FACULDADE DE DIREITO DA UNIVERSIDADE DE BRASÍLIA

DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS NO CIBERESPAÇO:

A ACCOUNTABILITY COMO FUNDAMENTO DA LEX PRIVACY

Defesa de tese apresentada ao Programa de Pós-Graduação da Faculdade de Direito da Universidade de Brasília, como requisito à obtenção do título de Doutor.

Orientadora: Profa. Dra. Ana Frazão

Brasília

2019

THIAGO LUÍS SANTOS SOMBRA

DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS NO CIBERESPAÇO:

A ACCOUNTABILITY COMO FUNDAMENTO DA LEX PRIVACY

Banca Examinadora:

_____

Profa. Dra. Ana de Oliveira Frazão – Orientadora
PPGD/UnB

_____

Prof. Dr. Fabiano Hartman
PPGD/UnB

_____

Prof. Dr. Vinícius Borges
PPGD/IMED

_____

Prof. Dr. Eduardo Magrani
PPGD/FGV-RJ/ITS

_____

Prof. Dra. Ana Cláudia Farranha
PPGD/UnB

Brasília-DF, março de 2019.

Para Laura e Thomás, pelo incentivo dos sorrisos diários.

Para Nat, pelo amor durante a longa jornada.

“Hoje em dia a maior parte das corporações e dos governos prestam homenagem à minha individualidade, e prometem fornecer medicina, educação, e entretenimento customizados para as minhas necessidades e meus desejos, que são únicos, somente meus. Mas, para poder fazer isso, corporações e governos precisam primeiro me decompor em subsistemas bioquímicos, monitorar esses subsistemas com sensores ubíquos, e decifrar seu funcionamento com poderosos algoritmos. Nesse processo, será revelado que o indivíduo não é senão uma fantasia religiosa. A realidade será uma malha de algoritmos bioquímicos e eletrônicos, sem fronteiras bem definidas, e sem centros de controles individuais”

Yuval Noah Harari, Homo Deus: uma breve história do amanhã.

AGRADECIMENTOS

Essa tese foi escrita em meio a um processo de transição de vida e carreira, com o apoio incondicional da minha família. Os primeiros passos começaram em 2015, num estágio de pesquisa na London School of Economics-LSE, que revolucionou a minha forma de pensar. De lá para cá, as experiências internacionais se somaram à atuação prática na área da privacidade e proteção de dados. Seminários e congressos na *Information Commissioner's Office-ICO*, *Federal Trade Commission-FTC*, Sciences Po e Singularity University contribuíram ainda mais para o mote dessa tese: o pluralismo e a policontextualidade na construção de um modelo regulatório da privacidade e proteção de dados.

O acúmulo de experiências somente foi possível graças à influência dos professores Andrew Murray, Orla Lynskey e Paul Bernal, com quem pude mergulhar nas mais intensas reflexões nesse período. A convivência profissional com Phil Lee, Eduardo Ustaran, Richard Cumbley, Bojana Bellamy, Rosemary Jay, Daniel Cooper, Daniel Solove e os demais colegas da *International Association of Privacy Professionals-IAPP* também enriqueceram a perspectiva de estudo. Além disso, o convívio com os principais pesquisadores brasileiros no tema como Bruno Bioni, Vinícius Borges, Eduardo Magrani, Carlos Affonso, Alexandre Pacheco e Renato Leite Monteiro permitiram o amadurecimento de ideias até então incipientes.

A Universidade de Brasília tem um papel fundamental nessa tese. A intensidade das aulas e vida acadêmica influenciou sobremaneira na forma de refletir sobre o processo de regulação da privacidade. Aos meus alunos de graduação e aos colegas de doutorado Fábio Almeida, Fabrício Lunardi e Frederico Gonçalves um especial agradecimento, bem como aos professores da Pós-Graduação.

Sem uma orientação amiga e próxima, nenhuma ideia se converte em tese. Esse foi o papel da minha orientadora, Ana Frazão, que mesmo nos momentos de pouca clareza e indefinição esteve ao meu lado na tentativa de buscar caminhos provocadores. Além da gratidão pela orientação, o carinho pela dedicação e convicção no projeto.

Por fim, um agradecimento especial aos meus pais, minha esposa e filhos pelas privações e compreensão. Essa tese é integralmente dedicada vocês.

RESUMO

A regulação do ciberpespaço tem representado um expressivo desafio para os reguladores estatais e privados. A análise dos modelos de regulação estatal, corregulação e autorregulação demonstram que a disrupção, convergência e digitalização são fenômenos da modernidade que demandam adaptações segundo uma perspectiva plural e policontextual. Por essa razão, nessa tese se demonstrará que a regulação plural pode contribuir para uma mais adequada tutela da proteção dos dados pessoais e privacidade, dada a legitimidade dos meios de controle, promoção da autonomia e responsividade. A manifestação da corregulação e da regulação estatal sobre a privacidade e proteção de dados pessoais deixa de ser antagônica para se tornar complementar. Nesse cenário, o consentimento deixa de ser encarado como uma solução para todas as operações de tratamento de dados para ser reposicionado em conjunto com a *accountability*. Por meio da conjugação dos variados modelos regulatórios que se concebe a figura da *Lex Privacy*, enquanto arcabouço normativo construído sobre o papel complementar da *accountability* na tutela da privacidade e proteção dos dados pessoais.

Palavras-Chave: Proteção de Dados; Privacidade; Regulação; Pluralismo Jurídico; Ciberespaço; Policontextualidade ; Corregulação; Lex Privacy.

ABSTRACT

The regulation of the cyberspace is a considerable challenge that public and private regulators have been facing. By analyzing the main theories on the regulation of the cyberspace, one can identify its strong influence on the privacy and data protection regulatory perspectives. The analysis of the state regulatory models, co-regulation and self-regulation indicated that disruption, convergence and digitalization are modern phenomena that require adaptations from a plural and multi-contextual perspective. This thesis will focus on the main aspects of the autonomy, control and accountability in order to explain that consent needs to be subject to a deep review. The expression of the co-regulation and the government regulation on privacy and personal data protection become complementary, instead of antagonistic. It is in this combination of regulatory proceedings scenario that the Lex Privacy arises, as a normative framework built on the complementary role of accountability on the privacy and personal data protection.

Key Words: Data Protection; Privacy; Regulation; Legal Pluralism; Cyberspace; Multi-conceptuality; Co-regulation; Lex Privacy.

Sumário

INTRODUÇÃO

Com a expansão de novos padrões de comportamento social em torno de valores e condutas a que se convencionou denominar cibercultura[1], uma vez que identificada pelas características da disrupção (rompimento de padrões), da convergência (direcionamento de funcionalidades) e da digitalização (transformação de informações em bits)[2], um fórum dinâmico de interação entre indivíduos se emancipou, o ciberespaço[3]. A riqueza deste processo de desenvolvimento de um nicho tecnológico de interação entre os indivíduos envolveu fatores de todas as grandezas e foi capaz de impactar quase todos os meandros da vida em sociedade, tal como até então não se conhecia[4].

Dois dos principais campos afetados por esse processo de desenvolvimento foram a privacidade e os dados pessoais. Em virtude da proeminência de gerar benefícios diretos e indiretos de todas as espécies[5], a privacidade e a proteção dos dados pessoais foram colocadas no epicentro do bem-estar social e do modelo de inovação[6]. Com uma nova força motriz de geração de riqueza - os dados pessoais - , a privacidade se viu diante de uma encruzilhada: tornar-se um obstáculo rígido ao fluxo transacional de informações ou adaptar-se à nova realidade econômica para viabilizar ganhos sociais mais difundidos.

Embora esse processo tenha sido marcado por expressiva assimetria informacional, o fato é que os dados pessoais e a privacidade tornaram-se o motor do que se convencionou denominar da *data driven economy*[7], deveras marcada pelo suposto compartilhamento e pela capacidade de auto-geração de riqueza a partir de ferramentas como

---

[1] LÉVY, Pierre, **Cibercultura**, São Paulo: Editora 34, 2010, p. 25.

[2] GUIMARÃES JÚNIOR, Mário J. L., De pés descalços no ciberespaço: tecnologia e cultura no cotidiano de um grupo social on-line, **Horizontes Antropológicos**, v. 10, n. 21, p. 123–154, 2004.

[3] BOMSE, Amy Lynne, Dependence of Cyberspace, The, **Duke Law Journal**, v. 50, p. 1717, 2000.

[4] MONTEIRO, Silvana Drumond; PICKLER, Maria Elisa Valentim, O ciberespaço: o termo, a definição e o conceito, **DataGramaZero-Revista de Ciência da Informação**, v. 8, n. 3, p. 1–21, 2007.

[5] VELLOSO, Ricardo Vianna, O ciberespaço como ágora eletrônica na sociedade contemporânea, **Ci. Inf., Brasília**, v. 37, n. 2, p. 103–109, 2008.

[6] COHEN, Julie E., Cyberspace as/and Space, **Columbia Law Review**, v. 107, p. 210, 2007.

[7] **Data is giving rise to a new economy: Fuel of the future**, The Economist, disponível em: <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy>, acesso em: 7 fev. 2019.

o emprego da inteligência artificial e uso de algoritmos. Em outras palavras, um modelo de desenvolvimento econômico construído pelo poder informacional derivado, ou seja, baseado na possibilidade de geração exponencial de riqueza e proliferação de situações de poder por parte daqueles que possuem o controle sobre dados qualitativamente relevantes para o redimensionamento da privacidade.

A despeito dos ganhos proporcionados pela economia dirigida por dados na reformulação de políticas públicas e do modelo de desenvolvimento, a reflexão em torno da redução da esfera de proteção da privacidade e dos dados pessoais exige maior recontextualização. Os parâmetros convencionais de proteção da privacidade e dos dados pessoais exigem uma revisão contextual para proporcionar respostas mais efetivas às formas pouco transparentes utilizadas pelas empresas e desenvolvedores.

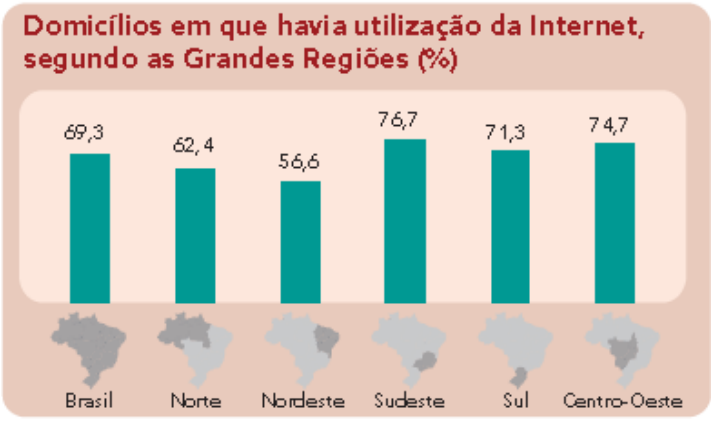
Neste sentido, **o problema analisado nesta tese envolverá o redimensionamento de instrumentos de *accountability*, em complemento ao consentimento do titular dos dados, como fundamento de um modelo regulatório híbrido, contextual e plural, a que denominaremos de *Lex Privacy***. A escolha da privacidade e proteção de dados, dentre tantos outros direitos afetados pelo processo de desenvolvimento tecnológico, se deve ao fato de que ambos demandam expressiva e dinâmica interação, *trade-offs* e incentivos comportamentais entre agentes privados, com uma intermediação estatal variável.

As hipóteses de investigação serão apresentadas por meio de modelos regulatórios das mais diversas características para se concluir que a policontextualidade deve ser a marca de um modelo responsivo da tutela da proteção dos dados pessoais e da privacidade. Por outro lado, os objetivos específicos envolverão as particularidades da privacidade no ciberespaço, a delimitação de um sistema de governança para a proteção dos dados pessoais e o processo de ressignificação, de sorte a demonstrar a insuficiência do consentimento como meio de controle e adequação para proteção de dados.

Como forma de ilustrar com dados empíricos a transformação proporcionada pelo desenvolvimento tecnológico no ciberespaço e como isto pode ter impactado na privacidade e proteção dos dados da população brasileira, utilizaremos como evidência para o recorte os resultados da Pesquisa Nacional por Amostra de Domicílios-PNAD de 2016, publicada em 2017, na qual se observou elementos relevantes em torno da cibercultura. O

primeiro deles refere-se ao número de brasileiros que acessam a internet. Constatou-se a utilização da internet em 69,3% dos 69.318 mil domicílios particulares permanentes do País, o que revela a sua presença na maioria dos domicílios em todas as Grandes Regiões: na Sudeste, 76,7% das residências a possuíam; na Centro-Oeste, 74,7%; na Sul, 71,3%; na Norte, 62,4%; e na Nordeste, 56,6%"[8].

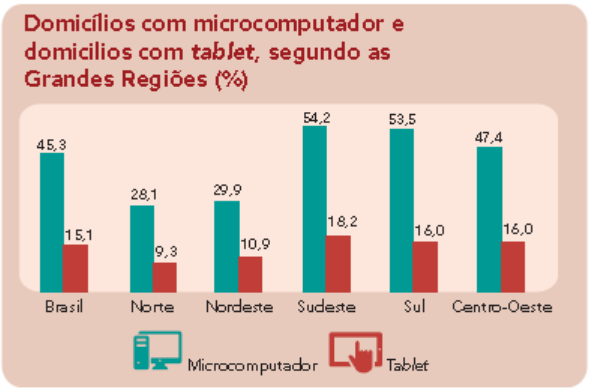
Curiosamente, dentre as finalidades do acesso à internet investigadas, a que mais se destacou foi envio ou recebimento de mensagens de texto, voz ou imagens por aplicativos diferentes, indicada por 94,2% das pessoas de 10 anos ou mais de idade que utilizaram a internet. Assistir a vídeos, inclusive programas, séries e filmes foi apontada como a finalidade preferida por 76,4% dessas pessoas, ao passo que 73,3% indicaram as conversas por chamadas de voz ou vídeo. O envio e recebimento de e-mails ficou em quarto lugar com 69,3%.



Fonte: IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento, Pesquisa Nacional por Amostra de Domicílios Contínua 2016.

Por outro lado, em 45,3% (31.377 mil) dos domicílios particulares permanentes do País foi constatada a existência de um microcomputador. Nas Grandes Regiões, os resultados desse indicador apontam que as Regiões Norte (28,1%) e Nordeste (29,9%) foram as com a menor presença do equipamento, ao passo que a Região Centro-Oeste (47,4%) e as Regiões Sul (53,5%) e Sudeste (54,2%) tiveram a maior presença. Os domicílios com existência de *tablet* (10.488 mil) representaram cerca de ⅓ daqueles que dispunham de microcomputador. Nas Grandes Regiões, o Sudeste apresentou o percentual mais elevado de domicílios com *tablet* (18,2%), enquanto o Norte, o menor (9,3%).

[8] IBGE, **PNAD Contínua: Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal**, Rio de Janeiro: IBGE, 2018.



Fonte: IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento, Pesquisa Nacional por Amostra de Domicílios Contínua 2016.

Em 97,2% dos 48.070 mil domicílios em que havia acesso à Internet, o telefone móvel celular foi indicado como o principal equipamento de conexão. Substancialmente abaixo e representando pouco mais da metade dos domicílios em que havia acesso à Internet, o microcomputador foi indicado como o equipamento utilizado (57,8%). O *tablet* foi mencionado em 17,8% dos domicílios em que havia acesso à Internet, e a televisão, em 11,7%. Equipamento diverso foi utilizado para acessar a Internet em 620 mil domicílios, o que representou somente 1,3% das residências em que houve utilização dessa rede. Como visto, nos domicílios em que havia acesso à Internet, o telefone móvel celular era utilizado para este fim em 97,2%, porém, em 38,6% deles, somente esse meio era utilizado para acessá-la.

Outro dado relevante demonstra a mudança do perfil etário e ocupação daqueles que acessam a internet. Na população ocupada de 14 anos ou mais de idade, o percentual das pessoas que utilizaram a Internet atingiu 97,4% no grupamento dos profissionais das ciências e intelectuais, que reúne ocupações que demandam normalmente maior nível de educação formal. A seguir, constam os membros das forças armadas, policiais e bombeiros militares, com 96,8%. Além desses dois grupamentos, em três outros (trabalhadores de apoio administrativo, técnicos e profissionais de nível médio, e diretores e gerentes) observou-se, também, a boa difusão do acesso à internet (acima de 93%).

Embora o foco de análise seja um modelo regulatório amplo, o recorte em torno dos dados da PNAD 2016/2017 revela uma série de modificações nos padrões de comportamento da sociedade e com ele a necessidade de repensar os parâmetros regulatórios. A partir do desenvolvimento de um eixo relacional no qual o ciberespaço ocupou o centro, as relações de ordem econômica sofreram uma considerável migração de um modelo de

capitalismo construído por átomos, essencialmente fundado na propriedade física e exclusividade de bens, para um sistema de *bits*, marcado pelo parcial compartilhamento de informações, dados e auto-geração de riqueza[9]. E tal aspecto pode ser facilmente constatado quando são analisados os dados de distribuição de renda *per capita* pela modalidade de conexão utilizada pelas famílias brasileiras[10] na PNAD 2016/2017.

Naturalmente, essa mudança cultural impactou as relações políticas, na medida em que o cenário constituído pelo ciberespaço criou foros de debate, essencialmente dinâmicos quanto à atuação e sobremaneira diversificados quanto à identificação dos valores e preferências dos indivíduos[11]. A relativa migração de um mundo físico para outro virtual facultou aos indivíduos amplos poderes de conformação da autonomia privada, além de ter viabilizado o acesso a posições pouco transparentes no ambiente factual.

No entanto, as externalidades positivas vieram acompanhadas de custos sociais expressivos. A ausência de fronteiras reais, com o comprometimento de conceitos dogmáticos tradicionais como soberania, território, propriedade e jurisdição logo causou a eclosão de fenômenos contrafactuais para os quais a teoria geral das fontes do Direito não conseguiu apresentar respostas satisfatórias e apropriadas[12]. A proteção dos dados e da privacidade foi apenas mais uma delas e, ainda assim, multiplicaram-se as proposições legislativas que almejam regular o ciberespaço.

E essa a razão pela qual essa tese se propõe a analisar os modelos regulatórios e identificar o desenvolvimento de um sistema próprio de proteção de dados no ciberespaço, sob a perspectiva do pluralismo jurídico global, enquanto fenômeno marcado pelo surgimento de várias fontes de tutela da privacidade e proteção dos dados pessoais, numa clara junção de modelos ora marcados pela atuação estatal, ora fruto de expressiva atuação privada.

---

[9] BARLOW, John Perry, The next economy of ideas: selling wine without bottles on the global net, **Wired**, v. 8, 2000; BENKLER, Yochai, **The wealth of networks: How social production transforms markets and freedom**, New Haven: Yale University Press, 2006.

[10] GUIMARÃES JÚNIOR, De pés descalços no ciberespaço; JUNGBLUT, Airton Luiz, A heterogenia do mundo on-line: algumas reflexões sobre virtualização, comunicação mediada por computador e ciberespaço, **Horizontes Antropológicos**, v. 10, n. 21, p. 97–121, 2004.

[11] SUNSTEIN, Cass, **Republic.com 2.0**, 2. ed. Princeton: Princeton University Press, 2009.

[12] JOHNSON, David R.; POST, David, Law and borders: the rise of law in cyberspace, **Stanford Law Review**, v. 48, p. 1367, 1995.

O objetivo da tese é demonstrar que a regulação da privacidade e proteção de dados associada exclusivamente à atuação estatal é pouco propensa a assegurar parâmetros adequados de tutela em âmbito global. Os paradigmas de concreção não guardam, a rigor, profunda identidade entre a privacidade vivenciada no mundo real e no virtual, além de também não se expressarem de maneira uniforme em âmbito regional e global.

Se no ciberespaço os indivíduos são realmente afeitos a impulsos e comportamentos pouco comuns quando comparados com os da vida real, tal como sustenta Turkle[13], tal fato se deve em grande medida pela percepção - falsa ou não -, de se tratar de um foro menos propenso a qualquer tipo de regulação e intervenção estatal. A conjugação de fatores como a ausência de fronteiras físicas e dinamicidade das interações torna o ciberespaço um *locus* de permanente reflexão a respeito de seus matizes regulatórios.

Os modelos regulatórios analisados nessa tese almejam de algum modo restabelecer nichos de regulação e proteção da esfera individual e de valores sociais. A partir de uma clara demonstração de sucessividade - e até complementariedade de algumas das propostas formuladas - , temas como crimes virtuais, pornografia infantil, discurso de ódio, privacidade e proteção de dados foram utilizados como testes de funcionamento e de efetividade das respostas apresentadas por cada uma das vertentes regulatórias. Esta é a principal razão pela qual se escolheu a privacidade e os dados pessoais como elementos que demandam alguma espécie de regulação: conciliar a optimização da extração de benefícios e estabelecer um regime de governança sustentado por valores democráticos como a transparência e *accountability*.

Para tanto, a análise envolverá a existência de um modelo regulatório próprio sobre proteção dos dados e privacidade, como esse modelo deveria funcionar, quais as suas características e quais fatores contribuíram para a sua formação.

A partir da perspectiva da regulação, construir-se-á uma metodologia de análise em torno de ***cinco eixos*** para que seja possível viabilizar a demonstração de que o sistema de proteção de dados e privacidade no ciberespaço tem contornos diversos daqueles tradicionais. Os eixos compreendem:

- regulação do ciberespaço;
- a proteção de dados e privacidade no ciberespaço;

[13] TURKLE, Sherry, Cyberspace and identity, **Contemporary Sociology**, p. 643–648, 1999.

- a identificação de elementos de pluralismo jurídico capazes de promover outros meios de regulação;
- impacto da regulação na autonomia e identidade dos atores envolvidos;
- a construção de um regime de governança da proteção de dados e privacidade[14].

A constatação em torno do menor poder de controle dos Estados soberanos e organismos internacionais sobre o ciberespaço torna a proteção de dados e privacidade um dos principais focos de tensão nas relações entre os atores que interagem na sociedade da informação, essencialmente marcada por uma economia de compartilhamento de bens, informações e serviços[15].

Com o escopo de delimitar o espectro temporal e espacial da tese, o marco teórico terá como ponto de partida a perspectiva das aldeias ou vilas globais, apresentado por Günther Teubner[16]. Teubner aponta para o impacto do pluralismo jurídico global, viabilizado pela compreensão emancipatória das fronteiras e limites do direito estatal. Na *Bukowina Global* de Teubner, espelhada na obra de Eugen Ehrlich[17], os atores serão os principais responsáveis pela regulação de seus interesses, condutas e conflitos, tal como se identifica sobremaneira no ciberespaço.

A fragmentação, tratamento, gestão, armazenamento e a manipulação de dados para finalidades diversas daquelas em que originariamente autorizadas representa um dos desafios regulatórios e normativos para os atores que atuam no ciberespaço. O consentimento e o legítimo interesse, por exemplo, nem sempre reúnem todos os elementos necessários a dimensionar a destinação de dados disponibilizados na rede.

---

[14] GALGANO, Francesco, The new lex mercatoria, **Ann. Surv. Int'l & Comp. L.**, v. 2, p. 99, 1995; SWEET, Alec Stone, The new Lex Mercatoria and transnational governance, **Journal of European Public Policy**, v. 13, n. 5, p. 627–646, 2006; MUSTILL, Justice, The new lex mercatoria: the first twenty-five years, **Arbitration International**, v. 4, n. 2, p. 86–119, 1988; JUENGER, Friedrich K., The lex mercatoria and private international law, **La. L. Rev.**, v. 60, p. 1133, 1999; TEUBNER, Gunther, Breaking frames: economic globalization and the emergence of lex mercatoria, **European Journal of Social Theory**, v. 5, n. 2, p. 199–217, 2002.

[15] MURRAY, Andrew, **The regulation of cyberspace: control in the online environment**, London: Routledge, 2007.

[16] TEUBNER, Gunther, Global Bukowina: Legal Pluralism in the World-Society, **Global law without State**, p. 3–28, 1996.

[17] EHRLICH, Eugen, O estudo do direito vivo, **Sociologia e Direito, São Paulo, Pioneira Democracia: ideas y prácticas**, 1980; EHRLICH, Eugen, **Fundamentos da sociologia do direito**, [s.l.]: Universidade de Brasilia, 1967.

Compreender o fluxo transnacional e análise econômica em torno dos *trade-offs* realizados pelos titulares dos dados e as empresas exige a construção de marcos teóricos e a revisão de paradigmas sobremodo centrados na Teoria Geral do Direito e no positivismo jurídico formal, tal como se apresentam no ambiente físico, além de perspectivas de regulação que superem a singeleza da lógica regulatória binária proibir/permitir.

A atividade e a natureza dos atores envolvidos com a manipulação de dados também serão outros fatores de desenvolvimento na tese, uma vez que variam consideravelmente em função de sua natureza pública/estatal ou privada, bem como em função de maior ou menor expressão de poder social ou desigualdade de condições.

As hipóteses de respostas aos problemas apresentados considerarão algumas variáveis de impacto dependente e outras independentes, a partir de indicadores devidamente delimitados como os processos de transferência internacional e as formas de manifestação do consentimento. Um modelo de governança em torno da proteção de dados e da privacidade será identificado ao final da tese e será concebido em torno de mecanismos específicos de controle, a partir de uma regulação complexa e formada em conjunto por meio de camadas e variados *stakeholders*.

Para as relações entre atores privados e públicos/estatais, deveras marcadas pelo que Bauman chamou de vigilância líquida[18], o principal mecanismo de controle será a *accountability* e a *transparência* da fiscalização exercida pelos titulares dos dados em conjunto com as autoridades estatais. Por outro lado, para as relações entre atores privados, em igualdade de condições, serão indicados mecanismos de governança centrados em estruturas contratuais caracterizadas por incentivos e desestímulos.

No tocante às relações entre atores privados em desigualdade de condições, desniveladas por expressão de poder social, além de mecanismos de integridade (*compliance*), se proporá a ampliação de ferramentas que concretizem a *accountability* enquanto medida complementar da obtenção do consentimento dos titulares dos dados. Para tanto, serão apresentadas estruturas de valorização da proteção de dados e privacidade em âmbito global, tais como códigos de conduta, cláusulas-tipo e normas corporativas vinculantes.

---

[18] BAUMAN, Zygmunt, **Vigilância líquida: diálogos com David Lyon**, Rio de Janeiro: Zahar, 2013.

Ao final, se concluirá que os modelos regulatórios demandam uma interoperatividade para que possam representar com efetividade a tutela de direitos dos titulares dos dados, em especial porque a *Lex Privacy* será identificada a partir da atuação conjunta e mesclada dos parâmetros de corregulação, auto-regulação e regulação estatal.

CAPÍTULO 1 - CIBERESPAÇO E REGULAÇÃO

1. Para entender o ciberespaço: um novo cenário ou a projeção do mundo físico?

1.1 Delimitação regulatória preliminar

O ciberespaço foi originariamente concebido para ser um território que pudesse proporcionar certa autonomia e empoderamento aos seus usuários[19]. No entanto, a percepção de que o ciberespaço não deve ser um local infenso à regulação estatal tem se intensificado. A prática de crimes cibernéticos, a divulgação de *fake news* em eleições, a pirataria de bens digitais, a tributação de novos serviços, a concorrência desleal em conjunto com a violação dos direitos da privacidade e proteção de dados pessoais são apenas alguns indicativos da relevância do processo regulatório.

Neste capítulo se analisará os fatores que impulsionaram as principais vertentes regulatórias do ciberespaço e sua conexão com os modelos regulatórios específicos da privacidade e proteção de dados, de forma a se compreender como cada uma pretendia apresentar respostas aos novos desafios impostos pelo uso da tecnologia. Como forma de compreender as características evolutivas da regulação do ciberespaço, a abordagem escolhida partirá das três principais correntes teóricas e, em seguida, se fará o contraponto com o modelo teórico de Teubner em torno do pluralismo jurídico global. A escolha de Teubner como referencial teórico se deve ao fato de sua elaboração em torno de um protótipo de vila global em que o papel da policontextualidade faculta a maior participação dos demais atores no processo de regulação. Com esses elementos teóricos, teremos a base para o desenvolvimento do substrato dogmático desta tese e os instrumentos de análise da *lex privacy*.

Em grande medida, um dos fatores influenciadores da escolha de Teubner se deve à contraposição que apresenta à tendência regulatória de invariável associação a valores

[19] BERNERS-LEE, Tim, WWW: past, present, and future, **Computer**, v. 29, n. 10, p. 69–77, 1996.

relacionados à propriedade privada[20]. De certa forma, a tendência humana de associação de algo a alguém faz com quem as premissas de análise sejam costumeiramente calcadas em estruturas físicas e vinculadas a um indivíduo, o que tem contribuído para muitas incompreensões quando este modelo é transmutado para o ciberespaço e, mais especificamente para a tutela da privacidade e dados pessoais. Além de impactar na delimitação das características do fenômeno digital, a perspectiva em torno da propriedade privada ainda interfere na compreensão dos instrumentos de proteção da privacidade[21] e consequente regulação[22], sem muitas vezes apresentar respostas adequadas e atuais.

Além da identificação da constante associação com a propriedade privada em um mundo marcado pelo compartilhamento – ainda que desigual - de bens e serviços, o processo de regulação também perpassa por uma análise do papel do Estado e o seu intuito de regular de forma exaustiva os diversos setores da sociedade. Parte da questão pode ser resumida entre aqueles que acreditam ser a regulação do ciberespaço somente necessária naquilo que envolva a manutenção da funcionalidade da rede e, por outro lado, entre aqueles que sustentam a possibilidade de que muitas outras oportunidades floresçam se alguma ordem regulatória for assegurada. Em boa medida, isso também está associado ao fato de que o contramodelo de regulação totalitária tem se mostrado cada vez mais incapaz de dialogar com a dinâmica evolução da tecnologia[23] e simultaneamente admitir a participação de atores privados no processo de regulação.

Teubner aponta que "a tendência do constitucionalismo liberal está cada vez mais desacreditada por ignorar aquilo que tem denominado de "as constituições dos âmbitos sociais parciais",[24] ou seja, espaços de regulação privada destinados a respeitar as autonomias que deles surgem.[25] Embora alguns autores acreditem que a regulação é um tema estritamente

---

[20] HUNTER, Dan, Cyberspace as Place and the Tragedy of the Digital Anticommons, **California Law Review**, v. 91, p. 439, 2003, p. 441.

[21] Exemplo claro disso é a comparação feita com os mandados de busca de apreensão de celulares com a apreensão do conteúdo das mensagens nele existentes. Cf. Cap 3.

[22] KERR, Orin S., The Problem of Perspective in Internet Law, **Georgetown Law Journal**, v. 91, p. 357, 2002, p. 358.

[23] BALDWIN, Robert; CAVE, Martin; LODGE, Martin, **The Oxford handbook of regulation**, [s.l.]: Oxford University Press, 2010, p. 524.

[24] TEUBNER, Gunther, **Fragmentos constitucionais: Constitucionalismo social na globalização**, São Paulo: Saraiva, 2016, p. 80.

[25] Um claro exemplo desse fenômeno a quem podemos atribuir a condição de âmbito de regulação parcial privada e autônoma decorre da criação do protocolo IPv6, um novo padrão de comunicação e reconhecimento de

relacionado à intervenção estatal por meio da lei[26] e do mercado,[27] aqui se desenvolverá uma perspectiva centrada na relevância do papel de outros atores, algo que tem se revelado típico no ciberespaço:[28]

> "Given the increasingly complex and rapidly changing commercial and social usage patterns of the Internet, with the World Wide Web being their trans-border platform, we cannot even expect to find a tighly-knit web of regulatory elements in the form of legal rules and ordinances, mandatory and voluntary technical standards and protocols, international and national contracts and agreements, and informal codes of conduct and 'netiquette'(e.g. social conventions that are meant to guide all cyber-related interactions).[29]

A partir deste contexto, será analisada a contribuição normativa dos principais modelos teóricos referentes ao ciberespaço e, independentemente de qual deles seja mais aceito e adequado, o essencial será compreender como a regulação policontextual do ciberespaço se difere daquela do mundo físico e qual o caminho adequado para realizá-la[30] de forma a resguardar a proteção dos dados e privacidade. Em outras palavras, se partirá do processo regulatório amplo do ciberespaço para se delimitar a sua influência no modelo de governança da proteção de dados pessoais e privacidade que esta tese pretende sustentar.

A regulação do ciberespaço, compreendido como o ambiente virtual de interação social, tem se tornado um importante desafio para os mais variados ordenamentos jurídicos[31]. Mais do que uma concepção reducionista em torno apenas dos limites da internet, o ciberpespaço compreende todo o cenário virtual no qual se desdobra a arena pública de

---

sistemas como afirma Baldwin: "Internet standards are rarely purely technical, but they can obscure commercial interests, political preferences, and moral evaluations at the same time that these underlying interests and choices are brought to bear. Thus, the work that the W3C and the IETF engage in has political and regulatory consequences. The new generation of the generic Internet protocol suite offers an impressive case in point. In 1998, the IETF published a new Internet protocol suite as a draft standard, the so-called IP version 6 (or IPv6), also known as IP Next Generation". BALDWIN; CAVE; LODGE, **The Oxford handbook of regulation**, p. 530.

[26] JOHNSON; POST, Law and borders: the rise of law in cyberspace, p. 1367.

[27] Por esta razão, Baldwin prefere seguir a distinção entre Governança e Regulação. Cf. BALDWIN; CAVE; LODGE, **The Oxford handbook of regulation**, p. 525.

[28] As constatações de Cathy O'Oneil sobre a forma como a publicidade online é realizada, com direcionamento preciso ao público alvo, é uma das demonstrações de que a regulação tem ganhado novas facetas. O'NEIL, Cathy, **Weapons of math destruction: How big data increases inequality and threatens democracy**, [s.l.]: Broadway Books, 2017, p. 68.

[29] BALDWIN; CAVE; LODGE, **The Oxford handbook of regulation**, p. 525.

[30] LESSIG, Lawrence, **Code version 2.0 and other laws of Cyberspace**, New York: Basic Books, 2006, p. 27.

[31] TAYLOR, Josh, **France drops Hadopi three-strikes copyright law**, ZDNet, disponível em: <http://www.zdnet.com/article/france-drops-hadopi-three-strikes-copyright-law/>, acesso em: 2 abr. 2016.

deliberação, cuja regulação constitui um desafio para a preservação de valores democráticos, para a promoção da autonomia e liberdade, assim como para o desenvolvimento econômico, social e tecnológico. Fugir da perspectiva tradicional, limitada ao modelo binário proibir/permitir atividades, representa o ponto de partida desta viragem regulatória, cujo objetivo deve ser facilitar a transformação da realidade para promover um ambiente de governança virtual[32] capaz de proporcionar benefícios a todos indistintamente.

O incessante processo de disrupção, convergência e digitalização proporcionado pelo desenvolvimento tecnológico tem se mostrado incompatível com o modelo regulatório de simples contenção das demandas sociais mediante mera proibição e tributação, obstacularização de novos arranjos de trabalho, estruturas econômicas e inovações tecnológicas. Se por um lado esses fatores tem evidenciado um esgotamento do modelo regulatório convencional, por outro produtos e serviços como o Uber,[33] Prosper Marketplace[34] e AirBnB[35] tem suscitado a replicação de processos regulatórios sem a intervenção estatal, mediante o que se convencionou denominar de inovação digital evasiva. Em outros termos, uma escolha fundada no empreendedorismo digital para além das fronteiras e previsibilidade do regulador.

Por esta razão, sustenta-se que a regulação será melhor realizada se for fruto de atuação conjunta dos principais *players*, ao invés da concepção vertical caracterizada pela regulação estatal ou a completa ausência de intervenção estatal. Se o Estado limitar sua participação neste processo à simples proibição e tributação de produtos e serviços, outras formas de interação serão concebidas de modo a assegurar a viabilidade da interatividade e criatividade no ciberespaço, como salientado por Matt Ridley[36]:

---

[32] SAMUELSON, Pamela, Privacy as Intellectual Property, **Stanford Law Review**, v. 52, p. 1125–1173, 2000, p. 137.. Na visão da autora, algumas normas podem ser adaptadas, outras facilmente aplicadas, mas muitas normas novas serão necessárias em virtude da quebra de paradigmas proporcionada pelo ciberespaço.

[33] PRESSE, Da France, **Uber tem vitória na Suprema Corte da Inglaterra e do País de Gales**, Tem um aplicativo, disponível em: <http://g1.globo.com/tecnologia/tem-um-aplicativo/noticia/2015/10/uber-tem-vitoria-na-suprema-corte-da-inglaterra-e-do-pais-de-gales.html>, acesso em: 7 fev. 2019; PAULO, Rafael Barifouse Da BBC Brasil em São, **Mais da metade das capitais brasileiras já têm projetos de lei contra o Uber**, BBC Brasil, disponível em: <http://www.bbc.com/portuguese/noticias/2015/09/150908_uber_projetos_de_lei_rb>, acesso em: 27 out. 2015.

[34] CORTESE, Amy, Loans That Avoid Banks? Maybe Not, **The New York Times**, 2014.

[35] **Governo estuda taxar aluguel informal de imóveis, cômodos ou mesmo sofás - 07/08/2015 - Mercado**, Folha de S.Paulo, disponível em: <http://www1.folha.uol.com.br/mercado/2015/08/1665734-governo-estuda-taxar-aluguel-informal-de-imoveis-comodos-ou-mesmo-sofas.shtml>, acesso em: 7 fev. 2019.

[36] RIDLEY, Matt, The myth of basic science, **Wall Street Journal**, Online. 2015.

> Innovation is a mysteriously difficult thing to dictate. Technology seems to change by a sort of inexorable, evolutionary progress, which we probably cannot stop--or speed up much either.
> [...] By 2010, the Internet had roughly as many hyperlinks as the brain has synapses. Today, a significant proportion of the whispering in the cybersphere originates in programs--for monitoring, algorithmic financial trading and other purposes--rather than in people. It is already virtually impossible to turn the Internet off.
> The implications of this new way of seeing technology--as an autonomous, evolving entity that continues to progress whoever is in charge--are startling. People are pawns in a process. We ride rather than drive the innovation wave. Technology will find its inventors, rather than vice versa. Short of bumping off half the population, there is little that we can do to stop it from happening, and even that might not work.
> Indeed, the history of technological prohibitions is revealing. The Ming Chinese prohibited large ships; the Shogun Japanese, firearms; the medieval Italians, silk-spinning; Americans in the 1920s, alcohol. Such prohibitions can last a long time--three centuries in the case of the Chinese and Japanese examples--but eventually they come to an end, so long as there is competition. Meanwhile, elsewhere in the world, these technologies continued to grow.[37]

1.2 A alavancagem regulatória da digitalização, convergência e disrupção

Compreender as particularidades do ciberespaço não se resume a apenas promover a adaptação das estruturas normativas construídas para solucionar problemas pertinentes a questões como propriedade e titularidade de um bem, violação de direitos autorais, prática de crimes, relações contratuais e limitações físicas do mundo dos átomos[38]. Embora a teoria do direito ao longo do século XX tenha se concentrado em temas relacionados à posse e à propriedade de bens[39], o que é algo compreensível se o paradigma envolve bens materiais, quando o referencial muda para abarcar a informação, os dados, a privacidade e a economia (em parte0 compartilhada[40], o cenário demanda uma reconfiguração[41] do próprio processo de regulação.

Barlow lembra que no passado as grandes economias eram estruturadas em torno da propriedade de bens materiais[42], porém no atual contexto em que a informação se

---

[37] *Ibid*.

[38] BARLOW, The next economy of ideas: selling wine without bottles on the global net, p. 434–435.

[39] SMITH, Henry E., Property as the law of things., **Harvard Law Review**, v. 125, n. 7, 2012, p. 681.

[40] BERKELEY, John, Reinventing the company, **The Economist**, n. Online, 2015.

[41] BENKLER, **The wealth of networks: How social production transforms markets and freedom**, p. 15.

[42] BARLOW, The next economy of ideas: selling wine without bottles on the global net, p. 10.

tornou um ativo de capital ainda mais valioso[43], os *bits* tem avançado sobre a posição econômica dos átomos, o que pode ser demonstrado pela figura dos *bitcoins*[44]. Thomas Jefferson talvez tenha sido um dos primeiros a imaginar como o futuro seria modificado pela informação, especialmente num período em que a exclusividade da propriedade de bens seria confrontada com a perspectiva do compartilhamento[45].

O processo de digitalização, convergência e disrupção em curso demonstra que a não exclusividade dos bens viabilizará a produção e o consumo simultâneo de informação de forma ilimitada onde quer que se esteja e segundo as preferências de cada indivíduo[46]. O desafio envolverá o método e as respostas que o ordenamento jurídico apresentará a esta conjuntura. Compreender a existência de um ambiente diverso do mundo físico demanda um desafiador exercício de desprendimento de premissas e paradigmas até então inquestionáveis.

Se a informação se tornará o principal bem e uma das principais fontes de riqueza da sociedade, o rompimento com a exclusividade da propriedade será feito a partir da transferência internacional em massa de dados[47]. Este processo de fluxo indefinido acarretará mudanças na forma de atuação dos fornecedores e dos prestadores de serviços, mas não necessariamente nos serviços em si considerados. Música, transporte e hospedagem continuarão a existir nos moldes em que sempre existiram, porém em recipientes distintos[48].

---

[43] CASTELLS, Manuel, The rise of the network society: The information age: Economy, society, and culture, Londres: John Wiley & Sons, 2011, p. 23.

[44] DABROWSKI, Marek; JANIKOWSKI, Lukasz, **Virtual currencies and central banks monetary policy: challenges ahead**, Belgica: European Parliament's Committee on Economic and Monetary Affairs, 2018; KIVIAT, Trevor I., Beyond bitcoin: Issues in regulating blockchain tranactions, **Duke LJ**, v. 65, p. 569, 2015.

[45] Jefferson's letter: "If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea, which an individual may exclusively possess as long as he keeps it to himself; but the moment it is divulged, it forces itself into the possession of every one, and the receiver cannot dispossess himself of it. Its peculiar character, too, is that no one possesses the less, because every other possesses the whole of it. He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me". BENKLER, **The wealth of networks: How social production transforms markets and freedom**, p. 25.

[46] *Ibid*.

[47] BARLOW, The next economy of ideas: selling wine without bottles on the global net, p. 5.

[48] A partir da premissa da disrupção, a Moley, por exemplo, desenvolveu robots cozinheiros, os quais podem ser orientados de qualquer lugar por meio de um dispositivo como celular, email, aplicativo e dispositivo de voz. Cf. **Moley to present the world's first robot kitchen in 2017 - Business Insider**, disponível em: <https://www.businessinsider.com/moley-to-present-the-worlds-first-robot-kitchen-in-2017-2015-11>, acesso em: 7 fev. 2019; **The robot chef coming to a kitchen near you - Telegraph**, disponível em: <https://www.telegraph.co.uk/finance/businessclub/11912085/The-robot-chef-coming-to-a-kitchen-near-you.html>, acesso em: 7 fev. 2019.

A forma mudará, mas o conteúdo permanecerá o mesmo, ou como prefere Barlow, mudarão as garrafas, embora o vinho permaneça o mesmo[49].

Se o ordenamento jurídico não consegue sempre atingir diretamente a informação mediante a coerção dos *bits e algoritmos* (*tech enforcement ou law hacking)*, uma das alternativas é intervir no ciberespaço a partir das estruturas físicas que a ele dão suporte, isto é, os recipientes e as garrafas. Experiências revolucionárias na prestação de serviços e produção de bens tem ocorrido a todo instante, no entanto, apesar da relativa particularidade de algumas "garrafas", permanece a incógnita quanto à efetiva capacidade dos modelos regulatórios atuais em tangenciar e disciplinar as relações sociais no ciberespaço, em particular a proteção dos dados e privacidade.

Ainda que não seja um nicho de atuação regulado apenas por atores privados, as referências às estruturas do mundo físico ainda estão presentes em muitos dos temas relacionados ao ciberespaço[50]. Curiosamente, embora esse fenômeno possa parecer sintomático e demasiadamente peculiar ao ciberespaço, várias das "garrafas" mencionadas por Barlow comportam uma regulação semelhante à do mundo físico, como no exemplo das chaves privadas de criptografia e as chaves de uma porta. Mas por que o ciberespaço deve ser regulado e quem detém legitimidade para fazê-lo? De que modo as fronteiras territoriais serão redimensionadas e poderão interferir na forma com que o ciberespaço delas se vale? O compartilhamento ao invés da exclusividade será capaz de modificar a forma como as relações sociais se entabulam e o modo como o ordenamento jurídico atua junto aos atores? Estas são algumas das questões a serem enfrentadas doravante.

2. Das fronteiras às garrafas: os ciberlibertários e a rejeição à regulação estatal

Os ciberlibertários foram os primeiros a considerar de algum modo a regulação do ciberespaço, porém com o propósito de refutá-la. Desde a criação da World Wide Web em 1989 por Tim Berners-Lee[51], a rede tem se expandido em funcionalidades e sistemas de

---

[49] BARLOW, The next economy of ideas: selling wine without bottles on the global net.

[50] MAYER-SCHÖNBERGER, Viktor, Shape of Governance: Analyzing the World of Internet Regulation, The, **Va. J. Int'l L.**, v. 43, p. 605, 2002.

[51] BERNERS-LEE, WWW.

comunicação[52]. Em meio a este novo ambiente, os atores foram influenciados pela possibilidade de interação em tempo real por emails, chats, redes sociais, aplicativos e plataformas, ainda que carregados com as impressões e os estigmas do mundo físico. As perspectivas do mercado online também afetaram de forma incisiva a economia compartilhada e a forma como as empresas e os governos tem sido redesenhados[53], notadamente porque a gestão estratégica de dados se transformou numa *commodity* valiosa.

Para uma breve contextualização histórica do tema, nesta primeira fase do debate em torno da regulação, John Perry Barlow, um dos fundadores da Eletronic Frontier Foundation[54], teve um papel vital. Conhecido por ter declarado a independência do ciberespaço, em 1996, numa reunião do Fórum Econômico Mundial[55], Barlow foi o responsável pela defesa veemente de que o ciberespaço era um nicho de interação social que deveria permanecer isolado da influência dos atores estatais. Pautado por um considerável idealismo em torno da perspectiva de que a internet é capaz de proporcionar melhores condições de interação, *accountability* e maior autonomia aos indivíduos,[56] Barlow acreditava que o ciberespaço deveria ser um local de emancipação dos indivíduos, livre das influências do mundo físico, com ampla liberdade de expressão[57] e exercício de direitos[58]. Barlow faleceu em 2018 e até então ainda acreditava nos caminhos próprios da regulação no ciberespaço.

---

[52] DENARDIS, Laura, Internet points of control as global governance, **Internet Governance Papers**, v. 2, 2013.

[53] RUNDLE, Michael, Matt Hancock's smartphone state, via Uber and blockchain, **Wired UK**, 2015.

[54] COHN, Cindy, **John Perry Barlow, Internet Pioneer, 1947-2018**, Electronic Frontier Foundation, disponível em: <https://www.eff.org/deeplinks/2018/02/john-perry-barlow-internet-pioneer-1947-2018>, acesso em: 7 fev. 2019.

[55] **It's Been 20 Years Since This Man Declared Cyberspace Independence | WIRED**, disponível em: <https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/>, acesso em: 7 fev. 2019.

[56] VOLPICELLI, Gian, **Alex Pentland: Big data will help us hold governments accountable**, Wired UK, disponível em: <http://www.wired.co.uk/news/archive/2015-10/15/alex-pentland-wired-2015>, acesso em: 27 out. 2015.

[57] Sobre a liberdade de expressão no ciberespaço e o eventual conflito com outros direitos, cf. Reno v. ACLU (**Reno v. ACLU**, Oyez, disponível em: <https://www.oyez.org/cases/1996/96-511>, acesso em: 7 fev. 2019.) no qual a Suprema Corte dos Estados Unidos declarou inconstitucional o Communications Decency Act, sob o fundamento de que não tinha o efeito de atingir o legítimo interesse de proteção das crianças contra discursos obscenos. Cf. também a Child Online Protection (COPPA), cuja inconstitucionalidade foi questionada perante a Suprema Corte americana em Ashcroft v. American Civil Liberties Union ACLU) (FEDERAL TRADE COMMISSION, **Protecting Children's Privacy Under COPPA: A Survey on Compliance**, Estados Unidos: FTC, 2002.)

[58] JOHNSON; POST, Law and borders: the rise of law in cyberspace, p. 1373–1375.

À medida que a expansão do ciberespaço proporcionou o surgimento de novas funcionalidades, com outras interfaces, camadas e conexões, estas características o levaram a extrapolar os seus propósitos iniciais, os quais passaram a demandar maior intervenção estatal sob pena de se transformar numa arena anárquica. Barlow não estava sozinho na defesa do ciberpespaço como um lugar isolado, despido de associações com o mundo físico, no qual os agentes reguladores não teriam condições de meramente transpor conceitos e teorias[59]. Autores como Post e Johnson[60] e ativistas como Julien Assange[61] também foram ferrenhos defensores do ciberlibertarianismo e da perspectiva da impossibilidade de delimitação de jurisdição, território e soberania, com argumentos ainda mais contundentes do que os apresentados por Barlow. A despeito da posterior constatação das manifestações de poder grandes corporações e do poder de vigilância estatal, Post, Johnson e Assange não reviram suas posições históricas iniciais para indicar a necessidade de alguma espécie de regulação.

O grande desafio, à época, envolvia a forma como a regulação seria concebida, visto que a inexistência de fronteiras físicas que pudessem delimitar a rede de conexões e controlar a arquitetura representava um ponto de incompreensão para os atores estatais[62]. E ainda hoje representa uma incógnita, embora a regulação tenha aos poucos se tornado um fenômeno necessário e factível para que o ciberespaço pudesse prover tudo aquilo que dele se esperava. Um destes fatores de incompreensão é a proteção dos dados e privacidade que, como observam Post e Johnson, seriam incapazes de delimitação territorial em termos de fluxo transnacional de dados[63]. Como destaca Baldwin, um conjunto descentralizado de comunicações de proporções globais somente poderia funcionar se tivermos padrões mínimos de interoperabilidade:

> "It is undisputed that the Internet was only able to grow into a global network because it had met the critical operational requirements which any decentralised set of communications systems must meet in order to function as a single cohesive

---

[59] EASTERBROOK, Frank H., Cyberspace and the Law of the Horse, **U. Chi. Legal F.**, p. 207, 1996, p. 207–208.

[60] JOHNSON; POST, Law and borders: the rise of law in cyberspace, p. 1373–1375.

[61] ASSANGE, Julian, **Cypherpunks: liberdade e o futuro da internet**, São Paulo: Boitempo Editorial, 2015.

[62] O principal deles Frank H. Easterbrook, que não hesitava em afirmar que a multidisciplinariedade representaria uma esterilização do Direito. Isto deveria fazer com que hesitasse em prescrever adaptações legais para o ciberespaço. Cf. EASTERBROOK, Cyberspace and the Law of the Horse, p. 104.

[63] JOHNSON; POST, Law and borders: the rise of law in cyberspace, p. 1367. Para uma análise mais profunda em torno dos impactos no ciberespaço sobre a jurisdição, com enfoque nas dificuldades de enforcement, cf. PERRITT JR, Henry H., Jurisdiction in cyberspace, **Vill. L. Rev.**, v. 41, p. 1, 1996, p. 3.

> system. These requirements are compatibility, identification, and interconnectivity[64].

O surgimento de fenômenos semelhantes aos do mundo físico fez com que os tribunais apreciassem temas relacionados ao ciberespaço não como algo além e contraposto a ele, mas a partir de uma metáfora nele pautada na qual o consideravam um lugar próprio e específico, uma arena, e não um simples protocolo ou a peça de um código, como criticam Dan Hunter[65] e Mark Lemley[66]. Com o surgimento das ameaças a direitos, aos poucos as respostas dos ciberlibertários tornaram-se insuficientes e ilusórias para lidar com os crimes cibernéticos como a pedofilia, as violações de direitos autorais, os furtos de dados pessoais e corporativos, a vigilância em massa, a violação da privacidade, os ataques de hackers a contas bancárias e serviços, o ciberterrorismo, a pornografia de vingança e o discurso de ódio[67].

Por esta razão, o movimento ciberlibertário guardará expressiva correlação com o modelo de autorregulação de proteção da privacidade e dos dados pessoais a ser analisado no capítulo 2. Ademais, nota-se que o movimento ciberliberário em muito destoa das bases normativas do modelo regulatório de pluralismo jurídico de Teubner proposto nesta tese, visto que além de pregar a ausência de participação estatal, ignora o aspecto da policontextualidade que será vital para a tutela da privacidade e proteção dos dados pessoais.

O ápice da derrocada do movimento ciberlibertário ocorreu após países como China[68], Arábia Saudita[69] e Coréia do Norte[70] implementarem medidas de bloqueio ao acesso da internet em seus territórios, o que se repetiu durante as manifestações sociais na Primavera Árabe[71]. Isso demonstrou que a inexistência de fronteiras, território e soberania não eram

---

[64] BALDWIN; CAVE; LODGE, **The Oxford handbook of regulation**, p. 526.

[65] HUNTER, Cyberspace as Place and the Tragedy of the Digital Anticommons, p. 444.

[66] LEMLEY, Mark A., Place and cyberspace, **California Law Review**, v. 91, n. 2, p. 521–542, 2003, p. 522–523.

[67] BELLIA, Patricia L., Chasing bits across borders, **U. Chi. Legal F.**, p. 35, 2001, p. 37–38.

[68] LEVIN, Dan, At U.N., China Tries to Influence Fight Over Internet Control, **The New York Times**, 2017.

[69] DEUTSCHE WELLE, **Post-Arab Spring censorship on the rise**, DW.COM, disponível em: <https://www.dw.com/en/post-arab-spring-censorship-on-the-rise/a-16725701>, acesso em: 7 fev. 2019.

[70] BBC NEWS, **North Korea: On the net in world's most secretive nation**, BBC, disponível em: <https://www.bbc.com/news/technology-20445632>, acesso em: 7 fev. 2019.

[71] BEÇAK, Rubens; LONGHI, João Victor Rozatti, O papel das tecnologias de comunicação em manifestações populares: a "Primavera Árabe" e as "Jornadas de Junho" no Brasil, **Revista Eletrônica do Curso de Direito da UFSM**, v. 10, n. 1, p. 388–405, 2015; BLACK, Ian; EDITOR, Middle East, Saudia Arabia leads Arab regimes in internet censorship, **The Guardian**, 2009.

aspectos decisivos para a regulação do ciberespaço, visto que poderiam facilmente superar essas barreiras com o emprego de leis extraterritoriais como a *General Data Protection Regulation* (GDPR), o Marco Civil da Internet (MCI) e a Lei Geral de Proteção de Dados Pessoais (LGPD). A conjugação de todos estes aspectos contribuiu sobremaneira para que um novo movimento teórico, conhecido como ciberpaternalismo, apresentasse soluções alternativas para o ciberespaço.

3. Os Ciberpaternalistas e o protótipo da arquitetura

Depois dos ciberlibertários terem declarado o ciberespaço como o território das liberdades, insuscetível de controle estatal em termos de fronteiras e soberania, os ciberpaternalistas apresentaram uma outra visão do processo de regulação, cuja análise envolvia o controle, a filtragem e a *blacklist* dos sítios eletrônicos e softwares de acesso proibido.[72] Se os ciberlibertários estavam corretos em sua perspectiva, como os Estados deveriam lidar com o anonimato na internet, os crimes praticados por meio da *deep web - Dot Onion/Tor*[73] - , a pornografia infantil[74], o ciberbullying[75], a lavagem de dinheiro e os furtos, as fraudes, os hackers e extorsões[76]? Como os Estados iriam regular o empreendedorismo evasivo ou as novas funcionalidades disruptivas como o Uber[77] e o AirBnB[78], ou a criptografia[79] e os contratos de empréstimo por meio de sistemas peer-to-peer (P2P)[80]? De

---

[72] MURRAY, Andrew D., **Information technology law: the law and society**, Oxford: Oxford University Press, 2013, p. 75–76.

[73] GREENBERG, Andy, Mapping how Tor's anonymity network spread around the world, **Wired UK**, n. Online, 2015.

[74] THE CROWN PROSECUTION SERVICE, **Indecent photographs of children: Legal Guidance**, The Crown Prosecution Service, disponível em: <http://www.cps.gov.uk/legal/h_to_k/indecent_photographs_of_children/>, acesso em: 27 out. 2015.

[75] SIMPSON, Kevin, How a cyberbullying law in Colorado was tweaked to be more effective, **Denver post**, Online. 2015.

[76] PETERSON, Andrea, Could hackers take down a city?, **The Washington Post**, Online. 2015.

[77] GLOBALPOST, **Here's everywhere Uber is banned around the world**, Business Insider, disponível em: <https://www.businessinsider.com/heres-everywhere-uber-is-banned-around-the-world-2015-4>, acesso em: 7 fev. 2019.

[78] PLAUTZ, Jason Abbruzzese and Jessica, **New York Goes to War Against Airbnb for Disrupting Hotel Business**, Mashable, disponível em: <https://mashable.com/2014/04/26/new-york-vs-airbnb/>, acesso em: 7 fev. 2019.

[79] GREENBERG, Andy, The Senate's Draft Encryption Bill Is 'Ludicrous, Dangerous, Technically Illiterate''', **Wired**, 2016.

fato, o ciberespaço seria inconcebível enquanto arena democrática sem alguma forma de regulação, uma vez que não seria possível identificar o papel dos atores envolvidos, quem representa e quem atua em nome da sociedade[81]. Nesse contexto, a representação política[82] e a *accountability*[83] seriam apenas dois dos elementos político-democráticos cuja identificação e consolidação no ciberespaço constituiriam um desafio da ausência de regulação[84], em especial porque a deliberação e o processo decisório ainda se revelam pouco maduros[85].

O ciberlibertarianismo é uma corrente teórica que ignora o fato de que o ciberespaço difere do mundo físico, apesar da sua capacidade de conectar pessoas com interesses comuns e simultaneamente permitir que se mantenham isoladas, segundo seus desejos e suas preferências pessoais. Por outro lado, o ciberlibertarianismo – tanto quanto o modelo de autorregulação de dados pessoais – ignora que é comum os agentes estatais enviarem "mensagens" de cunho normativo ao regular atividades e tentar interferir na arquitetura da rede. França[86] e Austrália[87], por exemplo, aprovaram leis que admitem a filtragem e a lista negra de controle e vigilância com o objetivo de proteger os direitos autorais. AirBnB promoveu mudanças na política sobre *home sharing* depois que França e Reino Unido adaptaram suas leis para tributar os serviços por eles prestados. Ou seja, em comum, todos esses exemplos evidenciam que há não esfera de interação social infensa à

---

[80] **O papel do DevOps como alicerce da próxima revolução tecnológica**, Computerworld, disponível em: <https://computerworld.com.br/2016/09/16/devops-sera-o-alicerce-da-proxima-revolucao-tecnologica/>, acesso em: 8 fev. 2019.

[81] SUNSTEIN, **Republic.com 2.0**, p. 25.

[82] Para melhor compreender o sentido de representação política ora empregado, cf. DOVI, Suzanne, Political Representation, *in*: EDWARD N. ZALTA (Org.), **The Stanford Encyclopedia of Philosophy**, Spring 2014. [s.l.: s.n.], 2014, p. 311.

[83] O tema da accountability será aprofundado adiante como mecanismo de controle da atuação privada e estatal. Cf. BENKLER, **The wealth of networks: How social production transforms markets and freedom**, p. 871; PRZEWORSKI, Adam; STOKES, Susan C.; MANIN, Bernand, **Democracy, Accountability, and Representation**, London: Cambridge University Press, 1999; SCOTT, Colin, Accountability in the Regulatory State, **Journal of Law and Society**, v. 27, n. 1, p. 38–60, 2000.

[84] BENKLER, **The wealth of networks: How social production transforms markets and freedom**, p. 241; LESSIG, **Code version 2.0 and other laws of Cyberspace**, p. 28.

[85] PERRITT JR, Jurisdiction in cyberspace, p. 415.

[86] JONES, Jacqueline, **France top court rules surveillance law constitutional**, Jurist, disponível em: <http://jurist.org/paperchase/2015/07/france-top-court-rules-surveillance-law-constitutional.php>, acesso em: 1 ago. 2015.

[87] TAYLOR, Josh, **Rights holders could get sites blocked without evidence**, ZDNet, disponível em: <http://www.zdnet.com/article/rights-holders-could-get-sites-blocked-without-evidence/>, acesso em: 2 ago. 2015.

regulação estatal, ainda que ela ocorra em menor intensidade ou com uma momentânea tolerância.

3.1 Joel Reidenberg e a Lex Informatica

Seguindo a perspectiva que será retomada no capítulo 2, quando então se examinará o impacto de cada uma dessas correntes nos modelos regulatórios próprios da proteção e dados e privacidade, vale ressaltar que o primeiro autor a criticar as falhas do modelo libertário foi Joel Reidenberg[88], ainda que em parte concordasse com Post e Johnson acerca das fronteiras imaginárias e o processo de desintegração das referências territoriais[89]. Enquanto fundador da corrente ciberpaternalista, Reidenberg estabeleceu uma aproximação entre a teoria do direito no ciberespaço e a *Lex Mercatoria*, processo a que ele denominou de *Lex Informatica* e que será a matriz de formulação da *Lex Privacy*.

O ciberespaço não era, na visão de Reidenberg, imune a intervenções regulatórias. O problema residia na correta identificação dos atores responsáveis pela regulação, os quais ele identificou a partir de duas fronteiras de elaboração do processo decisório, que envolvia o Estado e o setor privado (os técnicos e os cidadãos) de outro[90]. Numa conjugação de temas seria possível asseverar que Reidenberg acreditava que o modelo de regulação estatal ou compreensivo, tal como será examinado no capítulo 2, não era condizente com as características do ciberespaço, pois demandava também a participação dos técnicos e cidadãos. Este processo de interação tinha alguns componentes e regras especiais para Reidenberg pelo fato de serem baseados em acordos contratuais entre provedores de serviço de internet (*ISPs-Internet Service Providers*) e a arquitetura da rede, o que representava o soerguimento de novas fronteiras controladas pela sociedade[91].

A *Lex Informatica* seria, então, o novo modelo de governança do ciberespaço, mediante o qual os tomadores de decisão atuariam pautados pelos processos de regulação desenvolvidos tanto pelos atores estatais, quanto pelos técnicos e as normas sociais, ou seja,

---

[88] REIDENBERG, Joel R., Lex Informatica: The formulation of information policy rules through technology, **Tex. L. Rev.**, v. 76, p. 553, 1997, p. 554–555.

[89] *Ibid*., p. 632.

[90] MURRAY, **Information technology law**, p. 60.

