Vigilância, controlo, crime, terrorismo, fraude: paradigma e sintagma

...cépticos, liberais, indivíduos com gosto para a vida privada e para os seus próprios padrões interiores de comportamento, são objecto de medo e zombaria e alvos de perseguição de qualquer dos lados... nas grandes guerras ideológicas do nosso tempo.

Isaiah Berlin

No ambiente do híper comércio do consumo contínuo e do dinheiro electrónico surgiram equipamentos, programas e comportamentos que evidenciam uma transformação substancial daquilo a que as pessoas até então chamavam de *direito à privacidade*.

No inverno de 1992, o filósofo Francês Gilles Deleuze publicou, no *MIT Massachusetts Institute of Technology*, um pequeno ensaio a que chamou de *Postscript on the Societies of Control*. Nele, Deleuze descrevia a emergência de um novo tipo de sociedade, que ele denominou como "sociedades do controlo". Revelando o fenómeno gerado com um uso intensivo e especializado da visão e a sua gradual desarticulação com os novos meios virtuais, o seu texto significou um grande impacte entre intelectuais de todo o mundo: «Foucault localizou as sociedades da disciplina nos séculos dezoito e dezanove; elas alcançaram o seu auge no final do século vinte. Elas deram início à organização de vastos espaços de *enclosure*». – *Enclosure* é um termo que acabou por ser geralmente traduzido por "fechamento do mapa". «O indivíduo nunca cessa de passar de um a outro ambiente fechado, cada um tendo as suas próprias leis; primeiro, a família; depois, a escola ("não está na escola quando estás com a tua família"); então, as barracas ("não mais estás na escola"); então, a fábrica; de tempos em

tempos, no hospital; possivelmente na prisão... (...) Foucault analisou brilhantemente o ideal desses ambientes de *fechamento*, particularmente visíveis na fábrica: concentrar; distribuir no espaço; ordenar no tempo... (...) Estamos numa crise generalizada em relação a todos os ambientes de fechamento – prisão, hospital, fábrica, escola, família. (...) ...todos sabem que essas instituições estão acabadas, não importando o tamanho dos seus períodos de expiração. É apenas questão de administrar os seus últimos ritos e de manter as pessoas empregadas até a instalação das novas forças que estão batendo à porta. Essas são as *sociedades do controlo*, que estão em vias de substituir as *sociedades da disciplina*. "Controlo" é o nome que Burroughs propõe como um termo para um novo monstro, aquele que Foucault reconhece como o nosso futuro imediato».

Curiosamente, aquilo que Deleuze dá o nome de *enclosure* é exactamente o fenómeno da *sístase*, típico na visão. Não menos curioso é o facto de tanto Deleuze como Foucault não terem

sido capazes de perceber que a transição de uma sociedade da soberania – ou da hierarquia – para a sociedade *low power* com controlo generalizado, é precisamente a interpretação da transição de uma sociedade da visão para algo que existia antes, para um mundo de culturas acústicas.

Se, por um lado, socorremo-nos do passado para explicar o futuro que ainda não compreendemos, por outro, o universo das culturas virtuais guardam alguns curiosos traços de semelhança com as antigas culturas orais – até mesmo por serem, como aquelas, sistemas de comunicação de *mão dupla*.

Toda sociedade acústica é uma sociedade do controlo. Mas, agora, a escala planetária e a diversidade da *paleta sensorial* produzidas pelos sistemas virtuais alteraram toda a realidade, gerando algo diferente do universo oral.

Na década de 1950, o genial antropólogo Americano Edward T. Hall chamava de *ambiente*

aquilo que posteriormente viria a ser denominado como *enclosure* por Deleuze.

Enclosure não parece ser apropriado quer para sociedades acústicas, quer para as virtuais – pois, em ambos os casos, o que temos é um *contínuum*. *Enclosures* são estabelecidos por *departamentos*, típicos nas culturas mecânicas e literárias.

O conceito de *enclosure* é tipicamente produto de um pensamento literário.

Em Maio de 2002, Brandon Mercer – jornalista para o programa de televisão *TechLive*, no Estados Unidos, que esteve no ar entre 1998 e 2004, lançava o artigo *Can Computers Read your Mind?* onde apresentava uma entrevista com o engenheiro Dave Schraer que desenvolvia para a *NCR* um novo tipo de caixa automático capaz de detectar o humor das pessoas. Assim, a máquina poderia alterar o seu próprio visual e oferecer produtos de diferentes naturezas dependendo do

humor do utilizador naquele momento. Por outro lado, a flutuação de humor poderia ficar registada no sistema, de forma a elaborar um perfil daquele utilizador em especial, assim como de conjuntos de utilizadores.

Conforme estivesse o humor da pessoa, uma informação especial apareceria no ecrã, mediocrizando ainda mais todo o sistema de comunicação, eliminando aspectos importantes da privacidade e estabelecendo mais um passo no desenvolvimento da vídeo vigilância.

Em 2008, a empresa Japonesa *Omron* apresentou uma máquina fotográfica que para além de tirar fotografias é capaz e identificar o género e a idade aproximada de uma pessoa.

No seu livro *2020 Les Scénarios du Futur*, publicado em 2008, Joël de Rosnay traçava uma curiosa imagem do que já era uma realidade quando o livro foi lançado: «Imagine-se entrando num ambiente que o identifica pessoalmente. O

ambiente ajusta imediatamente a temperatura do lugar, começa a tocar a música que você gosta ou fazer o *download* no seu computador pessoal do *software* sobre o qual trabalhou, se você esteve naquele lugar». De facto, o ambiente *conhece* tudo sobre a pessoa.

No Brasil, ilegalmente, desde o início dos anos 2000, sistemas de segurança de diversos edifícios apenas permitem a entrada de pessoas após deixarem uma fotografia, cópia de um documento de identificação, assinatura e impressões digitais nas suas bases de dados.

Cada vez que um *site* de vendas, como a *Amazon*, é acessado, um *cookie* é automaticamente instalado no computador do usuário, rastreando todos os seus movimentos automaticamente, mas sem a sua autorização ou conhecimento.

Programas de vigilância digital, como o *Spector*, são comercializados em grandes quantidades pela Internet. No *site* da *Spector*, por

exemplo, há uma descrição dos seus inúmeros benefícios: «Imagine uma câmara de vigilância apontada directamente para o écran do seu computador, filmando tudo o que é feito no seu Macintosh (ou PC). Essa é a ideia por trás do programa de Monitoração de Internet e Vigilância número um em vendas, Spector. Spector funciona captando uma imagem do que quer que seja no écran do computador e salvando num lugar escondido no seu disco rígido. Poucos segundos depois, Spector tira outra fotografia. Na verdade, Spector pode tirar fotografias do écran do seu computador numa frequência de uma por segundo. Você pega gravações de todas as conversas em *chat*, mensagens instantâneas, emails escritos e lidos, todos os *web sites* visitados, todos os programas e aplicações funcionando, todas as teclas tocadas – TUDO o que eles fazem no seu computador e na Internet. Você pode voltar ao seu computador poucos minutos, poucas horas, poucos dias ou semanas mais tarde e VER EXACTAMENTE o que eles estiveram a fazer, porque Spector gravou tudo. Spector é apropriado para pais preocupados

sobre o que os seus filhos estão a fazer *online*, ou preocupados com a protecção dos seus filhos em relação aos perigos da Internet. Spector também é ideal para os patrões preocupados sobre como os seus empregados usam os computadores da empresa. Os seus empregados estarão a perder demasiado tempo *online*? Estarão a enviar anedotas de mal gosto sobre sexo ou raça? Estarão a espalhar informação confidencial da empresa através de *chats* anónimos e plataformas de mensagens? Você vai descobrir com Spector. E, se você está preocupado com o que a sua esposa ou o seu marido estão a fazer *online* em qualquer hora da noite, não há forma mais rápida e mais precisa de descobrir do que com Spector».

