*P3P is dead, long live P3P!* Disponível: em <http://lorrie.cranor.org/blog/2012/12/03/p3p-is-dead-long-live-p3p/>. Acesso em: 15 out. 2015.

_____; MCDONALD, Aleecia M*Beliefs and Behaviors: Internet Users' Understanding of*

Behavioral Advertising. p. 1 Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092>. Acesso em: 15 jan. 2014.

DE VRIES, Jennifer Valentino.*The Economics of Surveillance*. Disponível em: <http://blogs.wsj.com/digits/2012/09/28/the-economics-of-surveillance/>. Acesso em: 20 jun. 2015.

DEMETRIO, Amanda. *São tantas emoções: empresas e pesquisadores buscam maneiras de captar, usar e interpretar os sentimentos dos usuários que navegam na internet*. Disponível em: <http://www1.folha.uol.com.br/fsp/tec/tc0405201101.htm>. Acesso em: 18 fev. 2014.

DEWEY, Caitlin.*9 answers about Facebook's creepy emotional-manipulation experiment*. Disponível em: <https://www.washingtonpost.com/news/the-intersect/wp/2014/07/01/9-answers-about-facebooks-creepy-emotional-manipulation-experiment/>. Acesso em: 26 nov. 2015.

DIAS, Roberto. Análise:*Aquisição do WhatsApp une duas visões de mundo opostas*. Disponível em: <http://www1.folha.uol.com.br/tec/2014/02/1414823-analise-aquisicao-do-whatsapp-une-duas-visoes-de-mundo-opostas.shtml>. Acesso em: 14 mar. 2014.

Display advertising technology landscape. Disponível em: <http://www.lumapartners.com/lumascapes/display-ad-tech-lumascape/>. Acesso em: 11 jun. 2015.

DONEDA, Danilo.*O IPv6 e a internet das coisas*. 05.01.2011. Disponível em: <http://observatoriodainternet.br/o-ipv6-e-a-internet-das-coisas>. Acesso em: 14 abr. 2014.

Dropbox política de privacidade. Disponível em: <https://www.dropbox.com/privacy#privacy>. Acesso em: 14 mar. 2014.

DUHIGG, Charles.*How companies learn your secrets*. Disponível em: <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0>. Acesso em: 8 mar. 2014.

ECKERSLEY, Peter.*What Does the "Track" in "Do Not Track" Mean?* Disponível em: <https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean>. Acesso em: 13 out. 2015.

EU privacy watchdogs give Google guidelines to change privacy practices. Disponível em: <http://www.euractiv.com/sections/infosociety/eu-privacy-watchdogs-give-google-guidelines-change-privacy-practices-308740>. Acesso em: 28 nov. 2015.

Facebook anuncia compra do aplicativo WhatsApp por US$ 16 bilhões Disponível em: <http://tecnologia.uol.com.br/noticias/redacao/2014/02/19/facebook-anuncia-compra-do-aplicativo-whatsapp.htm>. Acesso em: 14 mar. 2013.

FERREIRA, Ana Paula*O que são flash cookies? Por que é importante removê-los?* Disponível em: <http://www.tecmundo.com.br/seguranca/3046-o-que-sao-flash-cookies-por-que-e-importante-remove-los-.htm>. Acesso em: 4 set. 2015.

FILOMENO, Leonardo*10 termos absurdos de uso do Messenger do Facebook*. Disponível em: <http://manualdohomemmoderno.com.br/tecnologia/10-absurdos-termos-de-uso-messenger-facebook>. Acesso em: 28 nov. 2015.

FIORELLA, Sam*The insidiousness of Facebook Messenger's android mobile app permissions*. Disponível em: <http://www.huffingtonpost.com/sam-fiorella/the-insidiousness-of-face_b_4365645.html?utm_hp_ref=tw>. Acesso em: 25 jan. 2015.

FRANÇA, Guilherme.*Entenda melhor o NoSQL e o Big Data* Disponível em: <http://blog.websolute.com.br/entenda-melhor-o-nosql-e-o-big-data/>. Acesso em: 8 mar. 2014.

Global Privacy Enforcement Network (GPEN). Disponível em: <https://www.privacyenforcement.net/about_the_network>. Acesso em: 10 jun. 2015.

Google adwords. Disponível em: <https://accounts.google.com/ServiceLogin?service=adwords&continue=https://adwords.google.com/um/gaiaauth?apt%3DNone%26ltmpl%3Djfk&hl=pt_BR_BR&ltmpl=jfk&passive=86400&skipvpage=true&sa Acesso em: 14 fev. 2014.

Google confirma a compra da Waze. Disponível em: <http://g1.globo.com/tecnologia/noticia/2013/06/google-confirma-compra-da-waze.html>. Acesso em: 17 fev. 2014.

