

HUGO DE SOUZA MELO

COMUNICAÇÃO MEDIADA POR COMPUTADOR E PRIVACIDADE

Tese de Doutorado apresentada ao programa de Pós-graduação em Comunicação e Cultura, Escola de Comunicação, Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Doutor em Comunicação e Cultura.

Orientadora: Prof^ª Dr^a Fernanda Glória Bruno

Co-orientador: Prof. Dr. Paulo Roberto G Vaz

Rio de Janeiro

2006

S Melo, Hugo de Souza
Comunicação mediada por computador e privacidade
/ Hugo de Souza Melo. Rio de Janeiro, 2006.
vii, 214p.

Tese (Doutorado em Comunicação) -
Universidade Federal do Rio de Janeiro, ECO, 2006.

1. Privacidade. 2. Vigilância. 3. Comunicação mediada por
computador. 4. Comunicação - Tese.

I. Bruno, Fernanda Glória (orient.) II. Universidade Federal do
Rio de Janeiro. Escola de Comunicação. III. Título

CDD:

FOLHA DE APROVAÇÃO

HUGO DE SOUZA MELO

COMUNICAÇÃO MEDIADA POR COMPUTADOR E PRIVACIDADE

Rio de Janeiro, 25 de janeiro de 2006

Fernanda Glória Bruno, Dr^a em Comunicação, UFRJ

Paulo Roberto Gibaldi Vaz, Dr. em Comunicação, UFRJ

Ieda Tucherman, Dr^a em Comunicação, UFRJ

Fátima Cristina Regis Martins de Oliveira, Dr^a em Comunicação, UERJ

Luiz Alberto Rezende de Oliveira, Dr. em Física, CBPF

RESUMO

MELO, Hugo de Souza. **Comunicação Mediada por Computador e Privacidade**. Rio de Janeiro, 2006. Tese (Doutorado em Comunicação) Escola de Comunicação, Universidade Federal do Rio de Janeiro, 1996.

A noção de privacidade, como a entendemos no presente, é historicamente muito recente e pode diluir-se rapidamente em função das novas tecnologias de registro e controle de transações financeiras, movimentação física e históricos médicos e funcionais. A vigilância passou de uma ameaça a indivíduos infratores para uma experiência comum a todos, passíveis de exclusão de seus direitos civis, realizada por incontáveis órgãos públicos e privados e até aceita em um processo de mercantilização, em troca de praticidade ou reconhecimento em relações mercantis. Cada vez maiores e mais entrecruzados bancos de dados, de históricos financeiros, médicos e de identificação biométrica, criam perfis e categorias de risco em uma rede rizomática. Muitas das novas tecnologias de comunicação mediada por computador são utilizadas para a comercialização de dados sobre indivíduos, segmentados geralmente por perfis de interesse econômico, e geram classificações parciais que podem afetar a imagem pessoal em seu meio social ou profissional, afetando a vida de cada um em uma extensão ainda não completamente definida nem limitada por uma adequada legislação de proteção. A divisão público/privado está em relação direta com o desenvolvimento dos meios de comunicação. Este trabalho explora um dos aspectos dessa relação, ao estudar os instrumentos de vigilância presentes na comunicação mediada por computador.

Palavras-chave: Privacidade, Vigilância, Comunicação mediada por computador.

ABSTRACT

MELO, Hugo de Souza. **Comunicação Mediada por Computador e Privacidade**. Rio de Janeiro, 2006. Tese (Doutorado em Comunicação) Escola de Comunicação, Universidade Federal do Rio de Janeiro, 1996.

The notion of privacy, as we understand it in the present, is historically too new and can be quickly blurred because of new technologies of registration and control of financial transactions, physical displacement and medical or job histories. Surveillance has moved from a menace to criminals to a common's experience, subject of exclusion of it's civil rights, exerted by myriad public or private agencies and even accepted in a commodification process, in exchange for easiness or recognition in commercial transactions. Databases, each time bigger and more interlaced, including financial and medical histories, and biometric identification, create profiles and risk categories in a rhizomic network. Many of the new computer mediated technologies are used to sell individuals' data, usually segmented by economic profiles, that produce partial classifications that can affect the person's image in its social or professional environment, and affect each one's life in such an extent not yet completely defined nor limited by appropriate protection laws. The balance between public and private is directly related to the development of the communication media. This work explores one aspect of this relation, studying the instruments of surveillance existing in the computer mediated communication.

Keywords: Privacy, Surveillance, Computer mediated communication.

SUMÁRIO

Introdução	2
Capítulo 1: A noção de indivíduo e privacidade	11
Capítulo 2: Aspectos da vigilância e exemplos na mídia	29
A privacidade em obras de ficção-científica.....	80
Capítulo 3: As tecnologias de vigilância	83
A comunicação telegráfica.....	83
Códigos numéricos	90
RFID (Identificação por rádio-frequência)	91
Câmeras de vigilância.....	97
Reconhecimento facial.....	113
Raios X de baixa potência: vigilância muito pessoal	117
Sistemas biométricos nos EUA	118
Sigilo telefônico.....	121
A vigilância nos eletrodomésticos	122
A falsa identidade	124
A Internet: origens, evolução, situação atual	128
O novo protocolo IPv6.....	135
O papel do usuário conectado: a experiência da <i>Wired</i>	136
Segurança e privacidade na Internet	141
Identificação na Internet	161
O mercado de vigilância	163
Conclusões.....	170
Anexo 1: Glossário de termos da Internet	182
Anexo 2: Cartilha do e-Consumidor.....	194
Anexo 3: Movimento Internet Segura	201
Anexo 4: Política de Privacidade - Globo Online	204
Referências	207

Agradecimentos

Muito grato aos meus orientadores, Fernanda e Paulo, por suas indicações e correções de rumo, à minha esposa, pelo apoio e compreensão, à CAPES, pelo portal de periódicos e à Amazon.com, um recurso fundamental na aquisição de livros atuais e fundamentais para a pesquisa.

A economia do conhecimento só poderá oferecer seu potencial à humanidade se o ciberespaço se tornar mais acessível a todos e for utilizado não só para os negócios, mas também para debater e resolver coletivamente os grandes problemas da comunidade mundial.

Pierre Levy, 2002¹

¹ Lévy, Pierre, *Fundamentos da economia do conhecimento*. Em EXAME. São Paulo: Abril, http://www.uol.com.br/negocioexame/revista/revista0015_1.html, acesso em 27 jun. 2003.

Introdução

Esta tese pretende apresentar um histórico do crescimento, do alcance, e discutir, os mecanismos mais difundidos de vigilância e registro que, em diferentes, graus violam a privacidade dos indivíduos, suas justificativas e críticas, oferecendo exemplos e sua relação com algumas das vertentes teóricas mais pertinentes. Historicamente, mal entramos em uma época de poder usufruir de uma privacidade pessoal sem precedentes. As pequenas comunidades, até menos de um século atrás, eram o cotidiano de quase todos no planeta. Nas cidades modernas, o comércio com moeda (não o escambo) estimulou o anonimato, facilitando o aumento do individualismo, da autonomia, e da liberdade pessoal. O aumento da mobilidade, com o crescimento e a sofisticação dos meios de transporte, reduziu as ligações pessoais que antes duravam toda a vida.

Hoje existem milhares de grandes e médias cidades, onde a convivência tem alto grau de anonimato. Até o século 18, a grande maioria das pessoas não tinha muito espaço para a privacidade, mas isso geralmente não era uma preocupação, pois a baixa expectativa de vida, a não muito eficaz tecnologia médica e grande dificuldade em sobreviver com algum conforto já eram problemas suficientes para quase todos. Apenas questões levadas à esfera judicial, em alguns casos, consideravam problemas de invasão de privacidade. Mas ao menos essa falta de privacidade dava aos indivíduos uma percepção completa de sua individualidade, por parte de sua comunidade local. A atual divulgação de fragmentos privados cria uma imagem que não corresponde à totalidade do indivíduo e pode levar a julgamentos errôneos sobre suas ações.

Quando finalmente, em alguns locais no século 19 e na maioria, no século 20, alcançou-se um patamar de bem estar social que permite a uma parcela razoável da população ter tempo para o lazer, para o pensamento, e gozar da liberdade de escolha de sua identidade, por não ter de obrigatoriamente carregar um histórico passado que geralmente implicava um futuro predefinido (quem o indivíduo podia vir a ser era pesadamente determinado por seu passado, seu histórico familiar, e não por seu potencial e dedicação pessoal), os mecanismos de vigilância, cada vez mais presentes, anunciados pela mídia como garantia da segurança das pessoas, vêm tornando-se uma ameaça a essa duramente conquistada liberdade de escolha de seu futuro, sem garantir sua segurança.

Agora a reputação das pessoas não depende do olhar dos familiares e vizinhos, e muitas vezes também não dos colegas de trabalho. É o registro de sua vida financeira, seu histórico médico, escolar, eventualmente seu registro policial, que vai gerar uma imagem pessoal nas relações de troca e nas oportunidades disponíveis para o indivíduo. É uma vigilância abrangente, mas que não está perto de ser completa, gera uma imagem parcial, e portanto deturpada, do indivíduo, o que pode prejudicar seu desenvolvimento pessoal e profissional.

Um problema enfrentado nessa análise é a grande aceleração da mudança tecnológica, e os curtos períodos de uso de várias dessas tecnologias, o que impede uma análise comprovada de sua influência e abrangência, um “veredito” de sua boa ou má aplicação. O impressionante avanço da eletrônica e da computação em apenas 20 anos, as novas relações criadas pela telefonia celular e pela Internet, a globalização dos mercados, afetando o trabalho e o fluxo de informações, nem sempre garantem uma visão clara do presente, o que dirá do futuro.

Mas um ponto que parece destacar-se com clareza é que os mecanismos de vigilância estão criando um sistema de classificação social que podem levar à mesma ‘determinação’ de nosso passado histórico. O que o indivíduo fez, onde ele viveu, seu histórico financeiro, seu histórico médico, vão determinar de forma cada vez mais inflexível suas oportunidades no futuro, restringindo a liberdade e gerando conjuntos de informações pessoais fragmentadas, que não dão uma idéia adequada do indivíduo como um todo, mas que são usados para ele (e contra ele) em suas relações com os órgãos e sistemas da sociedade cada vez mais conectada, e excluindo sumariamente uma grande parcela da população que não tem os meios de participar dessa nova sociedade em rede como membros ativos, mas que sofre seus efeitos.

A mídia de massa com maior alcance ainda é a televisão, com seu mecanismo um-todos, onde uma mesma mensagem homogênea é enviada por um emissor para vários receptores. Décadas depois da afirmação que o meio é a mensagem (McLuhan), com a evolução tecnológica e a segmentação da audiência, que permite a uma mídia diversificada visar seu público-alvo, pode-se afirmar que a mensagem é o meio (Castells). Com a descentralização, a diversificação e a segmentação, os discursos das diversas mídias estão determinando as mudanças nos mecanismos de comunicação.

Ainda de acordo com Castells (2000), essa diversificação das mensagens não acarreta a perda de controle do discurso pelo poder, sejam as grandes empresas globalizantes ou os governos. Mesmo com mais concorrência, mais empresas de mídia a nível mundial, e com a concentração de várias mídias por uma empresa, a televisão é cada vez mais oligopolista.

Nesse ambiente, a comunicação interativa, mediada por computadores, se faz cada vez mais presente. As empresas físicas utilizam a rede para ampliar seu alcance (as redes de TV estão aprimorando e ampliando portais na Internet, e o maior grupo de entretenimento, AOL-Time Warner, investe simultaneamente em TV, cinema, música e Internet). Junto com as empresas “virtuais”, estão aperfeiçoando novas mediações, e as teorias que estudam os processos de comunicação por transmissão ou conversação não mediada não são mais suficientes para dar conta dos novos mecanismos mediados por computador: os de conversação mediada, consulta e registro (Mayer).

O registro é objeto de estudos acadêmicos norte-americanos, canadenses e europeus, por seu grande impacto na privacidade e nas relações sociais de todos, não apenas dos usuários de Internet, que, segundo levantamento da Nua Internet Surveys² em agosto de 2001, eram 513 milhões em todo o mundo, sendo 15 milhões na América do Sul³, em setembro de 2002, já alcançavam 605 milhões no mundo e, segundo a Computer Industry Almanac Inc.⁴ o número de usuários em todo o mundo vai alcançar um bilhão até o final de 2005, sendo 217 milhões com acesso em banda larga (no Brasil, 3 milhões). Para comparar, segundo a mesma fonte, o número de telefones celulares deve chegar a 2,06 bilhões até o final de 2005 (86 milhões no Brasil). O site Teleco⁵ indicava, em novembro de 2005, 82 milhões de celulares no Brasil. Com o aumento dos aparelhos de 3ª geração, com acesso rápido à Internet, a convergência tecnológica contribuirá para reduzir o custo e facilitar a integração de cada vez mais pessoas ao universo digital, embora no Brasil isso ainda se limite a cerca de 13% da população.

As diversas tecnologias de vigilância e coleta de informações (registro) têm pontos positivos e negativos, sendo importante definir limites e mecanismos de proteção

² <http://www.nua.com/surveys/>

³ O GLOBO, 2 out. 2001

⁴ <http://www.c-i-a.com/>, acesso em 14 nov. 2005

⁵ <http://www.teleco.com.br/ncel.asp>, acesso em 3 jan. 2006.

contra a discriminação de indivíduos. O rastreamento dos movimentos dos usuários de meios de comunicação, seu registro e correlação em bancos de dados, coloca em questão uma visão mais ingênua da Internet como o único local de liberdade, e essa questão do rastreamento do indivíduo é um dos debates mais radicais sobre a arquitetura da Internet, sobre a liberdade de informação, sendo um interessante objeto de análise, principalmente nos seus efeitos subjetivos e culturais, que definem a própria arquitetura da rede.

Novas e recentes propostas de legislação, nos EUA e no Brasil, pretendem o armazenamento de todos os cabeçalhos de e-mails durante prazos de um a dez anos. A Lei de Serviços da Sociedade de Informação e de Comércio Eletrônico, aprovada pelo Congresso espanhol em 12 de outubro de 2002, estabelece a guarda por um ano, sob sigilo, de todo o material que circula pela Internet em território espanhol, e estabelece que serviços fornecidos a cidadãos espanhóis fora do país também devem manter esses registros. Os registros telefônicos já são um objeto comum em questões judiciais. No Brasil as transações financeiras são armazenadas com detalhes, por prazos nunca inferiores a cinco anos.

A vigilância hierárquica informatizada talvez se aproxime da concepção ideológica do Panóptico de Bentham, atuando como uma sanção normalizadora, como a interiorização do olhar, a internalização da vigilância, a consciência de sua autodeterminação (Foucault). Mas o processo de formação do discurso dos bancos de dados opera de forma diferente do panóptico, pois essa sensação de interiorização é falsa. Com um 'superpanóptico' (Lyon, 1996) criado pelos bancos de dados, ocorre a produção de indivíduos com identidades dispersas, das quais eles podem nem ter conhecimento, mas que os afetam mesmo assim.

Os e-mails, o que é digitado em chats (sites de bate-papo limitados a um grupo de usuários) ou blogs (diários pessoais em páginas na Web abertas a todos), as buscas feitas via Yahoo, Google, Altavista ou outros mecanismos de busca de conteúdo na Internet, as compras, toda a navegação, são registrados nos servidores dos provedores.

Os cadastros em sites para acesso a conteúdo, pagos ou gratuitos, são detalhadamente registrados por cookies (arquivos de texto gravados no computador pelo

site visitado, com informações do usuário). E esses cadastros geralmente são a única maneira do usuário ter acesso ao conteúdo e aos serviços. Estabelece-se uma troca entre a privacidade e a segurança, um processo de mercantilização da privacidade. As políticas de privacidade apresentadas nos sites não inspiram muita confiança. Os dados dos que navegam na Internet são comercializados, total ou parcialmente, e produzem o imenso tráfego de spams (mensagens comerciais não solicitadas), que são uma ameaça real ao funcionamento atual da Internet. O tráfego diário de e-mails chega a 135 bilhões de mensagens, sendo que 67% delas são spams, revela estudo da empresa Radicati com dados consolidados de 2005.⁶ E aumentam os casos de roubo de identidade, uso fraudulento de depósitos bancários, cartões de crédito e celulares.

Essa coleta de informações sobre os indivíduos é impulsionada pelo comércio eletrônico globalizado. A segmentação do mercado consumidor se vale dessas ferramentas para tentar tornar mais eficiente a publicidade, estabelecer uma relação personalizada entre empresa e usuário, segmentando o mercado para melhor alcançá-lo, mas o exagero já obriga os provedores de Internet a manter filtros de spam que eliminam uma porcentagem significativa de todo o tráfego de e-mails, antes que eles cheguem à caixa postal do assinante.

Os bancos de dados que incluem informações pessoais, como o CPF, padrões de compra, páginas visitadas, consultas feitas, serão, num futuro bem próximo, o que era o exame no mundo da disciplina? Cada vez se coleta mais informações, sem uma definição clara de como são armazenadas, distribuídas, ou eventualmente apagadas. As restrições à retransmissão do material coletado na interação mediada por máquinas não é devidamente regulamentada. São questões importantes porque em vez de simplesmente tentar impedir diversos aspectos da violação da privacidade individual, é necessário compreender as formas de agenciamento adequadas a um sujeito múltiplo e disperso, para produzir estratégias de resistência adequadas à formação da identidade.

As mesmas tecnologias usadas para criar perfis de consumidores passaram a ser usadas para criar perfis de suspeitos de crimes, inicialmente com o discurso de que eram apenas para identificar potenciais terroristas, mas estão sendo usadas indiscriminadamente em segmentos inteiros da população.

⁶ <http://idgnow.uol.com.br/AdPortalv5/CanalDiretorioLista.aspx>, 4 jan. 2006, acesso em 6 jan. 2006.

Os atuais sistemas de vigilância, e de geração de bancos de dados de padrões de comportamento, não oferecem uma proteção satisfatória à privacidade dos indivíduos e empresas. Eles são uma ferramenta eficaz para invasão de privacidade ou discriminação, por não haver mecanismos legais adequados de restrição ao cruzamento de informações entre diversos bancos de dados nem quanto à sua utilização indevida, mas principalmente por fornecerem uma visão parcial, e portanto distorcida, do indivíduo.

Todos esses mecanismos estão tendo seu âmbito ampliado pelo uso da Internet como repositório de dados e fornecedora de meios baratos para a realização dessa prática. A questão da privacidade, por seu impacto na vida dos cidadãos, usuários diretos ou indiretos da rede, tem sua relevância reconhecida por diversos centros de estudo nos EUA, Canadá e Europa, mas no Brasil praticamente não existem publicações a respeito, e não foram localizadas pesquisas no âmbito da comunicação publicadas pela UFRJ, ou pela USP, por exemplo. As pesquisas no país limitam-se, geralmente, a mecanismos de segurança em transações financeiras ou redes de dados em empresas.

A própria definição do que é a Internet, como ela pode ser pensada, se é libertária ou uma ferramenta de controle, e como ela vem se modificando nos últimos anos, tornando-se uma ferramenta de acesso a bancos de dados cada vez maiores e mais integrados, são aspectos importantes e ainda pouco discutidos no âmbito da sociedade brasileira, ainda com baixo índice de usuários regularmente conectados à Rede.

Dada a importância da discussão desse papel da Internet, como libertária ou controladora, há centenas de livros publicados nos EUA, Canadá e Europa sobre um dos seus principais aspectos, os mecanismos de invasão de privacidade. E há matérias a respeito nos principais jornais norte-americanos, quase todas as semanas, mesmo muito antes do atentado de 11 de setembro de 2001. Mas há muito poucas matérias publicadas no Brasil sobre o tema, e o próprio desenvolvimento e penetração da Internet e das tecnologias de comunicação aumenta a cada dia a importância dessa discussão, que se relaciona a vários tópicos da teoria da comunicação.

As matérias publicadas nos últimos cinco anos em um dos jornais de maior circulação, O GLOBO, do Rio de Janeiro, na grande maioria limitaram-se a reportagens de agências internacionais sobre privacidade nos EUA, meios de identificação e

classificação, câmeras de vigilância, matérias locais sobre o uso de câmeras para auxílio ao policiamento e trânsito, os riscos do comércio via Internet e a discussão sobre a certificação digital. Essas matérias n'O GLOBO foram o material de análise do discurso da mídia local sobre o assunto e a maioria das reportagens é comentada nesta tese.

Uma parte significativa da teoria de comunicação analisa mecanismos de transmissão, ou de conversação, mas cada vez há mais utilização dos mecanismos de consulta e registro.

Os processos de comunicação interativa podem ser classificados, de acordo com Bordewijk e Kaam, em transmissão, conversação, consulta ou registro (Mayer):

Se a informação é produzida e distribuída por um provedor central, que controla a distribuição, temos a *transmissão*. É o caso da TV e do rádio, por exemplo.

O oposto é quando a informação é produzida e de propriedade dos seus consumidores, que controlam sua distribuição. É a *conversação*. São os telefones, o e-mail, as listas de discussão, o IRC.

Se a informação é produzida e de propriedade de um provedor de informações, mas o consumidor detém o controle sobre quais informações e quando são distribuídas, temos a *consulta*. Existem vários exemplos, como serviços por demanda, ou recursos de informações on-line usando FTP.

E se a informação é produzida pelo consumidor mas processada e controlada pelo provedor de informações, trata-se do *registro*. Uma central coleta informações do, ou sobre o, usuário. São as centrais de vigilância, sistemas de registro pessoal e/ou financeiro.

Esses processos apresentam algumas mesclas, em função do desenvolvimento de novas tecnologias, mas para a maior parte da discussão é válida a classificação acima.

A sofisticação dos sistemas de bancos de dados permite um grau de controle de informações pessoais sem precedentes na história. Esses mecanismos estão presentes na Internet, inclusive nos portais de grandes órgãos de comunicação, e não apenas nas empresas de venda de produtos ou serviços. E poderão ser aplicados na TV digital interativa, cuja implantação no Brasil está prevista para setembro de 2006. Fazem parte dessas tecnologias os novos mecanismos para coletar informações pessoais, que vêm sofrendo alterações de natureza quantitativa e qualitativa, que são a radicalização do

processo. E muitos desses mecanismos não contam com a opção de enviar (*opt-in*) ou não as informações pessoais, nem com opções para cancelamento (*opt-out*).

Uma pesquisa da revista Time, em 1991, indicou que 76% das pessoas consultadas estavam “um pouco” ou “muito” preocupadas com a quantidade de dados pessoais coletados por órgãos do governo. Um estudo da Equifax mostrou que 70% dos pesquisados considerou ‘ruim’ que empresas comerciais pudessem comprar dados sobre suas características de consumo (Lyon, 1994).

Uma pesquisa⁷ da Navis Interactive, que ouviu 1002 adultos nos EUA, por telefone, entre 19 e 24 de setembro de 2001, logo após os atentados terroristas, sobre a expansão da vigilância governamental, apresentou esses resultados:

- Uso da tecnologia de reconhecimento facial para procurar suspeitos de terrorismo em diferentes locais e eventos públicos: 86% a favor, 11% contra;
- Monitoramento de transações bancárias e com cartões de crédito, para descobrir fontes de financiamento: 81% a favor, 17% contra;
- Adoção de sistema nacional de identificação para todos os cidadãos americanos: 68% a favor, 28% contra;
- Ampliação da vigilância por câmeras em ruas e locais públicos: 63% a favor, 35% contra;
- Monitoramento de salas de conversação e outros fóruns, na Internet: 63% a favor, 32% contra;
- Ampliação do monitoramento, pelo governo, de telefones celulares e e-mail, para interceptar comunicações: 54% a favor, 41% contra.

Cerca de seis meses depois, em 2002, o número dos americanos a favor de um sistema nacional de identificação caiu de 68% para 26%. E o número dos contra subiu de 28% para 41%. (Rosen, 2004: 217).⁸

Nota publicada na coluna Panorama Político, O GLOBO, em 15 de julho de 2002, indicava a preocupação de brasileiros com sua privacidade:

“Pesquisa nacional do Instituto GPP revelou que 58,8% dos entrevistados não concordam em abrir mão de sua privacidade - e nem deixariam a polícia ter livre acesso ao seu telefone, correspondência e conta-corrente - para combater o tráfico de drogas.”

⁷ *Privacidade em tempos de terror*, BusinessWeek, em Valor Econômico, nº 378, 31 out. 2001.

Em uma pesquisa de 190 selecionados para jurados, na Flórida, EUA, em 2002 (Rosen, 2004: 59), os pesquisados consideraram que ser abertamente monitorados por câmeras nas ruas, onde as gravações não eram apagadas, era altamente invasivo, ou ligeiramente menos invasivo que uma busca policial em um quarto ou uma revista pessoal que incluísse cavidades corporais. Ao mesmo tempo, consideravam as câmeras em monumentos nacionais, aeroportos e estações ferroviárias, vigiando em tempo real, sem gravação, como minimamente invasivas, apenas um pouco mais que uma inspeção de saúde e segurança em uma fábrica. Ou seja, eles consideravam diferente a vigilância com gravações da vigilância em tempo real, e aceitavam uma ampla vigilância em eventos, como uma visita presidencial, limitada no tempo e no espaço.

A Internet tornou-se, recentemente, um importante veículo para os bancos de dados (cada vez mais integrados) de sistemas de vigilância, seja armazenando dados, seja permitindo a consulta, principalmente de sistemas de CCTV e outros de identificação biométrica, que estão sendo combinados e podem assim produzir e registrar um acompanhamento permanente de todos os passos dos indivíduos.

A luta por uma sociedade aberta não implica necessariamente uma sociedade transparente, onde vizinhos possam observar uns aos outros usando uma tela e um mouse. É necessário um controle desse processo, um conjunto de leis e normas claras que definam os tipos de informações registradas, os prazos em que permanecerão gravadas, as razões que permitam a consulta e principalmente, o cruzamento entre os bancos de dados, para que se garanta os direitos fundamentais dos cidadãos sem expor sua privacidade desnecessariamente.

⁸ SCHEERES, Julia. *Support for ID Cards Waning*. Em Wired.com, 13 mar. 2002.

1. A noção de indivíduo e privacidade

A preocupação legal com a privacidade existe há muitos séculos. A lei judaica, por exemplo, desenvolveu-se em torno do conceito de *hezzek re'iyah*, a injúria provocada por ver, ou por ser visto, que busca proteger as pessoas inclusive da possibilidade de ser observados por vizinhos (Rosen, 2000). O consenso entre os juristas medievais era tal que uma janela aberta para um quintal comum deveria ser eliminada mesmo se os indivíduos cuja privacidade fosse violada não reclamassem.

A privacidade, na definição de Ethan Katsh, é o poder de controlar o que os outros possam vir a saber a seu respeito (Lessig). Existe uma relação complexa entre a invasão de privacidade (o registro) e a possibilidade de livre expressão. É uma espécie de censura insidiosa porque vai direto ao indivíduo (Turkle), provocando vários efeitos na imagem que o indivíduo tem dele mesmo, como ele se pensa no mundo.

O sociólogo Marcel Mauss, citado por Rosen, traçou o significado da palavra 'pessoa' até sua origem, uma máscara. Em culturas indígenas de Pueblo, o símbolo da personalidade era a máscara utilizada pelos membros do clã nos dramas sagrados:

Em latim, *persona* é a máscara pela (*per*) qual soa (*sonare*) a voz do ator. Os cidadãos da Roma imperial eram definidos pelos privilégios legais que anexavam às máscaras, nomes e imagens de seus ancestrais. Em uma sociedade onde a representação do ser iguala-se ao ser, roubar a imagem icônica de alguém é roubar sua identidade. Por isso, em certas sociedades indígenas, as pessoas resistem a ser fotografadas. Na era Cristã, a personalidade embuti a idéia da alma interior, que acabou sendo transformada na noção de ser autônomo. Mauss acaba resumindo assim a evolução histórica da personalidade: “De uma mascarada para a máscara, de um papel para uma persona, um nome, um indivíduo. Deste para um ser que possui valor metafísico e moral. De uma consciência moral para um ser sagrado e daí para uma forma fundamental de pensamento e ação”.

A questão é complexa. Como existem fronteiras individuais que não podem ser cruzadas pelo Estado, o liberalismo expressa seu respeito pela dignidade, igualdade, individualidade, interioridade e subjetividade dos indivíduos. Quando o Estado ultrapassa o papel de evitar violar a dignidade e a privacidade de seus cidadãos, e usa seu poder para punir cidadãos por violar a dignidade e a privacidade de outros, ele pode

encorajar um grau de vigilância e exposição bem superior às indignidades que busca evitar (Rosen, 2000).

A evolução da sociedade ocidental passou por diversos estágios, cada qual com seus defensores e críticos. Durante muitos séculos não havia lugar para a expressão individual. Os grupos sociais permeavam a vida de cada um, do nascimento à morte. E os movimentos sociais geralmente eram vistos sem liderança individual, como conseqüência de uma reação do grupo às condições existentes. Exemplos como Joana D'Arc são a exceção que confirma a regra. A erupção das massas está ligada à formação dos centros urbanos, e sua presença é percebida por Hobbes (ou a guerra de todos contra todos, ou o Leviatã, que traz a ordem), ou temos também a atualização do local do indivíduo na sociedade. O velho instinto de sobrevivência virou egoísmo, refletindo o interesse do homem no meio social na medida em que não encontre freios à sua ação. Hobbes⁹ criou duas noções. Uma é a do estado natural, a guerra de todos contra todos, todos egoístas, que disputam com toda a violência possível, seus interesses. É a realidade dos bandos, dos pequenos grupos, e a outra é o que pode frear isso, o surgimento de uma violência ainda mais terrível, e maior, o Leviatã, o poder ilimitado do Estado, capaz de causar mais mal que os bandos. Mas em Hobbes esse terror é um valor positivo. Para ele a paixão básica é o medo, o terror. Leviatã é o lugar, a priori, da ordem social, sem ele não há sociabilidade. Temos ou a Ordem ou a Horda.

Para Rousseau, a cada vez que há um movimento de institucionalização, de constituição de soberania no terreno da legalidade social, há o avanço de um pacto entre as partes que formam a sociedade, impulsionado por essa elaboração da violência feita pela astúcia do fraco. A soberania não traz estabilidade suficiente para a sociedade e, pelas crises que provoca, não cessa de trazer perdas e crescimento da miséria em meio à abundância conquistada (pela astúcia de dominação técnica voltada para a natureza, contra a qual o homem se volta por não ser um animal natural). A arma do homem é o intelecto, essa astúcia técnica que serve para dominar a natureza e outros homens, e o importante é esse pacto implícito entre as diferentes forças da sociedade, expresso através da soberania. A duração dessa estabilidade depende do egoísmo do governante,

⁹ A partir de notas de aulas do curso de Redes e sistemas de pensamento na cibercultura, do Prof. Dr. Henrique Antoun, na ECO/UFRJ, em 2002.

que poderá evitar ou fomentar guerras intestinas. Sempre que o pacto é explícito há maior estabilidade e duração da ordem social.

A modernidade seria esse momento no qual o pacto chega à consciência da sociedade. Na democracia a sociedade teria alcançado uma certa maioria face à crise de convulsão social das revoluções e face ao avanço contra a natureza, trazido pelo domínio técnico, então nessa sociedade pode-se fazer um pacto explícito, no qual os grupos sociais cedem à violência de que são capazes em ação direta sobre o corpo social em troca do reconhecimento de sua posição e de sua “parte”. Agora se reconhece de direito o que antes vigorava de fato. A quebra do pacto implica mais perdas que ganhos. Por isso o homem moderno é o grande individualista. O egoísmo voltou a cobrar seu lugar na relação entre os homens. O homem moderno pode se entregar a esse individualismo devido à disponibilidade de riquezas dada pela vida social.

Em Rousseau há um afeto básico e essencial, o egoísmo, do qual derivam todos os demais afetos, que não são senão expressões do egoísmo dentro das condições nas quais ele se exerce: a individualidade, a identidade.

Hume abre uma perspectiva totalmente diferente. A parcialidade se acresce à paixão pelas condições de existência. Ela torna incômoda a existência no meio natural. O desenvolvimento se exprime e caminha quanto mais se ampliam as paixões. Hume vê a moral na sociedade não como algo que se explique pela repressão e sim como a astúcia que torna a paixão ampliável. A moral entra e vigora não pelo que reprime mas pelo que possibilita, ela reprime a parcialidade, não a paixão. A moral se justifica ao expandir a paixão. Um de seus exemplos: se meu cãozinho morre, fico triste. Se leio no jornal que milhares de soldados chineses morreram, fico indiferente. Mas ao me identificar com os mortos em uma guerra, ao pensar neles como homens como eu, lutando por sua crença, sinto-me triste por eles.

Nietzsche disse que para se constituir um pacto tem de haver risco de danos, enfrentamento de forças, por isso ele riu do pacto social de Rousseau. Pactuamos ao examinar os danos mútuos que podem existir, se não há danos, há dominação, não pacto. O acordo social deve ser pensado dentro de outro tipo de determinação que não o pacto, um certo estado da dívida. Para Nietzsche o sacerdote é o pastor do rebanho, o

máximo condutor da força reativa, expresso na figura do cientista. Ele critica fortemente os guerreiros.

O senso comum está mais ligado à solução consensuada, principalmente se incorporamos à enunciação filosófica o pragmatismo do seu exercício. O que torna democrática uma decisão é a consensuação entre parceiros. Regula o espaço e a partilha. Quem “inventa” o senso comum, que responde pela ordem das relações, da passagem do individual ao comunal, é Locke. O bom senso vem da herança aristotélica e diz respeito à compreensão da repartição do tempo. A causa é da ordem do antecedente e a consequência é da ordem do procedente. Para entender a ordem do encadeamento do raciocínio não se pode confundir o efeito com a causa. Ele regula a ordem do tempo.

A sociedade ocidental aos poucos foi reconstruindo suas redes de relações interpessoais, dando um espaço cada vez mais diferenciado à criança, reconhecendo o valor da privacidade, e seus membros duramente conquistaram direitos e reconhecimento. Um retrato dessa evolução, mais centrado na história francesa, baseado na análise de milhares de registros e documentos, é dado na série de artigos reunidos na coleção “História da vida privada”, principalmente nos volumes 3 e 4. A noção atual de vida privada, de um recato familiar, de espaços não abertos a todos os ocupantes da casa, formou-se no decorrer do século 19, na sociedade anglo-saxã, mas há toda uma evolução, que começa a definir-se no século 16, com a Renascença européia. Está fora do escopo da discussão desta tese uma descrição da evolução da privacidade antes desse período, por isso são apresentados aqui exemplos e um resumo histórico de sua evolução nos últimos cinco séculos, em aspectos da vida na Europa, do século 16 ao 20, no Brasil como colônia portuguesa, até o século 18, que desenvolveu-se muito à parte da situação européia, cuja influência se faz mais presente no Brasil do século 19 e da primeira metade do século 20, e da vida nas fronteiras do norte brasileiro que, no século 21, apresenta condições muito semelhantes às do século 16.

Os primeiros colonos no Brasil não tinham nenhuma privacidade, com um mínimo de roupas e bens pessoais, em longos deslocamentos do litoral até os locais onde fundaram as primeiras cidades, com uma convivência íntima ao longo de jornadas de

meses, compartilhando os poucos meios de higiene íntima, a preparação de refeições, os cuidados com os doentes e as poucas notícias que chegavam a qualquer membro de suas pequenas comunidades. A despreocupação com a privacidade pessoal era também estimulada por um sentimento de não pertencimento, os colonos, degredados, militares e funcionários nomeados pela Coroa portuguesa, não viam o Brasil como sua pátria, a colônia era apenas um evento temporário em suas vidas, não havia o desejo de fincar raízes, de investir nada além do essencial em suas casas, em suas vidas, pois o objetivo era voltar à Europa com melhores condições, com alguma riqueza acumulada, com alguns bens conquistados que garantissem uma fonte de renda. Isso é bem claro no parco mobiliário de todos, inclusive dos “governadores” locais, em casas construídas meio às pressas, sem muita preocupação com o acabamento, onde o elemento sempre presente era a rede, onde dormiam, amavam, trabalhavam, comiam, e os poucos exemplares de mobília não indicavam as posses do dono da casa. Naturalmente havia muita miséria mas as casas mais ricas, a não ser nas dimensões, pouco se diferenciavam das mais pobres.

Os demorados deslocamentos dos colonos para os assentamentos, dos religiosos para a catequese dos gentios ou ministrar os sacramentos, dos militares ou funcionários públicos para exercer o poder administrativo, motivavam mais desgosto para com a colônia, pois os insetos, fossem mosquitos sempre a picar, fossem formigas a devorar tudo que não fosse colocado fora de seu alcance, os riscos dos animais carnívoros ou dos índios, geralmente bem pouco amistosos, e as poucas perspectivas de melhora de situação a curto ou médio prazo, contribuía para esse desinteresse com o Brasil. Apenas uns poucos, no século 17, que ganhavam dinheiro com atividades como a mineração, o comércio de pau-brasil, e depois com o tráfico de escravos, que mesmo com todos os problemas rendia mais que as demais atividades, e por isso demorou tanto a ser eliminado, tinham um vínculo mais forte com a colônia mas estava sempre presente o sentimento de precariedade, a certeza de que em alguns anos estariam longe de todas essas atribuições, gozando de um futuro mais pródigo na Europa. Só a mudança da corte portuguesa para o Brasil, em 1808, e os consequentes investimentos criando uma estrutura administrativa no Brasil, com instituições, o fortalecimento da presença de governantes em áreas mais amplas, começou a criar um sentimento de

pertencimento e de que o futuro estava aqui, e não em uma condição idealizada na Europa.

No século 16, os poucos objetos pessoais, geralmente heranças familiares, eram copos ou caixas de rapé, pequenos objetos de cunho religioso, cofres ou acessórios para o transporte de poucos bens nas longas viagens. As casas pobres, com redes e pouquíssimo mobiliário, o contato com indígenas, atualmente menos beligerantes, mostram no século 21, em Rondônia e em outros pontos da Amazônia, praticamente as mesmas condições dos colonos do século 16, e inclusive muitas das expressões vocabulares e modo de falar, são nessas fronteiras, mais próximas do século 17 que do século 20 (Martins).

A distância da metrópole portuguesa e a pequena população feminina faz com que os colonos estabeleçam laços familiares na nova terra, uma situação que existe ainda hoje nas fronteiras amazônicas, onde colonos, principalmente do nordeste e do interior do sudeste, quase todos homens, formam novas famílias na fronteira norte, com “contratos” de casamento sancionados pela comunidade local.

Na vida doméstica na Colônia o domicílio era o espaço de convivência da intimidade, que nos permite avaliar, embora de modo ocasional e pontual, nos documentos da época, as condições de vida privada. O domicílio se sobrepõe à família, pois famílias constituídas a partir de diversos tipos de uniões, formais ou não, freqüentemente estavam dispersas por longos períodos, ou o pai se ausentava a serviço público ou particular, ou a filha casava em outro local, ou o filho partia em busca de novas oportunidades, além das esposas e maridos que abandonavam a família para viver com outros companheiros (Souza).

Inventários, testamentos, escritos de cronistas e correspondências informam dos bens, escravos, herdeiros, mas não de sua convivência. O casamento, embora importante no projeto colonizador do Estado e da Igreja, na prática, era mais comum na elite, embora colonos de origem humilde, inclusive escravos, tenham tido casamentos religiosos oficiais.

A distinção clássica entre público e privado não se aplica à vida colonial brasileira antes do final do século 18 e início do século 19, pois o privado da época não era como

atualmente. Muitas casas tinham apenas um andar e as pessoas passavam a maior parte do dia reunidas em um ou dois dos cômodos. À noite, as redes ou esteiras eram armadas no mesmo espaço de convivência diurna. Cercados de muros baixos, os quintais não isolavam os vizinhos, mas ficando nos fundos do terreno garantiam alguma privacidade aos ocupantes. Os viajantes, normalmente hospedados nas casas das famílias, dificilmente passavam da varanda, onde armavam sua rede. Algumas casas dispunham de um quarto de hóspedes. Nas casas com escravos, a senzala, os chiqueiros e uma fossa sanitária, ficavam nos quintais.

Na fronteira amazônica, no século 21, muitas casas simples têm como espaço privado a cozinha, um espaço mais feminino, nos fundos da casa, e um cômodo de uso genérico na frente, aberto às visitas.

Na época do Brasil colônia, em uma sociedade continuamente devassada pelo olhar dos vizinhos, com as ruas estreitas e a presença constante dos escravos, os jardins eram o mais próximo de um espaço privado, onde as mulheres e crianças da casa passavam a maior parte do dia. As casas mais pobres nem com estes espaços contavam, tendo geralmente apenas dois cômodos.

Nos primeiros séculos da colonização, a rua e a igreja eram os locais de interação social, não só dos moradores da cidade como também dos que viviam em sítios e fazendas nos arredores. Enquanto as mulheres das classes mais altas geralmente eram confinadas em casa e só saíam para a igreja, sempre acompanhadas, nas classes menos favorecidas o deslocamento, no campo ou na cidade, implicava um contato social maior, propiciando mais promiscuidade que intimidade.

A proximidade das casas fazia das visitas sem cerimônia uma prática usual, chegando sem aviso e surpreendendo moradores despreparados para recebê-las, hábito que continuou até o século 19. Mas essas visitas desempenhavam um importante papel na vida social dos indivíduos, e, nas camadas mais altas da sociedade, deram origem a reuniões com danças, jogos e até banquetes, as raras ocasiões em que eram costume usar talheres. Com o hábito de reunir a família para o almoço era sempre entre onze horas e

meio dia, não havia o costume de fazer visitas nesse período. Quem tinha condições, tanto no interior quanto no litoral, descansava após as refeições.

Pelas anotações e registros dos administradores, ou do próprio chefe de família, um dos poucos documentos não oficiais que permitem saber um pouco da vida cotidiana na época, há um registro do que era comprado para a família, como jóias ou roupas, e de algumas atividades domésticas, como a compra de escravos ou alimentos. Essas breves anotações revelam algumas normas de conduta em relação aos escravos da casa, aos devedores, aos negócios com outros membros da família.

Os registros pessoais indicam também que, tendo necessidade de ser praticamente auto-suficientes, as pequenas propriedades, seja no campo, nas vilas ou nos arraiais, envolviam nas tarefas diárias, de alimentação, vestuário, fabricação de ferramentas e utensílios, todos os habitantes da casa, quer diretamente na execução das tarefas, principalmente pelos escravos, quer na sua organização.

No avançar dos séculos, principalmente nos centros urbanos, os ofícios se especializam, embora o escambo continuasse sendo o principal mecanismo de troca econômica. O trabalho, seja dirigido à subsistência, seja voltado para o mercado, trazia dinamismo ao interior dos domicílios, e quanto mais pobre a família, menor a privacidade. Mulheres viúvas, ou casadas com maridos ausentes, administravam a casa e os negócios. Só em meados do século 18, quando a colonização se estabeleceu definitivamente, quando a maioria das pessoas passou a considerar o Brasil como seu país, é que começam a surgir mudanças na composição das casas, tanto no interior quanto no exterior, nas formas de sociabilidade e nos costumes domésticos. A intimidade começou a ser valorizada, principalmente na elite, com mais desejo de conforto, de investimento no mobiliário, e mudanças na própria educação dos filhos.

A Igreja, cada vez mais presente, era no século 18 um importante espaço de convivência e de fiscalização do comportamento pessoal. No aspecto religioso havia mais preocupação com a privacidade, não tanto pela preocupação com as normas do Tribunal da Inquisição ou dos draconianos artigos das Constituições do Arcebispado da Bahia, fosse no sincretismo religioso de cristãos-novos, protestantes, adeptos de religiões africanas ou de feitiçarias de inspiração européia. No segredo do lar, cristãos-

novos continuavam a praticar a lei de Moisés, uns poucos iniciados participavam de benzeções supersticiosas, tomavam remédios fitoterápicos, realizavam rituais africanos, estes geralmente afastados da povoação, em meio à escuridão e ao mato (Souza).

Na Igreja Católica o confessionário era um espaço privado, mantendo em segredo o diálogo com o sacerdote, mas ficava em local estrategicamente visível, público, evitando assim as tentações de intimidade entre confessor e penitente e os comentários dos circunstantes. Institucionalizada a confissão auricular como sacramento indispensável à vida cristã, a Igreja Católica devassou as secretas consciências de seus fiéis, obrigados a detalhar pensamentos, atos e omissões considerados pecados. Os fiéis, a partir dos sete anos, deveriam confessar a cada oito dias e nas festas religiosas, sendo obrigatória ao menos uma confissão anual, na Quaresma. O pároco devia listar nomes, sobrenomes e endereço detalhado dos confessados, sob pena até de excomunhão. Deveriam não apenas ouvir as confissões mas, quando incompletas, solicitar número, espécie e circunstância dos pecados, necessários para uma confissão bem feita, mas sempre com prudência, para que as perguntas não dessem ocasião, principalmente aos jovens, de novos pecados. O sigilo da confissão era obrigação dos padres, que nem sempre mantinham em segredo os pecados que ouviam. As mulheres eram vítimas dessa situação, pois não era incomum receberem no confessionário convites indecentes ou serem vítimas de assédio sexual, impossibilitadas que ficavam, principalmente onde havia somente um sacerdote, de ser absolvidas de seus pecados se recusassem, ou por temer ver reveladas suas intimidades.

Na França, Jean Marie Goulemot¹⁰ escreve sobre a utopia, ou a transparência do público, uma idéia que fez sucesso no século 18, com cerca de 80 novos títulos do começo do século até a Revolução, que traduz nostalgias muito reais. A utopia correspondia ao projeto absolutista que ela ilustra e reforça. Ela era o futuro do passado e, sem o messianismo dos socialistas do século 19, e os sonhos de uma terra prometida que se propagaram pelo ocidente, a utopia aparece como um discurso sobre o passado e suas origens. Sua especificidade reside no ato que a cria, a de Utopus na *Utopia* de Thomas More, de 1516, a de Sévarius em *L'histoire des Sévarambes*, de Vairasse

d'Alais, de 1712 ou na Victorin de *La découverte australe*, de Rétif de la Bretonne, de 1781, e que a instala num tempo sem história. Outro signo de sua perfeição é a organização social utópica: seus membros têm refeições conjuntas, educação coletiva, festas comunitárias. Ninguém nunca está sozinho, todos vivem sob os olhos da comunidade. As casas da Utopia não têm porta nem janela para que nada se esconda.

Os vários exemplos literários, alguns literais, outros metafóricos, mostram que a utopia se alimenta de um estranho paradoxo, pois é o Estado, extraordinariamente poderoso na maioria das utopias, e até mesmo onipresente, que organiza as formas do intercâmbio na comunidade. É como tentar conciliar os sonhos de liberdade e de intercâmbio de um tempo passado com as coerções institucionais do presente. Essa ausência de espaço privado era devida não às múltiplas interrelações comunitárias e sim a uma vontade organizadora do Estado.

Em vez de ser um local de liberdade conquistada, o espaço privado é visto como o que afasta os indivíduos. A nova prática de teatro, que Diderot tenta elaborar (*Conversações sobre o filho natural*, em 1757, ou *Da poesia dramática*, em 1758) apresenta a vontade de isolar-se como uma patologia moral, em vez de uma oposição ao controle do Estado. Jean-Jacques Rousseau denunciava o local da representação teatral como eminentemente corruptor. Ali eram exibidas as mulheres e ridicularizadas as virtudes. Para ele isso degradava os costumes familiares e a vida comunitária. Ao teatro, Rousseau opõe a festa popular, na qual o povo é ator e espectador. Isso é dizer que, além das aparências, a afirmação de um espaço privado não é vista de imediato como uma evolução e um progresso.

Nas memórias, que começaram a ser cada vez mais comuns a partir do século 16, os membros mais proeminentes da sociedade são os autores quase que exclusivos, e excluem delas tudo que não trate da vida pública. Dão a entender que o privado e o íntimo não existem ou não interessam ao discurso. E como são escritos pela parte interessada, buscam exaltar a importância do indivíduo aumentada às custas do coletivo. Seja nas memórias, publicadas, ou nos diários, geralmente relegados à esfera familiar, ressaltam o depoimento individual sobre o coletivo. Mas os diários estão relacionados a um conjunto mais amplo, que constitui os novos sistemas de credibilidade da escritura

¹⁰ As práticas literárias ou a publicidade do privado, in Ariès, p. 370-405.

de romances. Ao longo do século 18 vemos instalar-se no romance toda uma *mis-en-scène* para revestir o texto literário de uma capa de verdade. Em *Robinson Crusóé* evoca-se o manuscrito encontrado num sótão, em *Ligações Perigosas*, cartas descobertas. Ao assumir um papel de narrador, o autor busca revestir o romance de veracidade.

A Revolução Francesa, em 1792, proclama uma república que pretende fundar uma nova sociedade baseada no contrato social, que seja a comunidade de todos os cidadãos, querendo cada um o bem de todos, o sol se levanta sobre um mundo transparente e harmonioso no âmbito da lei e da adesão unânime.¹¹

O século 19 vê surgir um duplo tratamento da criança, que já é reconhecida como algo diferente de um adulto em miniatura, com os direitos e deveres que sua condição física e posição social permitissem. Ao mesmo tempo que há um investimento crescente no filho, uma preocupação com sua educação, com sua inserção e preparo para a ascensão social, por meio de disciplina rígida, ele também é objeto de amor em certas situações. A partir de 1850, na França, veste-se luto pela morte de uma criança, como se faz para adultos. A observação do comportamento da criança, seja pelos boletins escolares, seja pela visão não estereotipada de seu relacionamento com outras crianças, dá à infância a visão de momento privilegiado da vida. As autobiografias passam a se demorar na infância e juventude do autor. A infância se torna a idade fundadora da vida, a criança vira uma pessoa, um indivíduo. E a figura do adolescente também passa a ser reconhecida socialmente, embora o mercado segmentado para essa faixa etária só surja na segunda metade do século 20. E sua formação, principalmente entre 15 e 18 anos, sai do seio da família, para insatisfação dos que viam nisso uma quebra dos princípios morais, e passa aos externatos (mais comuns entre os de renda superior) e aos internatos, separados para meninos ou meninas, onde o convívio social não estimulava os mais nobres sentimentos familiares.

Nas classes mais ricas a criadagem sempre presente retira boa parte da privacidade das famílias, e no século 19 os banheiros passam a ser aposentos fechados e privados.

¹¹ Rousseau, J.J. *Du contract social*, Lignot ed., s.d., citado por Ariès, p. 446.

As jovens criadas, pois progressivamente a profissão foi ficando predominantemente feminina, nos serviços internos da casa, sofrem uma desconstrução de personalidade, não têm mais nome de família, apenas um prenome, não têm relacionamentos fora da casa, não saem da vigilância dos outros empregados ou patrões, e passam a perseguir seus próprios fins. Economizam o que podem para casar-se, diminui a oferta de mão-de-obra vinda do interior para a capital, os salários melhoram, há uma lenta mas progressiva democratização das relações patrão-empregado.

O casamento passa a ter uma conotação mais privada. Até o final do século 19 apenas as esposas francesas usam aliança. A aliança masculina passa a ser usada, sem obrigatoriedade, na passagem ao século 20. A moda da viagem de núpcias se difunde por volta de 1830. A lua de mel no campo garante a intimidade do casal que, se ficasse em casa seria freqüentemente visitado pelos parentes, numa seqüência pré-estabelecida pelos costumes. No final do século 19, em vez de saírem em viagem logo após o casamento, ato comum também na Inglaterra, os recém-casados franceses viajam uns dois meses depois. A viagem de núpcias, embora condenada por médicos que prescrevem um período tranqüilo no campo em vez do cansaço e perturbações das excursões, geralmente a outros países europeus, que é prejudicial à saúde da jovem esposa e a uma provável gravidez, é vista como testemunho de um momento especial, que gera boas lembranças principalmente para a noiva. A importância da cerimônia e da lua de mel ressalta o papel que a mulher, excluída da vida pública, ocupa na esfera privada. Aumenta a intimidade. Enquanto no século 19 defendia-se a vantagem de quartos separados, no início do século 20 tem-se um quarto com uma cama de casal.¹² E a partir daí a mulher passa a dedicar-se apenas à esfera privada familiar, a cuidar dos filhos e do marido. Há um aumento do convívio familiar, um reforço da paternidade.

Não que seja tudo harmonia. A família é criticada por ser um reduto de individualismo, o que se opõe ao igualitarismo pregado no século 19. As desavenças familiares são geralmente resolvidas privadamente, e nas classes mais pobres a violência física é mais freqüente.

“A vida privada deve ser cercada de muros. Não se permite esquadrihar e revelar o que se passa na residência de um particular”, escreveu Littré no *Dicionário* de 1863-

67.¹³ Pequenos grupos e sociedades passam a reunir-se em salões, gabinetes, clubes, às vezes alugados para uma noite, espaços predominantemente masculinos. A casa fixa o homem, lhe dá uma identidade, um lugar na sociedade. Como elemento de fixação, a casa dá origem às vilas operárias, na estratégia patronal de formar uma mão-de-obra estável, familiar. A Terceira República francesa prega a casa bem cuidada, sempre limpa e organizada, sem chegar ao rebuscamento. Um ‘luxo’ para poucos. No século 19 os jovens casais buscam cada vez mais sua própria casa, viver separado dos pais. A independência e a privacidade da própria casa, mesmo bem pequena, reforçam a noção de indivíduo. Isso na cidade, No campo não há muito espaço privado em casas grandes e superpovoadas. As classes populares urbanas desenvolvem uma forma diferente de intimidade, amontoadas em infectos pardieiros. No século 19 o orçamento dos operários não comporta a aquisição imobiliária, e atende à compra de roupas, que permitam seu relacionamento social, no espaço público, sem envergonhar-se de seus trajés.

Os operários nunca gostaram das vilas operárias, uma extensão dos regulamentos do trabalho. A crescente sedenterização da classe operária e o agravamento das condições de moradia aumentaram as queixas dos trabalhadores. Um inquérito parlamentar em 1884 registra as reclamações contra a sujeira dos cômodos de aluguel, “quartos de percevejos”, e das pensões: paredes imundas, latrinas sempre entupidas, odores nauseabundos. (...) Desejam um pouco mais de espaço, pelos menos dois cômodos, e, nas famílias com filhos, “se o pai de família se dá ao respeito, três ou quatro cômodos não são demais”. Assim que podem, os operários separam o dormitório dos pais e dos filhos. Transparece nos registros da época o horror à padronização e o desejo de uma moradia personalizada. Na Inglaterra, na mesma época, a classe operária apresenta um grande desejo de privacidade da casa, “tão grande é o temor de uma intromissão descontrolada do vizinho”.

O final do século 19 viu um desejo de intimidade familiar, conjugal e pessoal. Cresce a repugnância pelo panoptismo dos espaços coletivos, a prisão, o hospital, o quartel, o internato, ou pelos controles exercidos sobre o corpo. Já em 1848, um

¹² Na França, pois nos EUA, a imagem presente na mídia eram camas separadas, até a década de 1950.

¹³ Citado por Perrot, Michelle, em *Maneiras de Morar*, in Perrot, p. 307.

deputado francês de extrema esquerda, Glais-Bizouin apresenta um projeto de lei contra as revistas pessoais nos postos da alfândega.

Já no Segundo Império francês, inspirado em um modelo de casa operária unifamiliar inglesa, com porão, andar térreo com dois cômodos e uma cozinha, um segundo andar sob o teto com dois quartos e sótão, e privadas no jardim, constituiu-se em 1853 a Sociedade Mulhosiana das Vilas Operárias. Em 1862 havia 560 casas na vila, vendidas a preço acessível com financiamentos que chegavam a 30 anos. Em 1895 a vila de Mulhouse foi concluída com 1240 casas, habitadas até hoje, onde viviam cerca de 10 mil pessoas. Os salários dos chefes de família não bastavam para os encargos, esposas e filhos também trabalhavam, numa variedade de 80 diferentes profissões.

Em junho de 1904 o ministro do comércio francês, Georges Trouillot, inaugurou em Paris o primeiro imóvel construído pela Sociedade de Moradias Higiênicas Baratas, um edifício de cinco andares, estrutura de concreto preenchida com tijolos. Houve várias outras iniciativas isoladas mas nada coordenado. Mas a semente da individualidade estava lançada.

No final do século 20, a ocupação territorial do interior brasileiro, principalmente no norte, ocorre com um movimento de fuga de pobres desempregados para áreas que grandes proprietários e empresas vêm ocupando progressivamente, principalmente na Amazônia, com incentivos fiscais e subsídios públicos. No período colonial a renda fundiária não tinha papel social relevante, naquela época o escravo era patrimônio, a posse da terra apenas completava o direito sobre os cativos. Durante toda a colônia o rei tinha domínio da terra, e a posse era uma concessão transitória da Coroa. Se abandonada, voltava ao rei. O regime fundiário criado pela Lei de Terras de 1850, com poucas exceções, unificou domínio e posse, constituindo um moderno regime de propriedade. Tentativas posteriores de atenuar esse direito absoluto de propriedade, como o Estatuto da Terra, de 1965, culminaram nas disposições ambíguas da Constituição de 1988 sobre a chamada terra produtiva.

Hoje, a propriedade da terra e a renda fundiária definem os ritmos e modos de ocupação do país, da expansão de suas fronteiras econômicas, da mentalidade que aceita tomar posse do território, espoliar posseiros e indígenas e instituir a propriedade privada

da terra. Essa noção de posse como condição temporária, a violência presente na ocupação do território, tira dos posseiros, no Pará ou em Rondônia, o direito de uma propriedade nas quais às vezes vivem e trabalham há gerações. O legal e o legítimo se confrontam e documentos, supostamente legítimos, geram conflitos fundiários e expulsão de posseiros. Uma verificação num período mais agudo dos conflitos fundiários, na década de 1970, no antigo estado de Mato Grosso, mostrou que a soma das áreas concedidas nos títulos de posse era o triplo da área do estado (Martins). É uma situação em que o sentimento de comunidade cria laços entre estranhos, que se reúnem para defender um espaço duramente conquistado, pois em muitos casos os posseiros já foram expulsos de outros locais, ao longo dos anos. Diferentemente dos centros urbanos, não há ainda nesses assentamentos de fronteira, uma condição de vida privada muito afastada da realidade da colônia no século 16. Nos grandes centros, notadamente no sul e sudeste do Brasil, a evolução das condições da vida privada acompanhou, mais ou menos proximamente, a evolução européia, sendo que houve, principalmente na capital, no século 19, o Rio de Janeiro, uma considerável influência cultural francesa.

