



## TRATAMENTO DE DADOS PESSOAIS E A LEGISLAÇÃO BRASILEIRA FRENTE AO PROFILING E À DISCRIMINAÇÃO A PARTIR DAS NOVAS TECNOLOGIAS

Cinthia Obladen de Almendra Freitas\*

**Resumo:** Vive-se o universo digital e as TICs impõem a discussão sobre as novas tecnologias de tratamento de dados pessoais, apresentando tanto aspectos técnicos quanto jurídicos. Coube discutir os reflexos do tratamento de dados sob o enfoque do Direito, por meio da legislação pertinente, aqui incluídas as legislações sobre dados, como objeto de interesse ao legislador. A caracterização de perfil (*profiling*) e a discriminação são apresentadas como reflexos do tratamento de dados que permeiam o jurídico e a tecnologia. O artigo resulta de projeto de pesquisa e segue método dedutivo com caráter explicativo passando pelas fases de pesquisa exploratória e descritiva.

**Palavras-chave:** Direitos Fundamentais. Sociedades. Novas Tecnologias. Dados Pessoais. Perfilamento. Discriminação.

### COLLECTING AND PROCESSING PERSONAL DATA AND BRAZILIAN LEGISLATION FACED TO PROFILING AND DISCRIMINATION BASED ON NEW TECHNOLOGIES

**Abstract:** The digital universe is reality and the ICTs impose the discussion on the new technologies of treatment of personal data, presenting both technical and legal aspects. It was necessary to discuss the repercussion of data treatment under the law approach, through the relevant legislation, including legislation about personal data, being the data the object of interest to the legislator. The profiling and the discrimination are presented as reflections of the personal data treatment. The paper results from a research project and follows a deductive method with explanatory character passing through the phases of exploratory and descriptive research.

**Keywords:** Fundamental rights. Societies. New technologies. Personal data. Profiling. Discrimination.

---

\* Engenharia Civil pela Universidade Federal do Paraná (1985), Mestre em Engenharia Elétrica e Informática Industrial pela Universidade Tecnológica Federal do Paraná (1990) e Doutora em Informática pela Pontifícia Universidade Católica do Paraná (2001). Professora Titular da PUCPR (1985-atual) para os cursos de Direito (Fraudes e Crimes por Computador; Direito e Informática; Propriedade Intelectual; 2005-atual) e Ciência da Computação (1985-2015). Professora Permanente do Programa de Pós-Graduação (Mestrado/Doutorado) em Direito (PPGD) da PUCPR (2005-atual). Foi Professora Permanente do Programa de Pós-Graduação (Mestrado/Doutorado) em Informática (PPGIa) da mesma instituição (2001-2015). E-mail: cinthia@ppgia.pucpr.br



## INTRODUÇÃO

O volume de dados em formato digital gerado e armazenado vem crescendo exponencialmente com a evolução das Tecnologias de Informação e Comunicação (TIC) aplicadas nas mais diversas áreas e organizações. Gantz e Reinsel (2012, p. 01) estudaram o crescimento do volume de informações no planeta, apontando que de 2005 a 2020, o volume de dados digitais crescerá em um fator igual a 300, ou seja, passará de 130 hexabytes para 40.000 hexabytes ou 40 trilhões de gigabytes. Isto representa 5.200 gigabytes para cada homem, mulher ou criança em 2020.

Vive-se o “universo digital” tal qual denominado por Gantz e Reinsel (2012, p. 01), afirmando que de agora até 2020, o universo digital dobrará a cada 2 anos, lembrando que este universo compreende todo os dados digitais criados, replicados e consumidos, incluindo as imagens e vídeos em telefones celulares enviados ao YouTube, filmes digitais para TVs de alta definição, dados bancários em caixas automáticos, imagens de segurança, mensagens de voz veiculadas por linhas telefônicas digitais, e mensagens de texto (SMS ou WhatsApp).

Dados constituem um fator de grande interesse às organizações, possibilitando agilidade nos processos de busca e de recuperação de informações. Assim, a transformação de grandes volumes de dados textuais não estruturados em informação útil fornece elementos para a reorganização, avaliação, utilização, compartilhamento e armazenamento do conhecimento gerado a partir do conjunto bruto de dados.

As palavras de ordem da sociedade contemporânea são velocidade, mobilidade e acessibilidade. Não se pode imaginar um mundo sem a tecnologia, visto que ela está presente em todos os momentos, em todos os lugares. Fronteira, distância e informação são palavras que mudaram seus próprios significados nas últimas décadas, principalmente no século XXI.

Os dados pessoais podem ser capturados por meio de múltiplos dispositivos heterogêneos e os aplicativos seguem o usuário em movimento, ou seja, pode-se andar e falar ao celular, fotografar uma cena de interesse, postar em uma rede social e ainda indicar a localização, com latitude e longitude, da cena. Neste ambiente digital os dispositivos interagem entre si, por meio das mais variadas *interfaces* (*Universal Serial Bus* - USB, Infravermelho e *Bluetooth*) e, além disto, é importante salientar que o ambiente troca informações com os dispositivos e vice-versa, sendo que a aplicação responde às mudanças no ambiente.

Eis aqui o paradigma que norteia o desenvolvimento de um meio ambiente digital que congrega ubiquidade, pervasividade e inteligência, sendo o elemento de ligação formado pelo



conjunto de dados veiculados, capturados, tratados e armazenados. Na visão de Schwab (2016) vive-se a “Quarta Revolução Industrial”, uma vez que três razões sustentam tal revolução: velocidade, amplitude e profundidade e, por último, impacto sistêmico. O autor explica que as mudanças estão ocorrendo em um ritmo exponencial e não linear, como tradicionalmente se busca descrever e entender a tecnologia. Além disto, a combinação de várias tecnologias (multiplataformas, multitarefas, entre outros) e a transformação de sistemas inteiros (desde países até empresas) “não está modificando apenas o ‘o que’ e o ‘como’ fazemos as coisas, mas também ‘quem’ somos” (SCHWAB, 2016, p. 13).

É neste contexto de transformação que o tratamento de dados pessoais passa a assumir vital importância na vida dos usuários da Internet. Neste sentido, o artigo discute a legislação brasileira sob a ótica do tratamento de dados pessoais, apresentado a caracterização de perfil (*profiling*) e discriminação como reflexos no Direito destas novas tecnologias.

