

## “É de Comer?” Cookies de Navegador e os Desafios ao Direito à Privacidade na Rede

### RESUMO

Esta pesquisa visa a analisar o direito à privacidade no contexto tecnológico. Em termos metodológicos, aplica-se a afirmativa teórica de Lessig sobre as quatro modalidades de restrição dos comportamentos, a saber, leis, normas sociais, mercado e arquitetura, para promover uma análise qualitativa de conteúdo principalmente indireto. A principal conclusão é a de que o direito à privacidade sofre interferências dos elementos que compõem a arquitetura da rede, a exemplo do caso dos cookies de navegador. Portanto, é essencial conciliar proposições legais com o novo contexto tecnológico com vistas a oferecer uma melhor regulação a este tema.

**PALAVRAS-CHAVE:** Ciberespaço. Cookies. Direito e Internet. Privacidade.

Jordan Vinícius de Oliveira  
[jordanoliveira@tutanota.com](mailto:jordanoliveira@tutanota.com)  
Universidade do Estado do Rio de Janeiro

Lorena Abbas da Silva  
[lorena.abbas@tutanota.com](mailto:lorena.abbas@tutanota.com)  
Universidade Federal de Juiz de Fora

## INTRODUÇÃO

A expressão “*é de comer?*” pode ser utilizada no cotidiano popular para se referir a algo cujo funcionamento ou aplicação não é familiar a um dos interlocutores. No caso dos *cookies* de navegador, essa expressão pode ser empregada, já que as tecnologias atualmente empregadas por vários sites utilizam elementos obscuros para rastrear e tratar os dados pessoais, tornando complexo o processo de proteção à privacidade na rede.

Como explica Lessig (2006, pp. 07; 48), os *cookies* de navegador foram ferramentas imprescindíveis para o desenvolvimento da Internet, sobretudo em seu ajuste para comportar o comércio virtual. Em 1994, a empresa *Netscape* adaptou um protocolo de rede que tornava possível o depósito de um arquivo no computador do usuário que acessasse determinado site. Esse arquivo, o *cookie*, é o responsável por fazer com que o operador do site identifique o usuário e personalize a página para um futuro acesso.

O norte teórico da análise é composto pelas quatro modalidades de intervenção no comportamento humano (leis, normas sociais, mercado e arquitetura) estabelecidas por Lessig (2006, pp. 122-7), para verificar como as tecnologias contidas nos *cookies* podem afetar comandos legais que versem sobre a privacidade na rede. A estratégia metodológica empregada é a de análise qualitativa de elementos diretos e indiretos, para interpretá-los ante a afirmativa teórica escolhida e diagnosticar os novos contornos do direito à privacidade na rede. Serão analisadas obras interdisciplinares a fim de se verificar a intersecção entre direito e tecnologia, como a relação entre *cookies* de navegador e a privacidade na rede.

Dessa forma, a proposta é de investigar os desafios que as novas tecnologias trazem ao direito à privacidade na Internet. O problema de pesquisa estrutura-se na forma da seguinte pergunta: diante do constante fluxo de dados pessoais na atual sociedade da informação, de que maneira as tecnologias interferem na construção e sedimentação do direito à privacidade na rede?

Contextualizada no caso dos *cookies* de navegador, a hipótese a ser testada é a seguinte: diante da afirmativa teórica das quatro modalidades de regulação de comportamentos no ciberespaço – lei, norma, mercado e arquitetura –, afirma-se que as tecnologias de software e hardware que compõem a arquitetura da rede não apenas influenciam, mas são capazes de condicionar a formulação e a aplicação de normas sobre privacidade no ciberespaço.

## METODOLOGIA

O presente tópico apresenta os elementos basilares para o desenvolvimento da pesquisa realizada. Primeiramente a metodologia de trabalho é elucidada, seguida da afirmativa teórica escolhida.

Sob a perspectiva metodológica, esta pesquisa consiste em uma análise qualitativa de conteúdo, basicamente indireto, como obras bibliográficas sobre Direito e tecnologia. Poucos elementos diretos também serão trazidos à análise,

a exemplo de alguns referenciais sobre certos tipos de *cookie* de navegador. Como explica Groulx (2012, p. 97), a pesquisa qualitativa nas ciências sociais permite uma compreensão holística do problema de pesquisa, de maneira a contextualizar os elementos que compõem o conteúdo. Assim, a análise qualitativa trata-se de uma forma de investigação pela qual um conteúdo é investigado dentro de um contexto e de suas influências.