Na Europa, o sentimento de identidade individual acentua-se e difunde-se amplamente no decorrer de todo o século 19.¹⁴ Antes os prenomes vinham sempre da família, do pai ou do avô ao primogênito, mas cada vez mais essa tradição se esvai, e a perda de fé em um patrimônio de caráter transmitido pelo prenome opera a favor do individualismo. Não é só um desejo de individualizar-se, mas também de evitar os problemas de vários homônimos em sociedades cada vez mais numerosas. Os progressos na alfabetização e na escolarização estabelecem novo vínculo entre indivíduo, prenome e sobrenome. Cartões de visita, cartões postais, monogramas em lenços, guardanapos e roupas. Aumentam os registros de casamento assinados pelos dois cônjuges. A identidade corporal começa a aflorar, timidamente, com espelhos nos banheiros masculinos, e mascates que vendem pequenos espelhos para as mulheres.

No campo a identidade corporal ainda é vista pelos olhos dos outros, mas nas cidades há espelhos de corpo inteiro. No campo há interdições ao uso do espelho, mostrá-lo a um bebê pode interromper seu crescimento, deixar um espelho descoberto

após uma morte traz azar. Nas classes abastadas o código de boas maneiras proíbe que uma moça se veja nua, há pós para turvar a água da banheira. O estímulo erótico da imagem do corpo enche os bordéis de espelhos que, muito tempo depois, passam a ser pendurados na porta interna do armário nupcial (e nos tetos dos atuais motéis).

Mesmo hoje, nem sempre existe a preocupação com a privacidade, e ela pode incomodar quando afronta os costumes vigentes. Uma nota publicada pelo jornal O GLOBO, no suplemento Morar Bem, em 7 de dezembro de 2003, traz uma reclamação sobre vizinhos que andam em seu imóvel, a dez metros da janela do reclamante, em trajas sumários, e um deles completamente nu. A preocupação do reclamante era saber o limite entre seu direito e o dos vizinhos incômodos:

“Respeitando o direito de vizinhança, até onde vai o direito dele e onde começa o meu? O direito à propriedade inclui o ato de andar nu dentro de casa com janelas e cortinas abertas? Devo ajuizar uma ação? Para isso, como posso provar o que digo? Se eu o fotografar estarei invadindo sua privacidade? As providências devem ser tomadas pelo condomínio ou pelo condômino?”

A resposta do jornal foi:

“Qualquer pessoa tem o direito de, dentro de seu imóvel, andar nu com as janelas abertas. Se tal conduta incomoda o leitor, pode-se alegar violação ao artigo 1.277 do Código Civil (interferência prejudicial ao sossego), bem como o ilícito penal de ato obsceno, previsto no artigo 233 do Código Penal. Entretanto, não é uma posição unânime. Assim, sugiro, antes de qualquer ação judicial civil ou criminal (que deverá ser adotada pelo leitor e não pelo condomínio), que o leitor entre em contato com seu vizinho e exponha a questão e seu desconforto, podendo daí surgir uma solução amigável.”

Voltando ao século 19, a moda do retrato participa do processo de imitação por capilaridade, satisfazendo o desejo de igualdade. O retrato se difunde em pingentes, medalhões, cartões de visita. Em 1862, apenas um fotógrafo, Disdéri, vendia 2400 cartões por dia. Aumenta a auto-estima, o álbum de família delimita a configuração dos parentes, conforta a coesão do grupo, modifica a visão das idades da vida, muda o sentimento do tempo. Há uma mudança nas referências da memória familiar, valoriza-se

¹⁴ Corbin, Alain, *O segredo do indivíduo*, in Perrot, p. 419.

a relação visual em detrimento da orgânica. E o novo processo acaba por favorecer a vulgarização e a contemplação da imagem da nudez. Desde 1850 uma lei proíbe a venda de fotos obscenas em via pública. (No Rio, em 2005, a Câmara de Vereadores proibiu cartões postais com nádegas femininas expostas, alegando que estimulam o turismo sexual).

As autoridades, no interior do espaço público, cada vez mais se interligam em redes de conhecimento. Já a multidão nas ruas, cada vez maior, perde sua teatralidade, dissolve-se em indivíduos imersos em seus pensamentos privados. Começam a aprimorar os processos de identificação, de controle social. No final do século 18 haviam recenseamentos a cada cinco anos. As listas eleitorais foram estendidas a toda a população masculina em 1848. Os operários passam a portar uma carteira de identificação em 1854. Os militares têm papéis de identificação emitidos pelo governo e os domésticos, pelo patrões. As prostitutas eram registradas pela polícia ou prefeitura. Os viajantes, especialmente itinerantes e nômades, devem ter um passaporte. Inicialmente toda essa burocracia é ineficaz, o conhecimento pessoal impera. Mas com o progresso da alfabetização a identificação ganha força. A construção do tempo pessoal permite elaborar uma história individual, condição para a identificação.

Quando é imperativo perscrutar a personalidade de alguém, por exemplo, um candidato a casamento, emprego civil ou doméstico, o prefeito e o padre são solicitados a opinar. Embora seja uma prática sujeita a boatos, é bem aceita. Apenas os médicos parecem poupados, como se o segredo profissional inspirasse maior discrição.

Mas essa papelada não garante uma identificação correta. Qualquer um que saiba local e data de nascimento pode passar por outra pessoa, se for de constituição física ao menos parecida. Mesmo uma testemunha pode ser contestada, alegando-se que não se vêem há vários anos. Como a lei de 1832 aboliu a marcação a ferro em brasa de criminosos, os policiais só contam com uma boa capacidade de observação para identificar suspeitos.¹⁵ Em 1876 a polícia francesa começou a empregar fotografias. Mas sem um sistema de catalogação, eram inúteis. Em 1882 Alphonse Bertillon introduziu as medições antropométricas. Ele prova que cinco ou seis medidas ósseas efetuadas com

¹⁵ Mas no século 20 é comum que os presos que passam alguns anos na prisão saiam de lá com tatuagens

rigor e conforme um procedimento fixo são suficientes para identificar alguém. E Galton convence Bertillon a incluir as impressões digitais em seus registros.

A lei de 16 de julho de 1912 impôs a nômades e itinerantes, inclusive comerciantes e industriais de outros países, um procedimento antes restrito às delegacias e prisões: uma carta de identidade antropométrica, com nome, sobrenome, data e local de nascimento, fotografia e impressões digitais.

É o início de um processo que culmina com os *chips* de identificação, atualmente injetados em cães e gatos na Europa e nos EUA e, dentro de poucos anos, presos na orelha de todo o rebanho bovino brasileiro. E também presentes nos novos passaportes de diversos países. Com carteiras de identificação usuais, que têm de ser verificadas uma a uma, manualmente, apenas alguns dados são registrados, mas com um sistema digital de identificação pessoal, todas as vezes que houver uma coleta de dados, rápida e automática, sobre movimentação física, transações financeiras ou exames médicos, toda essa informação ficará registrada em um banco de dados, e com tudo padronizado, será fácil integrar as diversas bases de dados, criando um controle num grau apenas imaginado na ficção. Isso explica a grande resistência dos norte-americanos, com uma longa tradição de luta pelos direitos civis, a um documento de identificação nacional obrigatório. Na fantasia de *Futurama*, desenho animado de Matt Groening (criador dos *Simpsons*), que se passa na Nova Nova York do ano 3000, todos têm um chip de carreira implantado no pulso, o que define sua profissão, sua identidade, seu futuro.

Nosso futuro?

(Os chips RFID e diversas outras tecnologias de vigilância são discutidas no terceiro capítulo.)

2. Aspectos da vigilância e exemplos na mídia

Como comentado na introdução, a vigilância hierárquica informatizada busca convencer as pessoas a assumir normas de comportamento que as integrem “melhor” na sociedade. O dispositivo panóptico operacionaliza e aperfeiçoa as relações de poder. O ‘superpanóptico’ (Lyon, 1996) criado pelos bancos de dados produz indivíduos com identidades dispersas, das quais ele pode nem ter conhecimento.

Essa é a grande preocupação na defesa da privacidade. Dados diversos sobre alguém não formam um painel fiel de sua personalidade. O todo é maior que a soma das partes e apenas as pessoas mais íntimas podem chegar ao conhecimento da maioria das partes. Quem conhece bem outra pessoa é capaz de avaliar se determinado ato é ou não representativo da personalidade da pessoa. Divulgar dados parciais cria uma imagem que pode ser prejudicial à pessoa, às suas aspirações profissionais e pessoais.

O argumento aceito há dezenas de anos por juízes norte-americanos em defesa da liberdade individual é que não se pode divulgar informações parciais sobre alguém, e muito menos fazer um julgamento sobre as pessoas, com base em informações parciais. Ou se tem o quadro completo ou não se arrisca uma opinião. Na coleta de informações pelo mecanismo de registro, a personalidade integral do indivíduo não está em questão, o que importa é sua posição em um mercado segmentado. O que alguém comprou pode formar um padrão para novas ofertas de produtos, com uma margem de erro que diminui à medida que aumentam a base de dados. Mas quando essas bases de dados se ampliam para incluir dados financeiros e médicos, elas criam um grande potencial de ameaças, de várias formas e alcances.

Até agora a preocupação dos governos tem se voltado para os aspectos financeiros. O jornal Valor Econômico¹⁶, publicação conjunta de O GLOBO (Rio de Janeiro) e Folha de São Paulo, informa que o Ministério da Justiça anunciou que os contratos de planos de saúde contêm cinco cláusulas contratuais abusivas, que ferem os direitos dos consumidores. Três cláusulas são referentes a cadastros de consumidores. O Ministério pretende que seja considerado abusivo o envio do nome do consumidor a bancos de dados e cadastros de inadimplentes, como Serasa e o SPC (Sistema de

¹⁶ Governo restringe uso de cadastros, in Valor Econômico, São Paulo, 28 ago. 2002.

Proteção ao Crédito), sem notificação prévia do consumidor para defesa. O ministério não mais admitirá a imposição ao consumidor de cláusulas em contratos de adesão que o obrigam a se manifestar contra a transferência de seus dados cadastrais a terceiros. Esse tipo de cláusula é muito comum em consórcios e diversos contratos de prestação de serviços, e a tendência é que o Brasil adote a nova legislação norte-americana, que em vez do *opt-out* (se o cliente não se manifesta, dados seus são distribuídos ou vendidos a outras empresas), institui o *opt-in* (o cliente tem de claramente autorizar a distribuição de dados pessoais, para fins de mala direta ou ofertas personalizadas por mídia impressa ou online). Outra medida, de difícil execução, torna ilegítima a autorização ao fornecedor para investigar a vida privada do consumidor. Essa prática é comum em contratos de financiamento de compra de imóveis.

Mas ainda não há muita preocupação com os bancos de dados de laboratórios e clínicas, que, sem uma proibição legal explícita, poderiam vender informações de resultados de exames clínicos a empresas de planos de saúde ou eventuais empregadores. Muitas pessoas ainda não se deram conta do potencial dos bancos de dados, e principalmente do que publicam na Internet. Fotografias de estudantes bêbados em bailes de formatura podem ser um critério na seleção por futuros empregadores. Registros de clínicas de desintoxicação, internações hospitalares, exames clínicos podem ser fatores no cálculo de risco (e custo) de planos de saúde e também pesar nas entrevistas de emprego. Uma solução pode ser armazenar dados médicos em formato XML, o formato de dados adotado pelo pacote Office da Microsoft, e em muitas páginas da Internet, que, além do conteúdo e layout codificados pelo HTML, permite incluir informações de contexto dos dados, e se os dados forem criptografados, esses dados de contexto podem ser usados para restringir o acesso. Assim uma enfermeira teria acesso a alguns dados, um clínico a outros e um anestesista a outros, mas ninguém teria mais informações que as necessárias para sua tarefa.

Alguns países implantaram, e estão expandindo cada vez mais, sistemas de vídeo de vigilância e reconhecimento facial, e o processo foi acelerado após os atentados terroristas nos Estados Unidos em 2001. Na Inglaterra, em 2000, existiam 300 mil câmeras de vídeo instaladas nas ruas, prédios públicos e comerciais, monitoradas em parte por centrais de polícia, em parte por particulares. Em 2005, são 4,2 milhões.

Tanto na Inglaterra quanto nos EUA, parte dessas câmeras está sendo integrada a sistemas de reconhecimento facial que comparam o rosto das pessoas com um banco de dados de procurados pela justiça. Em 2003 ainda não havia um sistema aprimorado, pois um boné e óculos escuros eram suficientes para impedir o reconhecimento, pois os sistemas de então se baseavam em até 30 parâmetros físicos. Mas a próxima geração vai melhorar a precisão, utilizando 80 parâmetros.¹⁷

A invasão de privacidade está no fato de gravar as imagens, em vez de apenas compará-las com os bancos de dados de criminosos, em tempo real, e descartá-las em seguida quando não há uma combinação. Fiscalizar as ruas com câmeras sai mais barato que manter patrulhas motorizadas, porém foram identificados vários casos de policiais em Londres utilizando as câmeras para bisbilhotar pessoas em seus apartamentos.

Um artigo de Phil Patton, publicado na revista *Esquire* em 1996 (*Caught. You used to watch television. Now it watches you*) já se preocupava com câmeras de vigilância distribuídas por toda a cidade. Ele previa dois tipos possíveis de sociedade, uma em que há câmeras de vigilância em toda a parte, conectadas a centrais de “polícia”, e outra em que há câmeras de vigilância em toda a parte, inclusive nas centrais onde os policiais “vigiam”, mas as pessoas têm acesso a “vigiar” os vigias. Patton declara que não se trata de duas entre várias possibilidades, são as duas únicas possibilidades, e é preferível então viver onde se possa vigiar os vigias.

Os sistemas de reconhecimento biométrico podem trazer mais segurança contra a clonagem da identificação pessoal, como a leitura de impressões digitais, a identificação de voz, a varredura da retina ou da íris (esta já em implantação em aeroportos europeus), mas seu uso, estudado pelos bancos para os caixas automáticos, exige a regulamentação de melhores mecanismos de segurança dos dados.

Em nome da segurança pública, aceita-se cada vez mais a invasão de privacidade. O artigo ‘Big Brother’ nas ruas inglesas (O GLOBO, 18 jan. 2004), esclarece:

Qual o país do mundo que mais vigia os passos de seus cidadãos? Errou quem respondeu Coréia do Norte ou Cuba. Segundo um estudo apresentado semana passada numa conferência internacional em Sheffield, Inglaterra, cada residente de Londres tem

¹⁷ “Teste realizado nos EUA com 121.589 imagens de 37.437 pessoas foi desastroso”. (in Segurança para

sua imagem captada, em média, 300 vezes ao dia pelo sistema de CCTV (câmeras de televisão de circuito fechado) [por 30 redes diferentes (Rosen, 2004)]. São mais de quatro milhões de câmeras espalhadas pelo país, uma para cada 14 habitantes. Enquanto países como a Alemanha e o Canadá proíbem a coleta de imagens de pessoas na rua, a Inglaterra, tão zelosa de sua imagem de civilização recatada e privada, tem uma legislação particularmente branda quanto ao uso de CCTVs. Entidades de defesa dos direitos civis questionam a eficácia da medida no combate ao crime ou na prevenção de ataques terroristas. Pesquisa citada recentemente pelo jornal “The Independent” concluiu que uma melhor iluminação de rua é sete vezes mais eficaz para a diminuição de crimes. Pela Lei de Proteção de Dados regulamentada em 2000 na Inglaterra, o público deveria ser alertado para a localização de cada câmera e de como exercer o direito de acesso a sua imagem. Pelas contas de entidades civis, 70% das 4.285.000 câmeras instaladas no país violam algum artigo da lei. Agentes de segurança de lojas, prédios e shopping centers freqüentemente usam o sistema para efetuar o que o professor Clive Norris, do Centro de Pesquisa Criminalística de Sheffield, chama de “limpeza social” do local.

É possível localizar e enviar publicidade específica a usuários de telefonia celular. Isso permite enviar propaganda de uma empresa próxima ao usuário do telefone celular, maximizando a oportunidade de venda de produtos ou serviços, o que já ocorre em *shoppings* no Brasil, porém as operadoras de telefonia celular podem manter registros detalhados de toda a movimentação física do telefone, e esses dados podem ser vendidos a interessados.

Isso não é o registro das ligações feitas ou recebidas, que um software de reconhecimento de padrão pode utilizar para validar ou não ligações interurbanas ou internacionais, por exemplo, protegendo o usuário legítimo de alguém que use um telefone “clonado”, é um registro da movimentação do telefone, quarteirão a quarteirão, à medida que passa pelas várias células da operadora.

Dados gerados por acompanhamento de navegação na Internet e pagamentos eletrônicos podem ser interceptados, em geral em computadores de distribuição de fluxo de dados ou nos centros de processamento das empresas vendendo produtos ou intermediando transações, provocando prejuízos financeiros de difícil ressarcimento devido ao pouco uso de tecnologias seguras de criptografia, ainda não regulamentadas

na maioria dos países. A tecnologia de reconhecimento de usuários na Internet por meio de *cookies* (pequenos arquivos de texto com informações sobre a navegação do usuário) serve para criar um perfil de compras para cada usuário, e para identificar o usuário e sugerir produtos semelhantes às suas compras anteriores, o que é interessante. Vários sites na Web identificam o endereço Internet de quem navega por eles. A Amazon.com fazia uso de um sistema que utilizava o CEP e nomes de domínio para identificar os principais livros comprados por empregados de grandes empresas (Rosen, 2000). Mas a venda de listas de clientes (listas de *e-mails* ou mala direta de editoras) e a venda de estatísticas (sem relacionar as pessoas) de grupos de consumo devem ser regulamentadas para proteger a privacidade individual. E os cookies podem espionar computadores.

Sistemas de GPS (localização por satélite) e auxílio à navegação terrestre podem monitorar o percurso de veículos de carga ou passageiros, por um lado impedindo seu funcionamento em caso de roubo ou furto, e por outro gerando relatórios dos padrões de deslocamento dos indivíduos, aumentando sua vulnerabilidade a seqüestros, se os dados forem divulgados, ou localizando seqüestrados, se os criminosos não se desfizerem do chip, que pode estar na roupa, sapato ou embutido em telefones celulares, vendidos, por exemplo, em serviços de acompanhamento da movimentação de filhos menores, pelas operadoras, inclusive no Brasil.

Segundo a Secretaria da Segurança Pública de São Paulo, em matéria publicada em 1 de fevereiro de 2005, no Diário de São Paulo, ocorreram no início de 2005, de 9 a 10 casos de seqüestro por mês no estado. Apesar da tendência de queda nos casos de seqüestro, conforme as estatísticas de 2001 a 2004, esse tipo de crime ainda é um dos mais temidos pelo paulistano, que utilizam celulares com GPS, carros com rastreadores, monitorados 24 horas, chips colocados em cintos e sapatos e até mesmo sob a pele. Na Espanha, freqüentadores(as) assíduos de clubes noturnos usam chips implantados sob a pele para identificação e registro de consumo, posteriormente debitado no cartão de crédito, por considerar prático seu uso.

Esse serviço combina as tecnologias de telefonia celular e GPS, e opera onde há sinal de celular, o que permite localizar o aparelho com uma precisão de até dez metros. Nos EUA, no Japão e na Coréia, mais de cinco milhões de pessoas usam o serviço mas

para recreação e como utilidade pública. Além de localizar o usuário, o celular com GPS também oferece opções dos melhores itinerários urbanos e indica cinemas, bares e restaurantes próximos do cliente.

As câmeras de monitoração de trânsito urbano podem ser utilizadas para gerar informações sobre estrangulamentos no trânsito, enviadas a telefones celulares ou PDAs (computadores de mão) com acesso via rádio, com o potencial de ser uma ferramenta para indicar um percurso a ser evitado, se possível, mas geralmente não são utilizadas para combater esses estrangulamentos, reordenando o fluxo de trânsito ou a presença de policiamento, nem para ampliar o policiamento nos locais tradicionalmente afetados por excesso de veículos nos horários de pico. No Brasil elas têm sido usadas para controle de acidentes, em túneis, pontes e outras vias críticas, para deslocar reboques ou ambulâncias. Mas em outros países, principalmente na Inglaterra, seu uso em vigilância está ampliando-se exponencialmente, sem uma melhora correspondente no trânsito.

Sistemas de informações geográficas (GIS) acoplados a bancos de dados para prever padrões de consumo de energia ou água, por exemplo, úteis no planejamento urbano, podem ser cruzados com bancos de dados da empresa telefônica (na página da Telemar, na Internet, basta digitar o nome do assinante, mesmo incompleto, e o sistema fornece telefone e endereço) ou com os dados da Receita Federal (vendidos no centro de São Paulo, conforme divulgado nos jornais em 2004)¹⁸ para criar um perfil detalhado dos moradores de cada prédio.

Exames de sangue e fluidos detectam o uso de substâncias perigosas ou ilegais, buscando evitar a desigualdade de condições em competições esportivas e riscos sérios para empregadores em determinadas funções, mas os exames laboratoriais são arquivados em computadores e não há um impedimento legal para que esses dados não sejam transferidos para empresas de seguro de saúde. Nos EUA muitas empresas exigem exames de sangue com análise de doenças existentes e a tendência (por análise sanguínea ou de DNA) a sofrer de outras doenças, discriminando funcionários mais capazes que outros em função da probabilidade de um problema involuntário de saúde. Na Inglaterra há um projeto de lei para obrigar a informação de determinadas doenças

¹⁸ Ver nota na pg. 169.

não contagiosas ao seguro de saúde. A polícia inglesa conta com um banco de dados já com o DNA de 250 mil pessoas após dois anos em operação.

Segundo nota publicada na revista Domingo, do jornal O GLOBO, em 8 de janeiro de 2006, pessoas que fizeram testes de DNA, nos EUA, Austrália ou Europa, que indicaram a suscetibilidade a doenças, estão sendo rejeitadas, ou pagando mais, a seguradoras de saúde. Algumas pessoas alegam que exames de sangue de rotina foram utilizados por empregadores para testes de DNA. Para avaliar a situação e propor medidas contra o problema, foi fundado em Sydney, Austrália, o Projeto Contra a Discriminação Genética (<http://www.gdproject.org/>), que realizou uma pesquisa com pessoas que se submeteram a testes de DNA preditivos, nos últimos cinco anos, incluindo entrevistas confidenciais, para avaliar sua compreensão do conceito de discriminação genética, e suas experiências. As equipes do projeto coletaram, nos últimos anos, dados sobre o uso de informações genéticas pelas seguradoras, e pretendem realizar uma pesquisa nos casos de discriminação genética levados aos tribunais. E irão examinar as reclamações de tratamento injusto, sofrido pelos interessados que apresentarem suas questões às equipes do projeto.

Uma nota no jornal on-line M&C News (<http://news.monstersandcritics.com/>), de 2 de novembro de 2005, reproduz uma notícia da agência UPI:

Um crescente número de empregadores e seguradoras australianas foram acusados de discriminar pessoas com genes que as tornam suscetíveis a determinadas doenças. Na mais abrangente pesquisa contra discriminação genética, cerca de uma a cada 12 pessoas testadas geneticamente declararam ter sofrido discriminação, como a recusa de cobertura por seguro de vida. (...) A pesquisa analisou questionários enviados por mais de 1000 pessoas que realizaram testes genéticos preditivos para doenças como desordens neurodegenerativas ou câncer.

Uma reunião em outubro de 2005, da American Society of Human Genetics, em Salt Lake City, Utah, declarou que 87 pessoas, 73% da amostra, informaram ter sofrido de ocorrências específicas de tratamento negativo, mas nenhuma delas encaminhou uma queixa formal, em geral por não saberem a quem reclamar.

Mas há algumas experiências positivas. O Department of Veteran Affairs, dos EUA (a antiga Veterans Administration, VA) merece crédito por abraçar com

entusiasmo a noção de aprender com os erros em uma profissão que tradicionalmente evitava a admissão pública do fracasso. Em 1999 a VA pediu a James Bagian, médico, engenheiro e astronauta, para utilizar sua experiência científica para examinar o processo por trás dos erros médicos. E em maio de 2000 a VA anunciou que havia contratado a NASA para duplicar nos 172 hospitais da VA o programa que havia tido tanto sucesso no aumento da segurança na aviação, estabelecendo um sistema no qual os erros poderiam ser relatados sem medo de penalidades e as informações seriam analisadas para criar proteções contra erros no futuro. O prestigiado Instituto de Medicina relatou em 1999 que os erros médicos matam de 44.000 a 98.000 americanos hospitalizados por ano. Na nova iniciativa da VA/NASA, qualquer trabalhador da área de saúde pode relatar erros cometidos ou testemunhados. Após o trabalhador ser entrevistado para obter-se mais detalhes, as informações de identificação são retiradas do banco de dados (Russo, p. 235).

Uma opção para a proteção da privacidade, como a compra em espécie, oferece algum risco pessoal e não é estimulado, sendo que o uso de cartões eletrônicos, de débito ou de crédito, é estimulado por campanhas publicitárias que distribuem prêmios entre os usuários. Nos EUA é comum que os cartões da própria loja dêem direito a desconto no preço de todas, ou quase todas as mercadorias, forçando assim seu uso, e criando um perfil de consumo de cada consumidor.

Outros mecanismos, como a moeda virtualizada via rede (créditos adquiridos previamente, e usados anonimamente para pagamentos on-line), com a autenticação de transações (da Verisign, por exemplo), o uso de criptografia em *e-mails* e o uso de chaves pública e privada, ainda são pouco disseminados. O governo federal brasileiro está regulamentando a certificação, e abriu em 2001 uma discussão pública a respeito, para elaborar uma legislação a respeito.

Com os devidos cuidados (senhas, antivírus, firewall etc.) os cartões de crédito são mais seguros no mundo virtual que no físico. Matéria publicada na Gazeta do Povo, de Curitiba, PR, em 10 de maio de 2005¹⁹, intitulada “Fraudes com cartão afetam dez pessoas por dia em Curitiba”, informa que:

¹⁹ <http://tudoparana.globo.com/gazetadopovo/>, acesso em 10 maio 2005.

Em Curitiba, foram registrados mais de dez boletins de ocorrência por dia durante o mês de abril devido a prejuízos com cartões bancários. As 316 queixas correspondem a 62% do total de casos repassados ou atendidos no período pela Delegacia de Estelionato e Roubo de Carga. A maioria dessas reclamações está ligada à clonagem dos dados gravados nas tarjas magnéticas. (...) Para montar um “laboratório de clonagem” é preciso ter três equipamentos: uma impressora (para a fabricação da parte física do cartão), uma processadora de trilhas magnéticas (para a gravação e leitura dos dados lógicos contidos na tarja) e um skimming, conhecido como “chupa-cabra” (utilizado apenas para copiar os cartões, em geral operados por empregados [no comércio] que participam da fraude). Todos esses instrumentos podem ser comprados, inclusive pela Internet, por até R\$ 250 mil. O valor pode parecer alto, mas é irrisório perto dos R\$ 200 milhões de prejuízos causados por ano pelos fraudadores, segundo a Associação Brasileira de Empresas de Cartões de Créditos e Serviços (Abecs).

Durante um século e meio o panóptico despertou apenas o interesse de criminalistas até que Michel Foucault, em *Vigiar e Punir* (1975), argumentou que a cristalização do poder da visão, embutido na forma arquitetônica do panóptico, havia saído dos limites da prisão para alcançar hospitais, escolas, fábricas. Para Foucault, a vigilância do panóptico representa uma nova forma de poder, que opera pelo condicionamento e pela correção. Não é necessário um regime totalitarista com um controle centralizado, para reforçar normas disciplinares. A disseminação da vigilância pelos diversos agentes do tecido social não exige essa centralização para impor o controle. E as normas não têm de ser exatamente as mesmas em todos os locais. Um comportamento reprimido em escolas ou hospitais pode ser aceito em lojas ou órgãos públicos. O reforço é das normas específicas de cada local, e os indivíduos aprendem a comportar-se de acordo, pois em cada local haverá sanções específicas.

Norris e Armstrong comentam que não surpreende que várias análises, como as de Bannister²⁰ e Reeve²¹, comparem o sistema de câmeras de vigilância ao panóptico, no seu aspecto de potencial disciplinador. Mas esse aspecto disciplinador só é eficaz

²⁰ Bannister, J., Fyfe, N. e Kearns, A. *Closed Circuit Television and the City*, em Norris, C., Moran, J. e Armstrong, G. (eds.), *Surveillance, Closed Circuit Television and Social Control*, Aldershot: Ashgate, 1998.

²¹ Reeve, A. *The Panopticism of Shopping: CCTV and Leisure Consumption*, *ibidem*.

quando a vigilância é acompanhada de técnicas de modificação de comportamento, doutrinação e socialização. Eles lembram que Giddens²² argumentou que o totalitarismo é, primeiramente, um foco extremo na vigilância. E este “primeiramente” indica a presença de outros mecanismos disciplinares. Não basta o poder de vigiar para implicar o poder disciplinador do panóptico, no argumento de Foucault. Ou seja, a proliferação das câmeras em áreas públicas não implica o surgimento do estado totalitário do Grande Irmão. E também ainda não há um sistema centralizado de vigilância, pois além das câmeras em vias públicas, a maioria com controle centralizado na autoridade policial e/ou de trânsito, há milhares de sistemas de câmeras independentes, em escolas, hospitais, lojas, instituições financeiras, condomínios privados, e seus sistemas geralmente não se comunicam.

Norris e Armstrong (1999) citam o livro de James Rule, *Private Lives, Public Surveillance*, de 1973, onde ele descreve uma sociedade de vigilância total, onde só existe um sistema de vigilância e controle, que vigia a todos. Ele força o cumprimento de um conjunto de normas que ditam todos os aspectos comportamentais. Todas as ações dos indivíduos são registradas e avaliadas no momento e posteriormente. Todas as informações são armazenadas em um ponto e estão sempre disponíveis cada vez que for tomada uma decisão sobre o indivíduo. Qualquer sinal de desobediência, presente ou prevista, sofrerá uma ação corretiva, e as sanções serão imediatas. Com a detecção e retaliação inevitáveis, um sistema assim impede até o pensamento da desobediência.

É uma idéia presente em *We*, de Eugene Zamiatin, publicado inicialmente em 1924, onde todos, exceto os governantes, vivem em uma cidade futurista feita de vidro e retomada, no aspecto da previsão, em *Minority Report*, de Philip K. Dick.

Dandeker (1990) identifica quatro componentes que servem como referência para determinar quão próximo está um sistema de vigilância de ser total:

- 1) A dimensão dos arquivos do banco de dados em relação à população, ou seja, as imagens das câmeras estão vinculadas a registros sobre os indivíduos que as câmeras gravaram?

²² Giddens, A. *The Nation State and Violence*: v. 2 de A Contemporary Critique of Historical Materialism, Cambridge: Polity, 1985.

2) A centralização dos arquivos, pois se simplesmente mudando de cidade pode-se “fugir” dos registros na cidade anterior, o sistema não é tão eficiente.

3) A velocidade do fluxo de informações. [Atualmente esse é um componente obsoleto. Com intranets e a Internet, banda larga e baixo custo de armazenagem, o problema é relacionar imagens a registros, se o software for eficaz nisso, em minutos ou horas, todo o sistema terá acesso às informações.]

4) O número de pontos de contato entre os indivíduos e a população, que inclui não apenas o número de câmeras mas a rapidez com que a “autoridade” reage ao que as câmeras mostram.

Uma questão é se os sistemas de circuito fechado de TV (CCTV) implantados como câmeras de vigilância em diversas cidades, grandes e pequenas, em vias públicas, órgãos públicos e empresas privadas, realmente se aproximam, ou têm o potencial, de realizar a vigilância total descrita por Rule e, por meio dessa vigilância, reduzir a incidência de crimes, seja reagindo rapidamente a uma ocorrência, seja criando o sentimento de vigiado pelo panóptico, o que reduz a propensão aos crimes.

Norris e Armstrong (1999) relacionam as principais questões relativas à natureza dos sistemas de CCTV: (1) Se são uma ferramenta que reduz a criminalidade, e como são utilizadas na sua prevenção, ou seja, qual o julgamento provocado pelas imagens, quais comportamentos dos observados acionam medidas de repressão, e se são usadas para reprimir ações, não necessariamente criminosas, de segmentos da população. (2) Em uma sociedade onde freqüentemente os interesses de uma minoria mais poderosa sobrepõe-se aos da maioria, os sistemas de CCTV priorizam os comerciantes? (3) Com a aura de Grande Irmão associada à vigilância ostensiva, por que tem havido tão pouca resistência pública? (4) O olhar mediado pela câmera impede as interações pessoais. Isso provoca uma mudança no comportamento dos observados? Se grupos sociais consideram-se alvos preferenciais do sistema, isso os levará a desafiar a legitimidade de tais sistemas e aumentar a resistência? (5) Considerando a vigilância uma forma de poder, quais os limites que lhe são impostos? Qual a legislação e como ela é interpretada e aplicada? (6) É necessário considerar o impacto das novas tecnologias de computação, criação e integração de bancos de dados, pois os sistemas digitais permitem rápida captura e comparação das imagens obtidas pelas câmeras, e essas

informações podem ser redistribuídas para outros sistemas de vigilância e acompanhamento.

Os sistemas de CCTV são detalhados no terceiro capítulo, mas a discussão desses pontos pode ser iniciada aqui. As pesquisas já realizadas não comprovam uma redução, significativa ou ao menos razoável, da criminalidade em áreas observadas por câmeras e em suas proximidades. Brin (1998) cita estudos sobre Glasgow e King's Lynn, que ligam a redução nos crimes à instalação de câmeras de CCTV. Mas Rosen (2004) comenta que esses estudos foram excluídos pelo Ministério do Interior inglês, por sua metodologia não ser confiável.

Em 2002 o Ministério do Interior britânico fez uma revisão abrangente dos vinte e dois estudos empíricos mais confiáveis no Reino Unido e nos EUA, sobre a relação entre CCTV e redução dos crimes (Rosen, 2004). A conclusão foi que os sistemas de CCTV tiveram pouco ou nenhum efeito em crimes nos transportes públicos ou no centro das cidades. Em particular, observou que não tiveram efeito na redução de crimes violentos (a partir de cinco estudos) e a única categoria em que teve um efeito desejável significativo (a partir de oito estudos) foi no roubo de veículos em estacionamentos.

Como mostram alguns exemplos a seguir, a crítica principal é que há um deslocamento das atividades, há menos crimes na área sob vigilância e eles ocorrem nas áreas vizinhas. Em instalações fechadas, como *shopping centers*, a área vizinha mais próxima nem sempre é segura. A Inglaterra está tentando impedir esse deslocamento pela implantação de um sistema com milhões de câmeras, mas isso não é factível na maioria dos países. Um argumento que pode ajudar a entender o porque disso ser tão mais disseminado na Inglaterra que em qualquer outro país é que lá, há séculos, a sociedade mantém algum grau de separação entre classes, por nível econômico, formação educacional, local de origem, e até pelo sotaque. No decorrer do século 20 essa separação foi diminuindo e a classificação social estabelecida pelos sistemas de vigilância tem se mostrado eficaz ao erigir novamente barreiras entre segmentos da população. Claro que nem todos os cidadãos compartilham desse pensamento mas ele é ainda muito presente na Inglaterra. E os ingleses têm uma maior confiança nas “autoridades” públicas que os cidadãos de outros países.

O uso principal dos sistemas de CCTV beneficia, é claro, ao comércio, mas pode-se argumentar que esse benefício estende-se aos consumidores. Este aspecto ainda não é uma questão tão importante no Brasil. O discurso jornalístico vende a equação “vigilância = segurança”, e busca informar várias ocorrências de crimes que foram solucionados (mas não impedidos) pelos sistemas de CCTV em apoio à ação policial. Isso explica em parte a pouca reação negativa do público, que, movido por uma percepção psicológica do risco, nem sempre na medida de sua probabilidade real, prefere acreditar que a vigilância realmente vai trazer mais segurança.

Um ditado antigo diz que “notícia boa não vende jornal”, porque as tragédias atraem mais atenção e curiosidade. Um levantamento de Jason Ditton, da Universidade de Sheffield mostra que 45% dos crimes presentes nos jornais envolvem sexo e violência, mas eles são apenas 3% de todos os crimes informados. Uma pesquisa de audiência no horário nobre da TV americana, por George Gerbner, da Universidade da Pensilvânia, mostrou que quem assiste muito à TV tem uma percepção muito maior da probabilidade de crimes do que quem assiste pouco. Os espectadores regulares de mais horas superestimam a chance de serem vítimas de crimes violentos, acreditam que sua vizinhança é mais perigosa, acham que a criminalidade está aumentando mesmo quando ela diminui, e compram mais fechaduras, cães de guarda e armas (Rosen, 2004: 78).

Na Inglaterra, que é um bom campo de estudos, devido à abrangência dos sistemas de CCTV e à sua já “longa” implantação, pessoas em áreas mais distantes do centro da cidade vêem as câmeras como uma medida de repressão, uma tentativa de impedir o crime de cruzar fronteiras e consideram que não trazem melhorias para sua vizinhança.

Quanto aos limites, há uma série de novas legislações propostas, em diversos países, para ter algum controle sobre a vigilância eletrônica, mas o escopo da vigilância está aumentando mais rapidamente que a legislação que deveria regulamentá-la, legislação essa frequentemente sujeita à interpretação dos tribunais, ou seja, ainda não existe um *corpus* jurídico definido e bem claro a todos sobre o alcance e limites da vigilância.

As câmeras, como instrumento de vigilância pessoal, são de pouca utilidade se não produzirem material organizado, classificado e de rápido acesso, para uma

identificação precisa. No século 19 os prisioneiros já eram fotografados, mas não havia uma ampla distribuição local nem acesso a essas fotos em outras cidades, ou seja, não havia um registro acessível de identificação de criminosos. Os britânicos começaram a se preocupar com isso quando, em 1853, deixou de ser viável enviar os criminosos condenados para as colônias, como a Austrália.

A frenologia lombrosiana foi uma tentativa, mal sucedida, de identificação que pecava por tentar prever o comportamento criminoso futuro com base em uma interpretação da estrutura craniana. Mas a base dessa idéia, não comprovada cientificamente, persiste até hoje nos preconceitos contra diversos grupos étnicos, em vários países, e pondera o grau de atenção dos operadores dos sistemas de CCTV sobre quem está sujeito à vigilância das câmeras.

As fotografias não classificadas têm de ser observadas uma a uma, até localizar o suspeito, se a pessoa for boa observadora. Em 1874 a polícia metropolitana inglesa já tinha 117.568 criminosos registrados, e uns 30 mil a mais a cada ano. Como comentado no capítulo 1, em 1882 (conforme Ariès e outros autores), Alphonse Bertillon padronizou a tomada de fotografias, o sistema de fotos de frente e perfil de presos e, em conjunto com outras medidas antropométricas, além de sinais e tatuagens, iniciou um processo de classificação numérica para permitir uma identificação mais rápida de suspeitos, com razoável sucesso, embora pequenos erros nas medidas provocassem registros diferentes, mas reduzia muito a quantidade de fotografias a ser examinada. A partir de 1901, o sistema foi abandonado em favor das impressões digitais.

Um problema decorrente da vida em uma sociedade de estranhos, onde a maioria das pessoas não tem uma longa experiência em comum, é que, como já foi comentado, a construção da reputação pessoal depende de mecanismos de classificação e registro, como diplomas, registros de trabalho e criminais. Se, por um lado isso amplia as possibilidades de desenvolvimento pessoal, não vinculando o futuro da pessoa necessariamente a seu passado, já não basta mais o reconhecimento pessoal que garantia a reputação. Um exemplo disso é uma reportagem publicada no jornal inglês *Guardian*, de 22 de abril de 1998 (Norris e Armstrong):

Em outubro de 1997 foi aprovada uma lei na Califórnia, EUA, após uma adolescente ter sido supostamente assassinada por um cuidador de uma escola, que tinha registro criminal. A lei obrigava o registro das impressões digitais de todos os professores e demais profissionais das escolas, que têm contato com os alunos. Ken Payne, que já havia sido professor em tempo parcial, antes da vigência dessa lei, ao tentar novamente um contrato em tempo integral, e sendo aceito, não pôde ser contratado por sofrer de dermatite atópica, uma condição médica na qual a pessoa não tem digitais claras. Mesmo sem ter registro criminal, fato comprovado pelo FBI, e com uma declaração favorável de um capitão da polícia local, que o conhecia desde a infância, ele não pôde ser contratado.

No contexto da CCTV, Fyfe e Bannister (1998), citados por Norris e Armstrong, argumentam que outra consequência da sociedade de estranhos é o medo da diferença. Mas isso tem dois aspectos, pois a convivência urbana diminui as restrições ao desenvolvimento pessoal em função do passado de cada um, mas conta-se com a polícia para manter a ordem e resolver as desordens. Os indivíduos podem relacionar-se com estranhos para construir novos laços pessoais e profissionais. Antes não havia estranhos nem necessidade de uma polícia “externa” à comunidade, a própria comunidade resolvia seus conflitos. Com o crescimento da cidade, a ocupação dos espaços é melhor definida, e criam-se zonas de exclusão, segregação e controle. Essa classificação social, produto da vigilância que se torna cada vez mais impessoal, é estabelecida em função da segurança, uma demanda social cada vez mais presente. É a introdução de uma sociedade de risco, mais orientada pelas probabilidades futuras que pelos acontecimentos passados. E na qual a vigilância é cada vez mais presente. E onde a coleta, o registro de informações, é a ferramenta para aprimorar as previsões que norteiam a vigilância.

Não é mais o controle do indivíduo por seus pares. É o controle de grupos, determinados por mecanismos de classificação, que avaliam seu potencial de risco, e que para isso dependem de uma vigilância cada vez mais abrangente, e dos bancos de dados formados e alimentados por essa vigilância. A atual tecnologia digital permite que esses bancos de dados sejam integrados e consultados rapidamente, mas dadas as limitações dos sistemas de vigilância, uma combinação de tecnologias e operadores, estes mais sujeitos a erros que aquelas, a imagem resultante dos dados acumulados nem

sempre representa uma avaliação correta do risco que o indivíduo represente à sociedade.

Um veículo parado em local de grande movimento não é mais visto como enguiçado, o que é muito mais provável, mas como uma possível bomba, evento muito menos provável, e esse clima de medo é alimentado pelo discurso da mídia, freqüentemente na venda da equação vigilância = segurança, para justificar a implantação de mais e maiores mecanismos de vigilância.

Os direitos individuais tão duramente conquistados em muitos países, estão sendo simplesmente ignorados, em vista do ‘bem maior’ da segurança, por mecanismos de vigilância e repressão operados geralmente por pessoal sem um treinamento adequado, e a mídia ‘vende’ esses mecanismos como a melhor solução possível, quando ela mesma, às vezes, registra críticas e sugestões de medidas menos radicais e mais eficientes para a segurança pública.

Na maioria dos países europeus há uma grande preocupação com a instalação de sistemas de CCTV, geralmente em ritmo lento e acompanhada de uma nova legislação que a regule. Na Inglaterra, onde ocorre há vários anos a maior e mais rápida instalação de sistemas de CCTV, sem que a legislação de controle de uso acompanhe a velocidade da implantação, há uma questão que não é levantada pela maioria dos autores que escrevem sobre o assunto. A proibição de porte de armas pela quase totalidade da população e das forças policiais, uma medida que efetivamente reduziu muito os índices de homicídios, embora outros crimes tenham aumentado, pode ser um fator importante na aceitação de um sistema de vigilância tão abrangente, que promete tanta segurança, mesmo sem comprovação de resultados, pois há o reforço da medida anterior do governo, que realmente deu resultados positivos.

Um ponto de consenso entre vários autores é que o crescimento do complexo empresarial-militar, estimulado pelo final da Guerra Fria entre “EUA e aliados” e “URSS e aliados”, cujo ponto marcante foi em 1989, com a queda do Muro de Berlim, foi um fator importante no crescimento dos sistemas de vigilância em vários países.

Uma ‘novidade’ na implantação de CCTV é uma notícia de Matt Weaver, publicada no *SocietyGuardian*²³ em 11 de janeiro de 2006:

Até 20.000 residentes a leste de Londres terão cobertura de CCTV ao vivo de sua vizinhança disponível em seus televisores, em um projeto financiado pelo governo, que é parte de um amplo programa de oferta de conexão em banda larga a residências de baixa renda, por £3,50 semanais. A iniciativa desperta temores quanto à privacidade, junto a defensores dos direitos civis, e será testada inicialmente em dois distritos de Shoreditch, Hackney. Um “canal de segurança comunitária” exibirá imagens de 11 câmeras de CCTV próximas. Comportamentos suspeitos poderão ser informados por texto, pelo equipamento do televisor, à polícia local, que poderá divulgar no canal detalhes de pessoas suspeitas de conduta antisocial. Se for bem sucedido, o sistema será oferecido a 20.000 residências na área, coberta por 400 câmeras. O sistema está sendo organizado pela Shoreditch Trust, um órgão que recebeu £53 milhões para recuperar uma área empobrecida, do programa governamental “New Deal for Communities”. Duas outras vizinhanças de Londres expressaram interesse no plano. O chefe de polícia, Gareth Crossman, declarou que as implicações de privacidade reconhecidas da cobertura pelas câmeras significam que seu armazenamento, uso e apagamento estarão sujeitos a princípios de proteção de dados. Permitir o acesso amplo aumenta a possibilidade de infração dos direitos à privacidade. Um porta-voz do Shoreditch Trust insistiu que essa ação não conduz Shoreditch a um estado “Big Brother”, (...) pois todos comentam dos bons velhos tempos nas décadas de 1940 e 1950, quando os vizinhos cuidavam uns dos outros. Trata-se de usar a tecnologia para permitir que todos cuidem de todos. Não é um Grande Irmão anônimo vigiando, toda a comunidade terá acesso a essa tecnologia.” As imagens das câmeras serão transmitidas em blocos cíclicos de 30 segundos. Os residentes não poderão controlar a cobertura nem gravá-la. O Shoreditch Trust irá rever a iniciativa se houver abusos. Mas estão confiantes de que os residentes não farão uso dela voyeuristicamente, ela é para segurança. Ela foi sugerida por moradores, em grupos de estudo. Ela cuida não só da realidade do crime mas do medo do crime, que pode ser tão prejudicial quanto o próprio crime. Os moradores ficam mais confiantes.

A questão de não poder gravar é discutível. Se as imagens podem ser vistas no televisor, provavelmente poderão ser gravadas. Mas não é uma novidade. Norris e Armstrong comentam uma notícia publicada no *Yorkshire Post*, em 11 de abril de 1996,

²³ *Residents given access to live CCTV footage*, www.societyguardian.co.uk, acesso em 11 jan.2006.

que informa que em Doncaster, South Yorkshire, na Inglaterra, as câmeras que monitoram áreas públicas e estacionamentos podem ser vistas nos televisores dos moradores. Ainda não é como previu Phil Patton, em 1996, em que os vigiados poderão vigiar os vigias, mas já é um começo. Supondo que as câmeras só vigiem áreas públicas (funcionários britânicos já foram suspensos por estar observando apartamentos) o argumento é a segurança obtida pela volta da vigilância da vizinhança, cujos exageros já foram observados na Polônia, na Áustria e em outros estados autoritários, no século 20, mas a questão é mais ampla. Cada vez mais a responsabilidade pela segurança, concedida aos governos em “troca” de nossos impostos, recai sobre o cidadão.

Norris e Armstrong argumentam que dois fatores importantes na rápida e ampla implantação de sistemas de CCTV na Inglaterra foram a natureza privada da maior parte do sistema, consistente com a terceirização de cunho neoliberal implantada pelos governos, e um crime de repercussão mundial, o assassinato de um garoto de dois anos, em 1994, por dois estudantes de dez anos, identificados graças a imagens deles saindo juntos de um shopping, divulgadas repetidamente na TV. Um estímulo da mídia, que serviu para cristalizar o medo do público quanto à segurança, e que originou um grande debate a respeito dos sistemas de CCTV, estimulados pelo governo trabalhista.

Essa terceirização dos sistemas de vigilância teve um grande impulso na Inglaterra com a recessão econômica no final dos anos 1980 e início dos 1990. Os grandes *shopping centers* passaram a operar longe do centro da cidade, com uma oferta de amplo estacionamento, baixos preços, segurança e vigilância, e o comércio “de rua” teve uma queda de 40%, com muitas falências. E isso estimulou um sentimento de risco associado aos centros urbanos. Com isso, os interessados, comerciantes e prestadores de serviços localizados no centro das cidades iniciaram um movimento para administrar os problemas, desestimulando atividades que não interessavam aos comerciantes (reuniões políticas, jovens ‘vagando pelas ruas’ e mendicância). De seis cidades em 1986, o movimento expandiu-se para mais de 100 em 1995 (Reeve, 1996, citado por Norris).

Ou seja, não é apenas o temor do crime que estimula a vigilância, há outros fatores econômicos e políticos envolvidos.

A influência da mídia na criação de um discurso social de aceitação dos sistemas cada vez mais presentes de CCTV, faz-se notar nas matérias que geralmente apresentam um discurso otimista sobre a futura melhoria da situação com a implantação de câmeras de vigilância.

As relativamente poucas (145) matérias sobre vigilância ou privacidade, publicadas num dos principais jornais do país, O GLOBO, sediado no Rio de Janeiro, entre janeiro de 2001 e dezembro de 2005, compiladas para esta tese, são na grande maioria, de três categorias. Na primeira, medidas anti-terror, principalmente nos EUA, motivadas pelo ataque terrorista de 11 de setembro de 2001, e são quase todas matérias editadas a partir de reportagens recebidas de agências internacionais. Na segunda, matérias sobre implantação de vigilância, principalmente por câmeras, e resultados de seu uso, no exterior ou no Brasil. Na terceira, matérias de informática, sobre certificação digital, biometria e segurança na Internet, citadas e comentadas no terceiro capítulo.

Com algum destaque, neste período, também houve algumas matérias de cunho econômico, citadas no final deste capítulo, e poucas reportagens sobre ações que reduziram a violência e aumentaram a segurança, sem uso de tecnologias digitais de vigilância, sendo o principal destaque a implantação de restrições ao horário de funcionamento de bares de periferia, nas capitais e principalmente em cidades do interior do estado de São Paulo, após a constatação que a maioria das vítimas de armas de fogo eram baleadas após discussões fúteis, durante a madrugada, entre clientes alcoolizados. Um simples horário obrigatório de fechamento dos bares, em geral entre 23h e 24h, com alguma fiscalização e multas por descumprimento, em várias cidades, reduziu significativamente essas ocorrências.

Houve dezenas de matérias sobre *reality shows*, principalmente os da série ‘Big Brother’ da Rede Globo de TV, empresa da mesma holding que publica o jornal, mas não interessam à discussão apresentada aqui, e não são comentadas nem contabilizadas.

As matérias foram acessadas on-line no dia de sua publicação. Neste capítulo estão a maioria das matérias das duas primeiras categorias e as de cunho econômico. Os **destaques** em algumas matérias indicam pontos importantes para esta discussão. Na primeira categoria, em ordem cronológica, temos:

“Sites tiram do ar informações estratégicas”, de José Meirelles Passos, correspondente em Washington, publicada em 5 de outubro de 2001, que tratava da retirada da Internet de sites com endereços e mapas de instalações militares, de fábricas de produtos químicos, imagens aéreas de prédios de agências de espionagem, e gráficos delineando oleodutos e tubulações de gás.

Na mesma época o governo dos EUA recolheu de todas as bibliotecas públicas, CD-ROMs com informações detalhadas das redes de água e esgoto do país.

“Pacote que aumenta vigilância é aprovado nos EUA”, em 13 de outubro de 2001.

“EUA dão sinal verde para chip sob a pele”, do correspondente Toni Marques, em 22 de dezembro de 2001, sobre a aprovação pela FCC de testes de chips RFID em humanos, que serão aperfeiçoados a médio prazo para permitir a localização via satélite de cada usuário.

“Washington vigiada por câmeras”, publicada em 23 de março de 2002, sobre a instalação de câmeras de vigilância pelo Serviço Nacional de Parques dos EUA.

“União Européia cogita revisão de leis de privacidade de dados”, da Reuters, publicada em 30 de setembro de 2002, comentando que uma pesquisa on-line da Comissão Européia, de mais de 10 mil pessoas, mostrou que os cidadãos da União Européia não se sentem suficientemente protegidos em suas informações pessoais.

Segundo as diretrizes de proteção de dados da UE, assinadas em 1995, dados pessoais, como fichas médicas, números de telefones e endereços de e-mail só poderiam ser revelados ou transferidos para terceiros com a autorização explícita do indivíduo. Essa medida previa o aumento da proteção da privacidade, mas acabou causando uma dor de cabeça burocrática para empresas que queriam transferir dados para outros países. A Comissão Executiva da UE, que redigiu a lei, disse que avaliará os resultados da pesquisa e divulgará as conclusões em fevereiro de 2003.

“Bush vai propor monitoramento da Internet”, de John Markoff e John Schwartz, do New York Times, publicada em 21 de dezembro de 2002, comentava o relatório “A estratégia nacional para a segurança do ciberespaço”, a ser divulgado no início de 2003. A matéria comenta que seria criado um centro de monitoramento controlado pela indústria, mas a proposta abre caminho para que o governo tenha um papel de controle. A finalidade é que seja estabelecido um centro de aviso antecipado para que ataques à Internet sejam detectados logo no início. Mas os provedores argumentam que as funções de monitoramento de dados poderiam ser usadas para rastrear as atividades individuais na rede e é difícil fornecer essas funções ao governo sem o potencial para monitoramento em tempo real de indivíduos.

“MATRIX, ‘Big Brother’ Antiterrorismo”, de Robert O’Harrow Jr., Washington Post, publicada em 7 de agosto de 2003, comentava sobre como arquivos criminais e informações pessoais se juntam num veloz banco de dados na Flórida, para permitir a investigadores encontrar padrões e ligações entre pessoas e eventos muito mais rapidamente do que antes, combinando arquivos policiais com levantamentos comerciais e informações pessoais sobre a maioria dos adultos americanos. Isso permitiria, por exemplo, descobrir instantaneamente o nome e o endereço de todos os homens morenos proprietários de uma picape Ford vermelha num raio de 30 quilômetros do local de um evento suspeito.

“Paranóia com segurança aumenta nos EUA”, do correspondente José Meirelles Passos, publicada em 8 de setembro de 2003, começava com:

“Big Brother” saltou das páginas de “1984”, o famoso romance futurista de George Orwell, para as telas de televisão, transformando-se num programa de êxito mundial. Agora, porém, ele deixa a ficção e o entretenimento para se tornar parte da realidade: é o show da vida cotidiana nos Estados Unidos, figura central da paranóia de segurança na qual o governo vem investindo dezenas de bilhões de dólares. Olhos e ouvidos eletrônicos rastreiam a vida dos residentes, com ênfase especial nos estrangeiros.

A matéria continua com uma entrevista de um contador que veio do Paquistão três anos antes, legalmente:

No início de uma tarde, em abril de 2003, ele levou seus dois filhos, de 18 e 13 anos, para serem registrados no Serviço de Imigração, e a sua vida virou de cabeça para baixo: eles foram imediatamente algemados e passaram uma noite numa sala sem cadeiras. Na manhã seguinte ficou esclarecido que um problema técnico extraviara um pedido de residência permanente, feito meses antes. Mas isso não mudou a situação. Os três foram liberados, mas vêm sendo vigiados enquanto aguardam a decisão de um juiz que poderá deportá-los.

As escolas americanas — do secundário à universidade, passando inclusive pelos simples cursos intensivos de inglês — estão perdendo dezenas de milhares de alunos estrangeiros. E, com a ausência deles, lá se vai boa parte dos US\$ 13 bilhões que os EUA faturam anualmente graças a esses alunos. A média de vagas ociosas é de 20% devido às dificuldades burocráticas criadas para a inscrição de estudantes de outros países.

A seguir a matéria **repete** quase literalmente a reportagem anterior, “MATRIX, ‘Big Brother’ Antiterrorismo”, publicada 32 dias antes. É uma mistura de drama pessoal, a injustiça contra indefesos inocentes, com o problema financeiro e uma repetição de uma reportagem da mídia americana. Pode servir para reforçar a seriedade da questão, mas para quem acompanha o jornal regularmente a repetição, na terceira parte, passa uma impressão de colagem de várias reportagens sobre um tema, não é muito profissional.

Passaporte com chip deixa pessoa vulnerável”, de Matthew Wald, New York Times, publicada em 29 de novembro de 2004, informa que os circuitos integrados a serem embutidos nos novos passaportes americanos, com informações do usuário, eqüivalem a colocar um alvo nos americanos que só pode ser visto por terroristas. E essa preocupação também existe no Canadá, Alemanha e Grã-Bretanha.

“Relatório revela falhas do FBI que comprometem guerra ao terrorismo”, do correspondente José Meirelles Passos, publicada em 20 de dezembro de 2004, comenta o resultado de uma auditoria interna no FBI, revelando que 499 mil horas de escutas telefônicas em idiomas estrangeiros, a maioria em árabe, relacionadas ao terrorismo, colhidas a partir do 11 de setembro, até agora ainda não foram sequer traduzidas, e boa parte dos telefonemas grampeados pelo FBI vem sendo apagada antes mesmo de ser

traduzida. Isso acontece devido ao acúmulo de trabalho dos tradutores, cujo número, mesmo aumentado, é insuficiente para dar conta da tarefa.

“Pesquisa revela desleixo de britânicos com informações”, do correspondente Fernando Duarte, publicada n’O GLOBO, Informática etc., em 28 de fevereiro de 2005, reproduz um estudo publicado duas semanas antes pela Universidade de Glamorgan, no País de Gales:

Micros de segunda mão estão sendo comercializados no Reino Unido sem o devido cuidado de seus donos originais com os dados que eles possam conter. Analisando 111 discos rígidos usados e supostamente “zerados”, pesquisadores descobriram um manancial de informações pessoais e comerciais que poderiam fazer a festa de fraudadores e chantagistas. Ou pedófilos, já que um dos HDs analisados pertencia a uma escola primária da região de Yorkshire, norte da Inglaterra, cujos nomes e endereços de alunos ainda estavam gravados no disco. Os dados incluíam até observações psicológicas sobre crianças. Em outro disco, proveniente da Universidade de Hull, foram encontrados desde documentos confidenciais sobre provas a listas de sites pornográficos acessados por funcionários. Dos 111 HDs, 97 foram comprados no Ebay (site de leilões on-line, ‘matriz’ do Mercado Livre brasileiro). Apenas dez vieram de uma companhia especializada em zerar discos rígidos para revenda, não por acaso, foram os únicos que passaram no teste. Além de informações pessoais, os pesquisadores encontraram até planos de desenvolvimento de novos produtos num HD anteriormente pertencente à Monsanto, empresa de engenharia genética.

