CENTRO UNIVERSITÁRIO DE BRASÍLIA – UniCEUB
FACULDADE DE CIÊNCIAS JURÍDICAS E SOCIAIS

Juliana Macedo Tomazini

PRIVACIDADE DIGITAL: PERSPECTIVAS E DESAFIOS AO DIREITO HUMANO À PRIVACIDADE NO MUNDO ONLINE

BRASÍLIA
2016

Juliana Macedo Tomazini

PRIVACIDADE DIGITAL: PERSPECTIVAS E DESAFIOS AO DIREITO HUMANO À PRIVACIDADE NO MUNDO ONLINE

Monografia apresentada ao Centro Universitário de Brasília (UniCEUB) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Graduação Latu Sensu na área de Relações Internacionais.

Orientador: Prof. Dr. Carlos Ricardo Caichiolo

BRASÍLIA
2016

Juliana Macedo Tomazini

PRIVACIDADE DIGITAL: PERSPECTIVAS E DESAFIOS AO DIREITO HUMANO À PRIVACIDADE NO MUNDO ONLINE

Monografia apresentada ao Centro Universitário de Brasília (UniCEUB) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Graduação Latu Sensu na área de Relações Internacionais.

Brasília, _____ de _____ de 2016

Banca examinadora:

_____
Professor Dr. Carlos Ricardo Caichiolo
Orientador

_____
Professor examinador

_____
Professor examinador

AGRADECIMENTOS

Ao término desse trabalho, percebo que tenho um excelente problema nas mãos: pessoas demais para agradecer.

Agradeço aos meus pais por seu apoio amoroso, onipresente e incondicional, cujo valor não poderia descrever nem se tivesse mais 80 páginas disponíveis. Ao meu irmão, por seu perpétuo bom humor e por suas tentativas (infrutíferas) de conter o avanço do meu espírito octogenário. À Lilo, por me ensinar silenciosamente sobre as coisas importantes da vida, e por me acordar cedo todos os dias das minhas férias para comer tapioca ou ir à praia.

Aos meus amigos, agradeço pelo ombro amigo, risadas e companheirismo, especialmente durante longas horas, dias, finais de semana e meses na biblioteca.

Ao meu orientador, Professor Dr. Carlos Ricardo Caichiolo, deixo aqui o meu sincero agradecimento pela orientação cuidadosa, paciência infinita e apoio irrestrito.

RESUMO

O presente trabalho busca esclarecer os desafios à preservação do direito humano à privacidade como o conhecemos em face de novas tecnologias presentes no mundo digital, particularmente aquelas relativas a coleta, armazenamento e processamento de dados. Sendo assim, busca esclarecer divergências taxonômicas relativa ao conceito de privacidade, assim como expor a codificação do direito humano à privacidade no ambiente internacional. Realiza uma ilustração de tecnologias atuais e busca demonstrar o quão arraigados os mecanismos de coleta, armazenamento e processamento de dados estão em atividades corriqueiras no mundo moderno. Dessa forma, busca ilustrar o impacto potencial das mesmas sobre a privacidade e, em última instância, a liberdade dos indivíduos. Finalmente, através da análise de legislações relativas ao assunto da União Europeia e dos Estados Unidos, busca também elucidar estratégias e abordagens futuras para a questão.

Palavras-chave: Privacidade digital. Privacidade de dados. Privacidade. Mineração de dados. Vigilância em massa. *Dataveillance*. Direitos Humanos.

ABSTRACT

The following study seeks to elaborate on the challenges to the preservation of the human right to privacy as we know it in face of new technologies in the digital world, particularly those related to the collection, storage and processing of data. As such, it seeks to expose divergent taxonomic views on the concept of privacy, as well as display the formal mechanisms around the world that govern the right to privacy. This study also illustrates how pervasive some of these technologies are in daily activities in the modern world, so as to demonstrate their potential impact on individuals' privacy, and ultimately on their freedom. Finally, by examining the legal environment on both the European Union and the United States in relation to this matter, it aims to ellucidate future strategies and approaches to this issue.

Keywords: Digital privacy. Data privacy. Privacy. Data mining. Mass vigilance. Dataveillance. Human Rights.

.

SUMÁRIO

INTRODUÇÃO

Vivemos em tempos de grandes mudanças. Em um mundo em que a tecnologia parece evoluir cada vez mais rápido, as formas como interagimos com nosso ambiente e aqueles que nos cercam são constantemente recicladas e alteradas, às vezes perpetuamente, para o bem e para o mal.

Se a tecnologia altera tão profundamente a forma como vivemos, é apropriado que avaliemos seu impacto sobre âmbitos mais fundamentais da vida humana. É possível que a tecnologia impacte o "viver no mundo" de tal forma que até mesmo os direitos humanos, que consideramos intrínsecos à existência de cada indivíduo, tenham de ser repensados?

Este trabalho busca responder à pergunta acima, com foco específico no direito humano à privacidade e no impacto que mecanismos de coleta, armazenamento e processamento de dados online têm sobre o mesmo. Como veremos a frente, esses mecanismos estão arraigados em uma variedade de atividades conduzidas diariamente no mundo moderno. Se nossas atividades geram dados que, por sua vez, são captados praticamente em tempo real, podemos considerar adequadas as manifestações clássicas do direito à privacidade, ou devemos repensar nossos meios para operacionalizá-lo e protegê-lo?

Ao longo deste estudo, buscaremos respostas aos questionamentos acima. Isso será feito através de três abordagens, divididas aqui em três capítulos. No Capítulo 1, esclareceremos brevemente a codificação do direito humano à privacidade e abordaremos a difícil lacuna taxonômica ao redor do conceito, de forma a esclarecer alguns dos desafios enfrentados e a assentar bases sólidas para a compreensão dos fatos que estudaremos adiante.

No Capítulo 2, nos aventuraremos muito brevemente em áreas mais técnicas, relativas aos mecanismos de coleta, armazenamento e processamento de dados supracitados. Exporemos, então, a difusão desses mecanismos nas mais diversas atividades do cotidiano, em âmbito governamental e privado, e exploraremos seu impacto, real e potencial, sobre a privacidade dos indivíduos.

Finalmente, no Capítulo 3, apresentaremos duas abordagens legais contrastantes à regulamentação de tais mecanismos e à preservação do direito humano à privacidade em face dos mesmos. Essas abordagens são representadas pelas legislações distintas da União Europeia e dos Estados Unidos relativas ao assunto. Finalmente, utilizaremos o contraste entre as duas partes para buscar em cada uma delas seus méritos e deficiências, de forma a inferir potenciais instrumentos ou perspectivas legais que melhor protejam esse direito fundamental.

Aqui se fazem necessários alguns esclarecimentos. O primeiro é acerca do termo "privacidade digital". Por frequência de uso no campo, como observaremos adiante, essa expressão é utilizada nesse trabalho de forma a denominar a privacidade de dados; isto é, a privacidade do indivíduo em relação a seus dados no mundo online. Os dois termos serão utilizados indistintamente ao longo deste trabalho, após as devidas explicações.

Em segundo lugar, o já mencionado impacto do meio online sobre as interações humanas é, por natureza, multifacetado. Isso significa que dele emergem diversos problemas, todos merecedores de atenção. No entanto, nem todas essas questões são abarcadas por esse estudo, por limitações práticas de tempo e espaço. Não é o objetivo deste trabalho explorar, por exemplo, assuntos como ciberterrorismo ou cibersegurança; tampouco falaremos sobre o impacto das mídias sociais sobre as relações humanas, ou o complexo relacionamento entre a internet e a liberdade de expressão e de informação.

As mesmas considerações práticas expostas acima informam a escolha das partes abordadas no Capítulo 3. Diversos países possuem regulamentos variados relativos à privacidade de dados, inclusive o Brasil; no entanto, os Estados Unidos e a União Europeia foram escolhidos por representarem abordagens extremamente diferentes entre si no mundo ocidental, cujo contraste melhor ilustra os caminhos à frente para aqueles que buscam legislar a questão. Foi decidido que apenas a legislação federal dos Estados Unidos e a legislação aplicável à União Europeia como um todo seriam abordadas nesse trabalho. Embora as legislações dos 50 estados norte-americanos e a legislação doméstica dos 28 Estados-membros da União Europeia tenham suas peculiaridades, a vasta quantidade de leis a serem analisadas não seria adequada a esse estudo. Além disso, as legislações supracitadas influenciam e são influenciadas pelas legislações em nível federal e europeu que apresentaremos, cuja abordagem nos permite uma visão mais ampla dos desafios a serem enfrentados.

Ademais, por frequência de uso, termos como *databases* e websites foram mantidos em sua forma em inglês ao longo do texto. Ademais, para facilidade de compreensão e pesquisa entre os campos, termos técnicos apresentados no Capítulo 2, como *data overlapping*, serão devidamente explicados e então utilizados em inglês ao longo do texto.

Finalmente, alguns dos documentos citados ao longo desse trabalho, especialmente Políticas de Privacidade de empresas, estão em constante processo de revisão. Dessa forma, é importante ressaltar que as versões utilizadas neste trabalho são aquelas em efeito em suas respectivas datas de acesso, listadas nas referências.

1. A CONCEITUALIZAÇÃO E A CODIFICAÇÃO DA PRIVACIDADE

Este capítulo busca estabelecer uma base sólida sobre a qual construiremos a análise da questão em lide. Sendo assim, será dado um espaço expositivo para os diversos instrumentos legais internacionais que codificam a privacidade como um direito humano, de forma a esclarecer o pensamento clássico sobre a operacionalização desse direito.

Em seguida, realizaremos uma análise conceitual sobre a privacidade, visando expor a falta de consenso sobre no que exatamente consiste a privacidade, e os impactos de tal dissonância sobre a tradução e concretização desse direito. Finalmente, realizaremos uma brevíssima exposição sobre o valor da privacidade, para então seguir em frente.

1.1. A Privacidade e o Direito Natural

O conceito de direitos naturais implica um sistema de direitos cujo conteúdo não se restringe às reivindicações que podem ser feitas através da lei, tendo assim um caráter mais profundo e fundamental. Seu valor, portanto, não parte de um sistema positivista de regras, mas tem como base leis que partem da própria natureza e, portanto, têm uma qualidade superior. As chamadas "leis naturais" (*Ius naturale*) partem de princípios imutáveis, de validade permanente e aplicação universal, e independem de qualquer decreto formal. Isto não significa que uma lei natural não possa ser positivada na forma de um código legal, e sim que essa lei natural existe, independentemente de sua codificação (BLAKE, 1925).

O direito natural não seria, portanto, aplicável a apenas um povo ou cultura em concreto; ele é caracterizado por seu universalismo, ou, como seus críticos apontam, por sua suposição de que as reivindicações legais de um povo em particular podem ser aplicáveis a todos os povos, independentemente de seus respectivos governos ou sistemas legais. Para compreender esse universalismo e como ele se reflete em nosso entendimento atual sobre direitos naturais, devemos mencionar muito brevemente a compreensão desse conceito ao longo do tempo. Historicamente, esse universalismo se apresentou de várias formas. A primeira é derivada de Tomás de Aquino e seus sucessores, que definiram o direito natural como um conjunto de princípios inseridos no coração dos homens por Deus. Todos, portanto, possuiriam tais direitos, simplesmente em virtude de sua humanidade. A segunda forma de apresentação de tal universalismo tem como base a tradição Hobbesiana; na visão reducionista de Hobbes, o fator comum entre todos os seres humanos é o movimento natural no sentido de evitar a morte. Para Hobbes, os princípios que regem a natureza não partiam de

Deus ou da humanidade de cada indivíduo, e sim da noção de que é sempre permissível defender a própria vida contra aqueles que a ameacem (PAGDEN, 2003). A lógica Hobbesiana para a universalidade do direito natural à preservação da própria vida foi explicada sucintamente por Steven Forde (2011) da seguinte forma: "a natureza fez os indivíduos independentes; a natureza deixou cada indivíduo para se defender sozinho, à sua sorte; logo, a natureza deve ter dado a cada indivíduo o direito de defender-se" (tradução nossa).

O mais famoso estudioso dos direitos naturais foi John Locke. Embora a visão de Locke do estado da natureza seja distinta da visão brutal de Hobbes, ambos concordam que a vida em sociedade não é natural ao homem. Os dois autores também divergem sobre a capacidade de ação do indivíduo dentro do estado da natureza; enquanto Hobbes defende que o indivíduo é livre para fazer o que quiser para se manter vivo e atingir seus objetivos, Locke defende em "*Two Treatises of Government*" que os indivíduos – mesmo no estado da natureza – têm o dever de respeitar os direitos dos outros indivíduos com os quais coexistem. Esse dever, segundo Locke, advém da lei natural. Sendo assim, não surpreende que, para Locke, os governos – uma vez que são formados como um produto de um "contrato social" e existindo apenas através do consentimento dos governados – tenham também o dever de proteger os direitos dos indivíduos (FORDE, 2011).

O conceito de dignidade da pessoa humana está intimamente ligado ao direito natural. Sarlet definiu a dignidade da pessoa humana da seguinte forma:

> A dignidade da pessoa humana é uma qualidade intrínseca, inseparável de todo e qualquer ser humano, é característica que o define como tal. Concepção de que em razão, tão somente, de sua condição humana e independentemente de qualquer outra particularidade, o ser humano é titular de direitos que devem ser respeitados pelo Estado e por seus semelhantes. É, pois, um predicado tido como inerente a todos os seres humanos (SARLET, 2002, p.22, apud PUC-RIO, [20--], p.15).

A dignidade da pessoa humana é, então, ontologicamente, um corolário da existência de cada indivíduo, cuja violação atinge o cerne da condição humana e viola também o princípio da igualdade entre os homens. Se a dignidade é intrínseca à condição humana, não se pode entender que uns sejam mais dignos que outros sem aceitar que uns sejam mais humanos que outros (PUC-RIO, [20--]).

Deve-se destacar o trabalho de Kant sobre o assunto, que pode ser considerado como uma das maiores influências do pensamento ocidental sobre o tema. Para Kant, o ser humano é um fim em si mesmo, e não apenas um objeto. O pensamento kantiano foi determinante sobre produção jurídica sobre o assunto (PAIANO; FURLAN, 2009).

O tema ganhou ênfase na comunidade jurídica internacional após os horrores que ocorreram durante a Segunda Guerra Mundial (1939-45). A era pós-guerra foi caracterizada pelo grande foco da comunidade internacional sobre os direitos humanos, isto é, sobre o reconhecimento de direitos fundamentais à pessoa humana a serem universalmente protegidos (BELLINHO, 2013).

É justamente a partir do período supracitado que passamos a ver a privacidade reconhecida como um direito humano e codificada como tal. A codificação da privacidade como direito humano teve um desenvolvimento peculiar. Em geral, tais direitos são primeiramente codificados no núcleo de direitos fundamentais garantidos pelas constituições dos Estados, e posteriormente promovidos do nível nacional para o nível internacional, quando já estejam solidamente estabelecidos e exista um contexto internacional propício para sua promulgação. O caminho inverso ocorreu no caso do direito humano à privacidade; as constituições dos Estados protegiam apenas alguns aspectos da privacidade, como a inviolabilidade da residência e da correspondência de indivíduos. Não havia na constituição de nenhum Estado uma garantia geral do direito à privacidade, e a legislação internacional foi muito além das garantias dadas em âmbito nacional desde o princípio (DIGGELMANN; CLEIS, 2014).

A Declaração Universal dos Direitos Humanos, proclamada em 1948 pela Assembleia Geral das Nações Unidas e redigida por líderes de diferentes formações culturais e legais, foi o primeiro documento internacional a tratar da privacidade como um direito humano, especificamente no Artigo 12:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks* (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948).[1]

Na Declaração Americana sobre Direitos e Deveres do Homem, aprovada na Nona Conferência Internacional Americana em Bogotá, em 1948, o Artigo V especifica que "Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar", e os Artigos IX e X mencionam o direito à inviolabilidade do domicílio e da correspondência (COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS, 1948, tradução nossa). Já a Convenção Americana de Direitos Humanos, proclamada em 1969 e também conhecida como Pacto de San José, define em seu Artigo 11

[1] Tradução nossa: "Ninguém deve estar sujeito a interferência arbitrária em sua privacidade, família, lar ou correspondência, ou a ataques contra sua honra ou reputação. Todos têm o direito a proteção da lei contra tais interferências ou ataques".

"O direito à privacidade", redigido de forma similar ao Artigo 12 da Declaração Universal dos Direitos Humanos, adicionando apenas que "toda a pessoa tem direito ao respeito da sua honra e ao reconhecimento da sua dignidade" (COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS, 1969, tradução nossa).

No continente europeu, a privacidade foi codificada como direito humano na Convenção Europeia sobre Direitos Humanos, proclamada em Roma em 1950. Sua redação é similar àquela adotada pela Convenção Universal de Direitos Humanos, porém com a seguinte ressalva:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (UNIÃO EUROPEIA, 1950, p.10).[2]

O Artigo 17 da Carta Árabe dos Direitos do Homem, criada no Cairo em 1994 e ratificada em 2004, possui redação similar àquela encontrada na Declaração Universal de Direitos Humanos e na Convenção Americana sobre Direitos Humanos, mas inclui também em seu escopo "*other private means of communication*" (outros meios privados de comunicação, tradução nossa) além da correspondência (LEAGUE OF ARAB STATES, 1994).

A Declaração da Associação de Nações do Sudeste Asiático (ASEAN) sobre Direitos Humanos (2012) possui redação similar àquela encontrada na Declaração Universal de Direitos Humanos, porém inclui "*personal data*" (dados pessoais, tradução nossa) sob sua proteção contra interferência arbitrária (ASSOCIATION OF SOUTHEAST ASIAN NATIONS, 2012).

Como se pode ver, a privacidade é codificada como direito humano em diversas convenções sobre o assunto ao redor do mundo. No entanto, embora todos os documentos supracitados mencionem a privacidade como um direito fundamental e universal a ser protegido, nenhum deles especifica o que exatamente é a privacidade, ou quais elementos compõem esse direito considerado tão fundamental para a dignidade da pessoa humana. Para responder a essa pergunta surpreendentemente complicada, abordada por diversos autores ao longo dos anos, devemos realizar uma análise conceitual sobre o tema.

---

[2] Tradução nossa: Não deve haver interferência por uma autoridade pública sobre o exercício desse direito, exceto em concordância com a lei e conforme o necessário em uma sociedade democrática no interesse da segurança nacional, segurança pública ou bem-estar econômico do país, para a prevenção da desordem ou do crime, para a proteção da saúde e da moralidade, ou para a proteção dos direitos e liberdades de outros.

1.2. Privacidade: uma análise conceitual

A legitimidade do direito à privacidade é raramente questionada em sociedades ocidentais democráticas. Por outro lado, o conceito de privacidade é sujeito a grande debate em termos legais e filosóficos, e um consenso ainda não foi atingido na comunidade acadêmica. Este trabalho se propõe debater inicialmente essa lacuna taxonômica, já que de sua resolução depende a concretização formal do direito à "privacidade" na comunidade internacional. Assim, antes de avaliarmos a preservação da privacidade do indivíduo na era digital, devemos nos perguntar: o que é a privacidade? E qual é seu valor?

Parte do problema de conceituar a privacidade tem origem em sua natureza multifacetada; uma análise a respeito inevitavelmente envolve elementos de Antropologia, Psicologia e Ciências Políticas, entre outros. Como veremos adiante, a natureza da condição de privacidade é elástica; sendo assim, o desafio enfrentado pela comunidade acadêmica é atingir um conceito isolado, indo além da descrição da condição de privacidade e seu gerenciamento.

Existem aqueles que defendem uma análise reducionista da privacidade, e a encaram como um derivado de direitos mais imediatos, como, por exemplo, a liberdade. A privacidade, portanto, não mereceria uma conceituação própria, sendo apenas parte do "pacote" de direitos mais fundamentais cuja preservação seria o suficiente para proteger a privacidade e o direito à mesma (DAVIS, 1959). Ademais, reducionistas não consideram imperativo que a privacidade seja conceituada isoladamente; pelo contrário, consideram que a privacidade é composta pela acumulação de diversas noções centrais relativas a outros conceitos, como liberdade e propriedade; o conceito seria, portanto, irreversivelmente heterogêneo (THOMSON, 1975).

Outros afirmam que, embora a privacidade tenha suas raízes em outros conceitos e seja formada por uma diversidade de outros direitos fundamentais, esta mistura dá forma a um conceito de caráter distinto e individual, que deve, portanto, ser abordado de forma isolada. A esta visão se dá o nome de "tese de coerência" (tradução nossa). Esta visão possui maior aceitação no campo de estudo em comento, em particular nos dias atuais (SCHOEMAN, 1984), e será a visão adotada por este trabalho.

Embora a maioria dos autores concorde sobre a necessidade de um conceito isolado para a privacidade, ou seja, adotem a linha da tese de coerência, isso não quer dizer que exista entre eles algum consenso sobre como essa conceituação deve ocorrer. Ao longo desta análise conceitual, a ausência de um léxico comum relacionado à privacidade se revelará um problema persistente desse campo. Essa ausência leva também a um obstáculo epistemológico

na busca por um conceito isolado. Observaremos que alguns autores buscam definir a privacidade de forma normativa; isto é, fazendo referência a obrigações éticas e considerações morais. Outros buscam definir a privacidade de forma descritiva, ou seja, buscando descrever as condições em que a privacidade ocorre (DECEW, 2015). Essa discrepância em relação a como a privacidade deve ser abordada conceitualmente é apenas mais um desafio a ser enfrentado nesta análise conceitual.

Como exposto acima, existem diversas formas e linhas de pensamento em relação à conceituação da privacidade. Com o propósito de atingir maior clareza, este trabalho irá utilizar a abordagem proposta por Tavani (2007) e dividir as principais visões do campo em duas categorias: aqueles que buscam definir a privacidade em termos de acesso, e aqueles que buscam fazer o mesmo em termos de informação. Dentro destas categorias, observaremos que existem diversos aspectos considerados fundamentais para a conceituação da privacidade, como a não-intrusão (*nonintrusion*), reclusão (*seclusion*), controle e limitação.

1.2.1. A Privacidade Definida em Termos de Acesso

A definição da privacidade em termos de acesso está presente em teorias que têm em comum o foco no acesso físico ou psicológico aos indivíduos, seja este na forma de observação ou através da intrusão no espaço pessoal do indivíduo (TAVANI, 2007). Em trabalhos de autores que adotam essa abordagem, frequentemente encontramos referências à não-intrusão sobre o indivíduo e à conexão entre privacidade e reclusão.

A noção da não-intrusão sobre o indivíduo como elemento essencial da privacidade foi introduzida por Samuel Warren e Louis Brandeis. Escrito em 1890, o artigo dos autores, "*The Right to Privacy*" (O Direito à Privacidade, tradução nossa), é considerado o trabalho seminal da empreitada da exploração legal e acadêmica do conceito de privacidade e sua aplicação ao mundo real (WESTIN, 1967). A privacidade está intrinsecamente ligada ao acesso para os autores, que definem o conceito como "o direito de ser deixado em paz" (WARREN; BRANDEIS, 1890, p. 195, tradução nossa). Isto é, o indivíduo se encontra na condição de privacidade quando está livre de intrusões externas.

Para Warren e Brandeis, assim como o direito natural do homem à propriedade surgiu a partir do direito natural do homem à vida, o direito à privacidade evoluiu a partir do direito natural do homem à propriedade, sob o qual era antes encapsulado. No entanto, a análise não é de forma alguma reducionista; se antes a privacidade era parte do direito natural do indivíduo à propriedade, os autores julgam que em sua época ela deveria evoluir como um

direito separado, devido a novas tecnologias emergentes na época, como fotografias instantâneas e jornais. O código legal da época seria, portanto, inadequado a esta necessidade gerada pela tecnologia; se antes o diário de um indivíduo devia ser protegido para que sua publicação não gerasse potencial lucro não autorizado a outrem, na nova era (de 1890) esta publicação devia ser prevenida, simplesmente pela paz de espírito gerada pela não-divulgação do conteúdo. Isto porque o direito à privacidade está ligado ao princípio de personalidade inviolada, o direito de um indivíduo à própria personalidade (WARREN; BRANDEIS, 1890).

Deve-se notar que a privacidade definida no âmbito da não-intrusão, como apresentado por Warren e Brandeis, possui caráter normativo. Em momento algum a condição de privacidade é descrita; ela é exposta com um bem de valor intrínseco, um direito, e não uma condição. Além disso, a relação estabelecida pelos autores entre o direito à privacidade e o princípio da personalidade inviolada parte claramente de considerações éticas. No entanto, é possível que essa ausência de valor descritivo seja um impedimento à completude desta definição. Embora os autores afirmem o valor do "direito de ser deixado em paz", em momento algum ocorre uma especificação do que exatamente constitui o "ser deixado em paz". Por exemplo, se durante uma caminhada um indivíduo A pede a um indivíduo B informações sobre um endereço, o indivíduo B não foi "deixado em paz", porém certamente não podemos afirmar que sua privacidade foi violada. Similarmente, se um indivíduo A agride fisicamente um indivíduo B, este definitivamente não foi "deixado em paz"; porém, a quebra desta paz nada teve a ver com a privacidade do indivíduo B (MOOR, 1990).

