



MP investiga UOL, Yahoo e iG por causa de cookies

Os provedores Universo On Line (UOL), Yahoo do Brasil e Internet Group (Internet Grátis – iG) estão sendo investigados pelo Ministério Público do Estado de São Paulo. Três inquéritos civis foram instaurados para apurar as responsabilidades dos provedores por violação da privacidade dos usuários na Web. O MP também poderá entrar com uma Ação Civil Pública contra os provedores, se for necessário.

O pedido para a investigação foi feito pelo advogado **Amaro Moraes e Silva Neto**, devido ao uso de *cookies* pelos provedores. Os cookies são pequenos programas coletores de informações deixados pelos sites que o usuário visita, em seu computador. Segundo o advogado, as empresas “vasculham as preferências de compra do internauta e podem espalhar estas informações para outros sites de comércio eletrônico, normalmente sem o seu consentimento”.

De acordo com o pedido feito no Ministério Público, cada clique do mouse pode espalhar informações pela Web como hábitos de compra, idade dos filhos e preferências. Os dados seriam utilizados, posteriormente, por sites para conquistar o consumidor.

Veja o despacho do MP para a investigação dos sites

Protocolado nº 71.532/00

Representante: Amaro Moraes e Silva Neto

Representadas: UNIVERSO ON-LINE LIMITADA (UOL), YAHOO DO BRASIL, INTERNET LIMITADA E INTERNET GROUP DO BRASIL LIMITADA (IG)

Ementa do assinto: Violação da privacidade dos usuários na Internet, mediante o emprego de cookies, pequenos programas coletores de informações deixados pelos sites que o usuário visita, no seu computador, que são utilizados por empresas que, entre outras finalidades, sorrateiramente vasculham as preferências de compra do internauta e espalham estas informações para outros sites de comércio eletrônico, normalmente sem o seu consentimento.

1. Trata-se de representação formulada pelo advogado AMARO MORAES E SILVA NETO e apresentada à douta Procuradoria Geral de Justiça, de onde foi remetida para este Centro de Apoio Operacional das Promotorias de Justiça do Consumidor do Estado.



Referida representação descreve, em síntese, que as empresas UNIVERSO ON-LINE LIMITADA (UOL), YAHOO DO BRASIL INTERNET LIMITADA E INTERNET GROUP DO BRASIL LIMITADA (IG) estariam empregando tecnologia suscetível de violar a privacidade dos usuários da Internet, consistente nos denominados cookies, que são pequenos arquivos de textos que são gravados no computador do usuário, pelo browser, cujo objetivo é guardar alguns dados, como nomes e senhas, para que, quando o internauta volte a determinados sites, não tenha necessidade de digitar tudo novamente. A outra finalidade dos cookies é o direcionamento dos anúncios com base nos interesses e no comportamento dos usuários.

Narra, o ilustre advogado representante, que contatou, “navegando pela internet, que raro, é o site (ou seja, aquele lugar inapontável onde estão armazenadas informações – de texto, de som, de imagens e outras – disponibilizadas aos internautas) que, ao ser visitado, não tenta introduzir um “programinha” em seu computador. Esse pequeno arquivo espião é o tão falado cookie”.

Aduz ainda que:

“Via de regra, quando de uma primeira visita a um website podem ser formuladas perguntas que vão de nomes e e-mails a informes financeiros. Até esse ponto, nada de incomum e nada a reclamar. Informações podem ser pedidas. Dá-se-as ou não se as dá. Respeito esse direito de me inquirirem como aguardo que igualmente seja respeitado o meu direito de ficar calado.

“Entrementes, não são essas meras bisbilhotices que objetivamente me assustam. O que me perturba é o fato de que outras informações que não me foram solicitadas sejam sub-repticiamente obtidas através desses mecanismos sorrateiros chamados cookies, que, de tocaia, são plantados no sistema operacional do webnauta para que suas futuras navegações sejam ‘personalizadas’... Maquiavelicamente ‘personalizadas’...

Prossegue indagando: “Como os sites visitados conhecem certas preferências do cidadão/usuário cujas quais (sic) esse nunca informou?”

