COOKIES DE NAVEGADOR E HISTÓRIA DA INTERNET: DESAFIOS À LEI BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS *

BROWSER COOKIES AND THE INTERNET HISTORY: CHALLENGES TO THE BRAZILIAN GENERAL DATA PROTECTION LAW

Jordan Vinícius de Oliveira **

Lorena Abbas da Silva ***

RESUMO: Este artigo investiga a história dos *cookies* de navegador, sua conexão com o surgimento da web e suas implicações ao direito de proteção dos dados pessoais. O principal objetivo é o de analisar elementos envolvidos com a implementação dos *cookies* nos anos 90 e identificar os principais desafios que impõem à Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/18. As quatro modalidades de influência sobre o comportamento humano – lei, normas sociais, mercado e arquitetura –, expostas por Lessig, compõem o substrato teórico do estudo e a questão de pesquisa indaga se é possível afirmar que uma dessas modalidades foi determinante para a padronização técnica dos *cookies*. A sessão de discussão demonstra que a esfera de mercado teve um papel preponderante na estabilização de parâmetros para os *cookies*. Assim, o principal desafio à regulamentação da Lei Geral de Proteção de Dados é o de harmonizar aspectos técnicos, sociais e legais com vistas a viabilizar de forma concreta o controle dos cidadãos sobre os seus dados.

Palavras-chave: Cookies de navegador. Dados Pessoais. Lei 13.709/2018. Privacidade. Rede Mundial de Computadores.

ABSTRACT: *This paper investigates the historical background of browser cookies into the web development and their implication on the right to data protection. The main objective is to analyze the elements involved in the implementation of cookies in the 90s and identify the challenges they pose to the Brazilian General Data Protection Law nº 13.709/2018. Lessig's four modalities of constraint in human behavior – law, social norms, market and architecture – set the theoretical framework and the research question examines whether is possible to affirm that one of these modalities took a central place in the cookies technical standardization. The discussion session shows that the market sphere had a prominent influence over how cookies were configured.*

* O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

** Doutorando em Direito Civil pela UERJ. Pesquisador Sênior do Projeto de Conformidade Leis de Dados Pessoais da FGV/SP. Mestre em Direito e Inovação e Bacharel em Direito pela UFJF. Atuou como técnico em informática pela loja *CyberTech Informática SJDR/MG*. <jordanoliveira@tutanota.com>

***Mestranda em Direito e Inovação e Graduada em Direito pela UFJF. Bolsista CAPES/DS de Mestrado. <lorenaabbas@tutanota.com>.

Artigo recebido em 02/04/2019 e aceito em 22/04/2019.

Como citar: OLIVEIRA, Jordan Vinícius de; SILVA, Lorena Abbas da. *Cookies* de navegador e história da internet: desafios à lei brasileira de proteção de dados pessoais. **Revista de Estudos Jurídicos UNESP**, Franca, ano 22, n. 36, p.307, jul/dez. 2018. Disponível em: <https://ojs.franca.unesp.br/index.php/estudosjuridicosunesp/issue/archive>.

Therefore, the main challenge for the regulation of Brazilian General Data Protection Law is to harmonize technical, social and legal efforts in order to better enhance the practical path for subjects control their data.

Keywords: *Browser cookies. Personal Data. Law n° 13.709/2018. Privacy. World Wide Web.*

INTRODUÇÃO

Como você se sentiria se alguém pudesse visualizar todo o histórico do seu navegador de internet (Chrome, Firefox, Safari…) neste instante? As respostas podem oscilar entre a resignação e o apavoramento, com notas de "não me importo, não tenho nada a esconder". Ao realizar buscas na internet, navegar nas redes sociais ou acessar canais de vídeos online, estamos deixando traços que podem, e com frequência, são utilizados para diversas finalidades e por agentes desconhecidos.

Os chamados *cookies*[1] de navegador são cada vez mais utilizados como opção de ferramenta de coleta de informações para monitorar e compreender o comportamento dos internautas[2]. Nesse sentido, o propósito deste artigo é examinar os *cookies* e sua relação com o direito à proteção de dados pessoais, dedicando especial atenção aos seguintes pontos: (i) a relação entre o momento histórico de surgimento dos *cookies*, no ano de 1994, e o processo de desenvolvimento da web e; (ii) o diagnóstico dos desafios trazidos pelos *cookies* aos princípios previstos na Lei Geral de Dados Pessoais, Lei nº 13.709/18.

O marco teórico utilizado é o das quatro modalidades de regulação do comportamento humano – lei, normas sociais, mercado e arquitetura, segundo Lawrence Lessig (2006, p. 122-130). A abordagem metodológica privilegia uma análise qualitativa de referenciais bibliográficos indiretos e dados secundários, sob uma perspectiva historicista, de acordo com Fonseca (2012, p. 35-6).

O problema de pesquisa é estruturado na forma da seguinte pergunta: a partir de uma contextualização histórica dos *cookies*

[1] Os *cookies* de navegador serão melhor explicados ao decorrer deste artigo. Por ora, basta compreender que os *cookies* são pequenos arquivos de texto depositados pelo site provedor de conteúdo, ou *servidor*, no computador do usuário, ou *cliente,* para os fins de "recordar" o status da conexão e algumas informações pessoais do internauta (CAHN outros, 2016, p. 891).

[2] O navegador *Google Chrome*, por exemplo, foi recentemente denunciado pelo colunista de tecnologia Geoffrey Fowler, do jornal *The Washington Post*, após um experimento de uma semana no qual autorizou cerca de 11,189 (onze mil, cento e oitenta e nove) requisições de rastreadores de navegação. Estas requisições foram majoriariamente bloqueadas no navegador concorrente *Mozilla Firefox* (FOWLER, 2019).

de navegador e considerando as quatro formas de intervenção no comportamento humano – lei, normas sociais, mercado e arquitetura –, é possível afirmar que houve predomínio de uma dessas modalidades na fixação dos parâmetros técnicos de funcionamento e adoção dos *cookies*?

O trabalho está dividido da seguinte maneira: no próximo item o quadro teórico e metodológico é apresentado, em conjunto com uma revisão bibliográfica sobre dados pessoais e *cookies* de navegador. No item 3, uma análise histórica e pormenorizada do caso dos *cookies* é feita com o auxílio de alguns dados indiretos, responsáveis por retratar a disseminação contemporânea dessa tecnologia. Ao final, no item 4, as conclusões do estudo são sintetizadas.

1 PRESSUPOSTOS DA ANÁLISE: QUADRO TEÓRICO-METODOLÓGICO E O DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Esta seção visa explicar a metodologia de pesquisa e o substrato teórico do estudo. Após a exposição da técnica metodológica e da afirmativa teórica escolhidas, o tópico segue com uma revisão bibliográfica sobre os *cookies* de navegador e a proteção dos dados pessoais.

De acordo com Fonseca (2012, p. 29), embora possuam traços distintivos, metodologia e teoria integram um painel mútuo cujo resultado é o de operacionalizar saberes contidos fora de seus escopos. Assim, a teoria e a metodologia não se esgotam em si mesmas e auxiliam no desenvolvimento de novos saberes.

Nesse sentido, a presente pesquisa se vale de um recorte qualitativo histórico acerca da proteção de dados pessoais e sua relação com os *cookies* de navegador, sob o prisma teórico das quatro esferas de interferência no comportamento humano, exposto por Lawrence Lessig (2006).

O objetivo principal é analisar a história dos *cookies* de navegador com base em uma bibliografia interdisciplinar sobre essa tecnologia e sua relação com o desenvolvimento da web no decorrer dos anos 90. Já o objetivo específico, é avaliar os principais desafios que os *cookies* podem trazer para a regulação do chamado direito à proteção dos dados pessoais, tendo em vista os princípios consagrados pela Lei Geral de Proteção de Dados Pessoais (LGPD).

Metodologicamente, como perspectiva histórica se entende aqui não a construção de uma "linha do tempo", na qual o momento contemporâneo representa uma evolução perfeita e acabada do fenômeno

analisado. Como bem assevera Fonseca (2012, p. 35-6), o objetivo é inserir a situação presente em uma contingência histórica e contínua a partir de uma leitura interdisciplinar de épocas e eventos específicos pertinentes à investigação.

Dessa maneira, o percurso metodológico se inicia com a apresentação do marco teórico escolhido, seguido de uma revisão bibliográfica relativa às nuances mercadológicas, técnicas, sociais e legais dos dados pessoais. Na seção 3, emprega-se a análise qualitativa de alguns episódios históricos relativos à sedimentação dos *cookies* na web, bem como de dados indiretos sobre a sua realidade empírica atual e de suas implicações ao controle dos dados pessoais e aos princípios da LGPD.

Com relação ao marco teórico, primeiramente é necessário elucidar como ele contribui para a interpretação dos objetos de pesquisa. Segundo Lessig (2006, p. 122-130), convivendo em sociedade os seres humanos são influenciados e limitados pela atuação de quatro forças centrais: a lei, as normas sociais, o mercado e a arquitetura. A esfera *legal* diz respeito aos regulamentos, tanto internos quanto externos, positivados por Estados e por particulares. As *normas sociais* expressam costumes e convenções humanas fixadas graças aos hábitos adotados e reiterados com o decorrer do tempo. A dimensão do *mercado* caracteriza a relação dos mecanismos de preço, organização, oferta e procura de bens e serviços. Por fim, a esfera da *arquitetura* se refere aos elementos estruturais que compõem os ambientes físico e virtual.

A escolha desse marco teórico se justifica pelo potencial de compreensão multidisciplinar dos fenômenos complexos da sociedade da informação, como a proteção de dados pessoais e os *cookies* de navegador. Tal como expõem os parágrafos a seguir, as dimensões da lei, das normas sociais, do mercado e da arquitetura estão interligadas e em constante transformação. Assim, a análise das particularidades de uma camada não exclui sua relação com as demais.

