COOKIES: VULNERABILIDADE DO DIREITO À PRIVACIDADE NOS MEIOS DIGITAIS NO ÂMBITO DA LEGISLAÇÃO BRASILEIRA

Mário Furlaneto Neto[1]

Júlio César Lourenço do Carmo[2]

Bruna de Oliveira da Silva Guesso Scarmanhã[3]

Sumário: Introdução; 1. Sigilo das comunicações: uma análise principiológica 2. Dos cookies; 3. Riscos à privacidade frente as novas tecnologias. Considerações finais. Referências.

Resumo: O aperfeiçoamento das ferramentas da tecnologia da informação tem proporcionado às empresas avanços nos mecanismos virtuais para captação de dados dos consumidores personificando seus clientes através da utilização de cookies. Porém, o desvirtuamento no emprego dessa ferramenta esbarra na violação de princípios norteadores do uso da Internet no Brasil, pontuados pelo Marco Civil da Internet. Assim, por meio de revisão bibliográfica e legislativa, questiona-se a eficácia da proteção à intimidade em face do uso dos cookies e a dificuldade da aplicação do Direito diante das constantes inovações tecnológicas. Conclui-se que a obtenção e utilização de dados pessoais sem o

[1] Delegado de Polícia e professor da graduação e do Mestrado em Direito do Univem - Centro Universitário Eurípides de Marília. Doutor em Ciência da Informação pela Unesp. Coordenador do NEPI - Núcleo de Estudos em Direito e Internet.

[2] Graduando em Direito do Univem - Centro Universitário Eurípides de Marília. Integrante do grupo de pesquisa NEPI (Núcleo de Estudos em Direito e Internet).

[3] Mestranda em Direito na área de concentração "Teoria do Direito e do Estado" no UNIVEM/Marília-SP. Bolsista CAPES/PROSUP. Integrante dos grupos de pesquisas NEPI (Núcleo de Estudos em Direito e Internet) e GRADIF (Gramática dos Direitos Fundamentais) no UNIVEM.

consentimento dos usuários caracteriza violação a privacidade, ferindo a dignidade da pessoa humana, motivo pelo qual propõe-se um modelo de transparência desde a coleta até a utilização dos dados pessoais, de forma a estar ao alcance dos usuários tanto a autorização para a coleta e uso quanto a desistência e exclusão total dos dados pessoais pelo titular da aplicação de Internet.

Palavras-Chave: Privacidade; Dados Pessoais; Cookies, Internet, Vulnerabilidade.

COOKIES: VULNERABILITY OF THE RIGHT TO PRIVACY IN DIGITAL MEDIA UNDER BRAZILIAN LEGISLATION

Abstract: Improved information technology tools have provided companies with advancements in virtual mechanisms for capturing consumer data by embodying their customers through the use of cookies. However, the distortion in the use of this tool runs counter to the principles guiding the use of the Internet in Brazil, punctuated by the Civil Internet Framework. Thus, through a bibliographical and legislative review, the effectiveness of the protection of privacy in face of the use of cookies and the difficulty of applying the Law in the face of constant technological innovations is questioned. It is concluded that the collection and use of personal data without the consent of the users characterizes a violation of privacy, harming the dignity of the human person, which is why a model of transparency is proposed from the collection to the use of personal data, in a way to be within the reach of the users both the authorization for the collection and use and the total withdrawal and exclusion of the personal data by the holder of the Internet application.

Keywords: Privacy; Personal Data; Cookies; Internet;

Vulnerability.

INTRODUÇÃO

s últimas décadas foram marcadas por grandes avanços tecnológicos, a ponto de ser denominada a Era digital. A expansão da Internet fomentou o crescimento de serviços oferecidos e prestados por meio da rede mundial de computadores. Os desenvolvedores de sistemas da web têm criado novas ferramentas que permitem o acesso a Internet enquanto uma experiência exclusiva. Para tanto, necessitam conhecer as características, preferências e interesses dos usuários, em cujo contexto se insere a coleta de dados pertinentes à navegação.

Tendo em vista a necessidade de fomento do mercado econômico, muitas ferramentas são desenvolvidas com a finalidade de captação de dados e informações, cujo contexto se insere os cookies. Inicialmente criados para agilizar a resposta do navegador, atualmente têm a capacidade de coletar dados dos usuários, desde preferência de idioma em um navegador até "logins" e senhas, informações pessoais estas que, em algumas ocasiões, são coletadas sem a ciência do usuário.

Assim, por meio de revisão bibliográfica e legislativa, analisar-se-ão as espécies de cookies, a fim de estabelecer se sua utilização viola o estipulado pelo art. 5º, inc. X, da Constituição Federal (CF) e o estabelecido no Marco Civil da Internet (MCI) no que concerne ao direito a privacidade, como referencial teórico para propor um modelo ideal de coleta de dados garantista.

Para tanto, necessário realizar uma análise principiológica a permear o uso da Internet no Brasil, o que se fará a seguir.

1 SIGILO DAS COMUNICAÇÕES: UMA ANÁLISE PRINCIPIOLÓGICA[4]

[4] Tópico extraído e adaptado do artigo apresentado no evento no VI

O indivíduo possui o direito de manter aspectos de sua vida em sigilo, seja no âmbito familiar, profissional ou social. Assim, a informação de caráter íntimo ou privado de cada pessoa, não poderá ser manipulada sem o consentimento do usuário, sob pena de violar a tutela à liberdade.

Nessa seara, Montesquieu (1956 apud SILVA, 2016, p. 233) conceitua a liberdade como "o direito de fazer tudo o que as leis permitem", contudo, Silva (2016, p. 233) adverte que este conceito traz um risco, pois deve levar em conta, para fins de validade, leis consentidas pelo povo. Mais aceitável, de acordo Silva (2016, p. 234), é o conceito trazido pela Declaração de 1789 (ONU, 1789) que condicionada o direito à liberdade aos limites que tangenciam os direitos dos demais membros da sociedade, os quais têm direito ao gozo dos mesmos direitos. Destaca que apenas a lei pode estabelecer tais limites, isto é, estipular aqueles que sejam nocivos à sociedade.

Nessa dimensão, o conceito de liberdade frente ao armazenamento de dados abrange outros direitos fundamentais, tais como a privacidade, a intimidade e a vida privada.

