DENNYS MARCELO ANTONIALLI

A arquitetura da Internet e o desafio da tutela do direito à privacidade pelos Estados nacionais

Tese de Doutorado

Orientador: Prof. Dr. Virgílio Afonso da Silva

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo - SP

2017

DENNYS MARCELO ANTONIALLI

A arquitetura da Internet e o desafio da tutela do direito à privacidade pelos Estados nacionais

Tese apresentada à Banca Examinadora do Programa de Pós-graduação em Direito da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para a obtenção do título de Doutor em Direito, na área de concentração Direito do Estado, sob a orientação do Prof. Dr. Virgílio Afonso da Silva.

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo - SP

2017

Ficha catalográfica

ANTONIALLI, Dennys M.

A arquitetura da Internet e o desafio da tutela do direito à privacidade pelos Estados nacionais. 158 fls.
Tese de Doutorado.
Faculdade de Direito da Universidade de São Paulo
São Paulo-SP
2017

DENNYS MARCELO ANTONIALLI

A arquitetura da Internet e o desafio da tutela do direito à privacidade pelos Estados nacionais

Tese apresentada à Banca Examinadora do Programa de Pós-graduação em Direito da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para a obtenção do título de Doutor em Direito, na área de concentração Direito do Estado, sob a orientação do Prof. Dr. Virgílio Afonso da Silva.

Aprovado em: _____

Banca Examinadora:

Prof. Dr._____ Instituição: _____

Julgamento: _____ Assinatura:_____

Prof. Dr._____ Instituição: _____

Julgamento: _____ Assinatura:_____

Prof. Dr._____ Instituição: _____

Julgamento: _____ Assinatura:_____

Prof. Dr._____ Instituição: _____

Julgamento: _____ Assinatura:_____

Prof. Dr._____ Instituição: _____

Julgamento: _____ Assinatura:_____

AGRADECIMENTOS

Além de desafiadora, a tarefa de escrever uma tese de doutorado pode, por vezes, pesar sobre os ombros. São momentos de angústia, incerteza e insegurança que podem tornar o processo muito penoso. Ao longo dos cinco anos em que estive comprometido com este projeto, tive a sorte de poder contar com o apoio de muitos amigos, colegas, professores e familiares, a quem agradeço de forma geral e irrestrita. Também tive a oportunidade de passar duas temporadas fora do Brasil para avançar na pesquisa de temas ligados a este doutorado; a primeira em Berlim, como pesquisador do *Alexander von Humboldt Institute for Internet and Society* e a segunda de volta a *Stanford Law School*, a convite do Prof. Lawrence Friedman, como pesquisador visitante. Nessas experiências, muitas pessoas cruzaram meu caminho e agradeço a todas aquelas que, a seu modo, me ajudaram a superar a saudade e a distância de casa. Nos parágrafos a seguir, tento resumir minha gratidão a todas essas pessoas citando algumas que foram especialmente importantes nesse processo.

Agradeço ao Prof. Virgílio Afonso da Silva, meu orientador, pela oportunidade, pelos ensinamentos, pelos aconselhamentos precisos e sinceros sobre a vida acadêmica e, sobretudo, pela confiança que depositou em mim e nos projetos que encampei nesse período, em especial o Núcleo de Direito, Internet e Sociedade (NDIS-USP), atividade de cultura e extensão da Faculdade que tive o prazer de poder fundar e coordenar sob sua supervisão nesses cinco anos. Agradeço a ele também por ter me engrandecido como pessoa e como acadêmico, me ajudando a deixar de lado a pequeneza que ronda a academia;

Agradeço ao Francisco Brito Cruz, meu grande amigo e parceiro de múltiplos projetos, com quem divido tantos momentos, pelo apoio constante e incondicional. Agradeço também pelas palavras de conforto que frequentemente me oferece e pela paciência com as minhas variações de humor, que o submetem a tantas grosserias. Foi com o Chico que desenvolvi minha consciência política e a ele eu devo tudo o que isso me trouxe de bom. Com o Chico também fundei as duas atividades que movem a minha vida profissional e que me fazem tão realizado, o NDIS-USP e o InternetLab. Obrigado por ter aceitado trilhar esses caminhos comigo; você mudou minha vida!;

Agradeço à Mariana Valente, amiga querida e também parceira de tantos projetos, pela profundidade e delicadeza que acrescenta aos meus dias. Agradeço também por me ajudar a superar minhas incertezas e angústias e a me ensinar a olhar para o mundo de forma mais tranquila e consciente do papel das coisas. Com a Mari aprendi a aceitar melhor meus erros e a prestar mais atenção no que eu tenho de bom. Com a aposta dela no InternetLab também tive mais certeza de estar no caminho certo. Obrigado por ter aceitado dividir planos e sonhos comigo e com o Chico;

Agradeço à Camila Moraes Baceti, pela amizade sincera e por se fazer sempre presente, mesmo à distância; sem você eu não teria conseguido superar muitos obstáculos;

Agradeço à Beatriz Kira e à Jacqueline Abreu não só pela ajuda valorosa no desenvolvimento e revisão desta tese, mas também por acreditarem e apostarem no InternetLab, junto de quem também agradeço a toda a equipe do InternetLab, em especial Natália Néris, Thiago Oliva, Juliana Ruiz e Maike Wile dos Santos.

Agradeço ao Rafael de Souza Lourenço, pela amizade que resistiu ao tempo e por me resgatar dos meus momentos de instabilidade ou incoerência;

Agradeço ao Bruno Moschetta, Carla Gasparian, Claudia Figueira, Amanda Rivellis, Danilo Cymrot, João Brandão, Guilherme Genestretti, Estela Takahashi e Manuela Camargo, meus amigos da turma de graduação, por não terem me abandonado a despeito das minhas viagens e ausências;

Agradeço aos professores da Faculdade de Direito da Universidade de São Paulo, em especial Conrado Hübner Mendes, Diogo Rosenthal Coutinho, Marcos Paulo Veríssimo, Ronaldo Porto Macedo Jr. e Juliano Maranhão, pelas discussões enriquecedoras;

Agradeço aos amigos da pós-graduação, Artur Péricles Lima Monteiro, Rafael Bellem de Lima, Luciana Oliveira Ramos, Natália Pires, Carolina Marinho, Rodrigo Nitrini e Pedro Aleixo, por dividirem comigo angústias e reflexões;

Agradeço ainda a todos aqueles que contribuem para as discussões sobre políticas de Internet no Brasil, com quem aprendo e aprendi tanto: Rafael Zanatta, Marcel Leonardi, Carlos Affonso de Souza Pereira, Ronaldo Lemos, Luiz Moncau, Pablo Ortellado, Laura Schertel Mendes, Daniel Oppermann, Ana Carolina Monteiro, Danilo Doneda, Bruno Bioni, Renato Leite Monteiro, Marcelo Crespo, Margareth Kang, Nahema Falleiros, Tiago Cardieri.

Agradeço a todos os alunos de graduação que participaram do NDIS-USP, cujas opiniões e reflexões me ajudaram a amadurecer minha visão sobre o campo;

Agradeço ao Prof. Lawrence Friedman, pela orientação transformadora durante o SPILS e pela confiança no meu potencial;

Agradeço à Sarah Shirazyan, pela amizade, apoio e por ter tornado as minhas temporadas nos Estados Unidos tão especiais;

Agradeço aos amigos que fiz ao longo das minhas experiências internacionais, com quem dividi momentos inesquecíveis, Diego Gil McCawley, Juan Diego Castañeda, Laura Van Den Eynde, Hulda Magnusdottir, Loic Coutellier, Eduardo Armas, Janet Merkel, Crystal Abidin, Fernán Restreppo.

Agradeço também àqueles com quem tive a oportunidade de discutir temas afetos a esta tese, Chris Hoofnagle, Victoria Nash, Woodrow Hartzog, Deborah Hensler, Katitza Rodriguez, Kristina Irion, Dennis Hirsch, Riana Pfefferkorn, Jennifer Granick, Barbara van Schewick.

Por fim e certamente não menos importantes, agradeço ao meu pai, minha mãe e minha irmã, pelo amor e apoio incondicional.

Muito obrigado a todos.

RESUMO

ANTONIALLI, Dennys M. A arquitetura da Internet e o desafio da tutela do direito à privacidade pelos Estados nacionais. 2016. (Doutorado) - Faculdade de Direito da Universidade de São Paulo, São Paulo, 2016.

A indústria da publicidade digital é a base de grande parte dos modelos de negócios das empresas do setor de Internet e envolve uma complexa cadeia de atores intermediários que desempenham atividades de monitoramento, coleta e tratamento de dados pessoais. Dada a arquitetura da Internet, essas atividades são viabilizadas pela utilização de tecnologias que operam de forma globalizada, independentemente das fronteiras territoriais que delimitam a aplicação das normas constitucionais e legislações de proteção de dados pessoais. Sendo assim, sua utilização coloca em colisão os diferentes modelos regulatórios de privacidade adotados pelos Estados nacionais. Considerando a concentração significativa das empresas do setor de Internet nos Estados Unidos, esta tese de doutorado investiga *(i)* se e de que forma o modelo regulatório de privacidade estadunidense possibilita a responsabilização de atores privados lá sediados em relação a violações de normas constitucionais e legislações de proteção de dados estrangeiras; e *(ii)* se e de que forma a interferência desses atores privados gera repercussões para as capacidades de tutela do direito à privacidade no âmbito dos Estados nacionais. Para tanto, a tese está organizada em cinco capítulos: *(i)* o capítulo 1 descreve o ecossistema da indústria de publicidade digital e apresenta os desafios adicionais introduzidos pela arquitetura da Internet para a tutela do direito à privacidade, destacando as caraterísticas de funcionamento técnico das tecnologias de monitoramento e coleta de dados pessoais, bem como dos sistemas de compra, venda e alocação de anúncios na Internet; *(ii)* o capítulo 2 analisa a implementação do *Safe Harbor* como tentativa de compatibilização dos modelos regulatórios de privacidade adotados nos Estados Unidos e na União Europeia para possibilitar a transferência internacional de dados entre as duas regiões, identificando suas principais características e limitações; *(iii)* o capítulo 3 analisa a atuação da Comissão Federal do Comércio dos Estados Unidos, apresentando suas prerrogativas e limitações para fiscalizar e responsabilizar atores privados localizados nos Estados Unidos por violações a normas constitucionais e legislações de privacidade estrangeiras; *(iv)* o capítulo 4 analisa os obstáculos impostos pela legislação estadunidense ao reconhecimento e execução de ordens judiciais estrangeiras e suas repercussões para as possibilidades de responsabilização desses atores por outros Estados nacionais; *(v)* o capítulo 5 reflete sobre como a insuficiência de mecanismos jurídicos de responsabilização de atores privados sediados nos Estados Unidos pode implicar a sua interferência sobre a tutela de direitos fundamentais para os Estados nacionais, apresentando argumentos para o aprofundamento das teorias ligadas ao constitucionalismo transnacional nesse sentido.

Palavras-chave: privacidade, dados pessoais, jurisdição, Internet, publicidade comportamental, tecnologias de coleta de dados, constitucionalismo transnacional, direitos fundamentais.

ABSTRACT

ANTONIALLI, Dennys M. Internet architecture and the challenge of enforcing online privacy rights by national states. 2016. (Doctorate) - Faculty of Law, University of São Paulo, São Paulo, 2016.

The online advertising industry is the basis of many of the business models adopted by Internet companies and involves a complex chain of intermediary actors who perform data collecting and data processing activities. Given the architecture of the Internet, these activities are enabled by the use of technologies that operate globally, regardless of the territorial boundaries that govern the application of national constitutional norms and local data protection laws. Therefore, their use may result in an overlap of conflicting privacy regulatory regimes adopted by different national states. Considering the significant concentration of Internet companies in the United States, this doctoral thesis investigates *(i)* whether and how the U.S. privacy regulatory regime makes it possible to enforce foreign privacy laws against actors solely based in the U.S.; and *(ii)* whether and how the interference of these private actors generates repercussions on the ability that national states have to enforce their local privacy laws. To this end, the thesis is strcutured in five chapters: *(i)* chapter 1 describes the ecosystem of the online advertising industry and presents the additional challenges introduced by the Internet architecture for the protection of the right to privacy, explaining how online tracking and ad serving technologies work; *(ii)* chapter 2 examines the implementation of the Safe Harbor Agreement as an attempt to reconcile the privacy regulatory regimes adopted in the United States and in the European Union in order to enable international transfers of data between the two regions, identifying their main characteristics and limitations; *(iii)* chapter 3 examines the role of the Federal Trade Commission of the United States in policing and enforcing foreign privacy laws, addressing its main obstacles and limitations; *(iv)* chapter 4 examines the obstacles imposed by U.S. law to the recognition and enforcement of foreign court orders and their repercussions to the possibilities of foreign national states to enforce their local privacy laws; *(v)* chapter 5 reflects on how the insufficiency of legal mechanisms to enforce foreign privacy laws against U.S.-based private actors may result in their interference in the ability of national states to enforce local privacy laws, providing concluding arguments for theories related to transnational constitutionalism.

Keywords: online privacy, data protection, enforcement, jurisdiction, Internet, online advertising, behavioral advertising, online tracking technologies, transnational constitutionalism, fundamental rights.

ABSTRACT (ITALIANO)

ANTONIALLI, Dennys M. L'architettura di Internet e la sfida della tutela del diritto alla vita privata da parte degli Stati nazionali. 2016. (Dottorato) - Facoltà di Diritto, Università di São Paulo, São Paulo, 2016.

Il settore della pubblicità digitale è alla base di gran parte dei modelli di business delle aziende del settore Internet e comporta una complessa catena di attori intermedi che svolgono attività di monitoraggio, raccolta e trattamento dei dati personali. Data l'architettura di Internet, queste attività sono rese possibili mediante l'uso di tecnologie che operano su base globalizzata, indipendentemente dai confini territoriali che limitano l'applicazione delle norme costituzionali e la legislazione sulla protezione dei dati personali. Così, il loro uso mette su una collisione dei diversi modelli normativi di privacy adottate dagli stati nazionali. Considerando la notevole concentrazione di aziende del settore Internet negli Stati Uniti, questa tesi di dottorato indaga (i) se e in che modo il quadro normativo degli Stati Uniti privacy consente la responsabilità di attori privati là basati in relazione alle norme costituzionali violazioni e le leggi la protezione dei dati estera; e (ii) se e come l'interferenza di questi attori privati solleva implicazioni per il diritto alla capacità di protezione della privacy all'interno degli Stati nazionali. Pertanto, la tesi è organizzata in cinque capitoli: (i) il Capitolo 1 descrive l'ecosistema del settore della pubblicità digitale e presenta ulteriori sfide introdotte dalla architettura di Internet per la tutela del diritto alla privacy, mettendo in evidenza le caratteristiche di funzionamento di tecniche tecnologie di monitoraggio e raccolta di dati personali, così come sistemi di acquisto, vendita e assegnazione di annunci su Internet; (ii) il capitolo 2 analizza l'attuazione del Safe Harbor come un tentativo di conciliare i modelli normativi di privacy adottate negli Stati Uniti e l'Unione Europea per facilitare il trasferimento internazionale di dati tra le due regioni, individuando le sue principali caratteristiche e limitazioni; (iii) il capitolo 3 analizza le prestazioni della Commissione federale del commercio degli Stati Uniti, con le sue prerogative e limitazioni per monitorare e tenere attori privati situati negli Stati Uniti per violazioni delle norme costituzionali e le leggi sulla privacy stranieri; (iv) il capitolo 4 analizza gli ostacoli imposti dalla legge degli Stati Uniti e il riconoscimento e l'esecuzione delle decisioni giudiziarie straniere e il loro impatto sulle possibilità di potenziamento di tali attori da parte di altri Stati-nazione; (v) Capitolo 5 riflette sulla mancanza di meccanismi legali di responsabilità di soggetti privati con sede negli Stati Uniti può portare ad interferenze sulla tutela dei diritti fondamentali per gli stati nazionali, presentando gli argomenti per l'ulteriore sviluppo delle teorie relative al costituzionalismo transnazionale.

Parole chiave: vita privata, dati personali, giurisdizione, Internet, pubblicità comportamentale, tecnologie di raccolta di dati, costituzionalismo transnazionale, diritti fondamentali.

Lista de gráficos

Lista de tabelas

SUMÁRIO

INTRODUÇÃO

Em 1999, o então diretor executivo da empresa Sun Microsystems[1], Scott McNealy, respondeu a uma pergunta durante o lançamento de um produto com a seguinte afirmação: "Você tem privacidade zero, acostume-se com isso."[2] No mesmo ano, a matéria de capa do mês de maio da revista britânica *The Economist* chegava a essa mesma conclusão, em tom conformista: a privacidade estava fadada à morte.[3] No ano seguinte, Michael Froomkin publicou artigo questionando se se estaria, de fato, diante do fim do direito à privacidade.[4] Apesar de a resposta do autor ter sido negativa[5], a ideia de que a privacidade teria deixado de existir continuou a ser preconizada por empresários[6] e acadêmicos[7].

Dezessete anos depois, esse debate ainda persiste. Constantemente, os anúncios de novos produtos[8], por parte da iniciativa privada, ou de novas capacidades de vigilância[9], por parte do Estado, levantam questões a respeito da extensão desse direito e provocam reflexões sobre os novos contornos que teria assumido.

Enquanto o futuro da privacidade não se define, a Internet invade a vida dos cidadãos de forma quase implacável. De transações bancárias a consultas médicas, ela

---

[1] A empresa ficou conhecida por desenvolver a linguagem de programação Java, que possibilita a exibição de imagens animadas, vídeos e sons em anúncios *online*. Posteriormente, a empresa foi adquirida pela Oracle Inc.

[2] Cf. Polly Sprenger, "Sun on privacy: 'Get Over It'", *Wired* (26/01/1999) <disponível em: http://archive.wired.com/politics/law/news/1999/01/17538, último acesso em 23.05.2016>.

[3] Cf. Conselho Editorial da The Economist, "The end of privacy", *The Economist* (1999) <disponível em: http://www.economist.com/node/202103, último acesso em 02.01.2017>.

[4] Michael Froomkin, "The Death of Privacy?", *Stanford Law Review* 52 (2000), 1461.

[5] Cf. Michael Froomkin, "The Death of Privacy?", p. 1466.

[6] Cf. Bobbie Johnson, "Privacy no longer a social norm, says Facebook founder", *The Guardian* (11.01.2010) <disponível em: http://www.theguardian.com/technology/2010/jan/11/facebook-privacy, último acesso em 02.01.2017>.

[7] Cf. Mark Prigg, "Privacy is dead, Harvard professors tell Davos forum", *Mail Online* (2015) <disponível em: http://www.dailymail.co.uk/sciencetech/article-2921758/Privacy-dead-Harvard-professors-tell-Davos-forum.html, último acesso em 02.01.2017>.

[8] A chegada dos chamados "vestíveis", como o *Google Glass*, é um exemplo disso. Cf. Anna Carolina Papp, "Óculos do Google elevam receio com a privacidade", *Link Estadão* (2013) <disponível em: http://link.estadao.com.br/noticias/geral,oculos-do-google-elevam-receio-com-a-privacidade,10000033200, último acesso em 02.01.2017>.

[9] Os balões utilizados para a segurança nos jogos olímpicos de 2016, no Rio de Janeiro, despertaram, por exemplo, uma série de preocupações ligadas à privacidade dos cidadãos. Cf. Conselho Editorial do G1, "Balões com câmeras vão ajudar na segurança das Olimpíadas no Rio", *G1 Rio* (02.10.2015) <disponível em: http://g1.globo.com/rio-de-janeiro/noticia/2015/10/baloes-com-cameras-vao-ajudar-na-seguranca-das-olimpiadas-no-rio.html, último acesso em 02.01.2017>.

transformou a dinâmica de boa parte das atividades cotidianas, passando a intermediar não só as relações que se estabelecem entre as pessoas, como também as que se estabelecem entre elas e os setores público e privado. Evidência disso é o número cada vez maior de dispositivos que adquirem capacidades de conexão à Internet, movimento que se convencionou chamar de "Internet das coisas": lâmpadas[10], relógios[11], aviões[12], aparelhos de ginástica[13] e até mesmo objetos como garrafas de bebidas[14].

As transformações pelas quais o conceito de privacidade tem passado ocupam as agendas de pesquisa de áreas do conhecimento que vão da filosofia à ciência da computação e são objeto de inúmeras propostas e formulações teóricas.[15] A falta de consenso entre os acadêmicos também pode ser percebida na própria sociedade, que abriga perspectivas muito diferentes em relação ao conceito de privacidade.

Quando o *Google Street View* começou a ser disponibilizado fora dos Estados Unidos, em 2008, por exemplo, as reações nos países em cujo lançamento foi anunciado foram bem diferentes: no Japão, houve muita resistência à ideia de que fotografias das calçadas, consideradas um espaço privado, fossem publicadas na Internet[16]; na República Tcheca e na Suíça, também foi recebida com reservas a digitalização das imagens das

[10] Cf. James Stables, "The best smart bulbs for your connected smart home", *Wareable* (2016) <disponível em https://www.wareable.com/smart-home/best-smart-bulbs-for-your-tech-home, último acesso em 02.01.2017>.

[11] Cf. Galen Gruman, "Apple Watch: the internet of things' new frontier". *InfoWorld* (2014) <disponível em: http://www.infoworld.com/article/2608996/consumer-electronics/article.html, último acesso em 02.01.2017>.

[12] Cf. Woodrow Bellyamy, "The connected aircraft: Beyond passenger entertainment and into flight operations", *Avionics Today* (2014) <disponível em: http://interactive.avionicstoday.com/the-connected-aircraft/, último acesso em 02.01.2017>.

[13] Cf. DC Rainmaker, "Wahoo fitness announces GymConnect: Treadmill integration & control", *DC Rainmaker* (2016) <disponível em: https://www.dcrainmaker.com/2016/01/announces-gymconnect-integration.html, último acesso em 02.01.2017>.

[14] Por exemplo, os rótulos de garrafas do uísque "Johnnie Walker Blue Label" podem detectar quando a garrafa foi aberta e enviar notificações e mensagens interativas para o dispositivo móvel cadastrado Cf. Jennifer Hicks, "Johnnie Walker smart bottle debuts at mobile world congress", *Forbes* (02.03.2015) <disponível em: http://www.forbes.com/sites/jenniferhicks/2015/03/02/johnnie-walker-smart-bottle-debuts-at-mobile-world-congress/, último acesso em 02.01.2017>.

[15] Para uma discussão aprofundada sobre algumas delas, cf. Robert C Post, "Three concepts of privacy". *Geo. LJ* 89 (2000), 2087.

[16] Cf. Dennys Antonialli, "Watch your virtual steps: An empirical study of the use of online tracking technologies in different regulatory regimes", *Stanford Journal of Civil Rights and Civil Liberties* VIII (2012), 325-327 (comentando a associação do fenômeno à chamada "cultura da vergonha" na sociedade japonesa).

casas e carros dos cidadãos.[17] Em outros países, como o Brasil, a novidade foi recebida em tom de comemoração.[18]

Essas diferenças de percepção ilustram como a privacidade está intrinsecamente ligada a valores sociais, políticos e culturais. Isso se reflete na forma como esse direito é tutelado e regulado pelas legislações nacionais. Enquanto, na Coreia do Sul, por exemplo, a lei de proteção de dados abre caminho para que se considerem como dados pessoais até mesmo a imagem e a voz de uma pessoa, outras legislações não vão tão longe.[19]

A adoção de níveis diferentes de proteção entre os países não é algo exclusivo do direito à privacidade, mas algo que pode ser observado também em relação a outros direitos fundamentais. Cada Estado, por motivos de cunho social, cultural, histórico ou político tem a possibilidade de adotar regulamentações mais ou menos restritivas em relação ao exercício desses direitos. Por exemplo, em alguns países da Europa, como Alemanha[20] e França[21], a legislação penal restringe a liberdade de expressão ao proibir que sejam divulgados materiais que façam apologia ao nazismo ao passo que, nos Estados Unidos, não há proibição expressa nesse sentido.

Enquanto a grande maioria das condutas e relações sociais estavam adstritas a um território específico, a falta de uniformidade na regulação de direitos fundamentais era menos problemática. Os Estados tinham mais condições de identificar e punir potenciais violações uma vez que seus infratores agiam, na grande maioria dos casos, sob sua jurisdição, ou seja, dentro de seu território.

O objeto de estudo desta tese de doutorado, apresentado a seguir, se insere nesse contexto de transformação e olha para a Internet tal qual ela foi explorada e exportada comercialmente pelos Estados Unidos. Nesse sentido, contextos em que a rede se desenvolveu de forma mais endógena, como em alguns países da Ásia, por exemplo, mereceriam estudo separado.

---

[17] Cf. Dennys Antonialli, "Watch your virtual steps: An empirical study of the use of online tracking technologies in different regulatory regimes", p. 326.
[18] Cf. Danilo Amoroso, "Google Street View chega ao Brasil", *TecMundo* (2010) <disponível em: http://www.tecmundo.com.br/google-street-view/5650-google-street-view-chega-ao-brasil.htm, último acesso em 02.01.2017>.
[19] Cf. Margareth Hyun Suk Kang, *A proteção de dados pessoais e o sistema legal sul coreano*. São Paulo: dissertação de mestrado (Universidade de São Paulo), 2016.
[20] Cf. Seções 86 e 86a do Código Penal Federal alemão.
[21] Cf. Artigo R645-1 do Código Penal francês.

Nota metodológica e objeto de pesquisa: escopo, perguntas e limitações

Esta tese de doutorado pretende analisar de que forma a arquitetura da Internet impacta a tutela do direito à privacidade no âmbito dos Estados nacionais, sobretudo no que diz respeito à sua capacidade de responsabilizar atores *privados* que, mesmo sediados fora de seu território, praticam atividades de coleta e tratamento de dados dentro de suas jurisdições.

Com isso, esta tese analisará a possível interferência de atores não-estatais estrangeiros na eficácia dos níveis de proteção conferidos a direitos fundamentais pelas constituições nacionais. Isso contribuirá com o debate em torno do fenômeno do entrelaçamento de dois ou mais ordenamentos jurídicos no mundo globalizado, sobretudo no que diz respeito às teorias do constitucionalismo transnacional ou do movimento de constitucionalização global. Espera-se, dessa forma, que esta tese aproxime campos do conhecimento que parecem não estar plenamente entrosados: o das políticas públicas de Internet e o do direito constitucional, sobretudo em sua interface com os direitos fundamentais.

A escolha de se ater às formas de responsabilização de atores privados se justifica tanto pela sua imensa penetração nas relações cotidianas travadas na Internet, como o uso de redes sociais, jogos e outras aplicações quanto pela necessidade de se realizar um recorte temático que tornasse factível a realização da pesquisa. As formas de responsabilização e interferência de outros tipos de atores, como autoridades de investigação criminal, portanto, não fazem parte do objeto de análise desta tese.[22]

Isso significa dizer que esta tese parte de um referencial teórico que encara o direito à privacidade como uma espécie de poder de controle de dados pessoais, poder esse que faz frente e pode ser oponível a atores privados que realizam quaisquer operações de coleta, armazenamento, tratamento e transferência de dados pessoais. Na literatura especializada, há extenso debate a respeito do conceito preciso que pode ser atribuído a esse direito e foge ao escopo desta tese adentrar essa discussão ou propor um conceito que

[22] Essas discussões envolvem, por exemplo, questões ligadas ao acesso a dados de usuários de Internet armazenados em outros territórios para fins de investigação criminal e têm assumido diferentes e complexos contornos com o desenvolvimento de tecnologias como a criptografia de ponta a ponta. Esse debate será mencionado de forma marginal ao longo da tese, apenas quando pertinente.

nos pareceria mais adequado.[23] Também há divergências em relação à nomenclatura que deve ser dada a esse direito.[24] Para os fins desta tese, utilizar-se-ão, de forma intercambiável, os termos "privacidade" e "proteção de dados pessoais". Da mesma forma, não adotaremos uma concepção específica a respeito do conceito de "dados pessoais", que recebe tratamento diferenciado de acordo com cada legislação. Para os fins desta tese, o termo será utilizado de forma genérica e seu conceito será aquele adotado pelo modelo regulatório a que se estiver fazendo referência. Nesse sentido, esta tese adota uma perspectiva de análise dogmática.

Ao realizar a discussão proposta, esta tese levará em conta a constatação de que há uma concentração desses atores privados nos Estados Unidos, sobretudo no estado da Califórnia, onde estão sediadas não só muitas das grandes empresas do setor de Internet, como também empresas de pequeno e médio porte que, por meio da Internet, atuam de forma globalizada.[25]

Por essa razão, esta tese parte da premissa de que as vias de acesso e formas de responsabilização dos atores privados sediados nos Estados Unidos são relevantes para que outros Estados nacionais possam fazer valer os níveis de proteção de privacidade conferidos por suas constituições e legislações nacionais. Nesse sentido, esta tese explorará com profundidade o modelo regulatório de privacidade adotado nos Estados Unidos, com especial destaque para os mecanismos de responsabilização disponíveis para remediar violações a legislações de proteção de dados estrangeiras. Com isso, as características e mecanismos previstos em outros modelos regulatórios serão abordados apenas na medida em que forem necessários para o objeto desta tese, não sendo seu objetivo refletir sobre ou descrever nenhum deles em particular, nem mesmo aquele adotado no Brasil. Esta tese se foca nos impactos do modelo estadunidense para o resto do mundo e não para um país ou região em específico.

Diante do exposto, a presente tese visa a investigar as seguintes hipóteses (perguntas de pesquisa): *(i)* se e de que forma a arquitetura da Internet apresenta desafios adicionais, próprios e específicos para a tutela do direito à privacidade; *(ii)* se e de que

[23] Para uma taxonomia dos diferentes valores englobados pelo direito à privacidade aplicado a esse contexto, cf. Daniel Solove, *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.

[24] As nomenclaturas mais comuns dentre os autores estadunidenses são *information privacy*, *online privacy*, *electronic privacy* e *consumer privacy*. Entre autores de tradição europeia, a nomenclatura mais comum é aquela adotada pelas legislações nacionais, que costumam se referir a esse direito como "proteção de dados pessoais" (*data protection law*). Ficou difundido, ainda, o conceito de "autodeterminação informacional" (*informationelle Selbstbestimmung*), tal como consagrado pelo Tribunal Constitucional alemão em 1983.

[25] Dados que embasam essa hipótese são apresentados no capítulo V desta tese, acompanhados da respectiva metodologia utilizada para obtê-los.

forma o modelo regulatório de privacidade adotado nos Estados Unidos possibilita a responsabilização de atores privados sediados em seu território em relação a violações de privacidade cometidas por eles em outras jurisdições; e *(iii)* se e de que forma a interferência desses atores não-estatais gera repercussões para as capacidades de tutela do direito à privacidade no âmbito dos Estados nacionais.

Para tanto, a presente tese envolveu a revisão e análise da produção bibliográfica especializada, dos marcos normativos vigentes e a utilização de métodos de pesquisa empírica variados, que serão expostos em detalhe quando da apresentação de seus resultados (notadamente nos capítulos III e V).

Em relação à sua organização, esta tese está estruturada em cinco capítulos. No capítulo I, descreve-se como a evolução do ecossistema de publicidade na Internet incluiu e consolidou a participação de uma complexa cadeia de atores intermediários nas atividades de coleta e tratamento de dados pessoais, acrescentando novos desafios para a tutela da privacidade. Além disso, são apresentadas as características técnicas de funcionamento das tecnologias intrusivas de coleta e tratamento de dados pessoais, destacando em que medida a arquitetura da Internet favorece a sua utilização.

No capítulo II, são abordadas as principais diferenças de racionalidade regulatória por trás dos modelos adotados nos Estados Unidos e na União Europeia. Também é analisada a experiência com o arranjo *Safe Harbor*, que pretende equalizar as incompatibilidades que poderiam obstar a transferência de dados pessoais entre as duas regiões.

O capítulo III dedica-se ao estudo da atuação da Comissão Federal de Comércio dos Estados Unidos, tida como principal órgão regulador das questões ligadas à privacidade no país. Nesse capítulo, são analisadas as limitações que comprometem a possibilidade de colocá-la como principal responsável pela resolução de casos que envolvam violações de legislações estrangeiras.

No capítulo IV, são apresentadas as regras para reconhecimento e execução de ordens judiciais estrangeiras nos Estados Unidos, com especial destaque para suas limitações no que tange aos casos envolvendo o direito à privacidade. Além disso, esse capítulo explora como o argumento da jurisdição tem servido de escudo para alguns atores privados, que buscam se eximir de submissão a qualquer ordenamento jurídico estrangeiro, adicionando obstáculos para a utilização da via judicial como forma de responsabilização.

No capítulo V, as conclusões extraídas a partir dos capítulos anteriores são analisadas a partir de suas repercussões para as teorias do constitucionalismo transnacional. Além disso, são apresentadas propostas de adoção de modelos regulatórios de privacidade no plano internacional, destacando, a partir das experiências encampadas no âmbito da ONU, suas principais limitações.

CAPÍTULO 1 - A ARQUITETURA DA INTERNET E O ECOSSISTEMA DE PUBLICIDADE DIGITAL

Não parece exagerado dizer que a conectividade se tornou uma marca da vida contemporânea. De acordo com a pesquisa TIC Domicílios, realizada pelo Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (CETIC.br), no Brasil, há cerca de 94,2 milhões de usuários de Internet, 80% dos quais podem ser considerados usuários frequentes, isto é, que acessam a Internet diariamente.[26] Apesar de perdurarem as desigualdades regionais[27] e socioeconômicas[28], o número de usuários tem aumentado de forma constante nos últimos dez anos no país, o que também se observa em outros países da América Latina.[29]

O crescimento do número de pessoas conectadas aquece o mercado de produtos e serviços disponíveis na Internet, dinamiza as formas de interação entre os usuários e alimenta a rede com novos conteúdos.[30] Sendo assim, atrair novos usuários para a Internet continua sendo um objetivo compartilhado por muitos atores do setor, não só pelos benefícios que a universalização do acesso pode trazer em relação ao acesso ao conhecimento e à informação, mas também pelo aumento das oportunidades de mercado que isso representa.

---

[26] Coordenação do Ponto BR, *Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros 2014* (2015) <disponível em: http:// http://cetic.br/media/docs/publicacoes/2/TIC_Domicilios_2014_livro_eletronico.pdf, último acesso em 02.01.2017 >, p. 150.

[27] Enquanto nas regiões Norte e Nordeste o percentual de domicílios conectados à Internet é de 37% e 35%, respectivamente, na região Sudeste, esse percentual é de 60%. Cf. Coordenação do Ponto BR, *Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros 2014*, p. 141.

[28] A proporção de domicílios com acesso à Internet é de 14% na classe DE; na classe A é de 98%. Cf. Coordenação do Ponto BR, *Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros 2014*, p. 141.

[29] Cf. Coordenação do Ponto BR, *Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros 2014*, p. 149.

[30] Em um segundo, por exemplo, são postados mais de 7.000 conteúdos no Twitter, visualizados mais de 125 mil vídeos no Youtube e enviados mais de 2 milhões de emails. Cf. Stacy Liberatone, "Live map shows Google searches, Tweets and YouTube views every second", *Mail Online* (2016) <disponível em: http://www.dailymail.co.uk/sciencetech/article-3662925/What-happens-internet-second-54-907-Google-searches-7-252-tweets-125-406-YouTube-video-views-2-501-018-emails-sent.html, último acesso em 02.01.2017>.

Nesse sentido, pode-se dizer que hoje a Internet é uma realidade consolidada e há poucas dúvidas sobre as vantagens de se viver em um mundo conectado.[31] Mas nem sempre foi assim. Durante os primeiros anos depois de sua abertura comercial, em 1993, a Internet era um ambiente pouco conhecido e, de certa forma, hostil. A navegação não era intuitiva, dependia de grande familiaridade com a tecnologia e havia pouca diversidade de produtos e serviços disponíveis.[32]

Isso exigiu um esforço maior por parte daqueles que apostavam no valor comercial da Internet, que tinham o desafio de atrair novos usuários para torná-la um espaço lucrativo. Nesse contexto, a aposta de muitos desses atores foi a de despertar o interesse e a curiosidade das pessoas oferecendo produtos e serviços de forma gratuita, o que ajudaria a estimulá-las não só a vencer a hostilidade de navegação e as barreiras iniciais de acesso, como também a constituir uma massa de usuários que fariam visitas frequentes.[33]

No início, como se verá ao longo deste capítulo, ainda não pareciam existir estratégias claras de monetização por parte desses atores. A preocupação maior era ganhar escala e atrair um número significativo de usuários para a Internet com base na gratuidade. Mesmo assim, o potencial da Internet convenceu investidores e motivou novos empreendimentos, o que possibilitou o seu desenvolvimento, tornando-a um ambiente dinâmico e atrativo.

Com o crescimento rápido da Internet, veio a atenção do setor publicitário e, com isso, uma forma de viabilizar a lucratividade desses negócios sem afetar a gratuidade dos produtos e serviços oferecidos. Desde então, a venda de espaços publicitários virtuais passou a ser a base dos modelos de negócios adotados por essas empresas e, de certa forma, permanece sendo a principal estratégia de monetização desses serviços até hoje.

---

[31] Isso tem se refletido, inclusive, em propostas de se considerar o acesso à Internet como um direito fundamental, o que tem sido encampado por algumas organizações e fóruns de discussão internacionais, como a Organização das Nações Unidas. Cf. David Kravets, "U.N. report declares internet access a human right", *Wired* (2011) <disponível em: https://www.wired.com/2011/06/internet-a-human-right/, último acesso em 02.01.2017>.

[32] Embora o número de páginas disponíveis tenha começado a aumentar rapidamente, serviços como mecanismos de busca, troca de mensagens instantâneas e compartilhamento de arquivos só apareceram mais tarde. Além disso, foi só com o desenvolvimento de navegadores mais simples e intuitivos, como o Netscape, que os usuários adquiriram mais autonomia para navegar na rede.

[33] No caso do Netscape, por exemplo, para fazer frente ao Mosaic, navegador que o antecedeu, a estratégia era distribuir a versão beta de maneira gratuita para alcançar o maior número possível de usuários. A licença das versões futuras é que seriam cobradas. O mesmo aconteceu com Yahoo!, que se preocupou em aumentar a sua base fiel de usuários antes de pensar numa estratégia de monetização de seus serviços. No caso do portal AOL, a estratégia era parecida: os serviços de bate-papo, notícias e email eram todos oferecidos de maneira gratuita; a cobrança era feita com base no serviço de provimento de acesso à internet. Cf. Internet History Podcast. "Interviews", *Internet History Podcast* <disponível em: <http://www.internethistorypodcast.com>.

Acompanhando a evolução desses modelos de negócios, o desenvolvimento de tecnologias de coleta e tratamento de dados de usuários abriu caminho para formas cada vez mais sofisticadas de alocação e direcionamento de anúncios, o que alavancou preços e tornou o setor publicitário digital tão atrativo.[34]

O aumento do volume e da complexidade dessas transações fez surgir um complexo ecossistema, marcado pela presença de diferentes intermediários e pela automatização de processos de tratamento de dados e alocação de anúncios. Ao mesmo tempo, financiados pela indústria da publicidade, os produtos e serviços disponíveis na Internet se multiplicaram e se diversificaram, assumindo enorme relevância na vida dos usuários.[35] Em poucas palavras, a Internet revolucionou a indústria da publicidade e a indústria da publicidade revolucionou a Internet.

Nesse contexto, potencializaram-se as ameaças ao direito à privacidade e aprofundaram-se as críticas a modelos de negócios baseados na monetização de dados pessoais.[36] Para entender as raízes desse debate, que constitui o pano de fundo desta tese, é necessário avaliar em que medida a Internet oferece obstáculos adicionais, próprios e especiais para a tutela do direito à privacidade.

Para tanto, este capítulo pretende *(i)* analisar o histórico de evolução e apresentar as principais características do ecossistema de publicidade digital, destacando as suas relações com alguns modelos de negócios na Internet, sobretudo aqueles que envolvem o oferecimento de produtos e serviços de forma gratuita; e *(ii)* avaliar de que forma o desenvolvimento desse ecossistema contribuiu para o surgimento de tecnologias de monitoramento e coleta de dados de usuários, identificando suas principais características de funcionamento técnico e as ameaças específicas que podem representar à privacidade.

---

[34] De acordo com estudo de Howard Beales, em 2009, por exemplo, o preço de uma publicidade dirigida com base no comportamento do usuário era 2,68 vezes mais cara que uma que não fosse dirigida. Para outros dados sobre o valor que a possibilidade de direcionamento agregou ao preço da publicidade, cf. Howard Beales, "The value of behavioral targeting", *Network Advertising Initiative* (2010) <disponível em: http://www.rutadonvasco.mx/web/20130406015458/http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf, último acesso em 02.12.2017>.

[35] Vale registrar que a referência à "Internet" abrange a navegação em todas as formas de dispositivos conectados a ela, além daquela tradicional, feita em computadores. Nesse sentido, o surgimento dos smartphones e dos aplicativos desenvolvidos para eles, intensificou ainda mais a penetração e utilização da Internet para a realização de tarefas cotidianas. No Brasil, por exemplo, o celular se consolidou como o principal meio de acesso à Internet. Cf. IBGE, "Celular se consolida como o principal meio de acesso à internet no Brasil", *Agência Brasil* (2016) <disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2016-12/ibge-celular-se-consolida-como-o-principal-meio-de-acesso-internet-no-brasil, último acesso em 02.01.2017>.

[36] Para um resumo das posições e argumentos levantados nesse debate, cf. Chris Jay Hoofnagle / Ashkan Soltani / Nathan Good / *et al*. "Behavioral advertising: The offer you cannot refuse" *SSRN* (2012) <disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2137601, último acesso em 02.01.2017>.

1.1. Histórico e evolução do ecossistema de publicidade digital

A indústria publicitária movimenta o setor de Internet há mais de vinte anos. Pouco tempo depois de sua abertura para usos comerciais, em 1993[37], a Internet já começou a ser encarada como uma oportunidade de acesso a novos públicos e potenciais consumidores.[38] Naquele mesmo ano, um dos primeiros portais comerciais da rede, *Global Network Navigator*, vendeu o primeiro anúncio virtual, comprado por um escritório de advocacia do vale do silício.[39] No ano seguinte, 1994, a página da revista *HotWired* consolidou a prática, com a venda de espaços de publicidade virtual (anúncios "clicáveis", em formato de *banner)* a algumas empresas, como a operadora de telefonia estadunidense *AT&T*.[40]

Não é difícil perceber que muita coisa mudou desde os anúncios que eram exibidos nas páginas de Internet em meados dos anos 90. As telas de interface com esses conteúdos se multiplicaram e migraram para vários novos dispositivos: dos computadores para os aparelhos de celular, *tablets*, relógios de pulso, e até mesmo carros e refrigeradores. Os anúncios exibidos, por sua vez, passaram a ser mais variados, abundantes, personalizados[41], persistentes[42] e interativos.[43] Com isso, tornaram-se também mais

[37] Cf. James D. Ratliff / Daniel Rubinfeld, "Online advertising: Defining relevant markets", Journal of Competition Law and Economics 6 (2010), 653–686, p. 655. (esclarecendo que a abertura comercial da rede se deu por uma nova interpretação das políticas de uso aceitável (Acceptable Use Policy) da National Science Foundation, que até então só admitia seu uso para propósitos relacionados à pesquisa e à educação.) No Brasil, o uso comercial da Internet foi autorizado pela Portaria nº 295 do Ministério das Comunicações, de 20/08/1995.

[38] Antes de sua abertura para usos comerciais, a única forma de propaganda acontecia via *e-mail*.

[39] James D. Ratliff / Daniel Rubinfeld, "Online advertising: Defining relevant markets", p. 657.

[40] Barbara K Kaye, *Just a click away: advertising on the Internet*. Boston: Allyn and Bacon, 2001, p. 6.

[41] Conforme se explorará neste capítulo, as tecnologias de coleta e tratamento de dados pessoais possibilitam o direcionamento de anúncios com base nas preferências dos usuários. Cf. Chris Jay Hoofnagle / Ashkan Soltani / Nathan Good / *et al*. "Behavioral advertising: The offer you cannot refuse".

[42] Desde que foi desenvolvida, a técnica de redirecionamento (retargeting) permite que os usuários sejam expostos, repetidas vezes, aos mesmos produtos e serviços pelos quais de alguma maneira demonstraram interesse. Cf. Miguel Helft / Tanzina Vega, "Retargeting ads follow surfers to other sites", *The New York Times* (30.08.2010) <disponível em: http://www.nytimes.com/2010/08/30/technology/30adstalk.html, último acesso em 02.01.2017>.

[43] Um exemplo é o da campanha publicitária da companhia aérea British Airways, que usava paineis digitais com crianças apontando para as aeronaves da companhia enquanto passavam no céu, indicando número do vôo e destino. Cf. Gabriel Beltrone, "Kids point to British Airways flights as they pass overhead on magical U.K. billboards", AdWeek <disponível em: http://www.adweek.com/adfreak/kids-point-british-airways-flights-they-pass-overhead-magical-uk-billboards-154067, último acesso em 02.01.2017>. Além disso, o reconhecimento facial e a ativação de anúncios por gestos também têm sido estratégias testadas por diferentes marcas. Cf. Ann-Christine Diaz, "Facial recognition technology makes marketers a fun Big Brother", *Advertising Age* (2013) <disponível em: http://adage.com/article/news/brands-facial-recognition-campaigns/244233/, último acesso em 02.01.2017>. Cf. também Christopher Heine, "This interactive coke ad in a subway station winks and smiles when you do", *AdWeek* (2015) <disponível em:

persuasivos: em artigo para o jornal *The Atlantic*, por exemplo, a jornalista Rebecca Rosen comenta pesquisa divulgada por agência de publicidade que sugere os horários e dias da semana em que as mulheres se sentiriam mais insatisfeitas com sua aparência, recomendando que os anúncios publicitários relacionados a cosméticos e produtos de beleza sejam exibidos nesses períodos para explorar esse momento de maior vulnerabilidade.[44]

1.1.1. Compra e venda de espaços publicitários virtuais: atores e funcionamento

No caso dos primeiros anúncios comercializados pela revista *Hotwired*, as negociações foram feitas de forma direta: de um lado, a página, interessada em vender seus espaços publicitários; de outro, os anunciantes, interessados nos espaços publicitários disponíveis. Nesse modelo de contratação direta, os anunciantes precisam decidir, de antemão, em quais páginas desejam ter seus anúncios exibidos e entrar em contato individualmente com o responsável por cada uma delas.[45]

Como é de se imaginar, em pouco tempo, o volume e a complexidade dessas transações aumentou significativamente. Em 1995, cada anunciante já podia escolher entre mais de quarenta mil páginas para divulgar seus anúncios, o que tornou o modelo de contratação direta demasiadamente oneroso.[46] Nesse contexto, começou a ser importante a existência de atores intermediários, especializados em aproximar os responsáveis pelas páginas (*publishers*) de potenciais anunciantes. Os primeiros são vendedores; os segundos, compradores. Para cumprir essa tarefa, surgiram as redes de publicidade digital (*online advertising networks*), que, além de reunir os espaços de publicidade virtual disponíveis

---

http://www.adweek.com/news/technology/interactive-coke-ad-subway-station-winks-and-smiles-when-you-do-166930, último acesso em 02.01.2017>.

[44] Cf. Ann-Christine Diaz, "Facial recognition technology makes marketers a fun Big Brother".

[45] Negociados caso a caso, os contratos costumavam estabelecer preços pré-fixados com base em uma quantidade de exibições do anúncio por mês. Cf. Benjamin Edelman / Michael Ostrovsky / Michael Schwarz, "Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords", *The American Economic Review* 97 (2007), 245.

