"O DIREITO À PRIVACIDADE E A INTROMISSÃO ESTATAL ATRAVÉS DOS SISTEMAS DE INTELIGÊNCIA E FERRAMENTAS DE ESPIONAGEM DENTRO DA INTERNET" [1]

"THE RIGHT TO PRIVACY AND THE STATE THROUGH THE MEDDLING SYSTEMS INTELLIGENCE AND ESPIONAGE INSTRUMENTS IN THE INTERNET"

Resumo

O presente ensaio tem o intuito de apontar à sociedade e à academia jurídica dos diversos tipos de sistemas de inteligência e ferramentas de controle que o Estado Nacional ou Transnacional com respaldo de agências governamentais possuem para vigiar e monitorar os internautas dentro da Rede das redes, ferindo direitos fundamentais, tais como a privacidade do usuário da internet. Elenca diversos potências mundiais que se valem dessas ferramentas de espionagem, tais como os EUA e a Inglaterra, através de pactos internacionais e algumas experiências incipientes no Brasil. Comenta brevemente da colisão de princípios fundamentais entre a segurança e a privacidade dos internautas.

Palavras-chave: poder público, privacidade, sistemas de inteligência e ferramentas de espionagem.

Abstract

This essay aims to point out to society and the legal academy of different types of intelligence systems and control instruments that the state-backed National or Transnational government agencies have to oversee and monitor the Internet within the network of networks, wounding fundamental rights such as privacy of Internet users. It lists various world powers who use these instruments of espionage such as the U.S. and Britain, through international covenants and some embryo experiences in Brazil. Briefly comments the collision of fundamental principles of security and privacy of Internet users.

Key-words*:* government, privacy, intelligence systems and instruments of espionage.

Introdução

Consagrado pelo notório e visionário Panóptico de Bentham[2], até hoje em dia, existe no globo terrestre, um infindável número de pessoas e organizações públicas com interesse em informações pessoais dos usuários dentro da internet. Nessa Sociedade da Informação, todo conhecimento tem valor inestimável. Sendo assim, o Poder Público em nome do Estado, com respaldo na disfarçada *idéia de proteção à coletividade* e em nome da *segurança nacional*, criaram motivos considerados por todos "politicamente corretos"

[1] GUILHERME TOMIZAWA é advogado, mestre em direito público pela UGF – RJ, professor de direito eletrônico da OPET-PR. É membro e vice-presidente do IBDE (Instituto Brasileiro de Direito Eletrônico).

[2] Em "*Vigiar e Punir* – história da violência nas prisões" de Michel Foucault, Editora Vozes, 19ª. Edição, Petrópolis, 1999. p.165-187

para violar a privacidade e a intimidade dos usuários dentro da rede das redes. O Professor Alberto Nogueira em seu livro *Jurisdição de Liberdades Públicas* identifica a questão da *segurança* como o seguinte: "Nela estão envolvidos diversos atores: bandidos, vítimas e os "garantidos", que são todas as pessoas. Os sistema é do tipo "vasos comunicantes" e, nessa visão, cada um espera ter direito ao tratamento justo"[3].

Seguindo essa linha de raciocínio, as empresas privadas também no afã de obterem dados e informações pessoais com o nítido e escancarado fim de engordarem o seu faturamento anual, se sucedem através de suas agressivas e apelativas políticas de marketing e publicidade, com o auxílio de *spams, cookies,* e outras "pragas digitais", muito bem *nominadas pelo* Prof. Walter Aranha Capanema[4]. Devemos nos atentar para essa novel modalidade de invasão invisível e quase imperceptível aos desavisados internautas que trafegam diariamente na internet (v.g.: cadastros comerciais e de atualização em *web-pages*, declarações de imposto de renda, contas bancárias, *chats*, grupos de news, etc.) deixando seus rastros e dados sensíveis[5] e pegadas ao insaciável olhar do nosso maior "*Big Brother*"[6].

Tudo isso nos leva a crer que não estamos sós, quando acessamos a internet, pois basta alguns "cliques" do mouse para se verificar que somos vigiados quase todo o tempo em que começamos nossa jornada diária. Ao entrar no elevador e sair de sua garagem, existem câmeras no seu condomínio, a fim de nos dar proteção. Ao adentrarmos nos carros podemos ser vítimas de máquinas fotográficas e câmeras que com intuito de penalizar o infrator do trânsito devassando a nossa intimidade com o mesmo fundamento da ordem e da paz social. Ao caminharmos nas ruas e outras vias ou locais públicos[7], somos controlados por câmeras de vídeo-vigilância a fim de controlar o número de assaltos e furtos em uma determinada rua. Logo após entramos numa loja ou em qualquer estabelecimento comercial e nos valemos do cartão de crédito para efetuar um pagamento

---

[3] NOGUEIRA, Alberto. *Jurisdição das Liberdades Públicas*. Editora RENOVAR, Rio de Janeiro, 2003.

[4] Para quem ter uma leitura mais profunda sobre essa pragas digitais *in* CAPANEMA, Walter Aranha. *O Spam e as pragas digitais – uma visão jurídico tecnológica* . Editora LTR. 1ª. edição, Rio de Janeiro, 2010.

