

Se você sabe quem eu sou, eu quero saber quem você é

Alexandre Pacheco da Silva

Mestre em Direito e Desenvolvimento pela Fundação Getúlio Vargas - FGV. Professor de Direito e Comércio Internacional do curso de graduação em Direito da Universidade Ibirapuera - UNIB, São Paulo, SP - Brasil. Membro do Grupo de Pesquisas em Direito e Inovação (GPDI) e do Núcleo de Metodologia de Ensino da Direito da Fundação Getúlio Vargas - FGV. São Paulo, SP - Brasil. E-mail: alexandre@pachecodasilva.com.br

Resumo

A associação entre tecnologias de rastreamento de dados pessoais de usuários na internet com o mercado da publicidade on-line tem ampliado o conjunto de preocupações com a proteção de dados pessoais na internet nos dias atuais. O debate sobre como garantir ao usuário um acesso eficaz a informações sobre a coleta, análise e destinação de seus dados, bem como assegurar que ele tenha instrumentos de gestão e bloqueio dessa coleta tem ganhado relevância. Este trabalho busca apresentar como empresas que atuam no ciclo da coleta, análise e destinação de dados pessoais de usuários de internet empregam duas tecnologias de rastreamento (cookie e deep packet inspection) e como esses dados são utilizados pelo mercado da publicidade on-line comportamental, intensificando o processo de personalização de serviços na internet. Aponta para as insuficiências e contradições do modelo regulatório da autogestão da privacidade, reforçando a necessidade de desenvolvimento de ferramentas gráficas de auxílio ao usuário na gestão de seus dados pessoais.

Palavras-chave

Privacidade. Tecnologias de rastreamento. Dados pessoais. Cookie, deep packet inspection. Publicidade on-line. Publicidade comportamental. Personalização. Provedores de conexão. Provedores de conteúdo e coleta de dados.

If you know who I am, I want to know who you are

Abstract

The association between personal data tracking for internet users with the Market of on-line advertising has broadened the scope of the concerns regarding on-line personal data protection nowadays. The debate on how to ensure the adequate information regarding the collection, analysis and destination of personal data is gaining greater importance, as well as how to ensure that user may have proper tools for managing and preventing the collection. The objective of this paper is to discuss how the companies dealing with collection, analysis and destination of personal data of internet users are making use of two of the available tracking technologies (cookie and deep packet inspection) and how this data is used by the behavioral market that advertise and enhance the process of customization of internet services. Inexactness and contradictions of the regulatory model for self management and privacy are pointed out. The conclusion is that there is a need for improving the graphic tools for helping the user to manage his personal data.

Keywords

Privacy. tracking Technologies. Personal data. Cookie. deep packet inspection. Online advertising. Behavioral advertising. Customization. Internet service providers. Content providers. Data collection.

UM PONTO DE PARTIDA: “NÓS SABEMOS QUEM VOCÊ É”

Matt é estudante, estadunidense, mora com seus pais e é usuário do Facebook. Recentemente, foi surpreendido com a recomendação da notícia assinada pelo terapeuta sexual Rick Clemons em seu *feed* (painel personalizado de notícias), com o seguinte título: “*Quer sair do armário? Precisa de ajuda?*”¹.

Matt era de fato homossexual, mas ficou surpreso com a recomendação, uma vez que ainda não havia assumido sua preferência sexual perante seus familiares e seus amigos. Curioso, decidiu investigar quais informações a rede social dispunha a seu respeito.

Ele suspeitou que a rede social coletasse e analisasse as informações presentes no seu mural de notícias e comentários de amigos. Contudo, aos olhos de Matt, nenhuma das informações presentes em seu mural, nos *links* que “curtiu” e compartilhou com seus amigos, indicaria ao Facebook sua preferência sexual. Em nenhum momento acessou *sites* com conteúdo que sugerisse sua preferência, bem como não revelou de maneira explícita essa informação para nenhum de seus amigos. Então, como a rede social descobriu?

Enquanto Matt investigava como as informações de seu perfil no Facebook poderiam indicar sua preferência sexual, a rede social enxerga Matt como um agregado de informações capazes de serem comparadas com as informações de outros usuários. A partir de uma análise estatística que compara sua idade, seu endereço, seus hábitos e comportamentos na internet em relação a notícias e comentários e seu histórico de navegação com o de outros usuários, o Facebook passa a ser capaz de classificar Matt segundo suas características mais marcantes e prever quais são suas angústias e necessidades.

A rede social pode não ter absoluta certeza de que Matt é homossexual, porém, o seu perfil eletrônico sugere que existe alta probabilidade de que ele deseje conselhos para “Sair do armário”. Como?

Andrew Pole, estatístico chefe de uma das principais empresas de coleta e análise de dados nos Estados Unidos da América, a Target, costuma dizer em entrevistas que a correlação de informações que não nos parecem relevantes individualmente, quando olhadas no agregado, nos dizem muito sobre cada um de nós.²

Atualmente, a coleta e análise de informações é feita de outro modo, que coloca o usuário em uma posição de vigilância permanente, no contexto de um número crescente de empresas privadas ávidas por descobrir quais são suas preferências, suas necessidades, quanto está disposto a gastar, com quem deseja se relacionar, dentre amplo repertório de informações úteis.

A Target, por exemplo, especializou-se em coletar informações sobre um conjunto específico de usuários: pais e mães de recém-nascidos. A intenção da empresa é reunir informações de navegação de usuários por meio das tecnologias de rastreamento de que dispõe, identificando mulheres grávidas dentre os usuários para fins de veiculação de produtos e serviços associados aos cuidados com a gravidez e aos bebês recém-nascidos.

A empresa adquire informações de sites provedores de conteúdo com alto número de visitantes, tais como *sites* de compra, jornais e revistas *on-line*, *sites* de jogos, dentre outros. Cada usuário recebe um número de nove algarismos para identificá-lo e associá-lo com a informação coletada. As informações obtidas podem adquirir diferentes feições: desde informações sobre os *links* clicados pelo usuário até informações sobre sua localização física, compras que tenha realizado, dentre outras.

² Para ver mais detalhes sobre a entrevista em que o estatístico Andrew Pole descreve como empresas analisam os dados que obtêm de usuários de internet, visite: <<http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>>. Acesso: 15/08/2012.

¹ Tradução livre da frase “Coming out? Need help?”. Para preservar o sentido coloquial da expressão “Coming out”, escolhemos o equivalente em língua portuguesa “Sair do armário” como melhor tradução em relação ao sentido que a frase deseja passar. Disponível em:

Dispondo das informações coletadas, classifica informações segundo a criação de perfis e nichos de mercado específicos. No caso da Target, mulheres grávidas. A diferenciação é deste grupo-alvo do restante dos usuários é feita por meio de um conjunto de características próprias na navegação e nos hábitos de compra de mulheres grávidas que não se repetem nos demais grupos de usuários.

Por exemplo, com base nos dados coletados, foi possível perceber que, nos Estados Unidos, mulheres grávidas no início do segundo semestre de sua gestação passam a adquirir grandes quantidades de cremes hidratantes sem cheiro, pois, segundo algumas delas, neste período elas estão mais sensíveis a odores fortes. No mesmo período, mulheres grávidas passam a comprar os maiores pacotes disponíveis no mercado de bolas de algodão e de tolhas de rosto nas cores rosa, branco e azul.

Também foi percebido que, durante as 20 primeiras semanas de gravidez, as gestantes adquirem grandes quantidades de suplementos vitamínicos como cálcio, magnésio e zinco.

Com base na análise dos dados de compra coletados, nos últimos anos, a empresa foi capaz de identificar uma lista de 25 produtos que, quando comprados em conjunto, ou individualmente em certa quantidade, podem indicar que a compradora está grávida. A empresa desenvolveu um sistema de pontuação para os usuários analisados que denominou *pregnancy prediction score* (índice de probabilidade de gravidez) para identificar quando o usuário é uma mulher grávida e quando não é. Todavia, o que a empresa faz com essa informação?