[46] É o que argumenta a empresa estadunidense *FocalLink Media Services,* que se intitula pioneira no oferecimento do serviço de intermediação dessas transações. Cf. Focal Link Press Release, 17/07/1995, Palo Alto, CA, <disponível em: http://www.zinman.com/images/FocalinkPressRelease.JPG, último acesso em 26.05.2016>.

nas diferentes páginas (*advertising inventories*), também gerenciam a sua contratação pelos anunciantes.

Assim, o surgimento dessas redes contribuiu para o aperfeiçoamento do processo de direcionamento de publicidade na medida em que elas conseguem agregar dados sobre os diversos anunciantes com os quais transacionam, como a sua audiência e público-alvo, facilitando a segmentação.

Em meados dos anos 2000, aparecem também os mercados de troca de anúncios em tempo real (*Ad Exchanges*). Tratam-se de plataformas de negociação automatizada, que congregam páginas, anunciantes e redes de publicidade digital, em um sistema que emprega sofisticados mecanismos de compra e venda de espaços publicitários baseados no conceito de leilão.

Com o passar do tempo, foram desenvolvidos também diferentes tipos de *software* para agir em nome dos vendedores e dos compradores nesses mercados: as "plataformas de fornecimento" (*supply-side platforms*) atendem aos interesses dos vendedores; as "plataformas de demanda" (*demand-side platforms*), dos compradores. A função desses *software* é maximizar o preço de venda para os primeiros e encontrar os melhores espaços publicitários dentro dos lances oferecidos pelos segundos.

Isso significa que, por trás do processo de exibição dos anúncios na Internet, existe um processo complexo, que leva em consideração não só os preços envolvidos nessas transações, como também o perfil e as características do usuário para quem o anúncio será exibido, o que torna a alocação de anúncios muito mais direcionada e personalizada.

Basicamente, o funcionamento técnico desse processo de alocação de anúncios parte da comunicação que se estabelece entre o dispositivo do usuário e os servidores responsáveis pela exibição dos conteúdos de uma determinada página. Esses conteúdos podem ser tanto aqueles oriundos da própria página, como uma notícia ou uma foto, quanto anúncios publicitários, que podem estar hospedados em outros servidores. Isso quer dizer que a exibição dos conteúdos de uma só página pode exigir a comunicação do dispositivo do usuário com mais de um servidor.

Ao acessar uma página, portanto, o dispositivo do usuário se comunica não só com o servidor do conteúdo da página, como também com os servidores responsáveis por preencher os espaços virtuais de publicidade disponíveis. As plataformas de fornecimento interagem com esses servidores e classificam o espaço virtual oferecido com base em dados que permitem traçar o perfil e preferências do usuário a quem o anúncio será

exibido. Isso determina as características daquele espaço publicitário, que é então ofertado nos mercados de troca de anúncios. É como se o espaço publicitário genérico ("anuncie aqui") fosse substituído por um mais específico ("anuncie aqui para mulheres moradoras do bairro de Moema, entre 30 e 35 anos, interessadas em moda e artigos de luxo").

Quando esses espaços publicitários são lançados nos mercados de troca de anúncios, as plataformas de demanda analisam automaticamente, e em tempo real, as suas características e determinam para quais compradores seriam mais adequados ou vantajosos, dentro também dos lances oferecidos. O comprador que for escolhido depois desse processo tem então seu anúncio exibido naquele espaço publicitário. No caso acima, por exemplo, possivelmente seria exibido um anúncio de sapatos ou de bolsas, ao invés de um sobre aulas de mandarim.

Essa classificação de relevância e valor dos espaços publicitários é possível graças à utilização de tecnologias de monitoramento e coleta de dados de usuários, cujas particularidades e funcionamento serão descritas ao longo deste capítulo. Além dessas tecnologias, vale registrar que há atores especializados em empregar outras técnicas para construir perfis e identificar preferências de grupos de usuários, como o cruzamento de dados armazenados em diferentes bancos de dados, públicos e privados.[47]

As corretoras de dados (*data brokers*) são exemplos de atores que oferecem serviços como esses para anunciantes e redes de publicidade digital. Depois de uma extensa investigação sobre as suas práticas, que costumam acontecer de forma invisível aos olhos do consumidor, a Comissão Federal do Comércio dos Estados Unidos (*Federal Trade Commission*) publicou relatório destacando três principais estratégias de atuação dessas empresas no ramo da publicidade digital.[48]

A primeira diz respeito à utilização de bases de dados de assinatura de usuários em páginas e serviços da Internet. São listas de assinantes de boletins e newsletters ou mesmo da criação de cadastros. Com base no cruzamento dessas listas, as corretoras têm a

[47] No Brasil, por exemplo, em 2013, noticiou-se um acordo entre o Tribunal Superior Eleitoral e a Serasa Experian, que possibilitaria o repasse de dados de cidadãos para a empresa. Depois de ser duramente criticado pelas implicações que representava para a privacidade dos brasileiros, o acordo foi suspenso. A empresa usaria os dados para enriquecer seus bancos de dados. Cf. Tribunal Superior Eleitoral, "Corregedoria-Geral Eleitoral suspende acordo entre TSE e Serasa", *Imprensa* (2013) <disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2013/Agosto/corregedoria-geral-eleitoral-suspende-acordo-entre-tse-e-serasa, último acesso em 02.01.2017>.

[48] Cf. Federal Trade Commission, "Data brokers: A call for transparency", *Federal Trade Commission* (2014) <disponível em https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf, último acesso em 02.01.2017>.

possibilidade de construir perfis mais apurados sobre as preferências e interesses de usuários.[49]

A segunda estratégia depende da combinação de listas de assinantes com listas de clientes fornecidas pelos próprios anunciantes. Isso permite a análise de compatibilidade entre determinadas páginas e determinado público-alvo buscado pelo anunciante. Por exemplo, se a empresa P gostaria de fazer anúncios sobre artigos para praia mas não sabe se a página da empresa V, sobre viagens, seria uma boa opção, essa análise pode ser feita pela corretora. Com base na lista de assinantes da página V e na lista de clientes da empresa P, a corretora pode determinar se há um grau suficiente de coincidência para justificar a compra de espaços publicitários na página V pela empresa P.[50]

A terceira estratégia é mais elaborada e envolve a combinação de dados disponíveis em bancos de dados *online* e *offline*, obtidos de diversas formas diferentes por essas corretoras, com a utlização de tecnologias de monitoramento e coleta de dados pelas próprias corretoras. Isso permite construir perfis bastante detalhados sobre os interesses dos consumidores já que são congregadas informações sobre suas atividades *offline*, como as lojas nas quais realizou compras ou participou de promoções, com as suas atividades de navegação *online*.[51]

Ao mesmo tempo em que o processo de compra e venda de espaços publicitários na Internet foi grandemente facilitado pelo surgimento desses intermediários e sistemas automatizados, seu aparecimento também alimentou o desenvolvimento de técnicas mais intrusivas de monitoramento dos dados e preferências dos usuários, que puderam então ser gerenciadas de forma centralizada por esses atores. Como se verá adiante neste capítulo, o "monitoramento por terceiros" (*third-party tracking*) está por trás das principais formas de direcionamento de publicidade na Internet e é uma das questões que levanta mais preocupação em relação à tutela do direito à privacidade.[52]

---

[49] À essa técnida dá-se o nome de *registration targeting*. Cf. Federal Trade Commission, "Data brokers: A call for transparency", p.26.
[50] À essa técnida dá-se o nome de *collaborative targeting*. Cf. Federal Trade Commission, "Data brokers: A call for transparency", p.27.
[51] À essa técnida dá-se o nome de *onboarding*. Federal Trade Commission, "Data brokers: A call for transparency", p.28-30.
[52] Cf. Jonathan R. Mayer / John C. Mitchell. "Third-party web tracking: Policy and technology", *IEEE* (2012): 413–427 <disponível em: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6234427, último acesso em 02.01.2017>

1.1.2. Modelos de precificação e técnicas de alocação de anúncios

À medida em que foi se sofisticando, a indústria da publicidade digital também foi aperfeiçoando as formas de precificação e de alocação de anúncios. O histórico dessa evolução permite compreender as razões pelas quais as técnicas de direcionamento da publicidade passaram a ocupar uma posição tão central para o segmento. Cada vez mais, a tarefa de identificar quais são os usuários potencialmente mais interessados em determinados anúncios se tornou o caminho para a lucratividade, o que estimulou o desenvolvimento de tecnologias de coleta e monitoramento de dados de usuários que otimizassem a alocação e direcionamento dos anúncios.

No início, o modelo de precificação da publicidade ainda replicava o modelo adotado nas mídias tradicionais e se baseava no número estimado de visualizações do anúncio. Também conhecido como *cost per impression* ("CPI")[53], o modelo equivale, na Internet, a cobrar a cada vez que ocorre a *exibição* do anúncio em uma página.[54]

Dentro dessa lógica, quanto mais visitantes uma página atrai, mais rentável ela se torna pois mais vezes os anúncios são exibidos. Isso começou a justificar o oferecimento gratuito de conteúdo por parte dessas páginas, que tinham então um incentivo econômico não só para atrair o maior número possível de visitantes, por meio da publicação de conteúdos que despertassem o seu interesse e curiosidade, como também para mantê-los na página o maior tempo possível, navegando por diferentes seções e, consequentemente, visualizando outros anúncios.

Naquela época, entretanto, atrair visitantes também não era uma tarefa fácil. Além de pouco explorada, a Internet ainda era um ambiente hostil à grande maioria das pessoas e navegar exigia um certo conhecimento técnico e familiaridade com o funcionamento da rede. Estavam ainda surgindo os primeiros navegadores comerciais e era difícil encontrar páginas novas na ausência de mecanismos eficientes de busca. Somava-se a isso o fato de que o número de páginas disponíveis não era grande e nem muito variado, o que tinha pouco apelo para conquistar o público em geral.

---

[53] Uma medida comumente adotada é o *cost per mille*, que, para diminuir a grandeza dos números, usa como unidade o total de um mil visualizações do anúncio.

[54] Vale lembrar que em uma visita a uma página, o usuário pode se deparar com vários anúncios. Isso faz que uma visita possa representar mais de uma exibição. Além disso, costuma-se adotar mecanismos para excluir da contagem possíveis vícios como a re-exibição do anúncio por conta de uma atualização da página.

Mas a aposta no potencial da Internet motivou o surgimento de ferramentas que a tornaram mais atrativa. Em dezembro de 1994, foi lançada a primeira versão do Netscape, que prometia tornar a navegação uma tarefa mais acessível e dinâmica.[55]

Além disso, com a multiplicação do número de páginas de Internet, para auxiliar o processo de localização de endereços e navegação, começaram a surgir também os primeiros mecanismos de busca.[56] As estratégias de monetização desses serviços não pareciam estar claras desde o início. Em relatos sobre o nascimento da empresa Yahoo!, por exemplo, o que se percebe é uma preocupação maior com manter uma base atualizada e abrangente de endereços de páginas para conquistar uma base fiel de usuários do que com a lucratividade do negócio propriamente. Nascida de um projeto despretensioso de dois alunos da Universidade de Stanford, a empresa não apostava na cobrança dos usuários pelo uso da ferramenta, o que fez com que a venda de publicidade como modelo de negócios fosse uma boa alternativa.[57] O mesmo parece ter acontecido com os outros buscadores, que também se fiaram ao mesmo modelo.[58]

Inicialmente, essas empresas também passaram a monetizar seus espaços de publicidade virtual com base no modelo *cost per impression*.[59] Contudo, o modelo não se adaptava perfeitamente ao conceito dos buscadores que, se de um lado procuravam maneiras de agilizar e aperfeiçoar o processo de busca, de outro, precisavam desenvolver estratégias para maximizar o número de visualizações de anúncios por usuários, o que poderia envolver mantê-los navegando na página por mais tempo.

Com isso, em 1998, o então buscador *GoTo*[60] introduziu um modelo alternativo de precificação, baseado no número de cliques recebidos por anúncio.[61] Ao contrário do modelo CPI, no *cost per click (CPC),* não importa a quantidade de exibições, mas a quantidade de visitas efetivas que a página do anunciante recebe, o que se mede pelo

---

[55] Cf. David Schedden, "Today in media history: The first commercial web browser, netscape navigator, is released in 1994", *Poynter* (2014) <disponível em: https://www.poynter.org/2014/today-in-media-history-the-first-commercial-web-browser-netscape-navigator-is-released-in-1994/274065/, último acesso em 02.01.2017>.

[56] Cf. James D. Ratliff / Daniel Rubinfeld. "Online advertising: Defining relevant markets", p. 656 (comentando como os usuários dependiam, antes disso, de recomendações individuais e de listas para descobrir endereços de novas páginas).

[57] Cf. Internet History Podcast. "Interviews".

[58] Cf. Internet History Podcast. "Interviews".

[59] Cf. David S. Evans, "The online advertising industry: Economics, evolution, and privacy", *The Journal of Economic Perspectives* 23 (2009), p. 39. Cf. também James D. Ratliff / Daniel Rubinfeld. "Online advertising: Defining relevant markets", p. 657.

[60] A empresa foi posteriormente adquirida pela Overture que, por sua vez, foi adquirida pela Yahoo!. Cf. Stefanie Olsen, "Yahoo to buy Overture for $1.63 billion", *CNET* (2003) <disponível em: https://www.cnet.com/news/yahoo-to-buy-overture-for-1-63-billion/, último acesso em 02.01.2017>.

[61] James D. Ratliff / Daniel Rubinfeld. "Online advertising: Defining relevant markets", p. 657.

número de cliques. Sendo assim, identificar quais anúncios seriam mais atrativos para cada usuário significava aumentar as chances de cliques, isto é, as chances de lucro.

Além disso, a empresa foi a responsável por introduzir o sistema de alocação de anúncios com base no mecanismo de leilões, que eram realizados a partir de palavras-chave.[62] Basicamente, cada anunciante poderia propor um valor (lance) para a exibição de um determinado anúncio associado a uma palavra-chave (termo). A cada busca realizada pelo referido termo, o buscador considerava o lance do anunciante em comparação com os lances de outros anunciantes associados à mesma palavra-chave, como em um sistema tradicional de leilão. Os resultados de busca patrocinados (anúncios) eram então exibidos em ordem decrescente, ficando, no topo, o anúncio associado ao lance de maior valor e assim sucessivamente. Os anunciantes cujos anúncios recebessem cliques pagavam os valores com os quais haviam se comprometido (lance).[63]

Mais tarde, em 2002, o mecanismo de leilão com base em palavra-chave foi aprimorado pela Google. Em sua primeira versão, o *Google Adwords Select* introduziu as seguintes mudanças principais: *(i)* a ordem dos resultados de busca não era determinada somente pelos valores das propostas, mas também pelo índice de cliques que os anúncios recebiam em relação à quantidade de vezes em que eram exibidos, isto é, anúncios que tinham uma taxa maior de engajamento por parte dos usuários; e *(ii)* os anunciantes não pagavam mais o valor original da proposta, mas sim um centavo a mais do que a proposta imediatamente inferior.

Em 2003, Google anunciou o lançamento do programa *AdSense,* com o objetivo de estender seu serviço de alocação de anúncios para outras páginas de Internet. Em vez de alocar anúncios apenas entre os resultados de busca na sua página, o Google agora poderia ser responsável pela alocação de anúncios nos espaços de publicidade das páginas visitadas. Para isso, o mecanismo de alocação desses anúncios levaria em conta características do *contexto* da página: a partir do momento em que tinha que indexar as páginas para exibi-las como resultados de busca, a empresa também tinha boas condições de identificar que tipos de anúncios seriam mais adequados ao seu contexto. Por exemplo,

[62] Cf. Benjamin Edelman / Michael Ostrovsky / Michael Schwarz. "Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords", p. 245-246.
[63] Cf. Benjamin Edelman / Michael Ostrovsky / Michael Schwarz. "Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords", p. 246. Cf. também James D. Ratliff / Daniel Rubinfeld. "Online advertising: Defining relevant markets", p. 657.

ao catalogar uma página sobre sapatos femininos, anúncios relacionados ao assunto seriam os mais apropriados.[64]

A consolidação do modelo de precificação por cliques não veio acompanhada do aprimoramento desses sistemas de alocação de publicidade por acaso. Quanto melhor alocados, maior a possibilidade de os anúncios serem relevantes para os usuários, o que aumentava as chances de clique, isto é, de lucro.

Esse raciocínio ilustra a importância das estratégias de alocação de anúncios, sobretudo dentro do modelo de precificação de custo por clique. Desde 1995, as redes de publicidade digital, como a Focal Link, já investiam no desenvolvimento de ferramentas tecnológicas capazes de aprimorar essa tarefa (*advertising serving technologies*). O objetivo principal era criar um sistema automatizado de alocação de anúncios que fosse capaz de potencializar essas chances de sucesso.

As primeiras técnicas de alocação de anúncios levavam em conta informações como horário de acesso, tipo de dispositivo e sistema operacional, endereço de origem e nome do domínio visitado.[65] Embora essas informações poderiam dar pistas em relação aos interesses dos usuários, não era possível traçar um perfil completo ou detalhado sobre seu comportamento. Por exemplo, se um usuário estava visitando o endereço "www.petlovers.com", era razoável supor que essa página seria um bom local para fazer anúncios relacionados a animais de estimação, mas não era possível extrair inferências sobre essas preferências com base em elementos comportamentais do usuário, como passou a ser possível com o desenvolvimento das tecnologias de coleta e monitoramento de dados de usuários.

Essas técnicas também poderiam levar em consideração outros fatores, como o público-alvo da página (que poderia ajudar a identificar quais características demográficas eram as mais apropriadas para o direcionamento) ou a localização do usuário (a partir do código postal inserido em um cadastro ou do endereço IP do usuário por exemplo). O conteúdo da página, indexado pelos buscadores, também dava pistas a respeito de seu público-alvo e potenciais grupos perante os quais os anúncios poderiam ser mais relevantes.

---

[64] Cf. Google, "Google builds world's largest advertising and search monetization program", *Press release* (2003) <disponível em http://googlepress.blogspot.com/2003/03/google-builds-worlds-largest.html, último acesso em 02.01.2017>.

[65] Era o que anunciava a Focal Link em 1995.

Nesses casos, a alocação de anúncios era feita com base em elementos contextuais e não comportamentais. A incorporação de elementos comportamentais ao processo de alocação de anúncios foi possibilitada, de um lado, pelo desenvolvimento de tecnologias de coleta de dados de usuários e, de outro, pelo aparecimento da figura dos intermediários no processo de compra e venda de anúncios publicitários. Ao centralizar esse processo, os intermediários passaram a ter condições de coletar e agregar informações de diferentes fontes sobre os usuários, como se demonstrará neste capítulo.

Nesse contexto, em 2009, a Google anunciou que passaria a utilizar o histórico de navegação do usuário como parte do seu mecanismo de alocação de anúncios. Antes disso, a empresa dizia levar em conta apenas as palavras-chave escolhidas pelo anunciante, o conteúdo da página catalogada e o índice de cliques do anúncio. [66]

Pouco tempo depois, a Google introduziu também sua estratégia de redirecionamento de publicidade (*retargeting*), a partir da qual poderia alocar anúncios iguais ou semelhantes àqueles previamente consultados pelo usuário. Como a Google gerencia espaços publicitários em muitas páginas da Internet (ela também opera como uma rede de publicidade digital), isso gera a sensação de que determinados anúncios estão "perseguindo" o usuário.[67]

Especialmente dentro de um modelo de precificação por custo por clique, interessa não só anunciante, como também à página, que o usuário tenha interesse nos anúncios exibidos. Nesse sentido, aumentar as chances de clique significa também aumentar as chances de lucro. Por essa razão, paralelamente ao desenvolvimento desses modelos de precificação e alocação de publicidade digital, foram sendo desenvolvidas ferramentas que possibilitavam a identificação e personalização dos anúncios exibidos com base em dados coletados.

1.2. A arquitetura da Internet e a coleta de dados pessoais

[66] Cf. Susan Wojcicki, "Making ads more interesting" *The Official Google Blog* (2009) <disponível em http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html, último acesso em 02.01.2016>.
[67] Para mais detalhes sobre o funcionamento do mecanismo e o anúncio, cf. Erick Schonfeld, "Google ads will now follow you across the web", *TechCrunch* (2010) <disponível em: http://social.techcrunch.com/2010/03/25/google-ads-follow/, último acesso em 02.01.2017>. Cf. também Miguel Helft / Tanzina Vega. "Retargeting ads follow surfers to other sites".

De maneira geral, pode-se dizer que existem dois tipos de informações às quais os responsáveis por aplicações de Internet podem ter acesso: *(i)* informações *ativamente* fornecidas por usuários, como aquelas preenchidas em cadastros e na criação de perfis; e *(ii)* informações *passivamente* fornecidas por usuários, isto é, ativamente coletadas por meio de ferramentas tecnológicas, com ou sem o seu consentimento.

Quando começaram a surgir as primeiras páginas comerciais e desenvolvidos os primeiros navegadores, o conceito de coleta de dados de usuários ainda era pouco explorado. Isso fazia com que não fosse possível distinguir, por exemplo, entre usuários que estavam retornando a determinado endereço e aqueles que o estavam visitando pela primeira vez. Esse tipo de identificação é essencial para viabilizar muitas das facilidades que foram incorporadas à experiência de navegação do usuário, como o armazenamento de preferências de exibição de páginas ou a possibilidade de manter adicionados itens a carrinhos de compras virtuais.

Na verdade, implementar quaisquer dessas facilidades dependia, de certa forma, de encontrar uma maneira de criar uma espécie de memória para as páginas de Internet, memória essa que fosse capaz de reconhecer dispositivos e associá-los com registros e preferências. [68] Como se descreverá a seguir, as tecnologias de monitoramento e coleta de dados partem todas de um mesmo objetivo comum: identificar dispositivos e armazenar dados sobre eles que possam ser acessados em visitas futuras.

Invariavelmente, a capacidade de identificação dos dispositivos abriu caminho tanto para a coleta maciça de dados a seu respeito quanto para o monitoramento de suas atividades de maneira mais extensiva. A partir disso, ao longo dos anos, o uso dessas tecnologias tornou possível o aperfeiçoamento das técnicas de direcionamento da publicidade, que passou a utilizar dados sobre o comportamento do usuário para identificar interesses e fazer previsões.[69]

1.2.1. Tecnologias intrusivas

[68] John Schwartz, "Giving the web a memory cost its users privacy", *New York Times* (04.09.2001) <disponível em: http://www.nytimes.com/2001/09/04/technology/04COOK.html?pagewanted=1, último acesso em 02.01.2017>.
[69] Cf. Chris Hoofnagle / Ashkan Soltani / Nathan Good / *et al*. "Behavioral advertising: The offer you cannot refuse".

O uso dessas tecnologias desperta a preocupação de estudiosos já há bastante tempo. Referindo-se a esses mecanismos que possibilitam atividades de monitoramento e coleta de dados pessoais, em 2000, Michael Froomkin utilizou a expressão "tecnologias destrutivas da privacidade", que, segundo ele, estariam promovendo o maior assalto à privacidade da história.[70] Esta tese dividirá esses mecanismos em dois grupos: *(i)* tecnologias intrusivas; e *(ii)* tecnologias protetivas.

Para identificar de que forma a utilização desses mecanismos torna a Internet um ambiente diferente no que diz respeito às ameaças à tutela do direito à privacidade, é importante analisar o histórico de sua evolução e as suas principais características de funcionamento técnico.

1.2.1.1. *Cookies*

Um dos primeiros e mais conhecidos mecanismos de coleta de dados de usuários de Internet são os *HTTP cookies*[71]. Inicialmente desenvolvidos por Lou Montulli em 1994, os *cookies* foram idealizados justamente com o objetivo de tornar possível que os visitantes de uma página fossem identificados em visitas futuras.[72] Dessa forma, era possível, por exemplo, armazenar itens em cestas de compras virtuais ou salvar as preferências de exibição da página, como imagem de fundo e tipo de fonte. Antes disso, a cada nova visita, era necessário adicionar todos os itens novamente ou reconfigurar essas preferências pois era como se o usuário sempre estivesse visitando a página pela primeira vez.

Para desempenhar tal função, foi preciso criar um mecanismo de identificação dos visitantes. Basicamente, é isso que os *cookies* são: identificadores. Do ponto de vista técnico, *cookies* são pequenos arquivos de texto enviados ao dispositivo do usuário e que

[70] Michael Frommkin, "The Death of Privacy?", p. 1465.
[71] HTTP, sigla que, em português, corresponde a Protocolo de Transferência de Hipertexto, é um protocolo de comunicação desenvolvido para a troca ou transferência de textos estruturados que usam ligações lógicas (hiperlinks) na World Wide Web (WWW).
[72] Cf. John Schwartz, "Giving the web a memory cost its users privacy". Cf. Lou Montulli, "The reasoning behind Web Cookies" *The irregular musings of Lou Montulli* (2013) <disponível em: http://www.montulli-blog.com/2013/05/the-reasoning-behind-web-cookies.html, último acesso em 02.01.2017>.

podem ser salvos de maneira temporária ou permanente.[73] A cada pedido de exibição de um endereço de Internet, estabelece-se uma comunicação entre o dispositivo do usuário e o servidor responsável pelo conteúdo a ser exibido. Os *cookies* podem ser enviados ao dispositivo do usuário em resposta a essa comunicação, em conjunto com os demais conteúdos necessários para a exibição da página.[74]

Uma vez salvo no dispositivo, o *cookie* atribui um código de identificação ao dispositivo (ID) e pode armazenar informações sobre atividades e preferências do usuário, informações essas que poderão ser acessadas pelo servidor da página em uma próxima visita. Na exata medida em que permitem associar um determinado dispositivo com um conjunto de atividades, o uso de cookies tem gerado preocupações relacionadas à privacidade dos usuários praticamente desde a sua criação.[75]

Desenvolvidos em conjunto com o navegador Netscape, os *HTTP cookies* foram incorporados aos padrões de praticamente todos os futuros navegadores que surgiram. Por sua utilidade e relevância, sobretudo do ponto de vista da capacidade de monetização dos dados armazenados a respeito do usuário, os *HTTP cookies* se tornaram uma ferramenta largamente utilizada.[76]

1.2.1.1.1. *Cookies* de terceiros

Como dito, os *HTTP cookies* foram criados para identificar os dispositivos por cada uma das páginas exibidas. Nesse sentido, Lou Montulli acreditava ter minimizado a possibilidade de monitoramento dos hábitos de navegação dos usuários já que cada página

[73] Cf. Oppenheimer, Max Stul. "Internet cookies: When is permission consent", *Neb. L. Rev* 85 (2006), 383, p. 688. (esclarecendo que os cookies podem ser, permanentemente, salvos no disco rígido do dispositivo do usuário ou na sua memória temporária, que será apagada quando reiniciada a sessão de navegação, por exemplo.)

[74] Oppenheimer, Max Stul. "Internet cookies: When is permission consent", p. 687.

[75] Lou Montulli destaca que, já em 1994, antes da criação dos cookies, circulavam outras propostas que, na sua visão, representavam perigo maior à privacidade dos usuários na medida em que facilitavam o monitoramento dos seus hábitos de navegação. Uma delas, por exemplo, era atribuir um identificador único ao dispositivo do usuário por meio do navegador. Por outro lado, Lou Montulli também reconhece que, depois de sua criação, os *HTTP cookies* acabaram servindo à essa finalidade de monitoramento, o que não foi antecipado por ele. Cf. Lou Montulli, "The reasoning behind Web Cookies".

[76] Pesquisa realizada em 2009 já indicava que todos os 100 sites mais visitados no mundo utilizavam *cookies* para a coleta de dados pessoais, por exemplo. Cf. Ashkan Soltani *et al*. "Flash cookies and privacy" *SSRN* (2009) <disponível em http://ssrn.com/abstract=1446862, último acesso em 02.01.2017>.

deveria enviar seu próprio *cookie* ao visitante. Uma página não teria acesso às informações armazenadas pelo *cookie* de outra pois os identificadores utilizados seriam diferentes.

Com o surgimento das tecnologias de alocação de publicidade, entretanto, a exibição dos anúncios deixou de ser administrada pelo responsável de cada página. Isso significa que, ao visitar uma página na Internet, o dispositivo do usuário estabelece comunicação não só com os servidores da página, como também com os servidores das redes de publicidade digital (uma vez que virão desses servidores os anúncios que serão exibidos). Por exemplo, ao visitar um portal de notícias, além das notícias produzidas pelo portal, podem ser exibidos vários *banners* e anúncios, que são enviados ao dispositivo do usuário pelos servidores dos anunciantes, isto é, por terceiros.

Esses terceiros também podem enviar *HTTP cookies*, juntamente com os conteúdos que irão exibir. Isso faz com que, em uma só visita, o usuário possa receber vários *cookies*. O envio desses *cookies* por parte de terceiros faz com que o dispositivo do usuário também se torne identificável em relação a eles, que poderão reconhecê-lo em visitas futuras não só àquela página na qual o anúncio foi exibido, mas a todas as páginas nas quais detiver espaços publicitários.

Isso coloca as redes de publicidade digital e grandes anunciantes em uma posição privilegiada na medida em que detêm espaços publicitários espalhados por inúmeras páginas da Internet. Podendo reconhecer o dispositivo do usuário em visitas a essas várias páginas, esses terceiros podem identificar os hábitos de navegação do usuário, traçando um perfil mais completo sobre seus interesses e preferências.

Considerando que o mercado de publicidade digital começou e continua sendo concentrado, o poder de monitoramento desses terceiros aumenta consideravelmente dada sua presença em milhares de páginas na Internet. A Google, que também atua como rede de publicidade digital, por exemplo, detém a liderança isolada com mais de 80% da fatia desse mercado.[77]

O monitoramento dos hábitos de navegação de usuários pela utilização de *cookies* de terceiros gera sérias repercussões para o direito à privacidade na Internet, tendo sido objeto de inúmeros estudos e artigos científicos.[78]

---

[77] Em 2014, sua fatia de mercado foi estimada em 85%. Cf. "Usage of advertising networks for websites, web technology surveys" <disponível em https://w3techs.com/technologies/overview/advertising/all, último acesso em 17.07.2016>.

[78] Para um resumo dos argumentos envolvendo a utilização desses mecanismos, cf. Chris Hoofnagle / Ashkan Soltani / Nathan Good / *et al*. "Behavioral advertising: The offer you cannot refuse".

1.2.1.2. *Flash Cookies*

Assim como os *HTTP cookies*, *Flash Cookies* também podem identificar o dispositivo do usuário para reconhecê-lo em visitas futuras e armazenar informações sobre suas atividades e preferências. Do ponto de vista técnico, são arquivos desenvolvidos pela empresa *Adobe* no ano 2000 e incorporados à versão 6 da extensão *Flash,* utilizada para a exibição de muitos conteúdos multimídia na rede, como vídeos, com a intenção de manter armazenadas preferências do usuário a respeito de suas preferências, como os ajustes de volume para vídeos.[79] Por partirem do mesmo princípio, qual seja o de atribuir um código identificador ao dispositivo do usuário, os *Flash cookies* também geram preocupações em relação à privacidade.

Flash cookies são considerados mecanismos mais invasivos do que *HTTP cookies* por algumas características principais: *(i)* sua capacidade de armazenamento é maior: enquanto *HTTP cookies* costumam ter uma capacidade de armazenamento de 4KB, a dos flash cookies costuma ser de 100KB; *(ii)* ficam armazenados no dispositivo do usuário por padrão, ao invés de serem apagados quando a sessão de navegação é encerrada, como a maioria dos *HTTP cookies*; *(iii)* são acessíveis por quaisquer navegadores, ao contrário dos *HTTP cookies*, que respondem apenas a um navegador específico.

1.2.1.3. *Browser fingerprinting*

Cada navegador contém uma série de informações sobre o dispositivo do usuário: fontes e extensões instaladas, configurações de fuso horário e idioma, sistema operacional, versão do sistema operacional, etc. Por mais genéricas que possam parecer isoladas, essas informações, se combinadas, podem ser usadas para gerar uma espécie de "impressão digital" do navegador do usuário. Em estudo realizado pela *Electronic Frontier*

[79] Chris Hoofnagle / Ashkan Soltani / Nathan Good / *et al*. "Behavioral advertising: The offer you cannot refuse", p. 282–283.

Foundation, a combinação de características como essas foi suficiente para gerar uma impressão digital única em aproximadamente 85% dos navegadores analisados.[80]

Por meio de mecanismos e algoritmos que coletam, identificam e categorizam essas informações, é possível usar essas impressões digitais como identificadores, tal como acontece com *HTTP cookies*. Isso faz com que essas impressões digitais possam ser uma alternativa ao uso de *HTTP cookies* para monitoramento das atividades e preferências do usuário.[81]

1.2.1.4. HTML5

HTML5 é uma linguagem de programação que facilitou a estruturação de páginas, especialmente aquelas destinadas à exibição em dispositivos móveis. Com a linguagem, surgiu também um mecanismo de armazenamento local de dados de navegação (*HTML5 local storage*). Com características similares aos HTTP e *Flash cookies*, o mecanismo se diferencia sobretudo por sua capacidade superior de armazenamento (até 5MB). Por padrão, o mecanismo também é persistente, não sendo deletado automaticamente com o fim da sessão de navegação. Além disso, seu funcionamento independe da instalação de extensões específicas, como é o caso dos *Flash cookies*.[82]

1.2.1.5. ETAGs

Durante a comunicação entre o dispositivo do usuário e o servidor da página a ser exibida, são trocadas informações que permitem avaliar se os conteúdos da página já foram

[80] Cf. Peter Eckersley, "How unique is your web browser?", in Mikhail J. Atallah / Nicholas J. Hopper (orgs.) *Privacy Enhancing Technologies*. Berlin: Springer, 2010: 1–18, p. 2.
[81] É o que defende David Norris, diretor executivo da BlueCava, uma empresa dedicada ao desenvolvimento de mecanismos de identificação de dispositivos por meio de impressões digitais. Em 2010, a empresa dizia já ter reunido 200 milhões de impressões digitais únicas de navegadores. Cf. Julia Angwin / Jennifer Valentino-Devries. "Race is on to "fingerprint" phones, PCs", *Wall Street Journal* (30.11.2010) <disponível em: http://www.wsj.com/articles/SB10001424052748704679204575646704100959546, último acesso em 02.01.2017>.
[82] Chris Hoofnagle / Ashkan Soltani / Nathan Good / *et al*. "Behavioral advertising: The offer you cannot refuse", p. 284.

previamente exibidos e, em caso positivo, se sofreram modificações desde então. Esse processo torna possível que conteúdos inalterados de páginas já visitadas sejam carregados de forma mais rápida, a partir de cópias armazenadas na memória de navegação temporária do dispositivo (*cache*).

Por isso, ao acessar uma página, o navegador costuma armazenar uma cópia de seus conteúdos na memória temporária do dispositivo do usuário. Em uma visita futura, estabelece-se então um processo de verificação dos conteúdos da página: os que sofreram modificações são atualizados e carregados diretamente do servidor; os que não sofreram são exibidos a partir das cópias previamente armazenadas. Isso acelera o processo de navegação e economiza banda para os casos em que o conteúdo da página permanece idêntico.[83]

Esse processo de verificação é feito por meio da atribuição de valores únicos aos conteúdos exibidos no momento da visita à página (*Etag*). O valor de *Etag* corresponde, portanto, a cada conteúdo exibido (como uma imagem) e é calculado com base em fatores que se alteram de acordo com o conteúdo.[84] Dessa forma, se o conteúdo da página for modificado, o mesmo acontecerá com o valor de *Etag*. Quando um dispositivo solicita a reexibição de uma página, esses valores são comparados e, no caso dos valores idênticos, os conteúdos previamente armazenados são exibidos (já que não houve alteração).

Esses valores de *Etag* podem ser utilizados para identificar o dispositivo para fins de monitoramento dos hábitos de navegação. O emprego dessa técnica é difícil de ser evitada pelo usuário pois demandaria que fosse sempre deletada a memória temporária.[85]

1.2.2. Tecnologias protetivas

[83] Matthew Davis, "ETags allow tracking without cookies", *Future Hosting* (2014) <disponível em: https://www.futurehosting.com/blog/etags-allow-tracking-without-cookies/, último acesso em 02.01.2017>.
[84] Esses fatores são chamados de atributos de MBO rowstamp. Para maiores detalhes, cf. IBM. "Armazenamento em Cache de Solicitações GET", *IBM Knowledge Center* <disponível em: http://www.ibm.com/support/knowledgecenter/pt-br/SSFGJ4_7.6.0/com.ibm.mif.doc/gp_intfrmwk/rest_api/c_rest_get_caching.html, último acesso em 02.01.2017>.
[85] Cf. Mika Ayenson / Dietrich James Wambach / Ashkan Soltani / et al. "Flash cookies and privacy II: Now with HTML5 and ETag respawning", *SSRN* (2011) <disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390, último acesso em 02.01.2017>.

Se, de um lado, a tecnologia pode ser usada para monitorar e coletar dados dos usuários, como exemplificou-se acima, de outro, surgiram respostas, também tecnológicas, para aumentar o grau de proteção da privacidade. Focando-se em prevenir, evitar ou minimizar os efeitos colaterais do uso das tecnologias intrusivas, membros da comunidade técnica também se engajaram no desenvolvimento de tecnologias protetivas.

A ideia de usar a tecnologia como forma de tutela da privacidade dos usuários também ganhou apoio de membros da comunidade acadêmica. Lawrence Lessig, ao destacar a possibilidade de regulação por meio da arquitetura da Internet, defendeu a adoção de mecanismos embutidos no navegador do usuário que fossem capazes de sinalizar suas preferências em relação à coleta de dados e monitoramento, estabelecendo um processo automatizado de negociação entre dispositivos.[86] Em 1999, Tim Berners-Lee defendeu proposta no mesmo sentido.[87]

Antes disso, em 1995, já se discutia a ideia de que o desenvolvimento de qualquer tecnologia deveria incorporar, desde a sua concepção, elementos que protegessem a privacidade dos usuários, seja no seu desenho, forma de operação ou configurações padrão, conceito esse que, mais tarde, foi chamado de "privacidade pela arquitetura" por Ann Cavoukian (*privacy by design*).[88]

Além do engajamento da academia e da comunidade técnica, a crescente preocupação com o uso das tecnologias intrusivas despertou a atenção de reguladores, que passaram a pressionar o setor publicitário para oferecer mecanismos de escolha aos usuários. Como se verá a seguir, muitos desses mecanismos apostaram na criação de respostas meramente tecnológicas, isto é, se resumiram a oferecer aos usuários a possibilidade de utilizar tecnologias protetivas para se defender das intrusivas, sem estarem acompanhadas de instrumentos de política pública ou de responsabilização jurídica.

Analisar o funcionamento básico dessas tecnologias permite identificar suas principais limitações e identificar as razões pelas quais essa abordagem pode não ser suficiente para extinguir as ameaças à privacidade.

---

[86] Cf. Lawrence Lessig, *Code: version 2.0* (2006) <disponível em: http://codev2.cc/download+remix/, último acesso em 02.01.2017>, p. 228-230.
[87] Cf. Tim Berners-Lee, *Weaving the web: the original design and ultimate destiny of the world wide web by its inventor*. São Francisco: Harper Collins, 1999, p.147.
[88] Cf. Ann Cavoukian, "Privacy by design", *Info & Privacy Comml* (2009) <disponível em http://www.ipc.on.ca/images/resources/privacybydesign.pdf, último acesso em 02.01.2017>.

1.2.2.1. *Opt-out cookies*

Uma das primeiras soluções tecnológicas foi introduzida pelo próprio setor publicitário. Na realidade, a ideia era usar *HTTP cookies* que, ao invés de identificar e armazenar dados sobre as atividades e preferências do usuário, pudessem sinalizar que aquele dispositivo não desejava ser alvo de publicidade direcionada. É como se funcionassem como um aviso indicando a preferência do usuário em não receber publicidade daquele tipo.[89]

Por sua própria natureza técnica, os chamados *opt-out cookies* são específicos, isto é, só são legíveis pela página ou servidor que os criou. Isso significa que não era possível desenvolver um *opt-out cookie* genérico, que emitisse o aviso a todas as redes de publicidade digital de uma só vez. Para cada uma delas, era necessário criar um *opt-out cookie* diferente e disponibilizá-lo ao usuário que, então, poderia instalá-lo em seu dispositivo. Isso dificultava muito a implementação dessa solução porque obrigava o usuário a pesquisar, instalar e manter atualizados os *opt-out cookies* referentes a todas as redes de publicidade digital.

Na tentativa de facilitar essa tarefa, duas entidades que promoviam parâmetros de auto-regulação e boas práticas no setor da publicidade digital, a *Network Advertising Initiative* (NAI) e a *Digital Advertising Alliance* (DAA), elaboraram listas com os *opt-out cookies* referentes a cada rede de publicidade digital interessada.

Ainda assim, a adoção do mecanismo apresentava outras dificuldades: ao deletar os *HTTP cookies* instalados em seu dispositivo, por exempo, o usuário, automaticamente, acabava deletando também os *opt-out cookies* instalados. Para evitar o problema, era necessário um conhecimento técnico significativo, incomum à maioria dos usuários de Internet.

[89] Jonathan Mayer chama a atenção para o fato de que embora os opt-out cookies pareçam prevenir o monitoramento e coleta de dados do usuário, na verdade, o que previnem é meramente a exibição de publicidade direcionada. Em estudo conduzido no *Stanford Security Lab*, metade das páginas testadas continuava enviando *HTTP cookies* para monitorar as atividades do usuário a despeito de o *opt-out* cookie estar instalado. Cf. Jonathan Mayer, "Tracking the trackers: Early results", *Center for Internet and Society at Stanford Law School* (2011) <disponível em: http://cyberlaw.stanford.edu/blog/2011/07/tracking-trackers-early-results, último acesso em 02.01.2017>.

1.2.2.2. *Do Not Track*

A proposta de um mecanismo unificado com a função de evitar o monitoramento das atividades de navegação do usuário para fins de publicidade ("Do Not Track") começou a ser encampada por organizações da sociedade civil dos Estados Unidos em 2007, ano no qual encaminharam à *Federal Trade Commission* um documento apresentando suas justificativas para a medida.[90]

O mecanismo foi inspirado no "Do Not Call Registry", um banco de dados centralizado com números de telefones nos Estados Unidos que não desejavam receber ligações com ofertas e propagandas. Antes da regulamentação de *telemarketing* no país, anunciantes podiam fazer ligações livremente.[91] Com a criação do "Do Not Call Registry", ficou mais fácil evitar as ligações; bastava se cadastrar no sistema.

O modelo proposto no "Do Not Track" envolve um elemento tecnológico e um elemento normativo.[92] Do ponto de vista tecnológico, o mecanismo funciona a partir de um cabeçalho do protocolo HTTP que sinaliza a opção do usuário em não ser monitorado. Tal como os *opt-out cookies*, o cabeçalho "Do Not Track" também funciona como um aviso. A diferença é que, como se trata de um cabeçalho, ele vale para todas as páginas e redes de publicidade digital ao mesmo tempo, além de não ser deletado automaticamente junto com os *HTTP cookies*.

Do ponto de vista normativo, propunha-se a adoção de uma norma que tornasse obrigatório respeitar a opção do usuário em não ser monitorado, estabelecendo-se, inclusive, uma sanção para as páginas que desconsiderassem o cabeçalho "Do Not Track". Sem esse elemento, não é possível exigir o cumprimento da determinação do cabeçalho "Do Not Track", que dependeria de um comportamento voluntário por parte das empresas.

Embora o elemento normativo nunca tenha sido completamente alcançado, a proposta do cabeçalho "Do Not Track" ganhou o apoio da *Federal Trade Commission*, que recomendou a sua adoção aos atores do setor privado.[93] Em 2012, a *Digital Advertising*

---

[90] Cf. CDT, documento disponível em https://www.cdt.org/files/privacy/20071031consumerprotectionsbehavioral.pdf

[91] Chris Hoofnagle / Ashkan Soltani / Nathan Good / *et al*. "Behavioral advertising: The offer you cannot refuse", p. 274.

[92] Electronic Frontier Foundation. *Do not track* (2015) <disponível em: https://www.eff.org/issues/do-not-track, último acesso em 02.01.2017>.

[93] Cf. https://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf

Alliance (DAA), Google e outras empresas se comprometem a respeitar o cabeçalho "Do Not Track".[94]

1.2.2.3. Bloqueadores de conteúdo publicitário de terceiros

Na medida em que, como se destacou acima, o monitoramento e a coleta de dados por terceiros é um dos principais fatores que favorece a formação de perfis detalhados a respeito das preferências e características de comportamento dos usuários, impedir o seu acesso a esses dados reduz significativamente os danos que podem ser causados à privacidade.

O funcionamento técnico da maioria das tecnologias intrusivas se baseia na comunicação entre o dispositivo do usuário e os servidores desses terceiros que, além do conteúdo a ser exibido (anúncios), enviam também mecanismos capazes de identificá-los para fins de monitoramento e coleta de dados. Nesse sentido, ao impedir a exibição de conteúdo publicitário de terceiros, os bloqueadores também impedem o funcionamento de algumas dessas tecnologias intrusivas.[95]

Há diferentes exemplos de bloqueadores disponíveis no mercado e, embora sua forma de funcionamento varie, eles estão essencialmente baseados em listas de bloqueio, que precisam ser constantemente atualizadas.[96] A definição de quais anunciantes entram e saem dessas listas é alvo de controvérsias. No caso do bloqueador *Adblock Plus*, por exemplo, é possível que os anunciantes paguem para se manter na lista de autorizados, o que gera uma série de discussões, sobretudo no âmbito do direito concorrencial.

Além disso, a indústria da publicidade digital tem se posicionado fortemente contra a utilização dessa tecnologia, questionando se ela não violaria a própria liberdade de

[94] Cf. Rainey Reitman, "White House, Google, and other advertising companies commit to supporting Do Not Track", *Electronic Frontier Foundation* (2012) <disponível em: https://www.eff.org/deeplinks/2012/02/white-house-google-and-other-advertising-companies-commit-supporting-do-not-track, último acesso em 02.01.2017>. Para outros exemplos de empresas que aderiram ao "Do Not Track", cf. http://donottrack.us/implementations

[95] Exemplos são as extensões *Ghostery* e *Adblock Plus*.

[96] Jonathan R. Mayer / John C. Mitchell. "Third-party web tracking: Policy and technology", p. 11.

expressão dos anunciantes.[97] Em alguns países, veículos de imprensa têm questionado judicialmente a legalidade dos bloqueadores. Na Alemanha, por exemplo, os tribunais têm decidido a favor de seu uso, como no caso envolvendo o jornal *Süddeutsche Zeitung*.[98]

Enquanto alguns veículos judicializam a questão, outros utilizam estratégias de sensibilização dos usuários. Carlos Affonso de Souza Pereira anota a iniciativa de dois jornais: o *The Guardian*, que insere o aviso "percebemos que você está usando um bloqueador de anúncios. Talvez você queira contribuir com o jornal de outra forma? Torne-se um apoiador por menos de 1 libra por semana."; e a Folha de São Paulo, no mesmo sentido, "Fazer jornalismo de qualidade exige recursos. A publicidade é uma fonte importante de financiamento para o jornal".[99]

Com o exposto neste capítulo, percebe-se que ao longo da evolução do ecossistema da publicidade digital foram surgindo diversos novos atores, que constituem uma complexa cadeia de intermediários nos processos de compra, venda, alocação e exibição de anúncios direcionados na Internet, subsidiando os modelos de negócios baseados na publicidade comportamental. Como visto, esses intermediários podem centralizar atividades de monitoramento, coleta e tratamento de dados pessoais, o que coloca em suas mãos a possibilidade de construir perfis detalhados a respeito das preferências dos usuários, aumentando os riscos em relação à proteção da sua privacidade.