O artigo é resultado de projeto de pesquisa e segue método dedutivo para relacionar o tratamento de dados pessoais e a legislação brasileira pertinente com os reflexos de caracterização de perfil (*profiling*) e, conseqüentemente, de discriminação a partir da aplicação de novas tecnologias de informação e comunicação. A pesquisa tem caráter explicativo, passando pelas fases da pesquisa exploratória e descritiva.

## **2. LEGISLAÇÃO BRASILEIRA E O TRATAMENTO DE DADOS PESSOAIS**

A análise ora realizada tem por base questões técnicas, visando avaliar como o legislador utilizou os seguintes termos: dado, informação, tratamento de dados, captura de dados; fazendo-se uma relação entre o que está na legislação brasileira e o que a área técnica de Informática tem por princípios.

Inicialmente, destaca-se que na Lei de Acesso à Informação encontra-se no art. 4º a definição de informação e de tratamento de dados, a saber (BRASIL, 2011):

I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

[...]

V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;



Observa-se na definição de informação a presença do trinômio: dado, informação e conhecimento; demonstrando a hierarquia de evolução de dado para informação e de informação para conhecimento. Observa-se também que a definição de informação menciona produção e transmissão, mas não explicita tratamento de dados e, sim, menciona processamento. Além disto, a definição considera informação como dados processados ou não, sendo esta questão abordada no item 3 deste capítulo.

Por outro lado, a lei traz a definição de tratamento de informação onde deveria ser tratamento de dados, visto que a base da informação é o conjunto de dados que pode ser tratado e/ou processado. Além disto, a definição não inclui o que se conhece na área de Informática, mais especificamente nas áreas de Gerência Eletrônica de Documentos (GED) e Gerência da Informação, como captura de dados. Na área de Informática, captura de dados é entendida como sendo (BUSINESS DICTIONARY, 2017):

Input of data, not as a direct result of data entry but instead as a result of performing a different but related activity. Barcode reader equipped supermarket checkout counters, for example, capture inventory related data while recording a sale.

Existem diferentes métodos para capturar dados de documentos não estruturados. De um modo geral, a captura de dados pode se dar de modo não automático, por meio da entrada de dados em aparatos tecnológicos, sendo que estes dados brutos podem ser obtidos ou coletados por uma organização ou empresa e, ainda, por meio de dispositivos externos, tais como: teclado, mouse, telas sensíveis ao toque (*touch screen*), mesas digitalizadoras, *scanners* (incluindo aqui os dispositivos de reconhecimento óticos de caracteres – OCR e o reconhecimento inteligente de caracteres – ICR), canetas óticas, dispositivos de entrada por voz, entre outros (LAUDON e LAUDON, 1999). Já a captura automática ocorre sem a intervenção humana, por exemplo, quando se utiliza a leitura do código de barras ou do QR-Code de um produto. Ou, ainda, quando se utiliza RFID (*Radio-Frequency IDentification*) que permite, por exemplo, passar e pagar um pedágio sem que se necessite parar, ou seja, o conhecido “sem parar”.

A Lei de Crimes Cibernéticos (BRASIL, 2012) não traz definições, mas especifica dispositivo informático “conectado ou não à rede de computadores” ampliando assim a abrangência da lei. Não há que se especificar qual o tipo, categoria, plataforma, sistema operacional ou formato do dispositivo, somente ressaltando que é informático já se tem a



aplicação necessária. Além disto, a lei de forma ainda abrangente, menciona no art. 2º, referente ao acréscimo no art. 154-A do Código Penal, “... obter, adulterar ou destruir dados ou informações sem autorização expressa”, fazendo alusão a dados e informações que estejam nos dispositivos informáticos que por ventura sejam invadidos. O legislador não apresentou conceitos e/ou definições de dados e informações, deixando a cargo do julgador constatar caso a caso, muitas vezes por meio de perícia digital, o que foi efetivamente violado.

O Marco Civil da Internet (BRASIL, 2014) menciona 23 (vinte e três) vezes a palavra ‘dados’, sendo que a Tabela 01 explicita a relação de artigos que tratam a referida terminologia. Observa-se a preocupação com os ‘dados pessoais’ (12) frente aos ‘dados cadastrais’ (1). No que tange ao tratamento, a legislação aplica de maneira genérica o termo ‘tratamento de dados’ (1) e de maneira específica o termo ‘tratamento de dados pessoais’ (1). Diferentemente da Lei de Acesso à Informação, no Marco Civil da Internet a preocupação recai sobre a coleta de dados pessoais, não se utilizando do termo captura de dados.

Tabela 01 – Uso da palavra “dados” no Marco Civil da Internet

<b>Palavra</b>	<b>Nº de vezes que é mencionado</b>	<b>Texto da lei</b>
Dados pessoais	12	art. 3º e inciso III art. 7º e incisos VII, VIII, IX e X art. 10º e § 1º art. 11º (2 vezes) art. 16º no inciso II
Pacotes de dados	3	art. 5º no inciso II art. 9º e § 3º
Coleta de dados pessoais	3	art. 7º no incisos VIII e IX art. 11º art. 11º no § 1º (coletados) art. 11º no § 3º (coleta)
Bases de dados	1	art. 4º no inciso IV
Dados cadastrais	1	art. 10º no § 3º
Dados coletados	1	art. 11º no § 1º
Tratamento de dados (somente)	1	art. 11º no § 3º
Tratamento de dados pessoais	1	art. 7º no inciso IX
Titular dos dados	1	art. 11º no inciso I
Dados e informações públicos	1	art. 24º no inciso VI
Centros de armazenamento, gerenciamento e disseminação de dados	1	art. 24º no inciso VII

Fonte: o autor, 2017.



Além disto, o Marco Civil da Internet (BRASIL, 2014) utiliza de maneira genérica o termo ‘pacote de dados’ para representar todo e qualquer tipo de conteúdo veiculado pela Internet, seja envio ou recebimento. Tecnicamente, deve-se esclarecer que pacote de dados é a fragmentação dos conteúdos utilizada pelos softwares e aplicativos para transmitir os conteúdos por meio da Internet. Entende-se por conteúdo, qualquer tipo de dado ou arquivo em formato de texto, voz, imagem, vídeo e som.

E, o Anteprojeto de Lei de Proteção de Dados Pessoais (Projeto de Lei Nº 5.276/2016). já carrega no próprio objetivo que “Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural”, destacando que o foco recai sobre dados pessoais, definidos no art. 5º, inciso I (BRASIL, 2016): “dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa”.