[91] REIDENBERG, Lex informatica, p. 576–577; MURRAY, Andrew D., Nodes and gravity in virtual space, **Legisprudence**, v. 5, n. 2, p. 195–221, 2011, p. 3–4.

um modelo mais próximo da corregulação que será examinada no capítulo 2. A regulação mediante intervenções normativas seria apenas uma das formas de interferir nas relações sociais ocorridas no ciberespaço. Reidenberg defendia que a principal atividade regulatória seria realizada por outras fontes primárias: as normas sociais e os desenvolvedores de tecnologia[92]. A posição de Reidenberg era mais consistente do que a dos ciberlibertários, em especial quanto à função das interações sociais no ciberespaço e o poder dos desenvolvedores de tecnologia em enviar "mensagens regulatórias" ao mesmo tempo em que promovem mudanças na arquitetura da rede[93]. Reidenberg teve a capacidade de compreender que valores democráticos e o bem comum são fatores diretamente dependentes de algum tipo de controle da rede, que pode ser efetivado por diferentes atores[94]. O que os ciberpaternalistas não atentaram desde o princípio, como se observará no modelo proposto por Teubner, é que a densidade e o dinamismo representam a principal marca das múltiplas e simultâneas interações entre os atores no ciberespaço.

3.2 Laurence Lessig e a regulação pelo Código

Lawrence Lessig adotou como ponto de partida para o desenvolvimento do seu marco regulatório a contribuição teórica de Reidenberg, todavia a adaptou a partir de uma percepção importante: as pessoas não deixam de cometer crimes simplesmente porque a lei os proíbe[95]. Se assim o fosse, a imposição de sanções pela lei seria totalmente desnecessária[96]. Em outras palavras, Lessig demonstra que a regulação é a capacidade do Estado de delimitar comportamentos segundo os seus próprios objetivos, o que no contexto do ciberespaço significa a habilidade dos atores estatais de controlar a conduta dos seus cidadãos[97]. Lessig

---

[92] REIDENBERG, Lex informatica, p. 577.

[93] *Ibid*., p. 588.

[94] SUNSTEIN, **Republic.com 2.0**, p. 32.

[95] LESSIG, **Code version 2.0 and other laws of Cyberspace**, p. 23; BROWNSWORD, Roger, Code, control, and choice: why East is East and West is West, **Legal Studies**, v. 25, n. 1, p. 1–21, 2005, p. 2–3.

[96] MURRAY, Andrew D., Regulation and rights in networked space, **Journal of Law and Society**, v. 30, n. 2, p. 187–216, 2003, p. 28.

[97] LESSIG, **Code version 2.0 and other laws of Cyberspace**, p. 23.Um exemplo de tal aspecto decorre da Lei 12.727/12, conhecida como Lei Carolina Dickmann, que promoveu alterações no Código Penal para introduzir o art. 154-A. A atriz teve seu computador hackeado e suas fotos íntimas publicadas na internet por um adolescente de 16 anos. A partir de então, ela iniciou uma campanha contra o hacking e a extorsão na internet. A lei foi aprovada no Congresso e acarretou a criminalização da conduta de invasão de dispositivos. O grande problema da lei, no entanto, é que ela persiste em adotar parâmetros do mundo físico, como a necessidade da "violação do dispositivo de segurança", o que nem sempre é necessário (Invasão de dispositivo informático: Art. 154-A - Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de

observou que quatro fatores de constrangimento influenciam o comportamento dos indivíduos: a lei, as normas sociais, o mercado e a arquitetura[98].

O papel desempenhado pela lei e pelas normas sociais, no tocante aos atributos sancionatórios e morais, é conhecido e objeto da teoria geral do direito, mas e os outros dois elementos, ou seja, o mercado e a arquitetura? Como eles podem interagir e atuar para regular o ciberespaço? Lessig enxergou no mercado o poder do constrangimento pela lógica da oferta e procura, ao passo que a arquitetura representaria o desenho pelo qual seria possível construir o ambiente virtual, traduzido por códigos[99].

De fato, o código tem demonstrado ser um agente regulatório capaz de determinar os rumos da arquitetura do ciberespaço de forma tão ou mais efetiva do que os demais atores regulatórios, como se observa com os arquivos MP3, os arquivos *bit torrents*, os livros digitais, os algoritmos e a criptografia[100]. A disrupção, a convergência e a digitalização são as marcas deste processo de atuação regulatória do código sobre a arquitetura da rede. Para a análise que se fará nos próximos capítulos em torno dos modelos de regulação estatal, auto-regulação e corregulação, o papel desempenhado pelos algoritmos e criptografia, por exemplo, será fundamental para demonstrar que a auto-regulação e corregulação tem se destacado no cenário regulatório atual.

Inovações deste porte somente são possíveis porque o ambiente virtual permite e estimula que os atores recriem e reconfigurem permanentemente a arquitetura e o código, o que resulta em um efeito regulatório incessante sobre comportamentos em massa. Esta é a razão pela qual Lessig afirma que o código é a lei do ciberespaço:

> There is regulation of behavior on the Internet and in cyberspace, but that regulation is imposed primarily through code. The differences in the regulations effected through code distinguish different parts of the Internet and cyberspace. In some places, life is fairly free; in other places, it is more controlled. And the difference between these spaces is simply a difference in the architectures of control--that is, a difference in code[101].

---

mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita).

[98] *Ibid*., p. 30; MURRAY, Andrew D.; SCOTT, Colin, Controlling the New Media: Hybrid Responses to New Forms of Power, **The Modern Law Review**, v. 65, n. 4, p. 491–516, 2002, p. 493.

[99] LESSIG, **Code version 2.0 and other laws of Cyberspace**, p. 32.

[100] MLCAKOVA, Adela; WHITLEY, Edgar A., Configuring peer-to-peer software: an empirical study of how users react to the regulatory features of software, **European Journal of Information Systems**, v. 13, n. 2, p. 95–102, 2004, p. 95–96.

[101] LESSIG, **Code version 2.0 and other laws of Cyberspace**, p. 24.

Lessig compreendeu que o processo de digitalização, isto é, a transformação da informação do mundo físico em linguagem binária, e a convergência dos dispositivos tem causado profundas mudanças na arquitetura da rede, como se observa em plataformas de ensino denominadas *Massive Open Online Courses* (MOOCs), das quais o Coursera e o EdX são bons exemplos[102]. A premissa essencial de Lessig para a construção da base do seu modelo teórico em torno do código envolve a percepção de que a lei é incapaz, enquanto fonte direta, de regular de forma dinâmica os avanços ocorridos no ciberespaço[103]. Por esta razão, o papel regulatório desempenhado pela lei seria complementado pelo código, pelo mercado e pelas normas sociais[104]. Lessig é claramente um adepto do modelo de corregulação, o que ficará ainda mais evidente pela defesa que faz do código e do papel dos atores privados. Por essa razão, Lessig terá grande relevância na análise do modelo de corregulação da proteção de dados pessoais a ser realizada no capítulo 2.

Apesar de ambos serem considerados ciberpaternalistas, uma das particularidades entre as posições de Reidenberg e Lessig está no fato de que este adotou o setor privado como um dos mecanismos regulatórios, porém o subdividiu em duas categorias: o mercado e as normas sociais. A influência da arquitetura é um ponto comum entre ambos os autores, que acreditam na sua capacidade de promover alterações estruturais no ciberespaço[105]. Lessig destaca, entretanto, uma diferença crucial entre a lei e o código: a lei permite que os indivíduos sejam previamente conscientes e responsáveis pelos seus atos, ao passo que o código impõe ajustes aos comportamentos sociais a partir de influências externas.

Estas diferenças se tornam evidentes quando refletimos sobre as nossas ações no mundo físico, no qual temos consciência da escolha de furtar ou não um objeto, isto é, a realidade concede a faculdade de obedecer ou não a lei, respeitar ou não o direito à proteção

---

[102] SUNDARARAJAN, Arun, **Why the Government Doesn't Need to Regulate the Sharing Economy**, WIRED, disponível em: <http://www.wired.com/2012/10/from-airbnb-to-coursera-why-the-government-shouldnt-regulate-the-sharing-economy/>, acesso em: 9 abr. 2016.

[103] Benkler também explica porque a lei às vezes não é o instrumento regulatório mais adequado em relação ao ciberespaço: "The primary reason that these laws have not yet passed, and are unlikely to pass, is that the computer hardware and software, and electronics and telecommunications industries all understand that such a law would undermine their innovation and creativity". Cf. Também MAYER-SCHONBERGER, Viktor, The authority of law in times of cyberspace, **U. Ill. JL Tech. & Pol'y**, p. 1, 2001, p. 1074.

[104] LESSIG, **Code version 2.0 and other laws of Cyberspace**, p. 27.

[105] Por sinal, a arquitetura tem sido um dos principais instrumentos de proteção da privacidade no ciberespaço por meio de fenômenos como a privacidade por desenho (*privacy by design*) e a privacidade por padrão (*privacy by default*)

de dados e privacidade[106]. A arquitetura, por sua vez, nem sempre assegura a mesma liberdade de escolhas. Se por um lado é possível decidir entre caminhar no meio de uma rodovia sem calçadas, por outro a simples existência de uma porta na entrada de uma casa impede ou dificulta o acesso a ela[107]. Este exemplo ilustra como o código é capaz de modificar a arquitetura da rede para reproduzir elementos do mundo físico, tal como fronteiras, barreiras, jurisdição e obstáculos[108]:

> Regulation in cyberspace can help us see something important about how all regulation works. That's the lesson of the first theme, "regulability." It will also introduce a regulator ("code") whose significance we don't yet fully understand. That's the second theme, "Regulation by Code." That regulation will render ambiguous certain values that are fundamental to our tradition. Thus, the third theme, "latent ambiguity." That ambiguity will require us, the United States, to make a choice. But this choice is just one among many that many sovereigns will have to make. In the end the hardest problem will be to reckon these "competing sovereigns," as they each act to mark this space with their own distinctive values[109].

O código representa, ainda que de forma ambígua, um novo conceito de liberdade e restrição no ciberespaço, afinal por meio dele é possível construir, arquitetar ou codificar de modo a proteger os valores que uma sociedade considera fundamental ou até fazê-los desaparecer em dado contexto[110], como constatado no episódio conhecido como *Wikileaks*[111]. Um destes pontos sensíveis envolve a utilização do código para a mudança da arquitetura enquanto mecanismo de controle e proteção dados[112]. Ambos desempenham

---

[106] LESSIG, **Code version 2.0 and other laws of Cyberspace**, p. 26.

[107] REIDENBERG, Joel R., Technology and Internet jurisdiction, **University of Pennsylvania Law Review**, p. 1951–1974, 2005, p. 1952.

[108] Mesmo que a recente Lei 12.965/14, conhecida como Marco Civil da Internet, seja considerada uma das mais revolucionárias normas em termos de marco regulatório democrático, suas falhas e omissões no tocante à jurisdição e proteção de dados são expressivas. Um exemplo disso decorre do fato de que ela apenas protege os dados armazenados em dispositivos e equipamentos fisicamente localizados no Brasil (art. 11, §1.º). No entanto, os dados armazenados mediante cloud computing, espalhados ao redor do mundo, ainda que de cidadãos brasileiros, não são atingidos pela lei. (Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.§ 1o O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil).

[109] LESSIG, **Code version 2.0 and other laws of Cyberspace**, p. 30.

[110] SAMUELSON, Privacy as Intellectual Property, p. 316.

[111] **WikiLeaks**, disponível em: <https://wikileaks.org/>, acesso em: 8 fev. 2019.

[112] BENKLER, **The wealth of networks: How social production transforms markets and freedom**, p. 42.

papéis decisivos e cada vez mais o farão[113], conforme se constata a partir do caso Max Schrems contra o Facebook, no qual a Corte Europeia de Justiça declarou a invalidade do *Safe Harbor Agreement* entre União Europeia e Estados Unidos, pertinente à transferência intercontinental de dados de cidadãos e empresas americanas e europeias[114].

E não apenas a privacidade e os dados tem sido diretamente afetados por este fenômeno. A propriedade intelectual também vivencia o dilema entre a cultura livre e a igualdade[115], de um lado, e o direito de propriedade sobre a criação de outro[116]. Esta disputa é o resultado do surgimento de novos valores, os quais desafiam a concepção tradicional de propriedade e sua função em termos de bem-estar econômico e social[117], com o intuito de extrair a máxima utilidade das possibilidades oferecidas pela economia compartilhada[118].

Lessig ilustra seu modelo por meio do que denomina de *pathetic dot*, uma representação do modo como o indivíduo é governado pela lei, pelo mercado, pelas normas sociais e pela arquitetura, mediante uma força centrípeta e unidirecional, contra a qual pouco pode influir. Este controle não será realizado apenas pelos atores estatais e pelos tribunais, mas também por atores privados, o que significa que a liberdade se torna a característica mais suscetível de remodelação e influência no ciberespaço.

---

[113] A preocupação com a proteção de dados no ciberespaço está no centro das atenções no momento no Brasil. A recente conclusão do Anteprojeto de Proteção de Dados e a regulamentação do Marco Civil da Internet foram as principais medidas adotadas desde que Edward Snowden revelou a espionagem realizada pela NSA. "Other cases like Ashley Madison, Target Supermarket and Amazon became famous as well and are being taken in account in the challenge of developing appropriate and effective legislation (DUHIGG, Charles, How companies learn your secrets, **The New York Times**, 2012.) .

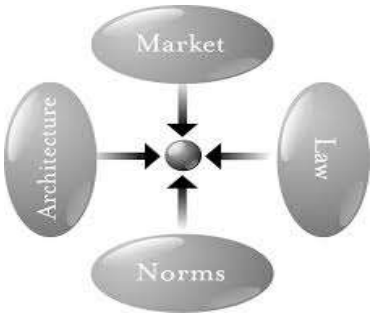
[114] EUROPEAN COURT OF JUSTICE, Maximillian Schrems v. Data Protection Comissioner (Case 362/2014).

[115] BENKLER, Yochai, Constitutional bounds of database protection: the role of judicial review in the creation and definition of private rights in information, **Berkeley Technology Law Journal**, v. 15, p. 535–603, 2000, p. 538.

[116] CASTELLS, Manuel, **The rise of the network society: The information age: Economy, society, and culture**, Londres: John Wiley & Sons, 2011, p. 43.

[117] POSNER, Richard, **Do patent and copyright law restrict competition and creativity excessively?**, The Becker-Posner Blog, disponível em: <http://www.becker-posner-blog.com/2012/09/do-patent-and-copyright-law-restrict-competition-and-creativity-excessively-posner.html>, acesso em: 1 nov. 2015.

[118] BERKELEY, Reinventing the company.



Pathetic dot

Embora a análise de Lessig tenha sido inovadora, ele ignorou três importantes aspectos, alguns deles identificados por David Post[119] e por Viktor Mayer-Schönberger[120]. Primeiro, a capacidade recíproca dos indivíduos de influenciar a arquitetura e de ser por ela influenciado, no sentido de que o *pathetic dot* não é apenas um ponto perdido no ciberespaço, crítica também válida se considerarmos o referencial teórico de Teubner. Não é raro encontrar situações nas quais um simples indivíduo é capaz de influenciar comportamentos, ideias e preferências, sem se valer de mecanismos políticos, de expressão do poder econômico ou de procedimentos deliberativos. Shawn Fanning e o Napster, por exemplo, tiveram grande impacto na transformação sofrida pela indústria da música[121], enquanto Aaron Swartz, criador do Reddit e do RSS, conseguiu atingir a política editorial da base de dados JSTOR[122]. Como observa Benkler, a emergência de uma economia da informação em rede tem o potencial de estimular a autonomia individual por três razões:

> First, it increases the range and diversity of things that individuals can do for and by themselves.
> [...] Second, the networked information economy provides nonproprietary alternative sources of communications capacity and information, alongside the proprietary platforms of mediated communications.
> [...] Third, the networked information environment qualitatively increases the range and diversity of information available to individuals[123].

---

[119] POST, David G., What Larry doesn't get: code, law, and liberty in cyberspace, **Stanford Law Review**, v. 52, n. 5, p. 1439–1459, 2000, p. 1454–1456.

[120] MAYER-SCHONBERGER, Viktor, Demystifying Lessig, **Wis. L. REv.**, p. 713, 2008.

[121] MITTEN, Christopher, **Shawn Fanning: Napster and the music revolution**, New York: Twenty-First Century Books, 2002.

[122] JSTOR, Evidence in United States vs. Aaron Swartz, 2013.

[123] BENKLER, **The wealth of networks: How social production transforms markets and freedom**, p. 137.

Em um mundo globalizado, a regulação não se limita a um código binário proibir-permitir como supõe grande parte dos agentes reguladores, tampouco é prerrogativa de atores estatais, por mais que os limites estabelecidos pela lei e pelas fronteiras sejam inflexíveis e expressivos. O processo de tomada de decisões no ciberespaço é significativamente plural, assimétrico, policontextual, marcado por decisões cujos parâmetros axiomáticos nem sempre são previamente conhecidos, como se observará no modelo proposto por Teubner[124]. Contudo, tal como Post observou na crítica a Lessig, o processo de tomada de decisões no ciberespaço nem sempre tem a característica de escolha coletiva ou de ação política, seja para promover a inovação seja para resguardar direitos como a privacidade e proteção de dados:

> I have no quarrel with the notion that the code/architectures of cyberspace embed fundamental values, and I have no quarrel with the notion that each of us, confronting the design of these new cyberplaces, faces a choice among different values. It does indeed matter, as Lessig says, whether the code of a cyber-place permits us to be anonymous or not, tracks our mouse droppings or not, allocates to us one screen name or ten, allows us to gather in groups of 20 or 50 or 500, or exposes us to many or to no random encounters.
> But I do quarrel with the notion that the choices to be made among value-laden architectures are therefore "political" decisions that should necessarily be subject to "collective" decision-making. Consider, by way of counterexample, the original, and still probably the most powerful, value laden code/architecture of them all: the English language. The semantic and syntactic structures of English (and of all natural languages) are deep architectural constraints on our social life, as the crits (and, indeed, Lessig himself) have been fond of pointing out (and, as it should in fairness be noted, the anthropologists have known for a while).
> Language is not just "a way of communicating propositions about the world," it is "a constitutive social activity," a means by and within which we "construct social reality." Like the network protocols they so closely resemble, these semantic and syntactic structures embed important and often fundamental values throughout. Each of us, therefore, has choices to make, choices about how our own personal architectures of social reality will be constituted[125].

A segunda crítica a Lessig se deve ao fato de não ter dimensionado de forma apropriada que a legitimidade e a *enforceability* no ciberespaço são construídas a partir de fronteiras virtuais, com valores sociais e atores variados, capazes de influenciar escolhas e

---

[124] TEMPERTON, James; BURGESS, Matt, **Net neutrality: European Parliament votes in favour of "two speed" internet**, Wired UK, disponível em: <http://www.wired.co.uk/news/archive/2015-10/27/net-neutrality-european-union-vote>, acesso em: 28 out. 2015.

[125] POST, What Larry Doesn't Get, p. 1456–1457.

comportamentos sob a perspectiva transnacional[126]. Ainda sob o prisma do modelo regulatório de Lessig, uma questão remanesce sem resposta: quem seria a instância regulatória neste ambiente transnacional do ciberespaço, no qual o conceito de soberania difere significativamente daquele do mundo físico?

Enquanto a União Europeia, por meio de diretivas e regulamentos, adota parâmetros mais incisivos de regulação da proteção de dados e privacidade – num modelo de corregulação eficaz - , Estados Unidos tem focado na adoção de mecanismos de vigilância em massa, proteção da propriedade intelectual e liberdade de expressão. Neste cenário de regulação por justaposição, a que instituições os cidadãos dos diversos países e culturas devem reportar suas demandas por proteção de interesses e disputas transnacionais? Qual o papel da accountability dos agentes de mercado que atuam na camada regulatória? Lessig avança pouco nesses temas.

Um dos possíveis fóruns de construção de mecanismos de regulação transnacional tem sido o *IGF-International Government Forum*, no entanto, apesar de ter se tornado uma arena de expressiva troca de experiências entre os *stakeholders*, a influência sobre os atores estatais não tem ocorrido com a mesma efetividade. A solução encontrada por muitos dos Estados que não desejam assegurar tanto espaço para a regulação privada foi conferir efeitos extraterritoriais às suas leis ou adotar mecanismos de *data localization*[127] com o intuito de assegurar que empresas estejam ao alcance das autoridades estatais de fiscalização e controle. Isto significa que não há uma política regulatória estável e uniforme que alcance *stakeholders* públicos e privados internacionais, o que pode ser evidenciado pela forma como o ciberespaço tem sido arbitrária e casuisticamente governado.

A última crítica ao marco regulatório de Lessig decorre do fato de ter sido construído com base na experiência de países do sistema *common law*, muitas vezes ignorando as particularidades do sistema continental europeu ou *civil law*, no qual mesmo as normas sociais, o mercado e a arquitetura atuam segundo parâmetros legais. Embora as grandes corporações de tecnologia tenham políticas globais de atuação, a pouca dinamicidade do legislador associada à pouca efetividade dos órgãos de fiscalização e controle, tem

---

[126] JOERGES, Christian; SAND, Inger-Johanne; TEUBNER, Gunther, **Transnational governance and constitutionalism**, Portland: Bloomsbury Publishing, 2004.

[127] CLARK, Sam, **Apple confirms Russian local data storage**, Global Data Review, disponível em: <https://globaldatareview.com/article/1180120/apple-confirms-russian-local-data-storage>, acesso em: 8 fev. 2019.

demonstrado que nos países de sistema *civil law* o Poder Legislativo não é capaz de acompanhar com a mesma velocidade e percepção as inovações no ciberespaço. Um claro exemplo disso é a LGPD, que somente após oito anos de tramitação foi aprovada no Congresso Nacional, e a GDPR, que teve os seus trabalhos preparatórios iniciados em 2012[128].

Curiosamente, uma grande quantidade de casos paradigmáticos relacionados ao ciberespaço ocorreu em países que adotam o sistema da *common law*, de modo que, ao contrário do que defendia Lessig, é impossível ignorar o papel desempenhado pelos tribunais e pelo Poder Legislativo nos países de *civil law*.

4. A regulação por camadas

Embora Yochai Benkler também possa ser considerado um ciberpaternalista, seu modelo regulatório, concebido pela superposição de camadas, adota premissas distintas dos modelos anteriores.[129] De acordo com Benkler, na economia da informação em rede, caracterizada pela descentralização das ações individuais,[130] cada ator exerce um papel relevante e é capaz não apenas de consumir como também de ser um centro de produção.[131] No novo modo econômico de produção, a remoção das restrições físicas sobre a efetiva produção de informação tornou a criatividade humana a base do desenvolvimento do ciberespaço.[132] Para explicar o fluxo da informação e como a economia compartilhada funciona, Yochai Benkler desenhou um sistema de comunicação definido em três camadas:[133] física, lógica e de conteúdo.

---

[128] LYNSKEY, Orla, **The Foundations of EU Data Protection Law**, 1 edition. New York: Oxford University Press, 2015, p. 6; JAY, Rosemary *et al*, **Guide to the General Data Protection Regulation**, [s.l.]: Sweet & Maxwell, 2017, p. 2–3.

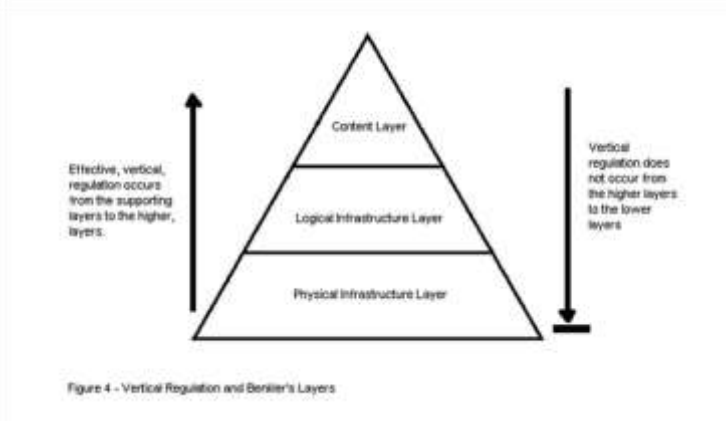
[129] BENKLER, **The wealth of networks: How social production transforms markets and freedom**, p. 384.

[130] BENKLER, Yochai, Freedom in the commons: Towards a political economy of information, **Duke LJ**, v. 52, p. 1245, 2002, p. 1248.

[131] BENKLER, **The wealth of networks: How social production transforms markets and freedom**, p. 32.

[132] LÉVY, **Cibercultura**.

[133] "But this technocratic approach is obviously difficult to realize because there is no unambiguous correspondence between technical functions and social action. Thus, the studies usually restrict the number of layers to three. Benkler (2006: 383–459), for instance, distinguishes a physical layer (e.g. cables), a code layer (e.g. browsers, e-mail, Internet protocols) and a content layer (e.g. videos, music, speech). Similarly, Zittrain distinguishes a physical layer, a protocol layer, and an application layer, which includes but could also be separated from a content layer ZITTRAIN, Jonathan, **The future of the internet–and how to stop it**, [s.l.]: Yale University Press, 2008, p. 65. Generally, the lower layers are more technical and the upper layers more social.



Matrix de camadas

A primeira camada, denominada de física, refere-se aos bens materiais e objetos utilizados para estabelecer conexões entre os indivíduos, como computadores, cabos, redes de conexão e celulares.[134] Por outro lado, a camada do conteúdo é considerada "the set of humanly meaningful statements that human beings utter to and with one another" and "includes both the actual utterances and the mechanisms, to the extent that they are based on human communication rather than mechanical processing, for filtering, accreditation, and interpretation".[135] Por último, a camada lógica consiste nos algoritmos, protocolos, plataformas, software, padrões, isto é, caminhos de linguagem que traduzem a vontade humana em *bits* capazes de serem transmitidos, armazenados e processados novamente para linguagem humana.

Benkler explica que a comunicação humana no ciberespaço deve seguir as três camadas de regulação para atingir seu propósito,[136] que nada mais é do que o surgimento de capacidades técnicas e práticas em um modelo de não exclusividade de bens, o qual permite o acesso mais econômico à rede, além de evitar o seu controle por uma das partes ou por determinada classe social.[137] Vale destacar, no entanto, que a observância das práticas indicadas por Benkler não transforma o ciberespaço numa arena livre de batalhas entre os atores reguladores sobre a forma como os bens exclusivos, os não-exclusivos e as plataformas

To address our questions concerning regulation, it is sufficient to differentiate only two layers: a technical layer and a content layer. BALDWIN; CAVE; LODGE, **The Oxford handbook of regulation**, p. 526.

[134] BENKLER, **The wealth of networks: How social production transforms markets and freedom**, p. 392.

[135] *Ibid*.

[136] Benkler se notabilizou pela forma como tratou da regulação do ciberespaço em camadas, o que pode ser identificado em outros trabalhos como BENKLER, Yochai. BENKLER, Constitutional bounds of database protection, p. 1203.

[137] BENKLER, **The wealth of networks: How social production transforms markets and freedom**, p. 392.

livres serão facilitados, proibidos ou conjugados de modo a otimizar os benefícios comuns e os individuais.[138] De fato, Benkler compreendeu melhor que Lessig algumas das particularidades das interações sociais no ciberespaço, especialmente pelo paralelo que foi capaz de traçar com os sistemas de comunicação e cooperação[139], os quais serão a principal premissa de análise dos network comunitaristas. Ademais, conforme se analisará ao final do capítulo, as redes de comunicação e cooperação serão elementos relevantes para o acoplamento estrutural proposto por Teubner, assim como para a construção da *accountability* como fundamento da *Lex Privacy*.

5. Os Network Comunitaristas e o modelo simbiótico de relação dos atores

Se por um lado o código e a arquitetura foram as principais características do modelo ciberpaternalista, por outro lado os network comunitaristas, liderados por Andrew Murray, Colin Scott e Paul Bernal, tiveram como foco o fluxo dinâmico da informação no ciberespaço. As bases teóricas do modelo network comunitarista advém de duas correntes teóricas importantes da sociologia, a Teoria dos Atores em Rede (*Actors Network Theory*-ANT) de Bruno Latour[140] e a Teoria dos Sistemas Sociais (*Social System Theory*-SST).[141] Esta última, formulada por Niklas Luhmann[142] esclarece que o ciberespaço deve ser compreendido a partir da complexidade do fluxo da informação em sistemas sociais e sua capacidade de afetar toda a organização da sociedade.

E como os sistemas são definidos por fronteiras entre eles e entre o ambiente, Teubner tenta mapear e estudar as interações sociais como um *proxy* para o controle da comunidade.[143] Com efeito, Luhmann e Teubner admitem que a sociedade não é formada apenas por indivíduos, mas pela comunicação simbiótica de redes.[144] A sociedade tem

---

[138] BENKLER, Yochai, Sharing nicely: On shareable goods and the emergence of sharing as a modality of economic production, **Yale Law Journal**, p. 273–358, 2004.

[139] Benkler desenvolve com maior profundidade o tema da cooperação em BENKLER, Yochai, **The penguin and the leviathan: How cooperation triumphs over self-interest**, [s.l.]: Crown Business, 2011.

[140] LATOUR, Bruno, **Reagregando o social: uma introdução à teoria do ator-rede**, [s.l.]: Edusc, 2012.

[141] MURRAY, Nodes and gravity in virtual space, p. 11.

[142] LUHMANN, Niklas, **Introduction to systems theory**, Malden: Polity, 2013, p. 25–28.

[143] TEUBNER, Global Bukowina, p. 2–4.

[144] LUHMANN, Introduction to systems theory, p. 29.

inúmeros sistemas herméticos que funcionam em uma lógica binária, tal como a lei (permitido/proibido) e a economia (valor/sem valor). Em outras palavras, o foco desta teoria está centrado em filtrar o fluxo de informação para os tomadores de decisão.

Ao contrário dos ciberpaternalistas, os network comunistaristas acreditam que não há um *pathetic dot* estático, incapaz de influenciar e ser influenciado no ciberespaço.[145] Na visão dos comunitaristas, o indivíduo não se resume a um ponto amorfo e estático; ele interage de forma ativa[146], mediante linhas multitudinais de comunicação, dentro de uma rede muito mais ampla do que se supõe.[147] Teubner denomina este processo de comunicação como "vilas globais", um sistema de pluralismo jurídico formado por diversos atores conectados pela informação, que, como referencial teórico dessa tese, ajudará na construção da *Lex Privacy*:

> The emerging global (not inter-national!) law is a legal order in its own right, which should not be measured against the standards of national legal systems. It is not - as is usually understood - an underdeveloped body of law which has certain structural deficiencies in comparison to national law. Rather, its peculiar characteristics as fully fledged law distinguishes it from the traditional law of the nation states. These characteristics can be explained by differentiation within world society itself. While global law lacks political and institutional support on the global level, it is closely coupled with globalized socio-economic processes.
> [...] From this, the main thesis follows: global law will grow mainly from the social peripheries, not from the political centres of nation states and international institutions. A new living law growing out of fragmented social institutions which had followed their own paths to the global village seems to be the main source of global law.[148]

Os network comunitaristas não enxergam o ciberespaço como uma arena que demande fatores de constrangimento, mas sim como um lugar em que a regulação pode ser feita por consentimento e outros valores democráticos como a *accountability*[149], ou seja, o ciberespaço não é um fórum que pertence apenas a agentes reguladores.[150] Por essa razão, a análise do consentimento em contraste com a *accountability* será um dos pilares de sustentação do modelo regulatório da *Lex Privacy.* Isto significa que os atores reguladores

---

[145] SCOTT, Colin, **Regulation in the age of governance: The rise of the post regulatory state**, [s.l.]: Edward Elgar Publishing, 2004, p. 145.

[146] SAMUELSON, Privacy as Intellectual Property, p. 318.

[147] SCOTT, Accountability in the Regulatory State, p. 45.

[148] TEUBNER, Global Bukowina, p. 2–4.

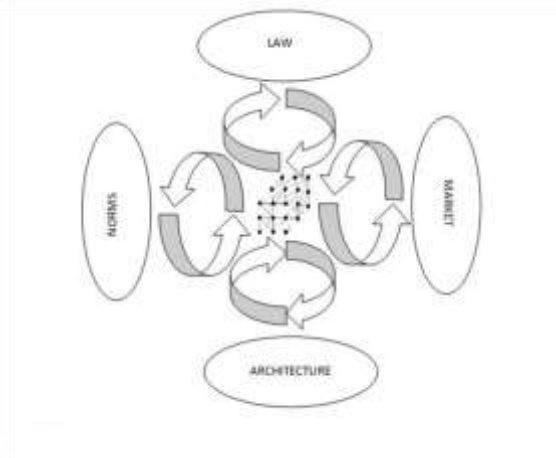
[149] SUNSTEIN, **Republic.com 2.0**, p. 74.

[150] BENKLER, **The wealth of networks: How social production transforms markets and freedom**, p. 42.

atuam mediante a representação da comunidade simbiótica e dela obtém sua legitimidade, conforme esclarecem Murray e Scott:

> Similarly Colin Scott and myself in our paper Controlling the New Media suggest a focus on hybrid models of regulation. We, like Lessig, suggest four modalities of regulation which we title, (1) hierarchical control (2) competition-based control, (3) community based control and (4) design-based control. Unlike Lessig, we acknowledge that the development of regulatory structures is often organic in nature.[151]

De certo modo, os network comunitaristas entenderam de forma mais precisa como o ciberespaço realmente funciona, quais forças o governam, que atores o influenciam e, em grande medida, isso se deve ao fato de terem compreendido como a interação ocorre no sistema depois de um processo complexo caracterizado pelo fluxo dinâmico da informação disponível para os tomadores de decisão, a que denominam de *symbiotic web*.[152] Isso os aproxima ainda mais da premissa da policontextualidade de Teubner nas vilas globais. Os network comunitaristas conseguiram formular um juízo mais interativo do ciberespaço, no qual as normas sociais, a lei, o mercado e a arquitetura podem se influenciar mutuamente e ser influenciados pela comunidade.[153] A percepção estática do *pathetic dot* e a falta de cooperação entre os atores no ciberespaço é talvez a mais interessante contradição dos ciberpaternalistas quando criticam a ação coletiva, conforme se denota do esquema proposto pelo network comunitaristas:



Matriz simbiótica

[151] MURRAY; SCOTT, Controlling the New Media, p. 505; MURRAY, **The Regulation of Cyberspace**, p. 29.

[152] MURRAY, Nodes and gravity in virtual space, p. 8.

[153] SCOTT, Accountability in the Regulatory State, p. 48.

Bits e átomos se expressam em diferentes velocidades, algo que os ciberpaternalistas não atribuíram tanta relevância para estabelecer as diferenças entre o mundo físico e o virtual.[154] Apesar disso, as mesmas críticas feitas aos ciberpaternalistas podem ser dirigidas aos network comunitaristas por não considerarem as particularidades dos países de sistema continental europeu ou *civil law*, no qual a lei exerce um papel de extrema relevância no processo regulatório. Como o Poder Legislativo e o Poder Judiciário nem sempre estão preparados para conduzir a vanguarda dos debates em relação aos temas do ciberespaço, à sociedade é concedida uma larga margem de atuação para modelá-lo por meio da arquitetura e do código, do mercado e das normas sociais, tal como ocorre nos países de sistema *common law*.

6. O impacto do pluralismo jurídico na regulação da proteção de dados e privacidade: a Bukowiva do Ciberespaço

Compreender a regulação do ciberespaço a partir da perspectiva do pluralismo jurídico tem sido uma forma de superar o modelo exclusivamente estatal de regulação e abrir espaço para a corregulação e a autoregulação – temas cuja interação serão analisados no próximo capítulo - , o que pode ser observado no contraste existente entre ciberpaternalistas, ciberlibertários e network comunitaristas. E neste aspecto, Teubner pode ser considerado um dos principais articuladores da ideia de pluralismo jurídico global, com notável impacto no ciberespaço.[155] Por esta razão, como contraponto às teorias analisadas anteriormente - em especial as dos ciberlibertários e ciberpaternalistas - , Teubner será o marco teórico adotado como complemento dos parâmetros regulatórios até então desenvolvidos e se tornará o substrato da posterior identificação da *lex privacy* enquanto modelo regulatório próprio da privacidade e proteção de dados pessoais.

Teubner se vale de um modelo a que denominou de *Bukowina Global*[156] como um dos referenciais teóricos para a construção de um paradigma de pluralismo jurídico

---

[154] LESSIG, **Code version 2.0 and other laws of Cyberspace**, p. 20.

[155] Cf. TEUBNER, Gunther, Legal irritants: good faith in British law or how unifying law ends up in new divergencies, **The Modern Law Review**, v. 61, n. 1, p. 11–32, 1998, p. 598; TEUBNER, Gunther, **Direito, sistema e policontexturalidade**, Piracicaba: Unimep, 2005, p. 367; JOERGES; SAND; TEUBNER, **Transnational governance and constitutionalism**, p. 1056.

[156] TEUBNER, Gunther, A Bukowina global sobre a emergência de um pluralismo jurídico transnacional, **Impulso: Revista de Ciências Sociais e Humanas**, v. 14, n. 33, p. 9–31, 2003.

transnacional no qual o *direito vivo* de Eugen Ehrlich ocupa o centro de análise. Teubner parte da investigação do *direito vivo* para desenvolver um modelo normativo no qual as prescrições jurídicas não oferecem um quadro completo das condições jurídicas"[157], uma vez que estas deveriam supostamente guardar conformidade com as realidades do seu tempo, fenômeno este que também se identifica com a dinamicidade da evolução tecnológica do ciberespaço.

Neste cenário, o *direito vivo* se soma ao direito estatal vigente, isto é, aquele que domina a regulação das relações sociais apesar de nem sempre corresponder às prescrições jurídicas[158]. O direito vivo compreende o marco normativo no qual a própria sociedade desempenha um papel fundamental na criação do direito, e não a política ou o Estado.[159] E este aspecto será fundamental para a explicitação dos contornos de desenvolvimento de um modelo regulatório complementar ao estatal para a proteção de dados no ciberespaço.

A formulação de Teubner considera a existência de uma autônoma rede de comunicações jurídicas capaz de produzir normas dotadas de eficácia mediante uma pluralidade de processos transnacionais, segundo métodos de auto-organização e auto-coordenação em nível global, tal como se identificará posteriormente na *Lex Privacy*[160]. Em outros termos, Teubner aponta para a emergência de um processo espontâneo de multiplicação de subsistemas normativos autônomos, a que denomina "multiplicidade de constituições civis"[161]. Essas rotinas naturais de criação normativa se desenvolvem mediante tendências de coordenação em escala global[162], numa clara demonstração de que o modelo de organização em torno de Estados-nações soberanos não é capaz de suprir todas as demandas regulatórias e se adequar aos novos padrões sociais, os quais demandam algumas adaptações à teoria das fontes e dos discursos do Direito[163].

---

[157] EHRLICH, **Fundamentos da sociologia do direito**, p. 374.

[158] *Ibid*., p. 378.

[159] *Ibid*.

[160] VESTING, Thomas, Constitutionalism or legal theory: comments on Gunther Teubner, **JOERGES, Christian; SAND, Inger-Johanne; TEUBNER, Gunther. Transnational governance and constitutionalism. Oxford: Hart**, p. 29–39, 2004, p. 30.

[161] *Ibid*.

[162] AXELROD, Robert, **The Evolution of Cooperation**, New York: Basic Books, 1984, p. 809.

[163] JOHNSON; POST, Law and borders: the rise of law in cyberspace, p. 686.

Parte da inadequação do modelo normativo de sistemas jurídicos nacionais decorre da diferenciação promovida pelo impulso de processos econômicos, políticos e sociais - *e.g.* convergência, disrupção, desmaterialização e digitalização - , como os verificados com maior intensidade no ciberespaço e em especial no sistema global de proteção de dados pessoais. Um dos caminhos indicados por Teubner para realizar as modificações necessárias neste cenário perpassa pela repolitização do direito mundial, o que não ocorrerá necessariamente pela via das instituições políticas tradicionais[164], mas pelo amplo poder regulador concretamente exercido por outros atores. Isto dependerá essencialmente do acoplamento estrutural empreendido por discursos especializados como os realizados pelos desenvolvedores de tecnologia, as empresas e os usuários, como demonstrado por Orin Kerr ao dissertar sobre às perspectivas interna e externa do ciberespaço:[165]

> "the Internet's ability to generate a virtual reality creates what I will call the problem of perspective in Internet law. The problem is that whenever we apply law to the Internet, we must first decide whether to apply the law to the facts as seen from the viewpoint of physical reality or virtual reality. In a surprising number of situations, we arrive at one result when applying law from an internal perspective and a different result when applying law from an external perspective. In fact, many of the major disputes within the field of "cyberlaw"4 boil down to clashes between internal and external perspectives."

Na Bukowina Global, tanto a Política quanto o Direito recebem influxos dos efeitos da globalização, a evidenciar a relevância do *direito vivo* na construção de novas conjunturas associadas ao modelo de regulação estatal. Mas não se trata de um fenômeno homogêneo, com características uniformes em todas as suas manifestações, tampouco restrito à lógica da ordem econômica capitalista. O processo de globalização a que se refere Teubner é marcado por uma expressiva fragmentação, ou seja, é "impulsionado pelos sistemas parciais individuais da sociedade em velocidades distintas"[166], com fortes indicativos de regionalização, autonomia e delimitação da política pela capacidade de inovação dos principais atores.

---

[164] TEUBNER, A Bukowina global sobre a emergência de um pluralismo jurídico transnacional, p. 11.

[165] KERR, The Problem of Perspective in Internet Law, p. 358.

[166] TEUBNER, A Bukowina global sobre a emergência de um pluralismo jurídico transnacional, p. 12.

A reunião destes fatores tem propiciado o surgimento de verdadeiras *vilas globais*[167](*global villages*), cujo traço característico é a expressão da autonomia em contraponto às pretensões hegemônicas da política e da exaustiva regulação estatal. A ideia de vilas globais concebida por Teubner atuará em linha de conexão com instrumentos jurídicos capazes de identificar a existência de um modelo de governança do ciberespaço centrado no que neste trabalho se denominará como *Lex Privacy*, enquanto expressão de um modelo plural de normas de proteção de dados e privacidade.

Exemplos claros disso podem ser identificados a partir do papel desempenhado pela ICANN-*Internet Corporation for Assigned Names and Numbers*, pela IETF-*Internet Engineering Task Force*, pelas normas corporativas vinculantes (*binding corporate rules-BCRs)*, cláusulas-modelo, contratos-tipo, códigos de ética, certificações privadas, anonimização, pseudonimização e pelo uso da criptografia.

Esta percepção em torno do crescente papel de entes privados, desenvolvedores e usuários no processo regulatório do ciberespaço pode ser bem observada a partir da ICANN, uma organização privada capaz de ditar um ordenamento jurídico próprio em torno de um discurso especializado - nomes de domínio e números - , com incursões políticas fortes perante as *vilas globais*[168] - definições de procedimentos, padronização de linguagem e idiomas de acordo com segmentos (.org, .br, .adv, .edu). Isso demonstra que a regulação não tem se restringido a processos institucionais definidos por organizações estatais. Organizações não-estatais como a ICANN tem se "institucionalizado" sob o prisma da ordem privada dos atores do ciberespaço, a revelar o quão propício este fórum se revela para o pluralismo jurídico, como enfatizado por Teubner:

> "Over time, it has developed functional and territorial representation, forms of separation of powers, and an effective 'jurisdiction' over domain name allocation. This give rise to 'governance questions' of 'constitutional significance'. The ICANN panels, when asked whether fundamental rights also applied to the Internet, did not refer to national constitutions, which would then only apply to national segments of the Internet, but instead developed their own autonomous fundamental rights standards".

---

[167] *Ibid*., p. 13.

[168] LADEUR, Karl, ICANN and the Illusion of a Community-Based Internet: Comments on Jochen von Bersstorff, *in*: JOERGES, Christian; TEUBNER, Gunther (Orgs.), **Transnational Governance and Constitutionalism**, Oxford: Hart Publishing, 2004, p. 283.

> [...] 'Corporate constitutionalism' is the most prominent case of constitutional law created through multinational corporations' private ordering[169].

A ICANN atua a partir de uma rede de contratos que se estrutura em torno de um sistema regulatório abrangente, o qual transcende a sua própria organização formal. A ICANN celebra contratos com a Verisign, uma organização privada que atua como administradora de nomes de domínio e esta, por sua vez, celebra contratos com os administradores de domínio de cada país, numa clara demonstração de que o ordenamento estatal fica, de certo modo, relativamente à margem de todo o processo[170]. Por esta razão, Teubner ressalta que a constituição da ICANN envolve um complexo cenário de contratos e interações formais, de modo que "individual contracts and formal organizations are forming a whole regulatory network aimed at achieving one overriding purpose"[171].

Outro exemplo de arranjo privado capaz de evidenciar o poder da regulação privada advém da criptografia[172]. Considerada uma das ferramentas disponíveis para preservar a autonomia e a fragmentação desejadas nas interações no ciberespaço[173], a criptografia tem sido útil no aprimoramento dos subsistemas sociais que tem impedido que a política levante fronteiras nacionais como escudos contra a proliferação de mecanismos de pluralismo jurídico, sobretudo porque "outros subsistemas sociais já começaram a formar uma expressiva quantidade fragmentada de sistemas mundiais distintos"[174].

A marca da dinamicidade e da fragmentação deste processo criador é incapaz de ser compreendida por mecanismos de produção central do direito, frontalmente opostos "ao direito dos juristas, da decisão prática de conflitos jurídicos, e sobretudo em oposição ao

---

[169] TEUBNER, Gunther, **Constitutional fragments: Societal constitutionalism and globalization**, Oxford: Oxford University Press, 2012, p. 56.

[170] *Ibid*., p. 57.

[171] *Ibid*., p. 58.

[172] Cf. ABELSON, Harold *et al*, Keys under doormats: mandating insecurity by requiring government access to all data and communications, **Journal of Cybersecurity**, v. 1, n. 1, p. 69–79, 2015; RICE, Eric, The Second Amendment and the Struggle Over Cryptography, **Hastings Sci. & Tech. LJ**, v. 9, p. 29, 2017; PAAR, Christof; PELZL, Jan, **Understanding cryptography: a textbook for students and practitioners**, [s.l.]: Springer Science & Business Media, 2009.

[173] Colin Bennett desenvolve a premissa de que a regulação da privacidade no ciberespaço deve ocorrer segundo a ferramenta mais adequada para determinado contexto, de acordo com o espectro de instrumentos numa caixa de ferramentas, e não apenas a lei. BENNETT, Colin J., **The Governance of Privacy: Policy Instruments in Global Perspective**, Cambridge: The MIT Press, 2006, p. 470.

[174] TEUBNER, A Bukowina global sobre a emergência de um pluralismo jurídico transnacional, p. 13.

direito vivo da Bukowina"[175]. E a explicação decorre da inadequação das teorias positivistas, excessivamente centradas na unidade do Estado e do direito, para admitir a globalização da produção normativa[176].

Não por outra razão, o papel dos agentes reguladores estatais no ciberespaço tem sido marcado por intervenções pontuais e com o intuito de estabelecer normas-programa para a proteção de liberdades, direitos fundamentais, valores sociais e inovação tecnológica[177], como ocorre com o Marco Civil da Internet, a Section 5 do Federal Trade Commission Act, o *General Data Protection Regulation*, o *Privacy Act* do Canadá e, mais recentemente, a Lei n. 13.303/18, a Lei Geral de Proteção de Dados.

Isto demonstra que o acoplamento estrutural do sistema político do mundo físico, realizado pelo ordenamento jurídico não conta com idêntico processo de fechamento e reprodução no plano do ciberespaço[178], o qual funciona de acordo com a lógica da *lei das vilas globais*, o que, em relação à proteção de dados e da privacidade, desencadeará a formação de um arcabouço normativo plural consubstanciado na *Lex Privacy*.

A principal contribuição de Teubner para a compreensão de um modelo normativo no qual a *Lex Privacy* desempenha uma função-chave na governança do ciberespaço decorre da circunstância de que "o direito mundial se desenvolve a partir das periferias sociais, das zonas de contato com outros sistemas sociais, e não necessariamente no centro de instituições dos Estados-nações ou de instituições internacionais"[179]. Isto significa

---

[175] *Ibid*.

[176] Thomas Vesting apresenta uma contribuição relevante para tal fato. Acredita que "a teoria dos sistemas de Luhmann pode ser interpretada - segundo a teoria pura do Direito de Kelsen - como uma tentativa de reagir à crise do positivismo jurídico sem renunciar ao conceito de sistema. [...] Diferentemente do que ocorria no positivismo jurídico, o sistema da teoria dos sistemas não é mais constituído através de uma 'unidade interna' de normas jurídicas e instituições coordenadas entre si. A hipótese de Kelsen de que o sistema jurídico precisa pressupor uma 'norma fundamental' para poder operar com êxito também é abandonada. No lugar dela, surge a demarcação contínua do sistema jurídica em relação a tudo que não é Direito. Ao invés de orientar-se pela diferença, por um pensamento que concebe o sistema a partir de uma distinção sistema/ambiente" VESTING, Thomas, Teoria do direito: uma introdução, **São Paulo: Saraiva**, p. 226, 2015, p. 131.

[177] SCHWARTZ, Paul M., Privacy and Democracy in Cyberspace, **Vanderbilt Law Review**, v. 52, p. 0, 1999.

[178] Marcelo Neves considera que a "Constituição enquanto acoplamento estrutural e, ao mesmo tempo, como mecanismo de diferenciação funcional entre política e direito ou, em outras palavras, de desintricamento entre poder e lei, que surgiu na esteira de transformações radicais da estrutura social da modernidade, foi - como já salientado - fator e produto de uma nova semântica, o constitucionalismo". NEVES, Marcelo da Costa Pinto, **Transconstitucionalismo**, 3. ed. São Paulo: WMF Martins Fontes, 2013, p. 60.

[179] TEUBNER, A Bukowina global sobre a emergência de um pluralismo jurídico transnacional, p. 14.

que as *global villages* formam os novos núcleos de interação virtual e de produção jurídica da Bukowina da sociedade da informação.

A coesão de comunidades étnicas, o apelo às delimitações territoriais e a comunhão de ideais políticos, no entanto, não representam fatores decisivos para a composição das vilas globais, ao contrário do que se observa no mundo físico[180]. Mais do que a interface promovida por estes fatores, a nova Bukowina demanda a reorientação de discursos e redes de comunicação de forma a propiciar a arquitetura de um proto-direito de redes especializadas, organicamente estruturadas e funcionalmente voltadas à criação de uma identidade fragmentada para o ciberespaço[181].

A criação do direito nas vilas globais ocorre por meio da auto-reprodução contínua de redes de comunicação especializadas - plataformas, códigos, sistemas, *software*[182] - , definidas com alguma flexibilidade, e não mediante a simples reprodução da dogmática e da tradição dos sistemas jurídicos contemporâneos. Quatro elementos podem ser apontados como os principais indicadores operacionais de criação do direito nas vilas globais do ciberespaço, bem como de segmentação em relação ao direito dos Estados-nações: (i) a diferenciação interna; (ii) as fontes do direito; (iii) a independência e a (iv) unidade do direito[183].

A diferenciação interna ampara-se no fundamento territorial, na ausência de fronteiras físicas para a produção do direito nas vilas globais. O argumento é muito semelhante ao utilizado pelos ciberlibertários Barlow[184], Post e Johnson[185], que indicavam as fronteiras e a soberania como os principais paradigmas a serem rompidos quando em comparação com o ciberespaço. A particularidade aqui reside na específica construção feita por Teubner no sentido da busca de formas autônomas de regulação de conflitos, os quais ocorrem em panoramas inter-sistêmicos e não mais inter-nacionais[186].

---

[180] *Ibid*.

[181] *Ibid*.

[182] SCHOR, Juliet B.; FITZMAURICE, Connor J., Collaborating and connecting: the emergence of the sharing economy, **Handbook of research on sustainable consumption**, v. 410, 2015.

[183] TEUBNER, A Bukowina global sobre a emergência de um pluralismo jurídico transnacional, p. 14.

[184] BARLOW, The next economy of ideas: selling wine without bottles on the global net, p. 434.

[185] JOHNSON; POST, Law and borders: the rise of law in cyberspace.

[186] TEUBNER, A Bukowina global sobre a emergência de um pluralismo jurídico transnacional, p. 14.

No tocante às fontes do direito, nas vilas globais os órgãos legislativos gerais perdem parte da sua decisiva influência - embora ainda seja forte, como se percebe pelo papel regulatório da União Europeia, do Brasil e do Estados Unidos - para atores que atuam mediante processos técnicos auto-organizados de acoplamento estrutural do direito - os desenvolvedores, as empresas e os usuários.

A independência, por sua vez, envolve o grau de isolamento institucional alcançado pelo ordenamento jurídico de alguns Estados-nações em relação aos processos globais de interação social, o que fomenta as necessidades políticas por reformas estruturais do direito[187]. Este talvez seja o ponto mais sensível dada a necessidade de intervenção regulatória dos Estados-nações para resguardar a proteção de direitos, garantias e liberdades.

A unidade do direito sempre representou um dos traços marcantes da identidade nacional, um bem político supremo e intangível para os Estados-nações. No entanto, a unidade do direito em escala global representava uma ameaça à pluralidade de culturas jurídicas, sobretudo se consideradas as peculiaridades dos sistemas de *common law* e *civil law*. Ainda assim, a construção do direito em vilas globais é condizente com a combinação de experiências unificadoras e de fontes variadas - marcos regulatórios e instrumentos contratuais como normas corporativas vinculantes, o Privacy Shield, *Consent Decree* da FTC e a Lei Geral de Proteção de Dados, por exemplo - , mas sempre tendo em mira a pluralidade regional de valores[188].

6.1 A policontextualidade como premissa de desenvolvimento do pluralismo

Assim como a percepção de um direito vivo formado em vilas globais, a pluralização de discursos a que se denomina policontextualidade é uma típica experiência moderna, conforme se denota de Weber[189] e Lyotard[190]. Mas qual seria a posição do direito na pluralidade de discursos?

---

[187] *Ibid*.

[188] *Ibid*., p. 15.

[189] WEBER, Max, Economia e sociedade: fundamentos da sociologia compreensiva. v. 1, **Brasília: UnB**, 1999, p. 142.

[190] LYOTARD, Jean-François, **A condição pós-moderna. Tradução de Ricardo Corrêa Barbosa**, [s.l.]: Rio de Janeiro: José Olympio, 2004, p. 168.

Uma das grandes contradições do movimento Direito e Economia reside exatamente no fato de que a racionalidade econômica não é a única a possuir o privilégio da institucionalização na sociedade como um todo[191]. O politeísmo de discursos permite que se aponte a ciência e a tecnologia - ao lado da economia, da política e do direito - como meios capazes de construir racionalidades de forma muito centrada[192]. Ao estabelecer essas centralidades, cada um desses ramos imprimiu certa institucionalização e universalização na sociedade. Por exemplo, a rede de computadores a que denominamos ciberespaço tem sua racionalidade construída na *praxis* social, o que significa que esses ordenamentos parciais e universais têm um padrão social capaz de influenciar o direito de modo muito incisivo[193]. E isso ocorre de cinco formas muitos específicas.

A principal modalidade de influência sobre o direito ocorre a partir das práticas sociais e das várias universalidades, numa tentativa de exigir do direito medidas regulamentadoras que reflitam princípios universais do particularismo que cada uma desses setores institucionalizou separadamente. O papel do direito "é abandonar o simples modelo de ameaça a sujeitos (des)obedientes com sanções e reformular suas normas para enquadrá-las conforme as exigências específicas nos domínios econômico, político e científico-tecnológico[194].

Por esta razão, Teubner afirma que "a reflexão jurídica deve simular as práticas de outros subsistemas sociais de modo a produzir normas socialmente adequadas, isto é, normas que reflitam a lógica interna dos ambientes sociais do direito"[195]. Melhor seria, no entanto, que a influência se verificasse a partir de um complexo formado de instrumentos independentes de produção de normas sociais que proporcionasse a criação de normas jurídicas a partir destes mesmos subsistemas da sociedade, como fomentado pela *Lex Privacy*.

A dimensão da policontextualidade envolve a elaboração mais detalhada de gramáticas simbólicas de linguagem que viabilizam uma análise mais profunda das práticas sociais, além de admitir a incomensurabilidade dos discursos e a falta de qualquer

---

[191] TEUBNER, Breaking frames, p. 94.

[192] *Ibid*.

[193] *Ibid*.

[194] *Ibid*.

[195] *Ibid*., p. 96–97.

metadiscurso[196]. Isso significa que, na atualidade os conflitos aos quais o direito está exposto não resultam de valores ideais, mas do conflito entre práticas sociais reais, verificadas no contexto de novos cenários como a tutela da privacidade e proteção de dados no ciberespaço.

A menção feita por Teubner ao politeísmo representa o parâmetro por ele utilizado para atribuir densidade à diversidade de discursos - denominada policontextualidade - e sua capacidade de influir no ordenamento. Isso ocorre em meio a sistemas sociais complexos, cuja dinâmica interna é tão poderosa que é capaz de causar efeitos desintegradores nos indivíduos, como se observa em relação às práticas de *hackers, fake news* e *cyber hate speech*, sobretudo porque a atenção se deslocou dos indivíduos para os discursos[197].

É importante compreender que o processo de digitalização da comunicação existente no ciberespaço não gira em torno de questões meramente teórico-legais de contratação de provedores, de neutralidade da rede, e de validade e implementação de normas nacionais no fluxo transnacional da internet[198] ou da eficácia dos direitos fundamentais. O desafio na construção do marco regulatório do ciberespaço envolve, na visão de Teubner, o direito de livre acesso à internet em contraposição aos problemas de exclusão do processo global de comunicação[199].

O amadurecimento político deste debate perpassa, na atualidade, pelo questionamento da democracia dos algoritmos e a necessidade de concepção de mecanismos de *accountability*, tal como defendido por Frank Pasquale[200] e Solon Barocas[201], com o intuito de assegurar ampla acessibilidade à rede, privacidade e controle de dados. A preocupação com a potencialidade segregacionista do ciberespaço é de tal relevo que Teubner lança uma considerável dúvida:

---

[196] *Ibid*., p. 99.

[197] *Ibid*., p. 101.

[198] TEUBNER, Gunther, Societal Constitutionalism: Alternatives to State-Centered Constitutional Theory?, *in*: JOERGES, Christian (Org.), **Transnational Governance and Constitutionalism**, Oxford: Hart Publishing, 2004, p. 4.

[199] *Ibid*.

[200] PASQUALE, Frank, The Black Box Society, **Cambridge, MA: Harvard University Press**, v. 36, p. 32, 2015.

[201] BAROCAS, Solon; HOOD, Sophie; ZIEWITZ, Malte, Governing algorithms: A provocation piece, 2013.

> "will inclusion/exclusion become the meta-code of the 21st century, mediating all other codes, but, at the same time, undermining functional differentiation itself and dominating other social-political problems through the exclusion of entire population groups[202]?

A nova ordem constitucional é caracterizada pela coexistência de ordens normativas independentes não apenas dos Estados, mas ao mesmo tempo de estruturas sociais não estatais, o que será ainda mais perceptível quando analisados os modelos regulatórios de outros países no capítulo 2. A formalização - seja ela pela via constitucional ou legal - não conseguiu evitar que o direito sofresse a influência de racionalidades estranhas a ele. A isto se denomina *fragmentação constitucional*, o que equivale dizer que o processo de acoplamento estrutural e político da sociedade não é mais um campo exclusivo das constituições e dos ordenamentos jurídicos por elas constituído, mas encontra-se disseminado por variados centros normativos organizados em vilas globais ou "the self-constitutionalization of global orders without state"[203].

Isso pode ser observado a partir das normas produzidas fora do contexto jurídico que concorrem com aquelas oriundas dos tribunais, com as referências estranhas ao direito em análises doutrinárias e as práticas comerciais privadas, como no caso dos requisitos do consentimento, da anonimização, o papel dos controladores, a delimitação do interesse legítimo e das transferências internacionais. Neste contexto, um dos principais questionamentos apresentados por Teubner envolve a forma como o constitucionalismo apresentará respostas à digitalização, à privatização das relações e à globalização:

> "How is constitutional theory to respond to the challenge arising from the three current major trends - digitalisation, privatisation and globalisation - for the inclusion/exclusion problem? This is how today's 'constitutional question' ought to be formulated, in constrast to the 18th and 19th century question of the constitution of nation-states. While that had to do with disciplining repressive political power by law, the point today is to discpline quite different social dynamics. This is, in the first place, another question, for theory. Will constitutional theory manage to generalise its nation-state tradition in contemporary terms and re-specify it? Can we, then, make the tradition of the nation-state constitution fruitful, while, at the same time, changing it to let it do justice to the new phenomena of digitalisation, privatisation and globalisation[204]?"

---

[202] TEUBNER, Societal Constitutionalism, p. 4.

[203] Esclarece Teubner que "the comprehensive structural coupling of politics and law, observed by Luhmann in the constitutions of nation states, clearly has no equivalent at the level of world society". TEUBNER, **Constitutional fragments**, p. 52–53.

[204] TEUBNER, Societal Constitutionalism, p. 5.

A formalização normativa não deve ser considerada um escudo de proteção do direito que o torna infenso aos conflitos e à influência de elementos exógenos. Ainda que se questione acerca da capacidade dos subsistemas sociais do ciberespaço de manter o processo de auto-fundação e sustentação, sem um suporte político-constitucional, a universalidade do direito não pode evitar a concorrência imediata de outras universalidades como é o exemplo da *Lex Privacy* e sua policontextualidade fundada na *accountability*.

O processo de regulação segundo as diretrizes da policontextualidade deve considerar quando é possível aplicar as leis existentes, quando será necessário adaptá-las ou quando novas deverão ser elaboradas. Deve considerar, ainda, o modo de formulação razoável e proporcional da regulação, além de ter em mira que o processo legislativo deve resultar em normas flexíveis e facilmente adaptáveis às novas circunstâncias. Por fim, deve considerar os direitos fundamentais a despeito das pressões econômicas e tecnológicas, bem como coordenar com os demais países a construção de uma governança transnacional da internet em torno de leis e políticas públicas, de modo a proporcionar um ambiente virtual global mais seguro[205].

6.2 Aspectos da Lex Mercatoria como paradigma da Lex Privacy

Para melhor compreender a relação entre o modelo proposto por Teubner em torno da policontextualidade nas vilas globais, a *Lex Mercatoria* será utilizada como um instrumento de análise comparativa, assim como o foi para a *Lex Informatica* de Reidemberg, ainda que as suas características não se reflitam por completo para a caracterização da *lex privacy*. Seria ela um modelo de ordenamento jurídico independente ou se trata de um conjunto de normas sociais, usos e costumes, formadas à margem do Estado e por organizações com expressiva condição de poder? O que as demais experiências globais de produção espontânea do direito, especialmente as verificadas nas vilas globais do ciberespaço, tem a obter da experiência com a *Lex Mercatoria*[206]?