[5] Os Governos coletam uma variedade de dados pessoais. Alguns dados com registros fiscais e médicos, por exemplo, são extremamente sensíveis, tendo sido reconhecidos há muito tempo como fonte de preocupação na preservação da privacidade dos cidadãos. Outras espécies de informação são inofensivas, desde que coletadas de forma razoável, apesar de também poderem ser consideradas invasivas quando compiladas e cruzadas de forma a criar perfis mais abrangentes dos indivíduos *in* CALSON, Steven C.; MILLER, Ernest D. *Public Data and Personal Privacy. Santa Clara Computer& Hight International Law Jornal.* Santa Clara: HeinOnline, 2000, vol. 16, p.83-109 (Tradução do Autor).

[6] "Big Brother" – romance de George Orwell nominada "1984" onde se comenta sobre o grande irmão que vigia seus concidadãos retratando o cotidiano numa sociedade totalitária.

[7] Disponível no site http://maps.google.com/help/maps/streetview/index.html - Acesso em 14 mar. 2011.

qualquer e somos novamente vítimas da invasão do poder público sem podermos ao menos nos defender desse mal maior como bem mencionou o Prof. Dr. Gustavo E. L. Garibaldi, em sua última obra recém-publicada que dizia:

> Em la lista de inconvenientes, se suman:
>
> a) Afetación de la intimidad que abarca el derecho a la soledad y reposo, procurados em lugares públicos.
> b) Afetación de la libertad de expresión y asociación.
> c) Limitaciones a la libertad de desplazamiento.
> d) Afectación de la confianza y sinceridad social[8]

Essa ciberespionagem legitimada sempre formou parte da história da humanidade, em várias administrações em todo globo terrestre. Antigamente, os Estados realizavam atos de vigilância sobre determinados grupos ou indivíduos, atualmente, com apoio nas tecnologias emergentes, dentre elas, o avanço inexorável da internet, governos de muitos países seguem realizando atos de vigilância. Essa espionagem atinge milhões de pessoas, e não só à nível de internet, basta acessar o site do *google maps*[9], *google earth*[10], para vislumbrarmos que não estamos sozinhos em nenhum lugar do mundo. Fala-se então de uma vigilância digital global ou mundial.

Depois dos atentados terroristas de 11 de setembro de 2001, a maioria dos governos de todo o mundo dera início, e alguns casos continuidade, a uma vigilância global sem precedentes utilizando, para tanto, a estrutura física da Internet[11] e em alguns casos edições de leis mesmo que muitas vezes violadoras de nossas garantias fundamentais[12]. O que ocorre é que há muito tempo atrás, alguns governos já estão realizando atos de espionagem em grande escala na internet. Alguns deles se desenvolveram dentro da própria Rede, outros, no entanto, não foram criados com esse fim. Certamente devem existir outros países que desenvolveram sistemas e programas de vigilância em escala mundial, porém costumeiramente negam a sua existência a fim de não ferir diretos constitucionais de seus cidadãos. Contemporaneamente os países que possuem sistemas de vigilâncias eletrônicas admitem (e quando admitem) o funcionamento com base no combate a proliferação do terrorismo e outras condutas ilícitas que se espalham com o uso dessa nova ferramenta de

---

[8] GARIBALDI, Gustavo E. L. *Las Modernas tecnologias de control y de investigación del delito*. Editorial Ad-hoc. 1ª. Edição. Buenos Aires, 2010, p.337.

[9] Disponível no site http://maps.google.com.br/ - Acesso em 14 mar. 2011.

[10] Disponível no site http://earth.google.com/intl/pt/ - Acesso em 14 mar. 2011.

[11] PEREIRA, Marcelo Cardoso. *Direito à Intimidade na Internet***.** Curitiba: Juruá Editora, 2004. p. 166.

[12] Disponível no site http://www.cioinsig ht.com/c/ a/Latest- News/Agents- Can-Seize- Laptops/ - Acesso em 17 out. 2008.

tecnologia que é a rede mundial de computadores. Esses mesmos governos se respaldam na justificativa de garantir a ordem e a segurança pública da sociedade, seja ela virtual ou não. Por mais justificável que seja tal argumento, tais sistemas de vigilância eletrônica violam a privacidade e a intimidade dos internautas dentro da Rede ou fora dela.

A seguir, analisaremos alguns sistemas de inteligência e programas informáticos mais conhecidos *mundialmente* (aqui especificamente os EUA, Inglaterra, Nova Zelândia, Austrália e Canadá), a fim de mostrar que filmes de ficção tais como "Teoria da Conspiração", "Inimigo do Estado" "1984" e "V de Vingança", não são mais obras de mera ficção como se profetizava algumas décadas atrás.