O PL Nº 5.276/2016 diferencia ainda dados pessoais de sensíveis (art. 5º, inciso III), de maneira a deixar claro que todo o tipo de dados que possa gerar discriminação, segregação ou outra forma de violência contra a pessoa, também estará sob a égide da legislação, inclusive dados referentes à saúde ou à vida sexual, bem como dados genéticos (BRASIL, 2016). O projeto de lei é abrangente e necessário frente às técnicas de tratamento de dados.

Em relação ao tratamento de dados, o projeto de lei define no art. 5º, inciso III, que (BRASIL, 2016):

tratamento: conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração;

Deste modo o projeto de lei não somente apresenta o que se entende por tratamento de dados, mas, também, esclarece os meios, quais sejam: comunicação, interconexão, transferência, difusão ou extração; o que torna a definição abrangente e atualizada em qualquer tempo. Novamente, o legislador optou pelo uso da palavra ‘coleta’ e não ‘captura’. O termo ‘coleta’ também é utilizado pelo Google e pelo Facebook em suas Políticas de Privacidade (GOOGLE, 2016) (FACEBOOK, 2016).



Além disto, no art. 3º, explicita-se que o tratamento tanto se refere às operações realizadas em território nacional (inciso I) quanto aos dados pessoais que tenham sido coletados em território nacional (inciso III), uma vez que o titular dos dados se encontre em território nacional no momento da coleta (art. 3º, § único) (BRASIL, 2016).

A autodeterminação informativa está inclusa no Projeto de Lei no art. 2º, inciso I, figurando como fundamento de proteção aos dados pessoais e ao respeito à privacidade (BRASIL, 2016). A autodeterminação informativa, de acordo com a definição dada pela Constituição Federal Alemã, é um direito de personalidade, que garante ao indivíduo o direito de controlar a emissão e utilização de seus dados pessoais (ALEMANHA, 1983). Por isso, a autodeterminação informativa está tão ligada à privacidade, retomando-se a definição dada por Westin (1968, p. 7), a saber: “*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others*”. Assim, a autodeterminação informativa de cada indivíduo é assegurada pelo conceito de direitos de propriedade sobre seus dados pessoais.

Sobre o tratamento de dados pessoais, o projeto de lei prevê corretamente em seu art. 7º que o tratamento de dados pessoais “somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11º”, o qual por sua vez aborda o tratamento de dados pessoais sensíveis (BRASIL, 2016). As formas e especificidades do consentimento são abordadas nos arts. 7º, 8º, 9º, 10º e 11º, deixando claras as condições inclusive para crianças e adolescentes (BRASIL, 2016).

O projeto de lei traz ainda uma seção sobre o término do tratamento de dados (arts. 14º e 15º), de modo a estabelecer que os dados pessoais sejam cancelados após o término de seu tratamento, tendo o titular dos dados o direito de obter confirmação da existência de tratamento de seus dados (art. 17º, inciso I) (BRASIL, 2016). Cabe destacar que órgão competente poderá solicitar, a qualquer momento, aos órgãos e entidades públicos que realizam interconexão de dados e o uso compartilhado de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento (art. 26º) (BRASIL, 2016). Portanto, não se poderá escusar de tal responsabilidade os órgãos e as entidades públicos que realizem este tipo de operação a partir de dados pessoais.

Cabe comentar o art. 28º, o qual estabelece que a transferência internacional de dados pessoais somente é permitida para países que proporcionem nível de proteção de dados pessoais equiparável deste projeto de lei, destacando-se algumas exceções: cooperação judicial



internacional entre órgãos públicos de inteligência e de investigação, proteção da vida ou da incolumidade física do titular ou de terceiro, se for autorizada por órgão competente a transferência, nos termos do regulamento, compromisso assumido em acordo de cooperação internacional, execução de política pública ou atribuição legal do serviço público dando-se publicidade nos termos do §1º do art. 6º (BRASIL, 2016).

Finalmente, ficará estabelecido que “são agentes do tratamento de dados pessoais o responsável e o operador”, art. 34º e, ainda, estabelece-se um terceiro ator que é denominado como encarregado do tratamento de dados pessoais, o qual deverá ser indicado pelo responsável pelo referido tratamento (art. 41º) (BRASIL, 2016). Obrigando-se “os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de sigilo em relação aos dados pessoais, mesmo após o seu término” (art. 43º) (BRASIL, 2016).

Todos estes mecanismos visam coibir o uso indiscriminado de dados pessoais, visto que na prática são encontrados abusos relacionados, por exemplo, às redes sociais. Uma análise, por exemplo, da Política de Dados do Facebook (2016, p. 01) explicita quais dados são coletados pela rede social, podendo-se exemplificar: a) conteúdo e outros dados fornecidos pelo usuário, por exemplo, dados cadastrais, dados criados e compartilhados; mensagens; localização de uma foto; data em que um arquivo foi criado; dados de uso dos serviços; dados sobre o que usuário vê ou com que se envolve e a frequência ou duração de suas atividades; dados sobre as pessoas e grupos com que o usuário se conecta e sobre como interage com eles; dados das compras ou transações financeiras, abrangendo dados de pagamento (número do seu cartão de crédito ou débito e outras informações do cartão), informações de conta e autenticação, além dos dados de faturamento, envio e contato; dados sobre computadores, telefones e outros dispositivos em que você instala ou acessa nossos Serviços; atributos do sistema operacional, versão de hardware, configurações do dispositivo, nomes e tipos de arquivos e softwares, bateria e intensidade de sinal, e identificadores de dispositivo, localizações do dispositivo, incluindo localizações geográficas específicas, por meio de GPS, *Bluetooth* ou sinal *wi-fi*.

O volume de dados coletado é enorme. A rede social sabe tudo sobre o usuário e poderá, além disto, compartilhar os dados com fornecedores, provedores de serviços e outros parceiros (FACEBOOK, 2016, p. 01). Além disto, tomando-se por base as cláusulas da Declaração de Direitos e Responsabilidades descrita no Termo de Serviços do Facebook (2015, p. 01) entende-se que o usuário concede permissão à rede social para usar o nome, imagem do perfil, conteúdos e informações relacionadas a conteúdos comerciais, patrocinados ou relacionados (como uma





marca que o usuário curtiu) fornecido ou aperfeiçoado pelo Facebook. A atenção recai sobre o uso de conteúdos aperfeiçoado pela rede social, não esclarecendo o que vem a ser exatamente este aperfeiçoamento e que técnicas são aplicadas a partir dos dados coletados. Tecnicamente entende-se que o texto refere-se à Mineração de Dados. Outro ponto controverso é que o texto explicita a venda de dados aos parceiros comerciais da rede social.