“EUA: mais rigor na carteira de motorista”, de Matthew L. Wald e David D. Kirkpatrick, New York Times, publicada em 4 de maio de 2005, fala das regras mais severas a ser adotadas nos EUA na concessão de carteiras de motorista, que deverão verificar se o requerente está legalmente no país:

Atualmente, 11 estados americanos permitem que cidadãos não-americanos tirem habilitação mesmo sem visto. Não há estatísticas sobre quantos estrangeiros têm licença para dirigir, estejam legalmente ou não no país. Pessoas que apoiam a medida dizem que ela vai desestimular a imigração ilegal. Sob as regras propostas, o estado deve pedir uma prova de cidadania americana ou de presença legal, comprovante de residência e do número na previdência social. Deve ainda checar a situação de estrangeiros num banco

de dados nacional de imigrantes, guardar a cópia dos documentos e a foto digitalizada. A carteira deveria incluir a foto e o endereço de seu dono e, no caso de residentes temporários, sua validade acompanharia a do visto.

“EUA apertam o cerco contra crime na Internet”, publicada em 25 de maio de 2005, informa que a Câmara de Representantes dos EUA aprovou novas punições para quem dissemina *spyware*, por 395 votos a um, de até dois anos de prisão e multa de até US\$ 3 milhões por infração:

Quem usar o programa para roubar dados pessoais terá sua sentença aumentada em cinco anos. Os dois projetos de lei aprovados também tornam ilegais práticas associadas ao *spyware*, como programar a máquina para só abrir a Internet em um determinado site ou bombardear o usuário com anúncios pop-up (abertos automaticamente) que só se fecham quando se desliga o computador.

“Polícia busca pistas em celulares”, publicada em 11 de julho de 2005 é uma reportagem de agência estrangeira sobre o pedido da polícia britânica a operadoras de telefonia celular e provedores de Internet para que armazenem o conteúdo de correios de voz, e-mails e torpedos (mensagens SMS) que foram passados no dia dos atentados em Londres:

Esses dados podem ajudar nas investigações. Isso não é obrigatório e algumas empresas responderam ser impossível fazê-lo, por motivos técnicos. O ministro britânico do Interior, Charles Clarke, afirmou que reivindicará da União Européia novas leis para obrigar as empresas de comunicação a reter as informações por mais tempo.

“Polícia britânica identifica os quatro autores dos atentados”, publicada em 13 de julho de 2005, informa sobre as investigações sobre o ataque terrorista ao metrô e ao ônibus, em Londres, na semana anterior:

A polícia britânica disse já ter identificado, em gravações de circuitos de TV, os quatro autores diretos das explosões de 7 de julho. (...) Estamos tentando estabelecer os movimentos deles antes dos ataques da semana passada e, especificamente, determinar se todos eles morreram nas explosões.

“Após novos atentados, polícia britânica pede mais poderes”, publicada em 21 de julho de 2005, informa que a comissão de combate ao terrorismo da Associação dos Chefes de Polícia (ACPO), entre outros pedidos de endurecimento do combate ao terrorismo, reconhecendo o uso crescente da Internet para planejar ataques, pediu poderes para atacar sites específicos.

“Polícia mata um suspeito e prende outro em estação de Londres”, publicada em 22 de julho de 2005, continua a detalhar as investigações sobre o atentado, e pediu a ajuda da população para tentar identificar os quatro suspeitos flagrados em vídeo, com imagens coloridas de boa qualidade. A mesma matéria comenta que:

Por volta das 10h (horário local), um homem não identificado foi morto a tiros no metrô de Londres, na manhã desta sexta-feira, depois de uma perseguição de vários agentes armados, confirmou a polícia.

Tratava-se do eletricitista mineiro Jean Charles de Menezes, depois objeto de diversas reportagens em toda a mídia, brasileira e estrangeira, criticando as falsas alegações da polícia londrina, a desorganização na coleta e distribuição de informações, em um assassinato violento por parte de um agente da polícia londrina.

“Um aparelho para garantir a privacidade nos escritórios”, do New York Times, publicada no suplemento Boa Chance, em 14 de agosto de 2005, comenta sobre um aparelho composto por um processador de som e por vários alto-falantes que multiplicam e embaralham as vozes que estão na sua área de alcance, tornando a conversa próxima a ele inaudível para as demais pessoas. Do tamanho de um rádio-relógio, o primeiro modelo foi projetado para uma pessoa que esteja utilizando o telefone, mas outros modelos podem funcionar em toda a área do escritório.

“Imagens cruciais de Jean Charles”, de Fernando Duarte, correspondente em Londres, publicada em 25 de agosto de 2005, comenta a polêmica sobre a existência (primeiro negada, depois comprovada) de imagens do sistema de segurança da estação onde ocorreu a morte de Jean Charles.

“Rede de câmeras no metrô de NY”, de Helena Celestino, correspondente em Nova York, publicada em 25 de agosto de 2005, anuncia a instalação de um sofisticado sistema de vigilância eletrônica nos metrôs da cidade:

Uma rede com mil câmeras de vídeo e três mil sensores de movimento vai equipar as estações, aumentando a segurança e permitindo o uso de telefones celulares nas plataformas, mas ainda não dentro dos trens. (...) Na primeira fase, a vigilância eletrônica cobrirá 277 das 468 estações, além de duas linhas de trens e nove pontes e túneis.(...) Cada câmera custa US\$ 1 mil. A idéia central é uma complexa rede de câmeras, capazes de transmitir e gravar imagens extremamente nítidas do que acontece em plataformas e túneis de uma distância de até cem metros. As imagens serão **arquivadas** em bancos de dados e oito centros de controle ficarão responsáveis por gerenciar situações de emergência.

“O ano da outra guerra, contra a pornografia nos EUA”, publicada em 18 de dezembro de 2005, Comenta o ataque implacável do procurador-geral Alberto Gonzales à indústria pornográfica, e dá informações sobre a legislação dos EUA a respeito:

De um lado, há a ameaça de uma lei que a comunidade pornô considera draconiana e irreal; de outro, a ação da recém-instituída força-tarefa da polícia federal (FBI) contra a obscenidade. O suporte das duas frentes está nos grupos de lobby conservador e cristão, em nome da família. Em outubro, o FBI simplesmente fechou o site Red Rose Stories. O site não tinha imagens nem sons. Apenas palavras, histórias de bestialismo, pedofilia, escatologia, sexo grupal. Sua autora, Rosie, sequer estava em casa quando os agentes chegaram para apreender seu equipamento. (...) Pelo sim, pelo não, um reduzido número de sites tomou a iniciativa de sair do mercado, vender seu acervo e o domínio na Internet para empresários europeus ou mudar de nicho. Ao anunciar a criação da força-tarefa, Gonzales avisou que atacaria imagens de escatologia, bestialismo e sadomasoquismo. Está mesmo atacando, muito embora, dentro do FBI, segundo comentários na imprensa americana, haja quem considere ridícula a iniciativa, diante das prioridades de segurança do país, como a defesa contra o terrorismo. Consta que a convocação de agentes, iniciada em julho, tem lá suas dificuldades. Mas o que, no país da emenda constitucional que garante a liberdade de expressão, seria obscenidade? Um caso examinado pela Suprema Corte em 1973 foi inconclusivo. Na disputa “Miller vs. Califórnia”, a corte decidiu que a

obscenidade não é protegida pela Primeira Emenda. Contudo a determinação do que é obsceno não cabe à nação, e sim às comunidades locais.

Some-se ao precedente a lei de Decência na Comunicação, aprovada em 1996 mas raramente utilizada, até a explosão da multibilionária indústria da pornografia on-line. Partes da lei foram derrubadas, mas a seção de obscenidade continua de pé. Como a Internet não tem fronteiras, defensores do discurso livre sustentam que ela se choca com a decisão da Suprema Corte de 1973, que devolve à comunidade local o poder decisório acerca do que é obsceno. A lei está sendo contestada na Justiça. (...) A associação da classe, a Free Speech Coalition, acha que acabará vencendo uma luta que, para todos os efeitos, é travada dentro da letra da lei, ou das brechas. Mas para Alberto Gonzales e George W. Bush, a questão parece ser exclusivamente política.

“Bush afirma ter ordenado escutas secretas”, publicada em 18 de dezembro de 2005, informa a razão do Congresso norte-americano não ter prorrogado automaticamente a Lei Patriótica:

O presidente dos Estados Unidos, George W. Bush, reconheceu que deu ordens para que a Agência de Segurança Nacional (NSA) realizasse um programa de escutas eletrônicas em território americano sem antes conseguir permissões da Justiça, e afirmou que daria prosseguimento ao programa secreto porque ele seria “uma ferramenta vital em nossa guerra contra os terroristas.” A revelação de que Bush instruiu secretamente a NSA para que interceptasse as comunicações de americanos e suspeitos de terrorismo dentro dos EUA, sem antes obter permissão de um tribunal secreto que supervisiona assuntos de espionagem, foi citada por muitos senadores como tendo sido a razão pela qual eles votaram contra o governo na renovação da Lei Patriótica.

“Senado prorroga Lei Patriótica nos EUA”, publicada em 23 de dezembro de 2005, informa que:

Num acerto de última hora entre democratas e republicanos, o Senado dos Estados Unidos aprovou a prorrogação da Lei Patriótica por mais seis meses, numa vitória temporária da Casa Branca, que mantém por mais algum tempo sua principal ferramenta legal na luta contra o terror.

Mas diversas outras fontes consultadas informam que a renovação aprovada pelo Congresso americano é por um mês, até 3 de fevereiro de 2006, quando os diversos pontos da legislação serão discutidos, para determinar quais serão renovados, e por quanto tempo.

“Espionagem do governo dos EUA foi maior que a divulgada pela Casa Branca”, da agência Reuters, publicada em 24 de dezembro de 2005, comenta que:

O volume de informações adquiridas por meio de grampos telefônicos e espionagem de e-mails pela Agência Nacional de Segurança dos Estados Unidos sem a aprovação da Justiça foi muito maior que o divulgado, conforme o jornal The New York Times. (...) Autoridades disseram que a agência teve a cooperação de companhias de telecomunicações para ter acesso aos dados locais e internacionais sem que antes tivesse ordens judiciais. (...) Um ex-funcionário do setor de telecomunicações do governo disse ao jornal que líderes da indústria estavam armazenando informações sobre ligações telefônicas e as entregando ao governo federal para ajudar a rastrear possíveis terroristas do atentado do dia 11 de setembro de 2001 no país. (...) O presidente dos EUA, assim como seus assistentes, disse que suas ordens para escutas clandestinas sem autorizações judiciais estavam limitadas ao segmento de chamadas e mensagens eletrônicas para o exterior relacionadas com pessoas com vínculos com o grupo al-Qaeda. (...) Algumas autoridades descreveram o programa como uma enorme operação de extração de informação, disse o jornal, e asseguraram que foi muito maior que admitiu a Casa Branca.

“Galileo estréia no espaço”, publicada em 29 de dezembro de 2005, informa que:

A Agência Espacial Européia colocou em órbita o primeiro satélite que comporá a rede Galileo, que promete revolucionar os sistemas internacionais de localização. (...) O sistema é considerado também o primeiro passo do desafio estratégico da União Européia aos Estados Unidos, ao inaugurar um sistema que tornará obsoleto o sistema militar americano de localização por satélite, o GPS, quando o Galileo estiver em pleno funcionamento, em 2010. (...) Ao todo, serão 30 satélites (27 em funcionamento e três de reserva), além de bases e transmissores em terra. Um convênio com EUA e Rússia permitirá a troca de dados permanente com os satélites das redes militares GPS (EUA) e Glonass (Rússia), ampliando ainda mais o serviço. (...) A navegação por ondas de rádio

será uma característica da vida cotidiana, auxiliando a evitar engarrafamentos e monitorando cargas perigosas. (...) Empresas de telefonia celular ainda estão estudando as possíveis aplicações. Sistemas de trânsito de grandes cidades ou estradas poderão ser mais bem coordenados para evitar problemas de tráfego, trabalhadores em atividades de risco poderão ser monitorados com precisão de centímetros. Companhias aéreas estão entre as mais entusiasmadas, pois cada aeronave poderá ter sua posição conhecida em tempo real, incluindo não apenas sua localização em relação a latitude e longitude, mas também altitude, o que poderia evitar virtualmente qualquer choque entre aviões. (...) Outra possibilidade do Galileo é a capacidade de o sistema receber e enviar sinais. Assim, uma pessoa que esteja perdida e envie um sinal de socorro poderá receber um sinal do sistema avisando que sua mensagem foi recebida e a ajuda está a caminho. O sistema pode funcionar também localizando receptores dentro de prédios e até em pequenas profundidades sob o solo.

O sistema de localização por satélite é comentado no capítulo três.

Dentro dessa primeira categoria algumas matérias receberam um destaque maior para a questão da privacidade, e foram mais elaboradas, como:

“Big Brother vigiará cada um nos Estados Unidos”, do correspondente José Meirelles Passos, publicada em 24 de novembro de 2002, tinha 719 palavras e noticiava o desenvolvimento do programa Consciência Total de Informações (TIA), da Agência de Pesquisas de Projetos Avançados de Defesa (Darpa), do Pentágono, que mesmo antes de concluído, testado e colocado em prática, já tinha um projeto de lei do executivo para lhe dar legitimidade. Tratava-se de uma emenda à Lei de Privacidade, de 1974, permitindo ao governos dos EUA espionar cidadãos americanos ou residentes nos EUA, por via eletrônica. O sistema, composto por uma rede de computadores e uma gigantesca rede de vídeo em circuito fechado, pretende registrar e cruzar informações sobre tudo o que as pessoas fizerem, disserem, escreverem, e a justificativa é o combate ao terrorismo:

Ele saberá o que elas comprem, comem, para onde viajam, o que lêem, quanto depositam na conta bancária, com quem falam ao telefone ou via e-mail e muitas outras atividades, através do rastreamento eletrônico de cartões de crédito, ligações telefônicas

e todos os demais registros do cotidiano. A justificativa para a montagem desse imenso banco de dados, atualizado a cada instante e para sempre, à moda do Big Brother — concebido pelo escritor George Orwell no livro “1984” — é o combate ao terrorismo.

— Temos de nos tornar bem mais eficientes, hábeis e espertos na forma de encontrar novas fontes de dados, e extrair informação de fontes antigas e novas, gerar informação, torná-la acessível para análise, convertê-la em conhecimento, e criar opções de ação legal — disse o almirante John Poindexter, idealizador do TIA e chefe do Escritório de Consciência da Informação, que faz parte do Darpa. No emblema do escritório há um lema em latim: *Scientia Est Potentia* (Conhecimento é Poder).

A matéria comenta as críticas a essa restrição das liberdades civis, um editorial do Washington Post recriminando o novo programa e seu idealizador, Poindexter, dizendo que a responsabilidade de tal projeto jamais poderia estar em suas mãos. Afinal, ele foi condenado por cinco delitos sérios cometidos quando era chefe do Conselho de Segurança Nacional, no governo de Ronald Reagan, como um dos responsáveis pelo esquema chamado Irã-Contras, que financiava o combate aos sandinistas na Nicarágua com a venda ilegal de armas ao Irã.

A matéria continua destacando que as autoridades americanas já começaram a monitorar os passos de todos os cidadãos do Iraque que residem nos Estados Unidos, e os que se naturalizaram americanos também vêm sendo observados, inclusive por via eletrônica, e podem ser convocados a qualquer momento para o que o governo define como “entrevistas voluntárias”.

A matéria destaca a principal crítica a essa ação, chamando as entrevistas de interrogatórios policiais, e informando o temor de atentados como retaliação, quando começar a anunciada guerra contra o Iraque, e que alguns cidadãos têm recebido propostas para se tornar informantes, infiltrados na comunidade iraquiana, o que vai sobrecarregar ainda mais a crescente discriminação contra os islâmicos em geral.

Em 4 de junho de 2004, com a matéria “Vinte anos depois, o Big Brother de Orwell”, do correspondente José Meirelles Passos, que vale a pena registrar na íntegra, reproduz as preocupações com o grau de vigilância e a grande perda de privacidade, e é coerente com outras matérias deste jornal e de várias outras fontes, e apesar disso,

apenas em dezembro de 2005, com o final da vigência da Lei Patriótica, com poucos resultados e grandes problemas no Iraque, o Congresso norte-americano mostrou-se mais resistente às medidas, e/ou sensibilizado às diversas críticas, e renovou a Lei apenas por um mês, para uma discussão mais ampla de sua aplicação e resultados:

Nunca os americanos e os estrangeiros residentes nos EUA tiveram sua vida tão devassada pelo governo quanto atualmente. No momento, 52 agências federais usam nada menos que 131 programas para invadir o dia-a-dia de cidadãos. E em breve estarão usando mais 68, em fase de planejamento. Com atraso de 20 anos, a vida está imitando a arte no país: a espionagem 24 horas por dia que o escritor inglês George Orwell imaginou e transformou em personagem — o chamado Big Brother — em seu livro “1984” foi transformada em realidade pelas mãos de Tio Sam.

A constatação acaba de ser feita pelo Escritório Geral de Controladoria (GAO), agência de investigação do Congresso dos EUA, que batizou os procedimentos de intrusão governamental de “escavação de dados”. O processo parte de nomes de indivíduos, endereços de e-mail, carteira de motorista e do número que identifica cada um no sistema de previdência social. A partir de um desses dados, agentes do governo se embrenham na busca eletrônica de informações sobre cidadãos e fazem um cruzamento entre elas, procurando sinais suspeitos. Cada vez mais o governo também utiliza “grandes quantidades de dados obtidos com fontes comerciais”, diz um relatório do GAO.

A justificativa para isso é a necessidade de deter terroristas. Mas, segundo o senador democrata Daniel Akaka, autor do pedido de investigação dos procedimentos, esses mecanismos vêm mutilando o direito à privacidade de cada cidadão: “A questão é que dados pessoais dos residentes no país são compartilhados por várias agências e não sabemos se acabam sendo utilizados para outros fins. Estou particularmente incomodado com o índice elevado de dados pessoais que o governo coleta.”

O informe do GAO diz que, com base nos dados que recolhe, o governo é capaz de produzir informações “sobre um determinado indivíduo ou pessoas desconhecidas cujo comportamento ou características se encaixam num padrão específico”. A credibilidade do sistema, no entanto, foi posta em dúvida pelos investigadores. Eles observaram que Tio Sam tem bisbilhotado tudo. O GAO constatou que o governo invade confidencialmente as contas bancárias de quem desejar; tem acesso a gastos com cartões de crédito, espionando todo tipo de produto e serviço adquirido; e sabe exatamente para quem a pessoa ligou e de quem recebeu telefonemas.

O governo tem acesso ainda à ficha médica de cada cidadão, podendo saber inclusive os medicamentos que ele consome. Sabe também para onde viaja, lê as mensagens de e-mail que ele transmite e recebe e, se quiser, participa, como ávido observador, de bate-papos na Internet. O Departamento de Segurança Interna teoricamente é o principal responsável pelo monitoramento das pessoas, mas a espionagem mais intensa é feita pelo Pentágono, diz o GAO.

As matérias da segunda categoria, reportagens do próprio jornal O GLOBO (não de agências internacionais) sobre câmeras ou sistemas de vigilância foram:

“Praia em Cabo Frio é vigiada por 20 câmeras”, de Aloysio Balbi, publicada em 13 de julho de 2002, sobre a instalação inicial de 20 câmeras, sob a responsabilidade da Guarda Municipal, ligadas ao site oficial da prefeitura e com as imagens transmitidas em tempo real pela Internet.

Cidade vigiada, publicada em 22 de setembro de 2002, é um interessante exemplo de câmeras na vigilância e combate ao crime, com o uso, no Rio de Janeiro, de um dirigível equipado com câmeras de alta resolução, capazes de registrar rostos e placas de veículos até a 15 km de distância. Voando a 3 km de altura, tem a cabine revestida de kevlar, tecido usado em coletes à prova de balas, além de drel e dacon, material usado na roupa de astronautas. Era um alvo difícil para fuzis de criminosos, que em 11 de setembro de 2002, quando monitorava a rebelião no presídio de Bangu 1, dispararam contra ele, sem atingi-lo.

Em 160 horas de gravação, em 2002, os serviços de inteligência da Polícia Civil mapearam 138 pontos de violência no Rio, 70% deles em favelas. Além da análise das imagens, a polícia baseou-se nas estatísticas de incidência de crimes, com dias e horários preferidos pelos bandidos, para relacionar os pontos críticos. Além disso, foram reativadas dez câmeras instaladas em hotéis da orla da Zona Sul, do Leme ao Leblon, do projeto Olho Vivo Contra o Crime, em setembro de 2002, transmitidas para uma sala no 23º BPM (Leblon), durante 24 horas, para prevenir, principalmente, assaltos a turistas. Elas começam a vigiar as ruas do Rio, juntamente com 92 câmeras da CET-Rio (operação de trânsito).

Antes de ser desativado, no final de 2002, pelo governo estadual, com a alegação que seu custo operacional, de R\$ 586 mil mensais, era excessivo, estavam prevendo instalar um espectrômetro no dirigível, para detectar metais a uma profundidade de até dois metros do solo, para descobrir onde estão escondidos os paióis do tráfico nas favelas. E um sensor de infravermelho, para detectar à noite, pela intensidade de calor, a presença de pessoas e até veículos com motor quente.

“Dez câmeras de vídeo já vigiam orla”, publicada em 7 de dezembro de 2002, fala da instalação de câmeras na orla de Copacabana, no Rio de Janeiro.

“Copacabana: sempre bela e, se depender dos novos ‘olhos’ da polícia, menos violenta”, de Daniela Leiras, publicada em 20 de agosto de 2003, informava a implantação de 20 câmeras em Copacabana, com um estilo literário e um discurso de convencimento com promessas de segurança para a população (a diminuição da incidência de crimes), integração social (Doze policiais portadores de deficiência física(...)), garantia de seriedade (para impedir a adulteração nas gravações, o sistema não permite a edição das imagens) e a preocupação com a privacidade (Não vamos filmar o apartamento dos moradores):

Ela está fadada ao olho da rua, mas sem correr o risco de perder seu posto de princesinha do mar e menina dos olhos do carioca. A partir desta quarta-feira, Copacabana terá um novo guardião que promete vigilância cerrada aos seus arredores. Grandioso e equipado com alta tecnologia, o 19º Batalhão da Polícia Militar será inaugurado na Rua Figueiredo Magalhães 550 e marcará o início do funcionamento de um inovador sistema de monitoramento de câmeras de vídeo, que estão espalhadas em 20 pontos estratégicos. O foco da novidade é o aumento da agilidade no policiamento e a diminuição da incidência de crimes no bairro. (...) Doze policiais portadores de deficiência física foram selecionados para acompanhar dia e noite as imagens através de computadores e de um telão instalados numa sala do batalhão. Se houver problemas como assaltos, acidentes e até a identificação de pedestres suspeitos ou de placas de carros roubados, o operador de rádio entrará em contato com uma das 24 viaturas ou com policiais à pé para ser realizada uma ação com mais eficiência. O zoom das câmeras tem a capacidade de captar desde uma imagem panorâmica da rua até detalhes do rosto das pessoas. Além disso, a central também vai monitorar a localização dos carros da polícia,

rastreados via satélite pelo sistema GPS (Global Positioning System). O trabalho será acompanhado ainda pela Secretaria de Segurança Pública no centro de monitoramento previsto para ser instalado no prédio da Central do Brasil. E para impedir a adulteração nas gravações, o sistema não permite a edição das imagens. O comandante do 19º BPM lembra que haverá o cuidado de evitar a invasão de privacidade das pessoas: - Não vamos filmar o apartamento dos moradores, apenas as ruas, as portas das lojas e a praia.

“Pais usam rastreador para monitorar localização e até a conversa dos filhos”, de Alba Valéria Mendonça, publicada em 7 de setembro de 2003, sobre equipamentos de rastreamento de veículos, via GPS, e na época as duas empresas citadas já tinham seis mil clientes no Rio de Janeiro e São Paulo.

“Polícia testa novidades hi-tech contra o crime”, de Elenilce Bottari, publicada em 4 de janeiro de 2004, informava que a Secretaria de Segurança do Rio de Janeiro estava desenvolvendo um programa para interceptar conversas via rádios como o Nextel, um dos sistemas de comunicação mais usados por traficantes do Rio, pois somente telefones fixos e celulares podiam ser rastreados. A polícia estava testando uma tecnologia canadense para escuta de radiotransmissores e um comparador de vozes dinamarquês, capaz de arquivar e identificar vozes de pessoas que tiverem conversas interceptadas.

O interessante da matéria são os elogios às parcerias com universidades públicas:

Segundo o delegado Anthony Alves, diretor do DGEE, a polícia do Rio conta hoje com avançados programas de interceptação telefônica, capazes de fazer frente às grandes agências de inteligência do mundo, como o Federal Bureau of Investigation (FBI) e a Drug Enforcement Administration (DEA), a agência antidrogas americana, como um programa desenvolvido pela Universidade de Santa Catarina e que já começa a ser adotado em unidades da Polícia Federal que antes usavam um programa canadense — diz Alves, com orgulho. Outro recurso hi-tech que o DGEE vai adotar em breve é um programa que permitirá ao policial localizar, num mapa on-line, o ponto de onde está sendo feita uma ligação telefônica. (...) Mesmo com todos os problemas que enfrenta com a falta de reagentes e material para perícia, a polícia técnica do Rio, graças a convênios com universidades, começa a avançar rumo a novas tecnologias. O luminol usado nas investigações do caso Staheli — casal de americanos assassinados na Barra — foi fundamental na obtenção de provas de que o comerciante chinês Chan Kim Chang foi

torturado no Presídio Ary Franco. Mesmo com o local lavado, o exame detectou enorme quantidade de sangue. O luminol é um reagente que há décadas é usado em investigação criminal. Mas o que está sendo utilizado pela polícia do Rio tem tecnologia nacional, desenvolvida pela UFRJ.

Na verdade, foram instaladas nove câmeras, não vinte como na matéria de 20 de agosto de 2003, objetos de várias matérias em 2004, e uma delas foi:

“Câmeras reduzem assaltos a turistas em 70%”, publicada n’O GLOBO, em 24 de maio de 2004, informava que o sistema de nove câmeras do 19º BPM (Copacabana), que vigia a orla do bairro desde agosto de 2003, reduziu em mais de 70% o número de assaltos a turistas, segundo o comando do batalhão:

Imagens feitas em março deste ano pelo sistema e exibidas ontem no programa “Fantástico”, da Rede Globo, mostram a ação de assaltantes no calçadão e nas areias da praia, que chegam a derrubar suas vítimas no chão. (...) Com o auxílio das câmeras, PMs prenderam os assaltantes nos dois episódios.

As estatísticas não são muito confiáveis para garantir o índice de redução de crimes, e houve no mesmo jornal algumas reportagens a esse respeito em 2004 e 2005, mas o tom otimista da matéria, com a referência a um programa de grande audiência nas noites de domingo, na TV do mesmo grupo do jornal, tenta reforçar a idéia de que a vigilância está produzindo bons resultados, embora com apenas dois exemplos. E a matéria continua com o subtítulo: “Linha Vermelha também é vigiada por câmeras”:

Desde o fim de abril, o sistema de vigilância passou a funcionar também na Linha Vermelha, com 16 câmeras vigiando 22 quilômetros da via. — Com o monitoramento, nenhum incidente grave tem acontecido na Linha Vermelha — diz o assessor técnico do Departamento de Estradas de Rodagem, Lineu Castilho.

Uma nota curta e um raciocínio ‘interessante’, pois a vigilância pelas câmeras não tem como impedir um incidente grave, pode apenas acelerar o socorro.

“Barra deve ganhar dez câmeras de vigilância”, de Maria Elisa Alves, n’O GLOBO, de 25 de maio de 2004, previa para meados de 2005 a operação de câmeras de vigilância em dez pontos da Barra e do Recreio, na zona oeste do Rio de Janeiro.

“Câmeras em Volta Redonda ajudam a reduzir os crimes em até 62,3%”, de Laura Antunes, publicada em O GLOBO em 5 de setembro de 2004, é sobre os três anos de uso de 26 câmeras na área central de Volta Redonda, RJ, que conseguiu reduzir em até 62,3% algumas modalidades de crimes, como homicídios. O equipamento, que na época da instalação chegou a receber protestos de moradores, se prepara para crescer: mais 61 câmeras vão chegar às ruas em seis meses. Daí a matéria detalha estatísticas de furtos de veículos, roubos e furtos a residências e homicídios, todos reduzidos após a instalação da vigilância. A matéria ainda comenta que as câmeras ajudaram ainda a melhorar o atendimento em casos de acidentes de trânsito e congestionamentos, além de inibir o estacionamento irregular e o comércio ambulante. A matéria traz o depoimento de um comerciante, dono de 13 drogarias, que diz que o sistema trouxe segurança: no ano anterior à instalação do circuito as drogarias sofreram 49 furtos e roubos, a partir do monitoramento, foram dois assaltos, e no último deles, em 2004, a dupla de bandidos, armada, acabou presa em flagrante por PMs. E prossegue:

Um outro caso de violência flagrado pelas câmeras ganhou repercussão. No dia 6 de julho do ano passado, sete jovens de classe média alta espancaram e lançaram de um viaduto um outro jovem. Ação foi filmada e os agressores autuados. Segundo o comandante do 28º BPM, coronel Jorge Sérgio de Freitas, os delitos registrados atualmente na cidade ocorrem, na maioria, **nas áreas sem câmeras**.

A matéria tem uma seqüência sobre “Vigilância em Petrópolis”, cidade da região serrana do Rio de Janeiro, que se prepara para implantar um sistema de monitoramento de 44 câmeras, se conseguir financiamento do BNDES.

“De olho na porta das escolas”, de Ruben Berta, publicada em 12 de setembro de 2004, comenta sobre a vigilância em escolas particulares na cidade do Rio de Janeiro, usando câmeras, ‘seguranças’ e rondas com veículos, provocadas por ameaças por telefone, casos de roubos e furtos sofridos por estudantes. Segundo a entidade, que reúne mais de 1.800 escolas particulares da cidade, saltou de 10% para 40% o índice de colégios filiados que aplicam recursos na segurança externa. Os maiores investimentos acontecem principalmente nos colégios da Zona Sul, que não poupam esforços. Rondas com veículos e vigias equipados com telefones para contato direto com os pais dos

estudantes estão entre as medidas tomadas para garantir a segurança dos alunos. O fecho crítico da matéria é:

(...) segundo o diretor de Comunicação Institucional da escola, Paulo Alonso, os seguranças estão à paisana: — O resultado tem sido muito bom, apesar de o colégio estar exercendo um papel que, na realidade, compete ao Estado.

O presidente da Associação de Pais do Rio de Janeiro (Apaerj), João Luiz Faria Netto, concorda que as medidas são necessárias, mas também critica as autoridades: — É importante, mas o pai acaba arcando com o custo de algo que o poder público deveria oferecer: segurança.

A assessoria de imprensa da Guarda Municipal informou que a corporação realiza rondas apenas nas escolas municipais. Procurado pelo GLOBO, o Setor de Relações Públicas da PM não retornou as ligações.

“Big Brother Esplanada”, de 21 de outubro de 2004, comenta sobre as câmeras superpotentes instaladas no alto do prédio do Congresso Nacional, em Brasília. Informa que há três anos o Senado tem um serviço de monitoramento que permite acompanhar toda a Esplanada e até bairros residenciais próximos, como o Lago Sul. E que em julho de 2004, a Câmara instalou equipamentos que identificam, com precisão, pessoas e placas de veículos em áreas próximas, acompanhando o movimento até a quase um quilômetro de distância. São no total 300 câmeras internas e 18 externas. As imagens, digitalizadas, ficam armazenadas por 60 dias. A matéria comenta que no Senado, o sistema já ajudou a evitar e a solucionar crimes, como um seqüestro-relâmpago numa agência do Banco do Brasil no Congresso.

“Projeto Vigia ajuda PM a prender 3 ladrões”, de Alessandro Soler, publicada em 30 de dezembro de 2004, informa que o sistema de vigilância integrada por 35 radiotransmissores, em Botafogo, operando há um mês, resultou na prisão de três dos sete assaltantes de um posto da Comlurb na Rua General Polidoro, em Botafogo. Usando uniformes de garis e infiltrados entre os funcionários, os bandidos haviam roubado R\$ 80 mil em vales-transporte e vales-refeição, além de telefones celulares e R\$ 50. Todos teriam fugido, não fosse o alerta dado via rádio por um porteiro. (...) Os policiais recuperaram dois telefones celulares e apreenderam cinco armas e munição de diversos calibres. A matéria não informa se os vales foram recuperados.

“Câmeras ajudam PMs a prender ladrões de turistas em Copacabana”, de Rafael Teixeira e Túlio Brandão, publicada em 14 de fevereiro de 2005, informa que o sistema de câmeras de Copacabana ajudou a prender cinco rapazes acusados de participar de assaltos a turistas estrangeiros na praia de Copacabana. Esta matéria informa que são 13 câmeras, em vez de nove. E que a polícia não conseguiu recuperar os objetos roubados, três câmeras digitais, cerca de R\$ 200, um colar e um brinco. A matéria prossegue comentando sobre o fluxo de turistas na cidade, vindos pelo mar, e que prevê-se que até 26 de abril terão passado pelo porto cerca de 135 mil turistas (45% a mais do que na temporada passada), num total de 85 atracções (10% a mais), resultando na entrada de US\$ 55 milhões na economia da cidade.

“Câmeras flagram três ladrões em Copacabana”, de Célia Costa, publicada em 5 de março de 2005, comenta duas prisões em Copacabana em função do monitoramento da orla pelo sistema de câmeras do 19º BPM, cujo coronel, Dario Cony, declarou que desde a instalação do sistema de monitoramento por câmeras, o número de assaltos na orla diminuiu cerca de 50%. E traz o depoimento da delegada Leila Goulart, que trabalhava em Volta Redonda onde, segundo ela, a instalação de câmeras provocou uma redução de 30% no número de assaltos. Nesta matéria o número de câmeras volta a ser mencionado como nove.

“Cabo Frio passará a ser vigiada 24 horas”, publicada em 24 de maio de 2005, informa sobre o projeto de instalar, até julho de 2005, 74 câmeras na cidade, com as imagens distribuídas em tempo real para as polícias Militar e Civil, Corpo de Bombeiros, Guarda Municipal, Capitania dos Portos, Guarda de Trânsito, Defesa Civil e Guarda Marítima e Ambiental do município. 40 câmeras deverão ficar visíveis. As outras ficarão escondidas em pontos estratégicos, para flagrar as ações de vândalos, pichadores e infratores de trânsito. Para operar o sistema, 610 guardas municipais estão sendo treinados para trabalhar junto a 16 técnicos em segurança.

Polícia terá central com 220 câmeras, de Marcelo Dutra, publicada em 1 de junho de 2005, informa a inauguração do Centro de Comando e Controle (CCC) da Secretaria de Segurança Pública, de onde será possível monitorar as imagens geradas por 220

câmeras que deverão estar instaladas em ruas da Região Metropolitana do Rio até o final de 2005:

O centro está funcionando de maneira experimental há seis meses, recebendo as imagens captadas por 38 câmeras instaladas nas áreas de três batalhões: 19º BPM (Copacabana), 23º BPM (Leblon) e 17º BPM (Ilha do Governador). De acordo com o projeto, as imagens captadas pelas câmeras poderão ser observadas em centros instalados em cada um dos 22 batalhões da Região Metropolitana e no CCC.

“Começa controle digital de presença em auto-escola”, de Marcel Frota, do Diário de São Paulo, publicada n’O GLOBO, em 11 de julho de 2005, trata do novo sistema de identificação de alunos e instrutores de auto-escolas da cidade de São Paulo, por leitura eletrônica da impressão digital. O sistema de leitura é ligado a um computador central na sede do Departamento Estadual de Trânsito (Detran), que tem a impressão digital dos alunos. O sistema tenta resgatar “a credibilidade do processo de formação” dos motoristas, e é mais eficiente do que a fiscalização tradicional.

“Universitário é indiciado por fraude em e-mail”, de Marcelo Dutra, publicada n’O GLOBO, em 20 de julho de 2005, informa:

A Delegacia de Repressão aos Crimes de Informática (DRCI) indiciou, por interceptação de dados de informática e por injúria, Robson Pacheco Pereira, de 27 anos, aluno do curso de doutorado em química da Universidade Federal do Rio Janeiro (UFRJ), acusado de ter invadido o computador de uma professora do mesmo curso e enviado mensagens com conteúdo sexual explícito em nome da vítima. Após a denúncia, a polícia solicitou os códigos de acesso de todos os computadores da universidade e detectou que a interferência partia de uma máquina num dos laboratórios de química da instituição, da qual apenas o acusado tinha a senha. Depois de um mandado de busca e apreensão expedido pela 1ª Vara Criminal da Ilha do Governador, os policiais fizeram a apreensão da máquina e confirmaram a origem da fraude. (...) Além de ser indiciado no artigo 140 do Código Penal, que dispõe sobre o crime de injúria, o acusado foi indiciado também no artigo 10 da lei 9296/96, que trata de interceptação de dados de informática, cuja pena varia de dois a quatro anos de prisão.

“Museus do Rio já usam tecnologia do futuro para proteger o passado”, de Paula Autran, publicada em 7 de agosto de 2005, comenta sobre a implantação de câmeras de segurança acessíveis via Internet, no Museu Histórico Nacional, e sobre os projetos ou sistemas já existentes na Biblioteca Nacional, Museu da República, Museu de Belas Artes, Museu de Arte Moderna, museus Castro Maya (Açude e Chácara do Céu).

“Mais controle no patrulhamento”, de Pedro Dantas, publicada em 25 de agosto de 2005, no suplemento TIJUCA, d’O GLOBO, informa:

Até o fim de setembro está previsto o início da operação da Central de Monitoramento das Vias Públicas do 6º Batalhão de Polícia Militar (Tijuca), para a vigilância 24 horas dos pontos de maior circulação de carros e de pedestres da região. Inicialmente dez câmeras vão monitorar trechos de ruas do bairro. (...) A instalação de câmeras em outras vias está sendo estudada.

“Búzios prepara o Big Brother da Região dos Lagos”, de Patrícia Faria, publicada em 11 de setembro de 2005, comenta o projeto da prefeitura de Búzios, de instalação de 58 câmeras de altíssima definição e com movimento de 360 graus, para controle policial, identificação das placas dos veículos, e segurança nas escolas. Além da instalação de computadores nas 14 escolas do município, com e-mails individuais para os alunos, há informações escolares disponíveis para os responsáveis, pela Internet, e controle da navegação dos estudantes na Internet.

“Jacarepaguá ganhará dez câmeras de vigilância até o fim deste mês”, de Cláudio Motta, publicada em 15 de setembro de 2005, informa que as câmeras serão instaladas até o fim do mês, para reduzir o número de roubo a pedestres, como ocorreu em Copacabana, desde a implantação do sistema, no ano passado.

“Diadema: violência cai com lei seca e câmeras”, de Flávio Freire, publicada em 12 de outubro de 2005, confirma a tese de que medidas não muito sofisticadas podem ter bom resultados na melhora das condições de segurança pública:

Diadema, no ABC paulista, ocupa agora a 18ª posição. Medidas como lei seca, fechamento de bares e controle de armas, implantadas a partir de 2001, quando foi criada

na cidade a Secretaria de Defesa Social, reduziram os homicídios. (...) Em 1999, Diadema registrava taxa de 31,2 mortes por cem mil habitantes. A partir de 2001, os homicídios caíram. A taxa de janeiro a setembro de 2005 foi de 7,9 por cem mil habitantes. Diadema tem 383 mil habitantes e é a segunda maior densidade demográfica do país — 12 mil habitantes por quilômetro quadrado. (...) Com estatísticas indicando que muitos dos assassinatos aconteciam em bares e imediações, a prefeitura decidiu implantar a lei seca. Desde 2002, a maioria dos 4.800 bares da cidade não funciona depois das 23h. Apenas 27 têm licença para ficar abertos, desde que ofereçam, por exemplo, seguranças particulares na porta. (...) Pesquisa encomendada pela prefeitura diz que o fechamento dos bares é aprovado por 93% da população. Segundo a pesquisa, 60% dos homicídios estavam ligados a brigas em bares. (...) Foram implantadas 27 câmeras em todas as regiões do município. Até 2008 o município pretende instalar cem equipamentos. O objetivo é monitorar o trânsito para ajudar em investigações ou no reconhecimento de criminosos. O contingente da Guarda Civil Metropolitana (GCM) foi aumentado. Os guardas fazem rondas diárias a pé, de bicicleta, moto ou carros.

“Tráfico usa câmeras para monitorar polícia em Itaquera”, de Giba Bergamim Jr, do Diário de São Paulo, publicada n’O GLOBO, em 14 de outubro de 2005, mostra que o uso das tecnologias de vigilância não é exclusivo do poder público:

Traficantes da zona leste da capital, montaram um esquema “Big Brother” para monitorar o trabalho da Polícia Militar e evitar que as bocas-de-fumo e locais usados como cativado fossem descobertos. (...) Os criminosos instalaram quatro minicâmeras de vídeo, com giro de 180°, em três postes de luz da Rua Chá dos Jesuítas e equiparam uma casa para funcionar como central de monitoramento do crime. O esquema foi desbaratado por policiais militares (...) após denúncia anônima. (...) Instalar câmeras para monitorar as ruas das cidades foi uma das medidas adotadas pelas prefeituras e associações de moradores da capital e do ABC paulista para acompanhar o trânsito e a criminalidade.

O suplemento Jornal de Bairro Niterói, d’O GLOBO, publicou em 6 de novembro de 2005 que todas as imagens captadas na Ponte Rio-Niterói são transmitidas para um *videowall* instalado no centro de controle na Ilha da Conceição. Até o fim do ano, a concessionária pretende instalar nos acessos à via três novas câmeras, com melhor resolução e capacidade de giro de 360 graus. Além disso, vai substituir outras duas por

equipamentos mais modernos. A Ponte S/A já está trocando as lentes do restante do sistema, além dos 15 painéis de informações sobre o tráfego na Ponte e em avenidas de Niterói.

“Capital terá mais 168 radares de rodízio”, de Regina Terraz, do Diário de São Paulo, publicada n’O GLOBO, em 12 de novembro de 2005, informa que o aumento do número de câmeras de fiscalização do trânsito já prevê um aumento significativo na arrecadação de multas por infrações:

A Prefeitura de São Paulo instalará mais 168 “dedos-duros” na capital, equipamento que faz a leitura automática das placas dos veículos, detecta e multa os que desrespeitam o rodízio. Hoje, já existem 38 “dedos-duros” funcionando na cidade: 23 acoplados a radares fixos, 11 em lombadas eletrônicas e 4 embutidos em veículos. Em 2006, serão 206 equipamentos deste tipo no município, um aumento de 442%. (...) O aperto na fiscalização trará conseqüentemente um aumento da arrecadação de multas. No Orçamento de 2006, a Prefeitura já projeta uma elevação de 57% na arrecadação com multas de trânsito.

“Alerj aprova multa para boates sem câmeras”, de Dimmi Amora, publicada em 23 de dezembro de 2005, informa que a Assembléia Legislativa do Estado do Rio de Janeiro apresentou um projeto de lei que determina:

As casas noturnas que não tiverem circuito interno de TV com sistema de gravação poderão ser multadas em até dez mil Ufirs (R\$ 10.600) e terem suas atividades suspensas. Uma nova lei estadual que determina os valores das multas foi aprovada ontem para complementar uma legislação que já está em vigor desde maio de 2004 obrigando as casas noturnas a manterem o equipamento funcionando. O projeto vai agora para a sanção ou veto da governadora.

Ele foi sancionado com a exigência de manter as gravações durante 90 dias, prazo considerado excessivo pelos empresários que se manifestaram.

“A tropa do PAN 2007”, publicada em 26 de dezembro de 2005, sobre a segurança para os Jogos Pan-Americanos de 2007, comenta que o número de câmeras de vigilância, hoje em torno de 200, será triplicado.

E também houve algumas matérias de cunho econômico:

“Fisco vigiará compras com cartão”, de Vivian Oswald, publicada em 29 de julho de 2002, comenta que a Receita Federal passará a ter acesso à movimentação financeira das administradoras de cartões e de seus clientes.

“Consumidor mais protegido contra abuso de empresas”, de Geralda Doca, Nadja Sampaio e Ana Cecília Santos, publicada em 28 de agosto de 2002, comenta uma portaria do Ministério da Justiça permitindo aos órgãos de defesa do consumidor coibirem abusos cometidos por empresas contra seus clientes, entre os quais a proibição dos contratos de transferir para o consumidor o ônus de avisar que não deseja ter suas informações pessoais repassadas a outros bancos de dados.

“O Leão ‘big brother’”, de Martha Beck, publicada em 30 de novembro de 2002, comentou o decreto que obriga os bancos a repassarem todas as informações das contas de pessoas físicas que tiverem movimentação financeira em um mês acima de R\$ 5 mil, incluindo depósitos mensais, débitos em conta, compra e venda de títulos, aquisições em moeda estrangeira, investimentos, resgates e compras com cartão de crédito. A matéria diz que o problema é que as pessoas terão quebra de sigilo sem serem suspeitas de crimes.

“CVM pune especulação pela Internet”, de Patricia Eloy, publicada em 16 de maio de 2003, é sobre uma tentativa de manipulação do valor de ações através da Internet. Foi o primeiro caso em que a manipulação de ações foi identificada na Internet. Em setembro de 2002 a CVM criou novas normas para corretoras on-line, estabelecendo que o endereço na rede de todos os participantes de salas de bate-papo fosse registrado, possibilitando a identificação de um investidor em caso de manipulação de mercado.

“Proposta de flexibilizar sigilo bancário e fiscal será enviada ao Congresso Nacional”, publicada em 8 de dezembro de 2003, comentava sobre uma proposta para flexibilizar a lei do sigilo bancário e fiscal, para que autoridades do Ministério Público, das polícias e de outras instituições que combatem a lavagem, tenham acesso direto a

movimentações financeiras e fiscais de pessoas sob investigação, pois a quebra do sigilo só é possível com autorização judicial. E também solicitava à Presidência da República que encaminhasse ao Congresso a votação, em regime de urgência, do projeto que cria o bloqueio administrativo, pelo qual o Banco Central poderia suspender instantaneamente a transferência de recursos de qualquer conta da rede bancária do país toda vez que receber do Ministério Público, ou das polícias, aviso de que as transações podem estar sob suspeita, pois hoje o bloqueio depende de autorização judicial prévia e, quando acontece, muitas vezes as contas já foram esvaziadas.

“Receita: vocação para grande irmão”, de Helena Chagas, publicada em 27 de fevereiro de 2005, informa:

A medida provisória 232, no Congresso, dá superpoderes à Receita Federal, com risco a garantias individuais e ao direito à privacidade. Ela prevê, por exemplo, a imposição de um endereço eletrônico ao contribuinte pela administração tributária, com o qual ele se relacionaria com a Receita. Isso modifica o conceito de domicílio tributário e fiscal, que passa a ser o do e-mail, que serviria, inclusive, para intimação legal. **Pelo texto, não há meio de não aceitar.** Outra polêmica é a certificação digital do contribuinte, que dará acesso aos dados pessoais, sociais, fiscais, bancários, contas correntes em todos os bancos. Num país de seqüestros-relâmpagos e das mais diversas modalidades de assalto, quem obtiver a senha do cartão não terá acesso apenas a uma conta bancária, mas a tudo o que diz respeito à vida da vítima. E transfere decisões de caráter político para a burocracia da Receita, que ganha poderes para regulamentar procedimentos processuais a serem feitos exclusivamente pela via eletrônica, como por exemplo, as intimações fiscais. Isso deveria estar em lei.

Os três primeiros artigos da MP 232, sobre legislação tributária, foram convertidos na Lei nº 11.119, de 25 de maio de 2005, que trata de valores relativos à declaração de imposto de renda. Seus artigos de 4 a 13 foram revogados pela Medida Provisória 243, de 31 de março de 2005. Mas a MP 243, em virtude da aprovação da MP 232 e sua subsequente conversão na Lei n.º 11.119, foi declarada prejudicada pela Câmara dos Deputados, em 16 de junho de 2005.²⁴ Com isso, apenas os dispositivos sobre valores

²⁴ <http://www.receita.fazenda.gov.br/Legislacao/MPs/2005/mp243.htm>, acesso em 28 dez. 2005.

de tributação e isenção de imposto de renda entraram em vigência. Os mecanismos de vigilância dependem da aprovação de novas leis.

“CPF digital, uma revolução muito além da declaração de renda”, de Nice de Paula, publicada em 28 de fevereiro de 2005, volta a falar do e-CPF:

De posse do e-CPF, o contribuinte pode acessar dados que a Receita protege sob sigilo fiscal, saber se e porque caiu na malha fina, dar as explicações necessárias e agilizar a liberação de sua restituição, emitir certidões de débito. Mas também poderá usar a assinatura eletrônica para abrir uma conta bancária ou fazer um financiamento de veículo sem precisar sair de casa. (...) Mas o brinquedinho custa caro. O kit com cartão e a leitora óptica para ser ligada ao computador custa entre R\$ 100 e R\$ 350. A mais barata é chamada de certificação A1, espécie de código eletrônico instalado no computador. O número de operações é mais restrito, a validade é de um ano e não pode ser usada fora da máquina em que foi instalada. Já a certificação A3, é considerada a mais adequada porque permite um número maior de operações. Inclui um cartão com chip e uma leitora para os dados, o que torna seu preço mais alto. (...) A Caixa Econômica Federal, que investiu R\$ 27 milhões em tecnologia de certificação, já emitiu 15 mil e-CPFs ou identidade digital para pessoas físicas, e cobra R\$ 150 pelo kit A3. O banco oferece o serviço nas agências de Pernambuco, em quatro de São Paulo e em quatro do Rio Grande do Sul. E também prepara a transformação do sistema eletrônico já adotado por 1,6 milhão de empresas para envio dos dados relativos ao pagamento do INSS e FGTS em uma certificação digital tipo ICP Brasil, que pode ser usado para todas as operações.

A certificação digital também já é oferecida pela Serasa, empresa de análise de crédito. Custa R\$ 100 o tipo A1, fornecido em disquete, com validade de um ano, e R\$ 350 o e-CPF A3, com validade de dois anos, incluindo certificado, cartão inteligente e a leitora. Outra certificadora é a Certi Sign, que também cobra R\$ 350 pelo kit do A3 e R\$ 100 pelo A1. Há ainda o Serpro, ligado ao Ministério da Fazenda, ao preço de R\$ 95 por um e-CPF A3, com validade de um ano.

A matéria encerra comentando o interesse do Banco do Brasil e de grandes bancos privados em implantar o sistema ainda em 2005. Mas no final de 2005 sua penetração ainda era bem reduzida.

“Microsoft abre guerra contra roubo de dados”, publicada em 4 de abril de 2005, informa que a Microsoft deu início a uma batalha judicial contra o *phishing* (uso de e-mails falsos para “pescar” informações como dados bancários, senhas ou número de cartão de crédito de outros internautas). A empresa abriu 117 processos no tribunal de Seattle, Washington, para descobrir a identidade de internautas que praticam o *phishing*. (...) Ela tenta se proteger de uma onda de e-mails dirigidos especificamente contra usuários de serviços da Microsoft, como o sistema de mensagens eletrônicas gratuito Hotmail e o MSN Messenger.

“Novo título de eleitor terá retrato e impressão digital”, publicada em 28 de abril de 2005, informa que o novo título de eleitor que o TSE está confeccionando não terá mais o chip que armazenaria todas as informações do eleitor. O uso do dispositivo foi descartado em função do seu alto custo. O novo título de eleitor terá retrato, impressão digital eletrônica, registro geral, CPF, e tipo sanguíneo. Para que o documento comece a ser emitido, é necessário ainda um recadastramento de eleitores. O TSE calcula que até 2008, os 121 milhões de eleitores vão estar com o novo título. Não será preciso pagar pelo novo documento. Para as próximas eleições, em 2006, o título atual continua valendo.

“Vem aí operação bancária pelo celular”, de Cleide Carvalho, publicada em 4 de maio de 2005, informa que:

Os clientes do Banco do Brasil poderão pagar contas, ver saldo e fazer pelo celular qualquer tipo de operação bancária disponível hoje no site do banco. E que estuda adotar a Web também nos caixas eletrônicos externos, compartilhando os terminais de autoatendimento do banco com clientes da Caixa Econômica Federal (CEF) e, futuramente, do Bradesco. (...) Não há motivos para temer pela segurança, pois a plataforma Internet já permite mobilidade e uso em caixas eletrônicos externos sem qualquer problema em seus protocolos de privacidade.

Até o final de 2005 nem esta integração nem o acesso via celular haviam sido implementados. A matéria termina comentando um estudo da McAfee, segundo o qual as ferramentas preferenciais dos fomentadores de pragas virtuais hoje são os vírus de

celular, os phishings (mensagens falsas como a do Serasa, que levam incautos a enviar seus dados para sites de hackers) e a exploração de vulnerabilidades nos programas.

“Anatel: clonagem de celular já aumentou 57%”, de Mônica Tavares, publicada em 21 de setembro de 2005, informa que:

Nos oito primeiros meses de 2005, cresceram as queixas em 57,22% em relação a todo o ano passado. Foram 7.380 queixas entre janeiro e agosto, contra 4.694 em 2004. Em 2003, foram 603 reclamações. Em dois anos e meio, chega a 12.677 o número de queixas feitas apenas à agência. Ou seja, sem considerar casos encaminhados aos Procons e às próprias empresas. No Rio de Janeiro, desde 2003 já são 1.178 casos.

O regulamento do Serviço Móvel Pessoal (SMP) da Anatel, de 2002, prevê que as empresas tenham meios para identificar a existência de fraudes. Em 99% dos casos, a Vivo diz detectar o problema antes de o cliente perceber. Nos demais, a clonagem é resolvida sem prejuízo financeiro ao cliente.

A Claro também informou que trabalha para combater clonagens e fraudes. Esclareceu ainda que os dois problemas têm ações distintas. No caso de fraude de subscrição, pessoas mal-intencionadas usam dados falsos de clientes para habilitar novas linhas. Todas as contas que não procedem são canceladas, sem ônus para os consumidores.

Segundo a assessoria da Telemig Celular, o volume de reclamações sobre clonagem no seu Centro de Relacionamento com Clientes caiu 68% em agosto de 2005, se comparado a janeiro. A empresa assume o custo das ligações.

As empresas que utilizam tecnologia GSM, na qual os celulares usam chips, que dificultam a clonagem, têm explicações diferentes. A Claro argumenta que o problema pode acontecer quando o cliente de outras tecnologias usa aparelho em rede analógica ou recorre a uma assistência técnica não recomendada.

Já a TIM garante que não há registro em todo o mundo de clonagem de um telefone TIM GSM. Nas regiões onde oferece serviço com outras tecnologias, a empresa faz um acompanhamento para evitar a clonagem. A Oi e a Brasil Telecom acreditam que pode ter havido equívoco de interpretação da reclamação.

O uso da vigilância na segurança pública pode ser uma ferramenta eficiente, desde que sejam implantados mecanismos de controle e fiscalização dessa vigilância, e um treinamento adequado e periódico dos agentes.

Mas se está em questão um orçamento limitado, a experiência demonstra que há mais resultados investindo no treinamento e acompanhamento dos agentes, em análises de informações (inteligência), na integração dos serviços policiais, e em medidas simples que resultaram em redução de mortes, como a restrição da venda de bebidas alcoólicas de madrugada, do que simplesmente em novas tecnologias de vigilância.

As empresas sempre exerceram algum tipo de vigilância sobre as outras. No século 18 a revista sueca *Den Goteborg Spionen* informava os avanços tecnológicos produzidos em outros países, como a fabricação de porcelana. Poucos países produziam inovações e o progresso técnico era lento (Castells e Bosch, 2001). Hoje, apesar da imensa quantidade de informações na Internet, que Cornella, A, em *Los recursos de información*, Madri: McGraw-Hill/ESADE, 1994, chama de “infoxicação”, das publicações técnicas e das patentes, boa parte das informações relevantes são de circulação restrita, em teses, atas de congressos, documentos de trabalho. Atualmente a vigilância recebeu um grande impulso devido à proliferação das bases de dados, ao crescimento da Internet e principalmente aos novos programas capazes de administrar imensas quantidades de informações.

Os governos também sempre investiram na vigilância nacional e estrangeira.

O jornalista Elio Gaspari, publicou em sua coluna n’O GLOBO, em 17 de abril de 2005, a matéria “Vem aí o Estado policial-informático”, que dispensa mais comentários:

O banco de dados americano LexisNexis avisou na terça-feira que o sistema de segurança de seus computadores foi furado por “ladrões de identidades”. Trata-se de delinquentes que capturam informações pessoais para fraudar contas bancárias, cartões de crédito e transações financeiras. Levaram dados de 310 mil pessoas. Em fevereiro, uma invasão nos computadores da empresa ChoicePoint sugou 145 mil identidades. Esse tipo de crime custa US\$ 50 bilhões à economia americana e no ano passado vitimou dez

milhões de cidadãos. (...) Segundo a organização Electronic Privacy Information Center, a ChoicePoint comprou (há anos) o cadastro brasileiro de proprietários de veículos. Documentadamente, essa empresa tem um contrato no valor de US\$ 1 milhão anuais para fornecer dados de cidadãos latino-americanos ao Serviço de Imigração dos Estados Unidos. Desde setembro de 2001, o governo americano terceirizou seu fichário e as empresas LexisNexis e ChoicePoint tornaram-se os maiores arquivos de dados pessoais da história. Armazenam as contas de três bilhões de cartões de crédito, 139 milhões de números de telefones, 200 milhões de pleitos junto a seguradoras e mais 100 milhões de fichas criminais. (...) Esses bancos de dados surgiram para aconselhar o comércio e proteger o crédito. Fazem cruzamentos que a mente humana é incapaz de processar. Depois dos atentados de 11 de setembro, o criador de um sistema chamado Matrix espremeu o fichário e chegou a uma lista de 1.200 suspeitos. Entre eles estavam cinco dos seqüestradores dos aviões usados nos atentados. Em 2002, quando um atirador misterioso matou 16 pessoas e assombrou os Estados Unidos, o Matrix cruzou uma lista de 21 mil cidadãos com o nome de John Williams e identificou o assassino. Um livro do repórter Robert Harrow Jr, “No place to hide” (“Sem esconderijo”, inédito em português) mostra que em 2001 a ChoicePoint também capturou, armazenou e pôs à venda os nomes e os endereços de todos os eleitores mexicanos, os passaportes de todos os cidadãos da Costa Rica, o RG e o número do telefone de todos os argentinos e o registro civil de todos os colombianos. A empresa oferece dados pessoais de 300 milhões de pessoas em dez países. Ela assegura que não armazena dados obtidos ilegalmente.