A Target oferece para anunciantes de produtos e serviços destinados ao público de gestantes e de bebês recém-nascidos um conjunto de informações mais detalhadas sobre as preferências de um nicho de mercado muito específico, bem como a oportunidade de anunciar nos *sites* visitados pelas grávidas, direcionando os anúncios de produtos e serviços aos hábitos de compra e interesses dessa usuária.

Aos olhos dos anunciantes, a veiculação de suas

peças publicitárias a um público específico (mulheres grávidas) amplia a capacidade do anúncio em convencer esse público a adquirir seus produtos.

A Target e provedores de conteúdo partilham as receitas auferidas junto aos anunciantes pela disponibilização de espaços publicitários, de responsabilidade do *site*, pela informação sobre as preferências dos usuários, análises feitas pela Target, e pela veiculação de anúncios direcionados a um nicho específico de mercado, correlação feita em parceria entre a Target e o *site* que disponibiliza o espaço para anúncio.

O presente artigo tem dois objetivos. Em primeiro lugar, irá apresentar como empresas que atuam na internet coletam, analisam e empregam dados pessoais de usuários de internet em arranjos envolvendo tecnologias de rastreamento, publicidade *on-line* comportamental e a personalização de serviços na internet.

Em segundo lugar, busca discutir como a combinação de tecnologias de rastreamento de dados pessoais impõe uma agenda ampla e complexa de pesquisas sobre seus impactos sobre a privacidade de usuários na rede, com especial destaque para a gestão de dados por parte de usuários.

Por tal razão, o trabalho está dividido em três partes: inicialmente, faremos uma descrição do funcionamento das duas principais tecnologias de rastreamento de dados pessoais empregadas por empresas na internet. Em seguida, apresentaremos uma descrição sobre a associação entre essas tecnologias, seu uso na estruturação do mercado da publicidade *on-line* comportamental e seu emprego na personalização dos serviços oferecidos aos usuários na internet. Por fim, trataremos a discussão sobre quais são as propostas de instrumentos regulatórios de proteção de dados pessoais e como cada uma posiciona o usuário diante da coleta, análise e emprego de seus dados pessoais.

COLETA, ANÁLISE, CLASSIFICAÇÃO E DESCARTE DE DADOS DE USUÁRIOS DE INTERNET

“Se você não estiver pagando por algo, se você não for o consumidor, você é o produto”.

Essa máxima do mercado publicitário tem ganhado muita força com a expansão do mercado da publicidade comportamental, a qual tem como principal produto os dados pessoais de usuários de internet.

Hoje, todos os *sites*³ registram informações de seus visitantes. A coleta varia quanto ao tipo de informação obtida, quanto ao seu emprego e quanto aos terceiros com quem o *site* compartilha tais informações. Aqui, trataremos de três formas em particular: a coleta de informações para gestão das visitas em *sites*, a coleta de informações de análise do desempenho do *site* e a coleta destinada à captação de receitas para o *site*. Começamos pela gestão de visitas em *sites*.

Saber informações sobre a navegação do usuário que visita um *site* é muito valioso para seu administrador, a medida que essas informações ampliam sua capacidade de melhorar a experiência de navegação e as funcionalidades que o *site* oferece ao seu público.

Por exemplo, quando o administrador de um *site* insere um novo conteúdo (por exemplo, um comentário sobre um filme que estreou recentemente), a utilização de uma tecnologia de rastreamento como *cookie* pode ser útil para verificar o número de usuários que se interessaram pelo comentário. O administrador pode comparar o número de visitas com seu histórico de visitas e avaliar o sucesso de sua iniciativa, pode verificar qual o período de maior visitação da página, dentre diversas outras informações que podem aprimorar sua

capacidade de gestão de seu *site*. Com base nestas informações, o administrador pode investir mais esforços em iniciativas que tenham sido bem-sucedidas e avaliar as razões de parte de seu conteúdo não obter o resultado esperado.

Da mesma forma que conhecer a sua audiência é importante para o administrador de um *site*, oferecer novas funcionalidades que aprimorem a experiência de navegação dos usuários que o visitam são fundamentais para um administrador ser bem-sucedido em seu empreendimento. A relevância e a variedade dessas funcionalidades variam segundo os serviços que cada *site* oferece.

Por exemplo, ao visitar o *site* de uma livraria *on-line*, uma funcionalidade importante para o usuário é a possibilidade de identificar um livro que lhe interessou hoje, mesmo que não exista o interesse ou recursos imediatos para adquiri-lo, e ser lembrado posteriormente, pelo próprio *site*, do interesse em comprar determinado produto em nova visita dias mais tarde. Apenas tecnologias de rastreamento de dados pessoais são capazes de coletar a informação do usuário (a escolha por um livro em uma livraria *on-line*), armazenar a informação e resgatá-la no momento oportuno em que o usuário visita novamente o *site* da livraria.

A última forma de coleta de informações, a coleta para a captação de receita para o *site*, articula os elementos do modelo de negócio mais popular na web, a junção entre coleta de dados e publicidade comportamental.

Se nas duas formas anteriores a coleta de dados servia para melhorar a gestão do *site* e sua oferta de serviços, na última a coleta de dados serve como fonte de recursos para financiar a manutenção e receita do *site* (complexo de conteúdos, funcionalidades e serviços oferecidos por uma plataforma eletrônica). Para isso, vale analisarmos as duas principais tecnologias de coleta de dados pessoais e como essas tecnologias são empregadas por *sites* para gerar receitas a partir do mercado da publicidade comportamental.

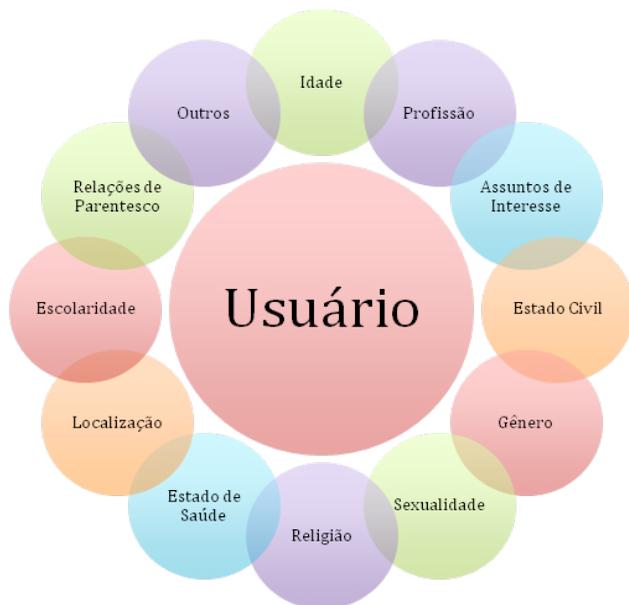
³ O termo *site* é utilizado neste artigo em uma acepção ampla, podendo representar amplo conjunto de formatos eletrônicos, a mencionar blogs, redes sociais, dentre outros. Nossa intenção aqui é oferecer uma introdução às relações entre as tecnologias de rastreamento e o mercado da publicidade on-line.

a. Tecnologias de rastreamentos de dados pessoais

Antes de analisarmos quais as principais características das tecnologias de rastreamento de dados pessoais, cabe refletir quais são os dados que compõem a navegação do usuário na web, os quais poderão ser coletados por tais tecnologias. O quadro 1 exemplifica esse complexo de dados:

QUADRO 1:⁴

Usuário como um complexo de dados



Cada uma dessas informações pode ser coletada por tecnologias de rastreamento que operam em diferentes momentos da navegação do usuário. Por exemplo, quando o usuário clica em um *link* associado a uma notícia que lhe interessou, quando ele faz um *check-in* em um restaurante por meio de um aplicativo de seu celular (e.g. Foursquare), quando acessa uma rede de internet sem fio em um restaurante ou cafeteria (e.g. Starbucks), quando aperta o botão *like* na rede social Facebook, quando insere um termo de pesquisa no buscador da empresa *Google* ou quando faz uso dos serviços de e-mail (Gmail) da mesma empresa, dentre outras ações que podem coletar as informações dos usuários.