No mesmo site, a empresa acrescenta o seu comprometimento com as autoridades governamentais: «A nossa missão na *Spy Chest Inc* é fornecer as agências governamentais equipamento em tempo adequado. Através da coordenação dos processos de *procurement* de forma a identificar as necessidades e recursos

das agências governamentais, os equipamentos podem ser obtidos quando forem necessários através de uma das várias opções de aquisição. Nós compreendemos a urgente necessidade dos nossos clientes governamentais, portanto asseguramos que os pedidos são processados de forma precisa e em tempo adequado. Procuramos fornecer o seu equipamento com inultrapassável profissionalismo e precisão».

Para além dos sistemas de vigilância virtual, a *Spy Chest* oferece uma grande quantidade de equipamentos de espionagem, dignos de um filme com *James Bond*, por preços extremamente baixos.

Outra empresa Americana de espionagem é a *Spy Associates*: «Somos dedicados a lhe fornecer o melhor equipamento de vigilância e detecção do mercado hoje. SpyAssociates.com fornece equipamento de vigilância a indivíduos, empresas, escolas, investigadores privados, agências governamentais e organizações religiosas. Os

nossos estoques incluem: câmaras escondidas, mini câmaras, mini câmaras de espionagem sem fios, CCTV, sistemas de vigilância e aparelhos secretos de gravação; aparelhos de escuta, gravadores de telefone digitais, microfones sem fios, gravadores escondidos de voz analógicos e digitais, ouvidos biónicos e bloqueadores áudio; equipamento GPS passivo e em tempo real para seguir o seu carro e / ou seus bens; aparelhos de detecção, testes caseiros para detecção de consumo de droga, de álcool ou de comportamentos de infidelidade, detectores de frequências de rádio, detectores de câmaras escondidas, detectores de câmaras sem fios, monitores de contra vigilância; equipamentos para mudança de voz; equipamentos para mudança de voz em telefones celulares; equipamentos profissionais para mudança de voz e transformação de voz; segurança telefónica; detecção de grampo; equipamentos de espionagem; detectores de metal...», entre outros.

Em Janeiro de 2009, a *Spy Tools Directory* lançava um comunicado de imprensa onde relatava

as qualidades de um novo produto: «Você está a procura de um programa de espionagem para um *smartphone* de forma a poder secretamente obter cópias de mensagens de texto de um adolescente rebelde, de uma esposa infiel, ou de telefones celulares de empregados suspeitos na empresa? Os recursos tecnológicos de espionagem *online* da *Spy Tools Directory* lança agora o *Mobile Spy*, um programa que captura secretamente toda a actividade do telemóvel de um *smartphone* e a salva para que você a possa ver à distância através da Internet vinte e quatro horas por dia».

Em Abril de 2008, a empresa *Record Cell Phones* anunciava um programa de espionagem, em formato popular, que «permite qualquer utilizador de telemóvel gravar conversas feitas em telemóveis para serem ouvidas através de atendedores automáticos ou serem salvas e guardadas em formato MP3. O serviço, conhecido como *Call Record Cards*, permite aos utilizadores reencaminhar todas as chamadas de telemóveis através de um canal de telecomunicações onde

as conversas são gravadas digitalmente. As chamadas gravadas podem ser operadas *online* através de uma interface num *site* de Internet, ou acessadas para audição através de um sistema de atendedor automático. O serviço é comprado em formato de pré pagamento, presentemente com a possibilidade de aquisição de parcelas adicionais de duzentos e cinquenta e quinhentos minutos».

Isso, sem contar com os chamados *malicious software*, como programas *Trojan Horse* e *network worms*, por exemplo.

Em 2005, uma notícia na imprensa informava que a «polícia israelense usou cavalos de tróia para espionar algumas das mais importantes empresas do país. O caso terá profundas implicações para a comunidade empresarial em Israel – e possivelmente para além dela – porque as empresas acusadas de terem utilizado aqueles programas são, elas mesmas, as empresas mais importantes. Uma reportagem no Há'aretz detalhou como uma grande quantidade de empresários – incluindo

os mercados da televisão, da telefonia celular, da importação de automóveis, das empresas de utilidades – usaram programas de cavalos de tróia, que se acredita terem sido escritos por duas pessoas que vivem no Reino Unido, para espionar os seus mais próximos rivais nos negócios com um elevado grau de sucesso».

Em Abril de 2009 o site com o sugestivo título de *Go Hacking* ensinava todos os passos para se fazer um *Trojan Horse* utilizando linguagem C para computadores. O autor explicava que «este cavalo de tróia funciona bem rápido e é capaz de devorar aproximadamente 1 GB de disco rígido a cada minuto de funcionamento. Assim, eu o chamo *Space Eater Trojan*. E devido ao faceste cavalo de tróia funciona bem rápido e é capaz de devorar aproximadamente 1 GB de disco rígido a cada minuto de funcionamento. Assim, eu o chamo *Space Eater Trojan*. E devido ao facto de ter sido escrito utilizando um alto nível de linguagem de programação, ele normalmente não é detectado por anti- vírus».

Entre seis de Abril a seis de Agosto de 2009, especificamente em relação às instruções sobre como construir um *Trojan Horse*, o site *Go Hacking* recebeu dezenas de mensagens de mais de sessenta pessoas de diversos países, todos manifestamente adolescentes, um dos quais assumia o *nickname* de *Hitler*. O autor do site, que se dizia chamar Srikanth, aparentemente era um jovem e brilhante estudante de engenharia na Índia.

O mesmo site ainda oferecia: um programa de vírus para inutilizar portas USB, um programa de vírus para bloquear *sites* na Internet, um programa de vírus para reiniciar o computador todas as vezes que for iniciado, outros cavalos de tróia e *backdoors*.

Nessa mesma época havia, ainda, o *Sniffer* – para além de inúmeras outras ferramentas de espionagem na rede. O *Sniffer* regista o tráfego de dados, captura partes e descodifica o seu conteúdo. É um instrumento que tem sido frequentemente

utilizado por *hackers* para obter cópias de ficheiros durante a sua transmissão, obter *palavras passe* e até mesmo capturar conversações em tempo real.

Se por um lado a espionagem activa, como o uso de câmaras ou de programas de computador, alcançou uma formidável expansão no início do século XXI, a espionagem passiva – que opera com dados fornecidos de livre vontade pelas pessoas – não estava menos exuberante.

Cada vez que um cartão de crédito é utilizado, muitas informações do consumidor transitam pela rede de computadores. Cada vez que nos conectamos à rede digital, o número do nosso computador e localização são automaticamente identificados – e o mesmo acontece com o uso de telemóveis e até mesmo de telefones fixos.

Em Julho de 2009, jornais Brasileiros anunciavam uma nova moda no país: o uso de telefones móveis também com a função de cartões

de crédito. Esse uso já era muito popular no Japão. Quando uma pessoa realiza um pagamento através do telefone móvel, não apenas transmite imediatamente todos os seus dados pessoais, mas também a sua localização geográfica.

Glenn Hastings e Richard Marcus – dois nomes falsos – conheceram um grande sucesso editorial, principalmente nos Estados Unidos, com a publicação do livro *Identity Theft Inc*. O livro conta a história, presumivelmente verdadeira, de como os autores se tornaram milionários através da descoberta e uso criminoso de identidades. Ao longo das suas mais de trezentas páginas, todo o processo de roubo de identidade é cuidadosamente descrito, passo a passo.

«Mesmo no início dos anos 1990, os bancos estaduais e federais já operavam com uma rede de computadores altamente eficiente que armazenava oceanos de dados bancários detalhados sobre virtualmente todas as pessoas que tivessem tido alguma vez uma conta bancária nos Estados Unidos.

