Revista de Estudos Politécnicos
Polytechnical Studies Review
2008, Vol VI, nº 9
ISSN: 1645-9911

A intercepção legal de comunicações em redes IP

Irene Portela[1]

Resumo. No âmbito das vigilâncias electrónicas, o conceito tradicional de "escutas telefónicas" está desadequado à realidade criminal. O uso do ciberespaço pelas células do terrorismo internacional, torna imprescindível a intercepção de comunicações em redes IP. Mas a utilização das novas tecnologias envolve riscos e tem impactos consideráveis nos meios e na operacionalidade da segurança nacional, além de elevados custos inerentes à sua utilização indiscriminada. No âmbito do terrorismo internacional, não só a intelligence, como as investigações criminais, implicam uma elevada concentração de recursos orientados para o combate, mas especialmente para a prevenção. Neste contexto, o uso como meio de prova do material interceptado através das novas tecnologias de informação implica profundas alterações no regime legal das provas admissíveis em julgamento.

Palavras-chave: provas processuais, Internet, terrorismo, vigilância electrónica, escutas.

Abstract. The traditional concept of "wiretapping" or "eavesdropping"within the scope of electronic surveillance is inadequate to current criminal reality. The use of the cyberspace by international terrorists' cells have made indispensable the intersection of IP communication net. But using new technologies involves risks and have a significant impact in National Security, as well in the high costs related to its indiscrimated use. As far as International Terrorism is concerned not only the intelelligence but also the law enforcement imply a high concentration of resources in order to the fight and, especially to the prevention. In this context, the utilization as evidence of the material intercepted by the new Information Tecknologies means profound changes in the legal model of the evidences admited on trial.

Keywords: Evidence, Internet, Security, terrorism, surveillance technology, eavesdropping.

[1] Escola Superior de Gestão - Instituto Politécnico do Cávado e do Ave.

1. Introdução

Para fazer frente ao *modus operandi* do terrorismo internacional, inscrito nas catacumbas internaúticas, secreto mas omnipresente, as políticas governamentais são compelidas a encontrar novos instrumentos de combate, sob pena de deixar ruir o paradigma do Estado de Direito que levou mais de duzentos anos a construir, a "democracia".

A constatação de que a internet é o instrumento privilegiado no contacto entre as células terroristas, e verificando que o terrorismo internacional deixou de ser linear, passando a organizar-se em redes acéfalas, pulverizadas, invisíveis, cujos braços anónimos se reproduzem de forma pandémica, o uso das novas tecnologias de comunicação na recolha de meios de provas na investigação criminal é uma questão obrigatória para a defesa da segurança nacional.

A reinvenção dos modelos de organização, de operacionalidade, de estratégia da segurança interna, a que os americanos denominam *latu sensu* de *"Homeland Security"(Davis, 2002;* Wisniewski, 2001) passa pelo crivo da globalização. O combate global é a única forma de travar o factor extraordinariamente multiplicador do "potencial de combate" das organizações terroristas orientadas pelo fundamentalismo religioso, e predispostas ao sacrifício da vida na busca de paraísos prometidos. Como Brown (2005) explicou "a conjunção da velocidade da internet do século XXI com o fanatismo do século XII transformou o nosso mundo num barril de pólvora" (p. C01). O terrorismo é agora um epifenómeno mundial, já não nacional, localizado intra-fronteiras, mas letalmente omnipresente e intangível. A este propósito Vitorino (2007), escreve "a estratégia do terror indiscriminado, usa meios de uma irracionalidade sanguinária, mas apresenta-se como muito racional na definição da sua mensagem política, na utilização dos meios de comunicação modernos como instrumentos propulsores da própria ameaça e na criteriosa definição dos alvos tendo em vista a repercussão pretendida"(p.1). Portanto "Não é de surpreender que terroristas em rede já tenham começado a influenciar as TIs (Tecnologias da Informação) com a gestão da percepção e a propaganda com o objectivo de influenciar a opinião pública, recrutar novos membros e gerar recursos", "Enviar uma mensagem", "e receber ampla exposição dos meios de comunicação jornalística são componentes importantes da estratégia terrorista, que tem como finalidade minar a determinação de um oponente. Além dos meios tradicionais, como televisão ou imprensa, a internet agora oferece aos grupos terroristas uma forma alternativa de atingir o público, em geral com muito mais controle directo sobre a mensagem." Zanini and Edwards, 2001).

O uso destas tecnologias deve ser objecto de regulamentação na medida em que o seu campo de acção é agora o ciberespaço, novo "*virtual criminal field"* (Capeller 2001; Grabosky and Smith, 2001; Wall, 2001), como campo poliárquico de poderes assimétricos potenciador do "empreendedorismo criminoso" ilimitado.

Por um lado, as novas tecnologias facilitam a disseminação das actividades criminosas tradicionais, e por outro lado, abrem potencialidades exponenciais para a cibercriminalidade para as quais o sistema legal ainda não tem resposta. Na guerra de informação, em rede, descentralizada, o *near to real time intelligence* é o agente impulsionador que reinventa o próprio processo de planeamento e de decisão, com flexibilidade e rapidez de resposta às novas ameaças (Garcia, 2008), num espaço completamente paralelo ao espaço jurídico tradicional.