E responde:

“Por uma singela razão: PORQUE aquele ‘programinha’ personalizador que foi colocado no computador manda informes para o posseiro digital toda vez que o cidadão/usuário se conecta à rede. O cozinheiro desse infame biscoito passa, então, a saber quais outros sites o usuário visitou, se fez compras com cartão de crédito, se consultou médicos, que tipo de viagem pretende fazer e via... Mais grave a situação se torna quando nos defrontamos com o que os constitucionalista espanhóis chamam de dados sensíveis, ou seja, os dados pessoais referentes a ‘ideologia, religião, crenças, saúde, origem racial e vida sexual’ do cidadão/usuário. Tais dados nas mãos erradas podem causar prejuízos irreparáveis a esses.

Com essas prévias informações, os mantenedores do website introdutor do cookie poderão propiciar a suspeita visitação ‘mais personalizada’, remetendo o cibernavegante que os acessa por uma segunda vez a lugares ‘pré-selecionados’ e ‘provavelmente de seu interesse’ – só que, para tanto, foram colocados no computador do internauta os pequenos programas apropriadores de dados, sem que esse fosse consultado



quanto a essa colocação; sem que lhe fosse esclarecido a que fins estão destinadas as informações obtidas pelos cookies. Inconcebível invisibilidade...

Com esta pequena armadilha no computador do cidadão/usuário, esses posseiros virtuais-calados, arredios e dissimulados – recebem informações de seu hard disk, quando conectado à grande rede de comunicações, graças aos bits que ‘grilaram’ para colocar sua aziático.

Como o verbo descortina e a intuição induz, o que num primeiro momento parecia oportuno e comodamente conveniente é, em verdade, algo perigoso, eis que entidades e pessoas sem escrúpulos vêm nesse processo um meio para acompanhar os movimentos dos internautas através da web. E fazem isso sem seu consentimento!

Esse monitoramento intrusivo decorrente do cookie (...) é uma afronta moral, social e constitucional ao cidadão/usuário; é uma apropriação indevida e desautorizada de dados particulares, é uma intromissão intolerável no dia a dia”.

Remata afirmando que:

“uma vez colocado um cookie (ou mais ..., o que é a regra) no disco rígido do cibernauta, toda vez que houver uma conexão com a rede, serão enviadas informações coletadas do modus navegandi do internauta quando de seus passeios pela Internet para aquele que introduziu o ‘programinha’ em questão, qual seja: ou o webmaster (responsável pelo conteúdo e funcionamento das informações) do site ou um de seus subordinados”

2. Segundo a notícia jornalística publicada no jornal O Estado de S. Paulo, ed. De 4.9.2000, p. 17, juntada pelo autor da representação, as informações coletadas pelos cookies são chamadas de “seqüência de cliques” ou “rastreamento de cliques”, que também podem descrever quais páginas o usuário visitou em cada loja do vendedor. Na mesma reportagem está consignado ainda o seguinte.

“Mas eles (cookies) podem capturar números de cartões de crédito? Teoricamente sim, diz Paulo Vianna, diretor de tecnologia da Alladin. ‘Mas lembrem-se os números de cartões não são armazenados na máquina. Eles moram no servidor do site onde faz compras. O cookie apenas avisa ao servidor que aquele cliente específico chegou para comprar mais coisas’, explica Viana”.

Os anúncios têm gerado tanta desconfiança dos usuários que as novas versões dos browsers (navegadores) Internet Explorer 5.5 e Netscape 6.0 já vêm com tecnologia para um controle rígido dos cookies. Claro que já há programas específicos que fazem isso. O Idcide Privacy Companion é gratuito e pode ser pego em <http://www.idicide.com/download>. Com ele você pode ver quais sites estão lhe espionando e definir o nível de controle da privacidade. Outra opção é o Cookies Viewer, que permite ler e apagar os cookies armazenados no micro. O download está em <http://www.winmag.com/scripts/download.pl/karen/ptcookie-setup.exe>” (grifos nossos).