Com efeito, de acordo com Canotilho (2003, p. 383), "os direitos fundamentais cumprem a função de direitos de defesa dos cidadãos sob uma dupla perspectiva", isto é, em uma primeira premissa, "constituem, num plano jurídico-objetivo, normas de competência negativa para os poderes públicos, proibindo fundamentalmente as ingerências destes na esfera jurídica individual" e, em uma segunda dimensão, "implicam, num plano jurídico-subjetivo, o poder de exercer positivamente direitos fundamentais (liberdade positiva) e de exigir omissões dos poderes públicos, de forma a evitar agressões lesivas por parte dos mesmos (liberdade negativa)".

Simpósio Internacional de Análise Crítica do Direito – SIACRID, em 26 ago. 2016. Publicação disponível em: <http://siacrid.com.br/repositorio/2016/sistema-constitucional-de-garantia-de-direitos_II.pdf>. (SCARMANHÃ; FURLANETO NETO, 2016, p. 179-181).

Em consonância, preceitua Miranda (2012, p. 7, grifo do autor) que "por direitos fundamentais entendemos os direitos ou as posições jurídicas subjectivas das pessoas enquanto tais, individual ou institucionalmente consideradas, assentes na Constituição, seja na Constituição formal, seja na Constituição material" […] daí falar-se em […] "*direitos fundamentais em sentido formal e direitos fundamentais em sentido material*".

Assim, dispõe o artigo 5º, inciso X, da CF, acerca da inviolabilidade da intimidade, da vida privada, honra e imagem das pessoas (BRASIL, 2016).

Nas palavras de Lafer (1998 apud MEIRA, SOARES e PIRES, 2012) privacidade é "o direito do indivíduo de estar só e a possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que a ela só se refere, e que diz respeito ao seu modo de ser no âmbito da vida privada".

Na definição de Bastos (2000, p. 55-56, apud MEIRA, SOARES e PIRES, 2012), o direito à privacidade é "a faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano".

Nesse passo, Silva (2016, p. 239) conceitua a privacidade enquanto gênero, dos quais são espécies, a intimidade, a vida privada, o direito à honra, à imagem das pessoas, entre outros. Dessa maneira, a privacidade compõe um conjunto mais amplo que a intimidade, pois todo íntimo é privado, mas nem todo o privado é íntimo, a ponto de agrupar no direito à privacidade.

Logo, "o conceito de direito à privacidade é subjetivo, pois é inerente a cada individuo delimitar os fatos e informações que deseja manter sob sigilo" (MEIRA, SOARES e PIRES, 2012).

Nesse raciocínio, acrescenta Bastos (2000, p. 55-56 apud MEIRA, SOARES e PIRES, 2012) que o direito a intimidade

"consiste na faculdade que tem cada indivíduo de obstar a intromissão de estranhos na sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um (...)", e finaliza seu pensamento ao afirmar que o direito a intimidade também visa "(...) impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano".

- Dotti (1980, p. 69) conceitua a intimidade como "a esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais", isto é, evitar disponibilizar ao conhecimento de outrem aquilo que é pessoal, íntimo ou particular.
- Sob o enfoque da vida privada, Silva (2016, p. 208) relata que, a rigor, a CF deveria tutelá-la como a esfera mais "íntima da pessoa", por contextualizar o "repositório de segredo e particularidades de foro moral e íntimo" da pessoa humana, porém, a Lei Maior a tratou em um aspecto mais amplo, "como conjunto de modo de ser e viver, como o direito de o indivíduo viver a sua própria vida".
- O autor salienta que a vida de uma pessoa compreende dois aspectos: um exterior e outro interior. O primeiro, público, passível de divulgação, por compreender aspectos da vida social e pública da pessoa, enquanto a vida interior "se debruça sobre a mesma pessoa, sobre os membros de sua família, sobre seus amigos" a exigir a tutela do "segredo da vida privada", enquanto "condição de expansão da personalidade", e a permitir o exercício da "ampla liberdade de realizar sua vida privada, sem perturbação de terceiros" (SILVA, 2016, p. 208).

Nessa seara, Davara Rodríguez (2008, p. 55) explica que os dados pessoais têm conexão com a intimidade (unidos ao indivíduo e em seu entorno social) e que a privacidade é a possibilidade de mantê-los em sigilo, resguardados de acesso e intromissões alheias, ressaltando, no entanto, que o surgimento da informática e a rápida transmissão de informações possibilitou

uma fonte potencial de agressividade contra a intimidade da pessoa em diferentes formas.

Ocorre que no meio ambiente da rede mundial de computadores a discussão sobre a intimidade, a vida privada e a privacidade não pode ficar restrita aos arquivos de dados pessoais. Assim, levando em conta o sigilo das comunicações de informática ou telemática, necessária se torna que tais informações também sejam objeto de alguma proteção pelo ordenamento jurídico, pois, de acordo com Davara Rodríguez (2008, p. 49, tradução nossa) "(...) trata-se de proteger as pessoas ante o manejo ou manipulação, não autorizada, de seus dados pessoais" [5].

Nessa dimensão, nota-se que a Constituição Federal brasileira, em seu artigo 5º, X, preocupou-se em tutelar a intimidade, que por sua vez engloba o sigilo das comunicações de informática ou telemática, especificada no inciso XII do mesmo codex.

Os dispositivos informáticos contemporâneos possibilitam armazenar dados pessoais, assim como o resultado do fluxo das comunicações de informática. Destarte, os dados e informações armazenados em dispositivos informáticos estão tutelados pela CF, em respeito ao direito à intimidade.

Deveras, a obtenção do fluxo das comunicações de informática, em tempo real, é regida pela Lei nº 9.296/1996.

Com efeito, as ferramentas como *cookies* e *sniffers* possibilitam monitorar o fluxo do acesso individual do internauta dentro da rede mundial de computadores, alimentando o banco de dados do titular da aplicação de Internet, de forma a permitir estabelecer as preferências do usuário, em patente violação à intimidade. Nessa linha de raciocínio, a ilegal interceptação do fluxo das comunicações de informática ou telemática se amolda ao tipo penal previsto no artigo 10 da Lei Federal nº 9.296/1996.