Se por um lado a tecnologia actual permite o acesso a fontes de informação aberta com baixo custo e sem limites de utilização, por outro lado a revolução na informação trouxe também novas vulnerabilidades para a segurança. A crescente dependência dos Sistemas de Informações torna as infra-estruturas vulneráveis a vários tipos de ataques:

- A segurança é normalmente confiada a agências privadas, ou muito dependentes das infra-estruturas comerciais;
- A grande quantidade de informação levanta problemas na sua gestão;
- A filtragem da informação implica muitos meios humanos e materiais;
- A transformação em tempo útil, da amálgama de informação recolhida, em conhecimento utilizável implica custos extremamente elevados.

É perante estas vulnerabilidades contextuais inscritas num ciberespaço hostil que o combate ao terrorismo é alvo de excessos por parte dos Governos que sofrem o seu flagelo. As medidas antiterroristas centradas no objectivo de aumentar a segurança, vão alargando o âmbito e os mecanismos legalmente permitidos para efectuar vigilâncias, colheitas, buscas e apreensões de registos confidenciais, proibindo o recurso judicial e restringindo o acesso às provas que sustentam a condenação dos suspeitos, detidos por tempo indeterminado...[2]

> A questão a que importa responder é a de saber se é possível usar *as novas tecnologias e interceptar as comunicações para obter meios de prova que possam ser usados em Tribunal conseguindo condenações efectivas dos suspeitos de terrorismo?*

A vigilância pelas autoridades ou agências de segurança, do Estado ou privadas, através da intercepção das comunicações é uma questão central na medida em que determina a fiabilidade das provas recolhidas, cujo destino é a sustentação da acusação em julgamento e a consequente condenação dos crimes de terrorismo. Trata-se de uma questão cada vez mais importante, já que o uso da internet para praticar crimes continua a aumentar (Jancsewski and Colarik, 2005).

---

[2] Sendo esta questão que nos preocupou durante alguns anos e sobre a qual escrevemos a nossa tese de doutoramento

2. As dificuldades de intercepção de comunicações em redes IP

O uso das novas tecnologias na intercepção das comunicações com vista à obtenção de meios de prova passa a ser um instrumento privilegiado ao serviço da garantia e da efectiva manutenção da segurança nacional. Não obstante, a utilização destas tecnologias envolve riscos e tem impactos consideráveis nos meios e na operacionalidade da segurança, além dos custos inerentes à sua utilização indiscriminada.

As investigações criminais, relativas ao terrorismo, implicam uma elevada concentração de recursos orientados especialmente para a prevenção. Neste contexto a utilização das tecnologias aplicadas a operações de intercepção afim de recolher meios de provas provoca alterações visíveis no regime legal aplicável às provas legais, provocando alterações no âmbito e na forma como as investigações são conduzidas neste e noutros domínios da ordem jurídica.

O uso das novas tecnologias da informação envolve dois tipos de riscos (Privy Council, 2008):

- Riscos directos da exposição que resulta do uso e das potencialidades das técnicas que permitem a intercepção.
- Riscos indirectos decorrentes das mudanças que resultam do uso cada vez mais extensivo e indiscriminado das novas tecnologias de comunicação na "intercepção" .

A migração maciça e paulatina do uso dos telemóveis e dos telefones fixos para um tráfego baseado no Internet Protocol IP[3], em que não há distinção entre a voz e os dados, é irreversível, na medida em que os fornecedores de serviços de comunicações estão a aderir massivamente às redes IP.

[3] Designa-se por protocolo um conjunto de regras que definem o modo como a informação é formatada – os pacotes – e como os sistemas que constituem a Internet interagem de modo a garantir o fluxo coerente e eficiente de informação na Internet. Um dos protocolos estruturais da Internet é o IP (*Internet Protocol*) Padrão internacional usado para fornecer material através da internet. Os protocolos estruturais da Internet são dois, o IP (Internet Protocol) e o TCP (Transmission Control Protocol), e costumam ter a designação de TCP/IP. Estes protocolos funcionam nos sistemas internos da Internet, e também nos computadores e outros sistemas que pretendemos ligar à Internet (por exemplo, um computador, um telemóvel). Douglas E. Comer, Internetworking with TCP/IP, Volume 1: Principles, Protocols, and Architectures, Fourth Edition, Prentice Hall PTR, Upper Saddle River, NJ, 2000

Na rede IP, a comunicação não necessita de um circuito físico aberto e fixo, porque utiliza vários "caminhos" para chegar do utilizador-emissor até ao utilizador-receptor, através de um conceito de comutação de pacotes (Veiga, 2004).

O que significa que, a existência de uma comunicação IP, não implica que ambos os interlocutores possuam nem um terminal IP nem sequer Internet de banda larga. As redes IP podem comunicar também com terminais fixos analógicos, que podem ser um telefone ou fax com rede IP, ou um computador equipado com um software específico.

Os circuitos comutados dos telefones permitiam que o modelo de intercepção fosse simples, ou seja, nesse sistema, sempre que uma chamada de um ou para um alvo fosse estabelecida, a autoridade/agente podia aceder a qualquer uma das partes do circuito e copiar todo o conteúdo da chamada. Como já vimos, este modelo é inaplicável se os circuitos individuais são substituídos por redes IP.