Iniciando a análise pela esfera da arquitetura, é possível constatar maneiras pelas quais os dados pessoais são coletados em ambientes informatizados e como os *cookies* de navegador, entre outras tecnologias, operam nesse contexto. Castelluccia (2012, p. 23) explica que no mundo virtual o processo de rastreamento (*tracking)* de dados pessoais ocorre de três formas, que podem estar interligadas: *(i)* pela própria web (*web tracking*), (ii) pela localização (*location tracking*) ou (iii) pelas redes sociais (*social tracking*).

O rastreio de dados pessoais do internauta pelas *redes sociais* acontece em serviços cujo requisito de funcionamento é o fornecimento de uma série de informações do usuário. Essas informações, como nome, documento e hábitos, são compartilhadas via navegadores ou aplicativos de celulares, e disponibilizadas para outras pessoas e empresas. O rastreio por *localização* é potencializado com a redução de custos e melhoria no desempenho de dispositivos, como GPSs, sensores, cartões de acesso ou câmeras, os quais transmitem com precisão informações relacionadas ao deslocamento das pessoas. Por fim, o rastreio pela *web* pode ocorrer graças a um conjunto de expedientes tecnológicos de alta complexidade, como aplicações de *javascript,* técnicas de *browser fingerprinting* e os *cookies* de navegador (CASTELLUCCIA, 2012, p. 25-9).

Javascript é uma linguagem dinâmica de programação, cuja execução é altamente funcional. Seu uso para fins potencialmente ofensivos é limitado, mas pode acontecer pela exploração de seu atributo dinâmico, capaz de executar certos conteúdos online e depositar arquivos no navegador com o objetivo de extrair informações do histórico ou contas associadas dos usuários. Já a técnica de *browser fingerprinting* significa literalmente a "impressão digital" do navegador. Tal artifício compreende a associação de parâmetros únicos de determinado navegador – como resolução de tela, usuário logado, número de IP[3] etc. –, de forma que o utilizador possa ser identificado plena ou parcialmente durante a navegação, mesmo sem a ajuda de tecnologias rastreadoras adicionais (CASTELLUCCIA, 2012, p. 24-5).

Os cookies, por sua vez, são arquivos de texto codificados. Estes arquivos são comumente depositados no computador do usuário pela página acessada e permitem a identificação desse internauta para facilitar o funcionamento do site e/ou o monitoramento a da navegação. Os cookies podem pertencer à própria página visitada ou a outras entidades (cookies de terceiros), além de serem temporariamente apagáveis (cookies de sessão) ou persistentes (cookies permanentes) (CASTELLUCCIA, 2012, p. 23-4).

O usuário pode, em tese, gerenciar e bloquear os *cookies*. Porém, Castelluccia (2012, p. 23-4) alerta que existem alguns tipos cuja gestão é complexa, são os chamados *supercookies* e os *evercookies*. Os *supercookies* funcionam graças a elementos adicionais dos navegadores (*plug-ins*) e

[3] *Internet Protocol* é uma estandardização técnica de rede que atribui um número de identificação ao computador no acesso e comunicação a outras máquinas. De forma análoga, o protocolo de rede funciona como uma espécie de endereço, permitindo o encaminhamento de pacotes de dados na transmissão de informações pela rede (LESSIG, 2006, p. 43).

conseguem gerenciar os dados dos usuários de modo a contornar o controle humano sobre o que é ou não deletado. Já os *evercookies* são capazes de manipular técnicas de armazenamento das aplicações de navegação (como o armazenamento temporário de informações – *cache*) para permanecerem no computador do usuário, mesmo após serem deletados.

Ainda no debate sobre as formas de obtenção de informações pessoais dos internautas por empresas, governos ou terceiros, cabe acrescentar algumas classificações. Ao discorrer sobre técnicas de extração e análise de dados pessoais, Abrams (2014, p. 6-8) estabelece uma taxonomia pautada em quatro modelos: os dados providos, os observados, os derivados e os inferidos.

Dados providos são aqueles fornecidos pelo indivíduo para iniciar e completar transações em ambientes negociais ou então para se expressar em redes sociais, como os cadastros de consumo e atualizações de status online. Dados observados representam registros de ações humanas, geralmente com o auxílio de mídias, a exemplo dos já mencionados cookies de navegador que gravam padrões de navegação, sensores digitais que captam expressões humanas ou câmeras que registram imagens e sons de locais públicos e privados. Já os dados derivados são aqueles frutos de transformação por processos aritméticos e de agrupamento, como a classificação de clientes, por empresas, em perfis específicos de consumo. Por fim, os dados inferidos são os que passam por um processo mais refinado de análise, como a probabilidade do consumidor se tornar inadimplente ou contrair uma doença, graças ao exame detalhado de suas informações de crédito e consumo, bem como os dados sobre sua saúde (ABRAMS, 2014, p. 06-8).

O que Castelluccia (2012) e Abrams (2014) demonstram é que a camada da arquitetura, formada por códigos de softwares, protocolos e dispositivos, interfere diretamente na captação e no uso dos dados pessoais na rede. As implicações para a privacidade e o controle do usuário sobre os seus dados são diretas, uma vez que esses conjuntos de códigos podem ser manipulados conforme os interesses de seus desenvolvedores.

Como ressaltado anteriormente, a camada da arquitetura não interfere de forma autônoma no modo como o ser humano interage na internet. Por isso, é necessário dar sequência à explicação das camadas do mercado, das normas sociais e da lei, para compreender o fenômeno de uma maneira mais integrada.

No que diz respeito à esfera do mercado, é preciso compreender como os indicadores negociais de grandes empresas do setor de tecnologia enxergam a relação dos dados pessoais com as tecnologias de monitoramento. Desse modo, o relatório desenvolvido pelo *MIT Techonolgy Review Custom* (2016, p; 01; 04) foi consultado tendo em vista seu potencial agregado de avaliação da relação entre dados pessoais e empresas no setor de tecnologia. A principal constatação do estudo é a de que esses dados adquiriram status de ativos intangíveis, tornando-se estratégicos para os negócios no setor. Assim, empresas como *Google*, *Amazon*, *Uber* e *Netflix* possuem nos dados de seus clientes o principal ativo de sua atividade empresarial.

De acordo com o relatório, três elementos-chave auxiliam a compreensão sobre como o "capital de dados" funciona: atividade; impulso autogenerativo e plataformas. Por *atividade* entende-se que os dados deixaram de ser um acessório e agora compõem a base da organização de produtos e serviços de muitas empresas. Basta imaginar que as opções de sensores hoje à disposição das empresas de tecnologia (GPSs, câmeras, sistemas de rastreamento e contagem…) viabiliza a sua sobrevivência no mercado e a sua diferenciação frente aos concorrentes. O *impulso autogenerativo* significa que dados geram mais dados. Uma vez organizada a atividade a patir de dados pessoais, os segredos e aprendizados exclusivos daquele empreendimento fomentam o seu aperfeiçoamento contínuo e o seu destaque concorrencial. Por fim, as chamadas *plataformas* ganham cada vez mais destaque nesse cenário, porque concentram pessoas e empresas, reduzindo custos e facilitando a ocorrência das transações negociais (MIT TECHNOLOGY REVIEW CUSTOM, 2016, p. 05).

Nesta roda viva tecnológica dos dados pessoais, tecnologias cada vez mais invasivas são utilizadas para extrair e analisar padrões de comportamentos online e estas informações passam a constituir a base de diversas atividades empresariais. "Não existe almoço grátis" é um ditado bem pertinente quando o assunto é coleta e utilização de dados pessoais. As empresas do setor tecnológico se especializam cada vez mais para fornecer produtos aparentemente gratuitos ao usuário, cujo "preço" embutido é o da coleta, refinamento e até venda de seus dados estrategicamente.

Ainda na esfera de mercado, cabe relevar um elo poderoso de ligação entre os dados pessoais coletados na rede e empresas do ramo de tecnologia: o mercado crescente de publicidade digital. Segundo Castelluccia (2012, p. 22), esse mercado é composto por três tipos de agentes responsáveis por

tornar dinâmico o fluxo de dados pessoais nos anúncios: o anunciante, o veiculante e o agenciador. O anunciante (*advertiser*) tem seu produto, serviço ou marca exposto em páginas e aplicativos de terceiros (*publisher*), responsáveis por veicularem determinada mídia. A negociação entre ambos é feita muitas vezes por uma agência (*adnetwork*), que é responsável por coletar e posicionar os anúncios, e recebe uma contrapartida financeira baseada geralmente no número de *clicks* que o anúncio recebeu.

É possível afirmar que esse modelo publicitário na rede pode ser lesivo ao usuário? De acordo com Calo (2014, p. 1025-1034), a resposta é positiva. Para o autor, a utilização de dados pessoais para oferta de produtos e serviços pode ser danosa em três aspectos: (i) danos econômicos, pois dados pessoais podem servir como instrumentos para a discriminação de preços contra usuários, segundo indicadores geográficos e financeiros; (ii) danos de privacidade, onde dados pessoais íntimos podem ser trocados livremente na rede para os mais variados fins, sem que o usuário consiga estabelecer o efetivo controle sobre os mesmos e (iii) danos à autonomia, porque o banco de dados sobre determinada pessoa pode ser tão apurado a ponto de induzir comportamentos e impulsionar preferências e necessidades artificiais de consumo.

Observa-se, assim, um conjunto de tecnologias, empresas e agentes voltados para a coleta, utilização e intermediação de dados pessoais, cujo resultado é a criação de bases de perfis muito complexas e precisas. A essa altura, vale questionar: e a sociedade? Como os usuários comuns percebem a relação entre novidades tecnológicas e a exposição de dados pessoais na rede?