---

5 Texto original: [...] se trata de proteger a las personas ante el manejo o manipulación, no autorizada, de sus datos personales […] (DAVARA RODRÍGUEZ, 2008, p. 49).

Ressalta-se, no entanto, que quanto ao emprego do *cookie*, apenas poderá caracterizar interceptação do fluxo das comunicações de informática se instalado e monitorado por terceiro, ainda que com o conhecimento do responsável legal ou administrador do *site*, mas desde *que* sem conhecimento do internauta monitorado.

Assim, diante desse contexto, compreende-se que o fluxo e o armazenamento de dados são inúmeros e diante dessa nova situação surge a discussão sobre a intimidade, a vida privada e a privacidade, pois, se por um lado as novas funcionalidades dos dispositivos informáticos têm contribuído para o desenvolvimento tecnológico e social, em contrapartida tem sido utilizado como meio indevido de armazenamento de dados pessoais.

Frisa-se que os dispositivos informáticos estão aptos a armazenar dados pessoais, assim como o produto do fluxo das comunicações de informática, motivo pelo qual formula-se a assertiva de que os dados armazenados estão protegidos pelo manto do sigilo que decorre da privacidade, intimidade e vida privada, ambos tutelados constitucionalmente.

Pois bem, acerca dos dados pessoais, não há no Marco Civil da Internet (Lei nº 12.965/2014) um conceito específico do que os seria, porém, Lima (2014, p. 155) chega à conclusão de que dado pessoal pode ser considerado "como qualquer informação que permita a identificação, direta ou indireta, de um usuário, incluindo dados cadastrais (...) e técnicas (endereço de IP) (...)".

Sob o aspecto dos dados cadastrais, o Decreto nº 8.771, de 11 de maio de 2016 (BRASIL, 2016b), que regulamentou o Marco Civil da Internet, estipulou-os como sendo os relativos à filiação, endereço e a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário do provedor.

O Marco Civil da Internet (MCI) introduziu em seu art. 3º, IV como um dos princípios para a disciplina do uso da internet no Brasil a preservação e garantia da neutralidade da rede.

De acordo com Pretto (2017):

> A neutralidade da rede, ou neutralidade da Internet, em sua essência, representa a garantia de que os dados receberão tratamento isonômico independente de seu conteúdo, dispositivo de acesso, origem e destino. Em um entendimento menos técnico, vídeos, textos, imagens serão transmitidos de forma igual na Internet. Para preservar a isonomia no tratamento dos dados é preciso garantir que os pacotes, de uma mesma conexão, não seguirão rotas diferenciadas, e não poderão ser discriminados ou encapsulados em função do seu destino e/ou origem, conteúdo, dispositivo e/ou aplicativo de acesso.

Nesse sentido, dispõe o *caput* do art. 9º que o "responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação" (BRASIL, 2014).

Assim, partindo do pressuposto das determinações do *caput* do art. 9º, "cumprir o princípio da neutralidade significa garantir que a navegação na internet continuará livre e aberta, como temos experimentado até hoje". Isso significa afirmar que "as empresas não poderão limitar o uso de aplicativos ou os sites a serem acessados pelos usuários de acordo com planos de serviços com preços diferenciados por tipo e quantidade de aplicativos e conteúdos a serem acessados, nem em função do tipo de terminal de acesso" (PRETTO, 2017).

Desse modo, constata da análise do MCI eventual reflexo quanto ao princípio da neutralidade no que tange ao emprego de *cookies* na rede mundial de computadores, haja vista que alguns sites, voltados, nomeadamente, ao *e-commerce*, só funcionam se o usuário autorizar a habilitação do *cookies*.

Portanto, por ser inerente ao sistema jurídico brasileiro o direito à intimidade e à vida privada consagram-se estes entre os direitos e liberdades fundamentais a serem assegurados ao indivíduo, impondo-se ao Estado a tutela da privacidade do indivíduo na sociedade digital em face da utilização indevida de *cookies*, cujo conceito e classificação discutir-se-ão no próximo

tópico.

2 COOKIES: CONCEITO E CLASSIFICAÇÃO

O Departamento Norte-Americano de Defesa, em 1969, com a intenção de compartilhar recursos computacionais, criou a ARPANET, uma rede de transmissão de pacotes entre três universidades americanas. Posteriormente, em 1971, foram criados os primeiros protocolos para utilização desta rede recém criada: o FTP e o Telnet.

Em 1972 surge o e-Mail, porém, o IP e o TCP, protocolos de rede e transporte utilizados ainda atualmente, só surgiram em 1980. Em 1989, já com 100.000 dispositivos conectados, a Internet já era uma rede de escala global, porém predominantemente acadêmica, até que neste mesmo ano a www foi criada por Tim Berners-Lee por meio da especificação do formato html e do protocolo http. A partir desta invenção, a Internet foi popularizada em todo o mundo, principalmente após o lançamento, em 1994, do primeiro Navegador www comercial, o *mosaic da ncsa*, que permitiu que pessoas fora do meio acadêmico acessassem a www (FRANCO; RUGGIERO, 2007, p. 28-29).

Desse modo, "diversos empreendedores, percebendo a adoção cada vez maior da utilização da Internet pela população em geral, passaram a utilizar a Internet como canal de venda de produtos e meio de prestação de serviços, criando desta forma o negócio eletrônico e as empresas .com" (FRANCO; RUGGIERO, 2007, p. 28-29).

Assim, houve maior competição entre as empresas, e o consumo de recursos computacionais passou a ser um fator primordial para a rentabilidade de um modelo de negócio eletrônico.

Desse modo, conforme elencam Franco e Ruggiero (2007, p. 28-29):

> A avaliação do potencial de retorno dos consumidores para um negócio faz parte da disciplina de marketing e é feita através

> da classificação dos consumidores em grupos através de um ou mais critérios socioeconômicos e comportamentais. Para avaliar o potencial de retorno de cada grupo de consumidores, as empresas tradicionais valem-se da observação do comportamento dos consumidores nos pontos de venda, de pesquisas qualitativas e quantitativas, e de aplicação de técnicas de *data-mining*[6] no seu repositório de informação sobre vendas. Já as empresas de negócio eletrônico não podem observar diretamente os consumidores e por isso precisam de métodos e ferramentas para avaliar o comportamento dos consumidores em seu *web-site*.