---

[205] SAMUELSON, Pamela, New Kind of Privacy - Regulating Uses of Personal Data in the Global Information Economy, A, **California Law Review**, v. 87, p. 0, 1999.

[206] TEUBNER, A Bukowina global sobre a emergência de um pluralismo jurídico transnacional, p. 15.

Ao longo de sua história, que remonta ao *merchant law* medieval, a *Lex Mercatoria*[207] tornou-se uma das mais exitosas formas de expressão de modelos jurídicos autônomos e racionais[208]. Baseada em práticas comerciais usuais do comércio internacional - contratos, costumes, códigos de conduta etc - , ela desempenha papel semelhante ao de normas elaboradas pelos Estados-nações, de modo que deles independe para atuar[209]. As corporações comerciais atuavam como verdadeiros Estados e as manifestações de poder impediam que as interações sociais ocorressem de forma paritária. Aquele que detivesse maior influência comercial, seja pela detenção de maior acesso a matérias-primas e produtos, detinha melhores condições de se impor sobre os demais.

Fenômeno semelhante ocorre no ciberespaço, no qual grandes corporações detentoras de expressiva quantidade e qualidade de dados pessoais conseguem centralizar o papel regulatório por meio de estruturas digitais normativas, para as quais estabelecem regras próprias sem a necessária transparência e responsividade. Embora partam de um ponto comum, ou seja, praticas regulatórias além da atuação estatal, *Lex Mercatoria* e *Lex Privacy* se diferem em substância. Enquanto uma é fruto da consolidação da expressão de poder econômico dos mercadores[210], a outra é uma tentativa de resposta, por meio da *accountability* e policontextualidade, às incessantes manifestações de poder que surgem à margem da atuação regulatória estatal. Embora a *Lex Privacy* não nos remeta a uma autorregulação pura, tal como a *Lex Mercatoria* - em que os mercadores "legislavam" em benefício dos próprios interesses[211] -, ela também surge como um fenômeno regulatório espontâneo, dinâmico e formado por redes de comunicação, porém como contraponto à dominação de agentes de mercado.

Os críticos da *Lex Mercatoria* são muitos e seus argumentos em geral vinculados à unidade do direito, soberania e particularidade do *enforcement* privado, na medida em que os mercadores desenvolveram seus próprios mecanismos para assegurar a prevalência dos seus interesses[212]. Argumentam que seria impensável eliminar as referências

---

[207] GALGANO, The new lex mercatoria.

[208] STONE SWEET, Alec, The new Lex Mercatoria and transnational governance, **Journal of European Public Policy**, v. 13, n. 5, p. 627–646, 2006; JUENGER, The lex mercatoria and private international law.

[209] MUSTILL, The new lex mercatoria; TEUBNER, Breaking frames.

[210] GALGANO, The new lex mercatoria.

[211] *Ibid*.

[212] *Ibid*.

territoriais para se admitir um direito *a-nacional*, de modo que todo e qualquer fenômeno jurídico deveria radicar em ordenamentos jurídicos nacionais, ou seja, ter um ponto de conexão mínimo com o direito nacional, tal como se evidencia no modelo da corregulação de dados pessoais, que indica essa conexão entre atuação privada e direito nacional. Mas para esses autores, por não dispor de um território definido no qual possa exercer o monopólio do uso da força, a *Lex Mercatoria* não teria a capacidade de criar e virar direito[213], o que não parece não ser correto na medida em que as corporações comerciais tinham as suas delimitações territoriais de dominação e imposição de regras.

A circunstância de a *Lex Mercatoria* desconhecer sanções jurídicas mandatórias nos estritos moldes daquelas impostas pelo Estado sempre foi um dos pontos sensíveis de sustentação de sua condição de fonte do direito, no entanto o essencial para a análise ora realizada é apenas entender que os mercadores tinham mecanismos próprios de incentivo e desestímulo comercial, sanções em outro formato e um discurso jurídico concreto capaz de comunicar a sua pretensão de vigência. Nesse sentido, se um discurso especializado também reclama vigência nas vilas globais do ciberespaço exatamente por melhor refletir aquela realidade, pouco relevo apresenta a circunstância de base em torno da eficácia e legitimidade simbólica ou não das sanções, sejam elas advindas de instituições globais, nacionais ou regionais. A rigor, o fato a ser considerado é a manifestação de capacidade regulatória dominante para além dos Estados-nação e a análise de quão nefastas podem ser as suas consequências se não combinadas com mecanismos de intervenção estatal.

O tom da crítica, portanto, ignora um dos contrapontos mais interessantes acerca da força normativa da *Lex Mercatoria*, isto é, a capacidade de disposições de índole jusprivatistas produzirem normas cogentes sem a imprescindível intervenção estatal[214]. Tampouco consegue fragilizar a tese o fato de que a *Lex Mercatoria* é aplicável até entre os Estados-nações. A concepção de uma teoria pluralista de produção de normas, engendrada em torno da tecnologia e da ciência, que admita a influência de processos políticos, econômicos e sociais de forma equânime na formatação da *Lex Privacy* fatalmente atuará em favor do acoplamento estrutural do direito nas vilas globais[215]. Em outas palavras, até mesmo a regulação estatal ganhará com o processo de agregação de outros atores numa perspectiva

---

[213] TEUBNER, A Bukowina global sobre a emergência de um pluralismo jurídico transnacional, p. 16.

[214] *Ibid*.

[215] *Ibid*., p. 18.

mais próxima da corregulação, os quais certamente contribuirão para dar conformação a uma perspectiva mais ampla de ordenamento jurídico.

Mas qual seria a natureza da *Lex Mercatoria* e, por conseguinte, da *Lex Privacy* diante de um modelo de predominância regulatória estatal? Por que o sistema jurídico em torno da proteção de dados pessoais e da tecnologia seria mais propenso às influências de um modelo regulatório policontextual?

Teubner indica que a razão seria a de um "discurso jurídico auto-reprodutor de dimensões globais que cerra as suas fronteiras mediante recurso ao código binário 'direito/não-direito' (recht/unrecht) e reproduz a si mesmo mediante o processamento de um símbolo de vigência global (não nacional)'"[216]. Em resumo, um direito no seu contexto, em que mais importantes do que as normas legisladas são os eventos comunicativos e as estruturas jurídicas que constituem o pluralismo e seus mecanismos de controle social[217].

Além de produzir expectativas, garantir direitos e formatar comportamentos, os diversos sistemas de pluralismo jurídico excluem convenções sociais e normas morais não fundamentadas no código direito/não direito. Isto significa que a teoria do pluralismo jurídico está focada na identificação de fenômenos jurídicos autônomos no plano global, desvinculados do discurso legitimador do direito estatal[218]. Mas a pergunta de ouro feita por Teubner é "como admitir que, sem a existência de um sistema político global ou de instituições globais, um discurso jurídico fundado na codificação binária e com pretensão de validade global se estabeleça sem fundamentação e coerção em um direito nacional[219]?" A resposta está na validação estatal e nos incentivos das práticas interpessoais como códigos de programação, contratos, certificações, selos, normas corporativas vinculantes elaborados pelos agentes privados, mas sujeitos à aprovação estatal.

O desenvolvimento da *Lex Privacy*, assim como ocorreu com a *Lex Mercatoria*, também se deu em boa medida no âmbito da práxis contratual e da interação privada, a qual não conhece fronteiras físicas e transforma a produção normativa em fenômeno global mediante operações transnacionais. Este processo desencadeia a

---

[216] *Ibid*., p. 19.

[217] *Ibid*., p. 22.

[218] *Ibid*., p. 21.

[219] *Ibid*.

emancipação da *Lex Privacy* das suas raízes exclusivamente no direito nacional de um único país. Entretanto, como poderia a *Lex Privacy* escapar do axioma consistente na ausência de vinculação a pelo menos um ordenamento jurídico? Novamente, mediante um de regime de validação estatal e incentivos das práticas interpessoais. Teubner responde que, diante de uma *Lex Mercatoria* sem fundamento em um ordenamento jurídico, os sociólogos do direito sustentaram que seria uma redução ao absurdo aceitar que os contratos se autocolocassem em vigor, numa clara demonstração de redução ao absurdo.

Vale salientar, contudo, que a práxis realmente contempla um espectro mais rico do que aquele oferecido pela dogmática jurídica, pois ela fez com que os contratos internacionais camuflassem o paradoxo da exclusiva atuação estatal, mediante o surgimento de novos arranjos contratuais, como se viu com o *Safe Harbor* e mais recentemente com o *Privacy Shield*[220] ou com outros fenômenos relacionados à linguagem de programação (criptografia, hasherização, anonimização).

Trata-se, deste modo, de uma verdadeira criação de ordenamentos jurídicos privados com pretensão de validade universal, conforme se verifica na dualidade entre o poder regulatório exercido por plataformas digitais normativas como Google, Mercado Livre e Amazon, em contraste com aquela exercida pelo Estado[221]. O desenvolvimento do tema sobre plataformas digitais normativas será um dos pilares da tese em torno do poder de regulação privado capaz de sustentar a *Lex Privacy* e será feito no capítulo 4.

No panorama da policontextualidade, basta observar que os contratos "temporalizam o paradoxo e transformam a sua circularidade de autoavaliação em um processo contínuo de propagação de atos jurídicos"[222], uma sequência voltada à constituição recorrente e recíproca da formação de atos e de estruturas jurídicas. A operação de retroalimentação atua mediante um componente retrospectivo e outro prospectivo, os quais

---

[220] EUROPEAN COMMISSION, **Reform of the data protection legal framework in the EU**, disponível em: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>, acesso em: 18 dez. 2015.

[221] Um exemplo relevante do poder de regulação das plataformas digitais normativas é o do Mercado Livre. A plataforma foi premiada pelo Conselho Nacional de Justiça, a principal instituição de administração judiciária do país, pelos expressivos resultados de conciliação e mediação de litígios realizados entre usuários. Por mais que o propósito primordial da empresa não seja conciliar litígios, a garantia de direitos a seus usuários de forma célere e efetiva conferiu à plataforma primazia sobre a atuação estatal. CONSELHO NACIONAL DE JUSTIÇA, **CNJ premia Mercado Livre por conciliar conflitos antes do processo judicial**, disponível em: <http://www.cnj.jus.br/noticias/cnj/84490-cnj-premia-mercado-livre-por-conciliar-conflitos-antes-do-processo-judicial>, acesso em: 9 fev. 2019.

[222] TEUBNER, A Bukowina global sobre a emergência de um pluralismo jurídico transnacional, p. 22.

remetem a um conjunto de normas já existentes e a outro destinado à solução de conflitos futuros, contínuos e permanentes, alimentados por uma rede de comunicação.

O paradoxo construído em torno da auto-referência do contrato e das plataformas digitais normativas, enquanto substrato da *Lex Privacy*, se utiliza da técnica de dissolução mediante externalização da autovalidação, como as políticas de proteção de dados de corporações transnacionais.

Nenhuma contradição existiria, portanto, em transformar uma relação interna circular em relação externa, segundo mecanismos reflexivos e constituintes da base do sistema jurídico autônomo. Desde o princípio, a ideia de Teubner ao recorrer ao direito vivo da Bukowina era demonstrar como determinados sistemas de comunicação social são capazes de seguir uma lógica própria de funcionamento, a partir de símbolos de validade referenciados não no direito nacional, mas em parâmetros globais[223], tal como ocorre com a *Lex Privacy* e seus subsistemas autônomos de proteção de dados.

A grande vantagem do mecanismo de externalização reflexiva reside exatamente na dinamicidade interativa entre as versões oficiais e não-oficiais do direito global, algo muito característico no atual cenário mundial sobre proteção de dados pessoais, cujo principal exemplo pode ser representado pela *CBPR-Cross Border Privacy Rules* do bloco *APEC-Asia-Pacific Economic Cooperation*[224], um conjunto de regras estabelecidas em acordo de cooperação para regular o fluxo transnacional de dados entre os países membros, sujeito à validação por órgãos certificadores privados. Este processo "introduz uma diferenciação interna entre produção jurídica organizada e espontânea que produz o equivalente funcional da separação do direito contratual-judicial e do ordenamento contratual com autonomia privada"[225].

Embora exista uma relativa influência de usos e costumes no fenômeno das vilas globais, Teubner afirma de forma categórica que se trata de decisões de instituição impositiva e positiva do direito por meio da legislação privada, da jurisprudência e dos contratos[226]. Mas a constatação da existência de um direito global não significa uma

---

[223] *Ibid*.

[224] A análise e conceituação do tema será feita no cap. 2.

[225] *Ibid*., p. 23.

[226] *Ibid*.

autorização para a criação de um novo direito nacional, em desalinho com o vigente no âmbito de fronteiras territoriais definidas[227].

O pluralismo jurídico global ora analisado não tem raízes na delegação de poder estatal, mas em duas importantes premissas: a teoria das fontes e a legitimidade do direito. No atual contexto das vilas globais, os ordenamentos jurídicos nacionais não são os únicos capazes de conferir fundamento de validade a fluxos transacionais globais e interações como os pertinentes à proteção de dados e regulação de tecnologias. Isto força o reconhecimento de que os arranjos contratuais privados também sejam considerados fontes do direito não menos relevantes do que o direito legislado.

No tocante à legitimidade, as regras de reconhecimento não devem ser produzidas de modo hetero-referencial por ordenamentos jurídicos independentes e públicos para somente em seguida serem transpostas para o ambiente contratual privado. O que se tem aqui, em resumo, é uma clara condição de autolegitimação das relações jurídicas segundo o substrato em que consumadas, ou seja, uma permanente interação conforme posteriormente se verificará no modelo da corregulação, analisado no próximo capítulo. Não se trata, portanto, de realizar uma análise comparativa e qualitativa do grau de normatividade entre figuras como a *lex privacy* e os ordenamentos jurídicos nacionais, tal como se aquelas fossem subclassificadas no plano global em relação a estes.

Assim como ocorre com a *lex mercatoria*, a *lex privacy* será o instrumento responsável pelo acoplamento estrutural do sistema de proteção de dados e regulação de tecnologias, que alcança a sua autonomia na exata expansão e emancipação das relações globais. O ponto fraco da *lex privacy* decorre da influência dos interesses e das manifestações de desigualdade do poder econômico de grandes corporações, que serão verificadas quando da análise das plataformas digitais normativas e o papel da *accountability.*

Em boa medida, a evolução interna deste modelo depende da evolução externa do sistema econômico e da concatenação de episódios no plano global realizados por regimes de *private governments*, ou seja, por toda uma rede ampla e ramificada de organizações privadas e até públicas[228]. Em vez de normas jusprivatísticas de conteúdo normativo concreto, a *lex privacy* se assemelha ao regime de *soft law*, com uma série de preceitos abertos,

---

[227] *Ibid*., p. 24.

[228] *Ibid*., p. 25.

princípios e conceitos indeterminados, cuja aplicação se altera de acordo com a essência e policontextualidade do problema.

Embora tais aspectos lhe rendam críticas quando em comparação com os ordenamentos jurídicos nacionais, o essencial é ter em mira que a *lex privacy* constitui um corpo complexo de regras conjugadas, sem referência com o processo regulatório de comunicação tradicional, que funciona na base do código jurídico binário direito/não-direito. A flexibilidade e dinamicidade são marcas positivas do seu padrão normativo, que não se coaduna com a codificação de um direito global, porquanto atua mediante um regime de valores e de princípios ao invés de formas e de estruturas inflexíveis.

Não se trata de um papel menor em termos qualitativos, mas uma característica capaz de fomentar a maleabilidade e a adaptação necessárias aos cenários em contínua transformação. E tão logo os arranjos contratuais e as plataformas digitais, enquanto principais instrumentos de atuação e consolidação do modelo normativo da *lex privacy*, contribuam para que ela promova o acoplamento estrutural do direito global entre fatores sociais, tecnológicos e econômicos, a política realizará a sua missão de reordenação das forças dos ordenamentos dos Estados-nações.

Em resumo, nesse capítulo se buscou uma análise dos contornos da regulação do ciberespaço para que atuassem como ponto de partida da regulação específica da proteção de dados pessoais e privacidade, a ser analisada no próximo capítulo. Como forma de estabelecer um diálogo entre modelos, Teubner foi apresentado como o marco teórico que auxiliará na contraposição entre a regulação do ciberespaço e sua influência sobre os modelos regulatórios concretos de proteção de dados pessoais.

A policontextualidade e seus desdobramentos nas vilas globais, com o surgimento de fontes autônomas do direito vivo em torno de redes de comunicação privadas, foram os principais elementos de Teubner trabalhados neste capítulo, dada a relevância teórica e filosófica para o referencial de *Lex Privacy* que se adotará nesta tese.

No capítulo a seguir, o consentimento e as transferências internacionais de dados serão utilizados como elemento de estudo das variadas formas de expressão da regulação estatal, auto-regulação e corregulação para que se possa observar a forma de interação entre agentes públicos e privados. O recorte em torno do consentimento e das transferências se justifica na medida em que são os principais fatores de interação entre os

principais *stakeholders* do fenômeno regulatório, permitindo uma análise sob os mais variados matizes e perspectivas

CAPÍTULO 2 – DO CIBERESPAÇO À PROTEÇÃO DE DADOS PESSOAIS: AS FACETAS DA REGULAÇÃO EM CONCRETO

1. A delimitação e o sentido da regulação da proteção de dados pessoais

Neste capítulo analisaremos o implemento da agenda regulatória sobre as novas formas de tecnologia na sociedade da informação e a recontextualização do direito à privacidade e proteção de dados, como forma de assegurar a tutela de direitos contra os processos hegemônicos de concentração de poder nas vilas globais. Para viabilizar a compreensão do tema, elegeu-se o consentimento e as transferências internacionais de dados, visto que constituem elementos de permanente intersecção entre atores públicos e privados, com maior ou menor densidade, a depender do modelo regulatório analisado. Após se examinar os modelos amplos de regulação do ciberespaço, é importante compreender em que medida transpuseram parte da sua influência para os processos regulatórios da privacidade e proteção dos dados pessoais.

A narrativa que teve início no capítulo anterior mostra que o paradoxo da modernidade tem indicado um suposto dualismo entre inovação tecnológica e regulação[229]. Em boa medida, parte do dualismo se deve à percepção de que a modernidade tem imposto um *trade-off* entre fomentar a inovação tecnológica, resguardar o direito à privacidade e impor um formato de regulação restritiva[230], como se necessariamente se excluíssem.

Tal como indicado por Teubner no capítulo anterior, a globalização não é um fenômeno essencialmente jurídico, embora tenha relevantes repercussões legais.[231] Por essa razão, Benoit Frydman destaca que a globalização é o reflexo de uma nova fase do capitalismo e da economia de mercado, na qual grupos econômicos conduzem diretamente

---

[229] BENOLIEL, Daniel, Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology, **California Law Review**, v. 92, p. 0, 2004; BENKLER, Yochai, Net Regulation: Taking Stock and Looking Backward, **U. Colo. L. Rev.**, v. 71, p. 1203, 2000; GUTWIRTH, Serge; DE HERT, Paul, Regulating profiling in a democratic constitutional state, *in*: **Profiling the European citizen**, London: Springer, 2008, p. 271–302.

[230] CASTELLS, Manuel, **A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade**, Rio de Janeiro: Zahar, 2003, p. 144–145.Castells, Galaxia, pp. 144-145

[231] Pierre Levy chega a questionar se poderemos falar em comunidades virtuais no mesmo modelo da cidade.LÉVY, **Cibercultura**, p. 193.

suas estratégias de negócios numa rede mundial[232], muitas vezes imbuídos da tentativa de escapar ao intento dos reguladores. A globalização tem acarretado o crescimento e o aumento da velocidade das relações internacionais não apenas na economia, mas essencialmente nos meios de comunicação e conexões interpessoais. Algumas dessas formas de relação requerem algum tipo de regulação, o que outrora seria naturalmente realizado pela lei enquanto expressão do Estado de Direito,[233] porém cada mais se ramificado em redes privadas dotadas de significativa autonomia e expressão de poder.

Tradicionalmente, os Estados eram os principais atores no processo de construção, implementação e aplicação das leis, ou seja, os Estados conduziam todo o processo regulatório. Para desempenhar essas atividades, os Estados nacionais desenvolveram instituições sofisticadas e suficientemente capazes de implementar as leis por meio da força.[234] Como premissa geral, não existia lei fora das fronteiras soberanas de um Estado. Por essa razão, o principal desafio imposto pela globalização envolve a definição dos instrumentos regulatórios em um ambiente exponencialmente em transformação.[235]

Em relação à privacidade e proteção dos dados pessoais não foi diferente. A globalização foi capaz de criar um cenário de transações instantâneas em âmbito global, por meio das quais uma expressiva quantidade de dados é transferida sem a plena consciência, conhecimento e consentimento dos usuários da rede.

Para fins de delimitação conceitual da ideia de regulação empregada nesta tese, vale observar que a utilizamos em sentido amplo, não se limitando ao papel desempenhado pelo Estado, em especial porque se tem constatado novas formas de regulação decorrentes da multiplicação de redes e atores não-estatais responsáveis pela sua execução.[236] Neste sentido, considera-se regulação pela perspectiva da proteção de dados pessoais todas as variedades de

---

[232] FRYDMAN, Benoît; DE SCHUTTER, B.; PAS, J., Coregulation: a possible model for global governance, **About globalisation: views on the trajectory of mondialisation**, p. 227–242, 2004, p. 227.

[233] BENKLER, **The wealth of networks: How social production transforms markets and freedom**; HILDEBRANDT, Mireille, Legal and technological normativity: more (and less) than twin sisters, **Techné: research in philosophy and Technology**, v. 12, n. 3, p. 169–183, 2008.

[234] BYGRAVE, Lee A., The Future of Privacy Law, **European Data Protection Law Review**, v. 2, 2016.

[235] HILDEBRANDT, Legal and technological normativity: more (and less) than twin sisters.

[236] BALDWIN; CAVE; LODGE, **The Oxford handbook of regulation**, p. 80; BENNETT, **The Governance of Privacy**, p. 118–119.

instrumentos que visam controlar o processamento de dados e suas consequências.[237] A rigor, regulação não envolve apenas o controle estatal e observância a preceitos legais, mas sim outras ferramentas capazes de regular comportamentos, restringir e otimizar ações, bem como definir diretrizes complementares para a execução de políticas públicas.[238]

2. Empoderamento e recontextualização enquanto objetivos do marco regulatório de proteção de dados

Por princípio, a regulação sob a perspectiva de proteção de dados pessoais deveria funcionar simultaneamente como um mecanismo capaz de resguardar direitos e facilitar atividades, além de empoderar indivíduos e nortear as condutas dos agentes de mercado. A exata combinação de ambos não tem sido uma atividade simples ora por conta do apego às premissas do mundo físico e dos anseios regulatórios que lhe são próprios, ora pela dificuldade inerente ao processo de regulação do novo e das suas formas variadas de expressão.

Neste panorama de busca pela harmonização das premissas de evolução da sociedade da informação, o consentimento se torna um elemento vital para o empoderamento e concretização de escolhas dos indivíduos sobre a maior ou menor disposição da privacidade e proteção de dados. No entanto, a cada dia o consentimento tem se tornado mais insuficiente ou tem sido fornecido em condições de desigualdade ou em circunstâncias alheias às manifestações de poder. Por essa razão, o consentimento tem deixado de ser a peça chave do controle sobre os dados pessoais e aberto espaço para outras ferramentas como a *accountability*. A rigor, quanto maior a percepção da ideia de propriedade vinculada aos dados pessoais, maior será o enfoque no consentimento. Por outro lado, quanto maior a percepção de que a privacidade e proteção de dados envolve um direito fundamental indisponível, menor o papel do consentimento.

Isso significa que, a depender dos parâmetros culturais e valores de uma determinada sociedade, os modelos regulatórios voltados a resguardar a proteção de dados e privacidade demandarão uma maior ou menor influência estatal para fazer um contraponto e promover o

---

[237] SOLOVE, Daniel J.; HOOFNAGLE, C. J., A Model Regime of Privacy Protection 2.0, **SSRN Electronic Journal**, 2015; MAYER-SCHÖNBERGER, Viktor, Virtual Heisenberg: The Limits of Virtual World Regulability, **Washington & Lee Law Review**, v. 66, 2009.

[238] BENNETT, **The Governance of Privacy**, p. 121.

reequilíbrio dessas relações não pautadas pelo consentimento, o que dará a exata dimensão da existência ou não de uma relação inversamente proporcional entre consentimento e *accountability*, a ser realizada no capítulo 4.

Neste capítulo se buscará a compreensão das premissas básicas dessa relação para se dimensionar a capacidade de plataformas digitais e de empresas de tecnologia em impor um regime de regulação próprio e cada vez mais distante da capacidade estatal de interferir em suas atividades. Para permitir uma análise mais pontual e com um recorte mais específico da agenda regulatória e da recontextualização do regime jurídico de proteção dos dados pessoais, utilizaremos como marco de análise as diferentes formas de regulação do consentimento e das transferências internacionais, segundo os principais modelos regulatórios existentes.

Por se tratar de um dos mais recentes e abrangentes marcos regulatórios em vigor, a análise do GDPR e outras normas correlatas poderá indicar as principais formas de manifestação da interação entre o modelo de regulação estatal, corregulação e auto-regulação, assim como suas capacidades de proporcionar formatos heterogêneos mais adaptáveis ao ciberespaço e capazes de se contrapor às manifestações de poder nas plataformas digitais normativas. Um dos casos analisados para se identificar esse processo será a legislação europeia de proteção de dados, a *General Data Protection Regulation-GDPR*, cujos efeitos extraterritoriais atingem todas as empresas que oferecem bens e serviços ou monitoram comportamentos de usuários residentes na União Europeia, independentemente de onde estejam localizadas. Indicativos claros desse novo traço da regulação foram as sanções aplicadas pelas autoridades francesa e inglesa de proteção de dados pessoais, com claros traços da natureza extraterritorial[239].

Em linhas gerais, diante de um modelo regulatório expansionista, torna-se ainda mais necessário compreender se outros países e autoridades de proteção de dados foram capazes de conferir tutela ao usuário a partir de outras concepções de consentimento e transferência internacional de dados. Para seguir este caminho, neste capítulo analisaremos os principais modelos regulatórios para então confrontá-los com o nível de proteção aos dados pessoais e privacidade, associado a maior ou menor participação do Estado.

[239] ICO, Aggregate IQ Data Services Ltd; CNIL, None Of Your Business and La Quadrature du Net vs. Google.

3. Modelos Regulatórios e suas principais características: como a agenda regulatória atua em favor do titular dos dados

No atual cenário sobre proteção de dados e privacidade, quatro principais modelos regulatórios podem ser identificados e agrupados para a melhor compreensão das suas particularidades, ainda que sua caracterização não seja simétrica e homogênea e comporte alguma espécie de sobreposição e confluência. Em grande medida, estes modelos se diferem pelo maior ou menor grau de participação do Estado e/ou órgãos reguladores, bem como em relação ao nível de receptividade da atuação regulatória conjunta atores privados.

A escolha do critério de aproximação decorreu da maior ou menor capacidade de influência estatal em conjunto com a existência de incentivos para atuação regulatória privada. Este recorte será relevante para indicar como o referencial teórico da policontextualidade de Teubner será contrastado em cada um deles e como contribuirá para a melhor tutela da privacidade e proteção dos dados pessoais nas vilas globais. Neste sentido, para fins de delimitar a premissa de trabalho e o problema desta tese, os principais modelos regulatórios foram agrupados em quatro categorias. Dentre esses modelos típicos do cenário de tecnologia da informação, destacamos os seguintes[240]:

a) Modelo Regulatório Estatal ou Compreensivo;

b) Modelo Regulatório Setorial;

c) Modelo de Corregulação;

d) Modelo de Autorregulação.

A conjugação das teorias do capítulo 1 sobre a regulação do ciberespaço permitirá que se dimensione como os modelos regulatórios ora analisados se comportam diante de duas hipóteses de pesquisa escolhidas: o consentimento e as transferências internacionais de dados. A escolha do consentimento e das transferências internacionais como hipóteses de análise se deve ao fato de que representam um ponto comum em todos os modelos a serem apresentados, além de conterem alguma forma de expressão da influência dos agentes de

[240] SWIRE, Peter P.; AHMAD, Kenesa, **US Private-sector Privacy: Law and Practice for Information Privacy Professionals**, [s.l.]: International Association of Privacy Professionals (IAPP), 2012; SWIRE, Peter P.; AHMAD, Kenesa; MCQUAY, Terry, **Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices**, [s.l.]: International Association of Privacy Professionals, 2012.

mercado e titulares dos dados, o que poderia melhor evidenciar o grau de participação deles. A verificação dessas duas hipóteses de pesquisa dará o substrato necessário para que se analise as manifestações de poder das plataformas digitais normativas e a forma de controle desempenhada pela *accountability.*

Para que seja possível entender a complexidade sobre a forma como o consentimento e as transferências internacionais podem se expressar nos mais diversos modelos, é importante examinar a realidade de países que se identificam com um ou outro modelo regulatório apontado anteriormente. Para esta análise específica, serão analisadas as características dos marcos regulatórios sobre proteção de dados pessoais da APEC, dos Estados Unidos com foco na FTC, da Austrália, do Canadá, da União Europeia e do Brasil. A escolha destes países se deve à dispersão da influência de seus modelos ou a relativa disparidade existente entre eles, que ao final serão relevantes para a conjugação dos elementos formadores da *Lex Privacy*. A análise desses modelos permitirá compreender como as experiências positivas de outros países, no tocante ao consentimento e transferência internacional de dados, podem indicar a existência de uma rede regulatória complexa, diversificada e capilarizada, que analisaremos no capítulo 4.

3.1 O modelo regulatório estatal ou compreensivo

O papel do Estado na regulação da privacidade sempre foi fruto de expressiva contestação. Sem uma definição clara se a regulação da proteção dos dados pessoais era voltada a proteger o titular ou assegurar meios que ampliassem o poder da vigilância, o fato é que o Estado foi aos poucos perdendo o posto de principal *stakeholder*. Apesar disso, o modelo Regulatório Estatal ou Compreensivo pode ser definido como aquele no qual são elaboradas normas gerais de proteção de dados, aplicáveis tanto ao setor público quanto privado e usuários, mediante a criação de um órgão governamental ou um órgão responsável pela fiscalização e imposição de sanções aos agentes que descumprem as referidas normas[241].

Trata-se de um modelo que segue o formato regulatório convencional, com a atuação estatal capitaneando todo o processo de conformação de condutas, implementação de políticas públicas e criação de incentivos, sem espaço para a influência de atores privados. Em linhas gerais, trata-se de um modelo que, conforme explicitado no primeiro capítulo, pouco se

[241] SWIRE; AHMAD; MCQUAY, **Foundations of Information Privacy and Data Protection**.

coaduna com a pluralidade de redes de comunicação e sem expressiva capacidade de reagir às escapadas regulatórias dos agentes de mercado[242].

Diante disso, nota-se que o modelo regulatório estatal se contrapõe às premissas da policontextualidade na medida em que nem sempre é aberto às manifestações do direito a partir das práticas sociais e das várias universalidades, o que revela a sua dificuldade de eleger um elemento responsável pelo acoplamento estrutural com subsistemas normativos privados. Sem a policontextualidade como força motriz do acoplamento, o modelo estatal perde a capacidade de compreender as diversas gramáticas simbólicas de linguagem que viabilizam uma análise mais profunda do conflito entre práticas sociais reais.

Em boa medida, este modelo é mais comum em países de tradição *civil law*, cuja atuação regulatória tem como pressuposto não restringir direitos senão em virtude de lei. No entanto, uma das formas encontradas por esse modelo para melhor conferir empoderamento aos indivíduos e ganhar em adaptabilidade foi utilizar o consentimento como substrato do processo de compartilhamento de dados e, a partir dele, tutelar a manifestação de vontade. Em outros termos, dada a dificuldade de implementação de uma agenda regulatória perene, suficientemente capaz de antecipar os conflitos reais em torno das práticas sociais, regular estruturas de direitos por meio de figuras como a manifestação da vontade pode representar uma forma eficiente de se atingir macro-objetivos regulatórios. Este será o eixo sobre o qual analisaremos na sequência a estrutura de modelos regulatórios de outros países.

3.2 O modelo Regulatório Setorial

O modelo Regulatório Setorial compreende um conjunto de normas editadas para segmentos específicos do setor privado e público, com a possibilidade de diversas agências e órgãos atuarem na fiscalização e imposição de sanções aos agentes que descumprem as referidas normas, a depender da natureza do setor da economia envolvido[243].

O modelo setorial tem a marca da especificidade, o que lhe confere maior poder de adequação às mais diversas realidades sem perder aderência e poder sancionador. O modelo setorial não deixa de também ter as principais características do modelo Regulatório Estatal,

---

[242] *Ibid*.

[243] *Ibid*.; USTARAN, Eduardo, European privacy: law and practice for data protection professionals, **Portsmouth, NH: International Association of Privacy Professionals (IAPP)**, 2012.

embora em alguns setores regulados assegure espaço para a elaboração de códigos de conduta, certificações e outros mecanismos de autorregulação. Essa fragmentariedade do modelo Setorial em alguma medida dialoga com a policontextualidade e as manifestações do direito em vilas globais defendida por Teubner, pois aponta para uma capacidade normativa mais adequada às práticas reais de determinados subsistemas sociais.

Conquanto se presuma que este modelo seja mais adequado para as especificidades setoriais da indústria da tecnologia, em verdade se trata de um modelo com pouca capacidade de interlocução com os diversos segmentos da sociedade, o que significa menor potencialidade de adesão por outros setores regulados, disformidade de regimes e assimetria cultural em torno dos verdadeiros ganhos de um marco regulatório claro e preciso. Em resumo, um modelo tão despido da policontextualidade – ainda que por outros fundamentos – quanto o modelo estatal ou compreensivo, sobretudo porque o modelo Regulatório Setorial perde em capacidade de se tornar exponencial e dispersar padrões de condutas de forma indistinta em outros setores da sociedade, mediante gramáticas simbólicas comuns.

3.3 A Corregulação

O modelo de Corregulação é aquele no qual o Estado atua mediante a elaboração de normas e diretrizes gerais que asseguram uma margem de atuação e complementação por entes privados dos diversos setores da economia. Este é um formato de regulação com claros indicativos da capacidade de assegurar a harmonização entre inovação tecnológica e proteção de dados. Neste modelo há o desenvolvimento de códigos de conduta, normas corporativas (*BCRs-Binding Corporate Rules*)[244] ou padrões de proteção da privacidade que são posteriormente validados por órgãos governamentais para posterior aplicação[245].

A rigor, a corregulação é o modelo mais próximo das premissas adotadas nessa tese como base para a *Lex Privacy.* A corregulação é o modelo que de forma mais consistente

---

[244] O tema é tratado nos arts. 44 a 49 do GDPR e pelas opiniões do Working Party 29. EUROPEAN COMMISSION, **Transatlantic Data Flows: Restoring Trust through Strong Safeguards**, Bruxelas: European Commission, 2016; EUROPEAN COMMISSION, **Adequacy of the protection of personal data in non-EU countries**, disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>, acesso em: 9 fev. 2019; WORKING PARTY 29, **Opinion 3/2010 on the principle of accountability**, Bruxelas: WP29, 2010.

[245] SWIRE; AHMAD; MCQUAY, **Foundations of Information Privacy and Data Protection**.

consegue promover um acoplamento estrutural entre Política e Direito, por meio de processos capazes de valorizar a experiência do direito vivo na construção de novas estruturas regulatórias. A corregulação consegue congregar os sistemas parciais individuais da sociedade que surgem em velocidades distintas nas vilas globais, além de impulsionar a autonomia em face das pretensões hegemônicas da política e do mercado.

Trata-se, de fato, de uma experiência positiva que, em relação ao cenário de proteção de dados, pode ser identificada em boa medida na Diretiva 95/46/CE, posteriormente substituída pela GDPR, cujas evidências tem indicado um papel bem mais efetivo no processo regulatório, na medida em que ao poder público apenas se atribui a função de tutelar direitos e impor sanções a partir de um referencial regulatório comum e conhecido nos Estados de Direito. Um dos diferenciais desse modelo em relação ao Regulatório Estatal decorre do fato de que, também como destinatário da regulação, a atividade do poder público é objeto da disciplina das normas gerais e a iniciativa privada tem alguns espaços de atuação assegurados por lei.

Nos Estados Unidos, embora o regime da autorregulação tenha um espaço maior, a corregulação tem sido desempenhada de forma impactante e com resultados expressivos por parte da Federal Trade Commission (FTC), que será analisada em seguida em virtude das suas características. A corregulação será identificada em boa parte dos modelos regulatórios analisados a seguir, o que demonstrará a clara tendência de vários países em adotá-la e da maior influência sobre a *Lex Privacy*.

3.4 A Autorregulação

A Autorregulação é o modelo no qual as empresas ou um conjunto de empresas elaboram regras próprias para disciplinar suas atividades por meio de códigos de conduta, selos, políticas, padrões tecnológicos e arranjos contratuais, dotados de flexibilidade e capazes de facilmente se adaptarem à evolução tecnológica[246]. Esses instrumentos costumam ser utilizados como forma de se antecipar à regulação ou até mesmo evitá-la[247]. A autorregulação

[246] BLACK, Julia, Constitutionalising self-regulation, **The Modern Law Review**, v. 59, n. 1, .

[247] CANNATACI, Joseph A.; BONNICI, Jeanne Pia Mifsud, Can self-regulation satisfy the transnational requisite of successful Internet regulation?, **International Review of Law, Computers & Technology**, v. 17, n. 1, p. 51–61, 2003; NETANEL, Neil Weinstock, Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory, **California Law Review**, v. 88, p. 395, 2000.

é o extremo oposto do modelo regulatório estatal, de sorte que as críticas a ele feitas aqui se aplicam com a mesma dimensão, em especial porque somente é capaz de compreender parte dos subsistemas sociais. Além de invariavelmente não contribuir para um panorama de valorização da policontextualidade, na medida em que ignora a produção do direito estatal, a autorregulação perde em legitimidade e densidade normativa por se enclausurar nas vilas globais e não ser capaz de também dialogar com o subsistema estatal.

O êxito dos instrumentos de autorregulação é imprevisível e bastante variável a depender do setor, país e condições de implementação. A rigor, dependem de um conjunto de fatores políticos, organizacionais, culturais, tecnológicos e econômicos, o que não necessariamente indica se tratar de um modelo de pluralismo jurídico, tal como sustentado nessa tese. Sem a presença de um arcabouço regulatório com capacidade de impor sanções e assegurar o efetivo equilíbrio entre tutela dos dados pessoais e fomento à inovação, a autorregulação padece de constante desconfiança.

Acredita-se que, enquanto os instrumentos de autorregulação forem capazes de proporcionar ganhos de oportunidade apenas para os seus regulados, certamente continuarão a ser defendidos como mais efetivos do que outros formatos de regulação, em especial para proteção de dados pessoais.[248] Se de um lado o papel exercido pela autorregulação pode em muitos casos tanto otimizar quanto retrair os benefícios dos indivíduos e o bem-estar comum, por outro lado na economia digital os indivíduos tem uma capacidade reduzida de tomar decisões e expressar o consentimento em função da assimetria informacional sobre os seus dados pessoais processados, a finalidade e as consequências.

O modelo de Autorregulação contribui muito pouco para corrigir essas assimetrias, manifestações de poder e remediar o processo decisório, notadamente o exercido pelas plataformas digitais normativas.[249] São alguns desses elementos que fazem com que a Autorregulação da indústria da tecnologia, no tocante à proteção de dados pessoais, tenha expressiva resistência tanto por parte dos cidadãos quanto dos órgãos estatais.

---

[248] ACQUISTI, Alessandro; TAYLOR, Curtis R.; WAGMAN, Liad, The economics of privacy, 2016, p. 40.

[249] Um exemplo deste modelo é o Payment Card Industry Data Security Standard ("PCI DSS"), conjunto de regras técnicas e operacionais estabelecidas por uma organização formada por entidades do setor financeiro. Cf. **Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards**, disponível em: <https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss>, acesso em: 3 mar. 2019.

3.5 Parâmetros gerais para a compreensão da regulação das transferências internacionais de dados pessoais:

3.5.1 O geographically-based e o organizationally based approach

Na medida em que a *Lex Privacy* é expressão da policontextualidade manifestada nas vilas globais, é relevante analisar o paradigma regulatório da territorialidade em contraposição às transferências internacionais de dados pessoais, que no ciberespaço despontam como a principal ferramenta de interlocução dos mais variados modelos regulatórios.

A despeito de o ciberespaço ignorar as fronteiras territoriais e as leis de proteção de dados serem cada vez mais dotadas de extraterritorialidade, dois modelos específicos destinados a regular as transferências se contrapõem, a despeito de existir alguma sobreposição entre eles: o *geographically-based* e *organizationally based.*[250] Ambos representam formas de indicar a maior ou menor atribuição de responsabilidade (*accountability*) ou a indicação de que a territorialidade constitui um fator relevante para a oferta de bens e serviços.

O *geographically-based approach* é responsável pela regulação da transferência internacional de dados pela perspectiva do país importador, o que requer a adoção de alguns requisitos mínimos de proteção jurídica e resultará numa eventual decisão de adequação (*adequacy standard*)[251]. Esse é o padrão adotado pela União Europeia e se tornou uma relevante ferramenta para influenciar outros países a adotar um arcabouço regulatório mais próximo ao seu, numa clara disputa comercial com Estados Unidos e o bloco APEC. Sob a égide do *adequacy standard*[252], a União Europeia tem exercido um controle relevante sobre o fluxo transnacional de dados para fora do bloco e constrangido países como Japão[253], com o qual tem relevante atividade comercial, a se adaptar ao seu regime.

---

250 KUNER, Christopher, **Transborder data flow regulation and data privacy law**, [s.l.]: Oxford University Press Oxford, 2013.

251 WORKING PARTY 29, **Opinion on Adequacy Referential**, Bruxelas: WP 29, 2018.

252 EUROPEAN COMMISSION, **ow the EU determines if a non-EU country has an adequate level of data protection**.

253 EUROPEAN COMMISSION, **International data flows: Commission launches the adoption of its adequacy decision on Japan**, disponível em: <http://europa.eu/rapid/press-release_IP-18-5433_en.htm>, acesso em: 9 fev. 2019.

Por outro lado, o *organizationally-based approach* está mais vinculado ao princípio da *accountability* e da responsabilidade dos agentes de tratamento pelas operações, que podem ocorrer mesmo sem o consentimento do titular dos dados. Esse regime transfere ao responsável pelo tratamento dos dados a responsabilidade pelas atividades e decisões, com a certeza de que as sanções serão mais rígidas caso sejam constatadas violações à lei. A rigor, aqui temos um regime com traços de corregulação, marcado por relevante espaço de confiança e responsabilidade entre agentes de mercado e poder público. Canadá, México e Colômbia são alguns exemplos de adoção desse parâmetro. A *accountability* será o principal fundamento de validade da *Lex Privacy* e atuará em complemento à insuficiência do consentimento.

Os principais requisitos para a transferência internacional de dados em países com marcos regulatórios já definidos tem sido a adequação da operação, a transparência, a responsividade (*accountability*), o consentimento e o uso legítimo (*fair use*). Entretanto, nada disso é um fenômeno exclusivamente europeu ou pós-GDPR. Países como Argentina[254] e Uruguai[255] tem sido promissores exemplos de um harmônico equilíbrio entre inovação tecnológica e proteção de direitos, por meio da *accountability* e da corregulação. Ainda que influenciada pelas decisões da União Europeia ns. 2001/497/CE e 2010/87/UE, bem como pelo princípio 8.º das Guidelines da OEA, a Argentina editou em novembro de 2016 a Disposición 60, que regulamenta o artigo 12 da Lei 25.326/2000 e o Decreto 1558/2001, na qual define o regime de transferência internacional de dados, bem como indica os países com um patamar adequado e condizente com os seus padrões.

A análise dos modelos de transferência internacional - *geographically-based* e *organizationally based* – indica que na economia dirigida por dados, as fronteiras entre as camadas lógica e física se tornam cada vez mais fluídas, de sorte que um dos principais

---

[254] Argentina – art. 12 da Ley N° 25.326/2000 e Decreto Reglamentario N° 1558/2001: Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no propocionen niveles de protección adecuados. **PROTECCION DE LOS DATOS**, disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/norma.htm>, acesso em: 18 fev. 2019.

[255] Uruguai – art. 23 – Se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia. Disponível em: http://agesic.gub.uy/innovaportal/file/302/1/Ley_N_18331.pdf, acesso em: 19.2.2019.

desafios regulatórios é definir com precisão os contornos da figura da imputabilidade[256] e da ubiquidade. Em outras palavras, quem seriam os responsáveis pela transferência e gestão dos seus dados pessoais em determinadas relações jurídicas: empresas ou cidadãos? Como o consentimento se posiciona na viabilização nesses processos?

3.5.2 A influência da ubiquidade e da imputação nas transferências em massa

Para se delimitar o macro cenário em torno das transferências internacionais de dados e o consentimento, o primeiro passo compreende a análise das premissas que autorizam essas atividades. A primeira delas envolve a inviabilidade de transmissão de dados *point-to-point* na economia global, tal como aponta Chris Kuner[257]. A massa de dados pessoais envolvidos numa singela operação como o embarque de passageiros num avião, contratos de *cloud computing*, investigações transnacionais e contratos de trabalho de empresas multinacionais revela a pertinência empírica do desafio regulatório.

A segunda premissa diz respeito à ubiquidade da transferência internacional de dados e a mudança do papel da territorialidade. Como saber por onde transitam os dados pessoais pelas vilas globais? Não é possível assegurar em algumas situações, em razão das malhas de infraestrutura física e lógica, que a simples transferência de dados de pacientes para uma pesquisa experimental de laboratório acarrete necessariamente o trânsito transnacional. E se tal elemento não pode ser definido com precisão empírica, mas apenas técnica, como definir o regime jurídico de proteção dessas transferências internacionais de dados? Embora possa parecer incongruente indicar a perda de relevância da territorialidade em alguns aspectos e simultaneamente enaltecer a ubiquidade em outros, este exemplo demonstra que, a cada dia mais, a intersecção entre camada física e lógica será vital para o processo regulatório da proteção de dados pessoais.[258]

A terceira premissa compreende a figura da imputação, anteriormente indicada. No contexto regulatório do regime de proteção de dados pessoais, o crescente envolvimento dos usuários, o consentimento e os novos papéis de protagonismo por eles desenvolvidos tem

---

[256] KUNER, Christopher, Extraterritoriality and regulation of international data transfers in EU data protection law., **International Data Privacy Law**, v. 5, n. 4, 2015.

[257] KUNER, **Transborder data flow regulation and data privacy law**. Cf. também KUNER, Regulation of transborder data flows under data protection and privacy law: past, present and future. OECD Digital Economy Papers, n. 187, OECD Publishing, 2011. Disponível em http://dx.doi.org/10.1787/5kg0s2fk315f-en, acesso em 18.2.2019.

[258] BENKLER, **The wealth of networks: How social production transforms markets and freedom**.

gerado dificuldades na reconstrução da cadeia de gerenciamento de dados em operações transnacionais, a revelar que a policontexualidade é um dos traços marcantes desse processo. Este é, por exemplo, um dos desafios dos órgãos de fiscalização e regulação para fins de definição dos responsáveis pelo dever de notificação dos usuários de mudanças de padrões de tratamento de dados, incidentes de segurança e compartilhamento com terceiros.[259]

Todos estes aspectos, no entanto, se encontram diante de uma mesma encruzilhada: o modelo regulatório de proteção de dados pessoais e sua capacidade de estabelecer redes de comunicações plurais próprias às realidades práticas dos subsistemas sociais das vilas globais. É com esse objetivo que a seguir serão analisados os modelos regulatórios de proteção de dados pessoais acerca do consentimento e transferências internacionais, com enfoque especial na disparidade existente entre eles e na capacidade de contribuírem para o processo de formação da *Lex Privacy.*

4. O papel regulatório da FTC

4.1 Private Enforcement e o papel do consent decree

O primeiro modelo regulatório a ser examinado será o americano, com particular enfoque na Federal Trade Commission (FTC), a agência governamental dos Estados Unidos responsável pela defesa da concorrência, defesa do consumidor e crianças. A FTC tem se destacado por uma medida que combina características dos modelos de autorregulação e corregulação: *o private enforcement,* conforme indicado anteriormente[260]. Por meio da Section 5 do FTC Act,[261] a FTC tem implementado com êxito medidas de *private*

---

[259] JONAS, Hans, **O princípio responsabilidade: ensaio de uma ética para a civilização tecnológica**, [s.l.]: Contraponto, 2006, p. 204–205.

[260] SWIRE; AHMAD, **US Private-sector Privacy**.

[261] "Under Section 5(b) of the FTC Act, the Commission may challenge "unfair or deceptive act[s] or practice[s]" (or violations of other consumer protection statutes) through maintenance of an administrative adjudication. When there is "**reason to believe**" that a law violation has occurred, the Commission may issue a complaint setting forth its charges. If the respondent elects to settle the charges, it may sign a consent agreement (without admitting liability), consent to entry of a final order, and waive all right to judicial review. If the Commission accepts such a proposed consent agreement, it places the order on the record for thirty days of public comment (or for such other period as the Commission may specify) before determining whether to make the order final." Cf. **A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority**, Federal Trade Commission, disponível em: <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>, acesso em: 1 mar. 2019.

enforcement a partir do *consent decree*,[262] que podem ser traduzidas na imposição de sanções decorrentes do descumprimento de códigos de conduta, códigos de ética e políticas de privacidade formulados pelas pelas empresas[263]. Em outros termos, no modelo da FTC tem-se a imposição de sanção pelo Estado em virtude do descumprimento de normas formuladas pelas próprias empresas e em relação às quais se obrigaram a cumprir perante o órgão regulador. Trata-se, portanto, de uma das mais ricas manifestações de interação entre subsistemas, com uma clara confluência entre *enforcement* estatal de um lado e poder regulador privado de outro, a revelar que é possível a construção de um modelo híbrido e efetivo de tutela da privacidade e proteção dos dados pessoais.

Como parâmetro de atuação híbrida e capacidade de interlocução entre atores públicos e privados, a FTC tem imposto sanções a entidades que assumiram publicamente o compromisso de cumprir os seus próprios códigos de ética, políticas de privacidade e os programas de autorregulação que aderiram e, posteriormente, os descumpriram, sob a premissa de se tratar de uma promessa desleal *(unfair ou deceptive practices*). Este é certamente o traço distintivo que justifica a análise do modelo da FTC a respeito do consentimento e transferência internacional

4.1.1 O poder de influência da FTC na atuação privada

O poder de estabelecer um diálogo aberto entre atores públicos e privados é o traço distintivo da atuação da FTC, que em muito se aproxima da capacidade de antecipar as gramáticas simbólicas e entender a autonomia dos subsistemas parciais das vilas globais defendidos por Teubner. O FTC Act é a lei que rege a criação, organização e competência da FTC. A *Section 5* é o capítulo do FTC Act que determina as competências da FTC para regular e fiscalizar os casos de concorrência desleal ou descumprimento de regras de mercado, defesa do consumidor e proteção da privacidade.[264] Quanto à proteção de dados

---

[262] Como exemplo, vale citar o consent decree celebrado pela FCT com o Snapchat (https://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf) Cf. SWIRE; AHMAD, **US Private-sector Privacy**.

[263] ALLEN, Anita L., **Privacy law and society**, [s.l.]: West Group, 2007, p. 892–894.

[264] "whenever the Commission shall have reason to believe that any such person, partnership, or corporation has been or is using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce, and if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public, it shall issue and serve upon such person, partnership, or corporation a complaint stating its charges in that respect and containing a notice of a hearing upon a day and at a place therein fixed at least thirty days after the service of said complaint. Cf. FEDERAL TRADE COMMISSION, **Protecting Children's Privacy Under COPPA: A Survey on Compliance**.

pessoais e privacidade, a FTC elaborou um relatório (Relatório FTC) com diretrizes para empresas e titulares de dados (*Protecting Consumer Privacy in na Era of Rapid Change: Recommendations for Businesses and Policymakers*) e sua atuação se baseia em 3 (três) princípios centrais:

> (i) *Privacy by Design*, o qual estabelece que as entidades deveriam fomentar e implementar regras de privacidade por toda a organização e em cada estágio de desenvolvimento dos seus produtos e/ou serviços;
> (ii) *Simplified Consumer Choice*, o qual recomenda que as entidades deveriam simplificar e esclarecer as regras e práticas que tratam da solicitação de autorização dos titulares para a coleta ou uso de seus dados;
> (iii) *Transparency*, o qual determina que as entidades deveriam buscar informar o titular da forma mais transparente possível a respeito das regras e práticas de privacidade que são adotadas pela entidade, por meio do envio de avisos claros, padronizados e simples aos consumidores, pela garantia de acesso aos dados armazenados, bem como por meio da promoção de medidas educativas do consumidor[265].

O Relatório FTC tem o intuito de servir de guia de melhores práticas para determinadas entidades que coletam e utilizam dados de consumidores nos Estados Unidos, na medida em que recomenda procedimentos específicos que podem ser adotados pelas entidades para o tratamento de informações, com vistas a assegurar a privacidade e a segurança, o que revela uma expressiva abertura para o estabelecimento de redes de comunicação fluídas. O Relatório FTC é destinado a todas as entidades que coletam ou utilizam dados que possam ser "razoavelmente relacionados" a um titular específico ou a um dispositivo, exceto nos casos em que a entidade coleta apenas informações não-confidenciais (por exemplo, um dado que não seja considerado sensível) de até 5 (cinco) mil consumidores por ano e não compartilha os referidos dados com terceiros[266]. O Relatório FTC esclarece que os dados não serão considerados "razoavelmente ligados" a um titular ou dispositivo caso a entidade:

> (i) tome medidas razoáveis para garantir que os dados não sejam identificados, como ocorre no caso de a entidade possuir um nível de confiança razoável e justificável de que os dados não podem ser usados para inferir informações ou serem relacionados a um consumidor específico, computador ou dispositivo;
> (ii) publicamente se comprometa a manter e usar os dados apenas de forma não identificada e a não adotar procedimentos que permitam associá-los novamente a seu titular; e

---

[265] **A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority**.

[266] ALLEN, **Privacy law and society**, p. 897.

> (iii) impeça, por meio de um contrato, que eventuais terceiros contratados pela entidade tenham acesso aos dados e adotem procedimentos que permitam associá-los novamente a seu titular.

O papel da FTC na promoção de um modelo de corregulação equilibrado e marcado pela compreensão dos subsistemas parciais tem se revelado muito peculiar quando comparado a outras autoridades de proteção de dados, que possuem atribuição específica, além de atuação não restrita às questões de defesa do consumidor.

4.2 O consentimento pela perspectiva da FTC

Na perspectiva da FTC, as organizações devem simplificar e esclarecer os titulares sobre as regras e práticas que tratam da obtenção de consentimento para a coleta e/ou uso de dados. Em linhas gerais, a FTC destaca em seu Relatório que o consentimento, quando necessário, deve ser "significativo" e rejeita a possibilidade de adoção pelas entidades de uma abordagem no sentido de "tomar ou largar" (*take it or leave it*) para serviços importantes em que os consumidores têm poucas opções[267].

Uma das particularidades do modelo de proteção de dados da FTC é que originalmente ele se restringia a consumidores, mas atualmente tem sido ampliado para as mais variadas hipóteses de proteção de usuários, o que evidencia a sua capacidade de dialogar e influenciar os mais diversos subsistemas sociais, sempre atento à policontextualidade da proteção dos dados pessoais.

Apesar de prever situações excepcionais, a FTC entende que as organizações devem obter o consentimento expresso antes mesmo de (i) utilizar os dados para finalidades diversas em relação às quais foram coletados, somente (ii) coletar dados sensíveis para determinados fins; ou (iii) para promover alterações materiais e retroativas em suas políticas de privacidade[268].

No que se refere às práticas de tratamento de dados que exijam o consentimento, a FTC recomenda que ele seja obtido no exato momento em que o titular realizar uma operação

---

[267] SCHWARTZ, Privacy and Democracy in Cyberspace.

[268] BELLIA, Patricia L.; SCHIFF BERMAN, Paul; POST, David G., **Cyberlaw: Problems of Policy and Jurisprudence in the Information Age**, [s.l.]: West Group, 2003.

ou atividade. A FTC admite, no entanto, que a forma como as entidades implementarão esta recomendação poderá variar de acordo com as circunstâncias. Em alguns casos excepcionais e devidamente justificados, por exemplo, a FTC permite que o consentimento seja obtido após a coleta de seus dados.

Uma importante diretriz da FTC envolve a dispensa da oferta de escolha (*choice*) ao titular dos dados antes da coleta ou do uso de dados quando (i) relacionados com práticas inerentes ao contexto da operação, ou (ii) quando vinculados a uma relação pré-existente entre a entidade e o titular, ou (iii) quando exigido ou autorizado por lei. Esta foi uma medida adotada pela FTC para estabelecer um equilíbrio entre flexibilidade e a necessidade de limitar práticas para as quais a escolha é dispensada[269].

No tocante aos dados sensíveis, o Relatório FTC determina que as entidades devem buscar o consentimento expresso e afirmativo antes de coletá-los, independentemente do uso de tais dados. É importante mencionar que a FTC não exige o consentimento expresso e afirmativo para a coleta de dados de adolescentes (indivíduos com idade entre 13 e 17 anos)[270]. Não obstante, a FTC ressalta que as entidades que tem adolescentes como público-alvo devem considerar proteções adicionais aos dados dos adolescentes, tais como períodos de retenção mais curtos.

Boa parte dessas características revela o modo equilibrado como a FTC tem atuado na corregulação das questões de proteção de dados, em especial se considerarmos as suas características[271] e a forma como realiza o *enforcement* de suas sanções.

4.3 A interoperalidade como marca das transferências internacionais para a FTC

Para a FTC, a diretriz primordial que deveria ser adotada pelas diversas jurisdições a respeito da transferência internacional de dados deveria ser a interoperabilidade, sobretudo em

---

[269] *Ibid*.; SOLOVE, Daniel J.; ROTENBERG, Marc; SCHWARTZ, Paul M., **Information privacy law**, New York: Wolters Kluwer Law Business, 2014.

[270] SWIRE; AHMAD, **US Private-sector Privacy**; **A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority**.

[271] SCHWARTZ, Paul M.; SOLOVE, Daniel J., The PII problem: privacy and a new concept of personally identifiable information, **NYU Law Review**, v. 86, p. 1814, 2011; SCHWARTZ, Paul M., Legal Access to the Global Cloud, **Columbia Law Review**, v. 118, n. 6, p. 1681–1762, 2018; BELLIA; SCHIFF BERMAN; POST, **Cyberlaw**.

razão do crescente volume de dados coletados em um dado país e tratados em outro.[272] Em outras palavras, por meio da interoperalidade a FTC promove a policontextualidade e interlocução entre as redes de comunicação que viabilizam uma análise mais profunda das práticas sociais e dos discursos.

Com relação ao compartilhamento transnacional de dados, em 2010, a FTC e a *Federal Communications Commission* (FCC), na qualidade de agência governamental responsável pela regulação da área de telecomunicações e radiodifusão dos Estados Unidos, aderiram ao *Global Privacy Enforcement Network* ("GPEN")[273] com o objetivo de fomentar um maior compartilhamento transnacional de dados relacionados a investigações e persecuções entre países aderentes. Vale mencionar, ainda, que além do GPEN, a FTC também atua em conjunto com a APEC para implementação do CPEA, conforme será a seguir analisado.

Nesse particular, a FTC ressalta que a proteção significativa a tais dados somente será alcançada se houver convergência dos regimes de proteção de dados, bem como se for verificada a habilidade dos diferentes modelos funcionarem em conjunto e assegurarem respostas consistentes para os titulares dos dados e às entidades que a eles se submetem. Vale destacar, por sinal, que a FTC desempenha um papel central nas transferências de dados com a União Europeia por meio do *Privacy Shield*, na medida em que atua como órgão certificador das empresas americanas que desejam realizar operações de tratamento com países membros do bloco.

Observa-se, portanto, que a FTC tem tido um amplo engajamento com os mais diferentes modelos e autoridades para tentar manter o fluxo de interoperabilidade nas transferências internacionais de dados, tal como se espera de um modelo de corregulação com capacidade de interlocução com os demais atores envolvidos no processo de fortalecimento da *accountability*.

---

[272] Cf. **Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers**, Federal Trade Commission, disponível em: <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers>, acesso em: 3 mar. 2019.

[273] Cf. **Global Privacy Enforcement Network: An International Network to Foster Cross-Border Co-operation**, disponível em: <https://www.privacyenforcement.net/about_the_network>, acesso em: 3 mar. 2019.

5. O modelo regulatório inovador da APEC: o consentimento flexível e o APEC Privacy Framework

Se por um lado o modelo da FTC pode ser reconhecido por explorar a interoperabilidade nas transferências internacionais e o diálogo entre os *stakeholders* no processo regulatório, a APEC otimizou ainda mais essas características. APEC ou Cooperação Econômica Ásia-Pacífico é um bloco econômico fundado em 1989, cujos principais objetivos consistem em estimular o comércio de produtos e serviços entre os países membros da região da Ásia e do Pacífico, bem como reduzir as tarifas alfandegárias nas relações comerciais entre os referidos países membros. Cabe destacar que a APEC não impõe um código de obrigações de caráter vinculante para os seus países membros, de modo que as suas principais diretivas são estabelecidas por meio de decisão consensual.

No que se refere à proteção de dados pessoais e privacidade, o modelo desenvolvido pela APEC é baseado no APEC Privacy Framework,[274] que contém princípios e diretrizes para o tratamento de dados a serem adotados pelos países membros[275], o que demonstra a potencialidade da rede de comunicações e capacidade de compreensão da autonomia de alguns dos subsistemas parciais de regulação.

Sob a perspectiva do *APEC Privacy Framework* e da *Cross Border Privacy Rules* (CBPR), a coleta de dados pessoais deve ser limitada aos dados relevantes para o propósito da atividade, além de ser obtida por meios legítimos. Ademais, quando apropriado, a coleta deverá ser precedida de notificação ao titular ou seu consentimento. Se coletada para outros fins, o consentimento do indivíduo deve ser exigido. Em todos os casos, não se estabelece a forma pelo qual o consentimento deve ser obtido, o que revela a flexibilidade e dinamicidade do modelo de regulação da APEC.

Vale ressaltar, no entanto, que a regra geral quanto à vinculação ao propósito da atividade poderá ser dispensada quando o consentimento do titular for obtido, ou quando o uso dos dados pessoais for necessário à prestação dos serviços e fornecimento de bens, ou quando for exigido por lei (art. 19, a, b, c).

---

[274] **APEC Privacy Framework**, disponível em: <http://publications.apec.org/Publications/2005/12/APEC-Privacy-Framework>, acesso em: 3 mar. 2019.