Duas pesquisas podem auxiliar a compreensão do relacionamento que os cidadãos brasileiros possuem com os avanços tecnológicos. A pesquisa desenvolvida por Silva (2015, p. 60-1), e cuja amostra é de 1.104 (mil cento e quatro) questionários de brasileiros de diversas regiões, faixas salariais e educacionais, demonstrou um altíssimo grau de preocupação com a privacidade dos dados bancários (senhas, números de cartão de crédito e conta corrente, saldo e histórico de consumo) na internet.

Em contrapartida, a mesma investigação revelou um grau consideravelmente menor de preocupação com dados relacionados à sexualidade, vícios, data de nascimento e informações escolares dos participantes. O estudo também constatou que indivíduos com maior poder aquisitivo se preocupam mais com a segurança de suas informações pessoais (SILVA, 2015, p. 61; 78-9).

O trabalho de Silva (2015), embora não-probabilístico, fornece alguns indícios acerca da percepção do usuário brasileiro sobre seus dados o plano virtual. Os resultados são complementados e a análise se torna mais rica na medida em que adicionamos outra pesquisa, de cunho probabilístico, divulgada ao término de 2016 pelo Datafolha (2016, p. 10). De acordo com o levantamento, cerca de 61% (sessenta e um por cento) dos brasileiros acessavam a internet regularmente por computadores, enquanto expressivos 92% (noventa e dois por cento) também o faziam por *smartphones*.

Dos usuários de *smartphones*, a pesquisa averiguou ainda que o aplicativo de mensagens privadas *WhatsApp* era utilizado por cerca de 92% (noventa e dois por cento) dos entrevistados. Segurança, privacidade e utilidade eram os fatores considerados como muito importantes e determinantes para o alto índice de utilização desse aplicativo de mensagens. Entretanto, no que diz respeito aos dados pessoais dos usuários, o mesmo estudo revelou que cerca de 79% (setenta e nove por cento) dos brasileiros não teria maiores problemas em ceder seus dados em troca de benefícios de conveniência, como a oferta de produtos mais personalizados no *Facebook*[4] (DATAFOLHA, 2016).

Embora não tenham sido encontrados levantamentos empíricos sobre a relação entre o usuário brasileiro e os *cookies* de navegador, os estudos de Silva (2015) e do Datafolha (2016) sugerem uma percepção utilitarista e patrimonialista do brasileiro em relação aos seus dados pessoais, sem a consciência da importância da proteção de dados sensíveis, como sexualidade, opinião política, religiosa ou hábitos pessoais.

Exploradas as camadas da arquitetura, do mercado e da sociedade, avalia-se, finalmente, a dimensão legal também exposta por Lessig (2006). O propósito é compreender como a esfera do direito interfere no regime dos dados pessoais e se é possível observar alguma regulamentação relevante acerca dos *cookies* de navegador em âmbito nacional ou internacional.

O debate jurídico acerca dos dados pessoais envolve os chamados direitos de personalidade, sobretudo o direito à privacidade. O trabalho dos juristas Samuel Warren e Louis Brandeis (1890, p. 195-6), intitulado "Direito à Privacidade" e publicado na *Harvard Law Review*, foi de

[4] O *WhatsApp* foi comprado pelo *Facebook*. Quando perguntados se concordariam em ceder informações pessoais de sua conta do *WhatsApp* para aquela rede social, 79% (setenta e nove por cento) dos entrevistados responderam, sem resistência, que cederiam seus dados em troca de uma oferta mais personalizada de produtos no *Facebook*. A pesquisa tem grau de confiança de 95% (noventa e cinco por cento) e incluiu 2.363 (duas mil, trezentas e sessenta e três) entrevistas realizadas em mais de 130 (cento e trinta) municípios brasileiros (DATAFOLHA, 2016, p. 20-4).

extrema importância para a história sedimentação desse direito. No artigo, os autores defendem a ideia de um "direito a ser deixado só" – expressão creditada ao magistrado estadunidense Thomas Cooley, em escrito datado de 1879 – e revelam preocupações com a intromissão da imprensa e de novas tecnologias, como as câmeras fotográficas, na vida privada.

Para Glancy, (1979, p. 4-6), a publicação do artigo foi contextualizada por diversos motivos, entre eles: o incômodo pessoal de Warren, membro da elite de Boston e casado com a filha de um Senador, acerca da exposição de sua família na imprensa local, considerada por ele como sensacionalista; a divulgação do nome da firma, Warren & Brandeis, recém-criada pelos dois advogados na assinatura do artigo; o aumento dos índices demográficos do país e o progresso tecnológico materializado pelas invenções, como as câmeras e o telefone, que incrementavam o debate a favor da proteção da vida privada.

Nesse sentido, Rodotà (2008, p. 26), afirma que a privacidade nasce eminentemente como um direito de isolamento da classe burguesa. Segundo Souza (2000, p. 37), com o decorrer das transformações tecnológicas e o fluxo constante dos dados pessoais, a proteção à privacidade deixou de ter contornos unicamente negativos e passou a se configurar a partir de um prisma positivo, fundado na busca de autodeterminação informativa dos dados. O autor ressalta a necessidade de conciliar o progresso tecnológico e o direito fundamental à privacidade.

De acordo com Doneda (2011, p. 96-8) e Mayer-Schönberger (1997, p. 221-35), embora as leis de proteção de dados estejam historicamente associadas ao direito à privacidade, é possível elencar quatro "gerações" de leis internacionais sobre o tema. A primeira, caracterizada a partir dos modelos legais de países como Áustria, Alemanha e Suécia ao longo da década de 70, foi marcada por disposições rígidas de ordem computacional e técnica destinadas aos recém-difundidos bancos de dados e à preocupação com o poder centralizado dos governos sobre os dados pessoais. Ao final da mesma década, os padrões legislativos da França, Dinamarca e Áustria apresentaram versões legislativas consideradas de segunda geração, nas quais a preocupação central passou a ser a descentralização do poder computacional e a criação de mecanismos rudimentares de correção e controle dos dados.

Nos anos 80, Alemanha, Áustria e Finlândia modificaram seus padrões normativos viabilizando a autodeterminação informativa, ainda custosa e de baixa acessibilidade às camadas mais populares. Por fim, a quarta

geração legislativa teve como ápice a Diretiva 95/46 do Conselho Europeu, em 1995. O alicerce dessa norma foi oreconhecimento da capacidade de barganha dos indivíduos junto às entidades que fazem o tratamento de dados pessoais e a proteção mandatória e coletiva contra o uso de certas categorias de dados, considerados mais sensíveis. É importante destacar que essas características continuam mudando e novas categorias geracionais de leis podem ser observadas e agrupadas às anteriores (DONEDA, 2011, p. 96-8; MAYER-SCHÖNBERGER, 1997, p. 221-35).

Com relação ao Brasil, Doneda (2011, p. 103-6) afirma que a Constituição Federal de 1988 trouxe uma preocupação fragmentada com a proteção à esfera individual, dividida em temas como a vida privada e o sigilo de informações pessoais. Segundo o autor, os paradigmas do texto constitucional – como grampos telefônicos, interceptações ou escutas de mensagens – foram ultrapassados, pois perderam a atenção para as novas tecnologias virtuais de comunicação. Desse modo, o autor defende a importância do reconhecimento autônomo do direito à proteção dos dados pessoais em relação ao direito à privacidade.

Tal reconhecimento autônomo pode ser considerado como atendido pela ordem legal brasileira. No âmbito constitucional, a Proposta de Emenda à Constituição 17/2019, elaborada pelo Senador Eduardo Gomes (MDB-TO) e aprovada no Senado em dois turnos, celebra, sob a ótica do parlamentar, o aprofundamento da defesa à intimidade no plano constitucional (BRASIL, 2019). Ademais, no plano infraconstitucional, após anos de intenso debate e três projetos de lei com tramitação concomitante, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/18 foi aprovada. Com as alterações introduzidas pela Medida Provisória 869, de 27 de dezembro de 2018, essa lei entrará em vigor em agosto de 2020 (BRASIL, 2018).

A LGPD possui muitos pontos que merecem maior reflexão acadêmica. Todavia, adequando a análise dessa lei para o escopo do presente artigo, serão apresentados e trabalhados apenas os princípios expostos nos incisos do artigo 6º da LGPD, essenciais para a próxima seção deste trabalho.

Ao lado da boa-fé objetiva, são dez os princípios previstos no artigo 6º da LGPD que devem guiar o tratamento ou a manipulação de dados pessoais por parte de empresas ou governos, quais sejam: (i) finalidade, (ii) adequação, (iii) necessidade, (iv) livre acesso, (v) qualidade dos dados, (vi) transparência, (vii) segurança, (viii) prevenção, (ix) não discriminação

e (x) prestação de contas (BRASIL, 2018). Esses princípios são abordados a seguir, divididos em três grupos: princípios com foco na aspiração do tratamento de dados pessoais (art. 6º, I; II; III e IX), no relacionamento com o cliente (art. 6º, IV; VI e V) e nas entidades que gerem estes dados (art. 6º, VII; VIII e X) (BRASIL, 2018).

O grupo ligado à aspiração do tratamento[5] é composto por quatro princípios que funcionam como espécies de guias ou anseios para o manejo dos dados. Primeiramente, deve haver uma *finalidade*, um propósito delimitado, legítimo, explícito e informado ao titular dos dados para a coleta e uso dos mesmos. Em conjunto, é preciso que haja *adequação* a posteriori deste tratamento com o propósito informado, sendo que os dados utilizados devem atender à *necessidade* desta finalidade, isto é, não serem desmoderados para o fim acordado. Ainda neste grupo, é preciso que o tratamento respeite princípios éticos e possua caráter *não discriminativo* contra o titular dos dados (BRASIL, 2018). A junção desses quatro princípios viabiliza uma primeira medida direcionadora para os fluxos de coleta, armazenamento e emprego de dados pessoais por entidades públicas e privadas elencadas na lei.