Sistema Echelon

Echelon é o nome de um sistema de interceptação de comunicações em escala mundial, com o objetivo de espiar as comunicações telefônicas e vigiar e interceptar mensagens cifradas de países, tais como Líbia ou Irã. Segundo o prof. Túlio Lima Vianna, o maior sistema de monitoração de comunicações já concebido até hoje por 5 países como veremos logo a frente.[13]

Originariamente o projeto da rede *Echelon* iniciou-se no ano de 1971. Tal projeto, firmado no ano de 1947, com a cooperação de cinco países (EUA, Inglaterra, Canadá, Austrália e Nova Zelândia) denominou-se UKUSA (*United Kingdom – United States of America*) com o objetivo de realizar interceptação massiva de comunicações em todo o globo terrestre. Tal acordo, permaneceu incógnito até o ano de 1999, sendo administrada pelos seus principais criadores, os EUA – com a NSA (*National Security Agency*) e a Inglaterra no GCHQ (*Governament Communications Headquarters*). Até pouco tempo atrás, os cinco países acordantes negavam a existência da rede espiã *Echelon*. Todavia, com o advento do atentado às duas "Torres Gêmeas" (11/09/2001), fez com que o governo norte-americano confessasse sobre sua existência. O próprio Presidente Bush não só afirmou a sua existência, como também ressaltou que tal rede de satélites seria a principal arma tecnológica para a luta contra o terrorismo internacional.

Coincidentemente verificamos que a rede das redes nasceu em meados dos anos 70, no mesmo período em que foi desenvolvido o sistema *Echelon.* Com isso o sistema supracitado, passou a se utilizar da infra-estrutura e a tecnologia da Rede para atingir o seu objetivo final, qual seja, interceptar informações, dados e comunicações a nível mundial.

[13] VIANNA, Túlio Lima. *Transparência Pública, Opacidade Privada* – O Direito como instrumento de limitação do poder na sociedade de controle, Editora Revan, Rio de Janeiro, 2007.p. 69-70

Acredita-se que o sistema *Echelon* seja formado por uma rede de 120 satélites, 11 estações terrestres de satélites e uma quantia incalculável de recursos financeiros a fim de manter tal avançadíssima tecnologia em funcionamento. Com esse considerável orçamento, o *Echelon* é capaz de interceptar diversos[14] tipos de transmissões realizadas momentaneamente em qualquer lugar do planeta, tais como ligações telefônicas, celulares, e-mails, fax, telex, transferências de arquivos, etc. Segundo estimativas, a *Echelon* consegue interceptar 90% de todas as comunicações em Rede. Tal sistema consegue interpretar mensagens interceptadas em escala mundial, com poderosos dicionários, que através de busca de palavras rastreiam as de cunho mais dúbios e perigosos, tais como: "atentado", "presidente", "Casa Branca", "EUA", sendo ela registrada e remetida às bases de dados da NSA[15] e do GCHQ[16].

Resumidamente, a interceptação de comunicações do sistema *Echelon* funciona dessa maneira bastante eficaz por sinal, cabendo a academia e os operadores do direito questionarem a sua legalidade no que diz respeito à privacidade dos usuários em rede, já que se trata de um sistema de espionagem em proporções estratosféricas.

Sistema Enfopol

A Europa também sua parcela de contribuição, em se tratando de um sistema eficaz de espionagem global. Trata-se do Enfopol, que é o nome utilizado para denominar o conjunto de documentos oficiais do Grupo de Trabalho sobre a Cooperação Policial da União Européia[17]

---

[14] Hodiernamente o Echelon tem capacidade global de vigilância, interceptando mais de 3 (três) bilhões de comunicações diariamente *in* SCHEINER, Bruce. *Segurança.com*: segredos e mentiras sobre a proteção na vida digital. Tradução de Daniel Vieira. Rio de Janeiro: Campus, 2001. p. 47.

[15] A Agência de Segurança Nacional (em inglês: *National Security Agency* - NSA) é a agência de segurança dos Estados Unidos, criada em 4 de novembro de 1952 e responsável pela SIGINT, isto é, inteligência obtida a partir de sinais, incluindo interceptação e criptoanálise. Também é o principal órgão estadunidense dedicado a proteger informações sujeitas a SIGINT, sendo dessa forma o maior núcleo de conhecimento em criptologia mundial, apesar de raramente divulgar alguma informação sobre as suas pesquisas. Disponível em http://pt.wikipedia.org/wiki/NSA. > Acesso em 17 mar 2011.

[16] O Government Communications Headquarters (GCHQ) é um serviço de inteligência britânico encarregado da segurança e da espionagem e contraespionagem nas comunicações, atividades tecnicamente conhecidas como SIGINT (Inteligência de sinais) O órgão também é responsável pela garantia de informação ao Governo Britânico e as Forças Armadas daquele país. Está sediado em Cheltenham. Disponível em http://pt.wikipedia.org/wiki/GCHQ. > Acesso em 17 mar 2011.

[17] Op. Cit.