[275] *Ibid*.

A despeito de uma maior flexibilidade sobre a apresentação do aviso de privacidade e/ou da coleta do consentimento, o *APEC Privacy Framework* estabelece que a coleta de dados pessoais deve ser limitada às informações relevantes para o propósito em relação ao qual os dados foram coletados e que tais informações devem ser obtidas por meios legítimos. Qualquer coleta realizada para outros fins ou em excesso com a finalidade esperada pelo titular de dados deve ser precedida do consentimento. No *APEC Privacy Framework* não há qualquer qualificadora para reconhecimento do consentimento, tal como a adjetivação do consentimento como expresso, implícito, afirmativo, ou de outra forma.

O *APEC Privacy Framework* também comporta exceções, tais como aquelas necessárias a resguardar a soberania nacional, a segurança pública e promoção de políticas públicas, mas desde que o uso de dados seja limitado e proporcional ao cumprimento de objetivos definidos, bem como divulgado ao público ou em conformidade com a lei.

O modelo da APEC estabelece que os responsáveis pelo tratamento de dados pessoais devem sempre notificar, clara e facilmente, as políticas e práticas relacionadas aos dados pessoais, o que inclui:

- quando ocorre a coleta de dados pessoais;
- os propósitos da coleta de dados pessoais;
- para que tipo de pessoas e organizações os dados pessoais podem ser divulgados;
- a identidade e a localização do controlador dos dados pessoais, incluindo informações para contato; e
- as escolhas e os meios disponibilizados pelo controlador para que os indivíduos possam limitar o uso e a divulgação, acessar ou corrigir seus dados pessoais.

Segundo o *APEC Privacy Framework* devem ser empregados todos os esforços razoáveis para garantir que a notificação seja enviada antes ou no momento da coleta de dados pessoais. Caso não seja viável, tal notificação deve ser enviada assim que for possível.

O *APEC Privacy Framework* também consagra o princípio da escolha (*choice*), que orienta as organizações a dar aos indivíduos acesso a mecanismos claros, destacados, facilmente compreensíveis e a preços acessíveis para exercer a escolha em relação à coleta, uso e divulgação de seus dados pessoais.

5.1 A certificação privada como paradigma da transferência internacional de dados pessoais e o funcionamento das CBPR

O modelo de transferência internacional de dados proposto pela APEC consiste em um sistema que tem por objetivo estabelecer uma proteção adequada à privacidade e evitar a imposição de obstáculos ao fluxo de dados na região sujeita às regras da APEC. Até aqui, nenhuma novidade se o compararmos aos demais. A diferença do modelo da APEC para os demais deve-se à inversão de papéis, em especial porque o agente fiscalizador e certificador também pode ser um *stakeholder* privado. Isso mostra como o modelo da APEC é aberto ao pluralismo jurídico e ao equilíbrio de papéis desempenhados pelos agentes reguladores.

Todos os países membros da APEC devem evitar a adoção de medidas que acarretem um desestímulo ao fluxo transnacional de dados quando um outro país signatário da APEC tenha instrumentos regulatórios e/ou legislativos considerados efetivos ou tenha suficientes salvaguardas que assegurem padrões mínimos de proteção ao processamento de dados pessoais. O modelo desenvolvido pela APEC é baseado no *APEC Privacy Framework*[276], que contém princípios e diretrizes para o tratamento de dados e inclui regras sobre transferência internacional entre os membros da APEC, mediante a adesão ao sistema *Cross-Border Privacy Rules* (CBPR).[277] O *APEC Privacy Framework* é elaborado no nível dos princípios, mas ainda há uma enorme incompatibilidade e dificuldade de implementação em virtude de outros países não reconhecerem o CBPR e o *APEC Privacy Framework* como capazes de proporcionar o mesmo nível de proteção adequada, como se verifica com a União Europeia em relação ao GDPR.

Trata-se de um sistema de adesão voluntária, construído sob um arranjo regulatório de cooperação entre os países membros, focado na premissa da responsividade (*accountability*), ou seja, voltado a conferir maior responsividade àqueles que desejam maior liberdade no tratamento de dados pessoais. Um exemplo desta característica envolve o trabalho conjunto desenvolvido pelos países membros da APEC e as organizações privadas transnacionais, com o intuito de desenvolver o *PRP-Privacy Recognition for Processors System* em complemento ao CBPR, de modo a viabilizar a implementação de obrigações para processadores e controladores de dados.

---

[276] *Ibid*.

[277] **Cross Border Privacy Rules System**, disponível em: <http://cbprs.org/>, acesso em: 3 mar. 2019.

Estados Unidos, China, Canadá, Japão, Chile, Peru, Singapura, Nova Zelândia e México são exemplos de países que já aderiram ao *Cross-Border Privacy Rules (*CBPR), cujo objetivo e missão se resume a ser um sistema de adesão simplificada e de baixo custo. Organizações que queiram aderir ao sistema devem implementar políticas de privacidade e práticas consistentes com os requisitos do CBPR.

Nos casos de transferência de dados para outra organização empresarial, seja a transferência nacional ou internacional, ou quando os dados são coletados para finalidades diferentes das quais foram originalmente obtidos, o consentimento do usuário deve ser obtido ou algumas medidas deverão ser adotadas para assegurar que o destinatário irá proteger os dados em conformidade com os preceitos do CBPR. Em todo o caso, a transferência internacional de dados dentro do sistema CBPR depende de adesão das organizações e países membros ao sistema.

Um dos traços distintivos do modelo de transferência internacional de dados da APEC refere-se à interoperabilidade entre sistemas normativos e a existência de um agente certificador privado (*accountability agent*),[278] responsável pelo cumprimento e *enforceability* dos requisitos do CBPR. Uma vez certificada pelo agente privado a partir da avaliação de compatibilidade com o sistema CBPR, a organização fica sujeita às suas regras de forma vinculante e autorizada a operar na APEC (*Cross-border Privacy Enforcement Arrangement* ou CPEA).

A despeito de o sistema CBPR utilizar agentes certificadores privados ou terceiros capazes de verificar se as políticas e práticas de privacidade de uma organização atendem aos requisitos do programa CBPR, os países membros integrantes do bloco também possuem liberdade para adotar leis e regulamentos internos voltados à proteção de dados pessoais, desde que em conformidade com o sistema CBPR. Além disso, o grupo de países membros pode trabalhar em conjunto para atuar em investigações relacionadas à proteção de dados.

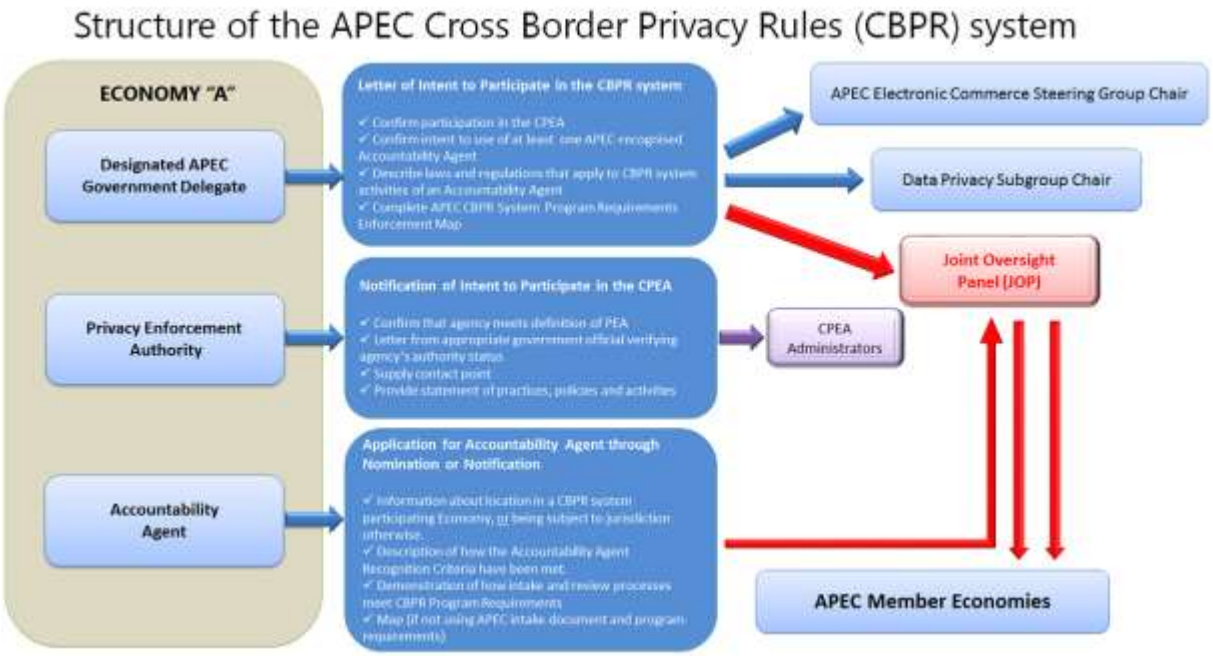
A certificação do sistema CBPR leva em consideração 4 (quatro) elementos: (a) auto avaliação; (b) análise de compliance; (c) reconhecimento/aceitação; (d) resolução de disputas e exequibilidade. O sistema CBPR é baseado na responsabilidade voluntária dos seus países membros para facilitar o fluxo de dados e privacidade.

---

[278] TRUSTe (EUA) JIPDEC (Japão). Cf. **Accountability Agents**, Cross Border Privacy Rules System, disponível em: <http://cbprs.org/accountability-agents/>, acesso em: 3 mar. 2019.

Desde que os Estados Unidos passaram a fazer parte do sistema CBPR, em 2011, a TRUSTe foi nomeada como agente certificador autorizado e a Federal Trade Commission foi designada como a principal autoridade de fiscalização. Em agosto de 2013, a IBM foi a primeira empresa dos EUA a ser certificada de acordo com o sistema CBPR.

A rigor, o *APEC Privacy Framework* e CBPR visam apenas assegurar um padrão normativo mínimo de proteção de dados, sem prejuízo da existência de normas elaboradas pelos países membros. Isso significa que em caso de transferências transnacionais de dados, a adesão à APEC não exclui a aplicação da legislação nacional de cada um dos países. Neste sentido, o sistema CBPR em muito se assemelha ao EU-EUA Privacy Shield.[279]



[279] The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States. The Privacy Shield program enables U.S.-based organizations to join one or both of the Privacy Shield Frameworks in order to benefit from the adequacy determinations. To join either Privacy Shield Framework, a U.S.-based organization will be required to self-certify to the Department of Commerce (via this website) and publicly commit to comply with the Framework's requirements. While joining the Privacy Shield is voluntary, once an eligible organization makes the public commitment to comply with the Framework's requirements, the commitment will become enforceable under U.S. law. All organizations interested in self-certifying to the EU-U.S. Privacy Shield Framework or Swiss-U.S. Privacy Shield Framework should review the requirements in their entirety. Cf. **Privacy Shield Program Overview**, disponível em: <https://www.privacyshield.gov/Program-Overview>, acesso em: 3 mar. 2019.

6. O Personal Information Protection and Eletronic Documents Act (PIPEDA) e a proteção de dados pessoais no Canadá

Se por um lado a marca do modelo de corregulação da FTC é a interoperabilidade, o Canadá adota um modelo de corregulação mais focado na atribuição de responsividade aos agentes de mercado. O Canadá promoveu a regulação das questões relacionadas ao tratamento de dados por meio do *Personal Information Protection and Eletronic Documents Act* (PIPEDA). O PIPEDA foi complementado pelas *Guidelines elaboradas pelo Office of the Privacy Commissioner of Canada*[280] - a autoridade de proteção de dados responsável pela fiscalização e imposição de sanções - e elenca disposições sobre o consentimento e a transferência de dados pessoais para processamento por terceiros, inclusive aqueles localizados fora do Canadá. Essas disposições não se aplicam a entidades públicas federais, estaduais ou municipais.[281] Desde que Ann Cavoukian se tornou a comissária da autoridade de Ontário[282], o PIPEDA e as Guidelines ganharam expressiva transformação e influenciaram sobremaneira outros ordenamentos jurídicos, dada a capacidade de fomentar redes de comunicação entre os subsistemas que pretende regular. A única particularidade que ainda desperta críticas envolve o fato de o PIPEDA não ter como destinatário prioritário o próprio poder público, o que indica uma perda de densidade normativa se considerado o seu objetivo geral de promover a *accountability*.

A regra motriz do PIPEDA é que as organizações canadenses são responsáveis pelo tratamento conferido aos dados pessoais coletados e devem protegê-los durante toda a cadeia de processamento, ainda que sob a custódia de terceiros. O meio mais básico de proteção de dados ocorre via arranjos contratuais, ou seja, o PIPEDA apresenta, ainda que de forma parcial, uma carga de responsividade articulada em torno da intercomunicação e responsividade dos envolvidos em todas as atividades de processamento de dados pessoais.

Nenhum contrato, todavia, pode afastar a aplicação de leis criminais, de segurança nacional ou outras leis do país de destino dos dados. É fundamental que as

---

280 CANADA, Office of the Privacy Commissioner of, **Office of the Privacy Commissioner of Canada**, disponível em: <https://www.priv.gc.ca/en/>, acesso em: 3 mar. 2019.

281 CANADA, Office of the Privacy Commissioner of, **Guidelines for Processing Personal Data Across Borders**, disponível em: <https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/>, acesso em: 3 mar. 2019.

282 CAVOUKIAN, Ann, Privacy by design: The 7 foundational principles, **Information and Privacy Commissioner of Ontario, Canada**, v. 5, 2009.

organizações promovam análises de risco que poderiam afetar a integridade, segurança e confidencialidade dos dados pessoais, especialmente quando tais dados estiverem fora do Canadá. Por sinal as organizações devem ser transparentes quanto ao uso de dados pessoais, durante toda sua cadeia de processamento. Isso inclui a notificação prévia da possibilidade de envio de dados pessoais para outras jurisdições, assim como as potenciais consequências deste envio. É possível dizer que o PIPEDA é um dos modelos mais próximos daquilo que se espera em termos de regulação de proteção de dados pessoais dos agentes de mercado, em especial pela carga conferida à transparência, responsividade e liberdade de fluxo informacional entre os *stakeholders.*

6.1 Os requisitos do consentimento segundo o PIPEDA: um modelo intermediário

O consentimento é um dos pilares do PIPEDA, o qual prevê que indivíduos podem expressar sua autonomia e controle sobre seus dados pessoais. A regra estabelecida pelo PIPEDA é de que o consentimento é requisito para a coleta, uso, compartilhamento e divulgação de dados pessoais.

Com o desenvolvimento tecnológico, o desafio passou a ser a obtenção de um real consentimento, visto que o trânsito de dados tem se tornado cada vez mais volátil e interativo, dificultando o controle dos titulares dos dados. Além disso, o correto entendimento dos propósitos para os quais os dados foram coletados é um importante elemento para a delimitação do consentimento exigido pelo PIPEDA.

Apesar do foco no consentimento, o PIPEDA consegue equilibrar por meio do dever de transparência e *accountability* a missão de promover a tutela dos dados pessoais e simultaneamente atuar como ponto de concentração das pretensões regulatórias públicas e privadas, numa indicação de que compreende a policontextualidade do objeto regulado. O principal problema, como enfatizado anteriormente, continua a ser a inaplicabilidade das suas normas ao próprio poder público, o que denota a incompreensão de parte do subsistema de linguagem do processo de tratamento de dados pessoais e proteção da privacidade.

O consentimento obtido pelas organizações deve ser pautado por informações completas e compreensíveis, assim como disponíveis previamente. Entretanto, para um real consentimento, o PIPEDA exige a observância do seguinte teste:

- A clara aposição de quais dados pessoais estão sendo coletados;

> - Com quem os dados pessoais estão sendo compartilhados, incluindo uma enumeração dos terceiros envolvidos;
> - Com quais propósitos os dados pessoais estão sendo coletados, usados e compartilhados;
> - Qual o risco de eventual dano para o indivíduo, se existir?

A autoridade canadense entende que as informações devem ser disponibilizadas em plataformas de fácil acesso e interação, assim como os indivíduos devem estar habilitados para controlar o nível de detalhamento que pretendem obter, a autoridade compreende a dimensão do poder exercido por elas. Para se contrapor ao predomínio irrestrito dos interesses das plataformas, o PIPEDA exige manifestações de consentimento positivo no formato *opt in* à medida que os níveis de detalhamento sobre a obtenção, uso e divulgação de dados pessoais sejam enumerados.

Como a responsividade é marca do PIPEDA[283], os agentes de mercado devem promover inovações que viabilizem novas formas de obtenção do consentimento que sejam adequadas para o serviço, produto, plataforma que exploram o tratamento dos dados pessoais. Por essa razão, os agentes de mercado devem sempre levar em consideração a acessibilidade da forma de obtenção do consentimento, assim como a facilitação da compreensão das informações previamente disponíveis, em especial porque o consentimento é um processo mutável dentro da perspectiva da policontextualidade.

Caso as circunstâncias envolvidas mudem - afinal os subsistemas parciais possuem linguagem própria e códigos em constante transformação - o consentimento deve ser novamente solicitado para atender os parâmetros das novas realidades práticas colocadas. A dinamincidade de transformação dos elementos responsáveis pelo acoplamento estrutural de um determinado modelo regulatório exige que os *stakeholders* envolvidos não se limitem a um consentimento estático, obtido em um determinado momento, mas o considerem em perspectiva e de forma interativo, tendo sempre em mira adequá-lo às reais circunstâncias. Por isso, as informações disponibilizadas para tomada do consentimento devem ser claras e transparentes, com o emprego de linguagem clara e adequada ao titular dos dados pessoais. Isso se reflete tanto no idioma, quanto na não utilização de termos excessivamente técnicos ou vagos.

---

[283] CANADA, **Office of the Privacy Commissioner of Canada**.

Para que a *accountability* tenha condições de ser mensurada em todas as etapas do processamento da atividade de tratamento de dados pessoais, o consentimento para a coleta, uso e compartilhamento deve ser obtido antecipadamente. Sob a égide do PIPEDA, o consentimento obedece ao "princípio da coleta limitada", segundo o qual a coleta de dados pessoais está restrita aos propósitos necessários e identificados pelo responsável pela atividade de tratamento. Dessa forma, o consentimento obtido não pode ser expandido para além dos propósitos necessários e identificados previamente pelo responsável, de forma que ficam adstritos aos termos estabelecidos. Logo, observa-se que o PIPEDA trabalha de forma muito consistente com a *accountability* e transparência para viabilizar que o titular dos dados tenha condições de compreender a dinamicidade do processo de tratamento.

A autoridade canadense entende que o nível de extensão e a forma de tomada do consentimento depende da sensibilidade do dado pessoal disponibilizado e do risco do dano posterior, ou seja, impõe exigências segundo os parâmetros da policontextualidade da atividade de tratamento. O conceito de sensibilidade da informação é variável nas normas canadenses, de forma que o contexto de sua utilização deve ser levado em conta para essa classificação. Nos casos de sensibilidade da informação, recomenda-se a obtenção de consentimento explícito.

O consentimento pode ser implícito, porém somente em casos de menor sensibilidade. Também há a possibilidade de consentimento por terceiro autorizado, como tutor, curador ou alguém com procuração para tal. Em casos no qual há maior dúvida quanto à extensão do consentimento, a legítima expectativa do titular dos dados pessoais quanto à extensão do consentimento deve ser levada em conta. Além disso, o titular dos dados pode, a qualquer momento, revogar o consentimento. Essa revogação pode estar sujeita a consequências contratuais ou demandar uma notificação específica, entretanto não se admite a imposição de empecilhos para que o titular o revogue.

6.2 O maior peso da accountability nas transferências internacionais de dados

A regra geral, adotada pela União Europeia, em questões relacionadas à transferência internacional de dados pessoais, tem como pressuposto a relação entre Estados-membros. Neste panorama, a transferência internacional de dados é restringida entre

jurisdições, a não ser que a Comissão Europeia aponte que a jurisdição de destino possui adequada proteção aos dados pessoais ou sejam adotadas salvaguardas[284].

No caso canadense, o pressuposto é a perspectiva organização-organização, que não contempla conceito de "adequação". Não há proibição para transferência de dados para processamento em organizações localizadas em outras jurisdições, todavia estas são consideradas responsáveis por cada acordo de transferência de dados. Este é um claro indicativo da forma como o modelo canadense explora a intercambiariedade entre consentimento e *accountability*, ou seja, determinadas operações intra grupos dispensam o consentimento para as transferências internacionais, mas por outro lado a responsividade é substancialmente maior.

Caso uma organização estabeleça um contrato que envolva o envio internacional de dados pessoais para outra, a organização sujeita às normas canadenses é responsável pela proteção dos dados ainda que estejam localizados fora do território canadense. O papel da autoridade de proteção de dados canadense é investigar e auditar esses acordos de transferência de dados, isto é, há espaço para manifestações de pluralismo jurídico na medida em que a atuação estatal envolve a fiscalização e controle, ao passo que os agentes atuam no limite da responsividade. Este é um elemento distintivo extremamente interessante e peculiar do modelo canadense, que revela a policontextualidade e capacidade de diálogos da corregulação[285].

Segundo o princípio motriz do PIPEDA, a *accountability*, a organização sujeita às normas canadenses é responsável pela proteção dos dados pessoais sob o seu controle. Pelo prisma da *accountability* está garantida a possibilidade e a legitimidade da transferência de dados pessoais a terceiros para processamento, porém a responsabilidade da organização canadense é ampliada, especialmente pelo fato de os dados se encontrarem sob a custódia do terceiro.

Há, portanto, um balanceamento entre a proteção individual de dados e as necessidades diversas do mercado e do desenvolvimento tecnológico. Entretanto, há expressa recomendação que as organizações canadenses providenciem mecanismos para que os níveis

---

[284] EUROPEAN COMMISSION, **ow the EU determines if a non-EU country has an adequate level of data protection**; EUROPEAN COMMISSION, **International data flows: Commission launches the adoption of its adequacy decision on Japan**.

[285] CANADA, **Guidelines for Processing Personal Data Across Borders**.

de proteção aos dados pessoais em posse de terceiros sejam equiparáveis às disposições legais do PIPEDA. Isso não implica que a organização estrangeira tenha de cumprir todos os requisitos legais canadenses, mas que o nível de proteção deva ser equiparado ao que ocorreria se os dados não houvessem sido transferidos internacionalmente.

Para o PIPEDA, a transferência deve ser compreendida como forma de uso do dado no âmbito da mesma organização, o que difere o modelo canadense de outros tantos, visto que o compartilhamento de dados dentro de um mesmo grupo econômico nem sempre é revestido da mesma finalidade e base legal. Por esta razão, para o PIPEDA, quando há transferência de dados pessoais, eles só poderão ser utilizados para os fins previamente estabelecidos na coleta.

Independentemente de onde os dados estão sendo processados, dentro ou fora do Canadá, a organização deve adotar todas as medidas e garantias com o fim de impedir o acesso e a divulgação de dados pessoais a terceiros não autorizados. Como o PIPEDA associa a transferência de dados pessoais ao uso, a legislação canadense não distingue transferências domésticas ou internacionais de dados pessoais, o que evidencia outro ponto distintivo da legislação canadense em relação às demais.[286]

O PIPEDA não proíbe a transferência internacional de dados pessoais entre organizações de jurisdições distintas se os dados pessoais transferidos estão sendo utilizados para os propósitos previamente disponibilizados no momento da coleta. Nestas circunstâncias, não é necessário novo e/ou específico consentimento para a transferência. O principal mecanismo privado utilizado para viabilizar as transferências e ampliar o controle do tratamento conferido aos dados pessoais são os arranjos contratuais. Esse é outro elemento que evidencia o poder conferido pelo PIPEDA para arranjos contratuais em conjunto com o princípio da *accountability*. Em outras palavras, maior liberdade de interlocução e atuação para os agentes de mercado, porém maior *accountability* e sanções, o que demonstra toda a complexidade e abrangência do modelo canadense na regulação da privacidade e proteção de dados pessoais. Este é certamente, o modelo que melhor espelha as principais características que serão apontadas como base para a *Lex Privacy.*

---

[286] *Ibid*.

7. A Austrália e o regime híbrido do Australian Privacy Act

Assim como o Canadá conseguiu promover a regulação da proteção de dados e privacidade sob uma perspectiva equilibrada entre consentimento e *accountability*, com a adoção de incentivos para as redes de comunicação entre os *stakeholders* e compreensão da policontextualidade das múltiplas atividades de tratamento de dados, a Austrália também se destaca pela forma conciliadora com que promoveu a regulação.

Na Austrália, as questões relacionadas ao tratamento e processamento de dados pessoais foram reguladas pelo *Australian Privacy Act* de 1988 (*Australian Privacy Act*),[287] ao passo que a fiscalização e as sanções são de responsabilidade do *Office of the Australian Information Commissioner* (OAIC),[288] a autoridade de proteção de dados australiana

O *Australian Privacy Act* é composto por 13 (treze) princípios sobre privacidade, denominados APPs, que definem padrões, direitos e obrigações para o uso, armazenamento, acesso e transferência de dados pessoais. Esses princípios são aplicáveis às agências de governo australianas, ao setor privado e às organizações sem fins lucrativos com faturamento anual maior que U$ 3 milhões. O arcabouço regulatório da Austrália é considerado razoavelmente dinâmico, dotado de capacidade de dialogar com os variados subsistemas e construído sob princípios que ampliam a sua efetividade de compreender a policontextualidade da tutela da privacidade e proteção dos dados pessoais, conforme a seguir se observará por meio da análise do consentimento e das transferências internacionais.

7.1 O consentimento segundo o Australia Privacy Principles

Na Austrália, o tema do consentimento é muito relevante para os denominados *Australia Privacy Principles* (APPs). Há dois tipos de tratamentos relacionados ao consentimento: ora o consentimento é entendido como uma exceção a uma regra proibitiva sobre algum tipo de tratamento de dados pessoais, ora o consentimento é visto como um mecanismo de autorização para que a autoridade promova certo tipo de tratamento.

---

[287] **Privacy Act 1988**, disponível em: <https://www.legislation.gov.au/Details/C2017C00283>, acesso em: 3 mar. 2019.

[288] **Office of the Australian Information Commissioner - OAIC**, disponível em: <https://www.oaic.gov.au/>, acesso em: 3 mar. 2019.

Os APPs apontam que nenhuma organização sujeita às normas australianas pode coletar dados pessoais que não sejam razoavelmente necessários ou diretamente relacionados com as funções ou atividades da organização. O consentimento é apresentado como condição necessária em casos de coleta de dados pessoais relacionados a informações sensíveis. Também é condição no caso de coleta indireta de dados pessoais realizada por agência governamental, mesmo que não se refiram a informações sensíveis, isto é, quando os dados pessoais não são fornecidos pelo próprio titular, mas por um terceiro que os detenha. Para o ordenamento jurídico australiano, informações sensíveis são:

- Informação ou opinião relacionada a: (i) origem étnica ou racial; (ii) posicionamentos políticos; (iii) associação política; (iv) religião; (v) posicionamentos filosóficos; (vi) associação profissional ou comercial; (vii) orientação sexual; ou (viii) antecedentes criminais;
- Informações de saúde de um indivíduo;
- Informações genéticas;
- Informações biométricas relacionadas a identificação ou verificação biométrica;
- Templates biométricos.

O consentimento também é condição necessária para qualquer uso ou compartilhamento praticado com propósitos secundários, isto é, não relacionados às funções ou atividades da empresa (propósitos primários). Nas circunstâncias em que exigido, o consentimento pode ser implícito ou explícito e é composto por 4 (quatro) elementos-chave:

- indivíduo deve ser adequadamente informado, de forma prévia e detalhada sobre as circunstâncias envolvidas no consentimento;
- consentimento deve ser espontâneo e voluntário;
- consentimento deve ser atual e específico;
-para consentir, o indivíduo deve ser capaz de entender e comunicar seu consentimento.

O consentimento explícito pode ser concedido oralmente ou por via escrita. Nesse contexto, são aceitáveis assinaturas, declarações ou gravações de voz. Já o consentimento implícito acontece quando das circunstâncias ou da própria atuação do titular é possível inferir a adesão. A mera não objeção não significa consentimento. Os princípios que regem o *Privacy Act* australiano afirmam que o silêncio não é considerado consentimento, mesmo que a coleta, uso ou compartilhamento dos dados pessoais seja benéfico ao titular. Ademais, uma mera notificação de uso, armazenamento ou compartilhamento de dados pessoais também não é suficiente para o consentimento. Todos esses fatores mostram a capacidade do modelo australiano em compreender as redes de comunicação e os sinais de

linguagem que se formam no contexto das atividades de tratamento, a evidenciar a sua percepção sobre a policontextualidade.

O uso de opções *opt-out* para aferição de consentimento é possível, porém limitado a circunstâncias específicas, pois a intenção do indivíduo ao não optar pela saída pode ser ambígua e o consentimento, nesse contexto, tem de ser específico. Para que a opção *opt-out* seja dada corretamente, ela (i) deve ter sido apresentada de maneira clara e detalhada, (ii) precisa estar disponível e não agrupada com outras opções, (iii) tem de ser de fácil acesso, (iv) não pode estar limitada por custos excessivos (v) e as consequências da opção de saída não podem ser excessivamente graves.[289]

O APP encoraja que, quando se tratar de informações sensíveis, o jurisdicionado sempre opte pelo consentimento explícito, dado o alto impacto na privacidade ao manipular dados dessa natureza. O APP também exige a presença de mecanismos e sistemas aptos a gravar o consentimento. Cabe ressaltar que há expressa recomendação para que todos os esforços para obtenção de consentimento expresso e específico sejam prévios a qualquer tipo de tratamento aos dados pessoais. Quanto à voluntariedade do consentimento, devem existir alternativas caso o indivíduo opte por não o fornecer e as consequências devem ser razoáveis frente à recusa.

Os APPs também tratam do conceito de "*blundled consent*", que se refere às hipóteses em que o consentimento é solicitado de forma misturada em meio a múltiplos pedidos, com mescla pouco clara acerca dos diversos tipos de uso, armazenamento e compartilhamento de dados pessoais, sem que seja dada a oportunidade de escolha específica sobre o que será consentido ou não. Seria uma forma de consentimento em bloco, desvestida da transparência necessária e incapaz de viabilizar a correspectiva responsividade pela atividade de tratamento realizada. Essa prática é considerada prejudicial à voluntariedade do consentimento,[290] notadamente porque prejudica a autonomia do titular e sua capacidade de conhecimento de toda a atividade de tratamento.

Para a obtenção do consentimento, todos as formas de usos e consequências do fornecimento de dados pessoais devem estar expressas no momento da aceitação, em inglês e

---

[289] **Chapter B: Key concepts - consent**, disponível em: </agencies-and-organisations/app-guidelines/chapter-b-key-concepts>, acesso em: 3 mar. 2019.

[290] *Ibid*.

sem expressões excessivamente jurídicas ou técnicas. Se alguma condição for alterada após consentimento, novo consentimento deve ser obtido. O consentimento obtido em determinadas circunstâncias não pode ser entendido como indefinidamente concedido ou suficiente para novos usos. Caso outra coleta, uso ou compartilhamento se faça necessário, o consentimento específico para o novo propósito deve ser obtido.

O consentimento pode ser revogado a qualquer momento e esse processamento deve ser fácil e imediato, não sendo mais possível que a organização use ou faça compartilhamento de quaisquer das informações anteriormente obtidas. Também devem estar claras as consequências da revogação do consentimento para o titular dos dados. Uma organização não deve buscar um consentimento mais amplo do que o necessário, mas apenas aquele específico para os propósitos primários de coleta, uso e compartilhamento.

Não há consentimento válido sem capacidade para consentir. O titular dos dados deve possuir a capacidade e o efetivo entendimento sobre os efeitos do consentimento, assim como a capacidade de o manifestar livremente. A organização pode presumir a capacidade, a não ser que haja fundados indícios de que ela inexista, como, por exemplo, a possibilidade de se tratar de uma criança ou indivíduo com limitada capacidade de entendimento do idioma inglês.

7.2 As transferências internacionais e o arranjo para compartilhamento dentro do mesmo grupo econômico

No caso australiano, apesar dos APPs não serem exaustivos, todas as organizações devem garantir que os princípios ali expostos sejam aplicados em cada caso concreto, mesmo durante a transferência internacional de dados pessoais.

Para viabilizar a transferência internacional de dados pessoais, a regra é de que a instituição sujeita à legislação australiana exija do destinatário transnacional o cumprimento dos APPs. Caso isso não seja possível, é necessário o consentimento prévio do titular dos dados pessoais para a transferência. Trata-se de um formato que envolve a combinação de fatores como o livre fluxo transnacional de dados, o consentimento e a accountability, o que pode ser considerado como um modelo de corregulação bastante equilibrado em várias fontes.

Entende-se por destinatário transnacional qualquer instituição ou indivíduo que recebe dados pessoais de alguém submetido à legislação australiana e, por conseguinte, (i)

não esteja estabelecido em território australiano, (ii) não seja uma filial estrangeira da própria instituição que está transferindo os dados pessoais e (iii) não seja alguém a quem os dados pessoais se referem.

Cumpre realçar que, mesmo na impossibilidade de conformidade com a legislação australiana, o consentimento não precisa ser obtido em toda e qualquer singular transferência internacional de dados pessoais. Ainda assim, o consentimento deve ser obtido para um envio reiterado do mesmo tipo de dado pessoal. Isso não significa dizer que o consentimento não é relevante, mas sim que a autorização para a operação deve ser solicitada claramente e em momento anterior à transferência[291] e será válida para os envios similares.

É importante observar que a transferência internacional de dados pessoais também poderá ser realizada, sem o consentimento do titular, caso o destinatário transnacional esteja sujeito a uma modalidade de legislação ou *enforcement* que apresente substancialmente o mesmo patamar de proteção dos APPs e respectivos mecanismos de controle. Em outras palavras, o modelo australiano adota em parte o requisito da adequação também presente na GDPR e construído sob o prisma do *geographically-based approach*, analisado no início deste capítulo, que prestigia processos comunicacionais de mesma linguagem e simbologia, sem que sejam necessários ajustes com foco na policontextualidade.

Ademais, caso uma instituição submetida à legislação australiana promova a troca de dados com uma filial sediada em outro país, tal operação não é considerada transferência internacional de dados. Todavia, se o destinatário transnacional não tiver vinculação direta com a organização submetida à legislação australiana, as normas de transferência internacional se aplicam, o que demonstra a predisposição de extraterritorialidade dos reguladores nas vilas globais, em paralelo com a adoção da adequação como requisito de transferência.

Vale observar, entretanto, que o fornecimento limitado de dados pessoais para organizações privadas internacionais com o propósito de prestação de serviços é considerado como uso e não compartilhamento de dados pessoais. Esta perspectiva tem uma relevância expressiva e contribui para tornar o modelo australiano mais simplificado.

---

[291] Cf. **Office of the Australian Information Commissioner - OAIC**.

O *Australian Privacy Act* e os APPs definem o "compartilhamento" como sendo a disponibilização de dados pessoais para alguém alheio a uma organização e a subsequente perda do efetivo controle sobre o dado disponibilizado. Essa disponibilização pode ser voluntária ou acidental, ou seja, não importa a intenção envolvida na disponibilização, mas apenas o acesso e a perda do efetivo controle.

A partir desta premissa, quando há prestação de serviços por um destinatário transnacional e não há qualquer tipo de divulgação a terceiros, tanto durante como após o tratamento dos dados e retorno à organização submetida à legislação australiana, considera-se que houve apenas um uso dos dados pessoais. Nesse caso, não há necessidade de cumprimento dos requisitos legais das APPs quanto ao consentimento. Se, no entanto, ocorrer qualquer falha ou vazamento de dados durante a operação internacional, a organização sujeita à legislação australiana será considerada responsável, pois ainda detinha o controle dos dados.

É exigido das organizações australianas que tomem precauções razoáveis para evitar qualquer tipo de incidente ou vazamento de dados pessoais durante a transferência internacional ou enquanto tais dados estiverem na posse de terceiros localizados em outros países. Essas precauções geralmente se consolidam em arranjos contratuais protetivos, com os seguintes elementos básicos:

> - Descrição dos dados pessoais a serem transmitidos e o propósito dessa transmissão;
> - Exigências de que as entidades internacionais cumpram os requisitos da legislação australiana;
> - Determinação de que as organizações internacionais exijam o cumprimento dos requisitos da legislação australiana de empresas subcontratadas ou terceiros envolvidos;
> - Devido processo de tratamento de queixas relacionadas a incidentes com vazamento de dados; e
> - Requerimento de que as organizações internacionais tenham um plano de contingenciamento para o caso de suspeita de incidentes com vazamento de dados pessoais que inclua notificação imediata e obrigatória a autoridades competentes e medidas de mitigação.

Em suma, caso a entidade internacional não cumpra com os requisitos previstos, a organização sujeita à legislação australiana será considerada responsável. Assim, se de um lado o consentimento para o modelo australiano é dotado de significativa relevância, de outro ele também é capaz de compreender as situações nas quais ele será insuficiente para apresentar as respostas desejadas para a tutela da privacidade e proteção dos dados pessoais.

Por esta razão, o modelo australiano também pode ser considerado como policontextual e aberto às manifestações de pluralismo jurídico norteadas pela *accountability*.

8. O modelo regulatório europeu e suas ambições extraterritoriais: o impacto da GDPR nos demais países

Dentre os modelos analisados, o europeu será aquele com maior dificuldade de compreender as manifestações da policontextualidade e o que mais buscará impor as suas gramáticas simbólicas aos demais *stakeholders* envolvidos no processo de regulação da proteção dos dados pessoais. Aqui se adotará uma postura crítica do modelo europeu, que por meio da adequação e extraterritorialidade buscará impor o seu próprio contexto a todos os atores envolvidos com a regulação.

Apesar da tradição cultural existente na União Europeia e, particularmente, em alguns dos países do continente cujo tema de proteção de dados é mais difundido (Alemanha, França, Espanha, Itália, Reino Unido e Holanda), desde a Diretiva 95/46/CE se busca de algum modo um regime jurídico capaz de harmonizar a livre circulação de dados pessoais e a defesa dos direitos e garantias relacionados à privacidade e proteção de dados pessoais. Desde o início das preocupações das autoridades europeias com proteção de dados em meados de 1970 e após a entrada em vigor da primeira Diretiva em 95, apenas 1% da população no continente europeu utilizava a internet, o que demonstra a pertinência da revisão do marco regulatório que resultou na entrada em vigor, em 2016, da *General Data Protection Regulation* (GDPR)[292].

Desde a entrada em vigor do *Foreign Corruption Practice Act* (FCPA), o mundo não conhecia uma lei com efeitos extraterritoriais tão amplos. Tanto quanto objetiva assegurar a proteção de direitos dos usuários da internet estabelecidos na União Europeia, o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia também revela uma subjacente disputa comercial entre Estados Unidos, Ásia e UE pelo fluxo de dados e comércio eletrônico global, que se expressa por meio do requisito da adequação e da aplicabilidade extraterritorial.

---

[292] JAY *et al*, **Guide to the General Data Protection Regulation**.

Embora aprovada em 2016, somente se tornou plenamente exigível em 25 de maio de 2018. O principal objetivo da GDPR foi influenciar os países membros da União Europeia a ter um regime jurídico uniforme e consistente, capaz de eliminar a discricionariedade de adequação interna, mas sem prejuízo da soberania de cada um deles.[293]

A GDPR tem muitas disposições que guardam semelhança com a legislação anterior, a Diretiva 95/46, porém a grande distinção diz respeito ao valor das multas decorrentes da sua violação: até 4% do faturamento global da empresa ou € 20 milhões. Estima-se que boa parte das empresas europeias poderia ir à falência no cenário atual, caso incorram em alguma violação.

Em linhas gerais, a GDPR é uma norma geral de proteção de dados para toda a União Europeia, mas cada país membro terá a faculdade de dispor sobre determinados temas de acordo com as particularidades culturais e sociais, tal como ocorre na definição da idade mínima para o tratamento de dados de crianças. Embora exista alguma flexibilidade para as leis nacionais, a GDPR tem como objetivo harmonizar o cenário regulatório e empoderar as 28 autoridades de proteção de dados dos países membros.

8.1 Premissas de aplicação da GDPR

A GDPR contempla quatro premissas básicas de aplicação. E aqui já é possível constatar que, além de proteger os direitos dos usuários, a norma tem também por escopo uma clara disputa comercial centrada na imposição de linguagens próprias e de interesses estranhos à policontextualidade. Como primeiro foco, a GDPR se aplica ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um controlador ou de um processador situado no território da UE, independentemente de o tratamento ocorrer dentro ou fora da UE. Para esta primeira hipótese, o fator territorialidade tem um peso expressivo.

A segunda premissa de aplicação da GDPR está relacionada ao tratamento de dados pessoais quando estas atividades estejam relacionadas com a oferta de produtos ou serviços para titulares de dados residentes no território da UE, independentemente da exigência de pagamento.

---

[293] LYNSKEY, **The Foundations of EU Data Protection Law**, p. 7; JAY *et al*, **Guide to the General Data Protection Regulation**.

A terceira premissa de aplicação diz respeito ao monitoramento de comportamentos de indivíduos, desde que estes comportamentos ocorram dentro do território da UE. Em grande medida, ferramentas como *cookies* são as principais responsáveis por estes monitoramentos de perfil do usuário. Esta talvez seja a premissa que mais claramente demonstra os outros propósitos da GDPR.

Por fim, a norma tem ainda um traço interessante da expressão do colonizador europeu, na medida em que a GDPR também se aplica ao tratamento de dados pessoais realizado por uma empresa não estabelecida na UE, mas localizada em algum lugar em que se aplique o direito de um Estado-Membro da EU por força do direito internacional público. Este é o exemplo de países colonizados por membros da União Europeia. Por este prisma, a GDPR poderia ser aplicada em contextos muito distintos do seu, o que revela uma significativa incompreensão da eclosão de fontes do direito em outros subsistemas sociais parciais.

O primeiro dilema enfrentado pela Comissão Europeia no processo de revisão do marco regulatório envolveu a melhor forma de equilibrar o desenvolvimento tecnológico com a amplitude de escopo das políticas públicas da União Europeia, em fase de plena recontextualização. O segundo, por sua vez, esteve relacionado com a dimensão conceitual e normativa que o novo regulamento daria ao regime de proteção de dados e privacidade, na medida em que certamente deveria ter mais densidade do que o anterior.

A localização dos servidores, o local de tratamento dos dados e volume de dados processados deixa de ser um fator preponderante para efeito de aplicação da GDPR, na medida em que as empresas estarão sujeitas à lei sempre que direcionem suas atividades a titulares localizados na União Europeia, por mais que o processamento ocorra fora do continente europeu. Em outras palavras, se de algum modo as vilas globais ganham em perspectiva regulatória referências específicas como a GDPR, por outro o aspecto da territorialidade não é por completo ignorado na tentativa de impor figuras de linguagem próprias aos demais envolvidos no processo regulatório.

A GDPR prevê 6 condições para o processamento de dados pessoais de usuários: o consentimento, a existência de uma relação contratual, uma obrigação legal, interesses vitais, interesses públicos e o legítimo interesse[294]. A despeito da excessiva

[294] JAY *et al*, **Guide to the General Data Protection Regulation**; LYNSKEY, **The Foundations of EU Data Protection Law**.

valorização do consentimento positivo, livre, específico, informado e inequívoco, o fato é que as demais condições de processamento autorizam as operações de processamento com as mesmas condições. Há uma ampliação das formas de tratamento e um nivelamento do consentimento com outros meios de processamento de dados pessoais, numa tentativa de conferir maior controle e empoderamento aos titulares.

No tocante ao processamento de dados de criança, a idade será mínima será aumentada para 16 anos. Abaixo disso, o processamento de dados exigirá a autorização dos responsáveis. Cada jurisdição da UE poderá definir a idade mínima, desde que não fique abaixo dos 13 anos. Vale ressaltar que dados de crianças não se sujeitam à manutenção do armazenamento mesmo após o pedido de exclusão sob o argumento da existência de alguma salvaguarda.

A GDPR tem um enfoque interessante sob a perspectiva de fomento da inovação e conciliação com a privacidade e proteção de dados pessoais. As empresas serão obrigadas a implementar em seus produtos a partir da criação medidas de proteção de dados que ampliem o poder de escolha do usuário e também garantir que mecanismos de proteção adequados sejam incorporados às tecnologias ou produtos já existentes (*privacy by design*).

Um dos principais papéis a ser desempenhado sob a ótica da GDPR é o do controlador de dados, ou seja, a pessoa jurídica ou física responsável pelo tratamento de dados pessoais. Se por um lado os controladores, ou seja, aqueles responsáveis pelo tratamento de dados pessoais dos usuários terão uma responsabilidade maior, por outro lado os processadores, aqueles que processam dados em nome dos controladores, também deverão observar algumas obrigações. Um desses exemplos ocorre em relação ao processador de dados que empregue 250 ou mais pessoas, visto que deverá manter registros detalhados de suas atividades.

Outro relevante passo para a implementação de um modelo de corregulação eficiente foi a previsão da figura de um *Data Protection Officer* (DPO) para empresas responsáveis pelo processamento de um volume significativo de dados ou de dados sensíveis. A figura do DPO será responsável pela eliminação das constantes notificações feitas às autoridades reguladoras no modelo da Diretiva 95/46[295]. O DPO será responsável por monitorar as atividades de processamento de dados, além de ser o ponto de contato com as

[295] LYNSKEY, **The Foundations of EU Data Protection Law**; MURRAY, **Information technology law**.

autoridades reguladoras em casos de implementação de novas tecnologias após prévia análise de risco (*Privacy Impact Assessment*) e incidentes de vazamentos. O papel do DPO monstra como é possível a centralização em atores privados de atividades regulatórias como a fiscalização e controle, contato que a *accountability* seja a diretriz de atuação subjacente ao tratamento de dados pessoais.

Um dos fatores de maior preocupação do GDPR envolve o prazo de notificação das autoridades reguladoras em casos de incidentes de vazamento de dados. O GDPR impõe que as empresas envolvidas devem realizar a notificação o mais rápido possível ou, no máximo, 72 horas após o incidente ser identificada. O cumprimento de um prazo tão exíguo em casos de incidentes de vazamento de dados de proporções transnacionais pode não ser factível. Mobilizar uma rede de investigação, apoio técnico-operacional e jurídico em várias jurisdições a ponto de responder dentro do prazo será um desafio. Por isso, construir uma rede de contatos será um passo importante para empresas transnacionais. Como primeira medida, o mais relevante é que as empresas sejam capazes de demonstrar que adotaram medidas para a identificação dos dados comprometidos, mitigação dos danos e aprimoramento de ferramentas de cibersegurança.

Conforme apontado no início deste tópico, com a eclosão de vilas globais como fruto da globalização e da queda das fronteiras físicas, as transferências internacionais se tornam o ponto de maior interesse do mercado. Isso porque as transferências de dados para países fora da UE somente poderão ser feitas para os que tenham requisitos de adequação aprovados pela Comissão da União Europeia e sejam capazes de prover o mesmo nível de proteção (*adequacy*). Na América do Sul, apenas Uruguai e Argentina são reconhecidos pela UE em razão do requisito da adequação. E embora tenham sido reconhecidos sob a égide da Diretiva 95/46, não se sabe se nos próximos 4 anos serão capazes de promover as adaptações necessárias para manter o reconhecimento e o fluxo comercial com a União Europeia.

Mediante a análise do consentimento e das transferências internacionais sob a a égide da GDPR será possível avaliar a forma como o marco regulatório europeu contém traços muito peculiares de corregulação, porém com pouca abertura para a policontextualidade e diálogo com fontes do direito que não sejam aquelas admitidas pelo poder público.

8.2 A GDPR e a dimensão do consentimento do titular dos dados

O consentimento continua a ser uma das seis bases legais para o processamento de dados pessoais,[296] todavia somente será considerado apropriado se o titular dos dados puder exercer o controle e tiver condições de recusar ou revogar o consentimento a qualquer momento. Vale observar que, se o responsável pelo tratamento optar por adotar o consentimento como sua base legal válida para as operações a serem realizadas, ele deve estar preparado para aceitar a escolha do titular e interromper a atividade se houver a revogação do consentimento[297]. Em outras palavras, se isto ocorrer em concreto, o responsável pelo tratamento não pode simplesmente trocar o consentimento revogado por outra base legal. Assim, não se admite a troca retroativa para o interesse legítimo ou outra base caso o consentimento seja revogado. Por força da exigência de divulgar a base legal com a qual atua antes do momento da coleta dos dados pessoais, o responsável pelo tratamento já deve ter sido capaz de tomar esta decisão.

O consentimento deve ser expresso e o uso de ferramentas de seleção *opt-in* deve ser a regra, de maneira que as escolhas não sejam pré-marcadas (*opt-out*), salvo se fundadas em relação jurídica anterior. Por esta razão, muitos dos pedidos de renovação do consentimento que usuários receberam às vésperas da entrada em vigor da GDPR eram desnecessários – afinal fundados em relação jurídica anterior com o usuário – ou incapazes de sanar a forma irregular pela qual os dados foram anteriormente obtidos[298].

Por esta razão, o consentimento precisa ser genuíno e capaz de atender os requisitos estabelecidos pela GDPR, sob pena de ampliar a exposição do controlador dos dados e ser considerado uma base inválida para o tratamento. Por outro lado, a obtenção do

---

[296] Artigo 6.o Licitude do tratamento

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

[297] WORKING PARTY 29, **Opinion 3/2010 on the principle of accountability**.

[298] *Ibid*.

consentimento válido não diminui o ônus do controlador em relação às demais obrigações legais e tampouco o autoriza a coletar mais dados do que necessário e para finalidades diversas.

A GDPR define consentimento como qualquer indicação afirmativa de vontade do titular dos dados fornecida de forma livre, específica, inequívoca e informada, mediante a qual é expressa a concordância com o processamento dos seus dados pessoais. Em linhas gerais, as diretrizes do consentimento da GDPR são muitos semelhantes às da Diretiva 95/46/CE. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva a fins múltiplos, deverá ser dado um consentimento para todos esses fins.

Quando o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá ser capaz de comprovar a integridade do consentimento dado para a operação e sua extensão. Além de fornecida de uma forma inteligível e de fácil acesso, com linguagem clara, simples e sem cláusulas abusivas, o titular dos dados deve ser capaz de identificar o responsável pelo tratamento e as finalidades a que se destina. Uma das principais preocupações da GDPR envolve as condições em que o consentimento é fornecido, ou seja, se a desigualdade de condições influencia sobremaneira nas escolhas dos titulares dos dados, o consentimento não deverá ser considerado uma base legal válida, na medida em que será improvável que tenha sido concedido de forma livre. Ademais, é possível presumir que o consentimento não foi fornecido de modo livre se o titular dos dados não puder dá-lo separadamente para as diferentes operações de tratamento em curso.

A rigor, a prestação de um serviço pode envolver várias operações de processamento e ser revestida de mais de uma finalidade. Em tais casos, os titulares dos dados devem ter a liberdade para escolher para quais das finalidades especificadas aceitam o processamento dos seus dados. Assim como na Austrália, a figura do "*bundled consent*" não é admitida pela GDPR na medida em que o consentimento deve ser granular. Por esta razão, em alguns casos a granularidade do consentimento será essencial para a prévia prestação de serviços distintos. Se o responsável pelo tratamento estiver diante de operações com finalidades distintas e não tiver obtido o consentimento para cada uma delas, ficará evidente a ausência de liberdade do titular dos dados. Assim, quando o processamento de dados envolve

várias finalidades e operações, o caminho para cumprir as condições de obtenção do consentimento válido é a granularidade, ou seja, a separação dessas finalidades e a obtenção do consentimento para cada uma delas. Se estivermos diante de várias operações, porém todas com a mesma finalidade, um único consentimento é suficiente. Por conseguinte, a fusão de consentimento específico com finalidade determinada é o que demonstra o grau de liberdade do titular dos dados e evita a ampliação gradual e o desvio de propósito em virtude da implementação de novas tecnologias ou funcionalidades, prática conhecida como *function creep*[299].

Vale observar ainda que o responsável pelo tratamento precisa demonstrar que é assegurado ao titular dos dados o direito de recusar ou retirar o consentimento sem incorrer em qualquer custo ou desvantagem para quem assim o desejar. A GDPR não impede que sejam suprimidos incentivos, mas o ônus de provar que mesmo assim o consentimento foi livremente concedido recai sobre o responsável pelo tratamento dos dados. Para assegurar que o consentimento seja considerado informado, é necessário que o responsável pelo tratamento comunique o titular dos dados sobre certas informações antes que manifeste a sua escolha, como por exemplo:

> - a identidade do responsável (controlador);
> - o objetivo de cada uma das operações de tratamento para as quais solicita o consentimento;
> - que tipo de dados serão coletados e usados;
> - o exercício do direito de revogar o consentimento;
> - informações sobre a utilização dos dados para a tomada de decisões automatizada;
> - possíveis riscos decorrentes de transferências de dados para outros países por falta de uma decisão de adequação e adoção de salvaguardas.

A GDPR não prescreve a forma ou formato em que as informações devem ser fornecidas para cumprir o requisito do consentimento informado. Informações válidas podem ser apresentadas em várias formas, como declarações escritas ou orais, ou mensagens de áudio

---

[299] Sobre *creepy function,* Tene e Polonetsky esclarecem que "there seems to be a category of cases where corporate behavior is labeled "creepy" for lack of better word. These cases often do not involve breach of any of the recognized principles of privacy and data protection law. They include activity that is not exactly harmful; does not circumvent privacy settings; and does not exceed the purposes for which data were collected. They usually involve either the deployment of a new technology or new use of an existing technology; the implementation of a feature that eliminates obscurity; or an unexpected data use or customization. In certain cases, "creepy" behavior "leans in" against traditional social norms; in others, it exposes a rift between the norms of engineers and marketing professionals and those of the public at large; and in yet others, social norms have yet to evolve in order to mediate a novel situation. TENE, Omer; POLONETSKY, Jules, A Theory of Creepy: Technology, Privacy and Shifting Social Norms, **Yale Journal of Law and Technology**, v. 16, 2013.

ou vídeo. A GDPR exige que o consentimento seja concedido por um ato afirmativo claro (*opt in*), ou seja, uma demonstração de que o titular dos dados por meio de uma ação deliberada concordou com o tratamento específico. Isso significa, portanto, que não se admite o consentimento implícito ou inferido ou que o silêncio possa ser admitido como. Por outro lado, embora a GDPR seja omissa a respeito, o consentimento deve ser sempre obtido antes que o responsável pelo tratamento inicie o processamento de dados pessoais para o qual o consentimento é necessário.

Finalmente, o responsável pelo tratamento deve manter um registro das declarações de consentimento recebidas para que ele possa comprovar como e quando o consentimento foi obtido. O responsável deve ser capaz de demonstrar que o titular dos dados foi informado e o fluxo de tratamento atende a todos os critérios relevantes para um consentimento válido (*accountability*). Em resumo, o consentimento ainda tem um papel relevante para o modelo europeu, que o considera a melhor forma de controle e empoderamento do titular dos dados pessoas em face dos responsáveis pela atividade de tratamento.

8.3 As transferências internacionais na GDPR: supervisão estatal e suas exceções

De acordo com a GDPR, as transferências internacionais somente podem ocorrer quando existente um nível adequado de proteção aos titulares dos dados pessoais. As avaliações sobre os parâmetros de adequação devem ser realizadas pela Comissão Europeia ou pelos responsáveis pelo tratamento que desejam transferir dados pessoais para fora União Europeia. Conforme mencionado anteriormente, esta representa uma forma de controle relevante sobre o fluxo informacional e uma medida efetiva de impor a sua própria linguagem às demais vilas globais, sem observar a autonomia dos subsistemas parciais e a policontextualiadade.

A Comissão Europeia considera vários países como capazes de garantir um nível adequado de proteção em razão de sua legislação interna ou dos compromissos internacionais assumidos. Os critérios gerais de adequação para as transferências internacionais devem considerar:

- a natureza dos dados pessoais transferidos;
- o objetivo da transferência proposta;
- o período durante o qual os dados pessoais serão processados;

> - medidas de segurança a serem tomadas em relação aos dados pessoais transferidos para outro país;
> - o país de origem dos dados pessoais; e
> - o país de destino final dos dados pessoais.

Na ausência de uma decisão de adequação por parte da Comissão Europeia, os dados pessoais ainda podem ser transferidos por uma empresa estabelecida na União Europeia para outra fora do bloco, desde que observadas certas condições:

> - Adoção de salvaguardas mediante a celebração de cláusulas-padrão,[300] contratos-padrão e normas corporativas vinculantes aprovadas pela Comissão Europeia;
> - Adoção de uma das derrogações previstas desde que a transferência não seja reiterada, massiva ou estrutural, além de não poder ser realizada por meio de uma salvaguarda. Dentre as derrogações se incluem o consentimento, conclusão ou execução de um contrato ou exercício de defesa em processos judiciais.

As cláusulas-modelo ou cláusulas-padrão e contratos-padrão são mecanismos que visam assegurar as transferências internacionais entre exportador e importador de dados em conformidade com a GDPR. As cláusulas-modelo são utilizadas entre parceiros comerciais que não integram o mesmo grupo econômico e objetivam conferir garantias aos titulares dos dados em relação aos danos que venham sofrer.

As normas corporativas vinculantes ou *binding corporate rules* (*BCRs*) destinam-se a permitir que empresas multinacionais transfiram dados pessoais da União Europeia para os seus afiliados localizados fora do bloco[301]. As BCRs também devem ajudá-lo a adotar padrões sobre proteção de dados e privacidade, bem como aumentar a conscientização dentro da organização. Parte essencial do processo de homologação de uma BCR é a exigência de que o requerente demonstre como os seus funcionários nas filiais em países fora da União Europeia observam as diretrizes corporativas sobre proteção de dados e privacidade. Embora seja uma medida que prestigia o fluxo informacional, a rigor ela sempre parte da mesma perspectiva de

---

[300] Commission Decision 2001/497/EC, 14 dated 15 June 2001 – in which the Commission approved model clauses for transfers from data controllers in the EEA to data controllers outside the EEA (Set I controller-controller). Commission Decision 2002/16/EC, 15 dated 27 December 2001 – in which the Commission approved model clauses for transfers from data controllers in the EEA to data processors outside the EEA (controller-processor). Commission Decision 2004/915/EC, 16 dated 27 December 2004 – in which the Commission approved an alternative set of model clauses for transfers from data controllers in the EEA to data controllers outside the EEA (Set II controller-controller).

[301] WORKING PARTY 29, **Explanatory Document on the Processor Binding Corporate Rules**, Bruxelas: WP29, 2013.

comunicação que é aquela definida pelos reguladores europeus, ou seja, nota-se uma clara tentativa de sobreposição de um modelo regulatório aos demais, sem admitir as contribuições que poderiam receber de outros atores.

Vale destacar que as transferências para organizações estabelecidas nos EUA, amparadas pelo acordo internacional denominado Safe Harbor, foram consideradas adequadas em conformidade com a Decisão 2000/520/CE da Comissão Europeia, de 20 de julho de 2000. No entanto, esta decisão de adequação foi invalidada pela Corte Europeia de Justiça em 6 de outubro de 2015 e, como resultado, as transferências para os EUA não puderam mais ocorrer sob este acordo.

Em 2 de fevereiro de 2016, a Comissão Europeia e os Estados Unidos celebraram um novo acordo para transferências internacionais de dados, o *Privacy Shield*, que substituiu o *Safe Harbor*, que levou à adoção de uma nova decisão de adequação pelo Comissão Europeia, adotada oficialmente em 12 de julho de 2016, para transferências para organizações dos EUA que assinam o *Privacy Shield*. Trata-se de uma tentativa da União Europeia de estabelecer um canal de comunicação que simultaneamente preserve a sua capacidade de controle sobre atividades com tratamento de dados pessoais de um lado e, de outro, mantenha o fluxo comercial com um dos seus principais parceiros econômicos.

Curioso notar como o modelo regulatório europeu tem dois pesos: ora busca construir pontes de conexão com modelos que considera relevantes para a sua atividade econômica, ainda que tenha que passar por ajustes para melhor se configurar à policontextualidade exigida - como na relação com Estados Unidos - ora simplesmente se impõe aos demais e ignora as particularidades e autonomia das demais vilas globais e atores que nelas atuam.

9. A aprovação da Lei Geral de Proteção de Dados no Brasil: virada cultural ou promessa?

Até meados de agosto de 2018, o Brasil era um dos poucos países entre as principais economias globais a não ter um marco regulatório de proteção de dados pessoais, ou seja, era um ator de menor expressão no tema ainda que com regulações esparsas como o Marco Civil da Internet, Código Civil e o Código de Defesa do Consumidor. Além de ter sido uma das últimas democracias da América Latina a ter um marco regulatório de proteção de

dados pessoas, a legislação brasileira pode ser considerada como um transplante legal da GDPR[302], na medida em que muitos dos seus pontos são frutos de inspiração do modelo europeu, dada a pressão comercial pela manutenção das relações com aquele bloco, conforme se observa na tabela abaixo:

GDPR	**LGPD**
Consentimento deve ser: • Prévio • Livre • Informado • Específico • Indicação inequívoca por declaração ou ação afirmativa	Consentimento deve ser: • Prévio • Livre • Informado • Para uma finalidade determinada • Inequívoco • Por escrito ou outro meio que demonstre a vontade do titular
Se para dados sensíveis, também deve ser: • Explícito	Se para dados sensíveis, também deve ser: • Específico • Em destaque
Consentimento pode ser revogado, a qualquer tempo.	Consentimento pode ser revogado, a qualquer tempo.
Consentimento deve ser manifestado de maneira apartada de outros termos.	Consentimento deve ser manifestado de maneira apartada de outros termos.

A Lei Geral de Proteção de Dados (LGPD) foi publicada no dia 15 de agosto de 2018 e somente entrará em vigor em agosto de 2020, ainda com uma grande expectativa em torno da sua capacidade de compreender a policontextualidade do processo regulatório e dialogar com as diversas manifestações do direito nas vilas globais.

A despeito das disposições introduzidas pelo Marco Civil da Internet e seu decreto regulamentador sobre os comportamentos na rede, consentimento e compartilhamento de dados pessoais, a LGPD representa um rompimento cultural mais incisivo, capaz de atingir os mais diversos setores da economia (usuários, desenvolvedores, poder público e iniciativa

[302] LEGRAND, Pierre, Impossibility of Legal Transplants, The, **Maastricht J. Eur. & Comp. L.**, v. 4, p. 111, 1997; MATTEI, Ugo, Efficiency in legal transplants: An essay in Comparative Law and Economics, **International Review of Law and Economics**, v. 14, p. 3–19, 1994.

privada), numa importante tentativa de introduzir valores voltados à transparência e *accountability*.