A sofisticação dessas atividades gerou também novos tipos de ameaça à privacidade, como o incremento da capacidade de inferir características da personalidade do usuário, aumentando a sua susceptibilidade e exposição em relação a esses atores.

Além disso, a atuação desses intermediários pode - e costuma - acontecer de forma invisível para os usuários, que ficam impossibilitados não só de compreender mas também de consentir com a coleta e utilização de seus dados para tantas práticas e operações. Essa atuação pode implicar, ainda, a transferência internacional de dados, introduzindo dificuldades de compatibilização entre ordenamentos jurídicos que adotam níveis de proteção diferentes em relação ao direito à privacidade.

---

[97] Foi nesse sentido o discurso de Randall Rothenberg, diretor da *Interactive Advertising Bureau* (IAB), disponível em http://www.iab.com/news/rothenberg-says-ad-blocking-is-a-war-against-diversity-and-freedom-of-expression/.

[98] Cf. Jasper Jackson, "Adblock Plus wins another legal battle with German publishers", *The Guardian* (30.03.2016) <disponível em: https://www.theguardian.com/media/2016/mar/30/adblock-plus-publishers-suddeutsche-zeitung-adblocking, último acesso em 02.01.2016>.

[99] Cf. Carlos Affonso Pereira de Souza, "Quem bloqueia os bloqueadores?", *Observatório da Internet* (2016) <disponível em: http://observatoriodainternet.br, último acesso em 02.01.2017>.

Mais do que isso: como se verá ao longo desta tese, nem sempre esses atores e intermediários estão sediados nos países onde atuam (e sobre cujos cidadãos suas atividades recaem), o que gera dificuldades adicionais relevantes para a sua responsabilização, em caso de violação de legislações nacionais de proteção de dados, por exemplo.

Do ponto de vista técnico, o que se percebe do uso das tecnologias intrusivas de monitoramento e coleta de dados é que são significativamente diferentes das técnicas tradicionais de direcionamento da publicidade empregadas no mundo *offline* pelas seguintes razões principais: *(i)* a arquitetura da Internet permite que sejam adotadas técnicas silenciosas, massivas, concentradas e persistentes de coleta de dados, o que dificulta seu monitoramento e fiscalização; e *(ii)* o uso de tecnologias intrusivas de monitoramento e coleta de dados costuma implicar a transferência internacional de dados, o que pode colocar diferentes modelos de regulação da privacidade em conflito. No caso das tecnologias protetivas, percebe-se sua insuficiência para coibir as interferências das tecnologias intrusivas na privacidade dos usuários se não aliadas a políticas públicas.

CAPÍTULO 2 - O FLUXO GLOBALIZADO DE DADOS E A COLISÃO DE MODELOS REGULATÓRIOS DE PROTEÇÃO DA PRIVACIDADE

No capítulo anterior, a partir da análise das principais características do ecossistema da indústria da publicidade digital, demonstrou-se que a existência de uma complexa cadeia de intermediários e o emprego de tecnologias intrusivas de monitoramento e coleta de dados representam desafios adicionais e específicos à tutela do direito à privacidade na Internet.

Considerando que a utilização dessas tecnologias acontece de forma globalizada, este capítulo aprofunda as consequências do fluxo internacional de dados de usuários, viabilizado pela arquitetura da Internet, para o direito à privacidade. Mais especificamente, pretende abordar as dificuldades de compatibilização que surgem da colisão entre os modelos regulatórios de privacidade adotados pelos Estados Unidos e pela União Europeia.

Dada a alta concentração de empresas do setor de Internet nos Estados Unidos, tal como se demonstrará nesta tese[100], e a influência do modelo de regulação europeu ao redor do mundo, a colisão entre esses dois modelos é representativa em relação àquelas que podem ocorrer entre os Estados Unidos e outras regiões. Além disso, o poderio econômico dessas duas ordens políticas contribuiu para a implementação de um arranjo normativo que se propunha a equacionar essa situação (*Safe Harbor Agreement*).

Ainda que limitada às operações de transferência internacional de dados realizadas entre Estados Unidos e os Estados-membros da União Europeia, deixando de fora aquelas realizadas entre Estados Unidos e o resto do mundo, a experiência com o *Safe Harbor* representa a primeira e mais importante tentativa estruturada de fazer valer as garantias referentes ao direito à privacidade de uma região em relação à outra.[101]

[100] O último capítulo desta tese apresenta dados de pesquisa que realizamos acerca da concentração das empresas do setor de Internet nos Estados Unidos, sobretudo no estado da Califórnia.

[101] A experiência com o *Safe Harbor* não foi a única tentativa de compatibilização entre modelos regulatórios de privacidade. Desde 2012, os Estados Unidos passaram a participar, por exemplo, de um arranjo com a Cooperação Econômica Ásia-Pacífico ("APEC") para viabilizar a transferência internacional de dados entre

Para avaliar até que ponto a adoção de modelos regulatórios de privacidade distintos ao redor do mundo pode afetar a capacidade dos Estados de tutelar o direito à privacidade em âmbito nacional, restringindo as suas possibilidades de responsabilizar atores sediados em outros países por violações cometidas em seus territórios, este capítulo analisará a experiência de implementação e vigência do *Safe Harbor*, dando especial destaque para *(i)* as principais razões que levaram à sua elaboração, notadamente as diferenças entre os modelos regulatórios adotados nos Estados Unidos e na União Europeia; *(ii)* suas principais limitações; e *(iii)* seu processo de invalidação e reforma.

Frise-se que as características dos modelos regulatórios de privacidade dos Estados Unidos e da União Europeia serão descritas apenas na medida em que forem necessárias para compreender as dificuldades de compatibilização entre eles no que diz respeito à transferência internacional de dados. Não faz parte do escopo deste capítulo apresentar detalhes sobre o seu funcionamento ou enfrentar disputas interpretativas que tenham se estabelecido ao longo de sua evolução.

2.1. Modelos regulatórios de privacidade

A tutela do direito à privacidade evoluiu de forma significativamente diferente ao redor do mundo, dando origem a diferentes modelos regulatórios. Isso se justifica, em parte, porque as concepções a respeito do papel do Estado na tutela de direitos e na regulação do mercado variam significativamente de país para país. Nos Estados Unidos, por exemplo, Stephen Kobrin assinala que o Estado costuma conferir maior deferência à livre iniciativa e à autonomia privada, ao passo que, na Europa, prevaleceriam as preocupações com os direitos individuais e o bem-estar social.[102] [103]

---

as regiões. O arranjo elenca nove princípios que devem ser observados para que as transferências possam ocorrer. Contudo, de certa forma, a experiência com o programa ainda é incipiente, razão pela qual se preferiu, nesta tese, avaliar a experiência com o *Safe Harbor*.

[102] Cf. Stephen J Kobrin, "Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance", *Review of International Studies* 30 (2004), 111–131.

[103] A discussão sobre as diferenças de atuação e interferência do Estado na ordem econômica e na tutela de direitos nos Estados Unidos e na União Europeia é profunda e extremamente complexa. Foge ao escopo desta tese aprofundar essas teorias, razão pela qual nos limitamos a abordá-las no que se referirem à regulação da privacidade. Para mais detalhes a respeito dessas teorias sob uma perspectiva comparada, cf. Joel R. Reidenberg, "Resolving conflicting international data privacy rules in cyberspace", *Stanford Law Review* 52

Nesse sentido, o autor esclarece que, em geral, nos Estados Unidos, as garantias individuais impõem limites à atuação do Estado, privilegiando a livre concorrência do mercado e a sua auto-regulação. Isso teria influenciado a regulação sobre privacidade no país, que, ao se desenvolver com base nessas premissas, teria adquirido contornos muito mais "reativos" e direcionados a setores específicos (*issue-specific*).[104]

No caso da Europa, a privacidade seria considerada segundo seu valor social, isto é, sua função de garantir o desenvolvimento livre e pleno da personalidade dos cidadãos.[105] Dentro dessa perspectiva, a regulação desse direito teria evoluído de forma a reconhecê-la como um direito fundamental e inalienável.[106] Ao contrário, nos Estados Unidos, "*a privacidade é vista como uma coisa alienável sujeita ao mercado. Disputas sobre informações pessoais e os mecanismos para sua proteção são postos em termos econômicos*".[107]

À medida em que a Internet tornou mais frequentes as operações internacionais de coleta, tratamento e transferência de dados, acirrou-se o embate entre os modelos regulatórios calcados nessas diferentes raízes, inviabilizando, em tese, a implementação dessas operações, especialmente por parte de atores privados, como as empresas de Internet. Nesse contexto, em 1998, Peter Swire e Robert Litan já alertavam para o fato de que Estados Unidos e União Europeia estavam em uma "rota de colisão" no que dizia respeito à tutela do direito à privacidade.[108]

Os itens a seguir exploram de maneira pormenorizada as características dos dois modelos, o estadunidense, fragmentado e de auto-regulação e o europeu, legislativo, destacando as principais dificuldades de compatibilização que apresentam.

(2000), p. 1339–1351. Cf. também Gregory Schaffer, "Globalization and social protection: The impact of EU and international rules in the ratcheting up of U.S. privacy standards", *Yale J. Int 'l L.* 25 (2000), 1.

[104] Cf. Stephen J. Kobrin, "Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance", p. 115.

[105] Paradigmática, nesse sentido, foi a decisão do Tribunal Constitucional alemão em 1983 (BVerfGE 65, 1), no caso envolvendo uma lei que previa a realização de um censo populacional, introduzindo o conceito de "autodeterminação informacional", segundo o qual deve ser reconhecido aos cidadãos um poder de controle sobre seus dados pessoais. Para uma discussão aprofundada a respeito do conceito e de suas repercussões para o desenvolvimento da regulação do direito à privacidade na União Europeia, cf. Bruno Bioni, *Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet*. São Paulo: dissertação de mestrado (Universidade de São Paulo), 2016.

[106] Gregory Shaffer anota, nesse sentido, que a privacidade não seria objeto de nenhum tipo de "barganha". Cf. Gregory Shaffer, "Globalization and social protection: The impact of EU and international rules in the ratcheting up of U.S. privacy standards"s, p.19.

[107] Stephen J. Kobrin, "Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance", p. 116 (tradução livre).

[108] Cf. Peter Swire / Robert Litan, "None of your business: World data flows, electronic commerce, and the European Privacy Directive", *Harvard Journal of Law and Technology* 12 (1999), 683, p. 3.

2.1.1. O modelo dos Estados Unidos

Apesar de a Constituição dos Estados Unidos não tutelar o direito à privacidade expressamente, ela estabelece uma série de garantias que se relacionam com a sua proteção, como o direito de se manifestar anonimamente, de manter sigilo sobre a participação em grupos e associações, de não ter a presença continuada de militares em suas residências, de impedir buscas e revistas injustificadas e de não revelar informações que possam levar à sua autoincriminação.[109]

Essas garantias, entretanto, estabelecem limites em relação à atuação do Estado e não costumam ser oponíveis entre particulares, como é o caso das relações estabelecidas entre empresas e usuários, principal objeto de análise desta tese.[110] O mesmo vale para as poucas constituições estaduais que adotaram dispositivos tutelando expressamente o direito à privacidade, com poucas exceções, como o caso da constituição do estado da Califórnia, cuja aplicação entre particulares já foi admitida.[111]

2.1.1.1. Legislações setoriais

Desde a década de 70, foram aprovadas mais de vinte leis federais que regulam a coleta e o tratamento de dados pessoais em setores específicos nos Estados Unidos. Boa parte dessas leis foi aprovada em resposta às crescentes discussões a respeito da

[109] Cf. Daniel Solove / Paul Schwartz, "Privacy, information and technology", pp.34-35 (destacando a evolução da jurisprudência da Suprema Corte dos Estados Unidos no sentido de incorporar novas dimensões a essas garantias). No mesmo sentido, cf. também Fred H. Cate, *Privacy in the Information Age*. Washington, DC: Brookings Institution Press, 1997, p.52.

[110] Cf. Robert Gellman, "Does privacy law work?", in Philip E. Agre / Marc Rotenberg (orgs.) *Technology and privacy: The new landscape*, Cambridge, MA: MIT Press, 1997 (esclarecendo que a jurisprudência da Suprema Corte dos Estados Unidos é clara no sentido de as proteções da Quarta Emenda não se aplicarem ao setor privado, por exemplo).

[111] Cf. Daniel Solove / Paul Schwartz, "Privacy, information and technology", p.37. Para uma lista completa dos onze estados que reconheceram o direito à privacidade em suas constituições expressamente, cf. também Daniel Solove / Paul Schwartz, Privacy Law Fundamentals, p.4.

necessidade de tutela da privacidade em face do desenvolvimento da tecnologia, sobretudo das capacidades de processamento automatizado de dados pelos computadores.[112]

Os setores abrangidos variam bastante: há leis que regulamentam a coleta e tratamento de dados financeiros[113], ligados à saúde[114], a crianças menores de treze anos[115] ou até mesmo ao histórico de vídeos alugados em locadoras.[116]

Além dessas legislações setoriais, há também legislações federais que tocam o tema da coleta e uso de dados pessoais. Contudo, essas legislações tem escopo de aplicação limitado aos órgãos da administração pública federal, como o *Privacy Act of 1974*[117] e o *Freedom of Information Act (FOIA)*.[118]

Fora dos segmentos abrangidos por essas leis, a coleta e tratamento de dados pessoais por atores do setor privado não são regulamentados no âmbito federal de forma genérica, o que confere considerável discricionariedade por parte daqueles que desejam colocar essas operações em prática.

2.1.1.2. Legislações Estaduais

Além de reconhecer o direito à privacidade em suas constituições, alguns estados possuem legislações específicas regulamentando diferentes hipóteses de coleta e uso de dados tanto no setor público quanto no setor privado. De acordo com Daniel Solove e Paul Schwartz, são sete as principais áreas que foram objeto de regulamentação no âmbito estadual: *(i)* acesso a dados por parte de autoridades; *(ii)* informações médicas e genéticas; *(iii)* bancos de dados e registros públicos; *(iv)* sigilo financeiro; *(v)* segurança da

[112] Jonathan Cody anota que, nessa época, já se discutiam boas práticas no uso de informações no âmbito do Conselho Consultivo de Sistemas Automatizados de Dados Pessoas do Ministério da Saúde, Educação e Bem Estar dos Estados Unidos. Cf. Jonathan P. Cody, "Protecting privacy over the Internet: Has the time come to abandon self-regulation." *Cath. UL Rev* 48 (1998), 1183.
[113] Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 12 U.S.C. §§ 3401-3422.
[114] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
[115] Children's Online Privacy Protection Act of 1998, Pub. L. No. 106-170, 15 U.S.C.
[116] Video Privacy Protection Act of 1998, Pub. L. 100-618, 18 U.S.C. §§ 2710-2711.
[117] A legislação exige que órgãos da administração pública federal coletem apenas os dados estritamente necessários para o desempenho de suas atividades e estabeleçam procedimentos para resguardar a sua segurança, por exemplo. Cf. 5 U.S.C. parag. 552a(e)(1)-(5).
[118] A legislação exclui a possibilidade de acesso do público a documentos que contenham informações pessoais, como registros médicos (5 U.S.C. parag. 552(b) (6)) e registros ligados à segurança pública (5 U.S.C. parag. 552(b) (7)).

informação; *(vi)* informações pessoais no contexto trabalhista; e *(vii)* dados de consumidores e informações cadastrais.[119]

A legislação estadual também é responsável por delimitar as circunstâncias de responsabilidade civil (*tort law*) nas quais se enquadram os atos ilícitos ligados à violação da privacidade. Embora variem de estado para estado, William Prosser define quatro principais tipos de atos ilícitos compreendidos nessas legislações e que foram adotados como parte do tratado sobre responsabilidade civil editado pelo *American Law Institute*[120]: *(i)* divulgação pública de fatos privados[121]; *(ii)* invasão da esfera íntima[122]; *(iii)* apropriação indevida de nome e/ou imagem[123]; e *(iv)* falsa impressão ("falsa luz")[124].

Fred H. Cate alerta, entretanto, que esses atos ilícitos não têm sido aplicados ao contexto da Internet por dificuldades de adaptação e interpretação desses conceitos.[125]

2.1.1.3. Auto-regulação

Como se viu, o modelo regulatório adotado nos Estados Unidos não oferece regulamentação aplicável às atividades de coleta e tratamento de dados pessoais por atores do setor privado, a não ser em segmentos específicos. Em parte, isso se justifica pela oposição tanto do governo quanto do congresso dos Estados Unidos em adotar uma legislação genérica nesse sentido.

---

[119] Cf. Daniel Solove / Paul Schwartz, "Privacy Law Fundamentals", p.24.

[120] Cf. William Prosser, "Privacy", *Cal. L. Rev.* 48 (1960), 383-423. A categorização proposta por William Prosser foi adotada pelo *Restatement (Second) of Torts*, que apresenta uma compilação da matéria no país.

[121] "Quem dá publicidade a um assunto relativo à vida privada de outrem responde por invasão de sua privacidade, se o assunto divulgado é de um tipo que (a) seria altamente ofensivo para uma pessoa razoável e (b) não é de interesse legítimo para o público." Restatement, Second, Torts, § 652D (1997), The American Law Institute (tradução livre).

[122] "Quem intencionalmente se intrometer, fisicamente ou de outra forma, na solidão ou reclusão de outrem ou em seus assuntos ou preocupações particulares, está sujeito a responder por invasão de privacidade, se a intrusão for altamente ofensiva para uma pessoa razoável." Restatement, Second, Torts, § 652B (1997), The American Law Institute (tradução livre).

[123] "Quem dá publicidade a um assunto relativo a outrem que o coloca diante do público em uma luz falsa responde por invasão de privacidade, se (a) a luz falsa em que o outro foi colocado seria altamente ofensiva a uma pessoa razoável, e (b) o ator teve conhecimento ou agiu com negligência quanto à falsidade da situação de luz falsa em que a pessoa seria colocada". Restatement, Second, Torts, § 652E (1997), The American Law Institute (tradução livre).

[124] "Quem se apropria para seu próprio uso ou benefício do nome ou imagem de outrem responde por invasão de sua privacidade." Restatement, Second, Torts, § 652C (1997), The American Law Institute (tradução livre).

[125] Cf. Fred H. Cate, *Privacy in the Information Age*, p. 89-90.

Em 1997, o então presidente Bill Clinton, quando da divulgação do seu plano estratégico para o desenvolvimento do comércio eletrônico, já defendia a auto-regulação como chave para o crescimento da Internet.[126] Nos governos que se seguiram, também não foram apresentadas propostas robustas no sentido de aprovar uma regulamentação abrangente sobre o tema.

Da mesma forma, no congresso, em parte, possivelmente, por pressão do setor privado, propostas de regulamentação costumam ser rechaçadas, principalmente sob o argumento de que prejudicariam a economia e inovação.[127]

Diante da inexistência de um marco regulatório genérico, a auto-regulação acabou se tornando o modelo mais adequado para inspirar a confiança dos usuários e fomentar a lisura das relações comerciais travadas na Internet. Como se descreverá pormenorizadamente no capítulo seguinte, por sua competência para fiscalizar práticas desleais ou enganosas, a Comissão Federal do Comércio dos Estados Unidos assumiu o papel de estimular o desenvolvimento de um conjunto de boas práticas que pudessem orientar a atuação das empresas do setor privado.

Desses esforços, surgiram os *Fair Information Practice Principles* ("FIPP"), sistematizados e promovidos pela Comissão a partir de um importante relatório que encaminhou ao congresso em 1998.[128] Os FIPP se tornaram diretrizes particularmente importantes para a atuação de empresas do setor de Internet nos Estados Unidos, tendo servido, inclusive, como fundamento para muitas das ações de fiscalização protagonizadas pela Comissão.

---

[126] Cf. ("For electronic commerce to flourish, the private sector must lead. Therefore, the Federal Government should encourage industry self-regulation wherever appropriate and support private sector efforts to develop technology and practices that facilitate the growth and success of the Internet.") William Clinton / Al Gore. *The framework for global electronic commerce* (1997) <disponível em: http://clinton4.nara.gov/WH/New/Commerce/, último acesso em 02.01.2017>.

[127] É como se posiciona, por exemplo, durante a discussão a respeito de proposta de adoção de uma legislação de proteção de dados pessoais em 2012, a deputada Marsha Blackburn ("Temos de nos lembrar que vivemos numa era da informação orientada por dados. E o que acontece quando você segue o modelo europeu de privacidade e tira informações da economia da informação? Essas são as perguntas que vamos fazer porque eu acho que há uma resposta muito simples, e você pode olhar para a Europa e ver, os lucros caem, a inovação fica paralisada, e você perde para os inovadores que escolheram trabalhar em outro lugar "). No mesmo sentido, o deputado Fred Upton ("Estou altamente cético em relação à capacidade dos reguladores do governo ou do Congresso de acompanhar o ritmo inovador e vibrante da Internet sem quebrá-lo. Os consumidores e a economia como um todo não estarão bem servidos com as tentativas do governo de envolver a Internet em burocracia. E não podemos ignorar que as empresas de Internet têm um forte incentivo para proteger seus usuários, chama-se escolha do consumidor"). Cf. Marsha Blackburn, "Balancing privacy and innovation: Does the President's proposal tip the scale? Hearing before the Subcomm. on Commerce, Mfg. & Trade f the H. Comm. Of Energy and Commerce", 112 Cong. 4 (2012) (tradução livre).

[128] Federal Trade Commission, "Privacy online: A report to Congress", *Federal Trade Commission* (1998) <disponível em http://www.ftc.gov/reports/privacy3/index.htm, último acesso em 02.01.2017>.

Os FIPP são compostos por quatro princípios centrais:

> "**(1) Notificação:** Os responsáveis por atividades de coleta devem divulgar suas práticas antes de coletar informações pessoais dos consumidores;
> **(2) Escolha:** devem ser dadas opções para os usuários para que possam decidir se e como informações pessoais coletadas podem ser utilizadas para fins que não aqueles para os quais foram originalmente fornecidos;
> **(3) Acesso:** os consumidores devem ter o direito de ver e contestar a exatidão e completude de dados coletados sobre eles; e
> **(4) Segurança:** os responsáveis pelas atividades de coleta de dados devem tomar medidas razoáveis para assegurar que as informações coletadas dos consumidores são corretas e protegidas contra usos não autorizados." (tradução livre e destaques nossos) [129]

Como também se verá no próximo capítulo, boa parte da jurisprudência da Comissão se baseia na aplicação desses princípios. Como destaca Chris Hoofnagle, a atuação proeminente da Comissão na promoção e fiscalização desses princípios também teria sido fundamental para angariar a confiança da comunidade internacional em relação à proteção conferida à privacidade nos Estados Unidos. Era importante mostrar que havia parâmetros para a atuação das empresas.[130]

2.1.2. O modelo da União Europeia

O modelo regulatório adotado pelos Estados-membros da União Europeia é o que convencionamos chamar de "legislativo", por se basear na aprovação de uma lei de proteção de dados pessoais. Nesse modelo, adota-se um marco regulatório de proteção de dados pessoais genérico, que estabelece parâmetros mínimos que devem ser respeitados para coleta e tratamento desses dados. Nesses casos, portanto, há uma liberdade mais restrita da iniciativa privada para moldar e implementar suas políticas de privacidade. A fiscalização e controle costumam ser feitos por órgãos especiais ("autoridades de proteção de dados"), cujas competências e atribuições também costumam estar definidos nessas legislações.

---

[129] Cf. Federal Trade Commission, "Privacy online: Fair information practice in the electronic marketplace: A report to Congress", *Federal Trade Commission* (2000) <disponível em https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf, último acesso em 02.01.2017>.
[130] Cf. Hoofnagle, Chris Jay. *Federal Trade Commission Privacy Law and Policy*, Cambridge, MA: Cambridge University Press, 2016, p. 514.

2.1.2.1. Diretiva 95/46/CE

Aprovada em 24 de outubro de 1995, a Diretiva 95/46/CE do Parlamento Europeu e do Conselho ("Diretiva 95") consolidou o modelo regulatório legislativo entre os Estados-membros da União Europeia ao impor a eles a obrigação de assegurar, em seus respectivos ordenamentos jurídicos nacionais, parâmetros mínimos de proteção à privacidade. Desde sua aprovação, a Diretiva 95 é a base de todo o sistema de proteção de dados que vigora na União Europeia.

Muito antes de a Diretiva 95 ser elaborada, entretanto, alguns países já adotavam legislações nesse sentido. A Suécia, por exemplo, foi um dos primeiros países no mundo a adotar, em 1973, uma lei que regulamentava o tema da proteção de dados pessoais (*Datalagen*); em 1977, foi a vez da Alemanha positivar as suas regras específicas sobre o tema (*Bundesdatenschutzgesetz*).

Na esteira dessas legislações que começavam a surgir, depois de dois anos de estudos, em 23 de setembro de 1980, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) publicou as "Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais" ("Diretrizes da OCDE").[131] O documento representa uma recomendação do Conselho da OCDE para a adoção de um conjunto de princípios básicos de aplicação nacional para a proteção da privacidade, tais como *(i)* limitação de coleta de dados; *(ii)* qualidade de dados; *(iii)* definição da finalidade; *(iv)* limitação de utilização; *(v)* segurança; *(vi)* abertura; *(vii)* participação do indivíduo; e *(viii)* responsabilização.

Em resumo, esse conjunto de princípios sugeria limites às atividades de coleta de dados pessoais, exigindo que só ocorressem mediante o consentimento do indivíduo e para finalidade determinada. Além disso, os dados coletados deveriam ser precisos, completos, atualizados e armazenados em condições seguras. Estabelecia, ainda, o chamado "direito de acesso" do indivíduo, a quem deveria assistir a faculdade de solicitar informações sobre os dados que estavam armazenados a seu respeito.

[131] Íntegra do documento disponível em https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, último acesso 21/03/2016.

Independentemente de seu caráter não-vinculante, o documento se tornou uma referência internacional para a elaboração de diversas leis e diretrizes de proteção de dados pessoais, como foi o caso da Convenção do Conselho da Europa para a "Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal" ("Convenção 108").[132]

Assinada em 1981, ao lado das Diretrizes da OCDE, a Convenção 108 se tornou um dos principais antecedentes para a Diretiva 95. Ao contrário das Diretrizes da OCDE, de aplicação voluntária, a Convenção 108 estabelecia regras vinculantes a serem implementadas e internalizadas pelos países-membro da União Europeia. No entanto, suas determinações também tinham caráter demasiadamente genérico.

Em resumo, a Convenção 108 exigia que os dados fossem *(i)* coletados e processados de forma leal e lícita; *(ii)* utilizados para finalidades determinadas e legítimas; *(iii)* adequados, pertinentes e não excessivos em relação às suas finalidades; *(iv)* precisos e atualizados; *(v)* armazenados por um período não excessivo. Os direitos de acesso e de retificação de dados armazenados sobre si próprio também foram garantidos no documento. Além disso, a coleta de dados sensíveis, isto é, de dados relacionados a origem racial, opiniões políticas e convicções religiosas, por exemplo, deveriam receber tratamento especial.

Embora estabelecessem princípios e direitos básicos dos indivíduos, os dois documentos não ofereciam regras concretas o suficiente para garantir uniformidade no tratamento das atividades de coleta de dados pessoais. Isso levou a Comissão Europeia a formular novas propostas para regulamentar essas questões de forma pormenorizada.[133]

Nesse contexto, depois de passar por várias rodadas de discussão e negociação entre os representantes dos Estados-membros da União Europeia, em 1995, a Comissão Europeia adotou a Diretiva 95, com um prazo de três anos para que os Estados-membros se adequassem às suas determinações.[134]

No que tange às garantias dos indivíduos em relação às atividades de coleta de dados, em linhas gerais, a Diretiva 95 consagrou o que já determinavam as Diretrizes da

---

[132] Íntegra do documento disponível em https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

[133] Para detalhes sobre o histórico e teor das propostas que antecederam o texto da Diretiva 95, cf. Michael P. Roch, "Filling the void of data protection in the United States: Following the European example", *Santa Clara Computer & High Tech. LJ* 12 (1996), 71, p. 80–82. Cf. também Robert R. Schriver, "You cheated, you lied: The safe harbor agreement and its enforcement by the Federal Trade Commission", *Fordham L. Rev.* 70 (2001), 2777, p. 2784–2786.

[134] Artigo 32, 1.

OCDE e a Convenção 108, no sentido de assegurar que os dados pessoais devem ser *(i)* processados de forma lícita (art. 6º, 1, a); *(ii)* coletados para finalidades determinadas, explícitas e legítimas (art. 6º, 1, b); *(iii)* adequados, relevantes e não excessivos em relação às finalidades para as quais foram originalmente coletados (art. 6º, 1, c); *(iv)* precisos e atualizados (art. 6º, 1, d); e *(v)* armazenados de forma identificável pelo menor período possível (art. 6º, 1, e).

Além disso, a Diretiva 95 proibia, em princípio, o tratamento de dados relativos a fatores como origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas, bem como aqueles ligados à saúde ou à vida sexual (art. 8º) e garantia ao indivíduo o direito de acesso e de retificação em relação aos dados coletados e armazenados sobre si próprio (art. 12).

Mais do que consolidar princípios e direitos ligados à proteção de dados pessoais, a Diretiva 95 trouxe avanços ao estabelecer regras mais concretas que regulamentavam as hipóteses de tratamento de dados pessoais, o que ficou consubstanciado em seu artigo 7º.

De acordo com o dispositivo, as legislações de proteção de dados dos Estados-membros deveriam autorizar o tratamento de dados pessoais apenas nas seguintes hipóteses: *(i)* se houvesse consentimento inequívoco por parte do titular dos dados (art. 7º, a); *(ii)* se o tratamento fosse necessário para a execução de um contrato do qual o titular dos dados é parte ou para a execução de diligências prévias à formação de um contrato a pedido do titular dos dados (art. 7º, b); *(iii)* se o tratamento fosse necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento estivesse sujeito (art. 7º, c); *(iv)* se o tratamento fosse necessário para a proteção de interesses vitais do titular dos dados (art. 7º, d); *(v)* se o tratamento fosse necessário para a execução de uma missão de interesse público ou o exercício de autoridade pública (art. 7º, e); *(vi)* se o tratamento fosse necessário para perseguir interesses legítimos do responsável pelo tratamento ou de terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos do titular dos dados (art. 7º, f).

Nesse sentido, é importante frisar que, além do consentimento inequívoco do indivíduo, a Diretiva 95 criou, portanto, outras hipóteses que autorizam o tratamento de dados pessoais. Desde da entrada em vigor da Diretiva 95, o Grupo de Trabalho criado por determinação de seu artigo 29 (*Article 29 Working Party*) se debruçou reiterada e

exaustivamente sobre essas hipóteses, tendo exarado importantes orientações e balizas de interpretação desses dispositivos.[135]

2.1.2.2. Regulamento Geral de Proteção de Dados Pessoais

Quase quinze anos depois da entrada em vigor da Diretiva 95, começaram a surgir propostas para a sua atualização. Desde janeiro de 2012, seguindo movimento capitaneado por Viviane Reding, então vice-presidente da Comissão Europeia, deu-se início a uma discussão sobre seus principais pontos críticos, o que deu origem a uma proposta formal de reforma do marco regulatório para proteção de dados pessoais da União Europeia.

Com os objetivos de atualizar os mecanismos de tutela do direito à privacidade frente ao desenvolvimento de tecnologias mais intrusivas de coleta e tratamento de dados pessoais e de corrigir assimetrias geradas pela pouca uniformidade entre as legislações nacionais de proteção de dados dos Estados-membros, a proposta era a de aprovar um regulamento e não uma nova diretiva.[136] A principal vantagem estaria no fato de que, no direito comunitário, os regulamentos são autoaplicáveis, ao contrário das diretivas, que dependem da incorporação pelo direito interno de cada Estado-membro.

Após um processo de intensos debates e rodadas de negociação, em 14 de abril de 2016, foi aprovado, pelo Parlamento da União Europeia, o "Regulamento Geral de Proteção de Dados Pessoais" ("RGPD"), que entrará em vigor em 25 de maio de 2018.[137]

---

[135] Uma lista completa com os mais de cem pareceres elaborados pelo Grupo de Trabalho pode ser encontrada em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

[136] Cf. European Commission. "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", *Press release* (2012) <disponível em: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en, último acesso em 02.01.2017>. A proposta também incluía a aprovação de uma Diretiva para a proteção dos indivíduos em relação ao processamento de dados pessoais por autoridades para fins de investigação e persecução criminal, em substituição à Decisão 2008/977/JHA, adotada pelo Conselho da Europa. Cf. European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" (25.01.2012) <disponível em http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, último acesso em 26.10.2016>.

[137] A íntegra do RGPD está disponível em http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32016R0679

Como o objetivo deste capítulo é o de analisar a experiência da tentativa de compatibilização entre os modelos regulatórios adotados nos Estados Unidos e União Europeia no que diz respeito às possibilidades de transferência internacional de dados, fugiria de seu escopo descrever pormenorizadamente todas características do RGPD ou ainda de especular sobre sua efetividade no futuro.

Para a discussão travada neste capítulo, entretanto, vale destacar que o RGPD consagra a hipótese de aplicação extraterritorial de seus dispositivos, determinando que eles também são aplicáveis a operações que envolvam dados de indivíduos residentes no território da União Europeia, independentemente de o ator responsável pelo tratamento dos dados pessoais estar sediado fora dele, desde que as atividades de tratamento estejam relacionadas *(i)* com a oferta de bens e serviços a titulares de dados pessoais residentes na União Europeia; ou *(ii)* com o controle de seu comportamento (art. 3º, 2). Isso colocaria fim a um longo debate acerca da possibilidade de aplicação extraterritorial no caso da Diretiva 95, cujos dispositivos são bem menos explícitos em relação a isso.

Além disso, cumpre registrar que o RGPD reproduziu em grande parte o regramento dado às transferências internacionais de dados previstas na Diretiva 95, tendo acrescentado poucas mudanças significativas, como a indicação de que o critério de adequação deveria ser revisto periodicamente. O capítulo V (artigos 44 a 49) do RGPD regula as transferências internacionais de dados pessoais. Quando forem oportunas para as discussões travadas neste capítulo, tais alterações serão abordadas.

2.1.2.3. Hipóteses de transferência internacional de dados

Considerando que as operações de coleta e tratamento de dados pessoais assumiam, cada vez mais, uma dimensão globalizada, o tema da transferência internacional de dados já havia sido enfrentado pelas Diretrizes da OCDE e pela Convenção 108. Ambos os documentos apontavam para a necessidade de se garantir o livre fluxo de dados transfronteiriços, sem a imposição de regras que pudessem inviabilizá-lo. No caso das Diretrizes da OCDE, a exceção seria feita em relação a países que não observassem os parâmetros mínimos de proteção que estabelecia, hipótese na qual esse livre fluxo poderia ser restringido. De forma similar, a Convenção 108 previa que o fluxo não poderia ser

restringido a menos que o país de destino não oferecesse condições de proteção equivalentes àquelas do país de origem.

No caso da Diretiva 95, as regras relativas à transferência internacional de dados pessoais se encontram delimitadas nos artigos 25 e 26.

Como se verá a seguir, o artigo 25 estabelece os princípios gerais que norteiam essas operações, baseando-se no conceito de "adequação". Já o artigo 26 estabelece as hipóteses nas quais as transferências podem ocorrer independentemente do preenchimento do critério de "adequação", tais como *(i)* consentimento inequívoco do indivíduo em relação à transferência (art. 26, a); *(ii)* necessidade da transferência para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento (ou de diligências prévias à formação do contrato) (art. 26, b); *(iii)* necessidade ou exigência legal da transferência para atender ao interesse público (art. 26, d); *(iv)* necessidade da transferência para proteger os interesses vitais do titular dos dados (art. 26, e), etc.

Apesar de as hipóteses do artigo 26 autorizarem a transferência de dados pessoais sem a necessidade de preenchimento do requisito de "adequação", o que viabilizaria algumas atividades corriqueiras como a transferência de dados para a reserva de hotéis e passagens aéreas ou para a efetivação de transferências bancárias internacionais, essas hipóteses eram insuficientes para autorizar a maioria das transferências envolvendo a coleta e tratamento de dados pessoais na Internet.

Nesse sentido, tornou-se ainda mais importante o preenchimento do critério de adequação, estabelecido pelo artigo 25.

2.1.2.3.1. O conceito de "adequação"

Ao regular a transferência internacional de dados pessoais, a Diretiva 95 autoriza a sua realização apenas *"para países terceiros que assegurem um nível de proteção adequado*" (art. 25, 1). Isso significa dizer que atores privados localizados fora da União Europeia que desejassem coletar e transferir dados de cidadãos europeus para tratamento deveriam comprovar um "nível adequado de proteção". Nesse sentido, caso o país destino dos dados tivesse em vigor uma legislação de proteção de dados pessoais que estivesse

alinhada, substancialmente, com as exigências da Diretiva 95, essa comprovação ficava facilitada.

Com isso, não causa surpresa o fato de que, a partir da entrada em vigor da Diretiva 95, não só os demais Estados-membros da União Europeia passaram a adotar legislações de proteção de dados pessoais, como também muitos outros países ao redor do mundo: até 2013, Graham Greenleaf já identificava a adoção dessas legislações por mais de cem países.[138] De certa forma, a relevância do mercado europeu pode justificar, portanto, não só a expansão do modelo regulatório legislativo de proteção de dados pessoais como também a adoção globalizada dos próprios parâmetros e princípios adotados na Diretiva 95.

Para avaliar a adequação dos níveis de proteção adotados em países fora da União Europeia (e que portanto não estavam vinculados aos parâmetros de proteção da Diretiva 95 na elaboração de suas leis nacionais de proteção de dados), a Diretiva 95 delegou a um "Grupo de Trabalho" a avaliação acerca do preenchimento desse requisito (art. 30, b).

Como visto, no caso dos Estados Unidos, não há legislação de proteção de dados que garanta os parâmetros mínimos de proteção exigidos pela Diretiva 95, o que gerou um impasse em relação à possibilidade de transferência de dados entre as duas regiões. Sem a garantia de um nível adequado de proteção, empresas estadunidenses não poderiam transferir dados de cidadãos europeus para fora da União Europeia em circunstâncias diferentes daquelas previstas pelo artigo 26, o que inviabilizaria os modelos de negócios de muitas das empresas de Internet atuantes no mercado europeu.

2.2. *Safe Harbor Agreement*

Para equacionar essa situação, logo depois que a Diretiva 95 entrou em vigor, em outubro de 1998, as negociações entre Estados Unidos e União Europeia para viabilizar a transferência internacional de dados entre as duas regiões avançaram e, em novembro, foi

[138] É o caso, por exemplo, de Canadá, México, Nova Zelândia, África do Sul, Austrália, Argentina, Colômbia, Chile, etc. Para uma lista completa dos países que adotam legislações de proteção de dados pessoais, cf. Graham Greenleaf, "Global data privacy laws 2015: 109 countries, with european laws now a minority", *SSRN* (2015) <disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529, último acesso em 02.01.2017>.

apresentada a primeira versão de um documento que oficializaria um acordo entre as duas regiões.[139]

Depois de 18 meses de discussão desse primeiro texto[140], em 21 de julho de 2000, celebrou-se um acordo bilateral entre a Comissão Europeia e o Departamento de Comércio dos Estados Unidos, a partir do qual empresas estadunidenses poderiam, voluntariamente, declarar adotar níveis de proteção de privacidade adequados, isto é, que estariam em conformidade com as exigências da Diretiva 95 ("Safe Harbor Agreement").[141]

Essa declaração estava baseada no comprometimento em cumprir um conjunto de princípios de proteção de dados previstos no acordo e era suficiente para incluir as empresas estadunidenses em uma lista, autorizando-as a transferir dados coletados de cidadãos europeus para os Estados Unidos ("US-EU Safe Harbor List").[142]

Embora fruto de negociações bilaterais, o acordo foi formalizado por dois atos unilaterais.[143] Do lado dos Estados Unidos, o Departamento do Comércio desenvolveu um conjunto de princípios com os quais os atores participantes deveriam se comprometer para participar do acordo. Do lado da União Europeia, esse conjunto de princípios foi submetido à apreciação da Comissão Europeia que, em 26 de julho de 2000, exarou decisão no sentido de entender que as empresas aderentes a ele deveriam ser consideradas como garantidoras de um nível de proteção adequada da privacidade para fins de cumprimento das exigências do artigo 25 da Diretiva 95.[144] Em outras palavras, a aderência por empresas estadunidenses ao acordo autorizaria a transferência internacional de dados pessoais coletados na União Europeia para os Estados Unidos.

Nesse sentido, a Decisão 2000/520 é o que legitimava o acordo perante as empresas estadunidenses, que tinham uma garantia de que a transferência internacional de dados que realizassem não seria considerada como uma violação da Diretiva 95.

---

[139] Para detalhes sobre o histórico do processo de negociação para a celebração do acordo, cf. Henry Farrell, "Negotiating privacy across arenas: The EU-US safe harbor discussions", in Adrienne Windhoff-Héritier, *Common goods: Reinventing European and international governance*, Lanham: Rowman & Littlefield, 2002: 105–127.

[140] Para detalhes sobre o período de negociação que antecedeu o acordo, cf. Robert R. Schriver "You cheated, you lied: The safe harbor agreement and its enforcement by the Federal Trade Commission", p. 2788–2789.

[141] Cf. "US-EU Safe Harbor Frameworks" <disponível em http://www.export.gov/safeharbor/eu/eg_main_018476.asp, último acesso em 02.01.2017>.

[142] A lista com as empresas participantes pode ser encontrada no endereço https://safeharbor.export.gov/list.aspx

[143] Cf. Stephen J. Kobrin, "Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance", p. 121.

[144] Decisão 2000/520 da Comissão Europeia, de 26 de julho de 2000, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML

2.2.1. Princípios

O "Safe Harbor" foi idealizado com base no seguinte conjunto de sete princípios:

***(i)* notificação:** os indivíduos devem ser informados de forma clara e acessível a respeito dos propósitos para os quais suas informações são coletadas e utilizadas, sobre formas de contato para solicitar esclarecimentos e sanar eventuais dúvidas, sobre os terceiros com os quais suas informações são compartilhadas e sobre as suas opções para restringir tais atividades;

***(ii)* escolha:** deve ser garantida ao indivíduo a oportunidade de escolher se seus dados pessoais poderão ser compartilhados com terceiros e se eles poderão ser utilizados para finalidades diferentes daquelas para as quais tiverem sido originalmente coletados, com mecanismos efetivos de exercício desse poder de escolha ("opt out"); ***(iii)* restrição de transferências subsequentes:** para compartilhar dados pessoais coletados com terceiros, os responsáveis pela coleta devem ter notificado o indivíduo e dado a ele mecanismos efetivos para escolher que a transferência não ocorra ("opt out");

***(iv)* segurança:** os responsáveis pela coleta, tratamento e armazenamento de dados pessoais devem tomar precauções razoáveis para protegê-los do acesso, uso, alteração ou destruição desautorizados por terceiros;

***(v)* integridade dos dados:** os dados coletados devem ser precisos, completos, atualizados e necessários para se atender às finalidades para as quais foram originalmente coletados, não se admitindo o seu uso para finalidades distintas sem o consentimento do indivíduo;

***(vi)* acesso:** os indivíduos devem ter direito de acesso às informações pessoais que tenham sido coletadas e armazenadas a seu respeito, podendo exigir também a sua retificação, correção ou destruição em alguns casos;

***(vii)* reparação:** devem existir mecanismos efetivos de reparação para o caso de descumprimento das obrigações assumidas pelo responsável pela coleta e tratamento de dados pessoais, inclusive com a manutenção de documentos que possam comprovar o seu cumprimento caso seja necessário.[145]

A definição clara dos princípios era importante na medida em que determinava os termos de participação das empresas estadunidenses que, ao aderir ao programa se

[145] Cf. "US-EU Safe Harbor Framework: a guide to self-certification" <disponível em http://trade.gov/media/publications/pdf/safeharbor-selfcert2009.pdf, último acesso em 26.10.2016>.

declarando como empresas que protegiam a privacidade de seus usuários de forma "adequada", elas se comprometiam a seguí-los tal como estavam definidos nos termos do arranjo.

2.2.2. Fiscalização e sanções

Como se verá no capítulo seguinte, a fiscalização a respeito de violações ao *Safe Harbor* ficava a cargo da Comissão Federal do Comércio dos Estados Unidos. Por essa razão, só eram elegíveis para participar do arranjo as empresas cujas atividades estavam sob jurisdição da Comissão Federal do Comércio dos Estados Unidos ou do Departamento de Transporte dos Estados Unidos, como empresas ligadas a turismo e transporte aéreo. Empresas que desempenhassem atividades estranhas a esses órgãos, como instituições financeiras e operadoras de serviços de telecomunicações, dependiam das hipóteses previstas no artigo 26 para realizar operações que demandavam transferência internacional de dados pessoais, ou seja, a via da "adequação" estava fechada para elas.

Além da jurisdição da Comissão Federal do Comércio para fiscalizar o *Safe Harbor*, as autoridades de proteção de dados dos Estados-membros da União Europeia também tinham competência para tanto. Chris Hoofnagle destaca, entretanto, que apesar das inúmeras críticas e relatórios indicando deficiências na sua implementação por parte das empresas participantes, durante a vigência do *Safe Harbor*, nenhuma autoridade de proteção de dados pessoais europeia formalizou uma reclamação à Comissão Federal do Comércio dos Estados Unidos em relação a potenciais descumprimentos do arranjo.[146]

2.2.3. Críticas e limitações

Durante seus anos de vigência, o acordo sofreu diversas críticas, sobretudo no que tange à possibilidade de fiscalização e responsabilização efetiva de atores que não honrassem com suas obrigações de observar os princípios do acordo.

[146] Cf. Chris Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, p. 537.

Ao ser aprovado, o *Safe Harbor* foi recebido com ceticismo. Entre os acadêmicos, havia pouco consenso a respeito da efetividade dos mecanismos de sanção previstos. Graham Pearce e Nicholas Platten criticaram a forma genérica de definição de tais mecanismos, destacando a possível leniência da Comissão Federal de Comércio com potenciais violações de legislações estrangeiras.[147] Joel Reidenberg argumentava, por sua vez, que a Comissão Federal de Comércio não tinha sequer competência legal para atuar em casos envolvendo o arranjo, o que fragilizava o arranjo consideravelmente.[148]

Do lado das empresas, a incerteza a respeito de como seria feita a fiscalização e de quais mecanismos de sanção poderiam ser empregados fez com que, no início, poucas decidissem participar.[149] Além disso, a participação no arranjo era tida por algumas empresas como custosa, inexequível e injusta.[150]

Com o passar do tempo, entretanto, o número de empresas participantes foi aumentando, tendo chegado a 5.465 até a sua invalidação.[151] Apesar disso, por ser de participação voluntária e por se basear na mera declaração das empresas participantes, sem um sistema de verificação por parte do Departamento de Comércio ou mesmo da Comissão Federal do Comércio (de maneira preventiva), diversos estudos apontaram uma série de deficiências na sua implementação.

