CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Tecnologia em Segurança da Informação

André Yuri Toledo

PRIVACIDADE NA WEB:
UMA ANÁLISE SOBRE A NAVEGAÇÃO PRIVATIVA DOS NAVEGADORES

Americana, SP
2014

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Tecnologia em Segurança da Informação

André Yuri Toledo

PRIVACIDADE NA WEB:
UMA ANÁLISE SOBRE A NAVEGAÇÃO PRIVATIVA DOS NAVEGADORES

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Tecnologia em Segurança da Informação, sob a orientação do Prof.° Me. Gabriel de Souza Fedel.

Área de concentração: Segurança da Informação

Americana, SP
2014

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Toledo, André Yuri
T58p Privacidade na WEB: uma análise sobre a navegação privativa dos navegadores. / André Yuri Toledo. – Americana: 2014.
43f.

Monografia (Graduação de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Me. Gabriel de Souza Fedel

1. Segurança em sistemas de informação 2.WEB – rede de computadores I. Fedel, Gabriel de Souza II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5
681.519

PRIVACIDADE NA WEB:
UMA ANÁLISE SOBRE A NAVEGAÇÃO PRIVATIVA DOS NAVEGADORES

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 24 de Junho de 2014.

Banca Examinadora:

_____
Gabriel de Souza Fedel (Presidente)
Mestre
FATEC – Americana

_____
Aloísio Daniel Vendemiatti (Membro)
Mestre
FATEC – Americana

_____
César Augusto Crócomo (Membro)
Especialista
FATEC – Americana

DEDICATÓRIA

Dedico a presente monografia a minha mãe, por ter me instruído, me auxiliado em ser um homem de bem e por ter confiado em mim. Cheguei onde estou por suas motivações. Obrigado.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por estar aqui e por ter dado forças quando precisei, jamais me deixando desistir. Sou grato ao professor Gabriel de Souza Fedel, pela colaboração, apoio, vontade e interesse pela orientação. Além dele, ao professor Leandro Halle Najm, que também sanou minhas dúvidas referentes à monografia por quanto pôde.

Agradeço também aos colegas Vinícius Guiara e ao Fábio Henrique Ribeiro Junior, por terem contribuído para o aperfeiçoamento deste trabalho, pelo apoio constante e interesse, além das ideias gentilmente cedidas. Agradecimentos adicionais ao Vinícius Guiara, pelas correções feitas.

Finalmente, os professores Alexandre Aguado e Clerivaldo José Roccia também têm minha gratidão pelo estímulo e entusiasmo

RESUMO

A presente monografia contextualiza e apresenta uma ideia muito subjetiva, mas que é de grande interesse global: a privacidade. Seja ela corporal, pessoal ou mesmo digital, esse assunto pouco difundido possui inúmeras definições. Um dos assuntos que mais carecem de atenção é a falta de normalização sobre a privacidade *on-line* e este é um dos maiores paradigmas desta sociedade digital, que além de ter a privacidade como um de seus assuntos mais desconhecidos, pouco se preocupa com ela. Mecanismos de anonimidade são formas de garantir esse direito, contudo, este é um cenário adaptado, devendo a privacidade ter suas próprias garantias. Meios “legais” de invasão, coleta de informações de forma implícita e explícita e a definição de rastreadores *on-line* são alguns dos temas aqui discutidos. Como o foco principal deste trabalho, será analisada a forma de navegação anônima, que já é existente na maioria dos navegadores, como no Mozilla Firefox, Google Chrome e Internet Explorer. Este modo será colocado em prova por meio de um estudo de caso, confirmando ou não sua declarada eficácia.

Palavras Chave: Privacidade digital, navegação anônima, invasão de privacidade.

ABSTRACT

This monograph presents and contextualizes a very subjective idea, but it is of great global concern: privacy. Be it body, personal or even digital, this little spread issue has numerous definitions. One of the issues most in need of attention is the lack of standardization on on-line privacy and this is one of the major paradigms in this digital society, which besides having privacy as one of its unknown subjects, little cares about it. Mechanisms for anonymity are ways to ensure this right, however, this is an appropriate scenario, privacy should have its own guarantees. "Legal" invasion, implicit and explicit of gathering information and the definition of on-line trackers are some of the topics discussed here. As the main focus of this work, the incognito mode that exists on most browsers like Mozilla Firefox, Google Chrome and Internet Explorer, will be analyzed. This mode will be put into evidence through a case study, confirming or not, their declared effectiveness.

Keywords: *Digital privacy, anonymous browsing, invasion of privacy.*

SUMÁRIO

1 INTRODUÇÃO.....15

2 REVISÃO BIBLIOGRÁFICA.....17

3 FUNCIONAMENTO DA *WEB*.....18

4 O QUE É PRIVACIDADE?.....19

4.1 LEGISLAÇÃO VIGENTE.....20

5 PRIVACIDADE DIGITAL.....22

5.1 NORMALIZAÇÃO SOBRE PRIVACIDADE DE DADOS.....22

5.2 NAVEGAÇÃO EM MODO ANÔNIMO.....23

6 VIGILÂNCIA NA REDE.....25

6.1 MONITORAMENTO GOVERNAMENTAL.....25

6.2 PERSONALIZAÇÃO E RASTREAMENTO NA WEB.....27

6.2.1 MECANISMOS DE COLETA DE DADOS.....29

6.2.2 FORMULÁRIOS.....29

***6.2.3 COOKIES*.....30**

6.2.4 *WEB BUGS*.....31

6.2.5 *CLICKSTREAM*.....32

7 NAVEGAÇÃO SEGURA – ESTUDO DE CASO.....33

7.1 METODOLOGIA.....33

7.2 INTERNET EXPLORER.....34

7.3 GOOGLE CHROME.....35

7.4 MOZILLA FIREFOX.....35

7.5 RESULTADOS OBTIDOS.....36

8 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS.....41

9 REFERÊNCIAS BIBLIOGRÁFICAS.....43

LISTA DE FIGURAS E DE TABELAS

Tabela 1 - Banners e Navegadores.....38

Figura 1 - Definição de Hall sobre perímetro privativo.....20

Figura 2 - Conexões de fibras ópticas da ligada ao Reino Unido.....27

Figura 3 - Esquema de criação e ação dos cookies.....32

Figura 4 - Google Chrome em modo normal, exibindo propaganda no Tec Mundo.....39

Figura 5 - Google Chrome em modo normal, exibindo propaganda no Tech Guru.....39

Figura 6 - Google Chrome em modo anônimo no Guru Tech.....39

Figura 7 - Firefox em modo anônimo exibindo publicidade genérica no Super Downloads.....40

Figura 8 - Internet Explorer In Private exibindo banner sobre busca em modo anônimo.....40

Figura 9 - Internet Explorer exibindo banner não associado à busca feita no modo In Private.....41

1 INTRODUÇÃO

Apesar do avanço exponencial da Sociedade da Informação nos últimos anos, algumas coisas – como a ética, a segurança e a privacidade – foram ignoradas ou esquecidas. Desde os primórdios da Internet até a segunda década dos anos 2000, questões como a privacidade dos indivíduos na rede vêm sendo discutidas e até então não há uma normalização, sequer uma padronização, adequada à invasão de privacidade na Internet. (GAERTNER, 2006)

Sendo a tecnologia cada vez de mais fácil acesso e a Internet uma das maiores ferramentas da publicidade moderna, algumas questões morais e éticas devem ser avaliadas, a fim de não invadir a privacidade dos usuários.

Algumas ações relacionadas à privacidade podem ser adaptadas ao cenário digital, como invasão de conta de *e-mail*, sendo caracterizada como invasão de privacidade, amparada pela constituição. Contudo, há ainda alguns assuntos mais específicos, como a permissão de ter seus dados coletados, que estão fora de qualquer adaptação da legislação vigente no Brasil e em muitos países.

Considerando esse cenário, este trabalho tem como finalidade realizar um levantamento sobre a atual situação da privacidade digital, informando suas normalizações e suas características legais, em âmbito mundial. Em adicional, foram declaradas informações a cerca de privacidade e personalização. As principais formas de invasão da privacidade em prol da publicidade foram citadas, como *cookies* e *clickstreams*.

Com intuito de analisar melhor as questões apresentadas, durante este trabalho também foi realizado um estudo de caso sobre os navegadores populares e seus comprometimentos com as informações dos usuários, além de suas características ditas privativas, com foco no modo “Navegação Anônima”.

O método de pesquisa utilizado foi um estudo de caso, evidenciando os níveis privativos dos navegadores através da navegação em alguns *site*s. Foi feito um perfil de usuário com as mesmas tendências de pesquisa e compra, analisando se os

*site*s revelam anúncios em relação aos produtos pesquisados, bem como se os mesmos mantêm os itens procurados no Modo Anônimo.