3. Noutra matéria jornalística, também juntada pelo autor da representação, intitulada De olho nos



cookies (criados para facilitar a navegação, estes arquivos podem estar sendo usados com espões) e assinada pelo Jornalista Eli Monteiro (Jornal do Brasil, ed. De 21.9.2000 p. 2), são tecidas interessantes considerações sobre os cookies. Merecem destaque alguns trechos:

“Mocinho ou vilão. O cookie, arquivo remetido pelo servidor de rede de Websites ao disco rígido do internauta, desperta discussões acaloradas no Brasil e no exterior sobre a privacidade na internet. Em tempos de personalização de serviços e páginas na rede, o temido arquivinho que muita gente nem conhece vem sendo acusado de espionagem. Ele estaria sendo inserido cada vez mais em HDs (discos rígidos) alheios pelo websites (provedores), para monitorar hábitos de navegação. Mas, afinal de contas, para que servem os famosos biscoitos da era digital?

Toda vez que acessa um site, o visitante recebe ‘de brinde’ este arquivinho, encaminhado automaticamente ao diretório c:\windowscookies, para quem usa o browser Internet Explore, e c:\arquivosdeprogramasnetscapeusers, para usuários do Netscape. Muitos sites não usam cookies,mas alguns mais espertinhos chegam a colocar mais de 15 biscoitos de uma só vez. (...). Depois de instalado no disco rígido, o cookies serviria teoricamente para facilitar a vida do navegante. Ele agiria como um tíquete de entrada, permitindo o acesso sem barreiras, como formulários e senhas, ao conteúdo da página. Isso teoricamente. Apesar das boas intenções, biscoitos pode servir também para facilitar a vida, mas das empresas. A intenção mais singela seria descobrir os hábitos de navegação do internauta. A mais perniciosa, porém,é conseguir dinheiro repassando a terceiros os dados obtidos.

Esse tipo de comércio já acontece na vida dos consumidores há algum tempo e usa a internet apenas como meio mais fácil e rápido. Quem nunca recebeu mala-direta sem que tivesse idéia de como as empresas tomaram conhecimento de sua existência? Simples. O cartão de crédito, a lista telefônica, os cadastros feitos em lojas, a assinatura de publicações e muitas outras fontes estão ai à disposição de quem está ávido por uma mailing list e tem dinheiro para pagar.

Para Carlos Cabral, coordenador do Programa Selo de Privacidade On-Line da Fundação Vanzolini, entidade sem fins lucrativos ligada à Universidade de São Paulo (USP), o cookie se torna preocupação a partir do momento em que é usado sem o controle e o conhecimento de usuário. ‘Ele tem uma função séria de reconhecer o visitante, mas nem sempre quem está por trás dos bancos de dados das empresas tem boas intenções’, analisa Cabral.

(...)O diretor chama a atenção para uma questão que ultrapassa a fronteira da privacidade. O cruzamento de bancos dedados seria uma praga mais perigosa ainda “Se você é usuário cadastrado de um site de bebida alcoólica’, alerta (grifos nossos)”.



Na mesma reportagem, Jason Carlett, presidente da Junkbusters Corporation, site americano que atua na defesa da privacidade on-line, “considera que os cookies só devem ser usados com autorização explícita dos usuários. ‘Eles deveriam ser administrados pelos fabricantes de browsers, mas eles também têm interesse comercial em seguir a navegação dos usuários, critica’. Assinala, ainda que “ficar esperando a boa vontade da indústria é perda de tempo”, .Para ele, **“uma lei específica para regular o uso de cookies é fundamental”**(grifos nossos).

Outro trecho da aludida reportagem que merece destaque está assim vazado: “Será que alguém, em sã consciência, abriria seus dados na internet mesmo ignorando seu destino? Por incrível que pareça, sim. Sites de prêmios, provedores de acesso gratuito e lojas de comércio eletrônico ‘oferecem’ formulários a serem preenchidos pelo internauta interessado em participar de promoções. O que estas empresas ganham em troca? Dados preciosos. Na era da tecnologia da informação, a identidade é a moeda de troca com maior valor. Preferências, horários de navegação e perfil social valem mais do que o internauta imagina e, para encher os bancos de dados, estão sendo trocados por moeda real. Especula-se que o lote com cerca de 100.000 e-mails, por exemplo, saia pela bagatela de R\$ 50.