⁴ Elaboração própria, baseada na experiência de navegação do autor do presente artigo.

Há vasto e complexo cardápio⁵ de tecnologias sendo usadas no âmbito da coleta de dados. Dentre elas duas se destacam, por sintetizarem os dois principais momentos da navegação do usuário onde ocorre a efetiva coleta de dados: a tecnologia *cookie* e a tecnologia *deep packet inspection* (DPI).

*Cookies*⁶ são pequenos arquivos de dados gravados no arquivo de texto do histórico de navegação de um usuário por um *site* que seja capaz de operar esta tecnologia. Sua função é armazenar as informações de navegação e preferências dos visitantes de um *site* (CLAYTON, 2008, p. 3).

No exemplo da livraria *on-line* mencionado anteriormente, na primeira visita do usuário ao *site*, um pequeno arquivo de texto (*cookie*) é gravado no histórico de navegação do usuário com a informação sobre o livro que demonstrou interesse em comprar, mas não comprou. Quando ele acessa novamente o *site*,

⁵ As tecnologias de rastreamento com maior notoriedade nos estudos sobre privacidade na internet são: cookie, flash cookie, evercookie, browser fingerprinting e deep packet inspection. Cada uma destas tecnologias se refere a um conjunto de características que permitem a coleta de dados de usuários, operando cada uma delas em faixas diferenciadas de navegação do usuário. Traçar as relações entre cada uma destas tecnologias com o mercado da publicidade on line mereceria por si só um estudo próprio. Para uma visão ampla sobre essas tecnologias, vale a menção do estudo: TENE, Omer; POLONETSKY, Jules. To Track or Do Not Track Advancing Transparency and Individual Control in Online Behavioral Advertising. Minnesota Voume 13, Issue 1, Winter 2012. Disponível em: <<http://cyberlaw.stanford.edu/publications/track-or-%E2%80%9Cdo-not-track%E2%80%9D-advancing-transparency-and-individual-control-online-behavioral>>. Acesso em: 18/06/2012.

⁶ Cabe aqui apresentar a definição de Leonardi, que incorpora outros aspectos técnicos sobre a tecnologia cookie: “Cookies são pequenos arquivos de texto oriundos de um web site que são gravados no disco rígido de um determinado computador e que são utilizados pelo programa navegador desse computador. Alguns cookies permanecem na memória RAM e são apagados assim que o programa navegador é encerrado, ao passo que outros são gravados no disco rígido quando do término da navegação. Os primeiros são chamados de cookies temporários, enquanto os segundos são conhecidos como cookies permanentes ou, ainda, cookies persistentes.” (Ver em: LEONARDI, 2005, p. 84).

esse arquivo pode ser lido novamente por quem o instalou, recuperando a informação em segundos para surgir novamente na tela do usuário.

Nesse sentido, a princípio, a tecnologia *cookie* rastreia informações que se reportam ao cliques feitos em um terminal (computador ou laptop) e não de um usuário específico. Isto porque o site resgata as informações registradas no arquivo gravado no navegador do usuário (e.g. Chrome, Explorer, FireFox, Safari, dentre outros).

Além disso, o âmbito da coleta não extrapola as ações do usuário fora de sua navegação. Por exemplo, *cookies* não têm a capacidade de vasculhar o conteúdo do disco rígido do usuário, ou de executar programas. Servem como arquivos de registro das ações do usuário em um *site* (LEONARDI, 2005, p. 84).

A primeira geração da tecnologia (chamados de *first-party-cookies*) é um exemplo de modelo de coleta de informação do usuário que se presta a aprimorar a gestão do administrador do *site* e das funcionalidades que oferece. *Sites* passaram a ter a capacidade traçar um perfil de seus visitantes, entender quais são suas preferências, categorizar seus hábitos e, como consequência de tudo isso, personalizar a experiência de navegação de cada um de seus visitantes, resgatando escolhas anteriores e sugerindo produtos, serviços, notícias, artigos com características semelhantes aos escolhidos pelo usuário segundo seu histórico de visitas anteriores (BERGER, 2011, p. 16).

Contudo, as informações coletadas na primeira geração não eram suficientes para induzir a construção de um modelo de negócio capaz de articular essas informações e anúncios personalizados segundo os interesses de cada usuário.

Foi a segunda geração da tecnologia (chamada de *third-party-cookies*) que permitiu o surgimento de um modelo de negócio que aproximou os administradores de *sites*, provedores de conteúdos e serviços na Web, aos anunciantes no mercado da publicidade *on-line*. Isto foi possível, pois com a segunda geração de *cookies* a leitura de informação das escolhas de usuários, que na primeira geração só poderiam ser lidas pelos próprios

sites que gravaram o arquivo de texto, na segunda geração poderiam ser lidas por *sites* que estabelecessem parcerias de negócio, incluindo novas empresas especializadas apenas na captação e análise dessas informações (TENE; POLONETSKY, 2012, p. 291).

Pelo processo chamado de "*cookie synching*", as informações captadas em um *site* poderiam ser encaminhadas a outras empresas que poderiam captar outras informações de outros *sites* e assim iniciar uma sequência ampla de coleta de dados (TENE; POLONETSKY, 2012, p. 291), permitindo a criação de perfis detalhados de usuários e a identificação de nichos de mercado muito específicos (e.g. leitores de obras literárias da autora Jane Austen com predileção por cachorros da raça *schнауzer* que residem em São Paulo há mais de dez anos).

Se a primeira geração não suscitava preocupações significativas com a profundidade e com o volume de informações coletadas, uma vez que eram utilizadas apenas para atos de navegação específicos, a segunda geração, por disseminar amplo processo de compartilhamento de dados entre diversas empresas, suscita algumas perguntas: como o usuário se informa sobre quais dados seus estão sendo coletados e como pode impedir ou restringir a coleta de suas informações pessoais?

Para impedir a coleta de informações por meio de *cookies*, basta o usuário apagar os registros do histórico de navegação de seu navegador (*browser*, e.g. Chrome, Explorer, FireFox, Safari, dentre outros). Todos os *cookies* serão apagados⁷. O comando para apagar os registros pode variar de navegador para navegador, com palavras como bloquear, apagar, eliminar *cookies*, contudo, de uma forma ou de outra estarão disponíveis ao usuário.

Não obstante a simplicidade do processo anteriormente

⁷ Os cookies comuns serão apagados. Nos últimos anos foram desenvolvidos cookies capazes de reconstruírem as informações que estavam gravadas nos cookies comuns destruídos, também chamados de evercookies ou indetectable cookies. Há também os cookies que uma vez apagados impedem que usuários aproveitem determinadas funcionalidades de programas, como o flash cookie, que impede que usuários consigam carregar programas na linguagem flash (SOLTANI, 2009, p. 1).

descrito, o que ocorre muitas vezes é a dificuldade do usuário na compreensão sobre o processo de coleta e destinação de suas informações. Como os serviços na web são oferecidos sem custos, em alguns casos, o usuário não busca se informar sobre como as empresas se remuneram para ofertar esses serviços, ou, quando buscam tal informação, tem dificuldade de compreender o funcionamento da coleta e destinação.

Idealmente, o usuário pode recorrer a dois principais documentos presentes em *sites* na web para verificar como cada empresa lida com a coleta de dados e com o compartilhamento destes com terceiros: os termos de uso do *site* e a sua política de privacidade.