A técnica metodológica utilizada é a da pesquisa por traços de significação, segundo Babbie (2007, pp. 318ss.). Compreendem essa técnica três passos essenciais: a leitura de conteúdo publicamente disponível sobre o tema com a elaboração de hipóteses iniciais, a análise do objetivo ancorada em componentes do plano prático e a contraposição entre elementos teóricos e fáticos para ressignificar um tema. Neste estudo, a técnica é empregada da seguinte maneira: estabelece-se inicialmente uma investigação bibliográfica sobre direito à privacidade na sociedade da informação. Procede-se à coleta e análise de alguns elementos que expõem o comportamento fático do objeto pesquisado, os *cookies* de navegador, e defronta-se os achados iniciais com esses achados para ressignificar o objeto de pesquisa.

Um fator importante que compõe esse procedimento é a afirmativa teórica, cuja função é a de orientar a análise das informações obtidas e fundamentar a interpretação do objeto de pesquisa. Neste trabalho, optou-se pela afirmativa teórica das quatro modalidades de interferência no comportamento humano, estabelecidas por Lessig (2006, pp. 122-7).

Segundo o autor, a criação de uma lei, código positivado que contém determinado comando, não é o único elemento capaz de interferir no agir humano. A lei, na verdade, faz parte de um quadro mais amplo de fatores capazes de moldar preferências e ações. Assim, ela está sempre acompanhada dos elementos norma, mercado e arquitetura. As normas revelam-se no conjunto de padrões do agir humano que são seguidos graças a uma sedimentação social. Elas não necessitam, pois, de positivação, a exemplo do costume de dar bom dia ao chegar ao trabalho. Os mercados constituem estruturas de oferta e compra de bens cujos preços são capazes de estimular ou desestimular comportamentos. Produtos em promoção, por exemplo, podem induzir a compra em sujeitos antes não dispostos a adquiri-los. As arquiteturas, por fim, compõem aspectos do meio em que os sujeitos se encontram, cuja estrutura pode favorecer ou desfavorecer o agir humano. A distância geográfica das sedes governamentais em relação aos grandes centros ou a outros órgãos, por exemplo, é um fator clássico na organização política de vários países (LESSIG, 2006, pp. 122-7).

Essa afirmativa revela que a ação estratégica do Direito frente a sociedade não pode se dar de forma isolada, mas deve levar em consideração os elementos intrínsecos ao ambiente do próprio corpo social. Dessa maneira, lei, norma, mercado e arquitetura compõem um enredo próprio de intervenções no agir humano e por diversas vezes são integrados de maneira múltipla para impulsionar ou breçar comportamentos.

A escolha dessa afirmativa para o contexto da pesquisa se deve ao fato de que analisar o direito à privacidade em plena sociedade da informação é uma tarefa que vai além de uma definição jurídica sobre o que é privacidade. É um empreendimento que demanda uma capacidade analítica multidisciplinar, na

qual a compreensão jurídica sobre privacidade deve ser capaz de interagir com normas sociais, mercados e arquiteturas próprias no plano da Internet.

## DESENVOLVIMENTO (RESULTADO E DISCUSSÕES)

### DIREITO À PRIVACIDADE E TECNOLOGIA

O grande desafio para o direito à privacidade no atual contexto tecnológico decorre do forte fluxo de informações pessoais na Internet. Como constata Huang (1998, pp. 02-4), a evolução tecnológica fez com que os custos para coletar, armazenar, processar, recombinar e manipular bases de dados se tornassem cada vez menores. Essa diminuição de custos estimulou um mercado próprio para explorar os perfis de consumidores, por meio de um processo conhecido como mineração de dados, ou *data mining*.

Dessa forma, a mineração de dados é um fenômeno inevitável e que suporta diferentes tipos de dados ou perfis pessoais. Segundo Huang (1998, pp. 28-30), a intervenção jurídica nesse campo deve considerar as diferenças substanciais sobre os tipos de dados (dados sensíveis, como informações sobre saúde e dados não sensíveis, como informações sobre preferências musicais) e sobre os indivíduos aos quais os dados se referem (são adultos que fornecem seus dados de forma livre e esclarecida ou são informações extraídas indiretamente de crianças e adolescentes na rede?). Assim, embora a mercantilização dos dados pessoais seja uma realidade mundial, a regulação por normas jurídicas desse novo universo precisa diferenciar categorias de dados para agir de maneira mais eficiente.