A falta de uma definição ou mesmo de uma elaboração sobre o que significa "ser deixado em paz" não permite que essa definição isole conceitualmente a privacidade de outros valores. Existem diversas formas de não se deixar um indivíduo em paz que nada têm a ver com privacidade, e poderiam ser melhor definidas através de conceitos como assédio ou violência, entre outros (PARENT, 1983). Ademais, a definição da privacidade como a ausência de intrusões parece confundir a privacidade com liberdade. Embora os conceitos estejam relacionados, não se referem à mesma condição. Pode-se afirmar que a privacidade é uma das condições que permitem o exercício da liberdade; se a liberdade é o que permite ao sujeito ter opiniões impopulares, a privacidade é o que lhe capacita a divulgar tais opiniões para alguns e ocultá-las de outros (TAVANI, 2007). Como observaremos ao longo deste capítulo, a não-diferenciação conceitual entre privacidade e liberdade é um problema persistente do campo.

Observamos, assim, que, embora a noção de não-intrusão possua grande valor na busca da conceitualização da privacidade, não é suficiente por si só para definir o conceito.

Devemos, portanto, explorar a noção de reclusão como elemento essencial para a garantia da privacidade.

A privacidade definida pela reclusão tem como principal característica a conexão entre a condição de privacidade e o "estar só". Sendo assim, a condição de privacidade perfeita ocorreria quando o indivíduo estivesse completamente só, fisicamente falando (TAVANI, 2007).

A reclusão é, por exemplo, essencial ao conceito de "privacidade natural". A privacidade natural refere-se a uma situação em que o indivíduo está naturalmente protegido de intrusões ou observações, por barreiras físicas ou naturais (MOOR, 1997). Neste caso, um indivíduo em uma ilha deserta se encontraria em uma situação de privacidade natural absoluta. Em termos menos absolutos, um indivíduo seria capaz de atingir uma condição de privacidade ao retirar-se de forma voluntária e temporária da sociedade em geral, física ou psicologicamente. Essa remoção física ou psicológica é apresentada por diversos autores como essencial ao desenvolvimento humano; Westin, por exemplo, argumenta que a privacidade é essencial, pois apenas através deste isolamento o indivíduo é capaz de fazer uma verdadeira reflexão sobre os acontecimentos e sua relação com eles, e assim atingir o autoconhecimento, considerado por ele essencial à condição humana (WESTIN, 1967). Novamente percebemos um valor normativo atribuído à privacidade.

A associação da privacidade à reclusão não é em si problemática; não confunde, por exemplo, privacidade com liberdade, uma confusão que encontramos anteriormente na relação entre privacidade e não-intrusão. Interessantemente, a relação entre privacidade e reclusão mistura valores normativos e descritivos, e talvez aí resida o problema maior nessa associação; o conceito da privacidade é confundido com a condição de isolamento. Isso torna difícil o isolamento conceitual entre a privacidade e a solidão, por exemplo. Além disso, se a privacidade pode ser atingida apenas na condição de reclusão, devemos nos perguntar qual é de fato o valor normativo da privacidade, pois o conceito torna-se claramente inatingível em boa parte da sociedade moderna. Dificilmente podemos defender a privacidade como valor essencial para a condição humana, se a própria privacidade é inatingível nas condições atuais; o conceito é, então, esvaziado de seu valor (TAVANI, 2007).

Ao analisar formas de se pensar a privacidade em termos de acesso, é interessante analisar o quão simbiótica é a relação entre reclusão e não-intrusão. William Prosser, por exemplo, buscou definir negativamente a privacidade através de quatro aspectos definitivos, que claramente combinam elementos das duas condições, incluindo a intrusão sobre a solidão ou reclusão de um indivíduo, a divulgação de fatos embaraçosos sobre o indivíduo, a criação

de uma imagem falsa do indivíduo para o público, e a apropriação da imagem de um indivíduo para o lucro indevido (PROSSER, 1960).

Observemos, também, que existe um elemento de privacidade informacional nas obras dos autores acima. Mesmo ao definir a privacidade em termos de acesso, Warren e Brandeis, assim como Prosser, inserem elementos referentes ao controle de informações relativas ao indivíduo, por mais que a preocupação com o controle informacional esteja ligada à possibilidade do caráter difamatório deste.

O fato de o acesso não se sustentar como pilar único para o conceito e a condição de privacidade não significa que as formas de pensamento expressas dentro dessa linha de raciocínio devam ser filosoficamente dispensadas. Embora autores modernos dificilmente busquem definir a privacidade apenas em termos de isolamento e reclusão, a associação entre a privacidade e a reclusão é recorrente até mesmo no trabalho de teóricos da privacidade informacional, que exploraremos no decorrer deste estudo. Alan Westin e James Moor, por exemplo, são teóricos da privacidade informacional que, como veremos mais à frente, fazem uma associação entre a condição de reclusão e a condição da privacidade.

A já aludida natureza multifacetada do conceito em lide faz com que dificilmente uma forma de conceituação seja capaz de sustentar sozinho todo o significado do conceito, mas torna igualmente difícil descartar totalmente o princípio por trás de cada forma de conceituação. Sendo assim, o pensamento da privacidade em termos de acesso não tem apenas papel histórico na conceitualização da privacidade, como também influencia outras teorias mais atuais de pensamento sobre o assunto. Por exemplo, devemos manter em mente o aspecto da reclusão e não-acesso psicológicos do indivíduo; mais adiante, observaremos que esse elemento é essencial na formação do pensamento sobre a privacidade na era da interconectividade.

Dessa forma, devemos buscar outras formas de atingir um conceito concreto de privacidade. A privacidade em termos de acesso, como vimos acima, atribui valor descritivo e normativo para o conceito, porém não é suficiente para uma caracterização completa. Analisemos, portanto, uma nova perspectiva: a definição da privacidade em termos de informação, também conhecida como privacidade informacional.

1.2.2. A Privacidade Definida em Termos de Informação

Ao buscarmos uma definição da privacidade em termos de informação, abandonamos a visão de que a privacidade do indivíduo é preservada apenas quando o acesso físico e

psicológico ao mesmo é controlado. As teorias que subscrevem essa visão têm em comum o caráter determinante atribuído à informação como fator definitivo da privacidade, seja através do controle da informação ou da limitação do acesso à mesma. Aqui observaremos dois aspectos principais apresentados por diversos autores como essenciais ao direito à privacidade: o controle sobre a informação e a limitação de acesso à informação. Isso não quer dizer que exista uma linha clara entre esses dois aspectos, que compartilham entre si linhas ainda mais difusas do que aquelas existentes na definição da privacidade em termos de acesso.

Antes de iniciarmos, deve-se ressaltar que não há que confundir a privacidade definida em termos de acesso, como exposta anteriormente, e a idéia da limitação de acesso à informação**.** Esta última não se refere ao acesso ao indivíduo, como a abordagem exposta anteriormente, e sim ao acesso a informações sobre o mesmo.

Alan Westin é o principal teórico da privacidade informacional. Sua obra, citada ad nauseam em trabalhos sobre o assunto, define o conceito como "*the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*"[3] (WESTIN, 1967, p. 7).

A definição de privacidade de Westin possui claro foco no controle sobre a informação, e tem como princípio fundamental a noção de que a privacidade não está necessariamente ligada ao conteúdo das informações sobre um individuo, e sim ao controle que o indivíduo em questão exerce sobre essas informações e sua divulgação (FRIED, 1984). Isto é, o indivíduo deve ser capaz de decidir quando, como e com quem compartilhar informações acerca de si mesmo. Um exemplo seria o compartilhamento de um indivíduo A sobre seu diagnóstico como HIV+ com um indivíduo B. O conhecimento do indivíduo B acerca desse diagnóstico não é em si uma violação da privacidade do indivíduo A, contanto que este tenha escolhido quando, como e até que ponto compartilhar esta informação com o indivíduo B. Esse foco no controle do indivíduo sobre suas informações é chamado de "privacidade decisional" (MOORE, 1965, p.5).

O foco no controle que o indivíduo exerce sobre as informações como elemento fundamental da privacidade ressalta a capacidade de escolha que é dada ao indivíduo *através* da privacidade. Ao reconhecer esse aspecto como essencial ao conceito, emerge a noção de que a privacidade é também pré-condição para uma série de outros direitos do indivíduo.

[3] Tradução nossa: A privacidade é a reinvindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como, e até que ponto informações sobre eles são comunicadas a outros.

Além disso, o foco no controle exercido sobre as informações, e não no conteúdo das mesmas, pode ser benéfico para garantir a universalidade do conceito de privacidade. O exercício do direito à privacidade passa necessariamente por um processo social inserido em um contexto cultural; isto é, a privacidade, ainda que seja um valor universal, tem manifestações psicológicas culturalmente específicas (ALTMAN, 1977). Ao se explorar o controle como cerne do conceito, garantimos que este se aplique universalmente, independentemente de culturas ou contextos específicos, pois a divulgação de uma informação com determinado conteúdo sobre um indivíduo A poderia ser considerada uma violação de privacidade em uma cultura X, porém ser considerada uma informação de caráter público em uma cultura Y. Por exemplo, culturas que valorizam o coletivismo, como a indiana, definem um indivíduo através de sua relação com o "todo", como sua família e sua comunidade. Na Índia, discutir informações de conteúdo médico de um indivíduo com seus familiares é uma prática normal. Já as culturas ocidentais, em sua maioria, possuem um maior grau de individualidade. Se um médico compartilhar informações médicas de uma mulher diretamente com seu marido em um país como a Inglaterra, essa discussão constituiria uma violação da privacidade da mulher em questão, pois informações médicas são consideradas privadas nessa cultura. Isso não quer dizer, no entanto, que a privacidade deixe de ser um valor universal, ou que seja menos valorizada na Índia que na Inglaterra – significa apenas que a manifestação psicológica da privacidade na Índia é diferente da manifestação ocidental do mesmo valor. No entanto, ao nos focarmos no aspecto do controle sobre as informações, poderíamos afirmar que, se a esposa britânica supracitada teve controle sobre o compartilhamento de suas informações médicas com seu marido, a privacidade dela não foi necessariamente violada (BASU, 2012).

No entanto, se encararmos o controle como único elemento do conceito, será difícil especificar como a privacidade se diferenciaria da autonomia ou da anonimidade. Por exemplo, suponha que um indivíduo A decida voluntariamente divulgar aos quatro ventos todas as informações sobre si mesmo. Certamente o indivíduo ainda possui controle sobre as informações divulgadas; afinal, foi ele quem decidiu onde, quando, como e o que seria divulgado. No entanto, o resultado dessa decisão não foi um aumento de sua privacidade, e sim uma diminuição da mesma (PARENT, 1983). O indivíduo, nesse caso, apenas exerceu autonomia sobre que informações a respeito de sua pessoa devem ser de conhecimento público.

Similarmente, podem existir situações em que o indivíduo não possui controle algum sobre a informação divulgada, porém sua privacidade não é necessariamente violada. Sugerir

que a privacidade é definida exclusivamente pelo controle sobre todas as informações relativas a si significa que tudo que é realizado em público por um indivíduo é uma violação de sua privacidade (FRIED, 1970), arriscando assim confundir a condição da privacidade com a condição de anonimidade. Em termos práticos, não existe nesta teoria uma definição sobre que tipos de informação pessoal podemos esperar controlar, e quanto controle devemos ser capazes de exercer.

Como se pode ver, a falta de importância atribuída por esta teoria ao conteúdo da informação em questão torna problemático o processo de isolar o conceito de privacidade. Alguns autores defendem que o relacionamento entre a privacidade e outros conceitos cognitivos, como anonimidade e liberdade, é irreversivelmente complexo, devido às discordâncias sobre o limite do conceito de privacidade (MARGULIS, 2011). No entanto, o foco exclusivo no controle exercido sobre informações, independentemente de seu conteúdo, é uma caracterização subjetiva da privacidade como apenas uma forma de liberdade. Se a liberdade significa a ausência de restrições ou coerções externas sobre as ações do indivíduo, o princípio do controle como elemento fundamental da privacidade apenas reafirma o direito dos indivíduos de exercer controle autônomo sobre suas escolhas. A idéia é certamente válida, porém fracassa em isolar conceitualmente a privacidade (PARENT, 1983).

Enquanto o foco no controle sobre a informação recai exclusivamente no controle exercido pelo indivíduo sobre informações relativas a si, aqueles que defendem a limitação do acesso à informação oferecem um foco alternativo que concentra-se no conteúdo da informação relativa ao indivíduo. Isso porque a privacidade é definida por expoentes desta teoria como "a condição caracterizada pela não-possessão de conhecimento pessoal não-documentado sobre o indivíduo por outras partes"[4] (PARENT, 1983, p. 269, tradução nossa).

Para compreender a definição acima, devemos primeiramente conceituar "conhecimento pessoal não-documentado", ou "Informações pessoais não-públicas"[5] (TAVANI, 2007, p. 7, tradução nossa). Essas informações são entendidas como fatos que a maioria dos indivíduos que vivem em sociedade não gostariam que fossem amplamente conhecidos pela sociedade em geral, mas cujo conhecimento por um círculo restrito de associados não seria necessariamente considerado problemático. A especificação sobre o caráter do conhecimento em questão ("não-documentado") é relevante, pois diferencia informações sobre o indivíduo que fazem parte de um acervo público (por exemplo, registros

[4] "Privacy is the condition of not having undocumented personal knowledge about one possessed by others."
[5] "Non-public personal information (NPI)"

de prisão) e informações de caráter não-público, como, por exemplo, orientação sexual (PARENT, 1983).

O foco no conteúdo de informações e o reconhecimento de zonas de privacidade para limitar o acesso a informações pessoais tem o benefício de evitar a confusão entre a privacidade e outros conceitos como a autonomia, a liberdade ou o isolamento, problema que encontramos no foco exclusivo sobre o controle (GAVISON, 1980).

No entanto, a limitação da privacidade simplesmente como a "não-possessão de informações não documentadas" sugere que um indivíduo possui privacidade apenas na medida em que informações sobre ele não estejam disponíveis; isto é, quanto maior a restrição ou ocultação de informações sobre o indivíduo, mais privacidade ele possui (SOLOVE, 2002). Além disso, nem toda informação que é de caráter não-público é necessariamente privada, e nem toda informação privada possui necessariamente caráter não-público. Por exemplo, planos militares secretos têm caráter não-público, mas não diríamos que possuem caráter "privado". Similarmente, embora as dívidas de um indivíduo estejam disponíveis para consultas e tenham caráter público, dificilmente afirmaríamos que, caso tais informações fossem divulgadas, a privacidade do indivíduo permaneceria inviolada. O conceito de privacidade, então, acaba por se misturar com o conceito de sigilo, novamente afastando-nos de um conceito isolado para a privacidade (DECEW, 1997).

É interessante notar que as deficiências apresentadas pela chamada "privacidade decisional" e aquela definida pela limitação do acesso a informações podem ser amenizadas caso princípios das duas visões sejam combinados. Esse fato não passou despercebido por alguns autores do campo. Mais recentemente, teóricos têm buscado uma versão hibrida das visões acima, que incluem elementos da privacidade definida em termos de acesso.

1.2.3. Conceitualização da Privacidade: Uma Visão Híbrida

Não é surpresa que teóricos do campo tenham buscado atingir uma visão híbrida dos conceitos explorados acima, de forma a balancear os méritos e deficiências de cada teoria. Deve-se enfatizar que esses teóricos buscaram definir a privacidade dentro da tese de coerência – ou seja, acreditam que a privacidade seja um conjunto multifacetado de idéias que, no entanto, culminam em um direito específico. Dessa forma, essa visão híbrida enfrenta o desafio de definir o direito à privacidade claramente, dentro de uma estrutura epistemológica rígida.

James Moor deu a essa visão híbrida o nome de *Restricted Access/Limited Control Theory* (RALC), ou Teoria do Acesso Restrito/Controle Limitado (tradução nossa) (MOOR, 1990, 1997). Embora nem todos os autores utilizem essa nomenclatura específica para essa teoria híbrida, observaremos que vários subscrevem às suas noções principais.

Moor explica que um indivíduo está em uma situação de privacidade se estiver protegido da "intrusão, interferência e acesso a informação por outras pessoas" (MOOR, 1997, p. 3, tradução nossa). Tal definição nos permite pensar na privacidade tanto em sua situação natural (aquela em que o indivíduo está naturalmente protegido de observação ou interferência) quanto normativa, isto é, quando o indivíduo é protegido da invasão de sua privacidade por normas e leis estabelecidas para protegê-lo nessas situações. Situações de privacidade normativa podem incluir locais (como a residência de uma pessoa), relacionamentos (como a confissão religiosa) e até atividades (como o voto). É importante observar também que a RALC busca definir a privacidade através de situações; isto é, busca definir a privacidade ao descrever no que consiste uma situação de privacidade (TAVANI, 2007).

Talvez a forma mais simples de definir a privacidade nesta visão seja a condição de proteção contra o acesso indesejado de outros ao "*self*". Esse "*self*" inclui desde a pessoa, fisicamente, até suas informações pessoais, pois expoentes dessa visão propõem que a privacidade é um conceito que abrange informações, acesso e expressões (DECEW, 1997).

Autores críticos dessa visão híbrida tendem a caracterizá-la como excessivamente vaga. A abrangência extensa do conceito tornaria difícil a diferenciação do privado e do público e, portanto, não serviria ao propósito de isolar a privacidade conceitualmente (ELGESEM, 1999). No entanto, observamos que a RALC possui elementos tanto da privacidade definida em termos de acesso quanto da privacidade informacional, e que sana algumas das deficiências de cada uma dessas visões ao combiná-las. Caracteriza o acesso ao indivíduo como importante, porém enfatiza que esse acesso deve ser regulado também normativamente, diferenciando assim o conceito da privacidade do de isolamento. Mantém elementos da privacidade informacional ao caracterizar as informações do indivíduo como parte do "self" a ser protegido, porém não restringe o escopo da privacidade a apenas dados. Também refere-se a elementos da privacidade decisional ao condicionar o conceito à proteção do acesso indesejado**,** sem, no entanto, descartar a importância do conteúdo das informações em questão (MOORE, 1965).

A visão híbrida da RALC será, portanto, a visão adotada por este trabalho, por se avaliar que a mesma possui abrangência que permite melhor abarcar as situações em que se necessita definir a privacidade no mundo atual.

O desafio de definir a privacidade como conceito e direito permanece até hoje. Como mencionado no início deste capítulo, não existe um consenso dentro das comunidades jurídica e acadêmica sobre o assunto. A intenção da análise conceitual exposta ao longo das últimas páginas foi apresentar ao leitor uma breve exposição dos diversos aspectos que constituem esse conceito indefinido e multifacetado, de forma a prover um referencial conceitual para os assuntos discutidos ao longo dos próximos capítulos.

1.3. A importância da privacidade: uma breve exposição

É possível que a busca pela conceituação de um valor tão vago tivesse sido abandonada, não fosse a importância que a privacidade como direito humano ocupa dentro do sistema de valores modernos. Não existe uma resposta específica sobre o porquê de a privacidade ser tão importante para a experiência humana, porém é inegável que valorizamos esse direito distinto como uma forma de regular e manter as demais relações sociais (RACHELS, 1975).

A privacidade ganha importância especialmente dentro do conjunto de valores liberais presentes nas sociedades ocidentais modernas, que colocam a liberdade do indivíduo como qualidade essencial para a experiência humana (BERLIN, 1969). Sendo assim, a privacidade é vista como um dos valores essenciais à manutenção da liberdade e da autonomia do indivíduo, e também à inviolabilidade de sua personalidade e dignidade (BLOUSTEIN, 1964). Sem a privacidade, a intimidade entre pessoas seria de impossível realização, impedindo assim a formação de laços como a confiança e a amizade, essenciais para a experiência humana (GERSTEIN, 1978).

Isso não significa que não existam aqueles que questionam a instrumentalização da privacidade. Autoras feministas como Anita Allen, por exemplo, afirmam que a privacidade pode ser instrumentalizada de forma a ocultar o abuso sistemático cometido por homens contra mulheres dentro do patriarcado. Apesar disso, nem mesmo Allen sugere que descartemos o direito à privacidade completamente devido a problemas em sua operacionalização (DECEW, 2015).

Este trabalho subscreve à visão de que a privacidade é um direito de suma importância para experiência humana. Ao longo do próximo capítulo, iremos olhar de perto a evolução da

tecnologia e seus potenciais impactos sobre a operacionalização da privacidade, particularmente em relação aos mecanismos atuais de coleta de dados.

2. BIG DATA ANALYTICS E A PRIVACIDADE NA ERA ONLINE

Não há dúvidas de que a tecnologia é um agente poderoso de mudanças. O avanço da tecnologia em diferentes áreas alterou profundamente a forma pela qual nos comunicamos, consumimos, aprendemos e até mesmo pensamos. O objetivo deste capítulo é investigar o impacto da tecnologia sobre o gerenciamento da privacidade. Iremos investigar se é necessário realizar uma nova tradução e interpretação desse direito universal, dadas as novas formas de acesso ao indivíduo tornadas possíveis pela tecnologia, especialmente aquelas relacionadas à coleção de dados e informações online (JOYCE, 2015).

Neste Capítulo, faz-se necessário um afastamento breve das Relações Internacionais de forma a esclarecer os mecanismos e instrumentos supracitados. Embora estes não sejam o foco principal deste trabalho, é necessário que o funcionamento desses instrumentos seja explicitado para que possamos, mais adiante, compreender seu impacto sobre o direito humano à privacidade nos dias atuais.

A coleta rotineira de dados (*data*, em inglês) sobre indivíduos, realizada por diferentes organizações, não é nada novo. Em âmbito governamental, alguns países da Europa ocidental, por exemplo, coletavam e mantinham dados sobre suas populações desde o século XVIII, de forma a melhor administrar o sistema previdenciário e a emissão de passaportes. O primeiro censo do Brasil, o Censo Geral do Império, ocorreu em 1872 (INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 20[--]). No século XX, antes da popularização do computador, a maior parte dos governos ao redor do mundo já havia estabelecido práticas de manutenção de registros de seus cidadãos, como carteiras de identidade, carteiras de motorista, registro de propriedade etc. A prática também não é nova dentro do âmbito das empresas; bancos e agências de crédito já mantinham e compartilhavam informações sobre a liquidez de clientes desde a metade do século XX. É razoável, portanto, concluir que organizações estão constantemente buscando novas formas de coletar, compartilhar e utilizar dados pessoais, que serão usados para propósitos definidos por essas organizações (RULE, 2007).

Embora a coleta de dados sobre indivíduos por diferentes organizações não seja novidade, as capacidades geradas pela tecnologia para esta prática são inteiramente novas; a amplitude, especificidade e volume de informações coletadas por organizações hoje são algo nunca antes visto. (GOLDFARB; TUCKER, 2012). As tecnologias a que faremos referência ao longo deste capítulo podem ser divididas amplamente entre aquelas dedicadas à coleta de informação e aquelas dedicadas ao processamento da informação coletada.

Todos os dias, bilhões de indivíduos geram e compartilham dados online entre si e com organizações. Esses dados podem ser compartilhados conscientemente, como, por exemplo, as informações fornecidas por um indivíduo em seu perfil do Facebook. No entanto, existe também aquilo que chamamos de coleta passiva de dados, que é realizada por uma variedade de organizações através de diversos mecanismos. Por exemplo, web sites, ou organizações que trabalham em parceria com *websites*, rotineiramente instalam softwares chamados "*cookies*" nos computadores de visitantes. O *cookie* comporta-se como um vírus: uma vez instalado no computador do usuário, pode rastrear diferentes informações sobre o mesmo. Que tipo de informação é coletada depende do tipo de *cookie* instalado. Alguns são programados para detectar os *websites* que foram vistos antes e após a visita, se o usuário já visitou aquele site antes, que itens foram vistos no *website* e até mesmo que informação foi inserida no computador enquanto o site era acessado. Outros podem rastrear o endereço IP[6] do usuário, o que por sua vez permite que tenham acesso ao seu endereço físico, ou toda a informação que é digitada enquanto o usuário está online e qual o conteúdo de outras janelas que estão abertas simultaneamente (WITTE, 2014).

Dispositivo popularizado nos dias atuais, os smartphones nada mais são que pequenos computadores. Ao realizar chamadas, um indivíduo gera informações sobre onde está, que são coletadas por sua operadora. Alternativamente, caso o indivíduo esteja simplesmente carregando consigo um celular que possui capacidade de GPS (*Global Positioning System*, ou Sistema de Posicionamento Global, em português), estará transmitindo constantemente dados sobre onde está e onde esteve. Estes são apenas alguns exemplos dos incontáveis mecanismos de coleta passiva de dados. Atualmente, existem poucas ações da vida diária dos indivíduos que não gerem algum tipo de dados residuais, que são coletados de tantas formas e por tantas organizações que se tornou virtualmente impossível saber exatamente que dados foram coletados, como essa coleta foi realizada e onde estão armazenados (MUNDIE, 2014).