Todavia, em geral, tais documentos estão muito distantes de servirem de fonte de informação para a tomada de decisão⁸ dos usuários de internet, seja por sua extensão (muito longos), seja por sua linguagem (utilizam uma terminologia técnico-jurídica em muitos casos), seja pela própria inércia dos usuários em lê-los (MCDONALD; CRANOR, 2010, p. 2).

Adicione-se à falta de clareza dos termos de uso e políticas de privacidade o compartilhamento de informações com terceiros, o que contribui negativamente na tomada de decisão do usuário sobre limitar ou não a coleta de suas informações (MCDONALD; CRANOR, 2010, p. 3).

Cabe agora a análise da outra tecnologia de coleta de dados pessoais, a *deep packet inspection*. Diferentemente do *cookie* que opera no âmbito dos navegadores (*browsers*), a DPI opera no âmbito do acesso à internet, sendo empregada pelo provedor de conexão ao qual o usuário contratou. Enquanto o *cookie* registra os dados de navegação em um

número limitado de sites, a DPI é capaz de coletar dados em todos os *sites* visitados pelo usuário sem conteúdo criptografado⁹, incluindo também aplicativos e outros programas não visualizados pela tecnologia *cookie*, como aplicativos de troca de mensagens, voz sobre IP (VoIP), compartilhamento de imagens, dentre outros (PERSON, 2010, p. 438).

A DPI inaugura a inspeção de dados na totalidade do acesso à internet do usuário. Até o desenvolvimento da tecnologia DPI, apenas parte das informações, referentes à origem e destino dos pacotes de dados, era visualizável por roteadores e servidores na internet. Dependendo do tipo de dado (texto, imagem, voz, vídeo, dentre outras), o conteúdo do pacote não poderia ser coletado. Porém, com o advento da tecnologia DPI, é possível que provedores de conexão coletem a maior parte das informações dos usuários em sua experiência *on-line* (PERSON, 2010, p. 439).

A principal vantagem da DPI para os provedores de conexão reside na capacidade de identificar

⁹ Criptografia é uma técnica de embaralhar dados de uma mensagem de modo que apenas o detentor dos códigos que permitem sua remontagem possa ser capaz de ler a mensagem. Uma das formas mais rudimentares de criptografia é a escrita ao contrário, em que, por exemplo, para que um leitor seja capaz de ler o termo “ODERGES”, ele saiba que o código da mensagem é a escrita ao contrário, permitindo que leia a palavra “SEGREDO”. Do ponto de vista da função de cada código de leitura da mensagem criptografada, existem dois tipos de criptografia, a simétrica e a assimétrica. A criptografia simétrica ou convencional funciona atrelando o mesmo código de envio de uma mensagem para o seu recebimento, ou seja, para que o destinatário seja capaz de decifrar a mensagem enviada é preciso que ele conheça o método (algoritmo) e o código utilizados para a cifragem. Este tipo de criptografia é comercialmente utilizado desde os anos de 1970 na indústria de produção de hardwares e mais recentemente em indústrias de software. É uma técnica muito segura e de baixo custo de processamento. Dentre os algoritmos simétricos mais conhecidos estão: DES (Data Encryption Standard) – chaves de 40 e 56 bits; Triple-DES – chaves de 80, 112 e 168 bits; RC2, RC3, RC4, RC5, RC6 – chaves que variam de 40 a 128 bits; e IDEA – chaves de 128 bits. Hoje, a maioria dos algoritmos modernos já opera com chaves de pelo menos 128 bits. (Ver em: MACHADO, 2010, pp. 25-38).

⁸ Em um estudo empírico conduzido em 2010 por McDonald e Cranor, nos Estados Unidos, sobre a capacidade de usuários de internet utilizarem as informações dispostas em termos de uso e políticas de privacidade para impedir a coleta de dados por meio de cookies, a pesquisa mostrou que apenas 11% dos usuários participantes entenderam a descrição de como impedir a coleta de dados feita por cookies descritas nos termos de uso e políticas de privacidade apresentadas a eles. (Ver em: MCDONALD; CRANOR, 2010, p. 10).

com maior eficiência o tráfego de programas maliciosos, tais como vírus e spam (e-mails não solicitados por usuários), uma vez que poderia visualizar o tipo e o conteúdo dos dados trafegados na rede, interceptando esses programas antes que alcançassem seus clientes (PERSON, 2010, p. 439).

Ao lado disso, a nova habilidade de vistoriar com maior eficiência os pacotes de dados oferecida pela tecnologia DPI aos provedores de conexão tornou a coleta de dados pessoais também uma oportunidade de negócio interessante para esses provedores. O detalhe interessante é que diferentemente dos *sites* que dispõem da tecnologia *cookie*, os quais coletam informações dos usuários como contrapartida ao acesso o seu conteúdo e de funcionalidades oferecidos sem custos, os provedores de conexão são contratados pelos usuários, que, além de pagar por serviços de conexão, têm seus dados coletados por esses provedores BENDRATH; MUELLER, 2011, p. 19).

Uma analogia já famosa de Lawrence Lessig (LESSIG, 2006, p. 37) sobre o tráfego de dados na internet explica as potencialidades da tecnologia DPI. Imagine que nossos dados equivalem a correspondências a serem entregues por um serviço postal. Como uma correspondência, nossos dados são colocados em um envelope que possui informações sobre o remetente e o destinatário. Até o advento da tecnologia DPI, servidores e roteadores apenas conseguiam identificar as informações de remetente e destinatário do envelope. Com a tecnologia DPI, provedores de conexão à internet passam a ter a capacidade de ler o conteúdo das correspondências de todos nós.

De um lado, inspecionar o conteúdo das correspondências representa um avanço significativo no âmbito do controle e da segurança no tráfego de dados. Contudo, a coleta de amplo conjunto de informações por parte de poucos atores (os provedores de conexão) e o seu compartilhamento com outras empresas, interessadas em utilizar tais informações para realizar negócios no mercado da publicidade

on-line, trazem preocupações importantes no campo da privacidade.

A amplitude da coleta de informações trazida pela tecnologia DPI ao lado da disseminação do compartilhamento das informações obtidas pelo processo de “*cookie syching*” intensificou a formação de bancos de dados sobre os hábitos, preferências e interesses de usuários de internet, com a criação de diversos perfis de consumo de produtos e serviços, nichos de mercado até então inexplorados por empresas (BENDRATH; MUELLER, 2011, p. 05).

Tais bancos de dados passaram a ser analisados e foram capazes de identificar comportamentos específicos de usuários durante sua navegação. Em muitos casos, observou-se que determinados usuários, ao serem apresentados a determinados anúncios, teriam maior propensão a comprar o produto ou serviço ali anunciados. A seguir trataremos da relação entre as tecnologias de rastreamento e o mercado da publicidade comportamental.

b. Organização do mercado da publicidade on-line comportamental e a personalização dos serviços na internet

Antes de definir como se organiza o mercado da publicidade comportamental, cabe uma pequena digressão para diferenciar o mercado da publicidade tradicional do mercado da publicidade *on-line* comportamental.

O mercado da publicidade em mídias tradicionais (como rádio, televisão, jornais e revistas) opera a partir de anúncios com espaço editorial limitado ou dentro de uma restrição de tempo para a veiculação de anúncios publicitários. Geralmente, televisões e rádios oferecem alguns minutos dentro de suas programações para empresas anunciarem seus produtos. Da mesma forma, mídias impressas oferecem um espaço gráfico dentro de suas publicações para que estas empresas apresentem seus produtos e serviços aos leitores de jornais e revistas.

Nesse sentido, na publicidade tradicional há uma disputa pelo espaço/tempo para veiculação de anúncios.

Outra característica importante da publicidade tradicional é a sua estratégia própria de associação

da programação de um canal de televisão/rádio ou da linha editorial de um jornal/revista com um público-alvo a ser atingido. Busca-se veicular anúncios que possam seduzir um público de espectadores e leitores a comprar produtos e serviços. Logo, há uma relação entre público-alvo e contexto em que o anúncio se insere.