Em 2002, um relatório da Comissão Europeia concluiu serem insatisfatórias as notificações oferecidas pelas empresas estadunidenses, que se valiam de políticas de privacidade longas e pouco claras para legitimar práticas massivas de monitoramento e coleta de dados.[152] Em 2004, um outro estudo identificou uma tendência por parte das empresas de adotar políticas de privacidade com termos vagos e genéricos para evitar sanções por parte da Comissão Federal de Comércio, o que prejudicava a possibilidade de os usuários terem ciência das práticas de coleta efetivamente implementadas pelas

[147] Cf. Graham Pearce / Nicholas Platten, "Orchestrating transatlantic approaches to personal data protection: A European perspective", *Fordham Int'l LJ* 22 (1998), 2024.
[148] Cf. Joel R. Reidenberg, "Resolving conflicting international data privacy rules in cyberspace", *Stanford Law Review* 52 (2000), 1315, pp.738-744.
[149] Cf. Juliana Gruenwald, "Safe harbor, stormy waters", *Interactive Week* 7 (2000), 26, p.26 (ilustrando o receio das empresas estadunidenses em relação ao arranjo). Stephen Kobrin também anota que até o mês de maio de 2003 apenas 338 empresas tinham aderido ao Safe Harbor, o que acenaria para o fracasso do arranjo. Cf. Stephen J. Kobrin, "Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance", p. 121.
[150] Cf. James M. Assey / Demetrios A. Eleftheriou, "The EU-U.S. privacy safe harbor: Smooth sailing or troubled waters?", *J. Comm. L & Pol'y* 145 (2001), 158.
[151] A lista com as empresas participantes pode ser encontrada no endereço https://safeharbor.export.gov/list.aspx
[152] Cf. European Commission, "Staff working paper on the application of Commission decision 520/2000/EC of July 26, 2000 on the adequate protections of personal data provided by the safe harbor privacy principles", 2002.

empresas.[153] Em 2008, um novo relatório denunciava sérias violações por parte das empresas participantes; aproximadamente apenas 1/5 delas pareciam preencher os princípios básicos do arranjo.[154]

Em 2013, um comunicado da Comissão Europeia para o Parlamento Europeu resumiu as principais limitações enfrentadas pelo *Safe Harbor* em três categorias: *(i)* transparência das políticas de privacidade das empresas participantes, que ainda não ofereceriam mecanismos adequados de notificação; *(ii)* observância dos princípios do Safe Harbor por parte das empresas participantes; e *(iii)* inefetividade das ações de fiscalização e responsabilização.

2.2.4. A invalidação: Max Schrems

Antes mesmo de chegar aos trinta anos, Maximilian Schrems já pode ser considerado uma celebridade entre os defensores do direito à privacidade na Europa. Ganhador de prêmios que atestam sua notoriedade, como o "Privacy Champion Award" da organização estadunidense *Electronic Privacy Information Center* (EPIC), o "Internet and Society Award", do *Oxford Internet Institute* e o "EFF Pioneer Award", da *Electronic Frontier Foundation* (EFF), o cidadão austríaco estampou os noticiários pela primeira vez em 2011, em um caso envolvendo o Facebook.[155]

Na época, Max era estudante de direito e participava de um programa de intercâmbio na *Santa Clara University*, na Califórnia. A partir de uma atividade proposta em sala de aula, decidiu exercer o seu direito de acesso a dados armazenados a seu respeito, garantido pela legislação austríaca, enviando ao Facebook um pedido formal. Depois de alguns contatos com a empresa, Max recebeu um CD contendo mais de 1.200

[153] Cf. Jan Dhont et. al. "Safe harbour decision implementation study", *European Commission* (2004) <disponível em http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf, último acesso em 11.11.2016>.
[154] Cf. Chris Connolly, "The US Safe Harbor-Fact or Fiction?", *Galexia* (2008) <disponível em: <https://pdfs.semanticscholar.org/8615/66e450b7934012651f7657a35f3283c6b533.pdf, último acesso em 02.01.2017>.
[155] A repercussão do caso foi grande, tendo a cobertura de veículos importantes como o jornal britânico The Guardian. Cf. Helen Pidd, "Facebook could face €100,000 fine for holding data that users have deleted", *The Guardian* (20.10.2011) <disponível em: https://www.theguardian.com/technology/2011/oct/20/facebook-fine-holding-data-deleted, último acesso em 02.01.2017>.

páginas de informações pessoais armazenadas pela rede social. Mais surpreendente do que o volume de informações era o fato de que muitas das informações recebidas já haviam sido permanentemente deletadas, como mensagens e "cutucadas" (*pokes*), o que suscitou dúvidas a respeito de a empresa cumprir a legislação da Áustria.[156]

Diante disso, Max apresentou vinte e duas reclamações formais à autoridade de proteção de dados da Irlanda (*Data Protection Commissioner*), país onde o Facebook tem sede formal na União Europeia.[157] Além disso, fundou a organização "Europe v. Facebook", com o objetivo de arrecadar fundos para defender a privacidade dos cidadãos residentes na União Europeia, especialmente em relação às possibilidades de responsabilização de empresas estadunidenses por práticas que violam as garantias previstas na Diretiva 95 e nas legislações nacionais de proteção de dados pessoais.[158]

As reclamações formais enviadas foram objeto de uma auditoria promovida pela autoridade de proteção de dados da Irlanda, que culminou na elaboração de um relatório com uma série de recomendações de ajustes e mudanças nas políticas de privacidade da empresa.[159] Visando a alcançar uma solução amigável, representantes do Facebook se reuniram com Max em Viena no dia 06 de fevereiro de 2012.[160] Após a reunião, a empresa anunciou mudanças em suas políticas, seguindo recomendações do relatório apresentado.[161]

Insatisfeito com as mudanças realizadas, que ainda estavam aquém de suas expectativas, e com a condução do processo pela autoridade de proteção de dados da Irlanda, que teria impedido o acesso a documentos apresentados pelo Facebook e considerado as alterações implementadas como suficientes, Max retirou as reclamações em 2014, quando já transcorriam outras medidas que ajuizara em decorrência das denúncias

[156] Cf. Cyrus Farivar, "Facebook now gives all new users a privacy tutorial, thanks to Irish authorities", *Ars Technica* (2012) <disponível em: http://arstechnica.com/business/2012/11/facebook-now-gives-all-new-users-a-privacy-tutorial-thanks-to-irish-authorities/, útlimo acesso em 02.01.2017>.
[157] Uma lista completa contendo as vinte e duas reclamações, na íntegra, está disponível em http://europe-v-facebook.org/EN/Complaints/complaints.html
[158] Cf. http://europe-v-facebook.org/EN/Objectives/objectives.html
[159] Data Protection Commissioner, "Facebook Ireland Ltd, Report of Audit" (2001) <disponível em http://europe-v-facebook.org/Facebook_Ireland_Audit_Report_Final.pdf, último acesso em 28.10.2016>.
[160] Para detalhes a respeito dos principais argumentos abordados na reunião, cf. Summary of Arguments: meeting of "europe-v-facebook.org" with Facebook representatives, disponível em http://www.europe-v-facebook.org/Summary_of_Arguments_VIE.pdf, último acesso em 28/10/2016.
[161] Cf. Cyrus Farivar, "Facebook now gives all new users a privacy tutorial, thanks to Irish authorities".

feitas pelo ex-agente da Agência Central de Inteligência dos Estados Unidos (CIA), Edward Snowden.[162]

Snowden teria revelado a existência de um aparato de vigilância implementado pela Agência de Segurança Nacional dos Estados Unidos (NSA) que contava com a suposta colaboração das maiores empresas do setor de Internet ("Programa Prism"). De acordo com as denúncias, o programa permitiria o repasse direto de informações coletadas pelas empresas de Internet, como Facebook e Yahoo!, para a Agência de Segurança Nacional. Os dados seriam coletados diretamente dos servidores dessas empresas, o que corroboraria o esquema de colaboração.[163]

A partir das revelações, Max decidiu ajuizar cinco reclamações perante as autoridades de proteção de dados de três países: Irlanda, Luxemburgo e Alemanha, países sede das empresas demandadas na União Europeia, quais sejam Apple, Facebook, Skype, Microsoft e Yahoo!.[164] Nas reclamações, solicitava que as autoridades investigassem potenciais violações cometidas pelas empresas a partir de seu suposto envolvimento com o programa PRISM.[165]

O principal argumento seria o de que o repasse de informações de cidadãos residentes na União Europeia à Agência de Segurança Nacional dos Estados Unidos pelas empresas de Internet violaria o critério de "proteção adequada", exigido pela Diretiva 95 para a transferência internacional de dados pessoais. Nesse sentido, questionou a validade do *Safe Harbor*, sob o qual essas transferências internacionais de dados estariam sendo legitimadas.[166]

---

[162] Max Schrems esclarece que a retirada das reclamações se deveu aos custos elevados de judicializá-las. Cf. Max Schrems, "Legal procedure against 'Facebook Ireland Limited'", *Europe versus Facebook* (2016) <disponível em http://europe-v-facebook.org/EN/Complaints/complaints.html, último acesso em 29.10.2016>.

[163] Cf. James Ball, "NSA's Prism surveillance program: how it works and what it can do", *The Guardian* (08.06.2013) <disponível em https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google, último acesso em 29.10.2016>.

[164] Cf. Max Schrems, "PRISM Complaints against Facebook, Apple, Skype, Microsoft and Yahoo!", *Europe versus Facebook* (2016) <disponível em http://europe-v-facebook.org/EN/Complaints/complaints.html, último acesso em 29.10.2016>.

[165] Além das cinco reclamações, que posteriormente deram origem ao Caso C-362/14 perante o Tribunal de Justiça da União Europeia, Max Schrems ajuizou, em 2014 uma ação coletiva em face do Facebook, em busca de indenização pelas violações supostamente cometidas. Mais de 17 mil pessoas se juntaram ao austríaco. Para uma lista completa dos documentos pertinentes, cf. Max Schrems, "Facebook Class Action", <disponível em https://www.fbclaim.com/ui/page/updates, último acesso em 29.10.2016>. Cf. também Juliette Garside, "More than 17,000 sign up to Austrian student's Facebook privacy class action", *The Guardian* (05.08.2014) <disponível em https://www.theguardian.com/technology/2014/aug/05/sign-up-austrian-student-facebook-class-action-data-violations, último acesso em 29/10/2016>.

[166] Cf. íntegra da reclamação em relação ao Facebook http://www.europe-v-facebook.org/prism/facebook.pdf

As reclamações feitas às autoridades de proteção de dados de Luxemburgo e da Alemanha não prosperaram mas aquelas endereçadas à autoridade de proteção de dados da Irlanda sim (em face das empresas Apple e Facebook).[167] Levado à Alta Corte da Irlanda, em decisão do dia 16 de julho de 2014, o caso foi remetido para apreciação do Tribunal de Justiça da União Europeia ("TJUE").[168]

2.2.4.1. Decisão do Tribunal de Justiça da União Europeia

A principal questão examinada pelo TJUE consistia em determinar se o *Safe Harbor*, consubstanciado pela Decisão 2000/520, por meio da qual a Comissão Europeia passava a considerar as empresas estadunidenses aderentes ao acordo como garantidoras de um nível de proteção "adequada" da privacidade, nos termos do artigo 25 da Diretiva 95, impediria a apreciação de violações decorrentes de transferências internacionais de dados pessoais realizadas por essas mesmas empresas por autoridades de proteção de dados dos Estados-membros.[169] Em outras palavras, o TJUE foi instado a decidir sobre a validade do *Safe Harbor* na medida em que, se decidisse pela possibilidade de responsabilização dessas empresas por transferências internacionais de dados pessoais realizadas nos termos da Decisão 2000/520, estaria anulando as garantias que a participação no acordo representava para as empresas participantes.

Ao apreciar a questão, o TJUE chegou à conclusão de que, para ser considerado país de destino que garanta nível de proteção adequado para transferência internacional de dados pessoais oriundos da União Europeia, nos termos do artigo 25 da Diretiva 95, os Estados Unidos deveriam ter tais níveis de proteção consubstanciados em sua legislação interna ou em tratados internacionais vinculantes. Nesse sentido, como a Decisão 2000/520 da Comissão Europeia toma como base princípios elaborados pelo Departamento de Comércio nos Estados Unidos, de aderência voluntária pelas empresas, e que não se

[167] Cf. http://europe-v-facebook.org/EN/Complaints/Safe_Harbor/safe_harbor.html

[168] Caso C-362/14; uma lista completa dos documentos disponíveis pode ser encontrada em http://europe-v-facebook.org/EN/Complaints/Safe_Harbor/safe_harbor.html. Cf. Judicial Review Case n. 2013/765JR, The High Court, Irlanda, disponível em http://www.europe-v-facebook.org/Order_ADJ.pdf

[169] Cf. parágrafo 37 da decisão C-362/14, disponível em http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30ddbb8c0c2b301a4ad08e2d83c41bc63c36.e34KaxiLc3qMb40Rch0SaxuRbxb0?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=253155, último acesso 29/10/2016.

encontram positivados em textos normativos vinculantes, ela não seria suficiente para garantir o cumprimento do artigo 25 da Diretiva 95 e autorizar a transferência internacional de dados pessoais para os Estados Unidos.[170]

Sendo assim, em 06 de outubro de 2015, o TJUE invalidou a Decisão 2000/520, o que pôs fim ao mecanismo de funcionamento do acordo *Safe Harbor*, que dependia da validade da decisão para garantir o cumprimento do artigo 25 da Diretiva 95.

2.2.4.2. *Privacy Shield*

Com o *Safe Harbor* invalidado, Estados Unidos e União Europeia iniciaram as negociações para a elaboração de um novo sistema que possibilitasse a transferência de dados entre as duas regiões. Em 12 de julho de 2016, foi anunciada a aprovação de uma versão reformulada do arranjo (*Privacy Shield*). Comparado com o *Safe Harbor*, pouca coisa mudou em relação ao sistema de auto-declaração das empresas, que continuam tendo que certificar sua "adequação" aos níveis de proteção europeus com base nos mesmos sete princípios anteriormente adotados.

A diferença principal do acordo está na exigência de mecanismos de fiscalização por parte do Departamento de Comércio dos Estados Unidos e da Comissão Federal de Comércio em relação ao cumprimento dessas certificações, além de abrir espaço para formas mais eficazes de reclamação e denúncias de violação por parte dos cidadãos europeus, o que ainda não ficou bem definido. Desde 01 de agosto de 2016, o Departamento de Comércio dos Estados Unidos está aceitando as certificações em conformidade com o novo acordo.

Da mesma forma como não importava a este capítulo proceder a uma análise pormenorizada do RGPD, pelo fato de que sua entrada em vigência só acontecerá em 2018, o mesmo pode ser dito em relação ao *Privacy Shield* que, embora já esteja em vigor, ainda representa uma iniciativa muito incipiente, sem nos permitir extrair dessa breve experiência conclusões muito significativas sobre a efetividade das mudanças introduzidas.

[170] Cf. parágrafos 68 a 106 da decisão de 06 de outubro de 2015 do caso C-362/14.

Diante do exposto neste capítulo, é possível concluir que *(i)* os modelos regulatórios de privacidade adotados nos Estados Unidos e na União Europeia foram construídos a partir de valores fundantes significativamente distintos; enquanto, no caso do primeiro, há uma maior deferência à livre concorrência de mercado e uma aposta na auto-regulação, no segundo, prevalecem acepções ligadas ao valor social da privacidade e sua relação com princípios como o da dignidade humana (autodeterminação informacional); *(ii)* a experiência com o *Safe Harbor* demonstra que arranjos normativos que pretendam viabilizar a transferência internacional de dados entre regiões que adotam modelos regulatórios diferentes devem vir acompanhados de mecanismos jurídicos efetivos de fiscalização e responsabilização de atores sediados em outros territórios, sob pena de se tornarem inócuos; *(iii)* o critério da auto-declaração de empresas em relação à aderência e cumprimento de princípios de proteção à privacidade exige uma atuação rigorosa por parte do órgão fiscalizador, sob pena de se traduzir em uma forma ilusória de compatibilidade; (iv) mesmo com o poderio econômico da União Europeia, o *Safe Harbor* vigorou por mais de quinze anos sem poder ser considerado um mecanismo eficiente de interoperabilidade[171], o que acentua as preocupações em relação à possibilidade de serem implementados arranjos similares e aprimorados em relação a outros países ou regiões que não tenham um poder econômico de pressão e barganha tão considerável.

[171] O conceito de "interoperabilidade normativa" pode oferecer diretrizes para o desenvolvimento de mecanismos de governança que pretendam superar dificuldades de compatibilização entre normas. Para tanto, componentes e aspectos variados, como os tecnológicos e os ligados a instituições podem ser conjugados para facilitar a integração entre sistemas jurídicos e modelos regulatórios distintos. Para uma discussão a respeito da aplicação do conceito ao caso da proteção de dados pessoais, cf. Urs Gasser, Perspectives on the Future of Digital Privacy, 134 Zeitschrift für Schweizerisches Recht [ZSR], 2015, p. 444-446.

CAPÍTULO 3 - A COMISSÃO FEDERAL DO COMÉRCIO DOS ESTADOS UNIDOS: TUTELANDO INTERESSES DE QUEM?

No capítulo anterior, demonstrou-se de que forma as diferenças entre os modelos regulatórios de privacidade adotados nos Estados Unidos e na União Europeia dificultam a compatibilização entre as duas regiões, sobretudo no que diz respeito ao fluxo internacional de dados. Nesse ponto, a implementação do *Safe Harbor* foi essencial para legalizar a transferência de dados de cidadãos residentes na União Europeia para os Estados Unidos, onde estão sediadas muitas empresas do setor de Internet.

Com o arranjo, a expectativa era a de superar os obstáculos jurídicos de compatibilização impostos pela Diretiva 95, viabilizando o livre trânsito de dados e informações pessoais na Internet, como seria próprio de sua arquitetura. No entanto, como se viu, o *Safe Harbor* contava com mecanismos limitados de sanção e fiscalização de cumprimento, que ficavam concentrados na Comissão Federal de Comércio dos Estados Unidos.

Pelo papel preponderante que ocupa dentro do modelo regulatório de privacidade dos Estados Unidos, sendo responsável pela manutenção e funcionamento das medidas de auto-regulação, a Comissão se consolidou como uma das vias mais importantes de fiscalização e responsabilização das empresas estadunidenses em relação a violações de privacidade.

O objetivo deste capítulo é o de refletir sobre a forma como a Comissão tem desempenhado essa função, especialmente no que tange às suas prerrogativas de responsabilização de empresas estadunidenses por violações cometidas em outras jurisdições.

Para tanto, serão analisados *(i)* os limites de competência da Comissão, *(ii)* a evolução de sua jurisprudência, que sedimentou um conjunto de regras aplicáveis à coleta e tratamento de dados de usuários por empresas do setor de Internet baseadas nos princípios de notificação e escolha; *(iii)* a sua atuação como órgão fiscalizador do *Safe Harbor*.

3.1. Competência e escopo de atuação

A Comissão Federal do Comércio dos Estados Unidos ("Comissão") foi criada em 1914 e é composta por 5 conselheiros, indicados pelo presidente da república com aprovação do Senado, para mandatos de sete anos.[172] Instituída para atuar em temas ligados à concorrência, a Comissão conquistou posição de destaque na defesa dos direitos do consumidor a partir da década de 70, sobretudo por conta de casos envolvendo propaganda enganosa.[173]

A Internet chamou a atenção da Comissão desde o início. Especificamente no caso do direito à privacidade, em 1995, foram organizados os primeiros encontros sobre o tema, que culminaram na publicação de um relatório no ano seguinte.[174] O ano de 1997 inaugura a atuação fiscalizatória da Comissão na área, com o caso envolvendo a página *KidsCom*.[175]

O rápido envolvimento da Comissão com o tema não foi injustificado. De acordo com Chris Hoofnagle, ele foi resultado da pressão do congresso estadunidense, preocupado com o regime de proteção de dados adotado na União Europeia, que proibia a transferência de dados de cidadãos europeus para países que não oferecessem proteções adequadas, tal como se explorou no capítulo anterior.[176]

Desde então, a Comissão foi ganhando espaço na tutela do direito à privacidade dos usuários de Internet nos Estados Unidos com base na sua competência para fiscalizar e atuar em casos envolvendo práticas desleais (*unfair*) ou enganosas (*deceptive*), prevista na Seção 5 da lei que institui a Comissão. Da forma como está delimitada, a competência da Comissão abrange praticamente todas as relações jurídicas de consumo, com algumas poucas exceções.[177]

---

[172] H.R. 15613, Public Law no. 63-203 §§ 6501-6506.
[173] Cf. Chris Hoofnagle, Federal Trade Commission Privacy Law and Policy, Cambridge University Press, p. 57-60 (comentando a atuação mais agressiva na área por parte da Comissão a partir da nomeação do conselheiro Miles Kirkpatrick como seu presidente).
[174] Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure | Federal Trade Commission, disponível em: <https://www.ftc.gov/reports/staff-report-public-workshop-consumer-privacy-global-information-infrastructure>, último acesso em 10/07/2016.
[175] Cf. Chris Hoofnagle, Federal Trade Commission Privacy Law and Policy, p. 157.
[176] Cf. Chris Hoofnagle, Federal Trade Commission Privacy Law and Policy, p. 157.
[177] 15 USC § 45 (5) (a) (2): "A Comissão fica habilitada e direcionada a impedir que pessoas, entidades ou corporações, exceto bancos, instituições de poupança e empréstimos descritas na seção 57a (f) (3) deste título, as cooperativas de crédito federais descritas na seção 57a (f) (4) deste título, entidades comuns sujeitas às leis de regulamentação do comércio, as companhias aéreas e companhias aéreas estrangeiras sujeitas à parte A do subtítulo VII do título 49, e pessoas, entidades ou corporações na medida em que estejam sujeitos

A abrangência da competência da Comissão para apreciar casos envolvendo violações do direito à privacidade foi recentemente contestada judicialmente. No caso envolvendo a rede de hotéis Wyndham, em face de quem a Comissão ajuizara uma ação por danos causados por uma falha de segurança em sua rede de computadores, que teria permitido que informações de hóspedes fossem acessadas, sem autorização, por terceiros, questionou-se se a Seção 5 abarcaria a competência de regular os padrões de segurança de dados de entidades comerciais. Em 24 de agosto de 2015, o Tribunal de Apelações do Terceiro Circuito julgou a demanda, confirmando a competência da Comissão para atuar nesses casos.[178] O caso consolidou a ampla competência da Comissão para atuar em casos envolvendo a privacidade dos consumidores.

3.1.1. Práticas desleais

Analisando de maneira minuciosa a jurisprudência[179] da Comissão, Daniel Solove e Woodrow Hartzog dividem em cinco as principais teses referentes a circunstâncias que podem ser consideradas como práticas desleais no que diz respeito à privacidade: *(i)* mudanças retroativas de políticas de privacidade; *(ii)* práticas clandestinas de coleta de dados; *(iii)* uso impróprio dos dados coletados; *(iv)* arquitetura desleal; e *(v)* práticas desleais de segurança de dados.[180]

Em relação às mudanças de políticas de privacidade de forma retroativa, a jurisprudência da Comissão condena alterações na forma de tratamento de dados e

---

ao Ato de embalagens e estoques, 1921, conforme alterado [7 U.S.C. 181 et seq.], exceto nos casos previstos na seção 406 (b) da referida Lei [7 U.S.C. 227 (b)], da utilização de métodos desleais de concorrência no ou que afetem o comércio e práticas ou atos desleais ou enganosos no ou que afetam o comércio". (tradução livre)

[178] Cf. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

[179] No plano administrativo, os procedimentos de investigação e reclamação (*complaints*) da Comissão podem culminar na homologação de acordos, que são consubstanciados em *consent orders*. Essas ordens operam como se fossem contratos estabelecidos entre as partes (o que, no direito brasileiro, equivaleria aos termos de ajustamento de conduta) e não tem força vinculante em relação a outros casos. Ainda assim, na prática, Daniel Solove e Woodrow Hartzog alertam para o fato de serem encaradas como verdadeiros "precedentes" pelas empresas. Por essa razão, apesar de essas ordens não constituírem um corpo vinculante de decisões, parece-nos adequado utilizar o termo "jurisprudência" para se referir a elas. Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, *Columbia Law Review*, p. 583–676, 2014, p. 607.

[180] Cf. Daniel Solove e Woodrow Hartzog, The FTC and the new common law of privacy, p. 638–643.

informações previamente coletados, que se submetiam a outras políticas.[181] Além de um dever de notificar o usuário a respeito de quaisquer mudanças significativas nos termos de suas políticas de privacidade, as empresas não devem aplicá-las de forma retroativa, sob pena de serem responsabilizadas por uma prática desleal.[182]

Em relação às práticas clandestinas de coleta de dados, a Comissão construiu entendimento no sentido de serem consideradas desleais práticas de coleta massiva de dados de forma silenciosa ou invisível, restringindo as possibilidades de resistência dos usuários, ainda que isso não signifique a violação dos termos de suas políticas de privacidade.[183]

Em relação ao uso impróprio de dados coletados, em vários casos a Comissão considera desleal a sua utilização para finalidades diferentes daquelas originalmente previstas e consentidas pelo usuário.[184] Por exemplo, a Comissão considerou desleal a utilização de endereços de e-mail coletados em desconformidade com os termos de uso e políticas de privacidade do serviço de leilão virtual eBay para o envio de mensagens publicitárias sem consentimento (*spam*).[185]

Em relação à arquitetura desleal, a jurisprudência da Comissão considera que a implementação de mecanismos técnicos ou de configurações padrão são desleais se estiverem em desacordo com as expectativas razoáveis de privacidade dos consumidores. Por exemplo, em *FTC v. Frostwire LLC*, a Comissão condenou a arquitetura do sistema, que disponibilizava para compartilhamento público arquivos armazenados no dispositivo dos consumidores.[186]

Por fim, em relação à segurança de dados, a Comissão tem uma atuação destacada no sentido de condenar a não adoção de medidas adequadas ou razoáveis para a proteção de dados coletados de consumidores, ainda que as políticas de privacidade do responsável pela coleta não disponham sobre essa obrigação.[187]

---

[181] Cf. Daniel Solove e Woodrow Hartzog, The FTC and the new common law of privacy, p. 638–643.
[182] Cf. Gateway Learning Corp., 138 F.T.C. 443, 470 (2004).
[183] Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 641 (citando Aspen Way Enters., Inc., F.T.C 112 3151, 2013).
[184] Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 642.
[185] Cf. FTC v. ReverseAuction.com, 2000.
[186] Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 642-643.
[187] Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 643.

3.1.2. Práticas enganosas

Também com base em sua análise da jurisprudência da Comissão, Daniel Solove e Woodrow Hartzog identificaram quatro teses principais de práticas consideradas enganosas em relação à privacidade: *(i)* quebra de promessas de privacidade; *(ii)* práticas enganosas de forma geral; *(iii)* notificação insuficiente; e *(iv)* segurança de dados.[188]

A quebra de promessas de privacidade é um dos principais pilares de atuação da Comissão. Isso porque, na ausência de uma legislação de proteção de dados pessoais, as empresas têm maior liberdade na definição de suas próprias políticas de privacidade. Nesse sentido, a Comissão entendeu como seu papel fiscalizar o cumprimento das configurariam práticas enganosas.

Daniel Solove e Woodrow Hartzog dão exemplos dos tipos mais comuns de promessas de privacidade fiscalizadas pela Comissão: *(i)* promessas de não transferir os dados coletados a terceiros; *(ii)* promessas de coletar apenas os dados mencionados nas políticas de privacidade; *(iii)* promessas de implementar medidas adequadas para garantir a segurança dos dados coletados; *(iv)* promessas de manter os dados armazenados de forma anônima; *(v)* promessas de não compartilhamento de dados com terceiros em casos de fusão e aquisição, especialmente em procedimentos de falência.[189]

Além dos casos de quebra de promessas de privacidade, a Comissão também desenvolveu teses no sentido de responsabilizar empresas por práticas enganosas de forma geral. Nesses casos, a Comissão costuma condenar atos que instiguem ou induzam os consumidores a fornecer dados pessoais, independentemente dos termos das suas políticas de privacidade. A Comissão condenou, por exemplo, várias empresas que mascaravam o envio e instalação de *software* de monitoramento e espionagem (*spyware*) nos dispositivos dos usuários.[190]

A jurisprudência da Comissão também se debruçou sobre as formas de notificação oferecidas aos consumidores. Como visto no capítulo anterior, os princípios de "notificação" e "escolha", presentes nos FIPP, constituem o alicerce de todo o sistema de auto-regulação de privacidade nos Estados Unidos. Dessa forma, a atuação da Comissão é

[188] Cf. Cf. Daniel Solove e Woodrow Hartzog, The FTC and the new common law of privacy, p.628–638.
[189] Cf. Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 628-629.
[190] Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 630-634.

firme no sentido de exigir que os consumidores recebam informações adequadas e suficientes a respeito das atividades de coleta e tratamento de dados pessoais. Em inúmeros casos, a Comissão repreendeu alterações substanciais dos termos das políticas de privacidade desacompanhadas de mecanismos eficientes de notificação.[191] Por essa razão, tornou-se praxe, por exemplo, entre as empresas do setor de Internet, a adoção de medidas para anunciar alterações em suas políticas de privacidade, como o envio de *e-mails*.[192]

Por fim, a Comissão tem sólida jurisprudência exigindo a implementação de medidas que garantam a segurança dos dados coletados. Daniel Solove e Woodrow Hartzog anotam, inclusive, que ao longo dos anos 2000, a Comissão deu prioridade a casos de violações dessa natureza.[193]

3.1.3. Cooperação Internacional

Tendo assumido o papel de "autoridade de proteção de dados *de facto*"[194], a Comissão se tornou a responsável não só pelas investigações referentes à privacidade no âmbito nacional, como também principal ponto de contato de autoridades estrangeiras que dependiam de auxílio na investigação e responsabilização de atores localizados nos Estados Unidos.

Nesse sentido, a Comissão passou a estruturar suas atividades no plano internacional também em relação à proteção da privacidade dos consumidores. Chris Hoofnagle identifica as seguintes funções principais desempenhadas pela Comissão no plano internacional: *(i)* prestar e receber assistência de autoridades internacionais; *(ii)* apoiar outros países no desenvolvimento de regimes regulatórios envolvendo concorrência

[191] Cf. Facebook, Inc., FTC File No. 092 3184, No. C-4365 (2012)
[192] Como exemplos, pode-se citar o anúncio divulgado pelas empresas WhatsApp e Spotify a respeito de alterações realizadas em suas políticas de privacidade. Cf. WhatsApp anuncia que passará a compartilhar dados com o Facebook - WhatsApp, Canaltech, disponível em: <https://canaltech.com.br/noticia/whatsapp/whatsapp-anuncia-que-passara-a-compartilhar-dados-com-o-facebook-77997/>, acesso em: 23/12/2016. Cf. também Claudia Tozzetto, Spotify impõe renúncia ao sigilo bancário em nova política de privacidade, O Estado de São Paulo, disponível em http://link.estadao.com.br/noticias/cultura-digital,spotify-impoe-renuncia-ao-sigilo-bancario-em-nova-politica-de-privacidade,10000096090, último acesso em 23/12/2016.
[193] Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 637-638.
[194] Nomenclatura proposta por Daniel Solove e Woodrow Hartzog. Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 609.

e a proteção de consumidores; *(iii)* disseminar informações a respeito do modelo regulatório de privacidade adotado nos Estados Unidos; *(iv)* fiscalizar o cumprimento de acordos como era o caso do *Safe Harbor*.[195]

Dentro da perspectiva de atuação internacional da Comissão, Dina Kallay e Marc Winerman assinalam a aprovação do "SAFE WEB Act" e a instituição do "Office of International Affairs" como marcos da última década.[196]

3.1.3.1. U.S. SAFE WEB Act

Atenta ao crescimento de operações e esquemas fraudulentos envolvendo atores localizados fora dos Estados Unidos, a partir de 2001, a Comissão começou a defender, no âmbito do Poder Legislativo, a necessidade de aprimoramento das suas capacidades de cooperação e assistência internacional.[197] Em 2005, a Comissão enviou uma recomendação ao Congresso, sugerindo a adoção de legislação nesse sentido.[198]

Em 22 de dezembro de 2006, foi sancionado pelo presidente George W. Bush o chamado "Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers Beyond Borders Act", que se convencionou chamar de "US SAFE WEB Act".

A legislação ampliou significativamente as capacidades de investigação e cooperação internacional da Comissão, introduzindo quatro modificações principais que importam para o objeto de estudo desta tese: *(i)* ampliação da capacidade de compartilhamento de informações[199]; *(ii)* ampliação da capacidade de prestar assistência internacional para investigação[200]; *(iii)* confirmação da jurisdição da Comissão em relação

[195] Cf. Chris Hoofnagle, Federal Trade Commission Privacy Law and Policy, p. 521.
[196] Cf. Dina Kallay / Marc Winerman, First in the World: The FTC International Program at 100, Antitrust 39, vol. 29, 1, 2014, p. 5.
[197] Cf. Federal Trade Commission, The U.S. Safe Web Act: The First Three Years - A report to Congress, 2009, p.2.
[198] Cf. FED. TRADE COMM'N, THE US SAFE WEB ACT: PROTECTING CONSUMERS FROM SPAM, SPYWARE AND FRAUD—A LEGISLATIVE RECOMMENDATION TO CONGRESS (2005), disponível em http://www.ftc.gov/sites/default/files/documents/ reports/us-safe-web-act-protecting-consumers-spam-spyware-and-fraudlegislative-recommendation-congress/ussafeweb.pdf.
[199] Cf. US SAFE WEB Act §§ 4(a), 6(a).
[200] Cf. US SAFE WEB Act § 4(b).

a casos internacionais de reparação[201]; *(iv)* ampliação das capacidades de cooperação entre a Comissão e o Departamento de Justiça em casos contenciosos[202].

No primeiro caso, a Comissão ficou autorizada a compartilhar com autoridades estrangeiras informações confidenciais obtidas no curso de investigações. Antes da aprovação da lei, a Comissão só tinha poderes para compartilhar essas informações com outras autoridades estadunidenses. A mudança abriu caminho para que se estabelecessem laços muito mais efetivos de cooperação entre a Comissão e autoridades estrangeiras, como as autoridades de proteção de dados pessoais de outros países.

No segundo caso, a Comissão ficou autorizada a conduzir investigações e diligências em nome de autoridades estrangeiras, auxiliando-as na obtenção de informações referentes a empresas sediadas nos Estados Unidos. Isso possibilitou que, em contrapartida, a Comissão recebesse auxílio de autoridades estrangeiras na investigação e obtenção de dados referentes a atores sediados em seus respectivos países.

No terceiro caso, ficou expressamente confirmada a competência da Comissão para processar e executar ações de reparação por danos causados nos Estados Unidos por atores localizados no exterior e também para processar e executar ações de reparação por danos causados no exterior por atores localizados nos Estados Unidos. Isso ajudou a evitar questionamentos protelatórios acerca da competência da Comissão para atuar nesses casos, incluindo perante o poder judiciário de outras jurisdições.

Por fim, no quarto caso, a Comissão ficou autorizada a receber assistência e recursos adicionais, financeiros e de pessoal, do Departamento de Justiça dos Estados Unidos para atuar em litígios no exterior. Isso possibilitou que o Departamento de Justiça agisse a pedido da Comissão para bloquear bens ou iniciar procedimentos de execução de ordens judiciais obtidas pela Comissão no exterior, o que facilita a atuação da Comissão fora da jurisdição estadunidense.

3.2. Limites de atuação

Apesar de desempenhar papel importante como órgão fiscalizador dentro do modelo regulatório estadunidense, como se viu acima, a Comissão sofre uma série de

[201] Cf. US SAFE WEB Act § 3.
[202] Cf. US SAFE WEB Act § 5.

críticas.[203] Para os fins desta tese, importa analisar aquelas referentes à possibilidade de a Comissão atuar na responsabilização de atores privados sediados nos Estados Unidos que possam estar agindo em desconformidade com as normas constitucionais e legislações de proteção de dados vigentes em outras jurisdições.

Nesse sentido, são três os pontos a considerar: *(i)* a atuação da Comissão está adstrita à sua missão de proteger o mercado e a livre concorrência, o que se traduz numa proteção da privacidade com base no "dano"; (ii) a discricionariedade na seleção de casos e temas a serem investigados dá margem para a interferência de interesses políticos na definição da agenda de atuação da Comissão; (iii) a jurisprudência da Comissão cristaliza os princípios de notificação e escolha, sedimentando o modelo de auto-regulação, o que confere discricionariedade para que as empresas definam suas próprias políticas de privacidade, respeitadas algumas regras consolidadas nos entendimentos da Comissão.

3.2.1. A fiscalização à serviço do comércio

Em primeiro lugar, cumpre destacar que a Comissão é um órgão ligado ao comércio e que, portanto, sua competência depende da existência de uma relação consumerista.[204] Ainda que essa competência seja conferida de forma bastante ampla e abranja relações que não envolvam pagamento direto pela prestação de um serviço ou pelo oferecimento de um produto, como é o caso de muitas relações estabelecidas entre usuários e empresas de Internet, esse já é um primeiro obstáculo para a atuação da Comissão.

Além disso, como mencionado nos itens anteriores, a Seção 5 institui a competência da Comissão para coibir práticas desleais ou enganosas e é o fundamento para as suas investigações e sanções no caso da privacidade. Sendo assim, a Comissão só pode agir caso se depare com práticas ou políticas que violem as legislações setoriais dos Estados Unidos ou que possam ser consideradas como desleais ou enganosas na linha da

[203] Por exemplo, a grande maioria das críticas atribuídas ao mau funcionamento dos mecanismos de sanção e fiscalização do *Safe Harbor* se dirige à atuação da Comissão. Para um resumo desses posicionamentos, cf. Graham Pearce / Nicholas Platten, Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective, Fordham Int'l LJ, v. 22, 1998, p. 2024.

[204] Cf. Chris Hoofnagle, US Regulatory Values and Privacy Consequences: Implications for the European Citizen, p.6.

jurisprudência que construiu ao longo de seus anos de atuação, sintetizadas nos itens anteriores.

Ao mesmo tempo em que essa competência pode parecer ampla o suficiente para abarcar novos entendimentos a respeito de práticas desleais ou enganosas, é preciso lembrar que ela está inserida e, portanto, limitada ao próprio âmbito de atuação da Comissão, que é o de proteger o mercado e a livre concorrência. É nesse exato sentido, anota Chris Hoofnagle, que a atuação da Comissão se volta para a proteção dos consumidores: coibindo práticas que possam se traduzir em formas de concorrência desleal.[205] Isso engloba as ações encampadas pela Comissão no caso do direito à privacidade.

Como se demonstrou no capítulo anterior, em modelos regulatórios de privacidade adotados em outras regiões, como na União Europeia, por exemplo, há uma tutela normativa desse direito, que está baseada em valores como a dignidade da pessoa humana e não na mera proteção do mercado e da livre concorrência. Nesses modelos, as violações ao direito à privacidade são coibidas independentemente de eventuais implicações para o direito econômico ou concorrencial. No caso da Comissão, isso não acontece.[206]

Na prática, isso significa que a atuação da Comissão em casos envolvendo privacidade depende da existência de um dano material.[207] Isso repercute significativamente nos tipos de casos encampados pela Comissão, que precisam vir acompanhados de uma fundamentação econômica robusta. Para tanto, a Comissão conta com um "Departamento de Economia" ("Bureau of Economics"), formado por um corpo de aproximadamente trinta economistas que avaliam a pertinência de casos envolvendo a proteção de consumidores.

Ao tomar o "dano" como métrica, os membros do Departamento de Economia acabam excluindo uma série de casos relevantes para o tema da privacidade, o que se justifica pelo próprio fato de o "dano ligado à privacidade" ("privacy harm") não ser algo

[205] Cf. Chris Hoofnagle, US Regulatory Values and Privacy Consequences: Implications for the European Citizen, 2 (2) European Data Protection Law Review 169 (2016), disponível em http://edpl.lexxion.eu/issue/EDPL/2016/2

[206] Nas palavras de Chris Hoofnagle, "A Comissão Federal do Comércio não protege a privacidade como um valor normativo." (tradução livre). Cf. Chris Hoofnagle, US Regulatory Values and Privacy Consequences: Implications for the European Citizen, p.2.

[207] Chris Hoofnagle esclarece que isso decorre de exigências legais e de pressões políticas. No caso de práticas desleais, é necessário que exista um "dano substancial". No caso das práticas enganosas, esse dano precisa ter assumido uma dimensão "material". Cf. Chris Hoofnagle, US Regulatory Values and Privacy Consequences: Implications for the European Citizen, p.3.

simples de se definir.[208] Ao enfrentar a questão, Ryan Calo identifica duas categorias distintas de danos ligados à privacidade: a subjetiva e a objetiva. Na primeira, o dano se configuraria pela intromissão na vida privada, o que pode gerar sensações indesejadas e desconfortos psicológicos, como ansiedade, medo e vergonha. Na segunda, o dano se caracterizaria pelo uso imprevisível ou desautorizado de informações pessoais contra o seu titular, geralmente causando externalidades negativas, como nos casos de roubo de identidade ou vazamento de informações confidenciais.[209]

A taxonomia proposta por Ryan Calo ajuda a ilustrar situações nas quais a ausência ou dificuldade de se demonstrar um dano *material* à privacidade poderia impedir a atuação da Comissão. Afinal, como atribuir um dano material a perturbações no plano subjetivo, psicológico?

Essas limitações de competência e de escopo de atuação, justificadas pela missão da Comissão de proteger o comércio e garantir a livre concorrência, moldam a sua jurisprudência, que, portanto, distancia-se de entendimentos que encarariam a proteção da privacidade como um direito fundamental ou como um valor ligado ao conceito de dignidade da pessoa humana, reforçando o abismo entre os valores fundantes do modelo regulatório estadunidense e o europeu.

3.2.2. Discricionariedade na seleção de casos e interferência política

Para além das limitações descritas no item acima, há uma importante dimensão política que interfere na atuação da Comissão.[210] Pressões vindas do Congresso ou do Poder Executivo podem influenciar as decisões tomadas pelos conselheiros e ser

[208] Nesse sentido, Chris Hoofnagle critica duramente a atuação do Departamento, que alega ser fortemente influenciado pela "Escola de Chicago". Como exemplo, cita a omissão da Comissão em casos envolvendo "data brokers". Cf. Chris Hoofnagle, US Regulatory Values and Privacy Consequences: Implications for the European Citizen, p.3.

[209] Cf. Ryan Calo, The Boundaries of Privacy Harm, Ind. LJ, v. 86, 2011, p. 1144–1153.

[210] Para Susan Wagner, a Comissão estaria, assim como outras agências no sistema estadunidense, pressionada entre o Congresso e o Poder Executivo. Nesse sentido, está submetida a pressões que podem se materializar em cortes de repasse de verbas, aprovações de legislações restringindo seus poderes de investigação ou mesmo com a indicação de conselheiros cujas plataformas de atuação sejam mais afinadas com os interesses desses poderes. Cf. Susan Wagner, The Federal Trade Commission, Nova Iorque: Praeger Publishers, 1971.

determinantes para a escolha de casos ou entendimentos a serem perseguidos ou adotados.[211]

Para Chris Hoofnagle, esse fator é ainda mais relevante se se levar em consideração o poder de influência de grandes empresas sobre membros do Congresso.[212] Nesse sentido, as estratégias de pressão e articulação política de atores privados (*lobbying*) podem repercutir diretamente nas decisões da Comissão, o que poderia desvirtuar a tutela dos interesses dos consumidores.

Mais do que isso, por ser sua missão também proteger o bom funcionamento do mercado, a Comissão pode não ficar confortável para adotar posicionamentos muito antagônicos em relação à iniciativa privada. Isso estaria ligado à própria ideia de que o sucesso do país e da economia adviria da livre iniciativa e da livre concorrência.[213]

Embora relevantes, fatores como esses são difíceis de ser identificados ou comprovados. Isso porque, diferentemente do Congresso, a cujos membros se aplicam regras de transparência sobre o envolvimento em atividades ou estratégias de articulação política, a Comissão está livre de obrigações nesse sentido. Como resultado, Chris Hoofnagle chama a atenção para a "opacidade" desses processos, que aconteceriam de forma intensa no âmbito da Comissão, e que poderiam estar por trás dos processos de seleção dos casos que decide encampar.[214]

Nesse ponto, vale destacar que há extensa discricionariedade da Comissão para selecionar os casos que serão objeto de investigação, de sanção ou de demandas judiciais.[215] Em razão de sua limitação de recursos (financeiros e de pessoal), a Comissão parece dar preferência para casos que considera estratégicos, seja pelo seu potencial de

[211] Os conselheiros participam de processos de deliberação para determinar quais casos e investigações serão perseguidos ou quais acordos serão homologados, por exemplo. Cf. Chris Hoofnagle, Federal Trade Commission Privacy Law and Policy, p. 152.
[212] Cf. Chris Hoofnagle, US Regulatory Values and Privacy Consequences: Implications for the European Citizen, p.6.
[213] Essa ideia já se reflete na opinião de conselheiros da Comissão há algum tempo, destaca Chris Hoofnagle. Em 1959, o então conselheiro Earl Kinter, por exemplo, declarou, em um congresso consumerista, que "nós poderíamos distribuir agentes federais de forma tão veemente que nenhum comerciante ousaria sequer pensar em desrespeitar a lei. O público estaria completamente protegido. Nada seria roubado que não nosso sistema de governo e a nossa liberdade" (tradução livre). Cf. Chris Hoofnagle, Federal Trade Commission Privacy Law and Policy, p. 382.
[214] Cf. Chris Hoofnagle, Federal Trade Commission Privacy Law and Policy, p. 183.
[215] São esses os três pilares de atuação da Comissão. Cf. Daniel Solove e Woodrow Hartzog, The FTC and the new common law of privacy, p. 608.

emplacar teses relevantes, seja pelo seu potencial pedagógico, incentivando a adoção de boas práticas por parte de outras empresas e atores.[216]

O alto índice de acordos celebrados pela Comissão também sugere que os casos selecionados sejam apenas aqueles que teriam grandes chances de sucesso se levados à apreciação do judiciário.[217] Daniel Solove e Woodrow Hartzog esclarecem que, antes de formalizar as reclamações (*complaints*), que dão início ao procedimento administrativo para eventual aplicação de sanção, a Comissão realiza uma série de diligências para avaliar a pertinência do caso. Esses procedimentos, que antecedem a formalização da reclamação, costumam acontecer em sigilo, o que dificulta a análise sobre os tipos de casos que são abandonados.[218]

Vários fatores podem influenciar essa decisão. Tipicamente, os membros da Comissão avaliam *(i)* a extensão do dano causado aos consumidores; *(ii)* se a matéria em questão está sendo objeto de disputa no judiciário; *(iii)* o volume de consumidores afetados; *(iv)* se a empresa já tem um histórico de violações; *(v)* se a violação é flagrante.[219]

Essa discricionariedade da Comissão para decidir quais tipos de casos serão perseguidos divide opiniões. De um lado, há quem defenda que seja vantajosa e necessária na medida em que evitaria a mobilização de recursos para demandas que teriam poucas chances de êxito ou cuja reparação não atingiria um número significativo de consumidores. O argumento seria reforçado ainda pelo fato de que a Comissão recebe um volume muito alto de demandas e reclamações de consumidores, sendo ineficiente averiguar todas.[220] De outro, há quem argumente que essa discricionariedade tem culminado na omissão da Comissão em relação a demandas importantes em relação à privacidade, especialmente aquelas ligadas a violações de legislações estrangeiras de proteção de dados pessoais.[221]

A seu turno, a Comissão defende ser uma referência na proteção da privacidade dos consumidores. De acordo com o seu último relatório, publicado em janeiro de 2016, a

---

[216] Cf. Chris Hoofnagle, US Regulatory Values and Privacy Consequences: Implications for the European Citizen, p.7-8.
[217] Dos 154 casos avaliados por Daniel Solove e Woodrow Hartzog, apenas 6 não culminaram em acordos. Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 611.
[218] Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 609.
[219] Cf. Chris Hoofnagle, US Regulatory Values and Privacy Consequences: Implications for the European Citizen, p.7.
[220] Cf. Chris Hoofnagle, US Regulatory Values and Privacy Consequences: Implications for the European Citizen, p.7-8 (salientando que a maioria das demandas formuladas pelos consumidores é inadequada ou impertinente e que a Comissão não tem recursos para lidar com todas elas).
[221] Cf. Graham Pearce; Nicholas Platten, Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective, Fordham Int'l LJ, v. 22, p. 2024, 1998.