Nos EUA, o FBI usa computadores e sistemas de vigilância eletrônica que operam em um sistema integrado batizado de Carnivore (agora chamado de DSC1000). Ele monitora e-mails, mensagens instantâneas e chamadas de telefones digitais. Isso gerou muitas controvérsias antes de 11 de setembro de 2001, por ser considerado poderoso demais. Instalado em um provedor de serviços de Internet, permite pesquisar atividades de suspeitos e todos os demais usuários. Após reclamações de defensores da privacidade, o FBI restringiu seu uso. Agora, não há mais freios. Comenta-se que o governo ligou o Carnivore a provedores com supervisão mínima. É provável que logo exija que os provedores de Internet e de serviços de telefonia digital sem fio projetem

redes mais fáceis de explorar. No início de 2001, o FBI não ousaria pedir isso. Agora, um pedido desses talvez nem seja noticiado nos jornais.²⁵

Mesmo numa época e local em que os direitos individuais eram mais respeitados, nos EUA em 1943, o governo não hesitou em utilizar cópias dos cartões do censo de 1940, com informações relativas aos cidadãos norte-americanos de ascendência japonesa, deslocando mais de 100 mil pessoas para campos de concentração no deserto, privando-os de seus direitos constitucionais, propriedades (os que conseguiram, venderam imóveis ou negócios por preços irrisórios) e de seu futuro, pela possibilidade de que representassem um risco à segurança nacional, na guerra contra, entre outros, o Japão.

Resumindo, no período de cinco anos, de janeiro de 2001 a dezembro de 2005, esta tese compilou todas as edições do jornal carioca O GLOBO, nos cadernos de notícias e suplementos, encontrando um total de 145 matérias sobre vigilância e/ou privacidade.

Algumas matérias do GLOBO não foram citadas aqui, por serem uma repetição de assuntos, sem nada acrescentar, e foram citadas algumas matérias de outras fontes, todas identificadas. A grande maioria das matérias é citada neste ou no próximo capítulo e fornecem, além de uma visão do discurso do jornal, às vezes bem político, outras técnico e objetivo, um conjunto que abrange vários pontos discutidos ao longo da tese, com explicações que muitas vezes dispensam mais comentários, e que complementam a apresentação das técnicas de vigilância, suas características, vantagens e riscos.

As matérias baseadas em reportagens de agências estrangeiras foram 37 e na maioria trataram das mudanças na legislação norte-americana, em consequência da aprovação da Lei Patriótica, nas ações de vigilância e controle, dentro e fora dos EUA, de cidadãos americanos ou estrangeiros, e dos sistemas de vigilância na Inglaterra.

Das 53 matérias sobre vigilância e privacidade apresentadas pela equipe do próprio jornal, a metade (25) trata de câmeras de vigilância nos estados do Rio de Janeiro e São Paulo, e uma em Brasília, com um discurso político que iguala vigilância

²⁵ *Privacidade em tempos de terror*, BusinessWeek, em Valor Econômico, nº 378, 31 out. 2001.

a segurança, mas algumas vezes com críticas nas matérias. Outras 13 matérias tratam do aspecto econômico (foram todas publicadas na seção de Economia do jornal) de tecnologias de vigilância e da privacidade na Internet.

Um grupo significativo de matérias (42) foi publicada no suplemento “Informática etc.”, parte integrante da edição de segunda-feira do jornal há mais de dez anos, e são principalmente sobre certificação e segurança digital, invasões de computadores, biometria e digitalização de documentos de identificação, e apresentam análises detalhadas sobre diversos aspectos técnicos e sua influência na vida dos usuários de computadores ligados à Internet, normalmente detalhando o problema, sugerindo soluções e cuidados, e redigidas por um pequeno número de jornalistas e colaboradores.

Este último grupo destoa do discurso vigilância = segurança, dos demais cadernos do jornal, e tem um conteúdo mais técnico, sem que o texto se torne hermético. E freqüentemente apresentam as fontes das informações. Ele procura enfatizar de forma objetiva que há vantagens e riscos na Internet, e que ainda há muito a ser discutido e regulamentado, e que os usuários devem participar dessa discussão, procurando informar-se e mantendo-se atualizados para correr o mínimo possível de risco no uso inevitável das novas tecnologias de comunicação mediada por computador.

No cômputo geral, vários aspectos de vigilância e privacidade foram abordados pelo jornal, com destaques para o uso e abuso de câmeras de vigilância, a questão da certificação digital, as medidas e conseqüências da Lei Patriótica nos EUA e, em menor grau, as tecnologias de identificação biométrica. Pontos como RFID, GPS e bancos de dados tiveram uma presença muito reduzida nesses cinco anos da publicação.

A privacidade em obras de ficção-científica

Dos autores mais ‘pessimistas’ em relação aos efeitos nocivos da tecnologia sobre a sociedade destacamos J. G. Ballard e Larry Niven. Ballard escreveu diversos contos onde explora efeitos negativos de determinada tecnologia, por exemplo, como a propaganda subliminar pode criar uma sociedade tão consumista que troca de carro a cada seis meses, que se estabelece uma relação como a de trabalhadores ‘escravizados’ em uma fazenda, que sempre devem mais à ‘loja’ local que seus salários a receber²⁶, ou como a evolução da tecnologia de transplantes cria leis tão rígidas que três infrações de trânsito no mesmo ano acarretam pena de morte para retirada dos órgãos do infrator.

Niven vem publicando regularmente desde 1964²⁷, criando uma visão particular de um universo em parte colonizado por humanos, em parte por alienígenas pilotando naves humanas, e tem histórias em que mescla detetives e ficção científica. Alguns dos romances seguem uma vertente mais clássica em FC, com o impacto de novas tecnologias no comportamento, a expansão humana, os problemas políticos e administrativos, guerras contra alienígenas etc.

Poucos autores limitaram-se a uma FC apenas com humanos (e robôs humanóides) e o destaque vai para Isaac Asimov, autor de cerca de 300 livros de FC, com o destaque para a série Fundação, sobre história, análises da Bíblia, divulgação científica, histórias de detetives (a série The Union Mysteries Club) e uns poucos sobre sua formação acadêmica (ele era doutor em bioquímica e escreveu contos e romances de FC durante toda a sua vida). Além de vários livros de contos de mistério e detetives (a série Union Mysteries Club) ele escreveu três romances onde o personagem principal é um detetive de Nova York, *Elijah Baley: The Caves of Steel* (1954, Caça aos Robôs), *The Naked Sun* (1957, Os robôs) e *The Robots of Dawn* (1983, Os robôs do amanhecer)

Eles se passam no século 30, quando dois avanços alteraram o rumo da história humana: naves que permitiram a colonização da galáxia e a criação de robôs com cérebros positrônicos. A superpopulação da Terra vive apinhada em bilhões de

²⁶ Ballard, J. G., *The Subliminal Man*, in *The Disaster Area*, Londres: Panther, 1969, p. 55-76.

²⁷ Os primeiros foram os romances: *World of Ptavvs*, *Protector*, *A Gift from Earth*, *Ringworld*, publicados pela Ballantine e diversas coletâneas de contos: *Neutron Star*, *The Shape of Space*, *All the Myriad Ways*, *The Flight of the Horse*, *A Hole in Space*, *Tales of Known Space*, *The Long ARM of Gil Hamilton*. Os mais recentes são *Ringworld's Children* (2004), *The Burning Tower* (escrito com

pequenos apartamentos (as cavernas de aço) que cobrem praticamente toda a superfície do planeta, sem nenhuma privacidade, enquanto que uma elite racial arrogante, eugenicamente selecionada, os Espaciais, emigrou para colonizar mundos espaciais onde poucas famílias vivem isoladas umas das outras, em meio a centenas de robôs que fazem todo o trabalho. Quando um proeminente membro dos Espaciais é morto sob circunstâncias misteriosas, Baley é enviado aos Mundos Exteriores para investigar. E ele tem um parceiro, o robô humanóide R. Daneel Olivaw, criado à imagem da vítima assassinada. É amplo o contraste entre a total falta de privacidade (na Terra, Baley está acostumado a usar banheiros coletivos, ou seja, junto com várias pessoas ao mesmo tempo, a usar transportes públicos apinhados, locais de refeição, trabalho e diversão com milhares de pessoas) e a total privacidade (o Espacial morto vivia em total isolamento físico, até mesmo da esposa). Os romances se desenvolvem em meio a uma intrincada composição psicológica dos personagens, uma história de amor platônico, e naturalmente, contra todas as expectativas, Baley descobre o que aconteceu. Asimov declarou que nunca conseguiu imaginar alienígenas convincentes, e então escrevia romances apenas sobre humanos. Em poucos contos (como “A anfitriã”, “O tubo da morte”, publicados em 1951, ou “Espaço vital”, ele se arrisca a criar um alienígena).

Embora o século 20 tenha sido pródigo em autores de ficção científica, e isso se reflita não só na produção bibliográfica mas também na ampla produção cinematográfica e para a TV, nenhuma seqüência tem presença tão longa quanto Jornada nas Estrelas (Star Trek), uma série de baixo orçamento, mas com bons roteiros, criada nos anos 1960 por Gene Roddenberry, que ganhou uma legião de fãs que foi aumentando nas reprises na TV durante 20 anos e gerou uma série de continuações, com mais de 700 episódios, já com mais orçamento e muitos efeitos especiais, todas (exceto os desenhos animados) ainda em exibição na TV, geralmente paga²⁸, de dezenas de países, cronologicamente encadeadas (todas exceto a mais recente) e, até agora 10 filmes de longa metragem, além de livros, roteiros, guias comentados de episódios, brinquedos, videogames, enciclopédias, milhares de sites na Internet, convenções regulares de fãs e cursos de um idioma alienígena, o klingon. Anualmente milhares de fãs reúnem-se em convenções e há centenas deles fluentes em klingon.

Jerry Pournelle em 2003), e Scatterbrain (2003). Ele venceu cinco prêmios Hugo e um Nebula.

A “exemplo” de J. R. R. Tolkien, que escreveu o *Hobbit* depois da trilogia *O Senhor dos Anéis*, Roddenberry criou e, mesmo após sua morte, continuou em produção até 2005, a saga inicial da aventura humana fora do sistema solar, cuja série mais recente, “Enterprise”, se passa em 2151 a 2153, um século antes da série original, no século 23, e dois séculos antes das três seguintes (The Next Generation, Deep Space 9 e Voyager), no século 24.

Tanto nos mais difundidos livros de FC, dos escritores mais famosos, quanto nas principais (mais duradouras e difundidas) séries de FC para a televisão e cinema, não se vê o uso da tecnologia sofisticada que já existe hoje, para não falar da imaginada na ficção, ser usada para promover sistemas eficientes de segurança baseados em reconhecimento de pessoas, pois isso complicaria muitos dos roteiros que lidam com conflitos “armados”, batalhas entre raças ou facções, e uso indevido de tecnologias.

Em *Minority Report*, filme dirigido por Spielberg, de 2002, a vigilância é feita por reconhecimento da íris, por sensores espalhados em toda a cidade e também em pequenos robôs aracnídeos dotados de impressionante inteligência artificial, tudo isso aliado a abrangentes bancos de dados. O que não impede que se abra portas com um olho humano removido cirurgicamente, guardado em um saco plástico, sem refrigeração adequada. Já os exemplos de vigilância apresentados em duas obras da primeira metade do século 20, 1984, de George Orwell, ou *We*²⁹, do russo Eugene Zamiatin são semelhantes entre si, e muito mais presentes. Nos dois romances o poder é exercido pelo Estado, um partido único sem espaço para oposição. O Grande Irmão preside a Oceania de Orwell enquanto que o Benfeitor rege o Estado Unido de Zamiatin. O poder é mantido por meio de uma vigilância minuciosa e abrangente, todas as ações dos indivíduos são monitoradas e os meios de comunicação os bombardeiam com uma doutrinação incessante. Todos são permanentemente treinados e disciplinados. Em *We* isso é destacado pelo fato da cidade futurista onde todos vivem ser feita de vidro. A transparência é total, exceto as atividades dos governantes.

²⁸ No Brasil, no canal pago Universal.

²⁹ Censurado na então URSS, *We* foi publicado na Inglaterra em 1924, republicado em 1952, possivelmente em vista do sucesso de 1984, publicado em 1949. Citado em Whitaker, p. 27.

3. As tecnologias de vigilância

Neste capítulo apresenta-se alguns exemplos de mecanismos de informação, para segurança e/ou vigilância, com seu desenvolvimento histórico, aplicações e implicações, que nos permitem uma compreensão clara da sua dimensão, abrangência e possibilidades. Em alguns casos, são citadas reportagens que ilustram determinados aspectos.

É interessante conhecer os mecanismos e sua evolução para ter uma visão detalhada da questão de vigilância e sua influência na vida dos indivíduos.

A comunicação telegráfica

A necessidade de comunicação à distância surgiu quando se passou a administrar grandes áreas, a efetuar guerras distantes das cidades de origem, e comerciar com outras cidades e países. O problema é que os sistemas mais rápidos, como tochas em uma seqüência de torres, só podiam enviar a longa distância mensagens bem simples, como Socorro! e era bem difícil esconder seu significado. Mensagens complexas, que podiam ser codificadas, tinham de ser enviadas por mensageiros, e demoravam o tempo necessário para os mensageiros deslocarem-se, geralmente a cavalo, até o destinatário, ou até outro mensageiro com um cavalo descansado, como no Pony Express, no oeste norte-americano no século 18.

Em 1793 os franceses começaram a construir torres com um sistema de sinalização composto de um travessão de madeira acoplado a dois braços menores, nas suas extremidades, que podiam ser movidos a 0, 45, 90, 135 ou 180 graus, formando dezenas de combinações, cada qual representando uma letra, e permitiam transmitir mensagens de torre a torre, desde que houvesse alcance visual, usando telescópios. Em 1794, a primeira linha de 15 torres, ligava Paris a Lille, a 200 km. Em 1804 Napoleão estava estendendo linhas de Paris a Milão, Lyons e Turim.

Em 1797 a Inglaterra começou a construir torres usando seis painéis de madeira, em duas colunas de 3 linhas, onde cada painel podia ficar na vertical ou na horizontal, em um sistema binário, visível ou não, dando um total de 64 combinações. O sistema

Braille, de escrita para cegos, implantado a partir de 1837, usa o mesmo esquema. A vantagem dos painéis é que, iluminados por trás, também eram visíveis à noite.

Com o uso da eletricidade, novos horizontes se abriram, e vários sistemas de telegrafia foram implantados, alguns muito complexos, com diversos fios entre as estações, até se chegar aos sistemas que usam apenas dois fios, o que barateia os custos o suficiente para permitir sua implantação em grande escala. Os pioneiros tiveram grande dificuldade em convencer os governos e o público em geral que aquela “mágica” funcionava e trazia vários benefícios, como a rápida divulgação de notícias, de pedidos de prisão de criminosos enviados a outras cidades, mas principalmente, com a expansão dos negócios, um controle rápido do comércio entre várias cidades.

Em 24 de maio de 1844, depois de dois anos para convencer o congresso americano a financiá-lo, e de infrutíferas tentativas na Europa, Samuel Morse concluiu a instalação de uma linha telegráfica entre Baltimore e Washington. Na Inglaterra, William Cooke já havia conseguido instalar algumas linhas de poucos quilômetros, entre algumas estações ferroviárias, de seu sistema de múltiplos fios. A fama do telégrafo começou a espalhar-se quando o *Times* foi distribuído nas ruas de Londres, em 6 de agosto de 1844, anunciando o nascimento do segundo filho da rainha Vitória, 40 minutos após o anúncio oficial, graças ao “extraordinário poder do telégrafo eletromagnético” e, logo em seguida, três trens partiram de Londres para Windsor, com os convidados para o banquete de celebração. O duque de Wellington havia esquecido sua casaca, telegrafou para Londres e a mesma foi enviada no trem seguinte. Outro marco desse início foi a prisão de Fiddler Dick, um notório batedor de carteiras, e de sua gangue. Eles atacavam nas multidões nas estações ferroviárias e fugiam de trem para outra estação, de onde fugiam. Com uma linha telegráfica ao longo da linha Paddington-Slough, foi possível alertar aos policiais na próxima estação, antes da chegada do trem (Standage).

Na década seguinte, as linhas telegráficas espalharam-se pela Europa e pelos Estados Unidos. Em 5 de agosto de 1858, o primeiro cabo transatlântico ligou a Europa (Valentia Bay, Irlanda) à América (Terra Nova, Canadá). Dessa vez a aclamação pública foi imensa. A joalheria Tiffany's, de Nova York, comprou sobras do cabo, cortou em pedaços de 10 cm e vendeu como souvenir. Outras sobras foram usadas em guarda-

chuvas, bengalas e porta relógios. Como a tecnologia empregada ainda era muito rudimentar, o cabo apresentou falhas constantes e parou de funcionar em 1º de setembro, menos de um mês depois da inauguração. Em 1865 houve uma tentativa frustrada de instalar um novo e mais sofisticado cabo. Em 13 de julho de 1866, o Great Eastern partiu da Europa para a terceira tentativa. Duas semanas depois, chegou, sem problemas, à Terra Nova. A demanda pelo cabo era tão grande que no primeiro dia de operação a receita com os telegramas intercontinentais foi de mil libras esterlinas. Em agosto, recuperaram o segundo cabo, partido a uma profundidade de três quilômetros, e após consertá-lo, completaram a ligação até o Canadá, passando a contar com dois cabos operando.

A grande velocidade criou uma grande demanda por mensagens e os sistemas telegráficos começaram a ficar tão congestionados que passou a haver atraso nas mensagens, pois muitas mensagens eram transmitidas entre duas estações, impressas, e de lá retransmitidas a outro ponto, até o destino final.. (Um problema semelhante é previsto para a Internet, e uma solução proposta é a adoção do novo protocolo de comunicação e de medidas de autenticação). Na época, a solução européia foi a instalação de uma rede de tubos pneumáticos subterrâneos interligando estações telegráficas. Nos EUA a maioria das linhas corria ao longo das ferrovias, e não havia tanto congestionamento. O sistema pneumático em Paris operava tão bem que enviar uma mensagem, sem limite de palavras, em 1879 custava mais barato que um telegrama e era mais rápido que o correio.

Mas além de transmitir mensagens familiares, o sistema telegráfico também era usado para enviar cotações de ações, resultados de corridas de cavalos, e isso deu margem a fraudes e esquemas criminosos. Dois banqueiros franceses, em 1834, subornaram operadores do telégrafo para introduzir erros deliberados, mas reconhecíveis, nas transmissões do mercado acionário de Paris, que lhes permitia saber se a bolsa estava em alta ou em baixa, e só foram descobertos em 1836. Estações próximas a pistas de corridas foram usadas para enviar telegramas com os resultados, usando palavras previamente combinadas, a apostadores em outros locais, que podiam apostar antes das agências locais receberem os resultados. Uma idéia semelhante, interceptando e retransmitindo com um minuto de atraso, os resultados das corridas de

cavalos, foi o argumento do filme *The Sting* (Golpe de Mestre), de 1973, cuja história se passa em 1936.

Na Europa, na década de 1840, as empresas telegráficas não enviavam mensagens em código, a não ser de órgãos do governo, ou informações como cotações da bolsa. Mas havia uma grande demanda por mensagens codificadas, pois as pessoas não confiavam no sigilo dos diversos operadores envolvidos desde a recepção até a entrega final do telegrama. Os anúncios classificados dos jornais sempre foram um meio comum de enviar mensagens codificadas. As legislações variavam, conforme o país europeu e, por iniciativa francesa, em 1865 fundaram a International Telegraph Union, e as pessoas foram autorizadas a enviar telegramas codificados, o que elas começaram a fazer imediatamente.

Nos EUA, onde a rede telegráfica era privada, não havia impedimentos ao uso de códigos, que foram adotados desde 1845, e foram publicados muitos livros de códigos, que eram dicionários de palavras associadas a códigos alfanuméricos. O vocabulário de Francis Smith tinha 50 mil palavras. Não era muito secreto mas custava mais barato, pois os códigos usavam menos caracteres, mas como os operadores estavam acostumados a transmitir/receber palavras conhecidas, e já usavam muitas abreviações, para agilizar o trabalho, os erros eram freqüentes. Então os dicionários passaram a usar palavras, em inglês ou latim, que significavam outras palavras ou frases completas.

A ITU, sensível às reclamações das operadoras de que telegramas com poucas palavras não eram rentáveis, determinou que as mensagens sem códigos deveriam conter palavras pronunciáveis e com no máximo sete sílabas e nas mensagens codificadas, cada cinco caracteres seriam cobrados como uma palavra. Em 1875 o limite de caracteres por palavra caiu para 15, em 1885, para dez, e as palavras deveriam ser em alemão, inglês, espanhol, francês, italiano, holandês, português ou latim.

Muitas empresas criaram seus próprios dicionários de códigos, muitos com centenas de páginas e incrível nível de detalhamento. Muitas das palavras usadas eram extremamente parecidas, dando margem a erros nos telegramas e a possíveis imensos prejuízos por uma mensagem incorreta. Com o tempo, os códigos foram corrigindo os problemas e adaptando-se às normas das operadoras. Cerca de 95% dos telegramas

comerciais eram codificados. Nos EUA, em 1872, a Western Union criou um sistema de livros de códigos para suas agências, para controle das transferências de dinheiro, usando diferentes palavras para diferentes quantias, e senhas para conferência, em telegramas entre as agências.

Os governos interceptavam telegramas e diplomatas e espões usavam códigos cada vez mais elaborados, para tentar manter a privacidade de suas mensagens. Essa batalha prossegue até hoje, com os diversos meios de comunicação, e a censura volta e meia se manifesta, como neste exemplo:

O GLOBO republicou, em 19 de agosto de 2003, na seção “HÁ 50 ANOS” (19 de agosto de 1953), a matéria “Ministro aborda censura a telegramas”:

O Departamento de Correios e Telégrafos se recusou a transmitir diversos telegramas endereçados ao jornalista Carlos Lacerda. Em face dos protestos contra a censura havida, o diretor daquela repartição manifestou-se afirmando que tais telegramas haviam sido recusados em cumprimento ao artigo 19 do Regulamento dos Serviços Postais, o que diz “que o Departamento não transmite ou entrega telegrama que contenha dizeres ou representações indecentes, injuriosos, ameaçadores, ofensivos à moral ou, ainda, contrários à ordem pública e aos interesses do país”.

Um dos telegramas censurados era do seguinte teor, segundo revelou, ontem, o vespertino “Tribuna da Imprensa”: “Temos a imensa satisfação de hipotecar inteira solidariedade ao jornalista e grande brasileiro pela notável campanha em favor da moralização dos costumes. — Lídio Fonseca”.

Ouvindo hoje pelo GLOBO, assim falou o ministro José Américo sobre o assunto:

— O regulamento existe e não pode ser revogado. No caso em questão, vou dar instruções ao Departamento de Correios e Telégrafos, no sentido de que haja maior tolerância na interpretação do que possa ser injurioso ou atentar contra a ordem pública ou aos interesses do país.

O serviço de Correios e Telégrafos no Brasil é regido pela Lei nº 6.538, de 22 de junho de 1978, e os itens referentes a sigilo, censura, criptografia e privacidade são:

Art. 5º - O sigilo da correspondência é inviolável. Parágrafo único - A ninguém é permitido intervir no serviço postal ou no serviço de telegrama, salvo nos casos e na forma previstos em lei.

Art. 6º - As pessoas encarregadas do serviço postal ou do serviço de telegrama são obrigadas a manter segredo profissional sobre a existência de correspondência e do conteúdo de mensagem de que tenham conhecimento em razão de suas funções.

Art. 28º - Não constitui violação do sigilo de correspondência o conhecimento do texto de telegrama endereçado a homônimo, no mesmo endereço.

Art. 29º - Não é aceito nem entregue telegrama que:

I - seja anônimo;

II - contenha dizeres injuriosos, ameaçadores, ofensivos à moral, ou ainda, contrários à ordem pública e aos interesses do País;

III - possa contribuir para a perpetração de crime ou contravenção ou embaraçar a ação da justiça ou da administração;

IV - contenha notícia alarmante, reconhecidamente falsa;

§ 1º - Não se considera anônimo o telegrama transmitido sem assinatura, por permissão regulamentar.

Art. 30º - O telegrama, além de outras categorias que venham a ser estabelecidas em regulamento, se classifica:

II - Quanto a linguagem:

a) corrente - texto compreensível pelo sentido que apresenta;

b) cifrada - texto redigido em linguagem codificada, com chave previamente registrada.

IV - Quanto à entrega:

§ 1º - Na redação de telegrama em linguagem corrente podem ser utilizados, além do português, os idiomas especificados quando deva ser procurado e entregue em unidade de atendimento da empresa exploradora do serviço;

§ 2º - Para expedição de telegrama em linguagem cifrada, salvo nos casos previstos em regulamento, e obrigatória a indicação do código, previamente registrado, utilizado na sua redação, podendo seu tráfego ser suspenso pelo Ministro das Comunicações, quando o interesse público o exigir.

VIOLAÇÃO DE CORRESPONDÊNCIA

Art. 40º - Devassar indevidamente o conteúdo de correspondência fechada dirigida a outrem: Pena: detenção, até seis meses, ou pagamento não excedente a vinte dias-multa.

QUEBRA DO SEGREDO PROFISSIONAL

Art. 41º - Violar segredo profissional, indispensável à manutenção do sigilo da correspondência mediante:

I - divulgação de nomes de pessoas que mantenham, entre si, correspondência;

II - divulgação, no todo ou em parte, de assunto ou texto de correspondência de que, em razão ao ofício, se tenha conhecimento;

III - revelação do nome de assinante de caixa postal ou o número desta, quando houver pedido em contrario do usuário;

IV - revelação do modo pelo qual ou do local especial em que qualquer pessoa recebe correspondência; Pena: detenção de três meses a um ano, ou pagamento não excedente a cinquenta dias-multa.

Quando Alexander Graham Bell conseguiu sua patente do telefone, em 3 de março de 1876, e uma semana depois conseguiu que seu protótipo funcionasse com qualidade aceitável, ele era chamado de telégrafo falante, um aprimoramento da tecnologia existente, em vez de uma novidade. O telefone foi um rápido sucesso, basicamente porque era uma interface mais amigável. Qualquer pessoa podia aprender a usá-lo em minutos, e apenas operadores treinados operavam os telégrafos. Em 1880 já havia 30 mil telefones instalados no mundo. Uma das primeiras cidades a adotá-lo foi o Rio de Janeiro, por iniciativa de D. Pedro II, fotógrafo profissional e muito interessado em novas tecnologias. Na virada do século já eram 2 milhões de telefones em todo o mundo. Em 1903, o inglês Donald Murray inventou o teletipo, facilmente operado com um teclado de máquina de escrever.

A ITU, agora chamada de International Telecommunication Union, continua regulamentando as comunicações eletrônicas, como os protocolos usados na Internet. O impacto social da telegrafia guarda semelhanças com o desenvolvimento da Internet. Nos dois casos, foram novas tecnologias recebidas com otimismo e ceticismo, pela população em geral e por uma grande cobertura da mídia. O otimismo vitoriano que acreditava que o telégrafo eliminaria os desentendimentos entre as nações, também

estava presente nos primórdios da Internet. Em uma conferência em novembro de 1977, Nicholas Negroponte, chefe do Laboratório de Mídia do MIT, declarou que: “A Internet iria quebrar as barreiras nacionais e levar a um mundo de paz. As crianças do futuro não conhecerão o nacionalismo.” Na Internet também há fraudes, como os e-mails com esquemas financeiros e fraudes com cartões de crédito, e as empresas financeiras usam códigos (criptografia) em suas operações.

Códigos numéricos

Desde a década de 1970 usa-se amplamente etiquetas monocromáticas com código de barras, um sistema de identificação de produtos que é lido com um sensor óptico, presente em todos os produtos vendidos, na maioria dos supermercados, em livros e mídias audiovisuais, que agiliza o registro de produtos principalmente em pontos de venda, mas também encontra seu lugar em caixas automáticos, leitores de código de barras para pagamento de contas via Internet na própria residência, leitores de crachás etc. mas que é limitado por exigir uma leitura a curta distância (alguns centímetros) e tem vários códigos em uso no mercado para, a partir do código lido, efetuar um registro, abrir uma cancela, transmitir uma seqüência numérica, e geralmente tem de estar ligado a um banco de dados para saber o que tais dados significam. A Electrolux comercializa desde 2003 um refrigerador com um leitor de código de barras na porta, pelo qual deve-se passar qualquer embalagem que entra ou sai do refrigerador, e um software pré-programado pelo usuário, incluído no refrigerador, pode conectar-se a um supermercado, via Internet, e solicitar os produtos quando chegarem a um estoque predeterminado.

Outra aplicação para o uso das etiquetas é descrita na matéria de Miguel Portela intitulada “Código de barras contra roubo de carros”³⁰, um projeto aprovado no Instituto de Propriedade Industrial, com apoio do Sebrae, e proposto na Câmara dos Deputados pelo deputado federal Dilceu Sperafico, em 2005. O empresário e inventor Nilo Bergman, de Marechal Cândido Rondon, PR, foi motivado por levantamento da CPMI (Comissão Parlamentar Mista de Inquérito) do Congresso Nacional, de que são

³⁰ Gazeta do Povo, Curitiba, 6 fev. 2005

roubados 60 mil veículos por mês no Brasil e boa parte vai parar em desmanches e no Paraguai. O sistema consiste na aplicação de etiquetas adesivas de alta resistência ao calor e à abrasão, com códigos de barras, em até 15 pontos do veículo. Em caso de remoção de uma peça em que o código de barras está fixado, por exemplo, durante um conserto mecânico, o proprietário solicitaria uma nova etiqueta ao órgão responsável pelo trânsito e que também é detentor do sistema. A implantação do sistema é fácil e barata, cerca de R\$ 12,00 por carro.

RFID (Identificação por rádio-freqüência)

Em 1999, um grupo de empresas, apoiado pelo MIT (Instituto de Tecnologia de Massachusetts) formou o Auto-ID Center, para a pesquisa da utilização da identificação por rádio. Uma das empresas que participou dessa pesquisa inicial, da substituição dos códigos de barras pela RFID foi o Wal-Mart. Desde janeiro de 2005, todos os produtos comercializados pela Wal-Mart nos EUA vêm dos fornecedores com RFID. Como a RFID permite uma leitura a uma maior distância, e de centenas de itens praticamente ao mesmo tempo, é um sistema muito mais prático e eficiente, menos sujeito a falhas, para controle de estoque e movimentação de bens, inanimados ou animados, que permite economizar de 10 a 16% na distribuição de mercadorias, reduzindo a intervenção humana, e os erros, e permitindo um conjunto de informações mais específico que os códigos de barras. Num conjunto de caixas do mesmo produto no estoque, cada uma tem a mesma etiqueta de código de barras, freqüentemente já impressa na embalagem original, mas com RFID pode-se dar um código específico a cada caixa, controlando o tempo no estoque, o que é importante para produtos perecíveis.

Em um supermercado, por exemplo, em vez de passar item a item pelo leitor na caixa, pode-se passar com o carrinho e todos os itens são identificados em segundos.

Em São Paulo, nos estúdios do SBT (Sistema Brasileiro de Televisão), os crachás têm circuitos integrados RFID embutidos, que identificam quem passa em cada porta, liberando ou não o acesso em função de um banco de dados central, e que permitem saber onde está cada pessoa, em tempo real. E podem ser usadas em ingressos, bilhetes de metrô, ônibus, trens.

O código EPC, das RFID, permite incluir informações no próprio número do objeto, não sendo sempre necessário associar o número a um banco de dados, para saber do que se trata. Por exemplo, uma câmera em um radar de trânsito fotografa a placa de um veículo em velocidade acima da permitida, usa um software de reconhecimento óptico de caracteres, consulta o código da placa em um banco de dados para identificar o proprietário do veículo e emitir a multa. Sem o banco de dados, ele não sabe de que veículo se trata. Ter as informações já na identificação permite distribuir os bens sem necessidade de consulta a um banco de dados, como no envio de equipamentos militares ou suprimentos médicos a locais sem acesso a sistemas de informação.

O interesse pela RFID é grande porque elas aumentam a segurança, facilitando a identificação de produtos ao longo de toda a cadeia logística, permitindo identificar rapidamente e com baixo custo produtos roubados ou falsificados (que não tenham uma etiqueta válida embutida no produto), controlando melhor a bagagem em terminais rodoviários, ferroviários ou aeroviários, controlando a movimentação de bens em um prédio (uma RFID pode disparar um alarme e câmeras quando o produto passa por determinadas portas).

Em julho de 2004 o Departamento de Defesa (DOD) dos EUA detalhou a seus 40 mil fornecedores a exigência de que todos os produtos passem a ter etiquetas RFID passivas. Muitas empresas nos EUA e Europa estão adotando a tecnologia e o interesse dos fornecedores é estimulado pela redução nos prazos de pagamento pela aquisição dos bens, no caso do DOD, de 45 para 3 dias.

Uma RFID passiva é um chip com uma pequena antena. Quando passa até a 15 m de um leitor, que tem uma antena que irradia um campo eletromagnético, ele retira energia desse campo e envia o código numérico do chip pela antena. Uma RFID ativa tem uma pequena bateria e emite sinais mesmo sem energia do leitor. Seu custo ainda é muito alto, de 10 a 100 dólares, mas seu alcance é de 100m a 1000m e têm alta capacidade de armazenagem de dados.

As RFID geralmente operam nos EUA em uma frequência próxima à dos celulares (902-928 MHz) e em uma frequência bem menor na Europa (13,56 MHz).

O custo de uma RFID passiva, em 2005, está entre 22 e 120 centavos de dólar americano, mas a previsão para 2007 é que caia para 5 centavos de dólar.

O custo de implantação de um sistema pode ser muito alto pois há vários fatores a considerar na instalação física dos leitores, devido a interferência eletromagnética, compatibilidade dos sistemas de dados com os leitores, treinamento de usuários, mas a redução de custo e aumento da eficiência a longo prazo motivam cada vez mais empresas a adotar as RFID.

O custo dos leitores tende a cair muito, e prevê-se sensores simples (que só lêem os dados e os retransmitem a um sistema central) a 25 dólares até 2010.

As aplicações não se limitam a controle de movimentação de bens. Pode-se ter sensores espalhados para detectar ondas, furacões, flutuações de temperatura, vazamentos químicos ou nucleares. É como uma Internet de objetos inteligentes.

Até 2015 pode ser realidade, em alguns países, uma automação não imaginada nos Jetsons: o armário irá fornecer a roupa mais adequada ao compromisso marcado na agenda para o dia, o carro vai dirigir sozinho até seu destino, com o auxílio de sensores RFID e um receptor de GPS, desviando de engarrafamentos ou bloqueios. Se um pneu perder pressão, o sensor informa e o carro pára no próximo posto. As compras no supermercado, ao voltar para casa, simplesmente são armazenadas no porta-malas, pois a nota foi debitada em seu cartão de crédito ao passar com elas pela porta. E sua geladeira pode dar um alarme pois o número de calorias comprado para aquela semana está muito acima do prescrito por seu cardiologista. Vale a pena ter mais segurança e eficiência em troca da perda de privacidade? Para a maioria das pessoas, com base nas atuais condições de uso do sistema financeiro e da Internet, a resposta será afirmativa.

As RFID não deverão substituir os códigos de barras em todas as aplicações, mas apresentam muitas vantagens, seja na quantidade de dados (um código de barras comum tem até 30 caracteres, uma RFID passiva, 64KB, uma RFID ativa, 8 MB). A etiqueta de código de barras geralmente dura pela vida útil da embalagem, mas é frágil, uma RFID passiva pode durar muitos anos, uma ativa, de 3 a 5 anos, dependendo da bateria. Um código de barras é fixo, uma RFID pode ser fixa ou programável uma vez. RFIDs podem ser criptografadas, para mais segurança.

As RFIDs não são uma panacéia para resolver todos os problemas. Como o antigo ditado de que ao contratar um serviço deve-se escolher duas entre as três opções: rápido, bem feito e barato, com as RFIDs as duas escolhas são entre: rapidez, precisão e alcance. A frequência usada, a quantidade de metal presente no ambiente, o grau de interferência eletromagnética, o custo das etiquetas e sensores, o número de leituras por segundo, vão afetar o desempenho global.

Do ponto de vista da privacidade pessoal, não é barato implantar uma rede de sensores de RFID, capazes de registrar os movimentos em uma grande área, mas usa-se RFIDs em automóveis para controle de pedágio (as vias “rápidas”, com veículos passando no máximo a 30 ou 40 km/h, evitando as filas) e é fácil e barato ter um detector de sensores, pois todos operam na mesma faixa de frequências. Logo, uma vigilância onipresente como a do Grande Irmão não é muito prática de ser implantada. Mas é possível ter um controle por um grande número de locais, e registrar a movimentação do objeto portador da etiqueta, com data e hora, em grandes bancos de dados.

Se a etiqueta estiver colada no exterior do produto, pode ser facilmente destacada e destruída, mas se for embutida, será mais difícil ou ilegal eliminá-la. Vai depender do interesse ou necessidade do usuário.

Em outubro de 2004 o Escritório de Impressão do Governo dos EUA concedeu contratos de US\$ 373 mil a quatro fabricantes para projetarem passaportes com uma RFID embutida, com dados digitalizados sobre o rosto do viajante. Nos postos de controle nos aeroportos, uma antena leria o passaporte (até a 9 m de distância) e uma câmera digital enquadraria o rosto do viajante para compará-lo com os dados dos chips.³¹ Uma matéria de 6 de janeiro de 2005, no serviço noticioso on-line da CNN, informa que o Departamento de Estado dos EUA não deseja criptografar os dados no passaporte alegando que isso seria muito caro de implementar em países pobres.³²

Na Cúpula Mundial sobre a Sociedade de Informação, em Túnis, Richard Stallman, um dos criadores do Linux e defensor do software livre, protestou envolvendo

³¹ O GLOBO, 29 de novembro de 2004, matéria reimpressa de Matthew Wald, do New York Times.

³² <http://www.cnn.com/2005/TECH/01/06/passports/> acesso em 6 fev. 2005.

em papel alumínio seu crachá, para neutralizar a ação das RFID.³³ Mas nem todo tipo de papel alumínio é eficaz na eliminação dos sinais de rádio, só os com partículas ferrosas.

Uma coluna de B. Piropo, publicada no suplemento Informática etc. do jornal O GLOBO em 6 de junho de 2005, comenta outros aspectos de sua utilização:

“O sistema permite acompanhar todo o ciclo de vida de um produto, do momento da fabricação até seu lançamento em um aterro sanitário(...) Há chips RFID incrustados em pulseiras firmemente presas aos braços de internos no sistema carcerário norte-americano. E além dos crachás, também em telefones celulares, passaportes e carteiras de identidade.

O problema tornou-se tão sério que Congresso dos EUA solicitou que o GAO, Government Accountability Office, órgão do governo local, investigasse o uso da tecnologia pelas agências governamentais para “discutir aspectos de segurança e privacidade ligados à tecnologia, assim como ferramentas e práticas disponíveis para mitigar esses efeitos”.³⁴

O estudo concluiu que, das 24 agências governamentais investigadas, 13 informaram que já haviam implementado ou planejavam implementar esta tecnologia em uma ou mais aplicações, de controle de movimentação de bagagens até a emissão de “passaportes eletrônicos”. Três delas admitiram que a aplicação poderia permitir acompanhar os deslocamentos de seus empregados, porém apenas uma delas considerou que isso implicava considerações legais relativas à privacidade.

Além disso, o governo americano está prestes a implementar uma lei já aprovada pelo Congresso, o “Real ID Act”, que, pela primeira vez, cria um documento de identidade federal nos EUA. E esse documento poderá incluir um chip RFID.

A questão é tão controversa que em 2004 o congressista estadual da Califórnia, Joe Simitian, apresentou um projeto de lei proibindo o uso de chips RFID em qualquer documento de identidade emitido pelo Estado da Califórnia. A lei foi aprovada pela câmara de deputados local por 29 votos a 7.”

Esta discussão é mais antiga, uma matéria publicada no jornal O GLOBO em 22 de dezembro de 2001, por Toni Marques, comentava:

³³ O GLOBO, 18 nov. 2005

³⁴ www.gao.gov/new.items/d05551.pdf

Carteira de identidade e histórico médico estão prestes a se fundir graças à tecnologia de implante de microchips em seres humanos, desenvolvida pela empresa Applied Digital Solutions (ADSX), de Palm Beach, na Flórida. A empresa tornou-se, esta semana, a primeira a anunciar o domínio da tecnologia, que já foi aprovada pela Comissão Federal de Comunicações (FCC) — encarregada da aprovação, devido ao uso de transmissões de rádio. Os microchips estão sendo testados em seres humanos e serão submetidos à aprovação da Administração de Drogas e Alimentos (FDA).

A nova tecnologia terá numerosas aplicações médicas, mas abre um debate sobre a violação da privacidade porque poderia ser usada para identificar criminosos.

Usando um scanner, paramédicos poderão ter, no local de um acidente, todo o histórico clínico de uma vítima desacordada, por exemplo. No futuro, poderá ser usado para monitorar o estado de saúde de seu usuário, medindo a temperatura do corpo e os níveis de oxigênio no sangue, entre outros indicadores.

O chip também poderá ser útil para identificação: as alfândegas terão informações precisas, à prova de fraude, sobre passageiros desembarcados. O diretor-executivo de tecnologia da Applied Digital Solutions, Keith Bolton, antevê ainda aplicações em sistemas de segurança, tanto individuais quanto coletivos.

O microchip, segundo ele, será aperfeiçoado a médio prazo de modo a permitir a localização via satélite de cada usuário. O primeiro produto dessa linha deverá ser o Guardian Angel (Anjo da Guarda), disponível em 2001 em forma de relógio, para monitorar o deslocamento de crianças, idosos e deficientes: caso o usuário saia do raio geográfico predeterminado na configuração do serviço, um alarme é disparado no aparelho que fica em poder dos responsáveis.

(...) O executivo disse que o microchip não pode ser sentido pelo tato, nem denunciado por detectores de metais. Testes já realizados em humanos não constataram nenhum caso de rejeição ao chip, nem efeitos colaterais ou interferência em aparelhos de marca-passo.

O executivo não soube informar qual seria o prazo de validade de cada microchip, mas adiantou que deverá ter que ser substituído de tempos em tempos. A primeira versão a ser comercializada deverá estar disponível em 2002. Terá apenas a função de arquivo de informações, como suscetibilidade a alergias, tipo sanguíneo e doenças crônicas, e será limitado a 60 palavras.

Bolton não informou qual será o preço da nova tecnologia, mas o usuário terá que pagar tanto pelo chip quanto por seu implante, um procedimento cirúrgico bem simples. Quando a tecnologia incluir o rastreamento por satélite, será cobrada uma taxa mensal pelo serviço.

Uma nota no Diário de S. Paulo de 1 de fevereiro de 2005, comentava que um microchip cutâneo, importado dos EUA, já está sob a pele de 40 empresários brasileiros, 25 deles de São Paulo, que se consideram alvo potencial de seqüestros. Ricardo Chilelli, da RCI First Security, que importa os microchips, disse que há 2 mil clientes na fila de espera para instalar o produto que, alegam, em caso de seqüestro, permite à polícia localizar o cativo.

No Rio de Janeiro, em 2004 foi elaborado pelo coordenador do Renavan no Detran, Robson Cardinelli, e pelo gerente do projeto Gestão da Tecnologia da Informação do órgão, Emerson Tizziani, um projeto para instalar, inicialmente nos carros novos, e em cerca de 18 meses, em toda a frota de 3,5 milhões de veículos do estado, o Selo de Segurança Veicular, com um microchip RFID com informações básicas do carro (chassis, placa, cor, marca, modelo e Renavan) e data de emissão do dispositivo eletrônico, mais de 300 conjuntos de câmeras e antenas (colocados em postes, viadutos e pontes), três unidades móveis de leitura de dados, uma central de computação, 500 palmtops (computadores de mão) e 42 terminais instalados em locais como batalhões da Polícia Rodoviária e da PM. Em dezembro de 2005 isso ainda não havia sido implantado.³⁵

Câmeras de vigilância

As câmeras de vigilância têm tido um crescimento exponencial, principalmente na Grã-Bretanha, onde já estão em uso há mais de dez anos, e existem cerca de 4,2 milhões de câmeras no final de 2005, o que já permite uma análise adequada de sua atuação e do impacto dessa tecnologia como instrumento de controle social.

Ao longo do século 20, a idéia da vigilância vem sendo inscrita na consciência de massa principalmente por seu tratamento artístico na cultura popular, em filmes como

³⁵ SCHMIDT, Selma, *Novo sistema vai monitorar a frota de veículos*, n' O GLOBO, 30 set. 2004.

Janela indiscreta (1954), de Alfred Hitchcock, *A Conversação* (1974), de Francis Ford Coppola, músicas como *Every breath you take*, do grupo The Police (1983), além dos clássicos da literatura, *1984* de George Orwell (1948) e *Admirável mundo novo*, de Aldous Huxley (1932).

São clássicos da cultura popular com uma visão trágica e distópica do impacto pessoal e político da vigilância. A letra de Sting, *Every breath you take* diz: *every breath you take, every move you make, every bond you break, every single day, I'll be watching you*, mas trata da obsessividade de ex-amantes.

No livro *1984*, um aparato tecnológico reproduz a imagem do panóptico de Bentham, gerando um controle interior em cada sujeito observado, embora nem todos sejam observados todo o tempo, não sabem quando estão sendo observados e não desejam arriscar-se a um comportamento inadequado ser flagrado pela vigilância centralizada. Mas essa condição só é aceita por um cenário mais amplo de incerteza total quanto ao presente e ao futuro, pela permanente mas distante e mutável guerra entre os três continentes. A combinação de incerteza do passado/presente/futuro com a real possibilidade de punição por um comportamento inadequado cria as condições psicológicas para impor uma submissão sem questionamento às normas. A propaganda da vigilância, sempre presente, reforça a submissão às normas.

Na visão de Huxley, um mundo com humanos criados com manipulação genética, sujeitos à vigilância do estado e com comportamento controlado por psicotrópicos, gera uma sociedade de classes sem ascensão social e com padrões de comportamento reforçados também pela propaganda.

Em *Gatacca* (1997), a idéia de uma sociedade organizada pela engenharia genética só é desafiada por um indivíduo que consiga superar os mecanismos de vigilância.

Lyon (1994: 201) lembra que a vigilância tem duas faces. Ao lado de um estado totalitário, temos a proteção de um guardião benevolente.

A vigilância é reconhecida com um componente necessário à construção social, as crianças são culturalmente formadas sob a supervisão constante dos adultos.

O moderno estado de bem estar social usa a vigilância, o registro atualizado de informações diversas dos indivíduos, como ferramenta para tentar administrar da forma mais justa possível a educação, o atendimento médico (como as cadernetas de vacinação, necessárias para serviços educacionais, ou auxílios financeiros aos mais pobres), as aposentadorias e pensões.

O que está em rápida evolução é o cruzamento, permitido pela evolução das tecnologias de informação, das diversas fontes de informações, que permitem definir padrões de comportamento, ou criar análises para previsões de comportamento futuro.

As trágicas preocupações distopianas da cultura de massa também surgem no discurso acadêmico, que reconhece a vigilância como uma forma de poder, ampliado pela tecnologia, penetrando cada vez mais no tecido social. Quando trata da circuitos fechados de televisão (CCTV), o discurso acadêmico tem freqüentemente representado as câmeras de vigilância como uma extensão do panóptico.

O panóptico imaginado pelo filósofo inglês Jeremy Bentham, no século 18, constituía um programa para o exercício eficaz do poder pela construção de uma estrutura cilíndrica onde uma torre central abrigaria as salas dos vigilantes, com venezianas nas janelas, separações que as cortam em ângulo reto e biombos em vez de portas, o que impede ver a movimentação dos vigilantes. Cada seção da coroa circular ao redor da torre, como pequenas fatias de pizza, abrigaria celas individuais com uma janela voltada para o centro e uma janela voltada para fora da construção, garantindo uma visão irrestrita de seu interior e, por janelas na torre central, os vigilantes viam sem ser vistos, reforçando um comportamento dos presos, sempre conforme as normas, que não sabiam quando eram observados. E esse princípio aplica-se não só a condenados, mas também a loucos, doentes, operários ou escolares. Não há contato entre os presos, logo evita-se complôs, 'motins', fugas, más influências recíprocas. Nos doentes, evitaria-se o contágio. Nos alunos, a cola. Nos operários, as distrações que reduzem a produtividade.

E a vigilância não era mais completa por falta de tecnologia adequada. Na nota 4 do capítulo do Panoptismo, Foucault (1975) comenta que Bentham também imaginou uma vigilância acústica, por tubos que iam das celas à torre central, e que abandonou

essa idéia no *Post-crypt to the Panopticon*, de 1791, talvez por não poder impedir que os presos também ouvissem os vigilantes.

Foucault reproduz as medidas que deveriam ser adotadas em uma cidade, no final do século 17, quando era declarada como afetada pela peste: um policiamento espacial estrito, a cidade era isolada, a punição por sair da cidade era a morte, os animais errantes eram sacrificados, cada quarteirão, cada rua era vigiada por um síndico, que também não poderia abandonar essa vigilância, sob pena de morte, o síndico tranca todos em suas casas, leva as chaves ao intendente do quarteirão que as conserva até o final da quarentena. Eram tomadas providências para o fluxo de alimentação, mas sem contato entre fornecedores e consumidores. Todos vigiados todo o tempo e apoiados por uma estrutura militar, postos de vigilância e casas de guarda. Diariamente o síndico de cada rua observa os moradores pelas janelas, anota o relato de cada um sobre sua condição de saúde e repassa esses relatórios ao intendente do quarteirão e os intendentes os repassam ao prefeito. Os magistrados controlam o acesso dos médicos, boticários e confesores. E mesmo os rituais de purificação das casas, feitos isolando-se toda a casa, portas, janelas, buracos de fechadura, cinco ou seis dias depois de iniciada a quarentena, e queimando-se perfumes em seu interior, incluem a revista dos perfumadores, na presença dos moradores da casa, para que não levem nada que não tenham trazido.

Conforme nota da Secretaria da Agricultura da Bahia, publicada no Diário Oficial do estado de 11 de novembro de 2005:³⁶

A Agência de Defesa Agropecuária da Bahia (Adab) vai elevar o número de postos fixos de fiscalização sanitária nas divisas com os estados do Piauí, Tocantins, Goiás, Minas Gerais e Espírito Santo. As novas unidades serão implantadas onde hoje estão instalados os postos móveis, que serão deslocados para outras áreas, ampliando a vigilância agropecuária da Bahia. (...) A medida foi anunciada pelo secretário da Agricultura, Pedro Barbosa, e pelo diretor-geral da Adab, Luciano Figueiredo, que fizeram uma série de visitas às barreiras sanitárias que funcionam com o apoio da Secretaria da Fazenda (Sefaz) e da Polícia Militar. O objetivo da viagem foi ver de perto o funcionamento das barreiras sanitárias e conferir o cumprimento da Portaria 281, que suspendeu a entrada na Bahia de animais vivos suscetíveis à febre aftosa

³⁶ <http://www.seagri.ba.gov.br/noticias.asp?qact=view¬id=5320>, acesso em 13 nov. 2005

(bovinos, bubalinos, caprinos, ovinos e suínos) vindos de qualquer outro estado do país por um prazo de 60 dias. Houve apreensões de caprinos que tentavam entrar no estado através da divisa com o Tocantins, de 17 touros jovens vindos do Rio Grande do Sul na divisa com Minas Gerais, além de animais vindos do Paraná e Mato Grosso que tentavam ingressar por Correntina. Todas as áreas foram visitadas com o intuito de se verificar *in loco* todo o trabalho realizado para salvaguardar o rebanho baiano da entrada de animais possivelmente infectados. A agência agora vai em busca dos produtores que não cumpriram a determinação da Lei de Defesa Sanitária do Estado de vacinar, para que sejam aplicadas as sanções previstas na legislação, ou seja, multa de 50 Ufirs por cabeça não-imunizada, cerca de R\$ 51. A vacinação contra a febre aftosa é obrigatória em todo o país. “A Bahia alcançou índices muito bons de vacinação, muito acima do que é exigido pela Organização Internacional de Sanidade Animal (OIE), que é de 85%”, explicou Figueiredo. Ele destacou que a meta do Estado é alcançar 100% de animais vacinados.

E, conforme a Tribuna da Imprensa de 24 de outubro de 2005³⁷, o estado de São Paulo ergueu uma barreira contra a carne procedente do Paraná e o governador paulista informou que os animais que foram adquiridos nos leilões paranaenses e que já entraram em São Paulo foram localizados e foi coletado material para exame sorológico.

Sabendo-se que todos os animais das fazendas onde houve casos de febre aftosa foram sacrificados, e que a maior parte do rebanho bovino brasileiro já é identificada individualmente por circuitos integrados RFID implantados na orelha, observa-se que, mais de três séculos depois, o Estado toma praticamente as mesmas medidas de vigilância e segurança. Os mecanismos de registro são digitalizados, o que acelera sua distribuição e replicação, e a novidade é que agora existe o seguro, para compensar os produtores pelo abate dos animais suspeitos que estiverem em dia com sua vacinação.

Houve uma grande evolução desde o uso de fotografias, com seu demorado processo de revelação e cópia, até as câmeras eletrônicas, os gravadores de vídeo analógicos e as modernas câmeras e sistemas de gravação digital. Com o barateamento da tecnologia, e a simplificação de sua operação, o uso de câmeras cresceu muito.

³⁷ <http://www.financeone.com.br/noticia.php?lang=br&nid=15302>, acesso em 13 nov. 2005

O número de câmeras implantadas atualmente varia de três ou quatro, em pequenas cidades da região serrana do Rio de Janeiro, a 200, no final de 2005, na cidade do Rio de Janeiro, com previsão de instalação de mais 400 câmeras durante 2006, até cerca de 4,2 milhões, em 2005, na Inglaterra.

Os sistemas de gravação estão mudando rapidamente: de gravadores em fita magnética, um aparelho VHS modificado para gravar 24, 30 ou até mesmo 480 horas em uma fita, para interfaces entre câmeras e computadores, que gravam os dados em disco rígido e podem disponibilizá-los em intranets ou via Internet. E aliados a esses sistemas há softwares de reconhecimento facial, embora não infalíveis, cada vez mais sofisticados, que podem comparar milhares de rostos por minuto com os registrados em bancos de dados, em busca de criminosos ou suspeitos, ou identificar onde o mesmo rosto aparece, em diversos locais e horários, para tentar traçar um histórico do deslocamento do indivíduo.

Os principais argumentos a favor de tais sistemas são o auxílio à identificação de criminosos e o acompanhamento da movimentação de suspeitos de atos criminosos, e o melhor uso dos recursos policiais, deslocados para locais onde estão ocorrendo atividades suspeitas, sem a necessidade de um efetivo maior, e mais caro, para cobrir áreas sem risco de crimes.

Um estudo apresentado em janeiro de 2004 numa conferência internacional em Sheffield, Inglaterra, afirmou que cada residente de Londres tem sua imagem captada, em média, 300 vezes ao dia pelo sistema de CCTV. A matéria, “‘Big Brother’ nas ruas inglesas”, publicada pelo jornal O GLOBO em 18 de janeiro de 2004, continua:

São mais de quatro milhões de câmeras espalhadas pelo país, uma para cada 14 habitantes. Enquanto países como a Alemanha e o Canadá proíbem a coleta de imagens de pessoas na rua, a Inglaterra, tão zelosa de sua imagem de civilização recatada e privada, tem uma legislação particularmente branda quanto ao uso de CCTVs. Entidades de defesa dos direitos civis questionam a eficácia da medida no combate ao crime ou na prevenção de ataques terroristas. Pesquisa citada recentemente pelo jornal “The Independent” concluiu que uma melhor iluminação de rua é sete vezes mais eficaz para a diminuição de crimes.

Pela Lei de Proteção de Dados regulamentada em 2000 na Inglaterra, o público deveria ser alertado para a localização de cada câmera e de como exercer o direito de acesso a sua imagem. Pelas contas de entidades civis, 70% das 4.285.000 câmeras instaladas no país violam algum artigo da lei. Agentes de segurança de lojas, prédios e shopping centers freqüentemente usam o sistema para efetuar o que o professor Clive Norris, do Centro de Pesquisa Criminalística de Sheffield, chama de “limpeza social” do local.

A pesquisa comentada nessa matéria levanta a questão de se o que se propõe defender é o interesse público ou o interesse de uma parte dos comerciantes ou de outros interessados. Se outras medidas não seriam mais eficazes que a simples vigilância. Na cidade do Rio de Janeiro, no início da década de 1990, a Polícia Militar tinha um efetivo de cerca de 10 mil policiais, e havia uma visível presença deles em dezenas de bairros, nas zonas sul e norte da cidade, na orientação do trânsito e no patrulhamento. Em 2005, são cerca de 23 mil policiais e sua visibilidade é muito menor. O papel de vigilância e orientação do trânsito, que exerciam, e contribuía tanto para um melhor fluxo de trânsito quanto para menos ocorrências de assaltos que atualmente, foi eliminado, pois a Guarda Municipal, à exceção do bairro de Copacabana, não tem nenhuma atuação significativa no trânsito ou na segurança pública. Atualmente, muitos policiais militares estão oficialmente lotados exercendo função de segurança de políticos.

“De olho no crime”, de Fábio Vasconcellos, publicada em 27 de janeiro de 2004, elogiava o sucesso de nove câmeras de vídeo (sete na Avenida Atlântica e duas na Avenida Nossa Senhora de Copacabana) usadas pelo 19º BPM há cerca de seis meses:

Segundo dados da Secretaria de Segurança Pública, o número de assaltos a pedestres registrados na 12ª DP (Copacabana) e na 13ª DP (Posto 6) caiu 34% no segundo semestre de 2003, se comparado ao índice dos primeiros seis meses do ano passado, quando ainda não existiam câmeras na área. De janeiro a junho, foram 196 casos, contra 130 de julho a dezembro. A redução é ainda maior em relação a 2002. De agosto a dezembro daquele ano, ocorreram 202 assaltos. Em 2003, no mesmo período, os

registros caíram para 107 (uma redução de aproximadamente 52%). Também de agosto a dezembro, o roubo de veículos caiu de 35 casos para 18.

Os índices são comemorados pela Associação Brasileira da Indústria de Hotéis (ABIH). O vice-presidente da entidade, Alexandre Sampaio, diz que a sensação de segurança no bairro — que hospeda uma média de 25 mil turistas por mês — melhorou. Ele conta que têm sido menos frequentes os relatos de turistas vítimas de assaltos. Por isso, pretende propor à Secretaria de Segurança o aumento do número de câmeras. (...)

O delegado titular da Delegacia Especial de Atendimento ao Turista (Deat), Ricardo Andreiolo, diz que o número de assaltos a turistas caiu principalmente no calçadão, área monitorada pelas câmeras. No entanto, conta o delegado, os bandidos passaram a atuar em ruas internas. (...)