Até que ponto o regime jurídico da utilização de comunicações interceptadas como meio de prova é exequível e efectivo na estrutura tecnológica existente, o poderá ser numa estrutura baseada em IP?

Mas, previamente a esta questão, existem outras com contornos eminentemente técnicos. Como é que a identidade de um emissor ou de um receptor de comunicações pode ser seguido a partir de pacotes IP? Como é que a pessoa que envia ou recebe um pacote de um IP pode ser identificada se não tem de se registar antes de usar o serviço, ou pode fazê-lo com dados inventados? Os aeroportos, os cibercafés, as bibliotecas, são espaços públicos onde nem sequer é necessário haver um pré-registo para aceder ao serviço de internet. Como é que se pode seguir determinada identidade via internet? A única forma de identificação dos usuários parece ser a de controlar o próprio serviço usado pelas pessoas (Branch, Pavlicic, and Armitage, 2004)

Na rede IP, a mobilidade do utilizador é a sua característica essencial, pelo que cada utilizador é identificado por um ou mais endereços fictícios, os chamados *"alias address"*, identificados por números telefónicos ou por um conjunto de letras (nomes).

O fornecedor de serviços IP permite ao usuário a utilização do endereço em vários locais associados a endereços IP diferentes, por isso é muito difícil para o sistema de intercepção identificar um usuário alvo pelo endereço fictício, independentemente de sua localização e endereço IP.

A intercepção legal do tráfego das comunicações em rede é normalmente feita através da instalação dos "sniffer" de pacotes, que são equipamentos colocados em determinados pontos na rede e que através de cabos ópticos ou conectados directamente aos hubs ou switches, servem para examinar todo o tráfego comunicacional daquele ponto (Branch, 2003). Os "sniffers"de pacotes podem ser programados para capturar somente o tráfego que interessa, ou seja, o tráfego originado de ou enviado para algum IP particular. Estes pacotes são então transmitidos directamente para a agência ou serviço de segurança via internet ou

são armazenados no sniffer para serem descarregados posteriormente (Branch, 2003).

Os *"sniffer"* foram concebidos para diagnosticar falhas na rede, e a sua aplicação na intercepção legal de comunicações apresenta muitos problemas de utilização, além de serem sistemas caros e complexos.

Um dos maiores problemas no uso dos *"sniffers"* tem a ver com a falta de segurança na intercepção. Assim, por exemplo, no caso de se tratar de uma intercepção ilegal, por causa de uma falha no sistema, ou de um erro humano, não é possível controlar as informações obtidas porque as comunicações são indistintamente interceptadas, sejam elas pertinentes ou não.

Além das preocupações técnicas, ou seja, das possibilidades ou capacidades técnicas que permitam a intercepção, a relevância da comunicação interceptada é determinante na medida que o produto que resulta da intercepção tem de ser igualmente processado e avaliado em função da sua importância. São aplicadas numerosas técnicas, como a filtragem de mensagens, para seleccionar as podem ser relevantes e úteis para a intercepção. Por outro lado, os terroristas usam os mais avançados métodos de criptagem, além de terem desenvolvido os "re-mailers" electrónicos anónimos que é um sistema de comandos extremamente difícil de interceptar e que permite controlar grupos em qualquer lugar do mundo, o que causa dificulta mais ainda o trabalho dos serviços de segurança, implicando custos acrescidos através de mais recursos e mais tempo para decriptar as mensagens electrónicas (Malik, 1996; Furnell and Warren, 1999).

Outra forma de intercepção é o sistema de intercepção realizado na aplicação, segundo Branch. O conteúdo interceptado é captado antes ou depois de os pacotes IP iniciarem o seu percurso na rede. Usando o serviço de e-mail como exemplo, em vez de enviar um mandado judicial para a intercepção ao fornecedor dos serviços de *internet*, a agência encarregada da investigação/controlo requisitaria directamente as informações ao operador de e-mail, após uma consulta directa ao seu banco de dados (Jancsewski and Colarik, 2005).

Na prática é muito difícil usar como material probatório as informações interceptadas recorrendo ao Internet Protocol (IP) porque:

- a reunião de vários "inputs" implica um elevado grau de sofisticação na análise por parte da agência de intercepção, o que pode não ser muito fácil de explicar perante um Tribunal, além de que os alvos podem expressar-se em código, ou com dialectos obscuros e ininteligíveis.
- por outro lado, se algum destes "inputs" faltar é fácil para defesa alegar que o conteúdo em falta poderia ser importante para explicar que o acusado é inocente (Privy Council, 2008).

Alguns serviços são (ou podem alegadamente ser) vulneráveis ao "*hacking*" ou ao "*spoofing*".[4] É possível que a defesa alegue que as provas incriminadoras usadas pela acusação foram falsificadas (quer pela autoridade ou agência de segurança ou por um terceiro), tornando quase impossível a acusação refutar estes argumentos.

Enquanto as técnicas de identificação da voz podem (quase de forma infalível) ser usadas para provar que as chamadas de telefone foram de facto feitas pelo alvo a interceptar, é muito mais difícil provar que o *email* ou qualquer outra comunicação sem voz foi efectivamente enviada pelo suposto emissor.

O advento das novas tecnologias vai exigir uma ampla panóplia de novas tecnologias e outras mudanças que representam elevados custos no sistema de intercepções vigente. Além de que para proteger estas técnicas e as capacidades estratégicas possibilitadas por elas, há uma significante parte de intercepções de IP que nunca está disponível para ser usada como prova legal (Privy Council, 2008).