Para isso, são realizadas pesquisas de opinião entre espectadores, prévias de campanhas publicitárias, grupos de controle para verificar a aceitação de produtos e serviços entre públicos heterogêneos, dentre outras iniciativas de empresas de publicidade e propaganda.

Assim, na publicidade tradicional há uma necessária correlação entre o contexto da programação/linha editorial e o público-alvo que se queira atingir, mesmo que entre leitores e espectadores possam haver perfis de consumo muito diferentes.

A publicidade *on-line* comportamental se diferencia da publicidade tradicional, pois não há uma disputa pelo espaço/tempo de veiculação de anúncios: um espaço em um *site* pode ser preenchido por um número ilimitado de anúncios, a depender de qual usuário efetivamente acesse o *site*. Além disso, a publicidade *on-line* em sua modalidade publicidade comportamental faz uso de tecnologias de rastreamento de dados pessoais,

o que permite que ela crie perfis detalhados de usuários de internet, tornando a delimitação do público-alvo de uma campanha o mais preciso possível (BEALES, 2010, p. 19).

Ademais, há uma consequência fundamental do aumento do volume de informações sobre usuários e maior precisão em seu perfil de interesses: na publicidade *on-line* comportamental é possível acompanhar a reação de cada usuário aos anúncios oferecidos. É possível rastrear e controlar quando o usuário clica em um anúncio, quando efetivamente compra o produto ou serviço anunciado ou quando o ignora por completo (BEALES, 2010, p. 20).

Logo, pode-se definir a publicidade comportamental como uma forma de direcionamento preciso de anúncios publicitários que se apropria de tecnologias de rastreamento de dados para a coleta e análise de dados de usuários de internet, criando perfis com essas informações para associá-las ao conteúdo de anúncios publicitários (MCDONALD; CRANOR, 2010, p. 2).

Cookies de segunda geração e DPI são apenas duas das diversas tecnologias de rastreamento utilizados pelos agentes que atuam no mercado da publicidade online comportamental. De modo amplo, podemos categorizá-los da seguinte maneira (tabela1):

TABELA 1

Organização do Mercado de Publicidade Comportamental

	EDITOR	AUDIÊNCIA	REDE DE ANUNCIANTES	ANUNCIANTES
Descrição	<i>Sites</i> produtores de conteúdo, desenvolvedores de aplicativos, plataformas de busca, entre outros serviços.	Usuários de internet que visitam os <i>sites</i> dos editores.	Realizam a coleta e análise de dados de usuários de internet.	Produtores de anúncios.
Função no mercado da publicidade on-line	Produtores de conteúdo e serviços na internet.	São os destinatários finais dos anúncio.	São os intermediários, cujo objetivo é aproximar editores de anunciantes por meio da delimitação de perfis de usuários (hábitos, interesses e preferências) e nichos de mercado.	Buscam adquirir espaços publicitários para anunciar seus produtos e serviços.
Vantagem obtida no mercado	São pagos por anunciantes pela disponibilização de espaços publicitários em seus <i>sites</i> . Podem receber pelo clique no anúncio ou uma comissão pela venda dos produtos e serviços anunciados.	Beneficiam-se do conteúdo e dos serviços produzidos pelos editores sem custos. Fornecem seus dados para os <i>sites</i> que visitaram, que os compartilham com as redes de anunciantes.	Como intermediários, recebem comissão dos anunciantes por aproximar editores de anunciantes.	Anunciar seus produtos e serviços para uma audiência propensa a adquirir esses produtos e serviços em razão de seus interesses, hábitos e preferências.

Na disposição das funções entre os principais atores no mercado da publicidade *on-line* comportamental, destaca-se a rede de anunciantes (que apareceu na introdução deste artigo na figura da empresa Target). Porém, a figura da rede de anunciantes pode se revestir de diversas formas, como nos serviços *AdSense* e Double Click da empresa Google, ou nas redes *Rakuten*, *Linkshare* e *Amazonassociates*, cada qual com formatos particulares de articular tecnologias de rastreamento com a oferta de espaços publicitários para a veiculação de anúncios baseados no comportamento dos usuários.

Vale mencionar que, ao lado da combinação de tecnologias de rastreamento e direcionamento de anúncios publicitários, cresce hoje o fenômeno da personalização da navegação dos usuários da internet, que pode ser descrito como a sugestão ou a pré-seleção de conteúdos por parte dos editores com base no histórico de navegação do usuário. A iniciativa busca prever que conteúdos os usuários estão interessados em consumir, com base nas escolhas anteriores que fizeram (PARISER, 2012,).

Além de recolher anúncios baseados em nossos perfis de navegação, receberemos conteúdos,

sugestões de notícias, aplicativos, serviços, dentre outros itens baseados em nossa navegação. A respeito desse fenômeno, Eli Pariser descreve um experimento que realizou. O autor, como a maioria de nós, acreditava que o sistema de buscas oferecido pela empresa Google opera a partir de um sistema padrão de classificação de resultados de pesquisa com base nos termos de busca que inserirmos. Ou seja, quando duas pessoas diferentes inserem a palavra “British Petroleum” ou BP, os resultados de pesquisa seriam iguais para as duas pessoas. Contudo, para a surpresa do autor, não são (PARISER, 2012,).

A partir de 2009 e com mais intensidade em 2010, o autor convidou dois de seus amigos para pesquisar na plataforma de buscas do Google o termo “BP”. Ambos possuíam formação no ensino superior dos Estados Unidos da América e moravam em bairros próximos um do outro, compartilhando posições políticas parecidas (centro-esquerda). Os resultados das pesquisas para um deles foram *sites* com informação de investimento em ações da empresa BP. O outro amigo obteve como resultados notícias sobre acidentes envolvendo derramamento de petróleo pelos quais a responsável era a empresa BP. Até o número de resultados de cada um era distinto; no primeiro caso com 180 milhões de *sites* selecionados e no segundo com 139 milhões (PARISER, 2012,).

Eli Pariser descreve outro experimento que conduziu nos Estados Unidos, envolvendo publicações suas e de seus amigos na rede social Facebook. O autor percebeu que só conseguia visualizar comentários de seus amigos de mesma posição política que ele (democrata), não visualizando os comentários de seus amigos de outra orientação (republicana) em seu quadro de publicações na rede social.

Segundo o autor, a rede social, assim como a plataforma de buscas, estão criando filtros de conteúdo com base no histórico de navegação do usuário para oferecer apenas conteúdos que interessem a ele, sem deixá-lo “perder seu tempo” com notícias, aplicativos, programas e serviços que não lhe interessem (PARISER, 2012).

Um fenômeno que levanta a mesma inquietação de Matt, que, ao receber uma sugestão de notícia sobre como revelar para seus amigos e familiares acerca de sua opção sexual, não sabia como os administradores ou o sistema de análise de seus dados foram capazes de recomendar tal notícia, sugerindo que sabiam de sua opção sexual.

De um lado, o casamento de tecnologias de rastreamento com a publicidade comportamental e com os sistemas de personalização da navegação do usuário suscita questões importantes sobre privacidade na internet, tais como o nível de conhecimento dos usuários sobre a coleta e a destinação de suas informações, e a capacidade do usuário de tomar decisões sobre como gerir os seus dados na rede. De outro lado, atualmente existem poucas alternativas de remuneração na rede fora da estrutura deste casamento que não passem por recursos advindos do mercado publicitário, reforçando a máxima: “Se você não estiver pagando por algo, se você não for o consumidor, você é o produto”.

Na última seção deste artigo buscaremos relacionar as principais questões envolvendo o debate sobre privacidade e proteção de dados pessoais de usuários de internet, atribuindo especial destaque aos impactos do uso de tecnologias de rastreamento de dados.