A monografia segue organizada da seguinte forma:

No capítulo 2 descrevemos os trabalhos relacionados e a forma com a qual cada um participou deste texto.

No capítulo 3 realizamos uma introdução sobre a *Web* e aplicações de cliente-servidor e sobre a requisição HTTP. Definições de IP e DNS também foram mencionadas neste capítulo.

No capítulo 4 foi escolhida uma definição de privacidade de acordo com alguns autores e também falamos sobre a legislação da privacidade nos países, inclusive no Brasil.

No capítulo 5 foi coletado as principais legislações sobre a privacidade dos usuários na Internet. Relatamos o que é a navegação anônima, descrevendo suas funcionalidades.

No capítulo 6 foi exposto a vigilância na rede, dada por parte do governo e também por empresas publicitárias que comercializam informações e os métodos mais comuns de rastreio *online.*

No capítulo 7 foi introduzido o estudo de caso, a metodologia utilizada e descrevemos os navegadores usados, explicamos as análises A e B, além dos resultados obtidos em cada análise.

No capítulo 8 foi coletado as informações do estudo de caso e gerado as conclusões. Informamos adicionalmente, os trabalhos futuros planejados, como continuidade deste.

2 REVISÃO BIBLIOGRÁFICA

Este trabalho visa apresentar informações sobre a privacidade na *web*, conceitos sobre alguns invasores de privacidade e principalmente uma análise sobre o modo privativo que os navegadores fornecem. A fim de situar essa temática foi realizada pesquisa sobre outros trabalhos relativos à privacidade, apresentados a seguir.

Podemos destacar a dissertação de mestrado de Adriana Gaertner (GAERTNER, 2006) sobre sua análise das políticas de privacidade, auxiliando-nos principalmente sobre a legislação vigente.

De forma geral, o trabalho sobre a privacidade na rede de Piotr Pisarewicz (PISAREWICZ, 2013), auxiliou neste estudo com os conceitos sobre privacidade e *cookies*.

A tese de doutorado de Lucila Ishitani (ISHITANI, 2003) nos apresentou informações triviais a privacidade digital e *web bugs*. Neste trabalho de 2003 também foi apresentado o MASKS, um projeto que visa desenvolver um sistema que permite conciliar personalização e privacidade simultaneamente para o usuário.

A dissertação de mestrado de Luana Lobato (LOBATO, 2007) guiou-nos sobre conceitos de privacidade digital, legislação, técnicas de personalização e *cookies*.

Também obtivemos auxilio das informações contidas na monografia de Carlos Henrique de Fernandes e Fernando Mario Filho (FILHO e FERNANDES, 2003), onde buscamos informações introdutórias para a elaboração deste trabalho, bem como diversas referências.

3 FUNCIONAMENTO DA *WEB*

De acordo com Kurose (2010 p. 6), a *web* e todos os serviços de redes de computadores, para que possam se comunicar, devem seguir alguns protocolos. A maioria das comunicações se dá através de clientes (computadores solicitando alguma informação) e servidores (computadores que fornecem informações aos solicitantes).

Quando é digitado o endereço de um *site*, se está solicitando a visualização de uma página da *web* para o servidor que a mantém. Este pedido é feito com o protocolo HTTP (*Hypertext Transfer Protocol*), que funciona uma aplicação cliente-servidor. (KUROSE, 2010 p. 72)

A requisição HTTP utiliza o protocolo TCP (*Transmission Control Protocol*) como transporte adjacente, para poder chegar ao servidor. O servidor então responde o pedido de visualização e o manda para o cliente juntamente com a página a ser visualizada. (KUROSE, 2010 p. 73)

Para que haja a interação entre cliente-servidor, o solicitante precisa saber o endereço do servidor ao qual irá se conectar. Esse endereço é denominado endereço IP (*Internet Protocol*). Todos os equipamentos que trafegam pela *web* precisam ter um endereço IP. (KUROSE, 2010 p. 274)

Segundo Kurose (2010, p. 96), o serviço de DNS (*Domain Name System*), entre outras finalidades, visa facilitar a memorização dos *sites* por parte dos usuários. Ele traduz o endereço conhecido pela pessoa, por exemplo, www.linuxfoundation.org/, para o endereço IP do servidor *web* que hospeda o domínio Linux Foundation, que é 140.211.169.4[1].

Para este trabalho, é relevante mencionar que sempre que um *site* é acessado, o endereço IP do computador fica registrado na solicitação HTTP dentro do servidor *web* do portal acessado.

[1] 140.211.169.4 é o IP que o *site* da Linux Foundation responde no dia 07 de Junho de 2014, às 15h24.

4 O QUE É PRIVACIDADE?

Pela definição do Dicionário Houaiss da Língua Portuguesa (2001), privacidade diz respeito à vida privada, particular e íntima. Há também a teoria de Hubmann (HUBMANN, 1967) sobre a privacidade, classificada pelo autor em três esferas:

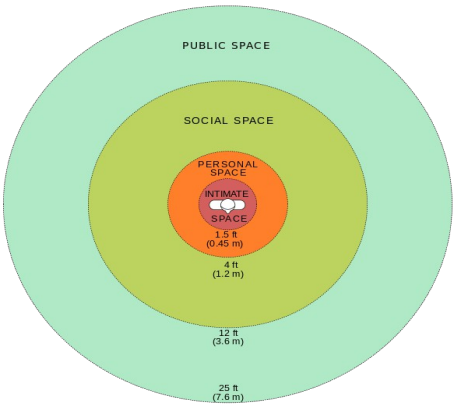
• A esfera pública, que diz respeito às informações do individuo que são conhecidas pela sociedade, sem nenhuma reserva, normalmente informações que possuem um grau de privacidade um tanto singelo;

• A esfera privada, que faz jus às informações da pessoa que são confiadas ao ambiente domiciliar, familiar ou ainda a uma pessoa de confiança, devido a isso, informações com grau de privacidade mediano se enquadram neste nível;

• A esfera íntima, na qual a privacidade atinge os níveis mais absolutos, onde se localizam as informações mais reservadas a respeito da pessoa, normalmente assuntos que nunca serão de conhecimento de outra pessoa, onde o indivíduo mantém sigilo total de seus segredos.

Edward Twitchell Hall produziu um trabalho, estabelecendo cientificamente, o perímetro pessoal de cada pessoa. Este trabalho, batizado de "*The Hidden Dimension*" foi publicado em 1966 e evidencia que a privacidade do individuo pode ser classificada em "círculos" classificando os níveis de privacidade de acordo com a distância, como demonstra em esquema, a imagem a seguir:

Figura 1 - Definição de Hall sobre perímetro privativo.



Fonte: https://en.wikipedia.org/wiki/Personal_space#mediaviewer/File:Personal_Space.svg

Como é amplamente visto em textos sobre a privacidade, uma boa definição sobre foi feita no pioneiro trabalho de Samuel Warren e Brandeis, que em 1890, publicaram um artigo intitulado “The Right of Privacy”, um notório trabalho na área de Direito. Foi deste trabalho também, de onde se originou a explicação sobre o que é privacidade: "*the right to be left alone*".

Pisarewicz (2013) completa ainda que, naquela época, as empresas de publicidade e jornalismo tinham a possibilidade de fotografar qualquer cidadão ao ar livre, uma horrenda invasão de privacidade, na concepção de Warren.

4.1 LEGISLAÇÃO VIGENTE

Em âmbito judiciário, o primeiro trabalho a respeito de privacidade legal foi de Warren e Brandeis[2], no qual se iniciou a preocupação com a mesma.

A primeira publicação sobre privacidade pessoal, que posteriormente propulsionou as demais leis sobre privacidade das pessoas foi da ONU, com a Declaração Universal dos Direitos Humanos, criada em 1948, onde todo indivíduo tem direito à privacidade, sendo este um dos direitos primordiais de cada ser humano:

> “Artigo XII: Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.”(ONU, 1948)

Em 1950, houve a declaração da Convenção Europeia dos Direitos Humanos, mencionando em seu artigo 8º que toda pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e correspondência. Ainda neste artigo, é declarado que este direito só será violado em casos previstos por lei, ou que seja necessário em caso de segurança nacional ou pública, bem como se este artigo afetar o posicionamento econômico do país.

O *Privacy Act* de 1974 dos Estados Unidos regulamenta a manutenção, uso e coleta de informações dos cidadãos por parte do governo americano. Contudo, essa lei pode ser violada em caso de:

---

[2] http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em 06 de Junho de 2014.

• Propósitos estatísticos do *United States Census Bureau*, que é o órgão governamental do censo norte-americano;

• Utilização de rotinas por parte de agências governamentais dos Estados Unidos;

• Fins de arquivamento, visando garantir e manter a preservação histórica da nação.