O sistema funcionava de forma muito parecida com o Centro Nacional de Informação Criminal do FBI. Introduzindo o seu nome, banqueiros tinham acesso instantâneo a todos os detalhes de informação relativos à sua história bancária, para além de detalhes pessoais como o seu número de Segurança Social, data e lugar de nascimento, e últimos endereços conhecidos. Eles podiam se intrometer na sua história de comportamento fiscal tão facilmente quanto os departamentos de crédito verificavam os seus arquivos. Eles poderiam saber até mesmo quando você preencheu um cheque ruim, se a sua conta algum dia ficou negativa, se você abusou de serviços bancários tais como ultrapassar o limite e, naturalmente, se você alguma vez esteve ligado a algum tipo de fraude bancária ou actividades bancárias questionáveis», e os autores acrescentavam que «a *Federal Trade Commission* estima que mais de dez milhões de Americanos têm a sua informação pessoal e de crédito roubada ou utilizada fraudulentamente de uma ou de outra forma», em 2006.

No final de 1997, a polícia Suíça rastreou secretamente a localização de utilizadores de telemóveis através das empresas de telecomunicação que registam milhares de milhões de movimentos por ano. Eles foram capazes, através da *Swisscom* de identificar a localização de utilizadores com uma precisão de poucas centenas de metros.

Com a *ITV* ou *TV interactiva,* também conhecida como *TV digital*, pela primeira vez a televisão se tornou um meio de *duas mãos*. Todos os movimentos da audiência são registados em tempo real pela rede de transmissão. Assim, passa-se a conhecer, aparelho a aparelho, as preferências de programas, filmes, jornais, horários, serviços como envios de mensagens, compras de bilhetes para o teatro ou jogos entre outros, criando um perfil do utilizador com dados que podem ser cruzados com outros, de diferentes naturezas – até mesmo de natureza fiscal.

Assim, o que antes era uma transmissão

"cega" se transformou numa *porta de vigilância*.

O mesmo aconteceu com os telefones fixos, que passaram a registar todas as chamadas automaticamente, independentemente da autorização do utente.

Em Novembro de 2002, William Safire publicava um alarmante artigo no *New York Times* com o título *You Are a Suspect*: «Se o Homeland Security Act não for alterado antes da sua aprovação, isto é o que vai acontecer com você: cada compra que fizer com um cartão de crédito, cada assinatura de revista que você fizer ou prescrição médica que preencher, cada site na Internet que visitar ou email que enviar ou receber, cada grau académico que receber, cada depósito bancário que fizer, cada viagem que reservar e cada evento em que estiver, todas essas transacções e comunicações irão para o que o ministério da Defesa descreve como "uma grande central de dados centralizada e virtual". A esse dossiê computadorizado sobre a sua vida privada a partir de fontes comerciais, adicione

cada peça de informação que o governo tem sobre você: cadastramento para passaporte, carta de condução e informação de portagens, registos de acções judiciais e de divórcios, reclamações à polícia contra vizinhos ruidosos, toda a sua vida colocada em papel mais a última imagem de uma câmara de vigilância – e você tem um sonho super-bisbilhoteiro: uma "Total Information Awareness" sobre todos os cidadãos Americanos. Isto não é algum distante cenário orweliano. Isto é o que vai acontecer com a sua liberdade pessoal nas próximas semanas se John Poindexter alcançar o poder sem precedentes que pretende».

TIA, ou *Total Information Awareness,* foi elaborado para ser um sistema controlado por computadores, condição operacional que passaria a ser conhecida como *COMPUTINT*; e não comandada por seres humanos, ou *HUMINT*. Assim, tal como acontece com as câmaras e sistemas de detecção de excesso de velocidade nas estradas, toda a informação recolhida sobre todas as pessoas seria superficial e não-subjectiva,

pretendendo respeitar os direitos de privacidade. Mas, ainda assim, os dados finais seriam, em última instância, operados por seres humanos, após vários níveis de análise digital que – tal como os programas de tradução automática de línguas em uso na Internet – eram extremamente falíveis. Isto é, a análise digital poderia produzir grandes distorções no cruzamento de informação que depois seria manipulada por seres humanos. Para além disso, todo o projecto estaria fortemente terceirizado, com uma operacionalidade centrada nas mãos de empresas privadas.

O projecto de Poindexter – que anos antes tinha sido o líder da desastrada operação Irão-Contras (*Irangate*), provocando um escândalo no governo de Ronald Reagan – chamava-se *TIA Total Information Awareness*, e acabou por não ser autorizado pelo Congresso Americano após uma grande onda de protestos populares em 2004.

Apesar do *TIA* não ter sido autorizado pelo Congresso Americano, outras operações

semelhantes, muitas vezes especializadas em ambientes e condições específicas, com idênticos objectivos e métodos, acabariam por ser criados não somente nos Estados Unidos, mas praticamente em todo o planeta.

A *DARPA Defense Advanced Research Projects Agency* – criada como reacção ao lançamento do *Sputnik* pela União Soviética em 1957 e responsável pelo surgimento da Internet – possui um projecto totalmente independente do *TIA*, chamado *LifeLog,* que visa colocar numa fantástica base de dados todo o tipo de informação possível sobre seres humanos – desde dados áudio visuais a informações biomédicas. Trata-se de uma base de informação tão poderosa que a sua aspiração seria a constituição de verdadeiros bancos de memória humanos.

Em 2003 foi criado em Nova Jersey, Estados Unidos, um instituto anti-terrorista que recebeu o nome de *CAT Eyes*. Segundo Reg Whitaker, sociólogo da Universidade de Vitória, no Canadá, «o fundador

do programa visa ambiciosamente cerca de cem milhões de informantes, um ratio de vigilantes de cerca de um para dois, comparavelmente menos com a *Stasi* da Alemanha Oriental que era de uma para oito pessoas».

Como esses, muitos outros projectos semelhantes foram surgindo em todo o mundo, tais como o *Bio-Surveillance* e o *BioAlirt – Bio-event Advanced Leading Indicator Recognition Technology*.

Um desses sistemas, ainda nos Estados Unidos, era conhecido como *CAPPS II* ou *Computer Assisted Passenger Prescreening System*. Estabelecido em 2003, como espécie de compensação pela impossibilidade de implantação imediata e radical do *TIA*, o *CAPPS II* substituiu o sistema anterior, *CAPPS*, com as seguintes prerrogativas, exigidas pelo Congresso Americano: o governo, não as empresas de aviação, vai controlar e administrar o sistema; cada passageiro será revistado, não apenas as suas bagagens; cada

companhia de aviação e cada aeroporto serão cobertos pelo sistema.

Em Julho de 2004, após muitas críticas, Tom Ridge, então *Secretary of Homeland Security*, equivalente a Ministro da Administração Interna, declarou o definitivo abandono do *CAPPS II*.

Outro programa, quase que totalmente desconhecido, suportado pelo Departamento de Justiça dos Estados Unidos, utilizando os mesmos princípios do *TIA*, chamava-se *MATRIX Multistate Anti-TeRrorism Information eXchange* – tal como o famoso filme de cinema que mostrava uma sociedade submetida a um governo totalitário controlado por computadores. *MATRIX* seria operado por entidades privadas, centralizada na empresa *Seisint Inc*. – fundada por Hank Asher que, segundo a *Associated Press*, estava associado ao tráfico de cocaína nos anos 1980. O *MATRIX* foi oficialmente terminado em 2005, mas os seus princípios, que eram os mesmos do *TIA*, continuaram a proliferar em muitos outros

projectos em todo o mundo.

Passou a ser comum a existência de programas de vigilância e controlo que iniciam e terminam subitamente, provocando confusão e abrindo portas para que procedimentos de captura de dados pessoais pareçam algo comum e perfeitamente aceitável para grande parte das populações.