3. O Regime Jurídico das provas e o uso de material interceptado em Portugal

É possível usar *as novas tecnologias na intercepção das comunicações com vista à obtenção de meios de prova que possam ser usados em Tribunal afim de condenar os suspeitos de terrorismo?*

Sob a epígrafe "Das escutas telefónicas", o Código do Processo Penal regulamenta todas as situações em que se interceptem, gravem conversações ou comunicações transmitidas não só por telefone, como por qualquer outro meio técnico, designadamente, correio electrónico ou outras formas de transmissão de dados por via electrónica, bem como intercepção das comunicações entre presentes, mas "não permite estender estas medidas às comunicações realizadas através de meios electrónicos cujo paradigma é a palavra escrita e não a palavra falada (e por isto mesmo não pode haver escutas do fax ou do telegrama)" (Andrade, 1997).

A constituição da República Portuguesa consagra no artigo 34º a inviolabilidade da correspondência e dos outros meios de comunicação, mas admite a ingerência

[4] No contexto de redes de computadores, o IP spoofing é uma técnica de subversão de sistemas informáticos que consiste em mascarar (spoof) pacotes IP utilizando endereços de remetentes falsificados. O pacote deverá ir para o destinatário sem a verificação do remetente — não há validação do endereço IP nem relação deste com o router anterior (que encaminhou o pacote). Assim, é fácil falsificar o endereço de origem através de uma manipulação simples do endereço IP. Assim, vários computadores podem enviar pacotes fazendo-se passar por um determinado endereço de origem.

das autoridades públicas na correspondência e nas telecomunicações, nos específicos casos previstos na lei em matéria de processo criminal. A privação injustificada e sem garantias legais deste direito à privacidade comportaria uma lesão dos direitos individuais incompatível com o seu reconhecimento constitucional, pelo que o legislador entendeu dever proibir qualquer ingerência nas telecomunicações fora dos casos previstos expressamente na lei processual penal – artigo 34 º nº 4 da Constituição da República Portuguesa – reputando de nulas, nos termos do artigo 126º nº 3 do Código do Processo Penal, quaisquer provas obtidas à revelia do quadro legal actualmente desenhado nos artigos 187º[5] e ss do mesmo código e no artigo 6º[6] da Lei 5/2002 de 11 de Janeiro (Cej, 2003).

---

5 O artigo 187º do CPP dispõe sobre a admissibilidade das escutas telefónicas o seguinte:
"1.A intercepção e a gravação de conversações ou comunicações telefónicas só pode ser ordenada ou autorizada, por despacho do juiz, quanto a crimes:
a) Puníveis com pena de prisão superior, no seu máximo, a três anos;
b) Relativos ao tráfico de estupefacientes;
c) Relativos a armas, engenhos, matérias explosivas e análogas;
d) De contrabando; ou
e) De injúrias, de ameaças, de coacção e de intromissão na vida privada, quando cometidos através do telefone, se houver razões para crer que a diligência se revelará de grande interesse para a descoberta da verdade ou para a prova.
2. A ordem ou autorização a que alude o nº 1 do presente artigo pode ser solicitada ao juiz dos lugares onde eventualmente se puder efectivar a conversação ou comunicação telefónica ou da sede da entidade competente para a investigação criminal, tratando-se dos seguintes crimes:
a) Terrorismo, criminalidade violenta ou altamente organizada;
b) Associações criminosas previstas no artigo 287º do Código Penal;
c) Contra a paz e a humanidade previstos no Título II, do Livro II do Código Penal;
d) Contra a segurança do Estado previstos no capítulo I do Título V do Livro II do Código Penal;
e) Produção e tráfico de estupefacientes;
f) Falsificação de moeda ou de títulos de crédito previstos nos artigos 237º, 240º e 244º do Código Penal;
g) Abrangidos por convenção sobre segurança da navegação aérea ou marítima.
3. É proibida a intercepção e a gravação de conversações ou comunicações entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que elas constituem objecto ou elemento de crime".

6 A Lei nº 5/2002 de 11 de Janeiro estabelece as medidas de combate à criminalidade organizada e económico-financeira e aplica-se, entre outros, aos cirmes de terrorismo e de organização terrorista (artigo 1º, b)). Em especial o artigo 6º refere-se, quanto à produção da prova, ao registo de voz e de imagem , e prevê que

Na verdade, o legislador estabelece um regime de autorização e controlo judicial, e um «sistema de catálogo», em que a escuta telefónica é reservada exclusivamente a tipos criminais que pelas suas características tornam tal meio de recolha de prova particularmente apto à investigação ou que, pela gravidade dos interesses em jogo (expressa numa moldura penal abstracta qualificada), podem justificar a adopção de uma medida consensualmente vista como portadora de um elevado potencial de «danosidade social» (Andrade, 1992). Tais normas estão em consonância com o art. 34º, nº 1, da Constituição da República Portuguesa, segundo o qual "O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis", bem como com o disposto no nº 4, do mesmo preceito constitucional, no qual se consagra que "é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação social, salvo os casos previstos na lei em matéria de processo penal"(Costa, 1998).