A análise de comportamento de consumidores em *web-sites* tem sido utilizada para conhecer o comportamento dos consumidores enquanto ferramenta para tornar o modelo de negócio eletrônico mais rentável, de modo que para que isto seja possível, foi necessário a criação e a inclusão de informações de controle de estado nas comunicações entre clientes e servidores www batizadas como *cookies*. "O advento dos *cookies* permitiu a criação de sessões explícitas de comunicação entre servidores e clientes www que permitiu uma interação mais rica e segura entre negócio e consumidor" FRANCO; RUGGIERO, 2007, p. 28-29).

Nessa seara, cumpre esclarecer que os *cookies*, em geral, são pequenos trechos de texto acondicionados no *browser* ou navegador *Web* utilizado pelo usuário, usados para armazenar informações. É uma ferramenta para personalizar páginas Web e permitir que acessos futuros do usuário ao *site* sejam de modo personalizado, pois podem ser reativados quando o usuário retornar à página web, identificando informações outrora coletadas e serem aplicadas naquele momento de acesso (DEITEL, 2010).

Com base em Pacheco (2005, p. 825), os "cookies são basicamente textos que o servidor Web pode colocar no navegador do cliente. Eles são transferidos via cabeçalho HTTP. À medida que o usuário visita várias páginas dentro de um site ou

---

6 Mineração de dados.

aplicação Web, o servidor (examina) o conteúdo desses cookies". Assim eles permitem uma interação entre servidor e navegador. Mantendo um "contexto persistente entre servidor e browser." (WEINMAN, 1997, p. 142).

Para Santos (2001, p. 151), cookies são "arquivos de dados gerados toda vez que a empresa que cuida da manipulação de dados, recebe instruções que os servidores Web enviam aos programas navegadores e que são guardados em diretório específico do computador do usuário".

De acordo com Rohr (2010):

> O cookie é um recurso básico da web. Ele é criado quando um site solicita ao navegador que uma informação seja armazenada. Por exemplo, quando você faz login em um site, o site pede que o navegador armazene um código. Toda vez que você visitar outra página naquele site, o navegador enviará o código. O site estará preparado para saber que o internauta com aquele código é você e o manterá logado no sistema.
>
> É por esse motivo que o chamado roubo de cookies[7] é problemático. Se um site tem alguma brecha que permite o roubo dos cookies, o código armazenado pode ser injetado no navegador do criminoso, que irá acessar a página como se fosse você. Por motivos de segurança, cada site só pode ler os próprios cookies, ou seja, a Globo.com só pode ler os cookies criados por sites dela mesma. É preciso uma falha de segurança nos sites para permitir a leitura dos cookies.

Vale ressaltar que quando foram inicialmente projetados pela Netscape, os cookies tinham a finalidade de corrigir uma "deficiência observada na interação entre servidores da Web e navegadores. E que sem os *cookies*, a interação entre servidores e navegadores sairia do controle" (GONÇALVES, 2007, p. 98).

Nessa seara, insta esclarecer que há algumas variáveis de

---

7 Em que pese Rohr (2010) fazer alusão à expressão "roubos de cookies", vale frisar que sob o ponto de vista da técnica jurídica, o roubo caracteriza-se pela subtração de coisa alheia móvel mediante o emprego de violência ou grave ameaça. No caso, poder-se-ia pensar em invasão de dispositivo informático para os fins de obter informações, o que pode caracterizar ou não o crime de violação de dispositivo informático. Tal confusão terminológica pode decorrer do fato de o autor ter formação na área da Ciência da Computação e não em Direito.

cookies: *cookies* de sessão ou temporários; *cookies* persistentes; *cookies* de primeira parte e *cookies* de terceiro.

Os cookies de sessão ou temporários, além de serem armazenados em uma pasta específica no *Hard Disc* (HD), enquanto estiverem em execução, também são armazenados na memória Ram[8]. Permanecem no computador do cliente somente enquanto ele está visitando o *site* da *Web*. Segundo Queiroz (2011, p. 32) "será gravado apenas enquanto durar a navegação em determinado *site*, ou seja, durante a sessão estabelecida entre o navegador e aplicação *web*".

Os cookies persistentes, por outro lado, podem durar meses ou até mesmo anos, pois são armazenados em um arquivo de texto no computador do cliente. "Esse arquivo de texto é denominado arquivo *Cookie* nos computadores com sistema operacional Windows e arquivo *Magic Cookie* nos computadores Macintosh" (GONÇALVES, 2007, p. 98).

Na mesma linha de raciocínio, Rohr (2010) explica que:

> Existem dois tipos de cookies: os cookies de sessão e aqueles que têm uma data de validade. Os cookies de sessão existem apenas até o navegador ser fechado. Quando você fecha o navegador, esses cookies são apagados. Um exemplo são os cookies em sistemas de login nos quais você não clicou em "lembrar de mim".
>
> Os *cookies* com data de validade permanecem no computador até serem removidos manualmente ou até a data especificada pelo *site*. Por questões técnicas, a data máxima hoje é o ano de 2038 – é claro que você não vai ficar com o mesmo computador até 2038, portanto essa é uma data simbólica. Alguns chamam os *cookies* marcados com validade até 2038 como "*cookies* eternos" por representaram a intenção do site de nunca remover aquele *cookie*.
>
> Esses *cookies* de longa validade são usados por sistemas de *login* quando você clica em "lembrar de mim" – e o roubo[9] deles é ainda mais perigoso. Eles são também usados por sistemas de

---

8 É um componente que armazena os dados de programas que estão sendo executados.

9 Vide observação na nota de rodapé precedente.

> publicidade na *web*, que rastreiam sua interação com anúncios para determinar qual é o seu perfil de acesso e ajudar a oferecer peças publicitárias mais próximas do seu interesse. Foram esses *cookies* que viraram alvo de *softwares* anti-*spywares*, que os consideravam uma forma de "espionar", por mais que os *cookies*, em si, jamais carregassem qualquer informação pessoal.

Os *cookies* de primeira parte "são os mecanismos de manutenção da sessão ou de captura de informações pertencentes ao domínio que o usuário está diretamente visitando" (QUEIROZ, 2011, p. 33). Há uma relação consciente entre o usuário e o titular do domínico acessado, pois ao acessar determinado *site*, o usuário aceita os mecanismos de funcionamento dos *cookies*.