(...) A saída que algumas empresas pontocom conseguiram para conquistar a confiança dos internautas se chama Marketing de Permissão. O nome pomposo nada mais é do que pedir a permissão do internauta para a inclusão de seu nome em mailing lists e malas-diretas. Assim, ao preencher cadastros, o usuário responde se as informações podem ser repassadas. Desta forma, a empresa dá ao internauta a chance de escolher se quer ou não ser vítima de uma enxurrada de correspondência em sua caixa postal. (...)

Mas nem todas as empresas oferecem escolha. Espalham seus pequenos espões no HD (disco rígido) e ficam à espreita.” (grifos nossos)

4. No site www.br-business.com.br/brb/cookies.htm, podem ser obtidas as seguintes informações sobre os cookies, todas relacionadas com sua utilidade (não se preocupa em mostrar os riscos que representam à privacidade e à segurança do consumidor-usuário):

Cookies podem ser definidos como pequenos textos (de geralmente 1 Kb), colocados no disco rígido do microcomputador do internauta por alguns sites que ele visitou. Contém informações que o próprio internauta ofereceu ao site, como e-mail, preferência, o que ele comprou, seu nome, endereço, data de nascimento, etc. Se ele apenas entrou no site e não digitou informação nenhuma, então o cookies não conterà informação nenhuma.

Alguns sites de comércio eletrônico colocam os cookies no hard disk (disco rígido) do usuário com o objetivo de personalizar os próximos atendimentos. Por exemplo, o usuário entrou em uma livraria virtual e comprou o livro O grande chefão, de Mario Puzzo. Pagou com cartão de crédito e forneceu seu nome e mais alguns dados para que a compra pudesse ser realizada. Em seu próximo acesso a esse site ele receberá uma mensagem em sua tela dizendo: “Bom dia Fulano de Tal, que tal conhecer O grande chefão II”. Isto significa que o atendimento foi personalizado para tal usuário. Ele foi reconhecido e um livro, que provavelmente será de seu agrado, foi-lhe oferecido. Tal exemplo mostra que, em razão do uso dos cookies o cliente pode ser atendido de acordo com o seu perfil e suas preferências, e o site terá uma maior probabilidade de vender-lhe outro livro. Esse tipo de operação envolvendo cookies e personalizando o atendimento visa a criar um vínculo com o cliente com o objetivo que este volte outras



vezes ao site.

A grande utilidade dos cookies é fornecer informação sobre o número, frequência e preferência dos usuários para que se possa ajustar a página de acordo com o gosto de cada um deles. Ainda sobre os cookies, o mencionado site revela, além de seu poder de captação de dados, outra utilidade.

“Nos sites de comércio eletrônico, os cookies também são utilizados para criar os carrinhos de compras. Digamos que o usuário esteja num site fazendo compras e de repente, por algum motivo, cai sua conexão. Acontece que eleja encheu seu carinho com um monte de coisas. Será que o site vai perder esta venda? Pois, mesmo que o cliente volte, será que ele terá paciência para comprar tudo outra vez?

Graças aos cookies está tudo bem. Se o cliente retornar ao site e quiser continuar de onde parou, os cookies ‘lembrarão’ o que tinha dentro do carrinho e o cliente não precisará começar tudo de novo”.

Esclarece que “os cookies não transmitem vírus e podem ser lidos apenas por aqueles que o colocaram no hard disk do usuário, evitando o tráfego aberto de informações pela rede”. Omite, todavia, a possibilidade de venda dos dados captados para empresas interessadas em mailing list, normalmente para fins de envio de publicidade, por e-mails ou mala-direta, aos usuários.

5. Preocupado com a segurança do usuário no mundo virtual da web, o Comitê Gestor da Internet no Brasil editou recentemente (15.10.2000) o que denominou de Cartilha de Segurança para a Internet, que, em resumo, se destina aos usuários finais com pouco ou nenhum conhecimento a respeito da utilização da Internet, com o objetivo de lhes dar uma visão geral dos conceitos mais básicos de segurança.