Ao aderir a qualquer produto ou serviço *online*, é evidente a intenção do provedor do serviço ou aplicativo em capturar para si um volume de dados pessoais ou não, sendo que todos os textos, seja da Política de Privacidade ou dos Termos de Serviços, consideram que o usuário lê e compreende a complexidade dos mesmos. Na prática, o usuário “clica” em um botão de ‘ACEITO’, mas dificilmente lê os longos termos e políticas atentamente. Além, de não possuir conhecimento técnico para desvendar os meandros da linguagem utilizada pelas empresas que ofertam os serviços e aplicativos *online*.

Percebe-se, portanto, que o conhecimento dos riscos e seus reflexos cada vez mais cabe ao usuário por meio dos Termos e Políticas disponibilizados pelos prestadores de serviços *online*. O hábito de “não ler” e simplesmente “aceitar” os Termos e Políticas precisa ser modificado diante da divulgação dos riscos, da discussão do conteúdo dos documentos ofertados pelos provedores aos usuários. Além disto, cabe ao usuário entender a profundidade do fornecimento de dados pessoais e, principalmente, entender que os provedores irão, com certeza, processar, descobrir, minerar dados e informações automaticamente. Todo este conjunto de dados capturados irão “contar” ou “dizer” muito a respeito de cada usuário.

Em agosto de 2013, levantamento realizado pela Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomercioSP), com base em 1000 usuários de Internet, nos principais pontos de fluxo da cidade de São Paulo, mapeou os hábitos na Internet, seja em redes sociais, em compras em lojas virtuais ou os tipos de dispositivos usados para acessar a web (FECOMERCIO SP, 2013). Neste levantamento foi determinado que “60% dos internautas paulistanos não leem os termos de uso de redes sociais, como Facebook e Twitter, antes de se cadastrar”. Os dados mostram ainda que “60,5% dos entrevistados ignora os termos de uso desses sites, enquanto 39,5% afirmam ler integralmente contratos associados ao cadastro em um site de relacionamentos”. Cabe perceber que dados em redes de relacionamento são mais “cuidados” pelos usuários, esquecendo que as redes sociais não somente mostram muito de quem o usuário é, mas capturam dados pessoais e não pessoais.



O trabalho aponta ainda que “Ao perguntar para os entrevistados se eles confiam na guarda de seus dados pessoais por empresas que oferecem redes sociais” os resultados mostram que 72,3% não confiam, sendo que o percentual de pessoas que tem dúvidas se suas informações cadastradas são guardadas da maneira correta é maior entre pessoas com mais de 35 anos (78%).

Interessante, que o estudo da FecomercioSP, mostra que “50,2% dos entrevistados afirmaram que as empresas não podem compartilhar seus dados com outras pessoas ou empresas sem sua expressa autorização”. Na verdade, a partir do que foi exposto, mostra-se que ao não ler os Termos de Uso e Políticas de Privacidade os usuários concordam que as empresas compartilhem seus dados sem sua expressa autorização, uma vez que a autorização já foi dada quando o usuário clicou no botão “Aceito” ou “Concordo”. E, importante ressaltar que “49,8% do total afirmaram acreditar que as empresas têm a permissão de compartilhar esses dados com terceiros”. Sim, as empresas têm a permissão e foi dada pelo próprio usuário.

Finalmente, deve-se ponderar que enquanto leis e políticas brasileiras não garantem a proteção completa dos dados e informações pessoais e não pessoais nem exigem esclarecimentos do motivo dos possíveis problemas decorrentes, por exemplo: indicação dos dados que foram divulgados, se ocorreu vazamento de dados e qual o período exato em que se deu o vazamento, quando e quais medidas foram adotadas para que o problema tenha sido sanado; deve-se ler e conhecer os Termos de Uso e as Políticas de Privacidade de qualquer serviço *online*, aplicativo ou software de interesse. Com isto em mente, deve-se reconhecer que os autores Warren e Brandeis (1890) sempre foram atuais e assim continuam.

### 3. CARACTERIZAÇÃO DE PERFIL (*PROFILING*) E DISCRIMINAÇÃO

O foco recai sobre um importante reflexo do tratamento de dados que é a caracterização de perfil (*profiling*) e, conseqüentemente, há que se discutir a discriminação. Talvez o termo mais adequado em português seja perfilagem ou perfilamento, mas o que se percebe, mesmo nos artigos científicos, é o emprego da palavra inglesa. Assim, a caracterização de perfil refere-se aos métodos e técnicas computacionais aplicados aos dados pessoais ou não dos usuários. E, em tempos de *Big Data*, dados não faltam para serem processados.

As técnicas de perfilamento têm como objetivo determinar o que é relevante dentro de um determinado contexto, por exemplo, quem pode estar interessado em um determinado produto. Além disto, estas técnicas auxiliam na representatividade estatística, ou seja, na



determinação da qualidade de uma amostra constituída de modo a corresponder à população no seio da qual ela é escolhida. Ou seja, busca-se generalizar a partir de uma amostra de indivíduos e dos seus respectivos interesses. Por exemplo, se um determinado grupo de pessoas está interessado em um determinado produto, outros grupos de pessoas ligados, conhecidos ou relacionados ao primeiro grupo também pode vir a se interessar por este mesmo produto.

Muitas são as definições de perfilamento, mas Ferraris *et al.* (2003, p. 06) apresentam definições relevantes: “*the act or process of extrapolating information about a person based on known traits or tendencies, e.g. consumer profiling*” ou “*the act of suspecting or targeting a person on the basis of observed characteristics or behaviour, e.g. racial profiling*”. Assim, Ferraris *et al.* (2003, p. 06) inferem que “*profiling is a process of construction of a series of information (a profile), which is then applied to something or someone (individual or group) by techniques of data elaboration*”.

De acordo com Hildebrandt, (2009, p. 243) *profiling* pode ser definido como uma nova maneira de conhecimento que torna visível os padrões que são invisíveis ao olho humano, de modo que “*the invisibility of the patterns become visible to the profiler and the inability to anticipate the consequences of the application of profiles derived from other people’s data clearly rule out informed consent*”.

Na sociedade informacional e tecnológica em que se vive determinar o que é ou não relevante para os indivíduos é tão importante que Pariser (2012, p. 16) menciona que a “*tarefa de examinar essa torrente cada vez mais ampla em busca das partes realmente importantes, ou apenas relevantes, já exige dedicação em tempo integral*”, de modo que “*somos cada vez mais incapazes de dar conta de tanta informação*”. Portanto, métodos e técnicas de tratamento de dados, independentemente de que dados sejam, tem sido aplicados pelos mais variados sistemas, serviços ou empresas.