Por outro lado, os *cookies* de terceiros surgem de relacionamentos entre múltiplos "domínios e serviços oferecidos entre eles; são *web sites* que mantém relação comercial com o *site* utilizado pelo usuário", de forma que referidos "*cookies* são criados e manipulados por provedores terceiros" em relação à requisição inicialmente estabelecida entre o usuário e o titular do domínico inicialmente acessado (QUEIROZ, 2011, p. 33).

Outrossim, com os avanços tecnológicos surgem novas modalidades de *cookies* visando a manutenção das sessões dos usuários na *Internet*. Dentre os novos *cookies*, pode-se citar os *cookies* de *flash* e os *evercookies*.

Desse modo, os *cookies* de *flash* possuem "algumas vantagens em relação ao espaço de armazenamento de dados e a forma de comunicação com o servidor", de forma que esta nova tecnologia permite a "implementação proprietária, não permitindo a manipulação dos seus objetos pelos navegadores, sendo necessária a instalação de uma aplicação para a exclusão de dados". Assim, "os usuários normalmente deixam suas informações valiosas nestes objetos por muito tempo, gerando mais um problema para segurança destes dados" (QUEIROZ, 2011, p. 64).

Contudo, os *everycookies* são os mais danosos, por usarem técnicas de persistência. Nesse sentido, mesmo que o

usuário venha a apagar as informações, o *everycookie* possibilita recuperá-las.

Ao explicar a arquitetura de funcionamento do everycookie, Rohr (2010) salienta ser

> […] o cookie que não pode ser removido. O cookie é um recurso intencional da web, criado quando se percebeu que era necessário identificar um mesmo internauta que acessava diferentes páginas de um site. O evercookie não é exatamente um cookie e sim um mecanismo criado pelo programador Samy Kamkar para armazenar uma informação de forma permanente no computador. Isso é possível graças ao uso subvertido de diversos recursos.
>
> O evercookie é armazenado como um cookie normal, mas também como um "cookie" do Flash (chamado de Local Shared Object ou LSO), "cookie" específico do Internet Explorer, do Silverlight (tecnologia semelhante ao Flash, da Microsoft), como valores no banco de dados do HTML5 (outro recurso polêmico) e ainda como arquivos cacheados e no histórico da web. No total, são 13 formas de armazenar a mesma informação, com mais duas previstas. Enquanto uma delas estiver presente, todas as demais podem ser recriadas, tornando o "cookie" permanente.

De acordo com o referido autor,

> O evercookie é armazenado também no cache do navegador. O cache é composto pelos arquivos já baixados da internet e que são usados em várias páginas (como o logotipo do G1) e que ficam no disco para que o navegador não precise baixar de novo, acelerando a navegação. A informação do evercookie é armazenada em um arquivo em cache, enviado pelo servidor. Quando o navegador perguntar ao servidor se o arquivo em cache pode ser usado ou se ele precisa ser baixado novamente, o site pode "mentir" ao navegador que o arquivo (que nunca existiu) não mudou e que não é necessário baixá-lo novamente, sendo possível ler a informação que o navegador armazenou em cache, exatamente como um cookie (ROHR, 2010).

E por fim acrescenta que

> Outra técnica interessante é a armazenagem do evercookie no histórico do navegador – o recurso que registra as páginas acessadas previamente. Ele armazena o cookie como uma sequência de endereços no histórico, que o navegador acessa

> silenciosamente durante o armazenamento do cookie. Para ler é preciso verificar todas as combinações possíveis do histórico – o que é muito rápido, porque o próprio navegador faz isso usando uma série de técnicas já conhecidas. Não existe maneira legítima de simplesmente "ler" o histórico – isso em si só acontece graças à subversão de outros recursos.
>
> Por causa disso, eliminar um evercookie pode significar remover o histórico, o cache e várias outras informações armazenadas no PC que, a princípio, não deveriam ser resgatadas por um site na internet. E o pior: algumas delas nem são fáceis de serem removidas, não existindo um botão que simplesmente realize a tarefa de forma centralizada (ROHR, 2010).

Portanto, nota-se a importância de destacar as funcionalidades das espécies de cookies, haja vista os respectivos reflexos em relação à violação da privacidade.

3 RISCOS À PRIVACIDADE FRENTE AS NOVAS TECNOLOGIAS

Com o decorrer das décadas os direitos humanos se positivaram nas constituições. Na República Federativa do Brasil, estabelecida como um Estado Democrático de Direito, a preocupação com os direitos do cidadão é claramente uma resposta ao período histórico diretamente anterior ao da promulgação da constituição, a chamada "ditadura militar". Durante vinte anos o povo foi repetidamente privado de inúmeros direitos e garantias básicas e fundamentais.

Desse modo, entre tais direitos fundamentais, tem-se o disposto no art. 5º, X, onde se encontra a garantida da inviolabilidade a intimidade e a vida privada (BRASIL, 1998, p. 8), conforme já discutido no primeiro tópico do presente artigo.

Entre os mais atentos e informados usuários da Internet, quem nunca se deparou com ofertas, promoções, anúncios oferecidos que atendessem suas preferências pessoais e entre estas, várias que tenham total relação aos *likes*, compartilhamentos e visualizações anteriores?

Os *cookies* ajudam a indicar a predileção de compras de um usuário além de apenas identifica-lo. Nas palavras de Deitel (2010, p. 971) "quando um servidor *Web* recebe uma solicitação de um cliente, o servidor pode examinar o(s) *cookie(s)* que ele enviou ao cliente durante a comunicação anterior, identificar as preferências [...] e exibir imediatamente produtos que interessem ao cliente".

Como evidência do valor que tem os dados coletados para as grandes corporações, Gonçalves (2007, p. 97) ressalta que a capacidade de identificar clientes e personalizar conteúdo permitiu ao comércio eletrônico Amazon.com tornar-se tão poderoso e prestigiado contemporaneamente.

Como um diretório digital, todos os acessos e preferências ficam registrados e criam um perfil de usuário. Como dizem Morey, Forbath e Schoop (2016, p. 46): "Os primeiros coletores de dados pessoais da internet foram os websites e aplicativos. Ao rastrear as atividades dos usuários online, os profissionais de marketing podiam oferecer anúncios e conteúdo direcionados [...]. A personificação permitida por esses dados, como a constante adaptação às preferências dos usuários, tornou-se central à experiência do produto".