Como disse David Lyon, « uma massiva e crescentemente entrelaçada rede de tecnologias de vigilância está cercando e definindo as sociedades contemporâneas ».

E acidentes acontecem. O jornal *Observer* de Novembro de 2007 anunciava, para o espanto geral, que o governo Britânico tinha perdido dados pessoais de vinte e cinco milhões de cidadãos, com o extravio ou roubo de dois discos compactos! Poucos dias depois, e apesar do escândalo, o governo reiterava, em Londres, a firme determinação de impor a todos as pessoas que desejassem se

deslocar ao exterior a obrigatoriedade de fornecer às autoridades cinquenta e três tipos de informação diferentes para obter a autorização de viagem! A justificação, como sempre, era a defesa contra ataques terroristas.

Em Julho de 2008, de acordo com o jornal *El Mundo*, setecentos e quarenta e sete computadores foram roubados do Ministério da Defesa Britânico, contendo informação altamente secreta. Dias antes, os Serviços Secretos Britânicos tinham anunciado terem perdido importante informação digital sobre a *Al Qaeda* e a segunda guerra do Iraque.

Em Agosto de 2008, uma nova perda chocou a opinião pública Britânica: o governo tinha perdido dados pessoais relativos a cerca de cento e cinquenta mil criminosos. A informação estava armazenada numa *pen drive* que foi simplesmente perdida, vendida ou roubada.

Para tornar tudo ainda pior, poucos dias

mais tarde um computador vendido no *site eBay* por um preço simbólico continha, acidentalmente, informação bancária de um milhão de cidadãos Britânicos, incluindo moradas, números de telefones e até mesmo assinaturas entre outros dados.

Entre o verão de 2005 e o verão de 2008, o governo Britânico admitiu oficialmente ter perdido ou terem sido roubados quarenta e três computadores portáteis e noventa e quatro telemóveis, com todas as informações que continham.

Entre 1998 e 2008, as autoridades Inglesas, especialmente o Ministério da Defesa, anunciou terem sido roubados das suas instalações cerca de seiscentos computadores portáteis.

As bases de dados geridas pelos governos se tornaram verdadeiros cenários para uma trama *Kafkiana*.

Outro projecto Britânico de controlo e vigilância, também do final de 2007, chamado *ECCO*, que estava sendo ensaiado em Edimburgo, provocou uma forte reacção por parte da população local. O sistema prevê colocar *online*, de acesso livre para qualquer assistente social, informações confidenciais actualizadas sobre pessoas que tenham tido problemas como alcoolismo, maus tratos ou perturbações mentais, permitindo uma permanente monitorização e intervenções relâmpago, mesmo contra a vontade pessoal – tudo em nome do bem estar social.

Um dos meus mais queridos mestres de arquitectura, para além de ter sido um inesquecível amigo, Eduardo Kneese de Mello, que viveu entre 1906 e 1995, para além de ter sido responsável por um grande número de excelentes projectos, foi ainda arquitecto chefe na construção de Brasília, ao lado de Oscar Niemeyer, Lúcio Costa, Burle Marx e de Juscelino Kubitschek; primeiro presidente do *Instituto dos Arquitetos do Brasil*; e foi grande amigo de Alvar Aalto, Kenzo Tange,

Marcel Breuer e Walter Gropius, para além de ter estado próximo de Frank Lloyd Wright e Le Corbusier entre outros.

Eduardo Kneese de Mello contou-me da estranheza que sentiu quando foi aos Estados Unidos em 1965. Depois de ter ficado alguns anos sem viajar para outros países, ele foi convidado para receber a medalha de sócio honorário do *American Institute of Architects*, em Washington DC. «Antes, praticamente não existiam linhas comerciais de aviões. As rotas eram relativamente poucas. Viajávamos sempre de navio. Quando íamos para a Europa, partindo do Brasil, levávamos semanas para cruzar o Oceano Atlântico. Quando entrávamos no navio, as pessoas já sabiam quem era quem. Quando saíamos, todos se conheciam muito bem. À saída dos navios nunca era necessária a apresentação do passaporte. O documento viajava connosco para o caso de um acidente, de uma emergência, apenas isso. Quando o navio atracava, as autoridades locais conheciam o comandante e tinham confiança

nele. Por outro lado, ele nos conhecia. Assim, nunca houve qualquer incómodo. Mas, quando cheguei aos Estados Unidos, a primeira coisa que me pediram no aeroporto foi o passaporte! Eu me senti como se fosse um criminoso. Para quê eu deveria me identificar? Eu não tinha cometido qualquer crime!».

Nos Estados Unidos, o passaporte apenas foi estabelecido em 1914 e o seu uso se tornou regular somente após a Primeira Guerra Mundial, tal como aconteceu nos países Europeus. Ainda assim, o controlo exaustivo da sua apresentação na entrada ou saída dos países, especialmente dos Estados Unidos, apenas teve início regular após 1950.

John Torpey, sociólogo da Universidade da Califórnia, relata detalhadamente a criação e desenvolvimento do uso dos passaportes ao longo dos séculos no seu livro *The Invention of the Passport – Surveillance, Citizenship and the State*, publicado no ano 2000.

Num mundo onde, de uma forma mais ou menos geral, a escala tornou impossível o conhecimento pessoal, a obsessão oficial passou a ser segurança e controlo.

Até ao início da era electrónica, praticamente qualquer pessoa podia imigrar com relativa facilidade. Quando, já no final do século XX, as ondas de imigração se tornaram avassaladoras, surgiram imensas barreiras burocráticas tornando boa parte do fluxo migratório ilegal! Algo que seria inimaginável poucas décadas antes: a proibição do direito de ir e vir!

De facto, já existia algum controlo de movimento durante a primeira metade do século XX – o que levou à morte de milhares de pessoas nos períodos de guerra.

Mas, ao longo de poucas dezenas de anos, os mecanismos de controlo electrónico se tornaram tão intensos que um caso como o do célebre

diplomata Português Aristides de Sousa Mendes – que, através da emissão de passaportes, salvou milhares de Judeus durante a Segunda Guerra Mundial, ainda que tal acto heróico condenasse o seu futuro e o da sua família – praticamente não mais seria possível.

O controlo e vigilância se estenderam rapidamente aos produtos e serviços.

Nos anos 1990, a comercialização de uma imensa quantidade de vinhos, queijos e produtos caseiros regionais foi proibida pela União Europeia, devido à dificuldade de os manter sob controlo. Alguns críticos acusavam essa devastadora estratégia – feita em nome da saúde pública – de ter sido uma forma de reforçar a pressão na cobrança de impostos, pois produtos regionais feitos em casa estão livres das garras do Estado. Assim, eles acabaram por ser simplesmente proibidos.

Alguns produtos especiais com tradição de milhares de anos, como queijos, doces, pães ou

vinhos, simplesmente desapareceram.

Em praticamente todos os países a lei passou a determinar a obrigatoriedade de apresentação prévia do número de identificação fiscal – nos Estados Unidos, o número de segurança social – para que uma transacção comercial, qualquer que fosse a sua natureza, pudesse existir. A informação era registada e automaticamente enviada para as autoridades, estabelecendo um controlo total.

Em Setembro de 2008, alguns críticos consideraram a avassaladora crise financeira mundial, anunciada como o início de uma nova e devastadora depressão internacional, como sendo uma violenta manipulação de massa numa escala planetária com o objectivo de criar um melhor ambiente para um dos candidatos na luta pela presidência Americana. Com o caos espalhado por todo o mundo, uma figura mais conservadora e mais velha teria mais chances de vencer. A tremenda crise mundial aconteceu exactamente sete anos depois dos terríveis ataques de 11 de

Setembro.

Mas, Barack Obama – o candidato mais novo e menos conservador – ganhou as eleições, fazendo uso intensivo dos efeitos da crise na sua campanha.