No grupo seguinte, focado no relacionamento com o titular dos dados pessoais[6], encontra-se o princípio do *livre acesso*, tanto ao estádio de desenvolvimento do tratamento, quanto ao manejo dos dados. É necessária, ainda, a *transparência*, para assegurar de forma inteligível e cristalina

[5] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (BRASIL, 2018).

[6] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (BRASIL, 2018).

ao titular o status das informações que lhe digam respeito e estejam em posse de terceiros. Deve-se, também, garantir a *qualidade* desses dados no sentido de que os mesmos expressem informações precisas e sujeitas a atualização por demanda, respeitado o propósito original de uso (BRASIL, 2018). Esse segundo rol de princípios permite regulamentar a coleta, o armazenamento e o emprego de dados para além do momento inicial de sua extração, com foco no relacionamento com os titulares.

Por fim, no último grupo de princípios[7], vislumbram-se aqueles cujo objetivo é regular as entidades que operam o tratamento de dados. Aqui, é necessário certificar que os dados em tratamento possuam espécies de travas de *segurança* contra situações inusitadas de perda ou ataque, sejam processados com técnicas *preventivas* contra danos aos titulares e, por fim, sujeitem o agente de tratamento a uma *responsabilização* em harmonia com o compromisso assumido para o tratamento de dados (BRASIL, 2018). Esses são parâmetros de defesa da coletividade contra os riscos da atividade de tratamento.

Da análise desses dez princípios, é possível notar que a legislação brasileira privilegia situações de controle dos dados pessoais para além do momento de sua transmissão. Nota-se, pois, a dimensão autodeterminativa dos dados em sua concepção mais moderna, sujeitos ao controle tanto na esfera individual quanto coletiva.

Com relação aos *cookies*, o ordenamento jurídico nacional não possui previsão específica e expressa para regulá-los. Entretanto, eles estarão futuramente sujeitos às disposições gerais da LGPD. Interessa, nesse momento, uma menção à União Europeia, que lançou mão de duas importantes Diretivas tendo expressamente a preocupação com os *cookies* de navegador: a Diretiva 2002/58/CE e a sua subsequente Diretiva 2009/136/CE.

[7] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

Na Diretiva 2002/58/CE, mais especificamente à consideração nº 25[8] de seu preâmbulo, é possível observar que os *cookies* são considerados legítimos para fins de coleta de informações de funcionamento de um site ou para facilitar a publicidade. A consideração ressalta a importância do dever de fornecimento claro e preciso de informações acerca do *cookie*, sobretudo quanto aos seus propósitos e ao seu armazenamento no computador do usuário. Destaca ainda que tais informações devem ser fornecidas de maneira acessível e amigável e deixa aberta a prerrogativa para que o site condicione a navegação à aceitação do *cookie*, desde que para fins legítimos (UNIÃO EUROPEIA, 2002).

[8] Todavia, esses dispositivos, por exemplo os denominados testemunhos de conexão («cookies»), podem ser um instrumento legítimo e útil, nomeadamente na análise da eficácia da concepção e publicidade do sítio web, e para verificar a identidade dos utilizadores que procedem a transacções em linha. Sempre que esses dispositivos, por exemplo os testemunhos de conexão («cookies»), se destinem a um fim legítimo, como por exemplo a facilitar a prestação de serviços de informação, a sua utilização deverá ser autorizada, na condição de que sejam fornecidas aos utilizadores informações claras e precisas, em conformidade com a Directiva 95/46/CE, acerca da finalidade dos testemunhos de conexão («cookies») ou dos dispositivos análogos por forma a assegurar que os utilizadores tenham conhecimento das informações colocadas no equipamento terminal que utilizam. Os utilizadores deveriam ter a oportunidade de recusarem que um testemunho de conexão («cookie») ou um dispositivo análogo seja armazenado no seu equipamento terminal. Tal é particularmente importante nos casos em que outros utilizadores para além do próprio têm acesso ao equipamento terminal e, consequentemente, a quaisquer dados que contenham informações sensíveis sobre a privacidade armazenadas no referido equipamento. A informação e o direito a recusar poderão ser propostos uma vez em relação aos diversos dispositivos a instalar no equipamento terminal do utente durante a mesma ligação e deverá também contemplar quaisquer outras futuras utilizações do dispositivo durante posteriores ligações. As modalidades para prestar as informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão conviviais quanto possível. O acesso ao conteúdo de um sítio web específico pode ainda depender da aceitação, com conhecimento de causa, de um testemunho de conexão («cookie») ou dispositivo análogo, caso seja utilizado para um fim legítimo (UNIÃO EUROPEIA, 2002).

Por sua vez, a Diretiva 2009/136/CE[9] alerta para a utilização dos *cookies*, inclusive de terceiros, para fins lícitos ou ilícitos. Ressalta também a importância do fornecimento de informações claras e precisas por parte do site para que o usuário possa avaliar e permitir o armazenamento ou o acesso avançado aos seus dados (UNIÃO EUROPEIA, 2009).

Além disso, a diretiva é favorável à exibição de avisos amigáveis e acessíveis durante o ato de navegação. Ela estabelece, contudo, uma exceção ao direito de informação e de escolha do titular dos dados nos casos em que exista uma justificativa técnica estritamente necessária para o emprego de *cookies* ou ferramentas similares. Há, ainda, a possibilidade de que o internauta fixe suas preferências de uso dos dados pelas configurações do navegador e a menção ao papel das autoridades nacionais para a proteção coletiva e individual de dados pessoais (UNIÃO EUROPEIA, 2009).

De acordo com Degeling *et al.* (2018, p. 12-4), as disposições europeias trouxeram o benefício global de promoção das discussões e práticas de proteção à privacidade na rede. Após a diretiva de 2009, os autores apontam uma difusão no uso de *banners* (janelas de aviso que surgem na tela após o acesso a um site) para informar sobre o depósito de *cookies* pelas páginas. Entretanto, criticam o fato de que, em termos práticos, as tecnologias de monitoramento não mudaram sua essência invasiva e as opções do usuário ainda são muito restritas: ao receberem inúmeros e distintos avisos acerca de *cookies* nos sites que acessam, eles são deixados à própria sorte e sem instruções claras acerca de como proceder para proteger seus dados pessoais.

[9] Terceiros podem desejar armazenar informações sobre o equipamento de um utilizador, ou ter acesso a informação já armazenada, para uma série de fins, que vão desde os legítimos [por exemplo, certos tipos de testemunhos de conexão («cookies»], até os que envolvem a intromissão indevida na esfera privada (por exemplo, software espião ou vírus). É, pois, de suma importância que sejam prestadas informações claras e exaustivas aos utilizadores, sempre que sejam encetadas actividades que possam resultar nesse tipo de armazenamento ou de possibilidade de acesso. As formas de prestação de dar informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão simples quanto possível. As excepções à obrigação de prestar informações e de permitir o direito de recusar deverão limitar-se às situações em que o armazenamento técnico ou o acesso é estritamente necessário para o objectivo legítimo de permitir a utilização de um serviço específico explicitamente solicitado pelo assinante ou utilizador. Sempre que tecnicamente possível e eficaz, e em conformidade com as disposições aplicáveis da Directiva 95/46/CE, o consentimento do utilizador relativamente ao tratamento de dados pode ser manifestado através do uso dos parâmetros adequados do programa de navegação ou de outra aplicação. O cumprimento destes requisitos deverá ser tornado mais eficaz através do reforço dos poderes concedidos às autoridades nacionais competentes (UNIÃO EUROPEIA, 2009).

No mesmo sentido, Tirteia *et al.* (2011, p. 12-3) expõem que ao acessar um site o internauta possui duas opções centrais: (i) tentar recusar os *cookies* e sofrer bloqueios de acesso pelo servidor ou (ii) aceitá-los e ficar exposto aos riscos de segurança e privacidade. Os autores defendem que caberá aos desenvolvedores de aplicações e de navegadores a consolidação de mecanismos mais eficientes para o controle dos dados pessoais. Contudo, alertam para os desafios trazidos por tecnologias como os *supercookies* e os *evercookies*, capazes de contornarem as preferências dos internautas.

Por fim, os *cookies* também aparecem expressamente no texto do Regulamento Geral Europeu de Dados Pessoais (GDPR), à consideração nº 30[10] do preâmbulo, citados como elementos potencializadores da identificação e do perfilamento de pessoas físicas (UNIÃO EUROPEIA, 2016). O regulamento poderá demandar futuras mudanças na Diretiva 2002/58/CE e, consequentemente, na Diretiva 2009/136/CE, com vistas à harmonização de suas disposições, especialmente com relação aos *cookies* de terceiros e aos usos publicitários de dados pessoais.

Desse modo, após avaliadas as dimensões legal, social, mercadológica e de arquitetura relativas ao objeto de pesquisa, na próxima seção aplica-se a perspectiva histórica para averiguar o fenômeno dos *cookies* e sua relação com a proteção de dados pessoais. Entre as fontes consultadas, destacam-se três obras que registram a história de atores essenciais para o desenvolvimento da web e dos *cookies*: *Tim Berners-Lee*, *David Kristol* e *Lou Mountulli*.