Comissão relata que encampou medidas de fiscalização envolvendo grandes empresas do setor de Internet, como Google, Twitter e Facebook, bem como empresas de menor porte. Teriam sido também medidas que enfrentaram questões ligadas à privacidade na Internet e fora dela. Além disso, "*as medidas de fiscalização da Comissão em relação à privacidade protegem não só os consumidores americanos; ao contrário, elas protegem consumidores do mundo todo de práticas desleais e enganosas encampadas por empresas que estejam sob a jurisdição da Comissão*".[222]

Nessa nota, a Comissão destaca sua atuação na fiscalização do acordo *Safe Harbor,* o que, a nosso ver, seria, de fato, um bom parâmetro para avaliar se a Comissão tem sido pró-ativa e rigorosa. No item 3.3.1, abaixo, apresentamos nosso levantamento empírico para proceder a essa análise.

3.3. Notificação e escolha: a jurisprudência da auto-regulação

Como já se salientou no capítulo anterior, por não dispor de uma lei genérica de proteção de dados pessoais, o sistema de auto-regulação estadunidense acabou sendo moldado pelas diretrizes consolidadas na jurisprudência da Comissão. Nesse sentido, Daniel Solove e Woodrow Hartzog defendem que essa jurisprudência, sintetizada nos itens acima e acumulada ao longo de seus anos de atuação em casos envolvendo o direito à privacidade, constituiria um complexo corpo de regras e orientações, que equivaleriam, na visão dos autores, a uma verdadeira regulamentação em matéria de proteção de dados pessoais.

Com isso, o papel da Comissão teria evoluído, passando de mera garantidora do cumprimento de promessas das empresas (em um modelo claro de auto-regulação) para uma fonte de regras substantivas de proteção à privacidade, em um modelo mais próximo daquele "legislativo", adotado na União Europeia, por exemplo. Essas regras constituiriam

[222] Cf. Federal Trade Commission, Privacy and Data Security Update (2015), disponível em https://www.ftc.gov/reports/privacy-data-security-update-2015, último acesso em 07/07/2016.

aquilo que a Comissão teria passado a considerar como "expectativas de privacidade", que não poderiam ser frustradas pelas empresas.[223]

À extensa jurisprudência da Comissão se somariam ainda os inúmeros materiais publicados e eventos realizados, como relatórios, discursos, anúncios públicos e oficinas, todos produzidos com a intenção de oferecer diretrizes concretas acerca das melhores práticas a serem adotadas pelos atores privados. Isso faria da Comissão um elo fundamental no modelo regulatório de privacidade adotado nos Estados Unidos.[224]

Chris Hoofnagle acrescenta que a atuação da Comissão também serviu para construir legitimidade em torno do modelo regulatório de privacidade estadunidense, na medida em que ela se coloca como um órgão que desempenha atribuições similares às de uma autoridade de proteção de dados. Nesse sentido, empresta credibilidade ao sistema de auto-regulação, aumentando os níveis de confiança depositados por países estrangeiros na tutela conferida à privacidade pelos Estados Unidos.[225]

Na jurisprudência da Comissão, entretanto, o que se percebe é que os entendimentos acerca das atividades que podem ser enquadradas como desleais ou enganosas no que diz respeito à privacidade ainda estão largamente centradas nos princípios de notificação e escolha. Daniel Solove e Woodrow Hartzog defendem a tese de que a Comissão teria solidificado um corpo de regras detalhado a respeito dessas práticas, especialmente no que se refere a critérios de segurança e notificação.[226] Isso teria aproximado o modelo estadunidense muito mais de um modelo de regulação do que de auto-regulação.

Ao mesmo tempo, os autores admitem que essas regras foram desenvolvidas com base em "práticas comuns da indústria".[227] Nesse sentido, discordamos da conclusão dos autores, na medida em que essa extensa jurisprudência da Comissão nada mais seria do que uma consolidação de boas práticas a serem seguidas e que foram desenvolvidas justamente dentro do modelo de auto-regulação, com base nos conceitos de notificação e escolha. Esse suposto novo corpo normativo formado pela jurisprudência da Comissão em pouca coisa parece ter alterado as características fundantes do modelo regulatório de privacidade dos Estados Unidos. As empresas continuam, portanto, livres para desenhar suas próprias

[223] Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 672. No mesmo sentido, cf. Chris Hoofnagle, Federal Trade Commission Privacy Law and Policy, p. 145.
[224] Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 604.
[225] Cf. Chris Hoofnagle, Federal Trade Commission Privacy Law and Policy, p. 521.
[226] Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 672.
[227] Cf. Daniel Solove / Woodrow Hartzog, The FTC and the new common law of privacy, p. 672.

políticas de privacidade, com a diferença de que agora existem regras ou diretrizes mais claras a respeito de como as notificações devem ser feitas ou a segurança dos dados protegidas para que se possa evitar alguma sanção vinda por parte da Comissão.

3.3.1. *Safe Harbor:* fiscalização ou encenação?

Para avaliar a atuação da Comissão nos casos envolvendo o *Safe Harbor*, realizamos uma pesquisa no repositório de casos na página da Comissão na Internet (www.ftc.gov). Até o mês de julho de 2016, a Comissão apresentou 208 reclamações ligadas à privacidade de consumidores, 39 das quais estão diretamente relacionadas com o acordo *Safe Harbor,* isto é, mencionaram explicitamente uma ou mais violações aos termos do arranjo em sua fundamentação jurídica.

A tabela abaixo resume os resultados de nossa análise do teor dessas reclamações, indicando as respectivas datas nas quais foram anunciadas e o fundamento sobre o qual foram calcadas.

Parte demandada	**Data**	**Motivo**
ExpatEdge Partners, LL	06/10/09	falsa declaração
Directors Desk LL	06/10/09	falsa declaração
Collectify LL	06/10/09	falsa declaração
World Innovators, Inc.	06/10/09	falsa declaração
Progressive Gaitways LL	06/10/09	falsa declaração
Onyx Graphics, Inc.	06/10/09	falsa declaração
Best Priced Brands, LLC, et al.	06/10/09	falsa declaração
Google, Inc.	30/03/11	violação de princípios
Facebook, Inc.	29/11/11	violação de princípios
Myspace LLC	08/05/12	violação de princípios
PDB Sports, Ltd., d/b/a Denver Broncos Football Club	21/01/14	falsa declaração
Atlanta Falcons Football Club, LLC	21/01/14	falsa declaração
BitTorrent, Inc.	21/01/14	falsa declaração
Baker Tilly Virchow Krause, LLP	21/01/14	falsa declaração
Apperian, Inc.	21/01/14	falsa declaração
Receivable Management Services Corporation	21/01/14	falsa declaração
Reynolds Consumer Products, Inc	21/01/14	falsa declaração

Level 3 Communications, LLC	21/01/14	falsa declaração
DDC Laboratories, Inc., also d/b/a DNA Diagnostics Center	21/01/14	falsa declaração
DataMotion, Inc.	21/01/14	falsa declaração
Charles River Laboratories, Int'l.	21/01/14	falsa declaração
American Apparel, Inc.	21/01/14	falsa declaração
Fantage.com, Inc.	21/01/14	falsa declaração
Tennessee Football, Inc.	21/01/14	falsa declaração
American International Mailing, Inc.	07/04/15	falsa declaração
TES Franchising, LLC	07/04/15	falsa declaração
SteriMed Medical Waste Solutions	17/08/15	falsa declaração
Pinger, Inc.	17/08/15	falsa declaração
One Industries Corp.	17/08/15	falsa declaração
NAICS Association, LLC	17/08/15	falsa declaração
Just Bagels Manufacturing, Inc.	17/08/15	falsa declaração
Jubilant Clinsys, Inc.	17/08/15	falsa declaração
IOActive, Inc.	17/08/15	falsa declaração
Inbox Group, LLC	17/08/15	falsa declaração
Golf Connect, LLC	17/08/15	falsa declaração
Dale Jarrett Racing Adventure Inc.	17/08/15	falsa declaração
Jhayrmaine Daniels (California Skate Line)	17/08/15	falsa declaração
Forensics Consulting Solutions, LLC	17/08/15	falsa declaração
Contract Logix, LLC	17/08/15	falsa declaração

A análise dos casos permite concluir que a Comissão realizou uma fiscalização pouco rigorosa do cumprimento do *Safe Harbor* por parte das empresas e organizações participantes. Em primeiro lugar, isso pode ser percebido pelo próprio volume de reclamações formalizadas, que está aquém daquele que seria esperado para um arranjo dessas proporções, especialmente se se considerar o seu longo período de vigência - dezesseis anos - e o grande número de participantes - 5.465.

Por mais que não seja característica da Comissão assumir um grande volume de casos por ano, é possível perceber que as reclamações não estão bem distribuídas no tempo, sinalizando períodos longos de inatividade: as primeiras reclamações foram apresentadas apenas nove anos depois da entrada em vigor do arranjo. Mais do que isso, a maioria das reclamações é apresentada em bloco, isto é, na mesma data; em geral tratam-se de reclamações similares ou idênticas dirigidas a diferentes empresas. O anúncio da instauração dos procedimentos administrativos ajudava a projetar uma imagem de pró-atividade da Comissão em momentos críticos. Coincidentemente ou não, os três períodos

principais de atuação da Comissão em relação ao *Safe Harbor* aconteceram pouco tempo depois da veiculação de críticas ou de acontecimentos que questionavam a sua legitimidade. Em 2008, Chris Connolly publicou um relatório apresentando uma série de críticas duras à fiscalização do *Safe Harbor*, sugerindo que apenas 1/5 das empresas e organizações participantes cumpririam os seus princípios[228]; em 2009, a Comissão anuncia procedimentos realizados em face de sete empresas. Em 2013, após as denúncias de Edward Snowden, a Comissão Europeia enviou um comunicado para o Parlamento Europeu e o Conselho identificando uma série de deficiências na implementação do arranjo[229]; em 2014, a Comissão anuncia catorze reclamações. Em 2014, é encaminhada para o Tribunal de Justiça da União Europeia a ação que questiona a validade do arranjo; em 2015, a Comissão anuncia outras quinze reclamações.

Outra característica comum a esses três blocos de ação diz respeito aos fundamentos das reclamações. Em todos os casos, a alegação da Comissão era a de que havia uma falsa declaração sendo feita aos consumidores. São casos em que, a despeito de a certificação dessas empresas estar expirada ou pendente de avaliação, havia menção em suas políticas de privacidade a respeito da sua participação no *Safe Harbor*. Esse é o fundamento de 36 das 39 reclamações analisadas.

Considerando que a aderência ao *Safe Harbor* significava o comprometimento por parte dos participantes em cumprir com os sete princípios do arranjo, o tema da "falsa declaração" não parece ser o mais relevante para a privacidade dos cidadãos europeus, cujos dados estavam sendo transferidos para os Estados Unidos com base no arranjo.

As outras três reclamações apresentadas pela Comissão envolveram grandes empresas do setor de Internet (Google, Facebook e MySpace). Nelas, o fundamento de violação ao *Safe Harbor* foi em relação aos princípios de "notificação" e "escolha", que são a base do modelo de auto-regulamentação nos Estados Unidos. Dessa forma, o argumento principal para as reclamações - e talvez a sua motivação primeira - era a violação desse modelo; o argumento ligado ao *Safe Harbor* era subsidiário.

[228] Cf. Chris Connolly, The US Safe Harbor-Fact or Fiction?, Galexia, 2008.
[229] Cf. European Commission, Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companhies Established in the EU, 2013.

CAPÍTULO 4 - DA DIPLOMACIA AO RADICALISMO: TERRITÓRIO, JURISDIÇÃO E TUTELA DA PRIVACIDADE

No capítulo anterior, demonstrou-se que a Comissão Federal de Comércio dos Estados Unidos apresenta características que a impedem de atuar de forma efetiva no combate a violações de legislações estrangeiras de proteção de dados, especialmente nos casos em que essas violações não são coibidas pelo direito estadunidense. Nessas circunstâncias, portanto, a atuação da Comissão fica restrita às medidas de auxílio e cooperação internacional previstas no U.S. SAFE WEB Act.

Embora essas medidas possam favorecer as investigações conduzidas por autoridades de outras jurisdições, facilitando a obtenção de informações que estejam nos Estados Unidos, por exemplo, elas não se traduzem em deveres de instauração de procedimentos administrativos para a investigação e responsabilização de atores sediados nos Estados Unidos. Isso restringe as opções de acesso a esses atores que, na omissão da Comissão, estão praticamente imunes ao poder sancionador de autoridades de jurisdições onde não estão sediados.

Diante disso, para fazer valer eventuais sanções em relação a esses atores, restam poucos caminhos às autoridades dessas jurisdições. O primeiro deles é o mais diplomático, qual seja o ajuizamento de um pedido formal de reconhecimento e execução de ordem judicial estrangeira perante a justiça estadunidense. Além dos trâmites processuais e burocráticos para proceder ao reconhecimento e à execução, essa alternativa envolve discussões complexas a respeito da legislação aplicável e dos elementos que ensejam jurisdição sobre os casos relativos à proteção de dados pessoais na Internet.

O segundo caminho aposta em medidas mais drásticas, como aquelas que se aproveitam do acesso a intermediários locais para determinar o bloqueio de aplicações de Internet na camada da infraestrutura[230] ou para estrangular a viabilidade econômica das

[230] As ordens de bloqueio do aplicativo de mensagens WhatsApp pela justiça brasileira são exemplos de como a jurisdição sobre os provedores de conexão à Internet (intermediários locais) pode ser utilizada nesse sentido.

atividades praticadas, como a proibição de transações envolvendo cartões de crédito emitidos por instituições bancárias nacionais.[231]

Como se verá ao longo deste capítulo, esses caminhos suscitam debates profundos sobre a extensão da jurisdição dos Estados Nacionais e suas repercussões para os conceitos de soberania e território, temas que serão objeto de aprofundamento no capítulo seguinte. Além disso, ensejam a formulação de teorias e propostas em relação aos elementos preponderantes para a definição de questões como legislação aplicável e foro competente. Embora façam parte do pano de fundo da discussão travada neste capítulo, foge ao escopo de análise desta tese propor respostas ou construir consensos em relação a essas questões.

Sendo assim, os objetivos deste capítulo são *(i)* esclarecer as hipóteses e requisitos para reconhecimento e execução de ordens judiciais estrangeiras nos Estados Unidos, sobretudo no estado da Califórnia, onde estão sediadas muitas empresas do setor de Internet; *(ii)* identificar as limitações de utilização dessa alternativa para os casos envolvendo violações a legislações de proteção de dados pessoais; *(iii)* explorar as opções legislativas que têm surgido como estratégia dos Estados Nacionais para estender o alcance de sua jurisdição em casos envolvendo a Internet; e *(iv)* refletir sobre a efetividade de medidas de constrangimento baseadas no território, como os bloqueios.

4.1. Reconhecimento e execução de ordem judicial estrangeira nos Estados Unidos

Embora existam tratados e convenções internacionais que uniformizem os procedimentos de reconhecimento e execução de ordens judiciais estrangeiras, como a Convenção de Haia, de 01 de fevereiro de 1971[232], os Estados Unidos não são signatários de nenhum deles. Além disso, a única legislação federal que regulamenta a questão se limita a casos de reconhecimento e execução de ordem judicial estrangeira para a recuperação de valores em dinheiro, excluindo-se os casos de natureza tributária, de

[231] Na Argentina, por exemplo, uma ordem judicial determinou que as instituições financeiras nacionais não autorizassem a utilização de cartões de crédito para o pagamento de corridas feitas por meio do aplicativo Uber. Cf. Argentinian Telecoms (and Credit Cards) Ordered to Block UBER App, disponível em: </blog/2016/05/argentinian-telecoms-and-credit-cards-ordered-block-uber-app>, último acesso em 22/12/2016.

[232] Convention on the recognition and enforcement of foreign judgements in civil and commercial matters, disponível em https://assets.hcch.net/docs/bacf7323-9337-48df-9b9a-ef33e62b43be.pdf

pensão alimentícia ou de outras penalidades pecuniárias ("Uniform Foreign Money Judgements Recognition Act of 1962" ou "UFMJR").[233]

Sem regulamentação no âmbito federal, a matéria é de competência estadual e seus procedimentos variam de estado para estado.[234] Vale destacar, contudo, que a Suprema Corte dos Estados Unidos, no caso *Hilton v. Guyot*, estabeleceu princípios que foram replicados em muitas legislações estaduais.[235] Além disso, a UFMJR também serviu de modelo para muitas legislações estaduais, o que confere relativa uniformidade para o regramento dado a questão entre alguns estados. Apesar disso, ainda há diferenças significativas entre os procedimentos adotados por determinados estados.[236]

Assim como em outros sistemas jurídicos, nos Estados Unidos, o reconhecimento e a execução de ordens judiciais estrangeiras são etapas distintas; a primeira deve sempre anteceder a segunda. O processo de reconhecimento é o que demanda o preenchimento dos requisitos estabelecidos nas legislações estaduais; uma vez reconhecida, a ordem estrangeira passa a ser considerada como equivalente a uma ordem emanada por uma autoridade judicial estadunidense, estando, portanto, apta a ser executada naquele território.[237]

Costumam ser passíveis de reconhecimento as ordens judiciais consideradas "finais", "conclusivas" e "válidas" (isto é, executáveis no seu país de origem).[238] Para efeitos do UFMJR, mesmo as ordens judiciais ainda susceptíveis de recurso podem ser consideradas "finais". Entretanto, em geral, o poder judiciário estadunidense costuma suspender o procedimento de reconhecimento enquanto estiver tramitando o recurso no país de origem.[239]

Em geral, os pedidos de reconhecimento podem ser indeferidos pela justiça estadunidense com base em hipóteses vinculantes e discricionárias. As hipóteses vinculantes costumam envolver sentenças que foram exaradas por autoridades judiciais

---

[233] Cf. Christopher Paparella / Andrea Engels, Enforcement of Foreign Judgments 2016 - ICLG - International Comparative Legal Guides, disponível em: <http://www.iclg.co.uk/practice-areas/enforcement-of-foreign-judgments/enforcement-of-foreign-judgments-2016/usa>, último acesso em 17/08/2016.

[234] Cf. Scott Edelman *et. al.,* Enforcement of Foreign Judgements in 28 jurisdictions worldwide - United States, Law Business Research 2014, p. 131.

[235] *Hilton v Guyot*, 159 US 113 (1895).

[236] Como se demonstra nesta tese, há uma concentração significativa dos atores privados do setor de Internet no estado da Califórnia. Por essa razão, sempre que necessário, este capítulo fará alusão a regras específicas deste estado, excluindo de seu escopo particularidades de outros estados.

[237] Cf. Scott Edelman *et. al.,* Enforcement of Foreign Judgements in 28 jurisdictions worldwide - United States, Law Business Research 2014, p. 131.

[238] Cf. Uniform Foreign Money Judgements Recognition Act of 1962, § 2

[239] Cf. Christopher Paparella / Andrea Engels, Enforcement of Foreign Judgments 2016 - ICLG - International Comparative Legal Guides.

que *(i)* não respeitam o princípio da imparcialidade; *(ii)* não garantem procedimentos compatíveis com o princípio do devido processo legal; ou *(iii)* não detinham jurisdição sobre o caso. Já as hipóteses discricionárias costumam envolver sentenças que *(i)* foram obtidas mediante fraude; *(ii)* estão em conflito com os dispositivos constitucionais dos Estados Unidos; *(iii)* estão em conflito com políticas públicas dos Estados Unidos, entre outras.[240]

4.1.1. Reconhecimento de ordem judicial estrangeira na Califórnia

Considerando que um grande número de atores privados do setor de Internet está sediado no estado da Califórnia[241] e que, portanto, o acesso a eles (a a seus bens, por exemplo) dependeria do reconhecimento e execução de ordens judiciais estrangeiras pela justiça desse estado, este capítulo dará especial atenção ao procedimento aplicável para esses casos.

O estado da Califórnia regulamenta o procedimento de reconhecimento de ordem judicial estrangeira em seu código de processo civil ("California Code of Civil Procedure" ou "CCCP"). Em grande parte, suas disposições são similares àquelas expostas no item anterior.

De acordo com o disposto na seção 1715, o procedimento se aplica a ordens judiciais que *(i)* defiram ou indefiram a recuperação de quantias em dinheiro; e *(ii)* sejam consideradas finais, conclusivas e executáveis de acordo com a legislação do seu país de origem. O dispositivo não se aplica, entretanto, a ordens judiciais que digam respeito a *(i)* questões tributárias; *(ii)* aplicação de multas ou outras penalidades; e *(iii)* questões ligadas ao direito de família, como o pagamento de pensão alimentícia, podendo, nesse último caso, ser pleiteado o reconhecimento mediante procedimento previsto na seção 1723.

A seção 1716 (b) do CCCP estabelece as hipóteses nas quais a autoridade judicial americana *deve* indeferir o pedido de reconhecimento. São três as hipóteses previstas:

---

[240] Cf. Christopher Paparella / Andrea Engels, Enforcement of Foreign Judgments 2016 - ICLG - International Comparative Legal Guides.

[241] Essa hipótese é comprovada pelo levantamento empírico que realizamos, cujos resultados estão apresentados no capítulo 5 desta tese.

> "(B) Um tribunal deste estado não reconhecerá uma ordem judicial de país estrangeiro em qualquer um dos seguintes casos: (1) A sentença foi proferida em um sistema judicial que não garante tribunais ou procedimentos imparciais compatíveis com os requisitos do devido processo legal. (2) O tribunal estrangeiro não detinha jurisdição pessoal sobre o réu. (3) O tribunal estrangeiro não tinha jurisdição sobre o assunto." (tradução livre)

Já a seção 1716 (c) do CCCP estabelece as hipóteses nas quais a autoridade judicial americana *pode* indeferir o pedido de reconhecimento. São nove as hipóteses previstas:

> "(C) Um tribunal deste estado não é obrigado a reconhecer uma ordem judicial de país estrangeiro em qualquer um dos seguintes casos: (1) O réu no processo no tribunal estrangeiro não recebeu notificação do processo em tempo suficiente para permitir sua defesa. (2) A sentença foi obtida por fraude que privou a parte perdedora de uma oportunidade adequada para apresentar seu caso. (3) A ordem judicial ou a causa de ação ou o pedido de reparação em que a ordem judicial se baseia é repugnante à política pública deste Estado ou dos Estados Unidos. (4) A ordem judicial entra em conflito com outra ordem judicial final e conclusiva. (5) O processo no tribunal estrangeiro foi contrário a um acordo entre as partes segundo o qual o litígio em questão devia ser dirimido de outra forma que não pelo processo nesse tribunal estrangeiro. (6) No caso de jurisdição baseada apenas na pessoa, o tribunal estrangeiro era um foro seriamente inconveniente para o julgamento da ação. (7) A ordem judicial foi proferida em circunstâncias que levantam dúvidas substanciais sobre a integridade do tribunal processador em relação a ela. (8) O procedimento específico no tribunal estrangeiro que conduziu à ordem judicial não era compatível com os requisitos do devido processo legal. (9) A ordem judicial demanda o pagamento de danos por difamação, a menos que o tribunal [da Califórnia] determine que a lei de difamação aplicada pelo tribunal estrangeiro proporcionou pelo menos a mesma proteção da liberdade de expressão e de imprensa, tal como previsto pelas constituições dos Estados Unidos e da Califórnia." (tradução livre).

A seção 1717 (a) estabelece as hipóteses nas quais o pedido de reconhecimento não pode ser indeferido com base na ausência de jurisdição pessoal:

> "(A) Uma ordem judicial de país estrangeiro não terá o reconhecimento indeferido por falta de jurisdição pessoal se qualquer um dos seguintes casos se aplicar: (1) O réu foi citado pessoalmente no país estrangeiro. (2) O réu apresentou-se voluntariamente no processo, com a finalidade de proteger bens apreendidos ou ameaçados de apreensão no processo ou de contestar a jurisdição do tribunal sobre o réu. (3) O requerido, antes do início do processo, concordou em se submeter à jurisdição do tribunal estrangeiro relativamente ao objeto em causa. (4) O réu estava domiciliado no país estrangeiro quando o processo foi instituído ou era uma corporação ou outra forma de organização comercial que tinha o seu principal local de negócios em, ou estava organizado sob as leis do país estrangeiro. (5) O réu tinha um escritório de negócios no país estrangeiro e o processo no tribunal estrangeiro envolvia uma causa de ação ou pedido de reparação decorrentes de negócios feitos pelo réu por meio desse escritório no país estrangeiro. (6) O réu operava um veículo a motor ou um avião no país estrangeiro e o processo envolvia uma causa de ação ou um pedido de reparação decorrente dessa operação." (tradução livre)

Demos destaque aos dispositivos citados acima porque são eles que podem justificar o indeferimento de pedidos de reconhecimento. Nesse sentido, podem servir de obstáculo para a execução de ordens estrangeiras que determinem a responsabilização por

violações a leis de proteção de dados pessoais. Esses obstáculos são explorados no item a seguir.

4.1.1.1. Obstáculos para reconhecimento de ordens judiciais envolvendo proteção de dados pessoais

Observando os dispositivos mencionados no item anterior e, levando em consideração o possível teor de ordens judiciais estrangeiras que ensejariam a responsabilização de atores privados pela violação de legislações de dados pessoais, pode-se dizer que são três os principais obstáculos ao reconhecimento dessas ordens no estado da Califórnia: *(i)* impossibilidade de reconhecimento de ordens que imponham o pagamento de multa; *(ii)* possível incompatibilidade com questões de política pública; e *(iii)* não reconhecimento da jurisdição da autoridade judicial estrangeira.

4.1.1.1.1. Impossibilidade de reconhecimento de ordens de multa

O pagamento de multa é uma sanção tipicamente prevista em legislações de proteção de dados pessoais.[242]Tanto é assim que são inúmeros os casos de aplicação de multa pelas autoridades de proteção de dados ao redor do mundo.[243]

É verdade que quando as multas são impostas em face de atores que têm representação comercial no país, a sua execução fica facilitada na medida em que podem

[242] Por exemplo, esse é o caso das legislações de proteção de dados da Argentina, Coreia do Sul, África do Sul, Colômbia, Chile, Peru, Israel e de praticamente todos os Estados-membros da União Europeia, por força da Diretiva 95. O novo Regulamento Geral para Proteção de Dados Pessoais também prevê multa como uma forma de sanção. Até mesmo o ordenamento jurídico brasileiro, que ainda não conta com uma lei geral de proteção de dados pessoais, tem previsão de multa como sanção pelo descumprimento da legislação brasileira em casos envolvendo a privacidade de usuários de Internet (Lei nº 12.965/14, art. 12).

[243] Cf. Google fined $1.2 million by Spain over privacy practices, PCWorld, disponível em: <http://www.pcworld.com/article/2082320/google-fined-by-spanish-data-protection-authority-over-privacy-policy.html>, acesso em 01/12/2016. Cf. também Natasha Lomas, Facebook Faces Fines Of $268K Per Day For Tracking Non-Users In Belgium. Cf. Facebook faces EU fine over WhatsApp data-sharing, Financial Times, disponível em: <https://www.ft.com/content/f652746c-c6a4-11e6-9043-7e34c07b46ef>, último acesso em 01/12/2016.

ser utilizadas todas as medidas de coerção disponibilizadas pelo ordenamento jurídico nacional. Com bens e receita sob jurisdição nacional, por exemplo, é possível executar ordens de bloqueio ou penhora para o pagamento de multas ou outras penalidades. Esse costuma ser o caso das multas vultuosas impostas às grandes empresas de Internet, que, por possuir escritórios em diversos países do mundo, ficam mais expostas à execução desses tipos de penalidades nos territórios onde atuam.[244]

Todavia, como se demonstra no capítulo 5 desta tese, há um grande número de atores privados que não estão sediados em diversos países e que, mesmo assim, podem ser responsáveis por violações de suas normas constitucionais e legislações de proteção de dados pessoais. Como um número significativo deles tem sede na Califórnia, a impossibilidade de reconhecimento de ordens judiciais estrangeiras que imponham pagamento de multa por essas violações nesse estado representa um obstáculo relevante para a possibilidade de responsabilização desses atores pela violação de legislações de países onde não estão sediados.

Em resumo, pode-se dizer que esses atores estão "imunes" à execução dessas sanções no estado da Califórnia, onde, provavelmente, encontra-se a maior parte de seus recursos.

4.1.1.1.2. Incompatibilidade por razões de política pública

O segundo possível obstáculo diz respeito à possibilidade de se indeferir pedidos de reconhecimento com base na incompatibilidade da ordem judicial estrangeira com questões de política pública dos Estados Unidos. Por não definir os termos dessa incompatibilidade ou explicitar quais políticas públicas estariam abarcadas, é possível dizer que essa hipótese pode representar um "cheque em branco" para a autoridade judicial estadunidense, abrindo caminho para a sua discricionariedade.

Isso porque, como se demonstrou no capítulo 2 desta tese, o modelo regulatório de privacidade adotado nos Estados Unidos serve a uma série de valores consagrados pela

[244] Cf. Reuters, Google faces $18 million fine for web privacy violation, disponível em http://www.reuters.com/article/us-privacy-google-dutch-idUSKBN0JT1TG20141215, último acesso 30/11/2016.

sociedade americana, como a autonomia privada, a livre concorrência e a liberdade individual. Além disso, na medida em que pretendem favorecer a inovação e o desenvolvimento da economia e do setor de Internet, as decisões regulatórias encampadas tanto pelo Congresso estadunidense quanto pela própria Comissão Federal do Comércio no que diz respeito à proteção da privacidade podem ser consideradas como razões de política pública.

Nesse sentido, ordens judiciais que, se reconhecidas, poderiam desvirtuar a natureza da tutela conferida ao direito à privacidade nos Estados Unidos podem ter seu reconhecimento indeferido com base nesse dispositivo.

O argumento da potencial incompatibilidade de uma ordem judicial estrangeira cuja execução se pretendia proceder nos Estados Unidos com razões de política pública já foi invocado no emblemático caso *LICRA v. Yahoo!*[245]. Depois de exarada decisão judicial na França determinando a suspensão de uma atividade de leilão promovida pela Yahoo! que violaria a legislação francesa, ao invés de aguardar a tentativa de reconhecimento e execução dessa sentença nos Estados Unidos, a Yahoo! ingressou com ação nesse país pleiteando a declaração judicial de que eventual tentativa de execução da sentença violaria a Primeira Emenda da Constituição estadunidense.

Em primeira instância, o pedido da empresa foi julgado procedente já que seria inconsistente com a Constituição dos Estados Unidos aceitar que uma outra nação restringisse a liberdade de expressão de um cidadão estadunidense. Na decisão, questiona-se a própria jurisdição da justiça francesa para decidir sobre um caso envolvendo uma empresa com sede nos Estados Unidos.[246]A decisão foi posteriormente reformada, por maioria de votos, não pelo mérito do pedido, mas por se ter considerado o pedido juridicamente impossível já que ainda não havia existido tentativa de se executar a sentença nos Estados Unidos.[247] Como explica Marcel Leonardi, o caso ficou sem decisão definitiva uma vez que, antes de executada a sentença, a Yahoo! decidiu suspender o leilão de artigos associados a grupos que promovessem o ódio e a violência, que dera causa à ação.[248]

---

[245] Cf. França, Le tribunal de grande instance de Paris, La Ligue contre le racisme e l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Societe Yahoo! France, n. 00/05308, julgado em 20.11.2000.
[246] Cf. Estados Unidos*, Yahoo! Inc. v. La Ligue contre le racisme et l'antisémittisme*, District Court of the Northern District of California, n. C-00-21275, julgado em 7.11.2001.
[247] Cf. Estados Unidos, *Yahoo! Inc. v. La Ligue contre le racisme et l'antisémittisme,* Court of Appeals for the Ninth Circuit, n. 01-17424, julgado em 23.08.2004.
[248] Cf. Marcel Leonardi, Tutela e privacidade na internet, p.255.

O interessante nesse caso foi a medida judicial ter sido concedida em caráter preventivo, sinalizando o indeferimento de eventual tentativa de reconhecimento da sentença francesa no país. Em outros casos, a justiça estadunidense também já decidiu pelo indeferimento de ordens judiciais que violariam políticas públicas.[249]

Christopher Paparella e Andrea Engels alertam, entretanto, para o fato de existirem entendimentos jurisprudenciais mais restritivos, no sentido de só considerar uma ordem judicial estrangeira incompatível com políticas públicas se ela estiver diretamente em contrariedade com políticas fundamentais ou que violem as noções mais básicas de moralidade e justiça dos Estados Unidos.[250] Como exemplo, citam um caso em que a justiça do estado de Nova Iorque indeferiu o reconhecimento de ordem judicial inglesa envolvendo um caso de calúnia por estar em desacordo com a garantia constitucional de liberdade de expressão.[251]

4.1.1.1.3. Ausência de jurisdição da autoridade judicial estrangeira

O terceiro obstáculo que pode ser apresentado diz respeito à ausência de jurisdição da autoridade judicial estrangeira sobre *(i)* a pessoa ou sobre *(ii)* o objeto da causa. Vale destacar que, conforme mencionado acima, essas são hipóteses de indeferimento obrigatório por parte da autoridade judicial estadunidense.

Avaliar se a autoridade judicial estrangeira tinha jurisdição sobre a demanda é uma tarefa complexa, tipicamente enfrentada pelo direito internacional privado. Em geral, a presença dos chamados "elementos de conexão", como o domicílio do réu ou o local de cumprimento de uma obrigação, determinam a jurisdição de uma autoridade judicial sobre o caso. Esses elementos variam de legislação para legislação e são definidos de acordo com a legislação aplicável ao caso.

A determinação da legislação aplicável, por sua vez, depende da aplicação de normas de conflitos de leis. No Brasil, por exemplo, a Lei de Introdução às Normas de

[249] Cf. *Osorio v. Dole Food Co., 665 F. Supp. 2d 1307* (em que uma decisão da justiça do estado da Flórida indefere um pedido de reconhecimento de ordem judicial da Nicarágua também por razões de incompatibilidade com políticas públicas).
[250] Cf. Christopher Paparella / Andrea Engels, International Comparative Legal Guides.
[251] Cf. *Bachchan v. India Abroad Publ'n Inc.,* 154 Misc. 2d 228, 230 (N.Y. Sup. Ct. 1992).

Direito Brasileiro (Decreto-lei nº 4.657) estabelece as situações nas quais se aplica a legislação brasileira. Nos Estados Unidos, a matéria também é regulada de maneira distinta pelos estados. No caso da Califórnia, a legislação aplicável segue o disposto na seção 187 do *Restatement of Law 2d (1971) 561* ("seção 187"), sobre conflito de leis:

> "§ 187. Lei do Estado sscolhida pelas Partes (1) **A lei do Estado escolhida pelas partes para governar seus direitos e deveres contratuais será aplicada** se a questão específica for aquela que as partes poderiam ter resolvido por uma disposição explícita em seu acordo dirigida a essa questão. (2) A lei do Estado escolhida pelas partes para regular seus direitos e deveres contratuais será aplicada, mesmo que a questão específica seja aquela que as partes não poderiam ter resolvido por meio de uma disposição explícita em seu acordo dirigida a essa questão, **a menos que** ou A) **o Estado escolhido não tiver qualquer relação substancial com as partes** ou com a transacção e não existir outra base razoável para a escolha das partes, ou (B) a **aplicação da lei do estado escolhido seria contrária a uma política fundamental** de um Estado que tenha um interesse materialmente maior do que o estado escolhido na determinação da questão específica e que, de acordo com o disposto no § 188, seria O estado da lei aplicável na ausência de uma escolha eficaz do direito pelas partes. (3) Na ausência de uma indicação de intenção contrária, a referência é à lei local do estado da lei escolhida." (tradução livre e destaques nossos).

Isso significa dizer que, salvo nos casos em que não houver qualquer relação substancial das partes com o local cuja legislação decidiu-se aplicar ou em que a aplicação da lei viole uma questão de política pública, a legislação aplicável aos casos é aquela determinada pelas partes.[252]

Sendo assim, para determinar se a justiça estrangeira detém jurisdição sobre a demanda, a justiça californiana deverá observar o que determina a legislação aplicável ao caso, que, via de regra, será aquela escolhida pelas partes e determinada contratualmente. No caso das empresas de Internet, isso justifica porque muitas delas incluem disposições em seus termos de uso e políticas de privacidade no sentido de ser aplicável a legislação do estado da Califórnia. Por força da seção 187, a autoridade judicial estadunidense provavelmente declarará a legislação da Califórnia como aplicável ao caso e utilizará, então, os critérios e elementos de conexão estabelecidos nessa legislação para definir a jurisdição sobre a demanda.

Para ilustrar a questão, pode-se tomar como exemplo a polêmica envolvendo a alteração dos termos da política de privacidade do aplicativo de mensagens instantâneas WhatsApp, que anunciou ter começado a compartilhar dados de usuários com a sua empresa controladora, Facebook. Supondo que uma decisão da justiça brasileira, com base

[252] O entendimento é consolidado jurisprudencialmente. Cf. *Nedlloyd Lines B.V. v. Superior Court*, 834 P.2d 1148, 1151-52.

no artigo 11 da Lei nº 12.965/14 ("Marco Civil da Internet"), que garante a aplicação da legislação brasileira a operações que envolvam dispositivos localizados no Brasil, determinasse a suspensão dessa atividade de compartilhamento, uma estratégia seria tentar reconhecer tal decisão perante a justiça californiana para então poder executá-la em face do WhatsApp, unicamente lá sediado.[253] Ao apreciar a questão, a justiça californiana teria de enfrentar um impasse em relação à determinação da legislação aplicável ao caso, o que complicaria a sua resolução.

Isso porque, de um lado, como em seus termos de uso e política de privacidade, o WhatsApp determina que a legislação aplicável é a da Califórnia, a justiça desse estado, com base na seção 187, provavelmente, afastaria a aplicação da legislação brasileira do caso e, nesse sentido, aplicaria a legislação da Califórnia para definir quem tinha jurisdição sobre ele. De outro lado, a jurisdição da justiça brasileira estaria garantida pelo Marco Civil da Internet, fator que não deveria poder ser ignorado pela justiça californiana. Para complicar a questão, registre-se ainda que o Marco Civil da Internet também abre caminho para que cláusulas de eleição da legislação aplicável, como essa utilizada pelo WhatsApp, possam ser declaradas inválidas pela justiça brasileira (art. 8º, II).

A situação não é meramente hipotética. Depois do anúncio da mudança na política de privacidade do aplicativo, decisões de países como Alemanha e Índia exigiram a suspensão do compartilhamento de informações. Embora não se tenha notícia de tentativas de reconhecimento e execução dessas decisões na justiça americana, nos dois casos, inicialmente, a empresa manifestou sua intenção de não acatar as ordens.[254]

Os exemplos ilustra como, no caso de ações envolvendo a aplicação de leis sobre proteção de dados pessoais, o tema da jurisdição assume contornos complexos e gera intensos debates, sendo fonte de profundas incertezas. Isso porque, na Internet, haveria uma multiplicidade de elementos de conexão, que desafiariam a definição da própria legislação aplicável a esses casos. Nesse sentido, Andrew Woods assinala que países, empresas e acadêmicos têm disputado diferentes teorias, muitas delas incompatíveis entre si, acerca do alcance jurisdicional a dados na Internet.[255]

---

[253] Apesar de essa ser uma situação hipotética, houve, de fato, quem entendesse que uma decisão com esse teor poderia ser tomada pela justiça brasileira. Cf. "Poder Público pode, em última hipótese, suspender atividades do WhatsApp", diz advogado do Idec, revistaepoca.globo.com, disponível em: <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/09/agora-sim-justica-tem-razao-para-bloquear-o-whatsapp-diz-advogado-do-idec.html>, acesso em: 31/12/2016.

[254] Cf. Mudit Mohilay, WhatsApp sharing data with Facebook despite an Indian High Court order. Cf. também "Facebook to appeal German order on WhatsApp data", Reuters, 2016.

[255] Cf. Andrew Woods, Against Data Exceptionalism, *Stanford Law Review*, 68, 729, 2016, p.731.

O autor divide essas formulações em dois grupos: *(i)* excepcionalistas, que defendem que as questões ligadas à jurisdição envolvendo dados pessoais na Internet mereceriam tratamento especial, com a definição de critérios específicos e novos[256]; e *(ii)* não-excepcionalistas, que defendem que essas questões não mereceriam tal tratamento, podendo ser dirimidas a partir da utilização de critérios tradicionais de definição de jurisdição, típicos do direito internacional privado, por exemplo.[257]

Apesar de não ser o objetivo desta tese determinar quais seriam os critérios de definição de jurisdição mais adequados, é importante destacar as principais teorias e alternativas aventadas, apontando de que forma poderiam servir de argumento para obstar eventuais pedidos de reconhecimento de ordem judicial estrangeira nos Estados Unidos.

Mesmo entre as empresas do setor de Internet, que costumam ser as partes demandadas nessas ações e que, portanto, poderiam adotar posicionamentos semelhantes, os entendimentos são bastante divergentes: a Microsoft recentemente defendeu a tese de que o critério determinante deveria ser a localização dos dados[258]; a Google, por sua vez, a de que o critério deveria ser o local da sede da empresa responsável pelos serviços (no caso Google Inc., nos Estados Unidos)[259]; já o Facebook argumenta que o critério deveria ser aquele previsto nos termos de uso da plataforma[260]; e a Netflix que esse critério deveria ser o país de incorporação da empresa[261].

---

[256] Desse grupo fariam parte, por exemplo: Jennifer Daskal, defendendo que a ubiquidade dos dados na Internet torna sua regulação incompatível com as noções territoriais de jurisdição; David Cole e Frederico Fabbrini, defendendo que deveria haver um acordo transatlântico em relação à privacidade, dadas as limitações do atual regime de regulação internacional; Zachary Clopton, defendendo que o poder judiciário deveria analisar o tema da jurisdição de forma especial no contexto da tecnologia; Damon C. Andrews e John M. Newman, defendendo que os conceitos tradicionais de jurisdição precisam passar por uma mudança fundamental, entre outros. Cf. Andrew Woods, Against Data Exceptionalism, p.734.

[257] Desse grupo, além do autor, fariam parte, por exemplo, Jack Goldsmith e Tim Wu, que defendem certo exagero na dificuldade atribuída por determinados autores para estabelecer sistemas de controle e jurisdição sobre fenômenos que acontecem na Internet. Cf. Andrew Woods, Against Data Exceptionalism, p.735.

[258] Cf. "Poder Público pode, em última hipótese, suspender atividades do WhatsApp", diz advogado do Idec, revistaepoca.globo.com, disponível em: <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/09/agora-sim-justica-tem-razao-para-bloquear-o-whatsapp-diz-advogado-do-idec.html>, último acesso em 02/01/2017.

[259] Cf. Rhiannon Williams, Google loses Court of Appeal bid to prevent UK users suing it, The Telegraph, 2015, disponível em http://www.telegraph.co.uk/technology/google/11499649/Google-loses-Court-of-Appeal-bid-to-prevent-UK-users-suing-it.html, último acesso em 27/11/2016.

[260] Cf. FORTUNE, Facebook Loses Another Jurisdiction Fight in Europe, Fortune, disponível em: <http://fortune.com/2016/02/15/facebook-loses-another-jurisdiction-fight-in-europe/>, último acesso em: 27/11/2016. Cf. também Israel approves class action against Facebook, invalidates jurisdiction clause, Geneva Internet Platform Digital Watch, disponível em http://digitalwatch.giplatform.org/updates/israel-approves-class-action-against-facebook-invalidates-jurisdiction-clause; último acesso em 27/11/2016.

[261] Cf. Dutch Government identifies Netflix privacy policy discrepancies but says enforcement outside of Dutch watchdog's jurisdiction, 09/10/2013, disponível em http://www.out-law.com/en/articles/2013/October/dutch-government-identifies-netflix-privacy-policy-discrepancies-but-says-enforcement-outside-of-dutch-watchdogs-jurisdiction/, último acesso em 27/11/2016.

Diante de argumentos tão variados, os tribunais ao redor do mundo também têm decidido a questão de forma pouco uniforme: na França, um tribunal decidiu que a justiça francesa tem jurisdição sobre um caso envolvendo a remoção de uma pintura artística do perfil de um professor francês, rejeitando o argumento do Facebook de que a ação deveria ser proposta na Califórnia, de acordo com seus termos de uso[262]; na Bélgica, uma decisão acatou o argumento do Facebook de que o caso deveria ser julgado na Irlanda, onde os dados coletados pela empresa eram efetivamente processados[263] - poucos meses antes, uma corte superior da Bélgica rejeitou o argumento da Yahoo! no sentido de que a justiça belga não teria jurisdição sobre dados armazenados nos Estados Unidos[264]; na Áustria, a decisão de um tribunal acatou o argumento do Facebook de que não teria jurisdição para apreciar uma ação coletiva proposta pelo cidadão austríaco Max Schrems[265]; em Israel, uma decisão não acatou o argumento do Facebook de que ações contra a rede social seriam de jurisdição da justiça do estado da Califórnia.[266]

Nos Estados Unidos, em 14 de julho de 2016, a corte de apelação do segundo circuito acatou os argumentos da Microsoft no sentido de não reconhecer a jurisdição da justiça estadunidense para determinar a entrega de dados de usuários localizados nos servidores da empresa na Irlanda.[267] A decisão reformou entendimento anterior, que determinava a entrega dos dados às autoridades estadunidenses.[268]

Apesar de se referirem a casos que abarcam discussões jurídicas significativamente diferentes, como o acesso a dados por autoridades ou pedidos de indenização por práticas lesivas aos usuários, as decisões citadas ilustram o amplo espectro de argumentos que

---

[262] Cf. Paris Court Rules Against Facebook in French Nudity Case, BBC News, 12/02/2016, disponível em http://www.bbc.com/news/world-europe-35559036, último acesso em 01/12/2016.

[263] Cf. Facebook Wins Belgian Court Case Over Storing Non-User Data, Bloomberg.com, 2016, disponível em https://www.bloomberg.com/news/articles/2016-06-29/facebook-wins-belgian-court-appeal-over-storing-non-user-data, último acesso em 01/12/2016. Cf. também ANTHONY, Sebastian, Facebook wins privacy case, can track any Belgian it wants, Ars Technica, disponível em: <http://arstechnica.com/tech-policy/2016/06/facebook-wins-privacy-case-against-belgiums-data-protection-authority/>, último acesso em 01/12/2016.

[264] Cf. Nicolas Rol, Court of Cassation definitively confirms Yahoo!'s obligation to cooperate with law enforcement agencies | Lexology, disponível em: <http://www.lexology.com/library/detail.aspx?g=46b1a5f4-1ec4-4318-b7e9-753b23afa79f>, último acesso em 01/12/2016.

[265] Cf. Facebook Privacy Suit Thrown Out By Austrian Court, Fast Company, disponível em: <https://www.fastcompany.com/3048127/fast-feed/facebook-privacy-suit-thrown-out-by-austrian-court>, último acesso em 01/12/2016.

[266] Cf. Israeli Court Might not Let Facebook off the Hook on Litigating in Israel, disponível em: <https://www.law.co.il/en/news/israeli_internet_law_update/2014/12/09/IL-Court-says-Facebook-may-be-forced-to-litigate-in-Israel/>, último acesso em 15/12/2016.

[267] CF. *MICROSOFT V. UNITED STATES*, NO. 14-2985 (2D CIR. 2016).