Enfopol é definido na prática como *Enforcement Police*, se apresentando como um plano que pretende levar à cabo uma escuta massiva das ligações telefônicas, comunicações na internet, fax, etc. Tal projeto se desenvolveu no âmbito da *Europol* e foi colocado em prática em 1995 em Bruxelas. De início a intenção desse plano era adequar os sistemas a permitir a interceptação pela polícia das comunicações de seus clientes. No ano de 1998, uma resolução obrigou os Provedores de Serviços (ISPs) e GMS (*Groupe Special Moviles*) a facilitarem a interceptação das comunicações de seus clientes, caso a polícia o necessitasse. Este documento é conhecido como *Enfopol* 98. [18]

Em 1999 foi publicado um documento dentro da Comunidade Européia, intitulado Enfopol 19, aplicável a internet, às comunicações por satélite e às novas ferramentas tecnológicas da comunicação. A *Enfopol* é também entendida como um conjunto de interceptação mundial de comunicações estabelecidos entre os EUA e a Europa, mantidos pela União Européia e pelo FBI (*Federal Bureau Investigation*). Deste modo, nos mesmos moldes do *Echolon* o sistema *Enfopol* foi desenvolvido a fim de se vigiar a nível global as mais diversas comunicações, dentre elas a internet. Outro motivo que justificaria sua existência seria o fato de monitorar e evitar atividades ilícitas de máfias e de outras organizações criminosas, dentre elas, o movimento terrorista que se propagou de maneira incomensurável com o advento da Rede das Redes.

Da mesma forma, tal sistema de vigília e interceptação se respalda numa segurança pública legitimada, a privacidade de usuários se viu novamente a mercê de um outro possível meio de invasão da intimidade dos mesmos, haja vista que os provedores de serviço facilitarão o acesso por parte destas autoridades públicas, às comunicações a seus clientes, 24 horas por dia e em tempo real[19]. Neste andar, prevê-se que os Provedores de Acesso serão obrigados a armazenar grande parte dos dados de conexão de seus clientes[20]. Em meados de 2002, as metas da *Enfopol* ganharam mais um reforço, com a aprovação da do Parlamento e do Conselho Europeus, sobre a Diretiva 2002/58/CE, conhecida como a diretiva da privacidade e das comunicações eletrônicas, autorizando os ISPs a reterem os dados de conexão e de tráfego de seus clientes e usuários.

---

[18] Op. Cit.

[19] DAVIES, Simon. *La Privacidad en la encrucijada.* (trad.) José Alfonso Acino, Novática, n. 145, may./jun./2000. p.36.

[20] Basta verificar o substitutivo do projeto de Lei do Senador Eduardo Azeredo para vislumbrar em seu art. 22, e incisos seguintes, o poder dos provedores que possibilitará o armazenamento (por 3 anos) e controle de dados dos usuários da Internet (indiscriminadamente), como verdadeiros delatores violando nitidamente a privacidade dos, caso a lei seja aprovada pela Câmara e sancionada pelo executivo.

Em síntese, a *Enfopol* nada mais é do que outra justificativa de se desenvolver um outro projeto de sistema de vigilância de informações e dados privados, violando e pondo em cheque a intimidade de usuários dentro da Internet.

Sistema Carnívoro (Carnivore)

O Carnívoro (*Carnivore*) traduzido ao pé da letra como um sistema informático, seria outra ferramenta de vigilância eletrônica a nível global, desenvolvida pelo FBI. É conhecido como DCS1000 (*Digital Collection System*). A diferença quase que gritante entre o *Echolon*, o *Enfopol* e o *Carnivore* é que esse último foi criado especialmente para a Rede, limitando-se a interceptar e interpretar comunicações realizadas por meio da estrutura física da internet.

Em suma, pode se definir o *Carnivore* como um sistema híbrido (de *hardware* e *software*) desenvolvido pelo FBI, que se instala nos ISPs [21]com o propósito de interceptar em *real-time*, o conteúdo das comunicações individuais dentro da *Internet.*

A justificativa do Governo Americano para a sua criação também foi a mesma dos outros dois sistemas retro comentados, ou seja, o combate a atividades ilícitas e criminosas, tais como o terrorismo, a espionagem, a pedofilia, etc., a fim de ameaçar a segurança do Estado e do povo americano. Um ponto importante de ressaltar é que o Carnívoro é capaz de rastrear e interpretar somente o conteúdo de mensagens que circulam dentro da Rede, excluindo desse universo a maioria das comunicações de usuários da net.

Mas como se define esse sistema híbrido? A parte *hardware* é um computador localizado dentro de uma caixa, que está conectado aos computadores de um certo Provedor de Serviço (ISP). Já o *software* encarrega-se de capturar toda a comunicação que circula pelos computadores dos ISPs. Logo após esse rastreamento, esses dados são enviados a uma base de dados que irá processar as informações selecionadas.

Tal sistema funciona através de palavras-chaves previamente escolhidas, tais como “bomba”, ”atentado”, “presidente” etc., tal mensagem será objeto de interceptação, etiquetada e enviadas às bases de dados desse programa, a fim de passar por uma análise mais criteriosa, realizada por especialistas do FBI[22].