2 ELEMENTOS DA ANÁLISE: PERSPECTIVA HISTÓRICA DOS *COOKIES* DE NAVEGADOR, A LGPD E OS DESAFIOS À PROTEÇÃO DE DADOS NA REDE

Apresentadas as matrizes metodológicas e teóricas, esta seção tem por intuito averiguar narrativas de importantes atores envolvidos no desenvolvimento da internet e dos *cookies* de navegador. O propósito não é estabelecer uma linha do tempo evolutiva e determinista da internet, na

[10] As pessoas singulares podem ser associadas a identificadores por via eletrônica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão (*cookie*) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares (UNIÃO EUROPEIA, 2016).

qual exista um ponto de chegada utilitarista para sustentar determinado conceito jurídico. Embora seja necessária a utilização de marcos temporais e de narrativas históricas, o objetivo é analisar criticamente aspectos fundamentais sobre o funcionamento da internet, dos *cookies* e sua conexão com o direito à proteção de dados pessoais.

Os *cookies* de navegador surgiram no ano de 1994. Antes disso, contudo, três dos grandes desafios técnicos para o mundo interconectado já haviam sido solucionados: a exteriorização do conceito de hipertexto, em 1965; a implementação da internet, em 1969; e a criação da *world wide web*, em 1990.

A ideia do hipertexto, publicada por Theodor Nelson (1965, p. 96), tinha como propósito criar uma forma de texto cuja leitura não seguiria um caminho predeterminado. Nessa forma de texto não sequencial, o usuário de um sistema informático conseguiria desenvolver sequências associativas de informações por meio de links, sem necessariamente observar uma ordem fixa.

A internet, por sua vez, surge em um contexto de Guerra Fria, marcado pela forte busca por avanços tecnológicos estratégicos. Como explicam Leiner *et al.* (2009, p. 23-4), esforços militares e de pesquisa, financiados pela agência norteamericana *Advanced Research Projects Agency*, ARPA, tinham como propósito a criação de uma arquitetura aberta de comunicação em rede (*open-architecture networking*), capaz de conectar dispositivos com diferentes configurações. De acordo com os autores, ao término de 1969, quatro pontos iniciais de comunicação em rede, ou *nós*, já haviam sido integrados: Universidade da Califórnia em Los Angeles (UCLA), Instituto de Pesquisa de Standford (SRI), Universidade da Califórnia em Santa Bárbara (UCSB) e Universidade de Utah.

Em torno de 1973, os pesquisadores Robert Kahn e Vincent Cerf se uniram para desenvolver a suíte básica de protocolos da internet, o conjunto TCP/IP (respectivamente, *Protocolo de Controle de Transmissão* e *Protocolo de Internet*). Enquanto o protocolo TCP viabilizaria eficientemente o controle de fluxo e recuperação de pacotes de dados transmitidos pela rede, o IP permitiria um esquema de direcionamento e endereçamento destes pacotes aos dispositivos corretos (LEINER *et al.*, 2009, p. 25).

Mesmo com o progresso da tecnologia, é só no ano de 1990 que as funcionalidades do hipertexto e da internet são integradas de forma única para criar a *world wide web*. Tim Berners-Lee, físico da Organização Europeia para Pesquisa Nuclear, CERN, desenvolveu um conjunto de

protocolos integrados, ou regras procedimentais e uniformizadas, capazes de traduzir a comunicação entre computadores com sistemas totalmente diferentes. Com o auxílio do colega belga Robert Calliau, Berners-Lee implementou e uniformizou protocolos como o *Identificador de Recursos Universal* (URI), o *Protocolo de Transferência de Hipertexto* (HTTP) e a *Linguagem de Marcação de Hiptertexto* (HTML), essenciais para o uso da web contemporânea por sua flexibilidade e interoperabilidade. Associados, esses protocolos são responsáveis, respectivamente, por: (i) criar um sistema nominal e universal de identificação de páginas, (ii) traduzir as solicitações e respostas entre um computador (*client*) e um servidor de conteúdo online (*server*) e (iii) exibir essas informações de forma gráfica e ordenada (BERNERS-LEE, 1999, p. 33-9).

Berners-Lee criou uma série orientada de instruções que permitiu a qualquer pessoa com um microcomputador, sistema operacional e uma conexão buscar informações online de forma sistematizada por meio de links, unificando o acesso aos conteúdos na web. Entretanto, para viabilizar a transmissão de informações de forma eficiente, rápida e universal, foi necessário disseminar programas especializados em estabelecer a comunicação entre o computador e a rede, chamados de navegadores. Como Berners-Lee e Calliau estavam envolvidos na popularização e na adaptação de parâmetros para o uso da web, eles incentivaram fortemente a criação de navegadores por outros pesquisadores e empresas (BERNERS-LEE, 1999, p. 55-6).

Em 1994, a expansão da web contabilizava mais de 200 (duzentos) servidores de conteúdo no formato *HTTP* e muitos projetos de navegadores (*web browsers*), como o *Erwise*, *Viola*, *Midas*, *Lynx*, *Cello*, *Navipress* e *Netscape*. No ano seguinte, o sistema operacional *Windows 95* foi lançado com um navegador nativo desenvolvido a pedido da própria Microsoft, o Internet Explorer (BERNERS-LEE, 1999, p. 67-82). Todavia, um problema continuava sem solução: a comunicação entre um computador e um provedor de conteúdo seguia desprovida de "memória", ou seja, o internauta e a página acessada jamais poderiam manter vínculos das sessões anteriores.

De acordo com Kristol (2001, p. 152-4), a comunicação entre um cliente e um servidor, ou página *HTTP*, é baseada na ordem requisição-resposta, formada por dois atributos centrais: a comunicação fica sem conexão (*connectionless*) e o sem estado (*stateless*) até a resposta ser obtida. Isso significa que, no intervalo entre a requisição e a resposta, a conexão entre o servidor e o cliente é desenhada apenas

temporariamente, sem que ambos mantenham um vínculo ou registro para futuras trocas de informações.

Como solução ao problema, o então funcionário da *Netscape*, Lou Montulli, desenvolveu os chamados "*cookies*" de navegador e disseminou as especificações para a sua adoção por outros navegadores e páginas. Desse modo, os *cookies* são responsáveis por manter a comunicação entre cliente e servidor e identificar de forma contínua um usuário enquanto ele navega por uma página na web (KRISTOL, 2001, p. 152-4).

Além de solucionarem um problema complexo de ordem técnica, os *cookies* também resolveram um anseio de mercado e fomentaram os primeiros debates públicos sobre a privacidade e a proteção de dados na internet. Segundo Montulli (2013a), entre 1996 e 1997 a web cresceu de forma exponencial e o modelo de negócio online predominante era o de oferta de conteúdo gratuito mediante a exibição de anúncios. À época, a utilização dos *cookies*, sobretudo por terceiros, expandiu-se profundamente para fins de rastreamento e publicidade na rede, viabilizando a promoção de anunciantes que não eram os administradores das páginas acessadas, chamados *cookies* de terceiros (*thirdy-party cookies*). Como o próprio Montulli (2013a) explica, grandes empresas começaram a utilizar esses *cookies* de terceiros para certificar que seus anúncios não iriam se repetir conforme o usuário navegava por páginas diferentes na rede. Também foi possível a personalização dos anúncios, conforme o perfil e o histórico de navegação do usuário.

Ainda sobre os *cookies* de terceiros, David Kristol (2001, p.159-64) relata o seu processo de normatização técnica e a difícil decisão de padronizar, ou não, o seu bloqueio por navegadores. Ele descreve os impasses no debate que se seguiu na *Força Tarefa de Engenharia na Internet* (IETF), organização aberta formada por engenheiros e pesquisadores responsável pela discussão dos parâmetros envolvidos com a rede. A organização trabalhava com um formato de discussões abertas, divididas em grupos de trabalho, visando a uniformização de vários protocolos e soluções cibernéticas. O resumo dessas discussões e soluções era publicizado por meio de documentos, chamados Solicitações de Comentários ou RFCs (*Request for Comments*).

Segundo Kristol (2001, p. 159-64), as controvérsias em torno dos *cookies* fomentaram a redação da RFC 2109/1997 e da RFC 2965/2000, nas quais ele e Montulli estiveram diretamente envolvidos. O autor explica que os *cookies* de terceiro viabilizam o rastreamento e a formação de bases

de perfis mais completos, pois não se originam de uma única página, mas do conjunto de várias delas. Além disso, com o *cookie* de terceiro, a oferta de anúncios é mais eficaz, uma vez que o internauta é "surpreendido" por um produto ou serviço inserido em uma página distinta da qual ele está acessando, processo capaz de captar a sua atenção de forma mais eficiente.

Kristol (2001, p. 161) sintetiza a experiência ao definir a discussão sobre permitir ou rejeitar os *cookies* de terceiros, como, provavelmente, o primeiro grande debate técnico com repercussões políticas na IETF. Ele comenta a decisão final – tomada no sentido de não bloquear os *cookies* de terceiro por padrão – recordando a batalha entre *Microsoft* e *Netscape* pelo domínio do mercado de navegadores à época, com as seguintes palavras:

> Empresas responsáveis pelo desenvolvimento de navegadores mostraram, por meio de suas ações, que não visavam desabilitar, por padrão, os *cookies* de terceiro. Na minha opinião, a escolha não era novidade. Àquele tempo, *Microsoft* e *Netscape* estavam fornecendo seus navegadores de graça ao público com vistas a tentar dominar o mercado de navegadores e, concomitantemente, ofereciam seus servidores pagos a outras empresas, então ambas estavam inclinadas a prestar mais atenção nos clientes remunerados e não nas pessoas que usavam os navegadores de graça. Aqueles que pagavam queriam a publicidade, desejavam usar redes de publicidade e as redes de publicidade, por sua vez, desejavam usar publicidade direcionada. A publicidade direcionada era mais fácil de ser implementada por meio dos *cookies* de terceiros, e seria improvável que os desenvolvedores de navegadores e servidores seriam capazes de desagradar seus clientes remunerados optando por desabilitar *cookies* de terceiro[11].