Por se tratar de uma lei com características exponenciais, sempre capaz de exigir um contínuo aprimoramento e adequação aos seus requisitos, a LGPD ainda é revestida de grande incerteza. A sua tentativa de compreender os diversos subsistemas sociais parciais merece destaque, embora ainda careça de comprovação empírica a efetividade como conduzirá o tratamento de dados realizado pelo poder público, o regime de proteção dos dados sensíveis, a forma como viabilizará as transferências internacionais de dados e o espaço que deixará para a regulação privada.

Fruto de um processo legislativo longo - afinal, foram quase oito anos de tramitação dos projetos de lei no Congresso Nacional - , marcado por expressiva disputa de interesses entre órgãos de fiscalização e controle de um lado e setor tecnológico de outro, ainda é prematuro indicar os concretos avanços a serem obtidos com o novo marco regulatório. Parte dessas incertezas decorre do modo como a lei foi aprovada, do veto presidencial originário à criação da Autoridade Nacional de Proteção de Dados e a posterior edição de uma medida provisória, no último dia do mandato presidencial, para efetivamente criá-la na forma de um órgão vinculado à Casa Civil da Presidência da República, despido de autonomia financeira, administrativa e orçamentária.

A mudança cultural a ser imposta pela LGPD pode ser percebida pela principiologia que confere substrato normativo à lei. Com cerca de dez princípios gerais, dentre os quais os da finalidade, necessidade, livre acesso, transparência, segurança, responsabilização e prestação de contas se destacam, a LGPD tem como objetivo reequilibrar o jogo de forças, ampliar a transparência, responsividade e empoderar os titulares dos dados pessoais em suas interações no ciberespaço. Se o excessivo alinhamento com o modelo europeu permitirá a efetiva transformação cultural que se pretende somente o tempo dirá. Se o modelo brasileiro terá condições de compreender a policontextualidade do processo regulatório e admitirá manifestações espontâneas do direito para além da regulação estatal também é algo incerto.

Apesar disso, a análise do consentimento e das transferências internacionais de dados demonstrará que ainda é possível superar o anseio hegemônico de regulação do modelo europeu, de modo a admitir a participação dos atores e as manifestações de pluralismo

jurídico necessárias para uma melhor efetividade da tutela da privacidade e proteção dos dados pessoais.

9.1 A proximidade da LGPD com o regime da GDPR de transferências internacionais

Parte da explicação sobre o alinhamento da LGPD com a GDPR decorre da preocupação e interesse em manter o contínuo fluxo comercial com a União Europeia, numa clara sujeição ao modelo de linguagem e regulação parcial dos subsistemas sociais. Muitos sustentam que se o modelo brasileiro de transferência internacional discrepasse das condições e requisitos da GDPR, certamente o Brasil permaneceria sem o reconhecimento da adequação e as transferências somente poderiam ser realizadas mediante a adoção de salvaguardas pelas empresas (BCRs, cláusulas-padrão, contratos-tipo, certificações e códigos de conduta), o que impactaria no custo das operações. A rigor, a LGPD inovou apenas naquilo que considerou possível ou particular à realidade do país, ou seja, o tratamento de dados realizado pelo poder público, que administra as bases de dados mais relevantes dos cidadãos.

O capítulo de transferência internacionais da LGPD revela uma especial atenção do legislador. Tal preocupação pode ser explicada pelo fato de que, caso os dados pessoais de um dado titular sejam coletados no Brasil, transferidos e tratados em outra jurisdição, os referidos dados poderão estar sujeitos a outras legislações – as quais poderão ser mais brandas e menos protetivas dos direitos dos titulares dos dados, se comparadas à futura legislação brasileira. Neste ponto, a LGPD em muito se aproximou da incompreensão incorrida pelo modelo europeu, na medida em que replica o discurso da imposição da sua linguagem e parâmetro a todos os demais atores que conjuntamente participam do processo de regulação nas vilas globais.

Outra explicação para o cuidado da LGPD com as transferências internacionais envolve as questões de territorialidade (*data localization* ou *data residency request*)[303] e seus impactos no *enforcement* pelas autoridades de segurança pública, que acreditam que os dados pessoais deveriam sempre ser armazenados no país para viabilizar o acesso nos casos de investigações criminais e assegurar a imposição de sanções. A despeito da concepção emancipatória da regulação segundo os parâmetros da policontextualidade manifestado nas

[303] SCHWARTZ, Legal Access to the Global Cloud.

vilas globais, o fenômeno da territorialidade ainda é também muito presente no Brasil. Embora o Marco Civil tenha abandonado a necessidade de que empresas estejam estabelecidas no Brasil ou que os dados aqui sejam armazenados, outros atos normativos como a Portaria GSI n. 9/2018[304] e as consultas públicas do Banco Central para a edição da IN CMN 4658/18[305] e da CVM[306] para a alteração da IN CVM 505/11[307] revigoraram o tema da territorialidade para impor exigências de armazenamento no país.

Como forma de tentar equilibrar esse debate, a LGPD optou por adotar o regime da extraterritorialidade ampla da sua aplicabilidade ao invés de se ocupar de exigências territoriais que se mostram incapazes de apresentar soluções plausíveis para regular as empresas de tecnologia. Assim, operações de tratamento de dados realizadas dentro do território brasileiro estão invariavelmente sujeitas à aplicação da LGDP. Além de operações realizadas dentro do país, quando o tratamento tiver por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no território brasileiro, a lei também será aplicável, ainda que a organização responsável por essa atividade esteja sediada ou localizada fora do país. Assim, o local onde os dados são tratados não é requisito único ou preponderante para aplicação da lei, sendo também importante identificar a localização do indivíduo cujos dados serão coletados.

É evidente, portanto, a reprodução dos mecanismos de transferências internacionais de dados da GDPR por parte da LGPD e a adoção do *geographically-based approach*. Para não se mencionar que o modelo brasileiro é uma cópia fiel da GDPR, cumpre esclarecer que em dois pontos relevantes deixou-se de seguir a legislação europeia. Primeiro, o Brasil não coloca como obrigatória a designação de um representante no Brasil quando o responsável pelo tratamento dos dados (controlador) aqui não esteja estabelecido no país, o que representa um sério risco à efetiva fiscalização e imposição das sanções previstas na lei. Segundo, ao contrário da GDPR, o Brasil não previu derrogações ao regime legal de transferência de dados, como aquelas pertinentes às transferências não reiteradas, massivas ou

---

[304] 5.3 Deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, bem como suas cópias de segurança, residam em território brasileiro;

[305] Edital 57/2017, https://www3.bcb.gov.br/audpub/DetalharAudienciaPage?4

[306] Art. 36. § 2º Os prestadores de serviços responsáveis pelos documentos digitalizados e as cópias de segurança dos documentos digitalizados devem estar sediados no país ou em países signatários dos Memorandos Multilaterais de Entendimento da IOSCO (MMoU)."(NR)

[307] Cf. file:///C:/Users/ts04233/Desktop/sdm0518Edital_com_minuta.pdf

estruturais, ou realizadas mediante o consentimento, conclusão ou execução de um contrato ou exercício de defesa em processos judiciais.

Se de um lado a LGPD acena com a percepção do impacto regulatório causado pelas vilas globais ao substabelecer o regime de extraterritorialidade, por outro o Brasil sequer olhou para modelos de transferência internacional mais aptos a estimular a *accountability* e dotados de fórmulas mais dinâmicas capazes de harmonizar o processo de inovação tecnológica com a proteção de direitos, tal como se observa em relação à APEC, o Canadá, a Austrália e as práticas implementadas pela FTC.

Um modelo responsivo e inovador, capaz de compreender as manifestações de pluralismo jurídico e as autonomias das redes de comunicação, com a devida mescla da corregulação e autorregulação, mediante o estabelecimento de normas gerais de proteção de dados e maior margem para atuação da iniciativa privada, poderia assegurar um ambiente mais condizente com a realidade brasileira. Se assim como aconteceu com a Austrália em 2000 e até agora com o Reino Unido, ainda não reconhecido por prover adequação em virtude do BREXIT, o Brasil estará atrás de países cujos modelos regulatórios contém particularidades identificadas com suas realidades, mas nem por isso com óbices à continuidade das relações com União Europeia. Para que o Brasil ingresse com altivez no cenário regulatório global de proteção de dados pessoais e atinja um patamar de fomento tecnológico semelhante ao dos países desenvolvidos, seria importante a adoção de modelos regulatórios mais equilibrados como os da Australia e Canadá.

9.2 O papel do consentimento na LGPD em comparação com as demais bases legais

A despeito de a LGPD prever dez bases legais para o processamento de dados pessoais contra seis da GDPR, o consentimento em ambas as leis tem um regime jurídico semelhante e é um requisito indispensável à coleta, salvo as exceções expressamente previstas em lei. A LGPD parte do pressuposto de que o titular dos dados poderá definir antes da coleta, a seu exclusivo critério e por meio do consentimento, se um agente poderá ou não realizar quaisquer atividades de tratamento de seus dados pessoais. Ou seja, a LGPD ainda atribui um peso considerável ao consentimento, ignorando as complexidades do processo regulatório nas vilas globais, que nem sempre viabilizam a obtenção do consentimento com transparência e efetividade.

A LGPD optou por seguir um modelo de consentimento qualificado, cujas condicionantes são que ele seja prévio, livre, informado, específico, inequívoco e por escrito ou por outro meio capaz de demonstrar a vontade do titular.

> - *Prévio e Livre*: sendo facultado ao titular dos dados conceder ou não o consentimento sem qualquer tipo de sanção ou obrigação imposta pelo controlador com quem o titular dos dados se relaciona. O consentimento genuinamente livre pressupõe a liberdade e a não coação (física ou moral) para que o titular dos dados possa decidir sobre os limites do tratamento;
> - *Específico e Informado*: no sentido de que o titular dos dados deve ter ciência de quais dados serão coletados, a finalidade e os possíveis riscos, consequências e/ou implicações de tal tratamento. O consentimento informado possibilita ao titular de dados avaliar previamente a dimensão da atividade de tratamento; e
> - *Inequívoco*: isto é, o titular deverá ter pleno conhecimento de que está autorizando determinado tratamento de dados. O silêncio não importa no consentimento, mas há controvérsia se o consentimento inequívoco exige necessariamente uma conduta afirmativa, de modo a ser compatível com o comportamento concludente. Somente quando criada a Autoridade Nacional de Proteção de Dados se poderá ter clareza sobre a admissão do comportamento concludente. A ciência inequívoca do tratamento de dados está relacionada à expectativa do titular em uma relação determinada e específica.

A rigor quanto mais qualificado o consentimento, maiores as dificuldades para a sua obtenção e os óbices ao fluxo informacional, o que pode representar um incentivo para que outras bases legais sejam utilizadas ou ainda que o consentimento perca a densidade normativa necessária. Quanto mais propenso a novas exigências, maiores as chances de que o consentimento não seja o elemento de acoplamento estrutural das operações de tratamento, o que demandará a identificação de outros mecanismos para assegurar padrões mínimos de transparência e responsividade. Essa será uma das críticas ao consentimento a ser analisada no capítulo 4.

Com relação ao tratamento de dados pessoais sensíveis, a LGPD prevê oito bases legais contra dez da GDPR. Para os dados sensíveis, além dos requisitos gerais acima descritos, o consentimento precisa ser específico e em destaque. Os dois adjetivos finais são uma particularidade deste tipo de operação. O consentimento específico estabelece a necessidade de fornecimento de informações claras, granulares e delimitadas sobre as atividades de tratamento de dados pretendidas, enquanto que o consentimento em destaca implica em uma conduta afirmativa ou indicação assertiva de que o titular dos dados autorizou o tratamento de dados. A exigência de consentimento específico e em destaque neste tipo de operação elimina a possibilidade de qualquer forma de comportamento

concludente, consentimento tácito ou implícito, ou ainda de qualquer aceitação passiva de tratamento de dados[308].

Outro aspecto relevante a ser destacado envolve a necessidade de que o consentimento seja prévio. Seria essencial compreender que nem sempre a obtenção prévia do consentimento é uma medida factível, o que significa que deveria ser admitido posteriormente de acordo com as circunstâncias da operação e em condições excepcionais. Uma alternativa seria dispensar a obtenção do consentimento e escolha antes da coleta ou do uso de dados quando (i) relacionados com práticas inerentes ao contexto da operação; (ii) vinculados à relação existente entre a organização e o titular; e quando (iii) requerido ou autorizado por lei.

A rigor, a imposição de mecanismos de *accountability*, transparência, escolha e sistemas operacionais acessíveis (*privacy by design* e *privacy by default*) são mais eficientes na proteção da privacidade do que a simples ampliação da camada de requisitos em torno do consentimento.

Em comparação com os modelos anteriormente analisados, o Brasil tem preferido adjetivar o consentimento sob a falsa pressuposição de que tal medida poderá ampliar as garantias e proteção de direitos. A forma como o Canadá e a Austrália optaram por exceções ao consentimento e, por outro lado, como a APEC decidiu por não o adjetivar demonstra que é possível a adoção de outras fórmulas eficazes para assegurar tanto a proteção de dados quanto o fomento ao desenvolvimento tecnológico.

Nesse capítulo foram analisados os modelos regulatórios associados à proteção de dados em concreto e a forma como dialogam com o referencial teórico do pluralismo jurídico surgido nas vilas globais. Por meio da análise específica de quatro macro modelos – regulação estatal, regulação setorial, corregulação e autorregulação – se identificou os pontos de contato com a regulação em países como Canadá, Austrália e membros da APEC, de maneira a demonstrar que a policontextualidade é o elemento capaz de conferir maior dinamicidade, efetividade e tutela da privacidade e proteção dos dados pessoais. Da mesma forma, por meio do recorte realizado em torno do consentimento e transferências internacionais de dados buscou-se uma análise transversal de como o pluralismo jurídico pode

[308] MENDES, Laura Schertel; DONEDA, Danilo, Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016, **Revista de Direito Civil Contemporâneo-RDCC (Journal of Contemporary Private Law)**, v. 9, p. 35–48, 2017.

ser conciliado com outras manifestações da atividade regulatória, em especial quando a transparência e a *accountability* atuam com arranjos contratuais para viabilizar o acoplamento estrutural.

No próximo capítulo a análise regulatória descerá mais um degrau. O foco agora será o conteúdo regulado, ou seja, o resultado da atividade regulatória, seja ela fruto exclusivo da expressão da regulação estatal ou resultado da harmonização de modelos como a corregulação e a autorregulação. Por meio da compreensão de elementos como anonimização, dados pessoais e vigilância será possível reunir as premissas básicas para se conjugar o conteúdo regulado pelo prisma da policontextualidade nas vilas globais com o papel desempenhado pela *accountability* enquanto substrato da *Lex Privacy*.

CAPÍTULO 3 - O CONTEÚDO REGULADO DA PROTEÇÃO DE DADOS E PRIVACIDADE

1. Em busca de um conceito de privacidade?

Um dos mais inquietantes aspectos de análise da proteção de dados e da privacidade envolve a tentativa de se delimitar um conceito adequado para tutelar a esfera de proteção individual. Neste capítulo será analisado o produto da regulação, ou seja, alguns temas sobre os quais a atuação regulatória conferiu contornos policontextuais e suas consequências sob o prisma do pluralismo jurídico. A análise do produto da regulação será a forma de demonstrar como o sistema de proteção de dados e privacidade tem sido construído de forma plural e invariavelmente sob a premissa da *accountability*[309].

Por esta razão, mais do que assumir como válidas teorias sobre a privacidade e proteção de dados, neste capítulo se demonstrará como a categoria dos dados pessoais foi concebida, sua interação com a autonomia no ciberespaço e porque ela deve ser protegida. Além disso, serão apresentados elementos de expressão regulatória híbrida, como os dados anonimizados, pseudonimizados e os papéis do controlador e do processador no âmbito regulado, que indicarão a dimensão da policontextualidade nas vilas globais.

Para os autores que se propõem construir um modelo normativo de proteção da privacidade e proteção de dados, esta tarefa parece ser fundamental, como se percebe do esforço de Daniel Solove[310] em apontar as falhas das principais formulações teóricas desde Warren e Brandeis[311]. Conceituar impõe delimitar, excluir, segregar fatores de composição cultural de soluções apriorísticas e temporais. Mas por que desenvolver um conceito de

---

[309] SCOTT, Accountability in the Regulatory State; SCHWARTZ; SOLOVE, PII Problem.

[310] Solove analisa as seis principais correntes teóricas: (i) o direito de ser deixado só (right to be let alone) de Warren e Brandeis; (ii) acesso limitado e o (iii) segredo de Ruth Gavison; (iv) controle sobre a informação pessoal de Alan Westin; (v) pessoalidade e (vi) intimidade. SOLOVE, Daniel J., **Understanding privacy**, [s.l.]: Harvard university press Cambridge, MA, 2008, p. 13; 38.

[311] WARREN, Samuel D.; BRANDEIS, Louis D., The right to privacy, **Harvard law review**, p. 193–220, 1890, p. 195–196. Análises evolutivas da privacidade também podem ser encontradas em Hirshleifer, que acreditava que " I will be contending that the mainland of "privacy" is not the idea of secrecy as our pioneers appear to believe-secrecy is only an outlying peninsula" (HIRSHLEIFER, Jack, Privacy: Its origin, function, and future, **The Journal of Legal Studies**, v. 9, n. 4, p. 649–664, 1980, p. 650.)

privacidade tornou-se um fetiche de parte da doutrina[312]? Estará a proteção da privacidade condicionada à apresentação de um modelo historicamente contextualizado e evolutivamente aprimorado de privacidade[313] ou se trata de um conceito normativo e contextual?[314]

Embora esta tese não tenha a pretensão de adotar um conceito específico e não compartilhe da segmentação estanque entre os elementos característicos de cada uma das teorias desenvolvidas em torno da conceituação do direito à privacidade[315] - razão pela qual não serão analisadas com o fim de apontar a mais consistente - , não se pode desconsiderar que a corrente de Alan Westin foi certamente uma das mais influentes e versáteis em virtude da associação à ideia de controle da informação[316]. Por outro lado, a vertente desenvolvida por Ruth Gavison é aquela mais próxima das características e inflexões pertinentes ao ciberespaço pelo fato de considerar a privacidade em linha de perspectiva com o segredo, o anonimato e a solidão[317]. Esse é o principal motivo pelo qual nessa tese se sustenta a necessidade de se regular a proteção dos dados pessoais, isto é, a proteção da esfera de autonomia das escolhas individuais nos subsistemas sociais parciais frente ao avanço da tecnologia de processamento de informações em larga escala.

Como toda e qualquer pretensão de esgotamento da dinamicidade e de depuração da historicidade cultural de uma categoria jurídica[318], o excessivo apego à

---

[312] MILLER, Arthur Raphael, **The assault on privacy: computers, data banks, and dossiers**, Michigan: University of Michigan Press, 1971, p. 35.

[313] Para um estudo evolutivo do Direito Privado e suas categorias jurídicas, cf. WATSON, Alan, **Legal transplants and European private law**, [s.l.]: Metro Maastricht, 2000, p. 126., que destaca a relevância de se compreender a distinção entre análise histórica legal e análise evolutiva das categorias jurídicas, tal como Eugen Ehrlich (EHRLICH, **Fundamentos da sociologia do direito**, p. 373.) Paolo Grossi apresenta uma visão particular do efeito histórico. Admite que "o problema histórico-jurídico está todo na crença difusa de conquistas últimas e eternas, na fixação de uma dogmática imobilizadora, na indiscutibilidade de certas categorias; o problema - que é absolutamente metodológico - está na des-historicização de todo um material historicíssimo, respeitável fruto de vicissitudes históricas, e por isso discutível, e portanto entregue ao devir do tempo e à sua usura" GROSSI, Paolo, O ponto e a linha. História do Direito e Direito Positivo na formação jurista do nosso tempo, **Seqüência: Estudos Jurídicos e Políticos**, v. 26, n. 51, p. 31–46, 2005, p. 89.

[314] NISSENBAUM, Helen, **Privacy in context: technology, policy, and the integrity of social life**, New York: Stanford University Press, 2009, p. 69–72.

[315] FRIED, Charles, Privacy: Economics and Ethics: A Comment on Posner, **Ga. L. Rev.**, v. 12, p. 423, 1977.

[316] WESTIN, Alan F., Privacy and freedom, 1970.

[317] GAVISON, Ruth, Privacy and the Limits of Law, **The Yale Law Journal**, v. 89, n. 3, p. 421–471, 1980.

[318] Historicidade é um dos elementos mais caros à metodologia do Direito Civil-Constitucional desenvolvida por Pietro Perlingieiri. Para ele "è necessario svincolarsi dalle strettoie di un sistema storicamente superato, dare piú spazio agli istituti maggiormente presenti nella realtà attuale e riservare minore attenzione a quelli ormai logori." PERLINGIEIRI (ORG.), Pietro, **Manuale di diritto civile**, 6. ed. Napoli: Edizione Scientifiche Italiane, 2007, p. 130.

dogmática se desvia do aspecto essencial quando o referencial envolve o direito à privacidade. Ao analisar os efeitos da tecnologia na evolução do sistema social, Luhamn aponta que na era da máquina a vapor, não era propriamente o vapor o centro dos problemas, mas a máquina[319]. Semelhante constatação pode ser feita com a privacidade se analisada sob o prisma da policontextualidade. Isoladamente, os potenciais pontos de estrangulamento conceitual da privacidade carecem de confirmação empírica. Somente a partir de um ou alguns cenários e contextos[320], nem sempre previamente definidos, os desdobramentos do preenchimento normativo e axiológico do direito à privacidade são justificáveis. Em grande medida, esta é a principal razão pela qual se proporá a análise de contextos em detrimento de conceitos e teorias isolados, mesmo porque a análise evolutiva das diversas teorias da privacidade nem sempre permitiu uma compreensão pluralística e clara do estágio em que o tema se encontra hoje dada a expressiva mudança proporcionada pela tecnologia.

1.2 Privacidade e a emancipação conceitual

Se em geral o objetivo das pesquisas em torno do direito à privacidade envolve a orientação dos formuladores de políticas públicas e dos tomadores de decisão, não será a definição de um conceito que viabilizará a consecução deste fim, mas a compreensão evolutiva e contextual do seu alcance atual. Em grande medida, os inúmeros problemas relacionados à privacidade decorrem da equivocada articulação dos pressupostos e elementos característicos da privacidade, isto é, das impropriedades do discurso argumentativo fundante, e não especificamente da atribuição de um sentido ao tema. A privacidade tem sido vista a partir de um esquema estritamente binário, monocultural e reducionista[321], ao invés de ser compreendida segundo a complexidade do seu processo de reinvenção, voltado a atender novas demandas por liberdade, autonomia, inovação, valores democráticos e quebra de paradigmas convencionais do mundo físico.

A proposta de modelo normativo do sistema de proteção da privacidade apresentada neste trabalho parte de uma linha oposta, ou seja, adota como ponto de partida a diversidade cultural e os múltiplos contextos de interação social para indicar parâmetros

---

[319] LUHMANN, **Introduction to systems theory**, p. 324.

[320] Um bom exemplo de análise contextual é a relação entre privacidade e dignidade nas esferas pública e privada, tal como apresentada por POST, What Larry Doesn't Get, p. 2092–2093.

[321] FORTES, Vinícius Borges, **Os direitos de privacidade e a de dados pessoais na internet**, [s.l.]: Lumen Juris: Rio de Janeiro, 2016, p. 219–222.

suficientemente seguros e flexíveis. Ao invés de apresentar um modelo pronto, a partir de denominadores comuns entre problemas de maior incidência na violação da privacidade e dados pessoais, se adotará como marco alguns indicadores permeados por um complexo de formulações e diretrizes principiológicas, tal como vem sendo feito por agentes reguladores na União Europeia, Estados Unidos, APEC, Canadá e Austrália. Esta abordagem terá a característica de apontar para rumos e processos de convencimento que determinem a relevância social da privacidade e não apenas seus impactos individuais e suas concepções em abstrato[322].

Por esta razão, a principal questão subjacente à privacidade e sua percepção contextual não são as diminuições sobre o controle da liberdade individual e intimidade, mas as transgressões ou tentativas de se furtar à atividade regulatória por parte das plataformas digitais normativas, visto que as normas sobre proteção de dados almejam preservar a integridade dos contextos sociais e dar suporte à finalidade e aos valores que os orientam[323].

1.3. Vigilância em massa: o desafio das pretensas justificativas

No cenário atual da modernidade, a separação entre política e direito permanece com um ponto de reflexão e delineamento do debate. Enquanto o poder se tornou um fenômeno global e extraterritorial, com a proliferação de centros de poder para além das relações estatais, a política tem se reduzido drasticamente a um fenômeno local - com expressiva repercussão local nas vilas globais -, incapaz de reagir, tanto na esfera pública quanto privada, e fornecer mecanismos de controle político às incertezas e avanços tecnológicos da modernidade[324]. Num cenário de vilas globais com redes regulatórias próprias, mais do que nunca o papel da política tornou-se essencial para proporcionar o acoplamento estrutural entre atuação estatal e atividade privada para evitar a falta de interoperabilidade entre regulações sobre privacidade e proteção de dados.

Por esta razão, compreender o papel da inexistência de fronteiras entre público e privado constitui uma das premissas para a identificação de um sistema normativo

---

[322] Em resposta à teoria da privacidade como controle sobre as informações pessoais, Daniel Solove ressalta que "privacy is not simply a subjetive matter of individual prerrogative; it is also an issue of what society deems appropriate to protect". SOLOVE, **Understanding privacy**, p. 25.

[323] BAMBERGER, Kenneth A.; MULLIGAN, Deirdre K., Privacy on the Books and on the Ground, **Stan. L. Rev.**, v. 63, p. 247, 2010.

[324] BAUMAN, **Vigilância líquida**, p. 13.

complexo, capaz de dialogar com a dinamicidade da necessidade regulatória do ciberespaço, em especial porque as formas sociais pré-prontas costumam se desmanchar mais depressa, tal como ocorre com o conceito de privacidade[325].

Se por um lado a fronteira entre o público e privado se tornam mais rarefeitas em razão das particularidades do ciberespaço e sua capacidade de ignorar as limitações de territorialidade, por outro tem se constatado que a vigilância estatal[326], aparentemente sólida e estável, tem se tornado cada vez mais móvel, flexível e também contextual, o que reforça a ideia em torno da necessidade de uma *lex privacy* igualmente capaz de se opor a este fenômeno. É aqui que a proposta de Bauman se aproxima da de Teubner na perspectiva da fragmentação e incerteza dos parâmetros de privacidade que teremos no futuro com a fluidez de significados, símbolos e instituições. Neste cenário, a fusão de formas sociais e a pouca agregação entre poder e política despontam como características da modernidade líquida[327], que, por sinal, demandam maior compreensão e aprimoramento.

Bauman acredita que no cenário da modernidade líquida o poder deve ser livre para flutuar, de modo que as barreiras precisam ser eliminadas para viabilizar o acoplamento estrutural entre política e poder. Um claro exemplo disso são as barreiras sociais baseadas na territorialidade, que deveriam ser eliminadas para que a instabilidade dos vínculos permita a ressignificação e nova compreensão da privacidade[328].

Os tempos líquidos exigirão um novo modelo de comportamento ético entre os agentes privados e o Estado, a ponto de Bauman dar uma ênfase maior no reencontro com o outro, ou seja, a *accountability* como substrato das relações em torno da privacidade. Perceber a responsabilidade com o outro será o ponto de partida de um arcabouço regulatório interativo, que contará tanto com a participação estatal quanto a influência privada no desenho adequado da proteção de dados.

---

[325] *Ibid*., p. 11.

[326] PASQUALE, The Black Box Society, p. 51–52.

[327] BAUMAN, Zygmunt, **Modernidade líquida**, Rio de Janeiro: Zahar, 2001.

[328] RODOTÀ, Stefano, **A vida na sociedade da vigilância: a privacidade hoje**, Rio de Janeiro: Renovar, 2008; RODOTÀ, Stefano, **Tecnologie e diritti**, [s.l.]: Il mulino, 1995.

Bauman usa o termo incertezas endêmicas e revela grande preocupação com os sistemas e processos que se divorciam de qualquer consideração de caráter moral[329]. Neste sentido, a adiaforização é um conceito trabalhado por Bauman para analisar a replicação de dados do corpo ou por ele derivados, ou seja, um típico processo de replicação e fragmentação de dados. É neste contexto que Bauman também trata da ideia de *hyperlink humano*, fruto da experiência advinda da migração da modernidade sólida para a modernidade líquida, dos átomos para bits, em que os indivíduos estão engajados no compartilhamento de dados[330] como moeda de troca.

Não por acaso Zuboff acrescenta outro ingrediente ao debate da vigilância a partir do processamento de dados pessoais, a saber, a possibilidade de rastreamento das experiências individuais por agentes de mercado para a definição de perfis comportamentais e posterior desapropriação da experiência humana como matéria prima da economia comportamental. Nesse contexto, a vigilância é impulsionada não apenas pelo poder público, mas também por atores privados que se valem da tecnologia para capturar dados pessoais e desenhar a experiência dos seus titulares[331].

Zuboff denomina este processo de vigilância do capitalismo, que nos indica o caminho do que não foi seguido pelo processo de transformação digital na medida em que não foi capaz de proporcionar aos indivíduos o poder de decidir sobre o destino e finalidade dos seus dados pessoais. Sob o conceito de *rendition*, Zuboff demonstra que a nova manifestação da vigilância é compreender o buraco existente entre "*dados e experiência"* para implementar ferramentas que transformem dados em experiência. Por essa razão, o imperativo de predefinição dos comportamentos da *rendition* transforma fronteiras e regulação em algo inaceitável, uma vez que transformariam a autonomia individual em ameaça aos ganhos advindos da vigilância do capitalismo:

> "Surveillance capitalism's rendition practices overwhelm any sensible discussion of 'opt in' and 'opt out'. There are no more fig leaves. The euphemisms of consent can no longer divert attention from the bare facts: under surveillance capitalism, rendition is typically unauthorized, unilateral, gluttonous, secret, and brazen. These

[329] BAUMAN, **Modernidade líquida**, p. 14. No mesmo sentido, CASTELLS, Manuel, **Communication power**, Oxford: OUP Oxford, 2013.

[330] BAUMAN, **Vigilância líquida**, p. 16.

[331] A este processo Zuboff denomina *rendition*, uma equação que capta a experiência existente entre a experiência humana e os dados comportamentais. ZUBOFF, Shoshana, **The age of surveillance capitalism: The fight for a human future at the new frontier of power**, Nova York: Public Affairs, 2019, p. 232–234.

> characteristics summarize the asymmetries of power that put the 'surveillance' in surveillance capitalism.[332]

Neste novo cenário pós-panóptico, a privacidade é comprometida por todos os lados – público e privado - , conforme se depreende da conjugação da visão de vigilância de Bauman com a de Zuboff, uma vez que se relaciona tanto com o crescente poder das novas tecnologias quanto com a forma como ele é distribuído de forma assimétrica na sociedade. A diferença no cenário atual envolve um quadro no qual as relações de poder fogem para um local inalcançável, nem sempre submetido a rastreamentos ou manifestações de consentimento e responsividade.

O modelo panóptico de Bentham cabe precisamente na percepção contextual da privacidade no ciberespaço, pois diz muito a respeito do que hoje compreendemos a respeito da vigilância[333], transformação de dados comportamentais em experiências e geração de riqueza[334]. O panóptico tem como marca a dinamicidade da capacidade de observação nos seus diversos panoramas e comportamentos, algo muito próximo do que se pode observar no cenário de esfacelamento de fronteiras.

Da mesma forma que o modelo panóptico causou profundas consequências políticas e sociais, esses efeitos acompanham os poderes pós-panópticos da modernidade líquida[335], notadamente porque a privacidade não é a sua maior baixa, visto que questões como autodeterminação informativa, transparência e *accountability* também foram comprometidas neste contexto de vigilância.

2. A análise econômica da privacidade e os perfis comportamentais

Tanto quanto a perspectiva pluralística e contextual da privacidade, a sua análise econômica permite compreender muitos dos custos e benefícios tangíveis e intangíveis

---

[332] *Ibid*., p. 241.

[333] BENTHAM, Jeremy, **O panóptico**, [s.l.]: Autêntica, 2013.

[334] NISSENBAUM, **Privacy in context**.

[335] BAUMAN, **Vigilância líquida**, p. 20.

relacionados aos *trade-offs* envolvendo a proteção e o compartilhamento de dados pessoais[336]. Assimetrias de informação quanto ao uso e consequências do compartilhamento, assim como pesquisas sobre decisão comportamental, levantam questões sobre as habilidades de consumidores racionais para otimizar as escolhas em torno da privacidade. Por esta razão, cumpre analisar até que ponto a responsabilidade individual, a concorrência e a regulação orientam o mercado para um equilíbrio entre tutela da privacidade e conversão de dados pessoais em experiências[337]. Nem sempre será possível constatar que a perspectiva mais próxima à proteção de dados invariavelmente acarretará mais impactos sociais e individuais positivos do que negativos ou, ainda, que teremos evidências concretas de que os indivíduos raramente têm plena consciente sobre os riscos e ameaças aos seus dados pessoais.

Se por um lado a proteção de dados é capaz de ensejar desafios regulatórios relevantes, conforme indicado nos capítulos anteriores, isso se deve em boa medida à possibilidade de que os dados pessoais sejam objeto de vantagens e benefícios economicamente tangíveis, suscetíveis de trocas, a depender dos valores em jogo e das contrapartidas oferecidas. E tal como os demais bens tangíveis, fatores como exclusividade da propriedade tornam esses bens ainda mais atrativos. Como veremos a seguir, a falta de exclusividade da propriedade sobre os dados será um fator muito relevante para a análise em torno dos seus impactos econômicos, assim como a construção de meios para induzir comportamentos a partir de estímulos e trocas.

Com a nova realidade do ciberespaço, na qual os indivíduos não são meros consumidores de informação, mas também produtores públicos de dados pessoais - não exclusivos - , a arquitetura descentralizada da rede propiciou o surgimento de serviços e produtos agregados à maior coleta de dados. Neste ambiente, algumas empresas alcançaram uma posição para melhor coletar, controlar, rastrear e definir perfis comportamentais de um grande número de titulares de dados pessoais, antecipando e induzindo preferências, escolhas e decisões. Como consequência, os mesmos fatores econômicos que auxiliam na compreensão do comportamento de trabalhadores e consumidores também podem determinar investimentos na obtenção e na blindagem do compartilhamento de dados pessoais.

---

[336] Rodotà considera inadmissíveis as análises de custos para o poder público e empresas em contraposição à regulação das normas de dados pessoais. RODOTÀ, **A vida na sociedade da vigilância**, p. 53.

[337] Conforme esclarece Pasquale, " 'better user experience' is the reason the major internet companies give for almost everything they do. But surely their interests must conflict with ours sometimes – and then what?" PASQUALE, The Black Box Society, p. 61.

Parte dessa estratégia de mercado de transformação de dados pessoais comportamentais em experiência advém do que Thaler e Sunstein denominam de arquitetura da escolha, que nada mais representa do que a incorporação de um princípio da psicologia em produtos e serviços: a compatibilidade de resposta de estímulo[338]. A ideia subjacente a essa prática de mercado com dados pessoais comportamentais envolve o recebimento esperado de sinais (estímulo) para que haja consistência com a ação desejada. A configuração de aplicativos e o desenho gráfico de plataformas digitais são construídos exatamente com o escopo de proporcionar o recebimento de sinais esperados para ensejar a adoção de ações desejadas.

O maior exemplo desse fenômeno advém da publicidade online praticada por redes sociais, que conseguem direcionar anúncios a partir da criação de incentivos para a troca de experiências com usuários, com o escopo de posteriormente monetizar aquilo que Zuboff denominou de "*rendition*"[339]. Em 2018, na conferência anual PrivacyCon da FTC, Alan Mislove apresentou uma pesquisa empírica na qual demonstrou que algumas plataformas digitais conseguem converter análises de enquetes e anúncios em perfis comportamentais para realizar ofertas diretas de produtos com público-alvo ainda mais preciso:

> "most advertising platforms have begun allowing advertisers to target users directly by uploading the personal information of the users who they wish to advertise to (e.g., their names, email addresses, phone numbers, etc.); these services are often known as custom audiences. Custom audiences effectively represent powerful linking mechanisms, allowing advertisers to leverage any Personal Individual Information (e.g., from customer data, public records, etc.) to target users."[340]

Com as estratégicas de mercado impulsionadas pela arquitetura da escolha em conjunto com mecanismos de *big data* e *data analytics,* o aumento da disponibilidade de dados pessoais fomentou atividades e benefícios até então impensáveis, mas, em contraposição, as posições de poder decorrentes da exploração econômica dos dados pessoais despertaram ainda mais a atenção dos reguladores e formuladores de políticas públicas.

---

[338] THALER, Richard H.; SUNSTEIN, Cass R.; BALZ, John P., Choice architecture, 2014; THALER, Richard H.; SUNSTEIN, Cass R., **Nudge: Improving Decisions about Health, Wealth, and Happiness**, [s.l.]: Penguin, 2009, p. 83–84.

[339] Segundo Zuboff, "rendition has become a surveillance capitalist project shaped by its imperatives and directed toward its objectives". ZUBOFF, **The age of surveillance capitalism**, p. 240.

[340] VENKATADRI, Giridhari *et al*, Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface, *in*: **Federal Trade Commission PrivacyCon**, Washington: [s.n.], 2018, p. 221–239.

Na medida em que a informação é, de fato, considerada uma expressão de poder, o controle sobre os dados pessoais inevitavelmente pode ser considerado um fator de desequilíbrio entre as partes envolvidas, sobretudo quando decorrentes de transformações de dados pessoais em experiência de consumo. Por esta razão, nessa tese se adotará a perspectiva de que a privacidade não é o oposto de compartilhamento, mas sim o efetivo controle sobre o compartilhamento para permitir aos titulares a decisão sobre quais dados pessoais desejam a conversão em experiências e perfis comportamentais[341]. As potenciais decisões de compartilhamento estratégico de certos dados em detrimento de outros deveriam decorrer de escolhas conscientes, a partir de meios transparentes, e não de vantagens psicológicas e econômicas fomentadas pelos agentes de mercado, como se verifica nos "negócios jurídicos gratuitos" de cupons de desconto online, programas de fidelidade e *ad advertising*[342].

2.1 Ineficiências de mercado e não exclusividade de dados compartilhados

Algo ainda pouco claro e com escassos dados empíricos envolve os custos sociais decorrentes das privações ou concessões individuais para o maior compartilhamento de dados pessoais, dada a possibilidade de que os dados compartilhados para uma finalidade específica tenham sido utilizados para outra desconhecida pelo titular. Ainda que estejam claros os benefícios individuais e os obtidos pelas empresas em detrimento da autonomia informativa, compreender os custos sociais da conversão de dados comportamentais em experiências monetizáveis ainda é um desafio relevante para os estudiosos de *behavioral economics*.[343]

A partir de uma visão mais liberal e menos protetiva, Posner considera clara a capacidade racional dos indivíduos em precificar os seus dados pessoais de forma a tornar uma relação mais eficiente, ou seja, embora os indivíduos nem sempre tenham condições de avaliar, sob a mesma expressão de poder e transparência, os riscos e ameaças a seus dados

---

[341] TIEGHI, Ana Luiza, **Conexão wifi é caminho para loja conhecer cliente e direcionar vendas**, Folha de São Paulo, disponível em: <https://www1.folha.uol.com.br/mpme/2019/02/conexao-wifi-e-caminho-para-loja-conhecer-cliente-e-direcionar-vendas.shtml>, acesso em: 11 fev. 2019.

[342] As experiências de Thaler com incentivos a partir de "negócios gratuitos" revela um interessante panorama da conversão de experiências em valor agregado e melhor qualidade de produtos em fase de implementação, como no caso do professor de sky. THALER, Richard H., **Misbehaving: The making of behavioral economics**, Nova York: WW Norton & Company, 2015, p. 116; THALER, Richard H., Behavioral economics: past, present, and future, **American Economic Review**, v. 106, n. 7, p. 1577–1600, 2016.

[343] ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George, Privacy and human behavior in the age of information, **Science**, v. 347, n. 6221, p. 509–514, 2015.

pessoas, eles teriam capacidade de compreender em boa medida o valor dos dados pessoais envolvidos e o impacto na eficiência de mercado.[344] Se por um lado a maior regulação da privacidade e a proteção de dados pessoais podem ser consideradas como formas de reduzir a eficiência de mercado, argumento combatido por Rodotà[345], por outro ela tem representado uma medida intervencionista redistributiva de oportunidades relevante e capaz de assegurar a proteção de direitos até então ignorados[346], viabilizando uma equalização de ganhos e custos sociais, ou seja, a regulação de proteção não é toda voltada a tolher as eficiências de mercado obtidas com a conversão de dados comportamentais em experiências.[347]

No entanto, é importante destacar que não há uma fórmula pronta sobre a maior ou menor extensão em que os dados pessoais e a privacidade precisam ser protegidos ou podem ser compartilhados para maximizar o bem-estar social e individual. Aqui, novamente, predominará o contexto em que a privacidade e proteção de dados serão analisados, em especial porque a privacidade pode ser considerada uma medida redistributiva, mas a sua ausência também. Em outras palavras, os benefícios se tornam custos de oportunidade quando há por parte dos titulares dos dados o desejo de não os compartilhar.

Outro desafio relevante acerca da análise econômica dos dados pessoais envolve a sua natureza não exclusiva, conforme destacado no capítulo 1. Ao contrário dos bens físicos, cuja propriedade e exclusividade da titularidade são evidentes, dados pessoais podem ser compartilhados, duplicados, enriquecidos e minerados, gerando verdadeiras cadeias desdobradas de informações relevantes para análise de mercado. Ainda são escassas as pesquisas empíricas e estudos sobre o real impacto em termos de ineficiência de mercado que a não exclusividade dos dados pessoais pode proporcionar.[348]

---

[344] POSNER, Richard, The economics of privacy, **The American Economic Review**, v. 71, n. 2, 1981, p. 406.

[345] RODOTÀ, **A vida na sociedade da vigilância**, p. 54; RODOTÀ, **Tecnologie e diritti**.

[346] ACQUISTI, Alessandro; GROSSKLAGS, Jens, What can behavioral economics teach us about privacy, **Digital Privacy: Theory, Technologies and Practices**, v. 18, p. 363–377, 2007.

[347] The analysis in this paper is also suggestive with regard to the possible sources of privacy legislation. The principal beneficiaries of such legislation are people with more arrests or convictions, or poorer credit records (more judgments, bankruptcies, etc.), than the average person. These groups are presumably not cohesive enough to overcomethe free-rider problems that plague efforts to form effective political coalitions, but they overlap strongly with racial and ethnic groups, namely black and Hispanic Americans, which are politically organized. POSNER, The economics of privacy, p. 407.

[348] ACQUISTI, Alessandro, Nudging privacy: The behavioral economics of personal information, **IEEE security & privacy**, v. 7, n. 6, 2009.

A rigor, o que se tem de concreto neste campo são inferências positivas de mercado sobre a capacidade redistributiva de benefícios e oportunidades que a natureza não exclusiva dos dados pessoais proporciona. Todo e qualquer agente, com condições tecnológicas de explorar soluções que viabilizem a coleta legítima e o enriquecimento de bases de dados, pode se tornar um potencial *stakeholder* sem que isso signifique, necessariamente, a impossibilidade de que outro agente atue em paralelo com a mesma gama de dados pessoais.

O fato é que os indivíduos realizam diariamente transações com seus dados pessoais. Por meio de uma consulta em um provedor de busca, o usuário está compartilhando e "entregando" gratuitamente informações sobre seus interesses atuais em troca de encontrar resultados relevantes[349]. Usando uma rede social, os indivíduos estão naturalmente "vendendo" informações sobre seus interesses, demografia e redes de amigos e conhecidos, em troca de um novo método de interagir com outros usuários.[350]

Sob a ótica do princípio da preferência revelada, seria possível inferir as avaliações das pessoas quanto aos seus dados observando o uso de ferramentas online. No entanto, para os provedores de serviços, a negociação de dados é a essência da operação, ao passo que, do ponto de vista do titular dos dados, a transação subjacente acaba sendo um aspecto secundário, quase imperceptível e muitas vezes totalmente invisível e indiferente se considerado um interesse predominante de outra operação.[351]

A lógica de funcionamento dos "negócios jurídicos gratuitos" é parte de uma nova forma de expressão das alocações e eficiências de mercado, na medida em que não há troca de valores econômicos tangíveis propriamente dito, mas há geração de benefícios precificáveis e não exclusivos para vários dos envolvidos com acesso aos dados pessoais compartilhados.[352]

---

[349] BORGESIUS, Frederik J. Zuiderveen, Personal data processing for behavioural targeting: which legal basis?, **International Data Privacy Law**, v. 5, n. 3, p. 163, 2015; AYENSON, M. *et al*, Behavioral Advertising: The Offer You Cannot Refuse, **Harvard Law and Policy Review**, v. 273, 2012.

[350] ACQUISTI; JOHN; LOEWENSTEIN, What Is Privacy Worth?

[351] ACQUISTI; TAYLOR; WAGMAN, The economics of privacy.

[352] ACQUISTI, Nudging privacy.

3. Proteção de dados e Cloud Computing: a nova fronteira regulatória?

A economia compartilhada tem como uma de suas marcas a projeção disruptiva de novas formas de bens e serviços, cuja principal característica envolve a mudança de paradigmas e estruturas físicas. Dentre delas, a computação em nuvem ou *cloud computing* representa um formato inovador na transferência, armazenamento e compartilhamento de dados, que por meio da superação das limitações impostas pelas camadas físicas, permite conferir exponencialidade à gestão de informações sob o controle dos usuários.

Além de ser uma ferramenta marcada pela disrupção e relativa convergência, as *clouds* atuam como meio de empoderamento do usuário, na medida em que estimulam o armazenamento descentralizado em vários dispositivos, bem como viabilizam o acesso em qualquer lugar, formatação e em larga escala. Por essa razão, os benefícios proporcionados pelas *clouds* atingem diferentes setores do mercado e de maneiras diferenciadas, com vantagens competivas tanto para o setor público quanto privado, bem como funcionalidades próprias para os usuários:

- proporcionam um aumento da produtividade e menores investimentos em ativos fixos;
- ampliam a gestão profissional e o acesso do consumidor a todas as aplicações em larga escala e qualquer lugar;
- viabilizam melhores controles de segurança e confuguração;
- asseguram mecanismos de atualização de sistemas mais eficientes e funcionalidades personificadas;
- conferem acesso a serviços sob demanda, por meio dos quais o usuário configura as aplicações em nuvem de acordo com suas preferências;
- permitem o agrupamento de recursos de computação para atender a vários usuários, com medição, alocação, realocação e redimensionamnto dinâmico de espaço de acordo com as demandas de armazenamento, transferência e gestão.

Ao mesmo tempo em que a ubiquidade, enquanto possibilidade de rompimento das fronteiras territoriais, representa uma das externalidades positivas de mercado do emprego de *clouds*, por outro lado a forma de regulação ainda desperta controvérsias. Na medida em que a principal característica das *clouds* advém da superação das limitações físicas de armazenamento de dados, o arranjo regulatório ideal para disciplinar esse fenômeno deveria

adotar como premissa a aplicação extraterritorial das leis de proteção de dados, e não o excessivo apego às premissas do mundo físico. Como forma de ilustrar os arranjos regulatórios de *clouds*, três modelos despontam como os mais relevantes para compreender as particularidades dessa ferramenta: o *data shard*, o *data localizaton* e o *data trust*.

O modelo *Data Shard cloud* é conhecido por permitir que uma empresa armazene informações em *clouds* em vários locais. Nessa abordagem dinâmica, a própria rede distribui dados para servidores domésticos e internacionais, de acordo com um processo de alocação estratégica de espaço. Um único arquivo pode ser dividido em componentes e armazenado em diferentes países, de modo que a inteligência incorporada na arquitetura da rede atua para definir o local para onde enviar e armazenar os dados. A arquiturea da rede se vale da sua própria inteligência para criar eficiências operacionais.

No modelo *Data Localization cloud*, uma empresa armazena informações em uma nuvem restrita a um único país ou região, em especial por conta de restrições legais ou regulatórias. Trata-se de um modelo de pouco aproveitamento da reduação dos custos e dos benefícios inerentes à ubiquidade e escalabidade das *clouds*, sem necessariamente assegurar a segurança da informação pretendida.

Por fim, o modelo *Data Trust cloud* contém uma abordagem aprimorada de localização de dados. Como no modelo de *data localization*, uma nuvem no formato *data trust* pode estar localizada em um país ou em uma única região, mas comporta uma segregação entre gerenciamento de rede e capacidade de acesso aos dados. O modelo de *Data Trust cloud* depende de construções legais e técnicas - fronteiras nacionais e instrumentos de confiança - e molda a tecnologia para se adequar às categorias legais selecionadas. Essa abordagem pode ser usada para estabelecer tanto uma localização extraterritorial de informação quanto um acesso extraterritorial a ela, o que demonstra a ampla dinamicidade desse formato.

Com exceção do segundo modelo acima, os demais foram construídos sob o prisma da regulação extraterritorial de *clouds (geographically-based approach*), a que mais se adequa a esse formato de armazenamento e transferência de dados. Em linha com a aplicação exterritorial das leis gerais de proteção de dados recentemente aprovadas, cujo objetivo é atingir os processos de transferências e armazenamento de dados em *clouds*, o Marco Civil da Internet abandonou a necessidade de que empresas estejam estabelecidas no Brasil ou que os

dados aqui sejam armazenados, fenômeno conhecido como *data residency request.* Essa posição é, por sinal, registrada no voto[353] do Ministro Benjamin Zymler do Tribunal de Contas da União, quando da análise do formato de contratação de *cloud computing* pela Administração Pública.

Na contramão da regulação mais moderna sobre o tema, atos normativos como a Portaria GSI n. 9/2018 e o edital 57/2017 relativo à consulta pública do Banco Central para a edição da IN CMN 4658/18 e Circular BACEN 3909/19 almejaram revigorar o tema da territorialidade para impor exigências de armazenamento no país. No mesmo caminho, aliás, seguiu a CVM com a consulta pública para a alteração da IN CVM 505/11. No entanto, na redação final da IN CMN 4658/18 e da Circular BACEN 3909/18, o Banco Central abandonou a territorialidade (*data residency request*) por perceber que essa perspectiva não necessariamente conferiria mais segurança e proteção aos dados pessoais. No mesmo sentido seguiu o Ministério do Planejamento quando do lançamento da consulta pública para a atualização da IN 4/2014, que resultou na IN 1, de 4 de abril de 2019. A CVM ainda não editou a nova instrução normativa que alterará a IN CVM 505/11, de modo que ainda não é possível saber se persistirá com a proposta inicial acerca da territorialidade.

E na medida em que a lei não impôs restrições dessa grandeza por meio do Marco Civil da Internet ou da Lei Geral de Proteção de Dados (LGPD), esses atos normativos secundários poderiam ser considerados ilegais ou inconstitucionais por impor restrições não previstas em lei e instituídas por órgãos reguladores destituídos de competência para tanto.

Em linha com as mais modernas regulações sobre proteção de dados, a legislação europeia – *General Data Protection Regulation (GDPR)* e a brasileira de proteção de dados (LGPD) optaram por adotar o regime da extraterritorialidade ao invés de se ocupar de meras exigências territoriais que se demonstraram incapazes de apresentar soluções plausíveis para regular as empresas de tecnologia e, em especial, os serviços de *cloud computing* em âmbito global.

Operações de tratamento de dados realizadas dentro do território brasileiro estão invariavelmente sujeitas à aplicação da LGDP, assim como as operações que tenham por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no

---

[353] Tribunal de Contas da União. TC 025.994/2014-0. Acórdão n. 1739/15, Rel. Min. Benjamin Zymler. DJ 15.7.2015

território brasileiro, ainda que a empresa responsável por essa atividade esteja sediada ou localizada fora do país.

Com a adoção da perspectiva da extraterritorialidade da aplicação da lei, em detrimento das exigências de *data residency request*, o regime jurídico de proteção de dados e as *clouds* se tornam duas faces complementares de um processo regulatório dinâmico, eficiente e bem mais adequado às características particulares do ciberespaço. Em outras palavras, as exigências de *data residency request* apenas representarão gargalos regulatórios que impactarão no processo de inovação, no fluxo das transações comerciais, na melhor alocação de recursos e na obstaculização da conversão de ativos físicos em digitais.

4. Dados pessoais: o processamento enquanto categoria regulada

Na perspectiva da policontextualidade, compreender os valores semânticos e o conteúdo regulado torna-se tarefa essencial para se identificar o papel dos atores no processo regulatório e como os modelos analisados reagem a cada um deles. O recorte eleito adota como ponto de partida as figuras que tiveram maior interação entre atores públicos e privados no processo de regulação, além de serem suscetíveis de avaliação segundo o referencial teórico de Teubner.

O conceito de dados pessoais para fins regulatórios adota como ponto de partida a real possibilidade de processamento, ou seja, a possibilidade de coleta e tratamento de dados pessoais para finalidades determinadas[354]. Isso significa dizer, em outras palavras, que nem toda a atividade de processamento terá relevância sob a perspectiva regulatória, como ocorre nos casos de processamento de dados de pessoas mortas[355]. É oportuno lembrar que as razões para a promulgação das primeiras leis de proteção de dados nos anos setenta decorrem do fato de que as novas tecnologias de processamento de dados em formato digital permitem mais fácil e mais amplo acesso aos dados pessoais do que as formas tradicionais de manipulação de dados[356]. Assim, seria uma melhor opção não restringir indevidamente a interpretação da definição de dados pessoais e sim delimitar as operações de processamento consideradas relevantes.

---

[354] WORKING PARTY 29, **Opinion 4/2007 on the concept of personal data**, Bruxelas: [s.n.], 2007.

[355] SCHWARTZ; SOLOVE, PII Problem.

[356] DONEDA, Danilo, **Da privacidade à proteção de dados pessoais**, Rio de Janeiro: Renovar, 2006, p. 209–212.

4.1 Delimitação do alcance: a atividade de processamento relevante e o sujeito identificado ou identificável

Um ponto comum entre os diversos instrumentos regulatórios sobre proteção de dados envolve a sua delimitação conceitual, isto é, toda e qualquer informação relacionada a uma pessoa natural identificada ou identificável[357]. No tocante à natureza da informação, o conceito de dado pessoal inclui toda e qualquer referência a um indivíduo, seja ela de ordem objetiva como dados genéticos, seja ela subjetiva, relatórios de perfil. O termo dado pessoal compreende, portanto, todas as informações que de algum modo se relacionam à vida privada e família, assim como aquelas pertinentes às relações empregatícias e perfil socioeconômico e comportamental.[358]

Sob o prisma regulatório, os dados somente serão objeto de tutela se forem pertinentes a uma pessoa natural, ou seja, todo aquele nascido com vida, pouco importando a sua nacionalidade. Os dados de pessoas jurídicas não se incluem no escopo de dados pessoais,[359] assim como o de pessoas mortas.

Para que seja considerado dado pessoal, não é necessário que a informação seja verdadeira ou passível de ser provada, em especial porque o direito de retificação, exclusão e atualização dos dados pessoais servirá exatamente para tutelar as situações nas quais as informações sejam imprecisas ou falsas. Se for considerado o recipiente ou meio pelo qual os dados pessoais serão disponibilizados, na delimitação normativa devem ser incluídas as informações oferecidas em qualquer formato, seja ele alfabético, numérico, gráfico, fotográfico ou acústico. Isso significa que as informações em papel ou aquelas armazenadas em uma memória de computador por meio de código binário tem a mesma natureza. Por outro lado, imagem e som somente serão considerados dados pessoais se puderem se relacionar a um indivíduo identificável ou identificado, como ocorre com fotografias pessoais e gravações de telemarketing dos consumidores[360].

---

[357] LEONARDI, Marcel, **Tutela e privacidade na internet**, [s.l.]: Editora Saraiva, 2012.

[358] BIONI, Bruno Ricardo, **Proteção de dados pessoais: a função e os limites do consentimento**, São Paulo: Gen Forense, 2019.

[359] Uma das controvérsias mais interessantes a respeito envolve a natureza dos dados relativos a emails corporativos de empregados. A rigor, é possível com um conjunto de dados identificar um empregado dentro de um universo específico, o que tornaria esse dado pessoal.

[360] WORKING PARTY 29, **Opinion 4/2007 on the concept of personal data**.

Uma categoria relevante de dados pessoais são os biométricos, ou seja, aqueles relacionados a propriedades biológicas, características fisiológicas, traços vivos ou padrões comportamentais que são únicos para um indivíduo, ainda que envolvam um certo grau de probabilidade.[361] Os principais exemplos de dados dessa natureza são as impressões digitais, padrões da retina, estrutura facial, voz, geometria da mão ou até características comportamentais como a assinatura manuscrita. Por se tratar de identificadores únicos, que conseguem estabelecer conexões precisas com um indivíduo, os dados biométricos costumam receber dos ordenamentos jurídicos uma atenção especial no tocante às formas de processamento[362].

O termo "relacionado" a um indivíduo é um delimitador importante para que se selecionem as informações e conexões cujos conteúdos são capazes de identificar alguém ou distingui-lo de outrem. Em boa parte dos casos, as conexões entre informação e um indivíduo podem ser facilmente estabelecidas, em outras as informações podem vir associadas a objetos e processos pertencentes a indivíduos ou a eventos que somente de forma indireta são capazes de identificá-los.

Uma pessoa natural pode ser considerada "identificada" quando, dentro de um grupo, consegue ser "distinguida" de todos os outros membros. Por outro lado, uma pessoa é "identificável" quando, embora não tenha sido identificada, ainda é possível fazê-lo. Esta segunda alternativa é, portanto, a premissa delimitadora do escopo do conceito de dado pessoal. Em geral, um indivíduo pode ser identificado por meio de informações específicas e que possuem uma vinculação particularmente próxima com as suas características[363].

Uma pessoa pode ser diretamente identificada pelo nome ou indiretamente por um número de telefone, CPF, RG, RENAVAM, número de carteira de trabalho, um número de passaporte ou por uma combinação de critérios que lhe permitem ser identificados dentro de um grupo de pessoas (idade, profissão, endereço). Isso reforça a tese de que a privacidade e a proteção dos dados pessoais devem ser sempre analisadas sob a perspectiva contextual e pluralística. A rigor, um nome de família muito comum não será suficiente para identificar alguém em relação ao grande número de indivíduos, enquanto é provável que ele alcance a

---

[361] FORTES, **Os direitos de privacidade e a de dados pessoais na internet**, p. 192–193.

[362] DONEDA, **Da privacidade à proteção de dados pessoais**; BIONI, **Proteção de dados pessoais: a função e os limites do consentimento**.

[363] WORKING PARTY 29, **Opinion 4/2007 on the concept of personal data**.

identificação de um aluno em uma sala de aula ou de um profissional numa repartição pública. Saber se o indivíduo a quem a informação se refere é identificado ou identificável depende das circunstâncias de análise. No que diz respeito a pessoas "identificadas" ou identificáveis "diretamente", o nome da pessoa é de fato o identificador mais comum e, na prática, a noção de "pessoa identificada" implica uma referência ao nome da pessoa, o que pode soar um critério pouco preciso.

No tocante às pessoas indiretamente "identificadas" ou identificáveis, vale observar que o critério predominante envolve a possibilidade de combinações de informações que levem a um determinado indivíduo[364]. A rigor, a depender da combinação de dados dispersos e o nível de complexidade do processo, é possível que a identificação indireta seja tão simples e conclusiva quanto aquela realizada de forma direta. Isso pode acontecer mesmo quando o nome seja desconhecido, como nos casos em são atribuídos identificadores universais para fins de publicidade online e identificação de celulares (ADID,[365] IDFA).[366]

Cumpre salientar, contudo, que uma mera possibilidade hipotética de identificar um indivíduo não é suficiente para considerá-lo como "identificável". Para que esta possibilidade seja concreta, é necessário que todos os meios razoavelmente disponíveis sejam utilizados pelo controlador ou outra pessoa. Este teste deve ser considerado uma medida dinâmica e levar em consideração as tecnologias disponíveis no momento do processamento dos dados pessoais. Isto significa que a identificação pode não ser possível hoje com todos os meios razoavelmente disponíveis, mas se os dados forem mantidos por dez anos, por

---

[364] *Ibid*.

[365] **ADID**: é um sistema para o registro de ativos de publicidade, ou seja, dispositivos que divulgam informações de natureza publicitária. Por meio desse sistema, é possível gerar e gerenciar códigos de identificação exclusivos que se aplicam a todas as mídias. De acordo com a página institucional do Ad-ID12, "ao registrar um anúncio com o Ad-ID, é possível promover maior transparência e responsabilidade no mercado de publicidade, ajudando a eliminar erros associados ao uso inconsistente de identificadores de ativos em toda a cadeia de fornecimento de publicidade e permite uma medição de público mais granular em várias plataformas. (...) O sistema Ad-ID simplifica o processo de registro de ativos de publicidade em toda a cadeia de fornecimento, incluindo anunciantes, agências, provedores de serviços, distribuidores, plataformas e inclui compra e venda de mídia como um caminho paralelo. O resultado do registro do material do anúncio é a geração de códigos Ad-ID válidos. (...) Considera-se código Ad-ID válido um identificador único para um ativo de publicidade".**Ad-ID Overview & Glossary of Terms | Ad-ID**, disponível em: <http://www.ad-id.org/how-it-works/overview-glossary-of-terms>, acesso em: 19 fev. 2019.

[366] **IFA ou IDFA:** trata-se de um identificador para anunciantes é um identificador de dispositivo temporário usado pelo conjunto de dispositivos móveis da Apple. O IDFA fornece a identificação do dispositivo, oferecendo aos usuários finais a capacidade de limitar as informações do dispositivo, acessadas por anunciantes ou aplicativos. **What is Identifier for Advertisers (IFA/IFDA)? - Definition from Techopedia**, disponível em: <https://www.techopedia.com/definition/29032/identifier-for-advertisers-ifa-ifda>, acesso em: 19 fev. 2019.

exemplo, este aspecto deve ser considerado para a aplicação dos requisitos de processamento de dados pessoais e implementação de medidas técnicas e organizacionais.

4.2 Pseudonimização enquanto mecanismo de proteção dos dados pessoais

A pseudonimização é um processo voltado a disfarçar a identificação de um titular de dados pessoais, de forma a garantir maior nível de segurança, mediante a substituição de um atributo exclusivo do titular por outro tipo de registro. Ao contrário do que muitos sustentam, dados pseudonimizados são considerados dados pessoais, ou seja, não envolvem um processo de anonimização, na medida em que o controlador ainda tem condições de identificar o titular. Na pseudonimização, o controlador tem informações adicionais capazes de refazer toda a cadeia de identificação até se chegar novamente no titular dos dados[367].