[268] Cf. Zack Whittaker, U.S. search warrant can acquire foreign cloud, email data, judge rules, ZDNet, disponível em: <http://www.zdnet.com/article/u-s-search-warrant-can-acquire-foreign-cloud-email-data-judge-rules/>, último acesso em 02/12/2016.

podem ser apresentados pelas empresas do setor de Internet para tentar se esquivar da jurisdição dos tribunais. Nesse sentido, o fato de que, na Internet, os dados estão "em todo e qualquer lugar"[269] facilita a construção de múltiplas teses jurídicas a respeito dos critérios determinantes de jurisdição, jogando fumaça à discussão ao invés de aclará-la.

A inexistência de regras claras a respeito dos critérios definidores de jurisdição somada à multiplicidade de linhas argumentativas adotadas pelas empresas do setor de Internet tornam a tarefa da justiça estadunidense de decidir sobre o preenchimento desse requisito extremamente complexa, desafiadora e imprevisível. Além disso, a deferência da seção 187, no caso do estado da Califórnia, acaba dando prevalência às regras sobre legislação aplicável contidas nos termos de uso e políticas de privacidade, que são definidos pelas empresas e não pelos usuários.

Em resumo: se a análise sobre a definição da jurisdição sobre a demanda cabe à justiça estadunidense e se do resultado dessa mesma análise depende o reconhecimento das ordens judiciais estrangeiras, é razoável concluir que ela também abre margem para um certo grau de discricionariedade dos juízes estadunidenses em relação às ordens que serão e as que não serão reconhecidas.

4.2. Jurisdição a qualquer custo: legislações nacionais e propostas de regionalização da Internet

As crescentes disputas em torno da extensão do alcance da jurisdição em casos envolvendo a Internet e, em especial, a resistência de algumas empresas do setor a se submeter à jurisdição de todos os países em que atuam têm gerado reações por parte dos Estados. Nesse contexto, têm ganhado força propostas legislativas nacionais no sentido de assegurar aos Estados jurisdição sobre os casos que, de alguma forma, trazem impactos para seus cidadãos ou para o seu território.

Em geral, essas propostas se baseiam na utilização de medidas nacionais para aumentar o alcance da própria jurisdição dos Estados. É o que Bertrand De La Chapelle e Paul Fehlinger chamam de "hiper-territorialização", que se manifestaria ou pela tentativa

[269] Expressão cunhada por Jennifer Daskal ("data is everywhere and anywhere"). Cf. Jennifer Daskal, The Un-Territoriality of Data, Yale Law Journal, vol. 125, n.2, p.326.

de extensão da soberania para além das fronteiras nacionais (extraterritorialidade) ou pelo fortalecimento da própria ideia de território. Na visão dos autores, esse apego à noção de território é inócuo e perigoso na medida em que simplesmente tenta transpor para o contexto da Internet visões ultrapassadas de soberania, o que desencadearia uma situação de disputa baseada na ação unilateral e descoordenada de Estados nacionais. [270]

No novo Regulamento Geral de Proteção de Dados, por exemplo, como se viu, adotou-se regra que consagra a hipótese de aplicação extraterritorial de seus dispositivos, determinando que eles também são aplicáveis a operações que envolvam dados de indivíduos residentes no território da União Europeia, independentemente de o ator responsável pelo tratamento dos dados pessoais estar sediado fora dele, desde que as atividades de tratamento estejam relacionadas *(i)* com a oferta de bens e serviços a titulares de dados pessoais residentes na União Europeia; ou *(ii)* com o controle de seu comportamento (RGPD, art. 3º, 2).

No Brasil, a inserção do artigo 11 ao texto do projeto de lei nº 2126/2011, que deu origem ao Marco Civil da Internet também exemplifica esse fenômeno. O artigo é o que estabelece as hipóteses de aplicação da legislação brasileira, nos seguintes termos:

> "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**.
>
> § 2º O disposto no **caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior**, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
>
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
>
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo." (destaques nossos)

De acordo com Francisco Brito Cruz, a inclusão do artigo decorreu de dois fatores

[270] Cf. Bertrand De La Chapelle / Paul Fehlinger, Jurisdiction on the Internet: from legal arms race to transnational cooperation, Internet and Jurisdiction paper, 2016, disponível em http://www.internetjurisdiction.net/uploads/pdfs/Papers/IJ-Paper-Jurisdiction-on-the-Internet.pdf, último acesso em 18/12/2016, p.9-10.

principais: *(i)* a repercussão das denúncias de Edward Snowden, que teriam instado o Poder Legislativo a oferecer uma "resposta política" aos Estados Unidos e às grandes empresas de Internet, no sentido de reafirmar a soberania nacional e a necessidade de cumprimento da legislação brasileira; e *(ii)* a frequente utilização, em casos que tramitavam perante a justiça brasileira, por parte das empresas do setor de Internet, do argumento de que não estariam submetidas à sua jurisdição, seja porque os dados estavam armazenados em servidores fora do território nacional, seja porque seus serviços estariam sendo prestados diretamente pelas suas respectivas matrizes, sediadas no exterior.[271]

Se, por um lado, o artigo 11 do Marco Civil da Internet torna clara a aplicação da legislação brasileira no caso de desempenho das referidas atividades, conferindo jurisdição sobre empresas que ofertem produtos e serviços ao mercado brasileiro, ainda que por pessoas jurídicas sediadas no exterior, de outro, continua dependente do processo de reconhecimento e execução de ordem judicial estrangeira se pretender atingir empresas que não tenham representação no Brasil, mas sim nos Estados Unidos.

Além de mecanismos como esses, que tentam reafirmar a jurisdição dos Estados sobre empresas de Internet sediadas no exterior, outras estratégias legislativas têm sido adotadas no sentido de facilitar o acesso dos Estados nacionais a essas empresas. As chamadas "leis de localização de dados" (*data localization laws*) são elaboradas nesse contexto e estabelecem regras como o armazenamento obrigatório de dados em servidores localizados dentro de seus territórios, garantindo, assim, a sua jurisdição sobre operações que os envolvam.

Na mesma linha, outras propostas apostam também em soluções técnicas, defendendo a implementação de redes segmentadas territorialmente ou de serviços de Internet operacionalizados pelo próprio Estado, como a criação de provedores de e-mails ou redes sociais nacionais. Depois das denúncias feitas por Edward Snowden, essas propostas ganharam força, inclusive no Brasil.[272]

Francisco Brito Cruz assinala que, durante o processo de elaboração legislativa do Marco Civil da Internet, cogitou-se inserir na lei um dispositivo que obrigaria as empresas provedoras de aplicações de Internet a manter, em *data center* localizado em território

[271] Cf. Francisco Brito Cruz, Direito, Democracia e Cultura Digital: a experiência de elaboração legislativa do Marco Civil da Internet, dissertação de mestrado, Faculdade de Direito, Universidade de São Paulo, São Paulo, 2015, pp. 111-115.

[272] O governo brasileiro chegou a anunciar que considerava algumas medidas, como o incentivo ao desenvolvimento de serviços de Internet nacionais, como provedores de e-mail. Cf. On Internet, Brazil is beating US at its own game, disponível em: <http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html>, acesso em: 23/12/16.

nacional, cópia dos dados pessoais coletados e armazenados a respeito de usuários localizados no Brasil.[273] Em outros países, há propostas similares: na Rússia, por exemplo, foi aprovada lei que obriga que os servidores de empresas que realizam o tratamento de dados pessoais de usuários na Rússia estejam localizados no seu território.

Propostas como essas, que tentam importar a lógica de territorialidade para a Internet, são duramente criticadas por aqueles que defendem que a arquitetura aberta e livre da rede é o que garante sua neutralidade, universalidade e, mais importante, o que sustenta a era da informação.[274] Seria o que esse grupo de críticos convencionou chamar de "balcanização da Internet", em alusão à fragmentação do império otomano.[275]

Na prática, enquanto propostas como essas também não equacionam a questão, dadas as limitações e dificuldades para reconhecer e executar ordens judiciais estrangeiras nos Estados Unidos para a responsabilização de atores unicamente lá sediados conforme evidenciou-se até aqui, multiplicam-se decisões que apostam em saídas mais radicais, como as ordens de bloqueio de aplicações de Internet, dirigidas aos intermediários localizados em seu território.

4.3. Bloqueios de aplicações de Internet como fronteiras artificiais dos Estados

Equalizar as situações de impasse e assimetria descritas no item anterior não é uma tarefa simples. Como visto, na Internet, as colisões entre ordens jurídicas são geralmente traduzidas em disputas por jurisdição.[276] Nessas disputas, as regras do jogo seguem baseadas em uma lógica ditada pelos conceitos de soberania e território, o que dificulta sua transposição para os fenômenos que acontecem no ciberespaço.

Jack Goldsmith e Tim Wu alertam que, ao longo dos últimos anos, a forma como essas disputas foram conduzidas acabaram contribuindo para o desenvolvimento de uma

[273] Cf. Francisco Brito Cruz, Direito, Democracia e Cultura Digital: a experiência de elaboração legislativa do Marco Civil da Internet, pp. 112-113.
[274] Cf. Eugene Kaspersky, What will happen if countries carve up the internet?, The Guardian, 17/12/2013, disponível em https://www.theguardian.com/media-network/media-network-blog/2013/dec/17/internet-fragmentation-eugene-kaspersky, último acesso em 23/12/2016.
[275] Para as origens do termo aplicado ao contexto da Internet, cf. Alves Jr., Sergio, The Internet Balkanization Discourse Backfires, 2014, disponível em https://ssrn.com/abstract=2498753, último acesso 23/12/2016.
[276] Cf. Jacqueline de Souza Abreu, From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp , *Columbia Journal of Transnational Law*.

série de estratégias e tecnologias de zoneamento da Internet, como os mecanismos de identificação e bloqueio de acesso por origem da conexão (*geo-blocking*).[277]

Na verdade, essa é uma tendência que começou a ser observada a partir do ano 2000, após a decisão do já mencionado caso *LICRA v. Yahoo!*.[278] Em resumo, o litígio envolveu a subsidiária da Yahoo! na França, que foi acionada por duas entidades ligadas à proteção de direitos humanos, em razão do oferecimento, pela empresa, de um mecanismo de leilão *online* contendo, dentre outros itens, objetos ligados ao período nazista, além de informações e materiais relativos à ideologia antissemita. Baseada na legislação penal francesa, que proíbe a disseminação de conteúdos que façam apologia ao nazismo, as entidades visavam a impedir o funcionamento do serviço na França, requerendo que a subsidiária francesa fosse proibida de disponibilizar *links* e anúncios que direcionassem usuários localizados na França (*i.e.* do website www.yahoo.fr) para o site principal da empresa (www.yahoo.com), hospedado nos Estados Unidos, no qual eram oferecidos os referidos artigos proibidos.

Além de questionar a competência da justiça francesa para julgar o caso, a Yahoo! se defendeu alegando que, por se tratar de serviço essencialmente voltado aos cidadãos estadunidenses, o nível de proteção conferido à liberdade de expressão que deveria prevalecer era aquele adotado nos Estados Unidos, segundo o qual a realização do leilão no país era considerada lícita. Naquela época, a empresa defendeu, ainda, ser tecnicamente impossível impedir que apenas os usuários localizados na França acessassem o serviço, o que a obrigaria a indisponibilizá-lo como um todo. Esse argumento técnico foi derrubado por peritos do caso, segundo os quais seria sim possível identificar os usuários localizados na França por meio de seu endereço IP e, a partir disso, implementar um filtro que bloqueasse acessos oriundos do país.

Em novembro de 2000, a sentença francesa determinou que a Yahoo! tomasse todas as providências necessárias para impedir o acesso de usuários localizados na França aos leilões de artigos nazistas, sob pena de multa diária.[279]

Ao longo dos últimos anos, disputas como essa se tornaram mais comuns, complexas e diversificadas e sua solução passou a envolver medidas drásticas. Estados

[277] Cf. Jack Goldsmith e Tim Wu, Who Controls the Internet, pp. 58-63.
[278] Cf. França, Le tribunal de grande instance de Paris, La Ligue contre le racisme e l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Societe Yahoo! France, n. 00/05308, julgado em 20.11.2000.
[279] Cf. França, Le tribunal de grande instance de Paris, La Ligue contre le racisme e l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Societe Yahoo! France, n. 00/05308, Ordonance de référé, julgado em 20.11.2000.

como o Irã, Paquistão, Iraque e China já determinaram o bloqueio completo de acesso ao Youtube por supostas violações às suas legislações nacionais.[280] Em 2014, o acesso à plataforma de vídeos Vimeo foi bloqueado na Indonésia por conter vídeos com cenas de nudez, o que contrariaria a legislação que restringe a pornografia no país.[281] Por motivos similares, o Twitter também já foi alvo de bloqueios em países como Irã[282], China[283], Turquia[284] e Egito[285].

Ao contrário do que possa parecer, entretanto, bloqueios não são medidas exclusivas de regimes considerados autoritários. No Brasil, por exemplo, têm ganhado notoriedade as ordens de bloqueio do aplicativo de mensagens WhatsApp, em razão da suposta recusa da empresa em fornecer dados de usuários às autoridades brasileiras.[286]

Em verdade, como anota Jacqueline Abreu, ordens de bloqueio como essas surgem de verdadeiros impasses jurídicos. Nesse sentido, "*originam-se de disputas que envolvem debates complexos sobre extensão da jurisdição nacional sobre serviços digitais, cumprimento de sentenças nacionais por empresas estrangeiras e não sediadas no país, limites da liberdade de expressão em face da proteção a outros direitos, abrangência da proteção da iniciativa privada e da inovação e até a utilização de tecnologias como a criptografia*".[287]

Apesar das diferenças que estão por trás de cada caso de bloqueio, o seu princípio de atuação mais comum é operar na camada de infraestrutura da Internet na tentativa de restringir completamente o acesso a determinados aplicativos, serviços e conteúdos. É justamente por se direcionar aos intermediários locais, isto é, àqueles que compõem a

---

[280] Cf. Google Transparency Report, <disponível em On Internet, Brazil is beating US at its own game, disponível em: <http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html>, acesso em: 3 jan. 2017., último acesso em 24.4.2014>.

[281] Cf. Dara Kerr, "Vimeo Banner in Indonesia for Allegedly Hustling Porn", CNET (13.5.2014), <disponível em http://www.cnet.com/news/vimeo-banned-in-indonesia-for-allegedly-hustling-porn/, último acesso em 26.6.2016>.

[282] Cf. Brian Ries / Lorenzo Franceschi-Bicchierai,"Facebook, Youtube, Twitter Blocked in Iraq Amid Crisis", Mashable (13.6.2014), <disponível em http://mashable.com/2014/06/13/facebook-youtube-twitter-blocked-iraq/, último acesso em 26.9.2016>.

[283] Cf. Jerin Mathew, "China Defends Blocking Facebook, Twitter and Bloomberg", International Business Times (16.01.2014), <disponível em http://www.ibtimes.co.uk/china-defends-blocking-facebook-twitter-bloomberg-1432488, último acesso em 30.09.2016>.

[284] Cf. Terrence McCoy, "Turkey Bans Twitter – and Twitter Explodes, The Washington Post (21.03.2014), <disponíve em http://www.washingtonpost.com/news/morning-mix/wp/2014/03/21/turkey-bans-twitter-and-twitter-explodes/, último acesso em 30.09.2016>.

[285] Cf. Leslie Horn, "Twitter Confirms Egypt Ban", PC Magazine (26.01.2011), <disponível em http://www.pcmag.com/article2/0,2817,2376704,00.asp, último acesso em 30.09.2016>.

[286] Cf. Jacqueline de Souza Abreu, From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp , Columbia Journal of Transnational Law.

[287] Cf. Jacqueline de Souza Abreu, Bloqueios.info: sobre, InternetLab, 2016, disponível em http://bloqueios.info/pt/sobre/, último acesso 18/12/2016.

infraestrutura da rede, como os provedores de conexão à Internet (como NET, VIVO, TIM, etc.), que os bloqueios são estratégias tão eficientes na visão dos Estados nacionais.

De outros pontos de vista, contudo, bloqueios não são considerados boas medidas, principalmente em razão de seus impactos para direitos humanos. Isso porque interferem diretamente na experiência de navegação de Internet dos usuários, prejudicando sua liberdade para procurar, receber e comunicar ideias e informações. Como assinala Jacqueline Abreu, "*bloqueios comprometem o livre fluxo de dados em um país ou região e, potencialmente, o acesso de milhões de pessoas a informações e serviços. Nas recentes ocasiões em que o WhatsApp foi bloqueado no Brasil, por exemplo, mais de 100 milhões de pessoas foram afetadas, o que constitui cerca de 50% da população do país e de 10% dos usuários do aplicativo no mundo*."[288] Os impactos também podem ser negativos para a economia: Ronaldo Lemos, baseando-se em estudo elaborado pelo Instituto Brookings, comenta que os bloqueios do WhatsApp teriam custado mais de 360 milhões de reais à economia brasileira.[289]

A despeito das consequências sérias que podem gerar, ordens de bloqueios têm sido cada vez mais frequentes. De acordo com a plataforma "Bloqueios.info", no Brasil, por exemplo, das 11 ordens judiciais que já determinaram bloqueios a aplicações de Internet no país, 7 delas foram proferidas nos últimos dois anos (2015 e 2016).[290]

O aumento do número de casos envolvendo bloqueios sugere que esse tipo de medida tem sido a resposta encontrada pelos Estados nacionais para lidar com as dificuldades de acesso e responsabilização de atores privados que não estejam sediados no seu território e que, mesmo assim, por meio da Internet, atuam em suas jurisdições.

Nessa nota, Bertrand De La Chapelle e Paul Fehlinger apontam que o radicalismo dessas medidas pode ter origem na sensação de impotência de autoridades e governos, que vêem frustradas as suas tentativas de fazer valer suas legislações nacionais em face desses atores. Isso pode dar origem, então, a estratégias que pretendam reerguer as fronteiras territoriais de aplicação do direito, criando uma espécie de "soberania digital".[291]

---

[288] Cf. Jacqueline de Souza Abreu, Bloqueios.info: sobre, InternetLab, 2016, disponível em http://bloqueios.info/pt/sobre/, último acesso 18/12/2016.
[289] Cf. Ronaldo Lemos, Bloqueio à internet no Brasil custou mais de R$ 360 milhões, Folha de São Paulo, 24/10/2016, disponível em http://www1.folha.uol.com.br/colunas/ronaldolemos/2016/10/1825554-bloqueio-a-internet-no-brasil-custou-r-360-milhoes.shtml, último acesso em 12/12/2016.
[290] Cf. www.bloqueios.info
[291] Cf. Bertrand De La Chapelle / Paul Fehlinger, Jurisdiction on the Internet: from legal arms race to transnational cooperation, p.4.

Jack Goldsmith e Tim Wu acrescentam ainda que a adoção dessas medidas é possível pelo fato de sempre existirem "intermediários locais" na Internet, o que abre caminho para que os Estados se utilizem de sua presença territorial para criar fronteiras artificiais no ciberespaço.[292] Como se mencionou, esses intermediários locais vão desde provedores de conexão à Internet, contra quem as ordens de bloqueio costumam ser direcionadas, por exemplo, até instituições como bancos, que podem ser instados a impedir transações financeiras com determinadas empresas, por exemplo.[293] Para os autores, isso é significativo na medida em que gera uma espécie de poder de "coerção territorial governamental" sobre a Internet.[294]

A forma como os Estados decidem fazer uso desse poder pode ser determinante para o futuro da Internet na medida em que coloca à disposição dos Estados a adoção de modelos rígidos de controle baseados na lógica territorial, como tem-se observado no caso da China, por exemplo. É a partir do poder coercitivo sobre a camada de infraestrutura da rede que são viabilizadas muitas formas de controle da rede.

Ao longo deste capítulo, demonstrou-se que existem sérios obstáculos para a adoção de medidas tradicionais - ou "diplomáticas" - de acesso e responsabilização de atores privados sediados nos Estados Unidos, especialmente no que diz respeito à possibilidade de reconhecimento e execução de ordens judiciais estrangeiras envolvendo violações a legislações nacionais de proteção de dados, objeto que interessa a esta tese.

Se não equacionados, esses obstáculos podem alimentar a proliferação de medidas radicais, como é o caso das ordens de bloqueio de aplicações de Internet, e ameaçar a dimensão livre e aberta a partir da qual a sua arquitetura foi concebida. Ao mesmo tempo, enquanto não forem dirimidas as incertezas que rondam a determinação da jurisdição na Internet, os Estados nacionais continuarão sem mecanismos jurídicos efetivos para promover a responsabilização desses atores fora de seus territórios. Nesse sentido, essas incertezas servem de escudo às próprias empresas do setor, que podem continuar explorando suas múltiplas teorias e divergências, esquivando-se da execução de ordens judiciais estrangeiras e protelando a resolução de ações de responsabilização que venham a ser impostas contra elas nos Estados Unidos.

---

[292] Cf. Jack Goldsmith e Tim Wu, Who Controls the Internet, p.63.
[293] É o caso da Argentina no Uber, cf. Argentinian Telecoms (and Credit Cards) Ordered to Block UBER App, disponível em: </blog/2016/05/argentinian-telecoms-and-credit-cards-ordered-block-uber-app>, último acesso em 22/12/2016.
[294] Cf. Jack Goldsmith e Tim Wu, Who Controls the Internet, pp. 179-184.

Portanto, essa situação de indefinição agudiza as tensões e embates jurídicos que têm sido travados e exige a formulação de novas estruturas transnacionais de governança que sejam capazes de encerrar as dúvidas ligadas à jurisdição e legislação aplicável no contexto da Internet, tornando consideravelmente mais viáveis os processos de reconhecimento e execução de ordens judiciais estrangeiras, mecanismos jurídicos que podem ser tão úteis para remediar a interferência de atores não-estatais em jurisdições nas quais não estão sediados. O capítulo a seguir aprofunda as consequências dessa insuficiência de mecanismos jurídicos para promover a responsabilização desses atores nos Estados Unidos e suas repercussões para os Estados nacionais e o direito constitucional.

CAPÍTULO 5 - A INTERNET NAS MÃOS DA CALIFÓRNIA: A INTERFERÊNCIA DE ATORES NÃO-ESTATAIS NA TUTELA DE DIREITOS FUNDAMENTAIS

Ao longo desta tese, ilustrou-se de que forma a arquitetura da Internet viabilizou operações globalizadas de monitoramento e coleta de dados pessoais por parte de atores privados, potencializando a sua atuação em jurisdições nas quais não estão sediados. Além disso, demonstrou-se que as características do modelo regulatório de privacidade adotado nos Estados Unidos dificultam a responsabilização de atores unicamente lá sediados em relação a potenciais violações de normas constitucionais e leis de proteção de dados estrangeiras, seja pelas limitações de atuação da Comissão Federal do Comércio, seja pelos obstáculos para o reconhecimento e execução de ordens judiciais estrangeiras.

Essa dificuldade agudiza, portanto, a interferência desses atores na tutela e regulação do direito à privacidade pelos Estados nacionais. A proposta deste capítulo é a de oferecer subsídios para que essa discussão seja aperfeiçoada à luz das premissas e propostas ligadas ao constitucionalismo transnacional.

5.1. Constitucionalismo transnacional: disputas teóricas

Acirrado pelo processo de globalização, o fenômeno do entrelaçamento de dois ou mais ordenamentos jurídicos tem sido estudado a partir de diferentes perspectivas não só do ponto de vista do direito constitucional, como também do direito internacional, da sociologia jurídica e da filosofia do direito.

Dentro das teorias ligadas ao direito constitucional, um lado do debate se preocupa com o futuro do constitucionalismo, aqui simplesmente entendido como o movimento político-jurídico a partir do qual as constituições dos Estados nacionais modernos se

desenvolveram.[295] Nesse sentido, diante da relativização do conceito de território e de suas consequentes repercussões para o conceito de soberania, discute-se em que medida o Estado não teria deixado de ocupar uma posição central nos processos de constitucionalização, dando espaço para uma ou várias formas de "constitucionalismo além do Estado", ou, como preferiu-se adotar neste tese, de "constitucionalismo transnacional".[296]

Apesar das profundas diferenças que marcam essa discussão, parece haver relativo consenso em relação à existência de uma ameaça que ronda o constitucionalismo enquanto movimento centrado na figura do Estado nacional. Isso se deve, em linhas gerais, à multiplicação das relações transfronteiriças, que acentuam um descompasso entre as esferas políticas e a noção de Estado.[297]

As divergências começam a ficar mais aparentes em relação ao que se pode esperar do futuro. De um lado, alguns autores adotam posicionamentos mais céticos, creditando à figura do Estado um papel essencial para o constitucionalismo, seja enquanto estrutura de legitimação das decisões políticas, seja enquanto unidade de poder soberano. Nesse sentido, não apostam em propostas que vislumbram estender para além do Estado um

[295] A definição do que se entende por constitucionalismo varia de acordo com o que se entende por constituição. Ressaltando não haver consenso a respeito do próprio conceito de constituição, Nico Krisch destaca que há visões igualmente divergentes a respeito do componente normativo do conceito de constitucionalismo: "para alguns, ele precisa ser direcionado a uma constituição em um dos sentidos mencionados acima; para outros, ele significa um movimento em direção a ideais de liberdade, democracia e boa governança; e às vezes ele também é tido como representativo de uma expansão desses objetivos do sistema político para estratos mais amplos da sociedade, incluindo o direito privado e as relações entre indivíduos". Cf. Nico Krisch, Beyond Constitutionalism: The Pluralist Structure of Postnational Law", Oxford University Press, 2010, p.39 (tradução livre). No mesmo sentido, Martin Loughlin anota que "a teoria do constitucionalismo exerceu tamanho impacto na elaboração de documentos constitucionais que ela é frequentemente entendida como equivalente ao próprio conceito de constituição moderna". Cf. Martin Loughlin, What is Constitutionalisation?, p. 55 (tradução livre), *in* Petra Dobner e Martin Loughlin (Orgs.), The Twilight of Constitutionalism?, Oxford University Press, 2010. Sendo assim, se o objetivo deste capítulo é promover uma reflexão que leve em conta o pensamento de diferentes autores a respeito do futuro do constitucionalismo e de sua possível faceta transconstitucional, não faz sentido tentar cravar uma única definição para o conceito, mas sim fazer referência aos diferentes pontos de vista defendidos pelos autores sempre que necessário.

[296] O fenômeno é tratado sob várias nomenclaturas diferentes, como transconstitucionalismo (Marcelo Neves), constitucionalismo social global (Gunther Teubner), constitucionalismo cosmopolitano (Mattias Kumm); constitucinalismo transnacional (Petra Dobner), entre outros. Para fins desta tese, preferiu-se adotar o termo proposto por Petra Dobner, por parecer o mais abrangente: "O constitucionalismo transnacional é aqui entendido num sentido abrangente como um denominador comum para várias tentativas de estender o projeto de lei global para além do quadro tradicional do direito internacional público. Por conseguinte, ultrapassa o tipo de lei que apenas diz respeito às relações entre Estados soberanos e organizações intergovernamentais." (tradução livre) Cf. Petra Dober, More Law, Less Democracy? Democracy and Transnational Constitutionalism, p. 148. *in* Petra Dobner e Martin Loughlin (Orgs.), The twilight of constitutionalism?, Oxford ; New York: Oxford University Press, 2010.

[297] Cf. Petra Dobner e Martin Loughlin, Introduction, in *Ibid*. (comentando ser essa uma das poucas questões sobre as quais há consenso dentre aqueles que discutem o fenômeno da globalização).

modelo de constitucionalização.[298] De outro lado, situam-se autores que defendem relativa autonomia do modelo constitucionalista em relação à figura do Estado, abrindo caminho para formulações que buscam formas de legitimação das esferas transnacionais de decisão política e novas estruturas de governança e equalização de poder.[299]

No centro dessas teorias parecem estar preocupações de duas naturezas distintas: a primeira estaria ligada ao possível deslocamento das fontes emissoras de normas para além dos Estados nacionais, abrindo espaço para a produção normativa de novos atores, como os do setor privado ou organismos internacionais[300]; já a segunda estaria ligada aos desafios gerados pela sobreposição das normas emanadas nessa nova ordem transnacional, que ocupariam níveis diferentes mas não hierárquicos, tornando complexa a resolução de eventuais colisões.[301]

Dentro do campo do direito internacional, disputam-se teorias a respeito da existência e das características de um possível movimento em direção à

[298] Podem ser incluídos nesse grupo, por exemplo, Dieter Grimm e Petra Dobner. Para Dieter Grimm, não é possível pensar no constitucionalismo sem pensar nas suas conquistas, intrinsecamente ligadas às suas condições constitutivas, que pressupõem a figura das constituições nacionais, não havendo espaço para a reconstrução do constitucionalismo nos planos internacional ou transnacional. Cf. Dieter Grimm, The Achievement of Constitutionalism and its Prospects in a Changed World, pp. 5-13, *in* Petra Dobner; Martin Loughlin (Orgs.), The twilight of constitutionalism?. Petra Dobner é pessimista em relação à possibilidade de exercício de uma autoridade pública em um arranjo globalizado; para ela, isso implicaria perda de controle democrático. Cf. More Law, Less Democracy? Democracy and Transnational Constitutionalism, pp. 160-161, *in* Petra Dobner; Martin Loughlin (Orgs.), The twilight of constitutionalism?.

[299] Podem ser incluídos nesse grupo, por exemplo, Mattias Kumm e Gunther Teubner. Para Mattias Kumm, os processos transnacionais exigem uma "guinada cosmopolita" dos Estados em direção a uma nova realidade de legitimidade, havendo espaço para que isso seja aconteça sem que haja uma completa dissociação com o constitucionalismo. Cf. Mattias Kumm, The Cosmopolitan Turn in Constitutionalism: An Integrated Conception of Public Law, *Indiana Journal of Global Legal Studies*, v. 20, n. 2, p. 605–628, 2013. Gunther Teubner se propõe a pensar sobre um novo conceito de constituição que seja adequado para o novo contexto transnacional. Cf. Gunther Teubner, Fragmentos Constitucionais - Constitucionalismo social na globalização, Ed. Saraiva, 2016, pp. 23-29.

[300] A esse respeito, por exemplo, cf. Gunther Teubner, Fragmentos Constitucionais - Constitucionalismo social na globalização, p.24 (definindo a "transnacionalização do Político"); cf. também Dieter Grimm, The Achievement of Constitutionalism, p. 4 (comentando as repercussões desse deslocamento).

[301] Nesse sentido, Virgílio Afonso da Silva esclarece que, quando se fala em transconstitucionalidade, "pode-se querer fazer menção a formas distintas de se garantir o mesmo direito ou a formas distintas de se solucionar uma mesma colisão entre direitos (seja em abstrato, seja em um caso concreto específico)." No primeiro caso, esse "tipo de colisão ocorre quando a proteção de um determinado direito, no texto de uma constituição nacional, é mais ampla ou mais restrita que a proteção do mesmo direito em nível transnacional". Cf. Virgílio Afonso da Silva, "Colisões de direitos fundamentais entre ordem nacional e ordem transnacional", *in* Marcelo Neves, *Transnacionalidade do direito: novas perspectivas dos conflitos entre ordens jurídicas*, São Paulo: Quartier Latin, 2010, p. 101. Nesse mesmo sentido, Marcelo Neves destaca que o "problema fundamental é precisar que os problemas constitucionais surgem em diversas ordens jurídicas, exigindo soluções fundadas no entrelaçamento entre elas. Assim, um mesmo problema de direitos fundamentais pode apresentar-se perante uma ordem estatal, local, internacional, supranacional e transnacional (no sentido estrito) ou, com frequência, perante mais de uma dessas ordens, o que implica cooperações e conflitos, exigindo aprendizado recíproco." Cf. Marcelo Neves, Transconstitucionalismo, Martins Fontes, São Paulo, 2009, p.121.

constitucionalização global.[302] Dentre elas, destacam-se aquelas que discutem modelos de constitucionalização setorial em oposição àquelas que anteveem a formação de uma nova ordem mundial, calcada em um ordenamento jurídico transnacional único.[303] Aqui também os autores se dividem entre os mais céticos e os mais otimistas, seja enfatizando as vantagens de se reconhecer uma estrutura normativa capaz de oferecer novas estruturas legítimas de governança política no plano transnacional[304], seja chamando a atenção para os obstáculos de movimentos de constitucionalização com essas proporções[305].

Seja no campo do direito constitucional, seja no campo do direito internacional, parece ser possível identificar dois tipos diferentes de abordagem propostas: *(i)* descritiva, que se preocupa em identificar as características dos fenômenos transfronteiriços e das novas questões transnacionais e classificá-las de acordo com as suas semelhanças ou diferenças em relação àquilo que conceituam como constitucionalismo; e *(ii)* normativa, que se preocupa em pensar novos arranjos jurídicos e institucionais que possam viabilizar a construção de estruturas de governança transnacionais de forma legítima e eficiente.

Nenhuma dessas frentes de análise, entretanto, parece levar em consideração de maneira satisfatória algumas particularidades dos dilemas que são delineados dentro e a partir da Internet, especialmente no que tange à possibilidade de interferência de atores privados na regulação e tutela de direitos fundamentais, objeto de estudo desta tese.

Sendo assim, a partir das conclusões a respeito dos desafios da tutela do direito à privacidade na Internet extraídas desta tese, o objetivo deste capítulo é contribuir com essas frentes de análise da seguinte forma: no caso da primeira (descritiva), a intenção é oferecer subsídios empíricos que permitam refinar os diagnósticos que são feitos a respeito desses fenômenos, particularmente em relação aos tipos de atores e suas formas de interferência na ordem jurídica dos Estados nacionais; no caso da segunda (normativa), a intenção é apresentar as dificuldades de se pensar em arranjos jurídicos e institucionais que ofereçam respostas satisfatórias para a tutela da privacidade na Internet no plano

[302] Jan Klabbers, por exemplo, chama a atenção para a insuficiência de evidências empíricas que poderiam comprovar a existência, de fato, de um movimento de constitucionalização global. Cf. Jan Klabbers, Anne Petters e Geir Ulfstein, The Constitutionalization of International Law, Oxford University Press, 2009, p. 4.
[303] Cf. Aoife O'Donoghue, Constitutionalism in Global Constitutionalisation, Cambridge University Press, 2014.
[304] Cf. Aoife O'Donoghue, Constitutionalism in Global Constitutionalisation, p. 148–151.
[305] Douglas Johnston cita fatores que colocariam em xeque a própria viabilidade de se pensar em um modelo como esse, como o apego de muitas cortes ao formalismo jurídico e as dificuldades para se superar diferenças culturais na definição de uma única ordem global. Cf. Douglas Johnston, World Constitutionalism, in Ronald MacDonald e Douglas Johnston (eds.), Towards World Constitutionalism - Issues in the Legal Ordering of the World Community, Leiden: Martinus Nijhoff, 2005, pp. 17-20.

transnacional, destacando as limitações de seus mecanismos de implementação e responsabilização no caso de violações (*enforcement*) a partir da experiência encampada pela Organização das Nações Unidas ("ONU"). Dessa forma, espera-se contribuir para o aprofundamento das teorias sobre o constitucionalismo transnacional no que diz respeito à sua interface com a Internet.

Para tanto, este capítulo se propõe a adicionar três argumentos principais ao debate: *(i)* a arquitetura da Internet modificou significativamente a forma de atuação de atores privados na tutela direitos fundamentais, abrindo caminho para a interferência de novos tipos de atores na regulação adotada pelos ordenamentos jurídicos nacionais; *(ii)* a concentração desses atores nos Estados Unidos, aliada às características do seu modelo regulatório, provoca uma situação de prevalência dos graus de proteção estadunidenses em relação a graus estabelecidos em outras jurisdições; e *(iii)* as propostas de compatibilização e resolução das colisões entre modelos regulatórios de privacidade no plano internacional precisam estar acompanhadas de mecanismos jurídicos de *enforcement*.

5.2. Da Califórnia para o mundo: quem são os novos atores transnacionais?

A interferência de atores não-estatais na regulação de determinados setores no plano transnacional tem sido estudada há algum tempo, especialmente no que diz respeito à ampliação de sua capacidade de produção normativa. Gunther Teubner, por exemplo, já se dedicou particularmente a essa questão, assinalando ser a "privatização do Político" uma das principais causas para a crise do constitucionalismo moderno.[306] Para o autor, pouca atenção tem sido dada ao rápido crescimento daquilo que chama de "regimes jurídicos privados" ou "não-estatais".[307] No mesmo sentido, Martin Loughlin alerta para o crescimento das atividades regulatórias que têm sido exercidas em searas transnacionais, alheias ao controle das constituições nacionais.[308]

[306] Cf. Gunther Teubner, Fragmentos Constitucionais - Constitucionalismo social na globalização, p.24.
[307] Cf. Gunther Teubner, Fragmented Foundations, p. 331. DOBNER; LOUGHLIN (Orgs.), The twilight of constitutionalism?
[308] Cf. Martin Loughlin, What is Constitutionalisation?, p. 47.

Gunther Teubner assinala ainda que esses atores podem ser identificados como "atores transnacionais privados", especialmente as "corporações transnacionais".[309] Dieter Grimm acrescenta que os Estados têm, de fato, compartilhado estruturas de poder com um número considerável de atores não-estatais, "a maioria dos quais organizações internacionais a quem se conferiu soberania e cujo exercício escapa dos arranjos das constituições nacionais."[310]

Com isso, estariam se consolidando novas fontes emissoras de normas no plano transnacional, fenômeno que colocaria em xeque o papel central até então ocupado pelos Estados nacionais. A atuação da Federação Internacional de Futebol ("FIFA"), por exemplo, ilustra a regulação de um setor específico, qual seja o da prática profissional de futebol e a participação em seus campeonatos oficiais internacionais, por um ator não-estatal. De forma similar, a Organização da Aviação Civil Internacional ("OACI"), agência especializada da Organização das Nações Unidas ("ONU"), também emite normas de aplicação internacional que disciplinam as atividades de navegação aérea e a organização dos transportes e do tráfego aéreo.

Nesses casos, a discussão envolve atores não-estatais cuja legitimidade para produzir normas se encontra fundada na própria ordem transnacional: a FIFA congrega mais de 200 associações e organizações esportivas e é filiada ao Comitê Olímpico Internacional ("COI"); a OACI se apoia na legitimidade da própria ONU.

No caso dos atores não-estatais aos quais se refere esta tese, quais sejam as empresas do setor de Internet, não se pode dizer que existe uma fonte de legitimidade pré-definida para a sua atuação como emissores de normas de aplicação internacional. Ao contrário, a rigor, eles estão submetidos às normas constitucionais e legislações vigentes nas jurisdições em que atuam. Mesmo assim, como demonstrou-se nesta tese, apropriando-se da arquitetura da Internet, esses atores passaram a ser capazes de interferir de forma significativa na tutela e regulação do direito à privacidade em jurisdições onde não estão sediados, sendo possível afirmar, em alguma medida, que definem as próprias normas e parâmetros que nortearão a sua atuação.

Isso porque, como o modelo regulatório de privacidade adotado nos Estados Unidos é calcado na auto-regulação, os atores privados lá sediados têm certa liberdade para construir suas próprias políticas de privacidade, desde que cumpram com alguns

[309] Cf. Gunther Teubner, Fragmented Foundations, p.328.
[310] Cf. Dieter Grimm, The Achievement of Constitutionalism, p. 4.

princípios, desenvolvidos e fiscalizados pela Comissão Federal do Comércio, sobretudo aqueles ligados à notificação e escolha. Como visto no capítulo 3, a Comissão atua no sentido de coibir práticas desleais e abusivas e, nessa atuação, atende aos ditames da legislação e opções de políticas públicas vigentes nos Estados Unidos, privilegiando o modelo regulatório estadunidense, por limitações de competência e conveniência política.

Nesse sentido, em relação às atividades de monitoramento e coleta de dados pessoais, essas empresas adquirem um grau considerável de discricionariedade para desenvolver suas próprias políticas, isto é, para criar suas próprias regras, desde que não violem a legislação estadunidense ou a jurisprudência da Comissão. As regras emanadas dessas empresas podem, portanto, acabar definindo, na prática, a forma como são coletados e tratados os dados de usuários localizados em outras jurisdições, a despeito da aplicação de suas normas constitucionais e legislações de proteção de dados nacionais. No caso de violações, sua responsabilização encontra obstáculos significativos, em razão do próprio modelo regulatório de privacidade adotado nos Estados Unidos, como também já se demonstrou.

Isso não significa necessariamente que esses atores privados tenham passado a ser fontes *legítimas* de produção normativa no plano transnacional mas sugere, pelo menos, uma capacidade de interferência que não deve ser desconsiderada pelos teóricos que se dedicam à análise de fenômenos como o constitucionalismo transnacional. O objeto de estudo desta tese é justamente este tipo de interferência que, de um lado, pode representar a "exportação" do modelo regulatório de privacidade dos Estados Unidos para outras jurisdições e, de outro, aponta para a própria inclusão desses atores privados como novos tomadores de decisão a respeito das regras sob as quais as atividades de monitoramento e coleta de dados que realizam serão calcadas, na medida em que dificilmente serão responsabilizados por descumprir quaisquer outras.

Um argumento que poderia ser levantado em relação a esse fenômeno seria o fato de que algumas das maiores empresas do setor de Internet já estão fisicamente localizadas em muitas das jurisdições onde atuam, o que facilitaria o acesso a elas e a sua responsabilização por eventuais violações. Faz sentido: a Google tem mais de 70 escritórios em 40 países[311]; o Facebook tem 49 escritórios em mais de 30 países[312]; a

[311] Cf. https://www.google.com/about/company/facts/locations/
[312] Cf. https://newsroom.fb.com/company-info/

Microsoft em mais de 100[313]; e a Uber está presente em 526 cidades ao redor do mundo[314], para citar alguns exemplos.

Vale lembrar, entretanto, que a arquitetura da Internet diminuiu significativamente os "custos de internacionalização" dos atores, cuja presença internacional deixou de depender do estabelecimento de escritórios de representação em outros lugares do mundo. Na Internet, a disponibilização de produtos e serviços pode ser feita em escala global sem que seja necessário incorrer em muitos desses custos, o que nos permite supor que ela tenha incluído novos tipos de atores nesses processos de interferência.

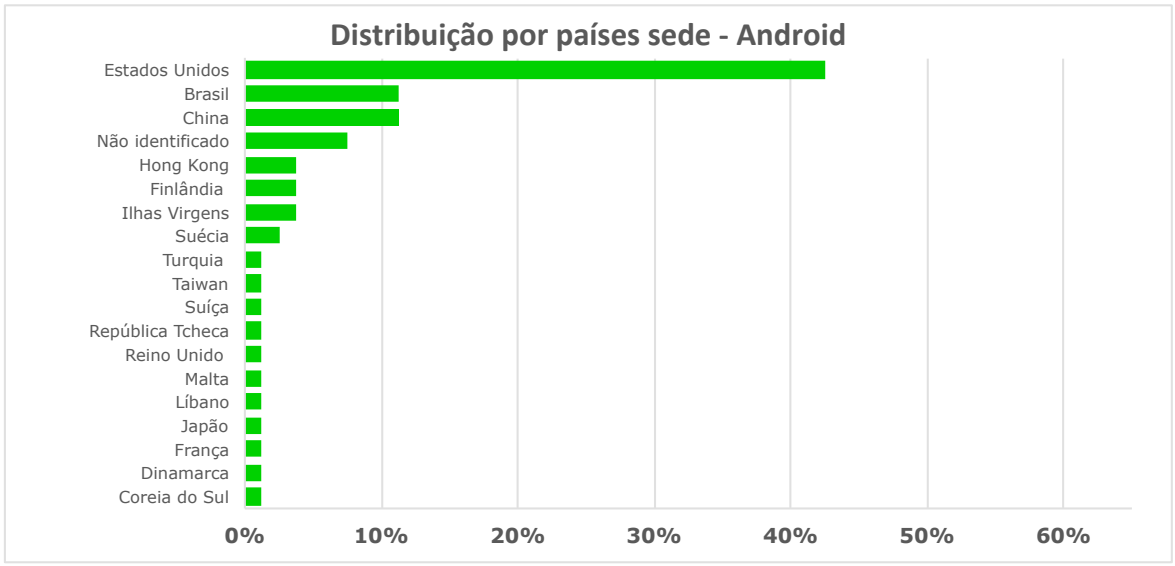
Para investigar em que medida essa hipótese se sustenta, realizamos uma pesquisa que analisou os 80 aplicativos mais populares no Brasil no dia 01/10/2016, segundo as listas disponibilizadas pelas lojas de aplicativos das empresas Google (Android) e Apple visando identificar *(i)* o país onde estão sediados (e, no caso daqueles sediados nos Estados Unidos, também em qual estado se encontram); e *(ii)* se possuem representação comercial no Brasil[315].

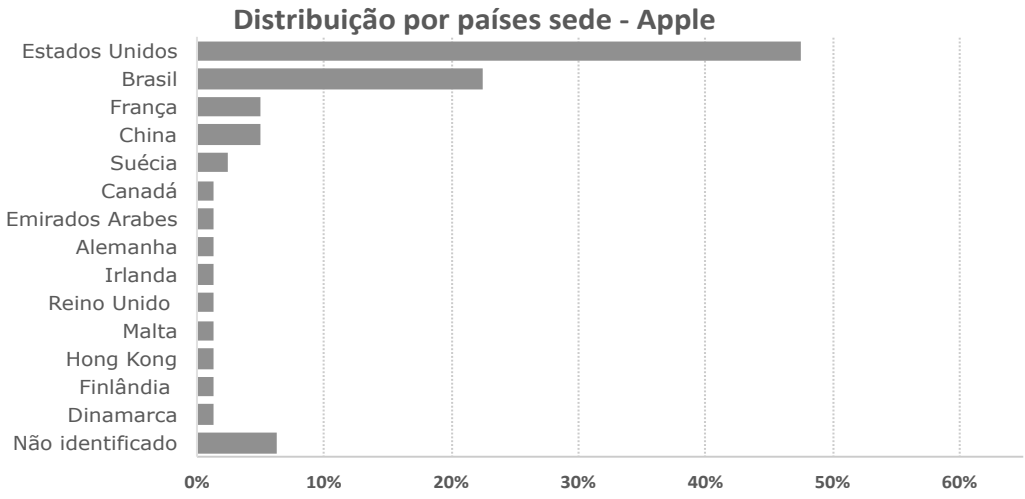
O dado referente à representação comercial no Brasil é especialmente relevante porque permite avaliar quantos desses aplicativos conseguiram conquistar mercado no país sem a necessidade de se estabelecer aqui, desmistificando a ideia de que apenas atores com presença transnacional importariam para a análise da configuração das searas transnacionais de interferência política. Embora o levantamento tenha adotado o Brasil

[313] Cf. https://careers.microsoft.com/locations
[314] https://www.uber.com/en-BR/our-story/
[315] Para determinar se a empresa tem representação comercial no Brasil, foram analisados todos os documentos disponibilizados em seus *sites* ou plataformas, como termos de uso de serviço, políticas de privacidade e informações divulgadas sobre a história da empresa. Se, nesses documentos, foram encontradas indicações de representação comercial no país, como endereços ou telefones de contato no Brasil, considerou-se a empresa como representada comercialmente no país. Para apurar os resultados da pesquisa, considerando que, em alguns casos, esses documentos fazem menção apenas ao endereço da empresa sede, foram realizadas também buscas no Google com o nome do aplicativo (ou da empresa responsável pelo seu desenvolvimento, informação essa que pode ser encontrada nas lojas de aplicativos consultadas) e o termo "Brasil". Os resultados foram analisados para detectar casos nos quais as empresas tenham anunciado publicamente que mantêm escritório no país apesar de não consubstanciarem essa informação em documentos oficiais, como foi o caso, por exemplo, da empresa Netflix que, embora não explicite a existência de subsidiária no Brasil nos referidos documentos, aparece em resultados ligados à abertura de uma subsidiária em São Paulo. Vale registrar, entretanto, que, no caso de empresas que pertencem a um mesmo grupo econômico mas que ainda assim não se identificam como sediadas no país, a empresa foi considerada como não tendo representação comercial no Brasil. Foi o caso das empresas WhatsApp e Instagram, por exemplo, que, embora pertençam ao grupo econômico do Facebook, afirmam não manter escritórios no país e operar separadamente. Nesse sentido, o critério adotado por essa metodologia se baseia na "auto-declaração" das empresas a respeito de sua representação comercial no país, seja pelo anúncio público da abertura de estabelecimento no país, seja pela inclusão dessa informação nos documentos oficiais. O critério nos parece o mais adequado e evita as dificuldades de se fazer essa busca em outros tipos de fonte, como as juntas comerciais estaduais, seja pela descentralização e custos envolvidos nessa pesquisa, seja pela dificuldade de se descobrir a razão social sob a qual todos esses oitenta aplicativos estariam registrados.

como país de referência da análise, acredita-se que seus resultados seriam semelhantes em outros países dada a popularidade global de muitos dos aplicativos analisados e a sua presença, em geral, restrita a um país sede.