---

[21] O fornecedor de acesso à Internet (em inglês *Internet Service Provider*, ISP ou ISPs - plural) oferece principalmente serviço de acesso à Internet, agregando a ele outros serviços relacionados, tais como *"e-mail"*, *"hospedagem de sites"* ou blogs, entre outros. Disponível no site: http://pt.wikipedia.org/wiki/ISPs - Acesso em 21 mar. 2011.

[22] Federal Bureau Investigation.

A princípio, se achava que o programa Carnívoro somente interceptasse mensagens de correio eletrônico, entretanto, crê-se que o sistema é capaz de rastrear e interpretar mensagens de lista de correio, grupo de *NEWS*, chats, mensagens *on-line*, etc.

Em linhas gerais, esse é o tão polêmico e legalizado programa Carnívoro, tratando-se aqui de uma extraordinária ferramenta de interceptação e interpretação de comunicações que fluem através dos Provedores de Serviço. Sendo assim, a pergunta ainda persiste, até que ponto o sistema Carnívoro ultrapasse o limite legal e invade a esfera de privacidade dos internautas?

Lanterna Mágica (*Magic Lantern*)

Além do sistema informático *Carnivore*, o FBI desenvolveu outro sistema de vigilância eletrônica na internet chamado Lanterna Mágica. Tal sistema seria um pequeno programa informático espião, pertencente à categoria dos cavalos-de-tróia (*trojans*), com o nítido intuito de espionagem.

Foi visto no tópico anterior, que o Carnívoro necessita de presença física para a instalação junto aos computadores de Provedores de Serviço. No entanto, com a utilização do desse *trojan* – Lanterna Mágica, seria possível instalar um pequeno programa espião no computador de um determinado suspeito, não necessitando, ter um acesso físico à sua máquina[23]. O *trojan* pode ser introduzido via Internet no computador de usuário suspeito, disfarçadamente com aparência de um programa ou arquivo eletrônico inofensivo. Dessa forma, qualquer atividade considerada corriqueira e usual, como baixar programas (*shareware* ou *freeware*) "baixar" músicas, ler *e-mails* ou comunicar-se por *chats* pode ser uma forma de introdução de um cavalo-de-tróia em um determinado computador.

Após a introdução do cavalo-de-tróia no computador do suspeito (aqui o suspeito em tese pode ler-se também como vítima), o FBI possui um amplo rol de possibilidades de seguir seus rastros. E ainda, poderá ler e-mails, senhas, contra-senhas, ler arquivos de seu disco rígido etc.

A aplicação desse *trojan* provocou uma certa antipatia e desconfiança pelos usuários da Internet, no que tange aos fabricantes de software antivírus. Não bastaria somente a instalação do Lanterna Mágica nas máquinas do suspeito, mas deveria essencialmente existir respaldo das empresas que atuam com programa antivírus no

[23] Op. cit.

mercado informático, para que permitissem que o *troyano* Lanterna Mágica não fosse perceptível pelos seus respectivos filtros.

Ademais, o próprio FBI reconheceu a existência desse programa espião, alegando se tratar de um mero projeto, destarte, a pergunta ainda permanece, levando em consideração o Estado norte-americano, existe a invasão de privacidade pelas autoridades governamentais?

Digital Storm (Tormenta Digital)

Além destes citados sistemas invasivos, temos conhecimento de outro sistema de interceptação de comunicações, nominado de *Digital Storm* (Tormenta Digital). Tal sistema tem novamente a participação do FBI. Manuel Castells, especialista na área, afirma que tal programa seria: "(...) uma nueva versión de la grabación de conversaciones telefônicas, combinada com programas informatizados para buscar palabras claves em los mensajes"[24]. Seguindo essa linha, o mecanismo e funcionamento do *software* Tormenta Digital seria idêntico ao do *Echelon* e do Carnívoro, ou seja, interceptação com palavras-chave, destinada especificamente para comunicações telefônicas, e também para a internet.

Quando o projeto *Digital Storm* for aplicado na prática, será eficazmente outra potente ferramenta de vigilância eletrônica, no auxílio de outras já existentes, tais como *Echelon*, Carnívoro, Lanterna Mágica, Matrix, TIASystems, ou outro sistema desconhecido pelo meio público. As existências de todos esses sistemas de inteligência e vigilância demonstram o poder que o Estado tem para atentar contra a privacidade de seus cidadãos.

A Intromissão estatal através de ferramentas e sistemas de inteligência no Brasil

Como é notoriamente sabido a Internet é uma fonte incalculável e ilimitada de informação. No Brasil não seria diferente, dentro da Rede das Redes, pode-se obter informações e dados de qualquer alçada. Entre essas informações, se destacam as informações de indivíduos, aqui no caso de internautas. Também é de conhecimento geral que o Estado é o maior detentor de informações, de caráter pessoal ou não, de seus administrados e que Poder Público possui muitas formas de realizar uma vigilância eletrônica mundial. Somente a título de exemplo aqui no Brasil, podemos citar a Receita Federal que detém informações detalhadas sobre a declaração anual de imposto de renda de