Sua reflexão é, portanto, de que fatores de mercado certamente tiveram forte influência na decisão final de regulamentação técnica dos *cookies* de terceiro. Pelo lado positivo, contudo, o autor ainda ressalta que

[11] Tradução livre de: "*The browser vendors showed, through their actions, that they were unwilling to change the third-party default to "off." In my opinion, that choice was hardly surprising. At a time when Microsoft and Netscape were giving away browsers to try to achieve market dominance, while at the same time selling servers, both vendors were most likely to heed their paying customers, not the people who got programs for free. And the people with the money wanted advertising, they wanted to use advertising networks, and most advertising networks wanted to be able to do targeted advertising. Targeted advertising was easiest to do using third-party cookies, and the server/browser vendors were unlikely to anger their paying customers by disabling third-party cookies.*" (KRISTOL, 2001, p. 169-170).

em conjunto, as RFCs levantaram o debate público acerca da privacidade na rede e tornaram usuários, imprensa e governo mais conscientes acerca do monitoramento online. O processo de discussão técnica e política das RFCs contribuiu para o surgimento de mecanismos de controle dos *cookies* e para a divulgação pioneira de políticas de privacidade em muitos sites (KRISTOL, 2001, p. 170).

Para Montulli (2013b), o modelo de negócios voltado para a publicidade online se estabeleceria de uma maneira ou de outra, sendo que a decisão de não bloquear os *cookies* de terceiro foi positiva no sentido de fixar parâmetros mínimos de controle e de transparência por parte dos usuários em relação a sites e anunciantes. A síntese do autor é de que "demônios conhecidos são melhores do que os que não se têm notícia" e que a busca por privacidade e por proteção de dados na rede precisa passar por um debate político e não apenas técnico.

Desenvolvido esse relato histórico, torna-se pertinente trazer algumas informações empíricas sobre a manifestação dos *cookies* na web contemporânea. Os relatos demonstraram a abertura de um caminho autorregulamentado e direcionado para a máxima exploração de dados pessoais. Observa-se, portanto, um modelo de negócios bem estruturado contra o qual objeções de privacidade não foram fortes o bastante para coibir a exploração ilimitada dos dados pessoais.

Hoofnagle (2012, p. 20-2) questiona o argumento da autodeterminação dos usuários perante a coleta de seus dados pessoais por *cookies* na web. O autor ressalta a dificuldade de fazer frente a visão utilitarista das empresas sobre as informações pessoais e às técnicas invasivas para obtenção dos mesmos. Dessa forma, afirma ser insustentável a ideia de autorregulamentação por parte das empresas de tecnologia.

O receio do autor possui evidência empírica[12]. Conforme estudo elaborado em 2009 por Soltani *et al.* (2009, p. 03-4), 54 (cinquenta e quatro) dos 100 (cem) sites mais acessados nos Estados Unidos utilizavam *cookies Flash*, um tipo de *cookie* mais invasivo, capaz de coletar informações mesmo com a utilização alternada de diferentes navegadores em um mesmo computador. Comparado aos *cookies* comuns, também chamados

[12] Acerca dos dados indiretos citados logo em sequência, cumpre ainda salientar que representam a principal limitação deste estudo, uma vez que se referem a estudos cujo recorte é o da internet norteamericana. Essa nuance não compromete, contudo, as considerações aqui reverberadas, visto como a publicidade online por meio dos *cookies* é um fenômeno global e, cada vez, mais a web se torna um ciberespaço integrado em torno de grandes corporações e páginas para as quais fronteiras de disseminação não existem.

de *HTTP*, os *cookies Flash* podem causar uma maior dificuldade de gerenciamento por parte do internauta.

Soltani *et al.* (2009, p. 03-4) constataram que os referidos 54 (cinquenta e quatro) sites depositaram um total de 281 (duzentos e oitenta e um) *cookies Flash*. Além disso, verificaram a ocorrência de uma prática chamada de reaparição (*respawning*), pela qual os valores coletados por um mesmo site pela via de *cookies HTTP e Flash* são replicados e redundantes. Desse modo, se o *cookie* do tipo *HTTP* for deletado pelo usuário, um *cookie Flash*, com informações pessoais idênticas, é utilizado para restaurar o status anterior de seu perfil.

Em um estudo sequencial a este, datado de 2011, Ayenson *et al.* (2011, p. 09-10; 16-8) relataram que a empresa *Adobe Systems*, responsável pela gestão e exploração comercial de arquivos com a extensão *Flash*, se diz ciente do uso de sua tecnologia de armazenamento local por parte de alguns sites, embora o classifique como "indevido". Os autores realizaram uma nova coleta empírica sobre o depósito de *cookies* e verificaram uma queda no uso dos *cookies Flash* entre os 100 (cem) sites mais populares nos Estados Unidos. Entretanto, observaram que algumas páginas populares (como o da rede de comunicação *Fox News*) ainda empregam a técnica de reaparição por meio do uso concomitante de *cookies* diferentes, como *HTTP*, *Flash* e um tipo mais recente, o *HTML5* (similar ao *HTTP*, mas com maior capacidade de armazenamento de informações).

Já em 2015, o levantamento similar de Altaweel *et al.* (2015, pp. 13-24) revelou um cenário de incremento e centralização nas técnicas de rastreamento. Das 100 (cem) principais páginas acessadas nos Estados Unidos, 83% (oitenta e três por cento) dos mais de 6 mil *cookies* encontrados eram provenientes de terceiros e, destes, 85 (oitenta e cinco) páginas apresentavam *cookies* concentrados na empresa Google. Além disso, os pesquisadores constataram que 5% (cinco por cento) das páginas utilizavam *cookies Flash*, de potencial manifestadamente mais invasivo.

Por fim, em um estudo empírico mais amplo, referente a 2015 e publicado no ano seguinte, Cahn e outros (2016, p. 893-900) acessaram os 100 (cem) mil sites mais populares dos Estados Unidos e observaram o depósito total de mais de 1 (um) milhão e 800 (oitocentos) mil *cookies,* dos quais um número superior a 1 milhão e 200 mil eram *cookies* de terceiros. O cenário deste tipo de *cookie* demonstra ainda uma maior concentração: apenas 1% (um por cento) das entidades que utilizam esta tecnologia de rastreamento em páginas alheias foram capazes de concentrar 75%

(setenta e cinco por cento) dos depósitos. Um outro dado a ser destacado na pesquisa é a segurança: apenas 0,36% (zero, vírgula trinta e seis por cento) dos *cookies* analisados possuem parâmetros de segurança estabelecidos (como o protocolo de segurança HTTPS, cujo 'S' é de *secure*, por emprega técnicas de cifragem para a proteção dos dados em trânsito). Este dado revela que a quase totalidade dos *cookies* analisados transmite dados online de forma vulnerável a ataques maliciosos[13].

Até o presente ponto, verificou-se que o cenário de sedimentação e desenvolvimento da internet é marcado por tecnologias de parâmetro – como protocolos e *cookies*, cujo design é originalmente aberto e influenciado fortemente por interesses de mercado –, com o predomínio do modelo negocial de oferta de conteúdo gratuito, patrocinado por publicidade. Historicamente, notou-se um esforço técnico para a estandardização de soluções tecnológicas cujas repercussões sociais e políticas são evidentes, como no caso dos *cookies* de navegador.

A última etapa do estudo consiste, portanto, em avaliar as diretrizes principiológicas expostas ao artigo 6° da Lei 13.709/18 frente aos dados indiretos e aos relatos trazidos neste capítulo, além de apresentar uma síntese de conclusões a partir do referencial teórico adotado. Vale lembrar que a análise ficará restrita aos princípios do artigo 6º, sendo que outros mecanismos de proteção expostos na LGPD deverão ser objeto de uma análise futura.

Antes de mais nada, faz-se pertinente dispor que o fato de muitas páginas e anunciantes, responsáveis por depositar *cookies*, estarem situados fora do país não afeta a jurisdição da lei brasileira. O artigo 3º da Lei 13.709/18 estabelece a sujeição às normas brasileiras de quaisquer empresas ou entidades cujas atividades de tratamento de dados (i) sejam realizadas no território nacional; (ii) tenham por objetivo oferecer serviços, bens ou tratar dados relativos a indivíduos localizados em território nacional ou (iii) tenham sido coletados em território nacional, independente da nacionalidade do agente de tratamento (BRASIL, 2018).

De forma condensada, as referências consultadas até aqui relataram a existência de quatro grandes fenômenos relacionados aos *cookies* de navegador e à proteção de dados pessoais na navegação online: (i) o intuito comercial de utilização de *cookies* para fins de propaganda e publicidade direcionada na rede; (ii) a predominância empírica de *cookies* de terceiro; (iii) a observância de técnicas pervasivas de monitoramento

[13] Nota: o estudo de Cahn e outros (2016) não leva em conta *cookies* depositados após logins em sites, o que poderia elevar o valor obtido para *cookies* com parâmetros seguros.

e rastreamento online, somada ao emprego de diferentes tecnologias de *cookies* para a coleta de dados idênticos e (iv) a ausência de técnicas seguras para transferência dos dados obtidos por meio dos *cookies* de navegador.

Com relação ao primeiro fenômeno, relatado historicamente por Berners-Lee (1999), Kristol (2001) e Montulli (2013a), vê-se que a expansão comercial da web passou pela utilização arquitetada dos *cookies* para fins de publicidade. Como também reforçam Calo (2014) e *MIT Technology Review* (2016), os dados pessoais coletados online se tornaram um ativo para as empresas de tecnologia e podem ser utilizados para fins de manipulação e predição de comportamentos de usuários/clientes.