A CRIAÇÃO DE INSTRUMENTOS REGULATÓRIOS DE PROTEÇÃO DE DADOS PESSOAIS

“Nós moldamos nossa ferramentas, depois nossas ferramentas nos moldam.”

Marshall McLuhan

a. Privacidade na internet como uma questão complexa

Não é objetivo deste trabalho apresentar um conceito jurídico de privacidade na internet. Não

teríamos espaço para tanto. Cabe aqui, contudo, fazer uma crítica ao núcleo conceitual das principais propostas regulatórias de proteção de dados pessoais na internet que estão sendo debatidas na União Europeia e nos Estados Unidos da América. A proposta ficou conhecida como modelo de autogestão da privacidade (“*privacy self-management model*”).

Dentre os diversos documentos que buscaram sintetizar o modelo de autogestão da privacidade, podemos citar a Diretiva 95/46/CE da União Europeia, que estabeleceu a política europeia de proteção de dados pessoais, e a política “*Do-not-Track*” (DnT) nos Estados Unidos, elaborada pela Casa Branca (Presidência) em conjunto com o Federal Trade Commission (UNITED STATES, 2012), que buscou criar um conjunto de princípios normativos que pudesse fortalecer o usuário ante a coleta de seus dados pessoais.

Em comum, ambas as propostas articulam como consequência do direito à privacidade, presente na esfera privada de todos os usuários de internet, o dever das empresas que de algum modo participam do ciclo da coleta, análise e emprego de dados pessoais de notificar os usuários sobre a coleta, análise e sobre o emprego de seus dados, o dever de acesso à informação sobre quais empresas tiveram acesso aos seus dados pessoais, e por fim o dever de obter o consentimento prévio e informado dos usuários para a realização da coleta de informações (SOLOVE, 2013, p. 2).

O Brasil não dispõe de diploma normativo que cuide do tema, conta apenas com a legislação civil que define o conceito de privacidade para as relações privadas, distantes dos novos desafios da associação entre tecnologias de rastreamento e a publicidade comportamental.

No entanto, cabe a menção ao anteprojeto de lei desenvolvido pelo Centro de Tecnologia e Sociedade (CTS) da Escola de Direito do Rio de Janeiro (Direito Rio) da Fundação Getúlio Vargas em conjunto com o Ministério da Justiça, que

utiliza-se do modelo de autogestão da privacidade, com profundas semelhanças em relação à proposta regulatória da União Europeia.

A partir da definição de três deveres (notificação, acesso e consentimento) mínimos às empresas que atuam dentro do ciclo da coleta de dados, os idealizadores das propostas europeia e estadunidense acreditam que poderão oferecer aos usuários de serviços na Web os instrumentos suficientes para que tomem decisões informadas, avaliando os benefícios dos serviços que recebem dessas empresas e os prejuízos que a coleta de seus dados possam ocasionar (SOLOVE, 2013, p.2).

Como contrapartida fática das empresas para dar conta dos três deveres do modelo de autogestão da privacidade, as empresas consideram que notificam e garantem o acesso a informações ao usuário de seus serviços quando disponibilizam informações genéricas sobre a coleta, análise e emprego desses dados em seus termos de uso e sua política de privacidade (NISSENBAUM, 2011).

Genérica, pois não especifica quais são as informações que estão sendo coletadas, sejam elas sobre o histórico de navegação do usuário, sua localização ou informações referentes à sua idade, sexo, estado de saúde, preferência sexual, dentre outras. Além disso, há a mera menção de que os dados coletados poderão ser compartilhados com outras empresas, a critério da ofertante dos serviços (*site*).

Acreditam que obtêm o consentimento dos usuários quando indagam se ele concorda com os termos de uso e a política de privacidade da privacidade no início do uso dos serviços da empresa (NISSENBAUM, 2011).

Em geral, a pergunta sobre a concordância ou discordância dos termos de serviço e com a política de privacidade do *site* ocorre quando o usuário inicia sua navegação, momento em que não se detém a examinar o conteúdo dos

documentos oferecidos, concordando pelo seu desejo em usufruir das funcionalidades dos serviços oferecidos pelo site.

Por fim, disponibilizam a possibilidade de o usuário interromper a coleta de dados a partir de uma opção de retirada, descrita nos documentos mencionados, seja por uma opção de navegação do *site*, seja por uma opção de configuração de determinados navegadores (*browsers*).

Nesse sentido, tanto o modelo de autogestão da privacidade falha, pois parte de um diagnóstico errôneo sobre o processo de tomada de decisão de usuários de internet, quanto a aplicação do modelo por parte das empresas que atuam no ciclo da coleta de dados falha ao não oferecer os instrumentos adequados para que o usuário possa identificar quais são os riscos da coleta de suas informações.

b. Problemas da gestão de dados pessoais

Há ainda pouca informação sobre a percepção da média dos usuários sobre a coleta de seus dados pessoais. Nos Estados Unidos, algumas pesquisas já avançaram no sentido de testar algumas associações e correspondências feitas por usuários na internet. Cabe a menção a algumas delas.

Em estudo¹⁰ de 2005 realizado pelo Annenberg Public Policy Center, 64% dos usuários de internet entrevistados não souberam que *sites* de supermercados compartilhavam suas informações de compra de produtos com outras empresas que nada tinham a ver com a atividade precípua do *site* do supermercado em que fizeram compras.

Na mesma pesquisa, 75% dos entrevistados acreditavam erroneamente que quando um *site* possui uma política de privacidade, esta significava que ele não compartilha dados pessoais de usuários com outros *sites* ou empresas. Uma falsa sensação de segurança, incompatível com o atual perfil dos atores presentes no ciclo de coleta, análise e destinação de dados pessoais.

Em estudo realizado em 2009¹¹ pelo mesmo instituto, verificou que apenas 30% dos entrevistados conseguiram responder a questões envolvendo suas últimas transações comerciais na internet, que variavam desde a descrição do que foi comprado ou vendido, até as informações que cada usuário acreditava estar fornecendo às empresas. Em outras palavras, apenas 30% dos entrevistados foram capazes de descrever que operação realizaram e quais as informações que efetivamente forneceram.

São dados que apresentam um usuário de internet com percepções equivocadas sobre o funcionamento do processo de coleta, análise e destinação de informações, guardando uma sensação de segurança incompatível com o atual cenário do desenvolvimento de tecnologias de rastreamento de dados, bem como um usuário com baixo grau de concentração e memória quanto às operações que realiza na rede. Vale nos questionarmos como um usuário com tais características pode ser protegido pelo modelo de autogestão da privacidade, baseado em políticas de privacidade e termos de uso de serviços.

¹⁰ O estudo traz ampla gama de informações sobre as percepções de usuários de internet nos Estados Unidos da América. Vale a pena conferir a metodologia empregada e os critérios de análise das respostas. Ver em: TUROW, Joseph; FELDMAN, Lauren; MELTZER, Kimberly. Open to exploitation: american shoppers online and offline. Annenberg Public Policy Center of the University of Pennsylvania, junho, 2005. Disponível em: < http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers>. Acesso em: 1 mar. 2013.

¹¹ A análise da percepção dos usuários de internet vem crescendo nos Estados Unidos da América e ganhando força em estudos como este. Há uma ampliação do escopo da pesquisa em relação a feita em 2005, bem como a delimitação maior do universo pesquisado. Ver em: TUROW, Joseph et. al. Americans reject tailored advertising and three activities that enable it. Disponível em: < http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf>. Acesso em 1 mar. 2013.