[24] CASTELLS, Manuel. *La Galáxia Internet*. 1 ed. Barcelona: Arete, 2001. p. 201

pessoas físicas ou jurídicas, ainda mais com o reforço extra de um dos maiores computadores do mundo, apelidado de "Hal", através do sistema Harpia[25] desenvolvido pela Receita Federal Brasileira, com a criação e justificativa de analisar o risco aduaneiro, mas que na verdade será um supercomputador que monitorará as contas bancárias, bens móveis e imóveis, etc. de brasileiros através de cruzamento de dados de CPF, CNPJ´s. Em via inversa, sabemos que os cidadãos não podem se abster de passar informações ao Poder Público, quando forem instados para tanto, mas logicamente quando justificáveis seus fins, ainda mais se tratando de informações sigilosas[26] ou via autorização judicial. Nesta esteira de pensamento avocamos os ensinamentos da Dra. Tatiana Malta Vieira que afirmou em sua obra no referido tema:

> Em regra, os cidadãos não podem negar informações ao Estado, quando essas mesmas são solicitadas para fins de recolhimento de tributos, identificação civil, vacinação, exercício de direitos eleitorais e outras atividades relacionadas ao poder de fiscalização. Uma vez coletadas, essas informações são armazenadas em bancos de dados públicos, podendo ser utilizadas para as mais diversas finalidades. O problema reside na utilização dessas informações para finalidades diversas daquelas para as quais foram coletadas sem que tenha havido autorização prévia de seus titulares [27].

Ou ainda a exemplo do Detran que possui informações de veículos de pessoas físicas ou jurídicas, ou o TRE (Tribunal Regional Eleitoral) com os dados atualizados de seus eleitores, bem como a Polícia Federal e os Institutos de Identificação contendo dados personalíssimos de indivíduos, Instituições Financeiras e Bancárias, e assim por diante...

Busco auxílio nas sábias palavras do Prof. Celso Bastos para elucidar melhor esse ponto nevrálgico:

> não é possível atender-se tal proteção (intimidade) com a simultânea vigilância exercida sobre a conta bancária ou as despesas efetuadas com cartões de crédito pelo cidadão pois "a doação feita a um partido político ou a uma seita religiosa (...) poderia ser identificada pelos órgãos fazendários que estariam desvendando uma vontade secreta do benemérito", e continua sua exposição dizendo "do atraso de pagamento da fatura de um cartão de crédito, ou de uma duplicata por dificuldades financeiras, ou da existência de saldo bancários desfavorável poderia ter ciência a União se houvesse a quebra do sigilo bancário e creditício, implicando, senão a comunicação a outros órgãos ou a adoção de medidas, ao menos o conhecimento de fatos relevantes e embaraçosos relativos à intimidade".[28]

Partindo dessa premissa, podemos afirmar que a informação pessoal angariada pelos diversos órgãos (diretamente e indiretamente) governamentais pode não estar

---

[25] Disponível em: http://www.harpiaonline.com.br/harpia/ - Acesso em 14 mar 2011.

[26] Com fulcro no artigo 4º, inciso XIII, e art. 37 inciso I do Decreto nº 4553/2002.

[27] VIEIRA, Tatiana Malta. *O Direito à Privacidade na Sociedade de Informação*. Efetividade desse direito fundamental diante dos avanços da informação. Porto Alegre: Sergio Antonio Fabris Ed., 2007, p. 237.

[28] BASTOS, Celso. *Estudos e pareceres de direito público*. São Paulo: Revista dos Tribunais, 1993. p. 63.

suficientemente protegida, transformando o Estado em um potencial ofensor ao direito à privacidade dos cidadãos. Somente para argumentar, e se essas mesmas informações, em tese, fossem vendidas e repassadas à empresas e pessoas físicas que exerçam atividade comercial dentro da Internet? Mais a frente, Tatiana Malta Vieira afirma:

> Assim não se aplica em relação aos órgãos públicos o direito de o titular vedar a utilização de seus dados para fins diversos daqueles para os quais foram fornecidos, ao contrário do que ocorre em relação a entidades privadas. Entretanto, essa maior liberalidade conferida ao Estado em razão o seu poder de fiscalização e controle, deve ser cotejada com a obrigação de conferir-se segurança a esses dados em todas as fases de seu tratamento, a fim de se garantir integridade, autenticidade e sigilo – os principais pilares da área denominada segurança da informação. Assim, recomenda-se a edição de ato normativo regulamentado a atividade de coleta e compartilhamento de informações pessoais entre os diferentes entes públicos, para coibir os abusos e a excessiva intromissão estatal na intimidade dos cidadãos.[29]

Essa é a maior preocupação entre os especialistas e estudiosos do direito, questões dessa ordem, envolvendo dois protagonistas, quais sejam, a influência dissimulada do Estado e a privacidade dos cidadãos, seja fora ou dentro da Internet. O Estado, que têm a incumbência de proteger os dados e informações de seus cidadãos, acaba sendo o maior ofensor a essa garantia constitucional que é violada constantemente a olho nu, e por que não dizer a olhos "digitais".