Entretanto, havia um outro cenário. Gradualmente, após a nomeação de George W. Bush para a presidência Americana em 2001, e rapidamente após 11 de Setembro, o poder mudou de mãos em diversos países, estabelecendo uma estrutura mais conservadora voltada para padrões de controlo e vigilância nunca antes vistos. Pensava-se que se as eleições de 2008 mudassem os grupos de poder, aqueles pesados – e muitas vezes ilegais – sistemas de controlo e vigilância tenderiam gradualmente a se desintegrar. Todavia, não foi o que aconteceu.

Em poucos dias, no meio da confusão e do pânico financeiro de Setembro de 2008, vários governos, em diversos países, intervieram

ilegalmente nos mercados, criando instrumentos de controlo e vigilância estabelecidos para longo termo, e não apenas para aquele momento específico. O governo Americano mudou de orientação, mas os instrumentos de controlo e vigilância se tornaram ainda mais rigorosos e abrangentes.

Assim, a crise financeira mundial de 2008 teria servido, de facto, para reforçar e tornar definitivos aqueles instrumentos, eliminando antigos procedimentos democráticos, apagando direitos dos cidadãos e estabelecendo uma realidade próxima dos mercados pesadamente controlados, como o que acontece em ditaduras – mas orientada para um crédito intenso e um consumo contínuo.

Em vinte e seis de Setembro de 2009, os jornais de todo o mundo anunciavam que os países do chamado G-20 tinham decidido por implantar ainda mais rígidos mecanismos de controlo, intervindo até mesmo em empresas

privadas, nos salários de executivos, lembrando os antigos ideais Marxistas de intervenção social nos meios de produção. A Alemanha e a França chegaram a pedir o estabelecimento de limites para salários de administradores de grandes grupos. O primeiro ministro Britânico, Gordon Brown, chegou a afirmar que aquelas medidas de controlo iriam salvar "milhões de empregos" – mesmo que poucos meses mais tarde, no início de 2010, a Europa e os Estados Unidos atingissem níveis recorde de desemprego.

No meio do furacão financeiro de 2008, Durval de Noronha Goyos, reconhecido advogado Brasileiro, árbitro da *Organização Mundial do Comércio*, manifestava a sua profunda indignação: «A injecção massiva de capital em empresas privadas, empréstimos a juros simbólicos, a expansão da base monetária, tudo isto feito sem a aprovação dos parlamentos, sem consulta popular, sem aprovação ou mesmo conhecimento prévio de instituições multilaterais como a *Organização Mundial do Comércio*, o *Banco Mundial* ou o

Fundo Monetário Internacional são não apenas ilegais mas acontecem em total desrespeito para com aquelas entidades multilaterais, afectando pesadamente a sua credibilidade».

Um possível resultado daqueles actos seria o gradual desaparecimento de tais instituições, mergulhando o planeta num híper controlado mercado assimétrico, beneficiando ainda mais pequenos grupos de interesse e lançando grandes redes descentralizadas de controlo, actuando localmente através de imensos conjuntos de leis voláteis, e eliminando a participação popular nas decisões colectivas.

Tal violento golpe, durante os últimos meses de 2008, implantaria em poucos dias, em praticamente todo o planeta, uma pesada estrutura de leis e regulações – permitindo ainda maiores controlo e vigilância – que poderia sobreviver durante décadas, praticamente imune às oscilações do poder político promovidas por um sistema democrático!

Provavelmente, a nacionalização do sistema bancário – que caracterizou as medidas assumidas pelos Estados em Setembro e Outubro de 2008, foi um passo prático de forma a aniquilar completamente o sigilo bancário e estabelecer mais um instrumento para o controlo total da vida privada dos cidadãos.

Entretanto, forças de controlo e vigilância divorciadas do interesse público não são novas. Em 1913, Charles Lindbergh – Congressista Republicano – foi um firme opositor ao estabelecimento do *Federal Reserve Act*: «Este Acto estabelece o mais gigantesco consórcio do planeta... Quando o Presidente assinar este Acto, o governo invisível do poder do dinheiro, provado existir pelo *Money Trust Investigation*, será legalizado... A nova lei criará inflação quando o consórcio quiser inflação... A partir de agora, a depressão será cientificamente criada».

Mesmo com a clara e frontal oposição de

Charles Lindbergh – pai do famoso aviador – o Presidente Woodrow Wilson aprovou o *Federal Reserve Act* naquele ano de 1913. Alguns anos mais tarde, Woodrow Wilson lamentaria: «Sou o mais infeliz dos homens. Involuntariamente, arruinei o meu país. Uma grande nação industrial é agora controlada pelo seu sistema de crédito. O nosso sistema de crédito está concentrado. O crescimento da nação, portanto, e todas as nossas actividades estão nas mãos de poucos homens. Seremos um dos países mais desastrosamente governados, teremos um dos mais completamente controlados e dominados governos no mundo civilizado – não mais um governo feito pela opinião pública, não mais um governo feito pela convicção e o voto da maioria, mas um governo feito pela opinião e coacção de um pequeno grupo de homens dominantes».

Em vinte e sete de Julho, em 1979, John Lewis foi ferido por um veículo pertencente e operado pela secção do *Federal Reserve Bank* de São Francisco, Califórnia. Três anos mais tarde,

a Nona Corte dos Estados Unidos estabelecia que «Examinadas a organização e a função dos *Federal Reserve Banks*, e aplicando os factores relevantes, concluímos que os *Reserve Banks* não são instrumentos federais para os propósitos do Acto Federal de Reclamação de Danos, mas são independentes, empresas privadas e corporações controladas localmente».

Em dezassete de Junho de 2009, o presidente Barack Obama anunciava o lançamento de «um novo sistema de regulamentação financeira que aumenta os poderes do Federal Reserve e cria uma agência de defesa do consumidor de produtos financeiros».

Mas, a vigilância e o controlo total não são uma prerrogativa exclusiva do Estado e das empresas. Um dos problemas com o qual o direito, em diversos países, tem lidado com dificuldades devidas à sua larga e crescente escala é a fotografia indesejada, muitas vezes feita com o uso de telemóveis em balneários e a seguir vendida no

mercado negro do mundo virtual.

Outras vezes, *hackers* roubam imagens de comunicações pessoais, que a seguir são transferidas de pessoa a pessoa na rede – muitas vezes imagens pornográficas ou eróticas – e iniciam um processo de chantagem.

Mesmo a imagem pessoal, que durante séculos contou com o rigor do pudor e da honra, passou valer praticamente nada quando inserida no contexto do universo *low cost*, ainda quando são imagens íntimas de relações sexuais.

Segundo uma reportagem realizada pela em 2008, a Televisão *Suisse Romande* mostrava que imagens pornográficas e eróticas guardadas na memória dos telemóveis de adolescentes, por vezes imagens de outros adolescentes seus colegas, eram por eles considerados verdadeiros trofeus, fortes sinais de poder. E existiam em grande quantidade, contando não raras vezes com a concordância da outra parte.

Esse quadro de uma sociedade de *baixo poder*, ou de generalizado poder em baixa concentração, indica uma população voltada para o entretenimento e para o consumo.

A formação de grupos de criminosos e terroristas passou a não mais ocorrer de forma concentrada, tal como era comum até ao século XIX e boa parte do século XX, mas passaram a participar dinamicamente em todas as esferas sociais – até mesmo em governos e instituições policiais.

Os filmes de *Hollywood* nos dão um claro exemplo de como tal acontece.

Da mesma forma, pessoas pertencentes a esse novo domínio social, bairros de lata, edifícios em ruínas, onde reina uma grande pobreza, não raramente fazem uso das mais avançadas tecnologias – e têm acesso ao que de mais avançado daquilo que antes era chamado de

cultura erudita.

Esse complexo fenómeno caracteriza, ainda, muito das redes de criminosos em todo o mundo.