Em resumo, por vezes, geramos e transmitimos dados a organizações de forma consciente e voluntária; no entanto, também estamos constantemente transmitindo dados involuntariamente, dados que são muitas vezes gerados e coletados sem nosso conhecimento ou consentimento.

A escala dessa coleta e armazenamento é outra novidade tornada possível por avanços tecnológicos. No passado, a coleta e o armazenamento de uma grande quantidade de dados eram empreitadas trabalhosas e extremamente custosas, de forma que apenas indivíduos que

[6] O IP, ou *Internet* Protocol (Protocolo de Internet, tradução nossa) é uma sequência numérica que identifica univocamente um usuário de internet entre os demais conectados à rede mundial (PISA, 2012).

possuíam uma posição merecedora de atenção específica corriam o risco de ter suas informações coletadas e armazenadas para o uso por organizações. Os avanços tecnológicos recentes tornaram essas práticas simples e baratas, alterando sua relação custo-benefício ao ponto de que quase todo o mundo apresente potencial suficiente para justificar a coleta e armazenamento de seus dados por organizações (GOLDFARB; TUCKER, 2012).

O aumento da capacidade de armazenamento e a diminuição do seu custo fizeram da criação e do armazenamento por um longo período de tempo de *databases* (ou "bases de dados", em português) uma prática comum dentro de organizações. Estas *databases* contêm diferentes tipos de informação, a depender da organização que as coletou. No entanto, através do acesso a mais de uma *database* contendo uma variedade de informações, um indivíduo ou organização pode fazer uso daquilo que os estudiosos decidiram chamar de *data overlapping* (literalmente "sobreposição de dados"), que consiste na associação de dados que, isolados, podem não ser particularmente reveladores, mas que, uma vez associados, podem expor algo sobre um indivíduo. Por exemplo, a compra de ingredientes comuns para a culinária de uma etnia específica pode não significar nada individualmente, mas seria particularmente reveladora se correlacionada com um endereço em uma região onde existe uma maior presença de membros daquela etnia em particular. O potencial revelador de *databases* aumenta exponencialmente caso estas sejam mantidas por um longo período de tempo (HEFFETZ; LIGETT, 2014).

Se no passado essas correlações exigiam grandes recursos financeiros e humanos, atualmente ela é feita por computadores, graças à grande capacidade de processamento dos mesmos. A isso damos o nome de *data mining* (literalmente a "mineração de dados"). O *data mining* é um conjunto de técnicas utilizadas para extrair de grandes bases de dados fragmentos de informação ocultos ou despercebidos, revelando assim padrões e correlações entre os dados e gerando informações "novas", que podem ser utilizadas na tomada de decisões (FROOMKIN, 2000). Um algoritmo faz o papel de investigador, analisando uma grande quantidade de dados aparentemente não relacionados e extraindo desses dados informações relevantes a uma situação ou organização em particular.

O *data mining* é um recurso valioso para organizações e seu uso é um verdadeiro avanço no processamento de dados, gerando descobertas que seriam impossíveis antes do surgimento dessa tecnologia. Por exemplo, em 2011, pesquisadores da empresa farmacêutica Kaiser Permanente analisaram o histórico médico de 3.2 milhões de indivíduos e descobriram uma correlação entre o uso de medicamentos antidepressivos por mulheres grávidas e distúrbios neurológicos relacionados ao autismo, concluindo que o uso de antidepressivos

durante a gravidez dobra as chances de uma criança nascer com o distúrbio. Essa descoberta certamente é benéfica para a sociedade e não teria sido possível sem a coleta e o armazenamento de uma grande quantidade de dados, ou o *data mining* (MUNDIE, 2014).

O exemplo acima é de vital importância antes que continuemos esse capítulo para que possamos entender o dilema que enfrentamos. Embora os avanços de algumas tecnologias específicas apresentem obstáculos para o gerenciamento da privacidade dos indivíduos, isso não significa que tais inovações não sejam em si bens valiosos, ou que representem a totalidade do problema. Como explicado anteriormente, a busca de organizações por novas formas de coletar e armazenar informações sobre indivíduos não é uma nova prática trazida à tona pelo avanço tecnológico. Dessa forma, nosso desafio não consiste em suprimir os avanços tecnológicos para proteger a privacidade dos indivíduos, e sim em criar formas de gerenciar a privacidade, dados os avanços tecnológicos.

Uma vez que descrevemos alguns dos mecanismos utilizados para coletar, armazenar e analisar dados de indivíduos, devemos estabelecer que tipos de organizações realizam a coleta, armazenamento e análise, e com que propósito. Estas se dividem essencialmente em duas categorias: organizações públicas/governamentais, e organizações privadas/empresas.

2.1. Coleta, Armazenamento e Processamento de Dados por Governos

Quando pensamos em grandes coletores de dados pessoais, governos são frequentemente os atores que nos vêm à mente. Essa associação não ocorre por acaso – agências governamentais possuem de fato uma diversidade de aparatos de coleta e processamento de dados. Esses atores governamentais buscam utilizar esses instrumentos de forma a discriminar, entre os cidadãos, aqueles que requerem formas diferenciadas de tratamento oficial (RULE, 2007).

Governos foram os pioneiros na coleta e processamento de dados de seus cidadãos. A consolidação do Estado como o guardião da lei, essencial para a construção do Estado nacional no século XVI, exigiu a implementação de um aparato administrativo que possuísse a capacidade de "individualizar os indivíduos", de forma a garantir a coleta de impostos, a aplicação da lei etc. Por essa razão, grande parte da interação entre cidadãos e seus governos ocorre através do registro dos cidadãos dentro de uma diversidade de bases de dados mantidas por esses governos. Carteiras de identidade e motorista, censos, declarações de imposto de renda, registros de veículos, registros para eleições, passaportes, previdência social – essas são apenas algumas das informações que provemos a nossos governos de forma a oficializar

nossa participação efetiva em sociedade e dar às agências governamentais a capacidade de nos individualizar em meio a outros cidadãos quando necessário (ANDRADE, 2011).

Para o governo interessa coletar, armazenar e manter tais dados por um longo tempo, em geral para garantir a aplicação da lei. Entende-se que cidadãos nem sempre cumprirão a lei voluntariamente – manter dados sobre esses cidadãos e sobrepor tais dados (o que chamamos acima de *data overlapping*) é uma forma de garantir esse cumprimento, discriminando aqueles que, por exemplo, não pagaram os devidos impostos ou receberam benefícios indevidos (CLARKE, 1994). Um exemplo da utilização do *data overlapping* pelo governo no Brasil é a obrigatoriedade de inquilinos declararem suas despesas com aluguel em sua declaração anual de imposto de renda. Embora as despesas com aluguel não sejam dedutíveis para o inquilino, sua declaração é uma forma de o governo assegurar que o proprietário/locatário do imóvel em questão pagará o imposto devido sobre a renda obtida através do aluguel de seu imóvel, mesmo que este falhe em declarar tal renda.

O exemplo acima é útil para que compreendamos que a coleta, armazenamento e processamento de dados pelo governo não é necessariamente realizada por razões nefastas. A maioria dos cidadãos cede as informações exemplificadas acima voluntariamente, mesmo que a contragosto, e confia que estas serão utilizadas para razões legítimas e de boa governança.

Isso não quer dizer que governos não realizem coletas de dados não autorizadas ou percebidas por seus cidadãos. Em um procedimento similar em boa parte do mundo ocidental, agências policiais podem, para garantir a manutenção da lei e ordem, obter mandados judiciais que dão a elas o direito de recolher informações que estão normalmente fora do alcance do governo sobre pessoas de interesse para investigação. Tais informações podem ser recolhidas através da intercepção de vários fragmentos de informação, geralmente fora do escopo governamental, como o monitoramento de ligações telefônicas ou transações bancárias. Como especificado acima, no entanto, tais interceptações em geral exigem um mandado judicial e são direcionadas a alguns determinados indivíduos, de interesse particular para a investigação em questão (GELLMAN R., 1997).

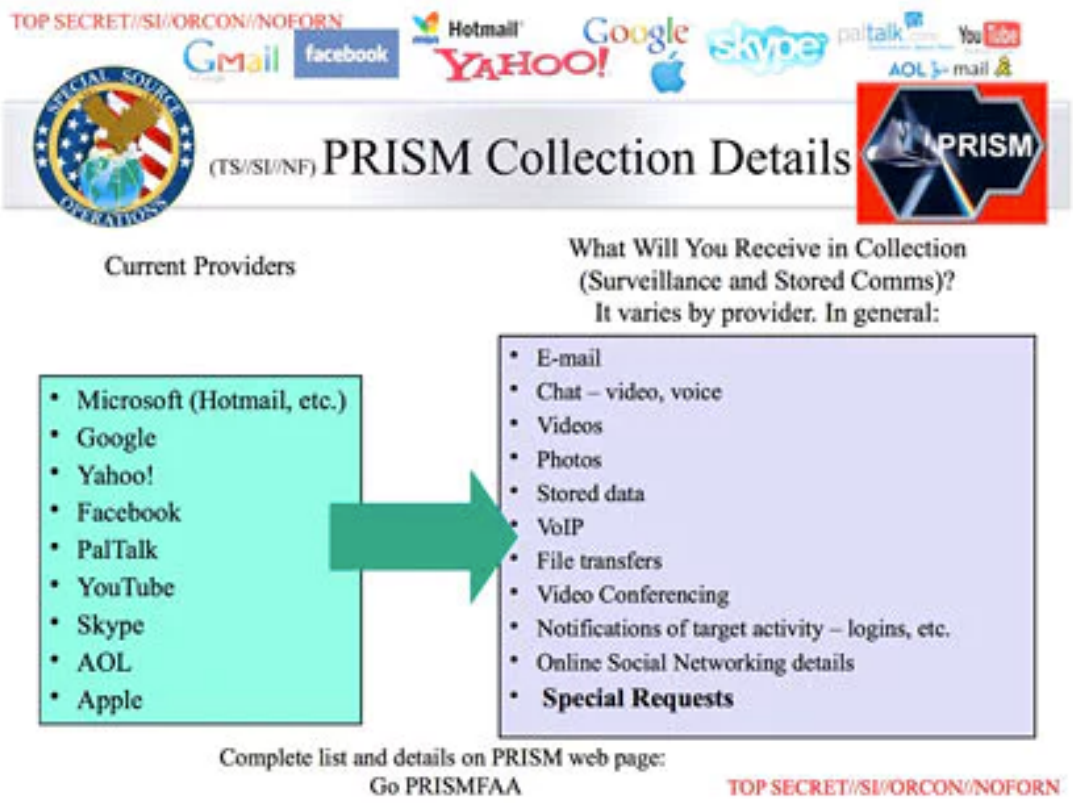
A associação de governos à imagem de vigilância em massa e omnipresença se deve, principalmente, aos métodos utilizados por diversos governos para combater a ameaça do terrorismo, que se tornaram particularmente evidentes depois dos ataques de 11 de setembro de 2001, em Nova Iorque. O caráter não-estatal e descentralizado de organizações terroristas fez com que Estados buscassem um novo método de gerenciamento dos riscos relacionados à segurança nacional, envolvendo especialmente o monitoramento preventivo de comportamentos ou ações que pudessem indicar que um indivíduo representaria uma ameaça

(AMOORE; DE GOEDE, 2005). Tal monitoramento preventivo ocorre principalmente através da criação de perfis pessoais, de forma a prever atividades perigosas ou antissociais antes que as mesmas ocorram. Caso a análise de dados identifique que um indivíduo se encaixa no perfil definido, ele pode estar sujeito a vigilância adicional, buscas e apreensões e/ou formas diferenciadas de tratamento oficial. Um bom exemplo de tratamento oficial diferenciado é a No-Fly List (Lista de Não-Voo), mantida pelo governo dos Estados Unidos, que lista indivíduos que apresentam uma chance maior que a média de tomarem parte em atividades terroristas (FROMKIN, 2000).

É importante ressaltar que esse monitoramento preventivo frente à ameaça do terrorismo não está de forma alguma restrito aos Estados Unidos ou a países europeus. Por exemplo, na preparação para os Jogos Olímpicos e Paralímpicos de 2016 no Rio de Janeiro, o governo brasileiro deflagrou a Operação Hashtag, conduzida pela Polícia Federal, que prendeu 10 suspeitos de planejar ações terroristas. Os suspeitos foram identificados através do rastreamento de redes sociais e dos aplicativos Whatsapp e Telegram (ROSSI; ALESSI, 2016).

Foi dentro desse contexto de monitoramento governamental que surgiu o escândalo relacionado à Agência Nacional de Segurança dos EUA (*National Security Agency*, ou NSA, que será a sigla adotada ao longo deste trabalho). Em 2013, Edward Snowden, um analista de infraestrutura da NSA, acessou documentos sigilosos que delineavam o funcionamento da agência, e utilizou tais documentos para denunciar ao mundo a existência do programa PRISM, em que a agência estava coletando quantidades imensas de dados de ligações telefônicas e correspondências por e-mail, oriundas tanto da população residente dos EUA quanto de populações estrangeiras. Embora a legalidade dessa coleta de dados esteja garantida pelo *Patriot Act* (sobre o qual falaremos no Capítulo 3) e a NSA afirme que os dados não podem ser acessados sem um mandado judicial, a revelação não deixou de chocar populações ao redor do mundo, que passaram a questionar quais informações sobre si estão ao alcance de seus governos (WITTE, 2014).

Figura 1: Slide sobre o funcionamento do programa PRISM



Fonte: (GREENWALD, MACASKILL, 2013)

A imagem acima é um slide obtido pelo The Guardian, que é parte de uma apresentação de PowerPoint elaborada pela própria NSA, contendo mais de 40 slides sobre o funcionamento da agência. A apresentação foi classificada pela agência como "Ultra Secreta" e "NOFORN", que significa que não deve ser disponibilizada para nações estrangeiras parceiras. O slide evidenciado acima explica especificamente o funcionamento do programa PRISM e a transmissão de dados para o *database* da NSA.

A Figura 1 é de particular importância devido às organizações listadas à sua esquerda. Como podemos ver, o NSA não realiza a coleta de informações diretamente na fonte – isto é, os próprios indivíduos. Os dados em questão são fornecidos ao NSA por uma diversidade de organizações, todas elas empresas privadas. Isso nos leva ao nosso próximo item, que discute a atuação de empresas privadas como as maiores coletoras de dados da modernidade (MUNDIE, 2014).

2.2. Coleta, Armazenamento e Processamento de Dados por Empresas Privadas

Uma pesquisa realizada pela Comissão Federal de Comércio (*Federal Trade Commission*, FTC, em inglês) nos EUA revelou que 99% das companhias online coletam informações pessoais dos indivíduos que visitam seus *websites* (TAYLOR, 2004). No setor privado, a coleta, armazenamento e processamento de dados de indivíduos ocorre por uma razão principal: a maximização do lucro (RULE, 2007).

Esse lucro se dá de diversas formas. Primeiramente, empresas podem utilizar os dados coletados passivamente online – como sites visitados, pesquisas realizadas anteriormente, a ordem de cliques e janelas realizados pelo usuário – para melhorar suas operações e assim aumentar seus lucros. Por exemplo, o site de comércio online Amazon.com utiliza os dados de seus usuários, como avaliações de produtos, produtos visitados e comprados, para criar um "filtro colaborativo", através do qual o algoritmo do site identifica usuários com preferências similares e sugere produtos comprados pelos mesmos a outros usuários que se encaixam dentro desse "perfil" (ORITO, 2011). Outros sites utilizam as janelas abertas por usuários e pesquisas realizadas para determinar que tipo de informações são levadas em consideração antes que a compra de um bem ou serviço seja realizada, e assim garantir que as informações mais relevantes para os clientes sejam divulgadas com maior destaque (BANKS; SAID, 2006).

A coleta, armazenamento e processamento de dados online também permite que empresas detectem demandas correntes e preferências gerais de consumidores. Por exemplo, já foi mostrado que o processamento de dados relativos a pesquisas em sites de busca como o Google pode prever tendências relativas a vendas de produtos. Isso permite que empresas se adiantem em relação à demanda latente de consumidores e assim maximizem seus lucros (CHOI; VARIAN, 2012).

Já sites como o Facebook utilizam os dados de indivíduos para customizar seu conteúdo para usuários e assim aumentar o seu apelo. Além das informações inseridas pelos usuários em seus perfis, como gênero, data de nascimento, relacionamentos, cidade de residência etc, o Facebook também tem acesso a conversas privadas, fotos e localizações. O site também possui mecanismos inteligentes para coletar os dados provenientes da socialização de seus usuários. Por exemplo, ao introduzir a ferramenta da "*Timeline*" no perfil de seus usuários, a companhia encoraja usuários a adicionarem informações históricas de sua vida, como cidades e empresas onde viveram e trabalharam anteriormente. Mensagens e fotos estão frequentemente "marcadas" em um local específico, com indivíduos específicos.

Finalmente, o Facebook expandiu seu alcance para fora de suas próprias fronteiras ao inserir o botão "*Like*" (Curtir) em conteúdos externos ao seu site, permitindo que usuários demonstrem seu interesse em uma marca, produto e/ou conteúdo digital (SIMONITE, 2012). Todos esses mecanismos permitem que o Facebook personalize a experiência de seu usuário, oferecendo acesso a conteúdos digitais similares àqueles sobre os quais o usuário já expressou interesse. Acima de tudo, isso permite ao Facebook fornecer publicidade e marketing de forma mais pessoal, em uma escala massiva (BALLVE, 2014).

O foco do Facebook em publicidade online não é uma exceção entre empresas. O mercado de publicidade online é um mercado extremamente lucrativo, para o qual a obtenção, uso e análise de dados de indivíduos é de evidente interesse. Não surpreende, portanto, que empresas de publicidade online tenham se tornado particularmente eficientes nessa área. Muitas dessas empresas possuem relacionamentos e conexões com múltiplos websites, que permitem que essas empresas utilizem instrumentos como *cookies* para monitorar e identificar usuários online, monitorando esses usuários de website em website. Esse relacionamento com empresas de publicidade é tremendamente lucrativo para os donos de websites – Evans (2009) demonstrou que, entre os 100 *websites* mais visitados, a grande maioria lista o montante advindo de publicidade como sua maior fonte de renda. É também extremamente lucrativo para as empresas de publicidade, que, além de espaço para seus anúncios, ganham acesso a uma quantidade imensa de dados de potenciais consumidores. Além disso, a publicidade online possui a capacidade de expor consumidores diferentes a anúncios diferentes, de acordo com suas preferências registradas através de seus dados, detectando assim consumidores mais vulneráveis a certos tipos de produtos. Finalmente, tais empresas podem também medir através dos dados dos usuários a efetividade de seus anúncios e assim realizar ajustes, tornando suas operações ainda mais lucrativas (GOLDFARB; TUCKER, 2012).

O relacionamento entre donos de websites e empresas é revelador justamente por demonstrar que a coleta, armazenamento e processamento de dados podem ser realizados por uma terceira parte, e não necessariamente apenas pelo website visitado. De fato, existem empresas dedicadas exclusivamente ao *data mining*. Empresas como a Mantas e a World Check têm como sua linha de negócio a criação de mecanismos como softwares e algoritmos para empresas de forma a extrair informações de dados coletados pelas mesmas. Por exemplo, a empresa britânica Mantas desenvolveu um software a ser utilizado por instituições financeiras minerar dados de forma a detectar transações suspeitas (AMOORE; DE GOEDE, 2005).

Vimos que informações diferentes podem ser obtidas ao se analisar a mesma *database*, a depender da "peneira" – como algoritmos e *softwares* – utilizada. No exemplo acima, interessa a instituições financeiras detectar transações suspeitas, e, portanto, o software utilizado é específico para essa necessidade. Já a empresas varejistas pode interessar saber o padrão de gastos desses mesmos clientes ao longo do ano, por exemplo. Dessa forma, as *databases* compiladas por uma empresa podem interessar – e muito – a outras empresas. Assim, entramos na parte mais controversa do uso de dados de consumidores pelas empresas: a venda e/ou o uso de suas *databases* por terceiras partes.

Para empresas, a venda de suas *databases* para outras organizações pode ser uma fonte de lucro. Existem exceções, é claro; algumas empresas, como o Wal-Mart, escolheram não comercializar suas *databases*, de forma a manter sua vantagem competitiva (sobre esta decisão, um porta-voz do Wal-Mart afirmou: "Nossos competidores estavam colhendo mais frutos dessas agregações de terceiras partes do que nós, então fazia sentido que parássemos", tradução nossa). Exceções à parte, empresas privadas estão comprando e vendendo dados sobre consumidores em múltiplas formas, volumes e detalhamento (RENDLEMAN, 2001).

A venda dessas bases de dados pode ser realizada tanto para outras empresas diretamente envolvidas no mercado quanto para empresas cujo único propósito é processar esses dados (para então revender suas conclusões para outras empresas). De qualquer forma, a venda de dados como *commodities* é um negócio extremamente lucrativo; quando o site de vendas online *Toysmart.com* faliu em junho de 2000, seus credores consideraram as informações que a companhia possuía sobre clientes como um de seus ativos mais valiosos (TAYLOR, 2004).

Não precisamos ir longe para encontrar vestígios dessas práticas. O Aviso de Privacidade (*Privacy Notice*) do site Amazon afirma que "Enquanto continuamos a desenvolver nosso negócio, podemos vender ou comprar lojas, filiais ou unidades de negócio. Em transações desse tipo, informações de clientes são geralmente um dos ativos comerciais transferidos" (AMAZON, 20[--], tradução nossa). Na seção intitulada "Privacidade" do *website* da empresa, uma mensagem assinada pelo CEO da Apple, Tim Cook, afirma:

> Há alguns anos, usuários de serviços na internet perceberam que, quando um serviço online é gratuito, você não é o cliente. Você é o produto. Mas, na Apple, acreditamos que uma excelente experiência como consumidor não deve vir às custas de sua privacidade (APPLE, 20[--], tradução nossa).

A mensagem pessoal de Tim Cook seria muito tranquilizadora, não fosse o fato de que uma rápida leitura da Política de Privacidade de Apple revela que "ocasionalmente, a Apple pode disponibilizar informações pessoais para parceiros estratégicos". Mais à frente, a mesma

Política de Privacidade identifica alguns desses parceiros estratégicos, que a Apple aponta como "empresas que fornecem serviços", como: "processamento de informações", "concessão de crédito", "gerenciamento e aprimoramento de dados de cliente" e "avaliação de seu interesse em nossos serviços e produtos" (APPLE, 2016, tradução nossa), entre outros.

Já o Facebook, cuja vasta quantidade e variedade de dados coletados listamos anteriormente, especifica em sua Política de Privacidade que pode compartilhar os dados de seus usuários com "apps, websites e partes terceiras integradas ou utilizando nossos serviços", "companhias dentro do Facebook" (como o Instagram e o Whatsapp), além de "serviços de publicidade, avaliação e de análise" e "fornecedores, provedores de serviço e outros parceiros" (FACEBOOK, 2016, tradução nossa). Caso a empresa ou parte dela seja vendida ou o controle sobre a mesma seja transferido, os dados de seus usuários serão parte da transferência. O Google não é tão específico, afirmando simplesmente que pode enviar as informações para "processamento externo" por "afiliados ou outras companhias ou pessoas de confiança" (GOOGLE, 2016, tradução nossa).

O Facebook, o Google, a Amazon e a Apple são apenas alguns exemplos da prática do comércio entre empresas dos dados de indivíduos como um produto. Se a coleta passiva de dados preocupa devido ao fato de que o indivíduo não sabe que informações sobre si estão sendo coletadas, a compra e venda desses dados preocupa ainda mais, pois impossibilita que tenhamos ao menos uma idéia de para onde e para quem esses dados estão sendo transferidos.

Se a prática de compra, venda e transferência de dados de indivíduos entre empresas é tão comum, devemos nos perguntar: governos podem ser uma dessas "partes terceiras" a quem dados são transmitidos, vendidos ou compartilhados?

2.3. Entidades privadas e governamentais: uma parceria

Embora governos sejam, tecnicamente, "partes terceiras" em relação a empresas, estas apresentam geralmente uma forma diferenciada de compartilhamento de dados com governos, em geral mais baseada em casos *ad hoc*. A forma de cooperação entre empresas e governos pode variar. Por exemplo, após a revelação em 2010 de que o Facebook fornecia informações sobre seus usuários com base em "pedidos informais" de agências governamentais, a empresa ajustou sua Política de Privacidade em relação a pedidos dessa natureza de forma a determinar que tais informações seriam fornecidas apenas através de "pedidos legais", como mandados ou ordens judiciais (WITTE, 2014).