De acordo com Bodin de Moraes (2012, pp. 14-5), a sociedade da informação traz uma espécie de mescla entre o sujeito e os dados responsáveis por definir, classificar e etiquetar seu perfil, de maneira que estas informações também constituem sua própria dignidade. Assim, é necessário que o indivíduo consiga controlar o uso de informações pessoais e ter clareza sobre sua utilização.

Zarsky (2006, pp. 212-3) compara as formas de obtenção de dados pessoais no mundo físico e virtual e constata a complexidade desse novo cenário. Se no mundo físico os dados pessoais são revelados somente ao término de uma transação, como maneira de conclusão do negócio, no mundo virtual eles estão expostos durante toda a navegação online do consumidor. Esses traços permitem cruzar padrões de consumo, prever ou até induzir preferências de mercado nos sujeitos.

O autor destaca a importância da notificação e do equilíbrio na forma de abordagem para ofertas aos indivíduos na rede. O processo de notificação deveria seguir a transparência nos conteúdos oferecidos individualmente, baseados em perfis de consumidores. Para tanto, é necessário que o consumidor saiba que determinada oferta é individualizada para o seu perfil e entenda como os seus dados contribuíram para que ela chegasse até ele. Esse primeiro passo tornaria possível a identificação de eventuais táticas de manipulação e o controle das informações que o consumidor julgar como indevidamente coletadas (ZARSKY, 2006, pp. 211-2).

Acerca do equilíbrio de ofertas de conteúdos, Zarsky (2006, pp. 211-2) afirma que é importante assegurar que nenhuma empresa centralize formas de influência sobre certo grupo de consumidores. Essa medida busca evitar que poderosos agentes de mercado discriminem consumidores com base em seus dados, ou que tratem alguns anúncios de maneira prioritária em detrimento de outros.

Para Hoofnagle e outros (2012, pp. 273-4), é possível identificar dois tipos de abordagem sobre a privacidade online: a regulatória e a mercadológica. Os autores afirmam que é comum a utilização pejorativa do termo “paternalista” às legislações que tratam sobre privacidade na rede, como se estivessem intervindo de maneira desarrazoada na liberdade individual. Entretanto, constatam que a verdadeira intervenção na autonomia individual decorre da abordagem mercadológica, pois ela inviabiliza as escolhas do sujeito graças a tecnologias inescapáveis de rastreamento na rede. Na esfera tecnológica, portanto, a abordagem de mercado decide o que é melhor para o próprio consumidor, retirando suas escolhas a partir da exploração de sua privacidade.

Rodotà (2008, pp. 190-1), por sua vez, alerta que no contexto das novas tecnologias é possível observar um processo de “*deregulation*”, onde as normas que regem a privacidade online são, na prática, elaboradas pelos departamentos jurídicos de grandes multinacionais, consultores de associações empresariais e escritórios de advocacia renomados. Essa desregulação leva a um processo de subversão do direito à privacidade, que passa a ser regido por agentes privados e não por leis discutidas publicamente.

Para o autor, a autossuficiência tecnológica ou legislativa não são por si só capazes de conjugar a complexidade advinda das novas tecnologias. A partir do exemplo das tecnologias de incremento de privacidade (*privacy enhancing technologies*) – que são programas e dispositivos tecnológicos utilizados para fins de proteção dos dados pessoais na rede –, Rodotà afirma que a relação entre Direito e tecnologia pode se estabelecer de maneira estratégica, pela incorporação das novas tecnologias para a valoração política de questões sobre privacidade na rede. Assim, o caminho deve ser estabelecido por uma relação harmônica entre esses dois planos, sem reduzir a importância de um ao poder do outro, mas associando-os (RODOTÀ, 2008, pp. 123-4).

No contexto brasileiro, a Lei nº 13.709 (Lei Geral de Proteção de Dados Pessoais – LGPD) foi sancionada em agosto de 2018 e representa um grande passo na regulação do tema tratando, por exemplo, sobre a necessidade, em regra, de consentimento do usuário na utilização de seus dados, a atenção aos chamados dados sensíveis, a proteção à liberdade de informação e a regulação do uso de dados por terceiros (BRASIL, 2018).

Da redação final, porém, foram vetados os artigos 55 e subsequentes, que tratavam da criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão fiscalizador que foi introduzido no projeto de lei para estabelecer parâmetros e aplicar sanções em caso de descumprimento das novas normas. A justificativa para o veto foi a de vício de iniciativa no projeto de lei, mas há promessa futura de criação da figura reguladora pelo próprio presidente (JUBÉ e ARAÚJO, 2018). Até lá, a nova lei passará por um período de 18 meses para entrar em vigor e, como se verá pelo caso dos *cookies*, dependerá em muito da criação da Autoridade para ganhar efetividade.