No ano de 2006, o cineasta e escritor Brasileiro Arnaldo Jabor lançou, como verdadeira, uma entrevista fictícia com Marcola, um perigoso criminoso, líder do mais poderoso sindicato do crime na cidade de São Paulo. A falsa entrevista foi caracterizada por um grande refinamento intelectual, mostrando na fictícia figura do criminoso real uma pessoa com profundos conhecimentos em filosofia, economia e sociologia. As revelações anunciadas na entrevista foram bombásticas, criando um escândalo nacional. O anunciado objectivo defendido pelo criminoso na entrevista era destruir a classe média e estabelecer uma ditadura liderada por assassinos cruéis. Ainda que o criminoso se vangloriasse de ter lido mais de três mil livros, ninguém imaginou que se tratava de uma ficção.

Num certo sentido, o conhecido cineasta Brasileiro reeditou, através do *antigo* jornal, o grande sucesso radiofónico de Orson Welles com a *Guerra dos Mundos* de H. G. Wells, então destinado a um *novo* meio de comunicação.

As pessoas acreditaram no que o texto dizia porque ele revelava um facto real, absolutamente claro a todos: a classe média estava sendo dizimada.

O mais interessante é que, durante longos meses, ninguém colocou em causa a autoria da entrevista. Praticamente ninguém sequer cogitou que seria impossível para alguém como aquele presidiário, nascido numa família miserável, criminoso desde a infância, tendo vivido uma adolescência praticamente abandonado, nas ruas, quando não estava em prisões e reformatórios, poderia subitamente se revelar como um intelectual daquele calibre. Ao contrário, todos consideraram algo muito natural! Mas, isso não seria natural poucas décadas antes.

As pessoas estavam correctas, pois essa possibilidade é também verdadeira, sinal dos novos tempos, um facto real e é um novo dado em termos civilizatórios.

Nos Estados Unidos, o *Unabomber* – presumivelmente Theodore Kaczynski – o mais procurado criminoso Americano nos anos 1990, terrorista contra a tecnologia e contra os centros de investigação nas universidades, lançou um manifesto, através de cartas enviadas a partir de 1995 ao *New York Times* e logo também publicadas pelo *Washington Post* com o título *The Future of the Industrial Society*. Contra a esquerda e contra as novas tecnologias, o terrorista revelava um surpreendente refinamento intelectual.

Tal como na entrevista fictícia criada por Arnaldo Jabor, no *Unabomber* outro clássico da literatura parece estar em evidência: *Mil Novecentos e Oitenta e Quatro* de George Orwell.

Em *Mil Novecentos e Oitenta e Quatro*, o personagem Emmanuel Goldstein lançava um enigmático manifesto onde afirmava que «ninguém jamais viu o Grande Irmão. A sua função é a de agir tal um ponto de focalização para o amor, o medo e a reverência; emoções que são mais facilmente sentidas num indivíduo que numa organização».

Por outro lado, o manifesto do *Unabomber*, depois de defender que existiriam três tipos de instintos – um primeiro, que exige um esforço mínimo da pessoa; um segundo, que exige um grande esforço; e um terceiro, que é inalcançável – tratava de defender que «na sociedade moderna, as necessidades tais como a sexualidade, o amor ou o estatuto social permanecem amiúde como instintos do segundo género, em função da situação individual. Mas, exceptuando-se as pessoas com um apego particularmente forte ao estatuto social, o esforço requerido para satisfazer esses instintos sociais é insuficiente para corresponder adequadamente ao processo de aquisição de poder. Criaram-se por isso necessidades artificiais

que se integram nos instintos do segundo género, com vista a satisfazerem o processo aquisitivo de poder».

A literatura tornada *conteúdo* de um novo meio.

A antiga condição de alta concentração e alto poder, que conduziu ao ideal do *welfare* na defesa de uma relativa estabilidade social, e que caracterizou uma nítida separação entre pessoas honestas e criminosos, tende simplesmente a desaparecer com a sociedade *low power*. Deixaram de existir as antigas barreiras de classes, de educação ou de desenvolvimentos tecnológicos – como também um bem determinado perfil de crime.

Em vários países, não raramente, a polícia passou a ter armamento menos sofisticado que o utilizado por grupos de bandidos e, em certos casos, até mesmo menos potentes que as armas utilizadas ou escondidas pela população em geral.

Era estimado existir cerca de uma arma por pessoa nos Estados Unidos, no início do século XXI!

Mesmo nos países mais desenvolvidos, redes de tráfico de drogas e de assassinos são muitas vezes organizadas a partir das próprias prisões onde estão encarcerados. Em alguns países, como o Brasil, por exemplo, bandos de criminosos chegam mesmo a fazer vídeo conferências ilegais em *tempo real* entre diversos estabelecimentos prisionais utilizando computadores e telemóveis.

No início dos anos 2000, traficantes de drogas transformaram a *Frederick Douglas Towers* – edifícios de habitação social localizados em Buffalo, Estados Unidos – num centro para venda de drogas ilegais. Então, o sistema de vigilância daquela instituição, composto por uma grande quantidade de câmaras de vigilância, passou a ser utilizado para controlar os movimentos de policiais.

Dados da *World Health Organisation*

mostram que, apenas nos Estados Unidos, mais de trinta e um mil grupos de criminosos identificados estavam em franca operação no ano de 1996. Um número que, seguramente, espantaria Al Capone. Naquele mesmo ano existia idêntico número de grupos de fabricantes de roupas nos Estados Unidos, empregando cerca de oitocentas mil pessoas.

Grupos organizados de criminosos comparados a verdadeiros complexos empresariais.

Em 2008 a empresa Alemã *BASF* foi alvo de ciber-extorsão. Atacados por um vírus devastador, foram obrigados a pagar um valor pelo "resgate", isto é, pela tele-liberação dos seus sistemas digitais e anulação do vírus.

Surgem novos tipos de cibercriminalidade, como o *clickjacking* – quando um pirata é capaz de activar à distância a câmara e o microfone que passaram a equipar boa parte dos computadores

em todo o mundo.

De tempos em tempos, jovens cibercriminosos são presos e têm as suas penas anuladas em troca de trabalhos para a polícia, na busca de outros *hackers* ou na espionagem sobre cidadãos comuns.

Em 2004, foi anunciado que o roubo de identidade teria ultrapassado o tráfico de drogas como principal problema criminal nos Estados Unidos.

Entre Abril de 1998 e Abril de 2003, segundo relato da *Federal Trade Commission* dos Estados Unidos, aconteceram mais de vinte e sete milhões de casos de roubo de identidade em solo Americano, sendo que cerca de dez milhões tinham acontecido apenas nos doze meses entre 2002 e 2003. As estimativas apontavam para que esse número superasse os setenta e cinco milhões num futuro próximo. O mesmo relatório mostrava que metade das pessoas simplesmente nem chegou a

perceber que tinha sido roubada.

Henry N. Pontell e Simon A. Cole – professores de criminologia na Universidade da Califórnia – explicavam, em 2005, a facilidade com que se realizava um roubo de identidade nos Estados Unidos, num processo muito semelhante senão idêntico a outros países: «Apenas com um nome e o número do INSS, um "especialista" pode solicitar uma cópia do relatório de crédito da vítima e obter informação sobre linhas de crédito abertas. Os números de identificação pessoal do cartão de crédito podem então ser acessados, os endereços originais são alterados de forma a reencaminhar contas para endereços fraudulentos, e múltiplos utilizadores são adicionados a uma conta já existente. O nome de solteira da mãe pode ser obtido através do contato com o gabinete das informações pessoais. As transações financeiras finais normalmente ocorrem através de intermediários, que compram caros equipamentos eletrônicos que são então vendidos a outro revendedor por metade do

valor real. Os intermediários recebem cerca de dez porcento do lucro auferido pelos falsários. Os outros participantes na rede – isto é, falsários de identificação e endereços que permitem que os produtos sejam entregues nas suas casas – são pagos de maneira semelhante. Para além dos produtos comprados, os intermediários podem ser contratados para fazer transações de grandes retiradas de dinheiro através do caixa rápido e das máquinas de cartões de crédito».