Outras empresas não são tão específicas. O Aviso de Privacidade da Amazon.com afirma que a informação de clientes pode ser compartilhada para a "Proteção da Amazon.com e Outros", especificamente quando o site "acredita que a divulgação das informações pessoais e da conta são apropriadas para o cumprimento da lei" (AMAZON, 2016, tradução nossa). A Apple afirma que pode divulgar informações pessoais de seus usuários a pedido de entidades públicas ou governamentais, dentro ou fora do país de residência do usuário, caso determine que a divulgação dessas informações é necessária ou apropriada para propósitos de "segurança nacional, cumprimento da lei ou outros assuntos de importância pública" (APPLE, 2016, tradução nossa). O Google determina que pode compartilhar os dados de seus usuários para cumprir qualquer "lei, regulamento, processo legal ou pedido governamental vinculante aplicável" (GOOGLE, 2016, tradução nossa).

Embora as circunstâncias para o compartilhamento de dados de indivíduos com agências governamentais sejam listadas nas Políticas/Avisos de Privacidade dessas empresas, falta especificidade sobre como e por que exatamente esse compartilhamento pode ocorrer. Na Figura 1, por exemplo, vimos que o Facebook, Google e Apple foram empresas fornecedoras de dados para o NSA durante o programa PRISM. Mais especificamente, o NSA teve acesso direto aos servidores dessas companhias, cujos mecanismos de criptografia e privacidade foram contornados com o auxílio das próprias empresas (GELLMAN B.; POITRAS, 2013). Como essa decisão foi tomada? As empresas em questão julgaram que os dados de seus clientes eram relevantes para a segurança nacional? Teriam considerado a demanda do NSA por esses dados como um "pedido governamental vinculante aplicável"?

Nem mesmo políticas de privacidade um pouco mais específicas em relação a pedidos governamentais (como a do Facebook, que exige ordens ou mandados judiciais) estão a salvo desta ambiguidade. Em 2013, o jornal *The Guardian* publicou a primeira revelação de Edward Snowden: o NSA, utilizando uma ordem judicial do Tribunal de Vigilância e Inteligência Estrangeira (*Foreign Intelligence Surveillance Court*, FISC, em inglês), exigiu que a gigante de telecomunicações Verizon entregasse todos os metadados[7] das ligações de milhões de norte-americanos. A ordem judicial também proibia a Verizon de revelar ao público a existência da própria ordem judicial e do pedido de informações sobre seus clientes (LYON, 2014).

Cláusulas em Políticas de Privacidade de empresas nos assegurando que os dados de seus usuários serão compartilhados com o governo apenas através de um pedido ou ordem do

[7] Metadados, ou *metadata,* são, literalmente, dados sobre dados. No caso de ligações telefônicas, os "dados sobre dados" podem ser, por exemplo, a informação de onde e quando as ligações foram realizadas (NISO, 2004).

mesmo deixam implícita a idéia preconcebida de que os pedidos do governo serão sempre razoáveis. O que protege os clientes das empresas, que são também cidadãos do governo, caso esta idéia esteja errada?

Em dezembro de 2015 e fevereiro de 2016, o aplicativo Whatsapp foi bloqueado em todo o território nacional brasileiro por determinação judicial, após a empresa ter se recusado a quebrar o sigilo de dados de conversas entre indivíduos de interesse para uma investigação criminal em curso. Em ambas as ocasiões, a empresa conseguiu derrubar o bloqueio através de um mandado de segurança. Posteriormente, em abril de 2016, o Whastapp implementou a criptografia "ponta-a-ponta", que permite que apenas os indivíduos na conversa possam ler as mensagens trocadas e, portanto, torna impossível a divulgação dos dados. Em julho de 2016, a juíza Daniela Barbosa de Souza, da 2ª Vara Criminal da Comarca de Duque de Caxias, suspendeu novamente o serviço, desta vez exigindo a desativação da criptografia do aplicativo para que as mensagens trocadas pelos investigados fossem transmitidas em tempo real para os investigadores. A empresa novamente derrubou a suspensão de seus serviços através de um mandado de segurança (FOLHA DE SÃO PAULO, 2016).

Na situação acima, o Whatsapp se posicionou de forma a proteger os dados de seus usuários e resistiu às demandas do governo. Embora não possamos apontar exatamente o que motivou a empresa a essa decisão, empresas privadas podem resistir a medidas tão abertamente invasivas não por uma proteção ativista do direito à privacidade, e sim por temer a perda de clientes que – com razão – temem o monitoramento pelo governo (HOGAN; SHEPERD, 2015). Isso não significa que não devamos nos perguntar: e se o Whatsapp tivesse tomado a decisão contrária? O único obstáculo entre o governo brasileiro e as conversas de cidadãos, no exemplo acima, foi a tomada de decisão da empresa, sobre a qual não temos controle, e cujo processo desconhecemos.

A parceria entre entidades privadas e governamentais na coleta, armazenamento e processamento de dados pode ser extremamente perversa, pois a distinção entre os dados disponíveis para empresas e para o governo torna-se irrelevante (WITTE, 2014). Como vimos, as empresas utilizam a coleta, armazenamento e processamento de dados em busca de lucros, enquanto os governos utilizam as mesmas técnicas de forma a "individualizar os indivíduos". Devemos nos perguntar o que pode ser feito pelos governos com esse excesso de informações sobre indivíduos à sua disposição. Se estamos sempre produzindo dados sobre nós mesmos, as empresas estão permanentemente coletando esses dados e o governo tem acesso a tudo coletado pelas empresas, estaríamos caminhando para uma era de vigilância em

massa dos cidadãos por parte de corporações e governos, realizada através dos dados de cada indivíduo?

2.4. "*Dataveillance*" e o Panóptico

A vigilância é, segundo Roger Clarke (1988), a investigação ou monitoramento sistemático das ações ou comunicações de uma ou mais pessoas, com propósito primário de coletar informações sobre os indivíduos, suas atividades, ou seus associados. Já a vigilância em massa, segundo o mesmo autor, consiste na vigilância de grupos de pessoas, em geral de maior tamanho, de forma a identificar indivíduos que pertençam a uma classe específica de interesse à organização realizadora da vigilância. A vigilância em massa, para Clarke, seria a forma mais perigosa da prática, justamente por ser arbitrária e atingir todos os indivíduos indiscriminadamente.

Foi esse mesmo autor que, em 1988, apresentou a idéia de que seria possível vigiar indivíduos apenas através de seus dados, sem a necessidade de vigilância física. A isso Clarke deu o nome de *dataveillance*, uma combinação das palavras *data* (dados) e *surveillance* (vigilância). É claro que a tecnologia da época era diferente; em seu trabalho "*Information Technology and Dataveillance*" (1988), ou "Tecnologia de Informação e *Davaveillance*" (tradução nossa) Clarke temia que agências governamentais compartilhassem todos os seus arquivos sobre indivíduos e formassem uma grande base de dados. Embora computadores já representassem um grande avanço em relação às formas de coletar e armazenar dados anteriores a esse tipo de tecnologia, os recursos e a altíssima capacidade de processamento que hoje caracterizam o *data mining* ainda não existiam.

Alguns anos depois, em 1994, o autor explorou novamente o conceito de *mass dataveillance* (*dataveillance* em massa, tradução nossa), dessa vez já em relação a tecnologias mais avançadas sendo utilizadas por entidades governamentais e privadas para a coleta, porém ainda com o foco no uso das informações obtidas pelo governo. Para Clarke, o mundo caminhava para que cada indivíduo tivesse também uma espécie de "pessoa digital", esta sendo facilmente vigiada pelo governo através simplesmente dos dados produzidos no dia-a-dia (CLARKE, 1994).

A tecnologia evoluiu rapidamente desde os anos 90, porém os conceitos principais do trabalho de Clarke ainda são relevantes. O indivíduo é, atualmente, uma "pessoa digital", nada mais que uma coleção de dados armazenados dentro de uma base de dados, pronta para ser processada para a extração de informações sobre si (ORITO, 2011).

Através da parceria entre entidades privadas, grandes coletoras de dados, e o governo, é hoje plenamente possível que uma abundância de informações sobre qualquer indivíduo – seus interesses, seus associados, seus hábitos diários – esteja disponível através de alguns cliques. Existem, é claro, aqueles que afirmam que a coleta, armazenamento e processamento de dados não significam que alguém esteja necessariamente nos vigiando continuamente. Isso é certamente verdade; na maior parte do tempo, empresas e governos estão utilizando algoritmos e softwares de forma a atingir comportamentos organizacionais mais efetivos, e não para vigiar indivíduos ou grupos específicos (STEIN, 2011).

Isso não significa, no entanto, que um indivíduo de carne e osso não poderia descobrir tudo sobre um indivíduo ou grupo particular se assim o desejasse. Uma vez que deixamos de controlar que dados sobre nós são coletados, onde estão armazenados, para que propósito estão sendo processados e por quem serão utilizados, abrimos a porta para que governos possam abusar da informação que têm sobre nós (WITTE, 2014). A *dataveillance* é utilizada hoje para identificar e monitorar indivíduos mais propensos a atividades criminosas como o terrorismo. No entanto, o que ocorreria caso um governo em particular decidisse que comunistas apresentam uma ameaça ao Estado, e, portanto, devem ser identificados, monitorados e passíveis de ação oficial diferenciada? É essa codificação e predeterminação de identidades que preocupa ativistas pela privacidade, além de organizações pela liberdade da sociedade civil e direitos humanos (AMOORE; DE GOEDE, 2005).

Não precisamos nos ater a exemplos abstratos ou hipotéticos. No dia 21 de Janeiro de 2014, ucranianos localizados nas proximidades da Praça de Independência de Kiev, palco principal de uma série de protestos contra o governo, receberam a seguinte mensagem em seus celulares: “Caro assinante, você foi registrado como um participante de um tumulto em massa” (tradução nossa). O governo ucraniano utilizou a tecnologia de localização de celulares, discutida anteriormente, para identificar celulares em uso nas proximidades de conflitos entre manifestantes e a polícia de choque. No mesmo dia, entrou em vigor uma lei que permitia sentenças de prisão de até 15 anos para participantes de tumultos em massa (WALKER; GRYTSENKO, 2014).

O exemplo acima é assustador por si só, mas se torna ainda mais preocupante devido ao fato de que a tecnologia para que a situação descrita ocorresse não está restrita à Ucrânia e a seu governo. Devido à tecnologia e práticas discutidas ao longo desse capítulo, a situação acima poderia ter ocorrido na maior parte do mundo, em diferentes sociedades e por diferentes razões. A vigilância em massa pode ser um elemento de uma democracia direta

racional-legal, mas também pode ser um elemento crucial para uma governança tirânica (CLARKE, 1994).

Existem autores que afirmariam que a repressão direta e violenta por parte do governo não é necessariamente a única forma de suprimir o comportamento de indivíduos. Em 1791, o legislador inglês Jeremy Bentham publicou uma proposta para um novo modelo de prisão, a que ele deu o nome de Panóptico. No Panóptico, uma estrutura complexa de celas e uma torre central possibilitaria a vigilância de todos os prisioneiros durante todo o tempo. A torre central seria visível para todos os prisioneiros, para que os mesmos soubessem que estão sendo vigiados continuamente. Não haveria espaço privado, ou momento algum em que indivíduos não estivessem sendo observados e escrutinizados. Para Bentham, a ausência de um espaço privado e a vigilância permanente funcionariam como um mecanismo de supressão de comportamentos negativos, pois os prisioneiros se comportariam bem, simplesmente por saberem estar sendo observados. Isso permitiria a uma única pessoa (na situação descrita por Bentham, o diretor da prisão) controlar um grande número de indivíduos, sem a necessidade do uso de força ou de grandes contingentes (STRUB, 1989).

O Panóptico de Bentham foi expandido por Michel Foucault em sua obra "Vigiar e Punir" (1975). Nesta obra, Foucault explora o relacionamento entre poder e conhecimento; o autor afirma que, na era moderna, o poder de punir parte da classificação e supervisão de indivíduos, com base no conhecimento que possuímos sobre a natureza e comportamento humanos. Existiria, então, um relacionamento simbiótico entre o conhecimento e o poder de punir. O poder de punir existe através do conhecimento que torna possível a classificação de indivíduos de acordo com uma norma pré-determinada, e esse conhecimento é extraído através de relações de poder e dominação (FOUCAULT, 1975).

Para Foucault, o Panóptico de Bentham é uma ilustração perfeita da forma pela qual a disciplina e a punição funcionam na sociedade moderna. Ao abolir o espaço privado e estabelecer mecanismos de poder que operam de forma invisível, formar-se-ia uma sociedade disciplinadora que garantiria, de forma econômica, a docilidade de seus elementos. O maior efeito do Panóptico, segundo o autor, seria impor ao prisioneiro um estado de vigilância permanente e consciente, de forma a garantir o "funcionamento automático do poder". Isso criaria mecanismos auto-sustentáveis para a manutenção da relação de poder entre o vigilante e o vigiado, impondo uma situação de poder aos prisioneiros em que eles mesmos são os guardiões da estrutura de poder vigente. Em outras palavras, os vigiados seriam os próprios vigilantes (FOUCAULT, 1975).

Autores como David Lyon (1993) argumentam que o Panóptico é uma metáfora atraente para a descrever o *dataveillance*, justamente pela idéia de que os dados coletados, armazenados e processados em diversas esferas sociais do indivíduo podem culminar em um estado de vigilância perpétua. Estudos modernos sugerem que, de fato, indivíduos se comportam de forma diferenciada quando sabem que estão sendo observados, em uma forma de conformidade antecipada (ZUBOFF, 1988). Sendo assim, o simples fato de indivíduos saberem que estão sendo observados através de seus dados já pode ser o suficiente para gerar uma espécie de "auto-censura" de comportamentos e idéias.

Os instrumentos de coleta, armazenamento e processamento de dados podem, portanto, representar instrumentos de poder punitivo de caráter repressor, através de sua capacidade de "monitorar, registrar e reconhecer" indivíduos (GUNDALINI; TOMIZAWA, 2013, p. 31). Em outras palavras:

> Nesta nova sociedade, a monitoração eletrônica pode ser reconhecida como um desenvolvimento tecnológico da antiga vigilância hierárquica, mas o poder punitivo não mais se manifesta por meio de uma sanção normalizadora, mas por um intricado sistema de registro e reconhecimento. Não mais é função social transformar o "anormal" em "normal" nas instituições disciplinares, mas registrar e reconhecer o "anormal" para filtrá-los da sociedade dos "normais" (VIANNA, 2007, p.83, apud GUNDALINI; TOMIZAWA, 2013, p. 31).

Existe, no entanto, uma diferença: enquanto a metáfora dos prisioneiros de Bentham e Foucault infere um grau de participação involuntária dos vigiados (são, afinal, prisioneiros), o uso feito por indivíduos de tecnologias e serviços *online* atualmente possui uma certa dose de voluntariedade. De fato, é impossível que uma pessoa saiba exatamente como, onde, quando e por quem seus dados estão sendo coletados. No entanto, frequentemente fazemos uso de tecnologias cuja natureza é inerentemente invasiva a nossa privacidade, e o fazemos voluntariamente por uma diversidade de razões, como a conveniência que essas tecnologias nos provêm. Por isso, é possível que estejamos, pouco a pouco, construindo um Panóptico participativo (ORITO, 2011).

Ao longo deste capítulo, exploramos os métodos utilizados para coleta, armazenamento e processamento de dados de indivíduos online, estabelecemos sua presença difusa e perene, identificamos o papel de atores privados e governamentais e exploramos o potencial mau uso dos recursos tecnológicos e das relações entre atores institucionais e empresariais envolvidos. Cientes de tudo o que exploramos, é justo que nos perguntemos: dada a invasão sistemática e onipresente da privacidade de indivíduos através dos mecanismos de *dataveillance*, podemos dizer que ainda exista a privacidade?

Alguns autores defendem que a privacidade está, de fato, morta. O rápido avanço de tecnologias do *Big Data*, em contraste com a lentidão da lei em compreender a ameaça dessas tecnologias e regular sua prática, teria dado origem a um conjunto de práticas que há muito se tornaram inerentes e até mesmo essenciais para o funcionamento da sociedade como um todo, ultrapassando e subjugando considerações normativas e nos levando à morte da privacidade (BRIN, 1999). Nas palavras do CEO da Sun Microsystems, Inc., Scott McNealy: "Você já tem zero privacidade. Supere." (BAIG et al, 1999, p. 84 apud FROOMKIN, 2000, p. 1463, tradução nossa). Essa visão pessimista, embora compreensível em vista do que já expusemos nesse capítulo, tem poucos adeptos. Froomkin (2000), por exemplo, condenou a visão fatalista exposta acima. Embora o autor reconheça que não existe uma resposta simples para a questão da privacidade online em face dos diferentes avanços tecnológicos de coleta de dados, Froomkin avaliou que não é tarde demais para que possamos encontrar métodos legislativos ou convencionais para a preservação do direito à privacidade.

Outros autores defendem que a privacidade no meio online se tornou uma escolha. Essa idéia está fortemente associada à noção de auto regulação ou auto-gerenciamento da privacidade, isto é, o princípio de que os próprios indivíduos devem fazer escolhas online que facilitem a proteção de seus dados e informações. O consentimento é um elemento central do princípio de auto-gerenciamento, pois o indivíduo teria a oportunidade de escolher em que situações específicas estaria disposto a abrir mão de elementos de sua privacidade, e em quais situações isso seria inaceitável. Um exemplo de auto-gerenciamento de privacidade seria um indivíduo que, ao ler a Política de Privacidade de um website (como as que mencionamos anteriormente), identifique a mesma como potencialmente invasiva, e assim deixe de usar este website. O outro lado da moeda é a possibilidade de o indivíduo encontrar-se nesta mesma situação e decidir que, em luz dos benefícios obtidos através do uso deste website, ele está disposto a abrir mão de sua privacidade nesta situação específica (NISSENBAUM, 2009).

A idéia da auto-regulação da privacidade possui raízes profundas na privacidade decisional que exploramos no Capítulo 1, cujo foco descansa sobre o controle que os indivíduos têm sobre suas informações. Embora o controle dos indivíduos sobre suas informações seja, de fato, importante, alguns autores apontam deficiências nessa abordagem que podem prejudicar o direito à privacidade como um todo. Primeiramente, a grande maioria dos websites, softwares e outros serviços online atuais já possuem a obrigação de divulgar ao indivíduo que tipo de dados serão coletados, para que serão utilizados e com quem serão compartilhados (vide as Políticas de Privacidade expostas anteriormente neste capítulo). No entanto, estudos mostram que um percentual minúsculo de pessoas lê tais avisos. Entre

aqueles que realizam a leitura, um percentual ainda menor abre mão da utilização dos serviços em questão (BEN-SHAHAR; SCHNEIDER, 2011). Em outras palavras, indivíduos preocupam-se com sua privacidade, porém estão dispostos a negociar parte dela, na maioria dos casos (STEPANOVIC, 2014).

Certamente é válido dizer que os indivíduos, nas situações descritas acima, consentiram a essas invasões específicas a sua privacidade, e, portanto, seu direito não foi "violado" per se. No entanto, isto pode ser um caso daquilo que o economista Alfred Kahn chamou de "a tirania das pequenas decisões", em que pequenas decisões que são individualmente benéficas ou até mesmo insignificantes para uma só pessoa podem ter efeitos coletivos inesperados e perversos para a sociedade como um todo. Vivendo em um mundo em que informação é poder, ao realizarmos escolhas individuais que cedem pequenas porções de nossa privacidade gradualmente em troca de serviços e conveniência do mundo moderno, incentivamos esse mundo a avançar por um caminho que nos leva à vigilância – ou *dataveillance* – total (RULE, 2007). Além disso, outros autores apontam que mesmo consumidores bem informados tendem a tomar decisões enviesadas em relação à própria privacidade, por não conseguirem avaliar adequadamente os efeitos das pequenas cessões que realizam (SOLOVE, 2013). Um indivíduo pode se sentir confortável em compartilhar sua localização através de softwares presentes em seu celular por julgar que a conveniência do uso do aplicativo Google Maps compensa a coleta do que ele percebe como um dado largamente irrelevante. Mas será que esse indivíduo sentiria esse mesmo nível de conforto com sua decisão ao receber uma mensagem de texto como a enviada pelo governo ucraniano para os participantes de protestos em Kiev?

Muitos consideram falho o princípio de auto-gerenciamento pelas razões supracitadas. Autores como Solove (2013) e Joyce (2015) defendem que o consentimento é apenas uma porção da garantia ao direito à privacidade dos indivíduos. Governos, segundo esses autores, devem legislar tendo em mente a nova paisagem digital em que o direito à privacidade existe, e legislar de forma que indivíduos estejam cientes de quando e por quem seus dados estão sendo coletados. Mesmo com o consentimento desses indivíduos para a coleta de seus dados, o governo deve intervir principalmente no que tange o *uso* desses dados coletados – como e para que eles serão processados, com quem e com que objetivo serão compartilhados.

Existe, portanto, a necessidade de legislar o direito natural do indivíduo à privacidade também como um direito digital. Enquanto alguns defendem a criação de legislação internacional relativa ao direito digital à privacidade (JOYCE, 2015), outros se perguntam: como se pareceria essa legislação, e qual seria sua abordagem?

Nesse aspecto, podemos identificar duas abordagens proeminentes distintas no mundo ocidental: enquanto a legislação de privacidade digital existente na União Européia possui caráter altamente paternalista, em suas exigências relativas tanto ao consentimento do indivíduo quanto à base legal para o processamento de dados, a jurisprudência dos Estados Unidos é muito mais flexível, permitindo o processamento de dados, a não ser que uma lei proíba especificamente a prática (SOLOVE, 2013). Devemos analisar, portanto, quais são os méritos e deficiências dessas abordagens, e quais lições podemos aprender de cada uma delas na proteção do direito à privacidade dentro do ecossistema digital. Esse é o objetivo que esperamos atingir no próximo capítulo.

3. A CODIFICAÇÃO DA PRIVACIDADE ONLINE

Os desafios para se codificar a privacidade online dentro de um corpo legislativo são vários. Enfrenta-se, primeiramente, a falta de consenso sobre o que exatamente seja a privacidade, assunto que exploramos no capítulo 1. Além disso, legislar sobre a privacidade online é uma luta contra o tempo; como exploramos no capítulo 2, os instrumentos tecnológicos para a coleta e o uso de dados estão em avanço constante e rápido, explorando cada vez mais espaços até então desconhecidos dentro da vida online de um usuário.

Em Dezembro de 2013, a Organização das Nações Unidas adotou a Resolução 68/167, que expressa preocupação sobre os impactos que a vigilância e interceptação de dados online podem ter sobre os direitos humanos. A Assembleia Geral da ONU determinou que os direitos humanos "off-line" devem também ser protegidos "online", e clamou para que os Estados revisem seus procedimentos, práticas e legislações relativas à vigilância de comunicações e à interceptação e coleta de dados pessoais, visando respeitar e proteger o direito à privacidade na era digital (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2016).

Sendo assim, este capítulo tem como objetivo explorar duas abordagens diferentes ao desafio supracitado. As manifestações da Organização das Nações Unidades relativas ao assunto, embora não possuam caráter vinculante, serão apresentadas, justamente por conterem recomendações para os países sobre como melhor preservar o direito humano à privacidade em face das novas tecnologias online. Em seguida, iremos explorar o corpo legislativo dos Estados Unidos e da União Europeia. Como mencionado anteriormente, o bloco europeu e os norte-americanos possuem abordagens legais distintas em relação ao assunto. Ao apresentar e comparar ambas abordagens, esse trabalho irá buscar méritos e deficiências presentes em cada uma delas, explorando a existência de possíveis soluções normativas ótimas para a questão apresentada.

3.1. A codificação da privacidade online nos Estados Unidos da América (EUA)

Diferentemente de outras nações, os Estados Unidos não possuem uma legislação abrangente para proteger os dados de cidadãos e consumidores. Embora existam diversos estatutos federais relativos ao assunto, estes tendem a legislar setores ou contextos específicos (SOLOVE; HOOFNAGLE, 2006). Como veremos abaixo, a privacidade de dados nos EUA é regulada através de uma série de leis setoriais e estatais. Além disso, existem diversas

diretrizes industriais que, embora constituam a formalização de "melhores práticas", não possuem força legal.

Dada a estrutura governamental dos Estados Unidos, cada estado da Federação possui autonomia para legislar sobre o assunto. No entanto, este trabalho abordará tão somente a legislação federal dos Estados Unidos, por uma questão de praticidade e por considerar que a natureza abrangente de leis federais torna-as mais adequadas para a avaliação de instrumentos legais de controle sobre mecanismos tão difusos quanto aqueles de coleta, armazenamento e processamento de dados, apresentados no Capítulo anterior.

No nível mais alto da lei, a Quarta Emenda à Constituição dos Estados Unidos determina:

> O direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas. (UNIVERSIDADE DE SÃO PAULO, [20-])

A Constituição dos Estados Unidos, promulgada em 1788, é, obviamente, anterior a muitas das tecnologias atuais; no entanto, permanece como autoridade legal maior no país, e sua aplicação nos tempos atuais tem como base a interpretação dos tribunais nos Estados Unidos.