O Canadá, por sua vez, criou seu *Privacy Act* em 1983, que é o manuseio das informações dos cidadãos canadenses e estrangeiros por parte do governo federal. Como a lei norte-americana, o Canadá também declara que o governo não coletará informações dos indivíduos, exceto se essa coleta estiver relacionada com alguma atividade da federação.

Segundo dados do *site* InformationShield[3], podemos identificar os países e quando estes aderiram alguma lei sobre privacidade de dados ou informações pessoais, além de conter o link para o documento. As Filipinas são a nação mais nova na lista, aderindo a uma lei no ano de 2011.

Em relação à legislação brasileira, contudo, ainda não há nenhuma lei tão composta quanto a dos países citados. O que existe em relação aos direitos de privacidade, é um artigo assegurado pela Constituição Federal (Artigo 5º, incisos X e XII):

> "X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal." (BRASIL,1998)

[3] http://www.informationshield.com/intprivacylaws.html Acesso em 25 de Janeiro de 2014.

5 PRIVACIDADE DIGITAL

Ao visitar a internet, seja efetuando compras, realizando pesquisa ou mesmo por lazer, o usuário deixa rastros das informações procuradas pela *web* (LOBATO, 2007). Diante disso, diversas empresas recolhem essas informações e acabam fazendo um perfil de preferências deste usuário em questão.

Isso pode, dependendo do ponto de vista, acarretar em benefício para o usuário, permitindo que quanto mais informações forem deixadas sobre si e sobre suas preferências, mais sua navegação será personalizada, facilitando suas compras e sempre lhe informando sobre as novidades daquilo que lhe interessa.

Muitas vezes, o usuário não possui ciência sobre tal acontecimento. Essa coleta de informações, além de não ser clara, é quase nunca de real consentimento do usuário. Este exemplo clássico de coleta de informações pode ser considerado como invasão de privacidade, pois em momento algum, o usuário se viu sendo rastreado e permitindo tal fato. (ISHITANI, 2003)

5.1 NORMALIZAÇÃO SOBRE PRIVACIDADE DE DADOS

Segundo Gaertner (2006), a primeira lei sobre privacidade digital surgiu na Alemanha, na década de 70. Posteriormente, leis foram criadas na Suécia (1973), Estados Unidos (1974) e França (1977).

Por quanto exista a falta de normalização mundial para a privacidade dos usuários da internet, as organizações EPIC (*Eletronic Privacy Information Center*) e *Privacy International*, realizam em conjunto, um relatório anual a respeito do avanço das legislações sobre privacidade da informação adotadas pelos países.

Em 2003, o relatório indicava 56 países com leis sobre privacidade de dados. Dentre todos eles, os que estão em destaque são os europeus e da Oceania. (ISHITANI, 2003)

Fora do ambiente europeu, a nação que mais demonstra preocupação com assuntos relacionados à privacidade de seus cidadãos é o Canadá. Em 2001, surgiu

a lei denominada PIPEDA (*Personal Information Protection and Eletronic Documents Act*). Essa lei visa complementar a lei de privacidade do país, o *Privacy Act,* pois, uma vez que este se trata da coleta de informações dos cidadãos por conta do governo, o PIPEDA cuida em especial das coletas realizadas por empresas privadas, porém apenas aquelas com regulação federal.

Em 2004, o PIPEDA foi aprimorado, abrangendo também os vários outros tipos de empresas, incluindo as de comércio. Foi a partir dessa adequação que o Canadá passou a possuir equivalência com as leis da União Europeia, ao que diz respeito à privacidade de dados dos cidadãos.

O Brasil, por sua vez, possui alguns projetos de lei a respeito de crimes cibernéticos, contudo, atualmente possuímos apenas uma lei aprovada, a 12.737/12. Essa lei que entrou em vigor em Abril de 2013, declara:

> "Artigo 154 A: Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.[...]"(CASA CIVIL, 2012)

5.2 NAVEGAÇÃO EM MODO ANÔNIMO

Segundo Grande (2006), a privacidade é um dos principais pilares da internet, sendo de vital importância para o usuário. Dentre inúmeras formas existentes de proteger suas informações particulares na rede, um método bem conhecido é a navegação em modo privado. Seja para acessar seu *e-mail* em um computador de uso coletivo ou para realizar uma "busca pura" utilizando o Google[4], este modo pode, entre outros fins, sanar essas necessidades.

[4]http://www.apartmenttherapy.com/7-situations-where-you-should-use-private-browsing-mode-179175. Quando usado de modo normal, o Google monitora as buscas e o comportamento de seus utilizadores na *Internet*, fornecendo assim, informações relacionadas (personalizadas e não puras) aos hábitos do usuário na rede. Acesso em 27 de Abril de 2014.

Primeiramente idealizado em 2005 para o navegador Safari[5], o modo visa proteger a privacidade de seus utilizadores, das seguintes formas:

• Não guardando o histórico de navegação, pois este pode ser consultado pelos *sites* que são visitados e fornecer publicidade relacionada ao conteúdo acessado;

• Revoga a preservação de *cookies* para que, em uma nova visita aos portais, não seja relacionado o acesso anterior ao decorrente;

• Elimina o acesso de entidades terceiras na conexão que o usuário faz com o *site*, evitando a coleta de dados.

Quando o modo anônimo é aberto, existe uma mensagem descritiva sobre as características do modo. Entre as informações, os navegadores alertam que, mesmo em modo anônimo, o endereço IP do usuário ainda pode ser rastreado.

Entretanto, existem algumas pesquisas e portais da *Internet* que apontam a ineficácia desta característica. Em 2013, uma equipe de pesquisa da Universidade de Newcastle elaborou um trabalho denominado "*On the privacy of private browsing – A forensic approach*[6]", onde indicam diversas vulnerabilidades no na navegação privativa dos quatro maiores navegadores – Firefox, Google Chrome, Safari e Internet Explorer[7].

[5]http://www.lifehacker.com/102146/safaris-private-browsing-mode. Acesso em 27 de Abril de 2014.
[6]http://homepages.cs.ncl.ac.uk/m.j.forshaw1/privatebrowsing/. Acesso em 27 de Abril de 2014
[7]https://www.sciencedirect.com/science/article/pii/S2214212614000118. Acesso em 27 de Abril de 2014.

6 VIGILÂNCIA NA REDE

Segundo Tomizawa (2011), o primeiro sistema de vigilância global de redes digitais se iniciou em 1971, com o Echelon. A partir daí, governos começaram espionar para fins militares e políticos. Posteriormente, as empresas começaram a monitorar os usuários, buscando seus interesses.

6.1 MONITORAMENTO GOVERNAMENTAL

Assim como diversos artigos sobre a privacidade da informação, existe uma alusão à obra de George Orwell, o livro “1984”. Este clássico da literatura retrata uma sociedade totalitária onde não existem quaisquer indícios de privacidade dos cidadãos. Todos são constantemente vigiados pelo *Big Brother*, figura icônica e suposto líder desta sociedade. A frase imortalizada “*Big Brother is watching you*” do livro, é referenciada até hoje quando se retrata a vigilância do governo.

Toda essa vigilância se dá em prol da segurança nacional. Entretanto, é neste momento em que privacidade e segurança se encontram em dilema, onde elas se veem em uma antítese, contradizendo o fato que, sob outros aspectos, fossem sinônimos.

Foi a partir do ataque de 11 de setembro de 2001 nos Estados Unidos, que os governos começaram (ou retornaram) a se preocupar com terrorismo e segurança pública, passando assim, a monitorar a rede, em busca de tais assuntos. Sabendo que essas ações contradiriam as leis constitucionais, as agências de monitoramento criadas sempre agiram em modo anônimo, para não infringir dados aos cidadãos. (TOMIZAWA, 2011)

Em 2013, devido ao vazamento de informações da NSA (*National Security Agency)* por parte de um ex-agente, Edward Snowden, um esquema de vigilância da Internet foi revelado, o projeto PRISM, criado em 2007. Este projeto existe para impedir futuros ataques terrorista. (MACASKILL e GREENWALD, 2013). A agência conta com informações dos bancos de dados das maiores corporações de tecnologia, entre elas, o Facebook, Microsoft e Google.