O subcomandante do 19º BPM, tenente-coronel Elson Haubrichs, afirma que o sistema de segurança tem ajudado a polícia a inibir assaltos e o tráfico de drogas. Além de câmeras, o batalhão tem computadores que monitoram em tempo real o posicionamento de todas as patrulhas. — Reduzimos muito o tempo que levávamos para atender aos chamados dos moradores. Com as câmeras, podemos acompanhar a movimentação dos banhistas e com isso fazer rapidamente prisões em flagrante. (...)

Mas nem tudo é comemoração. O presidente da Associação dos Amigos de Copacabana, Horácio Magalhães, acredita que ainda falta integração da prefeitura com a polícia: “As câmeras estão aprovadas, mas ainda falta parceria entre os órgãos. Não adianta inibir os assaltos se do outro lado ainda há um grande número de mendigos na área. Essas pessoas poderão um dia também praticar assaltos”.

A matéria apresenta a contradição mesmo quando não o pretende. No primeiro parágrafo ‘elogia’ a redução de 2002 para 2003, quando não havia câmeras, e atribui a redução de 2003 para 2004 às câmeras. E reconhece a mudança da ocorrência dos assaltos para ruas sem vigilância, mas os números não são confiáveis porque o próprio jornal já publicou várias reportagens afirmando que muitas ocorrências não são registradas e as estatísticas sobre segurança pública no estado do Rio não são confiáveis. Ao misturar no âmbito da segurança a questão do tráfico de drogas, que em Copacabana não tem um histórico de violência, como existe em outros bairros do norte da cidade, frequentemente motivos de matérias de primeira página, o discurso do jornal tenta reforçar a imagem positiva da vigilância com câmeras, apelando para uma correlação

com um tema que inspira preocupação e que busca legitimar a vigilância em troca de uma possível maior segurança. A matéria termina destacando o interesse dos comerciantes, projetando sobre os pedintes uma imagem de risco, de futuros possíveis assaltantes, em vez de buscar uma solução para um problema social. É o mesmo discurso presente nos exemplos sobre CCTV na Inglaterra.

As tecnologias de processamento de imagens estão ampliando a utilidade das câmeras de vigilância. A empresa Sisgraph lançou em 2005 o Intergraph Video Analyst, que usa a tecnologia VISAR (Video Image Stabilization and Registration), originalmente criada a pedido do FBI à NASA, a agência espacial americana, que usa a tecnologia para estudar melhor erupções ou fenômenos climáticos em planetas, para ajudar na investigação de vídeos de baixa resolução quando do atentado a bomba nas Olimpíadas de Atlanta em 1996. Ela estabiliza imagens de vídeo, especialmente feitas em movimento e melhora drasticamente sua nitidez, processando cada pixel da imagem. E o sistema pode separar simultaneamente as imagens de até 128 câmeras, ou compilar os fragmentos de imagens de várias câmeras num ambiente, montando uma seqüência.³⁸

Não há uma comprovação clara de significativos efeitos positivos no mundo real, a não ser nas séries policiais na TV, onde os criminosos acabam sendo localizados por uma gravação por câmeras de caixas automáticas, lojas ou controle de trânsito. Ou seja, não é comprovado que o investimento em sistemas de CCTV traz melhores resultados que o mesmo investimento realizado em treinamento de pessoal, ou em aquisição de veículos e outros equipamentos. O comprovado é que há um grande investimento em alguns países, notadamente a Inglaterra, em um período de mais 10 anos, e há pouco avanço, ou até mesmo piora, nos indicadores de crimes que são alvos dessa vigilância.

Um caso específico é o de multas de trânsito por avanço de sinal ou excesso de velocidade, em que os veículos são fotografados em condições de boa visibilidade, estando sempre a uma certa distância da câmera e iluminados por flashes, e as placas são identificados por um software de reconhecimento óptico de caracteres (OCR). Não é um caso de violação de privacidade pois as multas são emitidas para o proprietário do

³⁸ Machado, A. *Tratamento de vídeo como nas séries policiais*. n' O GLOBO, Informática etc., 28 fev.

veículo e o registro no departamento de trânsito geralmente não é compartilhado com outros órgãos e, com o pagamento das multas, é apagado depois de determinado período. No estado de São Paulo estão estudando implantar a partir de 2006, centenas de câmeras acopladas a um sistema de reconhecimento óptico das placas. A matéria “Governo caça devedor do IPVA”, de Osmar de Campos Soares e Ana Paiva, do Diário de São Paulo, publicada no O GLOBO em 1 de junho de 2005, comenta:

O governo do estado, em parceria com a Prefeitura de São Paulo e de outras cidades, testa um sistema de radar para identificar veículos não licenciados. (...) Câmeras colocadas nas principais vias e nas estradas vão flagrar os veículos e filmar as placas. Em 14 segundos é feita uma consulta automática no banco de dados da Secretaria da Fazenda para verificar se há alguma irregularidade no pagamento do imposto ou de multas. Um quilômetro depois, policiais vão parar o motorista. Além de verificar o pagamento do imposto, será possível também identificar carros roubados. A idéia é diminuir a inadimplência do IPVA. O pagamento do imposto é pré-requisito para fazer o licenciamento. A taxa de inadimplência é de 5,5% e o estado de São Paulo estima em 2004 foram de R\$ 250 milhões as perdas com carros que circulam sem o pagamento do imposto, pré-condição para o licenciamento do veículo. Em apenas uma semana de teste na Rodovia dos Bandeirantes, que liga São Paulo a Campinas, 2 mil devedores de IPVA foram flagrados. (...) De acordo com o Detran, cerca de 27% da frota estadual está sem licenciamento. (...) Os bloqueios nas rodovias terão furgões com postos da Caixa Econômica Federal e do Detran. O motorista em atraso pode pagar o IPVA no ato e receber o certificado. Em seguida, é liberado do bloqueio com sua situação regularizada.

Em Curitiba, os 110 radares, que em maio de 2005 notificaram 13.660 motoristas por excesso de velocidade, estão sendo ligados a um sistema de OCR das placas, para auxiliar a polícia em casos de seqüestros relâmpago, clonagem, furtos e roubos de veículos. Para isso, basta que a placa do automóvel em fuga ou irregular esteja no sistema de controle da Diretoria de Trânsito (Diretran) de Curitiba³⁹. Não informaram se essas imagens ficarão registradas, além das fotos nas multas, pois esse registro permanente permitiria vigiar o deslocamento dos veículos mesmo muito tempo depois.

2005.

³⁹ “Radares são usados para rastrear carros irregulares ou em fuga”, Gazeta do Povo, 8 jul. 2005

A UFRJ pretende instalar em três guaritas, nas entradas da ilha do Fundão, o Kapta (Sistema de Reconhecimento Automático de Placas de Veículos Automotores), um software de processamento de imagens e reconhecimento de padrões, para identificar os veículos em trânsito, desenvolvido inicialmente pelo professor Antônio Carlos Tomé, do IM. Em cada uma delas, o segurança responsável terá na tela do computador três imagens frontais e uma panorâmica dos veículos que entrarem no campus. Além disso, o Kapta disponibiliza para o operador uma imagem frontal do veículo e uma detalhada da placa, tanto a visualizada, como a identificada pelo sistema.⁴⁰

O esquema de segurança para as Olimpíadas de agosto de 2004 na Grécia teve orçamento de 650 milhões de euros, valor três vezes superior ao da edição anterior, em Sydney-2000. As medidas de segurança para os Jogos de Atenas incluíram aviões da Organização do Tratado do Atlântico Norte (Otan), laboratórios móveis russos capazes de detectar substâncias nucleares, químicas ou biológicas em caso de ataques, microfones para monitorar ruídos e 293 câmeras em Atenas e mais 113 em outros locais, para a vigilância do trânsito, além de verificação de disparos e explosões. O sistema também trabalhou para impedir um possível ataque de hackers na infra-estrutura dos Jogos. Placares eletrônicos, sinais de trânsito e as redes de tráfego aéreo foram testados por especialistas de eletrônica antes do evento para tentar impedir invasão de hackers. Foram monitorados nove portos, cada um com duas câmeras térmicas para visualização da faixa litorânea além das câmeras de vídeo. Todo o perímetro dos portos foi controlado por sensores eletrônicos de pressão e monitorados por câmeras fixas. Na Vila Olímpica, todas as câmeras foram rodeadas por cercas eletrônicas com duas tecnologias, uma de pressão e outra de movimento (vibração).⁴¹ Aparentemente, apesar das reclamações de extrema lentidão de deslocamento no trânsito, não houve problemas sérios de segurança nas Olimpíadas.

⁴⁰ CARMO, Diego, *KAPTAção de imagens*, informativo Olho no Olho, UFRJ, 18 out. 2005.

⁴¹ RODRIGUES, Jorge Luiz, *Pré-Olímpico contra o terrorismo*. O GLOBO, 7 mar. 2004.

Em relação ao total de capturas, há muito poucos casos comprovados em que a vigilância por vídeo resulte em captura de criminosos. Um dos casos mais conhecidos é o de uma série de garrafas de refrigerante contaminadas com arsênico, no meio-oeste americano, na década de 1990. Analisando (e esse é o grande feito) centenas de milhares de fitas de vigilância, de centenas de lojas, de dezenas de cidades, o FBI e as polícias locais conseguiram identificar um homem em atitude suspeita junto a prateleiras de refrigerantes, em diversas cidades onde ocorreram os crimes, e posteriormente ele foi preso e condenado pelo homicídio.

Uma notícia publicada pelo jornal inglês *Evening Standard*, de Ben Leapman, no site *This is London*, distribuído no metrô londrino, de 24 de fevereiro de 2005, intitulada “Grã-Bretanha: câmeras de vigilância não impedem o crime”, comenta que os pesquisadores do Ministério do Interior concluíram que as câmeras de vigilância não reduziram o crime em 13 das 14 configurações de uso estudadas. Os sistemas de circuito fechado de TV foram anunciados como uma importante iniciativa no combate ao crime na última década, mas as evidências não suportam sua eficiência. Embora tivessem grande apoio da opinião pública para sua instalação, essa opinião começou a mudar quando as pessoas não perceberam muita diferença com a presença das câmeras.

Os pesquisadores descobriram que alguns dos esquemas de uso de câmeras foram mal implantados, reduzindo sua eficácia. Seis das 14 salas de controle não tinham operadores parte do dia ou à noite. E em alguns casos as imagens noturnas eram pouco nítidas, devido à iluminação pública. As descobertas abalaram o Ministério do Interior, que havia anunciado as câmeras como uma importante arma no combate ao crime nos últimos 10 anos. O autor do relatório, Professor Martin Gill da Universidade de Leicester, declarou que quem apoiou o sistema ficou desapontado com as descobertas dessa pesquisa. Na maioria, os sistemas de CCTV não reduziram o crime nem deixaram as pessoas sentindo-se mais seguras. O único bem sucedido entre os 14 sistemas era o que vigiava estacionamentos, que levou a uma queda significativa nos crimes contra veículos. Outros sistemas em centros comerciais, áreas residenciais e hospitais não apresentaram benefícios claros. Um dos problemas era que contando com financiamento governamental, os órgãos policiais locais não implantaram as câmeras com metas claras

de uso. Outro é que não é tão difícil evitar ficar no raio de visão das câmeras, milhares delas instaladas em bairros da periferia de Londres, ou fugir rapidamente do local, antes da chegada da polícia.

Mas o sistema está em rápido crescimento. Steve Connor, do Independent, de Londres, teve uma matéria reproduzida pelo jornal O GLOBO, edição de 23 de dezembro de 2005, intitulada: “Britânicos sob vigilância total”, onde ele afirma:

O Reino Unido está prestes a se tornar o primeiro país do mundo onde o movimento de todos os veículos em ruas e estradas será gravado em imagens. Um novo sistema nacional de vigilância manterá os registros por pelo menos dois anos. Com uma rede de câmeras que podem gravar automaticamente cada placa de carro, o sistema permitirá criar um enorme banco de dados, de modo que a polícia e outros serviços de segurança possam analisar qualquer trajeto de qualquer motorista nos próximos anos.

A rede vai incorporar milhares de câmeras de circuito interno de TV já existentes, que serão adaptadas para ler automaticamente números de placas noite e dia, cobrindo todas as estradas e as principais ruas, bem como outras áreas das cidades, como portos e pátios de postos de gasolina.

Em março de 2006, um banco de dados central instalado num prédio da polícia em Londres armazenará diariamente os detalhes de 35 milhões de leituras de números de placas. O registro incluirá hora, data e localização precisa. Os locais das câmeras serão monitorados por satélites.

Também já há planos para ampliar o banco de dados, aumentando o período de armazenamento para cinco anos e ligando milhares de câmeras adicionais, de modo que os detalhes de mais de cem milhões de placas possam ser registrados a cada dia.

Os policiais britânicos afirmam que a rede de vigilância possivelmente é o maior avanço em tecnologia de prevenção e detecção de crimes desde a introdução do exame de DNA. Mas muitos, preocupados com as liberdades civis, temem que o movimento de milhões de pessoas cumpridoras das leis fique registrado num banco de dados central por muitos anos. O novo banco de dados nacional do movimento de veículos será a base de um sofisticado instrumento de vigilância que é o centro de uma operação destinada a tirar criminosos das ruas e estradas. No processo, o banco de dados fornecerá incomparáveis oportunidades para reunir informações secretas sobre movimentos e associações de

grupos organizados e suspeitos de terrorismo quando eles usarem carros, vans ou motocicletas.

O esquema está sendo organizado pela Associação de Chefes da Polícia (Acpo) e tem o apoio total de ministros, que este ano aprovaram o gasto de 24 milhões de libras esterlinas (R\$ 97 milhões) em equipamentos. Mais de 50 autoridades locais assinaram acordos para permitir que a polícia adapte milhares de câmeras de trânsito já instaladas de modo que elas leiam placas automaticamente [5000 por minuto, conforme Norris]. Os dados serão enviados à central em Londres por uma rede de comunicações da polícia.

Chefes da polícia também estão prestes a assinar acordos com o departamento de estradas, supermercados e donos de postos de gasolina para que eles incorporem suas câmeras de circuito fechado de TV à rede. Além de cruzar os números de cada placa com os de veículos roubados ou suspeitos, será possível checar se cada veículo está com os documentos em ordem.

Frank Whiteley, chefe da polícia de Hertfordshire e presidente da comissão da Acpo para reconhecimento automático de números de placas, declarou que: “Cada vez que você dirige um carro, isto já é registrado numa câmera de circuito fechado em algum lugar. A diferença é que no futuro a placa do carro será registrada também. O centro de dados será capaz de informar onde o veículo esteve e onde está agora, se esteve ou não numa área em particular e os percursos que ele fez. São particularmente importantes os veículos associados (comboios de carros, vans e caminhões para saber quem estava dirigindo perto de um veículo de interesse da polícia. Criminosos, por exemplo, vão dirigir em algum lugar um veículo em condições legais, roubar um carro e voltar em comboio para cometer novos crimes.)”

A matéria afirma que a nova rede de vigilância nacional para rastrear veículos em movimento, desenvolvida durante mais de 25 anos, é apenas o início de um plano para monitorar o movimento de todos os cidadãos na Inglaterra. A Seção de Desenvolvimento Científico do Ministério do Interior está elaborando técnicas de reconhecimento facial, e acreditam que é apenas uma questão de tempo para que máquinas possam recuperar a imagem de uma face numa multidão de pessoas em movimento.

E há o temor, cada vez mais justificado, de que se os serviços de segurança puderem mostrar que uma operação de vigilância nacional de veículos pode proteger o

público de criminosos e terroristas, haverá uma grande vontade política de fazer o mesmo com as câmeras instaladas nas ruas, para monitorar o fluxo de pessoas.

Norris (1999), cita Flusty (1994) e Davis (1990) que realizaram estudos de caso em Los Angeles, Califórnia, apresentando uma visão algo assustadora do potencial distópico da vigilância. Eles consideram que a cidade foi concebida historicamente como uma arena que fornece espaços para trocas e interações entre indivíduos e diferentes grupos sociais, espaços democraticamente abertos a todos, mas está sendo reconstruída como local de consumo de massa. Os indivíduos estão sendo reclassificados, não por seu potencial como cidadãos, mas como consumidores. O interessante aqui é o papel das câmeras de CCTV, usadas, por exemplo, para excluir quem não se enquadra no padrão de um 'bom' consumidor. Os shopping centers, nos EUA e no Brasil, além de diversos outros países, têm sistemas de CCTV para controle do movimento de todos os que circulam por seus espaços, e como ferramenta para coibir a permanência ou entrada de 'indesejáveis', sejam pessoas cuja vestimenta indique uma classe economicamente baixa, sejam comportamentos indesejados.

Em Los Angeles, as câmeras também servem para policiar as fronteiras de espaços segregados que, quando 'invadidos', provocam rápida repressão policial. E em bairros mais pobres, a polícia coíbe vários comportamentos. O Departamento de Polícia de Los Angeles restringe incansavelmente o espaço de reuniões públicas e a liberdade de movimentação de jovens, não explicitamente de gangues juvenis, mas de quaisquer grupos de jovens não anglo-saxões, erguendo barricadas em praças populares e controlando o fluxo, criando barreiras vigiadas entre bairros pobres e outras zonas da cidade. Flusty teme que a escalada desse processo leve a barreiras físicas permanentemente policiadas, com câmeras, sensores de movimento e vigilância aérea. Os recursos para isso já existem, a questão agora é política. E isso acontece também em outras cidades norte-americanas e britânicas.

Há soluções para melhorar a privacidade. Na Holanda, criaram um sistema chamado PrivaCam, que divide o fluxo dos dados digitais de imagem das câmeras de vigilância em diversos pacotes. Se alguém conseguir acesso a um desses pacotes, não terá como ver a imagem. As chaves para reunir os pacotes são distribuídas por órgãos e autoridades, como policiais ou juízes, que têm de concordar em reunir as informações

para ter acesso à imagens, garantindo assim seu uso apenas para as finalidades previstas na legislação.

No caso específico da Inglaterra, Norris e Armstrong argumentam que diversos motivos conduzem a uma disseminação cada vez maior das câmeras de vigilância na Inglaterra: (1) o discurso favorável na mídia, que iguala vigilância a segurança; (2) a ocorrência de crimes, em maior grau que antes ou não, em áreas sem câmeras, é vista como decorrente dessa falta de vigilância, e gera uma demanda por sua instalação; (3) a questão da importância relativa, de não ser considerado um distrito ou cidade de menos importância. Se outros locais ‘ganham’ câmeras, porque não temos câmeras aqui? (4) mesmo sem apresentar resultados expressivos na redução de crimes, os sistemas de CCTV podem ser muito úteis na investigação de crimes raros, mas sérios, como terrorismo, assassinato e estupro. As recentes explosões no metrô londrino estimulam esse aspecto. Mesmo que seja demorado e caro examinar milhares de gravações, se houver alguma identificação como resultado, o saldo é positivo para o sistema; (5) são uma ferramenta para melhorar a presença da polícia nos locais onde ocorrem distúrbios, otimizando a distribuição de recursos.

Por esses motivos, Graham sugere que o sistema de CCTV vai tornar-se o quinto serviço público na Inglaterra. No século 19, as redes de água, esgotos, energia e telégrafo surgiram lentamente, sem padronização, foram aos poucos se espalhando, sendo padronizadas, regulamentadas, até serem de uso de todos. Atualmente, os serviços de água e esgoto, gás, eletricidade e comunicação são comuns a todos e pode ser que em vinte anos ou menos, os sistemas de CCTV sejam encarados da mesma forma que os demais serviços, mais uma rede de utilidade pública.

A integração dos sistemas de vigilância está em progresso, incorporando diferentes sistemas, padronizando as tecnologias, trazendo economia de escala e centralização da vigilância. Não é simples, pois há sistemas públicos e outros privados, câmeras de diferentes resoluções, períodos de operação diferentes (em alguns locais são 8 horas por dia, em outros chegam a 24 horas), sistemas em tempo real e outros multiplexados. É necessário definir claramente critérios, procedimentos e providências, em função do que é observado. E também é importante realizar um treinamento adequado dos operadores, geralmente pessoal não muito qualificado profissionalmente,

executando um trabalho repetitivo e com conflitos de autoridade entre operadores civis e policiais que eventualmente atuam nas centrais de monitoração.

A identificação dos observados ainda ocorre em poucos casos, mas a implantação de sistemas de reconhecimento facial está a caminho e a integração com bancos de dados de criminosos registrados fará com que cada vez mais a identidade dos enquadrados pelas câmeras seja registrada. Quando a automação do sistema alcançar um grau de sofisticação que permita uma documentação efetiva da vigilância, um acompanhamento dos observados, o uso de algoritmos estatísticos, e até uma dispensa da maioria dos operadores humanos, aí estará implantada, ao menos na Inglaterra, uma sociedade de vigilância total, um cenário por enquanto apenas presente na imaginação distópica da ficção científica.

Reconhecimento facial

Existem mais de 130 tipos de biometria, sendo impressão digital, face e íris as mais conhecidas. Há testes de reconhecimento de indivíduos através de voz, cabelo, unhas, formato das orelhas, DNA, cheiro e até dinâmica datilográfica (como as pessoas digitam) e estão todas em evolução, mas atualmente as mais viáveis são a impressão digital e o reconhecimento facial, que exigem relativamente pouca infra-estrutura.

Um dos primeiros exemplos de uso de biometria é registrado pelo explorador português João de Barros, na China no século 14, onde os mercadores marcavam em papel as impressões de palmas de mãos e pés das crianças para distingui-las.

A impressão digital, depois de um início de desconfiança, revelou-se um sistema prático e eficiente, mas foi a tecnologia digital (como a do sistema Afis) que a tornou rápida. Mas tem falhas, como em pessoas com febre do feno, feridas ou calos nos dedos.

A fotografia percorreu um longo caminho até os sistemas de reconhecimento facial, que ainda não são tão precisos quanto a impressão digital.

O reconhecimento por meio da íris é o mais eficaz, mas os equipamentos ainda são caros e considerados, pelos clientes, como “invasivos”. Empresas ainda enfrentam resistência do mercado por exigirem a predisposição do usuário de oferecer os olhos

para averiguação. Já o reconhecimento de face é praticamente imperceptível, pois câmeras em locais estratégicos verificam quem se aproxima do caixa eletrônico ou da entrada de um prédio.

Um artigo publicado no *New York Times* de 16 de setembro de 2001 descreve uma visão do futuro “no Admirável mundo novo da Fortaleza de Nova York” (Barstow, 2001). Um caro porém seguro sistema de câmeras instaladas em cada cruzamento da cidade, todas conectadas a um sistema de reconhecimento facial para identificar os indivíduos nas ruas. A identificação facial foi a tecnologia favorita dos nove especialistas em segurança e terrorismo entrevistados (Gates).

Em 17 de setembro de 2001 a Visionics Corporation, a empresa líder em tecnologia de reconhecimento facial teve a sexta ação mais bem cotada na classificação da CNBC. Um grande avanço para uma empresa cujo primeiro produto, o FaceIt®, era facilmente confundido por mudanças de iluminação, ângulo da câmera, barba, mudança de peso e outras pequenas mudanças na aparência facial. Mas em 24 de setembro de 2001 a Visionics publicou um artigo chamado: “Protegendo a civilização das faces do terror: um avanço no papel que as tecnologias de reconhecimento facial podem desempenhar no aumento da segurança de aeroportos”⁴², que afirma que o FaceIt pode localizar suspeitos de terrorismo sem infringir os direitos à privacidade. O documento defende que as empresas, e não o Estado, são as principais responsáveis por proteger o país do terrorismo, mas em parceria com o Estado. É uma discussão entre segurança e privacidade, e a privacidade está perdendo tanto sua defesa na mídia de massa quanto no Congresso norte-americano.

Segundo a Visionics, câmeras nos aeroportos capturam imagens dos passageiros, passando em acessos individuais ou na multidão, e as imagens digitalizadas são convertidas em um código matemático que as representa. Em alguns segundos os códigos são enviados via Internet a um banco de dados de terroristas e suspeitos de crimes. Embora com uma margem de erro, quando o sistema encontra uma combinação, informa ao agente de segurança mais próximo. A tendência é que os sistemas fiquem mais sofisticados e precisos, mas até lá há uma grande chance de falsas indicações de

⁴² <http://www.visionics.com/newsroom/downloads/whitepapers/counterterrorism.pdf>

suspeitos. Mesmo que o sistema tivesse 99% de precisão, o número de falsos positivos seria imenso.

No Brasil, caixas eletrônicos da Caixa Econômica Federal, Banco do Brasil e Itaú já estão sendo equipados com tecnologia de reconhecimento de íris e de face, e o Congresso Nacional usa a impressão digital para votações, o Supremo Tribunal Federal, para acesso a ações sigilosas e processos, o Hospital Albert Einstein e Petrobrás para acesso aos prédios. O Restaurante popular da prefeitura de Curitiba, cadastrou os usuários carentes (é preciso comprovar baixa renda para ter o direito de almoçar por R\$ 1) que para entrar no restaurante têm de passar o dedo polegar num leitor óptico, que automaticamente reconhece as digitais e libera ou não a catraca, para evitar fraudes.⁴³

A empresa Global e-Secure, de tecnologia de reconhecimento aplicada, tem no reconhecimento de face seu principal campo de atuação. A imagem compara 32 pontos de identificação no rosto e gera um código digital que compara as informações com um banco de dados, e se não houver um impedimento, libera o acesso. Como avalia a estrutura óssea, não é afetada por envelhecimento, barba ou bigode. Um de seus projetos atuais, em parceria com a Itaotec, é o uso da biometria para emissão de passaportes.⁴⁴

Com 32 pontos de identificação, ainda há falhas, mas um equipamento de nova geração (80 parâmetros) instalado no final de 2003 no aeroporto internacional da Islândia, deverá produzir resultados melhores. No aeroporto de Dubai está sendo testado um sistema que, em um segundo, coleta 1.700 pontos de referência no rosto e pesquisa um banco de dados de cem mil imagens.⁴⁵

Em maio de 2004, no Congresso e Exposição de Tecnologia da Informação das Instituições Financeiras (CIAB), em São Paulo, três empresas (DBA, Politec e Itaotec-Philco) apresentaram produtos de reconhecimento de íris, impressões digitais e geometria da face.⁴⁶

A DBA, apresentou o Zyt, criado pela Tauá Biomática, com menos de 300 gramas, combinando biometria (leitor de impressões digitais) com certificação digital e

⁴³ *Frequêntadores aprovam refeição a R\$ 1*. Gazeta do Povo, Curitiba, 17 ago. 2005.

⁴⁴ O GLOBO, Informática etc., 13 out. 2003.

⁴⁵ Segurança para um bilhão, n'O GLOBO, 18 jan. 2004.

⁴⁶ O GLOBO, Informática etc., 7 jun. 2004

cartão inteligente. O hardware criptográfico, que elimina o uso de senhas e opera em Linux, tem um visor de cristal líquido que permite ao usuário acompanhar toda a operação, seja um depósito bancário ou uma transferência de valores e permite a assinatura de documentos, imagens, contratos de câmbio, qualquer aplicação do governo, qualquer transação que exija alta segurança. Estão estudando um Zyt doméstico, para acesso a bancos via Internet.

A Politec demonstrou o Identity Management, capaz de captar a imagem da íris em uma distância de até 53cm. É muito segura pois a chance de duas íris serem iguais é de uma em 10^{18} . Mas ainda é uma tecnologia muito cara. Nos EUA, adotam esse produto o Departamento de Estado, o Exército, a Marinha e o Children National Medical Center.

A Itaotec-Philco apresentou um sistema de identificação facial que usa 32 pontos de identificação.

Na Colômbia, mais de 1,5 milhão de correntistas de bancos usam autenticação facial para acesso a caixas eletrônicos. Além disso, a técnica foi adotada pelas Forças Armadas Colombianas.

Na Torre do Rio Sul, no Rio de Janeiro, mais de 110 mil pessoas tiveram seus rostos devidamente analisados e cadastrados pelo sistema Lobby Watch, da Cognitec⁴⁷. É um sistema que analisa os olhos e em seguida vários pontos na face. O sistema identificou um rapaz que foi apanhado em flagrante pichando os corredores e outro que roubava os sprinklers dos corredores para vender em uma loja do próprio shopping.

Na Alemanha (sede da Cognitec) ele é usado no controle de acesso em usinas nucleares, e no aeroporto de Sydney, Austrália, na conferência de passaportes.

Outros mercados são os condomínios residenciais e as empresas. Permite cadastrar moradores, funcionários, entregadores. Segundo a Cognitec para um prédio residencial, o preço do contrato de prestação de serviços é de cerca de R\$ 1.200 mensais (em 2005).

O futuro da biometria é tridimensional. Hoje, ela ainda é bidimensional, trabalhando com uma foto plana, porque 99% dos cadastros internacionais são em duas

⁴⁷ O GLOBO, Informática etc, 28 fev. 2005

dimensões. Já existem empresas que trabalham com imagens tridimensionais, mas os equipamentos que geram tais imagens ainda são muito caros. Quando essa tecnologia for acessível, o reconhecimento facial será preciso, usando mais pontos e sem problemas causados pela iluminação na foto.

Raios X de baixa potência: Vigilância muito pessoal⁴⁸

Uma das tecnologias mais controversas em estudo para implantação pela Administração de Segurança de Transporte (TSA) dos EUA é *backscatter body scanner*, que emite raios X de baixa potência através das roupas das pessoas e permite gerar uma imagem muito explícita do corpo e de objetos sob as roupas.

Estão implantando algumas máquinas para avaliação, e há uma solução para seu uso que equilibra segurança e privacidade, um software de camuflagem (*cloaking*), que transforma as imagens explícitas em uma semelhante a um contorno do corpo feito com giz, mas identificando claramente objetos de plástico, cerâmica, metal e materiais biológicos. A empresa American Science and Engineering declara que seu software respeita os padrões de privacidade.

Em um teste no aeroporto internacional de Orlando, Flórida, em 2002, o scanner foi experimentado juntamente com outras tecnologias emergentes, mas a TSA informou que os dados não foram divulgados. De acordo com a empresa Rapiscan, mais de 90% dos revistados durante testes de seus equipamentos no Aeroporto de Heathrow, em Londres, Inglaterra, aprovaram o *backscatter scanner* numa pesquisa. Mas a União Americana de Liberdade Civil sustenta que mesmo imagens retocadas pelo software de camuflagem são muito invasivas.

A finalidade do *backscatter body scanner* é detectar objetos metálicos e não-metálicos, ou seja, bem mais avançado que os detectores de metal existentes em quase todos os aeroportos. Mas Bob Postle, da American Science and Engineering, afirmou que o software poderia comprometer a eficácia na detecção de imagens, pois detalhes importantes poderiam ser perdidos.

⁴⁸ CONSIDINE, Austin, New York Times, *Entre a segurança e a privacidade do viajante*, n'º GLOBO, Boa Viagem, 24 nov. 2005

A BAA, empresa que administra sete aeroportos do Reino Unido, comprou três máquinas *backscatter* da Rapiscan em julho de 2005 para uso em Heathrow, e os equipamentos não utilizam o software de camuflagem. Embora o nível de radiação esteja conforme os padrões legais, crianças, dez vezes mais sensíveis à radiação que adultos, e mulheres grávidas, poderão apresentar problemas de saúde.

Este sistema é uma evolução dos sistemas convencionais de raios-X, usados em milhares de aeroportos para procurar objetos suspeitos nas bagagens. Mas em última instância tudo depende da vigilância humana, e uma falta de atenção, bastante provável nesta tarefa repetitiva, pode provocar falhas. Na Inglaterra as máquinas de raios X incluem um programa de computador conhecido como TIP (Projeção de Imagem de Ameaça), que exhibe, aleatoriamente, a imagem de algum objeto “ameaçador”, como uma arma ou faca, para testar a vigilância do agente.⁴⁹

Há outros sistemas em uso, não tão sofisticados quanto o *backscatter body scanner*, como a fotografia térmica, já em uso em aeroportos da Ásia e do Oriente Médio. O equipamento consiste numa câmera de raios infravermelhos que detecta a mais sutil elevação de temperatura no corpo humano. Desenvolvida pela empresa inglesa Land Instruments, está sendo vendido como meio de flagrar terroristas acometidos de transpiração nervosa. Ou seja, tecnologias mais sofisticadas buscam simplificar a operação, permitindo que operadores com pouco treinamento sejam eficientes em tarefas que até pouco tempo exigiam pessoal com ampla experiência.

Sistemas biométricos nos EUA

Para tentar impedir a entrada de criminosos e terroristas nos EUA, e melhorar a aplicação de leis de imigração, o governo dos EUA criou, nos últimos anos, enormes bancos de dados digitais de dados biométricos para identificar mais de 45 milhões de estrangeiros. As agências federais reuniram dados sobre mais de 70 milhões de americanos, num esforço para agilizar procedimentos legais em fronteiras e procurar terroristas internos.⁵⁰

⁴⁹ *Segurança para um bilhão*, n' O GLOBO, 18 jan. 2004.

⁵⁰ LIPTON, Eric, New York Times, *Uma obscura ciência a serviço da guerra contra o terrorismo*, n' O

O controle de imigração e a campanha contra o terrorismo foram estimulados pelos atentados de 11 de setembro de 2001 e por subsequentes medidas aprovadas pelo Congresso para melhorar a segurança no país. Mas o esforço ficou aquém de seus objetivos, provocando críticas de que o governo está comprometido com uma solução tecnológica tão ambiciosa, que nunca funcionará, a não ser a um preço inaceitavelmente alto.

Defendendo sua atuação, o Departamento de Segurança Interna cita as prisões nas fronteiras. Com o novo sistema os agentes da Patrulha de Fronteira podem verificar rapidamente as impressões digitais de cada estrangeiro detido. Em 2004 foram identificadas 437 pessoas procuradas por homicídio, 579 por agressões sexuais e mais de 18 mil por envolvimento em roubos, drogas, seqüestros e assaltos.

Os EUA têm diversos programas de identificação por biometria, implantados em 207 postos de processamento de visto do Departamento de Estado em todo o mundo. Desde o final de 2004, quase todos que solicitam visto deixam impressões digitais e foto, cujas cópias são enviadas ao Departamento de Segurança Interna, em Washington, que as compara com dados de cerca de cinco milhões de pessoas, na maioria criminosos, que podem ter o visto negado. As características de alguns desses programas são:

O Programa de Diversidade de vistos dos EUA oferece vistos anualmente por um sorteio entre pessoas de países com baixas taxas de emigração para os EUA. Candidatos recusados tentam burlar o sistema pedindo novos vistos com um novo nome e mudanças de aparência. O programa utiliza um novo software de reconhecimento facial para identificar, entre milhões de requerentes, os que o requerem mais de uma vez. Uma mulher russa foi apanhada pelo programa tentando disfarçar-se com pelo menos 12 penteados diferentes na tentativa de entrar nos EUA. 5731 pessoas não conseguiram visto depois que o software de reconhecimento facial revelou algum tipo de trapaça.

Os Vistos Biométricos são um novo sistema de vistos para estrangeiros, cujas impressões digitais são armazenadas digitalmente e fotografias tiradas no país de origem são comparadas com o candidato. Em menos de um ano o sistema verificou sete milhões de impressões digitais, e mais de 8500 foram barradas na lista do sistema.

O Cartão para Cruzar a Fronteira é emitido para alguns cidadãos mexicanos, e permite sua estada por um período em uma área limitada dos EUA. Tem impressão digital e foto registradas digitalmente. Ainda são muito fraudados por falta de equipamentos pois os funcionários de postos de fronteiras dispõem apenas de uma foto de tamanho médio, e não de uma análise biométrica em computador que poderia determinar com segurança se o portador do passaporte é seu proprietário legal.

O Gerenciamento do Sistema de Imagens de Registros de Passaportes é um arquivo digital com 70 milhões de pedidos de passaportes americanos e fotografias, a partir de 1994. Embora a foto seja digitalizada o arquivo ainda não é usado como um sistema biométrico. Como vários órgãos têm acesso ao arquivo, é uma preocupação quanto à privacidade dos indivíduos.

O Passaporte Eletrônico tem um chip RFID com imagens digitais e dados biométricos do proprietário. Nos postos de fronteira é lido via rádio, ou seja, não tem de ser formalmente apresentado. Como as fotos não têm alta qualidade, ainda não são usados para confirmação de identidade.

O US-Visit é a maior e mais cara iniciativa (já consumiu US\$ 1 bilhão e o custo total pode passar de US\$ 10 bilhões), para rastrear a entrada e saída de todos os visitantes estrangeiros. Nos aeroportos e nos principais portos são tiradas fotos e impressões digitais digitalizadas para confirmação de identidade. Mas a maioria dos que entram por fronteiras terrestres é isento da verificação. Assim, menos de um quarto dos visitantes é verificado na entrada, e ainda menos na saída.

Nos postos de fronteira há uma verificação de impressão digital, comparadas com uma base de dados do FBI de 47 milhões de impressões, para saber se há um registro criminal. Isso aumentou em sete vezes a chance de identificar alguém fichado. O uso do reconhecimento facial na fronteira do México, “apanhou” 490 mil pessoas em 2004.

Está em uso um protótipo do Cartão de identificação do trabalhador em transportes, que é um cartão biométrico de controle de entrada de mais de 12 milhões de trabalhadores de transporte aéreo, portuário, ferroviário ou rodoviário. Tem impressão digital e foto digitalizadas mas pode incluir geometria da mão e registro da íris. Com

implantação atrasada, é criticado pois as verificações de dados do passado podem custar o emprego do trabalhador.

O Viajante Registrado é um programa piloto que envolvia 12 mil pessoas em 2005. Busca acelerar a verificação de segurança em aeroportos. A identidade é confirmada por impressão digital ou íris. Mas não elimina a verificação por detectores de metal nem da bagagem por raios-X.

Sigilo telefônico⁵¹

Com o sistema de telefonia analógica, a única maneira de espionar ligações telefônicas era fazendo uma ligação física na linha do telefone, em qualquer ponto entre a central telefônica e a tomada do aparelho, para ouvir ou gravar os sons.

Já com a telefonia digital, fixa ou móvel, as centrais telefônicas se transformam em centros de redirecionamento de pacotes de dados, e há eficientes ferramentas para a quebra de sigilo telefônico, seja por demandas judiciais ou por investigações não oficiais.

Embora seja possível, mas muito caro, registrar o conteúdo das ligações, não é difícil registrar os dados sobre elas, ou seja, qual número ligou para qual número, e realizar pesquisas nesses bancos de dados de ligações, descobrindo quantas ligações houve para determinado número, quem telefonou em determinado período.

A reportagem “No rastro dos celulares do terror”, de Don Van Natta Jr e Desmond Butler, do New York Times, publicada em O GLOBO, em 5 de março de 2004, conta como uma investigação de terrorismo, iniciada em abril de 2002, acabou chegando a células de terror em três continentes. Por dois anos, as autoridades européias rastrearam as conversas e os movimentos de vários líderes e dezenas de agentes da al-Qaeda após descobrirem que eles preferiam chips de telefone celular pré-pagos, fabricados pela empresa suíça Swisscom, que permitiam o uso em qualquer lugar do planeta e que acreditavam lhes garantir anonimidade. As autoridades acreditam que a Al-Qaeda já se deu conta de estava sendo monitorada por meio desses telefones.

⁵¹ MACHADO, André. *A TI por trás da quebra do sigilo telefônico*. n’O GLOBO, Informática etc., 7 nov. 2005.

A empresa Tecnológica, softwarehouse carioca com clientes na América Latina, EUA e Europa, desenvolveu um software de quebra de sigilo chamado Search.RA, que torna a pesquisa de registros de chamadas telefônicas mais acessível, pois é fácil de configurar e pode ser acessado via Internet, embora, normalmente, as ações decorrentes de solicitações jurídicas de quebra de sigilo telefônico sejam enviadas offline, por segurança). O Search.RA permite que a operadora ou escritório jurídico busque e encontre rapidamente a origem e o destino de chamadas telefônicas, num período de tempo que pode recuar em um ano ou mais, o que exige um grande espaço de armazenagem da ordem de terabytes (trilhões de bytes).

O foco do software é mais voltado para os departamentos de cobrança, facilitando a consulta das chamadas de voz, mensagens de texto e multimídia de cada telefone. Mas não é difícil que as operadoras armazenem, por exemplo, o conteúdo das mensagens de texto, os torpedos, que exigem muito pouco espaço.

A vigilância nos eletrodomésticos⁵²

Muitas copiadoras coloridas a laser têm uma programação que bloqueia a cópia de papel moeda, dos modelos de notas de diversos países, armazenados em sua memória, para não servir de instrumento de falsificação.

A Electronic Frontiers Foundation (EFF), grupo de defesa dos direitos civis, em San Francisco, Califórnia, descobriu que os minúsculos pontos deixados no papel por algumas impressoras coloridas são um código que identifica o dia, a hora e o código de série da impressora em que o documento foi impresso.

São pontos amarelos de menos de um milímetro de diâmetro, repetidos em cada página do documento, geralmente invisíveis a olho nu.

A Canon e a Xerox são alguns dos fabricantes que incluem esses códigos. A EFF divulga a lista dos fabricantes, no site www.eff.org/Privacy/printers/list.php.

A Xerox já admitira que mantinha uma parceria com o governo nesse sistema de rastreamento, mas assegurou que somente entidades ligadas ao Serviço Secreto

⁵² CANTERO, Natalia Martín, *A impressora está alerta*, n' O GLOBO, Informática etc. 24 de out. 2005.

poderiam decodificar a informação. Por sua vez, o Serviço Secreto garante que usa essa informação somente em investigações relacionadas a falsificações. Mas não há uma legislação específica que impeça que o governo use tais informações.

O argumento da EFF é que panfletos políticos ou religiosos podem necessitar do anonimato, e essa tecnologia afeta a privacidade.

Outras tecnologias de comunicação sem fio, como o Bluetooth, um protocolo presente em telefones celulares, câmeras digitais, computadores e acessórios, que também está sendo implementado em diversos eletrodomésticos, como fornos de microondas, refrigeradores, sistemas de refrigeração e calefação e outros, pode formar uma rede doméstica de informações, de curto alcance, integrada à Internet. Outro protocolo, o WiFi, também presente em computadores e acessórios, tem alcance de centenas de metros e pode ser facilmente implantado em diversos equipamentos eletrônicos que se deseje manter on-line, em redes sem fio, cada vez mais comuns em aeroportos, empresas e até em cidades inteiras, como uma opção mais barata de oferta de acesso à Internet, sem fio, em uma grande área.

Mas a maioria dessas redes não implementa mecanismos de segurança adequados, sendo fácil, apenas com um computador de mão, e uma antena, capturar senhas e outros dados em locais públicos ou no exterior de prédios que tenham redes sem fio internas. É uma questão de investir na segurança do sistema, em hardware e software, mas principalmente na educação do usuário. Não custa lembrar que a maioria das “infecções” por vírus na Internet são provocadas por programas anexos a e-mails, indevidamente executados pelos destinatários. Nas palavras do analista B. Piropo, “Não se deve abrir anexo a e-mail nem da própria mãe, se não o estiver aguardando naquele momento”.

E até o telefone celular convencional, sem chip GPI, pode ser um instrumento de vigilância. A MobileIN.com (www.mobilein.com/location_based_services.htm) informa que o celular atual já permite traçar um registro da movimentação com relativa precisão e os aparelhos futuros permitirão elevar essa precisão consideravelmente. Há empresas que oferecem serviços baseados em localização. Isso pode trazer vantagens em caso de um pedido de socorro. E há o marketing segmentado ao extremo, ao único consumidor,

pois o celular pode receber uma mensagem informando que a loja em frente à qual você está oferece uma promoção. Mas existe a hipótese de que os passos do indivíduo sejam permanentemente monitorados.⁵³

A falsa identidade

Há vários livros publicados nos EUA sobre como burlar o ‘sistema’ criando falsas identidades, falsos números de seguridade social, como proteger seus ativos financeiros de ações de ex-cônjuges, como criar uma nova identidade para obter crédito e fraudar as operadoras de cartão de crédito.

Em uma sociedade onde, principalmente nas pequenas cidades, os representantes do poder policial detêm um controle que muitas vezes ultrapassa os limites legais (nas grandes e médias cidades o cidadão geralmente tem a quem recorrer contra arbitrariedades), e onde os registros policiais por pequenos delitos, como o consumo de bebida alcoólica em público, com qualquer idade, ou em qualquer local, por menores de 21 anos, ou o excesso de velocidade no trânsito, acompanham as pessoas por toda a vida, podendo ser um entrave a uma oportunidade de emprego, e muitas pessoas têm apenas um prenome e um sobrenome, com grande número de homônimos, há um interesse por uma nova identidade, além, é claro, de quem não deseja cumprir obrigações legais de pagamento de impostos, pensões alimentícias ou dívidas.

Com a facilidade de obter cartões de crédito de centenas de instituições, usando seu nome completo, ou combinações do nome, ou até nomes falsos, desde que se construa um conjunto de informações pessoais aceitável, como endereço, linha telefônica fixa e, o mais importante, um número do seguro social (SSN), há várias publicações recentes sobre como construir uma falsa identidade, utilizando modelos de documentos, em livros ou na Internet, usando as regras de criação de números de registro do SSN e outros documentos, como as licenças de habilitação.

O importante é ter mais de um documento com a identidade falsa. Não basta o SSN. Se a pessoa muda para outro endereço, terá contas de serviços como telefonia,

⁵³ PIROPO, B, *Sistemas de localização: Big Brother?*, n’O GLOBO, 2 fev. 2004.

energia, e é natural que também tenha um cartão de biblioteca pública, fácil de obter também sem muita burocracia.

Com o custo de ser incluído em cadastros de mala direta, pode-se obter um cartão plástico de uma empresa de seguros, com um emblema da águia americana, nome e número de seguro social, simplesmente cadastrando-se com um número telefônico fixo, que pode ser obtido sem burocracia, um número de SSN que a própria pessoa forneceu. Uma maneira de criar um número válido é levantar dezenas ou centenas de registros de óbitos, que são documentos públicos, e usar as regras de numeração, publicadas em vários livros, para criar um número possível de SSN. Não se pode usar o número de alguém falecido porque eles são divulgados periodicamente às instituições financeiras, para evitar fraudes (Charrett).

Isso, naturalmente é um crime previsto na Lei do Seguro Social que, em uma emenda em 1981, na seção 208g, torna crime alterar, comprar, vender ou falsificar um cartão do seguro social e portar um cartão genuíno ou falsificado, com a intenção de vendê-lo ou alterá-lo, punido com multa de até 5 mil dólares e/ou até cinco anos de prisão. Em 1982, a Lei de Controle de Crimes de Identidade Falsa acrescentou ao capítulo 18 do Código Civil dos EUA a seção 1028, que prevê penas de não mais de cinco anos e/ou multas de até 25 mil dólares por crimes relativos à falsificação de documentos.

Um exemplo comum é a “Indústria de identidades falsas”⁵⁴ para estudantes driblarem a proibição de venda de bebidas alcoólicas a menores de 21 anos, nos EUA, que agora vem sendo muito atacada por ser uma arma para terroristas escaparem da vigilância policial. Os bares estão usando uma nova ferramenta contra identidades falsas, o scanner E-Seek, que diferencia uma identidade falsa de uma verdadeira rapidamente. Mas um aluno da Universidade de Colúmbia que diz ter forjado mais de 400 identidades, afirma que com uma boa impressora é possível driblar o sistema.

Com amostras de imagens em alta resolução de documentos oficiais de todos os estados americanos, disponíveis na Internet, e programas de computação gráfica, universitários estão forjando identidades com surpreendente qualidade, com

⁵⁴ ST. JOHN, Warren, *The New York Times*, n’O GLOBO, Magazine, 21 mar. 2005

hologramas, tintas especiais e dados codificados, que podem enganar a polícia e até modernos scanners. Em chats dedicados a identidades falsas, falsificadores compartilham informações sobre técnicas de falsificação e até vendem códigos de barras e hologramas. Já foi mais fácil falsificar passaportes, um documento muito utilizado por norte-americanos como identidade, mas os novos modelos que incluem até chips RFID são mais difíceis de falsificar.

Num país que não tem (ainda) um documento de identidade oficial e obrigatório, o governo vem aumentando a vigilância sobre as falsificações. A pena para posse e confecção de identidade falsa varia em cada estado. Em Nova York, a pena é de até sete anos. Mas geralmente a polícia quer é saber como o menor a conseguiu. Várias mudanças estão previstas para dificultar a falsificação, como adoção de marcas d'água e scanners mais sofisticados. E em breve o Senado votará um projeto de lei que determina que os estados padronizem os dados codificados no verso das carteiras, tornando mais fácil digitalizá-las.

No Brasil os novos passaportes também estão muito mais sofisticados, pois havia uma reclamação de diversos países do uso indevido de passaportes brasileiros, falsificados ou adulterados, pois nossa diversidade étnica não permite identificar um portador como não sendo brasileiro, com base apenas em suas características físicas. Um sueco normalmente tem traços físicos bem definidos e conhecidos em todo o mundo. Um asiático teria dificuldades de se passar por sueco, e vice-versa, mas qualquer um pode afirmar ser brasileiro. Mas os demais documentos em uso no Brasil, embora na maioria emitidos por órgãos do governo, não têm padronização, e os do mesmo órgão mudam de tempos em tempos, o que torna praticamente impossível detectar falsificações.

O GLOBO publicou, em 19 e 20 de setembro de 2004, duas matérias sobre os sistemas de identificação pessoal dos órgãos que, no Rio de Janeiro, emitiram a quase totalidade das carteiras nas últimas décadas, o Instituto Félix Pacheco e o Departamento de Trânsito (Detran).

“Falsidade autenticada”, de Vera Araújo, comenta que o traficante Elias Pereira da Silva, o Elias Maluco, que matou o jornalista Tim Lopes, terá que se explicar pelos

crimes de falsidade ideológica e uso de documento falso, pois em 12 de setembro de 2000, pediu a primeira via da carteira de identidade pelo novo sistema de identificação civil do Detran, usando uma falsa certidão de nascimento em nome de Lucas Santos Silva. Consultado pelo Detran, o Instituto Félix Pacheco (IFP) informou que não havia localizado identificações anteriores, autorizando o Detran a emitir a carteira, registrada sob o número 20.444.363-4. A matéria continua:

Preso em 2002, Elias foi levado para prestar depoimento no Fórum do Rio, onde foram tiradas novas digitais do bandido. O Detran descobriu que havia duas digitais iguais com nomes diferentes. Casos como este se tornaram cada vez mais comuns no Rio. O descaso de anos e anos de abandono das 15 milhões de fichas cadastrais de identificação civil do IFP se reflete nos 10.281 casos de duplicidade de registros civis — há casos de pessoas com até quatro números de carteira diferentes —, detectados pelo Detran no ano passado. Por conta dessas fraudes, o departamento exclui, em média, 28 registros de carteira por dia. (...) Fichas desaparecidas ou até destruídas pela chuva (até pouco tempo os arquivos ficavam embaixo de goteiras) fizeram com que o IFP perdesse parte do acervo e, em consequência, facilitasse a vida dos estelionatários. Munidos de falsas certidões, de nascimento ou casamento, os bandidos se aproveitam da confusão no IFP para conseguirem carteiras “quentes” sem anotações criminais, para circularem livremente. A partir dessa carteira de identidade, o criminoso tira documentos como passaporte, abre contas bancárias e usa cartão de crédito, todos com informações falsas, mas com as digitais verdadeiras. A credibilidade do sistema fica em xeque.

Há críticas ao sistema automático de identificação por impressão digital (Afis) não consegue fazer as leituras das digitais com precisão e ao fato de apenas 250 mil de quase 1 milhão de prontuários com informações criminais terem sido digitalizados pela polícia. O Detran declarou que o sistema vem se aperfeiçoando, que o ideal seria inserir as 15 milhões de fichas no novo banco de dados, mas isto teria um custo alto para o estado e acarretaria uma sobrecarga no sistema e que é cada vez mais difícil cometer fraudes. Um decreto do governo do Estado do Rio obriga os cartórios a informarem os nascimentos e óbitos, para atualizar os registros do novo sistema. E as novas carteiras são emitidas com código de barras no verso, dados criptografados e foto digitalizada.

A matéria seguinte, “Detran vai digitalizar 15 milhões de fichas”, também de Vera Araújo, retoma o assunto, informando que o Detran pretende digitar 15 milhões de fichas de identificação civil abandonadas no Instituto Félix Pacheco (IFP), mas sem previsão para o serviço ser concluído, e repete parte das informações da véspera.

A Internet: origens, evolução, situação atual

É importante conhecer o histórico da rápida evolução da rede, para entender como alguns dos problemas de segurança que hoje nos afligem não foram imaginados na concepção original das redes que originaram a Internet, pois ela não foi pensada para fins comerciais e de uso generalizado, apesar de toda a experiência acumulada com a implantação da telegrafia e, depois, com a telefonia.

As origens das redes de computadores vêm dos esforços de Paul Baran e de Donald Davies, na década de 1960, que imaginaram um sistema de chaveamento de informações, Baran pensando na segurança em uma rede militar e Davies voltado para menor custo e mais confiabilidade em comunicações entre empresas. A intervenção do governo britânico no setor de computadores era encarada como um símbolo do compromisso do partido trabalhista com a modernização e propulsor do desenvolvimento econômico, enquanto que os EUA a capacitação tecnológica era uma arma na Guerra Fria e pesquisas na área de defesa eram generosamente financiadas por organizações como a Rand Corporation e a ARPA - Advanced Research Projects Agency (Abbate, 2000).

Em 1967, a aplicação prática dessas idéias era complicada pela incompatibilidade entre os diversos tipos de computadores existentes. Lawrence Roberts e outros cientistas trabalhando na criação da ARPANET, usaram o conceito de camadas, dividindo complexas tarefas de rede em módulos, e um gerenciamento descentralizado. No final de 1971 a maior parte da infra-estrutura da ARPANET estava implantada, com 15 locais interconectados, que podiam intercambiar pacotes de dados mas ainda não haviam implementado protocolos de rede e de servidores, nem as interfaces de hardware. Ainda não era possível um computador usar aplicativos em outro. Em outubro de 1972, na Primeira Conferência Internacional de Comunicação de Computadores, em Washington,

os esforços liderados por Robert Kahn e Lawrence Roberts permitiram que terminais se conectassem a computadores em outros estados e até em Paris. Isso aumentou o entusiasmo e estimulou empresas a oferecer serviços de redes comerciais de chaveamento de pacotes. Roberts saiu da ARPA para a presidência de uma dessas empresas, a Telenet que, em agosto de 1975 oferecia o serviço em sete cidades nos EUA.

O papel dos “consumidores” na ARPANET foi diferente do que geralmente acontece com a implantação de uma nova tecnologia, onde os usuários escolhem um produto ou serviço em detrimento de outros, ou criticam ou exigem alterações após a tecnologia estar razoavelmente disponível. Os pesquisadores que usavam a ARPANET estavam envolvidos diretamente em seu desenvolvimento (Abbate, 2000).

Sua participação, reclamações e sugestões moldaram os tipos de serviços que os usuários realmente necessitavam. E à medida que empresas e universidades conectavam-se à rede, geralmente qualquer um com uma conta válida tinha acesso a serviços de e-mail e FTP (transferência de arquivos) em toda a rede. Para simplificar o acesso, poucos administradores de sistemas implantaram restrições ou controles. Apesar da grande preocupação do Departamento de Defesa quanto a uso não autorizado de instalações governamentais, foi possível construir a ARPANET sem um complexo controle administrativo de acesso nem complexos procedimentos de conexão o que não permitia determinar quem estava usando a rede e para qual finalidade (Heart et al., 1978, citado por Abbate, 2000).

Mas o uso não era simples, não havia uma fonte centralizada de informações, obrigando os usuários a recorrer a outros sites para resolver problemas de conexão, o custo era alto se não se estivesse ligado a uma instituição de pesquisa ou educacional, a burocracia era complexa.

A ARPANET foi idealizada para interconectar computadores fisicamente distantes, mas a proliferação de redes locais, que interligavam computadores próximos, do mesmo fabricante, intensa nos anos 1980, foi a solução para interconectar computadores incompatíveis.

Em junho de 1973, um seminário na Universidade de Stanford discutiu o projeto da Internet, e seu protocolo host, o protocolo de controle de transmissão (TCP). A idéia era que o protocolo resolvesse os problemas de conflito de pacotes transmitidos e as incompatibilidades entre redes mais estáveis, como a ARPANET, por linhas telefônicas, e redes mais sujeitas a falhas, como a PRNET, que operava via rádio. O protocolo TCP seria responsável pelo tráfego de dados ordenado, sem erros, de um servidor para outro. Para conectar fisicamente as diversas redes locais, Vinton Cerf e Robert Kahn propuseram a criação de computadores host chamados de gateways, conectados a duas ou mais redes, para a transmissão dos pacotes de dados. Dentro de cada rede o servidor local cuidaria do tráfego dos pacotes, e o protocolo comum, o TCP, garantia que toda a inter-rede (internet) enxergaria o sistema de modo transparente, eliminando a necessidade de ter todo o hardware das redes compatível, o que permite a evolução tecnológica do sistema, sem afetar o tráfego de informações. Os gateways não seriam os únicos a ter de se preocupar com endereços em todo o sistema, cada endereço tem uma parte com o nome da rede e outra especificando o servidor na rede. Cada rede local cuidaria de encaminhar seus dados dentro da rede e de encaminhar para o gateway os pacotes com endereços fora da rede local.

Como os gateways usavam o protocolo TCP, eles desempenhavam funções de seqüenciamento, controle de fluxo e de erros, que eram também exercidas pelos servidores nas redes locais, o que tornava os gateways desnecessariamente complexos. A solução, proposta por Vint Cerf, Jon Postel e Danny Cohen, em janeiro de 1978, foi dividir o protocolo TCP em duas partes, um protocolo entre servidores (TCP) e um protocolo entre redes (IP). É o TCP/IP empregado atualmente na Internet. O IP cuida do tráfego de pacotes entre máquinas e o TCP da ordenação dos pacotes em conexões confiáveis entre servidores. Os gateways passam a executar apenas o IP e os servidores locais, o TCP. Embora atendesse às demandas dos militares de confiabilidade, compatibilidade com redes diversas e novas tecnologias, o TCP/IP, padronizado em 1980, refletia as idéias e interesses de uma comunidade internacional de pesquisadores em redes de comunicação.

Implementar eficazmente os protocolos foi uma tarefa de vários anos. Os servidores da ARPANET só implementaram integralmente o TCP/IP em janeiro de

1983, por interesse dos militares em que a Rede de Dados da Defesa operasse com a mesma linguagem.

Para permitir um roteamento entre redes locais, a Internet necessitava de um servidor de nomes, um banco de dados com os nomes de todos os servidores, que foi criado por um grande grupo de membros da ARPANET e começou a operar em julho de 1982 no Centro de Informações da Rede, que passou a ser conhecido como Sistema de Nomes de Domínio (DNS). Para evitar o envio periódico de listas atualizadas de domínios a todos os servidores, quando um servidor deseja acessar um domínio ele envia uma consulta a um dos servidores DNS com o nome do domínio e o DNS informa o endereço IP.