A Suprema Corte de Justiça dos Estados Unidos não exarou decisões ligadas diretamente à privacidade de dados. No entanto, já fez considerações nesse sentido. Em *City of Ontario, California, et al* v. *Quon et al* a Corte Suprema *presumiu,* por uma questão de argumentação (*arguendo*)[8], que indivíduos possuem uma expectativa razoável de privacidade relativa a comunicações armazenadas (ESTADOS UNIDOS, 2010a). Apesar disso, existem decisões pela Suprema Corte que criam lacunas na interpretação da privacidade do indivíduo relativa a seus dados online. Em *Smith v. Maryland*, em 1979, a Suprema Corte determinou que a proteção da Quarta Emenda não se aplica a uma situação em que um indivíduo entrega seus dados voluntariamente para uma terceira parte, como uma companhia, pois tal entrega voluntária elimina a expectativa razoável de privacidade (ESTADOS UNIDOS, 1979).

O precedente estabelecido pela decisão da Suprema Corte em *Smith v. Maryland* tem sido utilizado por tribunais de instâncias inferiores em suas decisões relativas à privacidade de dados. Por exemplo, em 2016, a Corte de Recursos dos Estados Unidos para o Quarto

[8] De acordo com a decisão citada acima, sobre City of Ontario, California, et al v. Quon et al, a Corte Suprema dos Estados Unidos afirmou-se indisposta a tomar uma decisão sobre a privacidade de comunicações eletrônicas em face das vastas consequências de tal decisão; sendo assim, apenas presumiu a expectativa razoável de privacidade em comunicações armazenadas por uma questão de argumentação, porém não tomou uma decisão sobre o assunto (ESTADOS UNIDOS, 2010a).

Circuito determinou em *United States of America v. Graham* que a Quarta Emenda não protege dados de localização de celulares ou registros sobre onde celulares foram utilizados, pois indivíduos compartilham esses dados voluntariamente com suas provedoras de serviço, como parte de seu contrato (ESTADOS UNIDOS, 2016a). Isso significa que forças policiais, por exemplo, podem exigir essa informação de companhias de celulares sem a necessidade de um mandado. Anteriormente, as Cortes de Recursos dos Estados Unidos para o Quinto, Sexto e Décimo-Primeiro Circuitos haviam chegado à mesma conclusão (MCLAUGHIN, 2016). Como a Suprema Corte dos EUA dificilmente se engaja em questões jurídicas a não ser que exista dissidência entre tribunais de instâncias inferiores, incluindo as Cortes de Recursos, a decisão desapontou ativistas pela privacidade digital que esperavam uma revisão pela Suprema Corte sobre no que consiste a "entrega voluntária" de dados para terceiras partes (GELLER, 2016).

Vemos, portanto, que embora a Quarta Emenda diga respeito à proteção da privacidade dos indivíduos, sua abrangência não se transfere com naturalidade para a questão da privacidade de dados, e por isso devemos explorar outras vias legislativas relativas ao assunto.

Em âmbito federal, existem algumas leis específicas que merecem destaque. O *Privacy Act* de 1974, 5 U.S.C. § 552a, regula a disseminação de dados de indivíduos entre agências governamentais, e "estabelece um código de práticas informacionais justas que governa a coleta, manutenção, uso e disseminação de informações sobre indivíduos mantidas em sistemas de registros por agências federais" (ESTADOS UNIDOS, 2015a, tradução nossa). Esta lei proíbe a disseminação de informações sobre indivíduos por agências federais para qualquer pessoa ou agência, a não ser que esta seja apresentada através de um pedido escrito e que o indivíduo em questão seja notificado e apresente seu consentimento. Existem algumas exceções para a disposição supracitada, que permitem a disseminação de informações para o cumprimento da lei, execução de atividades rotineiras de agências, atividades de contrainteligência, entre outras (ESTADOS UNIDOS, 1974).

Em 1988, o *Privacy Act* foi emendado através do *Computer Matching and Privacy Protection Act,* codificado como parte do *Privacy Act* e adicionando diversas disposições para que os mesmos direitos garantidos ao cidadão na lei de 1974 fossem garantidos caso as agências em questão realizassem comparações computadorizadas entre dois ou mais sistemas de registro automatizados ou entre dois ou mais sistemas de registros federais e não-federais. Essa emenda apresenta exceções às suas disposições similares às da lei original, que incluem comparações feitas para o cumprimento da lei ou para a administração rotineira da agência em

questão, assim como comparações relativas a impostos ou benefícios sociais, ou para produzir dados estatísticos agregados que não contenham identificadores pessoais (ESTADOS UNIDOS, 1988).

Embora as provisões do *Privacy Act* de 1974 e suas emendas sejam válidas, críticos apontam que essa lei é principalmente um exercício burocrático, e não possui papel regulador no controle de informações. A exceção relativa à execução de atividades rotineiras de agências, em particular, tornou-se uma lacuna que legitima praticamente qualquer uso dentro de cada agência e qualquer disseminação para qualquer outra agência. Isso ocorre porque as agências em questão podem declarar que sua operação eficiente, assim como a do governo federal como um todo, é um "uso rotineiro" da informação em questão (BERMAN; GOLDMAN, 1989).

O próprio governo americano reconhece as limitações do *Privacy Act*. No relatório "Visão Geral do *Privacy Act* de 1974" (tradução nossa), publicado em 2015, o Departamento de Justiça dos Estados Unidos afirma que, por limitações como "linguagem imprecisa" e "diretrizes regulatórias relativamente desatualizadas", o *Privacy Act* se tornou "um estatuto de difícil deciframento e aplicação" (ESTADOS UNIDOS, 2015b, p.1, tradução nossa). Já houve tentativas de atualizar o *Privacy Act* para que este se tornasse mais aplicável à tecnologia atual; por exemplo, em 2011 o Senador Daniel Akaka (D-HI) introduziu a proposta de emenda "*Privacy Act Modernization for the Information Age Act of 2011*" (Modernização do *Privacy Act* para a Era da Informação em 2011, tradução nossa), que propunha a redefinição dos termos "sistemas de registros" e "uso rotineiro", além da expansão de requisitos relativos à coleta, manutenção e disseminação de dados entre agências governamentais. Essa emenda, no entanto, jamais foi votada (ESTADOS UNIDOS, 2011).

Em 1968, o governo americano promulgou o *Omnibus Crime Control and Safe Streets Act*, que, em seu Título III, conhecido como *Wiretap Act* (Lei sobre Grampeamento, tradução nossa), proíbe a interceptação, uso e disseminação intencionais de comunicações por cabo. Comunicações por cabo, nesse caso, referem-se a quaisquer transferências fonéticas (contendo a voz humana) realizadas inteira ou parcialmente através do uso de um fio, cabo, ou qualquer outra conexão similar (ESTADOS UNIDOS, 1968). O *Wiretap Act* foi emendado e modernizado em 1986 pela passagem do *Electronic Communications Privacy Act* (ECPA), que, entre outras determinações, estabelece que comunicações eletrônicas estão sujeitas às mesmas restrições citadas anteriormente. A interceptação com o uso de equipamentos de comunicações por cabo (grampeamento) e a interceptação de comunicações eletrônicas (interceptação eletrônica) são permitidas pelo ECPA apenas caso uma das partes na

comunicação tenha dado consentimento à interceptação, caso a interceptação ocorra com a permissão jurídica e sob a supervisão legal de agências policiais ou de inteligência, ou caso a interceptação ocorra como ferramenta para prover ou regular serviços de comunicação (ESTADOS UNIDOS, 1986). Devemos notar que nessas exceções podem ser enquadradas a grande maioria dos processos listados no Capítulo 2 deste trabalho, através dos quais organizações obtêm dados de indivíduos.

O ECPA não regula apenas comunicações em trânsito. Seu Título II, também conhecido como *Stored Communications Act* (Lei de Comunicações Armazenadas), visa proteger a privacidade de comunicações eletrônicas armazenadas com terceiras partes. Embora essa proteção não se aplique a intimações ou mandados criminais, ela se aplica a intimações civis e outros pedidos de divulgação (ESTADOS UNIDOS, 1986). Dessa forma, o SCA pode ser a legislação mais eficiente para prevenir a divulgação do conteúdo de mensagens eletrônicas por empresas como o Google. Em *Crispin v. Christian Audagier Inc*., foi determinado que até mesmo o conteúdo do "mural" do Facebook pode ser considerado como conteúdo protegido de divulgação para terceiras partes (ESTADOS UNIDOS, 2010b).

No entanto, o SCA é limitado em sua capacidade de proteger a privacidade de dados justamente por ter escopo extremamente restrito. Sua proteção se estende apenas a comunicações, que são uma categoria extremamente específica de dados. Isso inclui e-mails, mensagens de texto e até mesmo o "mural" do Facebook, porém não dados como atividades online, janelas abertas, clicks realizados, entre os outros dados que são regularmente coletados, armazenados e processados, que listamos no Capítulo 2 (WITTE, 2014).

O ECPA como um todo teve seu poder regulatório limitado quando foi largamente emendado pelo *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (Lei para Unir e Fortalecer a América ao Fornecer Ferramentas Apropriadas Requeridas para Interceptar e Obstruir o Terrorismo, tradução nossa), também conhecido como *Patriot Act*, promulgado em 2001 como uma resposta aos ataques de 11 de Setembro de 2001 (ESTADOS UNIDOS, 2001). Emendas adicionais foram incluídas no *USA PATRIOT Act Additional Reauthorizing Amendments Act* (Lei de Reautorização e Emendas da Lei para Unir e Fortalecer a América ao Fornecer Ferramentas Apropriadas Requeridas para Interceptar e Obstruir o Terrorismo, tradução nossa) em 2006 (ESTADOS UNIDOS, 2006). O *USA PATRIOT Act* adicionou à lista de exceções do ECPA, citada anteriormente, a determinação de que provedores de serviço possam divulgar comunicações de indivíduos voluntariamente – isto é, sem a necessidade de um mandado judicial – caso acreditem que existe ameaça à vida ou integridade física de outrem.

Além de comunicações, o *USA PATRIOT Act* permite a divulgação voluntária de dados (e não apenas comunicações) sobre clientes caso a ameaça supracitada exista. A seção 216 do *USA PATRIOT Act* é de particular preocupação para os ativistas em prol da privacidade digital, pois regula o uso de equipamentos e processos de "*trap and trace*" (capturar e rastrear, tradução nossa), que são processos ou equipamentos que possam utilizar dados de uma ligação para identificar sua fonte (ESTADOS UNIDOS, 2001).

Ao expandir o tipo de informação que pode ser obtida através das provisões do Wiretap Act e do ECPA, o *USA PATRIOT Act* incentivou a expansão da variedade de informações registradas na Internet, incluindo mensagens e comunicações eletrônicas e navegação na Web. Embora os "impulsos" a que se refere a seção 216 não incluam o conteúdo de mensagens e transmissões, isso ignora a capacidade de extração de informações através da mineração de dados (*data mining*), que explicamos no capítulo 2 (ELECTRONIC PRIVACY INFORMATION CENTER, 20[--]a).

Além da regulamentação das atividades do governo atentatórias à privacidade de dados, os Estados Unidos também possuem organizações governamentais que funcionam como fiscalizadores da privacidade de dados para o setor privado, mesmo que esta não seja sua função primária. A *Federal Trade Commission* (FTC, ou Comissão de Comércio dos EUA, tradução nossa) foi instaurada em 1914 através do *Federal Trade Commission Act*. Sua missão desde o princípio foi coibir a competição desleal e atos/práticas enganosas ou desleais de comércio, declaradas como ilegais sob o FTC *Act*. Estão sob sua jurisdição quaisquer pessoas, empresas ou corporações (exceto instituições bancárias, de poupanças ou empréstimos) que atuem no comércio dentro dos EUA, assim como atos ou práticas envolvendo comércio internacional que possam causar danos previsíveis dentro dos EUA (ESTADOS UNIDOS, 1914).

A Seção 5 do FTC *Act* é dedicada à proteção do consumidor, e define "práticas desleais" como aquelas que podem causar "danos substanciais" a consumidores e das quais os mesmos não podem se defender "de forma razoável" (tradução nossa). A Seção 5 tem sido utilizada pelo FTC como uma abordagem legal à regulação da proteção de dados online (KEARNEY, 2011), ao considerar desleais e enganosas práticas como a falsa apresentação de políticas de privacidade ou acesso não-autorizado de terceiras partes a dados de consumidores.

Um exemplo desta abordagem foi a ação legal do FTC contra a empresa Facebook, em 2011, que afirmava que a empresa havia violado o FTC Act por sua política de privacidade enganosa. A ação consistia de sete acusações contra a empresa. A primeira afirmava que o

Facebook havia afirmado, implícita e expressamente, que usuários possuíam a habilidade de controlar o acesso a seu perfil a grupos específicos, quando na verdade tais informações eram acessíveis através de plataformas ou aplicativos separados. As acusações 2 e 3 eram relativas à atualização da política de privacidade da empresa em Dezembro de 2009, que passou a designar certas informações de usuários como "publicamente disponíveis"; a acusação 2 alegou que o Facebook não notificou usuários de que algumas de suas informações não eram mais "restritas", e a acusação 3 notou que a empresa alterou materialmente sua promessa a consumidores e aplicou retroativamente as mudanças de privacidade de Dezembro de 2009 sem o consentimento dos mesmos. Finalmente, as acusações 4 a 7 eram relativas à divulgação de informações de consumidores para terceiras partes, como aplicativos e anunciantes publicitários (ESTADOS UNIDOS, 2012a).

A FTC tem tido sucesso nessa abordagem. No caso do Facebook, a empresa chegou a um acordo com a FTC, contendo cinco provisões: que o Facebook não faria mais declarações falsas sobre a privacidade ou segurança das informações de consumidores; que o Facebook obteria o consentimento expresso de seus usuários antes de aplicar quaisquer mudanças que alterassem as configurações de privacidade de seus usuários; que a empresa tornaria a informação da conta dos usuários indisponível 30 dias após a mesma ser encerrada; que o Facebook elaboraria e manteria um programa de privacidade abrangente, feito para abordar riscos de privacidade associados com novos produtos ou serviços, e, finalmente, que o Facebook iria passar por uma inspeção conduzida por uma terceira parte dentro de 180 dias após a decisão e então a cada dois anos pelos próximos vinte anos, de forma a garantir a conformidade de seu programa de privacidade com os requerimentos da FTC (CHIU, 2013).

A ação da FTC e o acordo subsequente foram importantes para a atuação da agência nessa área, por abrir o caminho para ações similares. Apenas em 2016, a FTC abriu diversas investigações relativas à privacidade de dados de consumidores contra empresas em uma variedade de áreas, desde provedores de softwares como a Henry Schein Inc. e Vulcun, companhias telefônicas como a InMobi e gigantes eletrônicos como a ASUS (ESTADOS UNIDOS, 2015c). Devemos manter em mente, no entanto, que esta é uma prática majoritariamente reativa (KEARNEY, 2010).

A FTC também busca estimular "melhores práticas" para a preservação da privacidade digital de usuários dentro de empresas. Em 2009, a FTC publicou o relatório "*Self Regulatory Principles for Online Behavioral Advertising*" (Princípios Autorreguladores para Publicidade Comportamental Online, tradução nossa). O relatório trata da coleta, armazenamento e processamento de dados por empresas de publicidade online, como explicado anteriormente

no capítulo 2, e das preocupações relativas à privacidade de dados consequentes dessa prática. Contém recomendações que incluem maior transparência e controle de consumidores sobre a coleta de seus dados, retenção limitada dos dados de usuários, e obtenção de consentimento expresso de consumidores para a aplicação de mudanças em políticas de privacidade e para o uso de informações sensíveis (ESTADOS UNIDOS, 2009). As recomendações no relatório não possuem força de lei, e buscam apenas estimular melhores práticas. Em 2012, a FTC publicou um novo relatório, "*Protecting Consumer Privacy in an Era of Rapid Change*" (Protegendo a Privacidade dos Consumidores em uma Era de Rápidas Mudanças, tradução nossa), em que defendeu a criação de legislação abrangente sobre a privacidade online para incrementar esforços regulatórios, e declarou que a abordagem de autorregulação nos EUA falhou em produzir um cenário favorável para a privacidade digital (ESTADOS UNIDOS, 2012b).

Outras agências reguladoras nos Estados Unidos têm buscado agir em favor da privacidade digital. A *Federal Communications Commission* (Comissão Federal de Comunicações, tradução nossa), publicou em 1º de Abril de 2016 um Aviso de Proposta de Regulamentação entitulado "*Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*" (Protegendo a Privacidade de Clientes de Serviços de Banda Larga e Outras Telecomunicações, tradução nossa). Esse Aviso de Proposta de Regulamentação (ESTADOS UNIDOS, 2016b) busca obter comentários públicos sobre a regulamentação da privacidade digital, baseado na seguinte avaliação da FCC (ESTADOS UNIDOS, 2016b, p. 3, tradução nossa):

> [...] o regime de privacidade atual, incluindo a liderança importante da Comissão Federal de Comércio (FTC) e os esforços da Administração para proteger a privacidade do consumidor, não aplicam mais de forma abrangente os princípios tradicionais da proteção da privacidade para os serviços de telecomunicação fornecidos pelas empresas de banda larga no século 21.

Embora um relatório de recomendações relativas ao documento supracitado ainda não tenha sido emitido, esse esforço faz parte das tentativas da administração do Presidente Barack Obama (2008-2016) de alterar o cenário da privacidade digital nos EUA. Em 2013, o Presidente Obama assinou uma ordem executiva (*Executive Order on Improving Critical Infrastructure Cybersecurity*, ou Ordem Executiva para Melhorar Infraestrutura Crítica para a Cibersegurança, tradução nossa), em que abriu um programa voluntário de aprimoramento dos serviços cibersegurança para setores fora da indústria de defesa. Para participar do programa, agências e empresas devem incorporar às suas práticas a proteção da privacidade e

das liberdades civis, além de submeter-se a inspeções periódicas para verificar a solidez destes salvaguardas. Essa ordem executiva foi aplaudida por ativistas pela privacidade por inserir a privacidade como elemento essencial do esboço dos programas de cibersegurança do governo, e não apenas como uma consideração posterior (PETERSON, 2013).

É cedo demais para que se determine se a ordem executiva do Presidente Barack Obama representa uma mudança de longo prazo na abordagem "auto-reguladora" dos Estados Unidos à privacidade de dados, o que representaria um grande passo para a privacidade de dados ao redor do mundo, dada a atuação de empresas do país no setor de tecnologias de informação. No entanto, existem outras nações que buscam abordagens diferentes à questão; entre essas, o bloco da União Européia é provavelmente o mais prominente, como veremos adiante.

3.2. A codificação da privacidade na União Europeia

Como exposto anteriormente, a União Europeia possui uma abordagem muito mais paternalista em relação à privacidade de dados do que os Estados Unidos (SOLOVE, 2013) – isto é, busca legislar amplamente sobre o assunto e não confiar na auto-regulação. Na seção anterior, pudemos observar a ausência de uma legislação abrangente dos EUA relativa à privacidade de dados e a aplicação de legislações específicas a certos setores ou contextos que têm uma "sobreposição" com a privacidade de dados. Esse não é o caso da União Europeia. Como veremos abaixo, o bloco possui um corpo legislativo abrangente e específico acerca da privacidade de dados e busca regular ativamente o setor. A própria Carta dos Direitos Fundamentais da União Européia, promulgada no ano 2000, trata especificamente da privacidade de dados em seu Título II (Liberdades), Artigo 8 (Proteção de Dados Pessoais). A redação original do Artigo supracitado se manteve ao longo das atualizações da Carta ao longo dos anos e continua em vigor em sua atualização mais recente em 2010, e afirma:

> 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
> 3.O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente (UNIÃO EUROPÉIA, 2000c, p. 10).

Como mencionado no Capítulo 1, a Convenção Europeia de Direitos Humanos, promulgada em 1950, já havia codificado a importância do direito humano à privacidade no continente europeu. No entanto, durante as décadas de 1970 e 1980, houve crescente

preocupação sobre o rápido desenvolvimento de tecnologias de informação e comunicação e seu impacto sobre a vida dos cidadãos europeus. À luz desses avanços, o termo "vida privada" (utilizado na Convenção Europeia de Direitos Humanos) adquiriu um caráter difuso, justamente pela indefinição entre o público e o privado nesse novo cenário. Além disso, o foco da Convenção Europeia de Direitos Humanos era a prevenção da interferência na vida do cidadão por entidades públicas, como o governo. Sua aplicação em relação a entidades privadas nunca foi explicitada (UNIÃO EUROPÉIA, 20[--]c).

Foi nesse cenário que a *Convention for the Protection of Individuals with regard to automatic processing of personal data* (Convenção para a Proteção de Indivíduos relativa ao processamento automatizado de dados pessoais, tradução nossa, ou "Convenção 108") foi adotada pelo Conselho da Europa em 1981. Seu propósito autodeclarado era assegurar o respeito pelos direitos e liberdades fundamentais de todos os indivíduos, particularmente o direito à privacidade, em relação ao processamento automatizado de dados pessoais relativos aos mesmos. A Convenção 108 estabelece parâmetros mínimos que visam proteger o indivíduo (chamado de "sujeito de dados") de potenciais abusos à sua privacidade durante o processamento automatizado de dados. Esses parâmetros incluem a proibição do processamento automatizado de dados relativos a raça, opiniões políticas ou religiosas, práticas sexuais ou saúde, a não ser que o país signatário possua leis específicas sobre essas questões, que forneçam garantias apropriadas (UNIÃO EUROPÉIA, 1981).

Dentro desses parâmetros, também é estabelecido que dados pessoais processados de forma automatizada devem ser obtidos e processados de forma "justa e legal"; armazenados para propósitos específicos e legítimos, e processados de forma compatível com tais propósitos; adequados, relevantes e não excessivos em relação ao propósito de sua coleta; fidedignos e, quando necessário, atualizados, e, finalmente, processados de forma que permita a identificação dos sujeitos de dados por não mais que o tempo requerido pelo propósito para o qual os dados foram coletados (UNIÃO EUROPÉIA, 1981).

Aos indivíduos, ou sujeitos de dados, são dadas algumas garantias adicionais para a preservação de sua privacidade de dados. A Convenção 108 determina que qualquer pessoa deve possuir a habilidade de confirmar a existência um arquivo de dados pessoais relativos a si, além de seu propósito e local de armazenamento; obter confirmação dentro de um prazo razoável sobre a existência de um arquivo de dados pessoais relativos a si, além de receber essa informação de forma inteligível; obter, se necessário, uma ratificação ou remoção dos dados em questão, caso estes tenham sido processados de forma incongruente com as leis domésticas ou determinações da Convenção 108 relativas ao assunto, e, finalmente, que o

indivíduo tenha uma solução legal disponível caso as determinações supracitadas não sejam cumpridas (UNIÃO EUROPÉIA, 1981).

Além disso, a Convenção 108 busca regular o fluxo transnacional de dados, cujas complexidades exploraremos em maior detalhe mais à frente. É determinado que signatários não podem proibir o fluxo de dados entre fronteiras apenas pelo propósito de proteger a privacidade, a não ser que sua legislação doméstica inclua proteções especiais para categorias específicas de dados pessoais automatizados cuja proteção no país recebedor não seria equivalente àquela recebida no país signatário, ou quando os dados em questão são transferidos através de uma terceira parte de forma a circundar proteções domésticas (UNIÃO EUROPÉIA, 1981).

A Convenção 108 foi o primeiro instrumento internacional legalmente vinculante relativo à proteção de dados, atualmente ratificado por 47 Estados europeus e aberto para a adesão de Estados não-membros do Conselho Europeu, que incluem o Uruguai e as Ilhas Maurício (UNIÃO EUROPÉIA, 2016b). Organizações não-governamentais pela privacidade digital como a *Electronic Privacy Information Center* (Centro de Informações sobre a Privacidade Eletrônica, tradução nossa, ou EPIC) apontam que a Convenção 108 permanece sendo o único instrumento internacional legalmente vinculante no campo da privacidade de dados, e que suas determinações são razoavelmente rigorosas. Além disso, a possibilidade de adesão por Estados não-membros do Conselho Europeu maximiza o potencial da Convenção 108 como um instrumento verdadeiramente internacional para a regulação da privacidade de dados (ELECTRONIC PRIVACY INFORMATION CENTER, 20[--]b).