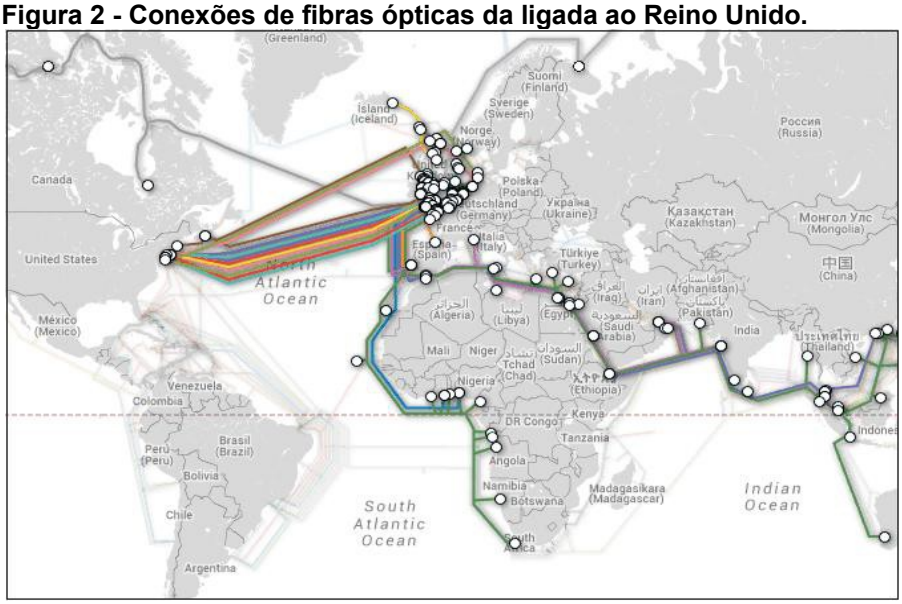
Segundo MacAskill *et al* (2013) existe, entretanto, um programa de vigilância da internet maior e mais agressivo do que o PRISM. Este programa, chamado de Tempora é de autoria da CGHQ(*Central Government Headquarters*), agência de segurança britânica. O Tempora também foi exposto ao mundo por intermédio de Edward Snowden, mesmo delator do projeto norte-americano de vigilância online.

O programa britânico não possui em teoria, uma limitação. Sua vigilância se dá através dos *backbones* de fibra óptica da Internet ligados à rede britânica, tendo acesso direto às informações que trafegam na rede. E o fato de ter esse livre acesso à rede, é o que o faz ser mais colossal, segundo um trecho de uma notícia do The Guardian:

> "Desde o ano de 2012, a agência tinha a conexão de sondas para 200 cabos de fibra óptica, cada um possuindo uma capacidade de 10 *gigabits* por segundo. Isso dava à CGHQ, em teoria, acesso a um fluxo de 21.6 *petabytes* em um dia."

Em acesso ao *site* SubmarineCableMap[8], que mostra os cabos *backbones* que interligam os continentes por meio de fibras ópticas, pode-se observar os cabos que estão sob constante monitoração do projeto Tempora:

Figura 2 - Conexões de fibras ópticas da ligada ao Reino Unido.



Fonte: www.submarinecablemap.com/#/country/united-kingdom

[8]Acesso em 05 de Junho de 2014.

Em território nacional, o que tivemos de semelhante a quaisquer indícios de vigilância da *Web* por parte do Estado, foi o projeto de lei 84 de 2011, conhecido como Lei Azeredo. Este projeto, de imediato foi batizado de AI-5 digital (Ato Institucional que visava oprimir a liberdade de expressão da população), pois se apresentava rijo em seus artigos iniciais. (SILVA *et al*, 2012)

6.2 PERSONALIZAÇÃO E RASTREAMENTO NA WEB

A internet é considerada hoje como o maior meio de comunicação em massa já criada e, com isso, o marketing *online* passou a gerar grandes lucros. Desses lucros em especial, a publicidade direcionada é a que mais possui rentabilidade. Contudo, esta se dá através da personalização dos anúncios, de acordo com os perfis dos compradores. (ISHITANI, 2003)

Grande parte dessa vigilância *online* é feita pelo Google. O gigante da tecnologia possui uma grande fatia dos serviços utilizados diariamente pelos usuários. Dentre esses serviços, podemos mencionar o Gmail, que é o serviço de *e-mail* mais utilizado do mundo, desde o final de 2012.[9] O provedor de *e-mail* já declarou que não respeita a privacidade dos usuários e informa para não esperarem confidencialidade em seus *e-mails*.[10]

No motor de busca, existe o chamado filtro-bolha, onde o Google faz uso de informações do usuário para mostrar-lhe um resultado de pesquisa personalizada, sempre variando de pessoa para pessoa.[11]

Recentemente[12], o Google atualizou seus termos de compromisso e admitiu explicitamente que possui um *software* que faz uma varredura minuciosa nos *e-mails*, tanto os em trânsito, quanto os já existentes na conta do Gmail. A nova inserção nos termos foi a seguinte:

---

[9]http://www.cnet.com/news/gmail-edges-hotmail-as-worlds-top-e-mail-service/.. Acesso em 24 de Maio de 2014.

[10]http://blogs.estadao.com.br/radar-tecnologico/2013/08/14/google-admite-que-usuarios-do-gmail-nao-tem-privacidade/. Acesso em 24 de Maio de 2014.

[11]Eli Pariser, The Filter Bubble: What the Internet Is Hiding from You.

[12] http://www.techguru.com.br/google-admite-analise-de-emails-para-vender-publicidade-sob-medida/ Acesso em 1º de Maio de 2014.

> "Nossos sistemas automatizados analisam o seu conteúdo (incluindo *e-mails*) para fornecer recursos de produtos pessoalmente relevantes para você, como resultados de pesquisa customizada, propagandas personalizadas e detecção de *spam* e *malware*. Essa análise ocorre à medida que o conteúdo é enviado e recebido, e quando ele é armazenado." (GOOGLE, 2014)[13]

A personalização é manter algo de acordo com o perfil de uma pessoa, seguindo suas preferências e vontades. É fazer com que a informação seja totalmente adaptável ao gosto do usuário. Neste cenário, personalização seria adaptar a nível individual, as características de acordo com os perfis de cada pessoa, mantendo assim, algo exclusivo para cada um. (GRANDE, 2006)

Para Gaertner (2006), a personalização tem um beneficiamento mútuo. Pelo lado do usuário, pois o mesmo pode receber informações segundo suas preferências e gostos, tornando assim uma navegação mais direcionada de acordo com seu perfil, facilitando suas rotinas.

Por outro lado, este benefício se dá principalmente pelo lado da empresa, pois a mesma, para fornecer essa facilidade da personalização colhe informações sobre os usuários e fornece a estes, aquilo que lhes é interessante. Com isso, a corporação tende a ter um maior número de visitantes, transformando posteriormente, estes visitantes em clientes.

Todavia, para tornar algo personalizado para uma pessoa em especial, é necessário se obter certas informações dela, sendo, por exemplo, convívio social, gostos musicais, áreas de atuação e preferências de bens de consumo. (GRANDE, 2006)

Para realizar este tipo de recolhimento de informações, as empresas criam e utilizam formas de coletas automáticas de informações que abrangem grande parte da rede. Esse processo, quase sempre, se dá sem o consentimento do visitante, pois, grande parte dos usuários da *web* não sabe que, acessando as páginas, são

[13] https://www.google.com/intl/pt-BR/policies/terms/.Acesso em 1º de Maio de 2014.

constantemente vigiados. Através dessa sucessão de acontecimentos de coleta e armazenagem de informações é que se dá a violação de privacidade.

6.2.1 MECANISMOS DE COLETA DE DADOS

Existem diversas formas de se criar a personalização nos *sites*. Os métodos utilizados podem ser de forma explicita ou implícita. De modo explícito, onde há a conscientização do usuário, a maneira mais utilizada é o preenchimento de formulário.

Há, contudo, a coleta implícita, que normalmente se dá sem a devida aprovação do usuário. Esta forma é a mais utilizada, pois se o usuário apenas acessar um determinado *site*, clicar em um *link*, ele já está tendo suas informações coletadas, por exemplo, pelos mecanismos de *cookies*, *web bugs* e *clickstream*.

6.2.2 FORMULÁRIOS

Dentre as coletas explícitas de informações dos visitantes, o preenchimento de formulário é método mais utilizado e um dos mais efetivos Este mecanismo consiste em oferecer ao usuário um formulário para preenchimento de suas informações pessoais (Nome completo, endereço, RG, CPF, telefone, entre outros) para que somente assim o visitante possa ter acesso a determinado conteúdo ou página do *site.* (MATOS, 2005)

Ainda que desta forma não exista a invasão da privacidade do cliente, este recurso é uma ótima forma de coleta de informações, pois, uma vez que o cliente se interessa pelo produto/serviço em questão neste *site*, ele irá preencher o formulário com suas informações de forma precisa e completa, afim de não obter quaisquer problemas com o acesso.

Em contrapartida, determinado usuário pode preencher os campos do formulário com informações errôneas, pois assim, ele pode ter acesso a tais produtos/serviços, sem comprometer suas informações pessoais.

Matos (2005) salienta ainda que, uma vez que a empresa detêm as informações dos clientes, ela pode trocar estas informações com terceiros, afim de

ampliar seu banco de informações ou lucrar, comercializando essas informações dos usuários.

6.2.3 *COOKIES*

Cookies são, segundo Lobato (2007) pequenos arquivos de texto que são armazenados no disco rígido e informados via HTTP ao servidor do *site*, através do navegador. Os *cookies* possuem validade e ao expirar, são apagados automaticamente pelo navegador.