Como retratado por Duhigg (2012, p.81-82), a Target, gigante rede de lojas de departamento dos Estados Unidos, atribuiu um número único a cada um de seus clientes e passou a armazenar dados relativos às suas compras, identificando assim seus produtos preferidos, hábitos de consumo, valor médio de gastos, uso ou não de cupons e cartão fidelidade. Juntamente com dados pessoais de cadastro que identificavam dentre outras informações, sexo, idade, profissão e local de moradia, contratou estatísticos que, utilizando ferramentas computacionais, analisaram estes dados para extrair conhecimento relevante, estabelecendo padrões de consumo de cada cliente, permitindo assim alavancar suas vendas.



Para tal, podem ser aplicados diferentes algoritmos tanto para descobrir padrões quanto para determinar a correlação entre conjuntos de dados, de modo a estabelecer um perfil, visto que tais padrões e correlações permitem identificar ou representar pessoas ou grupos de pessoas.

Outro reflexo ligado às técnicas de tratamento de dados é a discriminação, o qual pode ser considerado como um efeito colateral perigoso, portanto, é abordado a seguir de modo mais detalhado a fim também de se analisar a legislação brasileira pertinente, visto que ao se determinar quais indivíduos compõem um perfil, pode-se gerar discriminação.

Um exemplo é a discriminação a partir do perfil de uma pessoa à disposição de apresentar uma determinada doença. O Google possui uma *web page* denominada “*Google Flu Trends*” (GOOGLE, 2017), a qual foi especialmente criada para mostrar aos usuários quais são os locais em que a gripe e a dengue estão mais presentes, a partir das consultas realizada no buscador Google sobre estas doenças. O interesse do Google é estudar e permitir que pesquisas acadêmicas sejam realizadas a partir dos dados fornecidos no referido site.

No Brasil, pode-se citar como exemplo o Sistema de Registro de Identificação de Passageiros (PRN) e as Informações Antecipadas sobre Passageiros (API), os quais foram estabelecidos por meio da Resolução N° 255 de 13 de novembro de 2012 da Agência Nacional de Aviação Civil - ANAC (BRASIL, 2012). Tais sistemas foram criados para garantir a segurança tanto dos passageiros quanto da tripulação, porém ao se processar o conjunto de dados informados sobre os voos, os passageiros e a tripulação podem ser geradas distorções.

O objetivo de ambos os sistemas, de acordo com o art. 1º, parágrafo 1º, é: “...a prevenção e a repressão a atos de interferência ilícita e a facilitação do desembarço junto às autoridades de controle migratório, aduaneiro, sanitário e agropecuário.” (BRASIL, 2012). Isto voltado aos casos de evasão fiscal sobre produtos importados ou em casos de criminosos procurados em outros países que venham a ingressar no Brasil.

Todas as empresas brasileiras e estrangeiras que exploram serviço de transporte aéreo público estão sob a regência da Resolução, com exceção das empresas de táxi aéreo (art. 3º) (BRASIL, 2012). E, não são poucas os dados a serem transmitidos antes da decolagem da aeronave, sendo a transmissão por meio de mensagem eletrônica padronizada de acordo com o EDIFACT/ONU/PAXLST, mencionado no item 3.47 da 13ª edição do Anexo 9 à Convenção de Aviação Civil Internacional (art. 3º, parágrafo 1º) (BRASIL, 2012).

O sistema de Informações Antecipadas sobre Passageiros (*Advance Passenger Information* - API) considera e organiza um conjunto de dados de maneira a contemplar



(BRASIL, 2012): a) dados relativos ao voo, b) dados relativos a cada passageiro ou tripulante; c) Dados adicionais, por exemplo: assento designado para o passageiro no voo, número de malas despachadas, número das respectivas etiquetas e o peso da bagagem, número, data e local da emissão de visto, número e tipo de outro documento utilizado para viagem; incluindo também: dados completos da residência do passageiro ou tripulante, dados de interesse do destino e, ainda: local de nascimento, tipo de viajante, código localizador da reserva, entre outros.

O sistema de Registro de Identificação de Passageiros (*Passenger Name Record* - PRN) coleta e organiza um conjunto de dados, podendo-se exemplificar (BRASIL, 2012): nome do passageiro, endereço para contato, endereço para cobrança, contatos de emergência, endereço de e-mail, endereço para correspondência, endereço residencial, endereço no destino, telefones para contato, nome e número no passaporte, data de nascimento, sexo, nacionalidade, conta no programa de fidelidade do passageiro e categoria, código localizador da reserva, diversas informações sobre lista de espera, pontos e segmentos do itinerário do voo em PNR, histórico do itinerário, ponto de embarque, cidade de destino, segmentos ativos e cancelados do itinerário, dias em transito, segmentos efetivamente voados, informações de voo, datas de partida de voos, ponto de embarque, ponto de chegada, segmentos abertos, diversas informações sobre a forma de pagamento, informações sobre assentos, informação sobre bagagens, informações do agente de viagem, entre outros dados.

Todos esses dados devem ser transmitidos ao Departamento Polícia Federal (DPF), de modo que antes do voo chegar ao Brasil já se têm em mãos as informações exigidas por esta Resolução. Ressalta-se que o Brasil não é o único a implantar tais sistemas. Países como os Estados Unidos da América e países da União Europeia também já aderiram a estes sistemas. As informações armazenadas no sistema PRN serão mantidas por um período não maior que 15 anos, sendo que após este período as informações são apagadas. As informações são anonimizadas (despersonalizadas) nos primeiros 6 meses após o registro, de modo que nomes, informações de contato e outras informações de identificação pessoal são mascaradas. Os dados do sistema PNR serão ainda mantidos por um período adicional de dez anos e só poderão ser acessados com aprovação prévia da supervisão e apenas em resposta a um caso, ameaça ou risco identificável. Esse acesso e utilização limitados aos registros mais antigos do sistema PNR permite que seja atingido um ponto de equilíbrio entre a proteção das informações e a possibilidade de o CBP continuar a identificar potenciais viajantes de alto risco. Mas existem



exceções para que as informações fiquem registradas indefinidamente, ou seja, durante a aplicação de lei que faça uso do sistema PRN, sendo tais exceções ligadas à: ameaças específicas e credíveis e voos, indivíduos e rotas de interesse ou outros conjuntos de circunstâncias definidas.