A Convenção 108 não é, no entanto, um instrumento perfeito. Quando a Convenção 108 foi escrita, o processamento de dados era uma atividade de nicho, o que facilitava sua implementação e o monitoramento da mesma. No entanto, é difícil identificar atualmente uma atividade que não inclua interações com tecnologias computadorizadas, o que transporta atividades triviais como a compra de um café para a arena do processamento de dados. Além disso, a Convenção 108 não regula a coleta de dados, apenas seu processamento. Como exploramos no Capítulo II, a coleta de dados é quase omnipresente no uso da internet atualmente e é parte do problema de regular a privacidade digital dos indivíduos. Dessa forma, podemos avaliar que a abrangência do escopo da Convenção 108 é seu maior mérito, por estabelecer princípios legalmente vinculantes aplicáveis no âmbito internacional. No entanto, a ausência, em sua redação, de instrumentos específicos para operacionalizar tais princípios impedem que a Convenção 108 possa ser utilizada como o único instrumento legal para a privacidade de dados na Europa (KIERKEGAARD et al, 2011). Isso, é claro, não é

necessariamente um problema ou falha estrutural da Convenção 108. Existem diversos instrumentos legalmente vinculantes importantíssimos cuja operacionalização é garantida através de outros instrumentos legais mais específicos; isso não torna os princípios gerais menos relevantes. A própria Carta de Direitos Humanos da ONU não estabelece formas específicas de garantir os direitos que a mesma determina; no entanto, dificilmente poderíamos dizer que suas determinações são menos relevantes por isso.

De fato, existem diversas diretivas e regulamentos dentro da União Europeia que buscam maior especificidade na aplicação dos princípios da Convenção 108. Antes de falarmos sobre os mesmos, é necessário esclarecer o papel de diretivas e regulamentos dentro da União Europeia. Diretivas são endereçadas para os Estados-membros, e, portanto, só são legalmente vinculantes para os Estados nacionais. Através de um processo chamado de "transposição", a diretiva estabelece um "quadro de regulamentação", porém deixa os detalhes práticos da implementação a critério dos Estados individuais. Já regulamentos têm aplicação geral (*erga omnes*), o que significa que são legalmente vinculantes para indivíduos também. Regulamentos se tornam parte efetiva da legislação doméstica dos Estados uma vez que sejam adotados e não necessitam do processo de transposição. Isso significa que, uma vez que um regulamento seja adotado pela União Europeia, os Estados-membros não precisam aprovar novas leis domésticas para aplicá-lo, apenas emendar aquelas que contrariem as determinações do novo regulamento em efeito (BBC NEWS, 2009)

Nas últimas décadas, a diretiva europeia mais proeminente em relação à privacidade de dados foi a Diretiva 95/46/EC, também conhecida como *Data Protection Directive* (Diretiva de Proteção de Dados, tradução nossa). A Diretiva de Proteção de Dados (DPD) foi adotada em 1995, e tem como base a Convenção 108. Sob seu escopo estão organizações e indivíduos que estão baseados dentro de um ou mais Estados-membros da União Europeia (WONG, 2012). O objetivo da DPD era conciliar dois objetivos aparentemente conflituantes: proteger os "sujeitos de dados" (indivíduos) e facilitar o livre mercado dentro da União Europeia. Segundo a DPD, o estabelecimento de um mercado interno baseado na livre circulação de bens, pessoas, serviços e capitais requer que dados pessoais possam fluir livremente entre Estados-membros e que os direitos fundamentais de indivíduos sejam garantidos (UNIÃO EUROPÉIA, 1995).

A DPD determina que Estados-membros implementem leis baseadas nos princípios de proteção de dados determinados pela Convenção 108, que são listados novamente no artigo 6 da DPD com pequenas alterações. Uma das inovações da DPD em relação à Convenção 108 é o uso do termo *data controller* (controlador de dados, tradução nossa), que refere-se às

pessoas ou entidades que coletam e processam dados pessoais, assim como os propósitos e os meios do processamento de dados. Já o artigo 7 vai além da Convenção 108 e baseia-se em princípios de proteção de dados preparados pela Organização de Cooperação Econômica e Desenvolvimento (OCDE) em 1980, que especificam sete circunstâncias em que o processamento de dados pessoais é considerado legítimo. O processamento de dados pessoais é considerado legítimo nos casos especificados abaixo, de acordo com o artigo 7 da DPD:

> (a) o sujeito de dados deu seu consentimento de forma inequívoca; ou
> (b) o processamento é necessário para a execução de um contrato do qual o sujeito de dados é parte ou de forma a tomar providências por pedido do sujeito de dados antes de entrar em um contrato; ou
> (c) o processamento é necessário para o cumprimento de uma obrigação legal de que o controlador é sujeito; ou
> (d) o processamento é necessário de forma a proteger os interesses vitais do sujeito de dados; ou
> (e) o processamento é necessário para a execução de uma tarefa realizada pelo interesse público ou no exercício de autoridade oficial investida sobre o controlador ou a terceira parte a quem os dados são revelados; ou
> (f) o processamento é necessário para a prossecução de interesses legítimos do controlador ou da(s) terceira(s) parte(s) a quem os dados são revelados, a não ser que tais interesses sejam anulados no interesse dos direitos e liberdades fundamentais do sujeito de dados que necessitam de proteção de acordo com o Artigo 1 (1) (UNIÃO EUROPÉIA, 1995, tradução nossa).

A DPD também impõe uma série de deveres aos "controladores de dados", enquanto dá aos "sujeitos de dados" uma série de garantias. De acordo com a DPD, o controlador de dados tem a obrigação de notificar o sujeito de dados sobre a coleta e o uso de seus dados (artigo 10), de notificar, sempre que possível, o sujeito de dados caso obtenha dados do mesmo através de uma terceira parte (artigo 11) e de garantir a confidencialidade e a segurança dos dados (artigos 16 e 17, respectivamente); já o sujeito de dados tem o direito de acessar os dados em questão (artigo 12) e de contestar certos tipos de processamento (artigo 14) (UNIÃO EUROPÉIA, 1995).

Em seu artigo 13, a DPD dá aos Estados-membros o direito de adotar medidas legislativas para restringir as determinações dos artigos supracitados, caso tal restrição seja necessária para garantir a segurança nacional; defesa; segurança pública; prevenção, investigação, deteção e julgamento de ofensas criminais, ou quebras de princípios éticos em profissões regulamentadas; a execução de funções oficiais relacionadas às atividades mencionadas anteriormente, e a proteção do sujeito de dados ou dos direitos e liberdades fundamentais de outrem (UNIÃO EUROPÉIA, 1995).

Em relação à transferência de dados para outros países, a DPD mantém a mesma linha da Convenção 108, determinando em seu Artigo 25 que a transferência pode ocorrer caso o país recebedor garanta um nível "adequado" de proteção; caso contrário, a transferência pode

ser realizada em condições específicas, como com o "consentimento inequívoco" do sujeito de dados, a existência de regras vinculativas para empresas, ou para o cumprimento de uma obrigação contratual entre o sujeito e o controlador de dados (Artigo 26). Para a tomada de decisões como o nível de "adequação" de terceiros países, a DPD cria em seu Capítulo VI uma série de mecanismos de autoridade supervisora, como um Comitê formado por representantes de todos os Estados-membros (artigo 31) e O *Working Party on the Protection of Individuals with regard to the Processing of Personal Data* (Grupo de Trabalho para a Proteção de Indivíduos em relação ao Processamento de Dados Pessoais, tradução nossa), que ficou conhecido como Grupo de Trabalho 29 devido ao artigo que estabeleceu sua criação. O Grupo de Trabalho 29 atua em caráter consultivo para a União Europeia e seus Estados-membros em relação à proteção de dados pessoais (UNIÃO EUROPÉIA, 1995).

Como podemos observar, a DPD buscou especificar os princípios estabelecidos pela Convenção 108 para que os Estados-membros realizassem a transposição dos mesmos para suas legislações domésticas. A DPD vinculou 27 Estados-membros e três membros da Área Econômica Europeia (Noruega, Islândia e Liechtenstein) e ofereceu mecanismos para a transferência de dados fora da EU, e por isso alguns autores a consideram o instrumento internacional de leis de proteção de dados mais abrangente e bem-sucedido (GREENLEAF, 2012).

Já outros apontam falhas estruturais na DPD, que envolvem, inclusive, a base para seu estabelecimento. É fato que o livre fluxo de dados entre países é necessário para o estabelecimento de um mercado comum de bens, pessoas, capitais e serviços. No entanto, autores como Serge Gutwirth argumentam que existe um conflito inerente entre o fluxo livre de dados e a proteção da privacidade de dados; sendo assim, ao tentar conciliar ambos os conceitos, a DPD essencialmente elevou o objetivo de um mercado comum europeu à categoria de direito humano, condicionando, assim, o direito à privacidade aos interesses do mercado (BIRNHACK, 2008).

Existem também críticas relacionadas à forte ênfase dada na DPD em relação ao "consentimento" como critério de exceção. Como discutimos no Capítulo 2, a noção de "consentimento" em relação à privacidade é extremamente volátil e sujeita à manipulação por terceiras partes, podendo transformar-se facilmente em cessão de controle. Dessa forma, alguns autores defendem afastar do conceito de "consentimento" a legislação sobre proteção de dados e privacidade digital (NISSENBAUM, 2004). Já a DPD toma o caminho oposto; por exemplo, como mencionamos anteriormente, a transferência de dados pessoais para terceiros

países com proteções de dados consideradas inadequadas é permitida caso o consentimento explícito do sujeito de dados seja obtido.

O consentimento como base para transferência de dados para terceiros países apresenta desafios práticos e não apenas teóricos. Uma vez que o cidadão europeu dê seu consentimento para a transferência supracitada, não existe nenhuma forma de garantir que as condições especificadas pelos artigos da DPD, mencionados anteriormente, sejam cumpridas. Além disso, a especificação de que os dados podem ser transferidos para terceiros países "inadequados" para o cumprimento de um contrato entre o sujeito e o controlador de dados cria uma lacuna legal que já exploramos em relação à legislação dos EUA. Uma vez que o consentimento (ou cessão de controle) ocorre por parte do sujeito de dados, não existem mecanismos para controlar o que é feito com os dados pessoais posteriormente (BIRNHACK, 2008).

Outros apontam que a DPD se baseia em premissas subjetivas que, embora aceitáveis quando listadas como princípios gerais (como na Convenção 108), tornam-se inadequadas quando apresentadas como instrumentos de operacionalização. Por exemplo, o Artigo 6 da DPD afirma que dados pessoais não devem ser processados para propósitos diferentes daqueles para os quais foram coletados. Certamente esse é um princípio geral aceitável. No entanto, ao buscar aplicar esse princípio com base na DPD, percebemos que não há uma especificação sobre os propósitos de quem devem ser considerados. Sujeitos de dados cedem seus dados por propósitos que podem ser inteiramente diferentes dos propósitos dos controladores de dados que os coletam. Além disso, como vimos no Capítulo 2, dados pessoais podem ser coletados sem que seus sujeitos sequer estejam cientes da coleta; nesse caso, pelo menos pela perspectiva do sujeito de dados, é impossível que o mesmo designe um propósito para a coleta (ELGESEM, 1999).

Além das críticas citadas acima, a DPD enfrentou um desafio muito mais elementar: o atraso em sua implementação por parte dos Estados-membros, incluindo a Alemanha, Irlanda, Luxemburgo, Países Baixos e a França, que até 2003 não havia adequado sua legislação de proteção de dados à Diretiva. Além disso, o espaço de manobra garantido aos países durante o processo de transposição da DPD para suas respectivas legislações criou divergências internas que, embora não sejam consideradas violações da diretiva, ainda impedem um sistema de regulação uniforme entre os países da EU (SAXBY, 2003).

A DPD também enfrenta o desafio já explorado e inerente às tentativas de legislar a tecnologia: um relatório emitido em 2003 pela Comissão Europeia sobre a implementação da DPD aponta que mecanismos de coleta de dados pessoais, particularmente na internet, haviam

se tornado mais sofisticados e difíceis de detectar, coletando uma variedade e quantidade de dados pessoais não disponíveis anteriormente (UNIÃO EUROPÉIA, 2003).

Os esforços da União Europeia para regulamentar a privacidade de dados continuaram mesmo após a implementação da DPD. O *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (*Regulamento (EC) No 45/2001 do Parlamento e Conselho Europeus sobre a Proteção dos Indivíduos em relação ao processamento de dados pessoais por instituições e entidades da Comunidade Europeia e sobre o movimento livre destes dados, tradução nossa), assinado em 2000 e em efeito em 2001, buscou institucionalizar a proteção à privacidade de dados dentro das operações da própria Comunidade Europeia. Embora as determinações do Regulamento 45/2001 sejam largamente similares àquelas estabelecidas pela DPD, este tomou o passo notável de estipular a criação do cargo de *Data Protection Supervisor* (Supervisor de Proteção de Dados, tradução nossa), uma autoridade supervisora independente cuja principal função é garantir o respeito à privacidade e proteção de dados por instituições europeias, tanto em seu processamento de dados pessoais quanto na formulação de novas políticas e diretrizes dentro do bloco. Além disso, o supervisor de Proteção de Dados supervisiona o trabalho de *Data Protection Officers* (Oficiais de Proteção de Dados, tradução nossa) presentes em todas as instituições europeias (UNIÃO EUROPÉIA, 2000b). O Supervisor de Proteção de Dados tem tido um papel extremamente ativo na União Europeia desde seu estabelecimento *de facto* em 2004 e tem preservado sua natureza independente; em 2015, o Supervisor de Proteção de Dados Giovanni Buttarelli chegou a divergir publicamente das propostas de novas proteções de dados apresentadas pelo Parlamento Europeu, publicando sua própria versão de sugestão de legislação (MEYER, 2015).

Em 1997, foi aprovada a *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector* (Diretiva 97/66/EC do Parlamento Europeu e do Conselho de 15 de Dezembro de 1997 sobre o processamento de dados pessoais e a proteção da privacidade no setor de telecomunicações, tradução nossa), que buscava operacionalizar as determinações da DPD no setor de telecomunicações. No entanto, a Diretiva 97/66/EC já nasceu desatualizada, pois havia sido elaborada no começo dos anos 90. Além disso, como o próprio nome sugere, era direcionada apenas ao setor de telecomunicações, quando naquela época comunicações eletrônicas já eram usadas com relativa frequência. Embora o Grupo de Trabalho 29 tenha emitido a opinião de que a Diretiva 97/66/EC era também aplicável a

comunicações eletrônicas, ainda havia um grau de incerteza relativa ao assunto, e a União Europeia decidiu remediar a situação e adotar uma nova Diretiva. Essa iniciativa transformou-se na *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector* (Diretiva 2002/58/EC sobre o processamento de dados pessoais e a proteção da privacidade no setor de comunicações eletrônicas, tradução nossa), também conhecida como Diretiva E-Privacy (*E-Privacy Directive*) (DEBUSSERÉ, 2005).

Além da aplicação de princípios básicos da DPD, como o armazenamento proporcional aos propósitos dos dados e o requerimento de informar ao sujeito de dados sobre o tipo de dados coletados, a Diretiva E-Privacy buscou tratar de áreas não exploradas pela DPD no setor de comunicações eletrônicas. Algumas determinações são particularmente notáveis. Por exemplo, a Diretiva determinou que dados de transmissão devem ser apagados no momento em que a transmissão é considerada completa, ao final de uma ligação telefônica e no momento do recebimento do e-mail pelo destinatário (*recital* 27). Em relação a dados de localização, a Diretiva reconhece que estes são necessários para que o serviço de telefonia celular seja executado; no entanto, adiciona que redes digitais de celulares podem ser capazes de detectar a localização do usuário com maior precisão do que o necessário para oferecer o serviço em questão, e que esse tipo de localização particularmente precisa deve ocorrer apenas com o consentimento do usuário (*recital* 35). Finalmente, estabeleceu que sistemas para o fornecimento de serviços de comunicações e serviços eletrônicos devem ser elaborados já com o propósito de limitar, tanto quanto possível, o processamento de dados pessoais (*recital* 30) (UNIÃO EUROPÉIA, 2002).

Adicionalmente, foi explicitado que instrumentos como *spyware* e *cookies* devem ser utilizados apenas para propósitos legítimos (*recitals* 24 e 25); além disso, foi especificado que no caso de instrumentos para coletar dados, como *cookies*, o sujeito de dados deve também receber informações claras e abrangentes sobre os propósitos do processamento de dados, e ter a oportunidade de recusar esse tipo de processamento (artigo 5). No entanto, o *recital* 25 também especifica que acesso a um web site específico pode ser condicionado ao consentimento do uso de *cookies* ou instrumentos similares, desde que usados para propósitos legítimos (UNIÃO EUROPÉIA, 2002). Sendo assim, alguns autores apontam que a Diretiva E-Privacy parece não adicionar, de fato, novas obrigações em relação àquelas já especificadas na DPD, já que apenas reafirma a necessidade de se obter consentimento do sujeito de dados (DEBUSSERÉ, 2005). Enfrentamos, então, o mesmo problema relativo ao consentimento presente na DPD e já explicado anteriormente.

A Diretiva E-Privacy foi emendada em 15 de Março de 2006 pela Diretiva 2006/24/EC. A Diretiva 2006/24/EC determinou que, em cumprimento da Declaração de Combate ao Terrorismo adotada pelo Conselho Europeu em 25 de Março de 2004, Estados-membros devem reter os dados relativos a telecomunicações e comunicações eletrônicas por um período mínimo de 6 meses, que pode se estender a até no máximo 24 meses (UNIÃO EUROPÉIA, 2006). Embora a Diretiva 2006/24/EC especifique que apenas dados de transmissão, e não de conteúdo, devam ser retidos, ela foi objeto de fortes protestos por parte de organizações de direitos humanos e defensoras da privacidade. Em 2014, a Corte de Justiça da União Europeia (CJUE) declarou a Diretiva 2006/24/EC inválida, por considerar que a mesma violava os princípios básicos do direito à privacidade. Embora um espaço de 8 anos tenha se passado entre a aprovação da diretiva em questão e sua invalidação, a decisão da CJUE foi encarada como um marco em uma nova era na defesa da privacidade de dados na União Europeia, e uma demonstração da seriedade do bloco em relação ao assunto (STOEVA, 2014).

A União Europeia tem, de fato, dado demonstrações de que busca aprimorar sua legislação relativa à privacidade de dados. Em 2012, o bloco anunciou a *Data Protection Reform* (Reforma da Proteção de Dados*,* tradução nossa). Essa reforma iniciou uma rodada de debates e propostas de legislação que culminaram, em 27 de abril de 2016, no Regulamento (EU) 2016/679, também conhecido como *General Data Protection Regulation* ou GDPR (Regulamento Geral de Proteção de Dados, tradução nossa). O GDPR entrará em efeito em 25 de Maio de 2018; uma vez que isso aconteça, o GDPR substituirá a Diretiva de Proteção de Dados (DPD) discutida ao longo desse capítulo (UNIÃO EUROPÉIA, 2016a). Sendo um Regulamento, e não uma Diretiva, a GDPR não necessita do processo de transposição e se tornará parte efetiva da legislação doméstica dos Estados-membros tão logo entre em efeito.

Dado o fato de que o GDPR ainda não entrou em efeito, ainda não existem dados relativos à sua aplicação prática. Em relação ao texto do regulamento, no entanto, nota-se que o GDPR mantém muitos dos princípios da DPD, com algumas modificações importantes. Os parâmetros para consentimento válido, por exemplo, foram alterados. Cláusulas de consentimento em diretrizes e contratos devem estar completamente separadas de outros termos e condições, e não serão válidos a não ser que sejam prontamente disponíveis, específicos, informativos e explícitos (Artigos 4 e 6). Além disso, sujeitos de dados têm o direito de remover o consentimento fornecido anteriormente a qualquer momento, e esse direito deve ser prontamente acessível (UNIÃO EUROPÉIA, 2016a).

Além disso, sujeitos de dados adquiriram o "direito de ser esquecido" (*"right to be forgotten*", tradução nossa), que dá aos mesmos o direito de solicitar o completo apagamento de dados em posse do controlador de dados caso seja determinado que esse último não cumpriu as obrigações do GDPR ou da legislação doméstica relativa ao uso dos dados em questão. Também é dado aos sujeitos de dados o direito da "portabilidade", isto é, a habilidade de obter, do controlador de dados, todos os dados relativos a si de forma inteligível e de fácil acesso, dando ao sujeito de dados a habilidade de transmitir ele mesmo esse arquivo para outros controladores de dados (*recital* 68) (UNIÃO EUROPÉIA, 2016a).

O GDPR também estreita o conceito de "uso legítimo" de dados apresentado pela DPD, determinando que os usos legítimos de dados devem ser explicitados no momento da coleta, e que dados pessoais não devem ser processados a não ser que não existam outras formas possíveis de se atingir um propósito específico que não esse processamento (*recital* 26) (UNIÃO EUROPÉIA, 2016a).

Adicionalmente, caso ocorra uma violação dos dados pessoais (*data breach*, tradução nossa) – isto é, a divulgação involuntária de dados pessoais de indivíduos para outrem – controladores de dados têm até 72 horas para notificar os sujeitos de dados, a não ser que possa ser provado que essa violação não terá nenhum impacto material, não-material ou físico para os indivíduos em questão (*recital* 61). Sujeitos de dados também adquiriram o direito de compensação caso sua privacidade de dados seja infringida (artigo 56) (UNIÃO EUROPÉIA, 2016a).

O GDPR representa também a primeira vez em que a categoria de "processadores de dados" (*data processors*, tradução nossa) é regulada. Enquanto a DPD regulamenta o processamento de dados por controladores (aqueles que definem os meios e propósitos da coleta e processamento de dados), processadores – organizações que podem ser utilizadas por controladores para processar dados pessoais – estão, pelo GDPR, sujeitos a um conjunto de restrições similares aos de controladores de dados. Isso inclui fornecedores de serviços de armazenamento (*cloud,* ou nuvem) (DLA PIPER, [2016?]).

A mudança mais dramática entre a DPD e o GDPR é seu escopo. Enquanto a DPD tem sob sua jurisdição indivíduos ou organizações dentro da União Europeia, o GDPR se aplica a todas as organizações globais que possam ter dados de cidadãos e residentes da União Europeia. Isso implica um regime de transferência de dados para terceiros países ainda mais rígido. O chamado requisito de adequação (*adequacy requirement*, tradução nossa) determina que terceiros países devem fornecer no mínimo o mesmo nível de proteção de dados que a União Europeia, e deve ser levado em consideração seu respeito ao *rule of law* e direitos

humanos, além de suas leis gerais e setoriais. Caso o terceiro país não seja considerado adequado, deve haver mecanismos legais vinculativos, como acordos bilaterais, para garantir a proteção de dados de cidadãos ou residentes europeus. Embora existam exceções para este requerimento, como a defesa nacional, segurança pública, ou a investigação de atos criminosos, o GDPR especifica que essas derrogações devem ser interpretadas de forma restrita e que não será permitida a transferência estrutural frequente e em massa de dados pessoais, e sim apenas o estritamente necessário (artigos 67-72) (UNIÃO EUROPÉIA, 2016a).

Como dito anteriormente, o GDPR ainda não entrou em efeito. Não se pode, nesse momento, avaliar sua aplicação prática. No âmbito teórico, o GDPR ainda não foi submetido a escrutínio tão intenso quanto a DPD, especialmente dado seu pouco tempo de aprovação, o que pode contribuir para o otimismo relativo ao regulamento. Alguns autores apontam que apenas o processamento de dados por agências de segurança nacional secretas não está fortemente regulado pelo GDPR; de resto, existem poucos dados pessoais cujo processamento não será afetado (DE HERT; PAPAKONSTANTINOU, 2016). Outros autores, como Blume (2014) apontam que o GDPR mantém a subjugação da privacidade digital às forças do mercado, e que a aplicação prática do regulamento não será significativamente diferente daquela já praticada de acordo com o DPD; seu único mérito seria, então, o aumento da consciência relativa a seus direitos entre sujeitos de dados, especialmente à luz de seu extenso texto. No entanto, mesmo Blume admite que o GDPR tende a no mínimo manter a proteção de dados já existente, e pode melhorá-la quando em efeito. Resta ver como a GDPR será utilizada uma vez que seja implementada em sua totalidade em 2018.

Como observamos acima, existem diferenças dramáticas entre a legislação de privacidade de dados – ou a falta dela – entre os Estados Unidos e a União Europeia. Observamos que a preocupação com a venda, compra e troca de dados dentro de um mercado interconectado é uma preocupação, particularmente para a União Europeia. Sendo assim, dado o relacionamento transatlântico comercial entre ambos, devemos nos perguntar: em relação à privacidade de dados, como conciliar a abordagem paternalista da EU com a abordagem *laissez-faire* dos EUA, mantendo o relacionamento comercial entre o bloco europeu e o país norte-americano intactos e sem sacrificar a preocupação da EU com os dados de seus cidadãos? A questão obteve atenção especial de legisladores europeus, o que ensejou a criação de enquadramentos legais específicos à transação de dados entre empresas europeias e norte-americanas, como exploraremos a seguir.

3.3. Regulando o fluxo transnacional de dados: Estados Unidos e União Europeia

Muito foi dito anteriormente sobre países com legislações e proteções consideradas "adequadas" pela União Europeia para a transmissão de dados de cidadãos europeus. No caso dos Estados Unidos, o regime legal relativo ao assunto é caracterizado acima de tudo pela ausência de uma legislação federal abrangente, sendo a legislação existente mais direcionada para setores ou atividades específicas do que para o tema concreto da privacidade de dados.

