RICARDO NICOTRA

ONLINE PROFILING

A proteção dos dados pessoais no processo de geração de perfil digital

Dissertação de Mestrado

Orientadora: Professora Associada Dra. Cíntia Rosa Pereira de Lima.

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo - SP

2018

RICARDO NICOTRA

ONLINE PROFILING

A proteção dos dados pessoais no processo de geração de perfil digital

Dissertação apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para a obtenção do título de Mestre em Direito, na área de concentração de Direito Civil, sob a orientação da Professora Associada Dra. Cíntia Rosa Pereira de Lima. Versão corrigida em 13 de julho de 2018. A versão original, em formato eletrônico (PDF), encontra-se disponível na CPG da unidade.

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo - SP

2018

Nicotra, Ricardo
Online Profiling – A proteção dos dados pessoais no processo de geração do perfil digital / Ricardo Nicotra. -- São Paulo / SP, 2018. 148 f.

Orientadora: Profa. Associada Dra. Cíntia Rosa Pereira de Lima.

Dissertação (Mestrado em Direito Civil) - Faculdade de Direito da Universidade de São Paulo, 2018.

1. Online Profiling. 2. Privacidade. 3. Big Data.

RICARDO NICOTRA

ONLINE PROFILING

A proteção dos dados pessoais no processo de geração de perfil digital

Dissertação apresentada à Faculdade de Direito da Universidade de São Paulo, sob a orientação da Professora Associada Dra. Cíntia Rosa Pereira de Lima, como requisito parcial para a obtenção do título de Mestre, na área de Direito Civil.

Aprovado em: _____

Banca Examinadora:

Prof.: _____ Instituição:_____

Julgamento:_____ Assinatura:_____

Prof.: _____ Instituição:_____

Julgamento:_____ Assinatura:_____

Prof.: _____ Instituição:_____

Julgamento:_____ Assinatura:_____

Aos meus pais, João e Maria Nicotra, pela vida que me deram.

À minha esposa Andréia pela vida que me dá.

À minha filha Sophia que dá sentido à minha vida.

Ao Único Deus Criador e ao Seu Filho Jesus Cristo pela vida ontem, hoje e sempre.

“Além disso, meu filho, fique atento: fazer livros é um trabalho sem fim, e muito estudo cansa o corpo. Fim do discurso. Tudo foi ouvido. Teme a Deus e observa seus mandamentos, porque este é o dever de todo o homem. Porque Deus julgará toda obra, até mesmo a que está escondida, para ver se é boa ou má.” – Sábio Salomão – Eclesiastes 12:12-14 – Versão da Bíblia de Jerusalém.

RESUMO

NICOTRA, Ricardo. *Online profiling.*A proteção dos dados pessoais no processo de geração de perfil digital. 2018. 160f. Dissertação (Mestrado) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2018.

O avanço da tecnologia digital trouxe vários benefícios aos indivíduos, empresas e governos. Aplicativos gratuitos desenvolvidos por grandes empresas privadas permitem fazer buscas na internet, conectar-se com seus amigos, fazer compras online, encontrar pessoas para relacionamento, assistir vídeos do seu interesse e fazer você chegar mais rapidamente a um lugar desconhecido.

Ao utilizar estes aplicativos o usuário fornece a estas empresas seus dados pessoais, dados de comportamento, preferências, posição geografia e deslocamento físico, dentre outros. Os dados são capturados, armazenados, agregados, analisados, criando-se, desta forma, um perfil online do usuário, o qual é compartilhado com empresas terceirizadas e utilizado para diversas finalidades, dentre as quais a veiculação de publicidade adequada ao perfil.

Este processo multifásico, denominado de "online profiling", que vai desde a coleta até a utilização dos dados gera diversos riscos aos usuários de internet os quais podem ter sua privacidade violada, sendo discriminados e estigmatizados, muitas vezes em decorrência de uma decisão automatizada.

Não há dúvidas de que este novo fato social merece atenção do ponto de vista jurídico. O Direito, principalmente no Brasil, tem caminhado de forma mais lenta do que a tecnologia, claudicando em sua tarefa de regular este relevante fato social a fim de minimizar os riscos dos indivíduos.

Após uma análise do direito à privacidade em sua multiplicidade de aspectos, este trabalho tratará das iniciativas legislativas de proteção de dados pessoais e dos princípios subjacentes. Fará uma crítica a paradigmas e modelos de proteção que se baseiam em conceitos questionáveis como dados anônimos, dados sensíveis e consentimento informado.

O modelo de proteção estadounidense bem como o europeu, incluindo o novo Regulamento (GDPR), serão discutidos principalmente em seus aspectos

que dizem respeito à prática do "online profiling". Os projetos de lei em tramitação no Congresso Nacional brasileiro também são objeto deste estudo. No entanto, a presente monografia não se limita a discutir a legislação como única forma de resolver o problema da proteção dos dados pessoais no âmbito do “online profile”. É também feita uma análise sobre modos complementares de proteção como a autorregulação do setor e a instituição de um órgão independente de proteção de dados.

Palavras Chaves: proteção de dados pessoais – online profiling – perfil digital, big data – privacidade – direitos da personalidade

ABSTRACT

NICOTRA, Ricardo. *Online profiling.* Personal Data Protection in the online profiling process. 2017. 160f. Thesis (Master) – Faculty of Law of the University of São Paulo. São Paulo, 2017.

The development of digital technology has brought many benefits to people, companies, and governments. Free apps developed by big private companies allow users to search on internet, connect with friends, shop online, met someone special, watch videos online, get the best route for a unvisited place.

The user sends personal data to those companies every time he uses those applications. That includes behaviour data, preferences, tracking location and others. Those data are captured, stored, aggregated, analysed, building up a user online profile. This profile is shared with third party companies and used to several goals, among which the most publicized is the online advertising.

This multiphase process, the so-called online profiling, going from the data tracking and collection until the use of the data creates several types of risk to internet users. These users may have their privacy violated, being discriminated or stigmatized, many times by an automated decision.

The emergence of this new social fact deserves attention from a juridical viewpoint. The Law, mainly in Brazil, has evolved tardier than technology, hobbling in its duty of regulating this important social fact to diminish the individual risks.

After analysing the right of privacy in its broad range of aspects, this paper will mention the data protection initiatives, laws, and principles. A review of paradigms and models of data protection will be made discussing concepts such as anonymization, sensitive data, and informed consent.

The paper will discuss the data protection model adopted in United States and in Europe, including the new Regulation (GDPR), mainly in the aspects related to the online profiling. The data protection bills under discussion in the Brazilian Parliament are also object of analysis. However, in this monography the law is not

the only technique to solve the issue of data protection created by the online profiling. An analysis of additional ways to protect the individuals such as self-regulation in the industry and the establishment of a data protection independent supervisory authority.

Keywords: personal data protection – online profiling – big data – privacy – personality rights.

LISTA DE ABREVIATURAS

CC – Código Civil

CDC – Código de Defesa do Consumidor

CONAR – Conselho Nacional de Autorregulamentação Publicitária

CPF – Cadastro de Pessoas Físicas

DNT – Do Not Track

DPA – Data Protection Authority

FTC – Federal Trade Commission

GDPR - General Data Protection Regulation

HIPAA – Health Insurance Portability and Accountability Act

HTTP – Hyper Text Transfer Protocol

HTTPS – Hyper Text Transfer Protocol Secure

IAB – INTERACTIVE ADVERTISING BUREAU

IP - Internet Protocol

LSO – Local Shared Objects

MCI – Marco Civil da Internet

NAI – Network Advertising Initiative

NHS – National Health Service

OECD – Organisation for Economic Co-operation and Development

PCAST - President's Council of Advisors on Science and Technology

PII – Personally Identifiable Information

PL – Projeto de Lei

SNS – Social Networking Site

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

URL – Uniform Resource Locator

W3C – World Wide Web Consortium

LISTA DE FIGURAS

SUMÁRIO

1 ASPECTOS PRELIMINARES

1.1 Introdução

O objeto de estudo desta dissertação é a tutela da privacidade dos dados pessoais em face do processo de geração de perfil digital dos usuários da internet, prática mais conhecida na literatura especializada como "*online profiling*"[1]. Este processo consiste na captura, processamento, utilização e compartilhamento dos dados pessoais, estando nestes incluídos os dados de comportamento *online* de usuários da internet rastreados e coletados por aquelas que denominamos, de forma genérica neste trabalho, de "empresas de internet"[2]. Os dados obtidos por estas empresas são armazenados inicialmente de forma bruta em bases de dados que, posteriormente, são submetidas a um processamento cujo objetivo é compor o perfil do usuário (*profiling*). Este perfil pode ser usado para diversas finalidades, sendo a veiculação de publicidade personalizada a finalidade mais propalada.[3]

Inicialmente será descrito o processo de *online profiling,* o que incluirá desde as tecnologias de captura de dados por rastreamento até, finalmente, a utilização e eventual compartilhamento de dados entre as empresas de internet. Discorrer-se-á sobre os impactos do *online profiling* na esfera jurídica dos usuários de internet com ênfase nos riscos decorrentes de decisões automatizadas que geram discriminação e estigmatização dos sujeitos relacionados aos dados

---

[1] A expressão "*online profiling*" remete ao ato de compor, construir, elaborar o perfil digital de um usuário de internet, ou seja, em sentido estrito "*online profiling*" significa apenas a elaboração do perfil do usuário. No entanto, admite-se, neste trabalho, o significado em sentido amplo da expressão que remete ao processo que vai desde a obtenção dos dados, por captura ou rastreamento, até seu destino que pode ser a utilização ou o compartilhamento com terceiros das informações obtidas e processadas.

[2] Os agentes que protagonizam o processo de *online profiling* são designados neste trabalho de forma genérica como "empresas de internet". Na seção apropriada para a explicação dos termos comuns desta dissertação, as espécies deste gênero serão apresentadas e o papel de cada uma delas será detalhado.

[3] O Facebook, em seus termos e políticas de uso, informa que "Usamos as informações que temos para melhorar nossos sistemas de publicidade e medição; assim, podemos mostrar anúncios relevantes a você dentro e fora dos nossos Serviços, além de medir a eficácia e o alcance dos anúncios e serviços." – Disponível em: <https://www.facebook.com/about/privacy>. Acesso em: 17.nov.2017. A Google, na mesma linha, informa que "usamos essas informações para oferecer ao usuário um conteúdo específico, por exemplo, fornecer resultados mais relevantes de pesquisa e anúncios.". Disponível em: <https://www.google.com.br/intl/pt-BR/policies/privacy/?fg=1#infouse>. Acesso em: 17.nov.2017.

pessoais. Demonstrar-se-á o agravamento da vulnerabilidade do usuário e do risco de violação de sua privacidade em face da possibilidade real de diversas empresas de internet, em regime de parceria, compartilharem os dados pessoais, compartilhamento que permite a agregação de uma quantidade maior de dados possibilitando a geração de um perfil (*profiling*) mais preciso, detalhado e revelador não apenas sobre as características pessoais do sujeito relacionado aos dados, mas também sobre suas preferências e tendências. Apontar-se-á, por fim, o aumento da probabilidade de desanonimização de dados em decorrência do amplo compartilhamento dos dados pessoais entre as empresas de internet e do constante incremento informacional do famigerado Big Data.

A partir deste ponto, tendo já alcançado uma visão satisfatória do processo objeto de análise e da forma como ele coloca o usuário numa situação de vulnerabilidade, num segundo momento será abordado o tratamento jurídico conferido aos dados pessoais com ênfase na tutela jurídica do sujeito relacionado aos dados. Serão analisadas de forma crítica as normas jurídicas em vigor e as projetadas que regulam a proteção de dados pessoais no Brasil e no exterior, normas geralmente fundamentadas no princípio do consentimento informado e na crença da possibilidade de anonimização de dados.

A crítica da norma e de suas premissas será apresentada levando-se em conta os valores e princípios que justificam a proteção dos dados pessoais bem como a realidade fática e técnica do contexto do *online profiling*, em especial a forma como o consentimento para a coleta, tratamento, utilização e compartilhamento de dados tem sido obtido do sujeito relacionado aos dados.

Finalmente, algumas propostas de controle serão apresentadas objetivando-se tutelar de forma mais eficaz os direitos dos sujeitos relacionados aos dados de comportamento *online* e dados derivados do processo de *profiling*.

1.2 Objetivos

O objetivo geral da pesquisa é a apresentação do recente fato social denominado *online profiling* bem como a análise dos direitos do usuário da internet sobre a captura, processamento e utilização dos seus dados pessoais, incluindo os dados sobre seus hábitos de navegação e dados derivados de processamento ou

tratamento. Estes direitos serão analisados em face das práticas difundidas entre empresas de internet, práticas que envolvem a coleta dos referidos dados, muitas vezes sem informar de forma satisfatória ou receber o consentimento livre, específico e inequívoco do usuário.

Como objetivos específicos do estudo, elenca-se, de forma sucinta, os seguintes:

- Apresentar, de forma sucinta, algumas tecnologias utilizadas para a captura e tratamento de dados pessoais e discutir a adequação da cada uma delas em face do ordenamento jurídico vigente e projetado.
- Compreender como a evolução tecnológica é capaz de atribuir novos aspectos de interesse aos direitos clássicos como o direito à privacidade e intimidade.
- Analisar as dimensões do direito à privacidade, principalmente aquela envolvendo a proteção dos dados pessoais e os dados de comportamento e histórico de navegação na internet.
- Verificar quais dados, de fato, são coletados por empresas de internet e qual o nível de informação oferecido ao usuário antes da coleta bem como o grau de consentimento exigido para que a coleta, processamento, utilização e compartilhamento sejam realizados.
- Qualificar a natureza jurídica da conduta das empresas de internet que coletam estes dados tendo como base o ordenamento jurídico pátrio, em especial os princípios que tutelam o direito do consumidor e que estão na base principiológica dos projetos de lei que versam sobre proteção de dados pessoais.
- Discutir sobre as formas utilizadas para proteger o usuário da internet das práticas abusivas de uso de dados pessoais e de dados de navegação tendo como subsídio a análise da jurisprudência e legislação estrangeiras, principalmente aquela vigente na União Europeia.
- Propor modelos de governança a serem observados pelas empresas de internet, objetivando-se a adequação das necessidades de mercado com a proteção dos direitos de personalidade dos usuários da internet.

1.3 Problema

A presente dissertação se propõe a analisar as seguintes questões:

Qual a extensão do direito fundamental à privacidade e intimidade? Este direito inclui a proteção dos dados pessoais coletados na internet e dados de navegação que refletem o comportamento, preferências e interesses do usuário, ainda que o sujeito relacionado aos dados não esteja inequivocamente identificado?

A proteção de dados pessoais pode ser estendida aos dados pessoais públicos como, por exemplo, estado civil e data de nascimento? Deve a proteção ser estendida aos dados derivados, entendidos como aqueles que resultam da fase de análise dos dados coletados?

O direito sobre dados pessoais inclui o direito de navegar na internet de forma anônima? Quais são as limitações funcionais razoavelmente esperadas por um usuário que decida navegar na internet de forma anônima?

Qual é o nível de informação a ser disponibilizada e consentimento a ser obtido do usuário para que as empresas de internet possam: (a) capturar dados pessoais e de navegação, (b) submeter estes dados a análises estatísticas e algoritmos para projeções e tendências (e.g. agregação e mineração de dados), (c) utilizar os dados coletados e os dados resultantes das análises para diversas finalidades, incluindo o direcionamento de publicidade, (d) compartilhar estes dados com terceiros, (e) com base nos dados derivados tomarem decisões de forma automatizada que tenham impacto na esfera jurídica do sujeito relacionado aos dados?

O ordenamento jurídico brasileiro (incluindo os projetos de lei de proteção de dados pessoais) regula de forma satisfatória as práticas objeto deste estudo sendo, portanto, capaz de tutelar de forma preventiva o direito dos usuários da internet no tocante aos dados pessoais e de navegação coletados, processados e compartilhados? É possível aplicar o Código de Defesa do Consumidor (Lei 8.078/90) e o Marco Civil da Internet (Lei 12.965/2014) para regular as práticas de *online profiling*?

É possível falar em titularidade dos dados pessoais? Quem é o titular dos dados pessoais? Que direitos decorrem da titularidade destes dados? Estes direitos são absolutos ou podem ser mitigados? Em quais circunstâncias se dá a mitigação? Que outros direitos podem colidir com os direitos decorrentes da titularidade sobre os dados pessoais?

A quais riscos jurídicos estão submetidos os sujeitos cujos dados são coletados, processados e compartilhados por empresas de internet?

Que medidas podem ser tomadas para evitar abusos das empresas de internet que praticam o *online profiling*?

Que alternativas ao direito positivo podem ser implementadas para assegurar os direitos dos sujeitos relacionados aos dados?

1.4 Justificativa

O advento e a disseminação da tecnologia digital e das telecomunicações vêm causando uma verdadeira revolução nas relações humanas. As relações sociais, comerciais e jurídicas foram profundamente afetadas nas últimas décadas com a difusão das ferramentas que usam a internet como plataforma operacional. Este novo cenário impele o jurista à reflexão sobre os novos direitos que emergem desta nova realidade – direitos que, na verdade, podem ser considerados releituras ou novas dimensões de direitos já existentes.

A privacidade é um dos direitos que ganhou nova roupagem na sociedade digital. Da ideia de “o direito de ser deixado só” à proteção dos dados pessoais, a mudança de feição deste direito da personalidade decorreu, em grande medida, da evolução tecnológica.

LOUIS BRANDEIS e SAMUEL WARREN, em 1890, já haviam notado como o desenvolvimento tecnológico colocaria a privacidade numa posição de vulnerabilidade. À época escreveram o seguinte no clássico artigo “*The Right to Privacy*”:

> *Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". Instantaneous photographs and*

> *newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."*[4]

BRANDEIS e WARREN mencionam as “fotografias instantâneas” e seu meio de publicação, os jornais, bem como “numerosos dispositivos mecânicos” como elementos, fruto da evolução tecnológica, que ameaçariam a intimidade dos indivíduos. Se ambos tinham razão naquela época, é forçoso admitir que as ameaças se intensificaram hoje, momento em que a maioria dos transeuntes detém uma câmera fotográfica embutida num dispositivo que permite não só a captura de imagens em lugares públicos e privados, mas sua imediata publicação num espaço digital que pode ser acessado gratuitamente por qualquer pessoa do mundo que, por sua vez, poderá copiar, armazenar ou compartilhar a fotografia ou qualquer outro conteúdo publicado.

Atualmente é comum observar que algumas publicações são compartilhadas de maneira exponencial sendo acessível à maioria dos usuários de internet que utilizam redes sociais ou aplicativos de comunicação instantânea.[5]

Segundo BRANDEIS e WARREN a resposta eficaz para esta crescente capacidade dos governos, da imprensa e das empresas invadirem aspectos até então inacessíveis do indivíduo estaria no direito positivo. Remédios legais deveriam ser desenvolvidos para limitar o acesso destas entidades ao âmbito mais restrito do indivíduo.

O direito positivo, entendido como um conjunto de prescrições destinadas a regularem a conduta humana, tem uma dinâmica própria que, em relação à dinâmica da vida social, é reativa e não proativa. Equivale dizer que as

---

[4] WARREN, Samuel D.; BRANDEIS, Louis D.. The Right to Privacy. 4 HARV.L.REV. 193 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>. Acesso em: 01.dez.2017

[5] A este fenômeno de compartilhamento exponencial atribuiu-se a expressão “viralizar” que embora ainda não conste no Vocabulário Ortográfico da Língua Portuguesa (VOLP) da Academia Brasileira de Letras já foi dicionarizado no Houaiss como “*verbo - t.d.int. e pron. espalhar(-se) como um vírus (p.ex., na internet); tornar-se viral ‹v. uma entrevista nas redes sociais› ‹processo de afastamento viraliza nas redes› ‹o boato viralizou-se na internet›*”

alterações nas condutas sociais se refletem, apenas após algum tempo, no direito posto e não o contrário. É justamente nesta assincronia que está o espaço para o trabalho dos juristas. O vaticínio de BRANDEIS e WARREN se cumpre hoje de uma forma mais intensa do que eles poderiam prever, no entanto o arcabouço legal para a disciplina da matéria ainda é incipiente e insatisfatória e, mesmo quando existente, enfrenta óbices para a efetividade dos direitos e garantias uma vez que as práticas aqui referidas são de difícil fiscalização.

Como se não bastassem as dificuldades já expostas, demonstrar-se-á, ademais, que as pouco numerosas iniciativas legislativas repousam sobre premissas questionáveis, o que levanta dúvidas sobre a eficácia destas medidas protetivas.

As novas práticas perpetradas no espaço digital pelas empresas de internet demandam uma análise aprofundada e um tratamento jurídico adequado. A alimentação de bases de dados pessoais e comportamentais com base na navegação do usuário da internet (*online behavior*) realizada por empresas de internet merecem a especial atenção da sociedade e dos juristas em razão do seguinte:

(a) A coleta e processamento de dados pessoais têm como resultado a geração de informações[6] que, se publicadas ou utilizadas de forma inadequada, podem violar os direitos e causar danos aos sujeitos relacionados aos dados.

---

[6] Dados só se tornam em informação se organizados e analisados adequadamente. Danilo Doneda (2006) diferenciou “dados” de “informações” da seguinte forma: “Em relação à utilização dos termos ‘informação’ e ‘dado’, é necessário notar preliminarmente que o conteúdo de ambos os vocábulos se sobrepõe em várias circunstâncias, o que justifica uma certa promiscuidade na sua utilização. Ambos os termos servem para representar um fato, um determinado aspecto de uma realidade. Não obstante, cada um carrega um peso particular a ser levado em conta. Assim, o ‘dado’ apresenta conotação um pouco mais primitiva e fragmentada, como observamos por exemplo em um autor que o entende como uma informação em estado potencial, antes de ser transmitida; o dado estaria associado a uma espécie de ‘pré-informação’, anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição, e mesmo nos efeitos que esta pode apresentar ao seu receptor” – DONEDA, 2006. p. 152.

(b) Não é possível afirmar que a coleta e tratamento de dados pessoais e comportamentais realizada atualmente pelas empresas de internet é feita mediante real consentimento dos sujeitos relacionados aos dados. Observa-se, ademais, que o usuário, no momento de eventual autorização para a coleta e utilização de seus dados não recebe informações adequadas e específicas sobre (1) a quantidade e natureza dos dados coletados, (2) o tempo que os dados serão mantidos na base de dados do provedor, (3) o tratamento ao qual serão submetidos os dados, (4) o uso que será feito dos dados, incluindo a possibilidade de cessão ou compartilhamento dos dados com terceiros.

(c) Os dados coletados e as informações geradas a partir de tratamento destes dados têm inequívoco valor econômico porquanto podem gerar ao seu detentor incremento patrimonial em razão da sua utilização (aumento da eficiência de campanhas publicitárias, arbitramento de preços de produtos e serviços em função do potencial consumidor, cessão ou compartilhamento com terceiros, identificação de risco de crédito de determinados consumidores e quaisquer outras destinações que venham a gerar receitas para o detentor dos referidos dados). Nesta esteira, questiona-se sobre quem é o titular do direito sobre tais dados. Tratando-se de verdadeiras projeções da personalidade de vários indivíduos, não seriam estes os legítimos titulares dos dados e, portanto, merecedores de restituição sobre qualquer resultado economicamente quantificável em decorrência do uso dos dados?

1.5 Metodologia

A Ciência do Direito, por pertencer à categoria de Ciências Humanas ou Ciências Sociais, raramente lança mão de processos experimentais cujos resultados servem como “verificações sintéticas” com vistas à comprovação das hipóteses postas à prova.

Como leciona o jurisfilósofo MIGUEL REALE, “isto não significa que as ciências sociais sejam destituídas de certeza. Esta é obtida mediante o rigor do

raciocínio, a objetividade da observação dos fatos sociais e a concordância de seus enunciados”[7].

Na visão de REALE é possível estabelecer leis a partir da observância das mencionadas exigências. Não são leis de causalidade, como na Física ou Química, mas leis de tendência, ou seja, “leis que asseguram certo grau de certeza e previsibilidade”. Desta forma, a Ciência do Direito deve observar a lógica e os métodos adequados à sua finalidade.

No estudo do objeto desta dissertação serão utilizados os métodos indutivo e dedutivo.

Utilizando o método indutivo, partir-se-á da compreensão de fatos particulares para que se chegue a conclusões de ordem geral. Este método será aplicado na parte inicial da dissertação onde o processo de *online profiling* será apresentado e analisado. As conclusões de ordem geral, resultado da aplicação do método indutivo, devem ter a aptidão para explicar o que há de comum em fatos da mesma natureza. Perceba-se que nesta etapa busca-se melhor compreensão do fato social que é objeto da análise, qual seja, o processo de geração de perfil digital, o *online profiling*, o que inclui o processo de captura de dados, comumente denominado de *online tracking*.

Apenas na segunda parte da dissertação, lançar-se-á mão do método dedutivo. Com este método, parte-se de uma verdade sabida, de um fato social tomado em sua generalidade, e aplicando inferências de natureza axiológica, chegar-se-á à conclusão sobre alternativas para o tratamento jurídico do fato social sob análise.

A pesquisa fundamentar-se-á em análise de literatura específica, principalmente de artigos em idioma estrangeiro, uma vez que o tema “*online profiling*” ainda não é tratado de forma aprofundada na literatura nacional. A literatura nacional referenciada versará sobre os aspectos do problema apresentado sob a ótica do ordenamento jurídico pátrio (Constituição Federal,

---

[7] REALE, Miguel. Lições preliminares de direito. 25ª ed. São Paulo: Saraiva. 2001. p. 76.

Código Civil, Código de Defesa do Consumidor e Projetos de Lei de Proteção de Dados Pessoais).

Objetiva-se desenvolver a análise jurídica dos problemas propostos de forma independente das tecnologias atualmente utilizadas, embora tais tecnologias sirvam de base para a análise dos casos concretos e da apreensão do fato social *online profiling* tomado em sua generalidade, razão pela qual tais tecnologias serão abordadas sem aprofundamento técnico.

1.6 Termos e Definições

1.6.1 Online Profiling

Optou-se, neste trabalho, por adotar a expressão em inglês "*online profiling*" para denominar o objeto de estudo da dissertação. Desde já, ressalte-se, que a denominação é imprecisa e insuficiente para descrever o objeto em sua complexidade. Decidiu-se adotá-la em razão de sua simplicidade e de sua ampla utilização e compreensão nos meios tecnológicos e jurídicos.

Poder-se-ia cogitar a adoção da denominação traduzida e adaptada para a língua portuguesa: "geração de perfil por conexão na internet", no entanto a longa denominação em vernáculo comprometeria a fluidez do texto além de não resolver os problemas conceituais da denominação original em inglês, os quais passa-se a expor:

Inicialmente, a palavra *profiling* é um substantivo derivado do verbo inglês "*to profile*" que significa escrever, desenhar ou produzir uma representação com as principais características de um objeto. É o ato por meio do qual cria-se uma projeção de algo ou de alguém com atributos do objeto que se busca caracterizar. Como dito, esta expressão é insuficiente para traduzir o objeto de análise desta dissertação que, repita-se, vai além da mera geração de um perfil com características do indivíduo. *Profiling*, neste estudo, deve incorporar uma carga semântica ampla, referindo-se a todo o processo que vai desde a captura de dados pessoais, passando por seu armazenamento, processamento, compartilhamento até sua utilização para a tomada de decisões. É evidente que o termo *profiling* pode ser interpretado *stricto sensu*, referindo-se apenas ao tratamento ou

processamento de uma massa bruta de dados pessoais cujo resultado são informações úteis para determinados fins. No entanto, na maioria das vezes neste trabalho o termo *profiling* será usado em seu sentido amplo, qual seja, o já referido processo multifásico de tratamento de dados pessoais.

A expressão "*online*" é igualmente imprecisa como adjetivo a qualificar o ato que convencionou-se chamar de *profiling*. Comumente, no contexto das redes de computadores, atribui-se ao termo *online* o significado de simultaneidade, conectividade, disponibilidade, geralmente aplicando-se à possibilidade de imediata transmissão ou recebimento de dados. Em sentido oposto, o termo *off-line* refere-se, geralmente, à indisponibilidade de conexão ou troca de dados de forma imediata. No contexto do *profiling,* que ora se analisa, ao adjetivo *online* deve ser atribuída uma carga semântica diversa: *online*, nesta seara, deve se referir ao *locus* do *profiling*, qual seja, a Internet, ambiente no qual os dados são coletados, ainda que determinadas etapas do processo de *profiling* – e talvez a maioria delas – como as análises, compartilhamento ou até mesmo a captura de alguns dados podem ser realizadas sem conexão com a internet, ou seja, *off-line*.

1.6.2 Dados Pessoais

Não obstante a multiplicidade de conceitos atribuídos à privacidade, o ponto de interesse para este estudo é a dimensão da privacidade que se relaciona com a proteção dos dados pessoais.

Nesta linha, qualquer iniciativa que objetive a proteção de dados pessoais deve enfrentar a intrigante tarefa de definir o que se entende por "dados pessoais", uma vez que não se pretende proteger todos os tipos de dados, mas tão somente aqueles qualificados como "pessoais".

Observa-se na doutrina, na legislação estrangeira e nos projetos de lei sobre o tema que o conceito de "dados pessoais" está intimamente relacionado à possibilidade de vincular um determinado dado a uma pessoa física. Equivale dizer que se um determinado dado está ou pode ser relacionado a um indivíduo, este dado deve ser considerado, para fins de proteção, um dado pessoal.

Há dados que, tomados isoladamente, têm a capacidade de identificar univocamente o indivíduo que a ele está relacionado. Tome-se, como exemplo, o número da inscrição da pessoa no CPF ou seu número de cadastro numa universidade. No entanto, a maior parte dos dados que podem ser relacionados a um indivíduo dependem do contexto em que estão inseridos para que a identificação com o indivíduo seja possível. Isso porque, tomados isoladamente, tais dados não seriam capazes de identificar univocamente a pessoa relacionada ao dado. Como exemplo é possível citar o nome “José da Silva” ou a data de nascimento “25/12/1970”, dados que, tomados isoladamente, não são capazes de apontar para um sujeito determinado ao qual estão relacionados.

Desta forma, o adjetivo “pessoal”, atribuído ao dado quando este relaciona-se diretamente a um indivíduo, não é atributo intrínseco de um determinado dado considerado isoladamente da massa de dados da qual faz parte. O que faz um dado ser qualificado como “pessoal” é sua relação de pertinência com uma massa de dados relacionada a um indivíduo identificado ou identificável.

Há duas linhas para conceituar “dados pessoais”: uma restritiva e outra mais abrangente. De acordo com a interpretação restritiva, um dado é qualificado como pessoal se é possível, de imediato, identificar o indivíduo a ele relacionado. Neste caso convencionou-se dizer que o dado é relacionado à pessoa “identificada”. Já a interpretação abrangente qualifica um dado como pessoal se existe a possibilidade de identificar a pessoa a ele relacionada, embora, de imediato, tal relacionamento não se observe. Neste caso, diz-se que o dado é relacionado a pessoa “identificável”.