Cabe ressaltar que, no Brasil, somente são coletados dados de passageiros e tripulantes de empresas áreas de caráter público, haja vista a exceção para as empresas de táxi aéreo (art. 3º.) (BRASIL, 2012). Fato que explicita o caráter seletivo e, até mesmo, discriminatório a partir da origem dos dados seja público ou particular.

Outro exemplo de discriminação é a denominada *Pink Tax* (Imposto Rosa ou Custo Mulher), ou seja, discriminação de gênero por meio dos preços dos produtos. As mulheres geralmente acabam pagando mais que os homens pelo mesmo produto, em razão do produto ser feito para mulheres (ELLIOT, 2017) (TAYLOR, 2016). Eis o conceito de perversivo presente também nas questões de preço e discriminação por gênero.

Os preços de produtos iguais se tornam diferentes conforme o gênero, e isto fica evidente no Relatório “*From Cradle to Cane: The Cost of Being a Female Consumer - A Study of Gender Pricing in New York City*” (BESSENDORF, 2015). O estudo realizado pelo *New York City Department of Consumer Affairs* (DCA) computou o preço médio para 35 diferentes tipos de produtos com base em uma análise de 794 itens individuais e, em seguida, comparou os preços dos produtos masculinos e femininos análogos. Os resultados obtidos por Bessendorf (2015) demonstraram que em média, considerando todas as 05 (cinco) indústrias analisadas, o DCA descobriu que os produtos para mulheres custam 7% a mais que os produtos similares para os homens. Assim, de modo resumido tem-se que (BESSENDORF, 2015): os brinquedos e acessórios para meninas são 7% mais caros, o vestuário infantil feminino custa 4% mais caro que o masculino, sendo que o vestuário adulto feminino custa 8% mais caro. No que tange aos produtos de higiene e cuidados pessoais, a diferença alcança 13% e no caso de produtos de cuidados de saúde/casa a diferença é de 8%, sempre mais caros quando voltados às mulheres.

Em 30 (trinta) das 35 (trinta e cinco) categorias de produtos analisadas foram observados preços mais altos nos produtos para consumidores femininos do que os dos consumidores masculinos (BESSENDORF, 2015). O DCA descobriu que os produtos para mulheres custam mais caro em 42% dos 794 produtos analisados (168 produtos) enquanto os produtos masculinos custam mais caro somente em 18% dos 794 produtos analisados (72 produtos) e,



portanto, observou-se que somente em 40% dos produtos analisados (157% produtos) os preços são iguais para mulheres e homens (BESSENDORF, 2015).

Nos Estados Unidos da América há um movimento denominado “*Pink Tax Repeal Act*” contra este tipo de discriminação (ESTADOS UNIDOS DA AMÉRICA, 2016). Este projeto de lei proíbe a venda de serviços ou produtos de consumo substancialmente semelhantes, do mesmo fabricante, se tais produtos tiverem preços diferentes com base no gênero dos indivíduos a quem tais produtos serão destinados, comercializados ou ofertados. A simples diferença de coloração entre os produtos de consumo não poderá ser interpretada como uma diferença substancial. As violações serão tratadas como ato ou prática desleal ou enganosa sob a Lei Federal da Comissão de Comércio.

Sob a ótica da legislação brasileira a Constituição Federal de 1988 (BRASIL, 1988) preconiza no art. 5º que “todos são iguais perante lei”, não sendo necessário tratar especificamente a questão da discriminação.

Não se pode deixar de mencionar a Lei Nº 7.716/1989 que define os crimes resultantes de preconceito de raça, cor, etnia, religião ou procedência nacional (BRASIL, 1989). Esta lei trata ainda sobre as punições relacionadas à discriminação que por ventura venha obstar a promoção funcional (art. 3º), deixe de conceder os equipamentos necessários ao empregado em igualdade de condições com os demais trabalhadores (art. 4º, inciso I), proporcione ao empregado tratamento diferenciado no ambiente de trabalho, especialmente quanto ao salário (art. 4º, inciso III) e, ainda, pratique, induza ou incite, pelos meios de comunicação social ou por publicação de qualquer natureza, a discriminação ou preconceito de raça, por religião, etnia ou procedência nacional (art. 20º).

Mais especificamente sobre discriminação e tratamento de dados pessoais o Projeto de Lei Nº 5.276/2016 aborda a questão da discriminação ao considerar o princípio da não discriminação no art. 6º, inciso IX (BRASIL, 2016).

O PL Nº 5.276/2016 não regula de maneira direta o *profiling*, mencionado no art. 20º que: “O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade”. Porém, no art. 5º, inciso II, é explicitado o conjunto de etapas que compõem o tratamento de dados, incluindo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento,



eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração (BRASIL, 2016). De modo que o *profiling* está indiretamente considerado nestas etapas. No art. 13º, parágrafo 1º, o PL refere-se a considerar dados pessoais aqueles que possam ser utilizados para formação de perfil comportamental (BRASIL, 2016). Tecnicamente referindo-se à caracterização de perfil (*profiling*).

Outro aspecto relevante ao tema é que o PL Nº 5.276/2016, no art. 7º, traz o termo consentimento por parte do titular associado ao tratamento de dados, de modo que: “O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11º.” (BRASIL, 2016). Este artigo é composto de 08 (oito) parágrafos que também especificam que o consentimento para o tratamento de dados pessoais não é condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a sua realização, veda-se o tratamento de dados pessoais cujo consentimento tenha sido obtido mediante erro, dolo, estado de necessidade ou coação e esclarece que o consentimento deve ser fornecido por escrito ou por outro meio que o certifique, estando destacado das demais cláusulas contratuais. Além disto, o consentimento deve se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais. Tais finalidades estão por vezes apresentadas e descritas nos Termos de Uso e Políticas de Privacidade dos aplicativos e serviços online, o que nem sempre é de fácil leitura e compreensão por parte dos usuários. E, finalmente, o art. 11º aponta que o consentimento pode ser revogado a qualquer momento, sem ônus para o titular, que são nulas as disposições que estabeleçam ao titular obrigações iníquas, abusivas, que coloquem o titular em desvantagem exagerada, ou que sejam incompatíveis com a boa-fé ou a equidade, cabendo ao responsável pelo tratamento de dados o ônus da prova de que o consentimento do titular foi obtido em conformidade com o disposto no PL.