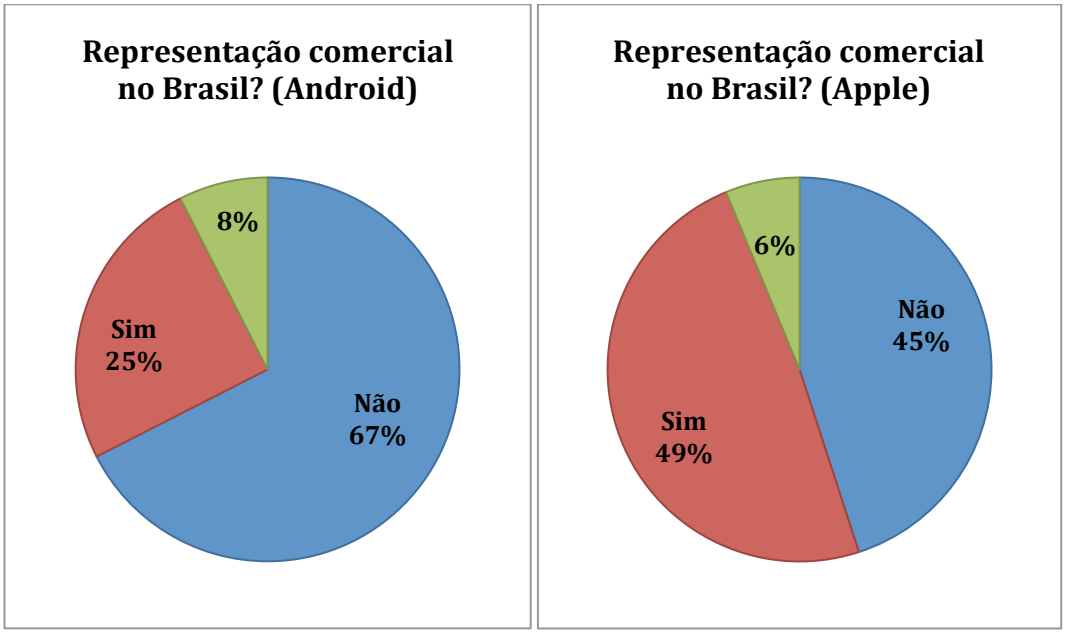
Os gráficos abaixo apresentam a distribuição desses 80 aplicativos de acordo com seus países sede, isto é, indica a nacionalidade das empresas responsáveis por eles para as lojas Android e Apple:



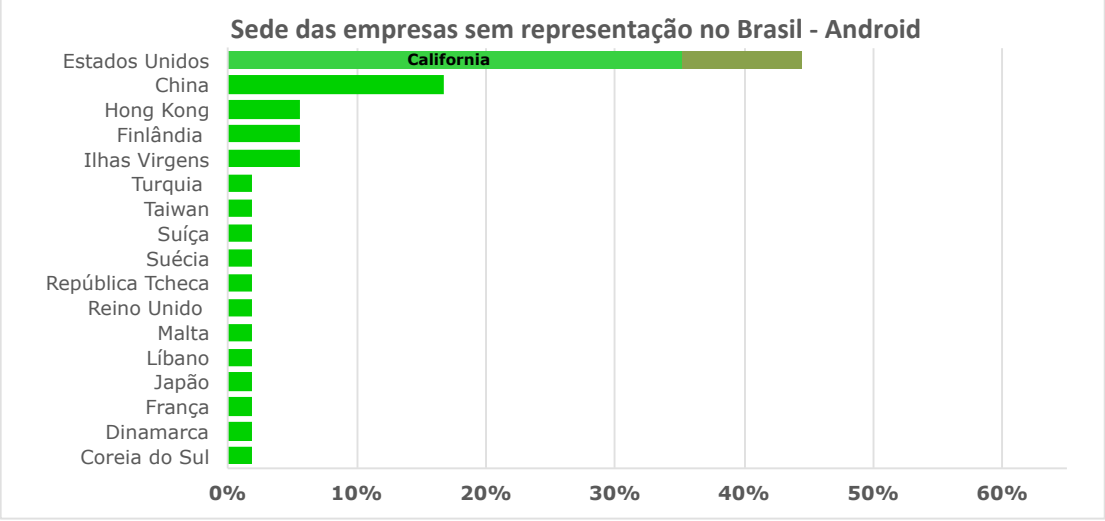


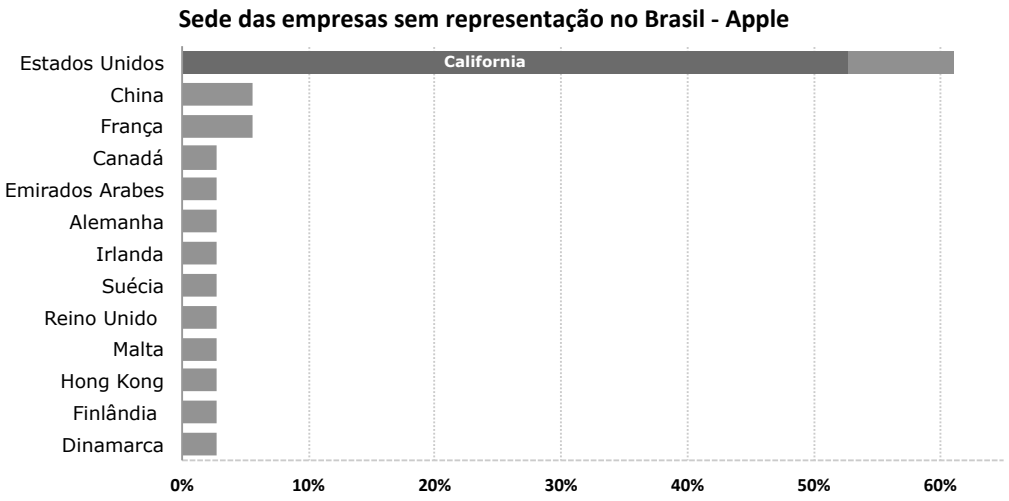
Em ambas as lojas de aplicativos, aproximadamente 50% dessas empresas têm sede nos Estados Unidos. Os próximos países a concentrar a sede dessas empresas são Brasil, o que é natural já que alguns desses aplicativos representam serviços locais como bancos e estabelecimentos comerciais, e a China, mas ambos com porcentagens bem menos expressivas.

Os gráficos abaixo apresentam as porcentagens dessas empresas que têm representação comercial no Brasil:



No caso dos aplicativos mais populares na loja mantida pela Google, 67% deles não tem representação no país; no caso da Apple, 45%. Os gráficos a seguir demonstram que dessas empresas não representadas no Brasil, **45% estão sediadas nos Estados Unidos** no caso da loja Android **(80% das quais estão sediadas na Califórnia)** e **62%** no caso da loja da Apple **(87% das quais estão sediadas na Califórnia).**





Se levarmos em consideração as conclusões desta tese a respeito da dificuldade de se responsabilizar empresas sediadas nos Estados Unidos por violações a legislações nacionais de privacidade, pode-se dizer que essas empresas estão, de certa forma, blindadas em relação à ação de responsabilização propostas por atores estrangeiros. Essa situação as coloca em uma posição privilegiada: utilizando-se da arquitetura da Internet, que permite que seus produtos e serviços atinjam os usuários da rede de forma praticamente irrestrita, isto é, independentemente de fronteiras físicas, elas podem atuar em diferentes jurisdições sem, no entanto, ter de arcar com a contrapartida de se submeter a seus regimes regulatórios, ou de, pelo menos, poderem ser responsabilizadas por não fazê-lo.

Nesse sentido, a arquitetura da Internet viabilizou a interferência de atores não-estatais diferentes daqueles que tradicionalmente participavam de processos transnacionais, como alguns organismos internacionais. Por meio dela, mesmo as empresas sediadas apenas em um ou em muito poucos países podem conquistar mercados significativos ao redor de todo o mundo, tal como indicam os dados acima.

A concentração dessas empresas nos Estados Unidos, entretanto, chama a atenção para o fato de que a arquitetura da Internet não tem sido aproveitada de forma uniforme ou descentralizada por esses atores. Vinte e cinco anos atrás, isto é, durante os primeiros anos após a abertura comercial da Internet, esse fato não deveria causar surpresa. Isso porque, tal como se descreveu no capítulo I desta tese, a Internet começou a ser povoada - e comercialmente explorada - justamente nos Estados Unidos.

Contudo, de lá para cá, a expansão da Internet pelo mundo deixa de justificar essa concentração. Em 1996, segundo dados da ComScore, 66% dos usuários de Internet

estavam localizados nos Estados Unidos; em 2012, de acordo com a mesma fonte, essa porcentagem havia caído para apenas 13%.[316]Além disso, o número de usuários de Internet saltou de 36 milhões em 1996 para mais de 3,5 bilhões em 2016.[317]

O fato de a concentração das empresas nos Estados Unidos ter perdurado, a despeito dessa expressiva transformação ocorrida em termos demográficos do ciberspaço, levanta questões importantes para o direito constitucional: qual a legitimidade desses atores não-estatais para interferir na tutela de direitos fundamentais em outros países? Em que medida isso abala a soberania dos Estados nacionais, restringindo a sua capacidade de responsabilizá-los por violações a direitos fundamentais dentro de seus territórios? Como reagir a essa interferência quando não há mecanismos jurídicos eficazes para proceder à sua responsabilização?

Tal como se verá a seguir, a construção da ideia de legitimidade dessa interferência por parte das empresas estadunidenses na forma como direitos fundamentais são regulados na Internet está intimamente ligada à disseminação de uma noção de independência do ciberespaço em relação aos Estados nacionais, o que alguns chamam de ciberlibertarianismo.[318]

5.3. Do ciberlibertarianismo ao imperialismo?

John Perry Barlow é uma referência do chamado movimento ciberlibertarianista. Inserido no campo das políticas de Internet desde o final da década de 80, Barlow não tem uma trajetória tradicional. Fazendeiro, criador de gado e compositor de músicas de rock, sua aproximação com a Internet se deu pela sua vontade de estar em contato com a comunidade de fãs da banda *The Grateful Dead*, para a qual compunha. Já em 1987,

[316] Cf. It's been 20 years since John Perry Barlow declared cyberspace independence, WIRED, disponível em: <https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/>, último acesso em 04/112016.
[317] Cf. Internet Growth Statistics - the Global Village Online, disponível em: <http://www.internetworldstats.com/emarketing.htm>, acesso em: 5 nov. 2016.
[318] Cf. Katherine Lynch, The Forces of Economic Globalization: Challenges to the Regime of International Commercial Arbitration, [s.l.]: *Kluwer Law International*, 2003, p. 353.

Barlow era usuário assíduo de um dos primeiros fóruns virtuais da rede, o *Whole Earth Lectric Link* ("The WELL").[319]

Fascinado com o poder da Internet e com o espaço único de interação que nela se estabelecia, em 1990, Barlow fundou, junto com John Gilmore e Mitch Kapor, a *Electronic Frontier Foundation (EFF)*, uma das mais influentes entidades do terceiro setor ligadas à pauta de direitos digitais no mundo. Além de seu trabalho na EFF, Barlow passou boa parte da década de 90 escrevendo sobre as potencialidades da Internet em uma série de colunas para a revista *Wired*. Com isso, além de apresentar a Internet para milhares de futuros usuários, Barlow propagava suas concepções libertárias a respeito da rede.

E é exatamente imbuído dessas concepções que Barlow escreveu, em 8 de fevereiro de 1996, o texto mais influente para o movimento ciberlibertarianista: a "Declaração de Independência do Ciberespaço". No documento, cuja estrutura foi inspirada na Declaração de Independência Americana, Barlow escorraça a ideia de regulação da Internet por parte de qualquer Estado, defendendo que o ciberespaço é um ambiente autônomo, paralelo e descolado da autoridade de qualquer governo:

> "Governos do Mundo Industrial, gigantes cansados de carne e aço, eu venho do ciberespaço, o novo espaço da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. Vocês não são bem-vindos entre nós. Vocês não tem soberania sobre o lugar onde nós nos encontramos. Nós não temos governo eleito, e é tampouco provável que tenhamos um, então eu me dirijo a vocês com não menos autoridade do que aquela com a qual a liberdade por si só sempre fala. Eu declaro o espaço social global que nós estamos criando como naturalmente independente das tiranias que vocês almejam impor sobre nós. Vocês não têm direito moral de nos governar e tampouco possuem quaisquer métodos de força que nós tenhamos razões verdadeiras para temer. [...]"[320]

Embora tenha sido escrita na Suíça, em Davos, por ocasião do Fórum Econômico Mundial, a Declaração foi uma clara reação à sanção do então presidente Bill Clinton a uma lei federal nos Estados Unidos que impunha sérias restrições à distribuição de

---

[319] Cf. Electronic Frontier Foundation, "All About John Perry Barlow", disponível em https://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/barlow_bio.html, último acesso em 27 de agosto de 2016. Cf. também Jack Goldsmith e Tim Wu, Who controls the Internet, pp.17-22.

[320] "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear." Cf. John Perry Barlow, A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation, disponível em: <https://www.eff.org/pt-br/cyberspace-independence>, último acesso em: 04/11/2016 (tradução livre).

conteúdos "obscenos" ou "indecentes" pela Internet a menores de 18 anos.[321] Era a primeira vez que uma legislação federal se propunha a regular o compartilhamento de conteúdos na rede, o que rapidamente despertou a ira de libertários como Barlow.

Mas talvez mais importante do que analisar o que representou para a discussão a respeito da lei, que foi posteriormente declarada parcialmente inconstitucional pela Suprema Corte dos Estados Unidos[322], é observar o quanto a forma como a Declaração foi construída favoreceu a criação de uma mentalidade de dissociação entre aquilo que acontece no ciberespaço e a ideia de legitimidade de regulação estatal desses fenômenos, mentalidade essa que ganhou aderência seja entre os usuários da rede, seja entre as empresas do setor de Internet.

Basicamente, a narrativa da Declaração está articulada em torno de dois pontos principais *(i)* o da existência de uma "sociedade do ciberespaço"; e *(ii)* o da existência de território soberano próprio do ciberespaço.

Em relação ao primeiro ponto, é interessante notar que, ao longo de toda a Declaração, Barlow emprega a primeira pessoa do plural ("nós"), dando a ideia de existir uma coletividade bem-definida em nome da qual ele se manifesta. O ciberespaço seria, portanto, constituído por um grupo uniforme e homogêneo de usuários e atores ("vocês não *nos* conhecem nem conhecem *nosso mundo*" [...] "vocês não conhecem a *nossa cultura*, a *nossa ética*, ou os códigos não escritos que já oferecem à *nossa sociedade* mais ordem do que poderia ser obtida por quaisquer das suas imposições").[323] Em outras palavras, a Declaração não só presume como defende que todos os usuários de Internet constituem um mesmo "povo", ignorando o fato de estarem inseridos em diferentes culturas e contextos, sociais, políticos e jurídicos.

Em relação ao segundo ponto, Barlow enfatiza ao longo da narrativa que o ciberespaço ocupa uma dimensão paralela, diferente, que não corresponde às divisas territoriais que pautam a atuação dos Estados nacionais ("O ciberespaço *não repousa* dentro das suas fronteiras. [...] O nosso mundo é um mundo que está ao mesmo tempo em *todo lugar* e em *lugar nenhum*, mas não é onde os corpos vivem. [...] Nós devemos declarar nossas facetas virtuais *imunes das suas soberanias*, mesmo que nós continuemos a consentir com o seu governo sobre nossos corpos."). Em outras palavras, a Declaração

[321] A lei ("Telecommunications Competition and Deregulation Act of 1996" ou, como ficou conhecido a sua seção V, "Communications Decency Act of 1996") foi sancionada no próprio dia 8 de fevereiro de 1996 pelo então presidente dos Estados Unidos, Bill Clinton.
[322] Cf. ACLU v. Reno.
[323] Cf. John Barlow, A Declaration of the Independence of Cyberspace. (tradução livre e destaques nossos).

defende que o ciberespaço estaria descolado da noção dos territórios nacionais, constituindo um espaço autônomo dentro do qual essas relações seriam travadas.

A conjugação desses dois elementos, quais sejam povo e território, é poderosa. Na época, encontrou ressonância no pensamento de diversos autores e ativistas, que passaram a enxergar a Internet como um espaço alternativo ao Estado e que, por consequência, deveria ser imune à regulação.[324] Sendo assim, Barlow teria exonerado a "sociedade do ciberespaço" das amarras territoriais que governam as relações no caso dos Estados nacionais.[325] É nesse sentido que Gunther Teubner defende que a retórica de Barlow contribuiu, de alguma forma, para o avanço de um ideário que poderia servir como fundamento para as propostas de uma "constituição global para as comunicações digitais".[326]

A unidade de povo e território que marcaria o ciberespaço, tal como idealizada por Barlow, entretanto, não impediu que, ao longo dos anos, mais e mais Estados passassem a regulá-lo. No caso do direito à privacidade, por exemplo, como já se mencionou, mais de cem países adotaram legislações nacionais de proteção de dados.[327] O mesmo acontece com outros temas que afetam as relações na Internet, como questões ligadas ao direito autoral, à responsabilidade de intermediários pela publicação de conteúdos de terceiros e à neutralidade da rede.[328]

Embora, como assinala Ronaldo Lemos, o movimento tenha perdido força alguns anos depois de sua disseminação, especialmente em razão das ideias de Lawrence Lessig a respeito da necessidade de se encarar a arquitetura da Internet como algo criado pelo ser humano e não como uma realidade imutável sobre a qual não se poderia ter controle[329], a ideia de resistência ao controle do ciberespaço pelos Estados parece ter sido incorporada, em alguma medida, pela cultura das empresas do setor de Internet.[330]

---

[324] Ronaldo Lemos anota que o pensamento de Barlow gerou efeitos até no Brasil, tendo contribuído para um atraso significativo na tramitação de projetos de lei dedicados a questões ligadas à Internet e que, de acordo com o autor, demandavam uma resposta normativa urgente. Cf. Ronaldo Lemos, Direito, tecnologia e cultura. Rio de Janeiro: Editora FGV, 2005, pp.94-95.

[325] Cf. Hans Lindahl, We and cyberlaw: The spatial unity of constitutional orders, *Indiana Journal of Global Legal Studies*, v. 20, n. 2, p. 697–730, 2013, p. 704.

[326] Cf. Gunther Teubner, Societal Constitutionalism: Alternatives to State-Centered Constitutional Theory?, in Transnational Governance and Constitutionalism, 3, 4, p.24.

[327] Cf. Graham Greenleaf, Global data privacy laws 2015: 109 countries, with european laws now a minority, 2015.

[328] No Brasil, por exemplo, algumas dessas questões são regulamentadas pela Lei nº 12.965/2014 ("Marco Civil da Internet").

[329] Cf. Lawrence Lessig, Code and Other Laws of Cyberspace, 1999, pp.43-44.

[330] Cf. Ronaldo Lemos, Direito, tecnologia e cultura. Rio de Janeiro: Editora FGV, 2005, pp.94-95.

A postura assumida pelo Twitter em relação à defesa da liberdade de expressão de seus usuários serve de exemplo. Durante os tumultos e saques que aconteceram em Londres, em agosto de 2011, por exemplo, o governo inglês solicitou informações sobre usuários que estariam utilizando a plataforma para divulgar e organizar as manifestações. Em resposta à solicitação, Dick Costolo, então diretor executivo da empresa, declarou: "Nós protegeremos nossos usuários dos governos", reiterando o compromisso da plataforma em garantir a liberdade de expressão e afirmando não ter a intenção de cooperar com pedidos de identificação das contas utilizadas para coordenar os episódios.[331] O mesmo aconteceu em relação a uma sentença proferida na França, em janeiro de 2013, exigindo a entrega das informações de identificação de usuários que teriam utilizado a plataforma para divulgar conteúdos de caráter antissemita. Apesar de ter retirado o conteúdo do ar, a empresa afirmou que "avaliaria suas opções" em relação ao fornecimento dos dados já que isso poderia estar em desacordo com os parâmetros de liberdade de expressão adotados nos Estados Unidos.[332] Na época, o Twitter não tinha representação comercial na França, o que deixava a empresa em uma posição mais confortável para resistir à ordem judicial francesa.

Postura semelhante pode ser observada por parte da Google no que diz respeito a pedidos de remoção de conteúdo. Em 2007, por exemplo, uma decisão do poder judiciário turco determinou que o Youtube retirasse do ar determinados vídeos que, no entendimento do tribunal, insultavam a memória do fundador da República da Turquia, Mustafa Kemal Ataturk. De acordo com o ordenamento jurídico do país, insultar ou criticar a figura do referido líder político é crime.[333]

Quando instada, entretanto, a impedir o acesso aos vídeos em questão, a empresa controladora do Youtube, Google Inc., se negou a retirar o conteúdo do ar, alegando não compactuar com a imposição de uma opção legislativa nacional – a de restringir a liberdade de expressão no caso de conteúdos envolvendo Ataturk – à totalidade de seus usuários, localizados em todas as partes do mundo.[334] A empresa se pautou ainda pelo

---

[331] Cf. Emma Barnett, "Twitter chief: we will protect our users from government", *The Telegraph* (18.10.2011), <disponível em http://www.telegraph.co.uk/technology/twitter/8833526/Twitter-chief-We-will-protect-our-users-from-Government.html, último acesso em 26.6.2016>.

[332] Cf. Eric Pfanner / Somini Sengupta, "In a French Case, a Battle to Unmask Twitter Users", *The New York Times* (24.1.2013), <disponível em http://www.nytimes.com/2013/01/25/technology/twitter-ordered-to-help-reveal-sources-of-anti-semitic-posts.html, último acesso em 25.6.2016>.

[333] Cf. Turquia, Lei n. 5816, de 25.07.1951.

[334] Sara Yin relata que, na época, Google Inc. teria justificado a negativa com a afirmação: "Nós nos negamos porque nós acreditamos que a legislação turca não deva ser aplicada fora da Turquia" (tradução livre). Cf. Sara Yin, "Youtube banned in Turkey (again)", *PC Magazine* (03.11.2010) <disponível em

extensivo grau de proteção conferido à liberdade de expressão nos Estados Unidos, onde está sediada. Para a Google, acatar a exigência significaria restringir também a liberdade de usuários de fora da Turquia – alguns dos vídeos haviam sido postados por usuários da Grécia, por exemplo.[335] Diante da negativa, o acesso ao site foi bloqueado por completo no país.[336] Tendo vigorado por aproximadamente dois anos, o bloqueio foi suspenso em 2010. Posteriormente, entretanto, o governo voltou a suspender o acesso ao Youtube no país.[337]

Os exemplos são representativos de uma postura de resistência - quiçá de insubordinação - dessas empresas em relação a legislações e/ou ordens judiciais estrangeiras que adotem graus mais restritivos da liberdade de expressão do que aquele conferido a esse direito nos Estados Unidos. Seria ingenuidade acreditar que as empresas atuaram dessa forma por terem sido influenciadas pelo movimento ciberlibertarianista. Há uma série de interesses conjugados nessa equação. O interessante é notar que, de certa forma, essas empresas parecem se sentir, de fato, independentes da regulação que lhes seria imposta por outros Estados nacionais, especialmente aqueles nos quais não estão sediados. Mais interessante ainda é pensar no que significa para as estruturas do direito constitucional - e do constitucionalismo - o fato de esses atores poderem tão claramente se opor às opções legislativas ou judiciais de Estados nacionais.

No caso do direito à privacidade, o mesmo fenômeno pode ser observado, ainda que com uma diferença principal: o modelo regulatório adotado nos Estados Unidos, no que tange à coleta, tratamento e transferência de dados pessoais, tal como se descreveu ao longo desta tese, adota um grau de proteção significativamente menor em relação a muitas legislações de proteção de dados em vigor em outros países (ao contrário do caso da liberdade de expressão, em que a proteção conferida nos Estados Unidos costuma ser considerada maior).

Independentemente de o grau de proteção conferido a determinado direito fundamental nos Estados Unidos ser considerado maior ou menor, o que importa para essa discussão é a possibilidade de atores não-estatais, como essas empresas, encontrarem condições de impor os graus de proteção a que estão submetidos (nesse caso, os estadunidenses) sobre outras jurisdições, graças à arquitetura da Internet. No caso da

---

http://www.pcmag.com/article2/0,2817,2372043,00.asp#fbid=NFZgGj_FTU6, último acesso em 25.06.2016>.

[335] Cf. Sara Yin, "Youtube banned in Turkey (again)", *PC Magazine* (03.11.2010).

[336] Cf. Associated Press, "Turkey Pulls Plug on Youtube Over Ataturk 'Insults'", *The Guardian* (7.3.2007), <disponível em http://www.theguardian.com/world/2007/mar/07/turkey, último acesso em 25.6.2016>.

[337] Cf. "Turkey lifts two-year ban on Youtube", *BBC News Technology* (30.11.2010) <disponível em http://www.bbc.com/news/technology-11659816, último acesso em 25.6.2016>.

privacidade, isso significa, como visto, a possibilidade de impor suas próprias regras, desenvolvidas dentro do modelo de auto-regulação, para outras jurisdições.

Em outras palavras, do ponto de vista da tutela de direitos fundamentais, isso significa que a arquitetura da Internet abre caminho para que esses atores – eminentemente privados –, refugiados em países que adotem modelos regulatórios que lhes sejam mais convenientes, tais como os Estados Unidos, interfiram na eficácia das normas constitucionais de outros países sem que existam mecanismos jurídicos efetivos que permitam equalizar ou obstar essa interferência. Mais do que isso: a concentração dessas empresas nos Estados Unidos, como demonstrou o levantamento empírico acima, pode implicar a *prevalência* dos graus de proteção conferidos a direitos fundamentais nesse país em relação aos adotados em outras jurisdições. É como se se estivesse assistindo, portanto, a uma "exportação" desses graus de proteção para outras partes do mundo.

Há que ser mencionado ainda um outro efeito colateral dessa concentração de atores nos Estados Unidos: o controle das estruturas normativas radicadas nas características tecnológicas que compõem a Internet, isto é, da camada do código. Como ensina Lawrence Lessig, determinar as características da arquitetura (código) é uma poderosa forma de regulação do ciberespaço:

> "[e]m algum lugares (serviços online como AOL, por exemplo) você deve inserir uma senha antes de ganhar acesso; em outros lugares, você pode entrar se identificando ou não. [...] O código ou o software ou a arquitetura dos protocolos determinam essas características; elas são características selecionadas pelos programadores; elas restringem o seu comportamento tornando outros comportamentos possíveis ou impossíveis. O código incorpora certos valores ou torna certos valores impossíveis. Nesse sentido, ele também é regulação, assim como as arquiteturas dos códigos dos espaços reais também são."[338]

Em uma sociedade na qual, cada vez mais, as atividades da vida cotidiana são *mediadas* por diferentes interfaces, como *tablets*, computadores, *smartphones*, caixas eletrônicos, entre outros, é fundamental atentar para quem são os atores que controlam e desenvolvem esses códigos.[339] Isso porque, como Kate Crawford destaca, algoritmos (códigos programados) atuam de forma invisível, sendo, muitas vezes, também responsáveis por processos de tomada de decisões que afetam a vida das pessoas. Essas decisões podem ser tomadas com base em critérios pouco usuais ou eticamente

[338] Cf. Lawrence Lessig, Code 2.0, p.124 (tradução livre).
[339] Cf. Ryan Calo, Digital market manipulation, *The George Washington Law Review,* 82, 4, 2014, p. 1003.

questionáveis, podendo, inclusive, gerar discriminação ou distorções da realidade. Vários são os exemplos recentes de casos que foram noticiados nesse sentido: seja a seguradora de carros que anunciou estar desenvolvendo um algoritmo que determinará o valor do seguro com base nas postagens do cliente no seu perfil do Facebook[340]; sejam as suspeitas de que os mecanismos de busca podem estar gerando percepções distorcidas da realidade, como recentemente declarou Angela Merkel[341]; sejam as denúncias de que os algoritmos utilizados pelo Facebook possibilitariam aos anunciantes discriminar o público alvo dos anúncios com base em critérios raciais.[342]

Do exposto, percebe-se que a concentração desses atores privados nos Estados Unidos e a ausência de mecanismos jurídicos de responsabilização adequados podem gerar assimetrias que culminem na *prevalência* dos: *(i)* graus de proteção atribuídos a direitos fundamentais nos Estados Unidos em detrimento daqueles adotados em outras jurisdições; e *(ii)* valores e visões desses atores que venham a ser incorporados no desenvolvimento e programação de códigos, o que também pode representar uma forma de interferência na regulação adotada pelos Estados nacionais.

5.4. Propostas de harmonização internacional

Para equacionar questões como as mencionadas acima, que envolvem a colisão de modelos regulatórios de direitos fundamentais na Internet, surgiram propostas de harmonização e regulação no plano internacional. Essas propostas não são novas. Já em 1996, David Johnson e David Post, observando que a arquitetura da Internet como rede de comunicação livre e global desafiava a noção de territorialidade do direito, propuseram a adoção de um ordenamento jurídico especial, supranacional, que fosse aplicável às

[340] Cf. Graham Ruddick, Admiral to price car insurance based on Facebook posts, The Guardian, disponível em https://www.theguardian.com/technology/2016/nov/02/admiral-to-price-car-insurance-based-on-facebook-posts, último acesso em 04/11/16.
[341] Cf. Kate Connolly, Angela Merkel: internet search engines are distorting perception", The Guardian, disponível em https://www.theguardian.com/world/2016/oct/27/angela-merkel-internet-search-engines-are-distorting-our-perception, último acesso em 04/11/2016.
[342] Cf. Ellen McGirt, Is Facebook Enabling Advertisers to Discriminate by Race?, Fortune, 28/11/2016, disponível em http://fortune.com/2016/10/28/facebook-ad-propublica-race/, último acesso em 04/11/2016.

relações que se travassem no espaço virtual.[343] Isso porque, para os autores, a Internet teria tornado ineficaz a utilização do território como critério preponderante para aplicação das leis já que *(i)* o poder coercitivo dos Estados está limitado à sua jurisdição, o que os impede de garantir o cumprimento de suas ordens em escala global; *(ii)* os efeitos de determinadas condutas na Internet podem ser sentidos em diferentes jurisdições simultaneamente; *(iii)* não há legitimidade para que os Estados regulem fenômenos globais de forma individual; e *(iv)* a localização física do usuário deixou de ser determinante para a legislação que lhe será aplicável.[344]

Propondo um modelo menos ousado e mais específico para lidar com os desafios referentes ao direito à privacidade, no ano 2000, Joel Reidenberg defendeu que se estabelecesse um consenso globalizado em relação a "normas de governança democrática para a privacidade informacional".[345] Ao contrário do que pode parecer, na visão do autor, isso não demandaria a harmonização das regras nacionais específicas que vigoram em relação ao direito à privacidade, o que seria, inclusive, para ele, indesejável. Isso porque, como argumenta, as raízes dessas diferenças estariam calcadas nos próprios valores fundantes do modelo regulatório adotado por cada país, conforme já se discutiu ao longo do capítulo 2. Nesse sentido, pretender superar essas diferenças significaria ignorar o "balanço político" realizado em cada país, o que não lhe parece acertado.[346]

Sendo assim, a proposta de Reidenberg está baseada na ideia de co-regulação, mecanismo que possibilitaria a aplicação simultânea de múltiplas regras diferentes a uma única atividade de processamento de dados.[347] Para o autor, além da cooperação internacional, a implementação de um mecanismo de co-regulação dependeria de quatro elementos principais: *(i)* a mobilização de atores intergovernamentais; *(ii)* o desenvolvimento de códigos de conduta técnica; *(iii)* a utilização de espaços multisetoriais de discussão; e *(iv)* a criação de uma espécie de tratado ou acordo internacional.[348]

No que diz respeito à mobilização de atores intergovernamentais, o autor assinala o papel estratégico que ocupam na medida em que gozam de legitimidade internacional para formular e propor diretrizes que podem acomodar divergências nos modelos regulatórios

[343] Cf. David Johnson / David Post, "Law and Borders – The Rise of Law in Cyberspace", *Stanford Law Review* 48 (1996).
[344] Cf. David Johnson / David Post, "Law and Borders – The Rise of Law in Cyberspace", p. 1370.
[345] Cf. Daniel Solove e Woodrow Hartzog, The FTC and the new common law of privacy, *Columbia Law Review*, p. 583–676, 2014, p. 638–643.
[346] Cf. *Ibid*., p. 1320.
[347] Cf. Joel R. Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, *Stanford Law Review*, v. 52, n. 5, p. 1315, 2000, p. 1352.
[348] Cf. *Ibid*., p. 1351–1362.

de privacidade.[349] Nesse sentido, o autor destaca as atuações proeminentes da OCDE e do Conselho da Europa no tema e chama a atenção para a entrada de novos atores, como a Organização Mundial do Comércio (OMC) e a Organização Mundial da Propriedade Intelectual (OMPI).[350]

Em relação à elaboração de códigos de conduta técnica, o autor defende haver espaço para engajar organismos ligados à comunidade técnica e de governança da Internet, como o *World Wide Web Consortium* (W3C), a *Internet Corporation for Assigned Names and Numbers* (ICANN) e a *Internet Engineering Task Force* (IETF). Organismos como esses poderiam criar recomendações e padrões técnicos (códigos de conduta) que aliviassem disparidades regulatórias. Aqui, a proposta de Reidenberg vai ao encontro da ideia de regulação pelo código, que se mencionou acima.[351] No exemplo do autor, se a arquitetura de um sistema *online* de pagamentos fosse concebida para realizar apenas transações anônimas, independentemente de onde ocorrer a transação - e, consequentemente, do modelo regulatório adotado -, os dados pessoais (de identificação) do usuário estariam protegidos já que seria impossível fornecê-los.

Da mesma forma como esses dois grupos de atores ocupam uma função estratégica, Reidenberg enxerga os espaços de discussão multisetorial como oportunidades para se construir consensos. Como exemplos, cita os encontros conduzidos pela OCDE, que congregam representantes de diferentes setores, como governos e setor privado, e que têm debatido o tema da privacidade. [352]

Nesse sentido, cumpre registrar que a OCDE tem, ao longo dos anos, encampado esforços para debater o tema da economia digital e direitos humanos em suas reuniões ministeriais. A primeira delas foi a Conferência de Ottawa, em 1998, em que representantes dos países-membros se reuniram para discutir o tema e desenvolveram planos para o comércio eletrônico global. Na segunda, que aconteceu em Seul em 2008, foram discutidos temas relacionados ao futuro da Internet – com o reconhecimento dos países sobre a sua natureza e função essencial.

Em 2016, em Cancun, foi realizada nova reunião ministerial sobre o tema, culminando na publicação da "Declaração sobre Economia Digital", que elenca uma série

[349] Cf. Joel Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, p. 1352.
[350] Cf. Joel Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, p. 1353–1355.
[351] Cf. Lawrence Lessig, Code 2.0, pp.120-124.
[352] Cf. Joel Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, p. 1358–1359.

de diretrizes em relação aos temas debatidos. Na declaração, fica explicitado o consenso em relação ao incentivo à inovação, à criatividade e ao compartilhamento de conhecimento, visando ao livre fluxo de informação na rede, mas se ressalta a necessidade de garantis a proteção da privacidade e da liberdade de expressão. Nessa nota, a declaração ainda expressa um comprometimento em promover a cooperação entre todos os atores envolvidos para desenvolver estratégias de proteção à privacidade que conciliem as oportunidades de inovação com as necessidades de tutela em diferentes jurisdições.[353]

Por mais que a conjugação desses três elementos - atores intergovernamentais, comunidade técnica internacional e fóruns internacionais de discussão - possa facilitar a acomodação das divergências existentes entre diferentes modelos regulatórios de privacidade, Reidenberg destaca que ainda restarão assimetrias. Para equacioná-las, propõe a elaboração de um tratado internacional sobre proteção de dados cuja principal função seria estabelecer um processo de elaboração de normas de governança, que norteariam a resolução dessas divergências.[354] Para tanto, o tratado deveria reconhecer princípios básicos de proteção de dados e criar um mecanismo de negociação que propiciasse a tomada de decisões com base no consenso.

A proposta do autor é importante na medida em que se diferencia de propostas mais ambiciosas de harmonização internacional, que se dependeriam da aprovação de documentos que uniformizassem as regras para as atividades de coleta e tratamento de dados pessoais em todo o mundo. Ainda assim, o autor reconhece a necessidade de reconhecimento de princípios básicos comuns. Mais do que isso, Reidenberg parece estar confiante de que haveria espaço para a construção de consensos a respeito de quais regras deveriam prevalecer nos casos em que diferentes graus de proteção de privacidade estivessem em contato ou em colisão.

Passados quase vinte anos desde a formulação da proposta de Reidenberg, entretanto, no plano internacional, ainda não há diplomas normativos robustos que promovam a harmonização das regras aplicáveis ao tema da privacidade ou tampouco regras transnacionais que estabeleçam formas compartilhadas de governança.[355]

---

[353] Para a íntegra da declaração e detalhes sobre o seu processo de elaboração, cf. Dennys Antonialli e Clarice Tambelli, "OCDE aprova declaração sobre economia digital", disponível em http://www.internetlab.org.br/pt/noticias/ocde-aprova-declaracao-sobre-economia-digital/, último acesso em 12/12/2016.

[354] Cf. *Ibid*., p. 1360.

[355] Tal como se demonstrou no capítulo 2 desta tese, o caso do Regulamento Geral para Proteção de Dados, que passará a vigorar em todos os Estados-membros da União Europeia a partir de 2018, não deve ser encarado como uma empreitada de harmonização internacional das regras de proteção de dados. Com

Isso sugere a dificuldade de se chegar a esses referidos consensos no plano internacional, especialmente no que tange à definição de mecanismos jurídicos de responsabilização de atores por violações a normas constitucionais e legislações de proteção de dados nacionais que poderiam equacionar os conflitos gerados pela colisão de diferentes modelos regulatórios nacionais.

Além disso, quaisquer empreitadas nesse sentido dependeriam da participação e comprometimento por parte dos Estados Unidos, onde se concentram esses atores privados. Por razões de conveniência política e econômica e pelos valores que estão na base do modelo regulatório de privacidade adotado nos Estados Unidos, é difícil acreditar que existam perspectivas reais de que esse comprometimento possa ser atingido com o nível de detalhamento necessário para solucionar os impasses gerados.

Enquanto as iniciativas de regulação internacional do tema não estiverem acompanhadas de mecanismos jurídicos para promover a responsabilização desses atores ou para que se garanta o seu *enforcement* por parte dos atores privados sediados nos Estados Unidos, elas estarão limitadas à enunciação de princípios genéricos a respeito da proteção da privacidade. O exemplo a seguir ilustra essas limitações no âmbito da Organização das Nações Unidas.

5.4.1. A experiência da Organização das Nações Unidas

A partir das denúncias realizadas, em junho de 2013, por Edward Snowden, ex-agente da Agência Central de Inteligência dos Estados Unidos (CIA), a respeito do aparato de vigilância implementado pela Agência de Segurança Nacional dos Estados Unidos (NSA) e que contava com a suposta colaboração das maiores empresas do setor de Internet, a então presidente da república Dilma Rousseff instou a comunidade internacional, em seu discurso de abertura da 68ª Assembleia Geral da Organização das Nações Unidas, a estabelecer "um marco civil multilateral para a governança e o uso da

aplicação limitada à União Europeia, o Regulamento partiu não só de um corpo normativo anterior, qual seja, a Diretiva 95, como também das legislações de proteção de dados aprovadas em âmbito nacional. Nesse sentido, representa uma consolidação da experiência normativa da União Europeia, não devendo se confundir com as propostas ambiciosas de consenso a respeito de um conjunto de regras que vigorasse perante toda a comunidade internacional.

Internet e de medidas que garantam uma efetiva proteção dos dados que por ela trafegam".[356]

A proposta ganhou aderência e, conjuntamente com a Alemanha, em 01 de novembro de 2013, o Brasil apresentou à Terceira Comissão da Assembleia Geral, que lida com questões ligadas a direitos humanos, uma primeira minuta de resolução sobre a proteção do direito à privacidade na era digital.[357] Sem sofrer mudanças significativas, no mês seguinte, o documento foi aprovado por consenso (sem votos explícitos) pelos 193 países membros da ONU e deu origem à Resolução 68/167, de 18 de dezembro de 2013.[358]

Dentre outras medidas, o documento conclama os Estados-membros a:

> "(a) respeitarem e protegerem os direitos referidos no parágrafo 1 acima, inclusive no contexto das comunicações digitais;
> (b) adotarem medidas com vistas à cessação das violações de tais direitos e a criarem condições para a prevenção de tais violações, inclusive assegurando que a legislação nacional relevante esteja em conformidade com suas obrigações no âmbito do direito internacional dos direitos humanos;
> (c) revisarem seus procedimentos, práticas e legislação no que tange à vigilância das comunicações, sua interceptação e coleta de dados pessoais, inclusive a vigilância, interceptação e coleta em massa, com vistas a assegurar o direito à privacidade e garantir a plena e eficaz implementação de todas suas obrigações no âmbito do direito internacional dos direitos humanos;
> (d) estabelecerem mecanismos nacionais independentes de supervisão, capazes de assegurar a transparência do Estado e sua responsabilização em atividades relacionadas à vigilância das comunicações, sua interceptação e coleta de dados pessoais."[359]

No ano seguinte, Brasil e Alemanha angariaram mais apoiadores para aprovar uma nova versão da resolução. Embora bastante similar à versão de 2013, o novo texto inclui dispositivo conclamando os Estados-membros a "oferecer aos indivíduos cujo direito à privacidade tenha sido violado por vigilância ilícita ou arbitrária acesso a remédios efetivos, consistentes com suas obrigações internacionais de respeito a direitos humanos".[360] Frise-se que a resolução se dirige à atuação dos Estados e não a atores privados, estando diretamente relacionada a atividades de coleta de dados pelo poder público e não pelo setor privado.

---

[356] Cf. Portal do Planalto, Discurso da Presidenta da República, Dilma Rousseff, na abertura do Debate Geral da 68ª Assembleia Geral das Nações Unidas - Nova Iorque/EUA, Palácio do Planalto, disponível em: <http://www2.planalto.gov.br/acompanhe-o-planalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua>, acesso em: 4 out. 2016.

[357] Cf. Brazil and Germany draft resolution: "The right to privacy in the digital age", disponível em http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45, último acesso em 04/10/2016.

[358] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

[359] Cf. http://www.itamaraty.gov.br/pt-BR/component/tags/tag/90-direito-a-privacidade-na-era-digital

[360] Cf. Organização das Nações Unidas , "The right to privacy in the digital age", disponível em http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/69/L.26/Rev.1

Em 2015, o Conselho de Direitos Humanos da ONU nomeou um relator especial, Joseph Cannataci, com a tarefa específica de avaliar a proteção à privacidade garantida pelos países membro.[361] Em 21 de novembro de 2016, a ONU adotou uma nova versão da resolução, dessa vez, dirigindo-se também aos atores privados:

> "[...]
> 6. **Conclama as empresas** a: (A) **cumprir a sua responsabilidade** de respeitar os direitos humanos de acordo os Princípios Orientadores sobre as Empresas e os Direitos Humanos: Implementando o programa "Proteger, Respeitar e Remediar" das Nações Unidas, que inclui o direito à privacidade na era digital; (B) **Informar os usuários** sobre a coleta, uso, compartilhamento e retenção de dados que possam afetar o seu direito à privacidade e estabelecer políticas de transparência, se adequado;
> 7. **Incentiva as empresas a trabalhar no sentido de** permitir comunicações seguras e a proteção de usuários individuais contra atos arbitrários ou ilegais de interferência com a sua privacidade, incluindo as soluções baseadas no desenvolvimento de soluções técnicas;
> 8. **Encoraja todas as partes interessadas a participarem em diálogos informais** sobre o direito à privacidade, e convida a contribuição do Relator Especial sobre o direito à privacidade nesse processo;
> [...]"[362]

Embora relevantes, os dispositivos se limitam a recomendações ou apelos, sem valor vinculante significativo ou oponível a atores privados, o que se pode constatar até mesmo pelos verbos utilizados na declaração.

A experiência com essas resoluções no âmbito da ONU ilustram a dificuldade de se construir consensos que possam representar regras claras, concretas e executáveis a respeito de atividades de coleta, monitoramento, tratamento e transferência de dados pessoais. Questões fundamentais como o conceito de dados pessoais, as formas de obtenção de consentimento e as finalidades admissíveis para a coleta permanecem sendo reguladas no plano nacional e, consequentemente, expostas a diferentes balanços e decisões políticas.

Desacompanhados de mecanismos jurídicos de *enforcement* que possam se mostrar eficazes e oponíveis em relação aos atores privados que foram objeto de estudo desta tese, as tentativas de harmonização encampadas no plano internacional estão fadadas a ser tratadas como "bons conselhos" que podem, como tal, ser sumariamente ignorados quando for mais conveniente.

---

[361] Cf. United Nations Human Rights Office of the High Commissioner, Special Rapporteur on right to privacy, disponível em http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

[362] Cf. Organização das Nações Unidas, The right to privacy in the digital age, disponível em https://www.accessnow.org/cms/assets/uploads/2016/09/privacy-resolution-2016-UNGA.pdf (tradução livre e destaques nossos).

CONCLUSÃO

Até 1992, a Internet era um ambiente praticamente inóspito, habitado apenas por alguns poucos integrantes das comunidades técnica, científica e militar. A navegação não era intuitiva e dependia de familiaridade com a tecnologia e a computação, o que restringia ainda mais o seu acesso e capacidade de ganhar escala. Isso mudou com a chegada de atores privados imbuídos de interesses comerciais, que transformaram a Internet radicalmente. O primeiro desafio era torná-la acessível e atrativa, empreitada que foi pulverizada entre diferentes atores, que assumiram demandas igualmente distintas, como o desenvolvimento de ferramentas de navegação, mecanismos de busca, serviços de *e-mail* e troca instantânea de mensagens ou até mesmo o oferecimento de conteúdo.

Como a Internet tem uma de suas raízes na academia, inicialmente, o seu acesso era facilitado dentro dos *campi* de algumas universidades dos Estados Unidos, que contavam com a infraestrutura cara e sofisticada que era necessária para a conexão. Instigados com as potencialidades de uso e exploração da Internet, que começavam a transparecer, estudantes dessas universidades, pelo seu contato com a rede, foram responsáveis pelo desenvolvimento de muitas das primeiras aplicações de Internet.