Referida cartilha, no subtem 4, trata da privacidade nas visitas aos sites. Esclarece que no momento em que o usuário entra em determinados sites aparecem na página dados de seu computador que às vezes até assustam. Parecem adivinhar até a cor do papel-de-parede que ele está utilizando em seu computador. Isto ocorre porque existe um bate-papo entre o seu browser e o site que está visitando.

Entre as informações que seu browser entrega de bandeja para o servidor do site visitado estão: (a) o endereço na Internet de seu computador (endereço IP); (b) nome e versão do sistema operacional; (c) nome e versão do browser; (d) última página visitada; e (e) resolução do monitor.

Com essas informações, os sites conseguem fazer as estatísticas de visitação, adequar a página do site ao browser do usuário, etc. A cartilha em tela faz o seguinte alerta ao usuário: se quer realmente esconder-se (ficar anônimo) e não passar nenhuma informação ao site visitado, deverá utilizar-se de serviços que o ajudam a preservar sua privacidade, como o Anonymizer (<http://www.anonymizer.com>).



A mesma cartilha sublinha que os cookies são utilizados pelos sites de diversas formas. Aponta algumas: (a) para guardar a identificação e senha do usuário quando ele pula de uma página para a outra (b) para manter uma “lista de compras” em sites de comércio eletrônico; (c) personalização de sites pessoais ou de notícias, quando o usuário escolhe o que quer que seja mostrado nas páginas destes sites; (d) manter alvos de marketing, como quando o internauta entre em um site de CDs e pede somente CDs de MPB.

Depois de um tempo, ele percebe que as promoções que aparecem são sempre de MPB (as que ele mais gosta), e (e) manter a lista das páginas vistas em um site, para estatística ou para retirar as páginas em cujos links o usuário não tem interesse.

Preocupa-se com os cookies ao assinalar que o problema com relação a eles é que “são utilizados por empresas que vasculham sua preferências de compras e espalham estas informações para outros sites de comércio eletrônico”. Assim, o usuário “sempre terá páginas de promoções ou publicidade, nos sites de comércio eletrônico, dos produtos de seu interesse. Na verdade, não se trata de um problema de segurança, mas alguns usuários podem considerar este tipo de atitude uma invasão de privacidade”.

6. segundo outra matéria jornalística, intitulada softwares espíões monitoram os computadores, publicada no jornal O Estado de S. Paulo, ed. De 30.10.2000, Caderno de Informática, de autoria de Kátia Arima – cuja cópia nos permitimos juntar ao presente protocolado os cookies levam informações dos usuários para os sites “Entretanto, são dados fornecidos pelo próprio internauta, digitados nos formulários da página (...) Os cookies ficam arquivados no disco rígido e servem como um cartão de identificação do usuário para a próxima visita. **Por si só, os cookies são inofensivos. O problema surge quando essas informações são fornecidas ou vendidas a outras empresas sem o consentimento do internauta. Agências de Publicidade, por exemplo, fazem cruzamentos de dados para levantar perfis de consumidores e realizar propaganda direcionada (...)** (grifos nossos).

Estas últimas notícias jornalísticas chamam a atenção para o fato de que “a legislação brasileira ainda não tem norma específica em relação à privacidade on-line O Código do Consumidor é aplicável a esses casos. Segundo a advogada Andrea Monteiro Affonso, da Tess Advogados, a tendência no Brasil é a adoção do modelo europeu Safe Harbor. De acordo com a resolução que institui o Safe Harbor, aprovada neste ano pela União Européia, **o usuário deve ter a alternativa de limitar o uso ou a revelação de informações. Ele deve ser avisado claramente sobre o propósito da coleta e uso de informações, o perfil de terceiros a quem são reveladas as informações, entre outras exigências.**”(grifos nossos)

Diz a notícia, ainda, que ‘nos Estados Unidos discute-se como conciliar o Safe Harbor com a tradição de privilegiar a liberdade contratual e auto regulamentação de mercados (...). A privacidade do americano, enquanto isso, é desrespeitada’.