O PL Nº 5.276/2016 prevê, ainda, condições diferenciadas aos adolescentes<sup>1</sup>, por entender sua condição de pessoa em desenvolvimento. Assim, o adolescente poderá fornecer consentimento para tratamento de dados pessoais que respeite sua condição peculiar, sendo ressalvada a possibilidade de revogação do consentimento pelos pais ou responsáveis legais, no

<sup>1</sup> De acordo com o Estatuto da Criança e do Adolescente (ECA), Lei Nº 8.069/1990, art. 2º, considera-se: “criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade”. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/L8069Compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/L8069Compilado.htm)>. Acesso em: 10 maio 2017.





seu melhor interesse (art. 8º). No caso de crianças<sup>8</sup>, o Projeto de Lei Nº 5.276/2016 prevê que o consentimento deverá ser fornecido pelos pais ou responsáveis legais, devendo o tratamento respeitar também a condição peculiar de pessoa em desenvolvimento (art. 9º). Este cuidado do PL com as crianças e adolescentes é importante devido ao fato de que cada vez mais cedo elas estão utilizando a Internet e as redes sociais. Por exemplo, no Facebook a idade mínima para que uma pessoa tenha um perfil é de 13 anos, sendo necessário concordar com a “Declaração de Direitos e Responsabilidades do Serviço” (FACEBOOK, 2015), de modo que o usuário se compromete a não incluir informações falsas, criar perfis para terceiros sem autorização e, ainda, confirma que tem a idade mínima para se cadastrar. De acordo com a “Política de Uso”, os perfis que não preenchem o requisito de idade podem ser denunciados por outros usuários, por meio de um formulário. A exclusão pode ocorrer quando claramente se identifica que o perfil da pessoa é de alguém com menos de 13 anos.

Os artigos 10º e 11º especificam que ao consentir com o tratamento de dados pessoais, o titular deverá ser informado de forma clara, adequada e ostensiva sobre os seguintes elementos: finalidade específica do tratamento; forma e duração do tratamento, identificação do responsável pelo tratamento dos dados, informações de contato do responsável pelo tratamento dos dados, sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados, bem como âmbito de difusão, responsabilidades dos agentes que realizarão o tratamento, e direitos do titular, com menção explícita a: a) possibilidade de não fornecer o consentimento, b) possibilidade de acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado; e c) possibilidade de denunciar ao órgão competente o descumprimento de disposições desta Lei.

Ainda, sobre consentimento, o Marco Civil da Internet no art. 7º, incisos VII, VIII e IX, é bem específico e assegura ao usuário o direito de não fornecer os dados pessoais a terceiros, bem como o direito ao consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais (BRASIL, 2014).

Finalmente, o art. 16º, incisos I e II, do Marco Civil da Internet estabelece que a guarda dos registros de acesso a outras aplicações de internet somente pode ser realizada com consentimento do titular e que não se pode guardar de dados pessoais que sejam excessivos em relação à finalidade do consentimento do titular (BRASIL, 2014).

A questão do perfilamento ou *profiling* não é uma tarefa trivial, visto envolver diferentes aspectos técnicos e jurídicos, incluindo aspectos legislativos que devem levar em consideração



as características intrínsecas dos sistemas computacionais frente a todas as possibilidades de tratamento de dados pessoais ou não, sendo mais preocupante a questão dos dados pessoais e dos dados sensíveis. Porém, deve-se ter em mente que a Internet possui vantagens, mas não se pode deixar de lado os problemas também advindos da discriminação que é aqui considerado um efeito colateral perigoso do tratamento de dados pessoais. Todos estes problemas não são necessariamente visíveis aos usuários, uma vez que o usuário está imerso em um ambiente digital que é ubíquo e pervasivo.

Com base no exposto, tem-se que os reflexos do tratamento de dados pessoais são múltiplos e podem trazer benefícios ou malefícios aos usuários, haja vista a legislação brasileira que vem se ocupando em fundamentar os princípios para uma Internet segura com base no uso responsável das tecnologias.

## CONSIDERAÇÕES FINAIS

A contextualização do tratamento de dados se faz diante da sociedade informacional, tecnológica e digital. Vive-se a 4ª. Revolução Industrial, a Computação Ubíqua, a Computação Pervasiva e a Computação Inteligente. Portanto, as Tecnologias de Informação e Comunicação (TICs) impõem a discussão sobre as novas tecnologias de tratamento de dados, apresentando tanto aspectos técnicos quanto jurídicos. Coube discutir os reflexos do tratamento de dados sob o enfoque do Direito, por meio da legislação pertinente, aqui incluídas as legislações sobre dados, como objeto de interesse ao legislador. Por conseguinte, foram analisadas a Lei de Acesso à Informação (Lei No 12.527/2011), a Lei de Crimes Cibernéticos (Lei No 12.737/2012), o Marco Civil da Internet (Lei No 12.965/2014) e o Anteprojeto de Lei de Proteção de Dados Pessoais no Brasil (Projeto de Lei No 5.276/2016). A caracterização de perfil (*profiling*) e a discriminação foram tratadas como reflexos do tratamento de dados pessoais que permeiam tanto o jurídico quanto a tecnologia.

Tratamento de dados é a ação de interesse global, porém deve-se lembrar que “como qualquer ativo, o dado tem um ciclo de vida” (O GUIA DAMA, 2012, p. 01), desde sua captura, passando pelo armazenamento, processamento e utilização ou aplicação, até seu descarte ou deleção. Sim, algum dia um determinado dado ou conjunto de dados pode não ter mais utilidade. Lembrar que a vida é líquida, tal qual preconizado por Bauman (2009, p. 9), e que dados também são líquidos e, portanto, não podem ficar parados, devem modernizar-se ou perecer. Os dados fluem entre estruturas, arquivos, formatos, sensores, câmeras, aparatos eletrônicos e



digitais. É preciso aprender “a andar sobre a areia movediça” (BAUMAN, 2009, p. 151), sendo a areia movediça o universo digital constantemente em mudança.

## REFERÊNCIAS

ALEMANHA. *German Federal Constitutional Court. BVerfG*, 15 December 1983. 1983. Disponível em: <<http://www.servat.unibe.ch/dfr/bv065001.html#Rn003>>. Acesso em: 05 ago. 2017.

BAUMAN, Zygmund. *Vida Líquida*. Trad. Carlos Alberto Medeiros, 2.ed., Rio de Janeiro: Zahar, 2009.