O objetivo da pseudonimização é coletar dados adicionais relacionados ao mesmo indivíduo sem a necessidade de saber sua identidade e, consequentemente, reduzir a possibilidade de identificação. Trata-se, portanto, de uma técnica de segurança particularmente relevante para pesquisas estatísticas. As principais técnicas de pseudonimização são:

> **- Criptografia:** somente os detentores da chave privada tem a capacidade de acessar os dados e reidentificar os titulares. A criptografia é um método de segurança que será posteriormente analisado.
> - **Função Hash**: é uma modalidade de algoritmo que mapeia dados de comprimento variável para se atingir dados de comprimento fixo. Em outras palavras, a função hash é um mecanismo responsável por transformar uma grande quantidade de dados em uma pequena quantidade de informações. Um claro exemplo são as imagens compartilhadas em redes sociais, cada qual identificada por um código hash e com uma grande quantidade de dados a ela associados.
> - **Tokenização:** é uma técnica usualmente aplicada no setor financeiro para substituir os números de identificação de cartões por valores que reduzem o tamanho da exposição a ataques. Ocorre geralmente mediante a atribuição de uma sequência de números gerados aleatoriamente e não derivados dos originais correspondentes aos dados do titular[368].

A pseudonimização pode ser realizada mediante a atribuição aleatória de códigos combinados de letras, números e sinais, que de forma reversa formam listas de

---

[367] WORKING PARTY 29, **Opinion 5/2014 on Anonymisation Technques**, Bruxelas: [s.n.], 2014.

[368] *Ibid*.

correspondência das identidades dos titulares dos dados pessoais (ex. número matrículas de empregadas, logins de usuário etc). A pseudonimização também pode ser utilizada por meio de criptografia bidirecional ou *end-to-end*, mas também é possível que seja utilizada a técnica unidirecional, que não comporta a reidentificação e culmina na anonimização[369].

A eficácia do procedimento de pseudonimização depende de vários fatores como o espaço amostral utilizado, capacidade de rastreamento reverso e vinculação de informações, motivo pelo qual os pseudônimos utilizados devem ser aleatórios e imprevisíveis. Quanto maior o número de caracteres de um código de um dado pseudonimizado mais difíceis as chances de identificação. Como o dado pseudonimizado ainda é considerado um dado pessoal, visto que pode indiretamente culminar na identificação de um titular por parte do controlador, em geral os marcos regulatórios continuam aplicáveis, ainda que menor o risco de exposição[370].

Na medida em que a pseudonimização não tem origem e formatação jurídica específica exaustiva, o papel dos desenvolvedores e agentes de mercado pode ser considerado crucial para fins regulatórios. Este é mais um dos temas em que a corregulação se evidenciou como um meio mais apropriado para delimitar condutas e fomentar o desenvolvimento tecnológico.

4.3 Criptografia: o desafio da liberdade de comunicação e dos meios de investigação

Dentre as técnicas de pseudonimização, a criptografia merecerá uma análise específica, na medida em que pode ser considerada uma das expressões mais elucidativas da capacidade regulatória privada em comparação com a estatal. A criptografia é uma forma de linguagem que tem como objetivo assegurar o sigilo de comunicações e ganhou ainda mais expressão dentro do debate de proteção da privacidade.

Um dos principais desafios em torno do uso da criptografia envolve o seu frequente emprego para evitar a atuação das autoridades de investigação e dificultar a obtenção de provas e evidências da prática de crimes (*going dark*), no entanto é consenso entre as empresas de tecnologia, representantes da sociedade civil, órgãos públicos e

---

[369] *Ibid*.

[370] *Ibid*.

comunidade acadêmica que a criptografia também é responsável por proteger milhões de pessoas contra roubos, fraudes e outros atos criminosos.

Essas duas perspectivas não são mutuamente exclusivas. A adoção generalizada de criptografia representa um desafio real para a aplicação da lei, ao passo que criptografia é essencial tanto para a privacidade individual como a segurança nacional. Uma narrativa que meramente posicione autoridades públicas e segurança nacional contra a indústria da tecnologia e privacidade não reflete a complexidade da questão[371]. Equilibrar essas diferentes perspectivas tem sido uma das tarefas mais difíceis no atual contexto regulatório da privacidade no ciberespaço, pois muitos sustentam que seria impraticável conceber e implementar um sistema que assegurasse o acesso excepcional aos dados criptografados sem comprometer a segurança contra hackers, espiões industriais e outros agentes maliciosos. Além disso, exigir o acesso excepcional a dados criptografados seria desestimular as melhores práticas de desenvolvimento de criptografia, que valorizam a sua importância para a privacidade individual, a liberdade de expressão, os direitos humanos e a proteção contra a intrusão governamental no país e advinda do exterior.

Na medida em que a lei não tem sido a melhor maneira de regular a criptografia, os *stakeholders* envolvidos com a sua utilização tem optado por caminhos mais associados à atuação na arquitetura como forma de superar as ameaças estrangeiras e domésticas. Até então, a criptografia era utilizada como forma de se contrapor às exigências de localização territorial de dados (*data residency request*), cujo objetivo era assegurar a aplicação da lei e cumprimento de mandados judiciais, todavia diante das constantes ameaças regulatórias por parte do Estado, vários serviços migraram para países com menores exigências.

Para melhor compreender a correlação da criptografia com a privacidade e proteção de dados pessoais, vale recorrer ao início da década de 90 nos Estados Unidos, conhecida como *crypto wars*[372], visto que a criptografia e o anonimato, enquanto mecanismos de expressão da liberdade de comunicação, pensamento e manifestação, estão no epicentro do debate regulatório.[373] Até meados de 1993, a criptografia era feita por meio de hardware.

---

[371] ABELSON *et al*, Keys under doormats.

[372] The Crypto Wars: Governments Working to Undermine Encryption, https://www.eff.org/document/crypto-wars-governments-working-undermine-encryption

[373] Revised U.S. Encryption Export Control Regulations, https://epic.org/crypto/export_controls/regs_1_00.html

Como a internet ainda não havia se popularizado, a técnica era usada pelo governo em redes privadas. O padrão criptográfico mais utilizado era o *Data Encryption Standard* (DES), desenvolvido pela IBM,[374] e posteriormente sucedido pelo Clipper.

Neste período, o Departamento de Estado dos EUA classificava a criptografia como munição militar e regulava sua exportação.[375] O governo americano exigia a obtenção de licenças de exportação para softwares de cifragem que estivessem ao alcance estrangeiros. As agências governamentais emitiam licenças de exportação de forma discricionária, sem prazos ou critérios pré-determinados.[376]

Este procedimento subsistiu até o julgamento pela Suprema Corte americana do *leading* case *Bernstein v. United States Department of State*.[377] Durante seu doutorado em matemática pela Universidade de Berkeley, Daniel Bernstein desenvolveu um algoritmo criptográfico denominado Snuffle. Submetido à classificação da criptografia como munição militar, Bernstein foi impedido de publicar seu código criptográfico em periódicos acadêmicos na internet sem antes se registrar como exportador de armas. Por esta razão, o matemático decidiu processar o governo americano sob o argumento de que, ao restringir o acesso às ferramentas que asseguravam maior proteção à privacidade, como a criptografia, os agentes estatais teriam violado o direito à ampla comunicação dos cidadãos:

> Without cryptography, what people send via computers is the electronic equivalent of a postcard, open to view by many people while the message is in transit. With cryptography, people can put both messages and money into electronic 'envelopes,' secure in the knowledge that what they send is not accessible to anyone except the intended recipient.
> Continued development of cryptography promises to make it possible for the worldwide computer Internet to offer private, secure and protected communication among billions of people worldwide.[378]

O governo americano, por sua vez, sustentava que o Ato de Controle da Exportação de Armas (*Arms Export Control Act*) expressamente vedava o controle judicial do que era incluído no rol de munições. Na ocasião, o Tribunal do Distrito do Norte da Califórnia

---

[374] KATZ, Jonathan *et al*, **Handbook of applied cryptography**, [s.l.]: CRC press, 1996.

[375] International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120-30 (1994).

[376] ROSS, Patrick Ian, Bernstein v. United States Department of State, **Berkeley Tech. LJ**, v. 13, p. 405, 1998, p. 405.

[377] https://www.eff.org/cases/bernstein-v-us-dept-justice

[378] ROSS, Bernstein v. United States Department of State, p. 406.

entendeu que a classificação da criptografia como munição era inconstitucional por violação à Primeira Emenda da Constituição americana, uma vez que o código criptográfico constituía uma manifestação do direito de liberdade de expressão:

> Even object code, which directly instructs the computer, operates as a "language." When the source code is converted into the object code "language," the object program still contains the text of the source program. The expression of ideas, commands, objectives and other contents are merely translated into machine-readable code.[379]

A decisão foi amplamente fundamentada em analogias com partituras musicais e direitos autorais. A Suprema Corte objetivou demonstrar que o caráter funcional do código fonte não o tornaria menos protegido que a partitura da música tocada por um piano. A partir do precedente *Bernstein v. United States Department of State*, a criptografia foi reconhecida como uma manifestação da liberdade de expressão e a sua regulamentação por órgãos estatais foi considerada inconstitucional.

Superou-se, assim, a compreensão belicista da criptografia, substituída por uma posição mais próxima da sociedade civil. Era o primeiro passo para que o código pudesse ser utilizado como instrumento voltado à efetiva proteção de dados pessoais e da privacidade dos usuários da rede. Entretanto, a criptografia representa apenas uma das vias de expressão da autonomia e proteção de direitos fundamentais[380].

No âmbito da União Europeia, a criptografia tem suscitado expressivos embates, sobretudo após o episódio que envolveu Edward Snowden, a *National Security Agency* (NSA), alguns Primeiros Ministros de países europeus e a Presidente do Brasil. O fluxo transnacional de dados, que ensejou a celebração de um novo acordo entre União Europeia e Estados Unidos (*Privacy Shield*),[381] em função da declaração de nulidade do anterior (*Safe Harbor*) pela Corte Europeia de Justiça no caso *Max Schrems v. Data Protection Commissioner*,[382] tem evidenciado a importância dos marcos regulatórios voltados à proteção dos dados pessoais.

---

[379] *Ibid*.

[380] UNESCO, **Human rights and encryption**, [s.l.: s.n., s.d.].

[381] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf

[382] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

O marco regulatório da proteção de dados e privacidade na União Europeia ocorreu com a entrada em vigor da Diretiva 46/95, conhecida como o Regulamento Geral sobre a Proteção de Dados, no qual foram definidos padrões mínimos de proteção, o que facilitaria a identificação de outros países que oferecessem níveis de proteção equivalentes aos europeus, conforme analisado no capítulo anterior. Com a entrada em vigor da GDPR em maio de 2018, em substituição à Diretiva 46/95, e com o objetivo de proteger a privacidade dos indivíduos, a confidencialidade e a integridade tornaram-se dois princípios essenciais para o tratamento de dados pessoais. A preocupação com este aspecto é tamanha que a GDPR prevê que os dados devem ser protegidos desde sua concepção, ou seja, desde a definição dos meios de tratamento o responsável deverá prever formas adequadas de garantir a confidencialidade e integridade.

Ao contextualizar a proteção de dados pessoais realizada na União Europeia observa-se que a adoção da criptografia, enquanto expressão da regulação privada, contribui para imprimir um padrão de proteção ainda mais elevado aos titulares de dados. E um claro indicativo disso pode ser percebido pela previsão na GDPR de que os dispositivos, serviços e plataformas na internet deverão garantir a proteção de dados e a privacidade por configuração e padrão de fabricação (*privacy by design* e *privacy by default*).[383] Em outras palavras, a criptografia constitui uma manifestação da regulação privada, que em boa medida remete novamente à análise feita sobre Lessig e o poder regulador do código no capítulo 1.

Apesar disso, a regulação do ciberespaço e as particularidades desta arena pública de interação social parecem ser algo de difícil compreensão para algumas autoridades estatais, que enxergam a arquitetura da rede apenas como um meio de obstaculizar o seu *enforcement* em investigações criminais, ao invés de constituir um sistema de proteção do sigilo de comunicação e dos dados da grande maioria dos usuários.[384]

---

[383] SCHAAR, Peter, Privacy by design, **Identity in the Information Society**, v. 3, n. 2, p. 267–274, 2010; RUBINSTEIN, Ira, **Regulating Privacy by Design**, Rochester, NY: Social Science Research Network, 2011.

[384] Diante da ocasional inadequação da lei para regular o ciberespaço, Reino Unido, Canadá, Austrália e França passaram a atuar na arquitetura da rede mediante ferramentas de bloqueio, filtragem e suspensão de acesso como o Cleanfeed e agências governamentais como a HADOPI. Medidas semelhantes têm encontrado resistência nos Estados Unidos em virtude Primeira Emenda, como se observa no julgamento do caso Reno v. American Civil Liberties Union (521 US 844, 1997).

4.3.1 Proteção de dados e investigações criminais: a criptografia em xeque

Muito se questiona sobre o emprego da criptografia - enquanto meio de proteção de dados pessoais - como forma obstaculizar a atuação estatal, especialmente em investigações criminais. É certo que a garantia de inviolabilidade do sigilo de dados não é absoluta e a Constituição Federal veda o anonimato, todavia o faz em associação à liberdade de manifestação do pensamento (art. 5.º, IV), o que não significa que em toda e qualquer interação no ciberespaço o anonimato seja vedado.[385]

A criptografia, enquanto técnica de pseudonimização de um dado ainda considerado pessoal, não é uma forma de burlar a disposição constitucional de vedação do anonimato, mas apenas um meio de melhor proteger o titular dos dados e o conteúdo das comunicações. Por esta razão, ganha relevo o princípio da proporcionalidade, que atuará de maneira a estabelecer o equilíbrio entre as medidas restritivas e o direito à proteção de dados pessoais. E com amparo nesta premissa, vale mencionar, por exemplo, que o art. 23 da GDPR destaca que as atividades de prevenção, investigação, repressão e sanção criminal podem limitar o direito à proteção de dados pessoais desde que minimamente respeitem a essência dos direitos e liberdades fundamentais que dele decorrem.

Percebe-se, portanto, que a proporcionalidade é a peça-chave para o alcance do equilíbrio entre o direito à proteção dos dados pessoais, criptografia e a segurança pública,[386] visto que as decisões judiciais de intercepção para fins de investigação criminal também devem ser proferidas em harmonia com a proteção dos direitos dos titulares dos dados, de modo a que não sejam prejudicados.[387] No Brasil, o Supremo Tribunal Federal, em mais de uma ocasião, se manifestou no sentido de que a proteção constitucional do sigilo de comunicações de dados não se confundia com a proteção aos dados em si. Entretanto, o

---

[385] QASIR, Sophia, Anonymity in Cyberspace: Judicial and Legislative Regulations, **Fordham Law Review**, v. 81, p. 3651, 2012, p. 3653.

[386] SHAH, Reema, Law enforcement and data privacy-a forward-looking approach, **Yale LJ**, v. 125, p. 543, 2015, p. 545.

[387] "O caráter fundamental de que se revestem as diretrizes que condicionam a atuação do Poder Público, em tema de restrição ao regime das liberdades públicas, impõe, para efeito de 'disclosure' dos elementos de informação protegidos pela cláusula do sigilo, que o Estado previamente demonstre , ao Poder Judiciário, a ocorrência de causa provável ou a existência de fundadas razões que justifiquem a adoção de medida tão excepcional , sob pena de injusto comprometimento do direito constitucional à privacidade. Nesse sentido, orientam-se diversas decisões proferidas pelo Supremo Tribunal Federal" (INQ 830/MS, Rel Min. Celso de Mello, DJ 1.02.95; INQ 899/DF, Rel Min. Celso de Mello, DJ 23.09.94; INQ 901/DF, Rel. Min. Sepúlveda Pertence, DJ. 23.02.95)

posicionamento da Corte, fruto de acórdão da lavra do eminente Ministro Sepúlveda Pertence, não mais reflete a realidade da evolução tecnológica e a relevância da proteção de dados pessoais no ciberespaço. Ainda assim, o precedente contém questões pertinentes:

> Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso.
> 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a consequente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental.
> 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial.
> 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial".
> 4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270).[388]

Por outro lado, vale observar que o Superior Tribunal de Justiça apreciou tema semelhante por ocasião da impetração de habeas corpus em favor de Daniel Dantas, decorrente de busca e apreensão que resultou na coleta de dados de um *hard drive* (HD) do Banco Opportunity, nas Operações Satiagraha e Chacal. Na ocasião, o STJ analisou especificamente a proteção da garantia constitucional de inviolabilidade do sigilo dos dados em si considerados, com as possíveis consequências ao direito à privacidade de terceiros, correntistas do Banco Opportunity.

Com o auxílio das atuais ferramentas de informática, é possível fazer a separação dos dados de um HD, evitando-se a eventual quebra do sigilo de dados criptografados acobertados pela garantia constitucional. O acesso a dados sigilosos de

---

[388] STF, RE 418.416, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, DJ 19.12.2006. Em precedentes mais antigos, o STJ também se limitava a proteger o sigilo do "fluxo de comunicações em sistema de informática e telemática" (STJ, HC 15.026/SC, Rel. Min. Vicente Leal, Sexta Turma, DJ 24.09.02; REsp 625.214/SP, Rel. Min. Hamilton Carvalhido, Sexta Turma, DJ 29.06.2007). Em precedente da lavra do Ministro Gilmar Mendes, HC 91.867, DJe 24.4.2012: Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados.

terceiros goza de proteção constitucional, não havendo ilegalidade na medida que autoriza o acesso aos dados pertinentes a um crime, mas desde que sejam utilizados instrumentos específicos para a correta busca e separação somente dos dados pertinentes ao fato investigado.[389]

Curioso notar como na referida decisão o Superior Tribunal de Justiça demonstrou um profundo cuidado com o sigilo, a privacidade e a proteção de dados de terceiros não sujeitos à investigação criminal, enquanto que nas recentes decisões judiciais de suspensão dos serviços de comunicação instantânea sequer se atentou para esta possibilidade (grupos de mensagens compartilhadas, fotografias armazenadas em *cloud computing* etc).

Em outro precedente relevante, o Superior Tribunal de Justiça teve a oportunidade de confirmar seu entendimento anterior em torno da proteção e inviolabilidade do sigilo dos dados em si, e não apenas da comunicação de dados. Ao analisar a ilicitude da prova decorrente da apreensão de um telefone celular, cujo acesso aos dados criptografados e às mensagens instantâneas ocorreu sem prévia autorização judicial, a Corte novamente afirmou serem também os dados sujeitos à proteção constitucional:

> Atualmente, o telefone celular deixou de ser apenas um instrumento de conversação pela voz à longa distância, permitindo, diante do avanço tecnológico, o acesso de múltiplas funções, incluindo, no caso, a verificação da correspondência eletrônica, de mensagens e de outros aplicativos que possibilitam a comunicação por meio de troca de dados de forma similar à telefonia convencional. Deste modo, ilícita é tanto a devassa de dados, como das conversas de whatsapp obtidos de celular apreendido, porquanto realizada sem ordem judicial. Ante o exposto, voto por dar provimento ao recurso ordinário em habeas corpus, para declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos.[390]

O precedente reúne elementos muito semelhantes ao julgamento do caso *Riley v. California*, no qual a Suprema Corte dos Estados Unidos reconheceu a necessidade de prévia autorização judicial para o acesso aos dados armazenados em aparelho celular, ou mesmo ao precedente do atentado ocorrido em San Bernardino, no qual se questionou a obrigação de uma empresa viabilizar a criação de um *back door* para corromper os dados

---

[389] STJ, HC 124.253/SP, Rel. Min. Arnaldo Esteves Lima, Quinta Turma, DJe 05.04.2010.

[390] STJ, RHC 51.531/RO, Rel. Min. Nefi Cordeiro, Sexta Turma, DJe 09.05.2016. Cf. Também RHC 75.800/PR, Rel. Min. Felix Fischer, Quinta Turma, DJe 26.09.2016; RHC 67.379/RN, Rel. Min. Ribeiro Dantas, Quinta Turma, DJe 09.11.2016

encriptados. A opinião da Corte foi pronunciada pelo *Chief Justice* John Roberts, que elucidou a necessidade de se separar o acesso físico a um celular do acesso ao conteúdo digital nele armazenado:

> Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon--say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.
> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life". The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.[391]

Um forte indicativo da mudança de panorama das investigações criminais e sua repercussão mundo afora advém da Suprema Corte americana. Em mais de um precedente (U.S. v. Carpenter , U.S. v. Graham[3],[392] e United States v. Wurie, US v. Jones), a Corte se debruçou sobre a licitude das provas digitais criptografadas obtidas de telefones celular pela polícia, sem mandado judicial específico para a apreensão do aparelho e das mensagens e dados nele contidos.

Para evitar as delimitações de escopo inerentes aos mandados judiciais como verificado no caso analisado pelo Superior Tribunal de Justiça, o *Federal Bureau of Investigation* (FBI) e *Department of Justice* (DOJ) tem tentado promover alterações na Rule 41 de modo a obter mandados de busca e apreensão sem limitações territoriais e de escopo[393].

A primeira medida desta natureza foi utilizada no caso Playpen com o intuito de espalhar um *malaware* por computadores mundo afora de modo a obter informações a respeito de uma rede internacional de pedofilia. A prática foi extremamente criticada por instituições como a *Eletronic Frontier Foundation* pela violação do direito à privacidade e inobservância das limitações territoriais e jurisdição para apurar crimes, mas já demonstra o interesse das autoridades em atuar na arquitetura para comprovar as barreiras impostas pela criptografia.

---

[391] ESTADOS UNIDOS DA AMÉRICA, Riley v. California.

[392] United States v. Graham, **Harvard Law Review**, v. 130, 2017.

[393] LERNER, Zach, A warrant to hack: An analysis of the proposed amendments to rule 41 of the federal ruled of criminal procedure, **Yale JL & Tech.**, v. 18, p. 26, 2016.

À medida que mais e mais estamos conectados à internet, maior é o número de "pegadas" digitais geradas a partir da produção de metadados, ou seja, dados sobre outros dados. Metadados são pegadas digitais relevantes, que, cruzadas com outras informações, podem compensar a dificuldade de obtenção de conteúdo criptografado. Na medida em que as empresas de tecnologia se valem a todo instante de metadados para desenvolver novos produtos a partir do diagnóstico de preferências comportamentais, também as autoridades públicas deveriam fazê-lo nas investigações ao invés de meramente de se opor à criptografia ou exigir a sua quebra.

Além do uso de metadados, o *hacking legal* – como no caso Playpen - também tem se popularizado como uma tática investigativa por meio da qual as autoridades, atuando na camada da arquitetura, exploram uma vulnerabilidade de segurança de um dispositivo ou serviço para obter provas de um crime, mediante prévio mandado judicial.

Para além das dificuldades de ordem investigativa e efetividade da persecução criminal, os casos mencionados demonstram que a reconstrução da prova no processo penal atravessa um importante marco de ordem técnica,[394] mas também indicam que o Estado tem buscado atuar na arquitetura da rede para interferir na regulação da proteção dos dados pessoais quando ela é fruto da exclusiva atividade privada e voltada à escapar do controle estatal.[395]

5. A anonimização como instrumento de proteção de dados e distanciamento da regulação

Dados anônimos são aqueles pertinentes a um titular não passível de ser identificado pelo controlador ou por qualquer outra pessoa, tendo em conta todos os meios e tempo razoavelmente necessários. Dados anonimizados não se submetem à aplicação dos marcos regulatórios se não puderem ser objeto de reidentificação[396].

---

[394] Uma das principais controvérsias do momento sobre as formas de contornar as limitações impostas pela criptografia envolve a técnica de espelhamento de conversas. No entanto, o STJ tem entendido que, sem mandado judicial específico, as provas colhidas desta forma também são consideradas ilícitas. Cf. RHC 99.735/SC, Rel. Ministra LAURITA VAZ, SEXTA TURMA, julgado em 27/11/2018, DJe 12/12/2018)

[395] O caso Olmestad v. United States tem uma característica interessante porque na época se entendeu que escutas telefônicas não seriam violação da privacidade pelo fato de não ter ocorrido violação física do domicílio. Este entendimento foi superado pela posição de Brandeis em Katz v. United States

[396] WORKING PARTY 29, **Opinion 5/2014 on Anonymisation Technques**.

Para se chegar à anonimização, a premissa base é a de que os dados pessoais tenham sido coletados e tratados até então em conformidade com a legislação aplicável para esta categoria. Se o processo inicial for de algum modo viciado, o controlador não se exime da responsabilidade pelo período em que os dados eram passíveis de serem associados a uma pessoa identificada ou identificável. Neste contexto, o processamento de dados pessoais para alcançar a anonimização é considerado um exemplo de processamento complementar.

O desenvolvimento de técnicas de anonimização é fruto da atuação regulatória dos desenvolvedores e agentes de mercado, o que mostra em boa medida a capacidade de também influenciarem a regulação feita pelos Estados, que tem incorporado esta técnica em vários ordenamentos jurídicos. Há grande controvérsia sobre a efetiva possibilidade de os dados pessoais estarem sujeitos a um processo que culmine na anonimização. Para alguns pesquisadores[397], a reidentificação é um processo menos complexo do que se supõe e passível de ser realizado por meio de *machine learning* graças à análise de padrões de codificação dos algoritmos. Para se ter a exata dimensão da efetividade das técnicas de anonimização empregadas, três perguntas devem ser feitas:

- Ainda é possível identificar um indivíduo?
- Ainda é possível vincular dados a um indivíduo?
- É possível inferir alguma informação referente a um indivíduo?

Se a resposta for negativa para o teste acima, o processo de anonimização obteve o resultado esperado, pois a reversão não é mais provável dentre de premissas de tempo e custo razoáveis. Apesar do sucesso inicial obtido com a aplicação de camadas que levem anonimização, com a evolução do estado da arte da tecnologia, controladores de dados anonimizados devem permanentemente rever os processos e resultados de modo a manter a consequências das premissas que culminaram no processo de dissociação[398].

Para que se tenha a exata dimensão da dissociação exigida em um efetivo processo de anonimização, vale observar que a "identificação" não significa apenas a possibilidade de recuperar o nome de uma pessoa e/ou endereço, mas também inclui a capacidade de identificação potencial, ou seja, a possibilidade de vinculação de dados a

---

397 Cf. https://freedom-to-tinker.com/2015/01/21/anonymous-programmers-can-be-identified-by-analyzing-coding-style/

398 WORKING PARTY 29, **Opinion 5/2014 on Anonymisation Technques**.

indivíduos e inferência de informações. Em circunstâncias como esta, não interessa quais as intenções do controlador dos dados ou do processador. Desde que os dados sejam identificáveis, invariavelmente serão considerados dados pessoais e sujeitos ao regime jurídico de proteção.

5.1 Técnicas de anonimização: os desdobramentos da regulação privada

A capacidade de atuação privada com as tecnologias disponíveis poderá ser um fator decisivo para o aumento exponencial do uso da anonimização. Atualmente, apenas duas técnicas são mais difundidas entre os desenvolvedores: a randomização e a generalização de dados. Ambas possuem seus pontos fracos, porém sob certas circunstâncias cada uma é capaz de conferir um nível adequado de proteção aos dados pessoais mediante a dissociação. Nem sempre a mera remoção de elementos de identificação direta será suficiente para viabilizar a completa anonimização, de modo que eventualmente será necessário a adoção de medidas complementares para impedir a associação de informações a um titular mediante a vinculação de registros ou a inferência de dados, preferências e comportamentos[399].

A randomização é o conjunto de técnicas que altera a veracidade dos dados para remover a vinculação a um indivíduo. A randomização nem sempre será capaz de reduzir as possibilidades de identificação do titular dos dados, pois os dados ainda serão derivados de um único conjunto, mas combinados com outras técnicas poderão assegurar um nível de abstração considerável.

A generalização é a segunda modalidade dentre as técnicas de anonimização e consiste em ampliar ou diluir os atributos dos titulares de dados, mediante a modificação da respectiva escala ou ordem de magnitude (ex. uma região em vez de uma cidade, um mês em vez de uma semana). Nem sempre a generalização eliminará por completo a possibilidade de identificação, pois requer a adoção de procedimentos sofisticados adicionais para evitar a vinculação e inferência[400].

---

[399] *Ibid*.

[400] *Ibid*.

Como espécies da técnica de generalização, as técnicas de agregação e k-anonimização[401] visam evitar que um indivíduo seja escolhido agrupando-o com pelo menos outros "k" indivíduos. Para viabilizar essa operação, os valores dos atributos são generalizados de tal forma que cada indivíduo compartilha o mesmo valor. Por exemplo, ao diminuir a granularidade de um local em uma cidade para um país, um número maior de dados estarão incluídos e impedirão associações imediatas. Assim, datas de nascimento podem ser generalizadas em um intervalo ou agrupados por mês ou ano para se atingir este objetivo.

Em resumo, a anonimização pode ser considerada uma forma de contornar a atividade regulatória mediante a eliminação irreversível de componentes que poderiam levar à identificação dos indivíduos. Curiosamente, caberá aos desenvolvedores o papel de manter a eficiência das técnicas convencionais de dissociação dos dados em relação aos titulares, o que novamente reforça a tese de que a *Lex Privacy* é um arranjo combinatório de múltiplos fatores regulatórios em torno da *accountability* e do consentimento.

6. A transparência e o acesso à informação como expressão da autodeterminação informativa

Se por um lado a complexa atividade regulatória desenvolvida em conjunto pelo Estado, agentes de mercado e titulares foi capaz de proporcionar o surgimento de novas formas de expressão do compartilhamento e utilização dos dados pessoais, por outro também foi responsável pelo surgimento de direitos específicos no ciberespaço, ainda que fruto do desdobramento de outros.

Em linhas gerais, é possível dizer que o direito de acesso à informação é a principal matriz de garantias asseguradas para os titulares de dados pessoais dentro deste contexto. O conhecimento sobre a finalidade, a duração e os responsáveis pelas atividades de processamento se tornou a base de toda a interação realizada no ciberespaço[402].

Também conhecido como parte da autodeterminação informativa, o direito de acesso é o instrumento capaz de empoderar os titulares dos dados pessoais de modo a

---

[401] QASIR, Anonymity in Cyberspace.

[402] WORKING PARTY 29, **Opinion 3/2010 on the principle of accountability**.

viabilizar a equalização das relações de poder e ampliar as possibilidades de maior controle. Com a magnitude da capacidade de processamento de dados proporcionado pelo *big data* e o *data analytics*, a autodeterminação será o elemento crucial para que os demais direitos tenham uma matriz axiológica sempre voltada aos melhores interesses dos titulares dos dados pessoais.

O direito de acesso aos pessoais significa a possibilidade de obter em tempo razoável do controlador e do processador as informações, confirmações e detalhes sobre a atividade de processamento. Como todo e qualquer direito, o acesso à informação não é ilimitado, porém somente poderá ser restringido por lei e com as razões plausíveis para tanto.[403] Ainda que o acesso seja limitado por lei, o titular dos dados ainda terá a possibilidade de acesso indireto para exercitar os demais direitos a ele associados, como o de retificar os dados, solicitar a exclusão, restringir e se opor ao processamento.

É nesse contexto que a transparência, enquanto fundamento ontológico do direito de acesso, desponta como base para o desdobramento de outros direitos como o direito de retificação, o direito de exclusão, o direito de revisão de decisões automatizadas e o direito de portabilidade. Mesmo antes da previsão legal de várias das hipóteses legais autorizadoras do processamento de dados pessoais, a transparência já era empregada como forma de justificar parte das operações realizadas, a revelar que antes mesmo da atividade legislativa era empregada como uma medida de governança e boas práticas.

Outro desdobramento da transparência e do direito de acesso envolve a forma como a informação deve ser prestada. A rigor, os pedidos dos titulares devem ser atendidos em prazo razoável e sem atrasos desmedidos, por meio de canal de fácil comunicação, em linguagem clara, precisa, concisa e objetiva.

Por isso, dentre outras informações relevantes, o controlador deve ser capaz de informar os tipos de dados que trata, com quem compartilha, as suas respectivas identidades e para quais finalidades. A reunião de todos esses elementos fornecidos pelo controlador permitirá ao titular dos dados identificar se o processamento ocorre em conformidade com

---

[403] Controvérsia relevante sobre o direito de acesso envolve a possibilidade de cobrança de taxas pelo acesso à informação. Embora em alguns países isso seja admitido - ex. Estados Unidos e Europa - , no Brasil a medida é vedada pela Lei Geral de Proteção de Dados Pessoais

alguma base legal, o que significa que o titular dos dados é parte relevante no processo de concretização da *accountability*.

6.1 Controladores e processadores: os destinatários da transferência e direito de acesso

As definições sobre controlador e processador de dados são tão relevantes quanto a delimitação do que sejam dados pessoais. A função de controlador e sua interação com o de processador de dados é fundamental para a compreensão do regime de responsabilidades, bem como para que se saiba em face de quem os titulares dos dados exercerão os seus direitos. A rigor, as funções de controlador e operador são fruto de uma evolução dos papeis dos agentes de mercado e da forma como essas interações envolvem a assunção de responsabilidades. Nem sempre a delimitação conceitual é clara e reflete a realidade das funções desempenhadas, todavia o desenvolvimento regulatório das duas posições demonstra como nem sempre só a regulação estatal foi decisiva[404].

A despeito da inicial definição pela via contratual dos papéis de controlador e processador, aos poucos as legislações foram incorporando os seus conceitos.[405] Mais recentemente, GDPR e LGPD trataram do controlador como toda pessoa física ou jurídica, pública ou privada, que sozinha ou em conjunto com outra determina os fins e os meios de processamento de dados pessoais. Por outro lado, consideram processador toda pessoa física ou jurídica, pública ou privada, que processa os dados em nome do controlador. Em outras palavras, as definições e os avanços em torno da posição de controlador e processador são fruto de dois aspectos relevantes, ou seja, a necessidade de se identificar os responsáveis pelo processamento de um lado e a consequente atribuição a eles do dever de assegurar direitos aos titulares.

6.1.1 O papel do controlador

Com efeito, o controlador era visto como alguém que desempenhava atividades estáticas estritamente vinculadas aos dados pessoais em si considerados, todavia com o passar

---

[404] WORKING PARTY 29, **Opinion 1/2010 on the concepts of controller and processor**, Bruxelas: [s.n.], 2010.

[405] A primeira aparição do conceito de controlador apareceu na Convenção 108 do Conselho Europeu. Cf. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

do tempo e evolução das habilidades de gestão das informações, a regulação passou a recair principalmente sobre as diversas atividades de processamento que poderiam ser realizadas e a simultânea capacidade de interação com outros controladores e processadores.

O primeiro e mais importante papel do controlador é ser o responsável pelo cumprimento das regras de proteção de dados e tornar-se referência para o exercício de direitos por parte dos titulares. O controlador é, portanto, o ponto de alocação operacional da responsabilidade sob todas as perspectivas: exercício de direitos e responsabilidade civil. A delimitação da atuação do controlador é essencialmente funcional e objetiva traçar um regime de responsabilidade em função da sua influência operacional.

Um dos principais pontos de atenção dos arranjos privados e seus reflexos sobre a definição dos papéis de controlador e processador envolve as estruturações societárias (empresas transnacionais e *offshores*, parcerias contratuais e subcontratação (*cloud computing*). Em algumas circunstâncias, arranjos privados podem dificultar e até objetivar descaracterizar a função de controlador de um determinado agente de mercado. Isso tem se revelado um fator preocupante em virtude de os dados serem hospedados em diversificadas jurisdições, bem como em função das operações de tratamento realizadas por empresas transnacionais[406].

A solução para parte desses desdobramentos proporcionados pela evolução da tecnologia decorre do regime de responsabilidade civil que alguns ordenamentos jurídicos adotaram como resposta para os arranjos mencionados. No Brasil, a responsabilidade solidária do controlador e do processador foi o caminho encontrado, ao passo que na União Europeia a nomeação de um representante por parte do controlador foi a forma de assegurar a eficácia das sanções impostas para aqueles que lá não estão fisicamente estabelecidos.

Importante salientar que a condição de controlador não é propriamente uma escolha passível de ser imposta contratualmente, mas decorre de uma circunstância factual fundada na opção por processar dados pessoais de acordo com a sua decisão. Por isso, uma indicação meramente formal da figura do controlador para cumprir obrigações legais não terá o condão de afastar as verdadeiras premissas fáticas da atividade de tratamento, isto é, em qualquer circunstância será considerado controlador aquele que estiver na condição de tomar as decisões e definir em concreto a finalidade do processamento de dados pessoais.

---

[406] WORKING PARTY 29, **Opinion 1/2010 on the concepts of controller and processor**, p. 1.

Por outro, a ausência de indicação legal ou contratual de quem seja o controlador também não é relevante dentro da perspectiva factual sobre quem é o responsável pela tomada de decisões. A análise da realidade em concreto poderá proporcionar a identificação dos critérios que levarão a esta conclusão. Uma das formas de analisar se determinado agente atua como controlador - e, portanto, influencia os meios do processamento - decorre da sua capacidade de definir a finalidade mediante a indicação de aspectos técnicos e organizacionais da delegação (natureza dos dados, forma de processamento, período de retenção e terceiros com quem compartilhar).

Sob o prisma da definição de responsabilidades e de modo a assegurar melhores condições para o exercício de direitos por parte dos titulares dos dados, não se deve confundir a indicação do controlador com a de um empregado nomeado para conduzir as atividades dentro de uma empresa ou grupo econômico. A rigor, esse indivíduo seria o *data protection officer*, cujas atribuições não se confundem com a do controlador, enquanto responsável pela indicação da finalidade do tratamento. Se um empregado ou outra pessoa física processar os dados fora do escopo de atuação da pessoa jurídica empregadora, ele poderá ser considerado controlador e responderá por seus atos. Esse é o caso, por exemplo, do responsável por um incidente de segurança com vazamento de dados, que será sempre considerado o controlador, seja ele pessoa física ou jurídica[407].

O controle poderá ser exercido individualmente ou de forma conjunta. O controle conjunto ocorre quando ao menos duas partes distintas determinam, em relação a operações específicas de processamento, a finalidade ou os elementos essenciais dos meios que caracterizam a atuação de um controlador, ainda que desempenhem papéis com pesos diferentes.

As funções do controlador tem se ampliado expressivamente em contraposição à constante diversificação das possibilidades de coleta e processamento de dados pessoais. No entanto, o anseio regulatório analítico empregado por muitos ordenamentos jurídicos tem feito com que as funções do controlador rapidamente se tornem obsoletas diante da efetividade de direitos a serem assegurados aos titulares.

Como a capacidade de processamento dos controladores é exponencial, a previsão exaustiva de suas funções fatalmente levará a um rápido esgotamento do padrão

---

[407] *Ibid*.

regulatório adotado para delimitar as suas atividades. O papel a ser desempenhado pela *lex privacy* é exatamente viabilizar ferramentas regulatórias capazes de compreender a posição contextual do controlador e, a partir desse patamar, regular o grau de responsividade e *accountability*.

6.2 As atividades do processador

Assim como as funções do controlador, o processador também pode desempenhar uma diversidade de papéis a partir de diferentes arranjos operacionais. A atuação do processador é praticamente toda definida pelo controlador, de sorte que existe pouca margem de atuação para a adoção de medidas fora das orientações do controlador. Ao contrário da originária previsão do controlador pela Convenção 108 do Conselho Europeu, a delimitação das funções do processador é mais recente (Diretiva 95/46/CE) e fruto do desenvolvimento de redes de interação entre agentes de mercado e desenvolvedores.

Duas condições essenciais são necessárias para a definição da posição de processador: (i) ser um ente distinto do controlador e (ii) tratar dados pessoais em seu nome. Em princípio, o papel do processador não deriva da natureza do tratamento realizado, mas de suas atividades factuais em um contexto específico, ou seja, o mesmo ente pode agir ao mesmo tempo como um controlador para certas atividades e como processador para outras[408].

Agir em nome do controlador significa atuar segundo as hipóteses legais de tratamento a ele aplicadas e por sua delegação, o que significa que se atuar fora das diretrizes estipuladas também poderá ser considerado um controlador (controle conjunto). Importante esclarecer, ainda, que, nem toda relação de subcontratação importa na condição de processador do subcontrato, visto que é possível que se trate de uma hipótese de controle conjunto ou até independente.

A despeito da condição de processador derivar de uma circunstância factual, os arranjos contratuais são deveras importantes para definir o compartilhamento de orientações, alocação de responsabilidade, previsão de ressarcimento por danos causados ou até limitação/exclusão de indenização. São comuns contratos de processamento de dados (*data processing agreements*) por meio dos quais as partes estipulam contratualmente medidas

---

[408] *Ibid*.

mitigadoras de sanções ou formas de compensação por força de um regime mais severo de responsabilidade civil.

Em virtude das complexas relações societárias e as redes contratuais distribuídas por várias jurisdições, não há nenhum óbice a que um controlador atue com vários processadores em uma mesma operação. A condição básica para esta atividade de processamento é que todos eles atuem em nome e segundo as diretrizes do controlador, com a alocação das suas respectivas atribuições.

A despeito das regulações estatais estarem muito focadas na posição do controlador, o papel do processador não deve ser considerado de somenos importância, em especial porque a atividade do processador é a mais frequente, na medida em que para um controlador é possível que existam processadores atuando sob diversas perspectivas. Uma tendência regulatória, portanto, é ampliar parte da responsividade do processador[409].

6.3 O papel do Data Protection Officer como parte da regulação privada e accountability

Como parte da internalização da responsividade, *accountability* e diminuição da presença estatal nas atividades cotidianas de processamento, a nomeação de um *data protection officer* (DPO) ou encarregado de proteção de dados pessoais tem se notabilizado por fomentar a cultura da privacidade em âmbito corporativo. A criação da figura do DPO é fruto da experiência de alguns ordenamentos com a incapacidade de lidar com as atividades cotidianas de processamento e os riscos dela decorrentes. Com efeito, nenhum órgão regulador estatal teria condições de fiscalizar e controlar as atividades de empresas dos mais diversos setores e com complexas operações. A solução encontrada, portanto, foi a designação de uma figura que pudesse concentrar internamente essas atribuições e funcionar como ponto de contato com as autoridades estatais de proteção de dados pessoais.

Em linhas gerais, a nomeação do DPO é obrigatória para os controladores e, em alguns ordenamentos, também para os processadores, mas mesmo em situações nas quais não há imposição legal, algumas empresas voluntariamente tem optado pela indicação como

---

[409] WORKING PARTY 29, **Opinion 1/2010 on the concepts of controller and processor**.

medida de governança[410]. Além de facilitar a implementação da responsividade mediante avaliações de impacto sobre dados pessoais (DPIA-Data Protection Impact Assessment) e auditorias, os DPOs também atuam como intermediários das empresas e demais funcionários, da empresa com clientes e da empresa com as autoridades. O DPO é o responsável pela difusão da cultura de proteção de dados, implementação de boas práticas e realização de constantes treinamentos. Importante ressaltar que os DPOs podem ser pessoas físicas ou jurídicas e não são pessoalmente responsáveis pelos atos praticados pelo controlador, pois sua única atribuição é demonstrar as condições em que a atividade de processamento de dados pessoais ocorre. Se for um empregado do controlador, o DPO deve ter acesso a recursos, independência e autonomia para exercer suas atividades, de sorte que não poderá estar submetido a orientações superiores para exercer suas funções precípuas e nem ser demitido ou punido por desempenhá-las corretamente.

A escolha e as características de um DPO são variáveis, dependem da complexidade das operações de tratamento do controlador e nem sempre decorrem de previsão em lei. Em boa medida, recomenda-se que o DPO seja alguém com conhecimento sobre proteção de dados e regulação, além de não ter conflitos de interesse para desempenhar a função. Dentre as principais funções do DPO, destaca-se a obtenção de informações para identificar atividades de processamento, análise e verificação da conformidade das atividades de processamento e aconselhamento e emitir recomendações ao controlador ou ao processador[411].

7. Interesse legítimo como instrumento dinâmico de controle da atuação privada

Outra categoria regulada considerada como uma expressão das interações contextuais ocorridas no ciberespaço é o denominado "interesse legítimo" do controlador dos dados pessoais. Um interesse legítimo pode ser definido como a ampliação da participação que um controlador pode ter no processamento de dados pessoais ou um benefício que o controlador pode obter do processamento. Para ser legítimo, o interesse deve ser suficientemente articulado com as atividades do controlador de modo a permitir que o teste de equilíbrio seja

---

[410] WORKING PARTY 29, **Opinion on Data Protection Officers (DPOs)**, Bruxelas: [s.n.], 2017.

[411] *Ibid*.

realizado em contraste com os direitos fundamentais do titular dos dados pessoais. Por essa razão, é essencial que se trate de um interesse real e atual, passível de ser exercido em conformidade com a lei, ou seja, algo que corresponda às atividades atuais ou benefícios que são esperados num futuro próximo, o que significa que interesse vagos ou considerados injustificados não serão suficientes.

Trata-se de uma ferramenta destinada a viabilizar determinadas operações de tratamento conduzidas pelo controlador a partir de uma relação intrínseca com suas atividades. Os principais exemplos do uso do interesse legítimo são o marketing direto, as mensagens não comerciais (ex. eleitorais e de caridade), *whisttleblowing*, monitoramento de funcionários para fins de segurança e prevenção à fraude e uso indevido de serviços.

A natureza aberta do interesse legítimo desperta uma série de controvérsias a respeito do seu âmbito de aplicação, o que não significa necessariamente que essa opção deva ser vista como um último recurso ou somente empregada quando as demais bases legais não forem aplicáveis. Também não deve ser considerada como uma opção preferida e empregada reiteradamente em detrimento das demais hipóteses legais, uma vez que invariavelmente demandará a submissão ao teste de equilíbrio com os direitos dos titulares dos dados pessoais. Assim, monitorar as atividades *on-line* de seus clientes, combinar grandes quantidades de dados de diferentes fontes, contextos e para fins diversos com o intuito de formar perfis de comportamento e preferências, sem o seu conhecimento, pode ser considerado uma medida abusiva.[412]

A despeito da ausência de hierarquia entre as hipóteses de tratamento de dados pessoais previstas nos ordenamentos jurídicos, é consenso entre a maioria da doutrina que o interesse legítimo pode ser considerado uma justificativa mais suscetível a contestações, na medida em que sempre sujeito à revisão caso-a-caso por parte das autoridades de proteção de dados, no tocante ao teste de necessidade e proporcionalidade.

Enquanto categoria dinâmica e de conteúdo variável, o interesse legítimo pode ser considerado uma das hipóteses de tratamento mais sujeitas à ideia de privacidade contextual e pluralística, corroborando a perspectiva de que a *lex privacy* deve ser compreendida como um modelo regulatório capaz de atender as mais diversas características de processamento do

[412] Uma das significativas controvérsias diz respeito à possibilidade de autoridades públicas processarem dados pessoais com base no legítimo interesse.

ciberespaço.

Nesse capítulo a regulação foi analisada sob a perspectiva do objeto regulado, ou seja, o produto da atuação regulatória por parte dos mais variados atores e segundo os ditames da policontextualidade. Para que fosse possível contrastar as diferentes formas de expressão da regulação sobre o conteúdo regulado, foram selecionados pontos de convergência entre atuação privada e pública. Com foco nos conceitos construídos a partir das manifestações de pluralismo jurídico ao longo da tese, no próximo capítulo serão apresentados os contornos da *Lex Privacy* e como a accountability lhe confere fundamento de validade axiológica para confrontar as assimetrias de poder manifestadas pelas plataformas digitais normativas.

CAPÍTULO 4 – A *LEX PRIVACY* EM PERSPECTIVA

1. Plataformas digitais normativas e o regime de governança da proteção de dados

Nos capítulos anteriores, analisamos a forma como a regulação do cibersespaço ganhou seus primeiros contornos e posteriormente descemos ao patamar da regulação da proteção dos dados pessoais para contextualizar a influência sobre os modelos apresentados em sintonia com a formatação do conteúdo regulado. Nesse capítulo, analisaremos o regime de governança da privacidade e a estruturação da *Lex Privacy*. Para tanto, adotaremos como referencial de estudo da governança da privacidade as interações ocorridas nas plataformas digitais e as manifestações de poder no tratamento de dados pessoais.

Vale ressaltar que, para os fins dessa tese será considerada governança da proteção de dados e privacidade as questões relacionadas à engenharia e gerenciamento de infraestrutura para transmissão de dados, o que inclui a forma sobre como essa infraestrutura é usada e como o *design* afeta o conteúdo dos dados transmitidos[413]. Governança parece ser o termo adequado para descrever os processos abertos e a concepção de estruturas normativas que se desenvolvem no ciberespaço a partir da atuação de vários tipos de atores. Governança também é um termo frequentemente utilizado para descrever estruturas e processos em diferentes níveis de comunicação e contexto, os quais podem ser distinguidos (i) em relação aos conteúdos informativos e serviços que os usuários das redes geram; (ii) em função de protocolos e outros requisitos lógicos destinados à habilitação de serviços e aplicativos com foco em geração e transmissão de conteúdo; (iii) e em razão da infraestrutura física, por meio de sistemas operacionais responsáveis pelas transferências de dados[414].

Quando olhada pelo prisma da privacidade, a governança tem sido compreendida como um conjunto de mecanismos voltados à coordenação de processos, atividades, pessoas e fluxos informacionais, sob influência da regulação estatal, da corregulação e da autorregulação, que proporcionam a compreensão policontextual da

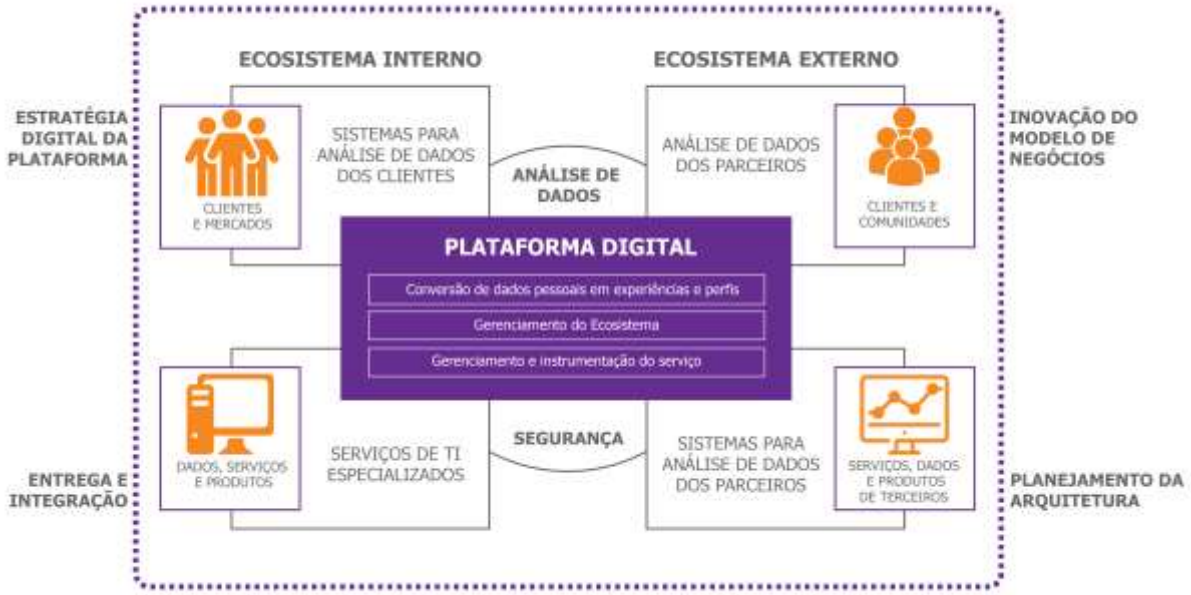
---

[413] BYGRAVE, Lee A., **Internet Governance by Contract**, [s.l.]: Oxford University Press, 2015.

[414] HILDEBRANDT, Legal and technological normativity: more (and less) than twin sisters.

proteção de dados pessoais[415]. Dessa forma, a definição de governança da privacidade tem sido aplicada principalmente a estruturas normativas mais ou menos institucionalizadas, materializadas nas políticas das corporações (internas e externas), contratos, códigos de conduta, leis e políticas públicas[416].

A configuração de processos, definição de linguagem, estruturação de respostas e fluxos, a criação de regras, preferências e decisões representa parte da definição policontextual de funcionamento de uma plataforma enquanto rede de interação entre empresas, desenvolvedores, usuários e poder público[417]. A governança de uma plataforma digital pode ter variados matizes – anticorrupção, lavagem de dinheiro, gestão etc - , de sorte que a privacidade é apenas um deles e nem sempre o de maior destaque.



A estruturação de um regime de governança é a base da funcionalidade de uma plataforma digital enquanto subsistema parcial destinado a proporcionar (i) meios de

[415] BENNETT, **The Governance of Privacy**, p. 237.

[416] MAST, Tobias; OERMANN, Markus; SCHULZ, Wolfgang, Doing Internet Governance: Constructing Normative Structures Inside and Outside of Intermediary Organisations, *in*: **Annual Symposium 2016**, Washington: [s.n.], 2016; EPSTEIN, Dmitry; KATZENBACH, Christian; MUSIANI, Francesca, Doing internet governance: practices, controversies, infrastructures, and institutions, **Internet Policy Review**, v. 5, n. 3, 2016.

[417] FLYVERBOM, Mikkel, **The power of networks: Organizing the global politics of the internet**, [s.l.]: Edward Elgar Publishing, 2011.

cooperação e compartilhamento entre usuários, (ii) interações de ordem social e econômica em condições de igualdade ou (iii) perpetuação de modelos de negócios com expressiva manifestação de poder econômico[418]. A linha de análise dessa tese é essencialmente focada na terceira hipótese indicada acima, sobretudo porque mais distante de preocupações com a privacidade e proteção de dados pessoais, bem como manifestações de pluralismo e policontexualidade. Apesar das manifestações de poder também ocorrerem fora das plataformas, a escolha delas como referencial de análise se deve à governança estruturada em torno dos dados pessoais e retroalimentação de interesses por meio deles.

Plataformas digitais são modelos de negócios que se popularizaram na economia do compartilhamento, ainda que a antecedam e a ela não se limitem[419], conforme pontua Ana Frazão[420]. Inicialmente destinadas à cooperação e coordenação entre usuários para viabilizar o compartilhamento de interesses, serviços, bens e diminuir eficiências alocativas, aos poucos as plataformas digitais tornaram-se arenas de concentração de poder econômico e orientação de tendências políticas e sociais.

No mundo físico, plataformas digitais nada mais consistem do que estruturas comerciais que aproximam produtos, serviços e pessoas, ampliando as possibilidades de interação e satisfação de interesses, como ocorre em feiras de antiguidades e de alimentos. A rigor, este modelo de atividade econômica representa a concregação de meios de produção, serviços e funcionalidades em uma mesma rede de comunicação, com o objetivo de facilitar e potencializar as transações e interconexões[421]. A principal particularidade do modelo de plataformas digitais do ciberespaço em relação às suas manifestações do mundo físico

---

[418] FRAZÃO, Ana de Oliveira, Plataformas digitais e os desafios para a regulação jurídica, *in*: PARENTONI, Leonardo; GONTIJO, Bruno Miranda; LIMA, Henrique Cunha Souza (Orgs.), **Direito, Tecnologia e Inovação**, Belo Horizonte: D'Plácido, 2018, v. I, p. 645.

[419] SCHOR; FITZMAURICE, 26. Collaborating and connecting.

[420] Ana Frazão salienta que "economia do compartilhamento diz respeito fundamentalmente à cooperação entre indivíduos autônomos a fim de assegurar o aproveitamento mais eficiente e racional de bens ociosos". FRAZÃO, Plataformas digitais e os desafios para a regulação jurídica, p. 644. Por esta razão, a associação automática entre economia do compartilhamento e plataformas digitais deve ser evitada. No mesmo sentido, cf. RANCHORDÁS, Sofia, Does sharing mean caring: Regulating innovation in the sharing economy, **Minnesota Journal of Law, Sciense & Technology**, v. 16, 2015.

[421] CALO, Ryan; ROSENBLAT, Alex, The taking economy: Uber, information, and power., **Columbia Law Review**, v. 117, p. 1623–1690, 2017.

envolve a exponencialidade com que promove o *matching*[422] entre indivíduos e seus interesses[423].

1.1 Primeira manifestação de normatividade: conversão de dados em experiências

Ao dar exponencialidade às interações, captar dados e convertê-los em experiências segundo os hábitos vivenciados pelos usuários, as plataformas digitais otimizam suas margens de lucro e operam em patamares expressivos de redução de custos, o que tem se tornado o primeiro degrau para as posteriores perpetuações de poder, como a definição da destinação e uso de bens titularizados pelos usuários[424].

Enquanto centros de coordenação e intermediação das interações entre usuários, as plataformas tornam-se um fim em si mesmo, na medida em que retroalimentam comportamentos a partir da reiterada conversão dos dados dos usuários em novas experiências, conforme destacado por Zuboff no capítulo anterior[425]. Por meio da conjugação do que Gutwirth e De Hert[426] denominam como *opacity normative tools*, isto é, o *targeting*, *tracking* e o *profiling*[427], as plataformas digitais se valem de técnicas de direcionamento de produtos, serviços e formação de perfis comportamentais para consolidar sua influência sobre os titulares dos dados pessoais nas vilas globais, ignorando a policontextualidade e os valores democráticos.

Com isso, as plataformas concentram mais informações sobre perfis comportamentais[428] e conseguem personificar os seus produtos e serviços de acordo com o tipo de interesse do usuário[429]. Essa é a primeira manifestação de normatividade das plataformas digitais: autogeração de riqueza a partir da conversão de dados em

---

[422] EVANS, David S.; SCHMALENSEE, Richard, **Matchmakers: the new economics of multisided platforms.**, Massachusetts: Harvard Business Press Review, 2016.

[423] SUNDARARAJAN, Arun, **The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism**, [s.l.]: The MIT Press, 2016.

[424] FRAZÃO, Plataformas digitais e os desafios para a regulação jurídica.

[425] ZUBOFF, **The age of surveillance capitalism**.

[426] GUTWIRTH; DE HERT, Regulating profiling in a democratic constitutional state.

[427] BERNAL, Paul, **Internet Privacy Rights: Rights to Protect Autonomy**, Cambridge: Cambridge University Press, 2014, p. 144–145.

[428] GUTWIRTH; DE HERT, Regulating profiling in a democratic constitutional state.

[429] BORGESIUS, Personal data processing for behavioural targeting; VENKATADRI *et al*, Privacy Risks with Facebook's PII-based Targeting.

experiências[430]. Em outras palavras, ao regrar e influenciar condutas a partir da prévia captação de dados pessoais para a transformá-los em novos produtos e funcionalidades, as platafomas digitais expressam sua normatividade por meio da tecnologia. É por esta razão que a cada dia se torna mais premente o emprego de *transparency tools* como a *Lex Privacy* para compelir plataformas digitais e os demais os *stakeholders* a agirem com clareza e *accountability.*

1.2 Segunda Manifestação de Normatividade: criação de regras e procedimentos próprios

Após a dominação dos dados pessoais e influência sobre as preferências, o segundo traço da normatividade das plataformas digitais advém da criação de regras próprias de conduta para os usuários, capazes de disciplinar conflitos[431] e inovar no desempenho da atividade econômica como nas relações *peer-to-peer*[432]. É o que Hildebrandt denomina de normatividade tecnológica:

> "If we look at the normative impact of technological devices or infrastructures we must admit that many of the effects they produce on our everyday behaviors have not been planned. Contemporary common sense would describe them as side-effects, even in the case that these unplanned effects outweigh explicitly intended effects. When speaking of technological normativity I do not focus on the intention of the designer, I simply refer to the way a particular technological device or infrastructure actually constrains human actions, inviting or enforcing, inhibiting or prohibiting types of behavior. Such normativity does *not* depend on deliberate delegation since it may emerge unexpectedly in the interactions between devices, infrastructures and humans who make use of them (and are to a certain extent constituted by them)." [433]

---

[430] THALER, Behavioral economics; ACQUISTI; BRANDIMARTE; LOEWENSTEIN, Privacy and human behavior in the age of information.

[431] CONSELHO NACIONAL DE JUSTIÇA, **CNJ premia Mercado Livre por conciliar conflitos antes do processo judicial**. Um dos mais interessantes exemplos de plataformas digitais normativas capazes de atuar na solução de conflitos é o Kleros, que utiliza o *blockchain* para arbitragens online. Cf. **Kleros:The Blockchain Dispute Resolution Layer**, disponível em: <https://kleros.io/>, acesso em: 12 fev. 2019. Sob o prisma da autorregulação e fragmentação de resolução de conflitos online, cf. ARBIX, Daniel do Amaral, **Resolução Online de Controvérsias**, São Paulo: Intelecto, 2017.

[432] CORTESE, Loans That Avoid Banks?; BENKLER, Yochai; NISSENBAUM, Helen, Commons-based Peer Production and Virtue, **Journal of Political Philosophy**, v. 14, n. 4, p. 394–419, 2006; RANCHORDÁS, Does sharing mean caring: Regulating innovation in the sharing economy.

[433] HILDEBRANDT, Legal and technological normativity: more (and less) than twin sisters, p. 175.

As regras e procedimentos criados pelas plataformas digitais por meio de termos de uso, políticas e regulamentos objetivam orientar comportamentos e ampliar os incentivos de interação com os demais usuários. Um dos mais marcantes exemplos desse fenômeno são os formulários e procedimentos adotados por *search engines* ou *buscadores*[434] para a desindexação e desvinculação de informações do perfil de determinados usuários, em especial após a decisão da Corte Europeia de Justiça no caso Mario Costeja vs. Google Spain[435], conhecido como o caso *Right to be Forgotten*[436]. Sem qualquer interferência estatal na intermediação da solução de conflitos, algumas dessas plataformas se tornaram verdadeiros responsáveis por tutelar direitos como a liberdade de expressão e o devido processo legal ou tolher condutas em seu ecossistema como o discurso de ódio[437] e fraudes, numa clara manifestação de pluralismo jurídico e percepção policontextual da privacidade[438]. Esse fenômeno aponta para a questão desta pesquisa:

> "how normative structures are established; in other words, how the rules for information flows on intermediaries evolve, especially in such situations of 'private ordering', 'transfer of law enforcement' or 'regulated self-regulation' to the organisations of intermediary service providers."[439]

Trata-se, portanto, da constatação de um fenômeno dado, ou seja, de uma manifestação de poder sobre a qual é necessária uma profunda reflexão e mecanismos de controle para que se tenha a certeza de que plataformas digitais normativas desempenham essa função com imparcialidade, igualdade de condições e em conformidade com o ordenamento jurídico estatal. A posição de centralidade ocupada por algumas das plataformas digitais no ciberespaço as coloca em expressiva condição normativa hierárquica se

---

[434] BERNAL, **Internet Privacy Rights**, p. 117; PASQUALE, The Black Box Society, p. 61–62.