Quando se digita um endereço (URL) no navegador, usando os nomes, como “ufrj.br”, um sistema de banco de dados tem de informar qual o endereço numérico (algo como 200.255.127.102) daquele site. Os endereços numéricos seguem normas internacionais de distribuição, e tem de haver um órgão central para cuidar disso. Essa é a tarefa dos servidores DNS. Como a maioria das redes começou nos EUA, a maioria dos poucos servidores DNS do mundo está nos EUA. Mas isso gera muitas preocupações de segurança e facilidade de acesso. Esses servidores têm espelhos (cópias sempre atualizadas) espalhados pelo mundo, para agilizar o tráfego. Atualmente vários países estão rediscutindo essa localização desses servidores e solicitando que o controle seja dividido entre vários países.

Após converter a ARPANET para o TCP/IP, o DCA e a ARPA passaram à tarefa de dividir a ARPANET em duas redes separadas, a rede de pesquisa de defesa, ainda chamada de ARPANET, e uma rede militar, a MILNET, para proteção contra invasões por usuários não autorizados, possivelmente maliciosos, pois a disponibilidade de computadores e modems baratos tornaram a rede acessível a amadores (Harris et al, 1982, citado por Abbate, 2000). A ARPANET continuaria a ser usada no teste e desenvolvimento de novas tecnologias de rede, e a MILNET equiparia os sites com criptografia e outras medidas de proteção. A MILNET foi iniciada oficialmente em 4 de abril de 1983.

Com isso a ARPANET voltava a ser uma rede voltada para a pesquisa, dominada pelas universidades, o que facilitava a idéia de transferi-la para o controle civil. A segunda etapa era comercializar a tecnologia da Internet. A ARPA já havia financiado empresas para escrever implementações do TCP, principalmente para o sistema operacional UNIX. O coronel Heidi B. Heiden, ex-diretor de planejamento de comunicações do exército norte-americano, implantou um programa de financiamento de 20 milhões de dólares para que fabricantes de computadores implementassem o TCP/IP em suas máquinas. Em 1990 o protocolo estava disponível em praticamente todas as máquinas vendidas nos EUA.

Os computadores pessoais foram lançados nos anos 1970. Em 1977 estavam no mercado norte-americano o Apple II, o PET da Commodore e o TRS-80 da Tandy/Radio Shack. Em 1981 a IBM lançou seu PC. Com o aumento de computadores, o número de redes aumentou rapidamente.

Duas tecnologias auxiliaram o rápido crescimento do mercado de computação pessoal, o disquete de 5,25", em 1978, onde podia-se gravar programas e dados, sendo o Visicalc, a primeira planilha bem sucedida, um grande estimulador desse mercado, e as impressoras a laser, que entraram no mercado em 1977 e tiveram uma grande queda de preço e aumento de qualidade na década de 1980.

O crescimento da Internet na década de 1980 foi meteórico. No terceiro trimestre de 1985, cerca de 2 mil computadores tinham acesso à Internet. Quatro anos depois, eram 159 mil. Segundo a UIT, em 2004 havia 220 milhões de PCs nos EUA e 19 milhões no Brasil. O Brasil ocupava em 2004 a 10ª posição em usuários de Internet, 9º em número de PCs e 7º em servidores da Internet.

Entre 1988 e 1989, diversos sites da ARPA transferiram suas conexões de servidores para a NSFNET, a rede da Fundação Nacional para a Ciência (NSF), que tinha um hardware bem mais rápido e foi concebida pensando na Internet como ela é hoje. Em 28 de fevereiro de 1990 a ARPANET foi formalmente desativada, mas a maioria dos usuários nem percebeu, pois já haviam sido transferidos para novos servidores. A NSFNET foi crescendo e agregando vários provedores comerciais, e atendia aos sites de pesquisa e educação da NSF e também a clientes comerciais.

Como o tráfego comercial ainda era proibido na NSFNET, várias empresas, principalmente as operadoras de telefonia, como MCI, AT&T e Sprint, expandiram suas operações e começaram a oferecer serviços comerciais de Internet em todo o território dos EUA. Para ampliar a oferta de serviços comerciais, três provedores, PSINet, CERFNet e Altnet, formaram em 1991 uma organização sem fins lucrativos, a Commercial Internet Exchange (CIX) que interligou suas três redes e distribuía gratuitamente o tráfego de dados de qualquer outra rede associada. Isso agregou valor aos serviços e teve a adesão de empresas de vários países.

Essa rápida expansão da infra-estrutura permitiu à NSF implementar, em 1994, um Plano de Desenvolvimento de Projetos, segundo o qual os serviços de Internet seriam assumidos pelos provedores e eventualmente a infra-estrutura da NSFNET seria desativada. Em 30 de abril de 1995 a MERIT encerrou formalmente a rede NSFNET, encerrando a propriedade do governo dos EUA sobre a infra-estrutura da Internet.

A privatização ampliou rapidamente o crescimento da rede, a adoção de sistemas para compatibilizar as diversas redes usando o mesmo protocolo, o TCP/IP, o que permitiu que Berners-Lee e sua equipe desenvolvessem o protocolo de transferência de hipertexto (HTTP) compatível com os diversos serviços oferecidos, como FTP, e-mail, gopher e WAIS, e criaram o URL (localizador de recursos uniforme), um sistema de endereçamento que identifica diversos protocolos, não apenas o HTTP, mas também FTP, gopher, WAIS e Usenet (servidores de notícias). Já em dezembro de 1990 o software da World Wide Web (teia mundial) começou a operar no CERN. Com a privatização da Internet e a difusão dos computadores pessoais, seu uso se multiplicou, criando a Internet audiovisual atual.

O artigo “As novas fronteiras da Internet”, publicado no suplemento *The Economist* do jornal Valor Econômico em 14 de agosto de 2001, discutia do ponto de vista legal a localização física dos servidores da Internet, pois se uma atividade ou site não é permitido em um país, pode-se instalá-lo em um servidor em outro país. E mesmo sem restrições legais, as empresas de mercado global têm interesse em disseminar seus dados pelo mundo, para facilitar o acesso dos usuários. Para isso armazenam cópias de seu conteúdo mais procurado em caches (servidores intermediários de acesso rápido) de dados espalhados pelo mundo. A líder neste campo, em 2001, com mais de 11 mil

servidores em 62 países, era a Akamai, de Cambridge, Massachusetts. A distribuição geográfica dos servidores da Akamai abrangia todo o mundo. A matéria detalha:

Os clientes da Akamai, entre os quais a CNN e o Yahoo!, são provedores de conteúdo preparados para pagar para garantir, a usuários no mundo inteiro, a capacidade de acesso fácil e rápido aos seus sites. Quando você visita um servidor da Web, normalmente recebe, através da rede, uma descrição da página que solicitou. Esta consiste no texto da página e referências a qualquer recurso gráfico (ou sonoro, ou clipes de filmes) a ela associados. Esses itens são, então, solicitados pelo seu navegador e entregues através da rede. Finalmente, o navegador reúne todos os componentes e exibe a página. O problema é que, enquanto o texto pode ser mostrado rapidamente, os itens “pesados” (como imagens e vídeo) são muito maiores e demoram mais para chegar. São esses os itens que a Akamai pode ajudar a entregar com maior rapidez.

Você solicita uma página da Web e a descrição da página é mostrada. Mas as referências aos itens “pesados” da página são modificadas, para levar seu navegador a solicitar aqueles itens aos servidores da Akamai, em vez do servidor original. A Akamai, levando em conta sua localização na rede e as condições de tráfego predominantes, entrega os itens pesados do cache disponível mais próximo e a página chega a você muito mais depressa. Monitorando a demanda para cada item e colocando mais cópias à disposição em seus caches quando sobe a demanda e menos, quando a demanda cai, a rede da Akamai pode ajudar a eliminar grandes flutuações no tráfego. Outro benefício é que o servidor do cliente não precisa entregar os itens pesados, fato que reduz drasticamente sua carga e reduz a probabilidade de colapso diante de um aumento súbito no número de visitantes.

Paralelamente a este esforço para ocultar a localização física de dados na Internet, há um crescente interesse em determinar a localização dos seus usuários, tanto para oferecer produtos em qualquer país quanto para identificar potenciais consumidores. Leis e regimes fiscais se baseiam em geografia, não na topologia da rede.

O aumento do interesse por serviços de “geolocalização”, que procuram identificar as localizações de usuários da Internet com base em seus endereços na rede, também sinaliza a compreensão de que técnicas tradicionais de marketing, baseadas em geografia, também podem ser aplicadas on-line, pois o marketing tradicionalmente é feito em bases geográficas. Isso permite oferecer a diferentes visitantes de um site na Web, produtos diferentes ou artigos especiais, dependendo da sua disponibilidade nas proximidades.

O serviço de geolocalização da Quova, denominado GeoPoint, baseia-se num banco de dados continuamente atualizado, que associa endereços de protocolo da Internet a países, cidades e até mesmo códigos postais. Ao visitar um site na Web equipado com software GeoPoint, seu endereço IP é transmitido a servidores da Quova, que determinam sua localização geográfica. Esta informação é então usada para modificar o conteúdo da página com base na sua localização física. A Quova afirma ser capaz de identificar o país de origem dos usuários da Web com 98% de precisão e a cidade de origem (ao menos, para usuários nos EUA) em 85% dos casos. Outras empresas, como Akamai, Digital Envoy, InfoSplit e NetGeo, oferecem serviços semelhantes.

Conhecida a localização do usuário, bases de dados demográficos existentes, que vêm sendo aprimoradas ao longo dos anos, para revelar quais espécies de pessoas vivem em quais lugares, podem entrar em ação. Mas, embora a propaganda direcionada seja a aplicação mais óbvia do sistema, a geolocalização tem muitos outros usos. Pode ser usada, por exemplo, para determinar o idioma no qual, em certo momento, um site poliglota na Web deve ser apresentado. Os comerciantes e as casas de leilões on-line podem usar a geolocalização para impedir a venda de bens que são ilegais em certos países; os cassinos on-line podem impedir o acesso de usuários de países nos quais o jogo on-line é proibido; as políticas de administração de direitos autorais para transmissões musicais ou em vídeo, que tendem a ser baseadas em territórios geográficos, também podem ser impostas. As indústrias farmacêutica e de serviços financeiros, que estão sujeitas a severas regulamentações nacionais, podem confiar que estão dentro da lei quando oferecem bens e serviços on-line. Assim, as fronteiras estão de volta à Internet.

O novo protocolo IPv6

Atualmente tudo o que circula pela Internet é “controlado” por um protocolo de comunicação chamado IP (Protocolo Internet), que está na versão 4. Ele usa um endereço composto (rede e usuário) com 32 bits. Embora teoricamente possam existir 2^{32} (mais de 4 bilhões) endereços, nem todos os endereços de usuário são utilizados em cada rede e o limite real é muito menor. O crescimento da Internet, de redes, hosts e usuários, e a sofisticação dos serviços, levou a um novo padrão, que está começando a ser implantado, ainda sem prazos determinados, a versão 6, ou IPv6.

Ele busca aprimorar a escalabilidade (aumentando o número de endereços de 32 para 128 bits, um número tão grande, 3×10^{38} , que permite, na pior hipótese, 1564 endereços por cada metro quadrado na superfície da Terra); facilitar a administração (simplificando o cabeçalho); reduzir as tabelas de roteamento (no IPv4 um roteador tem de ter uma tabela com uma rota para cada rede separada, no IPv6 não há uma noção de classes, o que simplifica o roteamento); aumentar a qualidade (para ter mais controle sobre fluxos de vídeo, para garantir que cheguem ao destino) e ampliar a segurança (autenticação e privacidade, com criptografia de todo o pacote de dados, inclusive do cabeçalho, o que impede a fácil obtenção de informações por interceptação do fluxo de dados e garante que só o destinatário terá acesso, e a capacidade de determinar se os dados foram modificados).

O papel do usuário conectado: a experiência da Wired

Existem diversas revistas sobre as novas tecnologias, publicadas durante mais de dez anos, inicialmente voltadas para um público mais técnico e depois, gradativamente, tornando-se menos analíticas e mais divulgadoras dos novos lançamentos, como a PC Plus inglesa, a PC Magazine norte-americana, Byte e várias outras, muitas das quais publicadas também no Brasil. Também há muitos suplementos de informática nos principais jornais impressos no Brasil, como o Jornal do Brasil, o Globo, Folha de São Paulo, Estado de São Paulo e outros, e publicações derivadas de outras, como a Exame informática, da Editora Abril. Entre todas essas, destacou-se uma das principais publicações sobre informática, Internet, comunidades virtuais, e que manteve durante vários anos uma discussão atualizada e politizada sobre a influência do ciberespaço na vida diária, e que discutiu de forma original, com base no direito à privacidade, proporcionado pela criptografia, a questão da identidade do indivíduo on-line e sua influência no mundo “real”, a revista *Wired*.

Lançada em janeiro de 1993 pela Wired Ventures, foi fundada por Louis Rossetto e Jane Metcalfe em outubro de 1992 (Frau-Meigs). Em outubro de 1994 foi lançada a versão on-line, a *HotWired Network*. A partir de maio de 1998 a revista passou a ser publicada pela Conde Nast e tornou-se mais comercial e menos política. Até então, a

revista (vendida também em bancas no centro do Rio de Janeiro) destacava-se por apresentar um design moderno, com cores chapadas, indicações de hyperlinks como no layout usado nos navegadores, anúncios inovadores e com forte presença de aparatos tecnológicos, e discussões aprofundadas sobre questões sociais decorrentes da era da informação. Os editores e articulistas buscavam tornar real a utopia virtual da tecnodemocracia. Nas palavras de Frau-Meigs:

A nova realidade buscada pelos editores da Wired organizava-se ao redor de duas noções, explícita ou implicitamente apresentadas, na ampla maioria das edições: ‘identidade’ e ‘comunidade’. Eles tentavam descrever uma identidade política e psicológica a ser adquirida, supondo que era possível derrubar as barreiras físicas, pelo uso da comunicação como ciência, como técnica e como meta final. Esta percepção da identidade foi primeiramente expressa e veio a florescer nas comunidades virtuais. Nesse contexto, desenvolveu-se a visão dos editores de Wired da relação entre a esfera privada e a pública, entre a privacidade e a visibilidade política. Seu discurso vinha da linguagem da democracia e da sociedade civil clássica. Mas a apresentação formal da revista, sua natureza altamente promocional, e sua visão do mundo, cujos elementos eram aparentes na demorada polêmica sobre criptografia e seu controle, revelam o desejo de tornar o modelo mercantil mais socialmente aceito. Essa aceitabilidade social é planejada utilizando a comunicação como interface.

Na década de 1990, quando os Estados Unidos discutiam a crise no sistema de saúde pública, violência urbana, desigualdades sociais, a politização do fundamentalismo religioso, a revista tinha um otimismo e um discurso de mudança e revolução, o que ocorreu no final da década, exceto pela “bolha” das empresas pontocom. A revista era voltada para a nova geração digital. Nicholas Negroponte, do MIT, autor de *Being Digital (A Vida Digital)*, lançado em 1995, onde ele comenta de forma bastante otimista sobre a presença cada vez maior da tecnologia digital na vida diária, nas comunicações, no ambiente de trabalho, na automação dos eletrodomésticos, na conversão de conteúdo físico (livros, fitas, discos) para digital, ou, como ele expressa, de átomos para bytes, da praticidade do e-mail, e isso em uma época sem celulares digitais nem acesso em banda larga à Internet, tinha uma coluna na Wired. Em 1995 ele declarou que uma identidade digital era uma licença para crescer. Muitas das definições de identidade virtual na revista tendiam a demonstrar que a identidade era

ligada ao cérebro, não ao resto do corpo, e que o computador e o cérebro eram duas entidades complementares. Steven Levy⁵⁵ escreveu que uma verdadeira *persona* digital é uma identidade permanentemente dissociada de seu corpo físico.

Dependendo de sua relação com o ciberespaço, desenvolve-se uma ambigüidade na relações do indivíduo com os outros, em função da interface empregada. A revista e seus articulistas, a grande maioria da Califórnia, onde a revista era editada, acabaram criando uma visão muito auto-centrada do mundo. E tinha uma postura muito crítica da mídia de massa, que era, e ainda é, aquela à qual a grande maioria das pessoas tem acesso. Mesmo agora, em 2005, a porcentagem da população com acesso regular ao ciberespaço é muito reduzida fora do “mundo desenvolvido”.

O historiador Mark Poster sugeriu uma nova abordagem à esfera pública no ciberespaço, redefinindo a relação entre identidade individual e comunidade (Frau-Meigs):

O intercâmbio de sons e imagens não substitui um encontro pessoal, ele tem sua própria lógica, suas maneiras de formar opiniões. (...) A Internet permite que as pessoas conversem como iguais. Mas o argumento tradicional raramente prevalece; e chegar a um consenso é amplamente considerado impossível. São sintomas de duas formas fundamentalmente diferentes de definir a identidade na esfera pública e na Internet. Tradicionalmente, a identidade de uma pessoa é definida pelo contato. A identidade é baseada no corpo físico. Essa estabilidade força os indivíduos a ter de assumir suas posições e permite construir a confiança entre as pessoas. Já na Internet os indivíduos podem definir suas próprias identidades e alterá-las à vontade (...) As diferenças na Internet não conduzem a um consenso, elas criam a profusão de diferentes pontos de vista. Sem a presença física, o carisma e o status dos indivíduos não têm força. As condições que encorajam o compromisso, o marco do processo político democrático, não estão presentes on-line (...) A tecnologia da Internet não deve ser vista como uma nova forma de esfera pública. (Poster, 1995)⁵⁶

A questão levantada por Poster é que a experiência de interação no tempo-espaço linear não é a mesma experiência das interações no ciberespaço. Em uma comunidade real as pessoas têm referências contextuais, e no ciberespaço elas não teriam esses

⁵⁵ LEVY, S. *Crypto-Rebels*. Wired 1(2), 1993.

⁵⁶ POSTER, M. *The Net as a Public Sphere?*, em *Wired* 3(11), 1995.

pontos de apoio. Mas as pessoas, cada vez mais, buscam quem tem referências semelhantes. As comunidades virtuais, sejam listas de discussão, blogs com ampla participação de leitores/comentadores, comunidades no Orkut ou Fotolog, reúnem cada vez mais pessoas com interesses e contextos culturais comuns. Não se trata mais dos MUDs discutidos por Turkle em *Life on the Screen*, pois as formas de relacionamento on-line sofisticaram-se muito desde então.

A situação atual é que o acesso regular de apenas uma minoria da população à Internet, e o aumento da oferta de serviços públicos e privados via ciberespaço, não permite considerar a esfera on-line como a solução de problemas da realidade física que foram criados pela migração para a Internet de parte das diversas combinações de relacionamentos entre indivíduos, empresas e estado. Sejam lojas on-line, a Secretaria da Receita Federal, as Secretarias de Fazenda das prefeituras, ou os sistemas de inscrição em vestibular ou matrícula em disciplinas das universidades públicas, cada vez mais serviços estão disponíveis apenas on-line, e isso é uma grande limitação para a maioria da população, que ainda não tem acesso regular ao ciberespaço.

A criptografia era defendida na Wired como meio de propagar a opinião da revista na promoção e preservação da realidade virtual. Eles defendiam calorosamente a liberação da informação em escala global, e na definição de uma identidade clara na esfera privada. Era a discussão, já presente, de retirar o controle da Internet do governo e colocá-lo nas mãos da iniciativa privada. E o argumento era que isso iria determinar o grau de liberdade na sociedade no século 21. Como visto pela publicação da ainda vigente legislação da Lei Patriótica, que retira diversos direitos civis e de privacidade, inclusive de cidadão norte-americanos dentro dos EUA, esta não era uma preocupação infundada. Eles invocavam a primeira emenda à Constituição norte-americana, a garantia de liberdade de expressão e de imprensa, para rejeitar qualquer tentativa de censura à informação.

Um dos principais defensores da criptografia, Phil Zimmermann, autor do software de criptografia PGP, bastante difundido, sugeria que as chaves de criptografia (seqüências de dezenas ou centenas de caracteres) para os sistemas de chave pública/privada, deveriam ser distribuídas ou vendidas às pessoas, sem controle do governo. Enquanto isso, a poderosa NSA (Agência Central de Segurança) dos EUA que,

como a maioria dos governos, sempre fez uso da mais sofisticada criptografia disponível, em nome da segurança nacional, tentou obrigar (em alguns casos, com sucesso) os fabricantes de circuitos integrados com sistemas de criptografia a instalar “portas dos fundos”, mecanismos de acesso a arquivos criptografados, para que órgãos do governo pudesse ter acesso a conteúdo criptografado de arquivos de indivíduos, empresas ou governos que utilizassem tais circuitos integrados. E também conseguiu, durante algum tempo, impedir a exportação de hardware ou software com criptografia forte (mais de 56 bits) até que, vencida pela realidade de mercado, com empresas em todo o mundo desenvolvendo tais sistemas, desistiu pois isso estava limitando o mercado para exportadores norte-americanos.

Conforme explica Frau-Meigs:

Em março de 1996, antes da campanha presidencial, esse impulso pela legitimidade da auto-disciplina assumiu uma nova forma, concreta e aplicável a todos os cidadãos virtuais, quando a *Wired* criou o neologismo *netizens*, para seus leitores, cidadãos da Internet. Eles explicitaram seu desejo de propor uma alternativa política. A coluna Netizen não apenas cobria a campanha eleitoral, ela era política em um contexto revolucionário, que questionava se a própria política não estava obsoleta na era digital. A visão do mundo no qual a tecnologia iria prevalecer sobre a democracia política claramente sustentava a luta entre a tecnologia e a política pelo controle da realidade e do poder.

Era um apelo à cidadania pela tecnologia que permitiria aos *netizens* exercer uma pressão ‘privatizante’, visando a desestabilizar as autoridades públicas, confundindo as noções de ‘público’ e ‘privado’, e criando uma oportunidade de impor seus interesses. Assim a *Wired* podia posicionar-se como um órgão central dando representação real à comunidade virtual de seus leitores.

Foi um discurso que atualizou valores éticos, introduzindo na esfera democrática pública as lógicas da esfera industrial, quanto à administração das relações humanas.

Os articulistas da revista alcançaram o nível das autoridades públicas, com a vantagem de não estarem diretamente envolvidos na campanha, não sendo criticados, e usufruindo das vantagens da tecnologia da computação para usufruir de uma aura de poder emanando da ciência e tecnologia. Logo o debate sobre criptografia evoluiu para uma discussão sobre os direitos garantidos pela Primeira Emenda e eventualmente

descreveram uma utopia de informações onde a democracia implicava acesso livre à informação, em vez do direito de expressar uma opinião. Era uma tentativa de usar a tecnologia para produzir um discurso ideológico sobre o direito ao poder de quem dominava a tecnologia.

Frau-Meigs defende que a visão da *Wired* do indivíduo, com várias identidades e personalidades dissociadas, demonstra uma coerência compatível com o modelo econômico e social dos EUA. A construção dessa identidade plural e da pseudo-comunidade foi criada pela desestabilização da identidade da comunidade civil. Não foi uma criação da *Wired*, mas a revista o formalizou em seu discurso e o redistribuiu à sociedade, na forma de uma ideologia liberal sem conteúdo político explícito, com um debate ilustrado pela polêmica sobre a criptografia, que busca definir quem, o público ou o privado, deve ter controle da vida política.

Mas eles discutiam esse controle apenas para os que tinham uma identidade virtual, que tinham acesso à tecnologia, e não para todos, o que é coerente com um sistema em que o voto não é obrigatório, e é exercido por relativamente poucos. E simplificaram demais o problema, com essa limitação. Mas seu mérito foi dotar uma mídia tradicional, a revista impressa, com um layout inovador e recortando o mundo virtual no real, de um papel atuante, uma presença marcante, ao estimular seus leitores, embora com argumentos questionáveis, a exercer uma mudança coerente com suas “novas” identidades.

Segurança e privacidade na Internet

As ferramentas básicas são o antivírus, um programa que analisa arquivos e anexos a e-mails em busca de seqüências conhecidas de vírus, programas que realizam ações indesejadas no computador onde se instalam. Devem ser atualizados periodicamente, em geral mais de uma vez ao dia, mas é uma corrida contra o tempo pois só depois que um novo vírus (e há vários novos todos os dias na Internet, cerca de metade criados por brasileiros) é identificado e sua assinatura é distribuída aos usuários é que o programa pode identificá-lo e eliminá-lo.

Outra ferramenta importante é o firewall, um programa para proteger o acesso não autorizado a uma rede ou a um computador conectado à Internet. Seu nome vem das paredes de fogo, fogueiras permanentemente acesas, erguidas em toda a volta do Vaticano para impedir os “maus humores” da peste negra de entrar na sede da igreja católica, na Idade Média. Como os ratos, reais vetores das pulgas contaminadas, não passavam a parede em chamas, atirou-se no que não viu e acertou-se no que viu, mas não o reconhecendo como o real perigo.

O firewall não é uma proteção automática, ele impede algumas tentativas de acesso ao computador por outros, via rede ou Internet, mas depende do usuário autorizar cada programa utilizado e cada site visitado, e se o usuário autorizar um site que tem um vírus ou programa espião, o firewall será burlado. Por exemplo, os softwares de comunicação de mensagens instantâneas, em tempo real, que também operam com áudio, como o ICQ e o MSN Messenger “atravessam” o firewall e a monitoração do antivírus e permitem a instalação de arquivos espões no computador. Além disso, as mensagens podem ser monitoradas, com facilidade em uma rede interna, ou com alguma dificuldade, na Internet.

Outro recurso muito em uso são os programas antispysware, que identificam pequenos programas espões instalados ao acessar determinados sites, que podem ser cookies para identificar o usuário ou registradores de teclado (keyloggers) que registram senhas e tudo o mais que for digitado e enviam via Internet para o site programado. Devem ser atualizados periodicamente (cerca de uma vez ao mês) e monitoram o tráfego da conexão à Internet.

Os computadores pessoais com spyware instalado podem apresentar alguns sintomas, como a página inicial do navegador ser alterada, os programas antispysware lentos e informando que faltam arquivos, o surgimento de novos itens no menu de Favoritos do navegador, a computador ficar muito lento, aparecem barras de ferramentas no navegador. Mas também podem não apresentar nenhum sintoma, e deve-se usar programas específicos para localizá-los e eliminá-los, como o PestPatrol <www.pestpatrol.com>, AdAware <www.lavasoftusa.com/software/adaware>, Spybot Search & Destroy <www.safer-networking.org/en/home>, System Detective <www.systemdetective.com> ou X-Cleaner <www.xblock.com>.

Há vários casos de ataques, individuais ou em equipe, a servidores na Internet, seja por ‘brincadeira’, seja para extorquir dinheiro das empresas para normalizar seus sistemas. Patrick Gray, ex-responsável pelo Esquadrão de Cibercrimes do FBI, e então diretor da X-Force Operations da ISS, comenta que os grandes hackers buscam dinheiro, e aproveitam a falta de segurança de diversos computadores domésticos, invadidos por programas espíões, via Internet, para lançar ataques a sites em datas predefinidas. Dois casos relatados por ele dão uma boa idéia da dimensão desses problemas⁵⁷:

Em 7 de fevereiro de 2000 o Yahoo! foi derrubado por um hacker, por ataque de DDoS (negação de serviço). Foram lançadas tantas solicitações nos servidores do Yahoo! que o site saiu do ar. No dia seguinte, a Amazon, o e-Bay, o Buy.Com, o e-Trade e a CNN saíram do ar sob ataques pesadíssimos. (...) A CNN pediu ajuda ao FBI. (...) No fim do dia, 10.273 sites hospedados pela CNN estavam fora do ar. (...) Usamos mandados de tribunais para obter de diversos provedores os logs que nos permitiriam traçar a rota usada pelo hacker. Oito dias depois, localizamos a residência do hacker, em Montreal, Canadá. (...) Monitoramos a digitação nos teclados de todos os computadores da casa. E, depois de alguns dias, soubemos quem era o hacker: um adolescente de 15 anos cujo apelido no IRC era Mafiaboy. Ele iniciou os ataques no Canadá e nos EUA, depois seguiu para o resto do mundo, tomando posse de diferentes redes de computadores e utilizando-as no ataque maior. Chegou a usar um modem discado em Paris para tentar apagar sua trilha antes de se voltar contra os sites americanos, através da rede de uma grande universidade. No fim, o prejuízo foi de US\$ 8 bilhões. Outro caso envolveu o administrador de sistemas de uma empresa de engenharia de Nova Jérsei, que tinha acesso a tudo na rede. Seu nome era Kim Lloyd e a empresa decidira despedi-lo porque não estava fazendo bem seu trabalho. Ele soube da demissão antes que ela acontecesse e escreveu uma “bomba” lógica com seis linhas de código. Embutiu-a bem no fundo do sistema. A demissão veio e Lloyd saiu sem despertar suspeitas. Uma semana depois, a bomba lógica “explodiu” (uma explosão de dados), praticamente destruindo o sistema operacional usado na empresa. Eles perderam todos os contratos, dados de recursos humanos, financeiros, informações sobre negócios(...) Gastaram US\$ 12 milhões para voltar a operar. Este é o risco que alguém de dentro com acesso indiscriminado pode representar. O próprio FBI teve um insider que roubou informações durante anos e as vendeu aos russos.⁵⁸ E nem imaginávamos...

⁵⁷ MACHADO, André, Informática etc., O GLOBO, 1 nov. 2004.

⁵⁸ Esse caso também é citado por Bamford.

Uma solução para garantir a privacidade é usar criptografia nas mensagens, nos países onde isso não é proibido por lei, e existem vários programas fáceis de utilizar, além do famoso PGP (Pretty Good Privacy), de Philip Zimmermann, para criptografar e-mails ou arquivos. Sua última versão gratuita com todos os recursos é a 7.0.3, para Windows 9x ou 2000, disponível em <http://www.pgpi.org/products/pgp/versions/freeware/win32/7.0.3/>. A versão atual (9.0), disponível em <http://www.pgp.com/downloads/desktoptrial.html>, permite uso gratuito por 30 dias, inclusive para criptografar todo o disco rígido, e o uso dos recursos básicos indefinidamente.

Mas os registros dos e-mails permanecem gravados nos provedores, e com isso a possibilidade deles serem acompanhados até sua origem, mesmo muito depois de enviados. E-mails de denúncias, de mensagens políticas ou simplesmente de usuários que não desejam ser cadastrados em inúmeras listas comerciais de envio de spams, podem usar alguns serviços de anonimato, como o famoso Anonimizer.com, ou outros. Mas nem sempre isso é garantia de anonimato.

Dois usuários japoneses que recorriam ao popular Winny para garantir anonimato enquanto trocavam arquivos de jogos e filmes, foram presos pela polícia japonesa, acusados de pirataria. E o desenvolvedor do programa também foi interrogado e sua residência foi vistoriada pela polícia. Ainda não se sabe como a polícia nipônica os identificou.⁵⁹

Até 2003 a maioria das pessoas usava programas clientes de e-mail, como Outlook Express, Eudora, Mozilla, ou clientes embutidos nos navegadores, que acessam o provedor e ‘baixam’ os e-mails para o computador do usuário. Mas cada vez mais pessoas estão preferindo a praticidade de manter seus e-mails, recebidos e enviados, gravados no provedor, que pode ser Yahoo, iG, Click21, Gmail (do Google) ou muitos outros provedores de e-mail gratuito, pela facilidade de ter acesso a eles de qualquer computador, pela Internet. Além dos cabeçalhos, que todos os provedores registram, nesses provedores de e-mail, todo o conteúdo dos e-mails fica registrado, indefinidamente.

⁵⁹ PIROPO, B. Coluna em O GLOBO, Informática etc., 8 dez. 2003.

O interesse desses provedores em oferecer caixas postais de até 1GB é que os e-mails, e as páginas visitadas por seus usuários, formam um imenso banco de dados que permite a formação de perfis de consumo cada vez mais específicos, e quanto melhores, mais valiosos para venda a empresas que vão anunciar seus produtos ou serviços a um público com mais probabilidade de consumi-los.

O Gmail é bom demais, simples demais, prático demais. Pois é, tem gente achando que esse “demais” está demais. Em maio, senadores da Califórnia, terra do Google, aprovaram uma medida freando os planos de Larry Page & cia. Os senadores consideram perigosos os planos da Google de “espionar” mensagens, analisando seu conteúdo para incluir anúncios personalizados. Ou seja, tratar o e-mail como se fosse uma página Web qualquer. (...) Não só nos EUA o Gmail tem sido alvo de graves críticas. Dezesete países europeus anunciaram que só deixarão o Google dar o latifúndio de gigas aos cidadãos quando a empresa discriminar como será a proteção dos dados pessoais que circulam lá dentro. Outra que também já declarou guerra às pretensões da Google é a Privacy International, organização não-governamental que defende a privacidade na Internet. Em comunicado enviado em abril de 2004 a agentes reguladores da Internet em países como Holanda, Espanha, França, Itália, Alemanha, República Tcheca, Portugal, Grécia, Bélgica, Canadá, Dinamarca, Irlanda, Suécia, Áustria, Austrália e Polônia, representantes da ONG sugerem que a Google estaria, com os termos atuais de privacidade do Gmail, violando o direito dos internautas de manter confidenciais as informações que circulam em seus próprios webmails. O alvo principal da Privacy Internacional é o mecanismo de busca do serviço, o mesmo que fez praticamente nascer um novo verbo (googlar) e fez de uma pequena empresa californiana a forte marca que é hoje. Dentro do Gmail, um sistema de busca, que também serve para que os proprietários das contas não se percam em espaço tão vasto, faz uma varredura em busca de conteúdos específicos que possam ser vinculados a anúncios e banners de publicidade.

Também em abril, 28 entidades de defesa da privacidade virtual e de direitos civis enviaram uma longa carta a Larry Page e Sergey Brin, os criadores do Google, pedindo que a empresa reconsidere a política de privacidade do Gmail. As entidades consideram que o scan automático de mensagens abre um precedente perigoso.⁶⁰

⁶⁰ MONTEIRO, Elis, n' O GLOBO, Informática etc., 7 jun. 2004.

Uma pesquisa da UIT, União Internacional de Telecomunicações, (www.itu.org), relativa ao ano de 1999, determinou que em 42% dos países pesquisados, os respectivos governos se posicionam contra qualquer restrição de uso “doméstico” da criptografia em transações eletrônicas, a maior parte destes “territórios livres” corresponde à nações desenvolvidas, e países em desenvolvimento como o Brasil, El Salvador e Granada. Por outro lado, 29% dos países pesquisados exigem alguma forma de aprovação governamental para a circulação das tecnologias de criptografia. Os demais 13% optam por um modelo “dirigista”, com o Estado definindo os destinos e caminhos para a produção de produtos com alguma forma de criptografia, muito mais do que uma aprovação, o governo é parte ativa do processo.

Quanto ao acesso dos governos aos códigos chaves (públicos) de uso privado, em outra pesquisa, somente 13% dos países apoiam a idéia de que não deve haver interferência estatal no sentido da revelação destes códigos-chave. Quase metade dos países pesquisados (48%) permite o acesso de autoridades nacionais aos códigos-chave de uso privado. 35% dos países admitem tal acesso mediante uma ordem judicial. 16% sustentam que qualquer autoridade governamental pode acessar códigos-chave públicos (Eslováquia, Tailândia, Turquia, Austrália e Dinamarca).

Muitos países (42%) manifestaram-se incertos acerca da conveniência da adesão a acordos internacionais de mútuo reconhecimento dos padrões de criptografia. Somente a França manifestou-se terminantemente contra qualquer espécie de apoio a um acordo desse tipo. 16% dos países pesquisados são signatários de algum acordo internacional de criptografia e 42% “consideram” uma possível adesão futura.

33% (desenvolvidas ou “em desenvolvimento”) das nações avaliadas afirmam ter alguma lei “forte” regulando a questão da criptografia. Outras 30% têm legislações mais “fracas”, pouco rigorosas ou aplicadas. Os demais países praticamente não têm legislação específica sobre privacidade e criptografia.

A pesquisa também perguntou aos Estados Membros da UIT sobre as obrigações dos proprietários de bancos de dados e dos provedores de serviços on-line em relação a temas como venda ou divulgação de dados pessoais. Várias opções, colocadas em uma escala de seriedade crescente, foram postas à disposição dos pesquisados.

Vários Estados Membros responderam que suas políticas requerem a combinação de diversas práticas relacionadas na escala, mas curiosamente nenhuma política individual foi citada por mais de 42% dos pesquisados. As respostas (várias possíveis) foram:

40% - notificação das políticas aos usuários

42% - autorização por escrito

35% - acesso às informações pelo usuário

40% - registro em banco de dados

32% - restrições à exportação.

Nem sempre os programas espões são instalados por hackers. A multinacional Sony, que inclui a gravadora Sony Music, usou os serviços de uma empresa especializada em proteção contra cópia de meios digitais, a First 4 Internet, que incluiu em CDs de música da Sony Music a tecnologia XCP, parte do sistema de proteção contra cópia DRM (Digital Restriction Management), que usa um programa espião do tipo *rootkit*, que se instala no núcleo do Windows, tornando muito difícil sua detecção.

Segundo Chad, especialista em segurança da Newsletter “Computer Tips & Techniques” da WorldStart (www.worldstart.com), o *rootkit* se instala usando um conjunto de drivers que impede que ele seja removido mesmo no modo seguro (safemode) do Windows. O problema é que a instalação de um *rootkit* torna o sistema vulnerável para qualquer hacker que tenha algum conhecimento de segurança. Tanto assim que, ainda segundo Chad, já começaram a surgir alguns vírus que exploram essa vulnerabilidade, inclusive o “breplibot”, uma conhecida “backdoor”. Com a repercussão do problema, a Sony, (em <http://cp.sonybmg.com/xcp/english/home.html>), além de uma completa admissão de culpa, admite a existência do problema e se propõe a trocar os discos afetados por outros, sem proteção contra cópia.⁶¹

A matéria “TST admite rastreamento de e-mail por empresa”, publicada n’O GLOBO, em 16 de maio de 2005, informa a decisão inédita da Primeira Turma do Tribunal Superior do Trabalho, que, de certa forma, cria uma jurisprudência a respeito, ao afirmar que o patrão pode sim, desde que “de forma moderada, generalizada e

⁶¹ PIROPO, B, *E a Sony? Quem diria...*, Informática etc. O GLOBO, 21 nov. 2005

impessoal”, controlar as mensagens enviadas e recebidas pela caixa de correio eletrônico da empresa para obter provas para a demissão por justa causa:

Rastreado o e-mail de um funcionário o HSBC Seguros Brasil S.A. descobriu que um dos integrantes da equipe de Brasília usava o correio eletrônico corporativo para envio de fotos de mulheres nuas aos colegas. Por unanimidade, a Primeira Turma decidiu que não houve violação à intimidade e à privacidade do empregado e que a prova é legal, pois o e-mail da empresa é uma ferramenta de trabalho e deve ser usada apenas para uso profissional e que “não haveria qualquer intimidade a ser preservada, posto que o e-mail não poderia ser utilizado para fins particulares”. O ministro João Oreste Dalazen enfatizou que o correio eletrônico corporativo não pode servir para fins estritamente pessoais, para o empregado provocar prejuízo ao empregador com o envio de fotos pornográficas, por meio do computador e provedor também fornecidos pela empresa. Quanto à senha pessoal fornecida pela empresa ao empregado, o ministro esclareceu que a senha “não é uma forma de proteção para evitar que o empregador tenha acesso ao conteúdo das mensagens, ela serve para proteger o próprio empregador para evitar que terceiros tenham acesso às informações da empresa, muitas vezes confidenciais, trocadas pelo correio eletrônico. O relator admitiu a “utilização comedida” do correio eletrônico para fins particulares, desde que sejam observados a moral e os bons costumes. Como não há nenhuma norma específica sobre a utilização do e-mail de trabalho no Brasil, o relator recorreu a exemplos de casos ocorridos em outros países.

É uma decisão que “interpreta” a legislação a respeito, que a rigor não permitiria essa vigilância, mas atualmente também considera o fato dos contratos de emprego, assinados pelos empregados de empresas com redes de computadores, preverem a monitoração, pelo empregador, das comunicações eletrônicas realizadas pelos equipamentos da empresa.

Esta questão é antiga, e o julgamento de primeira instância foi comentado em uma reportagem do UOL, em 23 de outubro de 2001⁶², intitulada “Sigilo na Web, Empresa não pode violar mensagens de empregados”, que informou que uma ação trabalhista julgada na 13ª Vara de Brasília, contra o HSBC Seguros, determinou que a empresa não tem o direito de violar as correspondências eletrônicas dos funcionários. Segundo a seguradora, o empregado utilizou indevidamente o correio eletrônico e distribuiu fotos

⁶² <http://cf6.uol.com.br/consultor/view.cfm?numero=7122&ad=b>, acesso em 24 out. 2001.

pornográficas pela Internet. Por isso, foi demitido por justa causa e não teria direito ao aviso prévio. A 13ª Vara entendeu que houve violação da correspondência do empregado, nos termos do §5º, XII, da Constituição Brasileira.

A Lei nº 9.296/96 visa regulamentar o dispositivo da Constituição. “Porém o parágrafo único do artigo 1º dessa Lei é flagrantemente inconstitucional”, afirmou a defesa do empregado. De acordo com o parágrafo único, “aplica-se a interceptação do fluxo de comunicações em sistemas de informática e telemática”.

A Justiça citou até a Constituição de Portugal para reforçar a inviolabilidade. “O mesmo ocorre em Portugal, onde a Constituição (1976), em seu art. 32, veda expressamente todas as provas obtidas mediante tortura, coação grave, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações”.

Como mostrado, a decisão foi invertida no Tribunal Superior do Trabalho.

A maioria dos usuários não cuida bem da segurança de seus computadores conectados à Rede. Uma pesquisa⁶³ publicada em outubro de 2004, com 329 usuários adultos de Internet (rápida e conexão discada) de 22 cidades americanas, que tiveram suas máquinas examinadas por técnicos na NCSA (National Cyber Security Alliance, uma organização privada de fins não-lucrativos destinada a informar usuários de computadores sobre segurança), disponível em www.staysafeonline.info/news/NCSA-AOLIn-HomeStudyRelease.pdf, revelou que:

A grande maioria dos entrevistados acreditava que seu computador estava protegido de ameaças via Internet (77%), seguro quanto a vírus (73%) e a salvo de hackers (60%). Não obstante, um em cada sete (15%) não tinha qualquer programa antivírus instalado e, nas máquinas dos que tinham, 67% dos programas não haviam atualizado a proteção na última semana. Uma em cada cinco máquinas (19%) estava contaminada por pelo menos um vírus e quatro em cada cinco (80%) abrigavam, em média, 93 adwares ou spywares. Dentre as vítimas, a imensa maioria (89%) declarou desconhecer que tais programas existiam em seus micros e 90% desconheciam o que são e o que fazem adwares e spywares. No entanto, dois terços (63%) reclamavam da abertura inopinada de janelas pop-ups, dois em cada cinco (43%) tiveram a página inicial

de seu navegador trocada à sua revelia e 40% alegaram que suas buscas eram redirecionadas. Quase todas (95%) as vítimas declararam que não haviam dado permissão para a instalação dos programas e muitas (86%) pediram aos técnicos que os removessem.

Mais de um terço (38%) dos usuários de conexões sem fio as deixavam completamente “abertas” (sem criptografia). Dois terços dos usuários (67%, metade dos quais dispunha de Internet rápida) não usavam qualquer tipo de firewall. Três em cada cinco (58%) desconheciam a diferença entre um firewall e um programa antivírus e mais da metade (53%) simplesmente não sabiam o que é e como funciona um firewall. Não obstante, a vasta maioria (84%) armazenava dados confidenciais em suas máquinas (registros financeiros e médicos) e usava seus micros para transações financeiras via Internet (74%). Uma situação assustadora.

Quem participa de listas de discussão tem todos os e-mails trocados via lista registrados durante anos nos provedores, cabeçalhos e conteúdos. Embora o acesso normalmente seja limitado aos que participam da lista, a grande maioria delas tem acesso inicialmente liberado, e mesmo sem acesso, são informações não criptografadas, disponíveis em servidores sem uma preocupação com rígidos esquemas de segurança. Ou seja, ao contrário de uma carta, que tem uma garantia razoável de sigilo em seu trajeto, um e-mail pode ficar registrado no ciberespaço para sempre, e a grande maioria dos dados pessoais, das informações sobre indivíduos, que venham a ser disponibilizados pela Internet, estão disponíveis a qualquer um, por meio dos mecanismos de busca, como o Google, Yahoo, Altavista, Teoma, A9 e outros, durante muitos anos, mesmo depois das páginas originais serem eliminadas. Basta clicar em *cache* para ter acesso a uma cópia da página disponível nos computadores dos provedores mecanismos de busca. Experimente dar uma busca pelo seu próprio nome, completo ou parcial, e veja quantas informações estão registradas.

Na visita a sites de empresas ou instituições financeira, o principal problema é a identificação correta do usuário, e seu isolamento durante a conexão, a solução usada é criptografar os dados durante a conexão, a sites como bancos e lojas, e exigir algum tipo

⁶³ PIROPO, B, n'º GLOBO, Informática etc., 1 nov. 2004.

de certificação digital, como uma assinatura, que identifique exclusivamente o usuário, o equivalente a uma “firma reconhecida”.

Várias empresas e serviços, como CEF, Febraban, IBM, Microsoft, Serpro, Serasa, SRF, já usam certificados digitais, para registro e autorização de uso do software ou identificação do usuário. Eles são arquivos alfanuméricos armazenados em um disquete, no disco rígido, em cartões inteligentes, ou *pen drives* USB.

Uma evolução do atual teclado padrão brasileiro, o ABNT2, o que tem a letra Ç ao lado do L, será o ABNT3, que prevê a incorporação de leitores de cartão inteligente, e é parte das ações de popularização do uso da certificação digital.

Vários sites têm certificados digitais e o navegador da Internet exibe uma mensagem perguntando ao usuário se aceita aquele certificado. Eles têm prazo de validade e servem para o navegador, em uma próxima visita ao site, reconhecê-lo como válido.

Os e-mails e outros documentos digitais podem incorporar uma assinatura digital, um conjunto alfanumérico que é reconhecido por um servidor central, uma autoridade certificadora, que garantirá que aquele documento é válido. Esse registro de assinaturas digitais tem um custo para os usuários e o governo brasileiro ainda não concluiu sua regulamentação. O e-CPF e o e-CNPJ da SRF são exemplos, e realmente agilizam os processos na Receita Federal. O e-CPF deverá ser uma exigência para os 374 mil profissionais de contabilidade do Brasil, até o final de 2006. Em junho de 2005 já havia 15.627 e-CPFs e 14.957 e-CNPJs e a meta da Febraban era alcançar meio milhão deles até o final de 2005. (Em 2004 a meta era alcançar 3 milhões em 2005.)

Um certificado de chave pública é uma credencial eletrônica que contém o nome da autoridade emissora, o nome do seu titular, a chave pública do titular, o período de validade, o número de série do certificado e a assinatura digital da autoridade emissora.

A criptografia de chaves públicas (PKI) usa um par de chaves (arquivos digitais com 128 a 1024 bits), uma pública, outra privada, relacionadas matematicamente. A chave privada serve para criptografar os dados, que são enviados a quem tenha uma chave pública (recebida previamente), usada para decodificar os dados recebidos.

Autoridade Certificadora é um órgão autorizado a emitir, renovar ou suspender certificados. Deve emitir certificados que vinculem cada chave pública ao seu titular. Pode ser Primária (como a AC-Raiz da ICP-Brasil) ou uma Autoridade Emissora subordinada a outras (como as da CertiSign estão subordinadas à VeriSign)⁶⁴.

O ITI, Instituto Nacional de Tecnologia da Informação (www.iti.br), realizou de 7 a 9 de outubro de 2003 um seminário em Brasília, e lançou um fórum virtual para a sistematização e o debate da certificação digital para toda a sociedade.⁶⁵

Um comitê formado por sete instituições governamentais, entre ministérios e autarquias, foi indicado em 2003 para estabelecer normas técnicas e a política para o sistema de certificação digital no país.

E há a questão da responsabilidade pelo uso do certificado digital. Quem usa, quem emite e quem fiscaliza pode ser responsabilizado por problemas de segurança. Na prática, as responsabilidades têm pesos diferentes. Quem emite o certificado pode ser responsabilizado, por exemplo, por erro na identificação do titular ou na datação de uma revogação. E, no caso da ICP-Br, a infra-estrutura de chaves públicas do país, a certificadora raiz poderá ser responsabilizada por falhas na fiscalização. Os problemas mais graves, do ponto de vista do custo social, podem ocorrer no varejo, através de fraudes no ambiente de uso de certificados e chaves privadas.

Quem for identificado como titular de um certificado envolvido em fraude será sempre vítima, pois terá de provar que houve fraude. E para processar o fabricante do software pelas vulnerabilidades que causaram o que consideramos ter sido fraude, há dois problemas. Podemos ser impedidos por termos concordado com a licença de uso e teremos dificuldade em provar que fomos vítima de fraude. Como a MP 2200 (que instituiu a ICP-Brasil) diz que o certificado dá presunção de autenticidade, cabe ao usuário revogar imediatamente seu certificado junto à autoridade certificadora em caso de roubo, para não incorrer em penalidade.⁶⁶

Há experiências bem-sucedidas no Brasil. No Tribunal de Justiça do Rio Grande do Sul, os julgamentos já estão todos devidamente informatizados. Todos os

⁶⁴ O GLOBO, Informática etc, 14 nov. 2005

⁶⁵ O GLOBO, Informática etc., 29 set. 2003

⁶⁶ O GLOBO, Informática etc., 13 out. 2003

documentos passam pelos integrantes do processo por meio eletrônico, e uma vez tomada a decisão, ela é assinada digitalmente com um certificado A3 da ICP-Brasil. Depois os documentos eletrônicos vão para um banco de dados. Só são impressos os autos, para os tribunais superiores.

Cada magistrado do TJ-RS tem seu próprio token com certificado, e com isso o tempo dos processos é reduzido em um mês. Uma decisão demora três dias. E a economia com o fim das impressões é de R\$ 740 mil anualmente, pois eram tiradas seis cópias de cada acórdão.

Em janeiro de 2006 o RS planeja implantar a Nota Fiscal Eletrônica (que já existe em SP e recebeu a adesão de 18 empresas). Ela vai acabar com muita burocracia, pois uma operação de compra e venda entre duas empresas é registrada 14 vezes.

A certificação digital também facilita a declaração de imposto de renda, permitindo localizar rapidamente discrepâncias em fonte pagadoras ou despesas.

Mas não é só no aspecto financeiro que a certificação tem sido aplicada. A Bélgica criou uma identidade eletrônica para a população e prevê que todos os belgas terão uma identidade, na forma de cartão inteligente, até 2009.

Na Malásia o governo incluiu diversos serviços na identidade eletrônica das pessoas. Um chip de computador permite que o cartão seja usado ao mesmo tempo como carteira de motorista, cartão para saques bancários, cartão do serviço nacional de saúde e passaporte. Os EUA estão mais cautelosos no uso da certificação digital. O uso de assinaturas eletrônicas está restrito a funcionários do governo americano e não há planos para alcançar a população em curto prazo.

Com uma carteira de identidade com um chip RFID, os cruzamentos entre bancos de dados geram resultados muito mais precisos, pois não há risco de erro de digitação de nome, confusão com homônimos. Mas a privacidade diminui, pois isso facilita o cruzamento não só de informações de identidade em portos e aeroportos, mas as transações financeiras e todas as demais atividades em que a identificação seja usada.

Um cartão de identidade nacional nos EUA feriria o âmago das liberdades constitucionais, e daria à população uma falsa sensação de segurança, pois os

documentos necessários para obter esse cartão ainda são fáceis de adulterar. Terroristas estrangeiros geralmente têm identidades falsas. E muitos terroristas americanos, em passado recente, não se esconderam por trás de uma falsa identidade.

Além da identificação eletrônica e da certificação da identidade por software, há outra solução. Um movimento, a Computação Confiável (www.trustedcomputinggroup.org), formado por Microsoft, IBM, HP, Intel, AMD, Sony e outras empresas, busca enfrentar as ameaças de segurança que se multiplicam cada vez mais rapidamente pela Internet. Seu objetivo é desenvolver, definir e promover padrões para computação confiável e tecnologias de segurança ativadas por hardware (inclusive os módulos de hardware e as interfaces de software) compatíveis com múltiplas plataformas, periféricos e dispositivos. A matéria⁶⁷ informa que:

Já existem vários produtos com a tecnologia trusted, como a linha de business desktops dc7100 da HP, que vem com segurança encriptada no hardware, no chamado TPM (trusted platform model). Ou notebooks como a linha T42 dos Thinkpads, que vêm com as chamadas tecnologias ThinkVantage, com um subsistema de segurança embutido e especificado conforme as regras do TCG (com chip & software seguros, que guardam as “credenciais eletrônicas” do usuário). Ou ainda os próximos processadores da família PXA27X da Intel, que incluem a Intel Wireless Trusted Platform, projetada para “prover confiança na plataforma e serviços robustos de segurança nos dispositivos sem fio atuais”. A WTP é construída segundo os conceitos do TCG e seus componentes, tanto em hardware quanto em software, estão prontos a oferecer boot seguro, armazenamento seguro de informações e chaves privadas, aceleração criptográfica, e suporta, além da OMA-DRM (Open Mobile Alliance Digital Rights Management), protocolos de segurança como SSL (Secure Sockets Layer, para login/senha mais seguros, encriptados) e VPN (Rede privada virtual).

Mas a matéria alerta que o conceito de computação confiável pode não ser tão confiável assim, pois máquinas construídas com as especificações do TCG seriam mais confiáveis do ponto de vista das vendas de software, mas menos confiáveis do ponto

⁶⁷ MACHADO, André, *É de confiança?*, n' O GLOBO, Informática etc., 7 fev. 2005

de vista do usuário, pois a especificação do TCG transferirá o controle final do PC para quem escreveu o software sendo executado.

E Lawrence Lessig (professor da Universidade de Stanford e fundador do Creative Commons) afirma que tais medidas de proteção tecnológica retiram dos usuários direitos que a própria lei antes garantia, como o direito ao *fair use*, que se aplica tanto nos EUA quanto no Brasil. O *fair use* permite gravar um programa de TV e assistir a ele mais tarde. Mas, nos EUA, uma das grandes redes de TV a cabo mandou recentemente um sinal para a casa de pessoas que tinham um sistema com DRM, impedindo a cópia de seus programas, ou seja, uma gravação programada era apagada pelo sistema.

Mas esses sistemas não são invioláveis. O CSS, o sistema de proteção contra cópias dos DVDs, que foi elaborado durante quatro anos, foi quebrado por um garoto e divulgado pela Internet. O DRM é um instrumento, principalmente das grandes gravadoras e estúdios cinematográficos, que busca garantir-lhes uma ocupação da rede equivalente à que têm no mundo físico. O importante é que em meio a inúmeros spams, phishing e outras ameaças, a computação confiável pode ser a solução para manter a Internet operacional, em acesso com ou sem fio, para garantia de que a fonte é segura.

Depois da quebra do sigilo bancário e do telefônico, pode vir a do sigilo eletrônico.⁶⁸ É o que consta no o Projeto de Lei nº 279/2003, do senador Delcídio Amaral (PT-MS). Sob o pretexto de combater crimes virtuais como pedofilia e tráfico, prevê que os provedores de acesso à Internet criem um cadastro detalhado dos usuários, pessoas físicas e jurídicas, com nome, endereço, identidade e CPF (ou CPNJ), e obriga os provedores a armazenar os dados cadastrais e os cabeçalhos das mensagens por dez anos. A matéria detalha, e critica:

O projeto sugere a Anatel como fiscal do cumprimento da Lei e cria a co-responsabilidade do provedor sobre a veracidade das informações fornecidas pelos usuários no momento da criação de suas contas de e-mail. O projeto, de 2003, ganhou notoriedade em novembro de 2005 quando foi apresentado em audiência pública à Comissão de Educação do Senado. Na audiência, Amaral recebeu críticas de representantes do Comitê Gestor (CG) e da Associação Brasileira de Provedores de Acesso de Serviços e Informações da Rede de Internet (Abranet).

⁶⁸ O GLOBO, Informática etc., 5 dez. 2005

Existe quem veja, no projeto de lei do senador Delcídio Amaral, um fruto indireto da adoção, nos EUA, da Lei Sarbanes-Oxley, de 2002, que, depois de escândalos de fraudes contábeis como os da Enron e da Worldcom, estabeleceu regras mais rígidas para a divulgação de balanços das empresas americanas e suas subsidiárias no exterior e aumentando controles internos, e obriga as empresas a manter registros de acesso (extratos) de mensagens, com nome de destinatários, remetentes, local de envio e terminal de onde saíram as mensagens, além de documentar toda a comunicação entre seus funcionários e auditores (e-mail, fax ou cartas) durante cinco anos. A lei americana também deixa com a empresa a responsabilidade pelo armazenamento de todas as correspondências.

Delcídio garante que não pretende invadir a privacidade de ninguém, mas que manter o cadastro (e os extratos) é fundamental. Ele declarou que resolveu aceitar as propostas de mudanças que lhe serão encaminhadas pelo Comitê Gestor e pela Abranet. A primeira é tirar da Anatel a responsabilidade de fiscalizar o cumprimento da lei. Ele sugere, como substituto, o próprio CG. E reconhece que o registro dos logs poderá afastar os usuários dos provedores nacionais e levá-los a serviços no exterior.

Atualmente, os provedores não são obrigados a fornecer os dados dos usuários para a polícia, por exemplo. Mas, para cooperar com as investigações, os grandes provedores assinaram um convênio com o Ministério Público para agilizar os processos de investigação.

O Comitê Gestor e a Abranet pediram 30 dias para enviar a Delcídio um documento sobre o que há de errado no projeto e suas propostas de mudanças. Dentre elas, a sugestão de cadastro de cibercafés ou outros pontos públicos de acesso à Internet, onde qualquer criminoso pode agir sob a proteção do anonimato. O senador prometeu incorporar estes pedidos também, mas disse que já está recebendo reclamações dos representantes destes pontos públicos de acesso.

Outro ponto fundamental apontado por quem não viu o projeto do senador Delcídio com bons olhos: apenas os provedores nacionais teriam que cadastrar seus usuários. O problema é que a maior parte dos crimes é praticada justamente usando provedores de e-mail internacionais como Yahoo!, AOL, Gmail, dentre outros. E a maior parte destes provedores nem pede documentos para a abertura das contas.