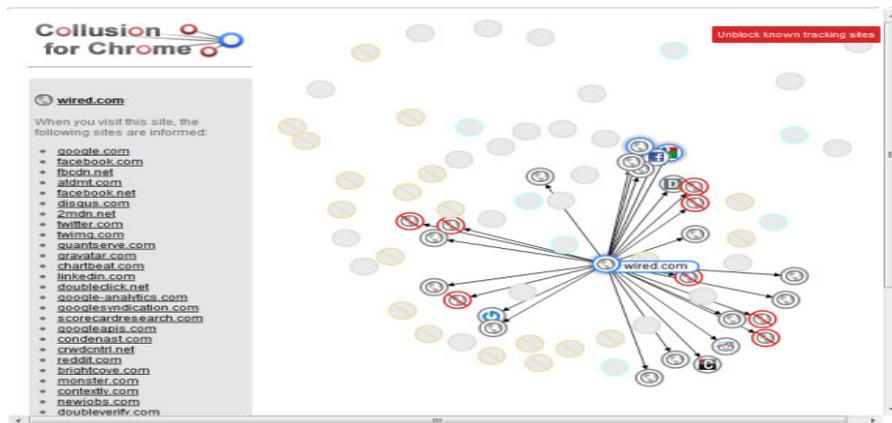
Em outro relevante estudo realizado em 2008 por Aleecia M. McDonald e Lourrie Faith Cranor¹², foi estimado que um modelo baseado na leitura de usuários de termos de uso e políticas de privacidade é muito custoso para eles e para a sociedade, seja pelo tempo que tomaria de cada usuário, aproximadamente 201 horas por ano em média, seja pelo custo do tempo perdido com essa leitura, aproximadamente US\$ 3.534 por usuário em média, e US\$ 781 bilhões no total de usuários nos Estados Unidos da América.

O estudo ainda aponta que mesmo que usuários se dispusessem a dedicar boa parte de seu tempo à leitura de termos de uso de serviços e políticas de privacidade, seria muito difícil ter a completa compreensão de seu significado pela excessiva utilização de terminologia técnica-jurídica, bem como pela utilização de termos técnicos ligados à computação.

¹² Recomenda-se a leitura integral do artigo de Cranor e McDonald. Após apresentarem as teorias econômicas que sustentam os modelos jurídicos de proteção de dados pessoais, com especial atenção ao modelo de autogestão da privacidade, os autores criam uma metodologia ímpar, cujo objetivo é avaliar o custo financeiro da leitura de termos de uso de serviços dos sites mais visitados na internet e de suas políticas de privacidade. Ver em: MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The cost of reading privacy policies. *Journal of Law and Policy for the Information Society*, 2008. Disponível em: <<http://www.is-journal.org>>. Acesso em: 8 jan. 2013.

TELA 1

Collusion – Visita ao site da Revista Wired



Cabe aqui o questionamento se, como sociedade, acreditamos que um usuário deva gastar 201 horas para leitura de tais documentos. Não haveriam alternativas, sejam elas do ponto de vista regulatório, sejam elas do ponto de vista técnico, que pudessem facilitar o acesso e a compreensão do processo de coleta, análise e destinação dos dados pessoais dos usuários, aprimorando sua tomada de decisão quanto à gestão de seus dados?

c. Ferramentas de gestão de dados pessoais

Ao lado do modelo de autogestão da privacidade tem crescido a oferta de serviços de proteção dos dados pessoais de usuários na internet. Eles podem ser observados na ampliação das opções de bloqueio de *cookies* presentes na maioria dos navegadores de internet nos dias atuais, até ferramentas específicas de visualização do rastreamento, bloqueio direto e auxílio na configuração de padrões de privacidade em redes sociais. É oportuno aqui uma menção mais detalhada os estes últimos.

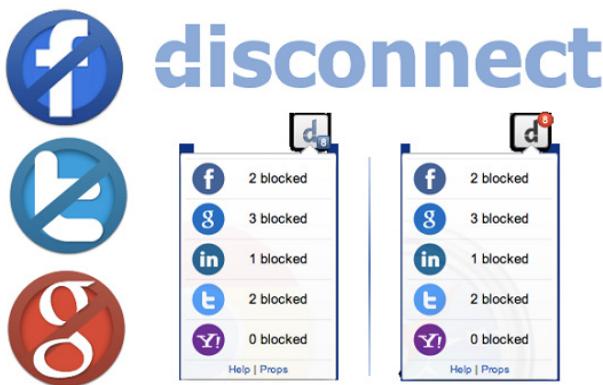
O aplicativo *Collusion* da empresa *Mozilla*, disponível para os navegadores *Safari* (*Apple*), *Chrome* (*Google*) e *Firefox* (*Mozilla*), é uma ferramenta que fornece a partir de elementos gráficos dados com quem o *site* por ele visitado compartilha sua informações. Não há nenhum bloqueio inicial, apenas a descrição do caminho que os seus dados percorrem entre os *sites* que você visitou e os *sites* que nunca visitou. Apresenta-se a seguir uma imagem que ilustra seu funcionamento.

A tabela 1 descreve o conjunto de *sites* que recebem os dados do usuário que visitou o *site* da revista *Wired*. Cada bola no centro da imagem representa um *site*, sendo que o *site* da revista *Wired* é o elo entre todos os demais. No canto esquerdo da imagem, o aplicativo elenca todos os *sites* que têm acesso às informações coletadas por tecnologias de rastreamento dispostas no *site* da revista.

Diferentemente de uma leitura exaustiva de documentos, a visualização rápida a partir do aplicativo *Collusion* nos parece mais eficaz e efetiva do que as descrições dos termos de uso e políticas de privacidade. Evitam-se equívocos de percepção e memória, pois a qualquer momento o usuário pode consultar quem está coletando suas informações.

O aplicativo *Disconnect*, desenvolvido pela *Disconnect Inc.*, empresa nascente de tecnologia do Vale do Silício, em Palo Alto, Califórnia, oferece gratuitamente a usuários a possibilidade de se desconectar dos principais *sites* na internet, Facebook, Google, Twitter, dentre outros. Basta instalar o aplicativo em seu navegador para servir como ferramenta de bloqueio da coleta de dados. Apresenta-se a seguir uma imagem que ilustra o aplicativo (tela 2).

TELA 2
Disconnect

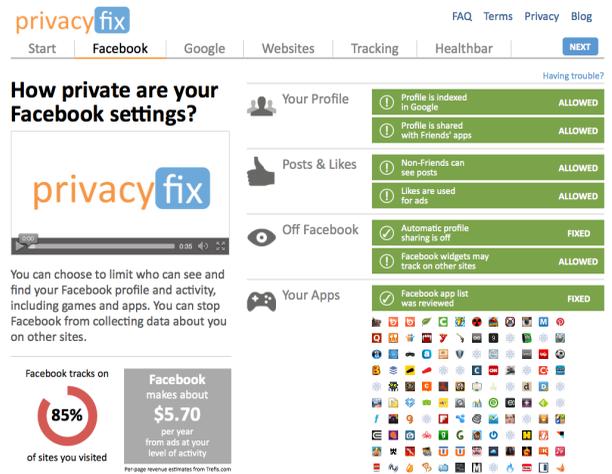


Por fim, a última ferramenta à qual faremos menção aqui se chama *Privacy Fix*. Desenvolvido pela organização não governamental *Privacy Choice*

nos Estados Unidos da América, o *site Privacy Fix* apresenta para o usuário qual o grau de exposição de suas informações para o seu rastreamento e o auxilia a corrigir, caso queira, suas configurações de privacidade, explicando, de modo mais simples do que termos de uso e políticas de privacidade, como proteger dados pessoais.

Informa também uma estimativa de quanto algumas empresas, como Facebook e Google, ganham com publicidade a partir das informações do usuário. Interessante notar a novidade desta informação para a tomada de decisão do usuário. Mostra-se a seguir uma ilustração sobre o funcionamento do aplicativo (tela 3).

TELA 3
Privacy Fix



A partir desses dados cabe propor uma reflexão: quando os usuários souberem quanto valem suas informações para as empresas, não poderiam escolher pagar pela total privacidade para receber os serviços que desejam ou pagar com suas informações, quando verificarem que seu benefício será maior do que o prejuízo do emprego de suas informações para fins de publicidade comportamental?