[435] ECJ, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Cumpre observar que, pelo regime de responsabilidade do art. 19 do Marco Civil da Internet, caberá ao Poder Judiciário, exclusivamente, a função de dirimir conflitos entre usuários e determinar qual direito deve prevalecer e, se for o caso, ordenar a remoção do conteúdo por meio de ordem judicial específica, com indicação precisa da respectiva URL.

[436] BERNAL, Paul Alexander, A right to delete?, **European Journal of Law and Technology**, v. 2, n. 2, 2011; MAYER-SCHÖNBERGER, Viktor, **Delete: the virtue of forgetting in the digital age**, New York: Princeton University Press, 2011.

[437] WOOLGAR, Steve; NEYLAND, Daniel, **Mundane governance: Ontology and accountability**, Oxford: OUP Oxford, 2013.

[438] MAST; OERMANN; SCHULZ, Doing Internet Governance.

[439] DENARDIS, Laura, **The global war for internet governance**, [s.l.]: Yale University Press, 2014, p. 154.

comparadas com outras fontes de manifestação do direito nas vilas globais[440], o que exige a adoção de medidas contrafactuais para se preservar a autonomia informativa, a privacidade e os valores democráticos[441].

1.3 Terceira manifestação de normatividade: empreendedorismo evasivo

A terceira manifestação de poder normativo das plataformas digitais envolve o que Elert e Henrekson denominam de empreendedorismo evasivo, que em parte se traduz na tentativa de fugir à regulação mediante a propagação discursiva da disrupção e o incentivo ao profissionalismo na oferta de bens e serviços de forma direta ou mediante intermediação, como forma de replicar modelos tradicionais de negócio no ciberespaço:

> "We define evasive entrepreneurship as we define evasive entrepreneurship as profit-driven business activity in the market aimed at circumventing the existing institutional framework by using innovations to exploit contradictions in that framework. We formulate four propositions regarding the character of evasive entrepreneurship, the institutional conditions that make evasive entrepreneurship likely, and its consequences for welfare and institutional change. While evasive entrepreneurship can take many forms depending on the context in which entrepreneurs operate, we identify a number of common features. First, evasive entrepreneurs are entrepreneurial in the Schumpeterian sense, creating and commercializing something new and disruptive – a technological and/or organizational innovation. Second, they use their innovations to behave in a Kirznerian fashion with respect to institutional contradictions, that is, they either engage in evasive behavior or enable others to engage in evasive behavior. Third, and as a consequence of the second feature, these entrepreneurs disrupt both market and institutional equilibria.
>
> As with other types of entrepreneurship, evasive entrepreneurship may be productive or unproductive, thus either increasing or lowering social welfare. Yet the most important effects of evasive entrepreneurship are likely to be dynamic, since it often functions as a remedy for the inertia of political and economic institutions. In times of rapid change, driven for example by a high rate of technological progress or new sup-plies of resources, economic adaptability may be difficult or impossible if actors invariably abide by existing institutions (Etzioni 1987). In such circumstances, evasive entrepreneurship prevents existing institutions from stifling economic development.
>
> Furthermore, if it becomes sufficiently economically important, evasive entrepreneur-ship can trigger a response from lawmakers and regulators." [442]

---

[440] BALKIN, Jack M., Virtual liberty: Freedom to design and freedom to play in virtual worlds, **Virginia Law Review**, 2004.

[441] SCHOR, Juliet, Debating the sharing economy, **Journal of Self-Governance & Management Economics**, v. 4, n. 3, 2016.

[442] ELERT, Niklas; HENREKSON, Magnus, Evasive entrepreneurship, **Small Business Economics**, v. 47, n. 1, p. 95–113, 2016.

Ranchordás ressalta que a economia do compartilhamento, inicialmente centrada no modelo de cooperação e coordenação *peer-to-peer*, se tornou um campo propício para a migração de modelos tradicionais de negócios[443], que sob o discurso da mudança das garrafas e não do vinho, objetivam a redução de custos marginais e externalidades de mercado[444].

Ao invés do aproveitamento racional de bens ociosos e otimização de oportunidades de interconexão sob o prisma da policontextualidade, as plataformas digitais se transformaram em instrumentos de propagação da tradicional subcontratação, ou seja, plataformas de intermediação de relações empregatícias e empresariais convencionais, cuja mera replicação naturalmente justificaria o recurso aos correspondentes mecanismos de regulação do mundo físico[445], sob pena de se estimular o empreendedorismo evasivo. Bens e serviços de mesma natureza devem se submeter aos mesmos parâmetros regulatórios para que se evitem distorcidos incentivos de mercado. A práxis discursiva orientada por "negócios jurídicos gratuitos" e outros benefícios econômicos não pode se sobrepor à realidade regulatória, como a necessidade do consentimento[446].

Sob a ótica da proteção dos dados pessoais e privacidade, o empreendedorismo evasivo também se vale da roupagem discursiva em torno de novos modelos de negócios e benefícios para se afastar da regulação. Sem uma clara percepção dos ganhos de *accountability,* legitimidade e transparência decorrentes de um modelo de corregulação equilibrado, conforme defendido pela Comissão Europeia[447], algumas dessas plataformas digitais buscam essencialmente na autorregulação as soluções para os subsistemas sociais

---

[443] Magrani analisa a contribuição da inovação sob o prisma dos impactos econômicos no processo capitalista e da perspectiva construtivista, MAGRANI, Eduardo, **A Internet das Coisas**, Rio de Janeiro: FGV, 2018, p. 21–24.

[444] RANCHORDÁS, Does sharing mean caring: Regulating innovation in the sharing economy.

[445] FRAZÃO, Plataformas digitais e os desafios para a regulação jurídica.

[446] É por essa razão que Thaler e Sunstein mencionam que a *choice architecture* pode ser essencial para influenciar determinados comportamentos, como se observa nos "negócios jurídicos gratuitos" que visam a coleta de dados pessoais cada vez maior em troca de vantagens: "*choice architecture is both good and bad, is pervasive and unavoidable, and it gratly affects our decisions"*. THALER; SUNSTEIN, **Nudge**, p. 255.

[447] EUROPEAN COMMISSION, **Regulation on promoting fairness and transparency for business users of online intermediation services**, Digital Single Market - European Commission, disponível em: <https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services>, acesso em: 12 fev. 2019.

parciais em que atuam[448]. O interesse legítimo, a criptografia e a anonimização foram no passado alguns desses exemplos, antes mesmo de se submeterem à regulação estatal[449], conforme destacado no capítulo anterior.

Plataformas digitais normativas constroem regimes de governança favoráveis aos seus interesses e nem sempre consentâneo com a privacidade e proteção de dados pessoais[450]. A policontextualidade é ofuscada em favor dos interesses corporativos e da perpetuação da conjuntura de poder normativo, ao invés de atuar como mecanismo de compreensão dos vários panoramas dos *stakeholders* envolvidos. Por essa razão, Jack Balkin sustenta que as plataformas digitais deveriam ser pensadas em um formato de governança plural:

> "In virtual worlds, the relationship between platform owners and players is not simply one between producers and consumers. Rather, it is often a relationship of governors to citizens. Virtual worlds form communities that grow and develop in ways that the platform owners do not foresee and cannot fully control. Virtual worlds quickly become joint projects between platform owners and players. The correct model is thus not the protection of the players' interests solely as consumers, but a model of joint governance."[451]

É neste sentido que a *Lex Privacy* deve ser compreendida como um instrumento regulatório de condução da governança das plataformas digitais normativas, que não devem ser imunes a outras formas de regulação[452]. A *Lex Privacy*, enquanto arcabouço normativo formado por um conjunto de instrumentos regulatórios e experiências plurais

---

[448] FINCK, Michèle, Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy, **European Law Review**, 2018.

[449] Hoje, a criptografia tem previsão em normas como a GDPR, o Cloud Act, o California Consumer Privacy Act, a Lei Geral de Proteção de Dados e o Decreto Regulamentador do Marco Civil da Internet. Da mesma forma ocorre com a anonimização, o interesse legítimo e as funções do *data protection officer*, do controlador e do processador.

[450] WICHOWSKI, Alexis, **Facebook and Google are actually "Net States" and they rule the world**, Wired, disponível em: <https://www.wired.com/story/net-states-rule-the-world-we-need-to-recognize-their-power/>, acesso em: 12 fev. 2019.

[451] BALKIN, Virtual liberty: Freedom to design and freedom to play in virtual worlds, p. 2082.

[452] EPSTEIN, Richard A., Can technological innovation survive government regulation, **Harv. JL & Pub. Policy**, v. 36, p. 87, 2013.

vivenciadas nas vilas globais, deve ser o mecanismo de condução do funcionamento das plataformas digitais e alavancagem da *accountability*[453].

2. Arranjos contratuais como meios de governança da proteção de dados

Assim como as atividades desempenhadas pelas plataformas digitais normativas tem despertado significativa controvérsia em virtude de serem pouco permeadas pela transparência e *accountability* no tocante à privacidade e proteção de dados, o papel desempenhado pelos arranjos contratuais privados também tem sido severamente questionado. Embora alguns sustentem que o ciberespaço deveria ser uma jurisdição apartada, com suas próprias regras e direitos[454], o fato é que até então a "*significant amount of the regulation and the protection of virtual spaces will occur through real-world law, not outside of it: through contract, through property, and through the protection of values of freedom of speech and association*"[455].

2.1 Características dos arranjos contratuais

Dentre os instrumentos regulatórios tradicionais, os arranjos contratuais - em especial os *end-users license agreement* (EULA), *cloud computing*, os *service level agreements* (SLA), os *terms of service* (ToS) e as *privacy policies* (PPs) - tem se destacado pela capacidade de se adaptar aos subsistemas sociais parciais e promover a regulação da privacidade e proteção de dados com maior adaptabilidade e alguma atenção para a policontextualidade. Em boa medida, isso se deve ao fato de que contribuem para a regulação de transferências internacionais de dados e outras interações *cross-border* com relativa independência[456].

---

[453] Na avaliação de Ohm, "regulators must respond rapidly and forcefully to this disruptive technological shift, to restore balance to the law and protect all of us from imminent, significant harm". OHM, Paul, Broken promises of privacy: Responding to the surprising failure of anonymization, **Ucla Law Review**, v. 57, 2009.

[454] LASTOWKA, Gregory F.; HUNTER, Dan, The laws of the virtual worlds, **California Law Review**, v. 92, 2004.

[455] BALKIN, Virtual liberty: Freedom to design and freedom to play in virtual worlds, p. 20146.

[456] BYGRAVE, **Internet Governance by Contract**.

Consideram-se arranjos contratuais o conjunto de obrigações relacionadas a dados pessoais e privacidade – legais ou não - que resultam de um acordo entre partes para viabilizar operações de tratamento. As cadeias contratuais sobre proteção de dados podem ser centralizadas, como as da ICANN[457], mencionadas no capítulo 1, ou capilarizadas, como as que desencadeiam relações entre controladores e processadores de dados pessoais (*data processing agreements*)[458]. Embora os arranjos contratuais firmados no ciberespaço possam ser autônomos, ou seja, não fundados em um ordenamento jurídico específico – como no exemplo dos contratos da ICANN - , a grande maioria encontra amparo em um ordenamento jurídico, ainda que para disciplinar relações transnacionais.

Sob outro prisma, os arranjos contratuais sobre proteção de dados podem ser empregados de forma conjugada com tecnologias e serem ajustados à medida que novas estruturas são concebidas, com maior ou menor autonomia para as partes envolvidas. Em outros termos, infraestruturas tecnológicas tem sido agregadas a arranjos contratuais sobre proteção de dados como forma de melhor acomodar as relações policontextuais no ciberespaço.

---

[457] "ICANN is a private, non-profit corporation registered in California. To fulfil ICANN's mission, an expansive web of contracts and more informal agreements has been spun between the corporation and other bodies". Bygrave, Lee A.. Internet Governance by Contract . OUP Oxford. Edição do Kindle. BERNAL, **Internet Privacy Rights**; ZITTRAIN, Jonathan, Icann: between the public and the private comments before Congress, **Berkeley Tech. LJ**, v. 14, p. 1071, 1999; LADEUR, ICANN and the Illusion of a Community-Based Internet: Comments on Jochen von Bersstorff.

[458] EUROPEAN COURT OF JUSTICE, Decision on standard contractual clauses for the transfer of personal data to third countries; EUROPEAN COURT OF JUSTICE, Decision amending decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries; EUROPEAN COURT OF JUSTICE, Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

2.2 Funções dos arranjos contratuais

Os arranjos contratuais podem desempenhar quatro funções relevantes para a governança da privacidade e proteção de dados pessoais: coordenação, controle, senso de comunidade e constituição[459].

Inicialmente, vale ponderar que boa parte dos arranjos contratuais objetiva coordenar os interesses de *stakeholders*, a alocação de bens, serviços e oportunidades, por meio de uma infraestrutura digital que permita o compartilhamento de dados pessoais. Existem inúmeras interconexões policontextuais entre os elementos anteriormente mencionados que propiciam o monitoramento de dados pelos pontos de conexão, sistemas e camadas lógicas do ciberespaço, de modo que o primeiro papel dos arranjos contratuais é coordenar os símbolos de linguagem[460].

Ao mesmo tempo em que os arranjos contratuais podem ser considerados ferramentas onipresentes de coordenação para a governança da privacidade e proteção de dados pessoais, suas manifestações físicas e digitais estão longe de ser invasivas, tal como a lei, para a maior parte dos titulares dos dados pessoais. E isso não se deve ao fato de que estas

---

[459] BYGRAVE, Lee A.; BING, Jon, **Internet Governance : Infrastructure and Institutions**, Oxford: Oxford University Press, 2009.

[460] BERNAL, Paul A., Web 2.5: the symbiotic web, **Review of Law, Computers & Technology**, v. 24, n. 1, 2010; BALKIN, Virtual liberty: Freedom to design and freedom to play in virtual worlds.

manifestações não sejam cogentes e até abusivas, mas sim à circunstância de que em boa parte das ocasiões os titulares dão pouca relevância aos seus termos.

Desse modo, a preferência pelos arranjos contratuais sobre proteção de dados apresenta limites contrafactuais de coordenação que podem interferir na causa da sua celebração, como a insuficiência do consentimento e o desconhecimento das finalidades de tratamento. Quanto mais próximos do radar do regime de corregulação, maiores as chances de que os arranjos contratuais melhor promovam a coordenação de atores e infraestrutura, bem como sejam menos frágeis.

A segunda função dos arranjos contratuais sobre dados pessoais é a de controle, ou seja, esses mecanismos são geralmente utilizados para gerenciar os serviços e o uso de produtos de acordo com interesses econômicos e para marginalizar, se não bloquear, o comportamento ou as normas que os ameaçam[461], em clara desarmonia com a *accountability* e a policontextualidade. Os arranjos contratuais são componentes de um sistema complexo de gerenciamento de dados pessoais formado por uma infraestrutura organizacional tecnológica destinada a gerenciar o compartilhamento e o tratamento, geralmente com o objetivo de proteger os interesses econômicos sob diferentes patamares.

Não surpreende, portanto, que sob a roupagem da disrupção e das "novas garrafas", o ciberespaço tenha potencializado a proliferação de um considerável número de *stakeholders* que operam como feudos, por meio de um modelo oposto ao das vilas globais. Para redistribuir e equilibrar as situações de controle, também neste cenário a maior intervenção estatal mediante a aproximação de um modelo de corregulação se faz necessária.

A terceira função refere-se à criação e reforço do senso de comunidade. Os arranjos contratuais contribuem para a construção de verdadeiras arenas digitais – ou, segundo o modelo teórico adotado, vilas globais - , que representam o espaço de interação onde titulares dos dados investem tempo e compartilham interesses, como ocorre com as redes sociais. Dentro dessas vilas globais, os titulares celebram verdadeiros contratos comunitários por meio do qual compartilham seus dados pessoais de forma direta ou intermediados por uma plataforma, por exemplo.

---

[461] BYGRAVE, **Internet Governance by Contract**.

Essa relação entre titulares e os agentes de mercado revela a linha tênue entre as funções de controle e comunidade, que em situações específicas podem ser marcadas por um efeito *top down* em razão das diferentes manifestações de poder[462]. A *accountability* tende a funcionar como uma contramedida de equilíbrio entre o senso de comunicadade e a apontada capacidade de controle, na medida em que as situações de disfuncionalidade serão mensuradas com mais transparência e efetividade.

Por último, a quarta função refere-se à capacidade de constituição, também abordada no tópico sobre plataformas digitais normativas. Muitos dos arranjos contratuais são concebidos de modo a promover valores e direitos constitucionais como o devido processo legal, vedação ao anonimato e liberdade de expressão[463]. E em virtude da interconexão com a infraestrutura digital, muitos desses arranjos conjugam a prestação de serviços, bens e benefícios com a garantia de alguns desses direitos constitucionais. A despeito da constatação desse fenômeno em alguns arranjos contratuais, a ideia contempla uma falácia em si: só faria sentido falar em direitos constitucionais garantidos por arranjos contratuais quando estejam fundados em algum ordenamento jurídico específico. Os arranjos contratuais não possuem uma força normativa própria hierarquicamente prevalente que pudesse lhes atribuir a função de garantir direitos que não estivessem previstos numa Constituição ou que com ela fossem incompatíveis[464].

2.3 Internet das Coisas: a interação entre tecnologia e contratos

A Internet das Coisas (IoT) é um exemplo típico deste processo de intercambiariedade entre tecnologia e arranjos contratuais, cuja mescla de componentes tem sido um terreno fértil para a autorregulação[465] por meio do *código* e da tecnologia. A IoT é "uma infraestrutura global voltada para a era digital, permitindo serviços avançados por meio

---

[462] *Ibid*.

[463] BALKIN, Virtual liberty: Freedom to design and freedom to play in virtual worlds; SUNSTEIN, **Republic.com 2.0**.

[464] SUNSTEIN, Cass R., **A Constitution of Many Minds**, New Jersey: Princeton University Press, 2009.

[465] Para mais detalhes sobre IoT no Brasil, cf. o Roadmap Tecnológico do BNDES https://www.bndes.gov.br/wps/wcm/connect/site/1970e8af-33d4-48a5-9522-d6335c931e26/170614_Produto_Parcial_Frente+2_Sumario_Executivo_Roadmap_Final.pdf?MOD=AJPERES&CVID=lOOitOz

da interconexão de coisas (físicas e virtuais) com base nas tecnologias de informação e comunicação interoperáveis existentes e em constante evolução"[466].

A IoT é projetada para funcionar como uma rede de conexões dinâmicas e retroalimentáveis – à semelhança da matriz simbiótica dos network comunitaristas - , semelhantes de algum modo com as plataformas, mas com uma interface física relevante na captação de dados pessoais. Hildebrandt ilustra com bastante acuidade essa interação entre arranjos contratuais e tecnologia, além de deixar no ar os riscos existentes sob o prisma da privacidade e proteção de dados pessoais:

> "If we take the example of a smart device to save energy in the house, we can illustrate how technological normativity can be either regulative or constitutive of human interaction. Image we all have a 'smart meter' in the cupboard that measures the amount of energy we use and the amount of carbon this emits. This will allow more accurate billing, taking into account the costs to the environment of the type of energy used. One could imagine a smart home that automatically reduces the consumption of energy after a certain threshold has been reached, switching off lights in empty rooms and/or blocking the use of the washing machine for the rest of the day." [467]

No exemplo de Hildebrandt, arranjos contratuais entre o proprietário da casa, a concessionária de energia elétrica e o desenvolvedor da solução tecnológica de medição demandarão interações de variadas grandezas: eletrodomésticos utilizados, hábitos cotidianos, número de pessoas e preferências[468]. De posse de todas essas informações, o valor da oferta do serviço de medição será definido e cada usuário terá um perfil de contratação próprio. A concessionária e o desenvolvedor do equipamento terão em seu poder uma vasta gama de dados pessoais, legitimados por um arranjo contratual, que se não contiver disposições transparentes, com condições de igualdade e *accountability*, serão capazes de representar significativas ameaças à privacidade, conforme indicado em relatório da FTC:

> "IoT devices may present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks. Although each of these risks exists with traditional computers and computer networks, they are heightened in the IoT, as explained further below.

---

[466] MAGRANI, **A Internet das Coisas**, p. 45.

[467] HILDEBRANDT, Legal and technological normativity: more (and less) than twin sisters, p. 175.

[468] MAGRANI, Eduardo, Threats of the internet of things in a techno-regulated society: a new legal challenge of the information revolution, **International Journal of Private Law**, v. 9, n. 1–2, p. 4–18, 2018.

> Some of these risks involve the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information – risks already presented by traditional Internet and mobile commerce. Others arise from the collection of personal information, habits, locations, and physical conditions over time, which may allow an entity that has not directly collected sensitive information to infer it.
> Such a massive volume of granular data allows those with access to the data to perform analyses that would not be possible with less rich data sets. According to a participant, 'researchers are beginning to show that existing smartphone sensors can be used to infer a user's mood; stress levels; personality type; bipolar disorder; demographics (e.g., gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement." This participant noted that such inferences could be used to provide beneficial services to consumers, but also could be misused. Relatedly, another participant referred to the IoT as enabling the collection of "sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals." Some panelists cited to general privacy risks associated with these granular information-collection practices, including the concern that the trend towards abundant collection of data creates a "non-targeted dragnet collection from devices in the environment."[469]

A IoT é apenas uma das hipóteses em que os arranjos contratuais podem afetar consideravelmente a autodeterminação informativa, a capacidade de acesso, controle e a *accountability* sobre os dados pessoais processados, em especial porque o consentimento tem se mostrado uma contramedida inócua para preservar a tutela da privacidade[470]. A potencialidade de redes de conexão criadas pela IoT revela riscos para a proteção de dados que sequer podem ser antecipados e previamente regulados, dada a exponencialidade com que a junção de tecnologias e arranjos contratuais pode atingir, conforme esclarece o Working Party 29:

> "There is a risk that the IoT may turn an everyday object into a potential privacy and information security target while distributing those targets far more widely than the current version of the Internet. Less secure connected devices represent potentially efficient new ways of attack including the ease of surveillance practices, data breaches resulting in personal data being stolen or compromised that can have widespread effects on consumer rights and individual's perception of the security of the IoT. IoT devices and platforms are also expected to exchange data and store them on service providers' infrastructures. Therefore the security of the IoT should not be envisioned by considering only the security of the devices but also the communication links, storage infrastructure and other inputs of this ecosystem"[471].

---

[469] FEDERAL TRADE COMMISSION, **Internet of Things: Privacy & Security in a Connected World**, Washington: FTC, 2015.

[470] *Smart contracts* e *blockchain* poderiam ser outros exemplos, todavia aqui se optou por um recorte específico sobre Internet das Coisas (IoT).

[471] WORKING PARTY 29, **Opinion 8/2014 on the on Recent Developments on the Internet of Things**, Bruxelas: WP29, 2014.

Essas redes de conexão, que viabilizam o compartilhamento de dados pessoais entre empresas de distintos setores da economia – seguros, saúde, transporte, segurança, educação e instituições financeiras – tem representado um desafio considerável para os modelos de regulação setorial e estatal sobre proteção de dados[472]. Ainda assim, a autorregulação da IoT pode representar riscos ainda maiores do que as limitações experimentadas pelo modelo de regulação estatal e setorial, dada a baixa capacidade de *accountability*, insuficiência do consentimento e perda do controle e finalidade do tratamento dos dados pessoais.

Embora seja um dado empírico que a autorregulação esteja por trás de boa parte dos arranjos contratuais sobre proteção de dados[473], a conjugação de arranjos contratuais com disposições legais num modelo equilibrado de corregulação ainda aparenta ser a melhor forma de tutela da privacidade, em especial em situações de manifestação de poder.[474]

3. Privacy by Design e Privacy by Default: a accountability embutida na arquitetura da governança sobre proteção de dados

A análise das plataformas digitais e dos arranjos contratuais indicou um caminho de governança da proteção de dados pouco pautado pela policontextualudade e *accountability* - ainda que marcado pela normatividade - , o que representa um risco para a tutela da privacidade. Como forma de conciliar em um modelo de corregulação elementos que permitam ampliar a transparência, controle e responsividade sobre os dados pessoais, mediante uma maior interação entre os *stakeholders*, uma das possíveis variáveis envolve embutir a *accountability* na arquitetura da rede[475].

---

[472] "Nevertheless, the convenience of these devices comes at a cost, namely security. In fact, most IoT devices were built without security in mind. Indeed, many of these devices have backdoors placed on them by manufacturers and hardcoded manufacturer passwords. Furthermore, the security and privacy standards for these devices have not been adequately identified. Ultimately, the rush to deploy IoT technology has outpaced the creation and implementation of security and privacy protections and standards for these devices. Users may have difficulty controlling their information because communications and data exchange between IoT devices 'can be triggered automatically as well as by default, without the individual being aware of it'. What is more, 'modern techniques related to data analysis and crossmatching may lend this data to secondary uses, whether related or not to the purpose assigned to the original processing". MARAS, Marie-Helen, Internet of Things: security and privacy implications, **International Data Privacy Law**, v. 5, n. 2, 2015.

[473] BYGRAVE, **Internet Governance by Contract**.

[474] BALKIN, Virtual liberty: Freedom to design and freedom to play in virtual worlds.

[475] RUBINSTEIN, **Regulating Privacy by Design**; SCHAAR, Privacy by design.

Conforme analisado no primeiro capítulo a partir da teoria de Lessig e Reidenberg, "*os arquitetos da rede*" desenham ambientes capazes de influenciar o comportamento humano a todo momento para atingir objetivos regulatórios, sejam eles econômicos, sociais ou políticos. Em algumas circunstâncias o fazem de forma explícita e sob estruturas físicas, como analisado no tópico sobre *vigilância*, em outras optam pela concepção de incentivos (*nudges* ou *behavioral economics*) para direcionar escolhas e condutas[476], segundo a análise econômica da privacidade também examinada anteriormente.

Claramente, a arquitetura da rede ser tornou o foco de atuação dos modelos regulatórios, que outrora a ignoravam ou acreditam que podiam controlá-la de fora. No cenário atual, cada vez mais a arquitetura é considerada para a regulação do ciberespaço mesmo quando fruto da atuação eminentemente estatal. Para ilustrar essa intersecção entre estruturas físicas da arquitetura e a privacidade, Waldman recorre a uma analogia bastante pertinente e em consonância com os parâmetros aqui analisados:

> "A room is not just a space, just like a privacy policy is not just legalistic argle-bargle. Rooms are social spaces, and the placement of the fixtures and pieces of furniture within them influences the social inter-actions that take place inside. Designers create 'circulation plans' for spaces, showing how a space and its constituent elements will encourage movement or discourage other behavior. Interior design thus has a direct coercive effect on behavior: because spaces require that we walk through them, our movement is manipulated and constrained by a space's design. A predetermined plan can direct movement along a path, like in any Ikea store, for example. Given a massive open space, Ikea's store planners lay out walls that separate their products into different departments in such a way as to create a single path through the stores. Following this prescribed course, a customer has to make her way through 'bedrooms' before reaching 'bathrooms'. Privacy policies today may be designed like a McDonald's restaurant. Privacy policies may deploy placement strategies that make users uncomfortable and keep them uninformed. They are, then, paradigmatic examples of "unpleasant design. Therefore, privacy regulators who seek to protect consumers from unfair, coercive, and deceptive practices should not only consider how a company's disclosures conform to its actual data practices. They should also investigate how websites use design to transmit those disclosures."[477]

A relação simbiótica entre infraestrutura digital e o comportamento dos usuários do ciberespaço pode ser observada a todo momento[478], como no caso dos *Digital Rights Management* (DRM), tecnologia que restringe as chances de comportamentos de

---

[476] THALER; SUNSTEIN; BALZ, Choice architecture; THALER; SUNSTEIN, **Nudge**.

[477] WALDMAN, Ari Ezra, Privacy, notice, and design, **Stanford Technology Law Review**, v. 21, p. 74, 2018.

[478] BERNAL, Web 2.5: the symbiotic web.

violação a direitos autorais[479]. Ampliar as possibilidades de incorporação de tecnologias, arranjos contratuais e harmonizá-los com a regulação estatal parece ser o caminho factível para ampliar a *accountability* por meio do pluralismo jurídico[480].

Por meio do acoplamento da *accountability* à infraestrutura, num formato diferenciado de corregulação, alguns autores acreditam ser viável conferir respostas mais adequadas e contextuais às situações em que o consentimento não for possível ou quando for insuficiente para resguardar a esfera de proteção dos titulares dos dados[481]. Um dos caminhos para viabilizar a instrumentalização desse processo seria representado pela ideia de *Privacy by design* e *Privacy by Default*, conhecidos pela sigla PbD[482]. O PbD consiste em vários princípios que podem ser aplicados desde o desenvolvimento de sistemas e aplicações para mitigar preocupações com a privacidade, conforme elucida Ann Cavoukian, uma das precursoras na defesa da conjugação entre infraestutura e regulação:

> *Privacy by Design* refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and systems. This approach originally had information technology as its primary area of application, but I have since expanded its scope to two other areas. In total, the three areas of application are: (1) information technology; (2) business practices; and (3) physical design and infrastructures.
> As a broad overarching concept, *Privacy by Design* encompasses many elements in practice:
> 1. Recognition that privacy interests and concerns must be addressed proactively;
> 2. Application of core principles expressing universal spheres of privacy protection;
> 3. Early mitigation of privacy concerns when developing information technologies and systems, throughout the entire information life cycle —end to end;
> 4. Need for qualified privacy leadership and/or professional input;
> 5. Adoption and integration of privacy-enhancing *technologies* (PETs);
> 6. Embedding privacy in a positive-sum (not zero-sum) manner so as to enhance both privacy and system functionality; and
> 7. Respect for users' privacy."

---

[479] BELLIA; SCHIFF BERMAN; POST, **Cyberlaw**, p. 340–341.

[480] Um interessante exemplo mencionado por Waldman são as políticas de privacidade. Segundo ele, "creating and presenting privacy policies in a way users can under-stand is an important part of making privacy by design a reality. This sends two messages, both of which encourage users to ignore the policies. First, many websites make them difficult to find, so most users give up trying; this operationalizes resignation as a business tool. Second, by placing the privacy policy link at the bottom of a page in a small font, the website's design diminishes the policy's importance, suggesting to users that their privacy is an afterthought, and that the act of reading the privacy policy is not worth their time. WALDMAN, Privacy, notice, and design.

[481] SCHAAR, Privacy by design.

[482] Ambos serão tratados sob a sigla PbD.

Enquanto o *Privacy by Design* envolve a adoção da privacidade como diretriz do processamento de dados pessoais em todas as etapas, por outro lado o *Privacy by Default* diz respeito aos produtos ou serviços disponibilizados para o público, que devem contemplar desde a origem configurações de privacidade mais rígidas[483], que não demandariam a atuação humana para serem ativadas como é o caso da minimização de dados. Enquanto o *Privacy by design* atua como uma diretriz de todos os processos de tratamento de dados desde a concepção, o *Privacy by default* contempla uma perspectiva mais operacional, vinculada à definição de funcionalidades que por essência preconizam a proteção de dados pessoais, de que são exemplos a minimização, a exclusão, a anonimização e a pseudonimização de dados.

Ainda que sujeitos a um juízo de efetividade em concreto, o PbD é uma forma de regular a proteção de dados e privacidade por dentro, ou seja, por meio da disposição de camadas na arquitetura da rede que garantam o possível controle e autonomia do titular dos dados[484]. Além da integração de sistemas, o PbD exige a implementação de requisitos funcionais que garantam o controle e autodeterminação informativa aos titulares dos dados. Embora seja uma diretriz principiológica, muito se sustenta que o PbD seria uma forma de, por meio da autorregulação, amenizar as contramedidas da regulação estatal, visto que se o consentimento tem as suas limitações para atingir determinadas hipóteses de tratamento de dados pessoais[485], também o teria o PbD dada a pouca experiência e habilidade dos titulares dos dados com determinados dispositivos[486].

Um indicativo dessa crítica advém, por exemplo, da constatação de que políticas de privacidade, termos de uso e outros arranjos contratuais são concebidos de forma extensa, pouco prática e sob a perspectiva de que o destinatário é um usuário racionalmente orientado e familiarizado com o ambiente digital[487], o que o tornaria invariavelmente capaz de manipular os dispositivos de forma consciente para proteger a sua esfera de privacidade. Ao contrário disso, as experiências e as limitações do mundo físico não se desvencilham dos

---

[483] **What does data protection 'by design' and 'by default' mean?**, European Commission - European Commission, disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en>, acesso em: 17 fev. 2019.

[484] GÜRSES, Seda; TRONCOSO, Carmela; DIAZ, Claudia, Engineering privacy by design, **Computers, Privacy & Data Protection**, v. 14, n. 3, p. 25, 2011; BERNAL, **Internet Privacy Rights**.

[485] MAROTTA-WURGLER, Florencia, What's in a standard form contract? an empirical analysis of software license agreements, **Journal of Empirical Legal Studies**, v. 4, n. 4, p. 677–713, 2007.

[486] WILLIS, Lauren E., Why not privacy by default, **Berkeley Technology Law Journal**, v. 29, p. 61, 2014.

[487] WALDMAN, Privacy, notice, and design.

titulares dos dados - tal como o Barão de Munchausen[488] se puxa pelos cabelos para fora de uma dada realidade. A racionalidade empregada no mundo virtual não se difere sobremaneira do comportamento humano no mundo físico[489], afinal, como bem observa Julie Cohen, "*cyberspace is not, and never could be, the kingdom of the mind; minds are attached to bodies and bodies exist in the space of the world*"[490]. Em outros termos, a racionalidade do destinatário não deveria ser presumida e ignorar as diferentes experiências dos titulares dos dados sob a prisma da policontextualidade[491].

Por outro lado, o PbD é uma concepção muito além da mera ampliação dos requisitos de segurança dos dados do titular, visto que incorpora a premissa de que os sistemas devem ser projetados e construídos de maneira a evitar ou minimizar o tratamento de uma desnecessária quantidade de dados[492]. Em linha com algumas das ferramentas indicadas no capítulo anterior, como a pseudonimização, a criptografia e a anonimização, o PbD representa um mecanismo de controle democrático e plural da privacidade se associado com outras ferramentas regulatórias. Concebido de forma isolada e descontextualizada, o PbD contempla uma baixa carga de legitimidade e *accountability*, porquanto se trata de solução tecnológica concebida pelos agentes de mercados para os titulares dos dados, como se pudessem se colocar na posição de tutelados e antever sob todos os panoramas os riscos à privacidade. Dentre as premissas de desenvolvimento do PbD, algumas se destacam com maior primazia:

> (1) **Soberania sobre o controle dos dados**: O titular tem amplo controle sobre seus dados.
> (2) **Base voluntária**: Os dados devem ser armazenados apenas de forma voluntária, a critério do titular. Nenhum tratamento preferencial ou discriminatório é permitido com base no acesso concedido ou negado.
> (3) **Extensão dos dados**: O titular deve poder decidir quais dados serão passíveis de tratamento e quando devem ser apagados.
> (4) **Acesso a dados**: o titular deve poder decidir, caso a caso, quem pode ter acesso a quais dados.
> (5) **Direito à informação**: O titular tem o direito à informação sobre os seus dados e todos os processos que lhes digam respeito.
> (6) **Capacidade de verificação**: O titular deve poder usar os registros para verificar quem acessou quais dados e quando.

---

[488] LOWY, Michael, **As Aventuras de Marx contra o Barão de Munchhausen**, São Paulo: Busca Vida, 1987.

[489] TURKLE, Sherry, **Alone together: why we expect more from technology and less from each other**, First Trade Paper Edition edition. New York: Basic Books, 2012.

[490] COHEN, Cyberspace as/and Space.

[491] NISSENBAUM, **Privacy in context**.

[492] DENARDIS, Internet points of control as global governance.

A rigor, o PbB é parte da solução do problema tratado nesta tese - o outro será o reposicionamento do consentimento em face da *accountability*. Na medida em que o problema envolve o redimensionamento de instrumentos de *accountability* como fundamento de um modelo regulatório híbrido, contextual e plural, a que denominaremos de *Lex Privacy*, o PbB será o elemento da infraestrutura que conjugado com a regulação estatal, de forma policontextual, poderá ampliar as formas de controle da transparência e da responsividade no tratamento de dados pessoais. Em outras palavras, o PbD é o meio que viabilizará a intervenção da regulação estatal na arquitetura para assegurar a *accountability* e impor um regime de responsividade sob o enfoque da policontextualidade, com benefícios também para as empresas, como destaca Cavoukian:

> "The "payoff" to organizations would come in many ways, including: improved customer satisfaction and trust; enhanced reputations; reduced legal liabilities; more efficient operations; commercial gains and enhanced ROI; and, ultimately, enduring competitive advantage."[493]

Vale salientar, no entanto, que a idea em torno do PbD não deve representar simplesmente um rótulo atribuído a produtos e serviços para que as operações de tratamento de dados pessoais aconteçam no mesmo formato. Ela deve compreender procedimentos que efetivamente estimulem a minimização na coleta de dados pessoais e outras medidas técnicas e operacionais que ampliem sobremaneira as formas de tutela da privacidade[494].

Para que não seja apenas uma estratégia de marketing digital, o meio de assegurar *enforceability* para o PbD é a conciliação de parte dos seus preceitos com a regulação estatal, tal como fizeram PIPEDA, GDPR e LGPD. A despeito de conferir espaço para o desenvolvimento de soluções de PbD segundo a arquitetura da rede, a incorporação ao ordenamento estatal atribuiu-lhe capacidade coercitiva ao invés de se restingir ao campo principiológico. Mais do que os meios de controle do consentimento, a junção de PdB e regulação estatal permite atingir hipóteses em que a arquitetura da rede foi projetada para coletar dados pessoais de forma indevida, como ocorre nos casos de compartilhamento de

---

[493] CAVOUKIAN, Ann; HAMILTON, Tyler J., **The Privacy Payoff: How successful businesses build customer trust**, [s.l.]: McGraw-Hill Ryerson, 2002.

[494] USTARAN, Eduardo, **The Future of Privacy**, Londres: Data Guidance, 2013, p. 154.

dados para finalidades desconhecidas ou diversas das originárias[495]. Analisadas as formas de intervenção na arquitetura e ampliação da *accountability*, cumpre seja feito agora um reposicionamento teórico e axiológico do consentimento.

4. Accountability e consentimento: uma relação de complementariedade

Diante da pouca percepção sobre como enfrentar o avanço da tecnologia e os desafios do tratamento de dados pessoais, o consentimento foi concebido como uma contramedida de empoderamento do titular, que diante da ampla pressuposição da racionalidade humana seria capaz de se opor a esse processo[496]. Sob o esvaziado preceito da autodeterminação informativa, acreditava-se na capacidade dos titulares de zelar pela sua privacidade e pela finalidade do uso dos dados pessoais, o que se revelaria uma clara ironia diante do futuro próximo que indicaria o valor econômico das transações com esses dados (cf. cap 3, tópico 2).

Para dar-lhe normatividade e *enforceability*, ondas legislativas optaram por colocar o consentimento no centro gravitacional da regulação estatal sobre proteção de dados, ainda que sob a fragilidade das mesmas premissas voluntaristas de que as operações de tratamento ocorreriam em ambiente hermeticamente isolado, controlado e infenso aos *trade-offs*. A excessiva percepção dos dados pessoais enquanto propriedade do seu titular – e, por conseguinte, sujeito ao consentimento – contribuiu sobremaneira para o seu enfraquecimento normativo. Aos poucos, no entanto, a realidade pré-normativa do consentimento contaminou o processo regulatório, de modo que a insuficiência factual do poder de controle da vontade também se revelou nesse contexto. Se o consentimento não seria capaz de, por si só, obstar o poder de barganha em torno das trocas com dados pessoais, não seria a regulação estatal a responsável por modificar o substrato fático desse fenômeno[497]. Somente com a elevação da privacidade e proteção de dados à condição de direito fundamental foi possível desviar do excessivo apego ao consentimento em benefício de meios de controle como a *accountability.*

---

[495] SUPERIOR TRIBUNAL DE JUSTIÇA, Recurso Especial 1.348.532/SP.

[496] USTARAN, **The Future of Privacy**.

[497] DONEDA, **Da privacidade à proteção de dados pessoais**; BIONI, **Proteção de dados pessoais: a função e os limites do consentimento**.

A regulação estatal nem sempre considera a insuficiência normativa de um instituto enquanto consequência fática do contexto em que inserido, ou seja, às vezes opta por ignorar a policontextualidade subjacente. A despeito das consistentes evidências de que o consentimento não seria a ferramenta ideal para empoderar os titulares e assegurar-lhes controle sobre os seus dados, uma nova onda legislativa sobreveio e atribuiu-lhe qualificativos – livre, específico, expresso, informado e inequívoco - ao consentimento como forma de torná-lo "inalcançável". Assim aconteceu com o GDPR e a LGPD, por exemplo, embora APEC, Canadá e Austrália não tenham embarcado nessa tentação.

Ao invés de remediar situações limítrofes em que o consentimento poderia ser uma solução factível, as excessivas qualificações o tornaram não apenas inalcançável, como também inadequado. Por sinal, os exemplos do GDPR e da LGPD em contraste com o do bloco APEC, Austrália e Canadá evidenciam um outro fator relevante para o ciberespaço: as qualificações atribuídas ao consentimento pela regulação estatal contribuíram para uma maior fragmentação e concepção da propriedade privada dos dados pessoais. Ao invés de uma ferramenta universal de controle para o titular, o consentimento se tornou a chave de portas pré-selecionadas, com pouca capacidade de conformação com a realidade policontextual em que inserido, em um cenário marcado pelas trocas e negociações envolvendo a privacidade.

Isso não significa, de todo modo, que o consentimento deva ser abandonado enquanto base legal para o tratamento de dados pessoais. Ao contrário, o que se propõe nessa tese é a recontextualização do consentimento, de maneira a que seja empregado apenas em situações marcadas pela natureza simétrica de poder e em harmonia com a *accountability*. A multiplicidade de bases legais existentes no GDPR (seis) e na LGPD (dez) evidencia a necessidade de justificativas de tratamento de dados pessoais cada vez mais diversificadas e adaptáveis à policontextualidade das operações de tratamento no ciberespaço. A ampliação das bases legais de tratamento de dados pessoais é mais uma expressão do recurso à *accountability* como meio de controle dinâmico e empoderamento dos titulares[498].

4.1 Dimensão regulatória da Accountability

Para esclarecer a dimensão em que o termo é empregado nessa tese, vale recorrer ao domínio da Ciência Política, que foi quem melhor trabalhou com o tema nas

[498] NISSENBAUM, **Privacy in context**; PASQUALE, The Black Box Society, p. 88–89.

relações de poder e regulação. Nesse sentido, *accountability* deve ser compreendida como o pressuposto de que uma ordem político-democrática se consolida e legitima mediante a responsabilização de uns perante os outros, tendo em vista uma relação balizada pelo exercício de manifestações de poder. Trata-se, sobretudo, de um princípio de legitimação de decisões sobre regulação, leis e política em um Estado de Direito"[499]. Por outro lado, a responsividade associa-se à ideia de que o representante deve agir no interesse do representado, ou seja, não apenas prestar contas da sua atividade. A *accountability* contribui, portanto, para que o representante seja mais responsivo[500] em relação aos interesses do representado.

Sob a perspectiva do controle, a *accountability* diz respeito à capacidade que os cidadãos tem de impor e cobrar a imposição de sanções aos seus representantes, o que inclui a prestação de contas das suas atividades. É algo que depende de mecanismos institucionais e de governança, ou seja, a conjugação de instrumentos públicos e privados concebidos sob a ótica da corregulação para proporcionar maiores benefícios, oportunidades e preservação de direitos. Já a *responsividade* refere-se à sensibilidade dos representantes aos interesses dos representados, ou, dito de outra forma, à disposição de adotarem políticas que proporcionem maiores benefícios aos representados[501]. No contexto indicado, representados seriam os titulares dos dados e representantes os controladores e processadores, sejam eles entes públicos ou privados.

Em boa medida, o problema central da *accountability* envolve a delegação de autoridade a atores públicos e privados por meio da legislação, contratos ou outros instrumentos regulatórios, bem como a autonomia que a eles será concedida para que possam desempenhar suas tarefas e, ao mesmo tempo, garantir um grau adequado de controle. Confiar nos mecanismos de *accountability* é, portanto, uma pré-condição para a legitimação desse processo[502].

---

[499] FILGUEIRAS, Fernando, Além da Transparência: Accountability e Política da Publicidade, **Lua Nova**, v. 84, p. 65–94, 2011, p. 67.

[500] ALMEIDA, Débora Rezende, **Representação Além das Eleições: Repensando as Fronteiras entre Estado e Sociedade**, Jundiaí: Paco Editorial, 2015, p. 77.

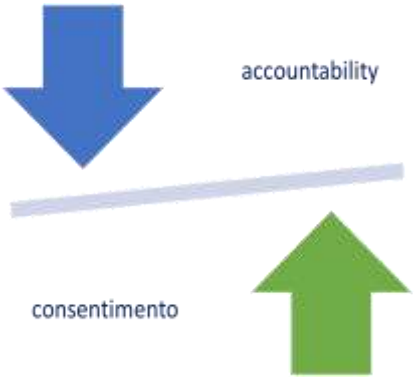
[501] PRZEWORSKI; STOKES; MANIN, **Democracy, Accountability, and Representation**; DOVI, Political Representation.

[502] SCOTT, Accountability in the Regulatory State; USTARAN, **The Future of Privacy**.

A *accountability* ou responsividade funciona como uma contramedida para as hipóteses de tratamento de dados em geral, mas em especial para aquelas em que o consentimento aparenta ser insuficiente ou pouco adequado. Trata-se, a rigor, de uma relação de inversa proporcionalidade entre consentimento e *accountabilit*y, que funciona como uma fórmula de complementariedade, a evidenciar que nas hipóteses de menor densidade axiológica do consentimento o peso da *accountability* deveria ser maior, com multas e hipóteses de responsabilidade civil mais severas. Onde houver menor participação do consentimento enquanto base legal para o tratamento de dados pessoais, maior deveria ser a *accountability* do responsável pela atividade.

Em algumas situações específicas a base dessa tese pode ser verificada em concreto: na minimização de dados, na nomeação de um encarregado de dados pessoais (*data protection officer*) e no relatório de impacto sobre proteção de dados (*Privacy Impact Assessment-PIA*). Conforme analisado no tópico anterior sobre *Privacy by Design* e *Privacy by Default*, quando a coleta e tratamento de dados não puder se fundar no consentimento ou outra base relevante, teoricamente a operação deveria se nortear pela perspectiva da minimização dos dados pessoais processados, sob pena de maior *accountability* por parte dos controladores e processadores. Em outros termos, a gradatividade das sanções será diretamente proporcional à capacidade dos controladores e processadores em tratar dados pessoais em descompasso com a *accountability*.

Sob a ótica do relatório de impacto sobre proteção de dados (*Privacy impact assessment*) também é possível identificar a pertinência da equação consentimento-*accountability*. Afinal, quanto maior for o risco de danos expressivos a direitos fundamentais dos titulares em virtude da operação de tratamento, mais indispensável se torna a realização de um PIA para documentar todas as atividades realizadas e as medidas mitigadoras para preservar a segurança. Os PIAs se tornaram meios relevantes de fiscalização e controle das atividades dos controladores e processadores, a partir da sua própria perspectiva, o que demonstra um olhar para as diversas variáveis envolvidas, em harmonia com a policontextualidade.



A sintonia e complementariedade entre *accountability* e consentimento não é um fenômeno decorrente puramente da regulação estatal. Ao contrário, a interação entre ambos precede à regulação e apenas ganha mais densidade com a normatização das suas consequências. Essa é a conclusão a que se chegou no capítulo 3 quando se promoveu uma análise do papel dos controladores, processadores, encarregados de proteção de dados, anonimização e interesse legítimo. O recorte material em torno dessas figuras foi capaz de evidenciar que o processo regulatório precede à atuação estatal e pode ser tão impactante quanto à normatização de um daqueles institutos. O traço marcante está na apreensão policontextual do processo, que tem início numa manifestação por meio da autorregulação, mas somente com a mescla via corregulação consegue atingir o colorido e a densidade normativa necessários à regulação nas vilas globais.

Certamente é possível que controladores e processadores queiram implementar políticas e medidas de proteção de dados e privacidade a partir de incentivos espontâneos e *accountability*. Nada obsta a que uma empresa opte por atender pedidos de acesso aos dados, portabilidade e exclusão em prazo menor do que estabelecido em lei ou decida nomear um encarregado de proteção de dados pessoais como medida de governança em circunstâncias nas quais não seja obrigatório[503]. Isso demonstra o oportuno papel da *accountability* mesmo em cenários pré-legislativos como fator impulsionador do pluralismo jurídico. Nesse sentido, o Working Party 29[504] destaca algumas das medidas que poderiam ser justificadas na *accountability*, mesmo sem previsão legal:

> • Establishment of internal procedures prior to the creation of new personal data processing operations (internal review, assessment, etc);

[503] WORKING PARTY 29, **Opinion 3/2010 on the principle of accountability**.

[504] *Ibid*.

> • Setting up written and binding data protection policies to be considered and applied to new data processing operations (e.g., compliance with data quality, notice, security principles, access, etc), which should be available to data subjects;
> • Mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations;
> • Appointment of a data protection officer and other individuals with responsibility for data protection;
> • Offering adequate data protection, training and education to staff members. This should include those processing (or responsible for) the personal data (such as human resources directors) but also IT managers, developers and directors of business units. Sufficient resources should be allocated for privacy management, etc;
> • Setting up of procedures to manage access, correction and deletion requests which should be transparent to data subjects;
> • Establishment of an internal complaints handling mechanism;
> • Setting up internal procedures for the effective management and reporting of security breaches;
> • Performance of privacy impact assessments in specific circumstances;
> • Implementation and supervision of verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc).

Sem qualquer pretensão de passagem do status canônico outrora conferido ao consentimento[505], a *accountability* reúne melhores condições para proporcionar o acomplamento estrutural entre Política e Direito, ou seja, detém pressupostos materiais mais sujeitos à policontextualidade do que o consentimento isoladamente considerado ou outra base legal. A *accountability* é dotada de substancial densidade axiológica que pode proporcionar a mitigação de cenários fragmentados e centrados na propriedade privada dos dados pessoais, como os relacionados ao consentimento qualificado, graças à sua complementariedade em relação aos parâmetros de voluntariedade do controle e autonomia almejados pelos ordenamentos jurídicos para o titular dos dados pessoais.

A questão que ainda remanesce é se para atingir todos esses objetivos a *accountability* deveria ser inserida nos marcos regulatórios estatais ou isso representaria uma contradição tão relevante quanto a fragmentação proporcionada pelo consentimento qualificado. A rigor, a *accountability* é marcada por uma razoável normatividade capaz de influenciar comportamentos de controladores, processadores e titulares dos dados mesmo fora da regulação estatal, como se observa na adoção de políticas de privacidade e regimes de governança. No entanto, é expressivo o aumento da carga de normatividade e *enforceability*

---

[505] BIONI, **Proteção de dados pessoais: a função e os limites do consentimento**, p. 134.

da *accountability* nas hipóteses de incorporação ao ordenamento jurídico estatal, sob a égide de um modelo de corregulação.

Em resumo, a definição de uma rede de comunicação em torno da *accountability* representa mais uma maneira de fomentar o modelo da corregulação, cuja expressão do pluralismo jurídico melhor se adaptará ao fenômeno da policontextualidade no ciberespaço[506].

4.2 Quem controla e fiscaliza a accountability?

Conforme indicado no tópico anterior, se bem adaptada a um modelo de corregulação, a *accountability* tem todas as condições para proporcionar um efetivo empoderamento do titular e controle sobre seus dados pessoais. A natureza híbrida de que pode se revestir a *accountability* é um dos principais fatores que lhe confere ampla capilaridade de controle e fiscalização[507], uma vez que tanto atores privados quanto públicos – os representados – estarão investidos nessa função. A marca da policontextualidade da *accountability* também se expressa nesse quesito, uma vez que confere legitimidade de controle a variados *stakeholders*[508]. Em virtude de não ser um preceito de ordem eminentemente estatal ou privada, mas comportar a delegação de autoridade por meio da legislação e arranjos contratuais, a *accountability* representa um meio policontextual mais propício à tutela da privacidade e proteção de dados pessoais, na medida em que atua acolmatando espaços de pouca densidade normativa e axiológica. Nesse contexto, uma das questões sempre presentes é o papel das autoridades estatais de proteção de dados (*Data Protection Authorities*-DPA) na fiscalização e implementação de mecanismos baseados na *accountability*.

Em primeiro lugar, a *accountability* não representa uma ameaça ao papel desempenhado pelas autoridades de proteção de dados, na medida em que ela atua para ampliar os meios de fiscalização e controle à disposição das DPAs tanto quanto dos titualres dos dados pessoais. Assim, com base na *accountability* as autoridades podem solicitar provas

---

[506] TAMANAHA, Brian Z.; SAGE, Caroline; WOOLCOCK, Michael, **Legal Pluralism and Development: Scholars and Practitioners in Dialogue**, New Haven: Cambridge University Press, 2012.

[507] OHM, Paul, Branding Privacy, **Minnesota Law Review**, v. 97, p. 907, 2012.

[508] ACQUISTI, Alessandro; GROSSKLAGS, Jens, Privacy attitudes and privacy behavior, *in*: **Economics of information security**, [s.l.]: Springer, 2004, p. 165–178.

e evidências da conformidade das operações de tratamento, o que lhes permitirá adotar medidas de execução muito mais efetivas do que apenas aquelas decorrentes de lei[509].

Além da ampliação dos meios de *enforcement*, a *accountability* permitirá que as autoridades de proteção de dados tenham parâmetros mais claros para monitorar os níveis de conformidade da governança dos controladores e processadores de dados pessoais. Se as informações de monitoramento não forem fornecidas após solicitação das DPAs, com base na inobservância da *accountability* será possível a imposição de sanções, sem que para tanto seja necessário recorrer a outras regras e princípios[510].

Ademais, enquanto meio de incremento de suas atividades, a *accountability* funcionaria como um instrumento em favor das DPAs para que pudessem realizar atividades mais seletivas e estratégicas, como a propagação exponencial da cultura de proteção de dados e tutela da privacidade. Como em geral a atuação das autoridades de proteção de dados é mais focada num papel "*ex post*" em vez de "*ex ante*", a *accountability* pode ser um meio de também propiciar uma atuação prévia e educativa voltada à preservação da privacidade. Por fim, no tocante ao poder sancionador, o emprego da *accountability* não afeta negativamente a capacidade e natureza das sanções impostas pelas DPAs; ao contrário, amplia as possibilidades de que penas mais expressivas sejam impostas como consequência também da sua inobservância.

5. O valor pluralístico e policontextual da privacidade a serviço da Lex Privacy

Ao longo dessa tese, a conjugação de elementos do pluralismo do jurídico e do marco teórico de Teubner foram apresentados em perspectiva para indicar um caminho dinâmico de compreensão da privacidade e proteção de dados pessoais. Mais do que definir um conceito de privacidade, buscou-se a ressignificação contextual como forma de desenhar soluções para casos concretos[511]. Por esta razão, a concepção de *Lex Privacy* parte exatamente de um conjunto de medidas protetivas contra a variedade de problemas inter-relacionados nas

---

[509] WORKING PARTY 29, **Opinion 3/2010 on the principle of accountability**; WOOLGAR; NEYLAND, **Mundane governance: Ontology and accountability**.

[510] BENNETT, Colin J., **Regulating privacy: Data protection and public policy in Europe and the United States**, [s.l.]: Cornell University Press, 1992.

[511] VIEHWEG, Theodor, **Tópica e jurisprudência**, Brasília: UnB, 1979.

vilas globais[512]. Em outras palavras, como a privacidade consiste em uma pluralidade de mecanismos de proteção contra diferentes tipos de ofensas, os seus contornos dogmáticos assim também deveriam ser entendidos, motivo pelo qual se percorreu um caminho de análises de modelos regulatórios (regulação estatal, corregulação e autorregulação) e dos produtos de sua atividade (anonimização, pseudonimização, *data protection officer* etc.).

Se por um lado atuar no campo sócio-normativo para otimizar resultados contribui para aumentar os parâmetros da *accountability* e evita tensões e desgastes epistemológicos em torno do direito à privacidade, por outro subsiste a ausência de parâmetros para a consolidação de um modelo contextual de tutela que não seja aquele consagrado só pelo ordenamento jurídico ou exclusivamente por expressão do pluralismo jurídico[513].

É neste contexto que a proposta apresentada por Lee Bygrave[514] tem a virtude de constituir um caminho alternativo e mais focado na policontextualidade. Sem se comprometer com uma apreensão dogmática, Bygrave defende que a busca deve ser feita em parte nos princípios presentes nas leis de proteção de dados, em parte na forma como eles são aplicados e em parte segundo a percepção social do que seja privacidade, segundo um recorte temporal[515]. O grande trunfo desta abordagem consiste na sua abrangência e atemporalidade, além da capacidade das redes de comunicação nas vilas globais[516].

A falha em se atribuir à privacidade uma definição precisa, analiticamente útil e genericamente aceitável não deve ser encarada, portanto, como uma inconsistência, como aponta Colin Bennett[517], afinal a privacidade representa um significado em latência e desordem. Elementos axiológicos frequentemente precisam ser agregados à ideia de privacidade para torná-la atual, multidimensional e tutelável. E é exatamente este aspecto que

---

[512] SOLOVE, **Understanding privacy**, p. 171–172. Solove indica que a referência ao direito à privacidade em abstrato nem sempre apresenta uma visão útil para a solução dos problemas.

[513] NISSENBAUM, **Privacy in context**; TEUBNER, **Direito, sistema e policontexturalidade**.

[514] BYGRAVE; BING, **Internet Governance**.

[515] BYGRAVE, Lee A., The place of privacy in data protection law, **UNSWLJ**, v. 24, p. 277, 2001, p. 278.

[516] FRYDMAN; DE SCHUTTER; PAS, Coregulation.

[517] BENNETT, **Regulating privacy**, p. 25. No mesmo sentido, destacando que o conceito de privacidade foi infectado por imprecisões e ambiguidades como as observadas em Griswold v. Connecticut, cf. GROSS, Hyman, The Concept of Privacy, **New York University Law Review**, v. 42, 1967, p. 35. Post considera que a privacidade "is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all" POST, What Larry Doesn't Get, p. 2087.

permite seja a privacidade compreendida como uma categoria contextual em evolução e um direito fundamental passível de permanente atribuição de densidade normativa[518].

Quando se analisam as repercussões do direito à privacidade no ciberespaço, invariavelmente o controle da informação, a não interferência e a acessibilidade limitada representam os principais focos de atuação das leis de proteção de dados, ainda que sem a preocupação com definições e delimitações teóricas. Aqui reside a principal justificativa para que a construção de conceitos não seja essencial para a solução do problema de pesquisa dessa tese: leis de proteção de dados, embora umbilicalmente vinculadas à privacidade, a ela não se restringem e demandam uma compreensão policontextual para assegurar a perene observância de valores democráticos[519].

A rigor, o direito à privacidade serve de base para outros tantos valores que são delineados por leis de proteção de dados - neutralidade de rede, autonomia, anonimato, liberdade de expressão, liberdade de associação, livre iniciativa - que a demasiada preocupação com a sua definição cria um desvio de foco dos desdobramentos dele decorrentes e empobrece todo o arcabouço normativo do qual faz parte.

Sob outra perspectiva, a arraigada pretensão de construir um delineamento teórico do direito à privacidade culmina por se restringir à sua perspectiva individual, em clara demonstração de menosprezo à dimensão dos valores sociais e dos significados culturais como o pluralismo, a democracia e a cidadania[520]. Ignora, ainda, o papel dos mecanismos de proteção de dados na formulação de padrões de qualidade das informações pessoais e no processamento de dados de terceiros por motivos legítimos[521]. Em resumo, esta vertente subdimensiona o papel da privacidade como um elemento base para a concepção de sociedade plural, democrática e dotada de poderes normativos de controle e aferição de *accountability*[522], conforme analisado ao longo da tese.

A fuga da desmesurada tentação de conduzir o debate rumo tão somente à conceituação do direito à privacidade, como se os problemas a ele relacionados não pudessem

---

[518] FREUND, Paul Abraham, **Privacy: one concept or many**, [s.l.]: Atherton Press, 1971, p. 187.

[519] SCHWARTZ, Privacy and Democracy in Cyberspace.

[520] BYGRAVE, The place of privacy in data protection law, p. 281.

[521] USTARAN, **The Future of Privacy**.

[522] PRZEWORSKI; STOKES; MANIN, **Democracy, Accountability, and Representation**.

ser solucionados sem o prévio cumprimento deste rito, nos remete a um dos mais interessantes trabalhos de Rudholf Von Jhering. Em *In the heaven for legal concepts: a fantasy*, Jhering constrói um diálogo fictício em torno do que deveria ser a preocupação de um jurista depois da sua morte. A crítica velada de Jhering parte de um rompimento temporal em que o teórico retorna ao passado, porém sem as preocupações de outrora em torno das construções dogmáticas:

> "Since you are a Roman scholar you will go to the heaven for jurisprudential concepts. There you will rediscover all the legal concepts with which you occupied yourself on earth. But these concepts will not be found in their imperfect and deformed state as the legislators and practitioners know them on earth. They will be perfect, unblemished, pure and ideal. Here legal theorists are rewarded for their services on earth. The concepts that appeared in veiled form on earth will be perfectly clear here. The theorists will behold the concepts face to face and associate with them as they associate among themselves. On earth, they looked in vain for solutions to questions. Here the questions will be answered by the concepts themselves. There are no more civil puzzles here. [...] The unshakable belief in the supremacy of concepts and abstract principles is what you'll find in common here[523]."

Com o direito à privacidade não é diferente. Os enfoques anteriormente expostos impedem que se compreenda a privacidade a partir de sua função prospectiva e da sua conotação defensiva. Por essa razão, Lee Bygrave apresenta uma oportuna analogia deste fenômeno mediante a comparação com as políticas de desenvolvimento sustentável. Tanto quanto uma política pública que objetiva uma maior interação social quanto a promoção da democracia[524], as leis de proteção de dados visam resguardar muito mais do que a privacidade, motivo pelo qual a busca dogmática apenas contribuirá para distanciamento temporal e a perda de efetividade.

A rigor, os modelos regulatórios analisados promovem tanto os legítimos interesses dos controladores e processadores de dados pessoais quanto asseguram patamares de adequada proteção à privacidade dos titulares[525]. Nesse contexto, é essencial observar que os modelos regulatórios de proteção de dados atendem a múltiplos objetivos, de modo que qualquer tentativa de restringir seu espectro de atuação à conceituação da privacidade

---

[523] VON JHERING, Rudolf, In the heaven for legal concepts: a fantasy, **Temp. LQ**, v. 58, p. 799, 1985, p. 802–804.

[524] FARRANHA, Ana Claudia, Estado, sociedade e interações digitais: expectativas democráticas, **RP3-Revista de Pesquisa em Políticas Públicas**, n. 2, 2014.