Dados que, por natureza, referem-se de alguma maneira a indivíduos como, por exemplo, estado civil, religião e domicílio, mas que num determinado contexto não podem ser relacionados imediatamente a uma pessoa identificada, são denominados “dados anônimos”, o que, a princípio, excluiria tais dados do escopo protetivo das já referidas iniciativas legislativas. No entanto, como demonstrar-se-á adiante, ainda que num determinado contexto os dados não possam ser imediatamente relacionados a um indivíduo, a agregação de mais dados àquela massa de dados poderá tornar a identificação possível. Equivale dizer

que num momento inicial o dado pode ter relação de pertinência com uma massa de dados que não identifica um indivíduo, mas num momento posterior pode haver a agregação de novos dados identificáveis a esta massa de dados outrora não relacionada ao indivíduo fazendo com que o dado inicialmente relacionado a uma massa de dados não identificada com o indivíduo passe a se relacionar com um novo conjunto de dados que permita a identificação do indivíduo. A este processo de agregação de dados que passa a permitir a identificação do sujeito relacionado aos dados convencionou-se chamar de desanonimização.

Em face da comprovada possibilidade de desanonimização, neste estudo a expressão “dados pessoais” deverá ter um sentido amplo não abrangendo apenas aqueles dados que permitam identificar imediatamente o sujeito relacionado ao dado.

O conceito de “dados pessoais”, no contexto do “*online profiling*”, deve admitir um sentido que inclua dados de comportamento *online*, ou seja, dados que, de forma mais precisa, dinâmica e incremental, têm o potencial revelar aspectos da personalidade do indivíduo que muitas vezes até as pessoas mais próximas dele desconhecem. Tome-se, como exemplo, um indivíduo que descobre ser portador de uma doença ou é adepto de uma determinada prática sexual, fatos que por razões de intimidade, prefere ocultar das pessoas que com ele têm uma relação de maior intimidade. Tais aspectos de sua intimidade são facilmente capturados por meio da coleta de dados de navegação (*online behavior*) e, portanto, tais dados devem ser considerados “dados pessoais” ainda que a base de dados não contenha dados que possibilitem a imediata identificação do sujeito. Pois, como já mencionado anteriormente, a identificação da pessoa relacionada aos dados pode ocorrer em momento posterior ao da coleta.

O comportamento *online* de um indivíduo, consubstanciado em pesquisas em motores de busca, visita a sites especializados, aquisições em lojas de comércio eletrônico, deslocamento geográfico, entre outros, poderá ser – e, de fato, é – monitorado pelas empresas de internet de modo que os dados de navegação (URLs visitadas, buscas realizadas e produtos adquiridos ou pesquisados) são incluídos em bases de dados que estarão à disposição da

empresa que os coletou e das empresas com as quais ela compartilhará os dados coletados. Ademais, inclua-se neste rol os dados de localização geográfica do usuário, dados sobre seus relacionamentos na internet (outros usuários com os quais ele está conectado) e tudo de forma incremental, ou seja, as empresas que coletam os dados mantêm um histórico sempre crescente que permite, por meio de análises cada vez mais precisas, prever determinadas ações ou situações envolvendo a pessoa relacionada aos dados[8].

É fato que boa parte dos dados de comportamento online coletados por estas empresas de internet num momento inicial pode não estar relacionada diretamente a um indivíduo, mas tão somente ao um endereço de conexão denominado endereço IP. No entanto, a ulterior associação de um endereço IP a um indivíduo permite que boa parte da massa de dados de navegação coletada para aquele IP seja atribuída ao indivíduo associado ao IP. Essa associação de endereço IP com um indivíduo ocorre com bastante frequência, principalmente num cenário onde se observa uma tendência decrescente na utilização de dispositivos compartilhados (desktops) e um aumento de dispositivos utilizados por apenas uma pessoa (dispositivos móveis).[9]

Por fim, destaque-se que a massa de dados pessoais coletada e atribuída a um indivíduo pode ser analisada e processada de modo a gerar dados derivados, também considerados como dados pessoais. Note-se que os dados derivados destas análises, dados que compõem o que convencionamos denominar de *profile*, não apenas consistirão de dados que refletem aspectos relacionados ao passado do sujeito, mas também ao seu futuro, na medida em que a massa de dados processada poderá sugerir categorias, tendências e prever condutas do indivíduo.

---

[8] Evita-se, neste ponto, fazer referência ao sujeito do qual os dados são obtidos como "titular dos dados". Por esta razão é dada a preferência à expressão "pessoa ou sujeito relacionado aos dados", por mais imprecisa que possa parecer. A possível relação de "titularidade" entre os sujeitos e os dados é questão que será discutida posteriormente nesta dissertação.

[9] Em termos práticos bastaria, por exemplo, a autenticação de um usuário a um serviço de internet (e.g. efetuar login no Facebook ou no Google) para que a empresa de internet associe o IP ao indivíduo. Esta associação é na maioria das vezes imediata pois os usuários dos serviços do Facebook e do Google geralmente acionam a opção para se manterem "logados" nestes serviços evitando que lhes seja exigida a senha todas as vezes que acessarem os serviços.

Além destes dados comportamentais coletados por rastreamento, também consideramos como “dados pessoais” todas as informações geradas como resultado do processamento dos dados brutos coletados. Nesta categoria são incluídos, por exemplo, dados de *rating* de crédito, nível de risco para contratação de seguros e graus de potencial interesse para aquisição de produtos ou serviços.

1.6.3 Sujeitos Relacionados aos Dados

Os usuários de internet que têm seus dados pessoais capturados por empresas de internet são denominados, na literatura estrangeira, de “*data subjects*”. Esta denominação consta nas versões em inglês da Diretiva 95/46/CE[10] e do novo Regulamento de Proteção de Dados Pessoais[11] que unificou os dispositivos sobre a matéria na União Europeia. No entanto, na versão em língua portuguesa consta a expressão “titulares dos dados”. Os projetos de lei que tramitam em nosso país também adotaram a expressão “titular dos dados” para se referirem à pessoa física à qual os dados estão relacionados.

Embora a expressão “titulares dos dados”, adotada em Portugal e no Brasil, seja mais concisa do que aquela que ora apresentamos – “sujeitos relacionados aos dados” – evitou-se, neste trabalho, adotar o termo “titulares” por conta da afinidade deste termo com o conceito de “propriedade” ou de outros direitos. Quem é titular, é titular de algum direito. No caso, os dados pessoais não são direitos para que sobre eles se exerça titularidade, entendida aqui no sentido de propriedade. Tais dados podem ser objetos de direito, havendo, portanto, direitos que podem ser exercidos sobre os dados pessoais, o que faz da pessoa relacionada aos dados, titular destes direitos (e.g. direito de não publicação, direito de esquecimento, direito de não compartilhamento com terceiros, etc...). No entanto, neste ponto não nos parece claro que um indivíduo seja titular dos mesmos direitos sobre todos os dados relacionados a si. Tome-se como exemplo o direito

---

[10] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data protection directive). 24.out.1995.

[11] Regulation 2016/679 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). 27.abr.2016.

de não ter um determinado dado compartilhado com terceiros. Parece evidente que um dado como número de cartão de crédito ou renda mensal de um indivíduo não deveria ser compartilhado sem seu consentimento. No entanto o mesmo não pode ser dito em relação a dados públicos que podem ser encontrados nos cartórios de registro civil ao alcance de qualquer interessado como, por exemplo, estado civil e data de nascimento.

Portanto, ao se dizer “titular dos dados pessoais” não está claro, *a priori*, quais são os direitos relacionados a esta titularidade. Por tais razões, nesta dissertação optou-se pela expressão “pessoa ou sujeito relacionado aos dados”.

1.7 Classificação dos Dados Pessoais

Os dados pessoais podem ser classificados em relação a diversos critérios. Este estudo se limita a apresentar as classificações que oferecem um resultado prático no âmbito da análise do *online profiling*.

O primeiro critério de classificação dos dados pessoais é o grau de intimidade do aspecto da personalidade refletido pelo dado pessoal. Características pessoais muito íntimas são classificadas como “dados pessoais sensíveis”. Nesta categoria comumente são incluídos dados como ideologia política, etnia, convicções religiosas, opções e preferências sexuais. Em decorrência da projeção de aspectos da personalidade com alto grau de intimidade, observa-se que os instrumentos de tutela conferem a estes dados maior grau de proteção.

O segundo critério de classificação dos dados pessoais está relacionado à possibilidade de identificação do sujeito a partir de um conjunto de dados. Denomina-se “dados anônimos” o conjunto de dados a partir do qual não é possível, de imediato, identificar o sujeito relacionado aos dados. A rigor, o atributo “anônimo” não é intrínseco de um determinado dado, mas de uma massa de dados tomada isoladamente. Equivale dizer que se a partir de um conjunto de dados não for possível identificar de forma imediata o indivíduo relacionado aos dados, a este conjunto de dados é atribuída a denominação de “dados anônimos”. No entanto, esta classificação não é estática, ou seja, um conjunto de dados pode ser, num determinado momento, insuficiente para identificar o sujeito relacionado a ele, mas havendo posterior agregação de mais dados ao conjunto ou a partir de correlação

com outras fontes de dados, pode ocorrer o fenômeno que convencionou-se chamar de “desanonimização”. Da mesma forma, um conjunto de dados não anônimo, ou seja, cujos sujeitos são identificados, pode ser submetido a um processo de deidentificação ou anonimização gerando um conjunto de dados anônimos.[12]

Portanto, o atributo “anônimo”, quando vinculado a um conjunto de dados, deve ser encarado como instável. Por tal razão, as iniciativas legislativas não deveriam, em abstrato, atribuir um nível de proteção menor ao conjunto de dados anônimo tendo-se em vista a possibilidade de reidentificação dos sujeitos relacionado aos dados. O Anexo I deste trabalho contém exemplos clássicos de desanonimização que suscitaram a discussão pública sobre a crença na proteção de dados por meio da anonimização.

No âmbito no processo de *online profiling*, os dados pessoais podem ser também classificados em função da iniciativa do fornecimento dos dados. Denomina-se “dados voluntários” aqueles dados que são voluntariamente fornecidos pelo sujeito com total consciência de que dados estão sendo transmitidos num determinado momento. Como exemplo, cita-se os dados fornecidos por um consumidor durante o preenchimento de um formulário de cadastro num website: nome, endereço eletrônico, endereço físico, documento de identificação e número de cartão de crédito são exemplos de dados voluntariamente fornecidos pelo usuário. Em contrapartida, os “dados não voluntários” são aqueles capturados ou produzidos pelas empresas de internet sem a imediata ciência do sujeito em relação à natureza e o momento em que o dado está sendo capturado ou produzido. Como exemplo de dados não voluntários cita-se os dados de navegação, dados referentes às pesquisas realizadas em sites de busca, dados do dispositivo, da conexão de internet e dados derivados de análises.

[12] A seção 4.2 deste trabalho abordará com mais detalhes a questão da anonimização e desanonimização de conjunto de dados.

Os dados não voluntários admitem uma subclassificação em relação à sua origem. Podemos classificar estes dados em dados de navegação, dados de dispositivo, dados de conexão e dados derivados, sem prejuízo de outras espécies.

Os dados de navegação consistem no histórico de navegação (*browsing history*) do usuário. Dentre estes dados estão os sites visitados, os links clicados e as pesquisas em motores de busca. Dados de navegação são sistematicamente coletados por empresas de internet e gravados no perfil do usuário. É por esta razão que um usuário após consultar um determinado produto num site de comércio eletrônico usando seu dispositivo móvel, pode ser surpreendido com uma propaganda do mesmo produto em seu computador pessoal no feed de notícias do Facebook em outro dispositivo, no seu computador pessoal, por exemplo.

Os dados de dispositivo incluem informações sobre o hardware e software do dispositivo utilizado na navegação. Isto inclui sistema operacional e sua versão. Houve casos em que a identificação do sistema operacional foi utilizada pelas empresas de internet como fator decisivo para a apresentação de ofertas e definição de preços. A Orbitz, empresa de reservas *online*, utilizando técnicas de mineração de dados, descobriu que os usuários dos dispositivos da Apple gastavam, em média, 30% a mais nos hotéis em comparação aos usuários de PC. A partir desta conclusão a Orbitz passou a exibir opções mais sofisticadas e caras na sua primeira página para os usuários de Apple.[13]

A Google admite que coleta informações do dispositivo utilizado para a navegação bem como informações de conexão como o endereço IP:

> *Quando você acessa nossos serviços (por exemplo, faz uma pesquisa no Google, recebe rotas no Google Maps ou assiste um vídeo no YouTube), coletamos dados para fazer com que esses serviços funcionem melhor para você. Isso pode incluir:*
>
> - *Coisas que você pesquisa*
> - *Sites que você visita*

[13] The Wall Street Journal. *On Orbitz, Mac Users Steered to Pricier Hotels.* Disponível em: <http://www.wsj.com/articles/SB10001424052702304458604577488822667325882>. Acesso em: 04.nov.2017.

- *Vídeos a que você assiste*
- *Anúncios nos quais você clica ou toca*
- *Seu local*
- *Informações do dispositivo*
- *Endereço IP e dados de cookies*[14]

Os dados derivados merecem atenção especial pois sua origem está no processamento e correlação da massa de dados obtida pelas empresas de internet. São dados que não são coletados, mas produzidos por algoritmos e ferramentas de análise podendo conter, em seu bojo, elementos de decisão automática como, por exemplo, *credit scoring* ou nível de risco para a contratação de seguro.

Embora as classificações acima tenham sido utilizadas no estabelecimento de normas de proteção (e.g. dados sensíveis recebem maior grau de proteção enquanto dados anônimos recebem menor grau de proteção), a nova realidade envolvendo o Big Data e o *online profiling* acabam por minorar a diferença entre os diversos tipos de dados fazendo com que a proteção mereça ser aplicada em todos os casos. Neste sentido lecionou STEFANO RODOTÀ:

> *O ponto de vista global torna a se impor nos temas ligados ao tratamento a ser reservado aos dados pessoais e àqueles anônimos ou agregados, à distinção entre privacidade individual e de grupo. Diante da nova realidade dos "perfis", essas distinções perdem significado: seja porque dados pessoais, aparentemente não "sensíveis", podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas.*[15]

---

[14] GOOGLE. Seus dados. Disponível em: <https://privacy.google.com/your-data.html>. Acesso em: 26.nov.2017.

[15] RODOTÀ, Stefano. *A vida na sociedade da vigilância:* a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 84.

2 O *ONLINE PROFILING*: A GERAÇÃO DE PERFIL DIGITAL

Uma regra geral no mundo dos negócios é “conheça o seu cliente”. Os fornecedores de bens e serviços que tiverem informações mais precisas sobre seus clientes e potenciais clientes (*prospects*), terão significativa vantagem competitiva no mercado. O online profiling é um recurso que possibilita ao controlador dos dados ter um conhecimento aprofundado e incremental dos clientes e potenciais clientes.

Online Profiling é um processo de captura, mineração e correlação de dados que, a partir de dados pessoais de um usuário ou de um grupo de usuários, é capaz de gerar o perfil (*profile*) do usuário ou do grupo qualificando-o e categorizando-o.

FREDERIK BORGESIUS, especialista em *behavior targeting* e *privacy law* da Universidade de Amsterdam, apresenta uma definição do processo de *online profiling* vinculada ao objetivo de direcionamento de publicidade adequada ao perfil do destinatário

> *Behavioral targeting, or online profiling, is a hotly debated topic. (...) Behavioral targeting is the monitoring of people's online behavior over time to use the collected information to target people with advertising matching their inferred interests.*[16]

É comum, na literatura especializada, encontrar conceitos que transcendem o aspecto ontológico do objeto de estudo e invadem a esfera teleológica. No caso do *online profiling* é prudente limitar a definição do objeto ao que ele, de fato, é, dissociando do conceito a suposta finalidade mais comum do objeto, no caso, o direcionamento de publicidade específica. Esta dissociação é recomendável pois a composição de um perfil de usuário, baseado em dados de diversas fontes (dados coletados, dados de comportamento *online*, dados de bases de terceiros), pode destinar-se a finalidades diversas da mera veiculação publicitária. E é na possibilidade de uso que transcende a mera veiculação de publicidade online que residem os riscos da prática de *profiling*. A natureza

---

[16] BORGESIUS, Frederik Zuiderveen. Behavioral targeting: A european legal perspective, IEEE Security & Privacy, vol.11, no. 1, Jan.-Feb. 2013. p. 82.

dinâmica e incremental do Big Data propicia um cenário favorável para a concepção de novas finalidades de uso dos dados capturados, finalidades que ainda não haviam sido concebidas no momento da coleta e para as quais não se obteve o consentimento específico do sujeito relacionado aos dados.

A política de privacidade da Google[17] elenca os dados coletados e, de forma muito genérica, as finalidades da coleta. A Google distingue os dados coletados em duas categorias:

(1) “Informações que o usuário nos transmite” tais como nome, endereço de e-mail, número de telefone ou cartão de crédito e

(2) “Informações que coletamos a partir do uso que o usuário faz dos nossos serviços”. Nesta categoria a Google elenca as seguintes subcategorias: (a) “Informações do dispositivo” (modelo de hardware, versão do sistema operacional, informações de rede móvel, inclusive número de telefone), (b) “Informação de registro” (detalhes das consultas de pesquisa, informações de chamada telefônica tais como número de quem chama, de encaminhamentos, duração das chamadas telefônicas, endereço de protocolo de internet (IP), configurações de hardware, tipo e idioma do navegador e cookies), (c) “Informações do local” – Com relação a este ponto a Google afirma que utiliza “várias tecnologias para determinar a localização, como endereço IP, GPS e outros sensores”, (d) “Números de aplicativos exclusivos” - Não fica claro se tais aplicativos são apenas aqueles fornecidos pela Google tais como o gerenciador de e-mails Gmail, Youtube e Google Maps ou quaisquer outros aplicativos instalados no dispositivo do usuário, (e) “Armazenamento local” – Neste ponto a Google admite que “podemos coletar e armazenar informações (inclusive informações pessoais) localmente em seu dispositivo usando mecanismos como armazenamento no navegador da web (inclusive HTML 5) e caches de dados de aplicativo.” e (f) “Cookies e tecnologias semelhantes” – Neste ponto a Google admite a participação de parceiros que usam “várias tecnologias para coletar e armazenar informações”.

---

[17] GOOGLE. Política e Termos. Disponível em: <https://www.google.com.br/intl/pt-BR/policies/privacy/?fg=1>. Acesso em: 28.set.2017.

Qual seria a finalidade dos dados coletados pela Google? Assim como a maior parte das empresas de internet, a Google declina as finalidades para a coleta de dados em termos muito genéricos:

> *Usamos as informações que coletamos em todos os nossos serviços para fornecer, manter, proteger e melhorar estes serviços, desenvolver novos e proteger a Google e nossos usuários. (...) Usamos as informações coletadas de cookies e de outras tecnologias, como etiquetas de pixel, para melhorar a experiência do usuário e a qualidade geral de nossos serviços.*[18]

A composição do perfil do usuário com base nos dados coletados é um processo recorrente no qual novos dados são agregados para tornar o perfil mais preciso e útil para as finalidades às quais ele se destina. Esta constante agregação de novos dados ao perfil ocorre por combinação de bases de dados de diversas fontes. A Google, em sua política de privacidade, admite que combina dados de seus serviços com dados pessoais do usuário bem como com dados de outros serviços da Google:

> *Podemos combinar informações pessoais de um serviço com informações, inclusive informações pessoais, de outros serviços da Google para facilitar o compartilhamento de informações com pessoas que o usuário conhece, por exemplo.*

Perceba-se que a combinação de informações de diversas fontes, inclusive com dados pessoais, destina-se ao compartilhamento com outras pessoas, finalidade mencionada na política de privacidade apenas como um exemplo. Este compartilhamento ocorre também com empresas afiliadas e empresas parceiras. Na política de privacidade da Google lê-se: “Fornecemos informações pessoais a nossas afiliadas ou outras empresas ou pessoas confiáveis para processá-las para nós”.[19]

Embora a Google afirme em sua política de privacidade que pode compartilhar com parceiros as informações que não são pessoalmente identificáveis (leia-se, dados anônimos), já está demonstrado que a grande massa

---

[18] GOOGLE. Política e Termos. Disponível em: <https://www.google.com.br/intl/pt-BR/policies/privacy/?fg=1>. Acesso em: 28.set.2017.

[19] GOOGLE. Política e Termos. Disponível em: <https://www.google.com.br/intl/pt-BR/policies/privacy/?fg=1>. Acesso em: 28.set.2017.

de dados sobre um indivíduo, resultado da coleta de dados voluntários e dados de navegação, enriquecida pela constante agregação de novos dados, serve como chave para a desanonimização de conjuntos de dados que isoladamente seriam considerados meramente dados anônimos ou dados que não são pessoalmente identificáveis.

2.1 Agentes Envolvidos

Este trabalho com frequência se refere às “empresas de internet” como protagonistas dos processos de *online profiling*. No entanto, tal denominação é demasiadamente genérica, o que exige uma especificação dos atores que pertencem a este gênero e os seus papéis no âmbito da atividade objeto da análise.

2.1.1 Empresas de Publicidade Online

O primeiro grupo de “empresas de internet” são as empresas de publicidade online, também conhecidas pela denominação de “*Online Advertising Networks*”. Com o incremento da dinâmica negocial na rede, ficou impraticável que os anunciantes tratem diretamente com todos os administradores dos espaços para a publicidade[20]. As empresas de publicidade online trouxeram a solução ao servirem como intermediárias entre os anunciantes e os “espaços virtuais”. Estas empresas agregaram eficiência ao processo de direcionar publicidade ao se basearem em critérios como, por exemplo, o tipo de destinatário (“*demographic targeting*”), o local do destinatário (“*geographic targeting*”), o conteúdo da página que irá exibir a propaganda (“*contextual targeting*”) e os hábitos de navegação do usuário destinatário da publicidade (“*behavioral targeting*”).

[20] As publicidades online podem ser publicadas em diversos “espaços virtuais” tais como websites (portais, blogs, sites temáticos), aplicativos, feeds RSS, e-mails, motores de busca ou outras mídias.

Os websites que hospedam conteúdo, geralmente portais, blogs e redes sociais, destinam parte do seu espaço para propaganda. Esta forma de publicidade tem crescido de forma acentuada nos últimos anos.

A PricewaterhouseCoopers divulgou estudo onde estima um crescimento 11,1% ao ano nas receitas com publicidade *online* que, em 2020, ultrapassarão a marca de 260 bilhões de dólares por ano.[21] Concluíram que em 2016, pela primeira vez, as receitas de publicidade online ultrapassaram as receitas com publicidade na TV[22], confirmando a previsão feita no relatório do ano anterior.

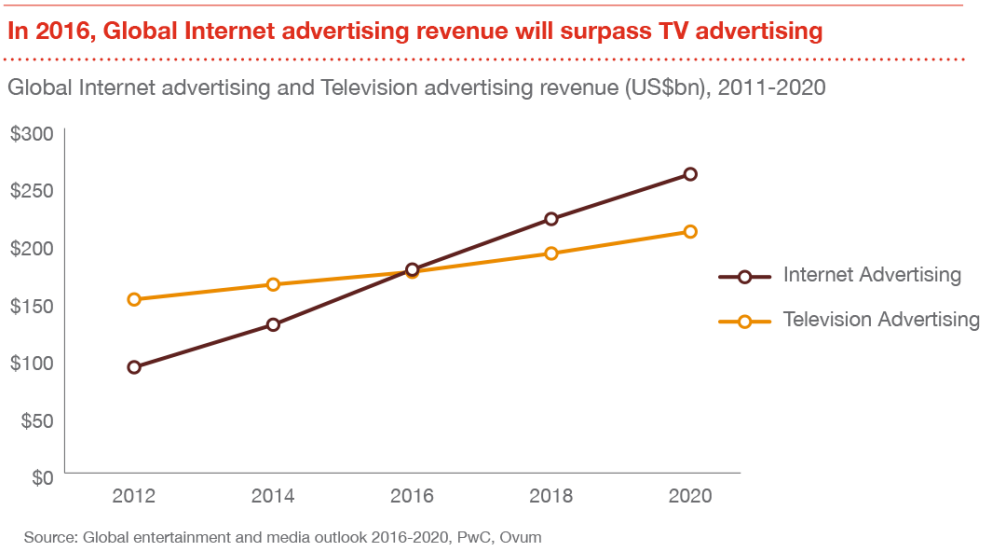

Figura 1 - Evolução das Receitas (Publicidade Online X TV)

Os anunciantes (websites, portais, blogs) reservam um espaço em seus sites onde é colocado um trecho de código de modo que quando a página é carregada, é feito um acesso aos servidores da empresa de publicidade *online*, a qual retorna o conteúdo com a publicidade. Desta forma, quando o usuário visualiza uma publicidade num blog, geralmente o conteúdo desta publicidade não foi elaborada pelo autor do blog, mas pela empresa de publicidade *online* à qual foi dedicado um espaço no blog. A empresa de publicidade *online* tem meios de apurar

[21] Disponível em:<http://www.pwc.com/gx/en/industries/entertainment-media/outlook/segment-insights/internet-advertising.html>. Acesso em: 07.dez.2017

[22] PWC Global Findings. Disponível em: <http://www.pwc.com/gx/en/industries/entertainment-media/outlook/global-data-insights.html>. Acesso em: 09.dez.2017

a quantidade de visualizações e cliques em cada publicidade, o que serve para remunerar o dono do espaço e cobrar o anunciante.

O site da revista Fortune publicou, baseando-se em dados do IAB, que Google e Facebook dominam 99% do setor de publicidade digital (54% para Google e 45% para Facebook), deixando apenas 1% do mercado para as empresas menores.[23]

2.1.2 Data Brokers

As empresas conhecidas como *Data Brokers* são as administradoras de gigantescos bancos de dados com informações sobre consumidores utilizadas em estratégias de *database marketing*.

Estas empresas coletam dados dos indivíduos de várias fontes públicas e privadas e posteriormente vendem dados para empresas que pretendem direcionar publicidade para consumidores dentro de um determinado perfil.

O desenvolvimento da internet, as possibilidades técnicas de captura de dados, a redução dos custos de armazenamento digital e a crescente demanda por dados pessoais contribuiu para que os *Data Brokers* se desenvolvessem rapidamente.

Os *Data Brokers* geralmente fazem a análise de dados (*Data Analytics*). A análise de dados é o processo de inspeção de dados que, utilizando-se de estatísticas e correlações, objetiva encontrar padrões e tendências. Geralmente a análise de dados é realizada com vistas ao apoio para a tomada de decisões. É a partir do processo de análise de dados que os dados crus (*raw data*) são transformados em informação.

---

[23] Fortune Website. How Google and Facebook Have Taken Over the Digital Ad Industry. 2017. Disponível em: <http://fortune.com/2017/01/04/google-facebook-ad-industry/>. Acesso em: 09.jun.2017.

Em Maio de 2014 a FTC, Federal Trade Commission, divulgou um relatório intitulado "*Data Brokers: A Call for Transparency and Accountability*" com um estudo sobre a forma de operação de nove grandes *Data Brokers* nos Estados Unidos. Neste estudo a FTC apontou que a Acxiom, uma das maiores empresas de dados tem informações sobre aproximadamente 700 milhões de pessoas no mundo[24]. A Corelogic, outra Data Broker, tem dados sobre 795 milhões de transações imobiliárias cobrindo 99% das propriedades residenciais dos EUA. A eBureau, que fornece serviços de análise de dados e "*predictive scoring*" adiciona em seus bancos de dados três bilhões de registros por mês.

Cada uma das nove empresas de *Data Broker* analisadas pelo FTC mantém bancos de dados gigantescos e, segundo a FTC, sete das nove empresas estudadas compartilham dados entre si.

Uma destas empresas, a Acxiom, mantém aproximadamente 3000 categorias de indivíduos em suas bases de dados. Dentre estas categorias encontramos "Donos de Cachorros", "Married Sophisticates" (que inclui casais de classe média alta sem filhos) e algumas categorias sensíveis tais como "Expectant Parents", "Diabetes Interest" e "Cholesterol Focus". Não há dúvidas de que a categorização dos indivíduos é decorrência do processo de *Data Analytics* citado acima.

Não obstante o poderio informacional destas empresas, poucas pessoas têm conhecimento de sua existência e de que elas estão ativamente coletando, processando e compartilhando dados pessoais.

2.1.3 Redes Sociais

Outro grupo de empresas que participam desta engrenagem são as que administram as redes sociais, Facebook e Twitter, por exemplo. As SNS (*Social Networking Services)* participam do processo de *profiling* nas duas pontas: Por um

---

[24] FEDERAL TRADE COMMISSION. Data brokers: a call for transparency and accountability. Maio 2014. Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em: 06.dez.2017. p. 8.

lado podem ser utilizadas para a captura de dados pessoais que, posteriormente, sofrerão o processo de análise e contribuirão para a composição do perfil digital (*online profile*). Na outra extremidade, a rede social é utilizada como forma de veicular propaganda compatível com o perfil do usuário.

As redes sociais capturam dados dos usuários não apenas durante o processo de cadastro ou durante a utilização e navegação no site da rede social, mas também durante a navegação do usuário fora do site da rede social. Na seção 3.2.3 ficará demonstrado como o Facebook e outras redes sociais capturam dados de navegação dos usuários em sites que mantêm ativos serviços destas redes sociais.

2.1.4 Provedores de Conteúdo

As empresas provedoras de conteúdo – e incluem-se neste grupo os grandes portais de informação – embutem conteúdo de terceiros (mapas, notícias, previsão do tempo, vídeos, informações da bolsa e mercados). No código fonte das páginas de conteúdo são reservados espaços para a publicidade *online*. Neste espaço o administrador da página inclui um trecho de código que faz referência ao servidor da empresa de publicidade online. Uma vez executado o código, o servidor da empresa de publicidade envia o conteúdo que será exibido na página que embutiu o código.

O tipo de conteúdo escolhido pela empresa de publicidade *online* dependerá do perfil do usuário, conforme profile já construído.

2.2 A Captura e Rastreamento dos Dados Pessoais

Na classificação dos dados pessoais apresentada na seção 2.7 foi feita uma distinção entre os dados voluntários – aqueles fornecidos voluntariamente pelos usuários como os dados de um cadastro pessoal – e os dados capturados sem a ciência imediata do sujeito.

Embora os dados voluntários sejam utilizados para a composição do perfil *online* do usuário, as questões de privacidade mais intrigantes se relacionam com os dados capturados por rastreamento digital, processo também conhecido como “*online tracking*”. As técnicas de *tracking* permitem que as empresas de

internet coletem uma quantidade gigantesca de dados dos usuários que navegam na internet.

Em 2016, JULIAN ASSANGE, fundador do Wikileaks, afirmou que empresas como Google e Facebook recebem mais informações do que a NSA (Agência de Segurança Nacional dos Estados Unidos) e denominou o novo modelo de negócios mundial de "capitalismo de vigilância".[25]

GEORGIA SKOUMA e LAURA LÉONARD definem da seguinte forma o processo de *online tracking*:

> *On-line tracking consists of recording and collecting data linked to an individual visiting the Internet through such tools over a period of time in order to gain information on this individual.*[26]

A cada dia as técnicas de rastreamento para a coleta de dados pessoais têm se aperfeiçoado sendo as tecnologias baseadas em cookies as mais conhecidas. No entanto, há outras tecnologias como, por exemplo, as etiquetas de pixel ("*pixel tags*") que são pequenas imagens de 1x1 pixels colocadas no código de uma página ou numa mensagem de email cujo objetivo é rastrear o acesso do usuário ao conteúdo daquela página ou e-mail.