Google's privacy policy 'too vague'. Disponível em: <http://www.theguardian.com/technology/2012/mar/08/google-privacy-policy-too-vague>. Acesso em: 28 nov. 2015.

Google Flu. Disponível em: <http://www.google.org/flutrends/intl/pt_br/about/how.html>. Acesso em: 8 mar. 2014.

GOULART, Guilherme; SERAFIAN, Vinicius. Data Brokers *Privacidade e Discriminação*. Disponível em: <http://www.segurancalegal.com/2014/06/episodio-52-databrokers-privacidade-e.html>. Acesso em: 11 jun. 2015.

HAYASHI, Eduardo Issao.*10 termos de uso do Facebook Messenger que vão deixar você boquiaberto*. Disponível em: <http://www.tecmundo.com.br/facebook/60271-10-termos-uso-facebook-messenger-deixar-voce-boquiaberto.htm>. Acesso em: 26 nov. 2015.

HOLLAND, H. Brian. Privacy Paradox 2.0 (April 4, 2010). Disponível em <http://ssrn.com/abstract=1584443>. Acesso em: 9 set. 2015.

IAB Europe. Consumers Driving the Digital Uptake: The economic value of online advertising based services for consumers, p. 7, Sept. 2010. Disponível em: <http://www.iabeurope.eu/files/7113/7000/0832/white_paper_consumers_driving_the_digital_u (IAB Europe Sept 2010). Acesso em: 13 mar. 2014.

Informational Commsioner's Office. Global survey finds 85% of mobile apps fail to provide basic privacy information. Disponível em: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/09/global-survey-finds-85-of-mobile-apps-fail-to-provide-basic-privacy-

information>. Acesso em: 20 set. 2015.

Interective Advertising Bureau/IAB. Disponível em: <www.iabbrasil.net>. Acesso em: 11 jun. 2015.

JÚNIOR, Hilário.*Facebook e Serasa fecham parceria para anúncios segmentados por renda*. Disponível em: <https://www.linkedin.com/pulse/facebook-e-serasa-fecham-parceria-para-anuncios-por-renda-junior>. Acesso em: 28 nov. 2015.

KELLEY, Patrick Gage; BRESEE, Joanna; CRANOR, Lorrie Faith; REEDER, Robert W. *"Nutrition Label" for Privacy*. Disponível em: <https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf>. Acesso em: 25 out. 2015.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. *Private traits and attributes are predictable from digital records of human behavior*. Disponível em: <http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html>. Acesso em: 11 abr. 2014.

KOSKINS, Tasny.*Luxury brands: higher standards or just a higher mark-up?* Disponível em: <https://www.theguardian.com/sustainable-business/2014/dec/10/luxury-brands-behind-gloss-same-dirt-ethics-production>. Acesso em: 28 nov. 2016.

KROES, Neelie.*Speech – Online privacy: reinforcing trust and confidence*. Disponível em: <http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm>. Acesso em: 13 out. 2015.

KWASNY, Sophie. Convenção 108+.*Apresentação no IX Seminário de Privacidade do Comitê Gestor da Internet no Brasil*, 2018. Disponível em: <https://www.youtube.com/watch?v=X3zdwB2xi_E&list=PLQq8-9yVHyOZVGYJeegT8I-mHrWOPIiYh&index=6&t=0s>.

LANEY, Doug.*3D data management: Controlling data volume, velocity and variety*. Disponível em: <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>. Acesso em: 8 mar. 2014.

LARDINOIS, Frederic*Microsoft will remove "do not track" as the default setting in its new browsers*. Disponível em: <http://techcrunch.com/2015/04/03/microsoft-disables-do-not-track-as-the-default-setting-in-internet-explorer/#.wko2bl:vxwq>. Acesso em: 13 out. 2015.

LEMOS, Ronaldo.*Ou a sociedade acompanha internet ou a democracia começa a ficar em xeque*. Disponível em: <http://blogdomorris.blogfolha.uol.com.br/2014/04/08/ou-sociedade-acompanha-internet-ou-democracia-comeca-a-ficar-em-xeque/>. Acesso em: 20 abr. 2014.

LOMAS, Natasha.*Samsung Edits Orwellian Clause Out Of TV Privacy Policy* Disponível em: <http://techcrunch.com/2015/02/10/smarttv-privacy/#.bbciupd:yfMB>. Acesso em: 28 nov. 2015.

MALDOFF, Gabe.*Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization* Disponível em: <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/>. Acesso em: 4 out. 2019.

MCENTEGART, Jane. *Proposed 'do not track' specs would kill ie10's default dnt* . Disponível em:

<http://www.tomshardware.com/news/Microsoft-Internet-Explorer-IE-10-Do-Not-Track-DNT-Specifications,15920.html>. Acesso em: 13 out. 2015.