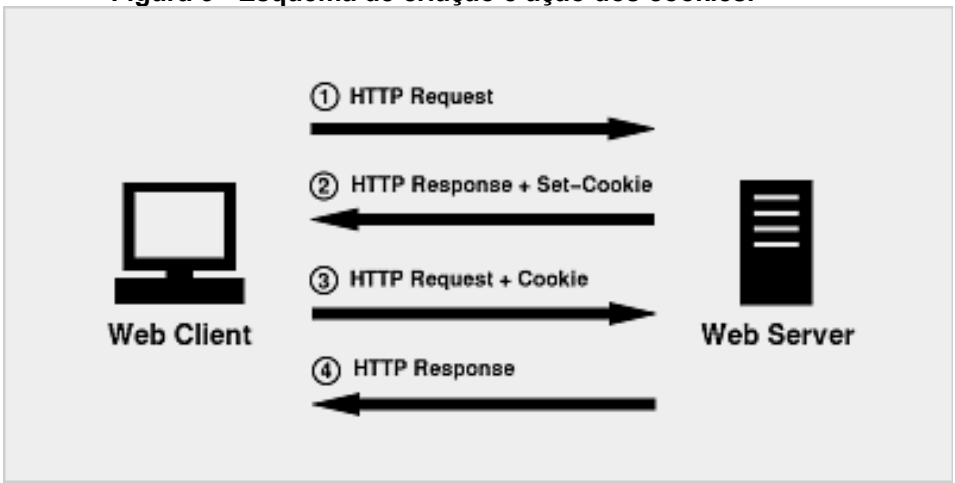
Na figura 3, podemos exemplificar o ciclo de atuação de um c*ookie.* Estes possuem a funcionalidade de informar ao *site* as preferências do usuário, fazendo assim, que este tenha uma experiência mais personalizada, facilitando sua busca e sua navegação. Dentre exemplos da atuação do *cookie*, podemos citar:

• Estatísticas de navegação, informando quantas vezes o *site* foi acessado, quando foi esse acesso, locais de mais *clicks*;

• Exposição de *banners* de propaganda, permitindo que o usuário não veja o mesmo *banner* seguidamente, fazendo um rodízio destes, propondo mais *marketing;*

• E principalmente, itens favoritos visualizados, informando ao *site* os produtos que são de interesse do usuário, fazendo com que o mesmo, em uma futura visita, tenha na *home page* itens semelhantes aos contemplados anteriormente.

Figura 3 - Esquema de criação e ação dos cookies.



Fonte: http://shiflett.org/articles/the-truth-about-sessions

De acordo com Pisarewicz (2003), há certo temor dos usuários em relação aos *cookies*, acreditando que os mesmos sejam uma fonte de vírus. Esta é uma ideia errônea, uma vez que estes são apenas arquivos de texto, não podendo executar qualquer código malicioso. Devido a isso, os *cookies* também não têm acesso a qualquer informação do disco rígido do usuário. O autor ainda nos explica que existem duas formas de *cookies*, que são:

i) *Cookies* diretos (*first-party cookies*), que se classificam como de propriedade do domínio acessado. Informações nesta classe são utilizadas apenas pelo *site* em questão, não sendo, teoricamente, informadas a *sites* terceiros.

ii) *Cookies* indiretos (*third-party cookies*) são *cookies* "terceirizados" nos quais se um produto é visualizado no *site* A, este pode vir a ser exposto posteriormente no *site* C, pois a visualização do item é enviada ao banco de dados da empresa que fornece os *cookies* indiretos para ambos os *sites* (p. ex. Adversing.com), que compartilha as informações do visitante.

6.2.4 *WEB BUGS*

Além dos *cookies,* outra forma de coletar informações dos usuários são os *Web bugs*. De acordo com Ishitani (2003) *web bugs* normalmente são transparentes e em formato GIF (*Graphics Intercharge Format*), cujo tamanho é de 1 pixel por 1 pixel. Eles monitoram as atividades dos usuários em páginas da internet e em *web-mails.*

Devido a seu tamanho, é muito difícil visualizar um *Web bug*, podendo ser confundido com um ponto, por exemplo. Eles podem ser visto mais facilmente no código-fonte do *site*. Um *Web bug* normalmente não pertence ao *site* acessado, sendo de uma empresa de publicidade (*third-party*).

Sempre que um usuário acessa um *site*, ele acaba baixando também os *Web bugs*. Estes, assim que carregados, começam a coleta de informações, que vão desde o navegador utilizado, passando pela hora em que o *site* foi acessado, até chegar ao IP do visitante. Ainda mediante Ishitani (2003) através dessas

informações, é possível verificar quantas vezes uma propaganda foi visualizada até realizar um perfil de usuário.

Alguns navegadores e certas páginas da *web* oferecem a opção de bloquear os *cookies*, para maior comodidade privativa. Contudo, não há como bloquear os *web bugs* dessa forma.

6.2.5 CLICKSTREAM

Outro mecanismo de coleta das informações dos visitantes muito utilizado é o *clickstream*. Este por sua vez, coleta informações baseado no tráfego dos visitantes entre as páginas, tempo de visualização de cada parte do *site,* além de captar seu comportamento através de seus cliques.

Segundo Amaral e Rodrigues (2007), análogo ao *clickstream*, temos a seguinte situação: Um cliente entra em uma loja de CDs. Ele pega e olha alguns, ouve músicas de outros, mas por fim, acaba levando apenas um terceiro. A loja só terá informações sobre este cliente quando ele sair e realizar o pagamento, onde o vendedor debita do estoque o CD adquirido pelo cliente.

Se esta situação acontecesse em uma loja virtual onde houvesse um *clickstream*, a situação seria a parcialmente a mesma, exceto pelo fato de que o *clickstream* teria guardado os CDs que o cliente visualizou, as sessões por onde ele passou e qual foi o CD que ele ouviu. Além é claro, daquele produto que ele comprou. Tudo isso foi analisado de forma invisível para o cliente, porém suas informações foram capturadas e enviadas ao servidor deste *clickstream*, fazendo um perfil de interesse deste usuário. (AMARAL E RODRIGUES, 2007)

O *clickstream* sozinho não fornece quaisquer dados úteis para analisar o comportamento do cliente apesar de ser uma fonte valiosa de informações. Apesar disso, ele pode ser analisado em conjunto com outros dados coletados, resultando em informação sobre o perfil de acesso.

7 NAVEGAÇÃO SEGURA – ESTUDO DE CASO

Com intuito de analisar ferramentas que visam garantir privacidade na navegação *web*, apresentamos nesse trabalho um estudo de caso. Nele será realizada uma análise no modo privativo dos navegadores, uma vez que estes garantem não armazenar rastros.

7.1 METODOLOGIA

Ao realizarmos tal investigação, selecionamos alguns *sites* de compras on-line onde faremos buscas de determinados produtos. Analisaremos se estas pesquisas serão guardadas e posteriormente em uma nova visita, confirmaremos se houve alguma guarda do perfil.

Para a análise, foram escolhidos os navegadores mais populares, segundo o StatCounter[14]: Internet Explorer, Mozilla Firefox e Google Chrome. Cada um destes navegadores possui um modo de navegação privativa os quais compartilham entre si a mesma essência de que *cookie*s e histórico de pesquisa não serão guardados após o fechamento do navegador. Serão realizados dois tipos de análise neste estudo de caso, descritas a seguir:

- Análise A: Realizaremos uma pesquisa de produtos em alguns *sites* de compras. Posteriormente, serão visitados outros *sites* que possuem anúncios para se verificar algum padrão. E por fim serão visitados, em modo anônimo, os mesmos *sites* com anúncios para verificar o comportamento.

- Análise B: Em modo anônimo, executaremos as pesquisas de produtos nos *sites* de compras. Contemplaremos também se há *banners* publicitários nos portais acessados neste mesmo modo. Finalmente, abriremos o navegador em modo normal para verificar se há algum compartilhamento de informações.

A fim de obter um resultado mais preciso acerca dos navegadores, cada um deles será testado em uma máquina virtual diferente, utilizando o *software* Virtual

[14] http://gs.statcounter.com/#all-browser-ww-monthly-201402-201402-map. Acesso em 07 de Maio de 2014.

Box versão 4.3.10 com uma instalação limpa do Windows 7, para que não haja qualquer alteração ou influência da máquina física.

Como metodologia, criamos uma rotina de pesquisa de *Smartphones* em determinadas lojas virtuais. Nesta rotina, estaremos visualizando os aparelhos de uma forma geral, não nos prendendo a sistemas ou capacidades. Foram abertas abas simultâneas de diversos aparelhos e cada uma das páginas foi vista até o final das descrições do produto.