As tecnologias de *online tracking*, por serem capazes de rastrear o comportamento do indivíduo durante a navegação, são aptas a capturar seus dados pessoais sensíveis e, desta forma, detectar ou inferir as convicções religiosas, as preferências sexuais, as afiliações políticas e outros aspectos da intimidade do sujeito. JONATHAN R. MAYER e JOHN C. MITCHELL, especialistas em segurança de sistemas e privacidade da Stanford University, demonstraram como o histórico de navegação pode revelar aspectos sensíveis do usuário de internet.

---

[25] UOL ECONOMIA. Google e Facebook coletam mais dados que EUA, diz fundador do Wikileaks. Disponível em: <http://economia.uol.com.br/noticias/efe/2016/07/12/google-e-facebook-coletam-mais-dados-que-eua-diz-fundador-do-wikileaks.htm>. Acesso em: 13.dez.2017.

[26] SKOUMA, Georgia; LÉONARD, Laura. On-line behavioral tracking: What may change after the legal reform on personal data protection. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (Eds). Reforming european data protection law. Springer, 2015. p. 37.

> *Collection of sensitive personal information is not a hypothetical concern. In mid-2011 we discovered that an advertising network, Epic Marketplace, had publicly exposed its interest segment data, offering a rare glimpse of what third-party trackers seek to learn about users. User segments included menopause, getting pregnant, repairing bad credit, and debt relief. Several months later we found that the free online dating website OkCupid was sending to the data provider Lotame how often a user drinks, smokes, and does drugs.*[27]

Atualmente, o conteúdo das páginas de um website não é mais composto por apenas uma pessoa ou instituição. Uma série de agentes (e.g. empresas de publicidade, redes sociais, empresas de análise de dados) contribuem para a formação do conteúdo de uma página web. A atuação destes agentes gera valor na medida em que possibilita acesso gratuito a determinados recursos e facilita a inovação. No entanto, esta evolução vem acompanhada de um custo e risco para a privacidade do usuário na medida em que, ao visitar uma página na internet, estes agentes passam a ter acesso aos dados pessoais do usuário bem como passam a registrar seu comportamento online.

Quando se acessa uma página de um portal na internet, com frequência observa-se propagandas veiculadas por meio de *banners* ou espaços dedicados à publicidade. Estas chamadas de marketing não são publicadas diretamente pelo portal ou blog, mas por empresas de propaganda terceirizadas. Estas empresas terceirizadas coletam dados ativamente durante a navegação, mas de forma invisível, sem o conhecimento e consentimento do usuário.

Os usuários de internet, por vezes, ficam cientes e anuem com a coleta de dados pessoais feita de forma explícita, geralmente pelo preenchimento de formulários *online* onde dados como nome, endereço e e-mail são fornecidos. No entanto, poucos usuários têm o conhecimento de que empresas terceirizadas de publicidade digital podem coletar seus dados pessoais e comportamentais. Estes dados, como visto, são os ingredientes para as fases posteriores de análise e elaboração do *online profile*.

---

[27] MAYER, Jonathan R.; MITCHELL, John C. Third-Party Web Tracking: Policy and Technology, Proceedings of the 2012 IEEE Symposium on Security and Privacy, p.413-427, May 20-25, 2012. Disponível em: <https://jonathanmayer.org/papers_data/trackingsurvey12.pdf>. Acesso em: 07.dez.2017. p. 3.

Passa-se a descrever, de forma sucinta, sem o objetivo de adentrar a detalhes técnicos, algumas tecnologias que permitem a coleta de dados de navegação.

2.2.1 Cookies

Os *cookies*, também conhecidos como HTTP *Cookies*, *Web Cookies*, *Internet Cookies* ou *Browser Cookies*, são pequenos arquivos de texto baixados para o dispositivo local (computador, smartphone ou tablet) onde são armazenados dados obtidos durante a navegação do usuário.[28] Nestes arquivos ficam geralmente armazenados os dados relacionados às preferências do usuário para um website específico, suas credenciais de acesso daquele website (usuário, email e senha) e, algumas vezes, o histórico de navegação. Cada vez que o usuário acessa aquele *website*, o navegador envia para o servidor as informações contidas no *cookie* de modo que o servidor possa retornar um conteúdo adequado em função dos dados contidos no *cookie*.

Ao longo da navegação, informações são gravadas nos *cookies* e também lidas dos *cookies*: pesquisas realizadas em motores de busca, websites visitados, downloads efetuados, produtos ou serviços contratados em websites de comércio eletrônico – todo o comportamento *online* é suscetível de ser registrado nos arquivos de *cookies*.

O *cookie* não é um programa instalável, ou seja, não contém software. Como dito, trata-se apenas de um arquivo texto gravado no dispositivo local no qual o website pode gravar dados e do qual pode ler dados. Os *cookies* são, portanto, uma porta de saída de informações do dispositivo do usuário para o servidor dos websites visitados.

---

[28] "Cookies são pequenos trechos de texto usados para armazenar informações em navegadores da Web. Os cookies são usados para armazenar e receber identificadores e outras informações em computadores, telefones e outros dispositivos. Outras tecnologias, inclusive os dados que armazenamos em seu navegador ou dispositivo, identificadores associados ao seu dispositivo e outros software, são usados com finalidades semelhantes." – Fonte: FACEBOOK.Cookies e outras tecnologias de armazenamento. Disponível em: <https://www.facebook.com/policies/cookies>. Acesso em: 12.dez.2017.

É possível configurar o navegador para informar o usuário e pedir sua autorização toda vez que um arquivo de *cookie* estiver na iminência de ser gravado no dispositivo local. É também possível configurar o navegador para bloquear a recepção deste tipo de arquivo. No entanto, a opção por bloqueio dos *cookies* poderá implicar num desempenho parcial das funcionalidades do website. É de se destacar que se adotou, como padrão nos navegadores, a sistemática do *opt-out*, ou seja, a configuração padrão dos navegadores permite a gravação de cookies sem a notificação prévia do usuário e, caso este deseje alterá-la, deverá fazê-lo de forma manual, o que raramente acontece na prática.

Os *cookies* foram desenvolvidos pela Netscape, empresa que dominou o mercado de navegadores (*browsers*) na década de 90, inicialmente com o Mosaic e, posteriormente, com o Navigator.[29]

O surgimento dos *cookies*, em 1994, está relacionado ao desenvolvimento do comércio eletrônico. Antes desta época os navegadores web eram ferramentas que não armazenavam informações contextuais de navegação, ou tecnicamente, o “estado” (diz-se, em inglês, *stateless machines*), sendo, portanto, comparáveis a máquinas automáticas de vendas (*vending machines*) que desconsideram quem é o cliente, quantas compras já efetuou e quais são suas preferências. A impossibilidade de armazenamento do “estado” (*state*) se configurava diante da impossibilidade dos navegadores conservarem as informações contextuais resultantes das opções do usuário. Durante o desenvolvimento de uma loja virtual pela *Enterprise Server Division* da Netscape, a equipe técnica foi desafiada a encontrar uma solução para que o conteúdo do carrinho de compras fosse mantido mesmo após o usuário visitar outros sites ou fechar e abrir nova sessão do navegador.[30]

---

[29] SHAH, Rajiv C.;KESAN, Jay P. *Recipes for cookies: How institutions shape communication technologies.* Illinois Public Law and Legal Theory Research Papers Series No. 01-14. p. 321. Disponível em: <https://experts.illinois.edu/en/publications/recipes-for-cookies-how-institutions-shape-communication-technolo>. Acesso em: 05.nov.2017

[30] Ibidem, p. 322

Antes da concepção dos *cookies*, outras formas para a manutenção do estado de navegação foram tentadas[31], no entanto a que prevaleceu, ao final, foi a solução baseada em *cookies*.

2.2.2 Cookies de Terceiros

Um dos aspectos polêmicos em relação ao risco à privacidade apresentado pelos *cookies* está na possibilidade técnica dos navegadores admitirem a implantação no dispositivo local de *cookies* de terceiros (*Third-Party Cookies*), o que abre as portas para o rastreamento efetuado por terceiros (*Third-Party Tracking*).

A Google, no seu site de suporte e ajuda, ao conceituar os cookies, distingue os gerados pelo site que está sendo visitado daqueles gerados por terceiros:

> *O que são cookies*
>
> *Cookies são arquivos criados pelos websites que o usuário visita. Eles armazenam informações de navegação, como preferências do site ou informações de perfil. Existem dois tipos de cookies:*
>
> - *Os cookies primários são definidos pelo site mostrado na barra de endereços.*
> - *Os cookies de terceiros vêm de outros sites que têm itens como anúncios ou imagens incorporados à página que o usuário está visitando.*[32]

---

[31] Uma forma de manutenção do estado de navegação foi o método URL que mantinha um histórico de opções do usuário como parâmetros na URL. Apesar de ter implementação mais simples por não exigir alteração no navegador, este método não funcionava quando o usuário pressionava a tecla “back”, visitava outros sites ou fechava o navegador. Outra abordagem sugerida por Brian Behlendorf (1995) foi a implementação de um identificador de sessão denominado “Session Id”. Este identificador era gerado no navegador e passado para o servidor. Esta implementação resolvia o problema da perda de informações quando a tecla “back” era pressionada e quando outros sites eram visitados, mas não preservava o estado do website em face do fechamento e reabertura do navegador.

[32] GOOGLE. Ajuda do Google Chrome. Limpar, ativar e gerenciar cookies no Chrome. Disponível em: <https://support.google.com/chrome/answer/95647>. Acesso em: 12.dez.2017.

Na especificação original de cookies feito pela Netscape, apenas o site que estava sendo visitado teria acesso para gravar e ler os cookies no/do dispositivo do usuário. Por exemplo, ao visitar um determinado website o usuário poderia receber em seu dispositivo os cookies do referido website que, permanentemente, poderiam ser alterados e lidos pelo mesmo website que o criou. Outros websites não poderiam ter acesso de leitura ou alteração a estes cookies. Ou seja, cada domínio teria acesso aos seus próprios cookies no dispositivo do usuário. Esta limitação preservaria a privacidade do usuário ao permitir que apenas o website gerador do cookie pudesse alterá-lo e consultá-lo.[33]

No entanto, esta limitação não se observou nas implementações subsequentes. Adotou-se uma implementação que permitiu a componentes de terceiros embutidos numa determinada página a gravação e leitura dos cookies.

Desta forma, suponha que um Website que denominaremos “W.com” seja acessado por um usuário. “W.com” poderá ter acesso ao dispositivo do usuário para nele gravar cookies que, posteriormente, poderão ser lidos por “W.com”. No entanto, o website “W.com” pode dedicar alguns espaços de suas páginas para terceiros, geralmente empresas de publicidade online, digamos “P.com”. Então ao acessar “W.com”, o usuário, mesmo sem ter ciência deste fato, permite que “P.com” acesse o conteúdo dos cookies gerados por “W.com”. Ocorre que “P.com”, que supomos ser uma empresa de publicidade online, também é parceira de “A.com”, “B.com” e “C.com”, outros sites ou blogs que dedicam espaço para a publicidade online e também geram cookies. Desta forma, a empresa “P.com” terá acesso ao conteúdo dos cookies de A, B, C e W.com, o que faz da empresa de publicidade online detentora de uma quantidade significativa de dados sobre um determinado usuário. Isso lhe permite a construção de uma extensa base de dados e a elaboração de perfis detalhados dos usuários.

---

[33] SHAH, Rajiv C.;KESAN, Jay P. *Recipes for cookies: How institutions shape communication technologies.* Illinois Public Law and Legal Theory Research Papers Series No. 01-14. p. 325. Disponível em: <https://experts.illinois.edu/en/publications/recipes-for-cookies-how-institutions-shape-communication-technolo>. Acesso em: 05.nov.2017

Atualmente os navegadores oferecem a opção de bloqueio de acesso por meio de cookies de terceiros. No entanto, a configuração não é intuitiva e os usuários geralmente não têm o conhecimento necessário sobre as implicações deste tipo de coleta de dados.

A configuração padrão dos três navegadores mais utilizados atualmente (Google Chrome, Mozilla Firefox e Internet Explorer) são permissivas com relação aos Cookies de Terceiros[34].

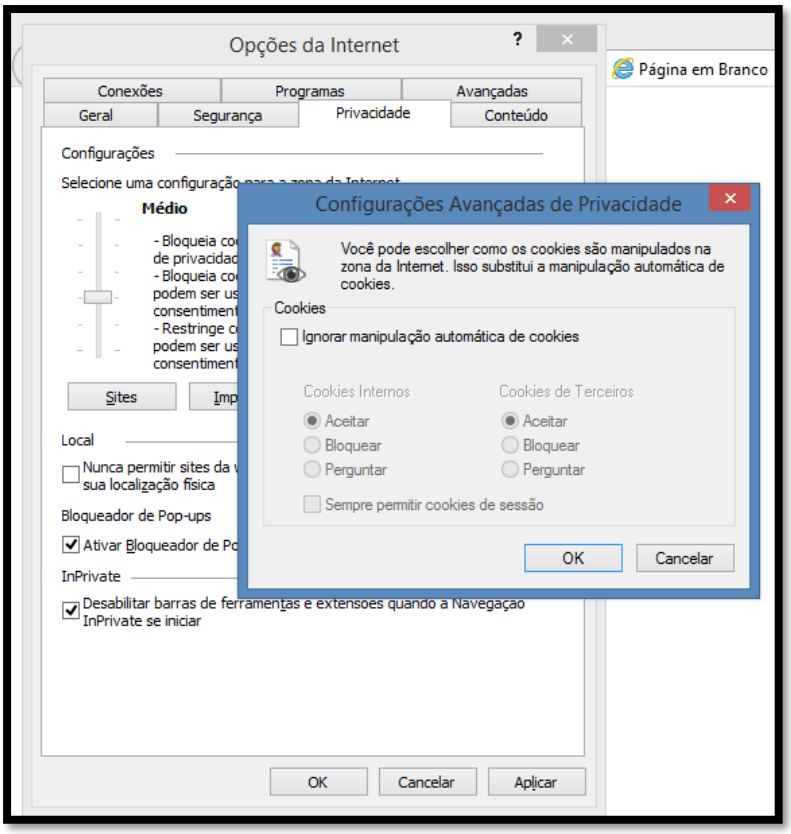

Figura 2 - Internet Explorer: Opções permissivas para Cookies de Terceiros

[34] A imagens mostram as opções presentes nas seguintes versões dos navegadores: Google Chrome versão 53.0.2785.116, Mozilla Firefox versão 49.0.1 e Internet Explorer versão 11.0.9600.18450

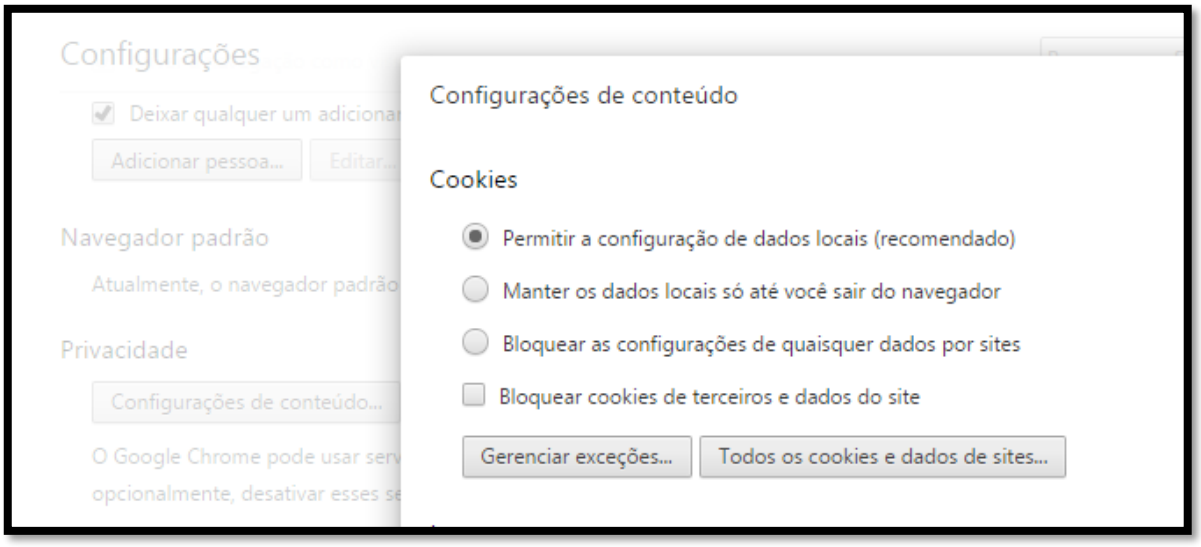

Figura 3 – Opção de Cookies padrão permissiva no Chrome

Figura 4 - Mozilla Firefox: Opções permissivas para “cookies de fora” (terceiros)

2.2.3 Rastreamento por Redes Sociais (Facebook)

As redes sociais utilizam cookies de forma cada vez mais sofisticada para capturar os dados de navegação dos seus usuários e até mesmo daqueles que ainda não são usuários.

Nesta seção será apresentado o modo como o Facebook realiza este rastreamento por meio dos botões de curtida, “Like Buttons”, disponibilizados para os provedores de conteúdo[35]. A maior parte dos websites contém ícones de redes sociais para que o visitante curta, compartilhe ou visite a comunidade daquele site na respectiva rede social. Comprovadamente, a inclusão destes botões de redes sociais auxilia na divulgação e no aumento de tráfego dos websites, razão pela qual a maioria dos sites opta por incluir botões de redes sociais.

Para que se compreenda o poder de rastreamento e captura de dados das redes sociais, que coletam dados de navegação dos usuários independentemente destes pressionarem os botões da rede social, utilizaremos o exemplo do ícone do Facebook no site de bibliotecas da Universidade de São Paulo (http://www5.usp.br/pesquisa/bibliotecas).

[35] O botão “Like” do Facebook é apenas um exemplo de conteúdo de terceiros (“third-party content”), que pode ser incorporado num website provedor de conteúdo e que é utilizado pela empresa terceira – no caso o Facebook – para rastrear a navegação do usuário. Qualquer outro conteúdo de terceiro embutido no código de uma página web é passível de operar de forma análoga.

Figura 5 - Botão Like no Site de Bibliotecas da USP

Observa-se na figura acima que o site de bibliotecas da USP, assim como boa parte dos websites, tem um botão de curtida (“Like”) onde o visitante pode clicar demonstrando seu apreço pelo conteúdo da página. Outras páginas podem disponibilizar o botão de compartilhamento (“Share”) que, para fins de rastreamento e captura de dados de navegação, funciona de forma análoga.

Ocorre que este ícone azul composto pela palavra “Like” e a letra “f” no lado esquerdo é uma imagem (arquivo) que não está hospedada nos servidores da USP, a figura não está armazenada no domínio usp.br. O referido ícone está armazenado nos servidores do Facebook e é carregado pelo navegador por meio de uma chamada aos servidores do Facebook, conforme se demonstra inspecionando o código fonte da página:

Figura 6 - Site de Bibliotecas da USP Conecta com Facebook

Portanto, é o Facebook que, no momento do carregamento do site, envia o ícone para compor o conteúdo da página de bibliotecas da USP. Os desenvolvedores do site da USP não incluíram a imagem do botão “Like” na página de bibliotecas, mas incorporaram no código fonte da página principal do site um trecho de código fornecido pelo Facebook que permite vincular o ícone apresentado à comunidade de bibliotecas da USP no Facebook. Durante a carga da página inicial, quando o código com o endereço do Facebook indicado na imagem acima é executado, o Facebook envia o ícone, a informação sobre a quantidade de “likes” atribuída até o momento ao site, bem como os cookies que são copiados para o dispositivo local do usuário. Em algumas situações pequenas fotos de amigos do usuário que também curtiram a página aparecem ao lado do ícone do Facebook, demonstrando que a carga do conteúdo é dinâmica e fornecida pelo Facebook.

O Facebook admite a coleta de informações por meio de cookies quando websites com botão “Like” são visitados pelo usuário:

> O Facebook recebe informações de cookies quando acesso um site com o botão Curtir ou outro plug-in social? Se você já tiver recebido um cookie do Facebook porque tem uma conta ou acessou o facebook.com, seu navegador nos enviará informações sobre esse cookie quando você acessar um site com o botão “Curtir” ou outro plug-in social. Usamos essas informações de cookies para ajudar a proporcionar uma experiência personalizada para você no site e também no Facebook, para ajudar a manter e melhorar nosso serviço e para proteger você e o Facebook contra atividades

> maliciosas. Excluímos ou anonimizamos essas informações dentro de 90 dias e não vendemos nem compartilhamos informações sem sua permissão.[36]

É importante ressaltar que o rastreamento por meio de cookies é feito independentemente do usuário clicar no botão “Like”. Basta que a página que contém a chamada externa para a carga do botão seja carregada para que o servidor do Facebook identifique que seu usuário acessou aquele website e capture e armazene esta informação. Estando o usuário cadastrado e permanentemente logado no Facebook este evento é imediatamente incorporado ao perfil do usuário. Caso o usuário esteja cadastrado no Facebook, mas não esteja logado, a informação pode ser atribuída ao perfil do usuário por meio da identificação do dispositivo. A identificação por meio de dispositivo é cada vez mais comum em razão da tendência cada vez maior de um dispositivo estar associado a apenas uma pessoa.[37]

Muitos usuários se surpreendem quando, após pesquisar preços de um determinado produto em lojas de varejo na internet utilizando um computador pessoal, verificam, pouco tempo depois, ao navegar numa rede social em seu dispositivo móvel, que os produtos outrora consultados em outro dispositivo aparecem sendo anunciados na rede social em seu celular. De fato, a loja virtual onde o produto foi consultado continha plug-ins da rede social, o que permitiu que esta rede social capturasse os dados de navegação vinculados ao usuário e, posteriormente, mesmo em outro dispositivo, veiculasse propaganda relacionada à navegação recente.

A captura de dados de navegação pelas redes sociais é questionável não apenas sob a perspectiva da construção de um perfil detalhado do usuário,

---

[36] FACEBOOK. Central de Ajuda. Disponível em: <https://www.facebook.com/help/206635839404055>. Acesso em: 22.03.2017

[37] No passado era muito comum que as pessoas de uma família compartilhassem um computador. Hoje cada membro da família tem seu dispositivo móvel e passa cada vez menos tempo no dispositivo compartilhado e cada vez mais tempo no dispositivo individual, o que facilita a identificação por meio do dispositivo ainda que circunstancialmente o usuário não esteja logado na aplicação (e.g. Facebook).

mas também sob o aspecto da vulnerabilidade do usuário da internet no tocante à coleta de dados sensíveis. A possibilidade técnica de coleta de dados sensíveis ficou evidente quando o Serviço Nacional de Saúde do Reino Unido (National Health Service) incluiu o botão “Like” do Facebook em suas páginas. Desta forma, quando o usuário pesquisa sobre uma determinada doença, o Facebook recebe esta informação de navegação independentemente do usuário pressionar o referido botão.

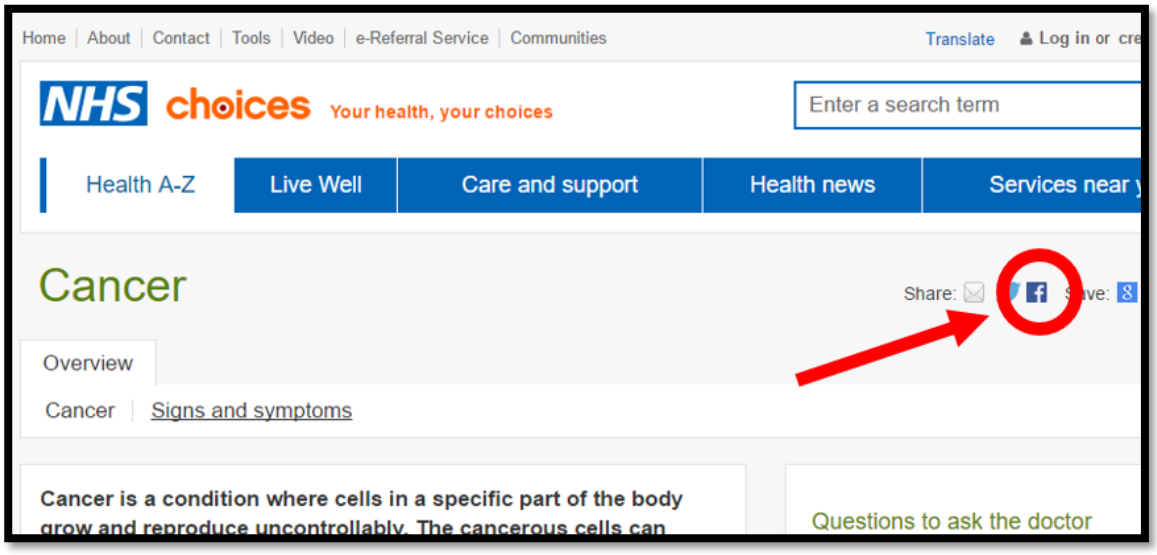

Figura 7 - Ícone do Facebook na Página Sobre Câncer do NHS

A inclusão de serviços de publicidade terceirizadas e rastreadores no site do NHS foi muito criticada em razão da natureza e sensibilidade das informações oferecidas e da possibilidade de rastreamento até mesmo dos dispositivos utilizados por pessoas que não são usuárias do Facebook:

> *Even if a visitor to NHS Choices is not logged into Facebook, the social networking site will still receive the person's IP address and operating system version, but not their user ID. Facebook will retain that data for 90 days before deleting it, an industry-accepted time frame.*[38]

[38] PC WORLD. NHS Link to Facebook Raises Privacy Concerns. Disponível em: <http://www.pcworld.com/article/211711/article.html>. Acesso em: 27.mar.2017.

Como afirmado, a coleta de dados de navegação é realizada durante a carga dos dados da página principal, independentemente do usuário clicar no botão "Like", como identifica ARNOLD ROOSENDAAL:

> *When data concerning web visits are combined based on the unique cookie, the browsing history of a web user can be mapped. The content is needed to load a page so, for tracking purposes, it is irrelevant whether a user actually clicks a piece of content or not, or whether the content is clickable at all.*[39]

Embora o Facebook afirme que mantém os dados capturados por rastreamento apenas por 90 dias, tal fato não pode ser comprovado e não é fiscalizado por autoridades independentes. Há, de fato, poucas chances de isso ser absolutamente verdade pois toda empresa, além de manter uma base de dados operacional, mantem também outros ambientes com estrutura semelhante (ambiente de testes, desenvolvimento, homologação, etc...), além de fazer backup integral e incremental periodicamente. Portanto, ainda que os dados fossem, de fato, apagados a cada 90 dias, seria possível restaurar um backup de mais de 90 para que se obtivesse, novamente, os dados coletados por rastreamento anteriores a este período.

2.2.4 Privacidade em Sites para Adultos

Questiona-se sobre a possibilidade técnica das empresas de internet incluírem no perfil do usuário informações sensíveis como, por exemplo, suas preferências sexuais.

Uma potencial fonte de informação para compor este delicado aspecto do perfil de um indivíduo seriam os websites de conteúdo adulto onde geralmente é possível, num campo de busca, filtrar o conteúdo por temas de preferência do usuário ou então acessar seções com categorias específicas. Ademais, seria possível inferir preferências sexuais do usuário pelo tempo gasto no consumo deste tipo de material.

---

[39] ROOSENDAAL, Arnold. We Are All Connected to Facebook . . . by Facebook! in: S. Gutwirth et al. (eds.), European Data Protection: In Good Health?, Heidelberg: Springer, 2012. p. 6.

A sensibilidade deste tema é muito acentuada pois há uma desaprovação geral em relação a conteúdos pornográficos por serem considerados imorais, contra os bons costumes e até mesmo crime em alguns países. Por conta desta reprovação social generalizada, poucos admitem que consomem material pornográfico na internet. No entanto, as estatísticas demonstram que o uso da internet para visualização de material pornográfico é muito mais comum do que se imagina.[40]

No Brasil, de acordo com o ranking da Alexia.com, o site de conteúdo adulto xvideos.com, figura entre os 25 sites mais acessados no país, à frente de sites como o do Banco do Brasil (bb.com.br), Itaú (itau.com.br) e Linkedin (linkedin.com.br). Dentre este grupo dos 25 mais acessados no Brasil o xvideos.com é o terceiro colocado no quesito "tempo diário de navegação no site por usuários" (10min24seg/dia), ficando ligeiramente atrás apenas de Facebook (12min27seg/dia) e OLX (12min26seg/dia).[41]

CHRIS JAY HOOFNAGLE, da UC Berkeley School of Information and School of Law, liderou um grupo de pesquisa com a finalidade de analisar o nível de privacidade ofertado pelos 11 mais populares sites de conteúdo adulto segundo o ranking da Alexia.[42] Como resultados relevantes da pesquisa, o grupo de estudo identificou que dos onze websites analisados, nove continham código de rastreamento do Google (DoubleClick ou Google Analytics) e sete websites

---

[40] O site pornhub.com, um dos maiores do mundo, publicou estatísticas de consumo apenas do seu site no ano de 2016: 91 bilhões de vídeos visualizados, 64 milhões de visitantes por dia, 4,6 bilhões de horas de visualização (equivalente a 5.246 séculos), 99 Gigabites de dados enviados por segundo. Se todos os dados transmitidos pudessem ser colocados em pen drives de 16Gb e estes fossem alinhados, percorreriam uma distância de 11.000 Km, o que corresponde a uma volta inteira na Lua. Disponível em: <https://www.pornhub.com/insights/2016-year-in-review>. Acesso em: 17.abr.2017.

[41] Top Sites in Brazil – By Country. Alexa. Disponível em: <http://www.alexa.com/topsites/countries/BR>. Acesso em: 12.abr.2017.

[42] ALTAWEEL, Ibrahim; GOOD, Nathan; HOOFNAGLE, Chris Jay. Privacy on Adult Websites. Workshop on Technology and Consumer Protection (ConPro '17), co-located with the 38th IEEE Symposium on Security and Privacy, San Jose, CA (2017). Disponível em: <https://ssrn.com/abstract=2851997>. Acesso em: 11.abr.2017.

vazavam termos de busca para terceiros, revelando, desta forma, a possibilidade técnica da Google reidentificar os usuários destes websites a partir de dados coletados do rastreamento de outros websites.[43]

A despeito destas observações, os analistas concluíram que a quantidade de cookies gerados por sites de conteúdo adulto é significativamente inferior à de sites de conteúdo diverso. Isso pode ser explicado pelo desinteresse de anunciantes associarem seus produtos ao conteúdo adulto.

Outro problema identificado pelos analistas à época foi a utilização do protocolo HTTPS em apenas dois dos onze websites analisados.[44] A utilização da tecnologia HTTPS impede que terceiros que eventualmente interceptem o conteúdo transmitido consigam acessá-lo, pois os dados trafegam numa camada de segurança com conexão criptografada.

Em março de 2017, após o congresso norte-americano aprovar a medida que permite às operadoras de internet – como Comcast e Verizon – venderem para terceiros os dados pessoais dos usuários, incluindo os dados de navegação[45], os sites pornôs Youporn e Pornhub anunciaram que passarão a utilizar o protocolo HTTPS[46], o que pode representar uma tendência para os demais sites do setor.