Em suma, devemos nos ater que às vezes, a violação da privacidade dos cidadãos vem justamente de quem deveria, por dever institucional, numa dimensão negativa do direito fundamental (direito de abstenção), protegê-los. Ainda que seja muito difícil imaginar a Internet ser tecnicamente controlável, ressalta-se a importância de se evitar a proliferação de dispositivos informáticos de controle na Rede em detrimento da privacidade de seus respectivos usuários. Mas o que fazer quando dois direitos da mesma categoria e de mesmo valor hierárquico colidem entre si? A ponderação ao caso concreto é muito bem trabalhada no ensaio jurídico da Profa. Teresa Negreiros, quando se trata da dicotomia Público-Privado frente ao problema da Colisão de Princípios[30].

O jusfilósofo Ronald Dworkin ressalta:

> Principles have a dimension that rules do not – the dimension of weight or importance. When principles intersect (…), one who must resolve the conflict has no take into account the relative weight of each. This cannot be, of course, an exact measurement, and the judgment that a particular principle or policy is more important than another will often be a controversial one. Nevertheless, it is an integral part of the concept of a principle that it has this dimension, that it makes sense to ask how important or how weighty it is[31].

---

[29] Op.cit. p.239

[30] Nos temas da Renovar *in* "*Teoria dos Direitos Fundamentais*" organizada pelo prof. Ricardo Lobo Torres, da Editora Renovar, 2ª. Edição – revista e atualizada, Rio de Janeiro, 2004, p. 343-381.

[31] DWORKIN, Ronald M. *The Model of Rules*. In: Law, Reason and Justice, Essays in Legal Philosophy. New York: New York University Press, 1969, p. 18-19.

Aqui no caso, é de uma clareza solar o conflito de princípios constitucionais que existem entre a segurança e a privacidade. Tal tema e possíveis soluções jurídicas já foram pontualmente discutidas em trabalho anterior, mais especificamente no capítulo da Colisão de Direitos Fundamentais[32].

Considerações Finais

Após essa breve análise de alguns meios de espionagem e vigilância global e local verificamos que não estamos sós e não possuímos formas ou meios técnicos de saber se estamos sendo ininterruptamente controlados e vigiados.

Avocamos, as célebres palavras de Garibaldi:

> En la balanza, se debe considerar que la soledad, intimidad, anonimato y reposo em lugares públicos, son derechos procurados particularemente por quienes carecen de sítios privados adecuados o suficientemente confortables, que así son suplidos en alguna medida. De modo que la protección de esos valores individuales em sítios públicos tiende a equilibrar y compensar desigualdades sociales[33].

Vimos no Brasil, como transnacionalmente que existem aparatos ou parafernálias eletrônicas demasiadamente modernas o suficiente para desnudar a nossa vida privada e intimidade (conforme o que reza o artigo 5º, incisos X e XII, ambos da Constituição Federal de 1988). A cada dia que passa, perdemos mais a nossa privacidade, é um dos direitos mais devassados e achincalhados no nosso país, segundo comentários do Prof. Ives Gandra Martins[34]. Logicamente que coadunamos com a linha de pensamento dos juristas[35] que já trabalharam exaustivamente quando se tratar de colisão de princípios ou garantias fundamentais. Os princípios da proporcionalidade e da razoabilidade[36] devem ser usados com moderação para essa nova modalidade de "espionagem" estatal por meio de recursos tecnológicos.

---

[32] TOMIZAWA, Guilherme. *A Invasão de Privacidade Através da Internet*. JM Livraria Jurídica, Curitiba, 2008. p. 78-82.

[33] Op. cit.

[34] Disponível em http://www.ambito-juridico.com.br/site/index.php?n_link=visualiza_noticia&id_caderno=20&id_noticia=2609. Acesso em 17 mar. 2011.

[35] Nessa linha de raciocínio e pensamento Robert Alexy, Ronald Dworkin e Chain Perelman, no tocante à colisão de princípios fundamentais.

[36] Ver a obra de Suzana de Toledo Barros que analise analiticamente o seguinte tema: "*O Princípio da Proporcionalidade e o controle de constitucionalidade das leis restritivas de direitos fundamentais*", Editora Brasília Jurídica, 3ª. Edição, 2003.

Diante de tudo que foi exposto, verifica-se que o Estado Nacional ou Transnacional representa uma séria ameaça à intimidade e vida privada dos cidadãos. O Poder Público se valendo de aparatos tecnológicos, sistemas e agências de inteligência interceptam milhões de mensagens que são diariamente transmitidas por e-mail, telefone, celular, etc. Vimos que os EUA e a Inglaterra, além de monitorarem seus concidadãos, interceptam mensagens de pessoas físicas, jurídicas, públicas ou privadas globalmente, independente de sua origem ou destino. Respaldados nessa política de espionagem eletrônica se sustentam e invocam o princípio da segurança nacional a fim de combater contra o terrorismo, o crime organizado, o tráfico de drogas, etc., todavia o que se verifica após esse estudo é o poder capitalista desmesurado das grandes potencias mundiais, v.g. do acordo internacional (UKUSA) celebrado entre aqueles países no projeto *Echelon,* que deliberadamente no afã de angariar informações privadas (transações comerciais, negociações políticas) e até sensíveis dos internautas numa tentativa de ampliar e globalizar seu alcance de privilégios e controle sobre todos os povos.