Do referido normativo da lei fundamental resulta que só em matéria de processo penal é admissível a limitação do direito fundamental do sigilo da correspondência e nas telecomunicações pelas autoridades públicas, corporizando os arts. 187º a 190º do Código do Processo Penal precisamente tal excepção indicada no segmento final do comando constitucional. "O teor particularmente drástico da ameaça representada pela escuta telefónica explica que a lei tenha procurado rodear a sua utilização das maiores cautelas. Daí que a sua admissibilidade esteja dependente do conjunto de exigentes pressupostos materiais e formais previstos nos arts. 187º e segs. da lei processual portuguesa (….)" (Andrade, 1992).

Como se disse, precisamente, porque a ingerência pelas autoridades públicas na correspondência e nas telecomunicações, só é constitucionalmente admissível no quadro de uma previsão legal atinente ao processo penal, uma vez que constitui um limite a um direito fundamental, a escuta telefónica estará sempre sujeita ao princípio da proporcionalidade, subjacente ao art. 18º, nº 2, da Constituição, garantindo que a restrição do direito fundamental em causa, se limite ao estritamente necessário à salvaguarda do interesse constitucional na descoberta de um concreto crime e punição do seu agente.

A lei portuguesa exige expressamente que haja razões para crer que a diligência se revelará de grande interesse para a descoberta da verdade ou para a prova, ou seja, a lei exige não um mero interesse para a descoberta da verdade ou para a

---

"1- é admissível, quando necessário para a investigação de crimes referidos no artigo 1.º, o registo de voz e de imagem, por qualquer meio, sem consentimento do visado.

2 - A produção destes registos depende de prévia autorização ou ordem do juiz, consoante os casos.

3 - São aplicáveis aos registos obtidos, com as necessárias adaptações, as formalidades previstas no artigo 188.º do Código de Processo Penal".

prova, mas que esse interesse seja grande, não sendo legítimo ordenar as escutas telefónicas nos casos em que os resultados probatórios almejados possam, sem dificuldades particulares acrescidas, ser alcançados por meio mais benigno de afronta aos direitos fundamentais (Silva, 2001)

Finalmente, nos termos do artigo 190º do CPP dispõe-se que é aplicável "às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática" o regime previsto para a intercepção e gravação de conversações telefónicas. Ou seja, são aplicáveis às comunicações electrónicas o regime da intercepção de comunicações «por remissão para o regime de intercepção de conversações telefónicas», pelo que se aplicam a estas, nessa medida, os mesmos procedimentos e autorizações judiciais previstas para as "escutas telefónicas" (artigos 187º a 189º do CPP). Atente-se ainda, com particular importância, que a aplicação do regime da intercepção de comunicações telefónicas às comunicações electrónicas abre também a possibilidade de intercepção de comunicações áudio realizadas através de "Voice Over IP" (Venâncio, 2006)

4. O Regime Jurídico das provas e o uso de material interceptado nos Estados Unidos

Os Estados Unidos têm dois sitemas separados para autorizar a intercepção das comunicações:

- O Título III do SAFE, (Omnibus Crime Control and Safe Streets Act of 1968)[7] que se aplica à intercepção de comunicações por cabo, orais pelas Autoridades Legais Nacionais no âmbito das investigações criminais e estabelece o regime geral que norteia esta matéria.

[7] *Title III of the Omnibus Crime Control and Safe Act Streets Act (Wiretap Act) 1968* e que a seguir designamos de *"Titulo III"*. Esta Lei veio definir as regras para obter mandados judiciais para poder efectuar escutas telefónicas nos Estados Unidos. O Título III Foi decretado pelo Congresso, em parte como resposta aos Acórdãos do Supremo Tribunal nos casos Berger v. New York, *388 U.S. 41 (1967) e Katz v. United States, 389 U.S. 347 (1967).* O Congresso procurou com o Título III fixar os requisitos e os procedimentos para obter um mandadoo judicial *"warrant"* permitindo aos funcionários do Governo colocar escutas telefónicas.

- O FISA[8]- que permite a intercepção para fins de protecção da segurança nacional, ou seja, para fins de Intelligência na recolha de material interceptado no estrangeiro ou por agentes de um pais estrangeiro.

O princípio geral proíbe a colocação de escutas electrónicas para interceptar conversas telefónicas, conversas orais (face a face), e comunicações por computador ou outras formas de comunicações electrónicas (18 U.S.C 2511)9 , excepto se as mesmas forem efectuadas dentro do âmbito de uma investigação criminal.

A Lei permite às Autoridades legais, e criminais em especial, o acesso a registos telefónicos e e-mail guardados por terceiros e afins nos termos do Capítulo 121 (18 U.S.C 2701-2709)[10], que em princípio estão ao abrigo da protecção 4ª Emenda Constitucional (Fourth Amendment)[11].

As autoridades de invistigação criminal podem ter acesso a determinadas informações desde que estejam munidas de uma ordem judicial ou de um mandado judicial, ou de uma notificação, desde que as informações visadas estejam relacionadas com investigações criminais, e finalmente, desde que não estejam abrangidas por outras normas restritivas ao abrigo do Título III.