De qualquer forma, como observado, não é possível descartar a possibilidade técnica de que informações de comportamento online em sites adultos sejam também incorporados ao perfil do usuário.

---

[43] Idem, pg. 5.

[44] Idem, p. 10.

[45] How the Republicans Sold Your Privacy to Internet Providers. The New York Times Website. 29.03.2017. Disponível em: <https://www.nytimes.com/2017/03/29/opinion/how-the-republicans-sold-your-privacy-to-internet-providers.html?_r=0>. Acesso em: 17.04.17

[46] Por mais segurança, Pornhub e YouPorn passam a usar HTTPS. IDGNow. Disponível em: <http://idgnow.com.br/internet/2017/03/30/por-mais-seguranca-pornhub-e-youporn-passam-a-usar-https>. Acesso em: 17.abr.17.

2.2.5 A Política de Não Rastreamento ("Do Not Track")

Em 2010, a *Federal Trade Commission* (FTC) recomendou que fosse colocado à disposição dos usuários da internet um mecanismo por meio do qual fosse dada a opção de não rastreamento, de modo a impedir que as empresas de internet coletassem dados de comportamento online para fins de veiculação de publicidade direcionada ao perfil.[47]

A esta iniciativa foi dada o nome de "*Do Not Track*" (DNT), inspirada em iniciativa análoga de 2003 da FTC denominada "*Do Not Call Registry*" que permitia aos consumidores o registro de números de telefones para os quais as empresas de telemarketing estariam proibidas de realizar chamadas não solicitadas para oferecer produtos e serviços.

A iniciativa da FTC objetivava uma solução que fosse persistente, ou seja, que oferecesse um modelo por meio do qual uma vez manifestada a opção do usuário, esta não fosse alterada sem o consentimento dele (e.g. uma atualização de versão do navegador não poderia alterar automaticamente a opção do usuário).

Desta forma, a captura e utilização de dados de navegação do usuário não ficaria sujeita apenas à aceitação dos termos de uso ou da política de privacidade impostos unilateralmente pela empresa de internet. Por meio desta configuração do navegador, o usuário poderia manifestar sua vontade de não ter suas informações de navegação capturadas e utilizadas para quaisquer finalidades.

A especificação do padrão de DNT foi confiada ao World Wide Web Consortium (W3C), entidade dedicada ao estabelecimento de padrões para a internet. É evidente que as discussões sobre tais especificações tiveram como pano de fundo o conflito de interesses entre os organismos representativos dos consumidores e as entidades representativas das empresas de publicidade online.

Do ponto de vista técnico, a implementação da opção "DNT – Do Not Track", consiste inicialmente numa configuração do navegador onde o usuário

---

[47] FEDERAL TRADE COMMISSION. Do Not Track. Disponível em: <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track>. Acesso em: 03.nov.2017.

manifesta sua vontade de não ser rastreado (os navegadores mais difundidos têm esta opção de configuração). Posteriormente, durante a navegação, a opção do usuário é sempre informada pelo navegador ao servidor dos websites acessados pelo usuário. Desta forma, os provedores de conteúdo podem identificar as requisições de usuários que optaram pelo não rastreamento e, desta forma, podem agir em conformidade com esta manifestação de vontade.

O primeiro problema da política de DNT é o comprometimento das empresas de internet em aceitar a opção do usuário. Isso porque a ativação da opção não impede automaticamente o rastreamento, mas tão somente informa a empresa de internet (no caso o website que se está a acessar) que o usuário não deseja ser rastreado, sem garantia de que a empresa irá atender à manifestação de vontade do usuário consubstanciada na configuração de DNT.

No auge das discussões sobre a implementação do modelo, circulavam na internet várias listas de empresas que se comprometiam a observar a informação de DNT proveniente dos usuários.[48] De fato, atualmente admite-se que muitos provedores de conteúdo desconsideram a opção do usuário pelo DNT e fazem a captura de dados de navegação a despeito da expressa manifestação de vontade do usuário em sentido contrário. A possibilidade de não conformidade por parte das empresas de internet decorre da opção do FTC no sentido de priorizar a autorregulação no âmbito da proteção da privacidade do usuário de internet.[49]

O segundo problema que surgiu durante as discussões do modelo de DNT foi o debate semântico sobre o que significa estar em conformidade com o modelo. O que, exatamente, as empresas de internet deveriam (ou não deveriam) fazer ao receber a *flag* de DNT numa requisição de um usuário? Muitas empresas

---

[48] Uma destas listas está disponível em <http://donottrack.us/implementations>. Acesso em: 28.nov.2017.

[49] "The Commission's goal has been to understand this new marketplace and its information practices, to assess the impact of these practices on consumers, and to encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online." – Disponível em: <https://w2.eff.org/Privacy/199907_ftc_online_privacy_report.html>. Acesso em: 01.dez.2017.

interpretavam a requisição como meramente uma manifestação de vontade dos usuários no sentido de não receber publicidade direcionada, entendendo que seria, no entanto, permitida a captura de dados de navegação daquele usuário, sendo-lhes proibida apenas a veiculação de publicidade.[50] Diante desta discussão do FTC manifestou-se no sentido que *Do-Not-Track* significa não capturar dados e não apenas não direcionar publicidade.

A grande polêmica no âmbito do DNT se deu por ocasião do lançamento da versão 10 do Internet Explorer[51]. A declaração da Microsoft de que o novo navegador traria a opção DNT acionada como padrão de fábrica causou o furor das empresas de internet que, em seguida, declararam que desconsiderariam a opção de DNT vinda do referido navegador.[52]

A questão subjacente à polêmica do I.E. 10 é se o mercado deve presumir que a vontade do usuário se orienta no sentido da permissão de rastreamento lhe oportunizando a possibilidade de manifestação no sentido contrário, acionando a *flag* DNT (modelo conhecido como *opt-out*) ou se é razoável presumir que um novo usuário não deseja ser rastreado, ofertando-lhe a possibilidade de permitir o rastreamento através da configuração do navegador (*opt-in*).

Admitindo-se que poucos usuários têm conhecimento das referidas configurações e dos seus impactos na prática, as configurações padrão acabam, na maioria das vezes, não sendo alteradas pelos usuários. Como resultado, as

---

[50] "The advertising group ("Digital Advertising Alliance"), however, defines it (DNT) as forbidding the serving of targeted ads to individuals but not prohibiting the collection of data".... "Users who turn on the Do Not Track option in their browsers and visit a Yahoo Web site will not see targeted ads, the company said, but the site will collect user data." - Conflict Over How Open 'Do Not Track' Talks Will Be. Disponível em: <http://www.nytimes.com/2012/03/30/technology/debating-the-path-to-do-not-track.html>. Acesso em: 01.dez.2017

[51] A Microsoft informou em seu blog sobre as novas características da versão 10 do seu navegador, o Internet Explorer: "IE10 also sends the "Do Not Track" signal to Web sites by default to help consumers protect their privacy.". Disponível em: <https://blogs.msdn.microsoft.com/ie/2012/05/31/windows-release-preview-the-sixth-ie10-platform-preview/>. Acesso em: 28.nov.2017.

[52] "Roy Fielding, an author of the Do Not Track (DNT) standard and principal scientist at Adobe Systems, wrote a patch for Apache that sets the Web server to disable DNT if the browser reaching it is Internet Explorer 10. "Apache does not tolerate deliberate abuse of open standards," Fielding titled the patch." – Disponível em <http://news.cnet.com/8301-1023_3-57508351-93/apache-web-software-overrides-ie10-do-not-track-setting>. Acesso em: 01.nov.2017

ferramentas disponíveis para a proteção da privacidade são entregues inativas por *default* e desta forma permanecem na maioria dos casos.

As configurações padrão de um navegador que representem uma manifestação de vontade do usuário em suas relações com as empresas de internet podem ser equiparadas, juridicamente, ao valor do silêncio no âmbito contratual. Nas situações em que o usuário se cala diante de uma opção de privacidade, adotando a configuração padrão, qual é o comportamento razoável a ser esperado das empresas envolvidas? É evidente que se tivermos em mente apenas a tutela da privacidade e dos dados pessoais, recomendar-se-ia opções padrão mais protetivas. No entanto, não só aqui como em todo este trabalho, o debate subjacente é o de ponderação entre a privacidade (proteção de dados pessoais) e o desenvolvimento científico e benefício social supostamente derivado da grande coleta de dados dentro e fora da internet.

JOSHUA FAIRFIELD defende que os navegadores, como o IE 10, possam conter, por padrão, a opção de DNT habilitada. Ele entende que o consumidor, em vez de selecionar a opção DNT no seu navegador, pode optar pela utilização de um navegador que tenha como característica opções padrão que garantam maior privacidade:

> *A consumer's choice to use a pro-privacy browser is a better indication of consent than is silence. (...) A pro-privacy browser is a better reflection of the desires of its users than is the TPE (Tracking Preferences Expression). (...) Just as consumers should be able to choose cars with a combined feature set that makes them fast, consumers should be able to choose browsers with a combined feature set that makes them private.*[53]

A proteção da privacidade do usuário num ambiente de autorregulação deveria se orientar por premissas que conjugassem razoabilidade e minimização

---

[53] FAIRFIELD, Joshua A.T. Do-Not-Track as Default. Northwestern Journal of Technology and Intellectual Property, Vol. 11, No. 7, 2013. p. 585 e 588. Disponível em: <http://ssrn.com/abstract=2338028>. Acesso em: 01.nov.2017.

dos custos de transação. Presumindo-se que o consumidor prefere não ser rastreado[54], esta conjugação levaria à adoção de um padrão de configuração do navegador com maior nível de privacidade, ou seja, com a opção DNT acionada por padrão.

Do ponto de vista do contrato de adesão, a opção DNT poderia ser interpretada como uma cláusula que reflete a vontade do usuário à qual as empresas de internet podem ou não aderir. O usuário opta por não ser rastreado e transmite esta informação a todos os websites que deseja acessar. O servidor do website interpreta a vontade do usuário (DNT *flag* acionada) e pode, se discordar das restrições impostas pelo usuário, negar acesso ao conteúdo do website, comportamento idêntico ao de vários websites que negam acesso aos usuários que configuram o navegador para não receber cookies ou acionam extensões de bloqueio (e.g. Adblock Plus).

2.2.6 Flash Cookies

Muitos usuários, na tentativa de preservarem a privacidade e impedirem o fluxo de dados para as empresas de internet, limpam constantemente o histórico de navegação e removem os cookies do dispositivo local. Todos os navegadores têm opções para a remoção destes dados que ficam armazenados localmente no dispositivo. Diante desta possibilidade, as empresas de internet desenvolveram tecnologias para impedir que o usuário obstrua o fluxo de dados do seu computador para os servidores da rede.

Uma forma engenhosa para obter este resultado foi o desenvolvimento dos Flash Cookies, também conhecidos como LSO (*Local Shared Objects*). Estes arquivos têm a mesma função dos cookies: armazenar informações de navegação. No entanto, eles não aparecem na lista de cookies apresentada pelo navegador e,

---

[54] Em pesquisa conduzida pela The Pew Internet & American Life, observou-se que 68% dos entrevistados responderam “I’m NOT OKAY with targeted advertising because I don’t like having my online behavior tracked and analyzed” - PURCELL, Kristen; BRENNER, Joanna; RAINIE, Lee. Search Engine Use 2012. p. 2. Disponível em: <http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf>. Acesso em: 01.dez.2017.

quando o usuário apaga todos os cookies tradicionais usando a opção apropriada do navegador, os Flash Cookies (LSOs) permanecem indeléveis.

Desta forma, os Flash Cookies também têm a função de restaurar eventuais Web Cookies que tenham sido apagados pelos usuários, servindo também como backup dos cookies removidos. Cookies com a função de restaurar aqueles apagados pelos usuários são conhecidos como Cookies Zumbi.

A tecnologia de Flash Cookies foi desenvolvida há aproximadamente 10 anos pela Macromedia, posteriormente adquirida pela Adobe e foi utilizada largamente por diversos sites. Os criadores da tecnologia bem como as empresas de internet que dela se utilizam para o rastreamento geralmente apresentam esta solução como uma forma de melhorar a experiência do usuário na internet. A Adobe® descreve o uso desta tecnologia da seguinte forma:

> *Do ponto de vista técnico, os cookies são chamados de "cookies HTTP". Existem outras tecnologias que podem ser usadas para fins similares, como armazenamento local com HTML5 e objetos compartilhados localmente (LSOs). Os LSOs são utilizados pelos autores de arquivos lidos pelo Adobe® Flash® Player e por sites que hospedam esses. Podemos usar armazenamento local com HTML5, LSOs e tecnologias semelhantes para autenticar você, acompanhando as informações que você nos forneceu e lembrando suas preferências. Quando você estiver usando um aplicativo off-line da Adobe, podemos armazenar informações relacionadas ao uso do site no seu dispositivo e, em seguida, transferi-las para nossos servidores na próxima vez em que você se conectar ao nosso serviço.*[55]

Logo após a introdução desta tecnologia de rastreamento observou-se um desconforto no mercado e uma insatisfação de usuários, o que acabou gerando ações judiciais contra várias empresas que utilizavam esta tecnologia para rastrear os internautas, dentre elas a NBC Universal e o Walt Disney Internet Group.[56]

---

[55] Adobe Website. Utilização de cookies e tecnologias similares. Centro de Privacidade da ADOBE. Disponível em: <http://www.adobe.com/br/privacy/cookies.html>. Acesso em: 05.abr.2017.

[56] The New York Times Website. Code That Tracks Users' Browsing Prompts Lawsuits. Disponível em: <http://www.nytimes.com/2010/09/21/technology/21cookie.html>. Acesso em: 05.abr.2017.

É de se destacar que a capacidade de armazenamento de um Flash Cookie (LSO) é 25 vezes superior à de um Web Cookie. Este pode armazenar, no máximo, 4Kb enquanto o flash cookie pode armazenar 100Kb.

2.2.7 HTML5

Na primeira metade da década de 2010 houve um declínio na utilização dos Flash Cookies e um aumento no uso da nova tecnologia, o HTML5.

A linguagem HTML é uma linguagem utilizada para a apresentação de conteúdos num navegador. A especificação desta linguagem é realizada pelo W3C (World Wide Web Consortium), uma organização internacional que congrega empresas de tecnologia, órgãos do governo e organizações independentes para especificar padrões de internet.

Os navegadores compatíveis com o HTML versão 5 (HTML5) alocam um espaço extra para o armazenamento de dados locais. O espaço mínimo para armazenamento de dados locais é de 5MB, mas alguns navegadores permitem a alocação de um espaço maior.[57]

Um estudo publicado em dezembro de 2015 pela Technology Science (www.techscience.org), jornal online da Harvard University's Data Privacy Lab, denominado "Web Privacy Census"[58] trouxe informações sobre a evolução das tecnologias de rastreamento utilizadas atualmente em comparação com aquelas utilizadas na época da publicação do estudo anterior (Web Privacy Census 2012).

---

[57] O Google Chrome, por exemplo, possibilita que os desenvolvedores aloquem espaço de forma ilimitada, bastando que haja espaço no disco rígido do usuário para o armazenamento de informações persistentes. Chrome DevTools Website. Managing HTML5 Offline Storage. Disponível em: <https://developer.chrome.com/apps/offline_storage>. Acesso em: 05.abr.2017.

[58] ALTAWEEL, Ibrahim; GOOD, Nathan; HOOFNAGLE, Chris Jay. Web Privacy Census (December 15, 2015). Technology Science. 2015121502, Online. Disponível em: <https://ssrn.com/abstract=2703814>. Acesso em: 04.abr.2017.

Este estudo foi realizado utilizando softwares para simular a navegação nos websites mais populares registrando os mecanismos de rastreamento de cada um deles. Foram obtidos os seguintes resultados relevantes:

a) Ao visitar os maiores 100 websites[59] foi possível coletar 6.000 web cookies, ou seja, uma média de 60 cookies por website. Para fins de comparação, em 1997 apenas 24 dos maiores 100 websites gravavam cookies.[60]

b) Do total de cookies coletados, 83% são de terceiros (*third-party cookies*) que representam 275 empresas de internet que fazem rastreamento por meio destes 100 websites.

c) Dentre todos estes terceiros, a infraestrutura de rastreamento da Google é a mais presente, sendo encontrada em 92% de todos os sites visitados.

d) Embora a maior parte destes websites utilizem web cookies para rastreamento, 34% dos websites utilizam também armazenamento HTML5, o que representa um aumento de 50% na utilização desta tecnologia em comparação com o estudo de 2012.

A tabela abaixo resume as principais conclusões do estudo desenvolvido pela Technology Science:

a) A utilização de web cookies continua crescendo e com uma participação ainda maior dos cookies de terceiros.

b) Houve uma diminuição na quantidade de empresas terceiras que fazem o rastreamento observando-se, em paralelo, um aumento significativo da infraestrutura de rastreamento da Google.

---

[59] Os sites analisados foram os de melhor posição no ranking da Quantcast (https://www.quantcast.com/top-sites).

[60] "Of the 100 sites, 24 enable cookies. The cookies feature is often used for registration and password storing, but may also be used to create logs of user interests and preferences" - Electronic Privacy Information Center Website. Surfer beware: personal privacy and the internet. Washington, DC. 1997. Disponível em: <https://epic.org/reports/surfer-beware.html>. Acesso em: 05.abr.2017.

c) Não houve aumento significativo na utilização de Flash Cookies no período provavelmente em razão da adoção em massa da nova tecnologia para rastreamento (HTML5).

Crawl Date	October 2012	October 2015	Trend
Do all popular sites have cookies	Yes	Yes	--
Sites with 100 or more cookies	21	45	up
Sites with 150 or more cookies	11	36	up
Percentage of cookies set by a third party host	84.7%	93.5%	up
Number of third party hosts	457	322	down
Number of top websites with a Google presence	74	92	up
Number of sites with flash cookies	11	10	down
Number of sites with html5 storage	38	76	up
Number of sites without third party cookies	5	6	up

Figura 8 - Alterações e Tendências nas Tecnologias de Rastreamento entre 2012 e 2105

2.3 O Armazenamento dos Dados Pessoais (Big Data)

Denomina-se Big Data[61] o conjunto muito grande e complexo de dados geralmente distribuídos em diversos servidores de banco de dados. Embora a denominação Big Data sugira uma referência apenas ao gigantesco conjunto de dados, fica implícito neste termo a existência de tecnologia capaz de não apenas obter, mas também processar, analisar e produzir informações a partir da massa de dados.

Isso significa que a denominação “Big” pode ser aplicada a dois aspectos desta estrutura: O primeiro é a gigantesca quantidade e variedade de dados

[61] Nas poucas vezes em que o termo “Big Data” é traduzido para o português costuma-se utilizar a expressão “Megadados”.

disponíveis para consulta e processamento e o segundo é a diversidade de formas, métodos e algoritmos usados para, por meio de processamento, fazer inferências, categorizar e estabelecer conclusões a partir dos dados. É como se um cozinheiro dispusesse não apenas de uma grande quantidade de ingredientes, mas também contasse com inúmeras receitas ou “modo de fazer”.

O McKinsey Global Institute define Big Data como os “datasets whose size is beyond the ability of typical database software to capture, store, manage and analyse”[62]. Esta definição chama a atenção para as duas características principais do Big Data: a grande massa de dados e as ferramentas apropriadas para a análise destes dados.

Outro aspecto importante do Big Data é o fato dos dados estarem distribuídos, ou seja, não estão necessariamente num único banco de dados. De fato, os dados pessoais capturados dos usuários da internet são armazenados em diversos servidores os quais são acessados pelas ferramentas de análise de dados.

Atualmente coleta-se dados de várias fontes a todo momento: dados de transações comerciais, dados das redes sociais, dados de sensores e dados de comunicação entre equipamentos. A análise e correlação de dados desta massa podem produzir predições, probabilidades e tendências. A este conjunto de análises a literatura confere a denominação de mineração de dados (*data mining*).

Os benefícios sociais e comerciais da mineração de dados são cada vez mais evidentes. Na área de saúde, por exemplo, foi como resultado da análise de um banco de dados da Kaiser Permanente, operadora de saúde dos Estados Unidos, com 1,4 milhões de pacientes que foi possível correlacionar aproximadamente 27 mil ataques cardíacos e mortes súbitas com o uso do anti-

---

[62] HEEGER, Eva. Controlling Your Online Profile: Reality or an Illusion? A Research into Informed Consent as a Mechanism to Regulate Commercial Profiling. 2005. Disponível em: <http://ssrn.com/abstract=2658651>. Acesso em: 12.dez.2017. p. 4.

inflamatório Vioxx, produzido pela farmacêutica Merck, medicamento que, posteriormente, foi removido do mercado.[63]

Outro exemplo clássico, desta vez relacionado com a captura de dados de navegação, foi o *Google Flu Trends*. Este serviço previa a difusão de gripe temporal e espacialmente com base em registros de pesquisas realizadas por usuários na ferramenta de buscas da Google. Alvo de muitas críticas[64], tanto relacionadas com a privacidade quanto relacionadas com a eficácia, ou seja, com relação a sua real capacidade de prever com precisão a propagação da doença, o serviço foi interrompido pela Google que, posteriormente, disponibilizou publicamente os dados capturados de forma agregada para fins de pesquisa científica.

Embora as tecnologias de análise de dados sobre o Big Data tenham o potencial de trazer muitas vantagens, há uma grande preocupação em razão da perda da privacidade informacional. OMER TENE e JULES POLONETSKY observam que estas preocupações se agravam diante da possibilidade do compartilhamento destes dados:

> *The harvesting of large data sets and the use of analytics clearly implicate privacy concerns. The tasks of ensuring data security and protecting privacy become harder as information is multiplied and shared ever more widely around the world. Information regarding individuals' health, location, electricity use, and online activity is exposed to scrutiny, raising concerns about profiling, discrimination, exclusion, and loss of control.*[65]

Ainda que se busque refúgio na anonimização de dados, estudos que serão apresentados posteriormente apontam para as tecnologias de

---

[63] USA Today Website. How did Vioxx debacle happen? 10.dez.2004. Disponível em: <http://usatoday30.usatoday.com/news/health/2004-10-12-vioxx-cover_x.htm>. Acesso em: 02.dez.2017

[64] Forbes Website. Why Google Flu Is A Failure. 23.mar.2014. Disponível em <http://www.forbes.com/sites/stevensalzberg/2014/03/23/why-google-flu-is-a-failure/#1305d46c344a>. Acesso em: 02.dez.2017

[65] TENE, Omer; POLONETSKY, Jules. Privacy in the age of big data: a time for big decisions, Stanford Law Review Online 64, 2012. Disponível em: <http://www.stanfordlawreview.org/online/privacy-paradox/big-data> Acesso em: 02.dez.2017, p. 65

desanonimização que, utilizando-se de correlação com dados relacionados aos indivíduos, são capazes de reidentificar o sujeito relacionado a um conjunto de dados outrora anônimo, o que derruba a falsa premissa segundo a qual os dados anônimos poderiam estar fora do âmbito de proteção dos dados pessoais.

2.4 O Processamento dos Dados Pessoais

O estudo conduzido pelo FTC[66] sobre o funcionamento dos Data Brokers revelou aspectos relevantes não apenas sobre como os dados são obtidos, mas também sobre como são mantidos, atualizados e processados.

O aspecto mais significativo do processamento dos dados pessoais é a geração de dados derivados realizada pelos *Data Brokers* por meio de complexos algoritmos. A partir dos dados crus (*raw data*), obtidos de diversas fontes públicas e privadas, os *Data Brokers* inferem aspectos de interesse dos indivíduos agrupando-os em diversas categorias. A análise realizada pelo FTC concluiu que os *Data Brokers* comercializam não apenas dados crus, mas também os dados derivados.[67]

Os *Data Brokers* utilizam modelos complexos de análise de dados para prever determinados comportamentos. Por exemplo, o modelo preditivo parte de um grupo de consumidores que adquiriu um determinado produto e, a partir desta informação, verifica os atributos comuns dos membros deste grupo. Desta forma podem inferir que outros indivíduos que compartilham destas características terão propensão para adquirir aquele produto.

Os algoritmos utilizados para deduzir padrões a partir dos dados coletados combinam elementos para criar categorias de consumidores com características similares num alto nível de detalhe como, por exemplo, a categoria

---

[66] FEDERAL TRADE COMMISSION. Data brokers: a call for transparency and accountability. Maio 2014. Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em: 06.dez.2017.

[67] Ibidem. p. 19.

“Soccer Moms” que inclui mulheres entre 21 e 45 anos com filhos que nos últimos dois anos comprou produtos esportivos.

Cada categoria criada pelos *Data Brokers* pode ter diversos atributos como segmento étnico, estado civil, nível de renda, ideologia política, faixa etária, etc... Como exemplo, extraído do estudo do FTC, cita-se a categoria “Rural Everlasting” que inclui mulheres ou homens solteiros com idade acima de 66 anos com baixo grau de educação e baixa renda.[68]

O estudo do FTC também concluiu que os *Data Brokers* que fornecem informações aos usuários sobre seus dados pessoais apenas o fazem de maneira parcial, ou seja, dão acesso a um conjunto limitado de dados crus, mas não informam de forma plena as categorias às quais o usuário foi incluído por meio do processamento e das inferências, ou seja, quando instados pelo indivíduo a exibir os dados pessoais que estão em seu poder, os *Data Brokers* exibem apenas dados crus e não os dados derivados.[69]

A diversidade de técnicas existentes (e futuras!) para o tratamento de dados crus e geração de dados derivados nos leva à conclusão de que no momento da coleta dos dados é impossível prever a quantidade e tipos de dados que desta massa podem derivar. Isso porque muitas informações poderão ser geradas a partir da combinação futura de mais de um conjunto de dados e também porque algoritmos de análise podem ser desenvolvidos em momento posterior ao da coleta dando ensejo à geração de novos dados derivados não idealizados no momento da captura dos dados originais. Ainda retomando a analogia do cozinheiro, é impossível saber a priori os pratos que poderão ser preparados quando houver mais ingredientes e mais receitas.

2.5 A Utilização dos Dados Pessoais

O interesse último das empresas de internet que coletam dados pessoais e dados de navegação não está nestes dados propriamente ditos, mas no conhecimento e informações que eles podem gerar. Como visto, a partir da

---

[68] Ibidem. p. 20.
[69] Ibidem. p. 42.

combinação de uma grande quantidade de dados é possível classificar um indivíduo sob diversos aspectos, incluindo-o em categorias ou grupos sobre os quais alguma ação será tomada. Na medida em que uma quantidade maior de dados é coletada ou recebida de outras empresas por compartilhamento, o perfil do indivíduo é aperfeiçoado possibilitando traçar conclusões sobre tendências e previsões de comportamento do indivíduo e dos grupos aos quais ele pertence. Pode-se afirmar que as empresas de internet estão a desenvolver uma biografia não autorizada de cada usuário de internet, uma biografia detalhada como poucos de nós poderia produzir de si mesmo.

As informações geradas a partir do processo de *profiling* são utilizadas para a tomada de decisão. O direcionamento de propaganda alinhada ao perfil do usuário é apenas a mais propalada das inúmeras decisões que podem ser tomadas a partir das informações geradas no processo de *profiling*.

As grandes empresas de internet, como Facebook e Google, adotaram um modelo de negócios que permite a oferta de serviços grátis ao usuário final. Este modelo, no entanto, prevê o recebimento de receitas dos anunciantes que veiculam propaganda direcionada ao perfil. Como exemplo, uma montadora de veículos poderá destinar uma campanha publicitária de sua nova pick-up esportiva para usuários homens entre 25 e 45 anos que tenham interesses em automobilismo e tenham feito pesquisas por veículos de outras montadoras nos últimos meses. O benefício da eficiência na veiculação de publicidade direcionada ao perfil é pago com os inconvenientes e riscos da concessão de dados pessoais. Desta forma, pode-se afirmar que o usuário final paga pelos serviços de internet com os seus dados pessoais.

Embora a utilização de dados pessoais para a veiculação de publicidade específica possa parecer algo inofensivo ou, até mesmo, benéfico para o usuário, a grande massa de dados que forma o perfil do usuário pode ser destinada a outros fins não declarados que ofereçam maior risco ao sujeito relacionado aos dados. Há grande preocupação sobre decisões tomadas exclusivamente de forma automática a partir dos dados coletados que venham afetar a posição jurídica do indivíduo. Tome-se como exemplo situações em que, a partir das informações de *profiling*,

geradas sem intervenção humana, uma empresa negue a celebração de um contrato ou estabeleça preços mais elevados por entender que o consumidor pertence a um grupo que está numa posição da curva de demanda e oferta onde se dispõe a pagar mais pelo mesmo serviço. Evidentemente, em tais situações teríamos o método de *online profiling* gerando discriminação e desvantagem na esfera jurídico-econômica do sujeito relacionado aos dados.

Com vistas a evitar violações aos direitos do consumidor, as novas leis de proteção de dados pessoais têm incluído dispositivos que vedam a tomada de decisões exclusivamente automatizadas que colocam em risco os direitos dos consumidores. Ademais, estas iniciativas incluem dispositivos que determinam a análise e mitigação de riscos aos consumidores, como será visto mais adiante.

2.6 O Compartilhamento dos Dados Pessoais

As empresas de internet que coletam dados pessoais de usuários reiteradamente informam que o fazem para melhorar a qualidade dos serviços. A Google, por exemplo, alega que coleta dados pessoais, do dispositivo e de navegação para melhorar a experiência do usuário completando automaticamente as pesquisas, encontrando vídeos pelos quais o usuário se interesse, completando automaticamente formulários do navegador (Chrome) e levando mais rápido aos lugares usando Google Maps.[70]

No entanto, os dados coletados pelas empresas de internet não são apenas utilizados pela empresa que os coletou. Facebook[71] e Google[72], por exemplo, admitem que compartilham dados com terceiros.

---

[70] GOOGLE. Seus Dados. Disponível em: <https://privacy.google.com/your-data.html>. Acesso em 26.abr.2017.

[71] O Facebook declara que compartilha "informações pessoais não identificáveis" com parceiros e clientes terceiros. Nesta categoria estão, segundo o Facebook, os seguintes tipos de terceiros: Serviços de publicidade, medição e análise e fornecedores, provedores de serviço e outros parceiros. Disponível em: <https://www.facebook.com/full_data_use_policy>. Acesso em 03.dez.2017.

[72] A Google, em sua política de privacidade, afirma que não compartilha informações pessoais com empresas, organizações e indivíduos externos à Google, SALVO em algumas situações. Uma destas situações é para "processamento externo" feito por "pessoas confiáveis para

A difusão das redes sociais e o aumento no uso da internet para diversas finalidades aumentou consideravelmente a quantidade de dados pessoais rastreados e compartilhados, o que chamou a atenção da Federal Trade Commission que, em 2014, elaborou um estudo sobre as empresas que mantêm as maiores bases de dados pessoais no mundo, os *Data Brokers*.[73]

Neste estudo foram analisadas as práticas dos nove maiores *Data Brokers*, a saber, Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, e Recorded Future.