[525] BYGRAVE, The place of privacy in data protection law, p. 282.

obscurecerá os benefícios dela advindos e comprovará a atuação abaixo do impacto esperado[526].

O valor pluralístico da privacidade é o elemento chave da identificação de um modelo regulatório a que denominamos *Lex Privacy.* Se por um lado, esse modelo é produto do pluralismo jurídico e fruto da manifestação da corregulação, por outro ele se vale da *accountability* como meio de promover a complementação normativa e axiológica das hipóteses de tratamento de dados pessoais, em especial o consentimento. A policontextualidade é então representada como fator responsável pelo acoplamento estrutural do ciberespaço e redimensionamento da fragmentação regulatória até então experimentada nas vilas globais.

[526] A promoção de políticas públicas digitais tem o poder proporcionar mais interação com valores democráticos. Segundo Farranha, "a ideia de publicizar os negócios estatais vem ganhando força nas democracias modernas. Fruto desta perspectiva é a instituição do direito à informação. Nesse sentido, o direito à informação está relacionado maior visibilidade e compreensão da ação pública, consistindo em instrumentos, os quais apontam uma preocupação com a transparência e com a divulgação da atuação do Estado, ligando-se a cultura da informação na medida em que favorecem a ampliação do controle social" (FARRANHA, Ana Cláudia; DOS SANTOS, Leonardo Tadeu, Administração pública, direito e redes sociais: o caso da CGU no Facebook, **Revista Eletrônica do Curso de Direito da UFSM**, v. 10, n. 2, p. 742–767, 2015.)

CONCLUSÃO

A difusão dos meios de interação no ciberespaço enquanto locus de participação de atores públicos e privados tem provocado um desafio regulatório relevante. Por essa razão, o objetivo da tese foi demonstrar que a regulação da privacidade e proteção de dados no ciberespaço contém elementos particulares que demandam a revisão do marco de atuação dos atores públicos e privados, em especial porque os paradigmas não guardam profunda identidade entre a privacidade vivenciada no mundo real e no virtual.

Como forma de endereçar a análise, o problema de pesquisa envolveu o redimensionamento de instrumentos de *accountability*, em complemento ao consentimento do titular dos dados, como fundamento de um modelo regulatório híbrido, contextual e plural, denominado de *Lex Privacy*. Esse problema foi delineado segundo duas específicas hipóteses de investigação, a saber, o pluralismo jurídico e a necessidade de se conceber a regulação estatal da proteção de dados pessoais em harmonia com outros modelos, bem como a concepção da *accountability* como elemento base de fundamentação da *Lex Privacy.*

Dentre as variáveis consideradas e capazes de influenciar o modelo de regulação em torno da *Lex Privacy*, foram especialmente consideradas a regulação do ciberespaço e seu impacto nos modelos regulatórios sobre proteção de dados e a insuficiência do consentimento

O principal desafio dessa tese envolveu a definição de parâmetros em razão dos quais a regulação da privacidade e proteção de dados no ciberespaço era necessária, a forma como ela deveria ser implementada e os atores envolvidos nesse processo. Para chegar aos resultados de análise esperados, o ponto de partida envolveu o estudo das teorias de regulação do ciberespaço e a definição do marco de análise do problema de pesquisa.

Teubner e seu modelo de pluralismo jurídico, marcado pela policontextualidade e dispersão em vilas globais – a *Bukowina* - foi eleito o referencial teórico em torno do qual se indicaria a insuficiência da regulação exclusivamente estatal para fazer frente à gama de ameaças disruptivas à tutela da privacidade e proteção dos dados pessoais.

A escolha da policontextualidade de Teubner se justificou pela necessidade de se promover o acoplamento estrutural entre Direito e Política, atores públicos e privados,

assim como variáveis de desenvolvimento tecnológico como as plataformas digitais. A policontextualidade e o pluralismo de Teubner representaram o substrato de desenvolvimento da principal ferramenta de adensamento axiológico da *Lex Privacy*, isto é, a *accountability*.

O dilema dos ciberlibertários, ciberpaternalistas e network comunitaristas foi objeto de específica contextualização com os modelos regulatórios sobre proteção de dados e privacidade. De um lado, constatou-se a perspectiva dos ciberlibertários como um fenômeno mais próximo do modelo de autorregulação ou até ausência de regulação; de outro, notou-se que os ciberlibertários e network comunitaristas estariam mais próximos de um modelo de corregulação.

Como não há uma linha estática e uma separação hermética entre as correntes teóricas e os modelos analisados, a harmonização dessas vertentes somente foi possível em razão da perspectiva de pluralismo jurídico adotada. Em outras palavras, os modelos analisados isoladamente foram incapazes de apresentar respostas efetivas e dinâmicas às interações verificadas no ciberespaço.

Para mensurar de forma mais concreta o impacto de cada modelo sobre elementos pré-definidos, foram selecionados o consentimento e as transferências internacionais de dados como ponto de comparação da influência de regimes como os da *Federal Trade Commission*, do Canadá, do bloco APEC, da União Europeia, da Austrália e do Brasil.

A escolha do consentimento e das transferências internacionais teve como justificativa o fato de reunirem pontos de interação regulatória entre atores públicos e privados, o que permitiria compreender o maior ou menor espaço de conformação atribuído aos atores públicos e privados. A análise comparativa demonstrou que o modelo de corregulação tem sido mais adequado frente aos desafios inerentes à tutela da privacidade e proteção dos dados pessoais, sobretudo porque permite a conciliação entre atuação estatal e fomento à inovação tecnológica.

Conquanto o modelo da GDPR tenha se mostrado menos propenso à influência de outros atores reguladores, foi possível identificar a sua influência econômica em novos modelos regulatórios, como o da recém aprovada Lei Geral de Proteção de Dados no Brasil, cuja capacidade de admitir a interação com variados atores no processo de regulação ainda é uma incógnita. O impacto causado pelo efeito da extraterritorialidade das regulações estatais

tem apontado para um fenômeno muito próximo das vilas globais de Teubner, ainda que capaz de inibir a influência recíproca de outros modelos.

Com a contextualização dos modelos regulatórios específicos, o passo seguinte foi a definição do conteúdo regulado, ou seja, a relevância de se atribuir uma delimitação conceitual para a privacidade. Na medida em que o marco teórico utilizado nessa tese envolveu mais do que a definição isolada de conceitos, mas a própria ressignificação da privacidade, concluiu-se que a abordagem mais adequada deveria ser aquela que considerasse o papel dos diversos atores e o emprego da *accountability* como meio de fiscalização e controle da tutela da privacidade e proteção de dados.

Dentro desse contexto, dois fenômenos mereceram uma particular reflexão: a vigilância em massa e a análise econômica da privacidade. Como forma de apontar a conexão entre ambos, a vigilância foi revista tanto sob o prisma da atuação estatal na coleta e tratamento de dados pessoais como forma de desempenhar atividades de *law enforcement*, quanto em razão da exploração privada do *profiling*, *tracking* e *targeting* para a definição de perfis comportamentais conforme a experiência dos titulares dos dados.

A compreensão do processo de autorregulação induzido pela inteligência artificial deixou ainda mais evidentes os contrastes com os modelos anteriormente examinados, na medida em que o *reinforcement learning* tem sido capaz de gerar impactos imprevisíveis sobre o tratamento de dados pessoais.

Além do papel desempenhado pela inteligência artificial no impulsionamento de novas formas de regulação, a anonimização, a pseudonimização e a criptografia possibilitaram a compreensão do reenquadramento regulatório da tutela da privacidade, em especial quando fruto de uma tentativa de se afastar da atuação do regulador estatal para melhor realizar as operações de tratamento de dados pessoais. Essas três modalidades evidenciaram como a policontextualidade pode contribuir para uma regulação mais efetiva e condizente com as realidades do ciberespaço, notadamente porque envolvidos os mais diversos atores no processo como um todo.

Não só a influência dos diversos atores e contextos foram considerados como ponto focal do pluralismo jurídico, a transparência da atividade de tratamento também exigiu que se delimitassem os papéis dos controladores, processadores e do *data protection officer*. Afinal, a defesa de um modelo de corregulação policontextual perpassa pela internalização da

cultura de proteção de dados e tutela da privacidade em todas as camadas de uma organização.

As funções desempenhadas por controladores e processadores, fundadas em arranjos contratuais com previsão de responsabilidade civil, foram capazes de demonstrar a natureza complexa existente entre os mais diversos atores, em especial porque em algumas situações se trata de contratos sujeitos à ratificação por parte de autoridade estatal, como no caso da União Europeia.

Com a definição dos elementos que comporiam a base da *Lex Privacy*, o último capítulo da tese contemplou a conjugação das estruturas normativas institucionais e contratuais, que, sob a perspectiva do pluralismo e policontextualidade, indicariam a necessidade de aperfeiçoamentos do regime de proteção de dados pessoais por meio da *accountability*.

Por meio da contraposição das posições de poder ocupadas por plataformas digitais normativas, mediante o empreendedorismo evasivo, a conversão de dados em experiências e a criação de procedimentos e regras próprios, desenvolveu-se a tese de que a autorregulação precisa ser melhor direcionada e a *accountability* tem uma função importante a desempenhar para desvendar práticas obscuras no tratamento de dados pessoais.

Se por um lado as plataformas digitais normativas são uma realidade na economia digital – nem sempre tão compartilhada - , de outro os arranjos contratuais tem representado um dos caminhos mais utilizados para viabilizar a dinâmica regulação de condutas no ciberespaço dada a sua flexibilidade e capacidade de interação com os diversos atores. A relação entre arranjos contratuais e tecnologia, no entanto, pode gerar um cenário de pouca transparência, dada a capacidade exponencial de compartilhamento para finalidades distintas que podem tomar as atividades de tratamento, como se observa no caso da Internet das Coisas.

A resposta a esses cenários de maior intensidade da autorregulação e regulação estatal demandam um equilíbrio e a chave para viabilizar esse objetivo foi o desenvolvimento de um regime de governança da privacidade fundado na *accountability*. Com a estruturação de modelos regulatórios nos quais a proteção de dados seja incutida desde a concepção (*Privacy by Design*) e com funcionalidades operacionais capazes de proporcionar o empoderamento dos usuários (*Privacy by Default*), a *accountability* foi apontada como o

elemento de complementação e adensamento axiológico para os casos de insuficiência do consentimento.

A relação de inversa proporcionalidade entre *accountability* e consentimento – quanto maior um, menor o outro – foi apresentada como a principal contribuição dessa tese para a definição do marco regulatório da *Lex Privacy*, que ao final se desnudou como um modelo regulatório pautado pelo valor pluralístico e contextual da privacidade, a exigir uma perene confluência de esforços dos os atores públicos e privados.

BIBLIOGRAFIA

ABELSON, Harold; ANDERSON, Ross; BELLOVIN, Steven M.; *et al*. Keys under doormats: mandating insecurity by requiring government access to all data and communications. **Journal of Cybersecurity**, v. 1, n. 1, p. 69–79, 2015.

ACQUISTI, Alessandro. Nudging privacy: The behavioral economics of personal information. **IEEE security & privacy**, v. 7, n. 6, 2009. Disponível em: <http://ieeexplore.ieee.org/abstract/document/5370707/>.

ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Privacy and human behavior in the age of information. **Science**, v. 347, n. 6221, p. 509–514, 2015.

ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy attitudes and privacy behavior. *In*: **Economics of information security**. [s.l.]: Springer, 2004, p. 165–178. Disponível em: <http://link.springer.com/content/pdf/10.1007/1-4020-8090-5_13.pdf>.

ACQUISTI, Alessandro; GROSSKLAGS, Jens. What can behavioral economics teach us about privacy. **Digital Privacy: Theory, Technologies and Practices**, v. 18, p. 363–377, 2007.

ACQUISTI, Alessandro; JOHN, Leslie K.; LOEWENSTEIN, George. What Is Privacy Worth? **The Journal of Legal Studies**, v. 42, n. 2, p. 249–274, 2013.

ACQUISTI, Alessandro; TAYLOR, Curtis R.; WAGMAN, Liad. The economics of privacy. 2016. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580411>.

ALLEN, Anita L. **Privacy law and society**. [s.l.]: West Group, 2007.

ALMEIDA, Débora Rezende. **Representação Além das Eleições: Repensando as Fronteiras entre Estado e Sociedade**. Jundiaí: Paco Editorial, 2015.

ARBIX, Daniel do Amaral. **Resolução Online de Controvérsias**. São Paulo: Intelecto, 2017.

ASSANGE, Julian. **Cypherpunks: liberdade e o futuro da internet**. São Paulo: Boitempo Editorial, 2015.

AXELROD, Robert. **The Evolution of Cooperation**. New York: Basic Books, 1984.

AYENSON, M.; WAMBACH, D. J.; SOLTANI, A.; *et al*. Behavioral Advertising: The Offer You Cannot Refuse. **Harvard Law and Policy Review**, v. 273, 2012.

BALDWIN, Robert; CAVE, Martin; LODGE, Martin. **The Oxford handbook of regulation**. [s.l.]: Oxford University Press, 2010.

BALKIN, Jack M. Virtual liberty: Freedom to design and freedom to play in virtual worlds. **Virginia Law Review**, 2004. Disponível em: <https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com.br/&httpsredir=1&article=1238&context=fss_papers>.

BAMBERGER, Kenneth A.; MULLIGAN, Deirdre K. Privacy on the Books and on the Ground. **Stan. L. Rev.**, v. 63, p. 247, 2010.

BARLOW, John Perry. The next economy of ideas: selling wine without bottles on the global net. **Wired**, v. 8, 2000.

BAROCAS, Solon; HOOD, Sophie; ZIEWITZ, Malte. Governing algorithms: A provocation piece. 2013. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2245322>.

BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro: Zahar, 2001.

BAUMAN, Zygmunt. **Vigilância líquida: diálogos com David Lyon**. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BBC NEWS. **North Korea: On the net in world's most secretive nation**. BBC. Disponível em: <https://www.bbc.com/news/technology-20445632>. Acesso em: 7 fev. 2019.

BEÇAK, Rubens; LONGHI, João Victor Rozatti. O papel das tecnologias de comunicação em manifestações populares: a "Primavera Árabe" e as "Jornadas de Junho" no Brasil. **Revista Eletrônica do Curso de Direito da UFSM**, v. 10, n. 1, p. 388–405, 2015.

BELLIA, Patricia L. Chasing bits across borders. **U. Chi. Legal F.**, p. 35, 2001.

BELLIA, Patricia L.; SCHIFF BERMAN, Paul; POST, David G. **Cyberlaw: Problems of Policy and Jurisprudence in the Information Age**. [s.l.]: West Group, 2003.

BENKLER, Yochai. Constitutional bounds of database protection: the role of judicial review in the creation and definition of private rights in information. **Berkeley Technology Law Journal**, v. 15, p. 535–603, 2000. (2).

BENKLER, Yochai. Freedom in the commons: Towards a political economy of information. **Duke LJ**, v. 52, p. 1245, 2002.

BENKLER, Yochai. Net Regulation: Taking Stock and Looking Backward. **U. Colo. L. Rev.**, v. 71, p. 1203, 2000.

BENKLER, Yochai. Sharing nicely: On shareable goods and the emergence of sharing as a modality of economic production. **Yale Law Journal**, p. 273–358, 2004.

BENKLER, Yochai. **The penguin and the leviathan: How cooperation triumphs over self-interest**. [s.l.]: Crown Business, 2011.

BENKLER, Yochai. **The wealth of networks: How social production transforms markets and freedom**. New Haven: Yale University Press, 2006.

BENKLER, Yochai; NISSENBAUM, Helen. Commons-based Peer Production and Virtue. **Journal of Political Philosophy**, v. 14, n. 4, p. 394–419, 2006.

BENNETT, Colin J. **Regulating privacy: Data protection and public policy in Europe and the United States**. [s.l.]: Cornell University Press, 1992.

BENNETT, Colin J. **The Governance of Privacy: Policy Instruments in Global Perspective**. Cambridge: The MIT Press, 2006.

BENOLIEL, Daniel. Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology. **California Law Review**, v. 92, p. 0, 2004.

BENTHAM, Jeremy. **O panóptico**. [s.l.]: Autêntica, 2013.

BERKELEY, John. Reinventing the company. **The Economist**, n. Online, 2015. Disponível em: <http://www.economist.com/news/leaders/21676767-entrepreneurs-are-redesigning-basic-building-block-capitalism-reinventing-company?frsc=dg%7Cd>. Acesso em: 28 out. 2015.

BERNAL, Paul. **Internet Privacy Rights: Rights to Protect Autonomy**. Cambridge: Cambridge University Press, 2014.

BERNAL, Paul A. Web 2.5: the symbiotic web. **Review of Law, Computers & Technology**, v. 24, n. 1, 2010.

BERNAL, Paul Alexander. A right to delete? **European Journal of Law and Technology**, v. 2, n. 2, 2011. Disponível em: <http://ejlt.org/article/view/75/144>. Acesso em: 17 dez. 2015.

BERNERS-LEE, Tim. WWW: past, present, and future. **Computer**, v. 29, n. 10, p. 69–77, 1996.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. São Paulo: Gen Forense, 2019.

BLACK, Ian; EDITOR, Middle East. Saudia Arabia leads Arab regimes in internet censorship. **The Guardian**, 2009. Disponível em: <https://www.theguardian.com/world/2009/jun/30/internet-censorship-arab-regimes>. Acesso em: 7 fev. 2019.

BLACK, Julia. Constitutionalising self-regulation. **The Modern Law Review**, v. 59, n. 1, 1996.

BOMSE, Amy Lynne. Dependence of Cyberspace, The. **Duke Law Journal**, v. 50, p. 1717, 2000.

BORGESIUS, Frederik J. Zuiderveen. Personal data processing for behavioural targeting: which legal basis? **International Data Privacy Law**, v. 5, n. 3, p. 163, 2015.

BROWNSWORD, Roger. Code, control, and choice: why East is East and West is West. **Legal Studies**, v. 25, n. 1, p. 1–21, 2005.

BYGRAVE, Lee A. **Internet Governance by Contract**. [s.l.]: Oxford University Press, 2015.

BYGRAVE, Lee A. The Future of Privacy Law. **European Data Protection Law Review**, v. 2, 2016.

BYGRAVE, Lee A. The place of privacy in data protection law. **UNSWLJ**, v. 24, p. 277, 2001.

BYGRAVE, Lee A.; BING, Jon. **Internet Governance : Infrastructure and Institutions**. Oxford: Oxford University Press, 2009.

CALO, Ryan; ROSENBLAT, Alex. The taking economy: Uber, information, and power. **Columbia Law Review**, v. 117, p. 1623–1690, 2017.

CANADA, Office of the Privacy Commissioner of. **Guidelines for Processing Personal Data Across Borders**. Disponível em: <https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/>. Acesso em: 3 mar. 2019.

CANADA, Office of the Privacy Commissioner of. **Office of the Privacy Commissioner of Canada**. Disponível em: <https://www.priv.gc.ca/en/>. Acesso em: 3 mar. 2019.

CANNATACI, Joseph A.; BONNICI, Jeanne Pia Mifsud. Can self-regulation satisfy the transnational requisite of successful Internet regulation? **International Review of Law, Computers & Technology**, v. 17, n. 1, p. 51–61, 2003.

CASTELLS, Manuel. **A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade**. Rio de Janeiro: Zahar, 2003. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=nCKFFmWOnNYC&oi=fnd&pg=PA5&dq=manuel+castells&ots=_CDORHz8ZP&sig=uEi4F8wSSNdLzVbgR31CJmRIKBk>. Acesso em: 14 dez. 2015.

CASTELLS, Manuel. **Communication power**. Oxford: OUP Oxford, 2013. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=qYAxAAAAQBAJ&oi=fnd&pg=PP2&dq=manuel+castells+communication&ots=zqkBfuY_8C&sig=LJXJSQCzROjRLrO_sXOc6FVkp3k>. Acesso em: 14 dez. 2015.

CASTELLS, Manuel. **The rise of the network society: The information age: Economy, society, and culture**. Londres: John Wiley & Sons, 2011.

CAVOUKIAN, Ann. Privacy by design: The 7 foundational principles. **Information and Privacy Commissioner of Ontario, Canada**, v. 5, 2009.

CAVOUKIAN, Ann; HAMILTON, Tyler J. **The Privacy Payoff: How successful businesses build customer trust**. [s.l.]: McGraw-Hill Ryerson, 2002.

CLARK, Sam. **Apple confirms Russian local data storage**. Global Data Review. Disponível em: <https://globaldatareview.com/article/1180120/apple-confirms-russian-local-data-storage>. Acesso em: 8 fev. 2019.

CNIL. None Of Your Business and La Quadrature du Net vs. Google. Disponível em: <https://www.cnil.fr/fr/node/15790>. Acesso em: 9 fev. 2019.

COHEN, Julie E. Cyberspace as/and Space. **Columbia Law Review**, v. 107, p. 210, 2007.

COHN, Cindy. **John Perry Barlow, Internet Pioneer, 1947-2018**. Electronic Frontier Foundation. Disponível em: <https://www.eff.org/deeplinks/2018/02/john-perry-barlow-internet-pioneer-1947-2018>. Acesso em: 7 fev. 2019.

CONSELHO NACIONAL DE JUSTIÇA. **CNJ premia Mercado Livre por conciliar conflitos antes do processo judicial**. Disponível em: <http://www.cnj.jus.br/noticias/cnj/84490-cnj-premia-mercado-livre-por-conciliar-conflitos-antes-do-processo-judicial>. Acesso em: 9 fev. 2019.

CORTESE, Amy. Loans That Avoid Banks? Maybe Not. **The New York Times**, 2014. Disponível em: <http://www.nytimes.com/2014/05/04/business/loans-that-avoid-banks-maybe-not.html>. Acesso em: 2 ago. 2015.

DABROWSKI, Marek; JANIKOWSKI, Lukasz. **Virtual currencies and central banks monetary policy: challenges ahead**. Belgica: European Parliament's Committee on Economic and Monetary Affairs, 2018.

DENARDIS, Laura. Internet points of control as global governance. **Internet Governance Papers**, v. 2, 2013. (Centre for International Governance Innovation). Disponível em: <https://www.cigionline.org/sites/default/files/no2_3.pdf>. Acesso em: 7 fev. 2019.

DENARDIS, Laura. **The global war for internet governance**. [s.l.]: Yale University Press, 2014.

DEUTSCHE WELLE. **Post-Arab Spring censorship on the rise**. DW.COM. Disponível em: <https://www.dw.com/en/post-arab-spring-censorship-on-the-rise/a-16725701>. Acesso em: 7 fev. 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. Disponível em: <http://egov.ufsc.br/portal/sites/default/files/anexos/29536-29552-1-PB.pdf>. Acesso em: 14 dez. 2015.

DOVI, Suzanne. Political Representation. *In*: EDWARD N. ZALTA (Org.). **The Stanford Encyclopedia of Philosophy**. Spring 2014. [s.l.: s.n.], 2014. Disponível em: <http://plato.stanford.edu/archives/spr2014/entries/political-representation/>. Acesso em: 9 out. 2015.

DUHIGG, Charles. How companies learn your secrets. **The New York Times**, 2012. Disponível em: <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>. Acesso em: 28 out. 2015.

EASTERBROOK, Frank H. Cyberspace and the Law of the Horse. **U. Chi. Legal F.**, p. 207, 1996.

ECJ. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>. Acesso em: 12 fev. 2019.

EHRLICH, Eugen. **Fundamentos da sociologia do direito**. [s.l.]: Universidade de Brasilia, 1967.

EHRLICH, Eugen. O estudo do direito vivo. **Sociologia e Direito, São Paulo, Pioneira Democracia: ideas y prácticas**, 1980.

ELERT, Niklas; HENREKSON, Magnus. Evasive entrepreneurship. **Small Business Economics**, v. 47, n. 1, p. 95–113, 2016.

EPSTEIN, Dmitry; KATZENBACH, Christian; MUSIANI, Francesca. Doing internet governance: practices, controversies, infrastructures, and institutions. **Internet Policy Review**, v. 5, n. 3, 2016. Disponível em: <https://policyreview.info/articles/analysis/doing-internet-governance-practices-controversies-infrastructures-and-institutions>. Acesso em: 11 fev. 2019.

EPSTEIN, Richard A. Can technological innovation survive government regulation. **Harv. JL & Pub. Policy**, v. 36, p. 87, 2013.

ESTADOS UNIDOS DA AMÉRICA. Riley v. California. Disponível em: <https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf>.

EUROPEAN COMMISSION. **Adequacy of the protection of personal data in non-EU countries**. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>. Acesso em: 9 fev. 2019.

EUROPEAN COMMISSION. **International data flows: Commission launches the adoption of its adequacy decision on Japan**. Disponível em: <http://europa.eu/rapid/press-release_IP-18-5433_en.htm>. Acesso em: 9 fev. 2019.

EUROPEAN COMMISSION. **Reform of the data protection legal framework in the EU**. Disponível em: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>. Acesso em: 18 dez. 2015.

EUROPEAN COMMISSION. **Regulation on promoting fairness and transparency for business users of online intermediation services**. Digital Single Market - European Commission. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services>. Acesso em: 12 fev. 2019.

EUROPEAN COMMISSION. **Transatlantic Data Flows: Restoring Trust through Strong Safeguards**. Bruxelas: European Commission, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0117&from=EN>. Acesso em: 18 fev. 2019.

EUROPEAN COURT OF JUSTICE. Decision amending decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of

personal data to third countries. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915>.

EUROPEAN COURT OF JUSTICE. Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. Disponível em: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087>.

EUROPEAN COURT OF JUSTICE. Decision on standard contractual clauses for the transfer of personal data to third countries. Disponível em: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32001D0497>.

EUROPEAN COURT OF JUSTICE. Maximillian Schrems v. Data Protection Comissioner (Case 362/2014). Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=617315>. Acesso em: 28 out. 2015.

EVANS, David S.; SCHMALENSEE, Richard. **Matchmakers: the new economics of multisided platforms.** Massachusetts: Harvard Business Press Review, 2016.

FARRANHA, Ana Claudia. Estado, sociedade e interações digitais: expectativas democráticas. **RP3-Revista de Pesquisa em Políticas Públicas**, n. 2, 2014. Disponível em: <http://periodicos.unb.br/index.php/rp3/article/download/10158/7468>. Acesso em: 14 dez. 2015.

FARRANHA, Ana Cláudia; DOS SANTOS, Leonardo Tadeu. Administração pública, direito e redes sociais: o caso da CGU no Facebook. **Revista Eletrônica do Curso de Direito da UFSM**, v. 10, n. 2, p. 742–767, 2015.

FEDERAL TRADE COMMISSION. **Internet of Things: Privacy & Security in a Connected World**. Washington: FTC, 2015. Disponível em: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

FEDERAL TRADE COMMISSION. **Protecting Children's Privacy Under COPPA: A Survey on Compliance**. Estados Unidos: FTC, 2002. Disponível em: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>. Acesso em: 7 fev. 2019.

FILGUEIRAS, Fernando. Além da Transparência: Accountability e Política da Publicidade. **Lua Nova**, v. 84, p. 65–94, 2011.

FINCK, Michèle. Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy. **European Law Review**, 2018. Disponível em: <https://ssrn.com/abstract=2990043>.

FLYVERBOM, Mikkel. **The power of networks: Organizing the global politics of the internet**. [s.l.]: Edward Elgar Publishing, 2011. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=yHpxUYsaiYYC&oi=fnd&pg=PR1&dq=mikkel+flyverbom&ots=VaGN-Urunx&sig=NoAbgHQ4DMWITO2q0u4SavIkZC0>.

FORTES, Vinícius Borges. **Os direitos de privacidade e a de dados pessoais na internet**. [s.l.]: Lumen Juris: Rio de Janeiro, 2016.

FRAZÃO, Ana de Oliveira. Plataformas digitais e os desafios para a regulação jurídica. *In*: PARENTONI, Leonardo; GONTIJO, Bruno Miranda; LIMA, Henrique Cunha Souza (Orgs.). **Direito, Tecnologia e Inovação**. Belo Horizonte: D'Plácido, 2018, v. I.

FREUND, Paul Abraham. **Privacy: one concept or many**. [s.l.]: Atherton Press, 1971.

FRIED, Charles. Privacy: Economics and Ethics: A Comment on Posner. **Ga. L. Rev.**, v. 12, p. 423, 1977.

FRYDMAN, Benoît; DE SCHUTTER, B.; PAS, J. Coregulation: a possible model for global governance. **About globalisation: views on the trajectory of mondialisation**, p. 227–242, 2004.

GALGANO, Francesco. The new lex mercatoria. **Ann. Surv. Int'l & Comp. L.**, v. 2, p. 99, 1995.

GAVISON, Ruth. Privacy and the Limits of Law. **The Yale Law Journal**, v. 89, n. 3, p. 421–471, 1980.

GLOBALPOST. **Here's everywhere Uber is banned around the world**. Business Insider. Disponível em: <https://www.businessinsider.com/heres-everywhere-uber-is-banned-around-the-world-2015-4>. Acesso em: 7 fev. 2019.

GREENBERG, Andy. Mapping how Tor's anonymity network spread around the world. **Wired UK**, n. Online, 2015. Disponível em: <http://www.wired.com/2015/09/mapping-tors-anonymity-network-spread-around-world/>. Acesso em: 27 out. 2015.

GREENBERG, Andy. The Senate's Draft Encryption Bill Is 'Ludicrous, Dangerous, Technically Illiterate'''. **Wired**, 2016. Disponível em: <https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/>. Acesso em: 7 fev. 2019.

GROSS, Hyman. The Concept of Privacy. **New York University Law Review**, v. 42, 1967.

GROSSI, Paolo. O ponto e a linha. História do Direito e Direito Positivo na formação jurista do nosso tempo. **Seqüência: Estudos Jurídicos e Políticos**, v. 26, n. 51, p. 31–46, 2005.

GUIMARÃES JÚNIOR, Mário J. L. De pés descalços no ciberespaço: tecnologia e cultura no cotidiano de um grupo social on-line. **Horizontes Antropológicos**, v. 10, n. 21, p. 123–154, 2004.

GÜRSES, Seda; TRONCOSO, Carmela; DIAZ, Claudia. Engineering privacy by design. **Computers, Privacy & Data Protection**, v. 14, n. 3, p. 25, 2011.

GUTWIRTH, Serge; DE HERT, Paul. Regulating profiling in a democratic constitutional state. *In*: **Profiling the European citizen**. London: Springer, 2008, p. 271–302. Disponível em: <http://link.springer.com/chapter/10.1007/978-1-4020-6914-7_14>. Acesso em: 16 dez. 2015.

HILDEBRANDT, Mireille. Legal and technological normativity: more (and less) than twin sisters. **Techné: research in philosophy and Technology**, v. 12, n. 3, p. 169–183, 2008.

HIRSHLEIFER, Jack. Privacy: Its origin, function, and future. **The Journal of Legal Studies**, v. 9, n. 4, p. 649–664, 1980.

HUNTER, Dan. Cyberspace as Place and the Tragedy of the Digital Anticommons. **California Law Review**, v. 91, p. 439, 2003.

IBGE. **PNAD Contínua: Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal**. Rio de Janeiro: IBGE, 2018. (PNAD Contínua). Disponível em: <https://agenciadenoticias.ibge.gov.br/media/com_mediaibge/arquivos/c62c9d551093e4b8e9d9810a6d3bafff.pdf>. Acesso em: 7 fev. 2019.

ICO. Aggregate IQ Data Services Ltd. Disponível em: <https://icoumbraco.azurewebsites.net/action-weve-taken/enforcement/aggregate-iq-data-services-ltd/>. Acesso em: 9 fev. 2019.

JAY, Rosemary; MALCOLM, William; PARRY, Ellis; *et al*. **Guide to the General Data Protection Regulation**. [s.l.]: Sweet & Maxwell, 2017.

JOERGES, Christian; SAND, Inger-Johanne; TEUBNER, Gunther. **Transnational governance and constitutionalism**. Portland: Bloomsbury Publishing, 2004. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=27zbBAAAQBAJ&oi=fnd&pg=PR1&dq=teubner+transnational+governance&ots=vB3PvPnHKc&sig=ywWb1Ku0blYXORsTdMkvxBcl5uk>. Acesso em: 20 dez. 2015.

JOHNSON, David R.; POST, David. Law and borders: the rise of law in cyberspace. **Stanford Law Review**, v. 48, p. 1367, 1995.

JONAS, Hans. **O princípio responsabilidade: ensaio de uma ética para a civilização tecnológica**. [s.l.]: Contraponto, 2006.

JONES, Jacqueline. **France top court rules surveillance law constitutional**. Jurist. Disponível em: <http://jurist.org/paperchase/2015/07/france-top-court-rules-surveillance-law-constitutional.php>. Acesso em: 1 ago. 2015.

JSTOR. Evidence in United States vs. Aaron Swartz. 2013. Disponível em: <http://docs.jstor.org/>. Acesso em: 8 fev. 2019.

JUENGER, Friedrich K. The lex mercatoria and private international law. **La. L. Rev.**, v. 60, p. 1133, 1999.

JUNGBLUT, Airton Luiz. A heterogenia do mundo on-line: algumas reflexões sobre virtualização, comunicação mediada por computador e ciberespaço. **Horizontes Antropológicos**, v. 10, n. 21, p. 97–121, 2004.

KATZ, Jonathan; MENEZES, Alfred J.; VAN OORSCHOT, Paul C.; *et al*. **Handbook of applied cryptography**. [s.l.]: CRC press, 1996.

KERR, Orin S. The Problem of Perspective in Internet Law. **Georgetown Law Journal**, v. 91, p. 357, 2002.

KIVIAT, Trevor I. Beyond bitcoin: Issues in regulating blockchain tranactions. **Duke LJ**, v. 65, p. 569, 2015.

KUNER, Christopher. Extraterritoriality and regulation of international data transfers in EU data protection law. **International Data Privacy Law**, v. 5, n. 4, 2015.

KUNER, Christopher. **Transborder data flow regulation and data privacy law**. [s.l.]: Oxford University Press Oxford, 2013.

LADEUR, Karl. ICANN and the Illusion of a Community-Based Internet: Comments on Jochen von Bersstorff. *In*: JOERGES, Christian; TEUBNER, Gunther (Orgs.). **Transnational Governance and Constitutionalism**. Oxford: Hart Publishing, 2004.

LASTOWKA, Gregory F.; HUNTER, Dan. The laws of the virtual worlds. **California Law Review**, v. 92, 2004. Disponível em: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com.br/&httpsredir=1&article=1345&context=californialawreview>.

LATOUR, Bruno. **Reagregando o social: uma introdução à teoria do ator-rede**. [s.l.]: Edusc, 2012.

LEGRAND, Pierre. Impossibility of Legal Transplants, The. **Maastricht J. Eur. & Comp. L.**, v. 4, p. 111, 1997.

LEMLEY, Mark A. Place and cyberspace. **California Law Review**, v. 91, n. 2, p. 521–542, 2003.

LEONARDI, Marcel. **Tutela e privacidade na internet**. [s.l.]: Editora Saraiva, 2012.

LERNER, Zach. A warrant to hack: An analysis of the proposed amendments to rule 41 of the federal ruled of criminal procedure. **Yale JL & Tech.**, v. 18, p. 26, 2016.

LESSIG, Lawrence. **Code version 2.0 and other laws of Cyberspace**. New York: Basic Books, 2006.

LEVIN, Dan. At U.N., China Tries to Influence Fight Over Internet Control. **The New York Times**, 2017. Disponível em: <https://www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.html>. Acesso em: 7 fev. 2019.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 2010. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=7L29Np0d2YcC&oi=fnd&pg=PA11&dq=pierre+levy&ots=giUuzyZujo&sig=XPSznoFZ2rb4tO5ELVa5j14f150>. Acesso em: 17 dez. 2015.

LOWY, Michael. **As Aventuras de Marx contra o Barão de Munchhausen**. São Paulo: Busca Vida, 1987.

LUHMANN, Niklas. **Introduction to systems theory**. Trad. Peter Gilgen. Malden: Polity, 2013.

LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. 1 edition. New York: Oxford University Press, 2015.

LYOTARD, Jean-François. **A condição pós-moderna. Tradução de Ricardo Corrêa Barbosa**. [s.l.]: Rio de Janeiro: José Olympio, 2004.

MAGRANI, Eduardo. **A Internet das Coisas**. Rio de Janeiro: FGV, 2018.

MAGRANI, Eduardo. Threats of the internet of things in a techno-regulated society: a new legal challenge of the information revolution. **International Journal of Private Law**, v. 9, n. 1–2, p. 4–18, 2018.

MARAS, Marie-Helen. Internet of Things: security and privacy implications. **International Data Privacy Law**, v. 5, n. 2, 2015.

MAROTTA-WURGLER, Florencia. What's in a standard form contract? an empirical analysis of software license agreements. **Journal of Empirical Legal Studies**, v. 4, n. 4, p. 677–713, 2007.

MAST, Tobias; OERMANN, Markus; SCHULZ, Wolfgang. Doing Internet Governance: Constructing Normative Structures Inside and Outside of Intermediary Organisations. *In*: **Annual Symposium 2016**. Washington: [s.n.], 2016. Disponível em: <https://ssrn.com/abstract=2909367>.

MATTEI, Ugo. Efficiency in legal transplants: An essay in Comparative Law and Economics. **International Review of Law and Economics**, v. 14, p. 3–19, 1994.

MAYER-SCHÖNBERGER, Viktor. **Delete: the virtue of forgetting in the digital age**. New York: Princeton University Press, 2011. Disponível em: <https://books.google.com.br/books?hl=pt-

BR&lr=&id=ZrqvYOBm_sMC&oi=fnd&pg=PP2&dq=viktor+mayer&ots=6obyU4xJfS&sig=8sKW5ZezOEp8WUte_D2Ai0hZJsw>. Acesso em: 11 dez. 2015.

MAYER-SCHONBERGER, Viktor. Demystifying Lessig. **Wis. L. REv.**, p. 713, 2008.

MAYER-SCHÖNBERGER, Viktor. Shape of Governance: Analyzing the World of Internet Regulation, The. **Va. J. Int'l L.**, v. 43, p. 605, 2002.

MAYER-SCHÖNBERGER, Viktor. Virtual Heisenberg: The Limits of Virtual World Regulability. **Washington & Lee Law Review**, v. 66, 2009.

MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. **Revista de Direito Civil Contemporâneo-RDCC (Journal of Contemporary Private Law)**, v. 9, p. 35–48, 2017.

MILLER, Arthur Raphael. **The assault on privacy: computers, data banks, and dossiers**. Michigan: University of Michigan Press, 1971.

MITTEN, Christopher. **Shawn Fanning: Napster and the music revolution**. New York: Twenty-First Century Books, 2002.

MONTEIRO, Silvana Drumond; PICKLER, Maria Elisa Valentim. O ciberespaço: o termo, a definição e o conceito. **DataGramaZero-Revista de Ciência da Informação**, v. 8, n. 3, p. 1–21, 2007.

MURRAY, Andrew. **The regulation of cyberspace: control in the online environment**. London: Routledge, 2007.

MURRAY, Andrew D. **Information technology law: the law and society**. Oxford: Oxford University Press, 2013.

MURRAY, Andrew D. Nodes and gravity in virtual space. **Legisprudence**, v. 5, n. 2, p. 195–221, 2011.

MURRAY, Andrew D. Regulation and rights in networked space. **Journal of Law and Society**, v. 30, n. 2, p. 187–216, 2003.

MURRAY, Andrew D.; SCOTT, Colin. Controlling the New Media: Hybrid Responses to New Forms of Power. **The Modern Law Review**, v. 65, n. 4, p. 491–516, 2002.

MUSTILL, Justice. The new lex mercatoria: the first twenty-five years. **Arbitration International**, v. 4, n. 2, p. 86–119, 1988.

NETANEL, Neil Weinstock. Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory. **California Law Review**, v. 88, p. 395, 2000.

NEVES, Marcelo da Costa Pinto. **Transconstitucionalismo**. 3. ed. São Paulo: WMF Martins Fontes, 2013.

NISSENBAUM, Helen. **Privacy in context: technology, policy, and the integrity of social life**. New York: Stanford University Press, 2009. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=_NN1uGn1Jd8C&oi=fnd&pg=PR7&dq=helen+nissenbaum&ots=_K5rYnf4CU&sig=yTWZHt7i0IMFSO6rTrx1V1zpuEM>. Acesso em: 28 out. 2015.

OHM, Paul. Branding Privacy. **Minnesota Law Review**, v. 97, p. 907, 2012.

OHM, Paul. Broken promises of privacy: Responding to the surprising failure of anonymization. **Ucla Law Review**, v. 57, 2009. Disponível em:

<https://pages.uoregon.edu/koopman/courses_readings/phil407-net/ohm_broken_promises_privacy.pdf>.

O'NEIL, Cathy. **Weapons of math destruction: How big data increases inequality and threatens democracy**. [s.l.]: Broadway Books, 2017.

PAAR, Christof; PELZL, Jan. **Understanding cryptography: a textbook for students and practitioners**. [s.l.]: Springer Science & Business Media, 2009.

PASQUALE, Frank. The Black Box Society. **Cambridge, MA: Harvard University Press**, v. 36, p. 32, 2015.

PAULO, Rafael Barifouse Da BBC Brasil em São. **Mais da metade das capitais brasileiras já têm projetos de lei contra o Uber**. BBC Brasil. Disponível em: <http://www.bbc.com/portuguese/noticias/2015/09/150908_uber_projetos_de_lei_rb>. Acesso em: 27 out. 2015.

PERLINGIEIRI (ORG.), Pietro. **Manuale di diritto civile**. 6. ed. Napoli: Edizione Scientifiche Italiane, 2007.

PERRITT JR, Henry H. Jurisdiction in cyberspace. **Vill. L. Rev.**, v. 41, p. 1, 1996.

PETERSON, Andrea. Could hackers take down a city? **The Washington Post**, Online. 2015. Disponível em: <https://www.washingtonpost.com/news/the-switch/wp/2015/08/18/could-hackers-take-down-a-city/>. Acesso em: 27 out. 2015.

PLAUTZ, Jason Abbruzzese and Jessica. **New York Goes to War Against Airbnb for Disrupting Hotel Business**. Mashable. Disponível em: <https://mashable.com/2014/04/26/new-york-vs-airbnb/>. Acesso em: 7 fev. 2019.

POSNER, Richard. **Do patent and copyright law restrict competition and creativity excessively?** The Becker-Posner Blog. Disponível em: <http://www.becker-posner-blog.com/2012/09/do-patent-and-copyright-law-restrict-competition-and-creativity-excessively-posner.html>. Acesso em: 1 nov. 2015.

POSNER, Richard. The economics of privacy. **The American Economic Review**, v. 71, n. 2, 1981.

POST, David G. What Larry doesn't get: code, law, and liberty in cyberspace. **Stanford Law Review**, v. 52, n. 5, p. 1439–1459, 2000.

PRESSE, Da France. **Uber tem vitória na Suprema Corte da Inglaterra e do País de Gales**. Tem um aplicativo. Disponível em: <http://g1.globo.com/tecnologia/tem-um-aplicativo/noticia/2015/10/uber-tem-vitoria-na-suprema-corte-da-inglaterra-e-do-pais-de-gales.html>. Acesso em: 7 fev. 2019.

PRZEWORSKI, Adam; STOKES, Susan C.; MANIN, Bernand. **Democracy, Accountability, and Representation**. London: Cambridge University Press, 1999.

QASIR, Sophia. Anonymity in Cyberspace: Judicial and Legislative Regulations. **Fordham Law Review**, v. 81, p. 3651, 2012.

RANCHORDÁS, Sofia. Does sharing mean caring: Regulating innovation in the sharing economy. **Minnesota Journal of Law, Sciense & Technology**, v. 16, 2015. Disponível em: <https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1356&context=mjlst>.

REIDENBERG, Joel R. Lex Informatica: The formulation of information policy rules through technology. **Tex. L. Rev.**, v. 76, p. 553, 1997.

REIDENBERG, Joel R. Technology and Internet jurisdiction. **University of Pennsylvania Law Review**, p. 1951–1974, 2005.

RICE, Eric. The Second Amendment and the Struggle Over Cryptography. **Hastings Sci. & Tech. LJ**, v. 9, p. 29, 2017.

RIDLEY, Matt. The myth of basic science. **Wall Street Journal**, Online. 2015. Disponível em: <http://www.wsj.com/articles/the-myth-of-basic-science-1445613954>. Acesso em: 28 out. 2015.

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

RODOTÀ, Stefano. **Tecnologie e diritti**. [s.l.]: Il mulino, 1995.

ROSS, Patrick Ian. Bernstein v. United States Department of State. **Berkeley Tech. LJ**, v. 13, p. 405, 1998.

RUBINSTEIN, Ira. **Regulating Privacy by Design**. Rochester, NY: Social Science Research Network, 2011. Disponível em: <http://papers.ssrn.com/abstract=1837862>. Acesso em: 13 dez. 2015.

RUNDLE, Michael. Matt Hancock's smartphone state, via Uber and blockchain. **Wired UK**, 2015. Disponível em: <https://www.wired.co.uk/article/matt-hancock-mp-interview-digital-government>. Acesso em: 7 fev. 2019.

SAMUELSON, Pamela. New Kind of Privacy - Regulating Uses of Personal Data in the Global Information Economy, A. **California Law Review**, v. 87, p. 0, 1999.

SAMUELSON, Pamela. Privacy as Intellectual Property. **Stanford Law Review**, v. 52, p. 1125–1173, 2000.

SCHAAR, Peter. Privacy by design. **Identity in the Information Society**, v. 3, n. 2, p. 267–274, 2010.

SCHOR, Juliet. Debating the sharing economy. **Journal of Self-Governance & Management Economics**, v. 4, n. 3, 2016.

SCHOR, Juliet B.; FITZMAURICE, Connor J. Collaborating and connecting: the emergence of the sharing economy. **Handbook of research on sustainable consumption**, v. 410, 2015.

SCHWARTZ, Paul M. Legal Access to the Global Cloud. **Columbia Law Review**, v. 118, n. 6, p. 1681–1762, 2018.

SCHWARTZ, Paul M. Privacy and Democracy in Cyberspace. **Vanderbilt Law Review**, v. 52, p. 0, 1999.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: privacy and a new concept of personally identifiable information. **NYU Law Review**, v. 86, p. 1814, 2011.

SCOTT, Colin. Accountability in the Regulatory State. **Journal of Law and Society**, v. 27, n. 1, p. 38–60, 2000.

SCOTT, Colin. **Regulation in the age of governance: The rise of the post regulatory state**. [s.l.]: Edward Elgar Publishing, 2004. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=1TmMDMIDgj8C&oi=fnd&pg=PA145&dq=colin+scott+regulation&ots=XcBXbCDdcG&sig=aPiWwTmci6N_XfoutFoVpuIY3w8>.

SHAH, Reema. Law enforcement and data privacy-a forward-looking approach. **Yale LJ**, v. 125, p. 543, 2015.

SIMPSON, Kevin. How a cyberbullying law in Colorado was tweaked to be more effective. **Denver post**, Online. 2015. Disponível em: <http://www.denverpost.com/news/ci_28479145/cyberbullying-tweaks-colorado-law-can-impose-fines-jail>. Acesso em: 4 ago. 2015.

SMITH, Henry E. Property as the law of things. **Harvard Law Review**, v. 125, n. 7, 2012. Disponível em: <http://www.questia.com/library/journal/1G1-289835955/property-as-the-law-of-things>.

SOLOVE, Daniel J. **Understanding privacy**. [s.l.]: Harvard university press Cambridge, MA, 2008.

SOLOVE, Daniel J.; HOOFNAGLE, C. J. A Model Regime of Privacy Protection 2.0. **SSRN Electronic Journal**, 2015. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=881294>. Acesso em: 11 dez. 2015.

SOLOVE, Daniel J.; ROTENBERG, Marc; SCHWARTZ, Paul M. **Information privacy law**. New York: Wolters Kluwer Law Business, 2014. Disponível em: <http://docs.law.gwu.edu/facweb/dsolove/information-privacy-law/files/ipl-update-2007.pdf>. Acesso em: 13 dez. 2015.

STONE SWEET, Alec. The new Lex Mercatoria and transnational governance. **Journal of European Public Policy**, v. 13, n. 5, p. 627–646, 2006.

SUNDARARAJAN, Arun. **The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism**. [s.l.]: The MIT Press, 2016.

SUNDARARAJAN, Arun. **Why the Government Doesn't Need to Regulate the Sharing Economy**. WIRED. Disponível em: <http://www.wired.com/2012/10/from-airbnb-to-coursera-why-the-government-shouldnt-regulate-the-sharing-economy/>. Acesso em: 9 abr. 2016.

SUNSTEIN, Cass. **Republic.com 2.0**. 2. ed. Princeton: Princeton University Press, 2009.

SUNSTEIN, Cass R. **A Constitution of Many Minds**. New Jersey: Princeton University Press, 2009.

SUPERIOR TRIBUNAL DE JUSTIÇA. Recurso Especial 1.348.532/SP. Disponível em: <http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/noticias/Not%C3%ADcias/%C3%89-abusiva-cl%C3%A1usula-que-obriga-cliente-de-cart%C3%A3o-de-cr%C3%A9dito-a-fornecer-dados-a-terceiros>. Acesso em: 18 fev. 2019.

SWEET, Alec Stone. The new Lex Mercatoria and transnational governance. **Journal of European Public Policy**, v. 13, n. 5, p. 627–646, 2006.

SWIRE, Peter P.; AHMAD, Kenesa. **US Private-sector Privacy: Law and Practice for Information Privacy Professionals**. [s.l.]: International Association of Privacy Professionals (IAPP), 2012.

SWIRE, Peter P.; AHMAD, Kenesa; MCQUAY, Terry. **Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices**. [s.l.]: International Association of Privacy Professionals, 2012.

TAMANAHA, Brian Z.; SAGE, Caroline; WOOLCOCK, Michael. **Legal Pluralism and Development: Scholars and Practitioners in Dialogue**. New Haven: Cambridge University Press, 2012.

TAYLOR, Josh. **France drops Hadopi three-strikes copyright law**. ZDNet. Disponível em: <http://www.zdnet.com/article/france-drops-hadopi-three-strikes-copyright-law/>. Acesso em: 2 abr. 2016.

TAYLOR, Josh. **Rights holders could get sites blocked without evidence**. ZDNet. Disponível em: <http://www.zdnet.com/article/rights-holders-could-get-sites-blocked-without-evidence/>. Acesso em: 2 ago. 2015.

TEMPERTON, James; BURGESS, Matt. **Net neutrality: European Parliament votes in favour of "two speed" internet**. Wired UK. Disponível em: <http://www.wired.co.uk/news/archive/2015-10/27/net-neutrality-european-union-vote>. Acesso em: 28 out. 2015.

TENE, Omer; POLONETSKY, Jules. A Theory of Creepy: Technology, Privacy and Shifting Social Norms. **Yale Journal of Law and Technology**, v. 16, 2013. Disponível em: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/yjolt16&div=3&id=&page=>. Acesso em: 11 fev. 2019.

TEUBNER, Gunther. A Bukowina global sobre a emergência de um pluralismo jurídico transnacional. **Impulso: Revista de Ciências Sociais e Humanas**, v. 14, n. 33, p. 9–31, 2003.

TEUBNER, Gunther. Breaking frames: economic globalization and the emergence of lex mercatoria. **European Journal of Social Theory**, v. 5, n. 2, p. 199–217, 2002.

TEUBNER, Gunther. **Constitutional fragments: Societal constitutionalism and globalization**. Oxford: Oxford University Press, 2012. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=kKDK5w5UJdMC&oi=fnd&pg=PP2&dq=teubner+constitutional&ots=fFyE0OGkd8&sig=kiWR82yAKYfBQzb9MYwucGf7Vjs>. Acesso em: 20 dez. 2015.

TEUBNER, Gunther. **Direito, sistema e policontexturalidade**. Piracicaba: Unimep, 2005.

TEUBNER, Gunther. **Fragmentos constitucionais: Constitucionalismo social na globalização**. São Paulo: Saraiva, 2016.

TEUBNER, Gunther. Global Bukowina: Legal Pluralism in the World-Society. **Global law without State**, p. 3–28, 1996. (Social Science Research Network).

TEUBNER, Gunther. Legal irritants: good faith in British law or how unifying law ends up in new divergencies. **The Modern Law Review**, v. 61, n. 1, p. 11–32, 1998.

TEUBNER, Gunther. Societal Constitutionalism: Alternatives to State-Centered Constitutional Theory? *In*: JOERGES, Christian (Org.). **Transnational Governance and Constitutionalism**. Oxford: Hart Publishing, 2004.

THALER, Richard H. Behavioral economics: past, present, and future. **American Economic Review**, v. 106, n. 7, p. 1577–1600, 2016.

THALER, Richard H. **Misbehaving: The making of behavioral economics**. Nova York: WW Norton & Company, 2015.

THALER, Richard H.; SUNSTEIN, Cass R. **Nudge: Improving Decisions about Health, Wealth, and Happiness**. [s.l.]: Penguin, 2009.

THALER, Richard H.; SUNSTEIN, Cass R.; BALZ, John P. Choice architecture. 2014.

TIEGHI, Ana Luiza. **Conexão wifi é caminho para loja conhecer cliente e direcionar vendas**. Folha de São Paulo. Disponível em:

<https://www1.folha.uol.com.br/mpme/2019/02/conexao-wifi-e-caminho-para-loja-conhecer-cliente-e-direcionar-vendas.shtml>. Acesso em: 11 fev. 2019.

TURKLE, Sherry. **Alone together: why we expect more from technology and less from each other**. First Trade Paper Edition edition. New York: Basic Books, 2012.

TURKLE, Sherry. Cyberspace and identity. **Contemporary Sociology**, p. 643–648, 1999.

UNESCO. **Human rights and encryption**. [s.l.: s.n., s.d.]. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000246527>. Acesso em: 3 mar. 2019.

USTARAN, Eduardo. European privacy: law and practice for data protection professionals. **Portsmouth, NH: International Association of Privacy Professionals (IAPP)**, 2012.

USTARAN, Eduardo. **The Future of Privacy**. Londres: Data Guidance, 2013. (Kindle). Disponível em: <https://www.amazon.com/Future-Privacy-Mr-Eduardo-Ustaran/dp/0992678005>. Acesso em: 19 fev. 2019.

VELLOSO, Ricardo Vianna. O ciberespaço como ágora eletrônica na sociedade contemporânea. **Ci. Inf., Brasília**, v. 37, n. 2, p. 103–109, 2008.

VENKATADRI, Giridhari; ANDREOU, Athanasios; LIU, Yabing; *et al*. Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface. *In*: **Federal Trade Commission PrivacyCon**. Washington: [s.n.], 2018, p. 221–239. Disponível em: <https://mislove.org/publications/PII-Oakland.pdf>.

VESTING, Thomas. Constitutionalism or legal theory: comments on Gunther Teubner. **JOERGES, Christian; SAND, Inger-Johanne; TEUBNER, Gunther. Transnational governance and constitutionalism. Oxford: Hart**, p. 29–39, 2004.

VESTING, Thomas. Teoria do direito: uma introdução. **São Paulo: Saraiva**, p. 226, 2015.

VIEHWEG, Theodor. **Tópica e jurisprudência**. Trad. Tércio Sampaio Ferraz Júnior. Brasília: UnB, 1979.

VOLPICELLI, Gian. **Alex Pentland: Big data will help us hold governments accountable**. Wired UK. Disponível em: <http://www.wired.co.uk/news/archive/2015-10/15/alex-pentland-wired-2015>. Acesso em: 27 out. 2015.

VON JHERING, Rudolf. In the heaven for legal concepts: a fantasy. **Temp. LQ**, v. 58, p. 799, 1985.

WALDMAN, Ari Ezra. Privacy, notice, and design. **Stanford Technology Law Review**, v. 21, p. 74, 2018.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard law review**, p. 193–220, 1890.

WATSON, Alan. **Legal transplants and European private law**. [s.l.]: Metro Maastricht, 2000. Disponível em: <http://www.ejcl.org/44/art44-2.html?iframe=true&width=100%&height=100%>. Acesso em: 9 dez. 2016.

WEBER, Max. Economia e sociedade: fundamentos da sociologia compreensiva. v. 1. **Brasília: UnB**, 1999.

WESTIN, Alan F. Privacy and freedom. 1970. Disponível em: <http://philpapers.org/rec/WESPAF-2>. Acesso em: 14 dez. 2015.

WICHOWSKI, Alexis. **Facebook and Google are actually "Net States" and they rule the world**. Wired. Disponível em: <https://www.wired.com/story/net-states-rule-the-world-we-need-to-recognize-their-power/>. Acesso em: 12 fev. 2019.

WILLIS, Lauren E. Why not privacy by default. **Berkeley Technology Law Journal**, v. 29, p. 61, 2014.

WOOLGAR, Steve; NEYLAND, Daniel. **Mundane governance: Ontology and accountability**. Oxford: OUP Oxford, 2013.

WORKING PARTY 29. **Explanatory Document on the Processor Binding Corporate Rules**. Bruxelas: WP29, 2013. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf>.

WORKING PARTY 29. **Opinion 1/2010 on the concepts of controller and processor**. Bruxelas: [s.n.], 2010. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf>.

WORKING PARTY 29. **Opinion 3/2010 on the principle of accountability**. Bruxelas: WP29, 2010. Disponível em: <https://www.dataprotection.ro/servlet/ViewDocument?id=654>.

WORKING PARTY 29. **Opinion 4/2007 on the concept of personal data**. Bruxelas: [s.n.], 2007. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.

WORKING PARTY 29. **Opinion 5/2014 on Anonymisation Technques**. Bruxelas: [s.n.], 2014. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

WORKING PARTY 29. **Opinion 8/2014 on the on Recent Developments on the Internet of Things**. Bruxelas: WP29, 2014. Disponível em: <https://www.dataprotection.ro/servlet/ViewDocument?id=1088>.

WORKING PARTY 29. **Opinion on Adequacy Referential**. Bruxelas: WP 29, 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108>. Acesso em: 9 fev. 2019.

WORKING PARTY 29. **Opinion on Data Protection Officers (DPOs)**. Bruxelas: [s.n.], 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>.

ZITTRAIN, Jonathan. Icann: between the public and the private comments before Congress. **Berkeley Tech. LJ**, v. 14, p. 1071, 1999.

ZITTRAIN, Jonathan. **The future of the internet–and how to stop it**. [s.l.]: Yale University Press, 2008. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=NiATs-C6nlQC&oi=fnd&pg=PA1&dq=zittrain+jonathan&ots=Cv9wUJprkx&sig=_0WVC790L4l9Nioto0zePCyPLns>.

ZUBOFF, Shoshana. **The age of surveillance capitalism: The fight for a human future at the new frontier of power**. Nova York: Public Affairs, 2019.

A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority. Federal Trade Commission. Disponível em: <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>. Acesso em: 1 mar. 2019.

Accountability Agents. Cross Border Privacy Rules System. Disponível em: <http://cbprs.org/accountability-agents/>. Acesso em: 3 mar. 2019.

Ad-ID Overview & Glossary of Terms. Disponível em: <http://www.ad-id.org/how-it-works/overview-glossary-of-terms>. Acesso em: 19 fev. 2019.

APEC Privacy Framework. Disponível em: <http://publications.apec.org/Publications/2005/12/APEC-Privacy-Framework>. Acesso em: 3 mar. 2019.

Chapter B: Key concepts - consent. Disponível em: </agencies-and-organisations/app-guidelines/chapter-b-key-concepts>. Acesso em: 3 mar. 2019.

Cross Border Privacy Rules System. Disponível em: <http://cbprs.org/>. Acesso em: 3 mar. 2019.

Data is giving rise to a new economy: Fuel of the future. The Economist. Disponível em: <https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy>. Acesso em: 7 fev. 2019.

Global Privacy Enforcement Network: An International Network to Foster Cross-Border Co-operation. Disponível em: <https://www.privacyenforcement.net/about_the_network>. Acesso em: 3 mar. 2019.

Governo estuda taxar aluguel informal de imóveis, cômodos ou mesmo sofás - 07/08/2015 - Mercado. Folha de S.Paulo. Disponível em: <http://www1.folha.uol.com.br/mercado/2015/08/1665734-governo-estuda-taxar-aluguel-informal-de-imoveis-comodos-ou-mesmo-sofas.shtml>. Acesso em: 7 fev. 2019.

It's Been 20 Years Since This Man Declared Cyberspace Independence | WIRED. Disponível em: <https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/>. Acesso em: 7 fev. 2019.

Kleros:The Blockchain Dispute Resolution Layer. Disponível em: <https://kleros.io/>. Acesso em: 12 fev. 2019.

Moley to present the world's first robot kitchen in 2017 - Business Insider. Disponível em: <https://www.businessinsider.com/moley-to-present-the-worlds-first-robot-kitchen-in-2017-2015-11>. Acesso em: 7 fev. 2019.

O papel do DevOps como alicerce da próxima revolução tecnológica. Computerworld. Disponível em: <https://computerworld.com.br/2016/09/16/devops-sera-o-alicerce-da-proxima-revolucao-tecnologica/>. Acesso em: 8 fev. 2019.

Office of the Australian Information Commissioner - OAIC. Disponível em: <https://www.oaic.gov.au/>. Acesso em: 3 mar. 2019.

Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. Disponível em: <https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss>. Acesso em: 3 mar. 2019.

Privacy Act 1988. Disponível em: <https://www.legislation.gov.au/Details/C2017C00283>. Acesso em: 3 mar. 2019.

Privacy Shield Program Overview. Disponível em: <https://www.privacyshield.gov/Program-Overview>. Acesso em: 3 mar. 2019.

PROTECCION DE LOS DATOS. Disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/norma.htm>. Acesso em: 18 fev. 2019.

Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers. Federal Trade Commission. Disponível em: <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers>. Acesso em: 3 mar. 2019.

Reno v. ACLU. Oyez. Disponível em: <https://www.oyez.org/cases/1996/96-511>. Acesso em: 7 fev. 2019.

The robot chef coming to a kitchen near you - Telegraph. Disponível em: <https://www.telegraph.co.uk/finance/businessclub/11912085/The-robot-chef-coming-to-a-kitchen-near-you.html>. Acesso em: 7 fev. 2019.

United States v. Graham. **Harvard Law Review**, v. 130, 2017. Disponível em: <https://harvardlawreview.org/2017/02/united-states-v-graham/>. Acesso em: 19 fev. 2019.

What does data protection 'by design' and 'by default' mean? European Commission - European Commission. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en>. Acesso em: 17 fev. 2019.

What is Identifier for Advertisers (IFA/IFDA)? - Definition from Techopedia. Disponível em: <https://www.techopedia.com/definition/29032/identifier-for-advertisers-ifa-ifda>. Acesso em: 19 fev. 2019.

WikiLeaks. Disponível em: <https://wikileaks.org/>. Acesso em: 8 fev. 2019.