---

8 FISA – Foreign Intelligence Surveillance Act 1978.

9Apesar de se usar vários termos como "*wiretapping, electronic eavesdropping,*", referem-se todos ao mesmo processo de intercepção. Os vários termos usam-se indistintamente. Mas, em termos técnicos, há algumas diferenças:
-"*wiretapping"* limita-se à intercepção mecânica ou electrónica de conversas telefónicas.
- "*eavesdropping"* ou "*electronic surveillance"* refere-se à intercepção mecânica ou electrónica de comunicações em geral.

10 Usamos a sigla U.S.C para designar o Código dos Estados Unidos, United States Code (U.S.C.) onde se encontra compilada toda a legislação geral e tendencialmente permanente do país.

11 O Supremo Tribunal em 1967 decidiu que os requisitos da Quarta Emenda se aplicam igualmente à vigilância electrónica e às buscas físicas através do acórdão *Katz v. United States,* 389 U.S. 347 (1967), no entanto, não decidiu se os requisitos em questão se aplicam à segurança nacional, tendo deixado em aberto a questão da colocação de escutas relacionadas com a "segurança nacional", além de nada estar previsto ao abrigo do Título III , que pudesse trazer luz à questão. Só em 1972 é que o Supremo Tribunal trata da questão deixada em aberto no caso *Katz v. United States, 389 U.S. 347 (1967)* quanto aos limites impostos pela Quarta Emenda em relação às vigilâncias electrónicas conduzidas em nome da segurança nacional, nomeadamente no caso *United States v. United States District Court (Keith), 407 U.S. 297 (1972). Ou seja,* tal como é exigido pela Quarta emenda, o Título III explicitamente requer que o Juiz determine da existência de uma causa provável, de que "um indivíduo está a cometer, cometeu, ou está prestes a cometer um crime" como requisito prévio à concessão de uma autorização para fazer as escutas.

O Título III contém o regime legal a que devem obedecer as ordens judiciais para efectuar vigilâncias (18 U.S.C 2518), nomeadamente devem conter:

-A duração da vigilância

-O âmbito da vigilância

-As conversas que podem ser interceptadas

-As medidas para evitar a intercepção de conversas inocentes

Mas, se assim o entender, por razões de segurança, o tribunal competente pode ordenar, e sob a verificação de determinadas condições, a notificação posterior à diligência de vigilância.

A norma 41 (d) do Federal Rule of Criminal Procedure continha a exigência legal de que, posteriormente à execução do mandado de busca federal, fosse entregue ou deixado uma cópia do mandado e um inventário contendo a descriminação dos objectos que tinham sido apreendidos, além de que o agente encarregue das operações devia avisar o Tribunal competente das operações efectuadas.

Com a entrada em vigor do USA Patriot Act 2001[12], a secção 213 fixa a competência para a notificação posterior à execução do mandado de vigilância, se tiver razões para acreditar que a notificação simultânea à diligência de busca pode ter as consequências adversas às descritas na Secção 2705, ou seja, pode:

(A) pôr em perigo a vida e a integridade fisica de um indivíduo;

(B) pôr-se em fuga impedindo a acusação;

(C) destruir ou falsificar as provas;

(D) intimidar potênciais testemunhas; e

(E) por qualquer outra forma pôr seriamente em perigo uma investigação ou atrasar indevidamente um julgamento".

---

[12] O *"USA Patriot Act 2001"* é o acrónimo para *"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism"*, ou seja, Unir e Fortalecer a América através de Instrumentos Apropriados para Interceptar e Obstruir o Terrorismo. O Patriot Act [Public Law nº 107-56, 115 Stat. 272, (2001)] é parte da resposta do Congresso Americano aos ataques terroristas do 11 de Setembro de 2001 ao World Trade Center e ao Pentágono.

Além da verificação das líneas anteriores, a notificação posterior deve conter as razões que fundamentam o atraso e deve efectuar-se dentro de um "período razoável de tempo."

Na intercepção de comunicações, as ordens judiciais podem aprovar o uso de dispositivos de *"trap e trace"* e dispositivos "*pens registers"*[13] pelo Governo. Porque é ao Governo, ou seja, às autoridades policiais que cabe certificar que o uso do dispositivo produzirá provavelmente informação relevante para a investigação de um crime, seja ele qual for (18 U.S.C 3123).

Podem ser utilizados mandados "*sneak and peek"*, que são mandados que autorizam os agentes policiais a penetrar secretamente no local (quer fisicamente, quer electronicamente), conduzir uma busca, observar, fazer medições, fazer exames, tirar fotografias, copiar documentos, fazer downloads ou copiar ficheiros do computador, ou outras operações similares, e finalmente sair ou deixar o local sem retirar nenhuma prova tangível ou qualquer sinal ou aviso que assinale a sua presença assim como das operações de vigilância e/ou busca efectuadas.

Depois de autorizadas pelo órgão superior do Departamento da Autoridade competente (18 U.S.C 2516), os agentes da autoridade devem obter uma ordem judicial que os autorize a captar ou interceptar secretamente as conversas ligadas a qualquer um dos crimes que consta de um catálogo de crimes denomidado de *"predicate offenses"*[14], nos quais se incluem os crimes de terrorismo.

A Secção 214 do Patriot Act 2001 vem alargar o âmbito de aplicação da utilização dos dispositivos "*Pen Register e Trap and Trace"* previsto ao abrigo do FISA. Ou seja, permite o uso de dispositivos *pen register e trap and trace* nas instalações usadas pelos agentes dos Serviços de Inteligência do Exterior ou dos

---

[13] Estes dispositivos servem para identificar a fonte e o destino de uma chamada telefónica feita por um determinado telefone. São um secreto "*caller id*".