Como resultado do estudo concluiu-se que mais da metade dos *Data Brokers* rastreiam redes sociais para capturar dados pessoais.[74] Além disso, sete dos nove *Data Brokers* analisados compartilham dados entre si.[75]

Em 2013 o Facebook firmou um acordo de compartilhamento de dados com alguns *Data Brokers*, dentre os quais Acxiom e Datalogix, o que suscitou preocupação com relação à privacidade dos usuários. Em nota intitulada “Advertising and our Third-Party Partners”, o Facebook alega que as parcerias com *Data Brokers* têm o objetivo de veicular publicidade relevante para o usuário e que fornece ferramentas disponíveis para que usuário tenha controle sobre os anúncios que lhe são exibidos.[76]

O fato é que a forma como os dados são coletados e compartilhados bem como quais são as fontes e o uso que deles é feito não é algo transparente

---

processá-las para nós". Disponível em: <https://www.google.com/intl/pt-BR/policies/privacy/#nosharing>. Acesso em 03.dez.2017.

[73] FEDERAL TRADE COMMISSION. Data brokers: a call for transparency and accountability. Maio 2014. Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em: 06.dez.2017.

[74] Ibidem. p. 13

[75] Ibidem. p. 14

[76] GOOGLE. Advertising and our Third-Party Partners. Disponível em: <https://www.facebook.com/notes/facebook-and-privacy/advertising-and-our-third-party-partners/532721576777729/>. Acesso em: 26.abr.2017

para o usuário, o que levou à FTC recomendar maior transparência no setor de *Data Brokers*:

> *As the Commission outlines in today's report, many data broker practices fall outside of any specific laws that require the industry to be transparent, provide consumers with access to data, or take steps to ensure that the data that they maintain is accurate. The Commission's legislative recommendations, if enacted into law, would add transparency across the data broker industry, provide more information about the sources of data brokers' information, help give consumers appropriate access and the ability to correct data used for marketing and risk mitigation products, and give consumers greater ability to correct data in their people search profiles. In addition, the report encourages data brokers to be more accountable by conducting due diligence on their customers' use of the data, and creating contractual requirements that prohibit their customers from using the data in an unlawful manner.*[77]

[77] FEDERAL TRADE COMMISSION. Data brokers: a call for transparency and accountability. Maio 2014. Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em: 06.dez.2017. Apendix C. p. C-3 e C-4.

3 IMPACTOS DO ONLINE PROFILING

3.1 Riscos de Dano no Uso Indevido dos Dados

Questiona-se sobre prejuízo real para o indivíduo em decorrência da geração de seu perfil digital pelas empresas de internet. Não se prestariam, tais dados, apenas para a veiculação de propaganda relevante ao sujeito relacionado aos dados? Que danos o *online profiling* poderia causar aos usuários de internet?

Com a agregação de dados e criação de perfis inaugura-se uma gama de possibilidades de uso para as informações. Geralmente, o resultado do *profiling* é o enquadramento do usuário em um conjunto de categorias. Esta categorização nem sempre é precisa, o que significa que um indivíduo pode ser enquadrado em categorias às quais ele não deveria pertencer. Decisões automatizadas em função da relação de pertinência do usuário com estas categorias podem significar discriminação, estigmatização e estratificação social. Falsas conclusões em razão de inferências equivocadas podem trazer danos para a esfera jurídica do sujeito relacionado aos dados.

DANILO DONEDA aponta as consequências do aumento da capacidade de armazenamento de informações e do desenvolvimento de técnicas de processamento (*data mining*):

> *Esta dinâmica apresenta claras implicações no que interessa às informações pessoais. Aumenta a quantidade de informação disponível sobre uma pessoa, informações que podem influenciar sua vida futura – uma simples busca na Internet pelo nosso nome ou pelo de pessoas conhecidas pode, em vários casos, elucidar o significado prático do registro aleatórios de informações a nosso respeito. Ganha peso a imagem do computador como o cão de guarda da sociedade da informação, que não esquece jamais.*[78]

Cada indivíduo exerce uma multiplicidade de papéis na sociedade em que vive: o mesmo indivíduo pode atuar profissionalmente como técnico em sua área de especialização, como voluntário na instituição religiosa a qual pertence, como pai no âmbito familiar, como amigo na mesa de um restaurante. Para cada

---

[78] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 177-178.

papel que exerce, atua com distinta disposição mental e psicológica. Projeta-se como indivíduo de forma diferenciada ao exercer cada papel: tom de voz, indumentária, vocabulário, senso de humor. Via de regra a conduta e atributos demonstrados em cada *locus* social não deveria invadir outras esferas: a conduta e características do indivíduo como esposo não deveriam ser reveladas em seu ambiente de trabalho assim como o vocabulário e disposição de ânimo neste ambiente não deveria ser revelado diante da comunidade religiosa. Este parece ser o desejo de todo o indivíduo: que suas características de personalidade e conduta em cada esfera estejam adstritas àquele âmbito de atuação. Tem havido, neste sentido, uma relativa "proteção de dados pessoais" de um mesmo indivíduo entre as várias esferas.

O *online profiling*, no entanto, não respeita esta segregação, o que pode, invariavelmente, causar constrangimento ao indivíduo que utiliza a internet para a sua atuação em múltiplos papéis sociais. Esta confusão de atributos de diversos papéis pode levar a uma visão distorcida do indivíduo, principalmente se os dados derivados de determinados atributos de um aspecto social forem utilizados para julgá-lo em relação a outro papel social.

3.2 Críticas ao Paradigma da Proteção Via Anonimização

Uma forma muito difundida de proteção de dados pessoais é a anonimização ou deidentificação[79]. O objetivo das técnicas de anonimização é impossibilitar ou dificultar a identificação do sujeito relacionado a um determinado conjunto de dados. Tome-se, como exemplo, uma tabela de base de dados, com as seguintes informações coletadas de pacientes atendidos num determinado hospital em 01/01/2016:

Nome	Sexo	CEP	Nascimento	Sintoma

[79] A versão em português do novo Regulamento Europeu (Regulamento (EU) 2016/679) traz a denominação "pseudonimização" (Ver considerandos 26, 28, 29, 75, 78, 85, 156 do preâmbulo e os artigos 6.4.e, 25.1, 32.1.a, 40.2.d e 89.1). O artigo 5.5 define "Pseudonimização" como "o tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável."

Sérgio Freitas	M	02345-000	23/03/1946	Hipertensão
Hellen Garcia	F	14534-010	14/08/1988	Febre
Felipe Cardoso	M	44398-110	30/01/1978	Dor nas costas
Gustavo Maia	M	02345-020	04/02/1972	Dor no peito
Julia Pereira	F	14534-010	31/12/2000	Tosse
Maristela Silva	F	02345-020	22/09/1997	Febre

Tabela 1

Esta massa de dados pode ser remetida para análise em outras instituições. No entanto, por haver dados sensíveis relacionados a sujeitos identificados, utiliza-se técnicas de anonimização para garantir a privacidade dos pacientes. A técnica mais comum de anonimização é a supressão de dados, ou seja, a remoção dos dados que permitem identificar o sujeito relacionado aos dados. No caso da tabela acima, a aplicação da técnica de supressão significaria a exclusão da coluna “Nome”, o que resultaria no envio da seguinte tabela para a análise de terceiros:

Sexo	CEP	Nascimento	Sintoma
M	02345-000	23/03/1946	Hipertensão
F	14534-010	14/08/1988	Febre
M	44398-110	30/01/1978	Dor nas costas
M	02345-020	04/02/1972	Dor no peito
F	14534-010	31/12/2000	Tosse
F	02345-020	22/09/1997	Febre

Tabela 2

Há outras técnicas de anominização como, por exemplo, a agregação. Com esta técnica os dados detalhados são consolidados em categorias para posterior disponibilização. Como resultado, após a manipulação cada linha não mais fará referência a um indivíduo, mas sim a um conjunto de indivíduos, dificultando significativamente a reidentificação. No entanto esta técnica limita significativamente a liberdade do analista de dados. Uma forma de anonimização

por agregação seria a tabela abaixo que indica a quantidade de pacientes apresentando determinados sintomas em 01/01/2016:

Sintoma	Quantidade de Pacientes
Hipertensão	1
Febre	2
Dor nas costas	1
Dor no peito	1
Tosse	1

Tabela 3

A desanonimização – processo inverso ao da anonimização – é aquele por meio do qual, a partir de uma massa de dados anonimizada, pode-se reidentificar os sujeitos relacionados aos dados. Quanto maior a possibilidade de reidentificação menor o grau de proteção dos sujeitos relacionados aos dados.

Percebe-se claramente que o grau de proteção dos dados pessoais no processo de anonimização via agregação exemplificado na tabela 3 é bem superior àquele que apenas suprimiu o nome do paciente.

De fato, demonstrar-se-á oportunamente que a partir de um conjunto de atributos, ainda que cada atributo isoladamente não identifique o sujeito, é possível que este seja identificado a partir do conjunto de outros dados. Por exemplo, é possível identificar um grande percentual dos indivíduos apenas a partir do trio CEP, data de nascimento e sexo. Esta possibilidade é real na medida em que haja outras bases de dados, de fontes diversas, que podem ser agregadas à base do hospital anonimizada por supressão.

Ocorre que quanto mais segura for a técnica de anonimização menos úteis serão os dados para análises. Uma base de dados fortemente anonimizada por agregação pouca utilidade terá nas mãos de um analista de dados que trabalha para deduzir padrões e estabelecer correlações úteis. Suas chances de obter alguma conclusão útil partindo de dados crus não agregados são bem maiores do que se os dados tiverem sido agregados ou fortemente anonimizados. Um analista de dados preferiria receber os dados da Tabela 2 supra a receber os da Tabela 3.

PAUL OHM (2010) demonstrou em seu paradigmático artigo *Broken Promises of Privacy*[80] que na medida em que novas bases de dados se tornam acessíveis em diversas fontes e são agregadas ao banco de dados original, é possível desanonimizar ou reidentificar os sujeitos relacionados às informações constantes de bases anonimizadas.[81] De fato, tal possibilidade é real pois ainda que numa base anonimizada não se observe dados de identificação pessoal tais como nome, CPF, RG – geralmente denominados na literatura técnica como PII (*Personally Identifiable Information*) -, os dados remanescentes podem ser vinculados a uma base não anonimizada, a qual servirá de chave para identificar o sujeito relacionado aos dados da base anonimizada. Tome-se como exemplo, a base de dados da biblioteca que fica no mesmo bairro do hospital que capturou os dados sensíveis da Tabela 1 acima. Dentre os dados da base da biblioteca, colhem-se os seguintes:

Nome	Sexo	CEP	Nascimento	Obras Emprestadas em 2017
Sérgio Freitas	M	02345-000	23/03/1946	3
José Cardoso	M	47689-010	16/01/1944	0
Julia Pereira	F	14534-010	31/12/2000	17

Tabela 4

A base de dados da biblioteca não contém dados sensíveis como aqueles coletados no banco de dados do hospital, portanto sua manutenção não envolveria cuidados especiais em relação à proteção. Desta forma, se disponibilizada ao público, a base de dados da biblioteca serviria como “chave” para reidentificação dos dados anonimizados do hospital (tabela 2), porquanto vincula, por exemplo, o indivíduo chamado Sérgio Freitas, por meio de seu CEP, sexo e

[80] OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Review, Vol. 57, 2010. Disponível em <http://www.uclalawreview.org/broken-promises-of-privacy-responding-to-the-surprising-failure-of-anonymization-2>. Acesso em: 14.nov.2017

[81] Paul Ohm defende o abandono do termo “anonimização” e “deidentificação”. Recomenda, simplesmente, a utilização da expressão “scrub” (limpeza) que sugere apenas um esforço para remover atributos que identifiquem um sujeito numa massa de dados. Ibidem. p. 1744-1745.

data de nascimento àquele portador de hipertensão constante da tabela supostamente anonimizada (tabela 2).

Desta forma, é possível exemplificar a fragilidade da técnica de anonimização que se limita exclusivamente a suprimir os PII (informações de identificação pessoal) das bases de dados. Na realidade, é necessário admitir que qualquer dado pode ser considerado PII (*Personally Identifiable Information*), uma vez que pode ser a chave de união entre duas tabelas para fins de desanonimização, como demonstrado, de forma singela, no exemplo da desanonimização com vínculo da tabela anonimizada do hospital com a tabela não anonimizada da biblioteca.[82]

A conclusão do trabalho de PAUL OHM é no sentido de que a premissa adotada pelos legisladores segundo a qual é possível proteger a privacidade com a anonimização de dados pessoais é premissa falsa. Isso significa que todo sistema normativo de proteção de dados pessoais que esteja fundado na falsa premissa da anonimização deve ser urgentemente revisado.

Convém, neste ponto, mencionar o exemplo do HIPAA (Health Insurance Portability and Accountability Act) que regulamenta a privacidade de dados de saúde nos Estados Unidos da América. As PHI (*Protected Health Information*), dados de saúde que recebem a proteção legal, não incluem os dados de-identificados ou anonimizados, ou seja, bastaria anonimizar a base de dados para removê-la do âmbito de proteção da lei. A página oficial do National Institute of Health afirma que “De-identified health information, as described in the Privacy Rule, is not PHI, and thus is not protected by the Privacy Rule.”[83]

A Diretiva Europeia 95/46/CE não prevê a proteção de todos os dados, mas tão somente daqueles ditos pessoais que são definidos como "qualquer

---

[82] O Anexo I deste trabalho contém três exemplos clássicos de desanonimização

[83] NIH – National Institute of Health. De-identifying Protected Health Information Under the Privacy Rule. Disponível em: <https://privacyruleandresearch.nih.gov/pr_08.asp#8a>. Acesso em: 14.nov.2017.

informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa"); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social."[84]

Justamente neste ponto é que a controvérsia encontra terreno fértil. No momento da concepção da Diretiva Europeia 95/46/CE a possibilidade de desanonimização bem como suas técnicas não estavam difundidas como hoje, de modo que o escopo dos dados que poderiam identificar um indivíduo era bem reduzido. Com o estado da técnica atual qualquer base de dados anonimizada pode conter um conjunto de dados com vocação para se tornar elemento de identificação, sendo de rigor, por esta razão, estender a proteção legal a esta massa de dados anonimizada.

O Novo Regulamento Europeu de Proteção de Dados Pessoais (GDPR), que será tratado com mais detalhes em seção posterior, reconhece a possibilidade de reidentificação de bases anonimizadas – denominadas neste instrumento como "pseudonimizada" – e estende a proteção legal a estes dados, ainda que anonimizados:

> *Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável.*[85]

Ocorre que a atribuição de proteção jurídica à base de dados anonimizada está vinculada à possibilidade de reidentificação. No entanto tal possibilidade nem sempre pode ser aferível a priori. Para sanar esta dificuldade,

---

[84] Diretiva 95/46/CE. Disponível em <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf>. Acesso em: 14.nov.2017.

[85] GDPR, considerando n° 26

recorre-se ao estado da técnica como indicador da probabilidade de desanonimização:

> *Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica.*[86]

Os considerandos 75 e 85 do GDPR refletem a preocupação do legislador com os riscos aos direitos e às liberdades individuais dentre os quais cita-se “a inversão não autorizada da pseudonimização”. De fato, a possibilidade técnica desta inversão à qual denominamos reidentificação ou desanonimização é precisamente reconhecida pelo GDPR no momento da conceituação da pseudonimização, notadamente ao se fazer menção aos “dados suplementares” que conteriam a chave para a desanonimização:

> *"Pseudonimização", o tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.*[87]

Embora reconheça de forma clara a sempre presente possibilidade técnica de reidentificação de massas de dados anonimizadas, o GDPR entende que a anonimização pode contribuir para a proteção dos dados pessoais (Considerandos 28, 29, 156 e Artigos 6.4(e), 25.1, 32.1(a), 40.2(d) e 89.1).

---

[86] Ibidem, considerando n° 26
[87] GDPR, Art. 4.5.

4 A PROTEÇÃO DA PRIVACIDADE INFORMACIONAL

4.1 A Privacidade e a Proteção dos Dados Pessoais

Juristas, filósofos, sociólogos e outros estudiosos têm, sem muito sucesso, tentado chegar a um consenso sobre o conceito de privacidade. Alguns já conceituaram a privacidade como o direito de estar só[88], outros a identificaram como o direito de limitar o acesso de si mesmo a outros[89] e há quem a definisse como o direito ao segredo em determinadas matérias[90].

A dificuldade para conceituar a privacidade está relacionada à abrangência de situações às quais ela pode se referir, inexistindo um ponto comum para todas estas situações que permita estabelecer um conceito único.

LOUIS BRANDEIS, autor do clássico artigo "The Right of Privacy" em coautoria com Samuel D. Warren, enquanto juiz da Suprema Corte americana, ao proferir decisão no caso *Olmstead v. United States* (227 U.S. 438), referiu-se à privacidade como "*the most comprehensive of men's rights*" ("O mais abrangente direito dos homens").

A abrangência do sentido da privacidade ficou clara para as gerações que sucederam Brandeis e Warren levando os estudiosos a entenderem a necessidade de sistematização do tema, o que, via de regra conduziu a uma subclassificação do direito.

---

[88] Samuel D. Warren e Louis D. Brandeis, autores do clássico artigo "The Right to Privacy" (1890), exerceram uma forte influência nos debates sobre privacidade no século 20.

[89] Adam Carlyle Breckenridge afirmou: "Privacidade, a meu ver, é a justa pretensão do indivíduo determinar a extensão a qual ele deseja compartilhá-lo com outros", The Right to Privacy (1970) – Tradução livre de "Privacy, in my view, is the rightful claim of the individual to determine the extent to which he wishes to share of himself with other").

[90] Richard Posner afirmou: "The word privacy seems to embrace at least two distinct interests. One is the interest in being left alone – the interest that is invaded by the unwanted telephone solicitation, the noisy sound truck, the music in elevators, being jostled in the street, or even an obscene theater billboard or shouted obscenity… The other privacy interest, concealment of information, is invaded whenever private information is obtained against the wishes of the person to whom the information pertains" – The Economics of Justice, p. 272/273.

WILLIAM PROSSER[91] (1960), autoridade em Responsabilidade Civil (*torts*), em seu artigo “Privacy”, na tentativa de sistematizar o instituto, fez uma análise jurisprudencial com casos que de certa forma tinham relação com a privacidade. PROSSER subclassificou o direito à privacidade em função dos danos que sua violação poderia causar. Neste sentido enumerou quatro categorias de possíveis danos:

1 – A invasão de alguém ao âmbito privado de outrem (“*Intrusion upon seclusion*”)[92]: PROSSER ressalta que a invasão não se limita ao aspecto físico como na invasão de um ambiente privado, mas alcança a esfera das comunicações sendo vedada, por exemplo, a interceptação de linha telefônica ou a violação de correspondências.

2 – Divulgação pública de fatos privados (*public disclosure of private facts*)[93]: Estariam incluídas nesta categoria as divulgações de fatos ofensivos sem interesse público, ainda que verdadeiros. A este respeito PROSSER levanta uma questão controvertida: E se um cidadão comum, estando embriagado e cambaleante, fosse fotografado em via pública e a foto fosse divulgada publicamente? Haveria neste caso violação à privacidade na modalidade de divulgação pública de fatos privados? O autor entende, baseado nas decisões tomadas à época, que não haveria violação pois o que estar-se-ia a fazer seria simplesmente dar publicidade a algo que já é público.

3 – Publicação de fatos falsos sobre um indivíduo (*false light in the public eye*)[94]: Esta categoria de condutas parece distanciar-se do que hoje entendemos estar sob a guarida do direito à privacidade e assemelha-se às condutas violadoras da honra, mas especificamente, neste caso, a difamação. No entanto, é possível

---

[91] PROSSER, William L. Privacy. California Law Review. Volume 48. Issue 3. 1960. p. 383-423 Disponível em: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview>. Acesso em: 12.jun.2017.

[92] Ibidem, p. 389-392.

[93] Ibidem. p. 392-398

[94] Ibidem. p. 398-401

traçar um paralelo entre este tipo de conduta e o risco de má utilização do Big Data na medida em que o tratamento dos dados pessoais por meio da análise de dados (*analytics*) e geração de perfil pode resultar em dados derivados que não necessariamente qualificam o sujeito relacionado aos dados implicando num risco de prejuízo em sua esfera jurídica.

4 – Apropriação indevida do nome ou da imagem objetivando vantagem comercial (*appropriation*)[95]: PROSSER menciona o caso de um fotógrafo que comercializou sem autorização a foto do autor da ação, o que foi entendido como uma violação da privacidade. Nesta subclassificação são mencionadas por PROSSER a apropriação de *name, picture and likeliness* o que, em nosso tempo, poderia ser interpretado como o uso comercial não autorizado de qualquer aspecto da personalidade, incluindo dados pessoais.

Observa-se que classificação apresentada por PROSSER é difícil encontrar um ponto de intersecção que permita conceituar a privacidade, um elemento comum às quatro situações. O próprio autor reconhece a possibilidade de encontrarmos pontos comuns entre duas ou três categorias, mas não entre todas:

> *Taking them in order-intrusion, disclosure, false light, and appropriation - the first and second require the invasion of something secret, secluded or private pertaining to the plaintiff; the third and fourth do not. The second and third depend upon publicity, while the first does not, nor does the fourth, although it usually involves it. The third requires falsity or fiction; the other three do not. The fourth involves a use for the defendant's advantage, which is not true of the rest.*[96]

A dificuldade no consenso para estabelecer um conceito único para a privacidade aliada às categorizações deste direito parecem indicar que LOUIS BRANDEIS estava correto ao conferir à privacidade o atributo de “o mais abrangente dos direitos dos homens”.

Esta abrangência foi também apontada por ARNOLD ROOSENDAAL (2012) que classificou a privacidade em quatro espécies: espacial, relacional,

---

[95] Ibidem. p. 401-407.
[96] Ibidem. p. 407.

comunicacional e informacional, sendo esta última vertente da privacidade subdividida em dois componentes: o primeiro está relacionado com o direito de impedir o acesso às suas informações e o segundo relaciona-se com o direito de limitar o uso e a disseminação da informação.

> *Privacy can be distinguished into different dimensions. Common distinctions are between spatial, relational, communicational, and informational privacy. Informational privacy relates to the protection of personal data and has two main components. The first, which is at the core of the right to privacy, is being free from attention of others and not being watched. The second element comes into play once a third party has information and the individual wants to control the use and dissemination of this information (Lloyd 2008, 7).*[97]

De fato, a abrangência do conceito de privacidade não se dá apenas num dado momento, como observou BRANDEIS no final do século 19 e como destacou ROOSENDAAL, mas destaca-se e potencializa-se ao longo do tempo, revestindo-se de nova carga semântica na medida em que novos fatos sociais passam incorporar o cotidiano de uma sociedade.

No âmbito informacional o direito à privacidade encontra-se na intersecção do direito à liberdade e do direito de propriedade, onde o objeto de incidência da liberdade e da propriedade são as projeções da personalidade do indivíduo. Na sociedade digital, onde os aspectos de personalidade do indivíduo são reduzidos a bits e bytes, a privacidade deve ser entendida como a liberdade de determinar o destino dos dados que reflitam aspectos caracterizadores de sua personalidade.

STEFANO RODOTÀ, neste sentido, observa que “na sociedade da informação tendem a prevalecer definições funcionais da privacidade que, de

---

[97] ROOSENDAAL, Arnold. We Are All Connected to Facebook . . . by Facebook! in: S. Gutwirth et al. (eds.), European Data Protection: In Good Health?, Heidelberg: Springer, 2012. p. 14. apud LLOYD, Ian J. Information technology law. Oxford: Oxford Univ. Press, 2008, 7.

diversas formas, fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas."[98]

ADRIANO DE CUPIS, ao lecionar sobre os direitos da personalidade, discorre sobre uma categoria especial que denomina de "direito ao resguardo", definindo-o como "a exclusão do conhecimento pelos outros daquilo que se refere somente a ela"[99]. Como uma manifestação deste direito, DE CUPIS apresenta o direito à imagem, especialmente a proteção contra a difusão arbitrária das feições do indivíduo. De fato, o direito ao resguardo não se limita à proteção da imagem, mas a todo "o modo de ser da pessoa que consiste na exclusão do conhecimento, por parte das outras pessoas, de quanto se refere à própria pessoa"[100]. Desta forma, o direito do indivíduo ter controle sobre seus dados pessoais pode ser considerado uma espécie do gênero do direito ao resguardo.

A dificuldade de estabelecer normas que garantam a privacidade informacional reside, dentre outros aspectos, no fato de que não basta ao sujeito relacionado aos dados decidir que um determinado aspecto a si relacionado não deve ser compartilhado ou publicado, mas o destinatário dos dados deve ser levado em conta no momento de estabelecer se o sujeito relacionado aos dados tem o direito de manter o dado livre do conhecimento de todos. Como exemplo, cite-se a noção de "conceito relacional" do dado pessoal trazida por CÍNTIA ROSA PEREIRA DE LIMA:

> *[O direito à privacidade] é um conceito relacional, por exemplo, o portador de uma doença grave e sexualmente transmissível como a AIDS tem o direito de não ter tal informação divulgada no seu ambiente de trabalho (não havendo justificativa para tal divulgação, o que seria apenas com o condão discriminatório). No entanto, este mesmo paciente pode ter tal informação comunicada e compartilhada entre autoridades sanitárias competentes para fins de controle da doença.*[101]

---

[98] RODOTÀ, STEFANO. A vida na sociedade da vigilância: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda.. Rio de Janeiro: Renovar, 2008. p. 92.

[99] CUPIS, Adriano de. Os direitos da personalidade. Tradução de Afonso Celso Furtado Rezende. 2ª ed., São Paulo: Quorum, 2008. p. 139.

[100] Ibidem, p. 155.

[101] LIMA, Cíntia Rosa Pereira de. A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil, Ribeirão Preto, 2015. p. 129.

Diante disso, o problema da privacidade informacional apresenta-se como questão multidimensional demandando respostas para as seguintes perguntas: Quais dados relacionados aos indivíduos merecem proteção? Que tipo de proteção pode ser conferida, ou seja, que ações são permitidas ou proibidas (coleta, armazenamento, análise, compartilhamento, uso)? Que entidades podem realizar as ações ou estariam impedidas de realiza-las? Quais as finalidades legítimas para a realização das ações em cada caso? Quando ou por quanto tempo as ações podem ser realizadas (limite temporal)?

4.2 A Titularidade dos Dados Pessoais

Quem deve ser considerado o titular sobre os dados pessoais? Que direitos o titular dos dados pessoais pode exercer sobre este objeto? A tendência é afirmar que cada pessoa é titular dos seus dados pessoais, sendo ela, portanto, a única a poder decidir quem poderá acessá-los, armazená-los, agregá-los, tratá-los, compartilha-los e utilizá-los. No entanto, a questão não pode ser tratada de forma tão superficial.

É possível afirmar que uma pessoa é titular do seu histórico de crédito ou de seus antecedentes criminais? Perceba-se a dificuldade de atribuir não apenas a titularidade dos dados a um ou mais indivíduos como também a definição dos direitos que esta titularidade implica (uso, armazenamento, processamento, compartilhamento, exclusão definitiva, etc...).

Como declinado anteriormente, optou-se neste trabalho pela expressão “sujeito relacionado aos dados” em vez da utilização da consagrada expressão “titular dos dados”. Tal opção, já justificada, decorreu do risco de interpretar a expressão “titular de um objeto” como sendo a titularidade do direito de propriedade sobre o objeto. Ainda que os direitos sobre os dados pessoais exercíveis pelo sujeito relacionado aos dados sejam distintos dos direitos relacionados à propriedade (usar, gozar, dispor, reivindicar), não estão claros quais são estes direitos. Na verdade, observa-se que a cada dado pessoal, estando este mais ou menos próximo da esfera íntima do indivíduo, podem ser atribuídos direitos distintos. Em outras palavras, há dados pessoais sobre os quais o sujeito relacionado a eles exerce direitos que não são exercidos sobre outros dados

pessoais que teriam, por exemplo, em sua natureza algum elemento que apontasse ao interesse público.

Como exemplo, mencione-se a decisão do Supremo Tribunal Federal nos autos do Recurso Extraordinário com Agravo nº 652.777/SP de relatoria do Ministro Teori Zavascki onde se discutiu tema de Repercussão Geral sobre a legitimidade da publicação da remuneração de servidores públicos em sítios da Administração Pública. No acórdão atacado pelo referido Recurso Extraordinário decidiu-se pela legitimidade da divulgação do salário, mas sem mencionar o nome do servidor. O relator do Recurso Extraordinário, Ministro Teori Zavascki, fez referência à decisão da lavra do Ministro Ayres Britto que no julgamento de Agravo Regimental na Suspensão de Segurança 3.902 decidiu com o seguinte fundamento:

> *Não cabe, no caso, falar de intimidade ou de vida privada, pois os dados objeto da divulgação em causa dizem respeito a agentes públicos enquanto agentes públicos mesmos; ou, na linguagem da própria Constituição, agentes estatais agindo "nessa qualidade" (§ 6º do art. 37). E quanto à segurança física ou corporal dos servidores, seja pessoal, seja familiarmente, claro que ela resultará um tanto ou quanto fragilizada com a divulgação nominalizada dos dados em debate, mas é um tipo de risco pessoal e familiar que se atenua com a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor. No mais, é o preço que se paga pela opção por uma carreira pública no seio de um Estado republicano. (SS 3902 AgR-segundo, Relator(a): Min. AYRES BRITTO, Tribunal Pleno, julgado em 09/06/2011, DJe-189 DIVULG 30-09-2011 PUBLIC 03-10-2011 EMENT VOL-02599-01 PP-00055 RTJ VOL-00220-01 PP-00149)*

Desta forma, o STF, ao julgar o tema de repercussão geral nº 483, deu provimento ao Recurso Extraordinário e fixou a tese segundo a qual é legítima a publicação, inclusive em sítio eletrônico mantido pela Administração Pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias.

Embora esta decisão não esteja diretamente relacionada ao objeto de estudo desta dissertação (*online profiling*), ela serve para demonstrar não apenas que eventuais direitos sobre os dados pessoais não são absolutos, mas também

que alguns dados pessoais podem receber maior proteção o que, na prática, equivale a dizer que há exercício de direitos distintos sobre dados distintos.

4.3 A Privacidade Informacional Como Direito da Personalidade

O conceito de privacidade informacional está relacionado ao direito de um indivíduo decidir sobre o destino de seus dados pessoais. O controle sobre seus dados implica na possibilidade de imposição de limitações quantitativas, temporais e de finalidades às entidades que coletam, armazenam, processam e usam os dados.

EVA HEEGER definiu a privacidade informacional da seguinte forma:

> *Informational privacy is the right concerning the (online) image of a person. In other words informational privacy is the right of an individual to control the personal data that concern him. This includes the right to autonomy and to decide for oneself with whom one shares the information.*[102]

A referida "imagem *online* da pessoa", composta por dados e informações pessoais suscetíveis de compartilhamento por meio digital, pode ser considerada uma projeção de sua personalidade, o que implica em reconhecer que o direito sobre os dados pessoais é um direito da personalidade.

CARLOS ALBERTO BITTAR define os direitos da personalidade como aqueles "reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade"[103].