De projetos que estavam originalmente adstritos ao ambiente universitário nasceram verdadeiros gigantes da Internet, como as empresas Yahoo! e Google, ambas fundadas por estudantes da Universidade de Stanford, na Califórnia. Na verdade, a Califórnia - e, mais especificamente, o Vale do Silício - concentrou muitos desses primeiros empreendimentos. Isso não aconteceu por acaso: a presença de investidores com experiência no setor de tecnologia alimentava as esperanças e o bolso de estudantes e desenvolvedores aventureiros, que encontravam ali capital para colocar as suas ideias em prática.

O desafio da monetização desses serviços veio logo, em parte pela pressão gerada pelos próprios investidores. Para não aplacar o crescimento da Internet entre os usuários recém-chegados com a cobrança de valores pela utilização das aplicações na rede, a indústria da publicidade foi uma boa alternativa. A venda de espaços publicitários virtuais subsidiava o ofercimento gratuito de produtos e serviços na Internet, o que parecia satisfazer os interesses de usuários e empresários.

Em pouco tempo, a Internet revolucionou a indústria da publicidade, que passou a contar com inúmeras novas capacidades de segmentação e direcionamento de anúncios, viabilizadas pela utilização de tecnologias de monitoramento, coleta e tratamento de dados pessoais. Em pouco tempo, o ecossistema de publicidade digital se transformou, dando origem a uma complexa cadeia de intermediários e de plataformas para a compra e venda de espaços publicitários virtuais.

O florescimento do mercado da publicidade digital foi financiado, então, às custas da privacidade dos usuários, cujos dados constituíam a base das estratégias de monetização presentes na grande maioria dos modelos de negócios das empresas de Internet. A evolução dos modelos de precificação das atividades de compra e venda de anúncios também aumentava a ânsia por dados dos usuários: no modelo de custo por clique, oferecer anúncios mais direcionados significava aumentar as chances de lucro.

Todas essas transformações aconteceram em um espaço curto de tempo. Em pouco mais de quatro anos, esses modelos de negócio estavam consolidados e a experiência de navegação comercial da Internet basicamente definida. Além de acelerado, esse desenvolvimento aconteceu de forma bastante concentrada, tendo sido protagonizado quase que exclusivamente por atores privados estadunidenses.

O fato de a Internet ter sido originalmente povoada por atores localizados nos Estados Unidos foi determinante para os contornos que o direito à privacidade assumiu na rede. Alicerçado fundamentalmente sobre interesses comerciais e econômicos, o modelo regulatório de privacidade estadunidense privilegia a livre iniciativa e a autonomia privada em detrimento de valores ligados à proteção de direitos fundamentais. Isso se traduziu em um modelo setorial, fragmentado e de auto-regulação, que conferiu aos atores privados discricionariedade para criar suas próprias políticas de privacidade e incorporar na arquitetura de seus produtos e serviços os padrões técnicos de proteção que julgassem mais adequados ou convenientes.

A atuação da Comissão Federal do Comércio dos Estados Unidos, que assumiu a função de fiscalizar essas práticas e tutelar os direitos dos consumidores, também é marcada pela conjugação de interesses econômicos e políticos, restringindo a sua capacidade de agir de forma rigorosa em relação a violações de normas constitucionais e legislações de proteção de dados estrangeiras. Por limitações de competência e conveniência política, a Comissão cristalizou entendimentos que empoderam atores privados sediados nos Estados Unidos frente a outros Estados nacionais.

Da mesma forma, a legislação estadunidense impõe sérios obstáculos ao reconhecimento e execução de ordens judiciais estrangeiras, o que aumenta as dificuldades de responsabilização de atores privados sediados nos Estados Unidos por violações a legislações de proteção de dados pessoais cometidas em países nos quais não estão sediados. A esse contexto somam-se ainda as disputas travadas por jurisdição na Internet, cuja multiplicidade de argumentos e teorias tem sido explorada pelas empresas do setor, gerando entendimentos jurisprudenciais conflitantes.

A conjugação desses elementos, quais sejam as restrições de atuação da Comissão Federal do Comércio e a dificuldade de reconhecimento de ordens judiciais estrangeiras nos Estados Unidos, permite concluir que há poucos mecanismos jurídicos eficazes disponíveis para responsabilizar atores privados sediados nos Estados Unidos por violações a normas constitucionais e legislações de proteção de dados estrangeiras. Em poucas palavras, o modelo regulatório de privacidade estadunidense representa um poderoso escudo para os atores privados unicamente lá sediados.

Do ponto de vista da tutela de direitos fundamentais, isso significa que a arquitetura da Internet abre caminho para que esses atores – eminentemente privados –, refugiados em países que adotem modelos regulatórios que lhes sejam mais convenientes, tais como os Estados Unidos no caso da privacidade, interfiram na eficácia das normas constitucionais de outros países sem que existam mecanismos jurídicos efetivos que permitam equalizar ou obstar essa interferência. Mais do que isso: a concentração dessas empresas nos Estados Unidos, como demonstrou o levantamento empírico apresentado nesta tese, pode implicar a prevalência dos graus de proteção conferidos a direitos fundamentais nesse país em relação àqueles adotados em outras jurisdições. É como se a Internet estivesse operacionalizando um movimento de ampliação da aplicação extraterritorial da legislação estadunidense sem precedentes.

Nesse sentido, por mais que tenha procedido a uma análise eminentemente jurídica dos seus problemas de pesquisa, esta tese de doutorado extrapola o plano do direito e revela impasses que passam por questões geopolíticas relevantes. A insuficiência de mecanismos jurídicos efetivos de acesso e responsabilização dos atores privados estadunidenses que atuam no setor de Internet torna a sua concentração ainda mais perigosa para a tutela de direitos fundamentais por outros Estados nacionais.

Na medida em que podem prevalecer decisões tomadas por atores privados com base nos valores e interesses estadunidenses, novas disputas de poder se estalecem na

Internet. São disputas que podem se camuflar em questões meramente jurídicas mas que dizem respeito aos valores sobre os quais a Internet foi e continua sendo construída. Equacionar essas disputas é fundamental para que evitar que a arquitetura da Internet dê espaço para novas formas de imperialismo, turvadas pela opacidade do código e pelos ideais da liberdade individual.

BIBLIOGRAFIA

Abreu, Jacqueline de Souza. "From jurisdictional battles to crypto wars: Brazilian Courts v. WhatsApp", *Columbia Journal of Transnational Law* (2016) <disponível em: http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/, último acesso em 02.01.2017>.

Abreu, Jacqueline de Souza. "Bloqueios.info: sobre", *InternetLab* (2016) <disponível em http://bloqueios.info/pt/sobre/, último acesso em 18.12.2016>.

Afonso da Silva, Virgílio. "Colisões de direitos fundamentais entre ordem nacional e ordem transnacional", in Marcelo Neves, *Transnacionalidade do direito: novas perspectivas dos conflitos entre ordens jurídicas*. São Paulo: Quartier Latin, 2010.

Amoroso, Danilo. "Google Street View chega ao Brasil", *TecMundo* (2010) <disponível em: http://www.tecmundo.com.br/google-street-view/5650-google-street-view-chega-ao-brasil.htm, último acesso em 02.01.2017>.

Angwin, Julia / Jennifer Valentino-Devries. "Race is on to "fingerprint" phones, PCs", *Wall Street Journal* (30.11.2010) <disponível em: http://www.wsj.com/articles/SB10001424052748704679204575646704100959546, último acesso em 02.01.2017>

Antonialli, Dennys. "Watch your virtual steps: An empirical study of the use of online tracking technologies in different regulatory regimes", *Stanford Journal of Civil Rights and Civil Liberties* VIII (2012), 325-327.

Anthony, Sebastian. "Facebook wins privacy case, can track any Belgian it wants", *Ars Technica* (2016) <disponível em: http://arstechnica.com/tech-policy/2016/06/facebook-wins-privacy-case-against-belgiums-data-protection-authority/, último acesso em 02.01.2017>.

Assey, James M. / Demetrios A. Eleftheriou. "The EU-U.S. privacy safe harbor: Smooth sailing or troubled waters?", *J. Comm. L & Pol'y* 145 (2001), 158.

Associated Press. "Turkey pulls plug on Youtube over Ataturk 'insults'", *The Guardian* (07.03.2007) <disponível em http://www.theguardian.com/world/2007/mar/07/turkey, último acesso em 25.06.2016>.

Ayenson, Mika / Dietrich James Wambach / Ashkan Soltani / et al. "Flash cookies and privacy II: Now with HTML5 and ETag respawning", *SSRN* (2011) <disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390, último acesso em 02.01.2017>.

Ball, James. "NSA's Prism surveillance program: how it works and what it can do", *The Guardian* (08.06.2013) <disponível em https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google, último acesso em 29.10.2016>.

Barlow, John Perry. "A declaration of the independence of cyberspace", *Electronic Frontier Foundation* (1996) <disponível em: https://www.eff.org/pt-br/cyberspace-independence, último acessso em 02.01.2017>.

Barnett, Emma. "Twitter chief: we will protect our users from government", *The Telegraph* (18.10.2011), <disponível em http://www.telegraph.co.uk/technology/twitter/8833526/Twitter-chief-We-will-protect-our-users-from-Government.html, último acesso em 26.6.2016>.

BBC. "Turkey lifts two-year ban on Youtube", *BBC News Technology* (30.11.2010) <disponível em http://www.bbc.com/news/technology-11659816, último acesso em 25.6.2016>.

Beales, Howard. "The value of behavioral targeting", *Network Advertising Initiative* (2010) <disponível em: http://www.rutadonvasco.mx/web/20130406015458/http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf, último acesso em 02.12.2017>.

Bellyamy, Woodrow. "The Connected Aircraft: Beyond Passenger Entertainment and Into Flight Operations", *Avionics Today* (2014) <disponível em: http://interactive.avionicstoday.com/the-connected-aircraft/, último acesso em 02.01.2017>.

Beltrone, Gabriel. "Kids point to British Airways flights as they pass overhead on magical U.K. billboards", *AdWeek* <disponível em: http://www.adweek.com/adfreak/kids-point-british-airways-flights-they-pass-overhead-magical-uk-billboards-154067, último acesso em 02.01.2017>.

Berners-Lee, Tim. *Weaving the web: the original design and ultimate destiny of the world wide web by its inventor*. São Francisco: Harper Collins, 1999.

Bioni, Bruno. *Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet*. São Paulo: dissertação de mestrado (Universidade de São Paulo), 2016.

Bodoni, Stephanie / Aoife White. "Facebook wins Belgian court case over storing non-user data", *Bloomberg* (2016) <disponível em: https://www.bloomberg.com/news/articles/2016-06-29/facebook-wins-belgian-court-appeal-over-storing-non-user-data, último acesso em 02.01.2017>.

Brasil. "Brazil and Germany draft resolution: 'The right to privacy in the digital age'" (2013) <disponível em http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45, último acesso em 04.10.2016>.

Brito Cruz, Francisco. *Direito, Democracia e Cultura Digital: a experiência de elaboração legislativa do Marco Civil da Internet*. São Paulo: dissertação de mestrado (Universidade de São Paulo), 2015.

Calo, Ryan. "Boundaries of Privacy Harm", *The. Ind. LJ* 86 (2011), 1131.

____. "Digital market manipulation", *SSRN* (2013) <disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703, último acesso em 02.01.2017>.

Canaltech. "WhatsApp anuncia que passará a compartilhar dados com o Facebook", *Canaltech* (2016) <disponível em: https://canaltech.com.br/noticia/whatsapp/whatsapp-anuncia-que-passara-a-compartilhar-dados-com-o-facebook-77997/, último acesso em 02.01.2017>.

Cate, Fred H. *Privacy in the Information Age*. Washington, DC: Brookings Institution Press, 1997.

Cavoukian, Ann. "Privacy by design", *Info & Privacy Comml* (2009) <disponível em http://www.ipc.on.ca/images/resources/privacybydesign.pdf, último acesso em 02.01.2017>.

Clinton, William / Al Gore. *The framework for global electronic commerce* (1997) <disponível em: http://clinton4.nara.gov/WH/New/Commerce/, último acesso em 02.01.2017>.

Cody, Jonathan P. "Protecting privacy over the Internet: Has the time come to abandon self-regulation." *Cath. UL Rev* 48 (1998), 1183.

Connolly, Chris. "The US Safe Harbor-Fact or Fiction?", *Galexia* (2008) <disponível em: <https://pdfs.semanticscholar.org/8615/66e450b7934012651f7657a35f3283c6b533.pdf, último acesso em 02.01.2017>.

Connolly, Kate. "Angela Merkel: internet search engines are distorting perception", *The Guardian* (2016) <disponível em https://www.theguardian.com/world/2016/oct/27/angela-merkel-internet-search-engines-are-distorting-our-perception, último acesso em 04.11.2016>.

Conselho Editorial da The Economist. "The end of privacy", *The Economist* (1999) <disponível em: http://www.economist.com/node/202103, último acesso em 02.01.2017>.

Conselho Editorial do G1. "Balões com câmeras vão ajudar na segurança das Olimpíadas no Rio", *G1 Rio* (02.10.2015) <disponível em: http://g1.globo.com/rio-de-janeiro/noticia/2015/10/baloes-com-cameras-vao-ajudar-na-seguranca-das-olimpiadas-no-rio.html, último acesso em 02.01.2017>.

Coordenação do Ponto BR. *Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros 2014* (2015) <disponível em: http:// http://cetic.br/media/docs/publicacoes/2/TIC_Domicilios_2014_livro_eletronico.pdf, último acesso em 02.01.2017 >.

Daskal, Jennifer. "The un-territoriality of data", *Yale Law Journal* 125 (2015), 326.

Data Protection Commissioner. "Facebook Ireland Ltd, Report of Audit" (2001) <disponível em http://europe-v-facebook.org/Facebook_Ireland_Audit_Report_Final.pdf, último acesso em 28.10.2016>.

Davis, Matthew. "ETags allow tracking without cookies", *Future Hosting* (2014) <disponível em: https://www.futurehosting.com/blog/etags-allow-tracking-without-cookies/, último acesso em 02.01.2017>.

DC Rainmaker. "Wahoo fitness announces GymConnect: Treadmill integration & control", *DC Rainmaker* (2016) <disponível em: https://www.dcrainmaker.com/2016/01/announces-gymconnect-integration.html, último acesso em 02.01.2017>.

De La Chapelle, Bertrand / Paul Fehlinger. "Jurisdiction on the Internet: From legal arms race to transnational cooperation", *Internet and Jurisdiction paper* (2016), <disponível em http://www.internetjurisdiction.net/uploads/pdfs/Papers/IJ-Paper-Jurisdiction-on-the-Internet.pdf, último acesso em 18.12.2016>.

Diaz, Ann-Christine. "Facial recognition technology makes marketers a fun Big Brother", *Advertising Age* (2013) <disponível em: http://adage.com/article/news/brands-facial-recognition-campaigns/244233/, último acesso em 02.01.2017>.

Dhont, Jan et. al. "Safe harbour decision implementation study", *European Commission* (2004) <disponível em http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf, último acesso em 11.11.2016>.

Dobner, Petra. "More law, less democracy? Democracy and transnational constitutionalism", in Petra Dobner e Martin Loughlin (orgs.), *The twilight of constitutionalism?*. Oxford: Oxford University Press, 2010:148.

____ / Martin Loughlin. *The twilight of constitutionalism?*. Oxford: Oxford University Press, 2010.

Eckersley, Peter. "How unique is your web browser?", in Mikhail J. Atallah / Nicholas J. Hopper (orgs.) *Privacy Enhancing Technologies*. Berlin: Springer, 2010: 1–18.

Edelman, Benjamin / Michael Ostrovsky / Michael Schwarz. "Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords", *The American Economic Review* 97 (2007), 245.

Edelman, Scott et. al. "Enforcement of foreign judgements in 28 jurisdictions worldwide", *Gibson Dunn* (2015) <disponível em: http://www.gibsondunn.com/publications/Documents/Edelman-Jura-Enforcement-of-Foreign-Judgments-US.pdf, último acesso em 02.01.2017>.

Electronic Frontier Foundation. *Do not track* (2015) <disponível em: https://www.eff.org/issues/do-not-track, último acesso em 02.01.2017>.

____. *All about John Perry Barlow* <disponível em https://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/barlow_bio.html, último acesso em 02.01.2017>.

European Commission. "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", *Press release* (2012) <disponível em: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en, último acesso em 02.01.2017>.

____. "Communication from the Commission to the European Parliament and the Council on the functioning of the safe harbour from the perspective of EU citizens and companhies established in the EU", *European Commission* (2013) <disponível em: http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf, último acesso em 02.01.2017>.

Farivar, Cyrus. "Facebook now gives all new users a privacy tutorial, thanks to Irish authorities", *Ars Technica* (2012) <disponível em: http://arstechnica.com/business/2012/11/facebook-now-gives-all-new-users-a-privacy-tutorial-thanks-to-irish-authorities/, útlimo acesso em 02.01.2017>.

____, Cyrus. "How one law student is making Facebook get serious about privacy", *Ars Technica* (2012) <disponível em: http://arstechnica.com/tech-policy/2012/11/how-one-law-student-is-making-facebook-get-serious-about-privacy/, último acesso em 02.01.2017>.

Federal Trade Commission. "Staff report: Public workshop on consumer privacy on the global information infrastructure", *Federal Trade Commission* (1996) <disponível em: https://www.ftc.gov/reports/staff-report-public-workshop-consumer-privacy-global-information-infrastructure, último acesso em 02.01.2017>.

____. "Privacy online: A report to Congress", *Federal Trade Commission* (1998) <disponível em http://www.ftc.gov/reports/privacy3/index.htm, último acesso em 02.01.2017>.

____. "Privacy online: Fair information practice in the electronic marketplace: A report to Congress", *Federal Trade Commission* (2000) <disponível em https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf, último acesso em 02.01.2017>.

____. "The US Safe Web Act: Protecting consumers from spam, spyware and fraud - a legislative recommendation to Congress", *Federal Trade Commission* (2005) <disponível em http://www.ftc.gov/sites/default/files/documents/ reports/us-safe-web-act-protecting-consumers-spam-spyware-and-fraudlegislative-recommendation-congress/ussafeweb.pdf, último acesso em 02.01.2017>.

____. "The U.S. Safe Web Act: The first three years - a report to Congress", *Federal Trade Commission* (2009) <disponível em: https://www.ftc.gov/reports/us-safe-web-act-first-three-years-federal-trade-commission-report-congress, último acesso em 02.01.2017>.

____. "Data brokers: A call for transparency", *Federal Trade Commission* (2014) <disponível em https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf, último acesso em 02.01.2017>.

____. "Privacy and data security update", *Federal Trade Commission* (2015) <disponível em https://www.ftc.gov/reports/privacy-data-security-update-2015, último acesso em 07.07.2016>.

Farrell, Henry. "Negotiating privacy across arenas: The EU-US safe harbor discussions", in Adrienne Windhoff-Héritier, *Common goods: Reinventing European and international governance*, Lanham: Rowman & Littlefield, 2002: 105–127.

Fox, Zoe. "66% of Internet users in 1996 were in the U.S", *Mashable* (17.10.2013) <disponível em: http://mashable.com/2013/10/17/internet-users-1996/, último acesso em 02.01.2017>.

Frosio, Giancarlo / Paula Vargas. "Argentinian telecoms (and credit cards) ordered to block Uber app", *Center for Internet and Society at Stanford Law School* (2016) <disponível em: http://cyberlaw.stanford.edu/blog/2016/05/argentinian-telecoms-and-credit-cards-ordered-block-uber-app , último acesso em 02.01.2017>.

Froomkin, A. Michael. "The Death of Privacy?", *Stanford Law Review* 52 (2000), 1461.

Garside, Juliette. "More than 17,000 sign up to Austrian student's Facebook privacy class action", *The Guardian* (05.08.2014) <disponível em https://www.theguardian.com/technology/2014/aug/05/sign-up-austrian-student-facebook-class-action-data-violations, último acesso em 29/10/2016>.

Gasser, Urs. Perspectives on the Future of Digital Privacy, 134 Zeitschrift für Schweizerisches Recht [ZSR], 2015.

Gellman, Robert. "Does privacy law work?", in Philip E. Agre / Marc Rotenberg (orgs.) *Technology and privacy: The new landscape*, Cambridge, MA: MIT Press, 1997.

Goldsmith, Jack / Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press, 2006.

Google. "Google Transparency Report", *Google* (2016) <disponível em https://www.google.com/transparencyreport/traffic/#expand=PK,TR,IR,IQ, último acesso em 24.04.2014>.

Greenberg, Andy. "It's been 20 years since John Perry Barlow declared cyberspace independence", *Wired* (2016) <disponível em https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/, último acesso em 02.01.2016>.

Greenleaf, Graham. "Global data privacy laws 2015: 109 countries, with european laws now a minority", *SSRN* (2015) <disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529, último acesso em 02.01.2017>.

____. "Global tables of data privacy laws and bills", *UNSW Law Research Paper* 39 (2013).

Grimm, Dieter. "The achievement of constitutionalism and its prospects in a changed world", in Petra Dobner e Martin Loughlin (orgs.), *The twilight of constitutionalism?*. Oxford: Oxford University Press, 2010: 5-13.

Gruman, Galen. "Apple Watch: the internet of things' new frontier". *InfoWorld* (2014) <disponível em: http://www.infoworld.com/article/2608996/consumer-electronics/article.html, último acesso em 02.01.2017>.

Gruenwald, Juliana. "Safe harbor, stormy waters", *Interactive Week* 7 (2000), 26.

Heine, Christopher. "This interactive coke ad in a subway station winks and smiles when you do", *AdWeek* (2015) <disponível em: http://www.adweek.com/news/technology/interactive-coke-ad-subway-station-winks-and-smiles-when-you-do-166930, último acesso em 02.01.2017>.

Helft, Miguel / Tanzina Vega. "Retargeting ads follow surfers to other sites", *The New York Times* (30.08.2010) <disponível em: http://www.nytimes.com/2010/08/30/technology/30adstalk.html, último acesso em 02.01.2017>.

Hicks, Jennifer. "Johnnie Walker smart bottle debuts at mobile world congress", *Forbes* (02.03.2015) <disponível em: http://www.forbes.com/sites/jenniferhicks/2015/03/02/johnnie-walker-smart-bottle-debuts-at-mobile-world-congress/, último acesso em 02.01.2017>.

Hoofnagle, Chris Jay. *Federal Trade Commission Privacy Law and Policy*, Cambridge, MA: Cambridge University Press, 2016.

____ / Ashkan Soltani / Nathan Good / *et al*. "Behavioral advertising: The offer you cannot refuse" *SSRN* (2012) <disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2137601, último acesso em 02.01.2017>.

Horn, Leslie. "Twitter Confirms Egypt Ban", *PC Magazine* (26.01.2011) <disponível em http://www.pcmag.com/article2/0,2817,2376704,00.asp, último acesso em 30.09.2016>.

IBGE. "Celular se consolida como o principal meio de acesso à internet no Brasil", *Agência Brasil* (2016) <disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2016-12/ibge-celular-se-consolida-como-o-principal-meio-de-acesso-internet-no-brasil, último acesso em 02.01.2017>.

IBM. "Armazenamento em Cache de Solicitações GET", *IBM Knowledge Center* <disponível em: http://www.ibm.com/support/knowledgecenter/pt-br/SSFGJ4_7.6.0/com.ibm.mif.doc/gp_intfrmwk/rest_api/c_rest_get_caching.html, último acesso em 02.01.2017>.

Internet History Podcast. "Interviews", *Internet History Podcast* <disponível em: <http://www.internethistorypodcast.com>.

Internet World Stats. "Internet growth statistics: the global village online" <disponível em: http://www.internetworldstats.com/emarketing.htm, último acesso em 02.01.2017>.

Israeli Internet Law Update. "Israeli Court might not let Facebook off the hook on litigating in Israel", *Law.co.il* (2014) <disponível em:

https://www.law.co.il/en/news/israeli_internet_law_update/2014/12/09/IL-Court-says-Facebook-may-be-forced-to-litigate-in-Israel/, último acesso em 02.01.2017>.

Jackson, Jasper. "Adblock Plus wins another legal battle with German publishers", *The Guardian* (30.03.2016) <disponível em: https://www.theguardian.com/media/2016/mar/30/adblock-plus-publishers-suddeutsche-zeitung-adblocking, último acesso em 02.01.2016>.

Johnson, Bobbie. "Privacy no longer a social norm, says Facebook founder", *The Guardian* (11.01.2010) <disponível em: http://www.theguardian.com/technology/2010/jan/11/facebook-privacy, último acesso em 02.01.2017>.

Johnson, David / David Post. "Law and Borders – The Rise of Law in Cyberspace", *Stanford Law Review* 48 (1996).

Johnston, Douglas. "World constitutionalism", in Ronald MacDonald / Douglas Johnston (orgs.), *Towards world constitutionalism - issues in the legal ordering of the world community*. Leiden: Martinus Nijhoff, 2005.

Kallay, Dina / Marc Winerman. "First in the world: The FTC international program at 100", *Antitrust 39* 29 (2014), 5.

Kang, Margareth Hyun Suk. *A proteção de dados pessoais e o sistema legal sul coreano*. São Paulo: dissertação de mestrado (Universidade de São Paulo), 2016.

Kaye, Barbara K. *Just a click away : advertising on the Internet*. Boston: Allyn and Bacon, 2001.

Kerr, Dara. "Vimeo Banner in Indonesia for Allegedly Hustling Porn", *CNET* (13.5.2014) <disponível em http://www.cnet.com/news/vimeo-banned-in-indonesia-for-allegedly-hustling-porn/, último acesso em 26.06.2016>.

Klabbers, Jan / Anne Petters / Geir Ulfstein. *The Constitutionalization of International Law*. Oxford: Oxford University Press, 2009.

Kobrin, Stephen J. "Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance", *Review of International Studies* 30 (2004), 111–131.

Kravets, David. "U.N. report declares internet access a human right", *Wired* (2011) <disponível em: https://www.wired.com/2011/06/internet-a-human-right/, último acesso em 02.01.2017>.

Krisch, Nico. *Beyond constitutionalism: The pluralist structure of postnational law*. Oxford: Oxford University Press, 2010.

Kumm, Mattias. "The cosmopolitan turn in constitutionalism: An integrated conception of public paw", *Indiana Journal of Global Legal Studies* 20 (2013), 605–628.

Lemos, Ronaldo. *Direito, tecnologia e cultura*. Rio de Janeiro: Editora FGV, 2005.

Lessig, Lawrence. *Code: version 2.0* (2006) <disponível em: http://codev2.cc/download+remix/, último acesso em 02.01.2017>.

Liberatone, Stacy. "Live map shows Google searches, Tweets and YouTube views every second", *Mail Online* (2016) <disponível em: http://www.dailymail.co.uk/sciencetech/article-3662925/What-happens-internet-second-54-907-Google-searches-7-252-tweets-125-406-YouTube-video-views-2-501-018-emails-sent.html, último acesso em 02.01.2017>.

Lindahl, Hans. "We and cyberlaw: The spatial unity of constitutional orders". *Indiana Journal of Global Legal Studies* 20 (2013), 697–730.

Lomas, Natasha. "Facebook faces fines of $268K per day for tracking non-users in Belgium", *TechCrunch* (2015) <disponível em: http://social.techcrunch.com/2015/11/11/facebook-faces-privacy-fines/, último acesso em 02.01.2017>.

Loughlin, Martin. "What is constitutionalisation?", in Petra Dobner / Martin Loughlin (orgs.), *The twilight of constitutionalism?*. Oxford: Oxford University Press, 2010: 55.

Lynch, Katherine L. *The forces of economic globalization: Challenges to the regime of international commercial arbitration*. The Hague: Kluwer Law International, 2003.

Mathew, Jerin. "China defends blocking Facebook, Twitter and Bloomberg", *International Business Times* (16.01.2014) <disponível em http://www.ibtimes.co.uk/china-defends-blocking-facebook-twitter-bloomberg-1432488, último acesso em 30.09.2016>.

Mayer, Jonathan R. / John C. Mitchell. "Third-party web tracking: Policy and technology", *IEEE* (2012): 413–427 <disponível em: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6234427, último acesso em 02.01.2017>.

____. "Tracking the trackers: Early results", *Center for Internet and Society at Stanford Law School* (2011) <disponível em: http://cyberlaw.stanford.edu/blog/2011/07/tracking-trackers-early-results, último acesso em 02.01.2017>.

McCoy, Terrence. "Turkey bans Twitter – and Twitter explodes", *The Washington Post* (21.03.2014) <disponível em http://www.washingtonpost.com/news/morning-mix/wp/2014/03/21/turkey-bans-twitter-and-twitter-explodes/, último acesso em 30.09.2016>.

McGirt, Ellen. "Is Facebook enabling advertisers to discriminate by race?", *Fortune* (2014) <disponível em: http://fortune.com/2016/10/28/facebook-ad-propublica-race/, último acesso em 02.01.2017>.

Mohan, Pavithra. "Facebook privacy suit thrown out by Austrian Court", *Fast Company* (2015) <disponível em: https://www.fastcompany.com/3048127/fast-feed/facebook-privacy-suit-thrown-out-by-austrian-court, último acesso em 02.01.2017>.

Montulli, Lou. "The reasoning behind Web Cookies" *The irregular musings of Lou Montulli* (2013) <disponível em: http://www.montulli-blog.com/2013/05/the-reasoning-behind-web-cookies.html, último acesso em 02.01.2017>.

Neves, Marcelo. *Transconstitucionalismo*. São Paulo: Martins Fontes, 2009.

O'Donoghue, Aoife. *Constitutionalism in global constitutionalisation*. Cambridge: Cambridge University Press, 2014.

Olsen, Stefanie. "Yahoo to buy Overture for $1.63 billion", *CNET* (2003) <disponível em: https://www.cnet.com/news/yahoo-to-buy-overture-for-1-63-billion/, último acesso em 02.01.2017>.

Oppenheimer, Max Stul. "Internet cookies: When is permission consent", *Neb. L. Rev* 85 (2006), 383.

Paparella, Christopher / Andrea Engels. "Enforcement of foreign judgments 2016", *International Comparative Legal Guides* (2016) <disponível em: http://www.iclg.co.uk/practice-areas/enforcement-of-foreign-judgments/enforcement-of-foreign-judgments-2016/usa, último acesso em 17.08.2016>.

Papp, Anna Carolina. "Óculos do Google elevam receio com a privacidade", *Link Estadão* (2013) <disponível em: http://link.estadao.com.br/noticias/geral,oculos-do-google-elevam-receio-com-a-privacidade,10000033200, último acesso em 02.01.2017>.

Pearce, Graham / Nicholas Platten. "Orchestrating transatlantic approaches to personal data protection: A European perspective", *Fordham Int'l LJ* 22 (1998), 2024.

Pidd, Helen. "Facebook could face €100,000 fine for holding data that users have deleted", *The Guardian* (20.10.2011) <disponível em: https://www.theguardian.com/technology/2011/oct/20/facebook-fine-holding-data-deleted, último acesso em 02.01.2017>.

Pfanner, Eric / Somini Sengupta. "In a French Case, a Battle to Unmask Twitter Users", *The New York Times* (24.01.2013), <disponível em http://www.nytimes.com/2013/01/25/technology/twitter-ordered-to-help-reveal-sources-of-anti-semitic-posts.html, último acesso em 25.06.2016>.

Portal do Planalto. *Discurso da Presidenta da República, Dilma Rousseff, na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas* (2013) <disponível em: http://www2.planalto.gov.br/acompanhe-o-planalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua, último acesso em 02.01.2017>.

Post, Robert C. "Three concepts of privacy". *Geo. LJ* 89 (2000), 2087.

Prigg, Mark. "Privacy is dead, Harvard professors tell Davos forum", *Mail Online* (2015) <disponível em: http://www.dailymail.co.uk/sciencetech/article-2921758/Privacy-dead-Harvard-professors-tell-Davos-forum.html, último acesso em 02.01.2017>.

Prosser, William L. "Privacy", *Cal. L. Rev.* 48 (1960), 383-423.

Ratliff, James D. / Daniel Rubinfeld. "Online advertising: Defining relevant markets", *Journal of Competition Law and Economics* 6 (2010), 653–686.

Reidenberg, Joel R. "Resolving conflicting international data privacy rules in cyberspace", *Stanford Law Review* 52 (2000), 1315.

Reitman, Rainey. "White House, Google, and other advertising companies commit to supporting Do Not Track", *Electronic Frontier Foundation* (2012) <disponível em: https://www.eff.org/deeplinks/2012/02/white-house-google-and-other-advertising-companies-commit-supporting-do-not-track, último acesso em 02.01.2017>.

Ribeiro, John. "Google fined $1.2 million by Spain over privacy practices", *PCWorld* (2013) <disponível em: http://www.pcworld.com/article/2082320/google-fined-by-spanish-data-protection-authority-over-privacy-policy.html, último acesso em 02.01.2017>.

Ries, Brian / Lorenzo Franceschi-Bicchierai. "Facebook, Youtube, Twitter blocked in Iraq amid crisis", *Mashable* (13.6.2014) <disponível em http://mashable.com/2014/06/13/facebook-youtube-twitter-blocked-iraq/, último acesso em 26.9.2016>.

Robinson, Duncan. "Facebook faces EU fine over WhatsApp data-sharing", *Financial Times* (20.12.2016) <disponível em: https://www.ft.com/content/f652746c-c6a4-11e6-9043-7e34c07b46ef, último acesso em 02.01.2017>.

Roch, Michael P. "Filling the void of data protection in the United States: Following the European example", *Santa Clara Computer & High Tech. LJ* 12 (1996), 71.

Rol, Stibbe-Nicolas. "Court of Cassation definitively confirms Yahoo!'s obligation to cooperate with law enforcement agencies", *Lexology* (2016) <disponível em: http://www.lexology.com/library/detail.aspx?g=46b1a5f4-1ec4-4318-b7e9-753b23afa79f, último acesso em 02.01.2017>.

Rosen, Rebecca J. "Is this the grossest advertising strategy of all time?", *The Atlantic* (2013) <disponível em: http://www.theatlantic.com/technology/archive/2013/10/is-this-the-grossest-advertising-strategy-of-all-time/280242/, último acesso em 02.01.2017>.

Ruddick, Graham. "Admiral to price car insurance based on Facebook posts", *The Guardian* (2016) <disponível em https://www.theguardian.com/technology/2016/nov/02/admiral-to-price-car-insurance-based-on-facebook-posts, último acesso em 04.11.2016>.

Schaffer, Gregory. "Globalization and social protection: The impact of EU and international rules in the ratcheting up of U.S. privacy standards", *Yale J. Int 'l L.* 25 (2000), 1.

Schedden, David. "Today in media history: The first commercial web browser, netscape navigator, is released in 1994", *Poynter* (2014) <disponível em: https://www.poynter.org/2014/today-in-media-history-the-first-commercial-web-browser-netscape-navigator-is-released-in-1994/274065/, último acesso em 02.01.2017>.

Schonfeld, Erick. "Google ads will now follow you across the web", *TechCrunch* (2010) <disponível em: http://social.techcrunch.com/2010/03/25/google-ads-follow/, último acesso em 02.01.2017>.

Schrems, Max. "Legal procedure against 'Facebook Ireland Limited'", *Europe versus Facebook* (2016) <disponível em http://europe-v-facebook.org/EN/Complaints/complaints.html, último acesso em 29.10.2016>.

Schriver, Robert R. "You cheated, you lied: The safe harbor agreement and its enforcement by the Federal Trade Commission", *Fordham L. Rev.* 70 (2001), 2777.

Schwartz, John. "Giving the web a memory cost its users privacy", *New York Times* (04.09.2001) <disponível em: http://www.nytimes.com/2001/09/04/technology/04COOK.html?pagewanted=1, último acesso em 02.01.2017>.

Solove, Daniel. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.

____ / Woodrow Hartzog. "The FTC and the new common law of privacy", *Columbia Law Review* 114 (2014), 583–676.

Soltani, Ashkan et al. "Flash cookies and privacy" *SSRN* (2009) <disponível em http://ssrn.com/abstract=1446862, último acesso em 02.01.2017>.

Souza, Carlos Affonso Pereira de. "Quem bloqueia os bloqueadores?", *Observatório da Internet* (2016) <disponível em: http://observatoriodainternet.br, último acesso em 02.01.2017>.

Sprenger, Polly. "Sun on privacy: 'Get over it". *Wired* (1999) <disponível em: http://archive.wired.com/politics/law/news/1999/01/17538, último acesso em 02.01.2017>.

Stables, James. "The best smart bulbs for your connected smart home", *Wareable* (2016) <disponível em https://www.wareable.com/smart-home/best-smart-bulbs-for-your-tech-home, último acesso em 02.01.2017>.

Swire, Peter / Robert Litan. "None of your business: World data flows, electronic commerce, and the European Privacy Directive", *Harvard Journal of Law and Technology* 12 (1999), 683.

Teubner, Gunther. *Fragmentos constitucionais - constitucionalismo social na globalização*. São Paulo: Saraiva, 2016.

____. "Societal constitutionalism: Alternatives to state-centered constitutional theory?", in Christian Joerges / Inger-Johanne Sand / Gunther Teubner (orgs.), *Transnational Governance and Constitutionalism*. Oxford: Hart Publishing, 2004.

Tribunal Superior Eleitoral. "Corregedoria-Geral Eleitoral suspende acordo entre TSE e Serasa", *Imprensa* (2013) <disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2013/Agosto/corregedoria-geral-eleitoral-suspende-acordo-entre-tse-e-serasa, último acesso em 02.01.2017>.

Tozzetto, Claudia. "Spotify impõe renúncia ao sigilo bancário em nova política de privacidade", *O Estado de São Paulo* (22.12.2016) <disponível em http://link.estadao.com.br/noticias/cultura-digital,spotify-impoe-renuncia-ao-sigilo-bancario-em-nova-politica-de-privacidade,10000096090, último acesso em 23.12.2016>.

Wagner, Susan. *The Federal Trade Commission*. New York: Praeger Publishers, 1971.

Weise, Elizabeth. "Microsoft argues email stored in Ireland not subject to search warrant, *USA Today* (2015) <disponível em: http://www.usatoday.com/story/tech/2015/09/09/microsoft-ireland-second-circuit-court--appeals-jurisdiction/71937870/, último acesso em 02.01.2017>.

Williams, Rhiannon. "Google loses Court of Appeal bid to prevent UK users suing it", *Telegraph* (27.03.2015) <disponível em: http://www.telegraph.co.uk/technology/google/11499649/Google-loses-Court-of-Appeal-bid-to-prevent-UK-users-suing-it.html, último acesso em 02.01.2017>.

Whittaker, Zack. "U.S. search warrant can acquire foreign cloud, email data, judge rules", *ZDNet* (28.04.2014) <disponível em: http://www.zdnet.com/article/u-s-search-warrant-can-acquire-foreign-cloud-email-data-judge-rules/, último acesso em 02.01.2017>.

Wojcicki, Susan. "Making ads more interesting" *The Official Google Blog* (2009) <disponível em http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html, último acesso em 02.01.2016>.

Woods, Andrew. "Against data exceptionalism", *Stanford Law Review* 68 (2016), 729.

Yin, Sara. "Youtube banned in Turkey (again)", *PC Magazine* (03.11.2010) <disponível em http://www.pcmag.com/article2/0,2817,2372043,00.asp#fbid=NFZgGj_FTU6, último acesso em 25.06.2016>.

ANEXO I - Tabela com 80 aplicativos mais populares na loja Android

	Nome	País de incorporação	Representação no Brasil? (S/N)	Estado Americano
1	WhatsApp Messenger	EUA	Não (Facebook Brasil)	California
2	Messenger	EUA	Sim*	California
3	Facebook	EUA	Sim*	California
4	Instagram	EUA	Não (Facebook)	California
5	Facebook Lite	EUA	Sim*	California
6	Palco MP3	Brasil	Sim	
7	Uber	EUA/Países baixos	Sim	California
8	PSafe Antivírus Acelerador & Limpeza	Brasil	Sim	
9	TopBuzz	Não Disponível		
10	Snapchat	EUA	Não	California
11	AliExpress Shopping App	China	Não	
12	4Shared	British Virgin Islands	Não	California
13	Netflix	EUA	Sim	California
14	OLX	Brasil	Sim	
15	Subway Surfers	Dinamarca	Não	
16	Pou	Líbano	Não	
17	slither.io	EUA	Não	Michigan
18	Baixar músicas gratis MP3	Ilhas Virgens Britânicas	Não	
19	Z Camera	China	Não	
20	Musically	EUA	Não	California
21	Trash Manager - Clean Cache	Não disponível		
22	Meu Talking Tom	EUA	Não	California
23	Teclado Emoji Kika Pro Grátis	EUA	Não	California
24	Editor Fotos Colagem Montagens	EUA	Não	Virgínia
25	Power Clean Limpeza/Otimização	Hong Kong	Não	
26	Lanterna LED Super Brilhante	Não disponível		
27	Pokémon GO	EUA	Não	California
28	imo chat e chamadas de vídeo	EUA	Não	California
29	Google Play Games	EUA	Sim*	California
30	FIFA Mobile Futebol	EUA	Não	California
31	Minha Talking Angela	EUA/ Londres/ Chipre	Não	Califórnia
32	Clean Master (Otimizador)	China	Não	
33	Kika Keyboard	China	Não	
34	Clash Royale	Finlândia	Não	
35	Spotify	Suécia	Sim	

36	8 Ball Pool	Suíça	Não	
37	Zombie Tsunami	França	Não	
38	CM Security Antivírus AppLock	China	Não	
39	Cymera - Editor Foto&Beleza	Coreia	Não	
40	Talking Tom: Corrida do Ouro	EUA	Não	California
41	Traffic Rider	Turquia	Não	
42	Google Fotos	EUA	Sim*	Califórnia
43	ES File Explorer File Manager	China	Não	
44	Youtube	EUA	Sim	California
45	Photo Grid-Criador de Colagens	EUA	Não	California
46	Drive for Speed: Simulator	EUA	Não	Carolina do Norte
47	iFunny :)	Ilhas Virgens Britânicas	Não	
48	Piano Tiles 2	EUA/China	Não	California
49	Mercado Livre	Brasil	Sim	
50	Waze	EUA	Não (Google)	Califórnia
51	VivaVideo: Grátis	China	Não	
52	YouCam Makeup	EUA	Não	Califórnia
53	Central das notícias	Não disponível		
54	Dream Leagues	Reino Unido	Não	
55	Angry Birds 2	Finlândia	Não	
56	Caixa	Brasil	Sim	
57	B612 - Selfie do	Japão	Não	
58	Bradesco	Brasil	Sim	
59	Sweet Selfie -	China	Não	
60	Sniper 3D Assas	Hong Kong	Não	
61	PinOut	Suécia	Não	
62	Central das Notícias	n		
63	Mobile Security	República Tcheca	Não	https://www.avast.com/pt-br/contacts
64	Pinterest	EUA	Não	Califórnia
65	Photo Editor	China	Não	
66	Bloqueio (AppLock)	Hong Kong	Não	
67	VSCO	EUA	Não	Califórnia
68	Quem chama	Taiwan	Não	
69	Tinder	EUA	Não	Texas
70	Temple Run 2	EUA	Não	Carolina do Norte
71	Memory Optimizer	n		
72	Itau	Brasil	Sim	
73	Twitter	EUA	Sim	Califórnia
74	Banco do Brasil	Brasil	Sim	
75	Minecraft	EUA	Não	Califórnia
76	GuiaBolso	Brasil	Sim	

77	PicsArt	EUA	Não	Califórnia
78	Sing Karaoke	EUA	Não	Califórnia
79	Clash of Cans	Finlândia	Não	
80	Candy Crush	Malta	Não	

ANEXO II - Tabela com 80 aplicativos mais populares na loja da Apple

	Nome	País de incorporação	Representação no Brasil? (S/N)	Estado Americano
1	Uber	EUA	Sim	California (para residentes)
2	WhatsApp Messenger	EUA	Não (Facebook Brasil)	California
3	Messenger	EUA	Sim*	California
4	Facebook	EUA	Sim*	California
5	Instagram	EUA	Não (Facebook)	California
6	Youtube	EUA	Sim	California
7	PinOut!	Suécia	Não	
8	Snapchat	EUA	Não	California
9	Spotify	Suécia	Sim	
10	Netflix	EUA	Sim	California
11	Chrome	EUA	Sim*	California
12	OLX	Brasil	Sim	
12	Gmail	EUA	Sim*	California
13	BeautyPlus - Camera	China	Sim	
14	Musically	EUA	Não	California
15	Fúria Sniper	EUA	Não	California
16	Waze	EUA	Não (Google)	Califórnia
17	Google Maps	EUA	Sim*	California
19	Pinterest	EUA	Não	California
20	GuiaBolso	Brasil	Sim	
21	Enem - 2016	Brasil	Sim	
22	Bradesco	Brasil	Sim	
23	Tinder	EUA	Não	Texas
24	Caixa	Brasil	Sim	
25	Wish	EUA	Não	Califórnia
26	Boomerang from	EUA	Não (Facebook Brasil)	Califórnia
27	AliExpress Shopping App	China	Não	
28	Musik	n		
29	Sonic CD	EUA	Não	California
30	MakeupPlus - Editor	China	Sim	
31	Banco do Brasil	Brasil	Sim	
32	Google	EUA	Sim	Califórnia
33	Gear.Club	França	Não	
34	Meu Vivo Móvel	Brasil	Sim	
35	Bitmoji - Teclado	Canadá	Não	
36	Mercado Livre	Brasil	Sim	
37	Twitter	EUA	Sim	Califórnia
38	Itaú 30 horas	Brasil	Sim	
39	iFood Delivery	Brasil	Sim	

40	Layout from	EUA	Não (Facebook)	Califórnia
41	Microsoft Outlook	EUA	Sim	
42	Skype para iPhone	EUA	Não (Microsoft)	
43	Netshoes - Conecta	Brasil	Sim	
44	FreeMusic - baixar	n		
45	Clash Royale	Finlândia	Não	
46	Meu TIM	Brasil	Sim	
47	Santander Brasil	Brasil	Sim	
48	Google Drive	EUA	Sim	
49	AirBrush - Selfie	EUA	Não	Califórnia
50	Ataque Zumbi	França	Sim	
51	Sniper 3D Assasin	Hong Kong	Não	
52	Livro de colorir para entretenimento	Irlanda	Não	
53	Rock in Rio Racing	Brasil	Sim	
54	Palco MP3	Brasil	Sim	
55	Google tradutor	EUA	Sim	Califórnia
56	YouCam Makeup	EUA	Não	Califórnia
57	iMusic IE	n		
58	Duolingo	EUA	Não	Pensylvannia
59	Subway Surfers	Dinamarca	Não	
60	PhotoGrid Criador	EUA	Não	Califórnia
61	Color Switch	Emirados Árabes	Não	
62	Meu Alelo	Brasil	Sim	
63	Pokemon GO	EUA	Não	Califórnia
64	Clue	Alemanha	Não	
65	Airbnb	EUA	Sim	Califórnia
66	G1 Enem	Brasil	Sim	
67	Google fotos	EUA	Sim	Califórnia
68	iMusic BG free	n		
69	Nubank	Brasil	Sim	
70	FIFA Mobile Futebol	EUA	Não	Califórnia
71	Dropbox	EUA	Não	Califórnia
72	Sing Karaoke Music	EUA	Não	Califórnia
73	Shazam	Reino Unido	Não	
74	Candy Crush	Malta	Não	
75	iScanner	n		
76	VSCO	EUA	Não	Califórnia
77	IMO	EUA	Não	Califórnia
78	Deezer	França	Não	
79	Meu Malvado Favorito	França	Sim	
80	PicZoo	China	Não	