Como bem explica Doneda (2018), a criação da Autoridade Nacional é elementar, por: (a) estabelecer parâmetros e proteger a esfera individual e coletiva dos dados pessoais; (b) mediar eventuais conflitos sem a necessidade de judicialização de demandas; (c) fiscalizar estipular sanções para descumprimentos e (d) viabilizar a credibilidade do Brasil frente a países e blocos econômicos dotados de leis avançadas sobre o tema de proteção de dados, o que traria benefícios políticos e econômicos ao empresas nacionais.

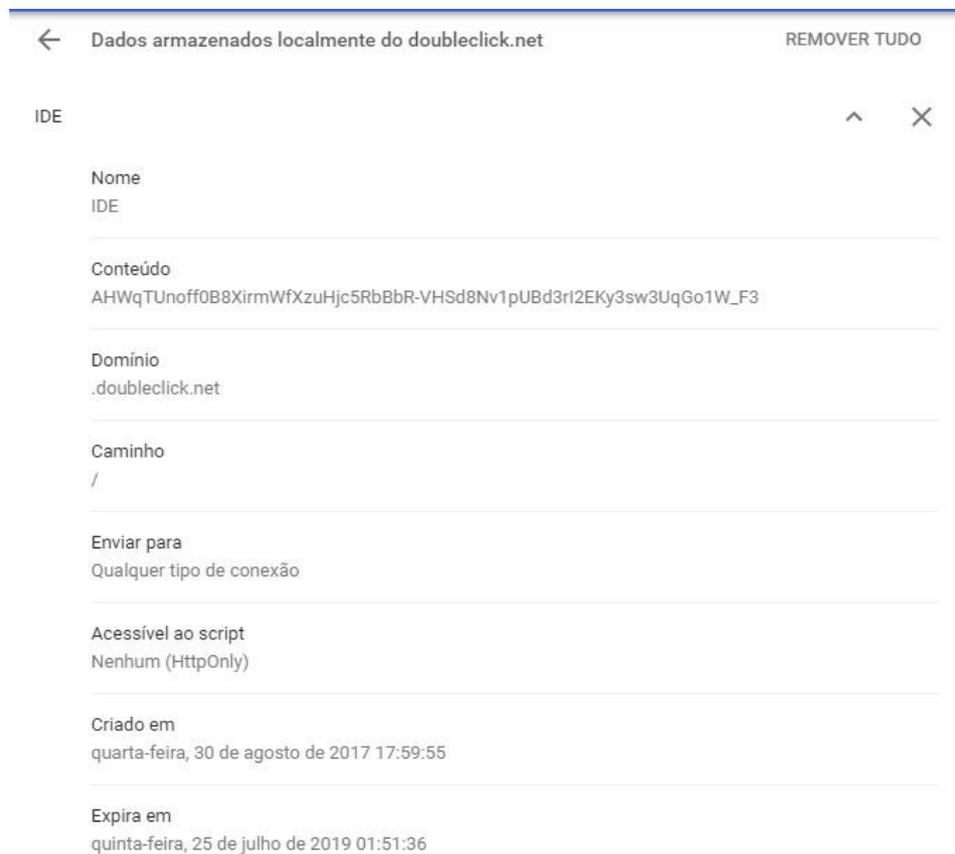
### COOKIES DE NAVEGADOR E A EXPLORAÇÃO DE DADOS PESSOAIS

Como explica Hormozi (2005, pp. 01; 03), o *cookie* trata-se de um pequeno arquivo, geralmente no formato de texto, depositado pelo servidor de um site no disco rígido do computador que o acessa. Seu propósito original era o de beneficiar o internauta, que pouparia tempo e poderia usufruir de visitas mais personalizadas ao mesmo site no futuro. Esse autor afirma que o *cookie* é um elemento importante e quase indispensável para a comunicação com os sites na Internet, de maneira que se tornaria muito difícil utilizá-la sem a sua presença.

De acordo com Siebecker (2003, pp. 893-6), o problema clássico em relação ao *cookie* diz respeito ao seu depósito pelo site sem a devida autorização do usuário e seu emprego na coleta e manutenção de informações pessoais, revelando padrões de acesso, preferências e característica. Ele cita o caso da empresa *DoubleClick Inc.*, pertencente à *Google*, responsável pela oferta de mais de 60 bilhões de anúncios mensais na rede, cuidadosamente interligados a perfis de mais de 100 milhões de usuários rastreados online.