Essa questão mereceu atenção especial da União Europeia justamente pelo volume do comércio entre o bloco e os Estados Unidos. Segundo a Comissão Europeia, o comércio entre os EUA e a EU corresponde a aproximadamente um terço do fluxo comercial mundial (UNIÃO EUROPÉIA, [2015?]). Dessa forma, um enquadramento legal específico foi elaborado entre os dois parceiros entre 1998 e 2000. A esse enquadramento legal inicial deu-se o nome de *Safe Harbour Privacy Principles* (Princípios de Privacidade em Porto Seguro, tradução nossa). Os Princípios de Privacidade em Porto Seguro ("Princípios") foram criados através de uma colaboração entre a Comissão Europeia e o Departamento de Comércio dos EUA, que deu origem à *2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce* (Decisão 2000/520/EC, relativa à Diretiva 95/46/EC do Conselho e Parlamento Europeu e à adequação da proteção provida pelos princípios de privacidade em porto seguro e perguntas frequentes relacionadas emitidas pelo Departamento de Comércio dos EUA, tradução nossa) (UNIÃO EUROPÉIA, 2000a).

O objetivo do enquadramento Porto Seguro era agilizar o processo para empresas norte-americanas que buscavam ser consideradas "adequadas" pela União Europeia em relação à privacidade de dados de usuários. A Decisão 2000/520/EC ("Decisão Porto Seguro") ecoa os princípios básicos da Diretiva 95/46/EC (Diretiva de Proteção de Dados) que exploramos anteriormente, como a notificação da coleta de dados, a obtenção de consentimento para a coleta e o processamento dos mesmos, a criação de protocolos internos para garantir a segurança e integridade dos dados em questão, o direito de acesso do sujeito aos dados relativos a si e mecanismos de controle e implementação (UNIÃO EUROPÉIA, 2000a). A adesão ao Programa Porto Seguro era voluntária, e aplicável a todas as empresas sob a jurisdição da Comissão Federal de Comércio dos EUA (FTC) ou do Departamento de Transporte. O Programa Porto Seguro não era aplicável a instituições financeiras, empresas de telecomunicações, associações trabalhistas, organizações não-governamentais (ONGs),

cooperativas agrícolas e instalações de processamento de carne (ESTADOS UNIDOS, 20[--]a).

O chamado Programa Porto Seguro era baseado na auto certificação. Isto é, as próprias companhias americanas se declaravam adequadas aos princípios Porto Seguro e os benefícios do programa se tornavam imediatamente aplicáveis a partir do momento em que uma carta para o Departamento de Comércio dos EUA com uma notificação de sua adesão e contendo as seguintes informações: nome e endereços de correspondência e contato da empresa, descrição das atividades da organização relativas a informações pessoais recebidas da EU e descrição da política de privacidade da organização relativa aos dados pessoais supracitados, incluindo o local de acesso para o público à política de privacidade, um ponto de contato para reivindicações relativas ao assunto, corpo estatutário cuja jurisdição recai sobre a organização, métodos de verificação e mecanismo de recurso independente para investigar reivindicações não resolvidas. Uma vez que essas informações fossem fornecidas para o Departamento de Comércio através desta carta, a empresa seria considerada "adequada" para receber dados de cidadãos europeus (ESTADOS UNIDOS, 20[--]a).

As diretrizes do Programa Porto Seguro não se aplicavam caso as mesmas fossem conflituantes com a segurança nacional, interesse público ou requerimentos de agências policiais, ou caso tais diretrizes entrassem em conflito direto com alguma lei ou regulamento local. Além disso, empresas deveriam se auto avaliar de forma a garantir conformidade e fazer uma reafirmação anual de sua adesão ao programa (ESTADOS UNIDOS, 20[--]a).

A base do programa na "auto certificação" de empresas, previsivelmente, provou-se frágil. Relatórios da União Europeia em 2002 e 2004 revelaram que muitas empresas auto certificadas não cumpriam os princípios requeridos. Além disso, não havia qualquer mecanismo para verificar a conformidade de empresas aos princípios do programa, de forma que muitas empresas violavam sistematicamente os princípios de transparência, notificação e recursos sem qualquer punição ou monitoramento, continuando assim com sua certificação Porto Seguro (CONNOLLY, 2008). Além disso, foi estabelecido que o *USA Patriot Act*, que mencionamos anteriormente, dava a autoridades a capacidade de acessar dados sem restrições relativas à sua origem, fragilizando assim as proteções estabelecidas pelos Princípios Porto Seguro (HOBOKEN et al, 2012).

Apesar de suas óbvias fragilidades, os Princípios Porto Seguro seguiram como enquadramento legal para a transmissão de dados de cidadãos europeus para os Estados Unidos até 2015, quando um cidadão austríaco processou a empresa Facebook declarando que, em luz das informações trazidas à luz por Edward Snowden, a empresa havia falhado em

proteger seus dados contra a vigilância do governo americano. O caso iniciou-se nos tribunais da Irlanda e foi eventualmente encaminhado pelo Tribunal Supremo do país para a Corte de Justiça Europeia, que declarou inválida a Decisão do Porto Seguro em 6 de Outubro de 2015 (UNIÃO EUROPÉIA, 2015).

De forma a substituir os Princípios Porto Seguro, a Comissão Europeia e o Departamento de Comércio dos EUA adotaram, em 12 de Julho de 2016, o *EU-US Privacy Shield* (Escudo de Privacidade União Europeia-Estados Unidos). O objetivo do Escudo de Privacidade UE-EUA ("Escudo") é o mesmo dos Princípios Porto Seguro: um mecanismo de conformidade para transmissão de dados da União Europeia para os EUA. O Escudo segue as linhas principais estabelecidas pelos Princípios Porto Seguro, com algumas diferenças. Entre elas, empresas devem incluir em suas políticas de privacidade os órgãos de conformidade relevantes, além de sua política para transferências adicionais ocorridas após o recebimento inicial de dados. Além disso, empresas só podem realizar transferências subsequentes para parceiros comerciais com propósitos limitados e sob um contrato que estabeleça um nível de proteção mínimo equivalente aos Princípios do Escudo de Privacidade. O Escudo também buscou corrigir algumas falhas dos Princípios Porto Seguro, dando ao Departamento de Comércio e à Comissão Federal de Comércio maiores poderes para monitorar e punir empresas que violem os princípios estabelecidos. Também foram dados a cidadãos europeus recursos mais eficientes para reivindicações relativas ao uso de seus dados por companhias americanas sob o Escudo; entre eles, cidadãos podem levar suas reivindicações diretamente às Autoridades de Privacidade de Dados europeias. Finalmente, o Escudo busca monitorar de forma mais ativa o uso de dados de cidadãos europeus por autoridades dos EUA, incluindo investigações e o monitoramento para assegurar que as leis dos EUA foram seguidas. O programa segue sendo de adesão voluntária e baseado na auto certificação por empresas (SOTTO; HYDAK, 2016).

O Escudo de Privacidade União Europeia-Estados Unidos entrou em efeito no dia 01 de Agosto de 2016 e já é alvo de diversas críticas. É considerado por muitos como uma atualização mínima dos Princípios Porto Seguro, e foi caracterizado como insuficiente para a proteção dos dados de usuários. O próprio Grupo de Trabalho Artigo 29 criticou o enquadramento atual, e o Parlamento Europeu também expressou preocupações. Além disso, dada a aprovação do Regulamento Geral de Proteção de Dados (GDPR), o Escudo terá de ser reavaliado quanto à sua conformidade com a nova legislação estabelecida pela GDPR, criando assim um ambiente de insegurança jurídica para companhias que possam vir a adotar

o Escudo como enquadramento legal para a transferência de dados da UE para os EUA (LOMAS, 2016).

A União Europeia também busca utilizar soluções dentro do direito do comércio internacional para tentar solucionar a questão de fluxos de dados transnacionais. Até Setembro de 2016, a Comissão Europeia disponibilizou, através das Decisões 2001/497/EC, 2004/915/EC e 2010/87/EU, cláusulas contratuais modelos consideradas adequadas ao nível de proteção de privacidade de dados europeu (UNIÃO EUROPÉIA, 20[--]a).

Anteriormente, já em 2003, o Grupo de Trabalho 29 propôs que a questão fosse abordada através de uma série de *Binding Corporate Rules* (Regras Empresariais Vinculativas, tradução nossa). As *Binding Corporate Rules* (BCR) são regras internas, como códigos de conduta, adotadas de forma voluntária por grupos multinacionais de forma a definir suas políticas de privacidade em relação à transferência de dados entre países. As BCR tornam-se legalmente vinculativas uma vez que sejam adotadas por um grupo multinacional, e devem refletir o nível de proteção de dados estabelecido pela legislação da União Europeia (KULESZA, 2012). Para que uma empresa adote as BCRs, sua política e práticas de privacidade digital devem ser inspecionadas por uma Autoridade de Privacidade de Dados (como um Oficial de Proteção de Dados, mencionado anteriormente), que então encaminhará sua revisão para a aprovação de Autoridades de Privacidade de Dados de outros países da União Europeia, comprovando que as políticas e práticas de privacidade do grupo empresarial em questão correspondem aos critérios estabelecidos pelo Grupo de Trabalho 29 (UNIÃO EUROPÉIA, 20[--]b).

As BCRs são aplicadas primariamente a grupos multinacionais e são vistas como mecanismos mais específicos de proteção da privacidade de dados do que, por exemplo, os Princípios Porto Seguro. Além disso, as inspeções realizadas por Autoridades de Privacidade de Dados as tornam mais confiáveis que a auto certificação dos Princípios Porto Seguro. A adoção das BCRs também obteve moderado sucesso: até outubro de 2016, 92 empresas multinacionais haviam adotado as BCRs (UNIÃO EUROPÉIA, 2016c). No entanto, a prática enfrenta algumas limitações. A primeira é relativa aos mecanismos de conformidade das BCRs. Embora as regras estabelecidas pelas mesmas tornem-se legalmente vinculativas, a conformidade legal entre diversas fronteiras nacionais e seus respectivos corpos legislativos é sempre uma questão complexa. Além disso, presume-se que a companhia multinacional em questão será capaz de impor as determinações da BCR sobre suas operações ao redor do mundo, que podem, naturalmente, enfrentar variações. Dessa forma, as BCR são encaradas mais como mecanismos de boa governança do que como regulamentos legais concretos; seus

benefícios são inegáveis, porém não necessariamente totalmente eficientes por si sós (ROWE, 2003).

3.4. Estados Unidos e União Europeia: uma breve comparação entre abordagens

Como pudemos observar ao longo deste capítulo, as abordagens da União Europeia e dos Estados Unidos relativas à privacidade de dados são completamente diferentes. Enquanto a União Europeia possui uma abundância de legislação abrangente relativa ao assunto específico da privacidade de dados, os Estados Unidos possuem leis setoriais e uma abordagem *laissez-faire* ao tema. (BIRNHACK, 2008).

Existem algumas razões para isso. Em nível geral, deve-se levar em consideração a diferença entre os modelos jurídicos de ambas as partes. Os Estados Unidos adotam, majoritariamente, o modelo da *common law*. Tendo sua origem na Inglaterra durante a Idade Média, a *common law* é, em geral, pouco codificada. Embora faça uso de estatutos, as decisões na common law são, na maioria das vezes, baseadas em precedentes. Isso dá a juízes enorme poder, criando uma cultura judicial em que duas partes apresentam seus argumentos para a decisão final do juiz. Já a *civil law* possui alto nível de codificação, contendo códigos que são constantemente atualizados de forma a especificar todos os assuntos que podem ser levados aos tribunais. A civil law não utiliza tanto precedentes como a common law, e o papel do juiz se resume a estabelecer e revisar os fatos do caso em questão e tomar uma decisão baseada no código legal aplicável (BERKELEY LAW, 19[--]).

Podemos perceber essa diferença na forma pela qual os EUA e a UE abordam a questão da privacidade digital. Enquanto os EUA possuem alguns estatutos, como o Privacy Act, as práticas legais relativas ao assunto são majoritariamente determinadas através das decisões de casos como *Smith v. Maryland*, mencionado anteriormente. Além disso, a baixa regulação do tema é compatível com a baixa codificação característica do sistema de *common law*. Já na União Europeia, a privacidade digital é altamente regulada, algo condizente com o alto nível de codificação característico da *civil law* (KIRTLEY, 1999).

Ademais, a estrutura constitucional dos Estados Unidos, que inclui a divisão dos três poderes e a atribuição de autoridade significativa aos estados da federação, enseja um governo federal pouco atuante. Embora a União Europeia seja composta de diferentes Estados nacionais, o continente como um todo tende a encarar com seriedade a privacidade como um direito humano fundamental, o que facilita a criação de legislação abrangente para o bloco, sem grande resistência ao princípio por trás da legislação proposta (KIRTLEY, 1999).

Ainda assim, a diferença entre sistemas jurídicos não é o único fator atuante. Considerações culturais também devem ser analisadas. No caso da União Europeia, o passado do continente, com regimes fascistas e totalitários, é claramente um fator contribuinte para uma visão mais rígida de seus legisladores e cidadãos sobre a privacidade de dados. Os Estados Unidos, por sua vez, não possuem um passado recente com regimes dessa natureza. Além disso, existe a percepção de que a tradição de inovação tecnológica presente no país norte-americano é consequência de uma diversidade de fatores, que incluem a ausência de regulação dominante do governo e a permissibilidade de práticas do setor privado, a não ser que estas sejam diretamente proibidas pela legislação vigente (WEISS; ARCHICK, 2016).

CONCLUSÃO

Ao longo deste trabalho, exploramos o direito humano à privacidade, os mecanismos tecnológicos atuais que desafiam a preservação desse direito no meio digital e duas abordagens diferentes, tanto em termos legais quanto culturais, à regulamentação desse direito no meio digital. Em face do que foi exposto ao longo desta monografia, emergem algumas conclusões.

A primeira é relativa aos desafios à manutenção do direito natural do homem à privacidade na era do Big Data. Instrumentos relativos à coleção, armazenamento e processamento de dados online não vão desaparecer. Pelo contrário: a tendência é que a "identidade digital" de indivíduos se torne cada vez mais integrada e interconectada, em busca de experiências ainda mais personalizadas, o que, como vimos no Capítulo 2, tanto viabiliza quanto estimula a criação e a agregação de bases de dados. Como exposto anteriormente, é pouco realista esperar que indivíduos abram mão do uso destas tecnologias em prol da privacidade. É ainda menos realista que esperemos que indivíduos abram mão de conveniências modernas – sejam elas aplicativos como o Google Maps, mídias sociais como o Facebook ou comércio online – sob o argumento de potenciais danos futuros à coletividade.

Sendo assim, o caminho à frente para preservar o direito humano à privacidade no meio digital deve envolver a regulamentação – o que não significa necessariamente a proibição – de atividades relativas a dados de usuários. Nesse caso, a exposição feita no Capítulo 3 dos sistemas legais dos Estados Unidos e da União Europeia, com seus respectivos méritos e deficiências, nos deixa algumas lições.

É evidente que a União Europeia está muito à frente dos Estados Unidos no caminho para a regulamentação da privacidade de dados. Isso é verdade tanto em relação ao respeito do bloco pelo princípio fundamental que guia a legislação – a visão de que a privacidade é um direito fundamental do ser humano e deve ser preservada em todos os meios possíveis – quanto em relação a existência de um corpo legislativo extenso e abrangente que diz respeito a privacidade de dados especificamente. Como vimos no Capítulo 3, isso não significa que a legislação europeia sobre o assunto seja infalível ou ideal; no entanto, sua mera existência cria um embasamento legal e filosófico para a busca da preservação da privacidade de dados de indivíduos, tanto como cidadãos em relação a seus governos quanto como consumidores em relação às empresas com as quais mantém relações comerciais.

No entanto, a União Europeia e suas propostas de legislação sobre a privacidade de dados enfrentam um problema comum à tentativa de legislar atividades no meio tecnológico:

a corrida contra a inovação. Como vimos no Capítulo 2, os mecanismos de coleta, armazenamento e processamento de dados são inúmeros, e a tendência é que continuem a evoluir. Legislações altamente específicas sobre tais atividades inevitavelmente se tornarão desatualizadas, tal qual a Diretiva de Proteção de Dados europeia que exploramos no Capítulo 3. Como é possível regulamentar de forma específica o processamento de dados de indivíduos, e ao mesmo tempo manter-se à frente de mudanças nos mecanismos que buscamos regulamentar?

Nesse aspecto, existe algum mérito na abordagem norte-americana da questão. Embora a legislação americana – ou ausência dela – deixe muito a desejar na área de privacidade de dados, os Estados Unidos possuem o benefício de uma agência reguladora forte, representada pela Comissão Federal de Comércio (FTC). A privacidade digital certamente não é a única função da FTC, e tampouco é seu propósito principal. No entanto, observamos no Capítulo 2 que a atuação da FTC nos EUA nesta área tem levado diversas companhias ao ajuste de suas políticas e práticas de privacidade de dados. Embora o FTC não possua embasamento legal específico à privacidade de dados para sua atuação, a abordagem litigiosa da Comissão dá a ela um maior grau de flexibilidade em sua luta contra práticas danosas à privacidade de dados. Não podemos fazer nada além de especular sobre como a atuação da FTC se daria caso a mesma possuísse um conjunto de leis mais específicos à privacidade digital para dar base à sua atuação, mas podemos imaginar que os resultados seriam positivos.

Dessa forma, podemos concluir que, em nível nacional, uma combinação de legislação abrangente relativa à privacidade de dados e de agências reguladoras fortes e atuantes seria benéfica para a preservação da privacidade de dados. No entanto, o direito à privacidade no meio digital só estará completamente garantido uma vez que esforços internacionais sejam feitos para harmonizar as legislações domésticas relativas ao assunto e a proteção garantida pelas mesmas aos dados de indivíduos.

Observamos, no capítulo 2, que não existem fronteiras para o processamento de dados. De que serviu a legislação europeia ao cidadão austríaco que teve seus dados processados de forma incompatível com a mesma nos Estados Unidos? Mecanismos de transmissão internacional de dados como os Princípios Porto Seguro e o Escudo de Privacidade certamente têm seu valor; no entanto, seu escopo é limitado principalmente pela complexidade inerente à garantia da aplicação de leis em âmbito internacional. Instrumentos do comércio internacional como as Regras Corporativas Vinculativas (BCRs) também são úteis e talvez representem uma forma viável de incorporar melhores práticas à atuação de

empresas na área, mas sua adesão é voluntária e limitada ao setor privado, e seria no mínimo inadequado posicionar as forças de mercado como a linha de frente na proteção a um direito humano tão essencial quanto a privacidade. Como na maioria das discussões relativas à harmonização de leis entre países, não existe uma resposta fácil para esta questão.

Acima de tudo, é importante educar indivíduos sobre a privacidade digital e sua importância, pois apenas assim se garante o incentivo para que governos e empresas mantenham a preocupação em pauta. No Brasil, muito embora leis como o Marco Civil da Internet – cuja abordagem relativa à privacidade digital merece ser explorada no futuro – estejam em vigor, a questão da privacidade de dados apenas recentemente começou a ser explorada pelo público geral, graças a casos como o bloqueio do aplicativo Whatsapp, mencionado no capítulo 2. Elevar o nível de informação da população para garantir que esse direito seja levado a sério pelo governo e por empresas privadas é essencial.

A privacidade, como mencionamos no Capítulo 1, é um direito humano que viabiliza outros direitos humanos, e por isso sua importância jamais deve ser minimizada. Como ficou claro ao longo deste trabalho, o desafio de traduzir o direito humano à privacidade para o meio digital é imenso, e o caminho longo; no entanto, esse caminho deve ser trilhado com urgência, para garantir que, no futuro, o direito humano à privacidade – e à liberdade de expressão, de opinião, entre tantos outros – seja respeitado, independentemente das tecnologias existentes.

REFERÊNCIAS

ALTMAN, Irwin. Privacy Regulation: Culturally Universal or Culturally Specific?. **Journal of Social Issues**, Hoboken, NJ, v. 33, n. 3, p. 66–84, 1977.

AMAZON, Inc. **Amazon Privacy Notice**, [20--]. Disponível em: <https://www.amazon.com/gp/help/customer/display.html?nodeId=468496>. Acesso em: 01 set. 2016.

AMOORE, Louise; DE GOEDE, Marieke. Governance, risk and dataveillance in the war on terror. **Crime, law and social change**, The Netherlands, v. 43, n. 2-3, p. 149-173, 2005.

ANDRADE, Norbert N. Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; LEENES, Ronald (Ed.). **Computers, Privacy and Data Protection**: an Element of Choice. Dordrecht, Heidelberg, London, New York: Springer Science & Business Media, 2011, p. 65-97.

APPLE Inc. **Privacy**, [20--]. Disponível em: <http://www.apple.com/privacy/>. Acesso em: 01 set. 2016.

APPLE Inc. **Privacy Policy**, 2016. Disponível em: <http://www.apple.com/privacy/privacy-policy/>. Acesso em: 01 set. 2016.

ASSOCIATION OF SOUTHEAST ASIAN NATIONS. **ASEAN Human Rights Declaration**, de 20 nov 2012. Disponível em: < http://www.refworld.org/cgi-bin/texis/vtx/rwmain?page=search&docid=50c9fea82&skip=0&query=ASEAN Human Rights Declaration >. Acesso em: 25 jul. 2016.

BALLVE, Marcelo. Facebook says its new focuses are personalized content and spreading the internet. **Business Insider**, New York, 30 Jan 2014. Disponível em: <http://www.businessinsider.com/in-2014-facebook-says-it-will-focus-on-personalized-content-and-spreading-the-internet-2014-1>. Acesso em: 15 ago. 2016.

BANKS, David L.; SAID, Yasmin H. Data mining in electronic commerce. **Statistical Science**, Hayward, v. 21, n. 2, p. 234-246, 2006.

BASU, Subhajit. Privacy protection: a tale of two cultures. **Masaryk UJL & Tech**., Brno, v. 6, n.1, p. 1-34, 2012.

BBC NEWS. Q&A: how the UK adopts EU laws. **BBC News**. Londres, 21 jul 2009. Disponível em: <http://news.bbc.co.uk/2/hi/europe/8160808.stm>. Acesso em: 21 ago. 2016.

BELLINHO, Lilith. **Uma evolução histórica dos direitos humanos**, 2013. Disponível em: <http://www.unibrasil.com.br/arquivos/direito/20092/lilith-abrantes-bellinho.pdf>. Acesso em: 24 jul. 2016.

BEN-SHAHAR, Omri; SCHNEIDER, Carl E. The failure of mandated disclosure. **University of Pennsylvania Law Review**, Philadephia, v. 159, n. 3, p. 647-749, 2011.

BERKELEY LAW. The common law and civil law traditions, 19[--]. Disponível em: <https://www.law.berkeley.edu/library/robbins/pdf/CommonLawCivilLawTraditions.pdf>. Acesso em: 1 out. 2016.

BERLIN, Isaiah. **Four Essays on Liberty**. London, New York: Oxford University Press, 1969.

BERMAN, Jerry J.; GOLDMAN, Janlori. A Federal Right of Information Privacy: The Need for Reform. **Benton Foundation**, Washington, D.C., 1989.

BIRNHACK, Michael D. The EU data protection directive: an engine of a global regime. **Computer Law & Security Review**, Amsterdam, v. 24, n. 6, p. 508-520, 2008.

BLAKE, Ralph Mason. On natural rights**. International Journal of Ethics**, Philadelphia, v. 36, n. 1, p. 86-96, 1925.

BLOUSTEIN, Edward J. Privacy as an aspect of human dignity: An answer to Dean Prosser. **New York University Law Review**, New York, v. 39, p. 962, 1964.

BLUME, Peter. The myths pertaining to the proposed General Data Protection Regulation. **International Data Privacy Law**, Oxford, v. 4, n. 4, 2014.

BRIN, David. **The transparent society**: Will technology force us to choose between privacy and freedom?. New York: Basic Books, 1999.

CHIU, Lori. Drawing the Line Between Competing Interests: Strengthening Online Data Privacy Protection in an Increasingly Networked World. **San Diego International Law Journal**, San Diego, v. 14, p. 281-321, 2013.

CHOI, Hyunyoung; VARIAN, Hal. Predicting the present with Google Trends. **Economic Record**, Oxford v. 88, n. s1, p. 2-9, 2012.

CLARKE, Roger. Dataveillance by Governments: the technique of computer matching. **Information Technology & People**, Bradford, v. 7, n. 2, p. 46-85, 1994.

_____. Information technology and dataveillance. **Communications of the ACM**, New York, v. 31, n. 5, p. 498-512, 1988.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Convenção americana sobre direitos humanos**, de 22 de novembro de 1969. Disponível em: <https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm>. Acesso em: 25 jul. 2016.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Declaração americana sobre direitos e deveres do homem**. Abril 1948. Disponível em: <https://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm>. Acesso em: 25 jul. 2016.

CONNOLLY, Chris. **The US Safe Harbor – Fact or Fiction?**, 2008. Disponível em: <http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf>. Acesso em: 13 out. 2016.

