Tempos difíceis para as liberdades civis

"Many men have been seized and imprisoned under the so-called prophilactic Precrime structure… Accused not of crimes they have committed, but of crimes they will commit. It is asserted that these men, if allowed to remain free, will at some future time commit felonies." (1)

O texto acima é a reprodução de um trecho onde um personagem da novela de ficção ***Minority Report***, escrita em 1956 por Philip K. Dick, discorre sobre o sistema de pré-cognição de crimes, chamado de *Precrime*. Com a utilização de três pessoas sensitivas imersas em líquido amniótico e conectadas a scanners que varrem seus sinais mentais, os delitos cometidos em determinada área são previamente visualizados e os futuros criminosos presos e julgados por aquilo que ainda não cometeram, mas que **iriam** cometer.

Esse exercício de ficção, imaginado na década de 50, é assombrosamente similar com a vontade de alguns governos após os ataques terroristas cometidos contra os Estados Unidos em 11 de setembro de 2001.

Coincidentemente com o longa-metragem, baseado na história, ter chegado às telas, a agência federal responsável pela pesquisa de defesa norte-americana (*Defense Advanced Research Projects Agency – DARPA*) lançou um programa que parece uma tentativa de pré-cognição de condutas exatamente como disposta em Minority Report, com a utilização de poderes provenientes não de pessoas sensitivas, mas da tecnologia.

O sistema, batizado de ***TIASystems*** (*Total Information Awareness Systems*) (2) pretende realizar algo ainda não pensado: prever os movimentos de todos os potenciais terroristas e prevenir suas ações. É o mais ambicioso sistema de vigilância já imaginado do mundo, e para bem cumprir seus objetivos, seu alcance não reconhece jurisdição. Sua capacidade de armazenamento de informações é da ordem de *petabytes*. Um *petabyte* é o equivalente a 1024 *terabytes*, então um **quatrilhão** de bytes. Nada equivalente existe hoje, e uma grande quantidade de pessoas e empresas está envolvida no desenvolvimento do projeto.

Segundo a *DARPA*, que tem se mostrado excessivamente econômica nos detalhes do projeto, seu funcionamento segue um encadeamento lógico:

DETECTAR -> CLASSIFICAR -> IDENTIFICAR -> RASTREAR -> COMPREENDER -> PREVENIR

Integrando arquiteturas de tecnologia da informação, os agentes federais norte-americanos pretendem colher toda e qualquer informação proveniente de transações financeiras, viagens, educação, serviços médicos e veterinários, transportes, entrada de estrangeiros no país, comunicações, eventos, movimentação geográfica, hospedagem, uso de recursos de comunicação e Internet, e cruzar esses dados com modelos de padrão de comportamento pré-estabelecidos, com o fito de encontrar supostos métodos potencialmente danosos.

O sistema trabalha formulando hipóteses e propondo teorias. Para alcançar esses objetivos, investimentos vultosos (e não divulgados) estão sendo gastos na invenção de novos métodos, modelos, algoritmos e ferramentas tecnológicas de inteligência artificial.

O objetivo do programa é alcançar, em 5 anos, "*a reinvenção total das tecnologias de armazenamento e acesso de informação*".

O *TIASystems* já colocou em alerta os ativistas das liberdades civis nos Estados Unidos, como demonstra o advogado Lee Tien, da *Electronic Frontier Foundation* (www.eff.org) :

"O Total Information Awareness Program, *com sua habilidade de prover armazenamento de todos os registros de cartão de crédito, empregos, médicos, provedores de acesso à Internet, é uma receita para o desastre das liberdades civis ao menos que existam provisões para os cidadãos tomarem conhecimento de quem está observando seus registros e possibilidades de verificação e correção dos mesmos registros*".

Discussões acaloradas surgirão com o desenvolvimento deste poderoso sistema de vigilância. Certo é que a tecnologia, ao permitir o aprimoramento das atividades humanas, traz no processo conseqüências nem sempre consideradas positivas. A diminuição da liberdade pessoal é apenas uma delas.