Aproveitando-se o caso da *DoubleClick*, a Figura 1 traz a apresentação de um *cookie* da empresa, contido no navegador de um dos próprios autores deste artigo.

Figura 1: Identificação do *cookie* “IDE” da DoubleClick no navegador Google Chrome



De acordo com a Google (2017), o *cookie* representado acima é o “IDE”, também chamado de “Id”, utilizado pela empresa em sites de terceiros para fins de veiculação personalizada de publicidade em toda a web.

Pela Figura 1 é possível observar algumas das propriedades que constituem um *cookie*. Consoante Hormozi (2005, p. 02), são elementos obrigatórios apenas o nome e o valor. No caso da imagem, o nome é “IDE” e o valor é o conteúdo, formado por vários caracteres. Este campo do valor permite à empresa individualizar o *cookie* e interligá-lo ao usuário, para vincular conteúdos personalizados. Os demais elementos são opcionais, como o caminho (que indica o endereço da web onde o *cookie* é válido, geralmente marcado com o símbolo “/”), o domínio (para onde o navegador deverá retornar as informações do *cookie*, no caso o domínio da empresa DoubleClick), os padrões de conexão e segurança para o uso do *cookie* e sua data de criação e de expiração (sendo que se não for designada uma data de expiração, o *cookie* caducará junto com o fechamento do navegador).

Segundo Wojtowicz (2013, pp. 21-2), é possível falar em famílias de *cookies* de navegador, conforme a sua finalidade. A primeira família listada pelo autor é a dos *cookies* técnicos. Eles se destinam ao correto funcionamento de uma página

na Internet, sendo subdivididos entre *cookie* persistente e *cookie* de sessão. O primeiro é utilizado para autenticar, rastrear e memorizar as informações sobre a sessão do navegador do usuário, permanecendo até a data programada para expirar, via de regra. Já o *cookie* de sessão se desfaz cada vez que o navegador é fechado. Ainda segundo o autor, outra família de *cookies* de navegador seria a de perfil, utilizada para traçar os padrões de navegação do usuário e coletá-los de maneira organizada com vistas a oferecer mensagens publicitárias específicas às suas preferências.

Hoofnagle e outros (2012, p. 276) destacam que esses *cookies* podem ser próprios, ou seja, gerenciados pelo respectivo site que o usuário acessa. Podem ainda ser de terceiros, quando gerenciados por um site diferente do acessado. Os *cookies* de terceiro fornecem os padrões de navegação dos usuários a empresas ou sujeitos que não guardam relação com seu acesso. Assim, ao acessar o “site A”, o sujeito pode interagir com *cookies* de navegador do mesmo site, mas também do “site B”, do “site C” e por aí em diante.

### NÃO É DE COMER! COOKIES E DESAFIOS REGULATÓRIOS

Até aqui foi possível verificar qual a constituição de um *cookie*. Vislumbrou-se que ele pode ser criado para diversas finalidades e também que pode ser destinado para o mesmo site acessado ou para site de terceiros, contendo informações sobre os padrões da conexão do usuário. Observou-se ainda que a sua existência é basilar para o funcionamento da Internet e que ele pode estar associado à exploração de dados pessoais e padrões de consumo dos usuários na rede.

Todas essas constatações já permitem estabelecer questionamentos sobre as implicações que os *cookies* trazem para o direito à privacidade em plena sociedade da informação. Basta cogitar as inúmeras informações que podem ser reveladas pelo simples histórico de navegação de um usuário: se está doente, se deseja adquirir um produto, se possui preferências políticas e sexuais determinadas, entre tantos outros elementos que constituem a esfera íntima da personalidade humana.

Cabe ainda elencar alguns resultados do estudo de Ayenson e outros (2011, p. 02), que potencializam essa reflexão sobre *cookies* e privacidade. Os autores identificaram três tipos diferentes de técnicas de armazenamento de *cookies* nos computadores dos usuários: os *cookies* comuns *HTTP*, os chamados *cookies flash* e os *cookies* de armazenamento *HTML5*, mais recentes.