Governos, como o da China, são acusados de utilizar prisões para falsificação de produtos que serão camufladamente exportados a seguir.

Os governos da China e da Rússia estão entre aqueles que utilizarão mais intensivamente *hackers* com o objectivo de atacar outros países, elevando o crime à dimensão de Estado – tal como têm sido frequentemente acusados os Estados Unidos, a Inglaterra, o Canadá e a Austrália entre outros pelo uso do *Echelon*.

Em 2009, um *hacker* aparentemente contratado pelo governo Francês roubou de um banco Suíço em Genebra informação bancária relativa a milhares de pessoas – dados que seriam utilizados pelo governo de Paris para perseguir fiscalmente cidadãos Franceses. O roubo levou ao governo Suíço a anunciar a suspensão da convenção fiscal de dupla imposição com a França. Essa convenção permitiria a troca de informações em caso de fraude fiscal. Uma vez estabelecida a evidência de fraude fiscal, as informações seriam fornecidas pelo governo, como exige a constituição Suíça. Mas, a convenção deixou de fazer sentido num contexto de roubo por parte de outro Estado.

Para Nicolas Arpagian, trata-se da eclosão de uma terceira Guerra Mundial, desta vez virtual, espalhada por todos os sectores da sociedade: a *ciberguerra*.

No dia dezasseis de Maio de 2008, o *Financial Times* anunciava que cerca de setecentos

e cinquenta mil computadores pertencentes a empresas Alemãs estavam contaminados por programas espias.

No dia três de Setembro de 2007, o Pentágono reconheceu oficialmente que parte da sua rede informática tinha sido desligada durante alguns dias, pois tinha sido vítima de um ciber-ataque.

Em Outubro de 2008 Kelly Humphries, porta-voz da NASA, anunciava que a Estação Espacial Internacional tinha sido atacada por um vírus informático chamado *W32.Gammima.AG*, alojado nos computadores portáteis dos astronautas. O objectivo desse vírus, segundo anunciado, seria apenas o de coligir informações sobre jogos de vídeo!

Ainda que fosse verdade, não tinha sido aquela a primeira vez que um vírus informático tinha entrado na estação orbital.

Três meses antes do anúncio feito por Humphries, a *OSCE Organização para a Segurança e Cooperação na Europa* lançaria a Declaração de Astana: «A Assembleia Parlamentar da OSCE exorta aos governos a condenar os ciberataques sobre um plano moral, ao mesmo título que trata os seres humanos ou a pirataria visando a propriedade intelectual, e a estabelecer normas de conduta universal no ciberespaço».

Para além de estabelecer regras universais sobre um meio que é aberto por natureza, a questão também é saber como seria possível estabelecer um direito que escapa ao princípio da propriedade da terra, legado pelo universo Romano, um direito imaterial, transnacional e transcultural.

Tal como os vírus informáticos, os sistemas de vigilância conhecidos como *Closed Circuit Television*, ou *CCTV*, equipados com programas de reconhecimento facial passaram a estar espalhados por todo o planeta e não passarão desconhecidos das redes criminosas mundiais.

Apenas na Grã-Bretanha era estimado, em 2002, existirem cerca de quatro milhões e duzentos mil sistemas *CCTV* em funcionamento – o que significava uma câmara para cada catorze pessoas. Elas representavam cerca de 25% das câmaras de vigilância de todo o mundo.

Em 2004, calculava-se que uma pessoa num único dia normal de trabalho em Inglaterra teria a sua imagem cerca de trezentas vezes capturada pelas câmaras de vigilância.

Em 2003, calculava-se que mais de 75% das novas escolas nos Estados Unidos estavam equipadas com sistemas de vigilância *CCTV*.

Em 2009, o *Government Computer News*, do Reino Unido, anunciava que parte das câmaras de vídeo vigilância não mais seria controlada por pessoas, mas sim por sistemas digitais. A tendência era de que todo o sistema de vigilância passasse a ser controlado por computadores.

Curiosamente, o primeiro sistema de *CCTV* foi instalado pelo regime nazi em 1942, pela empresa *Siemens AG*, para acompanhar o lançamento dos foguetes V2.

Não menos curioso é o facto de menos de 3% dos crimes terem sido resolvidos com o auxílio de câmaras de vigilância, de acordo com um relatório da polícia Britânica de 2008.

Desde 1997, na cidade de Nova York, o Central Park, as estações de metro e outros lugares públicos passaram a ser vigiados por câmaras escondidas vinte e quatro horas por dia. Um ano depois, em 1998, já haviam mais de três mil câmaras de vídeo vigilância pública em operação na cidade de Nova York.

Grande parte dos sistemas de vídeo vigilância passou a contar com a tecnologia conhecida como *VCA – Video Content Analysis*.

Algumas vezes, ainda que raramente, surgia uma reacção contra os movimentos de super vigilância e controlo. No final de Agosto de 2009, uma notícia veiculada pela *Agence France Presse* informava que o governo Suíço ordenava à *Google* a imediata suspensão do serviço conhecido como *Street View* – através do qual uma pessoa, em qualquer lugar do mundo, pode passear virtualmente pelas ruas de uma cidade. Segundo o governo Suíço, aquele serviço não estava atendendo às exigências legais de protecção à privacidade do país.

O mais impressionante, entretanto, foi constatar que algumas reacções de pessoas na Europa – através de comentários publicados em jornais – foi de classificar a atitude da Suíça como hipócrita e reaccionária!

Aquelas pessoas não tinham em conta os princípios de liberdade que caracterizaram o mundo Ocidental durante séculos forjando a aspiração ao que Karl Popper chamou de *sociedade aberta*.

Também não tinham consciência de que o governo da Suíça obedece às determinações estabelecidas pela população e não o contrário, como acontece com todos os outros países.

A vigilância, como fenómeno generalizado, contou com a emergência de sistemas com objectivo e métodos semelhantes ao temível *TIA Total Information Awareness*, de Poindexter, desenhado para detectar comportamentos – muitas vezes considerados absolutamente normais e perfeitamente aceitáveis por grande parte das pessoas.

Assim, em 2009 o governo Australiano anunciava a definitiva implantação do sistema *Smartgate* nos seus aeroportos e outras estações de transporte. Trata-se de um sistema que identifica automaticamente o viajante, através de sofisticados processos de reconhecimento facial, entre outros processos de identificação.

No aeroporto de Schiphol, em Amsterdão,

Holanda, estava sendo estabelecido o sistema de reconhecimento de identidade conhecido como *Privium*. Através dele, os dados capturados são automaticamente partilhados com o governo Americano, numa extensão que é mantida distante do conhecimento público pelo habitual secretismo Estatal.

Na sua página de "política de privacidade", o aeroporto de Schiphol promete que não usará a informação sobre os visitantes do *site*, mas não faz qualquer referência sobre o uso de informação acerca dos aderentes ao sistema *Privium*! Informa, ainda, que instala automaticamente um *cookie* de espionagem em cada computador que aceda ao seu site.

Ainda mais impressionante é o facto do aeroporto "vender" esse serviço na forma de um clube para sócios especiais. Aquele que se tornar membro do *Privium Clublounge* do aeroporto de Schiphol terá direito à entrada mais rápida com o rastreamento de imagem da íris,

prioridade no estacionamento do automóvel, descontos exclusivos para o uso de manobristas no estacionamento, check-in em *business class*, assistência especial no aeroporto e vários outros descontos. Benefícios que pretendem, como é claro, estabelecer um novo padrão de vigilância e controlo de passageiros.