O professor BITTAR utiliza-se da expressão "reconhecidos" por entender que os direitos da personalidade são inatos ao homem e, portanto, não são direitos concedidos pelo Estado, mas tão somente reconhecidos e declarados pelo ordenamento jurídico dado que tais direitos sempre existiram, ainda que não positivados. Estes direitos estão relacionados a atributos intrínsecos e indissociáveis da vida e existência humanas. Por tais razões são também ditos "direitos essenciais".

---

[102] HEEGER, Eva. Controlling Your Online Profile: Reality or an Illusion? A Research into Informed Consent as a Mechanism to Regulate Commercial Profiling. 2005. Disponível em: <http://ssrn.com/abstract=2658651>. Acesso em: 12.dez.2017. p. 1

[103] BITTAR, Carlos Alberto. Os direitos da personalidade. 8ª ed., São Paulo: Saraiva, 2015. p. 1

As “projeções na sociedade”, expressão utilizada pelo professor BITTAR, são as diversas formas pelas quais um indivíduo exterioriza sua existência no meio em que vive. As possíveis projeções pressupõem a existência de dimensões ou âmbitos de atuação do ser humano: físico, mental, moral, espiritual, etc. As qualidades humanas em todas estas dimensões se expressam, ou se projetam, na sociedade. Por exemplo, na dimensão física o indivíduo se projeta com sua imagem, sua voz, sua energia e saúde. Sob estes elementos, intrínsecos à existência humana, o indivíduo exerce direito subjetivo, qualificado como direitos da personalidade. Tais direitos são poderes que o homem exerce sobre sua própria pessoa, sobre elementos ou atributos intrínsecos a sua natureza.

A tecnologia digital permitiu que quase tudo, inclusive as projeções do indivíduo na sociedade, fosse passível de digitalização. Isso significa que aspectos essenciais da personalidade do indivíduo podem ser condensados numa sequência de bits e bytes. A imagem, a voz, as criações do intelecto, o que o indivíduo fala, faz e deseja são elementos suscetíveis de conversão em tipos de dados digitalizados. Esta possibilidade técnica – e realidade fática – coloca os direitos da personalidade em situação de extrema vulnerabilidade, mormente quando considerada não apenas a possibilidade técnica da digitalização destas projeções da personalidade, mas também a facilidade com que tais dados digitalizados podem ser replicados, rapidamente transmitidos e sucessivamente compartilhados.

O estabelecimento de limites e restrições para a multiplicidade de ações sobre os dados que refletem aspectos da personalidade está no âmago dos direitos relacionados à privacidade informacional, cabendo ao jurista a sistematização da disciplina que tratará destes limites e restrições.

5 PRIVACIDADE INFORMACIONAL - FORMAS DE PROTEÇÃO

Reconhecidos os direitos do indivíduo sobre seus dados pessoais como direitos da personalidade, indaga-se quais seriam as maneiras de garantir o exercício destes direitos, no âmbito privado, impedindo que o sujeito relacionado aos dados sofra prejuízos decorrentes da violação de sua privacidade informacional e do tratamento indevido dos dados.

Adiante serão apresentadas três formas de proteção da privacidade informacional: a regulação pelo livre mercado, a regulação por normas do estado e a autorregulação.

5.1 Regulação Pelo Livre Mercado

Admitindo-se a hipótese de total ausência de normas estatais de proteção à privacidade, o modelo de proteção de dados baseado no livre mercado parte da premissa liberal de que as empresas podem fornecer variados níveis de proteção da privacidade e os consumidores têm a liberdade de contratar com aquelas empresas que melhor satisfaçam suas necessidades e expectativas com relação à proteção de seus dados pessoais.

Se por um extremo as empresas tenderiam a gerar mais lucros ao usar e compartilhar dados de forma indiscriminada, esta conduta afastaria clientes desejosos de maior proteção. Já as empresas que operassem com políticas mais restritivas com relação aos dados pessoais poderiam amealhar mais clientes, no entanto não lucrariam com a exploração dos dados pessoais.

O equilíbrio de mercado seria obtido na medida em que empresas que frustrassem a expectativa dos consumidores no tocante à proteção de dados pessoais passassem a ser preteridas no momento da contratação. Em contrapartida, as empresas que comprovadamente oferecessem alto grau de proteção, passariam a gozar de boa reputação no mercado o que lhes auxiliaria na captação de novos clientes. Como analogia deste modelo hipotético é possível mencionar a reputação dos bancos Suíços com relação à garantia do sigilo sobre seus clientes.

Este modelo de mercado hipotético funda-se na liberdade de contratação das partes e na autonomia da vontade. Desta forma, o indivíduo tem o

direito de compartilhar seus dados pessoais com as empresas, negociando as regras de uso e compartilhamento dos dados.

Deste direito de decidir o que, para quem e para que compartilhar decorre a impossibilidade de terceiros capturarem, armazenarem, utilizarem e compartilharem os dados pessoais, salvo se houver consentimento do sujeito relacionado aos dados. E é justamente nas circunstâncias e elementos desta manifestação de vontade que surgem os problemas com o modelo hipotético de mercado.

Em geral, admite-se que a autorização para uso e compartilhamento de dados deve ser precedida de informação adequada com respeito a quais dados serão compartilhados, com quem serão compartilhados, por quanto tempo ficarão gravados nas bases de dados das empresas, que tipo de tratamento e processamento receberão e para quais fins serão utilizados. Daí convencionou-se dizer que o consentimento deve ser “informado”.

No entanto, na prática, tais informações são veiculadas por meio de políticas de privacidade ou termos ou condições de uso, geralmente extensos e com linguagem incompreensível, além de seu conteúdo ser alterado constantemente. Neste contexto, o usuário fica impossibilitado de consentir de maneira realmente informada sobre o destino dos seus dados, o que nos leva a admitir que o consentimento realmente informado é uma ficção jurídica.

Na seção apropriada, este trabalho abordará as iniciativas da Comunidade Europeia para a proteção dos dados pessoais, a saber, a Diretiva 95/46 e, mais recentemente, o Regulamento adotado pela Comunidade Europeia em abril de 2016 (GDPR) e que entrará em vigor em 2018, este com inovações nas disposições sobre a obtenção do consentimento, o direito de apagamento (também conhecido como o “direito ao esquecimento”) e com disposições sobre as obrigações e responsabilidade das empresas que fazem o tratamento dos dados pessoais. Observar-se-á, claramente, uma mudança de foco: da primazia do consentimento informado do usuário para as obrigações das empresas responsáveis pelo tratamento de dados, sendo estas supervisionadas por uma autoridade reguladora e fiscalizadora.

Atualmente, empresas como Facebook e Google coletam dados dos usuários e geram os perfis sob o dogma do “consentimento informado”. No entanto, os usuários frequentemente desconhecem o que estão consentindo bem como os riscos aos quais estão submetidos em face deste processo de coleta, análise e *profiling*. Dentre estes riscos, já mencionamos a discriminação, estigmatização além da criação de um perfil baseado em informações incorretas que pode, consequentemente, levar à tomada de decisões equivocadas sobre o sujeito relacionado aos dados. Ademais, os consumidores não têm condições de verificar se as obrigações assumidas pelas empresas que coletam dados estão sendo realmente cumpridas.

Demonstrar-se-á que a forma como o consentimento informado vem sendo obtido faz como que este mecanismo de proteção da privacidade torne-se, na prática, inócuo, porquanto os sujeitos relacionados aos dados têm pouco ou nenhum controle sobre seus dados após pressionarem o botão “Eu Aceito”.

5.1.1 A Ineficácia do Modelo de Consentimento Informado

O modelo de negócios adotado pelas grandes empresas de internet (e.g. Google e Facebook) prevê o fornecimento de serviço grátis em troca dos dados pessoais. MARCEL LEONARDI (2011) apontou que a cessão de dados é a forma de pagamento pelos serviços “grátis” e que os usuários preferem pagar pelos serviços com dados pessoais a desembolsar valores em dinheiro:

> *É a publicidade dirigida, possibilitada pelo tratamento de dados pessoais de usuários, que sustenta o ecossistema de serviços e de informações gratuitas online. Outros modelos de negócio – assinaturas, micropagamentos, sites fechados – não são aceitos pela esmagadora maioria dos usuários, acostumados com “tudo grátis” online. Entre pagar R$ 5 por mês ou ceder dados pessoais, quase todos preferem pagar com dados.*[104]

Embora seja admissível a troca de dados pessoais por serviços *online*, a preocupação decorre da incapacidade do usuário de internet compreender os

---

[104] LEONARDI, Marcel. Dados pessoais, regulação e a economia digital. Jornal da Tarde. 28.03.2011. p. 2. Disponível em: <http://leonardi.adv.br/2011/03/dados-pessoais-regulacao-e-a-economia-digital/>. Acesso em: 05.dez.2017.

riscos aos quais está sujeito quando sistematicamente fornece dados pessoais às empresas de internet. Há evidências suficientes de que o atual modelo de proteção de dados pessoais baseado exclusivamente no consentimento supostamente informado para a utilização de dados pessoais não se presta adequadamente aos fins para os quais foi concebido.

Embora a legislação em vigor garanta ao indivíduo o direito de receber "informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais"[105], observa-se que as informações veiculadas por empresas que capturam dados pessoais na internet nem sempre observam as disposições legais.

Demonstrar-se-á, a seguir, que a forma adotada para a expressão do consentimento não é apta a proteger a privacidade do sujeito relacionado aos dados.

O consentimento expresso ofertado pelo sujeito à uma organização para que se capture, armazene, utilize e compartilhe seus dados pessoais geralmente se dá pela aceitação de termos de uso ou de políticas de privacidade.

É fato incontroverso que pouquíssimos usuários, para não dizer nenhum, leem com atenção e integralmente os termos de uso ou políticas de privacidade dos serviços de internet. Os usuários de internet supõem que os termos de uso e as políticas de privacidade são documentos destinados à proteção de sua privacidade, como o nome sugere ("Política de Privacidade"), e que, portanto, impõem limitações às empresas quanto ao uso dos dados fornecidos, o que faz os usuários crerem que as grandes empresas de internet não adotariam, em nenhuma circunstância, práticas que pudessem causar danos ou risco aos seus usuários. Desta forma, sem titubear, os usuários aceitam os termos de uso clicando no botão de aprovação ou com outra ação equivalente.

A decisão de consentir sem ler e buscar compreender a "Política de Privacidade" é tomada tendo-se em vista diversos fatores dentre os quais menciona-se:

---

[105] Artigo 7°, VIII da Lei 12.965/2014 (MCI).

1. A extensão do instrumento de política de privacidade – Os termos de uso ou a política de privacidade são geralmente documentos extensos que levariam um tempo considerável para a leitura, análise e compreensão. A utilização das ferramentas e serviços da internet ocorrem de forma dinâmica sendo, portanto, a leitura de um longo texto incompatível com dinâmica da rede, pois o usuário geralmente necessita do serviço para uso imediato não podendo condicioná-lo a uma posterior análise de viabilidade dos termos de uso já que a aceitação dos termos, via de regra, deve ocorrer antes da utilização dos serviços.
2. A linguagem dos termos de uso – Estes documentos são comumente escritos em linguagem de difícil compreensão ao usuário e, muitas vezes, disponíveis apenas em idioma estrangeiro, inacessível à maioria dos usuários. Quando em língua pátria, termos jurídicos e técnicos são comumente utilizados, o que dificulta ou até mesmo impossibilita a compreensão por parte do usuário.
3. Termos Genéricos – Ainda que os termos de uso tenham sido redigidos em linguagem acessível aos usuários, as cláusulas que abordam aspectos críticos são genéricas como, por exemplo, sobre a finalidade da captura dos dados ou a possibilidade de compartilhamento com terceiros. Geralmente, neste ponto, as empresas alegam que usarão os dados para melhorar os serviços e facilitar a interação com o usuário compartilhando os dados com empresas de sua confiança. Quando alguma finalidade específica é mencionada, geralmente ela está relacionada ao direcionamento de publicidade adequada ao perfil, o que não gera muita preocupação ao usuário.
4. A Percepção de Baixo Risco – Geralmente o usuário tem uma percepção de que ao consentir com um contrato de adesão eletrônico ou com uma política de privacidade, ele o faz com baixo

risco de modo a não justificar o custo da leitura e compreensão do texto. Alguns fatores que corroboram para criar a percepção de baixo risco são os seguintes: (a) o serviço contratado é disponibilizado de forma gratuita de modo que o usuário não vislumbra risco de natureza financeira ao manifestar seu consentimento, (b) a denominação do texto que se está a consentir, “política de privacidade”, sugere que o fornecedor dos serviços mantém regras para proteger a privacidade do usuário o que gera a segurança para a aceitação dos termos sem a necessidade de lê-lo e compreendê-lo, (c) a percepção de que muitas pessoas aderem aos termos e não sofrem nenhum prejuízo perceptível.

5. Opções de Configuração Padrão Permissivas – Geralmente as opções de privacidade são previamente configuradas com uma política mais permissiva devendo o usuário reconfigurar para restringir as permissões. A reconfiguração para o “opt-out” nem sempre é facilmente acessível.
6. Tamanho Reduzido dos Displays – Observa-se que os usuários de internet cada vez mais acessam a rede utilizando dispositivos menores, geralmente, smartphones, o que dificulta ou inviabiliza a leitura de longos documentos.
7. Pegar ou Largar – Ao usuário que não aceitar os termos de uso não haverá outra opção senão abster-se da utilização do serviço, o que poderia implicar em exclusão digital e social. Ao usuário geralmente não é dada a opção de pagar uma mensalidade para utilizar os serviços sem fornecer seus dados pessoais.

Demonstrado que o propalado “consentimento informado” é, na realidade, uma ficção jurídica, porquanto nada tem de informado, chega-se à conclusão de que o tratamento de dados pessoais deveria ser regulado por legislação específica com a supervisão de agência regulatória, ficando o consentimento em segundo plano. Este novo paradigma não deveria valer apenas

no sentido de proibir o tratamento em situações onde há expresso consentimento, mas também para permitir a utilização de dados para outros fins mesmo sem o consentimento. Este último caso justifica-se pela prevalência do interesse público em detrimento dos interesses particulares do indivíduo. Tome-se como exemplo o tratamento de informações sanitárias ou de saúde coletadas pelo poder público em postos de saúde e utilizadas para a adoção de políticas de saúde. Não se espera que os pacientes que visitam o posto de saúde devam autorizar a utilização de seus dados para análises com finalidades de interesse público como, por exemplo, a propagação de epidemias.

Para regular a utilização de dados pessoais, OMER TENE e JULES POLONETSKY propõem uma ponderação que leve em conta os benefícios sociais da utilização dos dados e seus riscos para a privacidade do sujeito:

> *A coherent framework would be based on a risk matrix, taking into account the value of different uses of data against the potential risks to individual autonomy and privacy. Where the benefits of prospective data use clearly outweigh privacy risks, the legitimacy of processing should be assumed even if individuals decline to consent.*[106]

Desta forma a legislação deveria dispor sobre as situações para as quais o consentimento seria pré-requisito para a captura e utilização de dados pessoais. Tais situações deveriam acolher a publicidade direcionada por perfil, serviços que dependam de dados de informações sobre posicionamento geográfico e compartilhamentos com *Data Brokers*.

A legislação de proteção aos dados pessoais, como complemento ao consentimento, não é suficiente para atingir os objetivos de tutela dos indivíduos se não houver garantias de que as normas serão observadas por aqueles que detêm os dados pessoais. Isso porque a efetivação dos direitos dos usuários não ocorrerá sem um controle e fiscalização por parte de uma entidade externa com poderes e condições de apurar se a legislação está, de fato, sendo cumprida.

---

[106] TENE, Omer; POLONETSKY, Jules. Privacy in the age of big data: a time for big decisions, Stanford Law Review Online 64. 2012. p. 67. Disponível em: <http://www.stanfordlawreview.org/online/privacy-paradox/big-data> Acesso em: 02.dez.2017.

Neste sentido, CÍNTIA ROSA PEREIRA DE LIMA aponta para a imprescindibilidade de uma autoridade de garantia para dar efetividade às normas de proteção dos dados pessoais:

> *A proteção dos dados pessoais não pode ser estruturada tão somente com base no consentimento livre e informado do titular dos dados em razão de sua vulnerabilidade. Em outras palavras, o indivíduo que necessita de serviços essenciais na sociedade informacional, quando solicitadas informações que lhe digam respeito para poder usufruir do serviço, não poderá resistir à anuência exigida pelos prestadores de serviço ao tratamento de seus dados pessoais. Justamente por isso, o consentimento do titular dos dados é insuficiente para a efetiva proteção dos dados pessoais, daí a importância de uma entidade de controle, independente do Poder Executivo, cuja missão seja a de fiscalizar e garantir o cumprimento da legislação sobre proteção de dados pessoais.*[107]

Desta forma, fica evidente que um sistema de proteção de dados baseado simplesmente no modelo do consentimento do usuário, sem uma lei de proteção de dados pessoais e sem uma autoridade de garantia que confira efetividade às normas, não será suficiente para garantir os direitos de privacidade dos sujeitos relacionados aos dados, mas constituirá o que foi denominado por CÍNTIA ROSA PEREIRA DE LIMA como uma "ditadura dos contratos de adesão eletrônicos"[108].

5.1.2 A Impossibilidade de Enforcement

No modelo hipotético de mercado deveria ser possível ao consumidor não apenas compreender as políticas de privacidade propostas pelas empresas, mas também verificar se tais políticas estão sendo cumpridas.

---

[107] LIMA, Cíntia Rosa Pereira de. A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil, Ribeirão Preto, 2015. p. 134-135.

[108] LIMA, Cíntia Rosa Pereira de. O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos. *In: Direito e novas tecnologias I [Recurso eletrônico online]* CONPEDI/UFPB (org.) ROVER, Aires José; CELLA, José Renato Graziero; AYUDA, Fernando Galindo. Florianópolis: CONPEDI, 2014. pp. 343-365. Disponível em: <http://publicadireito.com.br/artigos/?cod=981322808aba8a03>. Acesso em: 02.jun.2017.

Se por um lado a compreensão das políticas de privacidade é inviabilizada em razão do custo (termos extensos, com alterações frequentes e linguagem inacessível), a verificação, a posteriori, do efetivo cumprimento das políticas por parte das empresas encontra óbice em aspectos técnicos já que o indivíduo não tem ferramentas para comprovar se a empresa cumpre suas políticas de privacidade.

Ao apresentar a impossibilidade de comprovar a conformidade com as políticas de privacidade, PETER SWIRE[109] aponta estratégias para monitorar eventuais violações da política de privacidade. Uma destas estratégias seria fornecer dados pessoais com pequenas alterações para cada empresa (e.g. fornecer uma inicial do nome do meio diferente para cada empresa), desta forma, havendo compartilhamento indevido confirmado por meio de carta ou e-mail não solicitado, verificar-se-ia qual é a inicial do nome do meio informada para que se descobrisse a empresa que violou as políticas de privacidade. No entanto, o próprio autor reconhece que este artifício, além de custoso, é ineficiente, pois considerando-se o compartilhamento de dados entre as empresas, os algoritmos de correção via referência cruzada poderiam corrigir a inicial do nome do meio que foi deliberadamente informada de forma distinta.

Diante da impossibilidade dos indivíduos verificarem se a empresa detentora de seus dados pessoais age em conformidade com sua política cria-se um cenário propício para o abuso por parte destas empresas, abuso que provavelmente nunca será identificado pelo sujeito relacionado aos dados e, portanto, dificilmente alguma punição será aplicada à empresa que fizer mau uso dos dados.

Em face desta hipossuficiência técnica do sujeito relacionado aos dados, as empresas não têm qualquer estímulo para abrir mão de benefícios financeiros ao se submeterem às regras de sua política de privacidade, regras que, como

---

[109] SWIRE, Peter. Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information. 1997. Disponível em: <https://ssrn.com/abstract=11472>. Acesso em: 25.mai.2017.

afirmado, se violadas, dificilmente gerarão algum tipo de punição ou impacto negativo em sua reputação.

Desta forma, no atual estado da técnica, o modelo hipotético puro de mercado conduz ao abuso por parte das empresas, não sendo capaz de garantir a privacidade dos sujeitos relacionados aos dados. Portanto, para a garantia da proteção dos dados pessoais, especialmente em face do *online profiling*, há necessidade de legislação específica e de uma entidade independente para regulamentar e fiscalizar o mercado.

5.2 Autorregulação

Uma alternativa ao modelo hipotético de livre mercado, o qual notadamente traria pouca ou nenhuma proteção ao sujeito relacionado aos dados, é o modelo de autorregulação. Neste modelo empresas privadas de um determinado setor se unem para estabelecer um código de conduta ética, práticas de governança, normas técnicas, confiando a uma entidade, criada e administrada por representantes do setor, as competências de fiscalização, julgamento e sancionamento de práticas vedadas pelo código de conduta.

Um exemplo típico de autorregulação no Brasil é o CONAR – Conselho Nacional de Autorregulamentação Publicitária cujo objetivo, além de defender a liberdade de expressão comercial, é de impedir que que a publicidade enganosa ou abusiva cause constrangimento ao consumidor ou a empresas[110]. O CONAR não faz censura prévia a campanhas publicitárias, mas atua de forma reativa levando ao seu Conselho de Ética as denúncias apresentadas por consumidores, associados ou autoridades.

No âmbito das práticas de coleta de dados pessoais, inclusive para a composição de perfis, há fora do país entidades setoriais de autorregulação como

[110] Missão do CONAR. Disponível em: <http://www.conar.org.br>. Acesso em: 14.jun.2017.

a NAI[111], o DAA[112] e a IAB[113]. Empresas associadas a estas entidades se comprometem a observar o código de conduta do setor e recebem em alguns casos, como consequência, a certificação ou selo de reconhecimento de sua adequação às normas e de sua submissão aos órgãos de fiscalização e sanção da entidade de autorregulação.

O FTC, desde a década de 1990, promoveu a sistemática de autorregulação. Em relatório destinado ao Congresso Norte Americano expôs o entendimento de que a "self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology"[114]. Desde então o FTC tem apoiado iniciativas do gênero, mas reconhecendo, por meio de novo relatório ao Congresso em 2012 que o modelo de autorregulação não avançou o suficiente.[115]

Embora algumas iniciativas por parte das entidades de autorregulação tenham merecido elogios por parte do FTC, boa parte das iniciativas acabam tendo efeito temporário, o que aponta para a necessidade de um modelo de proteção baseado numa lei geral nos Estados Unidos com o *enforcement* de uma entidade independente de controle.

CÍNTIA ROSA PEREIRA DE LIMA entende que a autorregulação não seria efetiva[116] por, pelo menos, três razões: Primeiramente porque neste setor tão

---

[111] O NAI, Network Advertising Initiative, é uma entidade autorregulatória, sem fins lucrativos, que congrega exclusivamente empresas terceiras de publicidade digital. (www.networkadvertising.org).

[112] A DAA, Digital Advertising Aliance, congrega diversas associações de empresas de publicidade digital com o objetivo de fomentar princípios e práticas relacionados à privacidade dos consumidores. (www.http://digitaladvertisingalliance.org).

[113] O IAB, Interactive Advertising Bureau, é composto por aproximadamente 650 empresas de mídia e tecnologia que atuam em publicidade digital. O IAB desenvolve pesquisa na área e tem definidos padrões, diretrizes e melhores práticas a serem observados pelas empresas associadas. (www.iab.com).

[114] FTC – Federal Trade Commission. Self-regulation and privacy online. 1999. p. 6.

[115] FTC – Federal Trade Commission. Protecting consumer privacy in an era of rapid change. 2012. p. 11.

[116] LIMA, Cíntia Rosa Pereira de. *Parecer Técnico encaminhado pela Professora Livre Docente de Direito Civil da Faculdade de Direito de Ribeirão Preto/USP, Dra. Cíntia Rosa Pereira de Lima à Comissão Especial da Câmara dos Deputados que proferirá parecer sobre o Projeto de*

sensível a decentralização não seria conveniente porquanto traria insegurança e incertezas com relação aos padrões éticos exigidos. Em segundo lugar o conselho de autorregulamentação não teria poder de polícia, o que enfraqueceria o sistema de proteção fazendo com que a efetivação dos direitos só fosse possível por meio do Poder Judiciário. Finalmente, não se poderia confiar num sistema onde o ente que fiscaliza é composto por representantes das entidades fiscalizadas.

A crítica acima deve ser entendida como sendo direcionada a um sistema de proteção estabelecido exclusivamente na base da autorregulação. A existência de entidades privadas, representativas de setores, que estabelecem códigos de conduta ética, melhores práticas e diretrizes gerais, bem como assumem o papel de fiscalização e sancionamento de práticas inadequadas não pode ser desconsiderado. Mas pode, e deve, exercer um papel complementar no sistema de proteção composto por lei geral de proteção e entidade independente reguladora.

5.3 Órgãos de Regulação e Controle

A efetivação dos direitos do usuário da internet no que tange à proteção dos seus dados pessoais não se consumará apenas a partir da entrada em vigor de leis gerais de proteção. Para que um modelo de proteção de dados seja bem-sucedido é imprescindível que a lei seja regulamentada e que exista efetiva fiscalização e adoção de medidas disciplinares sancionatórias contra aqueles que violarem as disposições da lei.

Embora o Poder Judiciário tenha recebido tradicionalmente a atribuição de impor sanções aos que descumprem a lei e causam danos a outrem, há motivos para acreditar que no âmbito da proteção de dados pessoais seria mais eficiente contar com a atuação de um órgão de controle independente. Este modelo de regulação, fiscalização e sancionamento, além de estar alinhado com a tendência de desjudicialização, reconhece a necessidade de conhecimento técnico e jurídico

---

Lei n. 4.060, de 2012, do Deputado Milton Monti, que dispõe sobre o Tratamento de Dados Pessoais. Ribeirão Preto: 2017. Disponível em: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/dra-cintia-rosa-pereira-de-lima-usp>. Acesso em: 05.jun.2017. p. 7 e 8.

específico para tratar com situações complexas envolvendo o domínio da tecnologia mais avançada. Como ocorre com outros órgãos de controle e em homenagem ao princípio constitucional da inafastabilidade da jurisdição, o Poder Judiciário poderia ser chamado a atuar após o esgotamento das vias administrativas e para dirimir controvérsias de ordem procedimental e não de ordem material e técnica.

A independência do órgão de controle se justifica pelo fato das entidades públicas também estarem sujeitas à lei de proteção de dados pessoais. Se, como dito anteriormente, a eficácia de um modelo de autorregulação pode correr riscos pelo fato da entidade ser administrada por representantes das entidades fiscalizadas, da mesma forma o órgão de controle sem independência das entidades estatais padeceria do mesmo problema em sua tarefa de fiscalizar aqueles que o administram. É nesta linha a recomendação de STEFANO RODOTÀ:

> *Para garantir a independência, é necessário portanto que o órgão de vigilância se localize fora das estruturas administrativas e burocráticas tradicionais.*[117]

Já no início da década de 1990, o Parlamento e Conselho Europeu entenderam a necessidade da existência de um órgão de controle independente de modo que passou a constar no considerando n° 62 da Diretiva 95/46/CE que a criação destas autoridades de controle seriam um "elemento essencial" para a proteção dos indivíduos:

> *(62) Considerando que a criação nos Estados-membros de autoridades de controle que exerçam as suas funções com total independência constitui um elemento essencial da proteção das pessoas no que respeita ao tratamento de dados pessoais;*[118]

Ademais, previu a referida diretiva sobre a concessão de poderes especiais de "inquérito ou de intervenção" bem como "poderes para intervir em processos judiciais".[119]

---

[117] RODOTÀ, STEFANO. A vida na sociedade da vigilância: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda.. Rio de Janeiro: Renovar, 2008. p. 86.

[118] Preâmbulo da Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046>. Acesso em: 19.jun.2017.

[119] Ibidem, Considerando n° 63.

O artigo 28 da Diretiva 95/46/CE dispõe que cada Estado-Membro deveria estabelecer uma ou mais autoridades públicas com a competência de fiscalizar as disposições sobre proteção de dados pessoais. As autoridades de controle deveriam ter poder de inquérito, poder de intervenção bem como deveriam cooperar com as autoridades de controle dos outros Estados-Membros.

Desta forma, encontramos na Europa órgãos de proteção de dados pessoais como, por exemplo, o ICO (*Information Commissioner's Office*) no Reino Unido[120], a CNIL (*Commission Nationale de l'Informatique et des Libertés*) na França[121] e a Autoridade de Proteção de Dados Italiana (*Garante per la protezione dei dati personali*)[122].

Defendendo a imprescindibilidade de um órgão independente de proteção de dados pessoais, CÍNTIA ROSA PEREIRA DE LIMA declina sua tríplice função:

> *Tal órgão [Autoridade Garante] teria uma tríplice função: 1) de fiscalizar o estrito cumprimento das normas de proteção de dados pessoais, inclusive com medidas de investigação quando*

---

[120] O ICO (Information Commissioner's Office) tem o papel de proteger os direitos informacionais com objetivos estratégicos que incluem o aumento da confiança pública em como dos dados pessoais são usados e disponibilizados, a melhoria dos padrões para a efetivação dos direitos informacionais, a manutenção e melhoria da influência na comunidade regulatória global relacionada a direitos informacionais, a manutenção de sua relevância fornecendo excelente serviço público alinhado com a evolução tecnológica e a prática de enforcement das normas relacionadas ao seu objetivo. A atuação do ICO é orientada pelo Data Protection Act de 1998. Disponível em: <https://ico.org.uk/about-the-ico/our-information/mission-and-vision/>. Acesso em: 25.jun.2017.

[121] A CNIL tem como objetivos principais a proteção dos dados pessoais, o apoio à inovação e a preservação das liberdades individuais. Dentre suas competências estão a veiculação de informação aos indivíduos sobre seus direitos, o recebimento de reclamações sobre violação dos direitos, a elaboração de pareceres e recomendações para controladores de dados e para projetos de lei, a certificação para produtos ou serviços que os distingam por sua qualidade e aderência aos padrões, fiscalização e sancionamento. Disponível em: <https://www.cnil.fr/en/cnils-missions>. Acesso em: 26.jun.2017.

[122] A Autoridade Garante Italiana, à semelhança da maioria das DPAs, foi estabelecida na segunda metade da década de 1990 como autoridade independente criada para proteger os direitos e liberdades fundamentais relacionadas com o processamento dos dados pessoais de modo a respeitar a dignidade dos indivíduos. Suas atividades incluem supervisão da conformidade com as leis de proteção da vida privada, administrar as reclamações e relatórios enviados por cidadãos, banir ou bloquear operações de processamento de dados com potencial de causar danos aos indivíduos, recorrer aos órgãos judiciais em caso de violações graves, levar ao conhecimento da população a legislação de privacidade, dentre outros. Disponível em: <http://www.garanteprivacy.it/web/guest/home_en/who_we_are>. Acesso em: 27.jun.2017.