Como os pesquisadores expõem, esses *cookies* se diferenciam basicamente quanto ao potencial de armazenamento, à forma de expiração e quanto à maneira de acesso. Quanto ao armazenamento, enquanto o *cookie* padrão *HTTP* só consegue arquivar uma quantidade muito pequena de informação por vez, apenas 4 Kbytes e o *cookie flash* atinge 100 Kbytes, o armazenamento por *HTML5* consegue salvar em média 5MBytes de informação. Quanto à expiração, os *cookies flash* e o *HTML5* são permanentes, enquanto o *cookie* padrão *HTTP* é eliminado após o término da sessão online, via de regra. Com relação à maneira de acesso do *cookie*, os tipos *HTTP* e *HTML5* somente são acessíveis pelo único navegador em que foram salvos originalmente, enquanto o *cookie flash* fica disponível a todos os navegadores do usuário. Isso significa que todas as suas

informações, independentemente do navegador utilizado em um mesmo dispositivo computacional, são armazenadas e compartilhadas de forma conjunta, caso o site acessado empregue *cookies flash* (AYENSON e outros, 2011, p. 07).

Superadas essas classificações, um aspecto que chama atenção no estudo de Ayenson e outros (2011, pp. 07-12) são os dados apresentados. Os autores investigaram a presença desses tipos de *cookies* nos 100 sites mais utilizados pelos usuários norte-americanos, constatando apenas neles a presença de 5.675 *cookies* do tipo HTTP, 100 *cookies* do tipo *flash* e 17 do tipo HTML5. Dessa amostra, 4.915 pertenciam a domínios de terceiros, sendo que dos 100 principais sites dos Estados Unidos, a supracitada *DoubleClick*, da Google, estava presente em 77.

Para além desses números, o ponto central do trabalho está na constatação de técnicas específicas para burlar o controle dos usuários sobre os *cookies*. Ayenson e outros (2011, p. 13-4) verificaram a existência de uma técnica de reaparecimento, ou *respawning*, de *cookies* deletados. Nessa técnica, o artifício empregado é o de espelhar as informações gravadas sobre as páginas visitadas pelo navegador (*cache*) por meio de um identificador específico, chamado de *Etag*. Com esse artifício mesmo que o usuário opte por bloquear ou deletar os *cookies* HTTP, *flash* ou HTML5, eles ressurgirão para rastrear a navegação do usuário. Assim, certos *cookies* utilizam-se de um recurso inerente ao funcionamento do navegador para se perpetuarem, mesmo quando apagados. Para se livrar desse recurso, o usuário teria de limpar o *cache* de navegação a cada site visitado, sendo que nem o modo de navegação anônimo seria capaz de blindar os seus dados contra o rastreamento.

Além dessa técnica de *Etags* nas páginas visitadas, os autores citam um estudo anterior que seguiu os mesmos moldes e constatou outra forma de reaparecimento de *cookies* HTTP deletados. No caso, mesmo se deletados pelos usuários, os valores dos *cookies* HTTP poderiam reaparecer como *cookies flash*, inclusive em outros sites. Dessa maneira, um *cookie* HTTP deletado de um “Site A”, por exemplo, poderia reaparecer com valores idênticos como *cookie flash* no “Site B”. Isso demonstra uma estratégia tecnológica capaz de minar as escolhas dos usuários sobre os *cookies* em seus computadores, haja vista que um *cookie* contendo dados pessoais, mesmo se deletado, pode se perpetuar entre terceiros que visam construir uma base minuciosa de perfis (AYENSON e outros, 2011, pp. 07-8).

O que os resultados de Ayenson e outros demonstram é que as tecnologias verificadas nos *cookies* possuem uma capacidade de disseminação e de operação que extrapolam as habilidades de usuários comuns da Internet. Assim, mesmo que o usuário opte por controlar os *cookies* de seu próprio navegador, é possível que ele não consiga lidar com certas estratégias de armazenamento e de coleta de dados pessoais na rede e permaneça incessantemente monitorado no plano virtual.

Conjugando-se essas informações sob a ótica teórica de Lessig (2006, pp. 122-7), constata-se que a construção e a sedimentação do direito à privacidade necessitam de estratégias bem elaboradas para comportar as conjunturas próprias da rede. Como explica o autor, não basta o estabelecimento de uma lei

que exija certo conteúdo, se as condições das normas sociais, do mercado e da arquitetura não são condizentes com esse mandamento original.

Para a situação específica dos *cookies*, a esfera da arquitetura tem grande importância na modulação de comportamentos na rede. A arquitetura significa o desenho de uma estrutura e a maneira pela qual esse desenho modula a ação humana. Assim, mesmo que os diferentes Estados estabeleçam medidas regulatórias específicas para o caso dos *cookies*, é necessário ter em mente que a arquitetura tecnológica pode utilizar subterfúgios para burlar as preferências dos usuários e essas diretrizes. Logo, cabe ao Direito ter em vista a necessidade de incorporar essas estruturas tecnológicas para agir neste plano, sob pena de desconexão entre o comando legal e a complexidade do real.