Desde quando criado pela Netscape, os cookies além da permitirem uma melhor interação servidor-navegador têm sido utilizados para "espionar os hábitos dos usuários na internet", permitindo assim ser traçado um perfil social, íntimo, preferencial e econômico. (SANTOS, 2001, p. 197).

Santos (2001, p. 197) ainda ressalta a origem da preocupação da utilização de cookies: "Depois que a Netscape criou o cookie, na sua versão 2.0, nos idos de 1995, teve início toda uma série de discussão sobre a validade da prática e se não há invasão à intimidade toda vez que o usuário é rastreado na internet".

De acordo com Silva (2016, p. 209), o perigo torna-se cada vez maior quanto mais a "utilização da informática facilita a interconexão de fichários com a possibilidade de formar

grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até mesmo sem seu conhecimento".

Herrmann (1997, p. 267) explica como os *cookies* são usados na identificação dos clientes ao salientar que "os cookies serão passados entre o cliente e o servidor nos dois sentidos, de modo a identificar um cliente da Web em particular."

Aduz Santos (2011, p. 197) que, "sob pretexto de produzir informações que não passarão do traçar de um perfil do consumidor, o servidor pode desbordar dos limites dessas simples informações e ter funda ingerência na intimidade das pessoas." Assim, por práticas ditas inofensivas, podem-se adquirir informações valiosíssimas.

Nessa seara, alerta Paesani (2006, p. 55) que as informações a respeito do comportamento do usuário na rede "são utilizadas para várias finalidades ou vendidas para um mercado que as considera um produto de grande interesse".

Nessa dimensão, insta esclarecer que a doutrina espanhola explora a teoria do mosaico em face da preocupação com os dados coletados (BESSA, 2017, p. 202). A aplicação da teoria do mosaico trata da "união de pequenos dados, tal qual num mosaico, que possibilita o acesso a relevantes informações acerca do indivíduo" (MORASSUTTIA, 2015, p. 159).

Assim, como o mosaico é uma figura criada a partir de pequenos pontos, dados veiculados pela Internet, que aparentemente, parecem irrelevantes enquanto informação como, por exemplo, os relativos a antigos locais de estudo, preferência musical e nome do cachorro, quando reunidos em um banco de dados possibilitarão formar a personalidade do usuário (informações tão pessoais que só a própria pessoa tenderia a saber). Informações e dados pessoais que aparentemente seriam irrelevantes, mas que permitem construir um cenário violador do direito a privacidade do usuário.

Preceitua o artigo 11 da Lei nº 12.965/2014, que "em todas as atividades que envolvam coleta, armazenamento, guarda

e tratamento de quaisquer dos registros eletrônicos", é imprescindível que "sejam respeitados o direito à privacidade e a proteção aos dados pessoais" (LIMA, 2014, p. 158).

Afora a tutela da privacidade, O Marco Civil da Internet sedimenta outros princípios fundamentais, em cujo contexto se inserem a neutralidade da rede e a liberdade de expressão.

De acordo com Ramos (2014, p. 166), a neutralidade de rede "é um princípio de arquitetura de rede que endereça aos provedores de acesso o dever de tratar os pacotes de dados que trafegam em suas redes de forma isonômica, não os discriminando em razão de seu conteúdo ou origem".

Para tanto, Ramos (2014, p. 166) conceitua provedor de acesso enquanto "empresas de telecomunicação provedoras de acesso à internet, em qualquer modalidade (dial-up, banda larga fixa ou banda larga móvel – 2G, 3G ou 4G)". Por sua vez, o Marco Civil da Internet conceitua conexão à internet como "a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP" (BRASIL, 2014).

Ramos (2014, p. 166) enfatiza que, em síntese, os artigos científicos que enfrentaram o tema permitem identificar elementos constitutivos da neutralidade de rede, em cujo contexto se insere a vedação de os provedores de acesso bloquearem requisições a *sites* e aplicações de *Internet*, assim como "arbitrariamente reduzir a velocidade" ou obstaculizar o "acesso a aplicações específicas"; "impedir a cobrança diferenciada para acesso a determinados conteúdos e aplicações", o que não impede a cobrança de valores distintos em face da contratação da velocidade ou capacidade da banda; impõe que os provedores de acesso adotem políticas transparentes a "respeito de sues padrões técnicos de gerenciamento de tráfego".

Em relação à liberdade de expressão, Viana (2014, p. 130, grifo nosso) a pontua enquanto um "rótulo jurídico-semântico" de gênero, que compreende as espécies: "(a) [...] liberdade

da manifestação do pensamento, (b) liberdade de consciência e de expressão religiosa, (c) liberdade de expressão da atividade intelectual, artística, científica e de comunicação e (d) *liberdade de informação*".

Ao enfrentar a dimensão conceitual de liberdade, Silva (2016, p. 232, grifo do autor) salienta que esta "consiste na ausência de toda coação *anormal, ilegítima* e *imoral".* Logo, toda e qualquer restrição à liberdade só poderá decorrer de "lei normal, moral e legítima, no sentido de que seja consentida por aqueles cuja liberdade restringe".

No que tange ao ambiente da liberdade de informação, Greco (1974, p. 38 apud SILVA, 2016, p. 245) salienta compreender dois aspectos: a liberdade de informar, enquanto expressão do pensamento materializado na palavra, independentemente do suporte de difusão para difundí-la, e a liberdade de ser informado, pontuada pelo "interesse sempre crescente da coletividade para que tanto os indivíduos como a comunidade estejam informados para o exercício consciente das liberdades públicas".

Segundo Martins (2014), ao discorrer sobre a neutralidade na rede mundial de computadores, afirma que tal princípio "[...] prevê que o tráfego de qualquer dado deve ser feito com a mesma qualidade e velocidade, sem discriminação, sejam dados, vídeos, etc".

Logo, nota-se conflito entre o princípio da neutralidade da rede e a ação de sites de aplicações de Internet que condicionam o pleno funcionamento dos serviços oferecidos à instalação de cookies por parte do usuário, violando, inclusive, a liberdade do indivíduo de ser informado. O princípio da neutralidade seria aplicável ao provedor de aplicação de Internet?