> *necessárias e impondo sanções administrativas ao constatar violação da lei; 2) de estabelecer padrões técnicos e administrativos para, de maneira eficaz e preventiva, garantir a proteção dos dados pessoais bem como desenvolver políticas públicas neste tema; 3) de resolver litígios pela violação das normas de proteção dos dados pessoais a partir de notificações que receba, além de avaliar a criação de Códigos de Boas Práticas e a transferência internacional de dados pessoais.*[123]

Já no âmbito nacional, o projeto de lei do Executivo que tramita no Congresso Nacional prevê a existência de um órgão de controle com competência equivalente àquela prevista no modelo europeu. Em seu artigo 53 o referido projeto de lei elenca as competências deste órgão que incluem a elaboração de diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade, a realização de auditorias para garantir a conformidade do tratamento de dados com as disposições da lei, a promoção do conhecimento das normas e políticas públicas perante a população e por meio de estudos sobre as práticas de proteção de dados pessoais, o estímulo para a adoção de padrões de produtos e serviços que facilitem o controle de dados pelos seus titulares, promoção de ações de cooperação internacional com autoridades de outros países, elaborar normas complementares sobre proteção de dados bem como relatórios periódicos sobre suas atividades.

---

[123] LIMA, Cíntia Rosa Pereira de. A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil. 487 p. Tese de Livre Docência. Faculdade de Direito Ribeirão Preto/USP. 2015. p. 11.

6 A Tutela Jurídica no Exterior e no Brasil

6.1 A Tutela Jurídica dos Dados Pessoais nos Estados Unidos

Nos Estados Unidos da América não há uma lei federal que regule de forma abrangente a coleta, uso e compartilhamento de dados pessoais. Há, no entanto, um conjunto de leis federais e estaduais aplicáveis a setores específicos que muitas vezes se sobrepõem ou até mesmo se contradizem.

Neste conjunto de disposições que regulam a coleta e uso de dados pessoais encontraremos aquelas relacionadas a categorias específicas de dados como, por exemplo, dados financeiros, dados de saúde e dados de comunicações eletrônicas. Outras disposições se aplicam a determinadas atividades como, por exemplo, telemarketing e e-mails comerciais.

6.1.1 Privacy Act (1974)

O *Privacy Act* é a parte do Título 5 do *United States Code*[124] que disciplina a coleta, uso e compartilhamento de dados pessoais por agências do governo americano. Sua concepção foi motivada pela necessidade do governo americano manter informações sobre os cidadãos americanos e sobre os estrangeiros residentes no país e, ao mesmo tempo, garantir os direitos individuais de proteção à privacidade. O fato social que serviu como catalisador para esta produção legislativa foram os atos abusivos de agências federais no processo de investigação de pessoas relacionadas no caso Watergate.[125]

Os principais objetivos do *Privacy Act* podem ser resumidos a quatro: (1) restringir a divulgação de dados pessoais mantidos por agências governamentais, (2) conceder a cada indivíduo o direito de acessar os dados que lhe digam respeito,

---

[124] 5 U.S.C. § 552ª. Disponível em: <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf>. Acesso em: 30.abr.2017.

[125] Departamento de Justiça dos Estados Unidos da América. OVERVIEW OF THE PRIVACY ACT OF 1974: Legislative History. 2015. Disponível em: <https://www.justice.gov/opcl/legislative-history>. Acesso em: 01.mai.2017.

(3) conceder aos indivíduos o direito de correção destes dados diante da demonstração de que tais dados não estão corretos, atualizados, completos ou que não são relevantes e (4) estabelecer um código de práticas justas ("*Fair Information Practices*") no trato com a informação exigindo que as agências sigam normas para a coleta, manutenção e disseminação dos dados.[126]

Embora o *Privacy Act* tenha escopo limitado, uma vez que é aplicável apenas às agências do governo norte americano em nível federal, ele traz aspectos de natureza principiológica que deveriam ser observados atualmente por empresas privadas de internet, principalmente em relação ao *online profiling.* Desta forma, deveria ser conferido ao usuário de internet o direito de obter informações junto às empresas de internet relacionadas aos dados que elas mantêm sobre ele bem como a possibilidade de correção ou eliminação destes dados.

Embora as práticas impostas pelo *Privacy Act* de 1974 só vinculem as agências públicas, as empresas privadas de internet poderiam e deveriam se submeter às mesmas regras em razão da privacidade informacional dos indivíduos estar em posição de maior fragilidade hoje do que há 40 anos tendo-se em conta a grande capacidade de armazenamento e processamento de dados destas empresas privadas.

Dentre as regras do *Privacy Act* que poderiam e deveriam ser rigorosamente observadas por estas empresas privadas estão as seguintes:

- 5 U.S.C. § 552a(b) – A divulgação ou compartilhamento das informações só poderia ser realizada mediante o pedido ou autorização por escrito do sujeito relacionado aos dados. O *Privacy Act* dispõe sobre as exceções a esta regra que em geral referem-se às situações onde a lei, a ordem judicial ou as práticas exigem o acesso e utilização das informações dentro da agência ou em órgãos como o *Bureau of the Census, National Archives* ou para análises estatísticas.

---

[126] Departamento de Justiça dos Estados Unidos da América. OVERVIEW OF THE PRIVACY ACT OF 1974: Policy Objectives. 2015. Disponível em: <https://www.justice.gov/opcl/policy-objectives>. Acesso em: 01.mai.2017.

- 5 U.S.C. § 552a(d)(1) – As agências devem fornecer ao sujeito relacionado aos dados, mediante requerimento, uma cópia de todos os dados relacionados num formato que lhe seja compreensível.
- 5 U.S.C. § 552a(d)(2) – O indivíduo pode solicitar a alteração das informações a seu respeito nas bases de dados da agência.
- 5 U.S.C. § 552a(e)(1) – O governo deve manter em suas bases de dados apenas os dados estritamente necessários e relevantes para a execução dos propósitos da agência definidos por lei ou por ordem executiva do presidente.
- 5 U.S.C. § 552a(n) – Dados com o nome ou endereço do indivíduo não podem ser vendidos ou alugados exceto se a lei especificamente assim autorizar.

Em 2013, um projeto de lei, denominado *Right to Know Act of 2013*, tramitou no estado da Califórnia que, se fosse aprovado, obrigaria as empresas que mantêm ou compartilham dados pessoais a fornecer a ele, mediante requerimento, no prazo de 30 dias e sem custo, uma cópia de todos os dados do indivíduo bem como os nomes e informações de contato de todas as pessoas para as quais os dados foram compartilhados nos últimos 12 meses.[127]

Empresas como Google, Facebook e Microsoft, alegando que haveria uma avalanche de solicitações e aumento de custos, trabalharam junto ao poder legislativo daquele estado para que o projeto de lei não fosse aprovado.[128] O trabalho destas empresas foi bem sucedido e em 2014 o projeto de lei foi arquivado.

---

[127] California Legislative Information. AB-1291 Privacy: Right to Know Act of 2013: disclosure of a customer's personal information. Disponível em: <http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201320140AB1291>. Acesso em: 02.mai.2017.

[128] The Mercury News. Silicon Valley companies quietly try to kill Internet privacy bill. Disponível em <http://www.mercurynews.com/2013/04/19/silicon-valley-companies-quietly-try-to-kill-internet-privacy-bill>. Acesso em: 06.dez.2017.

6.1.2 PCAST Report

Em maio de 2014 o Conselho de Consultores da Presidência em Ciência e Tecnologia (PCAST - President's Council of Advisors on Science and Technology) divulgou um relatório intitulado “Big Data and Privacy: A Technological Perspective”[129] no qual analisa os impactos na privacidade resultantes da difusão da coleta, tratamento e uso de dados pessoais.

O objetivo do estudo foi fornecer informações para que o Poder Executivo implementasse políticas públicas de proteção à privacidade bem como explorasse os benefícios que o Big Data e seu ferramental podem oferecer.

Ao reconhecer que os benefícios que o Big Data pode oferecer são superiores ao risco de danos (e.g. desenvolvimento de novas formas de tratar doenças, melhoria do transporte público, dados para pesquisas científicas, etc...), o Conselho apresentou recomendação no sentido de que as políticas de proteção à privacidade não enfatizem restrições na coleta e armazenamento de dados, mas que o foco das medidas protetivas seja colocado no efetivo uso dos dados bem como no cuidado com a informação processada e inferida.[130]

O Conselho reconhece o fracasso das políticas de privacidade fundadas no consentimento dado pelos usuários que, de fato, não leem os termos e não têm condições de entender as implicações do processo de coleta, tratamento e utilização dos dados.[131] Em seu lugar, propõe que entidades sirvam como intermediárias na relação entre os usuários e as empresas de internet para estabelecerem diferentes perfis de privacidade. Por exemplo, um indivíduo poderia aderir a um perfil de privacidade estabelecido pela *American Civil Liberty Union* que

---

[129] President's Council of Advisors on Science and Technology (PCAST). Big Data: A Technologyical Perspective. 2014. Disponível em: <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf>. Acesso em: 05.mai.2017.

[130] Ibidem, p. 7

[131] Ibidem, p. 38

enfatiza os direitos individuais enquanto outro usuário poderia adotar o perfil oferecido pelo *Consumer Reports* que enfatiza o valor econômico propiciado ao consumidor. Outra possibilidade seria a criação de perfis de privacidade distintos oferecidos pelas grandes empresas do setor (Apple App Store, Google Play, Microsoft Store).[132]

O relatório conclui com cinco recomendações:

1. As políticas de privacidade devem enfatizar a regulação do uso dos dados e das informações derivadas e não colocar o foco na restrição da coleta e do processamento de dados.
2. A normas e políticas de privacidade não devem determinar tecnologias específicas para a proteção da privacidade, mas devem se concentrar nos resultados pretendidos.
3. Devem ser realizados investimentos para pesquisa nas áreas de tecnologia e ciência social por meio dos órgãos responsáveis.[133]
4. Enfatizar o treinamento na área de proteção de privacidade incluindo a criação de carreiras para profissionais dedicados a esta área.
5. Os EUA devem assumir a liderança internacional na adoção de políticas que façam uso de tecnologia em favor da privacidade, promovendo a criação de padrões que possam ser utilizados em outros países.

6.2 A Proteção de Dados Pessoais na Comunidade Europeia

Embora os grandes debates sobre o direito à privacidade tenham se originado nos Estados Unidos, foi na Europa que se observou o desenvolvimento dos principais diplomas normativos gerais de proteção aos dados pessoais.

---

[132] Ibidem, p. 40.

[133] No caso dos EUA, a proposta é que a coordenação e o fomento da pesquisa fique a cargo do OSTP (The White House Office of Science and Technology Policy) enquanto a realização fique a cargo do NITRD (Networking and Information Technology Research and Development program).

Com o desenvolvimento tecnológico que implicou numa maior velocidade de processamento e maior capacidade de armazenamento de dados, o último terço do século 20 assistiu à produção de iniciativas legislativas que objetivaram a proteção dos dados pessoais na Europa. A partir da década de 60, países como Alemanha, Suécia, Dinamarca, França, Espanha e Portugal produziram normas de proteção.[134] No entanto, em face do dinamismo das relações entre os países europeus, que implicou não apenas num aumento do fluxo de pessoas e de capitais, mas também de informações, logo percebeu-se que as iniciativas legislativas seriam mais eficazes se tivessem um escopo supranacional.

Diante da crescente integração entre os países da Europa, observada principalmente no final do século 20, frutificaram disposições supranacionais sobre a proteção de dados pessoais.

Em 1980 a OECD (*Organisation for Economic Co-operation and Development*), que congrega 35 países, elaborou as *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[135]*,* de caráter principiológico, com o objetivo de harmonizar as regras nacionais sobre o tema. Dentre os princípios exarados nestas diretrizes estão os seguintes:

1) Princípio da Limitação da Coleta – Deve haver limitações na coleta de dados pessoais. Os meios de coleta devem ser legais e justos devendo o

[134] Demócrito Reinaldo Filho resume as iniciativas legislativas europeias da seguinte forma: “Em 1970, o Estado alemão de Hesse editou a primeira lei sobre essa matéria. A Suécia conta com o Datalegen, Lei 289 de 11 de maio de 1973. Desde 1977, a Alemanha tem uma lei federal de proteção de uso ilícito de dados pessoais. A Dinamarca regulamenta a questão da proteção de dados pelas Leis 243 e 244, ambas de 08 de julho de 1978, que estenderam a proteção também para as pessoas jurídicas. A França tem a Lei 78-77, de 06 de janeiro de 1978. A Espanha tem a peculiaridade de ter uma regra constitucional determinando a regulamentação da proteção da privacidade contra invasões da atividade informática (art. 18, par. 1º.). A Constituição de Portugal de 1977 tem texto ainda mais completo (art. 35), pois contempla a previsão do direito do cidadão de conhecer os dados que lhe são concernentes, de que esses dados sejam utilizados de acordo com a finalidade para o qual foram recolhidos e, ainda, de retificá-los (em caso de erro) e de atualizá-los”. - REINALDO FILHO, Demócrito. Disponível em: <https://jus.com.br/artigos/23669>. Acesso em: 02.dez.2017

[135] OECD - Organisation for Economic Co-operation and Development (Website). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Disponível em: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> Acesso em: 07.dez.2017

sujeito relacionado aos dados ter o conhecimento ou ofertando o consentimento com relação à coleta.

2) Princípio da Qualidade de Dados – O dado deve ser relevante para o fim ao qual se destina e deve ser preciso, correto e atualizado.
3) Princípio da Especificação do Propósito – O propósito para a coleta de dados deve ser especificado antes da coleta.
4) Princípio da Limitação do Uso – Os dados coletados poderão ser usados apenas para atender ao propósito especificado originalmente ou para outros propósitos que não sejam incompatíveis com o propósito original, exceto se houver previsão legal ou consentimento do sujeito relacionado aos dados.
5) Princípio da Segurança dos Dados – Os dados pessoais devem ser protegidos contra acesso, uso, alteração e destruição não autorizados.
6) Princípio da Participação do Indivíduo – O sujeito relacionado aos dados tem o direito de exigir do controlador dos dados informações sobre a existência de dados relacionados a si no banco de dados do controlador. Também tem o direito de exigir, quando aplicável, a alteração, retificação ou complementação de dados.
7) Princípio da Responsabilidade (Accountability) – O controlador dos dados é responsável pela execução de todas as medidas que tornem efetivos os princípios exarados acima.

Em 1981, o Conselho da Europa aprovou a Convenção para a Proteção dos Indivíduos com Relação ao Processamento Automático de Dados Pessoais.[136] Esta Convenção reafirmou princípios já exarados nas diretrizes da OECD, mas com ênfase na privacidade individual, preocupando-se com todas as fases do

[136] Concil of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 1981. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 05.mai.2017.

processamento dos dados, desde a coleta até a segurança do armazenamento, distinguindo categorias especiais de dados tais como os que revelam a origem racial, opiniões políticas, crenças religiosas, saúde e vida sexual[137].

Todo o desenvolvimento legislativo dos países europeus e as normas supranacionais sobre proteção de dados influenciaram a produção, em 1995, da Diretiva 95/46/CE[138] que acabou se tornando a referência normativa sobre o tema durante duas décadas. Esta diretiva foi concebida tendo-se em mente dois objetivos: a proteção do direito sobre os dados pessoais e a garantia do livre fluxo de dados pessoais entre os Estados-Membros.

Em dezembro de 2000 o Parlamento Europeu proclamou a Carta dos Direitos Fundamentais da União Europeia[139], cuja observância foi tornada obrigatória em 2009 pelo Tratado de Lisboa. Este diploma legislativo dispõe em seu artigo 8° sobre a proteção de dados de caráter pessoal. O item 2 do referido artigo disciplina o tratamento dos dados pessoais dispondo, de forma genérica, que ele deve ser realizado de forma “leal”. Aduz que o tratamento deve ser realizado “para fins específicos e com o consentimento da pessoa interessada”. Por fim, confere a todo indivíduo o direito de acesso aos dados que lhe digam respeito bem como o direito de retificação.

As disposições mencionadas forneceram diretrizes para que os Estados-Membros elaborassem suas normas internas de proteção de dados pessoais. É de se destacar que a iniciativa legislativa mais detalhada sobre o tema foi a Diretiva 95/46/CE que, por se tratar de “diretiva”, só passou a produzir efeitos nos Estados-Membros após o processo de transposição.

De fato, a função de uma diretiva é vincular os Estados em relação ao resultado que se deseja alcançar deixando a cargo das instâncias nacionais a definição da forma e meios de atingir os objetivos. É por meio do ato de

---

[137] Ibidem. Article 6.

[138] European Parliament and of the Council. Directive. Directive 95/46/EC. 1995. Disponível em: <http://eur-lex.europa.eu/eli/dir/1995/46/oj>. Acesso em: 05.mai.2017.

[139] Parlamento Europeu. Carta dos Direitos Fundamentais da União Europeia. 2000. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT>. Acesso em: 06.mai.2017.

transposição que os objetivos e resultados pretendidos pela diretiva são internalizados ganhando especificidade com relação ao meio e formas de alcançá-los. Desta forma a diretiva só produz efeito e só gera direitos aos cidadãos após o ato de transposição. Embora a sistemática da regulação por meio de diretiva com transposição ofereça aos Estados-Membros a liberdade de adaptar a norma comunitária à realidade local, tal sistemática compromete a uniformidade na disciplina de tratamento dos dados pessoais, uniformidade tão necessária quando se leva em conta o dinamismo no fluxo de dados entre os países da Comunidade Europeia e para fora da comunidade.

Com o objetivo de proporcionar aplicação uniforme da diretiva, foi instituído o Grupo de Proteção das Pessoas (*Working Party*). A este grupo, composto por representantes das autoridades de controle de cada Estado-Membro, foi atribuído um caráter consultivo e independente com o fim de dar parecer sobre as questões relacionadas à aplicação da Diretiva no âmbito nacional, aconselhar sobre projetos de alteração na Diretiva e elaborar relatórios sobre a situação da proteção das pessoas no tocante aos dados pessoais.[140]

Em janeiro de 2012, com vistas à obtenção de uniformidade e ao fortalecimento das normas já existentes, a Comissão Europeia propôs uma reforma profunda na legislação de proteção de dados pessoais da União Europeia. Em abril de 2016 o Parlamento Europeu aprovou a GDPR (*General Data Protection Regulation*)[141].

Este regulamento, que entrará em vigor em maio de 2018, substituirá a Diretiva 95/46/CE e, por se tratar de regulamento, não necessitará de ato de transposição para que produza efeitos nos Estados-Membros. Na realidade, o regulamento vincula os sujeitos que coletam ou processam dados pessoais de cidadãos europeus independentemente da posição geográfica do sujeito que coleta e trata os dados.

---

[140] O *Working Party* foi instituído no artigo 29 da Diretiva 95/46/CE e suas atribuições foram elencadas no artigo 30.

[141] Council of the European Union. General Data Protection Regulation. 2015. Disponível em: <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>. Acesso em: 08.mai.2017.

6.2.1 A Diretiva 95/46, Regulamento 2016/679 e o Profiling

O Big Data, as práticas de *profiling* bem como as técnicas de reidentificação não eram tão difundidas quando a Diretiva 95/46/CE foi concebida. Por isso não há na Diretiva referência explícita a estas práticas nem dispositivos específicos para a proteção dos indivíduos no âmbito da criação de perfis.

O Regulamento 2016/679 (GDPR – General Data Protection Regulation), por outro lado, foi gestado numa época em que as práticas de tratamento de dados para criação de perfis já eram uma realidade no mercado. Por esta razão, o Parlamento Europeu levou em conta esta prática no momento da produção deste novo diploma legislativo.

Destaque-se, de início, a definição de *profiling* constante no art. 4.4 do GDPR:

> *"Definição de perfis", qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;*

Ao se referir ao objeto da avaliação dos dados pessoais como “aspectos pessoais”, o Parlamento Europeu não circunscreve tais dados e aspectos ao âmbito do conjunto de atributos do indivíduo. A criação de perfis deve ser entendida como algo que pode ter um escopo mais amplo. Tais avaliações de natureza analítica ou preditiva se baseiam não apenas no que o indivíduo é, ou seja, nos seus atributos pessoais, mas também naquilo que o indivíduo faz, ou seja, no seu comportamento.

A preocupação com a criação de perfis baseada em dados da esfera comportamental do indivíduo coletados por meio de rastreamento (“*online behavior*”) motivou o Parlamento Europeu a incluir o considerando 24 no preâmbulo do GDPR, o qual trata do denominado “controle de comportamento”, especialmente

aquele comportamento na internet (sites visitados, compras efetuadas online, postagens em redes sociais, etc...).[142]

6.2.1.1 Decisões Baseadas em Tratamento Exclusivamente Automatizado

Embora a Diretiva 95/46 não tenha explicitamente disciplinado as situações de criação de perfil, algumas disposições da diretiva sobre a proteção do indivíduo no tratamento de dados podem ser aplicadas a esta prática.

O artigo 15 da Diretiva, por exemplo, dispõe sobre a proibição de decisões tomadas exclusivamente a partir de um tratamento automatizado de dados que afete a esfera jurídica do indivíduo.[143]

Como visto, o processamento de dados pessoais no contexto do Big Data e do *online profiling* poderá gerar dados derivados cuja utilização e compartilhamento têm o potencial de categorizar, estigmatizar e discriminar o sujeito relacionado aos dados. Em tais situações, o artigo 15 da Diretiva vem tutelar o indivíduo ao impedir que decisões que o afetem negativamente sejam tomadas de modo exclusivamente automático, ou seja, sem a intervenção humana[144].

---

[142] "O tratamento de dados pessoais de titulares de dados que se encontrem na União por um responsável ou subcontratante que não esteja estabelecido na União deverá ser também abrangido pelo presente regulamento quando esteja relacionado com o controle do comportamento dos referidos titulares de dados, na medida em que o seu comportamento tenha lugar na União. A fim de determinar se uma atividade de tratamento pode ser considerada ***"controle do comportamento"*** de titulares de dados, deverá determinar-se se essas pessoas são ***seguidas na Internet*** e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes." – Grifou-se – Considerando 24 do Preâmbulo do Regulamento.

[143] Artigo 15 da Diretiva 95/46: "1. Os Estados membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento."

[144] Este dispositivo da Diretiva 95/46/CE muito provavelmente buscou inspiração na Loi Informatique Et Libertes de 1978 que, em seu artigo 10, proíbe que informações derivadas de processamento automático de dados pessoais sirvam como base para (1) decisões da corte, (2) decisões que afetem juridicamente o indivíduo e (3) decisões no contexto de admissão para a contratação: "*No court decision involving the assessment of an individual's behaviour may be based on an automatic processing of personal data intended to assess some aspects of their personality. No other decision having a legal effect on an individual may be taken solely on the grounds of automatic processing of data intended to define the profile of the data subject or to assess some*

No entanto, como o disposto neste artigo se refere apenas às decisões exclusivamente tomadas por métodos automáticos, existe o risco de haver no processo decisório sobre o indivíduo uma intervenção humana meramente formal, intervenção sem o poder de alterar de forma significativa a decisão indicada automaticamente. Tratar-se-ia, no caso, de uma intervenção humana apenas para descaracterizar a conduta vedada no dispositivo, qual seja, a de tomada de decisão de forma "exclusivamente" automatizada. Como exemplo, pode-se citar a oferta de um serviço cujo valor é determinado de forma automática com base numa categoria do sujeito, categoria inferida por meio de processamento de dados brutos. Tal decisão, ao ser comunicada por um representante do ofertante, indivíduo que não pode se afastar dos números fornecidos automaticamente, deixa de ser qualificada como uma decisão tomada exclusivamente de forma automatizada na medida em que houve uma intervenção humana meramente formal[145]. Portanto, o referido artigo da Diretiva, como disposto, não é suficiente para proteger satisfatoriamente o indivíduo.

O risco de tomada de decisão baseada unicamente em processamento automático aumenta no contexto do Big Data e dos algoritmos de *profiling*. Neste novo cenário, o GDPR que substituirá a Diretiva 95/46/CE, apresenta em seu artigo 22 o congênere do artigo 15 da Diretiva. No entanto, o novo dispositivo leva em conta a realidade atual da elaboração dos perfis:

> *O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos*

---

aspects of their personality. Neither the decisions taken in the context of entering into or performing a contract and concerning which the data subject had an opportunity to give their remarks nor those that meet the request of the data subject shall be regarded as taken solely on the grounds of automatic processing." - Disponível em: <https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf>. Acesso em: 08.mai.2017.

[145] Esta preocupação foi apontada pelo Grupo de Proteção das Pessoas (*Working Party*) na Avaliação de Impacto "COMMISSION STAFF WORKING PAPER Impact Assessment /* SEC/2012/0072 final */". Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012SC0072>. Acesso em: 08.mai.2017.

> *na sua esfera jurídica ou que o afete significativamente de forma similar.*[146]

Embora esta disposição do GDPR não trate especificamente das situações em que uma atuação meramente formal de um indivíduo ocorra no processo para descaracterizar a prática vedada – o tratamento exclusivamente automatizado –, no considerando n° 71 de seu preâmbulo são apresentados exemplos de decisões automatizadas vedadas, onde poderia existir uma atuação humana meramente formal[147]. Fica claro neste item do preâmbulo que o sujeito relacionado aos dados tem o direito de obter uma intervenção humana para que possa manifestar sua opinião e obter uma explicação sobre a decisão, bem como contestá-la. Deve-se ressaltar que embora o preâmbulo e seus considerandos não tenham efeito vinculante, eles expressam a *mens legis* e podem influenciar bem como fornecer diretrizes para o intérprete e aplicador da lei.

Tanto a Diretiva quanto o GDPR estabelecem exceções para a regra geral de vedação às decisões baseadas exclusivamente em processamento

---

[146] Artigo 22 do GDPR.

[147] "O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como *a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana*. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o ***direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão***. Essa medida não deverá dizer respeito a uma criança." – Considerando n° 71 do GDPR – Grifou-se.

automático. O Regulamento reafirmou as duas exceções já estabelecidas pela Diretiva e inovou apresentando nova exceção.

De acordo com a Diretiva e com o Regulamento é possível a tomada de decisão baseada exclusivamente em informações geradas por processamento automático nos casos em que (1) a decisão ocorrer no contexto da celebração ou execução de um contrato entre o sujeito relacionado aos dados e o responsável pelo processamento dos dados[148] e quando (2) a decisão for autorizada por lei, desde que esta contenha previsão de medidas para proteger os direitos e interesses do sujeito relacionado aos dados[149]. O GDPR inovou apresentando uma exceção não prevista na Diretiva: o consentimento explícito do sujeito relacionado aos dados[150].

Embora estas três exceções estabeleçam situações nas quais é permitida a tomada de decisão com base em informações obtidas de forma exclusivamente automática, o Regulamento estabelece em seu art. 22.4 a "exceção das exceções" dispondo que as exceções não se aplicam se os dados forem aqueles referidos no art. 9° do GDPR, ou seja, se a decisão automatizada for tomada com base nos denominados "dados sensíveis". A complexidade do dispositivo é tamanha que na parte final do art. 22.4 é apresentada a "exceção da exceção das exceções", ou seja, as situações nas quais mesmo que os dados sejam sensíveis, é possível a tomada de decisão com base em processamento exclusivamente automático.[151]

---

[148] Art. 15°, 2(a) da Diretiva 95/46/CE e Art. 22°, 2(a) do GDPR.

[149] Art. 15°, 2(b) da Diretiva 95/46/CE e Art. 22°, 2(b) do GDPR.

[150] Lê-se no Art. 22° do Regulamento: "O n.º 1 não se aplica se a decisão: (...) (c) For baseada no consentimento explícito do titular dos dados."

[151] Transcreve-se a "exceção das exceções" bem como sua exceção: "As decisões a que se refere o n.º 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.º, n.º 1 [*dados sensíveis*], a não ser que o n.º 2, alíneas a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular." Art. 22.4 do GDPR. As referidas alíneas "a" e "g" fazem menção a situações em que a) a pessoa relacionada aos dados dá consentimento explícito para o tratamento destes dados pessoais e g) o tratamento de dados sensíveis for necessário por motivos de interesse público.

6.2.1.2 As Categorias Especiais de Dados

O GDPR, em seu artigo 9.1, apresenta uma relação de "categorias especiais de dados", comumente conhecida na literatura especializada como "dados sensíveis", os quais merecem maior cuidado no tratamento:

> *É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.*

Esta disposição é praticamente uma transcrição do artigo 8.1 da Diretiva[152], no qual foram adicionadas as categorias de dados genéticos e biométricos que não constavam do diploma de 1995. Ambas as disposições que versam sobre as categorias especiais de dados trazem hipóteses nas quais permite-se o tratamento dos dados sensíveis.

Discute-se, no entanto, se a apresentação de um rol taxativo de categorias especiais seria a melhor alternativa para proteger o sujeito relacionado aos dados em questões "sensíveis".

Tal questionamento justifica-se quando se leva em conta que é possível, a partir de dados pertencentes a categorias não consideradas "sensíveis", obter-se por meio de processamento de dados as informações de natureza sensível. Tome-se como exemplo uma instituição financeira que ao analisar a possibilidade de concessão de crédito ao um indivíduo não leve em conta sua origem racial ou etnia, respeitando desta forma as restrições decorrentes das categorias especiais de dados, no entanto, a partir de dados relacionados ao domicílio do sujeito é possível, por via oblíqua, deduzir a raça ou origem étnica e, consequentemente, negar-lhe o crédito, principalmente após obter, por meio de processamento e correlação de dados, a informação de que pessoas de determinada etnia são menos propensas

---

[152] O artigo 8.1 da Diretiva dispõe que "Os Estados membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual."

a cumprir suas obrigações financeiras e na região do domicílio do indivíduo sob análise a maioria dos residentes é daquela determinada etnia.

Desta forma, o foco deve ser colocado não na natureza do dado (sensível ou não sensível), mas na lógica subjacente para a tomada da decisão, o que será tratado a seguir.

6.2.1.3 O Direito à Lógica Subjacente

Outra questão controversa envolvendo a decisão tomada com base em tratamento exclusivamente automático é o direito do sujeito relacionado aos dados ter acesso à lógica subjacente ao processamento. A Diretiva, em seu artigo 12°(a) garante ao sujeito relacionado aos dados a possibilidade de obter da empresa que faz as análises informações sobre a lógica utilizada no tratamento:

> *"Os Estados-membros garantirão às pessoas em causa o direito de obterem do responsável pelo tratamento: a) Livremente e sem restrições, com periodicidade razoável e sem demora ou custos excessivos: (...) o conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito, pelo menos no que se refere às decisões automatizadas referidas no nº 1 do artigo 15°."*

Enquanto a Diretiva confere ao sujeito o direito de requerer e obter do controlador dos dados o conhecimento da lógica subjacente ao processamento, o GDPR, em seu artigo 13.2(f), vai além, aumentando significativamente a transparência do procedimento, ao dispor que já no momento da obtenção dos dados, ou seja, no momento da coleta ou rastreamento, o controlador deve fornecer não apenas informações úteis sobre a lógica envolvida no processamento, mas também a relevância e possíveis consequências do tratamento automatizado[153].

Aqui observa-se uma mudança significativa com relação à dinâmica do fluxo de informações do controlador dos dados para o sujeito relacionado aos dados. Inicialmente, por disposição da Diretiva, ao sujeito era garantido o direito de

---

[153] "Para além das informações referidas no n.º 1, aquando da recolha dos dados pessoais, o responsável pelo tratamento fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente: (...) f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados." – Artigo 13.2(f) do GDPR.

solicitar e obter do controlador as informações sobre os dados e o tratamento efetuado pelo controlador. O novo Regulamento amplia os deveres do controlador obrigando-o a informar ao sujeito a lógica do tratamento independentemente de solicitação prévia. Este dever do controlador é reforçado no preâmbulo do GDPR, especificamente no considerando 63, segundo o qual

> *"cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências."*[154]

6.3 A Tutela Jurídica dos Dados Pessoais no Brasil

O Brasil ainda não tem legislação específica sobre proteção de dados pessoais. As decisões judiciais sobre o tema se baseiam em princípios e regras gerais de tutela da privacidade encontradas na Constituição Federal e na legislação infraconstitucional[155].