CONCLUSÃO: UMA AGENDA AMPLA DE PESQUISA

No cenário atual, o desenvolvimento de tecnologias de rastreamento ganha novas linhas de sofisticação. O rastreamento de dados que em sua primeira fase se restringia à coleta de informações por apenas um *site* ganhou nova dimensão com o compartilhamento de informações entre *sites* e redes de anunciantes, bem como com o desenvolvimento de tecnologias que permitem que o provedor de conexão de serviços de acesso à internet possa coletar e analisar dados pessoais. Não há mais dados que não sejam passíveis de serem coletados na rede, a não ser que o usuário se resguarde em relação a essas tecnologias.

Ao lado de todos os benefícios oferecidos pela personalização de serviços aos usuários de internet, bem como trazidos pelo desenvolvimento de novas empresas na rede, financiadas pelos recursos advindos da publicidade comportamental, não há como negar que a combinação entre tecnologias de rastreamento e a publicidade comportamental suscita ampla agenda de debates sobre a proteção de dados pessoais.

Questões que se inserem nas percepções dos usuários sobre o funcionamento do mercado da publicidade comportamental e da personalização dos serviços na internet, passando pelo aprimoramento do processo de tomada de decisão sobre o fornecimento ou não de suas informações, alcançando, por fim, a gestão contínua da coleta, análise e destinação de seus dados pessoais.

Se o objetivo da construção de um regime jurídico de proteção de dados pessoais é conciliar os modelos de negócio que garantem a oferta de serviços sem custos a usuários de internet com a proteção de seus dados pessoais, mais importante do que gerar um volume grande de informações em documentos de difícil leitura, é desenvolver ferramentas de fácil visualização para a gestão de dados pessoais, tais como o *Collusion*, o *Disconnect* e o *Privacy Fix*.

REFERÊNCIAS

- BEALES, Howard. The value of behavioral targeting. Network Advertising Initiative (NAI), 2010. Disponível em: <http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf>. Acesso: 15 maio 2012.
- BENDRATH, Ralf; MUELLER, Milton. The end of the net as we know it? Deep packet inspection and internet governance. *New Media and Society*. Brussels, 27 abr. 2011. Disponível em: <<http://nms.sagepub.com/content/early/2011/04/27/1461444811398031.full.pdf+html>>. Acesso em: 20 mar. 2012.
- BERGER, Dustin D. balancing consumer privacy with behavioral targeting. *Santa Clara Computer and High Technology Law Journal*, Santa Barbara, v. 27, 2011. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1693029>. Acesso em: 5 jul. 2012.
- CLAYTON, Richard. The phorm “webwise” system, 4 abril 2008, p. 3. Disponível em: <<http://www.cl.cam.ac.uk/~rnc1/080404-phorm.pdf>>. Acesso em: 9 maio 2012.
- LEONARDI, Marcel. *Responsabilidade civil de provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005.
- LESSIG, Lawrence. *Code Version 2.0*. New York: Basic Books, 2006.
- MACHADO, Robson. *Certificação digital ICP-Brasil: os caminhos do documento eletrônico no Brasil*. Niterói: Impetus, 2010.
- MCDONALD, Alecia M.; CRANOR, Lorrie Faith. *Beliefs and behaviors: Internet user’s understanding of behavioral advertising*. TPRC 2010. Disponível em: <<http://ssrn.com/abstract=1989092>>. Acesso em: 5 maio 2012.
- MCDONALD, Alecia M.; CRANOR, Lorrie Faith. The cost of reading privacy policies. *Journal of Law and Policy for the Information Society*, 2008. Disponível em: <<http://www.is-journal.org>>. Acesso: 8 jan. 2013.

MUELLER, Milton. *DPI technology from the standpoint of internet governance studies: an introduction*. Syracuse University School of Information Studies, 2011. Disponível em: < http://dpi.ischool.syr.edu/Papers_files/WhatisDPI-2.pdf>. Acesso em: 4 jun. 2012.

NISSENBAUM, Helen. A Contextual Approach to Privacy Online. *Daedalus*, v. 140, n.4, fall 2011.

PARISER, Eli. *The filter bubble: how the new personalized web is changing what we read and how we think*. London: Penguin Books, 2012.

PERSON, Andrea N. Behavioral advertising regulation: how the negative perception of deep packet inspection technology may be limiting the online experience. *Federal Communications Law Journal*, v. 62, p. 439, 2010. Disponível em: < http://www.law.indiana.edu/fclj/pubs/v62/no2/11-PERSON_FINAL.pdf>. Acesso em: 8 abr. 2012.

SOLTANI, Ashkan et. al. Flash Cookies and Privacy. SSRN eLibrary, 2009. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862>. Acesso: 2 mar.2013.

SOLOVE, Daniel. Privacy Self-Management and the Consent Paradox. *Harvard Law Review*, v. 126, n. 6, abr. 2013.

TUROW, Joseph; FELDMAN, Lauren; MELTZER, Kimberly. Open to exploitation: american shoppers online and offline. Annenberg Public Policy Center of the University of Pennsylvania, junho, 2005. Disponível em: < http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers>. Acesso: 1 mar. 2013.

UNITED STATES. Federal Trade Commission. *Protecting Consumer Privacy in na Era of Rapid Change: Recommendations for Businesses and Policymakers*. FTC Report,

2012. Disponível em: <<http://ftc.gov/os/2012/03/120326privacyreport.pdf>>. Acesso em: 18 jun. 2012.

REFERÊNCIAS COMPLEMENTARES

BENDRATH, Ralf. Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection. International Studies Annual Convention. New York: Fev. 2009. Disponível em: < http://userpage.fu-berlin.de/bendrath/ISA09_Paper_Ralf%20Bendrath_DPI.pdf>. Acesso em: 20 mar. 2012.

CALO, M. Ryan. Against Notice Skepticism in Privacy (and Elsewhere). *Notre Dame Law Review*, v. 87, iss. 3, p. 1027 – 1072, 2012. Disponível em: < <http://ssrn.com/abstract=1790144>>. Acesso em: 12 maio 2012.

DALY, Angela. The legality of deep packet inspection. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628024>.

Acesso em: 31 mar. 2012.

EVANS, David S. The Online Advertising Industry: Economics, Evolution, and Privacy. *Journal of Economic Perspectives*, v. 23, iss. 3, summer 2009, p. 37–60. Disponível em: < <http://www.aeaweb.org/articles.php?doi=10.1257/jep.23.3.37>>. Acesso em: 7 jul. 2012.

UNIÃO EUROPEIA. Grupo de Trabalho do Artigo 29 para Proteção de Dados Pessoais. Parecer 2/20120 sobre publicidade comportamental em linha da União Europeia. Disponível em: < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pt.pdf>. Último acesso: 22 jun. 2012.

NISSENBAUM, Helen. *Privacy in context: technology, policy, and the integrity of social life*. Palo Alto: Stanford Law Books, 2009.

SANDOVAL, Catherine J.K. Disclosure, deception, and deep-packet inspection: the role of the Federal Trade Commission act's deceptive conduct prohibitions in the net neutrality debate. *Fordham Law Review*, v. 78, iss. 2, 2009. Disponível em: <<http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4481&context=flr>>. Último acesso: 22/07/2012.

SPRANKEL, Simon. Online Tracking, Targeted Advertising and User Privacy – The Technical Part. In: PRIVACY AND WEB 2.0 SEMINAR SUMMER TERM 2011, Technische Universität Darmstadt, 2011. Disponível em: <<http://www.coderblog.de/wp-content/uploads/online-tracking-targeted-advertising-user-privacy-paper.pdf>>. Acesso em: 22 abr. 2012.

SOLOVE, Daniel. *Understanding privacy*. Cambridge: Harvard University Press, 2008.