A Panda Software alertou em 22 de março de 2005, em uma matéria publicada no IDG Now!, sobre o surgimento de uma nova ameaça ao internauta, batizada de pharming.⁶⁹

Segundo a empresa, o *pharming* é um tipo de golpe fraudulento ainda mais perigoso do que o *phishing scam*, pois não precisa convencer o usuário a digitar os dados pessoais em uma página.

O *pharming* envolve modificações no sistema DNS (Domain Name System) de endereços, encaminhando o internauta para uma página que não corresponde à digitada no endereço, mas sim a um site malicioso na Web, desenvolvido especialmente com o objetivo de copiar o original nos mínimos detalhes e fazer com que o usuário não perceba que está em território perigoso. Segundo dados coletados pela Panda, a grande maioria dessas páginas falsas é relacionada a serviços que envolvem o uso de dados confidenciais e financeiros, como lojas virtuais e portais de bancos on-line.

Ataques de *pharming* podem ser direcionados a servidores DNS, fazendo com que todos os usuários que acessem determinada página sejam encaminhados a outra, modificada e maliciosa. Outra possibilidade, muito mais comum, é infectar algum internauta desprotegido com cavalos-de-tróia que modificam o arquivo HOSTS, localizado na pasta de sistema do Windows.

O arquivo guarda uma tabela com os endereços IP mais acessados pelo usuário, de modo que o navegador não precisa acessar um servidor DNS para visitar uma página. Se esse arquivo é modificado com falsos endereços para websites de bancos, por exemplo, toda vez que o internauta procurar entrar em determinada página, ele será automaticamente direcionado a uma página falsa, sem perceber qualquer sinal de que está caindo em um golpe fraudulento.

A Panda afirma que as famílias de pragas Bancos-PWS, Banbra e Banker (os dois primeiros muito ativos na Internet brasileira) possuem funções de modificação do arquivo HOSTS, e representam uma mudança de tática de criminosos para roubar dinheiro de internautas.

A companhia espanhola recomenda que os usuários criem o hábito de atualização periódica de softwares antivírus, além do uso de firewall e atenção total para arquivos vindos de remetentes desconhecidos.

⁶⁹ <http://pcworld.uol.com.br/AdPortalV3/adCmsDocumentoShow.aspx?documento=8205726&Area=975000Hot>

O governo britânico quer retirar o sigilo telefônico dos parlamentares, permitindo que o serviço secreto faça escutas em casos de investigação de terrorismo.⁷⁰

São muitas as ameaças à segurança do usuário conectado à Internet, e agora há mais uma, a telefonia via Internet, o conhecido protocolo VoIP (Voz sobre IP), oferecido por empresas como a UOL Fone (<http://fone.uol.com.br/>), CMSW.Telecom (www.erne.com.br), InterCall (<http://golda.intercall.com.br/portal/br/athomevoip.aspx>), Skype (www.skype.com), VoxFone (<http://www.voxfone.com.br/index.htm>), TVA Voz (<http://www.tvavoz.com.br>), que permite ligações entre computadores pagando apenas a conexão à Internet, e conexões entre computador e telefone, em todo o mundo, a custos muito inferiores às tarifas interurbanas e internacionais vigentes. Já usada por muitas empresas, agora a telefonia VoIP está acessível, e cada vez mais usada, por pessoas físicas. O especialista em segurança, Hal Tipton, ex-presidente do International Information System Security Certification Consortium (ISC²), recomendou⁷¹:

A voz sobre IP é muito desejada por reduzir custos. Mas é baseada no SIP (Session Initiation Protocol), um protocolo de sinalização para uma camada de aplicações que, embora propicie muitos serviços, é vulnerável a diversos ataques, como grampos (via *sniffers*), roubo de identidades, escuta, *spoofing* de interlocutor (quando o hacker se disfarça num IP confiável)... Sem falar na falta de uma legislação adequada. Há ainda spam via SIP, que pode resultar em mais ataques: bombardeamento de correio de voz, negação de serviço.

As diversas ameaças à segurança são discutidas no Information Security Common Body of Knowledge (CBK). em: <https://www.isc2.org/cgi-bin/content.cgi?page=706>

O sistema de VoIP não é imune a interceptação, pois a voz é codificada em pacotes de dados que trafegam abertamente pela Internet.

Esta nota, na coluna de Carlos Alberto Teixeira, publicada em O GLOBO, Informática etc., em 8 de dezembro de 2003, comenta a interceptação:

Segundo o “Los Angeles Times”, o FBI está preocupadíssimo com a possibilidade de não ser capaz de grampear ligações telefônicas realizadas através de VoIP (voice-over-internet-protocol). Para resolver a questão, o birô, juntamente com o Departamento

⁷⁰ ELLIOTT, Francis, *Blair quer vigiar deputados britânicos*. Independent, n’O GLOBO, 16 jan. 2006.

⁷¹ MACHADO, André. O GLOBO, Informática etc., 15 ago. 2005.

de Justiça dos EUA, solicitou à FCC (Comissão Federal de Comunicações) que abra uma brecha no sistema. A alegação é a de sempre: guerra ao terror. De fato, é brabeira interceptar chamadas feitas por VoIP, pois os pacotes de dados são picotados para serem transmitidos via Internet, sendo remontados lá na outra ponta. Não é impossível a interceptação, mas dá um trabalho do cão. Em termos práticos, a questão não passa de uma filigrana legislativa, pois se a tecnologia VoIP for classificada pela FCC como um “serviço tradicional de telecomunicações”, então as concessionárias e software houses se verão obrigadas por lei a desenvolver e oferecer soluções para que o governo americano grampeie estes chamados. Naturalmente, os grupos defensores das liberdades individuais são contra, já que a privacidade de cidadão ficaria mais uma vez comprometida.

Várias empresas oferecem mecanismos de criptografia ou anonimato na Internet. Agora a criptografia está disponível para usuários finais por meio de softwares de fácil instalação e uso. Já o anonimato exige o uso de software e hardware especiais, e um ‘controle’ diferente do envio dos pacotes de dados. Os dados, de navegação ou e-mails, são divididos, criptografados e enviados por servidores diferentes. No destino são reagrupados e decodificados. Se alguém interceptar um fluxo de dados, não poderá identificar de onde vem.

O anonimato é defendido por ser uma ferramenta que permite a dissidentes políticos expressarem-se sem temer represálias, muitas vezes ilegais, por governos menos democráticos, e é condenado por dificultar o combate à pornografia infantil, e a crimes como pedofilia e tráfico de drogas. Mas essa crítica já foi feita ao telégrafo e ao telefone.

Empresas como a canadense Zero-Knowledge (<http://www.freedom.net/>), oferecem programas antivírus, firewall, bloqueadores de pop-ups, como muitas outras, mas também programas para controle dos responsáveis por crianças (Parental Control) e sistemas de anonimato (Web Secure) ao navegar pela Internet.

O WebSecure impede que as informações pessoais sejam transmitidas pelo navegador do usuário para os sites visitados. Ele criptografa (com 128 bits) e redireciona as solicitações de conexão do usuário por meio de servidores proxy e assim nem os sites nem hackers podem obter informações pessoais, da conexão ou do

hardware/software do computador. Não podem então criar perfis pessoais com base na navegação do usuário. Ele bloqueia scripts maliciosos que possam existir nas páginas, não informa o e-mail nem o IP (pelo qual é possível identificar a cidade), e neutraliza cookies e anúncios.

O Parental Control é um serviços de bloqueio de acesso a determinados conteúdos na Internet. A empresa e o usuário alimentam um banco de dados com todos os sites que considerem impróprios. O banco de dados da empresa inclui mais de 15 milhões de sites bloqueados, com conteúdo sobre sexo, drogas, atividades criminais, que é atualizado automaticamente. Governos como a China usam um sistema semelhante para impedir acesso a milhões de sites estrangeiros, pelos chineses. Pais e escolas podem impedir que as crianças acessem sites de pornografia, violência, ódio, drogas etc. O software também impede que a criança informe nomes ou outras informações pessoais on-line, como números de cartão de crédito, seja em salas de bate-papo ou outros sites. E pode permitir a navegação apenas em determinados dias e horários. As senhas dos usuários são criptografadas e o programa também bloqueia cookies.

A idéia do anonimato na rede busca recuperar a condição existente antes das tecnologias digitais de comunicação. Uma carta é protegida até seu destino, e apenas com uma ordem judicial as autoridades policiais podem ir ao domicílio da pessoa e examinar seus documentos. Na Internet há pouca proteção, e nem os governos podem garantir a privacidade dos dados. Os sistemas de anonimato recuperam essa proteção, sem prejudicar a ação das autoridades legal constituídas, pois uma ordem judicial permite que examinem o computador de um suspeito de crime, e lá as informações estão acessíveis. E as empresas que oferecem esses serviços são protegidas pois se não armazenarem as informações, não terão nenhuma condição técnica de fornecer informações de seus usuários, nem mesmo com uma ordem judicial.

A defesa desse anonimato tem diversos exemplos em ações legais, algumas citadas por Rosen (2000), onde e-mails obtidos judicialmente foram utilizados em ações onde o conteúdo dos e-mails foi avaliado apenas parcialmente, e fora do contexto original, gerando interpretações diversas dos fatos reais, prejudicando os acusados.

Identificação na Internet

Há vários sistemas implantados, sendo que duas vertentes se destacam.

O primeiro é o sistema empregado nos sites de bancos. Atualmente, após digitar a agência e conta no site do banco, que recomendam, sempre deve ser digitado no navegador, e nunca acessado indiretamente, por um link em e-mail ou outra página na Web, pois o link pode conduzir a uma cópia falsificada do site apenas para conseguir registrar as senhas do usuário, deve-se informar uma senha exclusiva para acesso à via Internet, diferente da senha para uso do cartão do banco.

Antes de informar essa senha o site do banco muda para uma página criptografada (o endereço que começa geralmente com `http://` muda para `https://` e o ícone do cadeado no navegador fecha) na qual todos os dados enviados para, ou recebidos, do banco, são criptografados, atualmente com uma chave de 128 bits, com um número tão grande de combinações que é praticamente impossível descobrir o que está sendo transmitido.

Essa tecnologia também é usada por muitas lojas virtuais, quando se fecha detalhes financeiros da compra de um produto ou serviço.

Ao acessar algum site sem proteção adequada no computador (por isso a necessidade de manter um antivírus e um firewall atualizados, além de ao menos um programa anti-espiões) ou ao clicar em um link em um e-mail, pode-se, inadvertidamente, baixar um programa espião que se instala no computador do usuário.

E também recomendam só acessar o banco on-line de seu próprio computador ou de alguma máquina confiável, nunca em cibercafés ou outras máquinas de uso público.

A senha tem de ser clicada na tela, com cursor do mouse, pois um programa espião, instalado no computador, pode registrar tudo o que é teclado e, ao conectar o computador à Internet, o programa envia o que foi digitado ao site que instalou o programa. Mas ele também pode enviar pequenas imagens da tela ao redor do ponto que foi clicado. E o número de tentativas erradas em geral é de duas. Na terceira senha errada, o cartão fica bloqueado e só pode ser desbloqueado na agência bancária.

Para evitar que essas informações sejam obtidas por terceiros, há bancos que usam dois algoritmos por setor, de forma semelhante ao empregado nos caixas automáticos,

pois quem capturar as imagens não saberá qual dos dois algarismos é o certo, há bancos que usam apenas um algarismo por setor mas ao clicar o número apaga na tela, e há bancos que além da senha pedem uma frase ou seqüência de caracteres.

A partir do segundo semestre de 2005, alguns bancos introduziram mais um mecanismo de segurança. Envia-se por correio um cartão a cada correntista, com uma seqüência de números (de 1 a 60 ou de 1 a 70), e a cada número corresponde outra seqüência, aleatória, de três ou quatro algarismos. Ou seja, não há dois cartões iguais. Após digitar a(s) senha(s) acima, o banco gera aleatoriamente um dos números da seqüência e o usuário tem de digitar o número correspondente em seu cartão.

E somente aí pode começar a fazer consultas ou transações financeiras, com limites de valor para cada uma, cadastro prévio de beneficiados com transferências, e para algumas delas será exigida a senha do cartão, data de aniversário ou algum outro dado pessoal. O problema é a grande quantidade de números e senhas que o correntista tem de decorar, pois é fortemente recomendado pelos bancos não transportar os números anotados, não deixar um cartão de senhas junto com o cartão do banco etc. Enfim, um grande aborrecimento e uma quase impossibilidade para usuários mais idosos.

O segundo sistema de proteção é a certificação digital (mas ainda não se definiu qual a melhor maneira de manter os números, se em um cartão ou chip) com ou sem identificação biométrica. Já existem sensores de impressão digital na faixa de cem dólares, para uso em computadores domésticos.

Há vários projetos de instalar em poucos anos identificadores faciais nos caixas eletrônicos. Atualmente muitos deles têm câmeras que fotografam o usuário em saques, ou transferências, e registram essa imagem para comprovação de identidade em possíveis reclamações de fraude, perda ou roubo de cartão.

Outro processo de identificação, cada vez mais comum em sites que exigem cadastramento do usuário, para votação on-line, ou para consulta de dados, como a Receita Federal ou o Lattes, para verificar se é uma pessoa que está acessando o site e não um software robô, é o uso de imagens contendo letras e números, que têm de ser lidas pelo usuário e digitadas. Essa imagem se chama *captcha*, um acrônimo de

“Completely Automated Public Turing test to tell Computers and Humans Apart”, ou seja, um teste público completamente automatizado do teste de Turing para distinguir computadores de humanos. Para evitar o uso de um software de reconhecimento óptico de caracteres (OCR), as cores das letras, números e do fundo, a inclinação ou deformação das letras e números, e o uso de riscos ou outros desenhos, foram criados especificamente com base nas deficiências dos programas de OCR.

Conforme explica Carlos Alberto Teixeira⁷² :

O termo *captcha* foi cunhado no ano 2000 por Luis von Ahn, Manuel Blum e Nicholas J. Hopper, da Universidade Carnegie Mellon, e por John Langford, da IBM. Mas a idéia é anterior, de 1997, quando Andrei Broder e seus colegas de trabalho no AltaVista usaram o primeiro captcha para evitar que *bots* inserissem URLs em sua máquina de busca. Mas já encontraram uma solução para “enganar” os sites que usam captchas. Programadores escrevem *bots* (programas robôs) que capturam um captcha original em um site X, apresentam-no a um humano num site diferente Y, em outro contexto, registram a resposta da criatura e submetem-na de volta ao campo digitado no site X de onde capturaram a figura, transpondo a barreira de segurança e ganhando acesso ao que desejam acessar. Em geral, usam como site Y páginas de pornografia. Assim, fingindo que é uma barreira real, o bot apresenta ao ávido internauta o captcha capturado no site X. O camarada vai lá e digita sua interpretação da figura. O *bot* pega os caracteres digitados no site pornô Y, que está sob seu controle, e “digita” os mesmos caracteres no site X. E pronto, está aí mais uma vitória da inteligência a serviço do mal.

O mercado de vigilância

Em junho de 2002 a Unisys organizou, em St. Paul de Vence, França, o Seminário para a Imprensa Européia 2002, com cerca de 50 jornalistas europeus, apresentado por alguns especialistas em segurança e tecnologia. O que parecia ser um debate sobre os limites éticos da tecnologia de informação (“O preço da privacidade”) transformou-se na discussão de um problema cultural e ético, mais do que neo-econômico, pois na opinião

⁷² TEIXEIRA, Carlos Alberto, O GLOBO, Informática Etc, 26 set. 2005.

das empresas de segurança, o homem tem que se acostumar, pouco a pouco, a abrir seus segredos.⁷³

Em 2002, a indústria de software de segurança, de acordo com a ISS, já representava um mercado de US\$ 4,5 bilhões. E a vulnerabilidade dos servidores está crescendo. O ataque de 11 de setembro de 2001 a Nova York e ao Pentágono tem reverberado cada vez mais no mundo digital, e a discussão versou sobre privacidade versus segurança. Nos EUA a segurança está ganhando com grande vantagem mas na Europa há uma tentativa de conciliar vigilância tecnológica com a defesa da privacidade.

Os europeus estavam assustados com a invasão de privacidade nas suas vidas reais, e não tanto com esburacados sistemas governamentais que registram a vida toda de cada cidadão, cruzando dados os mais distintos. Na Inglaterra, por exemplo, os dados médicos de cada cidadão são registrados no hospital mais próximo da sua residência, e ele deve comunicar cada mudança de endereço, para que seu histórico seja remanejado. Com a certeza da vulnerabilidade, a paranóia tende a anular, pouco a pouco, os direitos individuais à privacidade, privilegiando a segurança, mas esses conceitos não são necessariamente excludentes.

A noção de risco não é muito baseada na probabilidade real, e sim na percepção psicológica do risco por cada um. Assim, as câmeras nas ruas impressionam mais que o número da conta bancária circulando pela rede.

Logo as empresas e indivíduos têm de ter uma prevenção a mais abrangente e atualizada possível, e as corporações encarregadas de concentrar dados alheios devem apresentar transparência e inspirar confiança. Por exemplo, algumas lojas on-line não registram o número do cartão de crédito usado em uma compra. Durante o processo de compra, em uma página criptografada, enviam o número do cartão e outros dados para a operadora e recebem o número da autorização, e é apenas esse número que elas registram, junto com nome e endereço do comprador. Isso torna mais seguro usar um cartão de crédito on-line, nessas lojas, que em um posto de gasolina ou restaurante, onde os números podem ser facilmente copiados.

⁷³ VASCONCELOS, Nelson, *É da natureza*, A Nova Economia, O GLOBO, 3 jul. 2002.

Logo, o uso correto das ferramentas de segurança, adaptadas para cada empresa e cada tipo de situação, pode garantir as operações sem comprometer a privacidade. Isso passa pela educação dos usuários e por pesados investimentos das empresas.

A Philips anuncia um futuro em que a tecnologia de vigilância garante a segurança e o conforto de usuários europeus⁷⁴:

Ellen volta para casa após um longo dia de trabalho. Na porta de frente ela é reconhecida por uma câmera inteligente de vigilância, o alarme da porta é desativado, a porta destranca e abre. Ao entrar, o mapa da casa indica que seu marido Peter está em uma feria de arte em Paris e sua filha Charlotte está no quarto, brincando com uma tela interativa. O serviços remoto de vigilância infantil é informado que ela chegou em casa, e sua conexão on-line é desligada. Quando Ellen entra na cozinha, o quadro de avisos familiar acende para indicar que há novas mensagens. A lista de compras predefinida precisa de confirmação antes de ser enviada ao supermercado, que fará a entrega. Também há uma mensagem avisando que o sistema doméstico de informações encontrou novas informações na Web semântica sobre hospedagem barata para o feriado na costa espanhola. Ela conecta-se rapidamente ao quarto para falar com Charlotte, e sua imagem aparece automaticamente na tela plana usada por Charlotte. A seguir, ela conecta-se com Peter na feira de arte em Paris. Ele mostra a ela, por sua câmera na lente de contato, algumas das esculturas que pretende comprar, e ela concorda. Enquanto isso ela seleciona um dos menus exibidos, que indica o que pode ser preparado com os alimentos disponíveis na despensa e no refrigerador. Depois ela liga o canal de vídeo por demanda para assistir ao noticiário mais recente. Mais tarde vai para o quarto, onde a tela plana passa sua sessão personalizada de exercícios daquele dia. Mais tarde, à noite, após Peter chegar em casa, conversam com um amigo da sala de estar cuja iluminação ambiente personalizada foi ativada. Depois assistem ao apresentador virtual que lhes informa sobre os programas e informações gravadas naquele dia pelo servidor doméstico.

Com exceção da câmera na lente de contato, todas essas tecnologias já estão disponíveis, a um alto preço e geralmente em grandes e médias cidades. É como o mundo dos Jetsons, com vários sistemas automatizados cuidando das tarefas repetitivas, mas com o adicional dos sistemas de vigilância, integrados pela Internet. Outras grandes empresas investem muito nesse mercado:

⁷⁴ <http://www.philips.com.br/InformationCenter/>, acesso em 13 out. 2003.

A Juniper Networks desembolsou US\$ 4 bilhões pela NetScreen Technologies. A Juniper é a segunda maior fabricante mundial de equipamentos para redes. Com a operação, trata de seguir a cartilha da número um, a Cisco Systems, e aumenta seu poder no mercado de soluções de segurança, que tem seu crescimento garantido para toda a eternidade.⁷⁵

A maior empresas de bancos de dados do mundo, a Oracle, vende e consolida sistemas de bancos de dados para empresas e governos em todo o planeta. Fundada há vinte e cinco anos, seu primeiro cliente foi a CIA, a central de inteligência norte-americana. Eles venderam um banco de dados relacional, o Oracle, que permita relacionar informações em diversos bancos de dados, desde que tivessem algo em comum, como o nome do funcionário da empresa, por exemplo. Reunindo os diversos conjuntos de informações, permitem extrair novas relações entre elas, não existentes em nenhum dos bancos de dados originais. Em uma empresa, um banco de dados pode conter nome, endereço, idade, dependentes dos empregados. Outro, nome, função, salário, períodos de férias. Outro, licenças médicas. Com um sistema relacional, pode-se consultar quais empregados, que moram em determinada cidade, tiveram períodos de férias ligados a licenças médicas e abrangendo férias escolares de seus filhos.

Estendendo isso para outros tipos de bancos de dados, pode-se obter perfis detalhados de pessoas. A Oracle já vendeu sistemas para diversos governos e empresas, na Europa, EUA em outros países. Em 2001, ofereceu um software gratuito para o governo dos EUA, cobrando apenas atualizações e manutenção, para integrar todas as informações das diversas agências do governo americano em um banco de dados nacional, como ferramenta contra o terrorismo.

Um de seus produtos, o LEADERS (Sistema Leve de Reação de Emergência e Detecção Avançada de Epidemiologias), coleta informações de pronto-socorros nos EUA para monitorar surtos de doenças suspeitas e emitir alertas de ataques biológicos. Às 9h20min de 11 de setembro de 2001, Brian Jones, chefe da unidade de consultoria médica da Oracle, recebeu um telefonema do Centro de Controle e Prevenção de

⁷⁵ VASCONCELOS, Nelson, *Conexão Global*, O GLOBO, 10 fev. 2004

Doenças, em Atlanta, que temia que houvesse um ataque bioterrorista, após o ataque ao WTC de Nova York. Em dez horas de trabalho, Jones reuniu em seu computador os endereços de todos os hospitais no estado de Nova York, para detectar surtos de doenças incomuns, como varíola. Todos os hospitais podem informar ao mesmo banco de dados. E pode-se ver um mapa digital da cidade. O mapa criado pela Oracle é formado por 7500 fotos digitais e plantas de mais de 9500 km de dutos subterrâneos, de cada prédio, duto de água e esgoto, e meio-fio em toda a cidade. (Rosen, 2004). A Oracle planeja implantar esse sistema em cada hospital do país e, eventualmente também nas clínicas e laboratórios, todos capazes de informar doenças suspeitas como antraz, varíola ou Ebola. Ela insiste que não há preocupações com a privacidade porque as informações são armazenadas sem ligação com a identificação dos pacientes, permitindo identificar tendências suspeitas sem identificar as pessoas.

Em Chicago, a Oracle criou um bancos de dados criminais integrado e aplicou a tecnologia de mineração de dados para prever onde há probabilidade de ocorrerem ondas de crimes. Por exemplo, se o software identifica que brigas entre gangues armadas tendem a ocorrer em determinadas vizinhanças, em dias com determinado clima ou eventos esportivos, a polícia pode enviar mais policiais para determinado bairro na noite de um jogo importante (Rosen, 2004).

A proposta da Oracle de centralizar todos os bancos de dados criminais dos diversos órgãos federais e estaduais dos EUA, faz temer um grande potencial de invasão de privacidade. A visão da Oracle é que há três pontos na questão: privacidade, segurança dos dados e facilidade de uso. Os clientes decidirão quais dois desses três pontos serão privilegiados.

Mas há maneiras de proteger a privacidade e garantir um razoável nível de segurança. Se um sistema de cartões de identificação pessoal for limitado a uma verificação um-para-um, em vez de um-para-todos, o dano à privacidade é pequeno. Um sistema um-para-todos, como a proposta atual do governo norte-americano, permite que uma impressão digital encontrada em algum local seja comparada com todo um banco de dados, não apenas de criminosos. Um sistema um-para-um usa a própria impressão digital como chave para ler informações criptografadas gravadas no cartão de identificação. O indivíduo grava no cartão as informações necessárias, por exemplo,

para passar na alfândega, usando sua impressão como chave. Na alfândega, coloca o dedo num leitor, que converte a impressão num código matemático e lê os dados criptografados no cartão para confirmar que o portador é quem diz ser.

Isso também é aplicável a sistemas de saúde. Pode-se tornar anônimas as informações médicas em um banco de dados com milhões de pacientes, separando as informações médicas das de identificação. Isso permite estudar padrões de doenças, por faixa etária ou local, sem identificar os doentes. Em vez de registrar a idade exata da pessoa nas informações acessíveis, pode-se registrar por faixa (por exemplo, de 31 a 35 anos). E isso vale para vários outros indicadores, como hábitos de compra, faixas de salário, nível educacional.

Existem tecnologias de revelação seletiva, que permitem buscar informações em bancos de dados sem que os parâmetros de busca fiquem registrados. O “dono” do banco de dados não saberá que conjuntos de informações estão sendo buscados.

Atualmente, agentes de órgãos de informações do governo norte-americano, como CIA ou NSA, podem fazer cruzamentos de informações, como: em determinado período, houve quem comprasse fertilizante e também fizesse cursos de pilotagem? Encontrando alguns resultados, mas sem saber de quem são, o agente pode refinar a busca, para ver se entre os resultados há ligações telefônicas para determinados países e, quando achar que tem motivos suficientes para investigar uma ou mais pessoas, solicitar uma autorização judicial, com base nessas evidências, para quebrar o sigilo do(s) suspeito(s).

Todos esses exemplos mostram a importância de definir é o que será a Internet como meio de comunicação. Ela já é usada como ferramenta para integrar muitas bases de dados, e oferecer diversos serviços. Ela tem uma acelerada difusão na sociedade, com os fortes investimentos em telefonia e outras mídias de acesso, por enquanto ainda restritas às camadas economicamente superiores do estrato social, mas ampliando-se graças a investimentos privados e públicos.

Das 145 matérias d'O GLOBO comentadas aqui, 29% foram publicadas em um suplemento semanal especializado em informática, e não no corpo do jornal. Outras 30% trataram da questão das câmeras de vigilância, ainda não tão presentes no Brasil quando nos EUA, e quase todas as restantes, na maioria matérias estrangeiras, trataram dos problemas de vigilância e privacidade em outros países como se não fossem presentes e cada vez mais urgentes no Brasil. Embora a porcentagem de população afetada nos países mais ricos seja muito menor que no Brasil e em outros países "emergentes", a discussão desses problemas naqueles países é muito mais freqüente e abrangente que no Brasil, onde o assunto não é muito discutido na mídia de massa, e as "soluções" do Executivo ou do Legislativo brasileiros estão muito aquém de resolver a questão.

E há um outro importante aspecto, que não está ligado diretamente à discussão desta tese, mas que vale a pena destacar. Como cada vez mais serviços e negócios (públicos e privados) migram para a Internet, e nem todos mantêm um correspondente no mundo físico, a exclusão dos "não-conectados" é uma questão cada vez mais séria.

4. Conclusões

A discussão apresentada aqui abrange a interação homem-máquina, seja pelos sistemas de vigilância, seja pela coleta cada vez mais ampla de informações sobre usuários, em sistemas de CCTV (já comentados) ou em sistemas de *e-commerce* (comércio eletrônico), onde os processos de registro e consulta se mesclam.

Seja por acesso físico ou sem fio, por computadores de mesa ou portáteis, às redes governamentais ou empresariais e à telefonia celular de terceira geração, o cruzamento dos bancos de dados, cada vez mais presente, tem efeitos positivos e negativos nas relações pessoais e profissionais, e afeta diversos aspectos do *ethos* social.

A Internet está cada vez mais articulada com o comércio, e as estratégias de marketing são baseadas também no rastreamento dos usuários. Isso decide sobre a arquitetura da Internet, como meio de comunicação, como espaço de liberdade ou controle, cuja definição e equilíbrio dependem da legislação que regulamente essas relações.

Os consumidores consideram privados os dados sobre suas transações comerciais, de acordo com a filosofia capitalista. Mas os bancos de dados são, no argumento de Mark Poster, um discurso pós-moderno que atravessa e cancela a distinção entre público e privado. Se virmos os bancos de dados como um exemplo da noção de discurso de Foucault, os vemos como ‘exterioridades’, não como sendo constituídos por agentes, e procuramos por suas regras de formação como a chave para a maneira como formam os indivíduos. Os bancos de dados são listas organizadas, que podem ser cruzadas com listas em outros bancos de dados, pela interseção de campos de identificação pessoal, como o CPF brasileiro ou o SSN norte-americano. Essas listas tornam-se identidades sociais adicionais, à medida que cada indivíduo é constituído para o computador, com base no banco de dados em questão, em um agente social.

Sem referir-se de volta ao proprietário e aos seus interesses, ou pelo retorno ao indivíduo em questão, como modelo de sua adequação ou exatidão, o banco de dados é compreendido como uma produção de discurso que inscreve as posicionalidades do sujeito de acordo com suas regras de formação. Assim, o banco de dados passa a ser visto fora da dicotomia público/privado e fora da dinâmica do modo de produção.

Em vez disso, o discurso do banco de dados é uma força cultural que opera em um mecanismo de formação do sujeito que refuta o princípio hegemônico do sujeito como centrado, racional e autônomo. Agora, apenas por intermédio do banco de dados, o sujeito foi multiplicado e descentralizado, e pode ser objeto dos computadores em muitos locais sociais sem ter consciência disso, como se o indivíduo estivesse dentro do computador. Pode-se argumentar que os bancos de dados não podem ser caracterizados como discursos no sentido apresentado por Foucault, que são grandes coleções de textos, ligados por argumentos. Mas os bancos de dados são aglomerados de palavras e números cuja localização tem um significado específico. Eles formam grades de especificação, que são uma das três regras de formação do discurso apresentadas por Foucault. E eles constituem seus objetos (Lyon, 1996).

A Internet poderia ser uma cultura de liberdade, mas a confluência da tecnologia com o comércio pode fazer dela um local de perfeito controle. Deve-se considerar a importância do código (software) e o modo de regulação. Sem o código não há comunicação entre as bases de informações. O código determina como as informações são usadas, determina o grau de vigilância.

Um exemplo é a experiência da Microsoft e de outras *software houses* em controlar o uso do software pela Internet, limitando atualizações ou recursos, em vez de simplesmente vender uma licença de uso de um software instalado localmente. Outro exemplo é a integração de bancos de dados com informações pessoais, realizada pela Oracle para diversos órgãos governamentais e empresas privadas.

A grande preocupação com privacidade nos EUA, Canadá e Europa, tem como temas principais a monitoração do deslocamento físico de pessoas e veículos, a monitoração dos meios de comunicação pessoal (que ocorre mesmo sendo ilegal de acordo com várias constituições, inclusive a brasileira), os cruzamentos de bancos de dados para agrupar padrões de comportamento e a venda dessas informações a empresas. Uma coisa foi a criação dos censos, para administrar melhor os recursos públicos. Outra é a classificação social efetuada pelos mecanismos de vigilância com base nas informações dos bancos de dados. É o perfil obtido dessas informações que, cada vez mais, garante ao indivíduo acesso, inclusão, exclusão, direitos e a suspeita da probabilidade de doenças ou de um futuro comportamento criminoso.

Essa discussão reflete-se em uma grande frequência de artigos, livros e publicações jornalísticas sobre o tema, principalmente por teóricos da comunicação e sociólogos, em universidades nos EUA e Canadá, e também em recentes mudanças da legislação em países europeus. No Brasil, os jornais já relataram alguns casos de venda ilegal de informações sigilosas da SRF.⁷⁶

As novas técnicas de vigilância, e de coleta e organização de informações, possibilitam, principalmente pelo uso do número de registro no CPF em quase tudo, de cadastros a transações financeiras, o cruzamento entre diversos bancos de dados, criando perfis de comportamento, consumo, de informações médicas, que podem constituir um mecanismo eficaz de discriminação profissional e da restrição a serviços de saúde.

Ainda não existe uma legislação abrangente que garanta o direito à privacidade e à não discriminação, no Brasil, apenas algumas normas para casos específicos. Pelo contrário, há projetos de lei de implantação de um número único de identificação (inspirado no número de seguridade social dos EUA), de registro de comunicações eletrônicas (e-mails, ligações telefônicas) com mais detalhes que apenas quem se comunicou e quando, de implantação de chips em todos os veículos, de manutenção do mesmo número telefônico (embora na proposta isso seja opcional), de um cadastro único de saúde. O que consta a respeito na Constituição Brasileira são os seguintes pontos, na sua maioria ainda não claramente regulamentados por legislação específica:

DOS DIREITOS E DEVERES INDIVIDUAIS E COLETIVOS

Art.5º - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e a propriedade, nos termos seguintes:

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

⁷⁶ “Presos em SP três integrantes de quadrilha que vende dados sigilosos da Receita”, n’O GLOBO, 4 dez. 2004.

ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

LXXII - conceder-se-á habeas-data:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público.

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

§ 2º - Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.

Uma regulamentação consta no Código Penal Brasileiro:

“Art. 151 - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem. Pena - detenção de 1 a 6 meses, ou multa.”

Que tem um adjunto, criado pela Lei 9296, de 24 de julho de 1996, onde:

“Art.10 - Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática. Pena - reclusão de dois a quatro anos, e multa.”

Em outubro de 2001 o CNPq anunciou que estava financiando pesquisas sobre diversos aspectos de privacidade na “Chamada de Projetos Cooperativos ‘Tecnologias para o Desenvolvimento e Pesquisa em Conteúdos Digitais’”, que prevê estudos sobre análise, prospecção aprofundada e impacto de aspectos específicos da implantação de conteúdos digitais no Brasil em escala significativa do ponto de vista econômico e/ou social, o que, embora voltado para a área de informática, indica interesse em vários aspectos do problema da privacidade.

Há casos isolados discutidos na justiça trabalhista, como o já citado, do HSBC.

Mas no Brasil é cada vez mais comum um empregado ter de assinar um contrato, ao entrar na empresa, pelo qual aceita que seus e-mails serão monitorados automaticamente e indícios de violação de princípios éticos ou normas de conduta da empresa poderão acarretar diversas sanções, de advertência a demissão.

Uma vitória dos consumidores foi uma decisão do Ministério da Justiça em 2002⁷⁷, que atacou o uso de cadastro de consumidores pelas empresas e cláusulas abusivas em contratos de planos de saúde. O ministro Paulo de Tarso Ribeiro anunciou cinco cláusulas contratuais abusivas, que ferem os direitos dos consumidores. As empresas que utilizarem essas cláusulas em seus contratos serão processadas e correm o risco de serem fechadas ou de pagar multas que vão de R\$ 200 a R\$ 3 milhões.

Três cláusulas são referentes a cadastros de consumidores. Pela primeira, será considerado abusivo o envio do nome do consumidor a bancos de dados e cadastros de inadimplentes, como Serasa e o SPC (Sistema de Proteção ao Crédito), sem notificação prévia do consumidor para defesa. O ministério também reduziu a possibilidade do uso de mala-direta. Não será mais admitida a imposição ao consumidor de cláusulas em contratos de adesão que o obrigam a se manifestar contra a transferência de seus dados cadastrais a terceiros. Esse tipo de cláusula é muito comum em consórcios e, em muitas vezes, engloba informações como as preferências de consumo do comprador. A terceira medida torna ilegítima a autorização ao fornecedor para investigar a vida privada do consumidor. Essa prática é comum em contratos de financiamento de compra de imóveis.

Já as empresas de planos de saúde terão de abandonar dois tipos de cláusulas. Primeiro, não poderão mais impor em contratos limites de tempo para internação hospitalar. A medida vale apenas para contratos firmados após a vigência da Lei nº 9.656, de 3 de junho de 1998, que regula esses serviços, e visa evitar a retirada de doentes dos hospitais pelo fim do prazo de cobertura do plano. A segunda medida obriga os planos de saúde a não discriminar as chamadas “doenças de notificação compulsória”, como dengue e malária, deixando de cobri-las. Ribeiro explicou que há cláusulas dos planos de saúde que não devem ser mercantilizadas. “Só quem pode dizer sobre o tempo de internação é o médico”, justificou o ministro.

As medidas foram definidas de acordo com orientações dos Procons dos Estados e municípios e do Ministério Público. Essas entidades coletaram decisões da Justiça a favor de consumidores que sofreram abusos por parte de planos de saúde ou pelo uso de cadastros e enviaram informações ao Ministério da Justiça. As medidas valem a partir da publicação de portaria do ministério, prevista para hoje no “Diário Oficial”.

⁷⁷Governo restringe uso de cadastros, por Juliano Basile, no jornal Valor Econômico, 28 ago. 2002.

“A portaria é uma expressão das decisões da Justiça e representa a consciência jurídica dos Procons e do Ministério Público”, declarou Ribeiro. “As medidas restauram a dignidade do consumidor, reconhecem sua vulnerabilidade e disciplinam o mercado”, afirmou o ministro.

Em 21 de agosto de 2001, a FTC (Comissão Federal de Comércio dos Estados Unidos) declarou ser improvável uma lei de privacidade na Web. Em outubro o Congresso dos EUA aprovou diversas medidas emergenciais (muitas ainda vigentes, outras (como a consulta aos registros dos leitores nas bibliotecas públicas), previstas mas não aplicadas, têm chance de ser revogadas em 2006) de interceptação de comunicações por diversos meios, censura parcial aos meios de comunicação de massa, e cerceamento de liberdades civis, nem sempre com prévia autorização judicial, em função dos ataques terroristas a partir de 11 de setembro de 2001. A “Lei Patriótica” permite às autoridades federais realizar buscas secretas, obter registros privados e interceptar telefonemas, entre outras medidas para caçar suspeitos de terrorismo. Os democratas e outros críticos reclamam que o governo acumulou poder demais de espiar as vidas privadas dos cidadãos americanos e querem mudanças na lei.

A RIAA (a associação das gravadoras musicais americanas) tentou embutir nessa legislação o direito de invadir computadores conectados à Internet, em busca de supostos arquivos MP3 “ilegais” e de apagar esses arquivos, mas essa medida extrema não foi aprovada.

A “Lei Patriótica” dos EUA será revisada até fevereiro de 2006, e vários de seus mecanismos podem ser revogados.

É necessário garantir que o uso de informações pessoais seja restrito ao previsto em lei, devido ao impacto que sua divulgação irregular pode provocar na vidas dos indivíduos. No caso específico dos dados de saúde, a distribuição de dados do histórico médico do paciente deve ser limitada ao que o médico que o está atendendo necessita saber, garantindo a privacidade desses dados para que terceiros não tenham acesso aos mesmos. Se os laboratórios divulgarem (ou venderem) os dados dos pacientes para seguradoras (planos de saúde), elas poderão negar tratamento a pessoas que contraíram doenças não-propositalmente, ou seja, sem exposição irresponsável ao risco.

Ou as empresas poderão negar a contratação de empregados com propensão a determinadas patologias, como já ocorre com indivíduos em alguns planos de saúde.

Praticamente todas as tecnologias de vigilância podem ser projetadas para obter um equilíbrio entre a proteção da liberdade e da segurança. Mas os exemplos aqui discutidos mostram uma menor liberdade sem dar em troca uma (efetiva) maior segurança. Para Lawrence Lessig, professor de direito em Stanford, e forte defensor das liberdades individuais, esse equilíbrio depende muito dos valores que norteiam os projetistas e as instituições que criam essas tecnologias.

Diversos exemplos de vigilância e controle apresentados são muito presentes no passado recente. A Gestapo nazista tinha cerca de um agente para cada 10.000 alemães. A Stasi soviética chegou, na década de 1980, a ter um agente para cada 200 russos. A Stasi alemã oriental tinha registros de 6 milhões, dos 16 milhões de habitantes, empregando 100 mil agentes diretos e 180 mil informantes. O ditador romeno Nicolau Ceausescu pretendia construir um sistema de monitoração eletrônica capaz de abranger todas as famílias do país. Esses exemplos podem parecer exagerados mas constituem ferramentas de Estados de vigilância que nelas investiram pesadamente, a exemplo do que fazem hoje com as modernas tecnologias de vigilância.

Essas tecnologias, aliadas à mudança nas relações sócio-econômicas provocadas, ou provocadoras, da globalização, em seus diversos aspectos, estão criando, na visão de Whitaker, uma sociedade de vigilância. Por exemplo, foi afirmado no final dos anos 1990 que a empresa suíça Crypto AG, fornecedora de tecnologias de criptografia para diversos governos e empresas, permitiu à Agência Nacional de Segurança dos EUA ter acesso a comunicações supostamente secretas (Whitaker: 107). Já houve reclamações formais na OMC de que empresas norte-americanas foram favorecidas em concorrências internacionais pela divulgação a essas empresas de documentos de empresas de países concorrentes, utilizando mecanismos militares de vigilância dos EUA, inclusive no caso do SIVAM (Sistema Brasileiro de Vigilância da Amazônia).⁷⁸

⁷⁸ Segundo Bamford, a NSA realmente fez isso para defender a Raytheon de uma empresa francesa que empregava suborno nas licitações.

A vigilância em massa apresenta, segundo Rosen, três perigos distintos:

Ela cria o risco de um sistema burocrático ilimitado, encorajando os agentes a buscar as menores infrações para justificar sua ação, e que tem se mostrado como levando a perfis de discriminação étnica, e a ações que usam pequenos delitos, como um retorno na rua, por jovens negros, sem ligar a seta, como motivo para revistar suspeitos.

O segundo é não dar chances a alguém de ocultar seu passado (mesmo sem nenhum ato criminoso) para ter melhores oportunidades no futuro. Alguém que furtou algo de uma loja, uma vez, e pagou por isso, fica registrado para sempre. Criminosos considerados plenamente reabilitados têm seus dados pessoais divulgados pela Internet, são rejeitados pela vizinhança e perdem a chance de empregos. São estigmas muitas vezes desproporcionais às ações dos indivíduos. E programas de proteção a testemunhas, que dão novas identidades a quem ajuda as autoridades a processar criminosos, ou a simples denúncia de crimes, poderão ser inviabilizados.

O terceiro, e que atinge a toda a população, é a classificação (discriminatória) das pessoas com base em seus perfis eletrônicos: financeiros, médicos, profissionais. Essa discriminação digital, como a batizou David Lyon, é baseada em perfis de risco. E não há muita proteção legal contra isso, a não ser quando os perfis usam etnia ou religião como critérios.

Só uma transparência nos mecanismos, uma legislação clara, e uma supervisão definida podem limitar os perigos de uma vigilância desenfreada. E uma conscientização pública dos riscos envolvidos na perda da privacidade, com uma noção correta do equilíbrio entre vigilância e segurança. Esse não parece um futuro muito provável.

A penetração cada vez maior da Internet, e do uso de computadores nas transações financeiras (seja no registro das transações por cartão de crédito, em lojas ou via Internet, ou por cartão de débito nos caixas de PDV), nas comunicações telefônicas de voz ou dados, os bancos de dados cada vez mais abrangentes e integrados, vêm tornando a privacidade nos EUA, Europa, e também no Brasil, um bem cada vez mais escasso. No hemisfério sul, onde o alcance dessas tecnologias, embora crescendo muito depressa, ainda alcança uma parcela relativamente pequena da população, por enquanto

o problema não se afigura tão sério, mas é questão de menos de 20 anos para que atinja todos os trabalhadores formais e parte dos informais. Segundo o idbrasil, o portal de inclusão digital do Ministério das Comunicações, em outubro de 2005 já existiam 3200 espaços públicos para acesso à Internet.

No presente, com a liberdade de escolher sua identidade, e quanto risco deseja correr (embora essa noção de risco seja muito mais psicológica e influenciada pela mídia, que baseada em probabilidades reais), o Estado neoliberal não interfere nas escolhas individuais, e transfere para o privado a responsabilidade com a saúde, segurança, proteção. Mas os indivíduos exigem proteção do Estado contra quem os coloca em risco sem sua vontade e forma-se aí uma identidade baseada na inocência e na vitimização. E em função de um discurso difundido pela mídia que iguala vigilância a segurança, pois não há um espaço de discussão política acessível na mídia de massa, os indivíduos abrem mão de liberdades fundamentais em troca de uma sensação, não comprovada, de mais proteção.

Nas relações comerciais on-line, os indivíduos abrem mão da privacidade, usando-a como uma mercadoria, uma moeda de troca, ao voluntariamente (geralmente, sem opção, pois sem o cadastro não há como usufruir dos serviços oferecidos ou acessar os dados desejados) informar uma variada gama de informações pessoais, para serem reconhecidos e ter acesso ao que está sendo fornecido, conseguindo assim uma sensação de segurança. Muitas vezes esses dados são utilizados na formação de perfis de consumo ou comportamento e vendidos a diversos interessados, sem consulta prévia aos indivíduos.

O prof. belga Armand Mattelart, em entrevista sobre o Fórum Mundial Social, realizado em Porto Alegre em 2002, à Revista Vox nº 16, da Companhia Rio-Grandense de Artes Gráficas, Imprensa Oficial do Estado do Rio Grande do Sul⁷⁹, lembrou que a Internet, em todos os países do hemisfério sul, é usada por uma minoria da população, mas isso pode mudar depressa. Segundo ele:

⁷⁹ <http://www.corag.rs.gov.br/revistas/vox/016-pre/entrevista.html>, acesso em 10 nov. 2002.

No sul do planeta, estamos à mercê de uma informação que nos vem pelos grandes jornais, grandes veículos de mercado que são, antes de veículos de comunicação, grandes empresas, portanto discursando a partir do ponto de vista das empresas. Ficamos à margem de uma melhor informação que não chega a uma maioria da população. A Internet, meio em que muita gente aposta, também acaba não se inserindo mais profundamente na sociedade...

Sim, hoje a Internet está reservada a uma minoria. Mas se poderia mudar isso. Poderiam haver centros comunitários de utilização de Internet, o que implica, evidentemente, em se fazer um treinamento, e esse é um processo longo. Mas poderíamos começar. Eu penso que uma reforma fundamental seria introduzir a formação ao mundo da comunicação nas escolas, em todos os níveis. Isso é fundamental, acho a única solução. Podemos fazer um esforço para isso. Não sei como é aqui, mas na França há uma política voltada exclusivamente para a leitura de jornais. Já desde o primário se está colocando a leitura da imprensa como maneira de se ter uma visão crítica do que acontece. Mas isso não deve acontecer só com a imprensa escrita, mas com a imagem também.

O governo federal brasileiro prometeu, em 2004, retomar a implantação de acesso à Internet em todos os municípios com mais de mil habitantes. Isso dependia de pequenas alterações na legislação de telecomunicações, que disciplinem a oferta de serviços de acesso via operadoras de telefonia, sem excluir outras empresas prestadoras de serviços ou fornecedoras de conteúdo. E os planos do Ministério da Comunicações para a implantação da TV digital no Brasil incluem mecanismos de acesso à Internet a partir do televisor doméstico. Em breve, de interessante ferramenta para o desenvolvimento, o acesso “universal” à Internet passará a ser uma necessidade individual. Hoje já há pagamentos de impostos, acesso a processos judiciais e a informações governamentais que só são disponibilizados via Internet. E nem sempre com todas as precauções de segurança necessárias à proteção dos dados individuais.

As pessoas são cada vez mais identificadas em função do grupo a que pertencem. O indivíduo, mesmo sendo reconhecido como tal, não está desligado de seu grupo, das relações de sua rede social. Em “Os Sertões”, de Euclides da Cunha, Antônio Conselheiro é amparado por uma rede que o recobre de grandeza e inteligência. Já Moreira César, cheio de qualidades, nada vale devido à rede que o apóia.

O que cada um é, cada vez é menos fielmente representado pela massificação da coleta de dados históricos, financeiros, de segmento de mercado. Giddens reconhece que vem ocorrendo um conjunto de transformações estruturais que afetam a evolução da interação social. Ele destaca que a uniformização global separa tempo e espaço, reduzindo o conceito de local. A descontextualização e a reflexividade são transformações estruturais na modernidade que podem levar a mudar o conceito de interação, pois cada vez há mais diferenças entre as relações locais e a interação à distância. Isso muda a forma como se estabelecem as ligações e relações humanas, mudando a importância relativa da família, das comunidades virtuais, do governo.

Como lembra Michelle Perrot (Perrot: 612), Rousseau sonhava com uma absoluta transparência, “Se eu pudesse escolher o lugar de meu nascimento, escolheria um Estado onde, como todos os indivíduos se conheceriam entre si, as obscuras manobras do vício ou a modéstia da virtude não teriam como se ocultar aos olhos e ao julgamento do público”. Tocqueville, ao contrário, sublinhava as vantagens do individualismo, “expressão recente”, escreveu em 1850, definindo-o mais como um equivalente das sociabilidades: “O individualismo é um sentimento apazível que leva cada cidadão a isolar-se da massa de seus semelhantes e retirar-se, à parte, com sua família e seus amigos; de tal forma que, após ter criado assim uma pequena sociedade para seu uso, ele abandona de bom grado a grande sociedade a si própria”.

Essa talvez seja a realização das comunidades virtuais, ligadas pela Internet, onde cada um pode ligar-se a um grupo fisicamente próximo ou distante, mas com interesses comuns. Algo bem mais provável que o isolamento individual descrito em “A cidade e as estrelas”, de Arthur C. Clarke, onde cada um tem em sua casa um dispositivo de telepresença que leva sua imagem e sensações, junto às de outros, a um ciberespaço comum, onde interagem, o que contentou à maioria dos indivíduos, mas nem todos aceitaram viver um relacionamento não-presencial.

O comentário final de Perrot é:

“Mais emancipados dos constrangimentos do tempo e do espaço, os indivíduos aspiram à livre escolha de seu destino pela estrada ilusoriamente aberta da ambição. O cuidado consigo, com um corpo mais bem tratado e conhecido em sua complexidade nervosa, com uma psiquê cujos abismos se começa a divisar, com uma sexualidade

liberada da reprodução, até mesmo do casamento e do credo heterossexual, está no coração tanto da nova estética quanto das interrogações filosóficas. Esta expansão de individualismo atinge, em maior ou menor grau, todas as camadas da sociedade, sobretudo as urbanas.”

Isso pode ser muito válido na Europa, um pouco menos nos EUA e de aplicação restrita no Brasil. Ainda temos um longo caminho pela frente para poder integrar uma parcela razoável da população na sociedade sem fronteiras do ciberespaço, e os mecanismos de vigilância e controle cada vez mais presentes não nos garantem um caminho tão tranqüilo.

Os estudos atuais sobre vigilância buscam explicar as questões fazendo uso de novos conceitos e teorias. Essa busca implica um trabalho transdisciplinar, envolvendo a comunicação, a sociologia, a história, a psicologia, a teoria política, a economia, o direito e a informática. Como técnicas semelhantes são empregadas em diferentes áreas, o conhecimento de uma área é útil para entender outras áreas. E o entendimento da evolução da tecnologia desempenha um papel importante na compreensão dessas questões.

Com a vigilância gerando cada vez mais divulgação da vida pessoal, é necessário um cuidado muito grande no armazenamento e no acesso às informações. Os processos têm de ser transparentes e a ética tem de ser uma preocupação constante. Ou só o que vamos obter é mais exclusão social, menos direitos, menos oportunidades, menos liberdade.

ANEXO 1

Glossário de termos da Internet⁸⁰

ACK (Reconhecimento)

Resposta enviada de um computador receptor a um computador emissor para indicar o recebimento bem-sucedido de informações. O TCP exige que os pacotes sejam reconhecidos antes de considerar concluída a transmissão.

Adware

Qualquer aplicativo no qual são exibidos banners de propaganda durante a execução do programa. Os autores desses aplicativos incluem códigos que apresentam os anúncios, os quais podem ser vistos em janelas instantâneas (pop-ups) ou através de uma barra que aparece na tela do computador.

Agente

Encaminhamento de software em um dispositivo gerenciado por SNMP que responde a solicitações de get e set e envia mensagens de trap.

API (Interface de Programação de Aplicativos)

Uma vinculação de linguagem de alto nível que permite ao programador usar facilmente as funções em outro programa.

ARP (Protocolo de Conversão de Endereços)

Protocolo na suíte TCP/IP usado para converter um endereço (IP) de rede no seu endereço da camada de ligação.

Assinatura Digital

Uma assinatura eletrônica impossível de falsificar que autentica o remetente de uma mensagem e garante, ao mesmo tempo, a integridade dessa mensagem.

Ataque

Uma “agressão” eletrônica (normalmente não provocada) cujo objetivo é, de alguma forma, prejudicar os computadores, as redes e os mecanismos de segurança que constituem os alvos.

Ataque de Espionagem

Espionar passivamente o tráfego da rede para coletar dados ou segredos valiosos tais como senhas do usuário.

Ataque de Reprodução

Reprodução dos pacotes ou de outras mensagens da outra parte gravadas em um ataque de espionagem anterior, na tentativa de obter os mesmos resultados, ou resultados semelhantes, obtidos anteriormente.

Autenticação

Um método sistemático de estabelecer a comprovação da identidade entre duas ou mais entidades, normalmente usuários e hosts.

⁸⁰ <http://www.Internetsegura.org/glossario/glossario.shtml>, acesso em 7 jun. 2005.

Autenticação por AH

Um aperfeiçoamento planejado de segurança no IP que possibilita o envio de autenticação de computadores e a integridade dos datagramas, mas não proporciona sigilo.

Autoridade de Certificação (CA)

Uma entidade confiável que assina digitalmente os certificados para confirmar a propriedade de chaves públicas.

Autorização

Direito predeterminado de acesso a um objetivo ou serviço, com base em informações de autenticação.

BSD Trust

Um mecanismo de confiança pelo qual um host confia na identidade de usuários de outro computador sem exigir que eles se autenticem através de senhas.

Cabeçalho

Dados que aparecem no início de um pacote ou de outro tipo de mensagem, contendo informações essenciais à distribuição.

Camada de Aplicativos

A camada de protocolo usado por aplicativos (tais como Telnet, FTP, etc.), posicionada sobre os serviços prestados pelas camadas de transporte e de rede.

Camada de Rede

Na Internet, a camada que implementa o IP e presta serviços à camada de transporte.

Camada de Transporte

Na Internet, camada que implementa o TCP e o UDP através da camada de rede.

Camping Out (Acampamento)

Criação de um ponto seguro e não-detectado para atividades de hacking, armazenamento ou acesso de informações, e/ou para criar outra forma de entrada em um momento posterior após a entrada em uma rede.

Cavalo de Tróia

Um programa incorporado em um programa que, de outra forma, seria inofensivo, usado para atacar um local.

Chave

Um entre todos os valores possíveis que podem ser aplicados ao texto simples com um algoritmo de criptografia para gerar texto codificado, ou vice-versa.

Chroot (Mudança do Diretório-Raiz)

Uma chamada de sistema UNIX usada para impedir intencionalmente que um servidor veja arquivos confidenciais no sistema de arquivos do host.

Ciphertext (Texto Codificado)

Texto simples convertido em um formato secreto através do uso de um algoritmo criptográfico. Uma chave criptográfica pode desbloquear o texto simples original a partir do texto codificado.

Comandos “r”

Comandos remotos usados em UNIX entre servidores confiáveis. Quando são usados entre hosts confiáveis, o servidor confiável não precisa de uma senha para ser acessado a partir do o servidor confiável. Os comandos rlogin, rsh e rcp têm os problemas de segurança mais graves.

Conexão

Caminho lógico entre dois módulos de protocolos, que presta um serviço confiável de distribuição.

Controle de Acesso

Técnicas de limitação do acesso a recursos com base em informações de autenticação e regras de acesso.

Conversão de Nomes

Processo de correlação do nome de um host a um endereço IP. O DNS é o principal sistema da Internet para conversão de nomes de host.

Conversor

Software cliente que dá acesso ao banco de dados do DNS.

Covering Tracks

Um invasor que existe sem ser apanhado porque elimina, substitui ou desativa arquivos de log que, de outra forma, indicariam uma violação de segurança.

Cracker

Um hacker que não respeita os computadores que invade. A palavra é derivada de Criminal Hacker (Hacker Criminoso).

Criptoanálise

Ciência de análise e decodificação de comunicações seguras.

Criptografia

Processo de conversão de dados de um formato facilmente compreensível (texto simples) no que parece ser texto aleatório e inútil (texto grifado), até ser posteriormente decodificado.

Criptologia

Estudo das comunicações secretas, inclusive a criptografia e a criptoanálise.

Datagrama

Um pacote de dados e suas informações de distribuição, normalmente associado ao serviço sem conexão.

Decodificação

Operação inversa da criptografia; processo de conversão de texto codificado em texto simples.

Decodificadores de Senhas

Programas que permitem a um hacker adivinhar a senha de um computador ou de um usuário, usando dicionários ou a técnica conhecida como “força bruta”.

DES (Padrão de Codificação de Dados)

Adotado pelo governo dos EUA em 1977 como padrão federal de criptografia de dados informáticos comerciais e confidenciais (apesar de não ter restrições de segurança de acesso) do governo.

Diffie Hellmann ou Exponential Key Exchange (Troca Exponencial de Chaves)

Um conceito relativo à criptografia de chave pública que proporciona um mecanismo de criação de uma conexão secreta, mas sem autenticação, entre as duas partes.

Discadores

Programas que usam o modem do computador para conexão com um número pago ou site da Internet, normalmente para cobrança de tarifas. Esses programas são muito pequenos, +/- 100Kb.

DNS (Sistema de Nomes de Domínio)

Um banco de dados distribuído usado para correlacionar endereços IP com nomes de host. O DNS também possui informações para troca de e-mails.

Endereço IP

O endereço de 32 bits que identifica de maneira exclusiva um nó em uma rede IP.

Engenharia Social

Uso de mentiras, fraudes, representação e engenhosidade na redação para induzir usuários legítimos a divulgar segredos.

ESP (Encapsulating Security Payload)

Um aprimoramento planejado de segurança do IP.

Extranet

Uma rede compartilhada que utiliza a tecnologia da Internet para conectar empresas com seus fornecedores, clientes ou outras empresas. As informações compartilhadas podem ser acessadas apenas pelas partes colaboradoras ou podem ser disponibilizadas ao público em geral.

Ferramentas de Administração Remota

Programas que permitem que uma pessoa assuma o controle de outro computador sem o consentimento do proprietário, normalmente para roubar informações.

Filtro de Pacotes

Um dispositivo conectado em rede que procura informações do cabeçalho dos pacotes para determinar se eles devem ser bloqueados ou liberados pelo filtro.

Filtro de Servidor

Um firewall de host que registra e filtra o acesso dos clientes aos aplicativos do servidor.