DAVIS, Frederick. What Do We Mean by Right to Privacy. **South Dakota Law Review**, Vermillion, v. 4, p. 1, 1959.

DE HERT, Paul; PAPAKONSTANTINOU, Vagelis. The new General Data Protection Regulation: Still a sound system for the protection of individuals**? Computer Law & Security Review**, Amsterdam, v. 32, n. 2, p. 179-194, 2016.

DEBUSSERÉ, Frederic. The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster? **International Journal of Law and Information Technology**, Oxford, v. 13, n. 1, p. 70-97, 2005.

DECEW, Judith Wagner. **In pursuit of privacy**: Law, ethics, and the rise of technology. Ithaca, London: Cornell University Press, 1997.

_____. Privacy. In: ZALTA, Edward (Ed.) **The Stanford Encyclopedia of Philosophy** (Spring 2015 Edition), 2015. Disponível em: <http://plato.stanford.edu/archives/spr2015/entries/privacy/>. Acesso em 10 Mar 2016.

DIGGELMANN, Oliver; CLEIS, Maria N. How the right to privacy became a Human Right. **Human Rights Law Review**, Nottingham, p. 441-458, 2014.

DLA PIPER. **EU General Data Protection – Key Changes**, [2016?]. Disponível em: <https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/>. Acesso em: 07 set. 2016.

ELECTRONIC PRIVACY INFORMATION CENTER. **Council of Europe Privacy Convention**, [20--]b. Disponível em: < https://epic.org/privacy/intl/coeconvention/>. Acesso em: 29 ago. 2016.

ELECTRONIC PRIVACY INFORMATION CENTER. **USA Patriot Act**, [20--]a. Disponível em: <https://epic.org/privacy/terrorism/usapatriot/>. Acesso em: 23 ago. 2016.

ELGESEM, Dag. The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. **Ethics and Information Technology,** Dordrecht, v. 1, n. 4, p. 283-293, 1999.

ESTADOS UNIDOS. Corte de Recursos dos Estados Unidos para o Quarto Circuito=United States Court of Appeals for the Fourth Circuit. United States v. Graham. **12-4649**. Maryland, USA, 23 mar 2016a. Disponível em: < http://www.ca4.uscourts.gov/Opinions/Published/124659A.P.pdf>. Acesso em: 17 set. 2016
.
ESTADOS UNIDOS. Department of Justice. **Overview of the Privacy Act**, 2015b. Disponível em: < https://www.justice.gov/opcl/file/793026/download>. Acesso em: 21 ago. 2016.

ESTADOS UNIDOS. Department of Justice. **Privacy Act of 1974**, 2015a. Disponível em: https://www.justice.gov/opcl/privacy-act-1974. Acesso em: 17 set. 2016.

ESTADOS UNIDOS. Department of Commerce. **US-EU SAFE HARBOR FRAMEWORK: A GUIDE TO SELF-CERTIFICATION,** 20[--]a. Disponível em: <http://www.trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf>. Acesso em: 13 set. 2016.

ESTADOS UNIDOS. **Federal Trade Commission Act**, 1914. Disponível em: <http://legcounsel.house.gov/Comps/Federal Trade Commission Act.pdf>. Acesso em: 20 ago. 2016.

ESTADOS UNIDOS. Federal Commerce Commission. **Notice of Proposed Rulemaking**: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 2016b. Disponível em: < https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf>. Acesso em: 20 set. 2016.

ESTADOS UNIDOS. Federal Trade Commission. **In the Matter of Facebook, Inc**, 2012a. Disponível em: <https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc>. Acesso em: 20 set. 2016.

ESTADOS UNIDOS. Federal Trade Commission. **Privacy & Data Security Update**, 2015c. Disponível em: <https://www.ftc.gov/reports/privacy-data-security-update-2015>. Acesso em: 21 ago. 2016.

ESTADOS UNIDOS. Federal Trade Commission. **Protecting Consumer Privacy in an Era of Rapid Change,** 2012b. Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>. Acesso em: 20 set. 2016.

ESTADOS UNIDOS. Federal Trade Commission. **Self-Regulatory Principles for Online Behavioral Advertising**, 2009. Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>. Acesso em: 20 set. 2016.

ESTADOS UNIDOS. **H.R. 3162 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism**, de 26 de outubro de 2001. Disponível em: <https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf>. Acesso em: 19 set. 2016.

ESTADOS UNIDOS. **Public Law 100-503, 100th Congress**, de 18 de outubro de 1988. Dá nova redação ao Título 5, parágrafo 552a, do United States Code. Disponível em: <https://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg2507.pdf>. Acesso em: 17 set. 2016.

ESTADOS UNIDOS. **Public Law 109-178 USA PATRIOT Act Additional Reauthorizing Amendments Act Of 2006**, de 09 de março de 2006. Disponível em:

<https://www.gpo.gov/fdsys/pkg/PLAW-109publ178/pdf/PLAW-109publ178.pdf>. Acesso em: 19 set. 2016.

ESTADOS UNIDOS. **Public Law 30-351 Omnibus Crime Control and Safe Streets Act of 1968**, de 19 de junho de 1968. Dá nova redação ao Título 42 do United States Code, alterando e inserindo parágrafos. Disponível em: <https://www.justice.gov/crt/omnibus-crime-control-and-safe-streets-act-1968-42-usc-3789d>. Acesso em: 18 set. 2016.

ESTADOS UNIDOS. **Public Law 99-508 Electronic Communications Privacy Act of 1986**, de 21 de outubro de 1986. Disponível em: <https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf>. Acesso em: 18 set. 2016.

ESTADOS UNIDOS. **S. 1732 - Privacy Act Modernization for the Information Age Act of 2011**, 112th Congress, de 18 de outubro de 2011. Proposta de emenda ao Título 5, parágrafo 552a, do United States Code. Disponível em: <https://www.congress.gov/bill/112th-congress/senate-bill/1732/text>. Acesso em: 18 set. 2016.

ESTADOS UNIDOS. Supreme Court of the United States. City of Ontario, California, et al v. Quon et al. **No. 08–1332**. Washington, D.C., 19 de abril 2010a. Disponível em: <https://www.supremecourt.gov/opinions/09pdf/08-1332.pdf>. Acesso em: 16 set. 2016.

ESTADOS UNIDOS. Supreme Court of the United States., Smith v. Maryland. **No.78-5374**. Washington, D.C., 28 de Março de 1979. Disponível em: <http://caselaw.findlaw.com/us-supreme-court/442/735.html>. Acesso em: 16 set. 2016.

ESTADOS UNIDOS. **Title 5, United States Code, paragraph 552a**, de 31 de dezembro de 1974. Disponível em: <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf>. Acesso em: 17 set. 2016.

ESTADOS UNIDOS. United States District Court, California CD. Buckley H. Crispin, v. Christian Audigier, Inc. et al. **CV 09-09509 MMM**. California 26 may 2010b. Disponível em: <https://scholar.google.com/scholar_case?case=12835592234641988839&hl=en&as_sdt=6&as_vis=1&oi=scholarr>. Acesso em: 18 set. 2016.

EVANS, David S. The online advertising industry: Economics, evolution, and privacy. **The journal of economic perspectives**, Nashville, v. 23, n. 3, p. 37-60, 2009.

FACEBOOK. **Data Policy**, 2016. Disponível em: <https://www.facebook.com/full_data_use_policy>. Acesso em: 29 ago. 2016.

FOLHA DE SÃO PAULO. Whatsapp é bloqueado no Brasil após decisão judicial. **Folha de São Paulo**, São Paulo, 19 Jul 2016. Disponível em: <http://www1.folha.uol.com.br/mercado/2016/07/1793221-whatsapp-comeca-a-ser-bloqueado-no-brasil-apos-decisao-judicial.shtml>. Acesso em 27 jul. 2016.

FORDE, Steven. **John Locke and the Natural Law and the Natural Rights Tradition**, 2011. Disponível em: <http://www.leffa.pro.br/textos/abnt.htm - 5.16>. Acesso em 4 de fev. 2016.

FOUCAULT, Michel (1975). **Discipline and Punish**: The Birth of the Prison. 2 ed. New York: Vintage Books, 1995.

FRIED, Charles. **An anatomy of values: problems of personal and social choice**. Cambridge: Harvard University Press, 1970.

_____. Privacy: A Moral Analysis. In: SCHOEMAN, Ferdinand (Ed.). **Philosophical Dimensions of Privacy:** An Anthology. Cambridge, UK: Cambridge University Press, 1984.

FROOMKIN, A. Michael. The death of privacy?. **Stanford Law Review**, Stanford, v. 52, n. 5, p. 1461-1543, 2000.

GAVISON, Ruth. Privacy and the Limits of Law. **The Yale Law Journal**, New Haven, v. 89, n. 3, p. 421-471, 1980.

GELLER, Eric. Federal appeals court says Fourth Amendment doesn't protect phone location data. **The Daily Dot**, 31 Mai 2016. Disponível em: <http://www.dailydot.com/layer8/phone-location-data-privacy-no-warrant-fourth-circuit-ruling/>. Acesso em: 15 set. 2016.

GELLMAN, Barton; POITRAS, Laura. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. **Washington Post**, Washington, D.C., 07 Jun 2013. Disponível em: <https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>. Acesso em: 18 ago. 2016.

GELLMAN, Robert. Does privacy law work?. In: AGRE, Philip E.; ROTENBERG, Marc (Ed.). **Technology and Privacy**: The New Landscape. MIT Press, 1997. p. 193-218.

GERSTEIN, Robert S. Intimacy and privacy. **Ethics**, Chicago, v. 89, n. 1, p. 76-81, 1978.

GOLDFARB, Avi; TUCKER, Catherine. Privacy and innovation. **Innovation Policy and the Economy**, Cambridge, v. 12, n. 1, p. 65-89, 2012.

GOOGLE, Inc. **Privacy Policy**, 2016. Disponível em: <https://www.google.com/policies/privacy/>. Acesso em: 29 ago. 2016.

GREENLEAF, Graham. The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108. **International Data Privacy Law**, Oxford, v. 2, n. 2, p. 2011-39, 2012.

GREENWALD, Glenn; MACASKILL, Ewen. NSA PRISM Program tapsin to user data of Apple, Google and others. **The Guardian**, 7 de junho de 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 6 set. 2016.

GUNDALINI, Bruno e TOMIZAWA, Guilherme. Mecanismo Disciplinar de Foucault e o Panóptico de Bentham na Era da Informação. **ANIMA: Revista Eletrônica do Curso de Direito das Faculdades OPET**. Curitiba, Brasil. Ano IV, nº 9, jan/jun, 2013.

HEFFETZ, Ori; LIGETT, Katrina. Privacy and data-based research. **The Journal of Economic Perspectives**, Nashville, v. 28, n. 2, p. 75-98, 2014.

HOBOKEN, J. et al. Cloud computing in higher education and research institutions and the USA Patriot Act. **Institute for Information Law**, Amsterdam, Nov 2012.

HOGAN, Mél; SHEPHERD, Tamara. Information ownership and materiality in an age of big data surveillance. **Journal of Information Policy**, University Park, v. 5, p. 6-31, 2015.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Recenseamento do Brasil em 1872**, 20[--]. Disponível em: <http://biblioteca.ibge.gov.br/biblioteca-catalogo?view=detalhes&id=225477>. Acesso em: 10 out. 2016.

JOYCE, Daniel. Privacy in the Digital Era: Human Rights Online. **Melbourne Journal of International Law**, Melbourne, v. 16, n. 1, p. 270-285, 2015.

KEARNEY, Michael. Legal Trends in Protecting Persona Information. **SciTech Lawyer**, Chicago, v. 7, n. 4, p. 20-22, 2011.

KIERKEGAARD, Sylvia et al. 30 years on–The review of the Council of Europe Data Protection Convention 108. **Computer Law & Security Review**, Amsterdam, v. 27, n. 3, p. 223-231, 2011.

KIRTLEY, Jane E. Is implementing the EU data protection directive in the United States irreconcilable with the first amendment?. **Government Information Quarterly**, New York, v. 16, n. 2, p. 87-91, 1999.

KULESZA, Joanna. Walled Gardens of Privacy or Binding Corporate Rules: A Critical Look at International Protection of Online Privacy. **UALR Law Review**, Little Rock, v. 34, n. 4, p. 747-765, 2011.

LEAGUE OF ARAB STATES. **Arab Charter on Human Rights**, de 15 set 1994. Disponível em: <http://www.refworld.org/docid/3ae6b38540.html>. Acesso em: 25 jul. 2016.

LOMAS, Natasha. EU-US Privacy Shield now officially adopted but criticisms linger. **TechCrunch**, 12 Jul 2016. Disponível em: <https://techcrunch.com/2016/07/12/eu-us-privacy-shield-now-officially-adopted-but-criticisms-linger/>.Acesso em 01 out. 2016.

LYON, David. An electronic panopticon? A sociological critique of surveillance theory. **The Sociological Review**, London, v. 41, n. 4, p. 653-678, 1993.

_____. Surveillance, Snowden, and big data: Capacities, consequences, critique. **Big Data & Society**, London, v. 1, n. 2, p. 1-13, 2014.

MARGULIS, Stephen T. Three theories of privacy: An overview. In: TREPTE, Sabrina; REINECKE, Leonard (Ed.). **Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web**. Dordrecht, Heidelberg, London, New York: Springer Science & Business Media, 2011, p. 9-17.

MCLAUGHIN, Jenna. Appeals Court Delivers Devastating Blow to Cellphone-Privacy Advocates. **The Intercept**, 31 Mai 2016. Disponível em: <https://theintercept.com/2016/05/31/appeals-court-delivers-devastating-blow-to-cell-phone-privacy-advocates/>. Acesso em: 01 set. 2016.

MEYER, David. Watchdog releases own version of data regulation. **Politico**, 27 Jul 2015. Disponível em: <http://www.politico.eu/article/watchdog-releases-data-protection-regulation-buttarelli-edps/>.Acesso em: 28 set. 2016.

MOOR, James H. The ethics of privacy protection**. Library Trends**, Urbana, v. 39, n. 1/2, p. 69-82, 1990.

_____. Towards a theory of privacy in the information age. **Computers and Society**, New York, v. 27, n. 3, p. 27-32, 1997.

MOORE, Adam. **Privacy Rights**: Moral and Legal Foundations. Kindle ed. University Park, Pennsylvania: The Pennsylvania State University Press, 1965.

MUNDIE, Craig. Privacy Pragmatism; Focus on Data Use, Not Data Collection. **Foreign Affairs**, New York, v. 93, n. 2, p. 28-38, 2014.

NATIONAL INFORMATION STANDARDS ORGANIZATION (2004). **Understanding metadata**. Disponível em: <http://www.niso.org/publications/press/UnderstandingMetadata.pdf>. Acesso em: 02 mar. 2016.

NISSENBAUM, Helen. Privacy as contextual integrity. **Washington Law Review**, Seattle, v. 79, p. 119-157, 2004.

_____. **Privacy in context**: Technology, policy, and the integrity of social life. Stanford, California: Stanford University Press, 2009.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. United Nations Humans Rights Office of the High Commissioner. **The right to privacy in the digital age**, 2016. Disponível em: <http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>. Acesso em: 15 set. 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Universal Declaration of Human Rights**. 10 dezembro 1948. Disponível em: <http://www.un.org/en/universal-declaration-human-rights/>. Acesso em: 24 jul. 2016.

ORITO, Yohko. The counter-control revolution:“silent control” of individuals through dataveillance systems. **Journal of Information, Communication and Ethics in Society**, Bingley, v. 9, n. 1, p. 5-19, 2011.

PAGDEN, Anthony. Human rights, natural rights, and Europe’s imperial legacy. **Political Theory**, Thousand Oaks, v. 31, n. 2, p. 171-199, 2003.

PAIANO, Daniela Braga; FURLAN, Alessandra Cristina. Direitos Humanos Fundamentais e Dignidade da Pessoa Humana: Evolução e Efetividade no Estado Democrático De Direito. **ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498**, v. 4, n. 4, 2009.

PARENT, William A. Recent work on the concept of privacy. **American Philosophical Quarterly**, Pittsburgh, v. 20, n. 4, p. 341-355, 1983.

PETERSON, Andrea. Online Privacy Advocates Applaud Protections in Cybersecurity Executive Order. **Think Progress**, 13 Fev 2013. Disponível em: <https://thinkprogress.org/online-privacy-advocates-applaud-protections-in-cybersecurity-executive-order-b4c703abfcce - .lgvlo9l8p>. Acesso em: 16 set. 2016.

PISA, Pedro. O que é IP? **TechTudo**, 07 mai 2012. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/05/o-que-e-ip.html>. Acesso em: 10 out. 2016.

PROSSER, William. Privacy. **California Law Review**, Berkeley, v. 48, n. 3, p. 383–423, 1960.

PUC-RIO. **A dignidade da pessoa humana**, 20[--]. Disponível em: <http://www.maxwell.vrac.puc-rio.br/13488/13488_3.PDF>. Acesso em: 27 mai. 2016.

RACHELS, James. Why privacy is important. **Philosophy & Public Affairs**, Princeton, v. 4, n. 4, p. 323-333, 1975.

RENDLEMAN, John. Customer data means money. **Information Week**, 16 Ago 2001. Disponível em: <http://www.informationweek.com/customer-data-means-money/d/d-id/1011498?>. Acesso em: 15 ago. 2016.

ROSSI, Marina; ALESSI, Gil. Polícia Federal prende 10 suspeitos de planejar ação terrorista na Olimpíada. **El País**, São Paulo, 21 Jul 2016. Disponível em: <http://brasil.elpais.com/brasil/2016/07/21/politica/1469112537_834424.html>. Acesso em: 5 ago. 2016.

ROWE, Heather. Data transfer to third countries: Transfers of personal data to third countries: the role of binding corporate rules. **Computer Law & Security Review**, Amsterdam, v. 19, n. 6, p. 490-496, 2003.

RULE, James B. **Privacy in peril**: How we are sacrificing a fundamental right in exchange for security and convenience. New York: Oxford University Press, 2007.

SAXBY, Stephen. Data protection directive gets its first progress report. **Computer Law & Security Review**, Amsterdam, v. 19, n. 4, p. 271, 2003.

SCHOEMAN, Ferdinand. Privacy: philosophical dimensions. **American Philosophical Quarterly**, Pittsburgh, v. 21, n. 3, p. 199-213, 1984.

SIMONITE, Tom. What Facebook Knows. **Technology Review**, Cambridge, v. 115, n. 4, p. 42-48, 2012.

SOLOVE, Daniel J. Conceptualizing privacy. **California Law Review**, Berkeley, v. 90, n. 4, p. 1087-1155, 2002.

SOLOVE, Daniel; HOOFNAGLE, Chris. Model Regime for Privacy Protection, A. **University of Illinois Law Review**, Champaign, v. 357, n. 2, 2006.

SOLOVE, Daniel. Privacy Self-Management and the Consent Dilemma. **Harvard Law Review**, Cambridge, v. 126, n. 3, p. 1880-1903, 2013.

SOTTO, Lisa; HYDAK, Christopher. The EU-US Privacy Shield: a How to Guide. **Hunton & Williams**, 19 de julho de 2016. Disponível em: <https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/07/EU-US_Privacy_Shield_A_How-To_Guide.pdf>. Acesso em: 14 set. 2016.

STEIN, Joel. Data Mining: How Companies Now Know Everything About You. **Time Magazine**, New York City, 10 Mar 2011. Disponível em: <http://content.time.com/time/magazine/article/0,9171,2058205,00.html>. Acesso em: 20 ago. 2016.

STEPANOVIC, Ivana. Modern technology and challenges to protection of the right to privacy. **Annals FLB – Belgrade Law Review**, Belgrade, Year LXII, n. 3, p. 167-178, 2014.

STOEVA, Elitsa. The Data Retention Directive and the right to privacy. In: **ERA Forum.** Springer Berlin Heidelberg, 2014. p. 575-592.

STRUB, Harry. The theory of Panoptical control: Bentham's Panopticon and Orwell's Nineteen Eighty-Four. **Journal of the History of the Behavioral Sciences**, Hoboken, v. 25, n. 1, p. 40-59, 1989.

TAVANI, Herman T. Philosophical theories of privacy: Implications for an adequate online privacy policy. **Metaphilosophy**, Oxford, v. 38, n. 1, p. 1-22, 2007.

TAYLOR, Curtis R. Consumer privacy and the market for customer information. **RAND Journal of Economics**, Washington, D.C., v. 36, n. 4, p. 631-650, 2004.

THOMSON, Judith. The right to privacy. **Philosophy & Public Affairs**, Princeton, p. 295-314, 1975.

UNIÃO EUROPÉIA. **Carta dos Direitos Fundamentais da União Européia**, de 7 de dezembro de 2000 (2000c). Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acessado em: 13 ago. 2016.

UNIÃO EUROPÉIA. Council of Europe. **Chart of signatures and ratifications of Treaty 108**, 2016b. Disponível em: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures>. Acesso em: 13 ago. 2016.

UNIÃO EUROPÉIA. Council of Europe. **Convention for the Protection of Individuals with regard to Automatic Processing of Data**, de 28 de janeiro de 1981. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37>. Acesso em: 04 ago. 2016.

UNIÃO EUROPÉIA. Council of Europe. **European Convention on Human Rights,** de 4 de novembro de 1950. Disponível em: <http://www.echr.coe.int/Documents/Convention_ENG.pdf>. Acesso em: 25 jul. 2016.

UNIÃO EUROPÉIA. Corte de Justiça da União Européia. Maximillian Schrems v Data Protection Commissioner. **C-362/14**. Luxemburgo, 6 de outubro de 2015. Disponível em: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>. Acesso em: 14 set. 2016.

UNIÃO EUROPÉIA. European Commission. **First Report on the Implementation of the Data Protection Directive (95/46/EC),** 2003. Disponível em: <http://aei.pitt.edu/45392/1/COM_(2003)_265_final.pdf>. Acesso em: 04 set. 2016.

UNIÃO EUROPÉIA. European Commission. **List of companies for which the EU BCR cooperation procedure is closed**, 2016c. Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm>. Acesso em: 29 set. 2016.

UNIÃO EUROPÉIA. European Commission. **Model Contracts for the transfer of personal data to third countries**, (20[--]a).. Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm>. Acesso em: 23 set. 2016.

UNIÃO EUROPÉIA. European Commission. **Overview on Binding Corporate Rules**, (20[--]b). Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm>. Acesso em: 23 set. 2016.

UNIÃO EUROPÉIA. European Commission. **Trade: United States**, [2015?]. Disponível em: <http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/>. Acesso em: 09 set. 2016.

UNIÃO EUROPÉIA. European Commission. **European Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce**, de 26 de julho de 2000 (2000a). Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML>. Acesso em: 13 set. 2016.

UNIÃO EUROPÉIA. European Data Protection Supervisor. **Data Protection Legislation**, (20[--]c). Disponível em: <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA2>. Acesso em: 05 set. 2016.

UNIÃO EUROPÉIA. The European Parliament and the Council. **Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector**, de 12 de julho de 2002. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML>. Acesso em: 04 set. 2016.

UNIÃO EUROPÉIA. The European Parliament and the Council. **Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC**, de 15 de março de 2006. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>. Acesso em: 05 set. 2016.

UNIÃO EUROPÉIA. The European Parliament and the Council. **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data**, de 24 de outubro de 1995. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>. Acesso em: 03 set. 2016.

UNIÃO EUROPÉIA. The European Parliament and the Council. **Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data**, de 18 de dezembro de 2000 (2000b). Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF>. Acesso em: 04 set. 2016.

UNIÃO EUROPÉIA. The European Parliament and the Council. **Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**, de 27 de abril de 2016a. Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 07 set. 2016.

UNIVERSIDADE DE SÃO PAULO. Biblioteca de Direitos Humanos. **Constituição dos Estados Unidos da América – 1787**. Disponível em: <http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-à-criação-da-Sociedade-das-Nações-até-1919/constituicao-dos-estados-unidos-da-america-1787.html>. Acesso em: 16 set. 2016.

WALKER, Shaun; GRYTSENKO, Oksana. Text messages warn Ukraine protesters they are 'participants in mass riot'. **The Guardian**, Kiev, 21 Jan 2014. Disponível em: <https://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot>. Acesso em: 20 ago. 2016.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard law review**, Cambridge, p. 193-220, 1890.

WEISS, Martin A.; ARCHICK, Kristin. **US-EU Data Privacy**: From Safe Harbor to Privacy Shield. Congressional Research, 2016.

WESTIN, Alan. **Privacy and Freedom**. New York: Atheneum, 1967.

WITTE, Derek S. Privacy deleted: Is it too late to protect our privacy online. **Journal Of Internet Law**, New York, v. 18, n. 1, p. 1-28, 2014.

WONG, Rebecca. The Data Protection Directive 95/46/EC: Idealisms and realisms. International Review of Law, **Computers & Technology**, v. 26, n. 2-3, p. 229-244, 2012.

ZUBOFF, Shoshana. **In the age of the smart machine**: The future of work and power. Basic books, 1988.