Conforme abordado em tópico precedente, o Marco Civil da Internet também tutela a privacidade no decorrer do uso da rede mundial de computadores no Brasil. O legislador infraconstitucional, no entanto, abordou a privacidade sob a dimensão de seu vínculo com os dados pessoais.

Nesse sentido, destaca Martins (2014) que

> O marco também garante a privacidade dos usuários da internet, ao estabelecer que informações pessoais e registros de acesso só poderão ser vendidos se o usuário autorizar expressamente a operação comercial. Atualmente, os dados são usados por grandes empresas para obter mais receitas publicitárias, já que elas têm acesso a detalhes sobres as preferências e opções dos internautas e acabam vendendo produtos direcionados.

Desse modo, "os internautas deverão, de acordo com a lei, ter informações claras e completas sobre os contratos de prestação de serviços e coleta, uso, armazenamento, tratamento e proteção de dados pessoais, bem como ter garantida a acessibilidade", considerando "as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário" (MARTINS, 2014).

Com efeito, resta evidente que os provedores de aplicações "[...] não podem usar dados dos usuários com fins comerciais, mas têm que guardar esses dados por pelo menos seis meses". Referida lei ainda impõe às empresas estrangeiras sujeitarem-se "as leis brasileiras de segurança à informação, ainda que os centros de armazenamentos de dados (datacenters) estejam fisicamente fora do país" (FIOCRUZ, 2016).

Portanto, "o Marco Civil da Internet define regras mais claras a respeito dos direitos, deveres e princípios para o uso da rede no Brasil", reconhecendo no "ambiente virtual princípios constitucionais como a liberdade de expressão, a privacidade e os direitos humanos, além de definir a responsabilidades dos provedores de serviços e orientar a atuação do Estado no desenvolvimento e uso da rede" (MARTINS, 2014).

Ademais, salienta-se, os dados pessoais e informações dos usuários estão resguardados pela cláusula geral de resguardo da intimidade, disposta no artigo 5º, X da Constituição Federal, sendo, portanto, a proteção dos dados e informações latente ao direito fundamental à privacidade.

Deveras, "o direito à privacidade e à intimidade nada

mais é do que projeção da dignidade humana", assim, "para ser digno, é necessário que o ser humano possa dispor, no âmbito da sua esfera individual, de um largo espaço em que prefira permanecer sozinho, sem a intromissão de terceiros", no qual "esse reduto diz respeito à própria liberdade individual", sendo que "nem o Estado, muito menos outros indivíduos podem nele interferir" (SANTOS, 2001, p. 166).

Posto isso, denota-se que a utilização oculta de *cookies* ou condicionar o usuário ao acesso de sites apenas com a habilitação da respectiva ferramenta viola o princípio constitucional do direito à intimidade, assim como o Marco Civil da Internet, no que tange ao princípio da neutralidade.

CONSIDERAÇÕES FINAIS

O avanço tecnológico ocasiona vulnerabilidade nos direitos básicos dos cidadãos como a violação à privacidade, pois os cookies permitem descobrir, armazenar e compartilhar informações particulares e eventualmente sensíveis.

Para aplicação das leis vigentes referentes ao Direito e à Internet é preciso entender que o ciberespaço é uma extensão do mundo real, onde há particularidades inerentes a ele.

Entretanto, o ciberespaço só existe em decorrência da criação e gestão humana. Logo, a proteção dos dados pessoais, face ao uso das novas tecnologias, deve ter como base os direitos e deveres já estabelecidos na Constituição. Direitos que visam salvaguardar a dignidade da pessoa humana. Dignidade, que muitas vezes, de modo silencioso e despercebido, é violada pelos cookies.

Ressalta-se, também, que mesmo em face ao Marco Civil da Internet, o direito à privacidade continua a ser violado. Primordial torna-se, portanto, a conscientização dos usuários quanto à disponibilização de dados pessoais e as formas de uso das ferramentas tecnológicas.

Ainda, nesse sentido, nota-se que a legislação vigente da matéria só será eficaz quando aplicada, para isto é necessário à conscientização dos usuários da rede e o cumprimento das normas tantos por entidades, quanto pelos usuários. Como assinala Reale (2006, p. 113): "O Direito autêntico não é apenas declarado, mas reconhecido, é vivido pela sociedade, como algo que se incorpora e se integra na sua maneira de conduzir-se. A regra de direito deve, por conseguinte, ser formalmente válida e socialmente eficaz".

Portanto, todo usuário deve ter sua privacidade protegida e garantia pelo Estado e pela sociedade, sendo certo que Constituição Federal assegura o direito à privacidade ao dispor sobre os direitos fundamentais. Desse modo, na esfera real ou no ciberespaço os direitos inerentes as pessoas devem ser preservados e praticados, mas ainda tendo em vista que a melhor proteção é a informação e o cuidado individual.

Para tanto, a obtenção e utilização de dados pessoais sem o consentimento dos usuários caracteriza violação à privacidade, ferindo a dignidade da pessoa humana, motivo pelo qual propõe-se um modelo de transparência desde a coleta até a utilização dos dados pessoais, de forma a estar ao alcance dos usuários tanto a autorização para a coleta e uso quanto a desistência e exclusão total dos dados pessoais por parte lo titular da aplicação de Internet

Nesse contexto, o usuário deveria ter assegurado a informação clara e precisa sobre a instalação de cookie, sua espécie e funcionalidade, quais dados são coletados pela ferramenta, qual o tratamento aos dados são conferidos pelo provedor, inclusive com a opção de poder navegar no sítio sem a necessidade de instalação do cookie, em observância ao princípio da neutralidade da rede, bem como ter um canal seguro para fazer postular o direito de correção dos dados armazenados e que contenham erro, sem que, para tanto, tenha que ingressar com Habeas data, assim como, pelo mesmo canal, solicitar a exclusão definitiva, a

qualquer tempo, de seus dados pessoais armazenados pelo provedor, em especial, quando houver cisão no relacionamento entre as partes.

REFERÊNCIAS

BESSA, Leonardo Roscoe. Os bancos de dados de proteção ao crédito na visão do Superior Tribunal de Justiça, *Revista de Direito do Consumidor*, São Paulo, v. 63, p. 202, jul. 2007.