Para selecionar as lojas, utilizamos o critério de acessos do Alexa[15], onde nos é informado que os *sites* com mais visitas são o Mercado Livre, Lojas Americanas e Submarino, respectivamente. Para verificar os *banners*, acessaremos os *sites* informativos Tec Mundo e o Tech Guru, além do *site* de *downloads* Super Download, para verificarmos se há alguma propaganda direcionada dos itens pesquisados.

7.2 INTERNET EXPLORER

O Internet Explorer é o navegador da Microsoft e foi criado em 1995. Desde então, tem sido um componente integrado a partir do Windows 98 e em todas as versões do sistema operacional[16].

Muito embora a Microsoft tenha adotado algumas diretivas de segurança, o navegador sempre foi criticado por conter falhas, possuindo sempre muitas brechas e vulnerabilidades para vírus e *malwares*. O modo privado no navegador, chamado de In Private, só foi adotado na versão 8 do Internet Explorer, em 2009.[17]

Utilizaremos a versão 9 do Internet Explorer, pois esta se mostrou ser uma versão estável do navegador, além de contar com o plug-in nativo Do Not Track, que aprimora a proteção de privacidade do usuários que não desejam ser rastreados na *web*. Como utilizamos a instalação padrão do navegador, nosso teste contou com o Do Not Track.

---

[15]http://www.alexa.com/topsites/category/World/Portugu%C3%AAs/Regional/Am%C3%A9rica_do_Sul/Brasil/Neg%C3%B3cios_e_Economia/Compras Acesso em 3 de Abril de 2014.
[16]https://en.wikipedia.org/wiki/Internet_explorer Acesso em 18 de Março de 2014.
[17] http://blogs.msdn.com/b/ie/archive/2008/08/25/ie8-and-privacy.aspx Acesso em 07 de Abril de 2014.

7.3 GOOGLE CHROME

O Google Chrome é desenvolvido pelo Google e foi lançado oficialmente em 2008. Em menos de dois anos de existência, o Chrome se tornou o 3º navegador mais utilizado. Foi somente em 2012 que ele atingiu o primeiro lugar, segundo o StatCounter[18].

O Chrome possui como base o navegador Chromium, que é um projeto *open-source* com participação comunitária, criado e mantido também pelo Google. De acordo com o blog do Chromium[19], o Chrome envia alguns dados dos usuários para os servidores do Google. Algumas dessas opções de envio de informações são facultativas, outras não.

Seu modo anônimo, chamado de Incognito, foi inserido na versão 1.0, de Dezembro de 2008. Ele foi o segundo navegador a adotar essa característica. Para este trabalho foi utilizada a versão 33, sendo esta a versão estável do navegador no momento dos testes (Março de 2014). O Google também adotou a tecnologia de Do Not Track em seu navegador a partir da versão 23. Contudo, essa opção vem por padrão desabilitada, necessitando que o usuário navegue até o menu de configurações avançadas para habilita-la.[20]Em nosso trabalho, como foi utilizada a instalação padrão do navegador, o Do Not Track estava desabilitado.

7.4 MOZILLA FIREFOX

O navegador Mozilla Firefox foi iniciado pelos desenvolvedores do Netscape e lançou sua primeira versão estável em 2004. Sendo o principal navegador de código-aberto (*open-source*), o Firefox tem cerca de 40% do seu código fonte criado por voluntários[21].

Apesar de adotar o modo privado de navegação, batizado simplesmente de Navegação Privativa em Junho de 2009, na versão 3.5, o Firefox possui uma vasta gama de recursos para garantir a privacidade e/ou a segurança dos dados dos

[18] http://gs.statcounter.com/press/chrome-overtakes-ie-globally-monthly Acesso em 31 de Março de 2014
[19]http://blog.chromium.org/2008/10/google-chrome-chromium-and-google.html Acesso em 02 de Abril de 2014.
[20]http://www.pcmag.com/article2/0,2817,2411916,00.asp Acesso em 02 de Abril de 2014.
[21]http://mashable.com/2012/09/23/firefox-10th-anniversary/ Acesso em 04 de Abril de 2014.

usuários. O Firefox também possui a característica “Do Not Track”, entretanto há também algumas características a mais do que “informar aos *sites* que não quero ser rastreado”, dentre elas, apagar os *cookie*s ao fechar a aba correspondente ao *site* ou nunca armazená-los.

O navegador da Mozilla também é conhecido por sua grande diversidade de extensões. Essas extensões têm como funcionalidade melhorar ou implementar determinada característica no navegador, como o AdBlock Plus[22], que visa bloquear os *banners* de publicidade que aparecem nos *sites.* O navegador da Mozilla também é o primeiro que desde a criação, possui suporte para extensões. A versão utilizada nos testes deste navegador foi a 29.0.

O Firefox enfatiza que se preocupa com a privacidade dos usuários. Essa informação é afirmada pelo próprio Mozilla[23], além disso, o Firefox foi o único dos grandes navegadores que não estava relacionado ao escândalo de vigilância da NSA.

7.5 RESULTADOS OBTIDOS

Começamos os testes com a análise A, onde observamos que, no quesito de não guardar histórico dos *sites* visitados, todos os navegadores em modo anônimo confirmaram essa funcionalidade. Nenhum dos *sites* visitados aparece no histórico ou no *cache* do modo normal. Percebemos que o histórico e o *cache* são acessados em modo anônimo. Pôde-se notar também que, se mantidas ambas as janelas abertas, o histórico é compartilhado simultaneamente com o modo privativo.

Em relação ao *cookies*, também houve a coesão com as declarações de advertência privativa dos navegadores. Em modo normal, diversos *cookies* foram criados a partir dos acessos ao Submarino, Mercado Livre e Americanas, dentre eles o Google AdWords, Xaris, Vizury, Maxymiser, New Relic entre outros.

De acordo com a tabela 1, nos navegadores Firefox e Chrome, todos os *banners* eram patrocinados pelo Google, através do AdSense[24]. Esse *banner* é

[22]https://adblockplus.org Acesso em 04 de Abril de 2014.
[23]https://webwewant.mozilla.org/pt-br/ Acesso em 1º de Maio de 2014.
[24] https://support.google.com/adsense/troubleshooter/1631343?hl=pt-BR. Acesso em 1º de Maio de 2014

exibido nos *site*s que participam da Rede de Display do Google, ou em parceiros. Os anúncios são exibidos de acordo com os *site*s acessados pelo usuário, como também com base nos seus interesses, entre outros fatores.

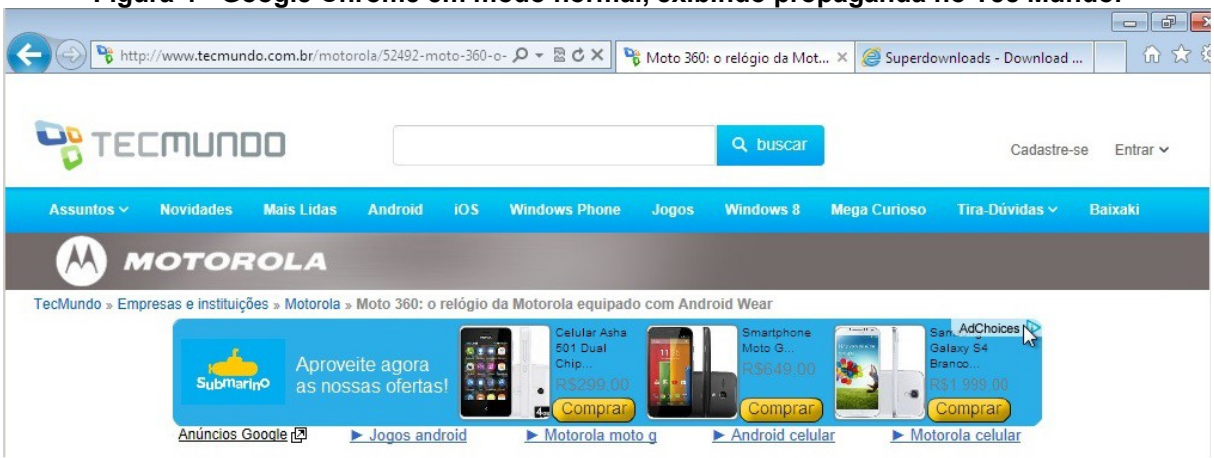
Tabela 1 – Banners e Navegadores

	Mozilla Firefox	Google Chrome	Internet Explorer
Guru Tech	Ad Sense	Ad Sense	Ad Sense
Tec Mundo	Ad Sense	Ad Sense	AdChoices
Super Downloads	Ad Sense	Ad Sense	AdChoices

Fonte: Autoria própria

Entretanto, nos *banners* apresentados nos *site*s Tec Mundo e Super Downloads no navegador Internet Explorer, houve uma pequena participação do AdChoices em relação ao exibidor dos produtos. Esse provedor de anúncios publicitários personalizados é uma subdivisão do Yahoo. Ele, segundo sua própria definição,[25] "trabalha em conjunto com empresas de publicidade *on-line* para prover ao consumidor apenas anúncios que sejam relevantes e úteis quanto possível".