7. A situação no Brasil, como noutros países, no que toca a violação da privacidade on-line, não é diferente. Está a exigir que providências sejam adotadas para inibir essa prática abusiva. O país conta, hoje, com a denominada Norma de Referências da Privacidade On-line – NRPOL, de junho de 2000, elaborada pela Fundação Carlos Alberto Vanzolini, ligada à Escola Politécnica da USP, com o objetivo



de estabelecer determinados princípios éticos que devem ser seguidos por organizações atuantes na Internet, visando a proteger a privacidade das informações pessoais identificáveis de seus usuários. Estabelecidos os princípios éticos, a NRPOL enuncia também um conjunto de atividades complementares e de procedimentos normativos, que deverão ser regularmente cumpridos por todos os componentes da Organização. Ademais, pode ser utilizada não apenas como um guia de referência, para uma organização implantar com eficácia uma cultura interna de preservação privacidade on line, mas também para propiciar a realização posterior de auditorias e para a obtenção do respectivo Certificado de Conformidade.

Os princípios éticos de proteção da privacidade individual do usuário na Internet, em que se assenta a NRPOL, são os seguintes: (a) as informações pessoais identificáveis podem ser obtidas para um ou mais propósitos e devem ser coletadas por meios éticos legais; (b) o propósito da coleta de informações pessoais identificáveis devem ser especificado antes do instante desta coleta; (c) as informações pessoais identificáveis solicitadas devem ser adequadas, relevantes e não superar os objetivos para os quais são coletadas; (d) as informações pessoais identificáveis coletadas devem ser mantidas integras, conforme fornecidas pelo usuário; (e) as informações pessoais identificáveis devem ser atualizadas quando necessário ou quando for solicitado pelo usuário; (f) a Organização deve ter uma política explícita de práticas e procedimentos com relação aos dados pessoais identificáveis de seus usuários (g) a Organização deve tomar medidas técnicas e organizacionais para evitar a utilização desautorizada ou desacordo com a lei e contra a perda acidental, destruição ou dano das informações pessoais identificáveis de seus usuários; (h) devem ser observados rígidos limites éticos na divulgação e utilização de informações pessoais sensíveis dos usuários; (i) os usuário deve ter acesso as informações pessoais identificáveis por ele fornecidas (j) usuários deve ter mecanismos para comunicar-se com a Organização que coletou seus dados pessoais identificáveis.

Segundo esclarece a NRPOL os citados princípios éticos foram elaborados com base na Legislação Brasileira e Internacional sobre o respeito e proteção a privacidade individual dos cidadãos e em outras matérias e princípios sobre Privacidade On-line, como, por exemplo, os publicados pelo Conselho Europeu, US Federal Trade Commission, OECD e IRSG.

Para fins da NRPOL, são consideradas informações pessoais identificáveis “dados de contato (nome completo, endereços, fones, emails, etc.), documentos de identidade e profissionais (CPF, RG, etc.) informações sócio-demográficas (sexo, idade, do estado civil, dados étnicos, etc.), dados médicos (históricos ou de condições de saúde, outros), escolaridade (graus e outros), imagens da pessoa e outras informações pessoais identificáveis como hobbies, áreas de interesse social, entretenimento, troca de informações (chat-rooms), lista de discussão, boletins, etc.”. São ainda consideradas informações pessoais as coletadas através de cookies² e arquivos de log³, quando tratadas de forma a permitir a identificação do usuário.

Por outro lado, são consideradas informações pessoais sensíveis “as informações pessoais identificáveis e cuja divulgação, não autorizada expressamente pelo usuário, a terceiros através de mecanismo afirmativo (opt-in), possa causar alguns tipo de constrangimento moral ou danos ou prejuízos à sua pessoa ou empresa à qual pertence. Estão incluídas neste critério os dados de históricos médicos do usuário ou relacionados a sua saúde (inclusive registros de compras de medicamentos, de pesquisas ou solicitações de serviços e informações ligadas à saúde), os dados que revelam origens raciais ou étnicas,



dados que revelem opinião política, hábitos sexuais, religião ou credos filosóficos e os dados econômico-financeiros como números de cartão de crédito, de contas correntes em Bancos de senhas dê acesso a serviço financeiros online, dados sobre renda ou patrimônio e outras informações confidenciais que se divulgadas sem o consentimento do usuário, possam dar origem a fraudes outros tipos de problemas.