No caso brasileiro, verifica-se que a aprovação da Lei nº 13.709/2018, é apenas o ponto de partida para regular a temática de privacidade na rede. O artigo 16, III, prevê, por exemplo, que os dados pessoais deverão ser eliminados após o tratamento, sendo sua conservação autorizada para fins de transferência a terceiros (BRASIL, 2018). Comandos legais como esses são, por si só, insuficientes para lidar com essa nova realidade tecnológica, em que os dados podem ser armazenados e compilados mesmo contra a vontade expressa do usuário e após o seu tratamento, graças a ferramentas técnicas.

Apesar de uma lei não ser capaz de comportar toda a complexidade advinda do real em tempos digitais, isso não significa que o Direito deve ficar de “mãos atadas” frente as novas tecnologias. Ele pode ser construído de maneira mais robusta quando a dimensão da lei conseguir articular os elementos da arquitetura do meio digital, como os *cookies*.

Assim, a existência, o assessoramento técnico e a composição democrática de órgãos regulamentadores, como a (futura) Autoridade Nacional, possuem papel central ao integrarem o Direito com a perspicácia tecnológica necessária para lidar com o tema. É nessa interação e cooperação entre Direito e tecnologia que residem os novos contornos da privacidade no Século XXI.

### SUGESTÕES DE ABORDAGENS FUTURAS

Por fim, a partir da experiência deste escrito, os autores sugerem, em caráter de futuras investigações no tema dos *cookies*, a análise empírica e multidisciplinar do uso destas ferramentas em sites com maior acesso do público brasileiro. A exemplo do estudo de Ayenson e outros (2011), voltado para o contexto americano, pesquisadores brasileiros poderiam formar uma equipe interdisciplinar (com estudiosos da Ciência da Computação, do Direito e de outras áreas) para coleta e análise de dados sobre o emprego dos *cookies* em sites de maior acesso no país.

### CONSIDERAÇÕES FINAIS

Esta pesquisa buscou analisar a interação entre o plano jurídico e as novas tecnologias na sociedade da informação. O plano teórico escolhido para a análise partiu da afirmativa teórica das quatro modalidades de regulação de comportamentos, segundo Lessig, para investigar o caso dos *cookies* de navegador.

A estratégia metodológica utilizada foi da análise qualitativa de conteúdo, na qual foram investigados elementos basicamente indiretos que retratam uma perspectiva holística da temática.

Constatou-se que, em plena sociedade cibernética, a tecnologia possui enorme capacidade de interferência na autonomia dos indivíduos na rede. A partir do caso dos *cookies* de navegador, verificou-se a diversidade de elementos e de estratégias técnicas que permeiam sua ação nos computadores pessoais, que podem se sobrepor às escolhas individuais sobre a privacidade eletrônica.

Assim, afirma-se que a construção e sedimentação do direito à privacidade no plano digital precisa considerar a capacidade das tecnologias atuais em extrair dados pessoais para traçar medidas interventivas mais adaptadas e contemporâneas. Embora não sejam “de comer”, os *cookies* de navegador podem conter maiores complexidades do que se imagina.

## “Can You Eat It?” Browser Cookies and the Right to Privacy Challenges in Cyberspace

### ABSTRACT

This research aims to analyze the right to privacy in the current technological context. Methodologically, the Lessig's theoretical affirmative of four forces of behavior constraint, namely law, social norms, market and architecture, it is applied to promote a qualitative analysis of mainly indirect data. The main conclusion is that the right to privacy is influenced by the elements that compose the web environment, as one can observe by the browser cookies case study. Therefore, it is essential to conciliate the legal propositions with the new technological context in order to offer a better suited regulation of this matter.

**KEYWORDS:** Browser Cookies. Cyberspace. Cyberlaw. Privacy.

## REFERÊNCIAS

AYENSON, Mika D. WAMBACH, Dietrich J. SOLTANI, Ashkan. GOOD, Nathan. HOOFNAGLE, Chris J. Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning. **Social Science Research Network**, jul. 2011, 21 p. DOI: <http://dx.doi.org/10.2139/ssrn.18983902011>, acesso em: 03 jul. 2017.