MOLON, Alessandro.*Apresentação do relatório do projeto de Lei do Marco Civil da Internet*. Disponível em: <https://www.youtube.com/watch?v=YE7wrCHqWFI>. Acesso em: 3 jun. 2015.

MOROZOV, Evgeny.*O perigo da publicidade baseada em emoções*. Trad. Paulo Migliacci. Disponível em: <http://www1.folha.uol.com.br/colunas/evgenymorozov/2013/12/1381821-o-perigo-da-publicidade-baseada-em-emocoes.shtml>. Acesso em: 10 dez. 2013.

NARAYANAN, Arvind; MAYER, Jonathan.*The trouble with ID cookies: why do not track must means do not collect*. Disponível em: <http://cyberlaw.stanford.edu/blog/2012/08/trouble-id-cookies-why-do-not-track-must-mean-do-not-collect>. Acesso em: 13 out. 2015.

NELSON, Brett.*The 'Freemium' Model: Top Flaws And Potent Fixes*. Disponível em: <http://www.forbes.com/sites/brettnelson/2013/07/23/the-freemium-model-top-flaws-and-potent-fixes/>. Acesso em: 14 mar. 2014.

Online display*: mercado brasileiro*. Disponível em: <http://pt.slideshare.net/DigiTalks/o-que-so-as-adnetworks-como-funcionam-quais-as-vantagens-e-como-esse-mercado-nos-eua-e-no-brasil>. Acesso em: 11 jun. 2015.

O que é internet das coisas. Disponível em: <http://www.futurecom.com.br/blog/o-que-e-a-internet-das-coisas/>. Acesso em: 14 abr. 2014.

O que o chip sensor de movimentos m7 da apple pode fazer. Disponível em: <http://www.technologyreview.com.br/printer_friendly_article.aspx?id=43921>. Acesso em: 18 fev. 2014.

OPSAHL, Kurt.*Facebook's Eroding Privacy Policy: a timeline*. Disponível em: <https://www.eff.org/deeplinks/2010/04/facebook-timeline>. Acesso em: 20 set. 2015.

PARRA, Henrique.*Privacidade como um bem comum:* privacy as a commons. Disponível em: <http://lavits.org/?p=1038&lang=pt>. Acesso em: 21 nov. 2015.

Privacy Groups File FTC Complaint Vs. Facebook-WhatsApp Deal Disponível em: <http://allfacebook.com/ftc-complaint-whatsapp_b129849?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=Feed%3A+allfacebook+%28Fac Acesso em: 14 mar. 2014.

RAMASASTRY, Anita.*Web sites change prices based on customers' habits*. Disponível em: <http://www.cnn.com/2005/LAW/06/24/ramasastry.website.prices/>. Acesso em: 15 abr. 2014.

REDING, Viviane. *Speech – Data protection reform: restoring trust and building the digital single market*. Disponível em <http://europa.eu/rapid/press-release_SPEECH-13-720_en.htm>. Acesso em: 12 dez. 2013.

RIBEIRO, Márcio Moretto. Criptografia como resistência à sociedade da vigilância. In: I SIMPÓSIO INTERNACIONAL LAVITS (Rede Latino-Americana de Estudos sobre Vigilân

Tecnologia e Sociedade). Disponível em: <https://www.youtube.com/watch?v=kyIX1na65DM>. Acesso em: 23 jul. 2015.

_____; Otavio Luiz. *Marco Civil e opção do legislador pelas liberdades comunicativas*. Disponível em: <http://www.conjur.com.br/2014mai14/Direitocomparadomarcocivilopcaopelasliberdadescomu Acesso em: 20 maio 2014.

RODRIGUES JUNIOR, Otavio Luiz. *Primeiras considerações sobre o Marco Civil da Internet*. Disponível em: <http://www.conjur.com.br/2014-mai-14/direito-comparado-marco-civil-opcao-pelas-liberdades-comunicativas>. Acesso em: 20 maio 2014.

ROMER, Rafael. *Como as empresas estão usando sua geolocalização para campanhas de marketing*. Disponível em: <https://canaltech.com.br/publicidade/como-empresas-estao-usando-sua-geolocalizacao-para-campanhas-de-marketing-48533/>. Acesso em: 4 out. 2019.

Saiba como a 'internet das coisas' vai mudar seu cotidiano em breve. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/05/saiba-como-internet-das-coisas-vai-mudar-seu-cotidiano-em-breve.html>. Acesso em: 14 abr. 2014.

SAMPAIO, Luciana. *NoSQL, SQL e Big data* Disponível em: <http://lucianasampaio.wordpress.com/2013/10/03/nosql-sql-e-big-data/>. Acesso em: 8 mar. 2013.