8. Parafraseando trecho da reportagem Privacidade (Revista Info-Exame, ed. Abril, ano 15, nº 171, Junho/2000) podemos afirmar que em nenhum lugar do mundo é tão difícil ter vida privada quanto na Internet. A cada clique do mouse, as pessoas são marcadas, seguidas, encaixadas em estatísticas anônimas – ou nem tanto – graças a tecnologias cada vez mais perversivas e onipresentes. Estaríamos, assim, sob o domínio do mal na WWW? Nada mais absolutamente falso. Essas tecnologias, ao tomar contadas informações pessoais na Web, melhoram incrivelmente a nossa vida, com sites personalizados, banners que parecem feitos sob medida para nós, ofertas de comércio eletrônico irresistíveis (...). O desafio, a esta altura é traçar os limites entre o que é aceitável e o que é abuso de privacidade na Internet.

No limiar dos século XXI, a metáfora do Big Brother, o grande irmão, espionando o menor movimento das pessoas constante do livro 1984, de George Orwell, está obsoleta, prezando pesadelos do século XX. Com efeito, hoje não é o Estado totalitário (praticamente desaparecido após a queda do Muro de Berlim) quem mais espionava a vida privada, “São empresas, milhares de empresas, conhecidas ou anônimas, que fazem essa vigilância 24 horas por dia. Somos filmados nos estacionamentos, identificados digitalmente na entrada dos escritórios, ‘escaneados’ a cada embarque num avião, monitorados por circuitos de tevê na entrada dos prédios, seguidos nos mínimos cliques na Internet. Monumentais bancos de dados garantem que informações desse tipo sejam acumuladas. Na Web entre senhas e cookies esse controle chega ao ápice. Qualquer coisa que respire, tenha um nome e movimenta um browser entra nesse jogo, voluntária e involuntariamente. Quem quiser escapar terá de virar um eremita”.

Sem que o internauta perceba, cada clique do mouse vai espalhando pela Web rastros sobre seus hábitos de compra, seus interesses, suas preferências, seu status conjugal, a idade dos filhos, as doenças dos pais... No Brasil, 49% dos 100 sites mais populares em 1999 usam cookies, segundo testes do INFOLAB – isto é, abrem caminho até o disco rígido do internauta e armazenam ali um arquivo de texto que identifica o seu computador com um número único. **Com os cookies, pode-se reconhecer quem entra num site, de onde vem, com que periodicidade costuma voltar.**”(grifos nossos)

9. Pelo que se observa do exposto, a representação que gerou o presente protocolado justifica a instauração de procedimento administrativo investigatório pelo Ministério Público, para apurar devidamente os fatos e verificar se é o caso, na espécie, de se tomar medidas com vistas à proteção da privacidade do usuário na internet. É inquestionável que os interesses em jogo são difusos e, por isso, está o MP legitimado a desencadear, se for necessário, a competente Ação Civil Pública.



A investigação com a qual se acena não pode, porém, ser desencadeada por este CAO, por lhe ser vedado legalmente o exercício de atividades de execução. Estas são próprias das Promotorias de Justiça por ele apoiada. No caso vertente, as atribuições para investigar os fatos em apreço estão afetas à Promotoria de Justiça do Consumidor, para onde determino, assim seja remetido o presente protocolado, para as providências que entender cabíveis.

10. Formem-se autos de acompanhamento e comunique-se o envio do protocolado a douta Promotoria de Justiça do Consumidor ao autor da representação.

São Paulo, 1º de dezembro de 2000.

MARCO ANTONIO ZANELATO

Procurador de Justiça e Coordenador do CENACON

Date Created

09/04/2001