BODIN de MORAES, Maria Celina. Ampliando os direitos da personalidade. **Academia.edu**, jan. 2012, pp. 01-20. Disponível em: <https://www.academia.edu/9689598/Ampliando\_os\_direitos\_da\_personalidade>. Acesso em: 29 abril 2017.

BRASIL. **Lei nº 13.709 de 14 de agosto 2018**, dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil\_03/\_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 18 out. 2018.

DONEDA, Danilo César Manganhoto. O que está em jogo com a nova Autoridade Nacional de Proteção de Dados. **JOTA**, 13 de agosto de 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-que-esta-em-jogo-com-a-nova-autoridade-nacional-de-protECAo-de-dados-13082018>. Acesso em: 14 ago. 2018.

GOOGLE INC. **Tipos de cookies usados pelo Google**. Disponível em: <https://www.google.com/policies/technologies/types/>. Acesso em: 01 set. 2017.

GROULX, Lionel-H. Contribuição da Pesquisa Qualitativa à Pesquisa Social. Em: POUPART, Jean. DESLAURIES, Jean-Pierre. GROULX, Lionel-H. LAPERRIÈRE, Anne. MAYER, Robert. PIRES, Álvaro. **A Pesquisa Qualitativa: Enfoques Epistemológicos e Metodológicos**. Petrópolis: Vozes, 2012, 3ª ed., 464 p.

HOOFNAGLE, Chris Jay. SOLTANI, Ashkan. GOOD, Nathaniel. WAMBACH, Dietrich J. Behavioral Advertising: The Offer You Can't Refuse. **Harvard Law & Policy Review**, n 06, vol. 273, 2012. Disponível em: <http://scholarship.law.berkeley.edu/facpubs/2086>. Acesso em 03 maio 2017.

HORMOZI, Amir M. Cookies and Privacy, **EDPACS: The EDP Audit, Control, and Security Newsletter**, vol. 32:9, pp. 01-13, 2005. DOI: <10.1201/1079/45030.32.9.20050301/86855.1>.

HUANG, Peter H. The Law and Economics of Consumer Privacy Versus Data Mining. **Social Science Research Network**, Maio de 1998. DOI: <<http://dx.doi.org/10.2139/ssrn.94041>>. Acesso em: 29 abril 2017.

JUBÉ, Andrea. ARAÚJO, Carla. Temer vai criar agência sobre proteção de dados por projeto de lei. **Valor Econômico**, 18 de agosto de 2018. Disponível em: <<https://www.valor.com.br/politica/5735299/temer-vai-criar-agencia-sobre-protecao-de-dados-por-projeto-de-lei>>. Acesso em: 18 ago. 2018.

LESSIG, Lawrence. **Code (version 2.0)**. Nova Iorque: Basic Books, 2006. 411p. ISBN-10: 0-465-03914-6. ISBN-13: 978-0-465-03914-2.

RODOTÀ, Stefano. **A Vida na Sociedade da Vigilância**. Rio de Janeiro: Renovar, 2008. 382 p. ISBN: 8571476888.

SIEBECKER, Michael R. Cookies And The Common Law: Are Internet Advertisers Trespassing On Our Computers? **Southern California Law Review**, vol. 76, nº. 4, Maio 2003. Disponível em: <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=300187](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=300187)>. Acesso em 02 maio 2017.

WOJTOWICZ, Patryk. **Darknet e Deep Web: il Lato Oscuro del Web per la Privacy e la Protezione dei Dati**. Tesi di Laurea, Corso di Laurea in Ingegneria Elettronica, Informatica e Telecomunicazioni, Anno Accademico 2013, sessione II, Università di Bologna, Italia. Disponível em: <[http://amslaurea.unibo.it/8456/1/wojtowicz\\_patryk\\_tesi.pdf](http://amslaurea.unibo.it/8456/1/wojtowicz_patryk_tesi.pdf)>. Acesso em mar. 2017.

**Recebido:** 14 jun 2018.

**Aprovado:** 31 out 2018.

**DOI:** 10.3895/rts.v15n37.8419

**Como citar:** OLIVEIRA, J. V.; SILVA, L. A. "É de Comer?" Cookies de Navegador e os Desafios à Privacidade na Rede. **R. Technol. Soc.**, Curitiba, v. 15, n. 37, p. 297-310, jul./set. 2019. Disponível em: <<https://periodicos.utfpr.edu.br/rts/article/view/8419>>. Acesso em: XXX.

**Correspondência:**

**Direito autoral:** Este artigo está licenciado sob os termos da Licença Creative Commons-Atribuição 4.0 Internacional.