SCHUNTER, Matthias; VAN HERREWEGHEN, Els; WAIDNER, Michael. *Expressive privacy promises: how to improve the platform for privacy preferences (P3P)*, p. 1-6. Disponível em: <http://www.w3.org/2002/p3p-ws/pp/ibm-zuerich.pdf>. Acesso em: 15 out. 2015.

Sensacionalista. Polícia apreende sapatilha que perseguia mulher há oito meses na internet. Disponível em: <http://sensacionalista.uol.com.br/2015/03/19/policia-apreende-sapatilha-que-perseguia-mulher-ha-seis-meses-na-internet/>. Acesso em: 11 jun. 2015.

SOLOVE, Daniel. Introduction: privacy self-management and the consent dilemma. *Harvard Law Review*, v. 126, 2013, p. 1.884. Disponível em: <http://www.harvardlawreview.org/media/pdf/vol126_solove.pdf>. Acesso em: 5 jan. 2014.

SOUZA, Carlos Affonso de. *Quadro Futuro: modo de usar junto ao jornal Globo News: Emoções de usuários são monitoradas na internet*. Disponível em: <http://globotv.globo.com/globo-news/jornal-globo-news/v/emocoes-de-usuarios-sao-monitoradas-na-internet/3081499/>. Acesso em: 18 fev. 2014.

STONE, Brad. Our Paradoxical Attitudes toward Privacy. *New York Times*, 02 de julho de 2008. Disponível em: <http://bits.blogs.nytimes.com/2008/07/02/our-paradoxical-attitudes-towards-privacy/.>. Acesso em: 9 set. 2015.

STUART, Heritage. *Beware the internet of things*. Disponível em: <http://www.theguardian.com/commentisfree/2014/jan/26/beware-internet-of-things-fridges>. Acesso em: 14 abr. 2014.

TAURION, Cezar. *Você sabe realmente o que é Big Data*. Disponível em: <https://www.ibm.com/developerworks/community/blogs/ctaurion/entry/voce_realmente_sabe_ lang=en>. Acesso em: 8 mar. 2013.

TEIXEIRA, Lucas. Data brokers e profiling: *vigilância como modelo de negócio*. Disponível em: <https://antivigilancia.org/boletim_antivigilancia/consultas/data-brokers-profiling>. Acesso em: 20 jun. 2015.

_____. *Teoricamente impossível: problemas com a anonimização de dados pessoais*. Disponível em: <https://antivigilancia.org/pt/2015/05/anonimizacao-dados-pessoais/>. Acesso em: 5 maio 2015.

The Chart That Shows WhatsApp Was A Bargain At $19 Billion. Disponível em <http://www.businessinsider.com/price-per-user-for-whatsapp-2014-#ixzz2vzLK2Kit>. Acesso em: 14 mar. 2014.

Tweetfeel. Disponível em: <http://www.tweetfeel.com/faq.php>. Acesso em: 18 fev. 2014.

Vendas de smartphones têm crescimento espetacular no Brasil. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/8-3-milhoes-de-smartphones-sao-vendidos-no-segundo-trimestre.> Acesso em: 18 fev. 2014.

Você trocaria sua privacidade por descontos em produtos? Disponível em: <http://www.privacidade.net/?p=62> ou <http://www.cartacapital.com.br/sociedade/voce-trocaria-sua-privacidade-por-descontos-em-produtos-4348.html>. Acesso em: 12 set. 2015.

W3C. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification p. 3. Disponível em: <http://www.w3.org/TR/P3P11/>. Acesso em: 15 out. 2015.

_ _ _ _ _ _ . *Tracking Protection Working Group Charter*. Disponível em: <http://www.w3.org/2011/tracking-protection/charter-draft.html>. Acesso em: 13 out. 2015.

WEBER, Rof H. *Internet of Things: New security and privacy challenges*. Disponível em: <https://www.academia.edu/32006659/Internet_of_Things_New_security_and_privacy_challeng Acesso em: 14 abr. 2014.

WhatsApp e aplicativos de mensagem ultrapassam SMS em 2012 Disponível em: <http://tecnologia.terra.com.br/internet/whatsapp-e-aplicativos-de-mensagem-ultrapassam-sms-em-2012,48db5334cc55e310VgnVCM4000009bcceb0aRCRD.html>. Acesso em: 18 fev. 2014.

What's the role of data scientists on online advertising? Disponível em: <http://www.theguardian.com/news/2013/nov/11/data-scientists-impact-online-advertising>. Acesso em: 8 mar. 2014.

When You Fall in Love, This Is What Facebook Sees Disponível em: <http://www.theatlantic.com/technology/archive/2014/02/when-you-fall-in-love-this-is-what-facebook-sees/283865/>. Acesso em: 8 mar. 2014.

WORLD ECONOMIC FORUM. *Big data, big impact: new possibilities for international development*. Disponível em:

<http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf>. Acesso em: 8 mar. 2014.