BRASIL. Constituição Federal: de 05 de outubro de 1988. In: Vade Mecum compacto. 7. ed. atual. e ampl. São Paulo: Saraiva, 2012. p. 7-92.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 24 abr. 2014. ed. 77. Seção 1. p.1. Disponível em <http://www.planalto.gov.br/ ccivil_03/2014/lei/l12965.htm>. Acesso em: 10 mar. 2017.

CANOTILHO, José Joaquim Gomes. *Direito Constitucional*: e a teoria da constituição. 7. ed. Coimbra: Almedina, 2003. 1522p.

DAVARA RODRÍGUEZ, Miguel Ángel. Manual de Derecho Informático. Ed. 10. Navarra: Arazandi, 2008. 534p.

DOTTI, René Ariel. *Proteção da vida privada e liberdade de informação*. São Paulo: RT, 1980. 299p.

DIETEL, P.; DIETEL, H. *Java como programar*. 8ª ed. São Paulo: Pearson Prentice Hall, 2010.

FRANCO, Eduardo V; RUGGIERO, Wilson V. Análise de Comportamento de Consumidores por Agrupamento de Sessões para Avaliar o Consumo de Recursos

Computacionais e de Comunicação. *Revista de Engenharia de Computação e Sistemas Digitais*, n. 3, 2007. Disponível em: <http://www.revistas.usp.br/recs/article/view/53357>. Acesso em: 12 mar. 2017.

FIOCRUZ. *Princípios fundamentais do Marco Civil da Internet*. Disponível em: <http://portal.fiocruz.br/pt-br/content/principios-fundamentais-do-marco-civil-da-internet>. Acesso em: 09 out. 2016.

GONÇALVES, Edson. *Desenvolvendo aplicações Web com JSP Servelets, Java Server Faces, Hibernate, EJB3 Persistence e Ajax*. Rio de Janeiro: Ciência Moderna, 2007.

HERRMANN, Eric. *Aprenda em 1 semana programação CGI com PERL 5*. Rio de Janeiro: Campus, 1997.

LIMA, Caio César Carvalho. Garantia da privacidade e dados pessoais à luz do marco civil da internet. In: LEITE, George Salomão; LEMOS, Ronaldo. *Marco civil da internet.* São Paulo: Atlas, 2014. p. 148-164.

MARTINS, Helena. *Entenda os três princípios do Marco Civil da Internet*, 2014. Dipsonível em: <http://www.jcnet.com.br/Geral/2014/04/entenda-os-tres-principios-do-marco-civil-da-internet.html>. Acesso em: 09 out. 2016.

MEIRA, Laís Moreschi de; SOARES, Matheus Fernandes de Souza; PIRES, Panmella Rodrigues. *Direito à privacidade e as relações na internet*, 2012. Disponível em: <http://www.jurisway.org.br/v2/7319>. Acesso em: 09 out. 2016. 12p.

MIRANDA, Jorge. *Manual de Direito Constitucional*: Tomo IV, Direitos Fundamentais. Coimbra: Editora Coimbra, 2012. 472p.

MORASSUTTIA, Bruno Schmitt. Considerações sobre bancos de dados e o comércio de informações. *Revista Direito & Justiça*, v. 41, n. 2, p. 154-166, jul.-dez. 2015. Disponível em:

<http://revistaseletronicas.pucrs.br/ojs/index.php/fadir/article/viewFile/21428/13325>. Acesso em: 21 out. 2017.

MOREY, Timothy; FORBATH, Theodore; SCHOOP, Allison. Dados dos consumidores: modelos de transferência e confiança. *Revista Havard Business Review:* Brasil, v. 94, n. 02, São Paulo, fev., 2016.

ONU. Declaração Universal dos Direitos do Homem e do Cidadão, 1789. Disponível em: < http://pfdc.pgr.mpf.mp.br/atuacao-e-conteudos-de-apoio/legislacao/direitos-humanos/declar_dir_homem_cidadao.pdf>. Acesso em: 21 out. 2017.

PACHECO, Xavier. *Guia do desenvolvedor de Delphi for .NET*. São Paulo: Pearson Makron Books, 2005.

PAESANI, Liliana Minardi. Direito e internet: Liberdade de informação privacidade e responsabilidade Civil. 3ª ed. São Paulo: Atlas, 2006.

PRETTO, Nelson. Neutralidade da rede no marco civil da internet, 2017. Disponível em: <http://marcocivil.cgi.br/contribution/neutralidade-da-rede-no-marco-civil-da-internet/139>. Acesso em: 10 mar. 2017.

QUEIROZ, Anderson Apolônio Lira. *A invasão de privacidade na Internet:* um modelo de boas práticas e uma proposta interativa de proteção da privacidade por meio dos *cookies*. Dissertação (Mestrado). Universidade Federal de Pernambuco, Recife, 2011. Disponível em: <http://repositorio.ufpe.br/bitstream/handle/123456789/1298/arquivo1177_1.pdf?sequence=1&isAllowed=y>. Acesso em: 02 abr. 2017.

REALE, Miguel. Lições preliminares de Direito. 27ª ed. São Paulo: Saraiva, 2006.

ROHR, Altieres. *'Cookie eterno' pode rastrear internauta e é impossível de apagar*, 2010. Disponível em:

<http://g1.globo.com/tecnologia/noticia/2010/10/cookie-eterno-pode-rastrear-internauta-e-e-impossivel-de-apagar.html>. Acesso em: 08 out. 2016.

SANTOS, Antônio Jeová. *Dano moral na internet*. São Paulo: Método, 2001.

SCARMANHÃ; Bruna de Oliveira da Silva Guesso Scarmanhã; FURLANETO NETO, Mário. O sigilo dos dados armazenados em dispositivos informáticos versus a prova pericial. *Anais* do VI Simpósio Internacional de Análise Crítica do Direito, 1. ed. – Jacarezinho, PR: UENP, 2016. Disponível em: <http://siacrid.com.br/repositorio/2016/sistema-constitucional-de-garantia-de-direitos_II.pdf>. Acesso em: 14 out. 2017.

SILVA, José Afonso. *Curso de Direito Constitucional Positivo*. ed. 39. São Paulo: Malheiros, 2016. 928p.

WEINMAN, William E. *Manual de CGI*: A mais completa referência de programação para World Wide Web. São Paulo: Makron Books, 1997.