Não houve qualquer protesto ou manifestação pública relevante contra aquelas acções do governo Holandês.

Apesar das medidas draconianas anunciadas pelo aeroporto de Schiphol, foi lá que embarcou o terrorista Nigeriano no dia vinte e seis de Dezembro de 2009 com destino aos Estados Unidos. A deflagração do controlo e vigilância exaustivos sobre todos os cidadãos é a prova cabal da completa falência dos sistemas de serviços secretos em todo o mundo.

Por isso, em Janeiro de 2010, Gilles de Kerchove, coordenador da política anti-terrorismo

da União Europeia, declarava que a Comissão Europeia já estava convencida da utilidade do uso de *scanners* corporais nos aeroportos – equipamento que permite electronicamente "tirar a roupa" das pessoas. A partir do seu uso, todas as pessoas terão de ficar nuas electronicamente antes de embarcar – num procedimento que lembra as medidas de segurança adoptadas nas prisões.

Um pouco como parte de uma quase histeria colectiva que tomou boa parte do mundo imediatamente após os ataques de onze de Setembro de 2001, Larry Ellison, presidente da *Oracle*, ofereceu ao governo dos Estados Unidos *software* grátis para a criação de *smart cards* de identificação para toda a população Americana.

No Peru, o governo estabeleceu o uso obrigatório de bilhetes de identidade com *chip* de reconhecimento facial para os seus habitantes.

Nos Estados Unidos, ao longo dos últimos anos, tem se discutido a inclusão de dados de ADN

nos *chips* de futuros cartões de identidade e até mesmo o implante de chips de identidade nos corpos das pessoas.

Em dezanove de Abril de 2009, Solomon Moore escrevia, no *New York Times*, que «oficiais dedicados à aplicação da lei estão expandindo vigorosamente o uso de informação genética de forma a incluir milhões de pessoas que tenham sido presas ou detidas mas ainda não sentenciadas. (...) Mas especialistas de justiça criminal citam as cautelas sobre privacidade contidas na Quarta Emenda da Constituição e se preocupam diante da possibilidade da nação estar se transformando numa sociedade de vigilância genética».

Smart cards passaram a ser impostos como cartões de identidade pelos governos de vários lugares como a Coreia do Sul, Malásia, Tailândia e Hong-Kong.

Empresas como a *L-1 Identity Solutions* passaram a oferecer todo o tipo de tecnologia para

vigilância e controlo, para governos, entidades privadas ou até mesmo para indivíduos.

Como o sociólogo David Lyon diz, «os dados de vigilância, antes mantidos em gabinetes fechados e lidando com informações orientadas a pessoas em lugares específicos, estão agora fluídos, fluentes e globais. (...) A fronteira deslocalizada é um exemplo primeiro da fronteira global».

Em 2006, David Stork, cientista que trabalha para a *Ricoh* na Califórnia, dizia: «Brevemente, quando fizermos uma fotografia com o nosso telemóvel, ele será capaz de descobrir quem é a pessoa, baseado na sua localização e lista de contactos».

Isto é, o reconhecimento facial há muito deixou de ser uma questão essencialmente humana.

Essa competência de reconhecimento humano, incluindo a detecção de preferências de

todo o tipo, cruzando informações como saldos em contas bancárias, hábitos de consumo, livros preferidos, restaurantes e pratos preferidos, perfumes, hábitos de comportamento como saídas à noite e horas médias de sono, deslocações territoriais, preferências musicais, hábitos de conversação, se a pessoa é mais tímida ou não dependendo da diversidade dos contactos telefónicos e de *social networks*, tendências políticas, evidências de níveis de consumo e muito mais – tudo poderá ser imediatamente cruzado e associado por sistemas digitais em tempo real.

Todas essas informações poderão ser utilizadas tanto para fins comerciais como pelas autoridades governamentais. De facto, em maior ou menor escala, isso já acontece.

Tudo o que tem sido imaginado como *solução* para essa complexa situação tem estado fundado numa abordagem lógica de *concentração*, que tende a desaparecer.

Para John Gilmore, co-fundador da *Electronic Frontier Foundation*, os computadores são literalmente extensões das nossas mentes e, portanto, os seus conteúdos deveriam permanecer privados tal como os nossos mais profundos pensamentos.

A questão é saber o que é o conceito de *mente* – se continua a ser um compartimento estanque como pretendiam os pensadores do século XIX, ou se a mente pode estar em diversos lugares e se aquilo que identificamos como consciência individual nada mais será que um momento, tal como uma espécie de macro sinapse num complexo quadro de relações.

As antigas noções de vida pessoal, de profissão e até mesmo de desígnio histórico, dependem do princípio de concentração. Mas, os novos tipos de organizações – e, entre elas, as criminosas – expandem-se através de nano associações, grupos voláteis, estratégias colaborativas não intencionais, ligações feitas ao

acaso, imprevisíveis e instáveis.

Da mesma forma, entre os grupos económicos, grandes empresas subcontratam fornecedores de toda a natureza, formando uma cadeia fortemente distributiva.

O surgimento do apelo ao *downsizing* nos anos 1990 transformou a estrutura de milhares de empresas em todo o mundo, distribuindo funções e eliminando benefícios sociais – desconcentrando e distribuindo risco. Mas, o *downsizing* também aumenta a rotatividade de mão de obra precária, eliminando muito do que era o antigo conceito de *profissão*.

A exclusão social não mais trata de uma ideia total, de um *paradigma*, mas sim de um *sintagma* – de natureza complexa, significando distribuição não linear por todos os lados e em diversas dimensões.

Na sua célebre obra *The Structure of*

Scientific Revolutions, de 1962, Thomas Kuhn estabeleceu o princípio segundo o qual as metamorfoses civilizacionais aconteciam em *saltos paradigmáticos*, espécies de mudanças de fase, tal como apontou a *Gestalt* muitos anos antes, no início do século XX.

Tal como as leis da *Gestalt*, as revoluções paradigmáticas são de natureza fortemente visual, funcionando muito bem na realidade industrial da sociedade literária.

Não por acaso, Thomas Kuhn resgatou da linguística a expressão que usou para designar os saltos revolucionários de transformação do conhecimento. Ferdinand de Saussure já utilizava a palavra *paradigma* para indicar um conjunto homogéneo de significado.

A palavra *paradigma* surgiu da contracção de duas palavras Gregas, *para* e *deiknynai*, que significam, respectivamente, *lado a lado* e *mostrar*, indicando a ideia de *modelo*, de *exemplo*.

Um copo, por exemplo, é um *paradigma*. Um automóvel é um *sintagma* – pois é formado por diversos *paradigmas*, como os pneus, o motor, portas, assentos e assim por diante.

O mundo industrial, *paradigmático*, visual e literário, fortemente designado pela emergência da classe média, transformou-se no mundo dos serviços, trans-sensorial, transdisciplinar e *sintagmático*, onde as metamorfoses acontecem nos mais variados níveis, de forma turbulenta e instável.

Um universo onde a própria imagem se tornou efémera e volátil. No início do século XXI, pela primeira vez, se tornou impossível identificar uma falsificação fotográfica. David Brin, em *The Transparent Society*, dizia que « uma das nossas previsões mais assustadoras que agora circulam é que nós estamos para abolir a era da prova fotográfica ».

Como um elegante paradoxo, o planeta é tomado por sistemas de memória sem precedentes, com um incalculável número de imagens – mas, nunca se poderá saber quais são verdadeiras, porque aquilo a que chamamos de *verdade* é uma questão essencialmente literária.

Muitas vezes, as pessoas parecem ter dificuldade em compreender a extensão das graves implicações geradas pela falta de privacidade, acreditando ingenuamente num aumento da segurança. Basta, entretanto, imaginar o que teria sido um regime como o nazista, se tivesse o controle da informação geral, para tremer diante de um cenário devastador.