É necessário alertar que não existe nenhuma vedação na lei brasileira para o simples fato do tratamento de dados ser realizado para fins comerciais. Entretanto, há de se observar que os dados pessoais coletados para fins de personalização de anúncios na rede podem ser subvertidos em táticas que ofendam o princípio da não-discriminação (artigo 6º, IV da Lei de Dados), sobretudo quando se tratam de dados sensíveis. Um exemplo trivial é o da utilização de ferramentas de monitoramento online para trocar informações acerca dos hábitos de saúde de pacientes com empresas prestadoras de serviço médico, de modo a classificar clientes em faixas de "risco" e tratá-los de forma discriminatória (RAVINDRANATH. 2019).

A análise do segundo fenômeno constatado, da massiva presença de *cookies* de terceiros em sites populares na web, foi relatada por Altaweel e outros (2015) e por Cahn e outros (2016). O *cookie* de terceiro, por si só, também não pode ser considerado ilícito no texto da lei nacional de dados.

Contudo, duas ponderações devem ser levadas mais afundo: do lado negativo, há de se considerar que, se os *cookies* de terceiro forem implementados sem a devida transparência, identificação de propósitos e de entidades envolvidas, terão o potencial de violar todas as provisões principiológicas do artigo 6º da Lei de Dados. Basta, para tanto, imaginar o impacto de uma empresa não identificada, hospedando *cookies* em sites de terceiros sem claros termos de serviço e ausente de provisões de prestação de contas e segurança. Nesse caso, tornar-se-ia praticamente impossível avaliar se os princípios envolvidos com a aspiração do tratamento, o relacionamento com o titular e a gestão dos dados pessoais estão sendo cumpridos.

Do lado positivo, contudo, vale recordar que o estudo de Cahn e outros (2016) averiguou que apenas 1% (um por cento) de empresas concentram cerca de 75% (setenta e cinco por cento) dos depósitos de

cookies de terceiros na vasta amostragem de mais de 100 mil sites. Desse modo, o cenário concentrado em poucas empresas, como a *DoubleClick* da *Google,* pode teoricamente tornar mais fácil a capacidade efetiva de fiscalizar o cumprimento de princípios ligados ao relacionamento com o cliente, como o *livre acesso*, a *transparência*, a *qualidade* dos dados e a *responsabilização* destas entidades, mais conhecidas do público.

A terceira consideração a ser analisada é a relativa ao emprego de diferentes tipos de *cookies* para a coleta de dados similares e do uso de técnicas pervasivas de monitoramento online. Como asseveraram Soltani *et al.* (2009) e Ayenson *et al.* (2011), é possível constatar o emprego de distintos tipos de cookies (*HTTP, Flash, HTML5*) para fins de coletar informações idênticas. O intuito: evitar que dados eventualmente deletados se percam e criar mecanismos obscuros de perpetuação dos mesmos. Neste ponto, há clara violação ao princípio da *necessidade*, uma vez que o tratamento de dados deve ser realizado no mínimo montante necessário para atingir as suas finalidades e não ser excessivo.

Ademais, o estudo de Castelluccia (2012) exemplifica como é possível empregar recursos mais invasivos de *cookies* (*supercookies* e *evercookies*), bem como técnicas de identificação da identidade do navegador a partir de *browser fingerprinting* e de explorações maliciosas na extensão *javascript*. Estas constatações demonstram igualmente o potencial de violação de todos os princípios do artigo 6º da lei de dados, relacionados aos momentos da aspiração do tratamento, do relacionamento com o titular e da gestão institucional dos dados pessoais.

Um último fenômeno a ser considerado é o da transferência de dados contidos nos *cookies* de terceiros por vias consideradas inseguras e facilmente interceptáveis na web. A constatação empírica de Cahn e outros (2016), de que apenas 0,36% (zero, vírgula trinta e seis por cento) dos *cookies* analisados transferiram informações com a sinalização de parâmetros seguros, deixa fortes indícios de problemas com os princípios da *segurança*, da *prevenção* contra danos e da *responsabilização.* Uma vez que as entidades responsáveis pelo tratamento de dados pessoais não se comprometem com diretrizes mínimas de segurança e prevenção na manipulação dos dados pessoais, elas terminam por expor estes dados a vazamentos e ataques mal-intencionados.

Empreendidas estas análises de potenciais desafios à LGPD a partir do cenário dos *cookies*, faz-se, por fim, pertinente realçar o papel das quatro modalidades de interferência do comportamento humano, lei,

sociedade, mercado e arquitetura, fixadas como marco teórico. A união de fatores históricos, instituições e técnicas de coleta de dados em torno do assunto dos *cookies* de navegador demonstra como o seu cenário regulatório é complexo e não pode ser realizado sem uma análise conjunta e interdisciplinar de elementos.

Sob o prisma teórico de Lessig (2006), fica evidente a necessidade de maior articulação e diálogo entre empresas, governos e sociedade na discussão das repercussões econômicas, políticas e humanas de tecnologias de monitoramento, como os *cookies*. É imperativo compreender que cada uma destas quatro dimensões possui suas próprias especificidades e que sua interação se dá de forma dinâmica, fluida e, por vezes, contraditória.

Nesse sentido, no cenário brasileiro será crucial o papel da Agência Nacional de Proteção de Dados (ANPD) já regulamentada na LGPD pelas alterações inseridas na Lei 13.853/2019. À ANPD caberá a fiscalização e a fixação de parâmetros recomendáveis a serem seguidos para o tratamento de dados pessoais, o que envolve o papel dos *cookies*. Embora o artigo 55-B da Lei de Dados assegure "autonomia técnica" à ANPD, resta questionar se o órgão, vinculado à Presidência da República, de acordo com o artigo 55-A (BRASIL, 2018)[14], terá autonomia política para lidar com temas complexos e cruciais para o futuro da sociedade da informação.

A síntese dos atores envolvidos com os *cookies* evidencia que, em se falando de dados pessoais e de privacidade, não é possível reduzir certos problemas a uma ordem meramente técnica, pois há sempre uma repercussão política, social e econômica subjacente. Os desafios à proteção dos dados pessoais são patentes para a lei brasileira.

Embora Lessig (2006) ensine que a articulação entre tecnologia, Estado, mercado e sociedade nem sempre é fácil, ela se faz mais do que urgente para que o Brasil atinja parâmetros respeitáveis na proteção de

[14] Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.
§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República;
§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD;
§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias (BRASIL, 2018).
Art. 55-B. É assegurada autonomia técnica à ANPD (BRASIL, 2018).

dados pessoais. O cenário é, certamente, desafiador. No entanto, a história da própria internet mostra que a articulação interdisciplinar em torno da criação de parâmetros e melhorias ao bem-estar geral é possível. Resta, contudo, saber se o Brasil conseguirá assumir um papel menos passivo e mais articulado perante as novas tecnologias de comunicação.

Desse modo, muito embora esteja difundido o argumento de que dados pessoais são ativos intangíveis e o "novo petróleo" das grandes empresas de tecnologia, é necessário tratar o assunto com muita cautela e transparência pública. Segundo Souza (2019), faz-se pertinente ressaltar que este petróleo é, antes de mais nada, um fiel retrato de nosso modo humano de ser, comunicar, informar e enxergar o mundo. Assim, para o autor, o questionamento que resta não diz respeito a regular ou não o tratamento de dados pessoais, mas sim como desenvolver esta regulação e quais as autoridades competentes para tanto.

Portanto, subliminarmente a cada atividade de tratamento de dados deve haver a ciência de que existem ali elementos intrínsecos e personalíssimos de nossa essência humana, capazes de revelar nossos segredos, fragilidades e tendências mais ocultas. O seu uso indiscriminado e sem critérios para fins de publicidade é preocupante e, certamente, não deve ser um assunto relegado à competência isolada das gigantes empresas do setor de tecnologia.

CONCLUSÃO

O presente estudo avaliou, sob uma perspectiva qualitativa e histórica, o fenômeno dos *cookies* de navegador e o desafio de sua regulação sob a óptica do direito à proteção dos dados pessoais, tendo por referência a Lei Geral de Proteção de Dados Pessoais.

Devido ao seu potencial multidisciplinar e adaptável para o tema, o marco teórico utilizado foi o das quatro modalidades de regulação do comportamento humano, de acordo com Lessig. Foram analisados referenciais bibliográficos de importantes atores envolvidos no desenvolvimento dos *cookies* e da própria internet, de maneira mais geral.

Como hipótese ao questionamento central do estudo, constatou-se que a sedimentação técnica dos *cookies* sofreu uma maior influência pela esfera do mercado, sem prejuízo de tentativas posteriores de regulação por parte da esfera legal e de requisições e repercussões na esfera social.

As implicações desta constatação foram as de que os *cookies*, criados para resolver um problema de ordem técnica no protocolo *HTTP,* revelaram-se determinantemente moldados para fomentar um modelo de negócios pautado na publicidade e no monitoramento da navegação de usuários na rede. De forma isolada, os *cookies* não puderam ser considerados "vilões" da publicidade extensiva na web, uma vez que outras tecnologias pervasivas - como *fingerprinting* de navegador e a exploração de vulnerabilidades em arquivos depositados por execução do *javascript,* bem como adaptações mais agressivas dos *cookies*, os *supercookies* e os *evercookies* – revelaram potencial lesivo igual ou até mais asseverado.

Contudo, vislumbrou-se ser necessária uma maior atenção para com os *cookies*, uma vez que dados empíricos demonstram forte disseminação de seu uso para fins de monitoramento e alimentação de bases de perfis para publicidade. Não raro, estes procedimentos podem ser desenvolvidos fora de parâmetros mínimos de legalidade e ética.