Um dos princípios exarados na Lei 12.965/2014 – Marco Civil da Internet – é a "proteção dos dados pessoais, na forma da lei" (art. 3°, III). A esta lei de proteção de dados, que ainda não existe, é feita referência novamente no artigo 7°, VII, onde o legislador restringe o fornecimento de dados pessoais, de registros de conexão e de acesso a aplicações de internet a terceiros ao consentimento livre, expresso e informado "ou nas hipóteses previstas em lei". Perceba-se que o MCI regula a captura de dados pessoais com base no paradigma do consentimento do usuário, modelo que, como já discutido anteriormente, sofre severas críticas.

No Brasil há, atualmente[156], três projetos de lei em tramitação cujo objetivo é a proteção de dados pessoais: um de iniciativa do Poder Executivo (PL

---

[154] Preâmbulo do GDPR, Considerando (63).

[155] Dentre os diplomas legislativos que dispõem sobre a tutela da privacidade menciona-se o Código Civil (art. 21), o Marco Civil da Internet (Lei 12.965/2014 arts. 3º, II; 7º, 8º, 10, 21 e 23), a Lei do Cadastro Positivo (Lei 12.414/2011).

[156] Este texto foi atualizado em novembro de 2017.

5.276/2016)[157], outro de iniciativa do Senado[158] e, finalmente, um projeto de iniciativa da Câmara dos Deputados (PL 4060/2012)[159]. Em julho de 2016 o Projeto de Lei do Executivo foi apensado ao Projeto de Lei da Câmara dos Deputados.

Estes projetos têm inspiração nos princípios e regras europeias conforme disposto na Diretiva 95/46 e no Regulamento (UE) 2016/679 (GDPR). Sobre estes projetos passa-se a discorrer a seguir.

6.3.1 Projeto de Lei nº 5.276/2016

Em 2015 o Ministério da Justiça abriu uma consulta pública sobre um anteprojeto de lei de proteção de dados pessoais. O resultado do anteprojeto, com as contribuições da consulta pública, foi remetido ao Congresso Nacional, o que gerou o PL 5.276/2016 que chegou a tramitar em regime de urgência constitucional, antes de ser apensado ao PL 4060/2012 em meados de 2016.

6.3.1.1 O Fornecimento de Serviço e o Consentimento para Tratamento de Dados.

Sabe-se que o modelo de negócios adotado por várias empresas de internet, principalmente o das ferramentas conhecidas como redes sociais (SNS – *Social Networking Site*), prevê a gratuidade dos serviços tendo como contrapartida a veiculação de publicidade direcionada ao perfil do usuário. Em tais situações o usuário se vê obrigado a concordar com a captura e tratamento de seus dados pessoais sob pena de exclusão digital. Equivale dizer que o consentimento para a captura e tratamento dos dados pessoais é condição indispensável para a disponibilização dos serviços.

O PL 5.276/2016 em seu art. 8º, §4º dispõe que "quando o consentimento para o tratamento de dados pessoais for condição para o

---

[157] BRASIL. PL 5276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 11.nov.2017.

[158] Tramitam em conjunto os Projetos de Lei do Senado nºs 330 de 2013; e 131 e 181 de 2014.

[159] BRASIL. PL 4060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 12.nov.2017.

fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre tal fato e sobre os meios pelos quais poderá exercer controle sobre o tratamento de seus dados".

Observa-se, neste dispositivo, a exigência de fornecimento de informação destacada sobre as formas de exercício da autodeterminação informativa, ou seja, o indivíduo que consente em conceder seus dados pessoais e disponibilizá-los para tratamento – pois este consentimento é condição para a utilização daquela rede social – tem o direito de ser informado com destaque sobre a captura e tratamento dos seus dados bem como sobre as maneiras de controlá-los.

6.3.1.2 O Consentimento para Finalidades Específicas

Dispõe o artigo 9º, §4º do PL 5.276/2016 que "o consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais." O texto do projeto de lei aponta para a necessidade de obtenção de nova autorização por parte do usuário caso a empresa altere a finalidade original para a qual os dados foram coletados.[160]

Esta disposição é de difícil implementação prática pois os analistas de dados, tendo em mãos grande massa de dados, concebem diuturnamente a possibilidade de novas análises e novos algoritmos para finalidades diversas. A obrigação de obter o consentimento do sujeito relacionado aos dados para cada finalidade nova inviabilizaria a dinâmica do tratamento de dados.

6.3.1.3 Dados de Perfil Comportamental

No que concerne ao *online profiling*, o projeto de lei do Executivo, o mais completo em tramitação, se orienta no sentido de considerar como "dados pessoais" e, portanto, merecedor da proteção legal, os dados utilizados para a

---

[160] O artigo 8º, I do PL dispõe que "O titular deverá ter acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva sobre, entre outros: I - finalidade específica do tratamento". Na mesma linha o artigo 9º, §6º dispõe que "Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 8º, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações."

composição do perfil comportamental de uma pessoa natural. Destaque-se, neste sentido, a inexigibilidade de que o sujeito relacionado aos dados seja identificado.

No parágrafo único de seu artigo 13 o Projeto de Lei nº 5.276/2016 estabelece que “poderão ser igualmente considerados como dados pessoais, para fins desta Lei, dados utilizados para a formação de perfil comportamental de uma determinada pessoa natural, ainda que não identificada.”

Este dispositivo justifica-se pelo fato dos dados de comportamento *online* não estarem, geralmente, vinculados a uma pessoa natural, mas sim associados a uma conexão, a qual é identificada pelo endereço de protocolo de internet (*IP Address*). É evidente que se os dados de comportamento *online* capturados pelas empresas de internet estiverem associados a uma pessoa identificada, tais dados serão considerados dados pessoais. A inovação do projeto de lei reside justamente na inexigibilidade da identificação dos dados com o sujeito.

A cautela do legislador em atribuir a proteção aos dados de pessoa não identificada é justificável, pois ainda que o sujeito relacionado aos dados não seja identificado no momento inicial da coleta de dados é possível sua identificação num momento posterior. Merece destaque a inclusão de dispositivo que considera o endereço de conexão (*IP Address*) como dado pessoal.[161]

[161] O art. 5°, I do PL 5.276 considera como dados pessoal os “números identificativos, dados locacionais ou identificadores eletrônicos”.

7 O Modelo da Matriz de Risco

OMER TENE e JULES POLONETSKY, num simpósio realizado em 2012 na Stanford Law School, criticaram os modelos geralmente adotados para a proteção de dados pessoais, em especial o novo Regulamento (GDPR) proposto em janeiro daquele ano pela Comissão Europeia a fim de substituir a Diretiva de 1995. No entendimento destes especialistas, o endurecimento das políticas de proteção de dados pessoais poderia resultar na diminuição de resultados socialmente proveitosos e inibição da inovação. Estes pesquisadores citam exemplos de situações nas quais resultados socialmente proveitosos decorrem do processamento e análise de dados pessoais (Vioxx e Google Flu Trends). Nos casos exemplificados o processamento não implica na criação de dados pessoais derivados de *profiling*, mas de estatísticas onde a identidade dos sujeitos relacionados aos dados é absolutamente irrelevante.

Em face de tais situações sugiram um modelo de proteção baseado numa matriz de risco[162]. Nesta matriz deveriam ser ponderados o valor social gerado pelo processamento dos dados pessoais e os riscos potenciais da autonomia e privacidade de cada indivíduo. Em favor desta tese argumentam que os usuários, no momento do consentimento, não têm a devida compreensão do valor social que seus dados poderiam representar. Desta forma, entendem que a autorização para a utilização dos seus dados pessoais só deveria ser solicitada em contextos tais como o de *profiling*, de direcionamento de propaganda específica, de serviços de geo-localização e de *data broker* terceirizado[163].

De fato, não se pode ignorar o proveito social decorrente de estudos científicos que se baseiam nesta gigantesca massa de dados. Desta forma, a grande questão que se impõe está relacionada com a ponderação entre a proteção

---

[162] TENE, Omer; POLONETSKY, Jules. Privacy in the age of big data: a time for big decisions, Stanford Law Review Online 64, 2012. Disponível em: <http://www.stanfordlawreview.org/online/privacy-paradox/big-data> Acesso em: 02.dez.2017. p. 67.

[163] Ibidem, p. 68.

da privacidade dos indivíduos e o benefício social derivado do tratamento de dados pessoais.

Mecanismos jurídicos que imponham maiores restrições na captura e uso dos dados pessoais podem assegurar maior privacidade mas, ao mesmo tempo, podem inviabilizar benefícios sociais advindos do tratamento adequado destes dados.

Considere-se também que o modelo de matriz de risco de Tene e Polonetsky, assim como o já mencionado PCAST Report, preocupa-se especialmente com as finalidades do tratamento, a utilização dos dados derivados deste tratamento e a relação entre benefícios sociais *versus* riscos para os sujeitos relacionados aos dados. Fica, portanto, em segundo plano a proteção contra a captura de dados. Observa-se que o desenvolvimento tecnológico ocorreu de forma tão célere e irreversível que o cenário para os que desejam limitar a captura de dados pessoais é bastante desanimador, restando apenas, como objeto das atenções e da proteção jurídica, as ações finais do que convencionou-se chamar de online profiling.

8 CONCLUSÃO

A evolução tecnológica municiou a sociedade com ferramentas que permitem a captura, armazenamento e transmissão de dados de forma mais rápida e em maior quantidade. Se por um lado o rápido progresso da tecnologia digital trouxe facilidade e conectividade, por outro lado colocou em posição de extrema vulnerabilidade determinados direitos do indivíduo.

O direito à privacidade, neste contexto, ganhou nova dimensão: o direito à proteção dos dados pessoais. Diversas normas foram elaboradas na tentativa de proteger os indivíduos da atividade de entidades públicas e privadas que capturam, armazenam, utilizam e compartilham dados pessoais. No entanto, na medida em que se observa um passo adiante na evolução tecnológica, o anacronismo das normas em vigor fica evidente.

A possibilidade de rastreamento do comportamento online aliado à grande capacidade de armazenamento e de processamento de dados (Big Data) permite às empresas de internet a elaboração de perfis dos usuários que refletem, de forma cada vez mais precisa, aspectos de sua personalidade, inclusive os aspectos mais íntimos.

O novo cenário coloca em cheque as premissas e conceitos tidos como verdadeiros pelos legisladores que elaboraram as normas de proteção de dados pessoais. Os conceitos de dados pessoais como aqueles que estão relacionados a um indivíduo identificado ou identificável pode estar superado diante da primazia da identificação da conexão. A premissa da anonimização e do consentimento informado também não estão livres das críticas.

O cenário é preocupante, na medida em que a utilização dos perfis gerados pelas empresas de internet pode transcender a mera veiculação de propaganda adequada ao perfil e invadir dimensões que afetem a esfera jurídica do sujeito relacionado aos dados. A discriminação decorrente de decisão exclusivamente automatizada é um exemplo dos resultados da má utilização dos perfis gerados na análise de dados pessoais.

A solução para a prevenção de danos aos indivíduos não deve estar limitada a um conteúdo meramente normativo. A auto-regulação setorial, a

instituição de um órgão de controle e fiscalização bem como a conscientização dos usuários de internet são parte do framework protetivo.

9 ANEXO I: EXEMPLOS DE DESANONIMIZAÇÃO

Diversas normas de proteção de dados pessoais são elaboradas sob a premissa de que se um conjunto de dados for anonimizado, então a este conjunto podem ser aplicadas regras menos rigorosas diante da suposta impossibilidade de identificação do sujeito relacionado aos dados.

Este anexo apresenta alguns casos que se tornaram públicos de conjuntos de dados originalmente anônimos que, após disponibilizados ao público, sofreram um processo de desanonimização causando não apenas constrangimento para as empresas que fizeram a publicação bem como o enfraquecimento da premissa exposta no parágrafo anterior.

9.1 Pesquisas do Motor de Buscas da America Online (AOL)

Em agosto de 2006 a America Online, pretendendo estabelecer uma comunidade de pesquisa aberta, divulgou na internet uma lista de 20.000.000 (vinte milhões) de pesquisas feitas no seu motor de busca por 657.000 (seiscentos e cinquenta e sete mil) usuários nos três meses anteriores.

Evidentemente os dados foram alterados pela AOL antes da divulgação apenas para ocultar o nome e o IP (*Internet Protocol Address*) dos usuários que fizeram as pesquisas. Em substituição aos dados que permitiriam uma identificação imediata do usuário, a empresa atribuiu um código numérico sequencial para cada usuário de modo que os pesquisadores que fossem analisar os dados pudessem agrupar todas as pesquisas feitas por um determinado usuário.

Não tardou para que uma série de publicações surgissem com fatos curiosos sobre os indivíduos por trás das pesquisas. Foram encontradas as seguintes pesquisas realizadas pelo usuário ao qual foi atribuído o código 17556639: “Como matar sua esposa”, “Fotos de pessoas mortas”, “Imagens de acidentes de carro”.

Um caso que demonstrou a fragilidade da anonimização foi o do usuário 4417749. Dentre as pesquisas deste usuário estavam as seguintes: “paisagistas em Lilburn, GA”, “casas vendidas em shadow lake subdivision gwinnett county georgia”, várias pesquisas com nomes de pessoas com sobrenome Arnold e “cachorros que fazem xixi em tudo”. Não foi necessário muito tempo para que a

identidade deste usuário fosse revelada. Tratava-se de Thelma Arnold, uma viúva de 62 anos que vivia em Lilburn, Georgia. Ao ser entrevistada por um repórter a Sra. Arnold admitiu que as pesquisas elencadas sob o código 4417749 eram realmente dela.[164]

Diante do evidente fracasso na anonimização a AOL removeu os dados, desculpou-se com a comunidade e foi processada numa *class action* onde pleiteou-se 5 mil dólares para cada usuário que teve seus dados divulgados. A falha por excesso de confiança na anonimização também custou o cargo do CTO (Chief Technology Officer) da AOL que renunciou duas semanas após a divulgação.[165]

9.2 Massachusetts Group Insurance Commission (GIC)

Em meados da década de 90, a agência governamental GCI de Massachusetts, objetivando apoiar pesquisas em benefício da sociedade, divulgou uma lista de registros médicos de pacientes que visitaram os hospitais estaduais com informações sobre diagnósticos e prescrições. Antes da divulgação, no entanto, os dados que permitiriam a identificação dos pacientes foram removidos (nome, *social security code*, endereço e outros). No entanto, aproximadamente uma centena de atributos foram mantidos.

LATANYA SWEENEY, que na época cursava seu PhD no MIT, conseguiu demonstrar que, apesar da tentativa de anonimização por supressão de identificadores, outros atributos poderiam ser utilizados para identificar os pacientes. Com apenas U$ 20,00, Latanya adquiriu um CD com uma base de dados dos eleitores de Cambridge onde constavam nome, data de nascimento, CEP e sexo. Ao correlacionar estas informações com a base de dados do GCI, Latanya conseguiu identificar os dados médicos do governador de Massachusetts, William

---

[164] The New York Times Website. A Face Is Exposed for AOL Searcher No. 4417749. Disponível em: <http://query.nytimes.com/gst/abstract.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63>

[165] The New York Times Website. AOL executive quits after posting of search data - Technology - International Herald Tribune. Disponível em: <http://www.nytimes.com/2006/08/22/technology/22iht-aol.2558731.html>

Weld, incluindo diagnósticos e prescrições médicas. A pesquisadora fez questão de enviar ao governador as informações relacionadas a ele que foram reidentificadas.

Posteriormente LATANYA SWEENEY, após o processamento do censo de 1990, chegou à conclusão de que 87% das pessoas pode ser identificada apenas utilizando-se do trio de informações CEP, data de nascimento e sexo.[166]

Sob a coordenação de Latanya Sweeney, o Data Privacy Lab de Harvard disponibilizou um website (http://aboutmyinfo.org/) onde é possível verificar quão facilmente um morador dos Estados Unidos poderá ser reidentificado em função do trio CEP, data de nascimento e sexo.

9.3 Caso Netflix

O Prêmio Netflix (Netflix Prize) foi uma competição patrocinada pela Netflix, empresa de entretenimento e vídeo sob demanda. A proposta da competição era o desenvolvimento de algoritmo que, baseado em dados de avaliação de usuários sobre filmes e sua correlação, pudesse prever qual seria a avaliação destes usuários em relação a outros filmes. O objetivo do algoritmo seria, portanto, permitir que a empresa sugerisse os melhores filmes para seus usuários.

Para fins de desenvolvimento do algoritmo, a Netflix disponibilizou publicamente uma base de dados de 100 milhões de avaliações de filmes feitas por 500 mil usuários. Antes de sua publicação, a base de dados foi anonimizada, ou seja, foram removidos todos os dados que pudessem identificar o usuário, permanecendo apenas um identificador numérico para cada usuário a fim de relacionar a avaliação de todos os filmes assistidos por este usuário agora anônimo.

Dois pesquisadores da Universidade do Texas (Austin)[167] foram capazes de reidentificar vários usuários por meio de correlação com as avaliações destes mesmos usuários publicadas em outra base de dados de filmes, o IMDb (Internet

---

[166] SWEENEY, Latanya. k-Anonymity: a model for protecting privacy. Maio, 2002. Disponível em: <https://epic.org/privacy/reidentification/Sweeney_Article.pdf>. Acesso em: 07.dez.2017. p. 2.

[167] NARAYANAN, Arvind; SHMATIKOV, Shmatikov. How to break anonymity of the netflix prize dataset. 2006. Disponível em: <https://arxiv.org/abs/cs/0610105>. Acesso em: 05.jun.2017.

Movie Database). Esta reidentificação foi possível em razão da correlação de dados tais como datas das avaliações e filmes que não estão entre os mais assistidos.

Este episódio demonstrou a fragilidade do conceito de que uma vez anonimizados os dados estão protegidos. Também demonstrou a possibilidade de produção de dados derivados sensíveis por meio de dedução ou inferência. Neste sentido, observa-se, ao final do relatório destes pesquisadores que eles puderam deduzir aspectos sensíveis da personalidade dos indivíduos reidentificados em face das avaliações atribuídas a determinados títulos:

> *First, we can immediately find his political orientation based on his strong opinions about "Power and Terror: Noam Chomsky in Our Times" and "Fahrenheit 9/11." Strong guesses about his religious views can be made based on his ratings on "Jesus of Nazareth" and "The Gospel of John". He did not like "Super Size Me" at all; perhaps this implies something about his physical size? Both items that we found with predominantly gay themes, "Bent" and "Queer as folk" were rated one star out of five. He is a cultish follower of "Mystery Science Theater 3000". This is far from all we found about this one person, but having made our point, we will spare the reader further lurid details.*[168]

Em razão deste episódio uma ação judicial foi proposta em 2009 contra a Netflix baseada no VPPA, Video Privacy Protection Act de 1988, lei que proíbe a divulgação de dados de locação ou aquisição de vídeos. A partir de então a Netflix cancelou as edições seguintes do Netflix Prize.

---

[168] Ibidem, p. 16

10 REFERÊNCIAS BIBLIOGRÁFICAS

10.1 LIVROS E MONOGRAFIAS

BITTAR, Carlos Alberto. *Os direitos da personalidade*. 8ª ed., São Paulo: Saraiva, 2015.

CUPIS, Adriano de. *Os direitos da personalidade.* Tradução de Afonso Celso Furtado Rezende. 2ª ed., São Paulo: Quorum, 2008.

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

LEONARDI, Marcel. *Tutela e privacidade na internet.* São Paulo: Saraiva, 2012.

LIMA, Cíntia Rosa Pereira de. *A imprescindibilidade de uma entidade de garantia para a efetiva proteção dos dados pessoais no cenário futuro do Brasil.* 487 p. Tese de Livre Docência. Faculdade de Direito Ribeirão Preto/USP. 2015.

MARTINS, Ives Gandra da Silva; PEREIRA JÚNIOR, Antônio Jorge (Coord.). *Direito à privacidade.* Aparecida, SP: Ideias & Letras; São Paulo: Centro de Extensão Universitária, 2005.

REALE, Miguel. *Lições preliminares de direito.* 25ª ed. São Paulo: Saraiva. 2001.

RODOTÀ, STEFANO. *A vida na sociedade da vigilância: a privacidade hoje.* Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda.. Rio de Janeiro: Renovar, 2008.

ROOSENDAAL, Arnold. *We Are All Connected to Facebook . . . by Facebook!* in: S. Gutwirth et al. (eds.), European Data Protection: In Good Health?, Heidelberg: Springer, 2012, pp. 3-19.

10.2 ARTIGOS E PARECERES

ALTAWEEL, Ibrahim; GOOD, Nathan; HOOFNAGLE, Chris Jay. Privacy on Adult Websites. Workshop on Technology and Consumer Protection (ConPro ’17), co-located with the 38th IEEE Symposium on Security and Privacy, San Jose, CA (2017). Disponível em: <https://ssrn.com/abstract=2851997>. Acesso em: 11.abr.2017.

BORGESIUS, Frederik Zuiderveen. *Behavioral targeting: A european legal perspective*, IEEE Security & Privacy, vol.11, no. 1, pp. 82-85, Jan.-Feb. 2013, Disponível em: <http://ssrn.com/abstract=2287956> Acesso em: 02.dez.2017

CRAWFORD, Kate; SCHULTZ, Jason. *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*. Boston College Law Review, v. 55, nº 93, 2014; NYU School of Law, Public Law Research Paper nº. 13-64; NYU Law and Economics Research Paper No. 13-36. Disponível em: <http://ssrn.com/abstract=2325784> Acesso em: 02.dez.2017.

FAIRFIELD, Joshua A.T. *Do-Not-Track as Default*. Northwestern Journal of Technology and Intellectual Property, Vol. 11, No. 7, 2013. Disponível em: <http://ssrn.com/abstract=2338028>. Acesso em: 01.nov.2017.

FEDERAL TRADE COMMISSION. *Data brokers: a call for transparency and accountability*. Maio 2014. Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em: 25.abr.2017

HEEGER, Eva. *Controlling Your Online Profile: Reality or an Illusion?* A Research into Informed Consent as a Mechanism to Regulate Commercial Profiling. 2005. Disponível em: <http://ssrn.com/abstract=2658651>. Acesso em: 12.dez.2017.

LEONARDI, Marcel. *Dados pessoais, regulação e a economia digital.* Jornal da Tarde. 28.03.2011. p. 2. Disponível em: <http://leonardi.adv.br/2011/03/dados-pessoais-regulacao-e-a-economia-digital/>. Acesso em: 05.dez.2017.

LIMA, Cíntia Rosa Pereira de. O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos. *In: Direito e novas tecnologias I [Recurso eletrônico online]* CONPEDI/UFPB (org.) ROVER, Aires José; CELLA, José Renato Graziero; AYUDA, Fernando Galindo. Florianópolis: CONPEDI, 2014. pp. 343-365. Disponível em: <http://publicadireito.com.br/artigos/?cod=981322808aba8a03>. Acesso em: 02.dez.2017.

LIMA, Cíntia Rosa Pereira de. Parecer Técnico encaminhado pela Professora Livre Docente de Direito Civil da Faculdade de Direito de Ribeirão Preto/USP, Dra. Cíntia Rosa Pereira de Lima à Comissão Especial da Câmara dos Deputados que proferirá parecer sobre o Projeto de Lei n. 4.060, de 2012, do Deputado Milton Monti, que dispõe sobre o Tratamento de Dados Pessoais. Ribeirão Preto: 2017. Disponível em: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/dra-cintia-rosa-pereira-de-lima-usp>. Acesso em: 05.dez.2017.

MACCLURG, Andrew J., *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*. Northwestern University Law Review, v. 98. p. 63-133, 2003. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628724> Acesso em: 02.dez.2017

MAYER, Jonathan R.; MITCHELL, John C. *Third-Party Web Tracking: Policy and Technology, Proceedings of the 2012 IEEE Symposium on Security and Privacy*, p.413-427, May 20-25, 2012. Disponível em: <https://jonathanmayer.org/papers_data/trackingsurvey12.pdf>. Acesso em: 07.dez.2017.

MITCHELL, I. D. *Third-Party Tracking Cookies and Data Privacy*. abr. 2012. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2058326>. Acesso em: 11.dez.2017.

NARAYANAN, Arvind; SHMATIKOV, Shmatikov. *How to break anonymity of the netflix prize dataset.* 2006. Disponível em: <https://arxiv.org/abs/cs/0610105>. Acesso em: 05.dez.2017.

OHM, Paul. *Broken promises of privacy: responding to the surprising failure of anonymization.* UCLA Law Review, Vol. 57, p. 1701-1777, 2010. Disponível em <http://www.uclalawreview.org/broken-promises-of-privacy-responding-to-the-surprising-failure-of-anonymization-2>. Acesso em: 12.dez.2017

PROSSER, William L. *Privacy.* California Law Review. Volume 48. Issue 3. 1960. p. 383-423 Disponível em: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview>. Acesso em: 12.dez.2017.

REINALDO FILHO, Demócrito. *A Diretiva Europeia sobre proteção de dados pessoais.* Revista Jus Navigandi, Teresina, ano 18, n. 3507, 6 fev. 2013. Disponível em: <https://jus.com.br/artigos/23669>. Acesso em: 07.dez.2017.

SHAH, Rajiv C.;KESAN, Jay P. *Recipes for cookies: How institutions shape communication technologies*. Illinois Public Law and Legal Theory Research Papers Series No. 01-14. pp. 315-336. Disponível em: <https://experts.illinois.edu/en/publications/recipes-for-cookies-how-institutions-shape-communication-technolo>. Acesso em: 05.dez.2017

SKOUMA, Georgia; LÉONARD, Laura. *On-line behavioral tracking: What may change after the legal reform on personal data protection*. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (Eds). Reforming european data protection law. Springer, 2015. pp. 35-60.

SOLOVE, Daniel J.. *Conceptualizing Privacy*. California Law Review, v. 90, p. 1087, julho/2002. Disponível em: <http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2/>. Acesso em: 02.dez.2017

SWEENEY, Latanya. *k-Anonymity: a model for protecting privacy*. Maio, 2002. Disponível em: <https://epic.org/privacy/reidentification/Sweeney_Article.pdf>. Acesso em: 07.dez.2017

SWIRE, Peter. *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*. 1997. Disponível em: <https://ssrn.com/abstract=11472>. Acesso em: 25.nov.2017.

TENE, Omer; POLONETSKY, Jules. *Privacy in the age of big data: a time for big decisions*, Stanford Law Review Online 64. p. 63-69, 2012. Disponível em: <http://www.stanfordlawreview.org/online/privacy-paradox/big-data> Acesso em: 02.dez.2017

WARREN, Samuel D.; BRANDEIS, Louis D.. *The Right to Privacy*. 4 HARV.L.REV. 193 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>. Acesso em: 01.dez.2017

WORLD ECONOMIC FORUM. *Personal Data: The Emergence of a New Asset Class*. Cologny/Geneva, Switzerland, 2011. Disponível em: <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>. Acesso em: 11.dez.2017.

10.3 RELATÓRIOS

ALTAWEEL, Ibrahim; GOOD, Nathan; HOOFNAGLE, Chris Jay. *Web Privacy Census* (December 15, 2015). Technology Science. 2015121502, Online. Disponível em: <https://ssrn.com/abstract=2703814>. Acesso em: 04.dez.2017.

FTC – Federal Trade Commission. *Protecting consumer privacy in an era of rapid change*. 2012. Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-

era-rapid-change-recommendations/120326privacyreport.pdf>. Acesso em: 14.nov.2017.

FTC – Federal Trade Commission. *Self-regulation and privacy online: a report to congress.* 1999. Disponível em: <https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf>. Acesso em: 14.nov.2017.

PCAST - President's Council of Advisors on Science and Technology. *Big data and privacy: A technological perspective*. 2014. Disponível em: <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf>. Acesso em: 05.dez.2016.[169]

PURCELL, Kristen; BRENNER, Joanna; RAINIE, Lee. Search Engine Use 2012. Disponível em: <http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf>. Acesso em: 01.dez.2017.

10.4 LEGISLAÇÃO

BRASIL. PLS 131/2014. Dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiros a organismos estrangeiros. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/116969>. Acesso em: 11.dez.2017.

BRASIL. PLS 181/2014. Estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/117736>. Acesso em: 11.dez.2017.

BRASIL. PLS 330/2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em:

[169] O site que hospedava o referido relatório (obamawhitehouse.archives.gov) foi removido em meados de 2017. A íntegra do documento pode ser acessada no seguinte link: http://www.nicotra.com.br/wp-content/uploads/pdf/pcast_big_data_and_privacy_-_may_2014.pdf

<https://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 11.dez.2017.

BRASIL. PL 4060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 12.dez.2017.

BRASIL. PL 5276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 11.dez.2017.

EUROPEAN PARLIAMENT AND COUNCIL. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). 12.jul.2002. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML> Acesso em: 02.dez.2017

EUROPEAN PARLIAMENT AND COUNCIL. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data protection directive). 24.out.1995. Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046> Acesso em: 02.dez.2017

EUROPEAN PARLIAMENT AND COUNCIL. Regulation 2016/679 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). 27.abr.2016. Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679> Acesso em: 02.dez.2017

10.5 WEBSITES

COMISSÃO EUROPEIA. Página de Proteção de Dados Pessoais. Disponível em: <http://ec.europa.eu/justice/data-protection/index_en.htm>. Acesso em: 07.dez.2017.

FACEBOOK. Termos e Políticas do Facebook. Disponível em: <https://www.facebook.com/policies/>. Acesso em: 11.dez.2017.

FACEBOOK. Cookies e outras tecnologias de armazenamento. Disponível em: <https://www.facebook.com/policies/cookies/>. Acesso em: 12.dez.2017.

FEDERAL TRADE COMMISSION. Do Not Track. Disponível em: <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track>. Acesso em: 03.dez.2017.

GOOGLE. Política e Termos. Disponível em: <https:// www.google.com.br/intl/pt-BR/policies/privacy/>. Acesso em: 28.nov.2017.

GOOGLE. Ajuda do Google Chrome. Limpar, ativar e gerenciar cookies no Chrome. Disponível em: <https://support.google.com/chrome/answer/95647>. Acesso em: 12.dez.2017.

PC WORLD. NHS Link to Facebook Raises Privacy Concerns. Disponível em: <http://www.pcworld.com/article/211711/article.html>. Acesso em: 27.nov.2017.

THE WALL STREET JOURNAL. On Orbitz, Mac Users Steered to Pricier Hotels. Disponível em: <http://www.wsj.com/articles/SB10001424052702304458604577488822667325882>. Acesso em: 02.dez.2017.

UOL ECONOMIA. Google e Facebook coletam mais dados que EUA, diz fundador do Wikileaks. Disponível em: <http://economia.uol.com.br/noticias/efe/2016/07/12/google-e-facebook-coletam-mais-dados-que-eua-diz-fundador-do-wikileaks.htm>. Acesso em: 13.dez.2017.