O *TIASystems* é a ferramenta mais avançada já projetada para obtenção de informações, porém há um verdadeiro arcabouço de sistemas condizentes com a metáfora do pós-guerra descrita por George Orwell em 1984, com a figura do "Grande Irmão" a vigiar os passos dos cidadãos. Elencamos apenas os principais:

Projeto Echelon – é um sistema de vigilância e interceptação de dados operado por agências de inteligência de 5 países, Austrália, Reino Unido, Estados Unidos, Canadá e Nova Zelândia. O *Echelon* data de 1971, e foi elaborado de acordo com o tratado UKUSA, de 1947. Acredita-se que o *Echelon* intercepte informações provenientes de satélites, Internet, telefonia, transmissões de rádio e até comunicaçõe subaquáticas. Um mapa completo das bases da rede de comunicação do *Echelon* pode ser visualizado no endereço www.fas.org/irp/program/process/echelon.jpg, *website* de língua alemã da *Federation of American Scientists*.

Carnivore – este programa espião foi desenvolvido pelo FBI e batizado de DCS 1000. Primeiramente destinado à obtenção de informação dos dados que trafegam na Internet interceptados diretamente no protocolo TCP, em todas as portas de comunicação. Instalado em provedores de acesso à Internet, o Carnivore filtra informações de acordo com programações prévias. Sua existência veio à tona em 2000, e já foi objeto de investigações na justiça norte-americana, por movimentação da *Electronic Privacy Information Center*, entidade defensora dos direitos civis.

Tempest – programa originado na *National Security Agency (NSA*) dos Estados Unidos, ainda carece de maiores informações sobre seu funcionamento. É direcionado para a captura de sinais eletrônicos através de paredes e edifícios, mesmo em sistemas não conectados em rede.

Magic Lantern – um cavalo de tróia (3) programado pelo FBI, capacita os investigadores a descobrir mensagens codificadas pelo sistema PGP (4) em comunicações de pessoas sob suspeita. Feito para trabalhar em conjunto em operações com uso de *key-logging* (5).

FIDNET – *Federal Intrusion Detection Network* (6), proposta aprovada no governo Clinton para procurar deter ataques em sistemas do governo Norte-americano. Prevê facilitar o grampo em telecomunicações, tendo como objetivo a segurança nacional.

Enfopol – é um documento que dispõe um conjunto de requerimentos técnicos para a interceptação de comunicações na União Européia, destinado às casas legisladoras participantes do sistema europeu.

Somem-se a estes iniciativas de vigilância tomadas na China, Rússia, França, Canadá, Israel e Alemanha, temos um campo árduo de batalha, onde o liame entre a quebra dos direitos individuais permeia a necessidade de prover segurança em sentido coletivo.

Constituições e jurisdições precisam ser preservadas. É irônico perceber como a tecnologia pode atuar em sentido duplo: ao mesmo tempo que promove intenso progresso nas relações humanas, também é passível de contribuição para o retrocesso nas conquistas pessoais contidas em princípios como o da presunção de inocência, privacidade de comunicações e dados pessoais, liberdade de opinião e expressão, e outros tantos garantidos em vários ordenamentos jurídicos ao redor do planeta. Individual e coletivo. Duas palavras que começam a se fundir em significado. Perigosamente.

Notas de rodapé:

(1) *Muitos homens tem sido capturados e encarcerados sob a chamada estrutura profilática Precrime… Acusados não de crimes que cometeram, mas de crimes que irão cometer. É certo que esses homens, se permitidos ficar em liberdade, irão em algum momento no futuro cometer delitos*. (tradução do autor)

(2) Sistemas de Conhecimento Total da Informação

(3) Programa invasor destinado a colher informações de computadores alheios

(4) *Pretty Good Privacy*, sistema de criptografia de mensagens eletrônicas

(5) Monitoração à distância dos movimentos do teclado do computador investigado

(6) Rede Federal de Detecção de Intrusos

Date Created
01/09/2002