[14] A secção 113 do USA Patriot Act 2001 aumentou a lista de crimes em que a lei pode coagir à obtenção de ordens judiciais para efectuar escutas, passando a incluir mais de 20 crimes federais, por exemplo: -crimes com armas biológicas, -violência em aeroportos internacionais, ameaças com armas nucleares de destruição massiva, -materiais explosivos, a recepção de treinos militares de terroristas, ataques terroristas contra locais de trânsito em massa, incêndio criminoso em jurisdição marítima ou territorial dos Estados Unidos, tortura, ataques com armas de fogo em instalações federais, assassinato de funcionários federais, assassinato de certos funcionários estrangeiros, conspiração praticar violência no estrangeiro, hospedar terroristas, assaltar um membro da tripulação de um avião com uma arma perigosas, certos crimes com armas a bordo de aviões, roubo de identidade agravado, lavagem de dinheiro com elevados montantes transaccionados em múltiplas pequenas transacções.

presumíveis envolvidos em actividades clandestinas e terroristas. A Autoridade requerente apenas deve certificar que a ordem judicial pedida se destina a fazer parte de uma investigação para proteger os Estados Unidos contra o terrorismo internacional e contra as actividades da inteligência clandestina estrangeira.

Além destes dispositivos, o FBI *(Federal Bureau of Investigation)*[15] pode emitir Cartas para a Segurança Nacional *(National Security Letter - NSL)* (Doyle, 2006), que são cartas em que o FBI requer que o seu destinatário forneça registos confidenciais de terceiros, nomeadamente listagens de dados referentes a utilizadores dos serviços de bibliotecas, livrarias, de empresas rent-a-car , de bancos, etc. As ordens 215 contém uma obrigação de não revelar o seu conteúdo, ou seja, impende sobre o seu destinatário a proibição de revelar que o FBI procura as coisas ou items tangíveis descritos na ordem. A única excepção a esta *"gag order"* ou ordem de guardar silêncio ou sigilo é a de que os destinatários podem revelar o conteúdo da ordem às pessoas cuja colaboração seja estritamente necessária para a executar nos termos exigido pelo FBI. Não está previsto um recurso judicial ao Tribunal FISA da própria ordem 215, ou seja, um processo judicial que permita ao destinatário recorrer do dever de silêncio, recorrer da "gag order"no sentido de o modificar ou de o extinguir., porque administrativamente já estão definitvamente fixados os termos da ordem. Portanto, o destinatário das cartas não pode recusar-se a revelar as informações requeridas alegando a violação do direito à privacidade e à confidencialidade dos seus clientes ou usuários.

A regulação legal das NSL é ampla (Doyle, 2006), e a sua utilização está presentemente prevista ao abrigo das seguintes leis:

- A Lei da Privacidade das Comunicações Electrónicas, *(the Electronic Communications Privacy Act)* para obter registos de comunicações telefónicas e electrónicas;
- A Lei da Privacidade Financeira *(the Financial Right to Privacy Act)* para obter registos financeiros;
- A Lei sobre Crédito *(the Fair Credit Reporting Act)* para obter registos sobre créditos.

---

15 O FBI (Fedeal Bureau of Investigation) norte-americano dispõe de um sistema de vigilância da Internet, denominado *Carnivore*, instalado directamente nas redes dos "*Internet Service Providers",* que permite gravar todo o tráfego de *sites* visitados e dos *e-mails* recebidos e enviados por pessoas ou entidades suspeitas de envolvimento em práticas criminosas, podendo também reconstruir e adulterar Webpages e captar comunicações de voz via Internet. Em princípio, o sistema só capta comunicações com base em autorização judicial, sendo os seus objectivos a investigação criminal e a segurança nacional dos EUA . Ver em http://epic.org/privacy/carnivore/foia_documents.html

Nos termos da secção 215, a uso de NSL ou de dispositivos de "pen register/trap and trace"(Kerr, 2003), não implicam que a autoridade requerente demonstre haver um nexo entre o "item" procurado e o agente ou poder estrangeiro clandestino. O item procurado, ou a informação solicitada não tem de estar relacionado com um agente estrangeiro identificado ou com uma autoridade estrangeira clandestina, a mera indicação de que fazem parte de uma investigação que visa proteger os Estados Unidos do terrorismo internacional ou que podem estar relacionados com actividades clandestinas dos serviços de inteligência exterior, é suficiente para que a sua realização seja autorizada. O Assistente do Agente Especial (the Assistant Special Agents) responsável pelos gabinetes do FBI pode solicitar o registo de todos os dados que entenda.

Por outro lado, a secção 210 do Patriot Act 2001 visa permitir que as autoridades legais estejam na pista de um suspeito através da determinação da sua verdadeira identificação, autorizando (18 U.S.C. 2703(c)) a notificação de fornecedores para que informem de todos os registos de transacções, dados sobre os serviços adquiridos, datas e tipos de negócios efectuados, incluindo a informação relativa à forma de pagamento, informações sobre o cartão de crédito ou sobre outros meios de pagamento.