A dra. Ana Prata em sua essência traz um comentário que julgamos oportuno para o desfecho da conclusão:

> O interesse público é entendido como consistindo apenas no assegurar das melhores condições de exercício e expansão dos interesses privados. Isto é, o interesse público não é concebido enquanto portador de um conteúdo de natureza diversa e contraditória com os interesses privados; ao contrário, consiste e esgota-se no assegurar das melhores condições de exercício e realização daqueles interesses privados[37].

Bibliografia

Livros e periódicos:

BARROS, Suzana de Toledo. **O Princípio da Proporcionalidade e o controle de constitucionalidade das leis restritivas de direitos fundamentais.** Editora Brasília Jurídica, 3ª. Edição, 2003.

BASTOS, Celso. *Estudos e pareceres de direito público*. São Paulo: Revista dos Tribunais, 1993.

CALSON, Steven C.; MILLER, Ernest D. **Public Data and Personal Privacy.** *Santa Clara Computer & Hight International Law Jornal.* Santa Clara: HeinOnline, 2000, vol. 16

CASTELLS, Manuel. **La Galáxia Internet.** 1 ed. Barcelona: Arete, 2001.

CAPANEMA, Walter Aranha. **Spams e as pragas digitais** . Editora LTR, 1ª. edição, Rio de Janeiro, 2010

[37] PRATA, Ana. A Tutela Constitucional da Autonomia Privada. Coimbra: Almedina, 1982, p. 28.

DAVIES, Simon. **La Privacidad en la encrucijada. (trad.)** José Alfonso Acino, Novática, n. 145, may./jun./2000.

DWORKIN, Ronald M. **The Model of Rules. In: Law, Reason and Justice, Essays in Legal Philosophy**. New York: New York University Press, 1969

FOUCAULT, Michel. **Vigiar e Punir** – história da violência nas prisões, Editora Vozes, 19ª. Edição, Petrópolis, 1999.

GARIBALDI, Gustavo E. L. **Las Modernas tecnologias de control y de investigación del delito – Su incidência em el derecho penal y los princípios constitucionales**. Editorial Ad-hoc. 1ª. Edição. Buenos Aires, 2010, p.337.

NOGUEIRA, Alberto. **Jurisdição das Liberdades Públicas.** Editora RENOVAR, Rio de Janeiro, 2003.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade na Internet.** Curitiba: Juruá Editora, 2004.

PRATA, Ana. **A Tutela Constitucional da Autonomia Privada**. Coimbra: Almedina, 1982.

SCHEINER, Bruce. **Segurança.com**: segredos e mentiras sobre a proteção na vida digital. Tradução de Daniel Vieira. Rio de Janeiro: Campus, 2001.

TOMIZAWA, Guilherme. **A Invasão de Privacidade Através da Internet.** JM Livraria Jurídica, Curitiba, 2008.

TORRES, Ricardo Lobo (org.). **Teoria dos Direitos Fundamentais.** Editora Renovar, 2ª. edição – Revista e Atualizada, Rio de Janeiro, 2004.

VIANNA, Túlio Lima. **Transparência Pública, Opacidade Privada** – O Direito como instrumento de limitação do poder na sociedade de controle, Editora Revan, Rio de Janeiro, 2007.

VIEIRA, Tatiana Malta. **O Direito à Privacidade na Sociedade de Informação**. Efetividade desse direito fundamental diante dos avanços da informação. Porto Alegre: Sergio Antonio Fabris Ed., 2007

Sites:

AMBITO JURIDICO. Disponível no site: http://www.ambito-juridico.com.br/ site/index.php?n_link=visualiza_noticia&id_caderno=20&id_noticia=2609.>Acesso em 17 mar. 2011.

BRASIL. Receita Federal do Brasil. Disponível no site: http://www.harpiaonline.com.br/harpia/ - Acesso em 14 mar 2011.

CIOINSIG. Disponível no site http://www.cioinsig ht.com/c/ a/Latest- News/Agents- Can-Seize- Laptops/ > Acesso em 17 out. 2008.

GOOGLE MAPS. Disponível no site http://maps.google.com.br/ > Acesso em 14 mar. 2011.

GOOGLE EARTH. Disponível no site http://earth.google.com/intl/pt/> Acesso em 14 mar. 2011.

GOOGLE STEET VIEW. Disponível no site http://maps.google.com/help/maps/streetview/index.html.> Acesso em 14 mar. 2011

WIKIPEDIA. Disponível no site <http://pt.wikipedia.org/wiki/GCHQ> Acesso em 17 mar 2011.

WIKIPEDIA. Disponível no site: http://pt.wikipedia.org/wiki/ISPs > Acesso em 21 mar. 2011.

WIKIPEDIA. Disponível no site http://pt.wikipedia.org/wiki/NSA.> Acesso em 17 mar 2011.