Figura 4 - Google Chrome em modo normal, exibindo propaganda no Tec Mundo.



Fonte: Autoria própria

Os *banners* relacionados aos produtos escolhidos se apresentavam em praticamente todas as visualizações dos *sites* de notícias, podendo ser confirmado

[25] https://info.yahoo.com/privacy/us/yahoo/relevantads.html. Acesso em 1º de Maio de 2014.

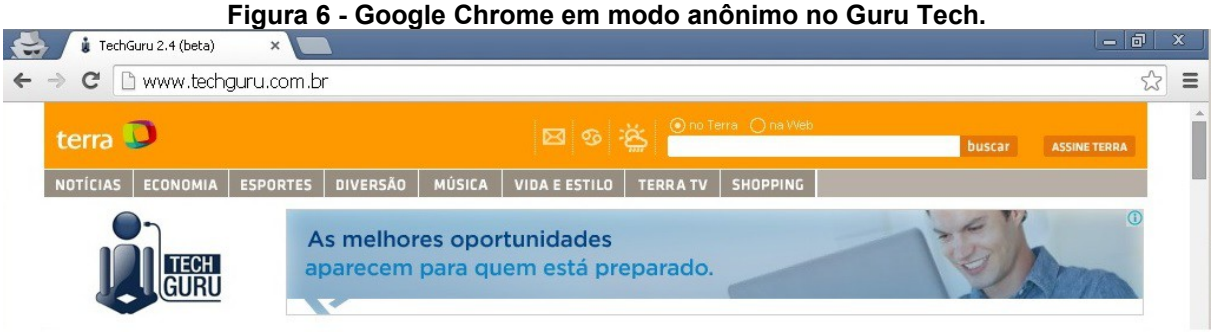
de acordo com a figura 4. Quando não, os *displays* apresentavam propagandas diversas, entre carros e imóveis. O Chrome e o Firefox se reservaram, quando não personalizados, a mostrar numerosas publicidades dos produtos Google, como sugestão de inscrição no Gmail e no Apps for Business.

Figura 5 - Google Chrome em modo normal, exibindo propaganda no Tech Guru.

Fonte: Autoria própria

A comparação foi feita no mesmo tempo em que a aba normal estava aberta exibindo o *display* do Submarino e instantaneamente foi aberta a janela anônima, que se demonstrou livre de *cookies,* como pode ser observado nas figuras 5 e 6.

Figura 6 - Google Chrome em modo anônimo no Guru Tech.



Fonte: Autoria própria

Já na visualização dos *site*s de notícias em modo anônimo, não foi apresentado nenhum *display* relacionado a *smartphones,* que foi o produto procurado. Houve apenas as exibições padrão de publicidade generalizada, como na figura 7, por exemplo, a Nextel, vestibular da FGV e modem da VIVO, dentre outros. Não houve nenhum vínculo publicitário entre os modos.

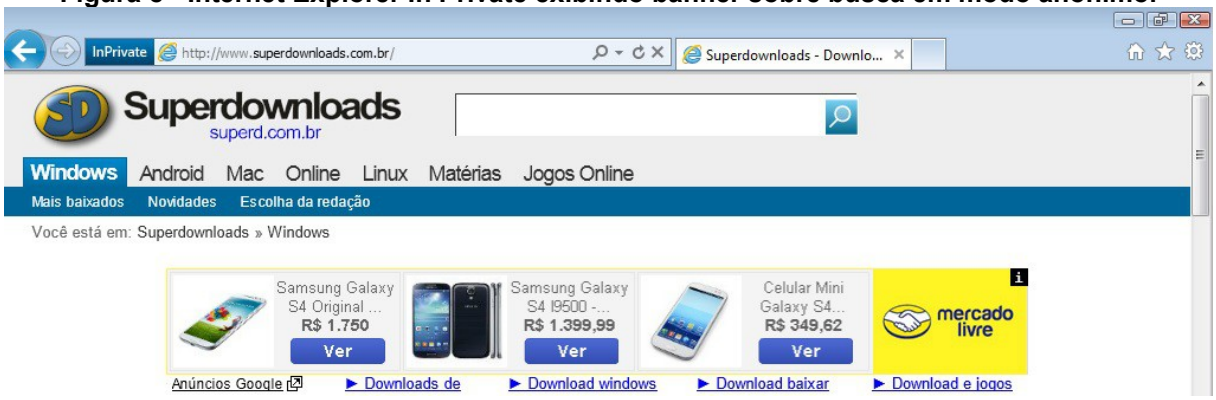
Figura 7 - Firefox em modo anônimo exibindo publicidade genérica no Super Downloads.

Fonte: Autoria própria

Ao final da Análise A, foi realizada a limpeza dos dados de navegação, como *cookies,* históricos e *cache*. Ao voltar para os *sites* de notícias, nenhuma personalização foi detectada, estando limpo de informações preferenciais.

Executamos a partir daqui, a Análise B: Realizar as buscas dos produtos em modo anônimo e verificar os *banners* em modo normal, para sabermos se há algum vinculo, de acordo com a Figura 8. Após ter visualizado diversos *smartphones*, contemplamos inúmeras vezes os portais de notícias e nenhum compartilhamento de informações foi identificado.

Figura 8 - Internet Explorer In Private exibindo banner sobre busca em modo anônimo.

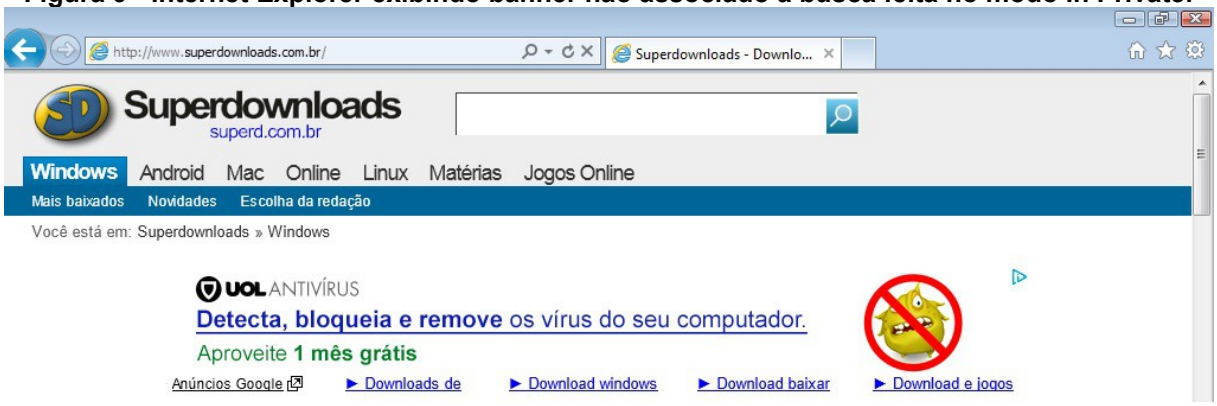


Fonte: Autoria própria

Em adicional, após ter buscado os celulares em modo anônimo, também foi observado que o Super Downloads e os outros apresentavam *banner*s publicitários,

ainda em modo anônimo. Ao verificarmos no modo normal, nenhuma informação coletada em modo anônimo foi compartilhada, como visto na Figura 9.

Figura 9 - Internet Explorer exibindo banner não associado à busca feita no modo In Private.



Fonte: Autoria própria

Também foi observado que a busca realizada no *site* da loja não gera *cookies*. Estes apenas são gerados ao clicar em algum determinado produto. Ao fazer isso, foi observado o tempo de resposta da personalização, desde a criação do *cookie* até a apresentação do mesmo no portal de notícia, que foi de 8 segundos. O primeiro *smartphone* exibido no *banner* foi exatamente o mesmo buscado na loja.

Mediante este estudo, podemos constatar que o modo anônimo funciona como um segundo navegador, tendo seus próprios *banners* e *cookies*, contudo não os salvando assim que o navegador é fechado. Assim podemos utiliza-lo a fim de não deixar rastros sobre interesses ou buscas que vamos realizar, auxiliando na nossa privacidade na *web*.

8 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

A sociedade digital ainda está dando seus primeiros passos no cotidiano das pessoas, e a sua privacidade, é um assunto mais recente ainda. Este trabalho apresentou alguns conceitos sobre a privacidade e a legislação vigente em alguns países onde o assunto vem ganhando notoriedade.

Os usuários da Internet muitas vezes não sabem que, ao acessar um *site* ou compartilhar alguma informação em uma rede social, estão na verdade criando um

perfil de comprador em potencial para as empresas publicitárias interessadas em suas preferências.