Assim, o estudo pretendeu demonstrar que o caminho da regulação destes *cookies* é complexo e não pode ser desbravado sem um esforço integrado e articulado entre juristas, *experts* das ciências da informação, representantes da sociedade civil, empresas e governantes. A Lei Brasileira de Dados Pessoais foi um importante passo inicial, mas que demanda discussão, fiscalização e conscientização para atingir seus propósitos fáticos de controle e proteção à dignidade humana.

Como sugestão para estudos futuros, pontua-se a necessidade de investigações empíricas interdisciplinares, voltadas à identificação da utilização de *cookies* em páginas para o cenário brasileiro. Tais estudos auxiliarão no diagnóstico mais preciso dos *cookies* no país e poderão fornecer valiosas pistas para a sua regulação futura.

REFERÊNCIAS

ABRAMS, Martin. The Origins of Personal Data and its Implications for Governance. *Social Science Research Network*, 2014. DOI: <http://dx.doi.org/10.2139/ssrn.2510927>.

ALTAWEEL Ibrahim. GOOD, Nathaniel. HOOFNAGLE, Chris Jay. Web Privacy Census. *Technology Science,* 2015, id 2015121502. Disponível em: <https://techscience.org/a/2015121502>. Acesso em: 07 dez. 2018.

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: <//dx.doi.org/10.2139/ssrn.18983902011>.

BERNERS-LEE, Tim. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*. Nova Iorque: HarperCollins Publishers, 1999, 226p.

BRASIL. *Lei n° 13.709, de 14 de agosto de 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: <https://bit.ly/2NH4yIF>. Acesso em: 05 jan. 2019.

BRASIL (2019). Senado Federal. *Proteção de dados pessoais deverá ser direito fundamental na Constituição*. Senado Notícias, 02 jul. 2019. Disponível em: <https://bit.ly/2xsLEiG>. Acesso em: 04 jul. 2019.

CAHN, Aaron. ALFELD, Scott. BARFORD, Paul. MUTHUKRISHNAN, S. An Empirical Study of Web Cookies. *25th International Conference on World Wide Web (WWW '16),* International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, pp. 891-901. DOI: <https://doi.org/10.1145/2872427.2882991>.

CALO, Ryan. Digital Marketing Manipulation. *The George Washington Law Review*, vol. 82, n 04, 2014, pp. 1018-1041.

CASTELLUCCIA, Claude. Behavioural Tracking on the Internet: A Technical Perspective. Em: GUTWIRTH, S. LEENES, R. DE HERT, P. POULLET, Y. (eds). *European Data Protection: In Good Health?* Dordrecht: Springer, 2012. DOI: <https://link.springer.com/chapter/10.1007/978-94-007-2903-2_2#citeas>.

DATAFOLHA. *Hábitos de Uso de Aplicativos*: população brasileira – 13 anos ou mais. Datafolha Instituto de Pesquisa, Dez. 2016. Disponível em: <https://bit.ly/2tWV1mH>. Acesso em: 01 out. 2018.

DEGELING, Martin. UTZ, Christine. LENTZSCH, Christopher. HOSSEINI, Henry. SCHAUB, Florian. HOLTZ, Thorsten. We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *ArXiv* 1808:05096, 2018. Disponível em: <https://arxiv.org/abs/1808.05096>. Acesso em: 25 nov. 2018.8.050

DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. *Espaço Jurídico Journal of Law*, vol. 12, nº 02, 2011, pp. 91-108. Disponível em: <https://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658>. Acesso em: 03 nov. 2018.

FONSECA, Ricardo Marcelo. *Introdução teórica à história do direito*. Curitiba: Juruá, 2012, 176 p.

FOWLER, Geoffrey A. *Goodbye, Chrome:* Google's web browser has become spy software. The Washington Post, 21 jun. 2019. Disponível em: <https://wapo.st/2NwieeI>. Acesso em: 03 jul. 2019.

GLANCY, Dorothy J. The Invention of the Right to Privacy. *Arizona Law Review*, v. 21, n. 01, 1979. Disponível em: <https://bit.ly/2Xjw9Ec>. Acesso em: 01 jul 2019.

HOOFNAGLE, Chris Jay, Post Privacy's Paternalism. In: DIX, Alexander. FRANSSEN, Gregor. KLOEPFER, Michael. SCHAAR, Peter (eds). *Informationsfreiheit Und Informationsrecht: Jahrbuch.* Lexxion, 2012. Disponível em <https://ssrn.com/abstract=2468322>. Acesso em: 03 nov. 2018.

KRISTOL, David M. HTTP Cookies: Standards, Privacy, and Politics. *ACM Transactions on Internet Technology*, Vol. 1, nº. 02, 2001, pp. 151–198. Disponível em: <https://www.cs.stevens.edu/~nicolosi/classes/17fa-cs578/ref4-1.pdf>. Acesso em: 30 jul. 2018.

LEINER, Barry M. CERF, Vinton G. CLARK, David D. KAHN, Robert E. KLEINROCK, Leonard. LYNCH, Daniel C. POSTEL, Jon. ROBERTS, Larry G. WOLFF, Stephen. A brief history of the internet. *ACM SIGCOMM Computer Communication Review, vol.* 39, nº 5, 2009, pp 22-31. DOI <=http://dx.doi.org/10.1145/1629607.1629613>.

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. Disponível em: <http://codev2.cc/download+remix/>. Acesso em: 20 ago. 2013.

MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection in Europe, p. 219-241. In: AGRE, Philip E.; ROTENBERG, Marc (eds.). *Technology and Privacy:* The New Landscape. Massachussets: The MIT Press, 1997. 325 p.

MIT TECHNOLOGY REVIEW CUSTOM. *The Rise of Data Capital*. In partnership with Oracle, 2016, 12p. Disponível em: <https://bit.ly/2tWV1mH>. Acessado em: 22 out. 2018.

MONTULLI, Lou (2013a). The reasoning behind Web Cookies. *The Irregular Musings of Lou Montulli (blog)*, 14 maio, 2013. Disponível em: <http://montulli.blogspot.com/2013/05/the-reasoning-behind-web-cookies.html>. Acesso em: 20 set. 2018.

MONTULLI, Lou (2013b). Why blocking 3rd party cookies could be a bad thing. *The Irregular Musings of Lou Montulli (blog)*, 17 maio, 2013. Disponível em: <http://montulli.blogspot.com/2013/05/why-blocking-3rd-party-cookies-could-be.html>. Acesso em: 20 set. 2018.

NELSON, Theodor HolmT. Complex information processing: a file structure for the complex, the changing and the indeterminate. *Proceedings of the 1965 20th national conference,* (ACM '65), Lewis Winner (Ed.). ACM, New York, NY, USA, 1965. Disponível em: <https://dl.acm.org/citation.cfm?id=806036>. Acesso em: 04 jan. 2018.

RAVINDRANATH, Mohana. *How your health information is sold and turned into 'risk scores'*. Político.com, 03 de fev. de 2019. Disponível em: <https://www.politico.com/story/2019/02/03/health-risk-scores-opioid-abuse-1139978>. Acesso em: 03 fev. 2019.

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

SILVA, Vergilio Ricardo Britto da. *Preocupação com a privacidade na internet: uma pesquisa exploratória no cenário brasileiro* / Vergilio Ricardo Britto da Silva. – Porto Alegre: Pontifícia Universidade Católica do Rio Grande do Sul, 2015, 117 p. Diss. (Mestrado) – Faculdade de Administração, Contabilidade e Economia, Orientadora: Profa. Dra. Edimara Mezzomo Luciano.

SOLTANI, Ashkan. CANTY, Shannon. MAYO, Quentin. THOMAS, Lauren. HOOFNAGLE, Chris Jay. Flash Cookies and Privacy. *Social Science Research Network*, 2009. DOI: <http://dx.doi.org/10.2139/ssrn.1446862>.

SOUZA, Carlos Affonso Pereira de. Com Quantas Regulações se faz uma Plataforma. *O Estado de São Paulo*, 03 fev. 2019. Disponível em: <https://link.estadao.com.br/noticias/empresas,com-quantas-regulacoes-se-faz-uma-plataforma,70002705219>. Acesso em: 03 fev. 2019.

SOUZA, Carlos Affonso Pereira de. O Progresso Tecnológico e a Tutela Jurídica da Privacidade. Direito, Estado e Sociedade, vol. 09, nº 16, jan/jul. 2000. Disponível em: <http://www.jur.puc-rio.br/revistades/index.php/revistades/issue/viewFile/62/5>. Acesso em: 03 set. 2017.

TIRTEA, Rodica. CASTELLUCCIA, Claude. IKONOMOU, Demosthenes. Bittersweet cookies: Some security and privacy considerations. *ENISA: European Network and Information Security Agency Publications*, 2011. Disponível em: <https://www.enisa.europa.eu/publications/copy_of_cookies>. Acesso em: 20 out. 2018.

UNIÃO EUROPEIA (2002). *Directiva 2002/58/CE do Parlamento Europeu e do Conselho.* Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas), 12 de jul. 2002. Disponível em: <https://bit.ly/2LWprQL>. Acesso em: 04 dez. 2018.

UNIÃO EUROPEIA (2009). *Directiva 2009/136/CE do Parlamento Europeu e do Conselho.* Altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e o Regulamento (CE) n.o 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor, 25 nov. 2009. Disponível em: <https://bit.ly/2HeNTyb>. Acesso em: 04 dez. 2018.

UNIÃO EUROPEIA (2016). *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), 27 de abril de 2016. Disponível em: <https://bit.ly/2EfI4tr>. Acesso em: 04 dez. 2018.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, v. 04 n. 05, 1890, p. 193-220. Disponível em: <https://bit.ly/2OVE5Io>. Acesso em 01 jul. 2019.