BESSENDORF, Anna. *From Cradle to Cane: The Cost of Being a Female Consumer. A Study of Gender Pricing in New York City*. New York City Department of Consumer Affairs, 2015. Disponível em: <<http://www1.nyc.gov/assets/dca/downloads/pdf/partners/Study-of-Gender-Pricing-in-NYC.pdf>>. Acesso em: 05 ago. 2017.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. 1988. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm)>. Acesso em: 05 ago. 2017.

BRASIL. *Lei n. 7.716, de 5 de janeiro de 1989*. 1989. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/17716.htm](http://www.planalto.gov.br/ccivil_03/leis/17716.htm)>. Acesso em: 05 ago. 2017.

BRASIL. *Lei n. 12.527, de 18 de novembro de 2011*. 2011. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/112527.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm)>. Acesso em: 05 ago. 2017.

BRASIL. *Lei n. 12.737, de 30 de novembro de 2012*. 2012. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2012/Lei/L12737.htm](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm)>. Acesso em: 05 mar. 2017.

BRASIL. ANAC - Agência Nacional de Aviação Civil. *Resolução n. 255, de 13 de novembro de 2012*. Estabelece regras sobre a disponibilização de Informações Antecipadas sobre Passageiros (API) e do Registro de Identificação de Passageiros (PNR). 2012. Disponível em: <[http://www.anac.gov.br/assuntos/legislacao/legislacao-1/resolucoes/resolucoes-2012/resolucao-no-255-de-13-11-2012/@@display-file/arquivo\\_norma/RA2012-0255%20consolidado%20at%C3%A9%20RA2014-328.pdf](http://www.anac.gov.br/assuntos/legislacao/legislacao-1/resolucoes/resolucoes-2012/resolucao-no-255-de-13-11-2012/@@display-file/arquivo_norma/RA2012-0255%20consolidado%20at%C3%A9%20RA2014-328.pdf)>. Acesso em: 05 ago. 2017.

BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. 2014. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/112965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm)>. Acesso em: 05 ago. 2017.

BRASIL. *Anteprojeto de Lei Proteção de Dados Pessoais, Projeto de Lei No 5.276/2016*. 2016. Disponível em: <<http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>>. Acesso em: 05 ago. 2017.



BUSINESS DICTIONARY. *Data capture*. 2017. Disponível em:  
<<http://www.businessdictionary.com/definition/data-capture.html>>. Acesso em: 05 ago. 2017.

DUHIGG, Charles. *The Power of Habit: why we do what we do, and how to change*. 1<sup>st</sup> ed. Random House. 2012.

ELLIOT, Candice. *The Pink Tax*. 2017. Disponível em:  
<<https://www.listenmoneymatters.com/the-pink-tax/>> Acesso em: 05 ago. 2017.

ESTADOS UNIDOS DA AMÉRICA. *H.R.5686 - Pink Tax Repeal Act*. Introduced in House (07/08/2016). House - Energy and Commerce. 2016. Disponível em:  
<<https://www.congress.gov/bill/114th-congress/house-bill/5686>>. Acesso em: 05 ago. 2017.

FACEBOOK. *Termos de Serviço*. 2015. Disponível em:  
<<https://www.facebook.com/legal/terms/update>>. Acesso em: 05 ago. 2017.

\_\_\_\_\_. *Política de Privacidade*. 2016. Disponível em:  
<[https://www.facebook.com/legal/FB\\_Work\\_Privacy](https://www.facebook.com/legal/FB_Work_Privacy)>. Acesso em: 05 ago. 2017.

\_\_\_\_\_. *Política de dados*. 2016. Disponível em:  
<<https://www.facebook.com/privacy/explanation#>>. Acesso em: 05 ago. 2017.

FECOMERCIO.SP. *Comportamento do Usuário Paulistano na Internet*. 2013. Disponível em: <<http://www.fecomercio.com.br/noticia/pesquisa-fecomercio-detalha-o-comportamento-do-usuario-paulistano-na-internet>> Acesso em: 05 ago. 2017.

FERRARIS, Valeria; BOSCO, Francesca; CAFIERO, G.; D'ANGELO, Elena; SULOYEVA, Y.. *Working paper: defining profiling*. United Nations Interregional Crime and Justice Research Institute (UNICRI), December, 2013. Disponível em:  
<[www.unicri.it/news/files/Profiling\\_final\\_report\\_2014.pdf](http://www.unicri.it/news/files/Profiling_final_report_2014.pdf)>. Acesso em: 05 ago. 2017.

GANTZ, John; REINSEL, David. *The digital universe in 2020: big data, nigger digital shadows, and biggest growth in the far east*. IDC iView - Analyze the Future, 2012.

GOOGLE. *Política de Privacidade*. 2016. Disponível em:  
<<https://www.google.com/policies/privacy/>>. Acesso em: 05 ago. 2017.

GOOGLE. *Google Flu Trends and Google Dengue Trends*. 2017. Disponível em:  
<<https://www.google.org/flutrends/about/>>. Acesso em: 05 ago. 2017.

HILDEBRANDT, Mireille. *Who is Profiling Who? invisible visibility*. In: Gutwirth S., Poulet Y., De Hert P., de Terwangne C., Nouwt S. (eds) *Reinventing Data Protection?*. Springer, Dordrecht, 2009. p.239-252. Disponível em:  
<[https://link.springer.com/chapter/10.1007/978-1-4020-9498-9\\_14](https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_14)>. Acesso em: 05 ago. 2017.



LAUDON, Kenneth C.; LAUDON, Jane Price. *Sistemas de informação*. Rio de Janeiro: Livros Técnicos e Científicos S.A., 1999.

O GUIA DAMA. *The DAMA Guide to the Data Management Body of Knowledge*. DAMA International. 2012. Disponível em: <<http://my.safaribooksonline.com/book/quality-management/9781935504177>>. Acesso em: 05 ago. 2017.

PARISER, Eli. *O Filtro Invisível: o que a internet está escondendo de você*. Trad. Diego Alfaro. Rio de Janeiro: Zahar, 2012.

SCHWAB, Klaus. *A quarta revolução industrial*. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

TAYLOR, Susan Johnston. *The Pink Tax: why women's products often cost more*. 2016. Disponível em: <<http://money.usnews.com/money/personal-finance/articles/2016-02-17/the-pink-tax-why-womens-products-often-cost-more>> Acesso em: 05 ago. 2017.

WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy*. Harvard Law Review, Vol. IV, No. 5, 1890. Disponível em <<http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>> Acesso em: 05 ago. 2017.

WESTIN, Alan F.. *Privacy and Freedom*. Bodley Head, London. 1968.