Muitas vezes não é culpa do individuo, pois esses rastreadores publicitários estão “invisíveis”, monitorando-os nos *sites* que acessam. As pessoas estão interessadas em proteger sua privacidade, mas, talvez pelo fato de não terem conhecimento técnico para identificar ou mesmo anular a “internet invisível”, muitas vezes acabam deixando essa preocupação de lado.

Contemplamos que, sem muito esforço, o governo e algumas empresas, como o Google, podem ter acesso às informações sobre os usuários na rede, através dos serviços por estes utilizados. Os rastreadores das empresas de *marketing* direcionado estão presentes na grande maioria dos *sites,* sempre visando colheres informações dos visitantes.

A partir do estudo de caso realizado, podemos perceber que o modo anônimo serve para uma navegação onde não há histórico dos lugares visitados. Sobre os *cookies,* estes são criados na visita ao *site,* mais assim que a página é fechada, estes arquivos são automaticamente excluídos do disco rígido do usuário. Isto pôde ser observado quando acessamos as lojas e posteriormente, os portais de notícias.

Através do estudo de caso, podemos concluir que utilizar o modo anônimo consegue manter as informações do usuário segura das empresas publicitárias que rastreiam os usuários na rede, buscando suas preferências.

Quando há o acesso a qualquer *site* da Internet, existe a exposição do endereço IP do usuário, mesmo que o acesso tenha vindo de um navegador em modo anônimo. Mediante isso, é correto afirmar que a navegação anônima se mantém privada até determinado ponto, onde na maioria das vezes, já é útil para um usuário comum.

Também de acordo com este trabalho, podemos ver que os modos anônimos dos três navegadores se comportam da mesma forma, mantendo a privacidade assim que o navegador é fechado.

Mesmo se o usuário estiver de acordo com a coleta de informações pessoais para personalização, existe ainda outro impasse: a retenção dessas informações por parte do mantenedor do *site.* Não há garantias de que essas informações não serão compartilhadas com terceiros, vendidas ou mesmo trocadas com outras fontes interessadas. Diversas corporações faturam bilhões com venda de informações de seus usuários, seja para empresas ou para espionagem governamental.[26]

Durante a execução do trabalho foi percebido a possibilidade de alguns trabalhos futuros, como: expandir o quesito privacidade na *web* também para os motores de busca, realizando uma análise sobre o buscador Google e o DuckDuckGo[27]. Além disso, poderá ser feito um levantamento sobre os provedores de *e-mail* e seus comprometimentos com a privacidade dos utilizadores.

Também se pode realizar uma observação sobre o comportamento do navegador TOR, que é famoso por garantir anonimidade na navegação sob ele realizada. Nele, poderão ser realizadas as Análises A e B, a fim de conhecermos o nível de sua anonimidade.

Ademais, pode-se criar uma pesquisa de campo para saber o nível de preocupação dos usuários com suas informações pessoais, seus conhecimentos a respeito do rastreamento publicitário e governamental.

[26]http://www.huffingtonpost.com/2013/07/08/att-selling-data_n_3561263.html. Acesso em 24 de Maio de 2014.

[27] https://duckduckgo.com/. Buscador da internet semelhante ao Google, contudo que não rastreia o usuário, nem cria um resultado de pesquisa tendenciosa baseado no perfil de informações do usuário. Acesso em 06 de Junho de 2014.

9 REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, G. C. M.; RODRIGUES, A. S. 2003. ***Clickstream* no Sistema de Acompanhamento do Plano Diretor.** Disponível em: <http://www.mar.mil.br/sdms/artigos/6847.pdf>. Acesso em 21 de Novembro de 2013.

BRASIL, Casa Civil. **Lei 12737/2012 – Tipificação Criminal de Delitos informáticos.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 06 de Novembro de 2013.

BRASIL, Constituição (1998): **Constituição da República Federativa do Brasil**. Disponível em: <http://www.senado.gov.br/legislacao/const/con1988/CON1988_02.09.1999/art_5_.shtm>. Acesso em 06 de Novembro de 2013.

CANADA, **Justice Laws Website, 2014.** Disponível em: < http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html >. Acesso em 24 de Fevereiro de 2014.

FERNANDES, C. H.; FILHO, F. M. O. **A Privacidade na Sociedade da Informação**, 2003. Disponível em: <https://linux.ime.usp.br/~carloshf/0302-mac339/fase2/privacidade.pdf> Acesso em 07 de Novembro de 2013.

GAERTNER, Adriana. **Privacidade - Ausência de Normalização, 2005.** Disponível em: <http://egov.ufsc.br/portal/*sites*/default/files/anexos/15640-15641-1-PB.pdf>. Acesso em 06 de Novembro de 2013.

GAERTNER, Adriana. **Privacidade da Informação: Um Estudo das Políticas no Comércio Eletrônico, 2006**. Disponível em: <https://repositorio.ufba.br/ri/bitstream/ri/12024/1/_Adriana_Gaertner_disserta%C3%A7%C3%A3o.pdf>. Acesso em 06 de Novembro de 2013.

GRANDE, Robson. E., 2006. **Sistema de integração de técnicas de proteção de privacidade que permitem personalização.** Disponível em: <http://www2.dc.ufscar.br/~zorzo/pagina_mestrado_robson/dissertacao_robson.pdf>. Acesso em 05 de Dezembro de 2013.

GREENWALD, G.; MACASKILL, E. Jornal The Guardian, 2013**. NSA Prism program taps in to user data of Apple, Google and others**. Disponível em: <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em 05 de Dezembro de 2013.

H HUBMANN, **Das Persönlichkeitsrecht** (Cologne/Graz: Böhlau Verlag, 1967, 2nd ed), 268-332.

Hall, Edward T, **The Hidden Dimension** (1966). Anchor Books.

HOUAISS, Antônio. (Ed.). **Dicionário Houaiss da língua portuguesa.** Rio de Janeiro: Objetiva 2001.

INFORMATION SHIELD, **Privacy Laws.** Disponível em <http://www.informationshield.com/intprivacylaws.html>. Acesso em 25 de Janeiro de 2014.

ISHITANI, Lucila. **Uma Arquitetura para Controle de Privacidade na *Web*, 2003.** Disponível em: <http://www.dcc.ufmg.br/pos/cursos/defesas/129D.PDF>. Acesso em 12 de Novembro de 2013.

KUROSE, J. F. **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. 5. ed. São Paulo, Addison Wesley, 2010.

LOBATO, Luana. **Avaliação dos Mecanismos de Privacidade e Personalização na *Web*, 2007**. Disponível em: <http://www.bdtd.ufscar.br/htdocs/tedeSimplificado/tde_arquivos/3/TDE-2009-09-21T133846Z-2450/Publico/2161.pdf>. Acesso em 07 de Novembro de 2013.

MACASKILL, Ewen; DAVIES, Nick; HOPKINS, Nick; BORGER, Julian; BALL, James. Jornal The Guardian, 2013. **GCHQ Intercepted Foreign Politicians' Communications at G20 Summits.** Disponível em: <http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits>. Acesso em 05 de Dezembro de 2013.

MATOS, Tiago Farina, 2005. **Comércio de Dados Pessoais, Privacidade e Internet.** Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=4146>. Acesso em 17 de Março de 2014.

OEA, **Convenção Europeia de Direitos Humanos**, **1950**. Disponível em: <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=536&IID=4>. Acesso em 26 de Fevereiro de 2014.

ONU. **Declaração Universal dos Direitos Humanos, 1948**. Disponível em: <http://unicrio.org.br/img/DeclU_D_HumanosVersoInternet.pdf>. Acesso em 06 de Novembro de 2013.

PISAREWICZ, Piotr. **Privacidade na Rede Aberta, 2003.** Disponível em: <http://cic.unb.br/docentes/pedro/trabs/PrivacidadePiotr.pdf>. Acesso em 09 de Novembro de 2013.

SILVA, A. N. C.; MARGARIDA, A. F.; OLIVEIRA, I. S.; SILVA, S. A. L., 2012. **A Regulamentação da Internet no Brasil Ante os Direitos de Privacidade do Usuário Comum.** Disponível em: <http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/view/3029/2987>. Acesso em 05 de Dezembro de 2013.

TOMIZAWA, Guilherme, 2011. **O Direito à Privacidade e a Intromissão Estatal Através dos Sistemas de Inteligência e Ferramentas de Espionagem Dentro da Internet.** Disponível em: <http://www.anima-opet.com.br/pdf/anima5-Professores/GUILHERME-TOMIZAWA-ANIMA5.pdf>. Acesso em 21 de Novembro de 2013.

WARREN AND BRANDEIS, **The Right to Privacy, 1890.** Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em 26 de Fevereiro de 2014.

WIKIPEDIA, **Personal space.** Disponível em: <https://en.wikipedia.org/wiki/Personal_space>. Acesso em 26 de Fevereiro de 2014.