Finger

Um comando do UNIX que fornece informações potencialmente úteis sobre um usuário e, às vezes, um servidor. Esse comando deve estar sempre desativado.

Firewall

Um ou mais filtros e gateways de pacotes que blindam as redes confiáveis “internas” das redes não-confiáveis “externas”, tais como a Internet.

Força Bruta

Também conhecido como “decodificação por força bruta”, é um método de tentativa e erro usado por aplicativos para decodificar dados criptografados tais como senhas ou chaves do Padrão de Codificação de Dados (DES), através de um esforço exaustivo (utilizando força bruta) em vez de estratégias intelectuais.

FQDN (Nome de Domínio Totalmente Qualificado)

Combinação dos nomes de host e de domínio de um computador.

FTP (Protocolo de Transferência de Arquivos)

Um protocolo de camada de aplicativos usado principalmente para cópia de arquivos entre computadores. Também se refere ao programa cliente que implementa o protocolo.

FTPD (Daemon de FTP)

Programa de servidor que implementa o protocolo FTP.

Gateway de Aplicativos

Sistema usado para restringir o acesso a serviços ou a funções específicas de serviços, através da fronteira de um firewall.

Hacker

Pessoa que obtém acesso ilegalmente ao seu computador.

Hash Único

Uma função que toma um texto simples de comprimento arbitrário como base e gera um valor pequeno (de tamanho fixo) que será a “impressão digital” da mensagem.

HTTP (Protocolo de Transferência de Hipertexto)

Protocolo de camada de aplicativos usado para distribuir texto, gráficos, sons, filmes e outros dados através da WWW, com a interface intuitiva de hipertexto de um navegador de Web.

HTTTPD (Daemon de HTTP (servidor))

Genericamente, refere-se a qualquer servidor de WWW.

ICMP (Protocolo de Mensagens de Controle da Internet)

Um protocolo de manutenção de IP que monitora e transmite informações de controle, inclusive a notificação de destinos inalcançáveis, entre participantes de uma rede.

IDEA (Algoritmo Internacional de Criptografia de Dados)

O IDEA é uma criptografia em bloco que funciona em blocos de texto simples de 64 bits. A chave tem comprimento de 128 bits.

Integridade

A condição de momento dos dados em comparação com o seu estado original.

Internet

Maior reunião mundial de redes, que chega a universidades, laboratórios de pesquisas de governos, empresas comerciais e instalações militares em muitos países.

IP (Protocolo de Internet)

Junto com o TCP, um dos protocolos mais fundamentais das redes TCP/IP. O IP é responsável pelo endereçamento e pela distribuição de datagramas pela Internet.

ISO (Organização Internacional de Normas)

Organismo internacional fundado para criar normas de protocolos de rede.

Java

Uma linguagem orientada a objetos, baseada em C++, que permite que os desenvolvedores desenvolvam aplicativos independentes de plataformas.

Kerberos

Um sistema distribuído de autenticação desenvolvido pelo MIT como parte do Projeto Athena, que identifica aplicativos de usuários, clientes e servidores um para o outro.

LAN

Uma rede de comunicações que cobre pequenas áreas geográficas.

Mascaramento de Endereços

Configuração de uma interface de rede com um endereço IP previsto para outro computador. Essa configuração enfraquece os mecanismos de controle de acesso baseados em endereços de rede.

MIB (Base de Informações de Gerenciamento)

Um banco de dados de objetos que representa vários tipos de informações sobre um dispositivo. Usado pelo SNMP para o gerenciamento de dispositivos.

MIT-MAGIC-COOKIE-1

O mecanismo disponível universalmente, mas usado com pouca frequência, para o X Windows System, que pode ajudar a evitar acessos não-autorizados à tela gráfica, ao teclado e ao dispositivo apontador do usuário.

MTA (Agente de Transferência de Mensagens)

Uma entidade que se responsabiliza pela transferência de mensagens de e-mail aos seus destinos, ou pelo menos a um passo antes deles.

Negação de Serviço (DoS)

Interrupção de serviços de Internet ou de IP por uma inundação de tráfego falso que entope a rede do provedor. SYN Flood, Ping o' Death e Ping Flooding são alguns exemplos de ataques de Negação de Serviço.

NFS (Sistema de Arquivos de Rede)

Um sistema distribuído de arquivos, com autenticação fraca, baseado no RPC, que foi desenvolvido pela Sun Microsystems. Os clientes do NFS montam diretórios remotos de servidor e, em seguida, os acessam como se fossem locais. Veja também NFS Seguro.

NFS Seguro

Uma versão aprimorada do NFS incorporada ao RPC Seguro, que permite o acesso autenticado e criptografado a arquivos armazenados em um servidor remoto.

NIS (Serviço de Informações de Rede)

Um serviço de nomenclatura desenvolvido pela Sun, que presta um serviço de diretório para informações sobre redes e hosts.

NNTP (Protocolo de Transferência de Notícias em Rede)

Usado para distribuição, consulta, acesso e publicação de artigos no sistema de notícias da Usenet.

OSI (Interconexão de Sistemas Abertos)

Um conjunto de normas da ISO que define a base de implementação de protocolos de rede em sete camadas.

Pacote

Uma unidade de dados de protocolo; muitas vezes, usado como sinônimo de segmento e datagrama.

PEM (Privacy Enhanced Mail)

Um padrão de criptografia de mensagens e de autenticação dos remetentes.

Phishing

Na Internet, o phishing (às vezes chamado de carding ou brand spoofing) é um golpe no qual o autor distribui e-mails com aspecto legítimo, aparentemente vindos de alguns dos mais importantes sites da Web, com a intenção de roubar informações particulares e obter acesso às contas bancárias ou aos serviços por assinatura da vítima.

Phreaker

Um hacker telefônico. Termo originado de PHone fREAKER.

Piadas

Não se trata de um vírus, e sim de um programa que simula comportamentos destrutivos, por exemplo: “o disco rígido do seu computador será apagado se você não responder a uma série de perguntas dentro de um determinado período de tempo”.

Ping Sweep

Uma técnica de reconhecimento de rede que usa o eco de ICMP (pings) para mapear uma rede.

Ping of Death

Um ataque de negação de serviço. O Ping of Death pode travar ou reiniciar um grande número de computadores através do envio de uma mensagem de “ping” maior que 65.536 bytes (o tamanho predefinido é 64 bytes).

POP3 (Protocolo de Correio, versão 3)

Um protocolo de e-mail usado principalmente para transferir novas mensagens de um servidor central de e-mail para as estações de trabalho dos usuários.

Porta

Identificadores de 16 bits, usados pelo TCP e pelo UDP, que servem para especificar qual processo ou aplicativo está enviando ou recebendo dados.

Port Sweep

Uma técnica de reconhecimento de rede que identifica os serviços disponíveis em um host.

Protocolo

Um conjunto de regras usadas para controlar a transmissão e o recebimento de dados.

Protocolos em Camadas

Protocolos que são “empilhados” um sobre o outro, onde os protocolos “inferiores” prestam serviços de maneira transparente para os “superiores”.

Punch

Criar um “buraco” em um dispositivo ou em uma rede, permitindo a entrada legal ou ilegal.

PUP

PUP (programa potencialmente indesejável) é um programa que pode ser indesejável, apesar da possibilidade de que os usuários tenham permitido o seu download. Entre os PUPs estão programas espiões (spyware), programas de propaganda (adware) e discadores. Muitas vezes, eles são baixados junto com um programa que o usuário deseja ter

Reconhecimento

Delimitação de possíveis alvos para concentrar-se no alvo mais lucrativo e menos protegido.

Relay

Um programa que transmite dados sem estruturação entre um aplicativo cliente e um servidor, através de um firewall intermediário.

Remetente de Correio Eletrônico Anônimo

Um programa que elimina todos os vestígios do verdadeiro remetente e da verdadeira localidade de mensagens de e-mail antes de encaminhá-las ao seu destinatário pretendido.

RFC (Solicitação de Comentário)

Documentos escritos para e pela comunidade da Internet, descrevendo protocolos da Internet, pesquisas, medições, idéias e observações.

RIPEM (Riordan's Internet Privacy Enhanced Mail)

Uma implementação específica e amplamente conhecida do padrão PEM.

Rota

Caminho tomado pelo tráfego de rede da sua origem até o seu destino.

Rota de Origem

Uma rota que identifica o caminho que um datagrama precisa seguir, determinado pelo dispositivo de origem.

Roteador

Dispositivo de computação específico, dedicado à distribuição de pacotes entre terminais de comunicação.

RPC (Chamada de Procedimento Remoto)

Um mecanismo fracamente autenticado que permite a um aplicativo chamar um procedimento que será executado em uma máquina remota. Veja também RPC Segura.

RPC Segura

Uma versão do RPC aprimorada para permitir o uso da criptografia DES através da conexão de rede.

RSA (Rivest-Shamir-Adleman)

O primeiro (e, ainda hoje, o mais usado) sistema criptográfico de chave pública a oferecer funções de criptografia e de assinatura digital.

Screening Router (Roteador com Triagem)

Um roteador com recursos de filtragem de pacotes ativada.

Segmento

Uma unidade de dados de protocolo que consiste no envio parcial de um fluxo de bytes entre duas máquinas. Além disso, ele possui informações sobre a posição de momento do fluxo e um valor de soma de controle (checksum).

Senhas Descartáveis

Senhas de usuários que são usadas apenas uma vez para estabelecer a autenticação, não estando, portanto, sujeitas a espionagem e ataques de reprodução.

Senhas Estáticas

Em contraste com as senhas descartáveis, as senhas de estáticas são reutilizadas várias vezes para fins de autenticação. Como podem ser reutilizadas, as senhas estáticas estão sujeitas a espionagem e ataques de reprodução.

Serviços Gerenciados de Segurança

Uma abordagem sistemática de gestão das necessidades de segurança de uma organização. Os serviços podem ser realizados internamente ou delegados a um provedor de serviços que supervisione a segurança das redes e dos sistemas de informação de empresas.

Serviço sem Conexão

Um serviço de distribuição que trata cada pacote de maneira independente de todos os outros anteriores ou posteriores a ele. Isso pode levar à perda, à duplicação ou à falta de seqüência dos pacotes.

Serviços Orientados à Conexão

Um serviço de distribuição que oferece um fluxo de dados bem organizado, inclusive disposições que dão garantia contra pacotes perdidos, fora de seqüência e duplicados.

Shadow Passwords (Senhas Ocultas Ativadas)

Senhas de usuários armazenadas em um banco de dados que pode ser acessado apenas por administradores de sistema com os direitos necessários.

Shoulder Surfing

Descobrir o que o usuário está digitando, olhando por cima do seu ombro e observando o teclado ou o monitor.

S-HTTP (Protocolo de Transferência Segura de Hipertexto)

Uma extensão do HTTP com melhorias de segurança, projetado para viabilizar o comércio pela WWW.

Sigilo

Garantia de privacidade, muitas vezes conseguida na através do uso da criptografia.

Sistema Criptográfico de Chave Pública

Um sistema de criptografia no qual metade de um único par de chaves é usada para criptografia, e a outra metade é usada para a decodificação.

Sistema Criptográfico de Chave Secreta

Um sistema criptográfico no qual a mesma chave é usada para criptografia e decodificação.

SKIP (Gerenciamento de Chaves Simples para Protocolos de Internet)

Um sistema de autenticação/criptografia que protege a rede no nível de pacotes de IP.

SMTP (Protocolo Simples de Transferência de E-Mails)

Protocolo usado para transferir mensagens de correio eletrônico de uma máquina para outra.

SNMP (Protocolo Simples de Gerenciamento de Rede)

Protocolo usado para gerenciar redes locais na Internet. O SNMP permite que uma estação de gerenciamento configure, monitore e controle dispositivos de rede tais como roteadores.

Soquete

Um caminho bidirecional para recebimento e envio de dados, permitindo que um aplicativo tenha acesso aos protocolos de TCP/IP.

SPAM

O spam é uma mensagem de e-mail não-solicitada. (As mensagens desejadas são, algumas vezes, chamadas de ham) Do ponto de vista do remetente, o spam é uma forma de mala direta, muitas vezes enviada a uma lista obtida através de um spambot, ou a uma lista obtida por empresas especializadas em criar listas de distribuição de e-mail. Para o destinatário, normalmente se trata de lixo eletrônico.

Spambot

Um spambot é um programa projetado para coletar, ou “colher”, endereços de e-mail na Internet para criar listas de envio de e-mail no sentido de enviar mensagens não-solicitadas. Um spambot pode coletar endereços de e-mail em sites, grupos de notícias, publicações em grupos de interesse especial (SIG) e diálogos em salas de bate-papo. Como os endereços de e-mail possuem um formato distintivo, é fácil escrever spambots.

Spammer

Pessoa que distribui mensagens não-solicitadas. (Veja SPAM)

Spoofing (Falsificação) de Endereços

Falsificação de datagramas IP para fazer o sistema receptor acreditar que eles são provenientes de um host que não seja o verdadeiro remetente.

Spyware (Programas Espiões)

Programas espiões são tecnologias que auxiliam na coleta de informações sobre uma pessoa ou empresa sem seu conhecimento. Na Internet (onde também são conhecidos como spybots ou software de rastreamento), os programas espiões são códigos inseridos no computador de uma pessoa para coletar secretamente informações sobre o usuário e enviá-las a anunciantes ou outras partes interessadas. Os programas espiões podem entrar em um computador como um vírus ou devido à instalação de um novo programa.

Squatting (Acantonamento)

Veja Camping Out.

SSL (Secure Sockets Layer)

Uma camada de segurança intermediária entre as camadas de aplicativos e de transporte. A SSL protege discretamente os protocolos da camada de aplicativos (tais como o HTTP, para o qual ela foi concebida inicialmente) e de dados, com pouco esforço por parte do desenvolvedor de aplicativos.

TCP (Protocolo de Controle de Transmissão)

Protocolo de transporte voltado para a conexão, que permite uma transmissão bidirecional completa (full duplex) de dados entre duas entidades, freqüentemente entre um aplicativo cliente e um servidor.

Telnet

Protocolo de terminal remoto que permite que um terminal conectado a um host se conecte a outros hosts, como se estivesse diretamente conectado à máquina remota.

Texto Simples

Texto que pode ser lido e compreendido livremente por qualquer pessoa; o oposto de “texto codificado”.

TFTP (Protocolo de Transferência Trivial de Arquivos)

Um protocolo não-autenticado e sem “enfeites”, usado para transferir arquivos. O TFTP depende do UDP e, muitas vezes, é usado para reiniciar estações de trabalho que não usam discos.

TTL (Time-To-Live, ou “Tempo de Vida”)

Número máximo de saltos de roteador que um datagrama pode realizar em uma rede antes de ser descartado. Usado para impedir que os pacotes entrem em um loop infinito.

UDP (Protocolo de Datagramas de Usuários)

Um protocolo de transporte sem conexão. A distribuição não é garantida, nem se garante que os datagramas serão distribuídos na ordem correta.

Verificação de Integridade

Mecanismo para garantir que os dados não foram adulterados através da adição, retirada ou outra modificação do seu conteúdo. Muitas vezes, é realizada através de assinaturas digitais e funções de hash unidirecional.

WAN (Rede Remota)

Uma rede física de comunicações que cobre grandes distâncias geográficas. Normalmente, as WANs funcionam em velocidades mais baixas que as LANs.

Worm

Num computador, um worm é um vírus que se copia sozinho e não altera arquivos, mas permanece residente na memória ativa. Os worms utilizam partes de um sistema operacional que são automáticas e, normalmente, invisíveis para o usuário. É comum que os worms sejam percebidos apenas quando a sua cópia descontrolada começar a consumir recursos do sistema, deixando lentas ou interrompendo outras tarefas.

Wrapper

O pacote “wrapper” realiza duas funções básicas: ele registra solicitações de serviços de Internet e proporciona um mecanismo de controle de acesso para sistemas UNIX.

WWW (World Wide Web, ou “Rede Mundial”)

Uma visão coesa e intuitiva da Internet através de muitos protocolos, especialmente o HTTP.

X Window System

Um sistema de criação de janelas gráficas, desenvolvido no MIT, que permite ao usuário executar aplicativos em outros computadores e exibir o resultado.

ANEXO 2

A Câmara Brasileira de Comércio Eletrônico (Camara-e.net) lançou em 2 de junho de 2005 uma cartilha que ensina o consumidor a se precaver dos maus negócios.⁸¹ Batizada de “Cartilha do e-Consumidor”, fica em <http://www.camara-e.net/e-consumidor/com>, e orienta como identificar uma loja virtual segura, que cuidados tomar com senhas e dados pessoais e como efetuar pagamentos seguros, entre outras questões.



Recomendações de segurança para compras bem sucedidas pela Internet.

Introdução

1. Comprando em uma loja virtual
 - 1.1 Identifique o fornecedor;
 - 1.2 Verifique a segurança do site;
 - 1.3 Proteja seus dados pessoais;
 - 1.4 Escolha uma senha segura;
 - 1.5 Verifique as características do produto;
 - 1.6 Verifique as políticas da loja quanto a entrega, formas de pagamento, garantia do produto e condições de troca;
 - 1.7 Verifique o preço e a incidência ou não de tarifas para envio;
 - 1.8 Mantenha registro de tudo;
 - 1.9 Muita atenção aos e-mails que recebe.

2. Comprando em um site de compra e venda
 - 2.1 Escolha uma senha segura;
 - 2.2 Proteja seus dados pessoais;
 - 2.3. Verifique se está de fato na página do site de compra e venda;
 - 2.4 Esgote suas dúvidas sobre o produto através dos campos de “perguntas e respostas”;
 - 2.5 Verifique se o preço do produto não está muito abaixo do valor de mercado;
 - 2.6 Verifique o histórico de negociações do anunciante;
 - 2.7 Verifique a possibilidade de pagar somente na entrega;
 - 2.8 Verifique titularidade e local da conta bancária do vendedor;
 - 2.9 Procure contatar o vendedor por um telefone fixo;
 - 2.10 Verifique as políticas do vendedor quanto a entrega, formas de pagamento, garantia do produto e condições de troca;
 - 2.11 Muita atenção aos e-mails que recebe.

⁸¹ GOMES, Wagner. *Cartilha orienta compras na Internet*. n’O GLOBO, 7 jun. 2005

Introdução

A Internet tem se revelado uma excelente ferramenta para compras. Ela permite que o consumidor compare preços, pesquise funcionalidades dos produtos e adquira o que melhor lhe convém confortavelmente, sem sair de casa e sem precisar adaptar-se aos horários das lojas convencionais.

A desnecessidade de manter espaços físicos como lojas, aliada à forte concorrência que acontece no ambiente virtual, faz com que a Internet também se mostre um excelente barateador de preços.

Além disso tudo, a rede mundial funciona como uma enorme vitrine, possibilitando que os produtos anunciados em qualquer canto do Brasil sejam visualizados em tempo real do outro lado do país, o que seria impossível no ambiente “não virtual”.

Muitas pessoas, contudo, hesitam antes de aventurar-se nesse novo modelo comercial por medo de fraudes de todo tipo. Más experiências de consumidores no comércio eletrônico são franca minoria, mas apesar disso, elas alertam para a necessidade de se tomar algumas cautelas básicas ao comprar pela Internet. Essas cautelas poderão evitar contratemplos e dissabores.

1. Comprando em uma loja virtual

Lojas virtuais são empresas que anunciam à venda produtos ou serviços sob seu próprio nome. Elas podem ter estabelecimentos físicos também ou não. O que importa é que a própria empresa mantenedora do site é quem está de fato vendendo os produtos ou serviços anunciados, como se tratasse de uma loja mesmo, apenas alocada não no espaço físico, mas na Internet. Veja algumas cautelas simples e úteis que você pode tomar quando se interessar por um produto anunciado por uma loja virtual.

1.1. Identifique o fornecedor

Ao interessar-se por adquirir um produto anunciado em uma loja virtual, o primeiro passo é procurar no site a identificação da loja. Averigüe se há no site informações sobre razão social, CNPJ, endereço e outras formas de contato além do e-mail.

Aumente as cautelas quando o site exibir como formas de contato, além da própria plataforma online, apenas um telefone celular. Sempre é bom comprar em estabelecimentos conhecidos, dos quais você tenha colhido bons testemunhos com amigos ou familiares.

1.2. Verifique a segurança do site

Toda compra em uma loja virtual implica no envio de dados como número de telefone, endereço para entrega, número do cartão de crédito etc. É importante, portanto, averiguar se a loja é segura, ou seja, se ela toma as medidas necessárias para evitar que esses dados sejam interceptados e utilizados de forma imprópria. Faça isso averiguando se existe um ícone em forma de um cadeado no canto inferior direito da tela. Lojas seguras também têm seu endereço eletrônico começando com a sigla “https”. Lembre-se de que é relativamente fácil para alguém que conheça um pouco de informática imitar a

aparência de um site. É possível que alguém mal intencionado, portanto, crie um site em tudo igual ao de uma loja virtual consagrada, simulando a venda de produtos com o intuito de se apoderar de dados como senha, telefone e número de cartão de crédito do comprador.

Para tanto, é possível que ele até mesmo imite a URL (o “endereço eletrônico” da página) do site, só fazendo faltar uma letra do nome, por exemplo. Aumente as cautelas quando houver alguma alteração em relação à página da loja virtual que você já conhece. Páginas que, embora mantendo cores e formatos originais, apresentam alterações e não têm os elementos mencionados acima (ícone de cadeado e “https” no endereço) devem ser evitadas.

1.3. Proteja seus dados pessoais

Ao preencher formulários para uma compra, evite acrescentar informações que não têm nenhuma utilidade prática imediata à concretização do negócio. Sempre é bom ter o máximo de cuidado com sua senha pessoal. Algumas lojas virtuais pedem que você escolha uma senha para poder comprar.

Esta senha, assim como as suas senhas bancárias, devem ser mantidas em total sigilo. Evite informá-las a quem quer que seja, evite responder e-mails que pedem sua senha (mesmo que esses e-mails pareçam ter sido remetidos pela loja na qual você é cadastrado) e evite colocar sua senha em uma página que não seja segura (veja o item 1.2).

Também vale a pena dar uma olhada na Política de Privacidade da loja virtual, para saber qual o compromisso que ela assume no que diz respeito à manipulação dos dados que você confiar a ela. Evite também colocar sua senha ou seus dados pessoais em e-mails, ainda que eles aparentemente tenham sido enviados pelo site no qual você se cadastrou.

1.4. Escolha uma senha segura

Caso a loja virtual exija a escolha de uma senha quando você se cadastrar, tenha cuidado para eleger uma senha que seja de difícil interceptação por terceiros. Evite senhas que você mantém em outros sites, bem como datas de aniversário (sua ou de familiares), seu número de telefone, palavras conhecidas (como “cavalo”, “casa”, etc) e seqüências numéricas ou alfabéticas (como 12345 ou ABCDEF).

Evite também seqüências de letras como encontradas no teclado do computador (como asdfg). Sempre é bom buscar escolher uma senha entre 6 e 12 caracteres, alternando letras minúsculas, letras maiúsculas e números de forma aleatória.

1.5. Verifique as características do produto

Evite comprar por impulso. Antes de efetivar a compra, analise bem a descrição do produto, faça comparações, certifique-se de que o produto se encaixa em sua necessidade ou interesse.

Aumente as cautelas quando a loja virtual exibir poucas informações sobre o produto.

Sempre é bom visitar a página do fabricante do produto na Internet, quando houver, e confirmar as funcionalidades do produto, tirando dúvidas que talvez a página da loja não tenha conseguido tirar.

1.6. Verifique as políticas da loja quanto a entrega, formas de pagamento, garantia do produto e condições de troca

Prazo de entrega, formas de pagamento que a loja aceita, tempo de garantia do produto e em que situações ele poderá ser trocado (e como isso será feito) são informações que a loja precisa fornecer em sua página na Internet. Certifique-se de que essas políticas sejam razoáveis.

Aumente as cautelas quando a loja tiver uma política de impossibilitar ou de tornar muito complicada a troca, ou ainda quando a loja se reservar o direito de não efetuar a devolução total do preço pago (fora frete) em caso de produto com defeito.

1.7. Verifique o preço e a incidência ou não de tarifas para envio

Muitas vezes o preço exibido no anúncio não envolve o custo da remessa do produto até a casa do consumidor. Certifique-se de que o valor do frete esteja claro.

1.8. Mantenha registro de tudo

Guarde toda informação relacionada à compra. Não apague e-mails. Sempre é bom imprimir o anúncio, as telas de compra e toda a comunicação trocada com a loja. Lembre-se de que o fornecedor de produtos (caso da loja virtual) é obrigado a cumprir com as ofertas que fizer, segundo o Código de Defesa do Consumidor.

1.9. Muita atenção aos e-mails que recebe

Tenha cuidado ao abrir anexos ou clicar em links de e-mails que você recebe, ainda que eles aparentemente tenham sido remetidos pela loja virtual na qual você é cadastrado. Eles podem esconder vírus ou programas que visam capturar informações suas.

Aumente as cautelas quando o e-mail tiver erros de ortografia e/ou exigir que você coloque sua senha ou outras informações pessoais na resposta ou na página da Internet para qual ele remeter.

Sempre é bom ao clicar no link contido em um e-mail recebido da loja virtual, verificar se a página da Internet que abrir é segura (ver o item 1.2).

2. Comprando através de um site de compra e venda

Sites de compra e venda são também conhecidos como “sites de leilão”. Esses sites são fornecedores de serviços (e não de produtos, como a loja virtual) e oferecem espaço para que terceiros anunciem seus produtos à venda, de forma bem parecida com a que jornais

fazem em suas sessões de classificados. Assim, a compra será efetuada não do site, mas de um terceiro, responsável pelo anúncio. Adote as seguintes cautelas e boas compras!

2.1. Escolha uma senha segura

Caso o site de compra e venda exija a escolha de uma senha quando você se cadastrar, tenha cuidado para eleger uma senha que seja de difícil interceptação por terceiros.

Evite senhas que você mantém em outros sites, bem como datas de aniversário (sua ou de familiares), seu número de telefone, palavras conhecidas (como “cavalo”, “casa”, etc) e seqüências numéricas ou alfabéticas (como 12345 ou ABCDEF). Evite também seqüências de letras como encontradas no teclado do computador (como asdfg).

Sempre é bom buscar escolher uma senha entre 6 e 12 caracteres, alternando letras minúsculas, letras maiúsculas e números de forma aleatória.

2.2 Proteja seus dados pessoais

Quando em contato com o vendedor, evite passar-lhe informações pessoais que não tenham relação direta com a concretização do negócio.

2.3 Verifique se está de fato na página do site de compra e venda

Lembre-se de que é relativamente fácil para alguém que conheça um pouco de informática imitar a aparência de um site. É possível que alguém mal intencionado, portanto, crie um site em tudo igual ao de um site de compra e venda consagrado, com o intuito de se apoderar de dados como senha, telefone e número de cartão de crédito do comprador.

Para tanto, é possível que ele até mesmo imite a URL (o “endereço eletrônico” da página) do site, só fazendo faltar uma letra do nome, por exemplo. Verifique se, no momento em que for solicitado que você digite sua senha ou coloque algum de seus dados pessoais, a URL começa com “https” e se há um cadeado no canto inferior direito da tela.

Aumente as cautelas quando houver alguma alteração em relação à página do site que você já conhece. Páginas que, embora mantendo cores e formatos originais, apresentam alterações e não têm os elementos mencionados acima (ícone de cadeado e “https” no endereço) devem ser evitadas.

Sempre é bom evitar colocar sua senha ou seus dados pessoais em e-mails, ainda que eles aparentemente tenham sido enviados pelo site no qual você se cadastrou.

2.4 Esgote suas dúvidas sobre o produto através dos campos de “perguntas e respostas”.

Uma característica dos sites de compra e venda é a possibilidade de os interessados no produto anunciado fazerem perguntas ao anunciante. Este é o momento de esgotar as dúvidas, avaliar compatibilidade, características e funcionalidades do produto. Aumente as cautelas quando o anunciante não responder às perguntas que são feitas.

2.5 Verifique se o preço do produto não está muito abaixo do valor de mercado.

Ainda que seja mais barato para o comerciante anunciar seus produtos na Internet do que em uma loja física, pagando luz, água e empregados, é impossível comercializar produtos por preços escandalosamente abaixo dos praticados no mercado. Se for o caso, redobre as cautelas.

2.6 Verifique o histórico de negociações do anunciante.

Uma característica dos sites de compra e venda é a possibilidade de verificar o histórico de negociações do anunciante com outros usuários do site. Esse histórico fica expresso em forma de pontuação ao lado do codinome do usuário, pois cada comprador que manifesta no site ter a negociação sido satisfatória representa um ponto para o vendedor.

Por outro lado, cada comprador insatisfeito representa um ponto negativo no histórico do vendedor. Assim, um vendedor com pontuação alta indica que ele já negociou com muitas pessoas, recebendo delas testemunhos positivos, o que gera uma presunção de idoneidade do vendedor.

Sempre é bom analisar o que as pessoas que negociaram com o vendedor disseram sobre a negociação. Verifique, também, se o usuário é cadastrado no site há tempo suficiente para ter o número de testemunhos positivos que tem, para evitar confiar em alguém que tenha testemunhos forjados.

2.7 Verifique a possibilidade de pagar somente na entrega.

Negocie com o vendedor a utilização de ferramentas como o Sedex a cobrar, dos Correios, ou um intermediador financeiro. Intermediadores financeiros são empresas que, mediante o pagamento de uma pequena taxa, recebem o dinheiro do comprador e só o liberam para o vendedor quando o comprador manifestar haver recebido o produto em boas condições.

Essas medidas são muito úteis para evitar perder o dinheiro depositando-o antecipadamente na conta de um estranho que pode não enviar o produto. Aumente as cautelas quando o vendedor se negar a utilizar esses expedientes, especialmente se o produto no qual você está interessado for de alto valor.

2.8. Verifique titularidade e local da conta bancária do vendedor.

Caso você decida depositar o valor do produto em uma conta bancária antes de receber o produto, certifique-se de que o titular da conta seja de fato o usuário do site de compra e venda. Lembre-se de que, ao manifestar interesse em um produto, lá no site, este lhe encaminha os dados de contato com o vendedor, incluindo-se aí o nome dele e a localidade em que ele mora.

Aumente as cautelas quando o vendedor pedir para que o depósito seja feito em nome de terceiros, como sócios ou parentes. Evite, também, depositar o dinheiro em conta poupança. Também redobre a atenção quando a agência bancária for de uma cidade diferente daquela na qual o vendedor deveria se encontrar. Isso pode ser feito acessando a página na Internet do banco onde se encontra a conta.

2.9. Procure contatar o vendedor por um telefone fixo.

Busque sempre fazer o contato com o vendedor através de um telefone fixo. Se o site não puder lhe informar o número de um telefone fixo do vendedor, peça a ele, por e-mail ou pelo celular, essa forma de contato.

2.10 Verifique as políticas do vendedor quanto a entrega, formas de pagamento, garantia do produto e condições de troca.

Prazo de entrega, formas de pagamento que o vendedor aceita, fornecimento de nota fiscal, tempo de garantia do produto e em que situações ele poderá ser trocado (e como isso será feito) são informações que o anunciante precisa fornecer. Certifique-se de que essas políticas sejam razoáveis.

2.11 Muita atenção aos e-mails que recebe.

Tenha cuidado ao abrir anexos ou clicar em links de e-mails que você recebe, ainda que eles aparentemente tenham sido remetidos pelo site de compra e venda no qual você é cadastrado. Eles podem esconder vírus ou programas que visam capturar informações suas. Aumente as cautelas quando o e-mail tiver erros de ortografia e/ou exigir que você coloque sua senha ou outras informações pessoais na resposta ou na página da Internet para qual ele remeter. Sempre é bom ao clicar no link contido em um e-mail recebido do site de compra e venda, verificar se a página da Internet que abrir é segura (ver o item 2.3).

ANEXO 3

O **Movimento Internet Segura**⁸² foi criado com o objetivo de tirar dúvidas e divulgar informações claras e precisas sobre questões relacionadas à segurança e à integridade na rede mundial de computadores.

- Vírus: é um programa ou código feito pelo homem...
- Worms: são vírus que residem na memória...
- Spywares
- Phishing & Scams
- Técnicas usadas pelos fraudadores

Práticas para evitar fraudes na Internet

1) Proteja seu computador

Tenha instalado antivírus (de preferência atualizado automaticamente, porque nós temos a tendência de esquecer de fazer as atualizações manualmente), um firewall e um anti-spams.

2) Não forneça senhas

Nunca informe qualquer senha para qualquer pessoa ou para qualquer pedido de cadastramento ou recadastramento sob nenhum argumento.

3) Atenção no destinatário

Recuse qualquer e-mail cujo o remetente seja desconhecido, ou que sua identidade levante suspeitas. Essas mensagens devem ser apagadas. Preste atenção em endereços falsos.

4) Pagamento

Uma das formas mais comuns de aplicação de golpes é a exigência de pagamentos antecipados. Certifique-se sobre a procedência do site e em caso de dúvida, contate a empresa através do atendimento on-line ou telefone fixo. Ao sentir qualquer desconfiança, não efetue o pagamento.

5) Dados pessoais

Forneça somente seus dados pessoais como CPF e RG para sites reconhecidos e de procedência confiável. Em caso de dúvida da procedência do site, não forneça os seus dados pessoais

⁸² <http://www.Internetsegura.org/>

6) Participação de sorteios

Todo sorteio deve estar devidamente regularizado através da Caixa Econômica Federal, do SEAE (Secretária de Acompanhamento Econômico) ou SUSEP (Superintendência de Seguros Privados). Recuse participar de sorteios de ofertas tentadoras e milagrosas, pois normalmente ações como estas são armadilhas para roubar dados e identidades.

7) Ofertas tentadoras

Não aceite ofertas tentadoras via e-mail , geralmente encaminhadas por logins falsos, que prometem prêmios instantâneos ou descontos especiais.

8) Programas de invasão

Cuidado com mensagens beneficentes ou que contenham imagens de catástrofes, atos de barbárie, pornografia, acidentes etc que são enviadas para que sejam abertas. A curiosidade do internauta é explorada pelos falsários, com o intuito de aplicar golpes. Geralmente os arquivos com as supostas imagens carregam programas de invasão que se instalam ocultamente no computador do usuário, para posteriormente roubar senhas e dados cadastrais da pessoa.

9) E-mails

Não abrir anexos de e-mails vindos de desconhecidos ou mesmo de conhecidos mas com texto suspeito ou sem sentido. Leia as mensagens antes de clicar nos links. Esse tipo de mensagem contem muitos erros gramaticais. Se ficar tentado em clicar no link de uma mensagem, verifique antes se a extensão é um arquivo .exe ou .zip , ou se refere a um formulário. Caso positivo apague imediatamente a mensagem Exemplo :

<http://65.75.191.196/e-mailscan.EXE>

POLÍTICA DE PRIVACIDADE⁸³

Condições Gerais

Este documento regula as condições gerais de uso do serviço de acesso e navegação do site do MOVIMENTO INTERNET SEGURA que a Câmara Brasileira de Comercio Eletrônico (Câmara-e.net) presta gratuitamente aos usuários de Internet.

Declaração de Privacidade

O MOVIMENTO INTERNET SEGURA tem o compromisso de proteger sua Privacidade.

A Política de Privacidade do MOVIMENTO INTERNET SEGURA tem como objetivo demonstrar o permanente compromisso com a segurança do conteúdo fornecido e das informações em nosso site. Todos os dados e/ou informações recebidas são de uso exclusivo do MOVIMENTO INTERNET SEGURA, serão tratados de forma confidencial e não serão divulgadas ou utilizadas com qualquer outra finalidade.

⁸³ <http://www.Internetsegura.org/privacidade/privacidade.shtml>, acesso em 7 jun. 2005.

Acesso Gratuito

As informações prestadas pelo MOVIMENTO INTERNET SEGURA através do site têm caráter gratuito e seu acesso independe de prévia inscrição ou registro do Usuário.

Links para outros sites

O site do MOVIMENTO INTERNET SEGURA não contém links para outras páginas na WEB.

Cookies

Cookies são pequenos arquivos no formato texto que ficam gravados em sua máquina, visando seu reconhecimento pelo site. O do MOVIMENTO INTERNET SEGURA não utiliza este recurso.

Privacidade dos Dados Cadastrais

O MOVIMENTO INTERNET SEGURA utiliza sistema de segurança apto a garantir a integridade e confidencialidade do recolhimento, registro, utilização e transmissão eletrônica de dados pessoais.

Direitos de Propriedade

O MOVIMENTO INTERNET SEGURA não concede qualquer licença ou autorização de uso de qualquer espécie sobre os direitos de propriedade industrial e intelectual ou sobre qualquer outro direito ou propriedade relacionada com o site.

Vedação ao Uso Incorreto

É vedada a utilização do serviço para fins ilícitos ou contrários, lesivos aos direitos e interesses de terceiros ou que de qualquer forma possam danificar, inutilizar ou deteriorar o Serviço, bem como os recursos necessários ao normal funcionamento do site e quaisquer espécies de conteúdo armazenado.

Compromisso anti-SPAM

SPAM é definido como sendo o envio de e-mails não solicitados. O e-mail é um dos componentes da Internet, e um dos principais meios de comunicação dentro dela. O MOVIMENTO INTERNET SEGURA, em sincronia com as melhores práticas de Internet, vem expor seu compromisso do cumprimento da regra de não fazer SPAM em hipótese alguma e sob nenhum pretexto.

Dúvidas

Se você tem qualquer dúvida sobre nossa política de privacidade ou sobre as práticas adotadas pelo site, envie um e-mail para: Internetsegura@camara-e.net

Esta Política de privacidade poderá ser eventualmente alterada, portanto sugerimos que todos a verifiquem periodicamente.

ANEXO 4

POLÍTICA DE PRIVACIDADE - GLOBO ONLINE

As reportagens citadas nesta tese, na sua maioria do jornal impresso O GLOBO, foram copiadas de sua reprodução eletrônica no site do jornal, na Web, que é acessado gratuitamente através da página do jornal on-line, <http://oglobo.globo.com/>, na qual basta registrar-se e aceitar a instalação de um cookie no computador. No acesso à página em 7 de julho de 2004, foi copiada a Política de Privacidade, transcrita a seguir:

O respeito à privacidade de seus leitores é um dos fundamentos do Globo Online.

A partir da adoção do cadastro gratuito para acesso ao site, o Globo Online passa a armazenar algumas informações pessoais de seus usuários.

O uso e o armazenamento destas informações serão realizados de acordo com as normas previstas nesta Política de Privacidade.

Estas normas podem passar por alterações futuras, que serão imediatamente registradas nesta mesma página.

A alteração mais recente foi feita no dia 22 de janeiro de 2004.

PRIVACIDADE E SEGURANÇA

As informações coletadas pelo Globo Online serão utilizadas para:

- 1) gerar estatísticas e análises genéricas sobre a utilização do site;
- 2) oferecer determinadas facilidades para os usuários, como acesso imediato ao site, sem necessidade de digitação de e-mail e senha a cada visita;
- 3) permitir que partes do conteúdo, da publicidade e das mensagens solicitadas pelos leitores sejam baseadas em preferências individuais;
- 4) limitar o acesso a determinadas áreas do site restritas a usuários com certos privilégios, como os serviços para assinantes.

Na análise destes dados e na divulgação das estatísticas, não haverá, em hipótese alguma, identificação individual de usuários com base nos seus dados pessoais e nos seus hábitos de visitação.

Nas pesquisas feitas no site, a identificação do usuário não será tornada pública; servirá apenas para evitar duplicidade de votos que possam distorcer os resultados.

Nas áreas interativas - fóruns, megafones, cartas dos leitores, blogs, etc - alguns dados de identificação do usuário poderão ser publicados junto aos comentários, quando isto for expressamente informado ao leitor.

As informações dos leitores cadastrados são armazenadas dentro de padrões de segurança que impedem o acesso de terceiros a estes dados.

Aos leitores cadastrados é assegurado o direito de acesso ao cadastro e alteração de suas informações pessoais.

As páginas onde há inserção de informações pessoais (cadastramento, exigência de login e senha e administração de preferências no cadastro) funcionam em site seguro (SSL) com criptografia, o que impede que estas informações sejam interceptadas.

USO DE INFORMAÇÕES CADASTRAIS

A utilização das informações cadastrais, contidas nos arquivos conhecidos como cookies ou não, permite:

- 1) que um determinado grupo de usuários visualize conteúdos e campanhas especialmente criados para ele (exemplos: homens com mais de 50 anos que se interessem por esportes; mulheres entre 21 e 40 anos que se interessem por economia; assinantes do Globo de fora do Rio; etc);
- 2) que cada usuário receba e-mails personalizados, contendo notícias, informações e publicidade do seu interesse, de acordo com as preferências especificadas no seu cadastro, sempre que solicitados ou autorizados;
- 3) que o Globo Online avalie a utilização do site de forma a aprimorar o conteúdo a partir da resposta dos leitores a determinados conteúdos publicados.

Estes dados não serão analisados e repassados a terceiros, em hipótese alguma, de forma a identificar individualmente um usuário e seus hábitos de visitação ou outras interações com o Globo Online e demais sites da Infoglobo.

As informações pessoais coletadas pelo Globo Online não serão vendidas ou transferidas a terceiros em hipótese alguma, exceto quando houver expressa autorização do leitor cadastrado, de acordo com as normas previstas nesta Política de Privacidade.

Para entender mais sobre o uso das informações no envio de mensagens solicitadas pelo usuário, leia o tópico Notícias e publicidade.

O sistema de cadastramento do Globo Online que permite acesso gratuito ao conteúdo do site funciona com base em cookies. O leitor que optar, nas preferências de seu navegador (browser), por não receber cookies será impossibilitado de acessar o conteúdo do Globo Online, com exceção da página inicial.

NOTÍCIAS E PUBLICIDADE

As informações dos leitores cadastrados não serão usadas para envio de mensagens não-solicitadas e nem disponibilizadas para terceiros em hipótese alguma, salvo em casos em que haja consentimento expresso do leitor cadastrado.

Newsletters, mensagens publicitárias e outras ações promocionais do Globo e de parceiros cuidadosamente selecionados serão direcionadas exclusivamente aos leitores cadastrados que expressamente optarem por isto, de acordo com as preferências expressas por cada cadastrado.

As newsletters e mensagens publicitárias enviadas por e-mail trarão, obrigatoriamente, opção de cancelamento do envio daquele tipo de mensagem por parte do Globo. A solicitação será atendida com a maior presteza possível, dentro do prazo máximo de 48 horas.

Os serviço de envio de e-mails é realizado por empresa contratada pelo Globo Online, que utiliza seus próprios servidores para realizar o envio.

A empresa contratada não armazena nem utiliza, de nenhuma forma e sob nenhuma hipótese, os e-mails do cadastro do Globo Online para qualquer outro fim que não o envio das mensagens, de acordo com as preferências de cada usuário registradas no Globo On Line.

As mensagens enviadas em formato HTML podem conter códigos que permitem personalizar mensagens de acordo com as preferências individuais do leitor cadastrado do Globo Online e elaborar relatórios sobre a visualização das mensagens, o número de vezes em que o e-mail foi aberto e o número de cliques feitos na mensagem.

Estas informações serão utilizadas, de forma genérica e agregada, para elaborar relatórios sobre o envio de mensagens. Estes relatórios poderão ser repassados aos anunciantes, como indicadores da efetividade das campanhas.

Em nenhuma hipótese o Globo Online vai divulgar estes dados de forma individualizada para terceiros, de forma a identificar um usuário ou seus hábitos de acesso e leitura de e-mails.

Ainda que coletivamente, os dados só podem ser utilizados para os fins previstos neste regulamento, que, em princípio, não autoriza (nem deve autorizar) a comercialização dos dados.

Perguntas ou dúvidas sobre a utilização da base de e-mails podem ser enviadas para o Globo On Line.

COOKIES

“Cookies” são pequenos arquivos que contém determinadas informações sobre os usuários de um site.

Os cookies são transferidos para o disco rígido do computador do usuário pelo computador onde o site está armazenado (servidor).

O Globo Online utiliza cookies que permitem que os servidores do Globo On Line identifiquem automaticamente algumas características do cadastro do usuário.

Os cookies serão utilizados pelo Globo Online com as seguintes finalidades:

- 1) permitir acesso imediato ao conteúdo gratuito do Globo Online (login automático), sem necessidade de identificação por e-mail e senha, aos usuários que optarem por isso;
- 2) permitir acesso imediato de usuários com privilégios especiais a áreas restritas (por exemplo, áreas de serviços exclusivas para assinantes do Globo);
- 3) oferecer conteúdo editorial e publicitário direcionado de acordo com preferências e características de grupos de usuários, quando solicitado ou autorizado;
- 4) acompanhar estatisticamente a utilização do site e as respostas (visualizações e cliques) dos usuários a links e anúncios.

Quando o leitor cadastrado opta por ter acesso automático ao site sem necessidade de digitar e-mail e senha, o cookie que permite o login automático fica armazenado no disco rígido do computador.

Este cookie e todos os demais cookies utilizados pelo Globo Online são apagados quando o leitor clica no botão de “log out” nas páginas da Central do Leitor do Globo Online.

Qualquer cookie, seja do Globo Online ou de outros sites, também pode ser apagado utilizando as ferramentas do navegador (browser).

Ao apagar o cookie, o usuário deverá voltar a informar e-mail e senha para acessar o site.

A opção por log out é recomendável quando o acesso se dá por computador não particular, compartilhado com outras pessoas - como no local de trabalho ou em cybercafés.

Por razões de segurança, certas alterações cadastrais, incluindo todos os dados referentes ao cadastro de assinantes do jornal O Globo impresso, só podem ser feitas com identificação por meio de e-mail e senha, independentemente das informações contidas em “cookies”.

Referências

ABBATE, Janet. *Inventing the Internet*. Cambridge: MIT, 2000.

ARIÈS, Philippe e Chartier, Roger. (org.) *História da vida privada*. Trad. de Hildegard Feist. Vol. 3. São Paulo: Companhia das Letras, 1995.

AGRE, Philip E. e ROTENBERG, Marc. *Technology and privacy: the new landscape*. Boston: MIT Press, 1998.

ALDERMAN, Ellen e KENNEDY, Caroline (Contributor) *The right to privacy*. Vintage Books, 1997.

BALLARD, J. G., *The Subliminal Man*, in *The Disaster Area*, Londres: Panther, 1969, p. 55-76.

BAMFORD, James. *Body of Secrets - Anatomy of the ultra secret National Security Agency*. Nova York: Doubleday, 2001.

BANISAR, David e DAVIES, Simon. *Privacy and Human Rights 1999: An international survey of privacy laws & developments*. Electronic Privacy Information Center, 1999.

BAUMAN, Zygmunt. *Globalização*. Rio de Janeiro: Jorge Zahar, 1999.

_____. *Identidade*. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2005.

BRIN, David. *The transparent society: Will technology force us to choose between privacy and freedom?* Massachusetts: Perseus Books, 1998.

CALVERT, Clay. *Voyeur Nation: Media, Privacy, and Peering in modern culture*. Westview Press, 2000.

CAMPBELL, John Edward, CARLSON, Matt. *Panopticon.com: Online Surveillance and the Commodifications of Privacy*. Em *Journal of Broadcasting & Electronic Media* 46(4), 2002. p. 586-606.

CASTELLS, Manuel. *A sociedade em rede*. trad. de Roneide Venancio Majer e Klauss Brandini Gerhardt. São Paulo: Paz e Terra, 2000.

_____. *O poder da identidade*. trad. de Klauss Brandini Gerhardt. São Paulo: Paz e Terra, 2002.

_____. *A Galáxia da Internet*. trad. de Maria Luiza X A Borges. Rio de Janeiro: Jorge Zahar, 2003.

CASTELLS, P. E. e BOSCH, R. M. *La vigilancia tecnológica, requisito imprescindible para la innovación*. Em GÜELL, A.M. e VILA, M. (coord). *El arte de innovar en la empresa*. Barcelona: Del bronze, 2001. p 97-132.

CAVOUKIAN, Ann e TAPSCOTT, Don (Contributor). *Who Knows : Safeguarding your privacy in a networked world*. McGraw-Hill, 1996.

CHARRETT, Sheldon. *Identity, Privacy, and Personal Freedom: Big Brother vs. The new resistance*. Paladin, 1999.

_____. *The Modern Identity Changer: How to create a new identity for privacy and personal freedom*. Paladin, 1997.

CHESBRO, Michael. *Privacy For Sale : How Big Brother and others are selling your private secrets for profit*. Paladin, 1999.

DANDEKER, C. *Surveillance, Power and Modernity*. Cambridge: Polity, 1990.

DAVIS, M. *City of Quartz: Excavating the Future in Los Angeles*. Londres: Verso, 1990.

DICK, Philip. K. *Minority Report, a nova lei*. Rio de Janeiro: Record, 2002.

DONALDSON, Molla S. e LOHR, Kathleen N. (eds.) Committee on Regional Health Data Networks. *Health Data in the Information Age. Use, Disclosure and Privacy*. Washington, National Academy, 1994.

DUBY, Georges. (org.) *História da vida privada*. Trad. de Maria Lúcia Machado. Vol. 2. São Paulo: Companhia das Letras, 2004.

ELMER, Greg. *A diagram of panoptic surveillance*. Em *New Media & Society*, Vol. 5, Nº 2, p. 231–247. Londres: Sage, 2003.

ERBSCHLOE, Michael e VACCA, John R.. *Net Privacy: A guide to developing and implementing an ironclad e-business Privacy Plan*. McGraw-Hill, 2001.

FLUSTY, S. *Building Paranoia: The Proliferation of Interdictory Space and the Erosion of Spatial Justice in Los Angeles*. Los Angeles: Forum for Architecture and Urban Design, 1994.

FOUCAULT, Michel. *Vigiar e punir*. Tradução de Surveiller et punir, 1975, por Raquel Ramallete. Petrópolis: Vozes, 1987.

FRAU-MEIGS, Divina. *A cultural project based on multiple temporary consensus*. Identity and community in *Wired*. Em *New Media & Society*, Vol. 2, Nº 2, p. 227–244. Londres: Sage, 2000.

FYFE, N. R., BANNISTER, J. *The Eyes on the Street: Closed Circuit Television Surveillance in Public Spaces*, apresentado na Conferência da Associação Americana de Geógrafos, Chicago, mar. 1994.

GARFINKEL, Simson e RUSSELL, Deborah. *Database Nation: The Death of Privacy in the 21st century*. Cambridge: O'Reilly & Associates, 2001.

GATES, Kelly A. *Wanted Dead or Digitized*. Facial Recognition Technology and Privacy. Em *Television & New Media* Vol. 3, Nº 2, maio 2002 p. 235–238. Londres: Sage, 2002.

GIDDENS, Anthony. *As conseqüências de modernidade*. São Paulo: Unesp, 1991.

HALL, Stuart. *Identidades culturais na pós-modernidade*. Tradução de Tomaz Tadeu da Silva e Guacira Lopes Louro. Rio de Janeiro: DP&A, 1997.

HAMMOND, Bob. *Super Privacy : The Complete Guide to personal privacy and financial freedom in tomorrow's cashless society*. Paladin Pr, 1997.

HARRIS, Thomas C., ABENE, Peter V., GRINDLE, Wayne W., HENRY, Darryl W., MORRIS, Dennis C., PARKER, Glynn E., MAYERSOHN, Jeffrey. *Development of the MILNET*. Em Proceedings of IEEE Electronics and Aerospace Systems Conference (EASCON). IEEE, 1982.

HAWKE, Constance S.. *Computer and Internet use on Campus: A Legal Guide to issues of intellectual property, free speech, and privacy*. Jossey-Bass, 2000.

HEART, Frank, MCKENZIE, Alex, MCQUILLAN, John, WALDEN, David. *ARPANET Completion Report*. McKenzie (caixa 2), Biblioteca de Bolt, Beranek e Newman. 4 jan. 1978.

HENDRICKS, Evan. HAYDEN, Trudy e NOVIK, Jack D.. *Your Right to Privacy : A Basic Guide to legal rights in an information society (An American Civil Liberties Union Handbook)*. Southern Illinois Univ. (Trd), 1990.

HOWLEY, Kevin. *Spooks, Spies, and Control Technologies in the X-Files*. Television & New Media, vol.2, Nº 3, agosto de 2001, p. 257-280. Londres: Sage, 2001.

IEEE. *Security and Privacy, 1998 IEEE Symposium*. IEEE, 1998.

JENNINGS, Charles. Fena, Lori e Dyson, Esther. *The Hundredth Window: Protecting your privacy and security in the age of the Internet*. Free Press, 2000.

KETCHER, Michael. *Closing door. The End of Financial Privacy in America and How to Protect Yourself*. 2ª ed. The Institute for the Preservation of the Wealth, 1992.

KING, Dennis. *Get the facts on anyone: Find out confidential information about any person or organization*. Arco Pub, 1999.

LANE III, Frederick. S. *The naked employee*. How technology is compromising workplace privacy. Nova York: Amacom, 2003.

LESSIG, L. *CODE: and other laws of cyberspace*. Nova York: Basic Books, 1999.

LÉVY, Pierre. *As Tecnologias da Inteligência*. Trad. de Carlos Irineu da Costa. Rio de Janeiro: Editora 34, 1994.

_____. *O que é o virtual?* Trad. de Paulo Neves. Rio de Janeiro: Editora 34, 1996.

LEVY, Steven. *Crypto: How the code rebels beat the government -- Saving privacy in the digital age*. Viking, 2001.

LUNA, J. J.. *How To Be Invisible: A Step-By-Step Guide to protecting your assets, your identity, and your life*. St. Martins (Trade), 2000.

LYON, David. *The Electronic Eye - The Rise of Surveillance Society*. Minneapolis: University of Minnesota, 1994.

_____. *An electronic panopticon? A sociological critique of surveillance theory*. Oxford: Blackwell., 1993.

_____. *Everyday Surveillance, Personal data and social classifications*. In *Information, Communication & Society* 5: 2. Routledge, 2002. p. 242-257.

_____. *Surveillance after September 11*. Cambridge: Polity., 2003.

LYON, David e ZUREIK, Elia. *Computers, Surveillance & Privacy*. Minneapolis: University of Minnesota, 1996.

MARTINS, José de Souza. *A vida privada nas áreas de expansão da sociedade brasileira*. Em SCHWARCZ, Lilia Moritz (org.). *História da vida privada no Brasil*, vol. 4. São Paulo: Companhia das Letras, 2004.

MARTIN-BARBERO, Jésus. *Dos meios às mediações*. Rio de Janeiro: UFRJ, 1997.

_____. *Identities: traditions and new communities*. Media, Culture & Society Vol. 24, Nº 5, p. 621-641, 2002.

MAYER, Paul. A., *Computer Media and Communication - A Reader*. Nova York: Oxford University, 1999.

MCKEOWN, Kevin e STERN, Dave (Contributor). *Your secrets are my business*. Plume, 2000.

MCLUHAN, Marshall. *A galáxia de Gutenberg*. Rio de Janeiro: Nacional, 1980.

MELNICK MD, Alan L, FLEMING, David. *Introduction to Geographic Information Systems for Public Health*. Aspen, 2002.

NEGROPONTE, Nicholas. *A Vida Digital*. Tradução de Sérgio Tellaroli. São Paulo: Companhia das Letras, 1995.

NORRIS, Clive e ARMSTRONG. Gary. *The maximum surveillance society*. Nova York: Oxford, 1999.

PANKAU, Edmund J.. *Hide Your Assets and Disappear: A Step-By-Step Guide to Vanishing without a trace*. Harperperennial Library, 2000.

PERROT, Michele. (org.) *História da vida privada*. Trad. de Denise Bottman e Bernardo Joffil. Vol. 4. São Paulo: Companhia das Letras, 2003.

PRIVACY FOUNDATION, página na Internet em: <http://www.privacyfoundation.org>

REEVE, A. *The Private Realm of the Managed Town Centre*. Em Oxford: Urban Design International, vol 1, nº 1, 1996.

ROSEN, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. Nova York: Random House, 2000.

_____. *The Naked Crowd*. Reclaiming security and freedom in an anxious age. Nova York: Random House, 2004.

ROTENBERG, Marc *The Privacy Law Sourcebook 1999: United States Law, International Law, and Recent Developments*. Electronic Privacy Information Center, 1999.

ROWLEY, Jennifer. *The basics of information technology*. Londres: Clive Bingley, 1988.

RUSSO, J. E. e SCHOEMAKER P. J. H., *Winning Decisions*, Currency, Doubleday: Nova Iorque, 2002.

SCHNEIDER, Jerome. Schneider e Weiner, Allison Hope *Hiding your money: Everything you need to know about keeping your money and valuables safe from predators and greedy creditors*. Prima Publishing, 2000.

SCHNEIER, Bruce. *E-mail security: How to keep your electronic messages private*. John Wiley & Sons, 1995.

SCHNEIER, Bruce e BANISAR, David. *The Electronic Privacy Papers: Documents on the battle for privacy in the age of surveillance*. John Wiley & Sons, 1997.

SMITH, Robert Ellis e MAJUMDAR, Sangram (Illustrator). *Ben Franklin's Web site: Privacy and curiosity from Plymouth Rock to the Internet*. Privacy Journal, 2000.

SOUZA, Laura de Mello. (org.) *História da vida privada no Brasil*. Vol. 1. São Paulo: Companhia das Letras, 2004.

SONTAG, Larry. *It's none of your business, a complete guide to protecting your privacy, identity, and assets*. PMI Enterprises. 3ª ed., 2000.

STANDAGE, Tom. *The Victorian Internet*. Nova York: Berkley Books, 1999.

STAPLES, William G., *The Culture of Surveillance - Discipline and Social Control in the United States*. Nova York: St. Martin's, 1997.

SWEENEY II, P. J. *RFID for dummies*. Hoboken: Wiley, 2005.

SWIRE, Peter. P, LITAN, Robert E. *None of your business*. Washington: Brookings Institution, 1998.

TURKLE, S. *Life on the Screen : Identity in the Age of the Internet*. Nova York: Touchstone, 1995.

WERTHEIM, Margaret. *Uma história do espaço de Dante à Internet*. tradução de Maria Luiza X A Borges. Rio de Janeiro: Jorge Zahar, 2001.

WHITAKER, Reg. *The End of Privacy*. Nova York: The New Press, 1999.

ZIMMERMANN, Philip R.. *The official PGP user's guide*. Cambridge: MIT, 1995.

Jornais (citações específicas em notas de rodapé):

FOLHA DE SÃO PAULO. São Paulo, de jan. 1995 a dez. 2002.

O GLOBO. Rio de Janeiro, de jan. 1999 a dez. 2005.

VALOR ECONÔMICO. São Paulo, de maio 2001 a nov. 2002.

<http://www.paramount.com>, acesso em 19 dez. 2003

http://www.fantasticfiction.co.uk/authors/Larry_Niven.htm, acesso em 17 dez. 2003.