O Título III exige um mandado de busca para obrigar os fornecedores do serviço a revelar o conteúdo de e-mails fechados. Mas a secção 220 do USA Patriot Act 2001 abrevia os requisitos necessários para obter um mandado, prescindindo da autorização dos juízes onde o Internet Service Provider (ISP) está colocado, ultrapassando a barreira da mudança de jurisdição. A norma 41 do *Federal Rules of Criminal* exigia que o mandado fosse obtido dentro do Distrito onde a propriedade ou a instalação estava localizada, mas a entrada em vigor da secção 220 passa a autorizar o Tribunal, com jurisdição sobre a investigação, a emitir um mandado directamente aplicável, sem necessitar da intervenção dos Juizes do Distrito onde o ISP está localizado, seguindo informação nos moldes da natureza trans-jurisdicional da Internet.

A Secção 209 trata os *voice mail* como os *e-mail.* Assim, os agentes federais do FBI podem ter acesso aos voice mail com um mandado judicial, sem ter de recorrer ao regime mais restrito do Titulo III que se aplica a comunicações telefónicas ao vivo, no entanto as empresas de telecomunicações que operam por cabo estão proibidas de revelar a informação de identificação dos seus clientes, sem o consentimento deste ao abrigo da Lei das Comunicações *(the Communications Act, 47 U.S.C. 551*), o que clarifica que uma empresa que opera por cabo, e que fornece serviços de comunicações está sujeita às normas do Título III (47 U.S.C. 551 et. Seg.).

Mas o âmbito de aplicação da secção 211 introduziu a seguinte alteração: os fornecedores de comunicações telefónicas e electrónicas solicitadas podem ser

obrigadas a prestar às autoridades judiciais informações sobre a identificação dos seus clientes sem que possam previamente ou em simultaneo informar-los de que vão transmitir as informações requeridas (18 U.S.C. 2705 (b)). Esta alteração não se aplica aos clientes que subscrevem registos de vídeo por cabo que continuam a ser tratados ao abrigo da protecção da Lei das Comunicações. *(the Communications Act, 47 U.S.C. 551)*

As secções 201 e 202 aumentam o âmbito dos poderes para interceptar comunicações electrónicas, por cabo ou orais, relacionadas com o terrorismo e com os crimes de burla e de abuso cometidos através de computadores.

A secção 201 e a secção 202 acrescentam outros crimes ao catálogo previsto no Título III do SAFE[16]:

1º - o cibercrime (fraudes e abusos fraudulentos efectuados com computadores)

2º - vários crimes de terrorismo:

- Crimes com armas químicas (18 U.S.C. 229)
- Crimes com uso de armas de destruição massiva (18 U.S.C. 2332ª)
- Crimes de terrorismo violento que transcendem as fronteiras nacionais (18 U.S.C 2332b)
- Transacções financeiras que envolvam países que apoiam o terrorismo (18 U.S.C. 2332d)
- Apoio material aos terroristas (18 U.S.C. 2339ª)
- Apoio ou suporte material a organizações terroristas, 18 U.S.C. 2339B

Quanto ao cybercrime, (18 U.S.C 1030), a secção 217 (2) altera a lei afim de permitir que as autoridades judiciais interceptem as comunicações do intruso num sistema de computador protegido (Smith, 2003).

A Secção 217(1) do Patriot Act adiciona às definições sob o 18 U.S.C. 2510 os termos:

---

16 O Titulo III da Lei do Controlo dos Crimes e da Manutenção da Segurança nas Ruas de 1968, (*the Omnibus Crime Control and Safe Streets Act of 1968, SAFE),* prevê um processo judicialmente controlado sob o qual, ao abrigo da lei, pode-se interceptar comunicações por cabo, orais e electrónicas. Este processo só pode ser usado quando houver alguma conexão com investigações de crimes graves, e catalogados legalmente como tais.

(1) "*Computador protegido"* : é um sistema usado pelo Governo Federal,[17] por uma instituição financeira, ou usado para comunicações inter-estaduais ou para comércio internacional (18 U.S.C 2511 (2) (i))

(2) *"Intruso dos computadores"* - é a pessoa que acede a um computador protegido sem autorização e que portanto não tem uma expectativa razoável de privacidade em qualquer comunicação transmitida através, ou, de um computador protegido.

A secção 219 prevê e organiza a única jurisdição para aprovação de mandados de busca nos crimes de terrorismo. "A norma 41(a) do Código Federal de Processo criminal (*Federal Rules of Criminal Procedure)* requer que o mandado de busca seja obtido junto do Tribunal do distrito judicial onde a propriedade ou instalação sujeita a revista está localisada" (Chemerinsky, (2004).

O USA *Patriot Act* 2001 alterou a Lei FISA para permitir uma colaboração mais estreita entre os investigadores criminais e os Serviços Secretos, em particular no que diz respeito aos crimes de terrorismo internacional, afim de conseguir uma maior aproximação e partilha de informações eliminando os limites impostos pela lei do FISA, deixando de ser exigido o requisito do "fim a que se destina a recolha de informações"(Doyle, 2001).

Em substituição da certificação FISA, a secção 218 requer apenas que o pedido para efectuar vigilâncias cumpra o requisito da certificação de que as vigilâncias visam prosseguir um fim significativo para a investigação (50 U.S.C. 1804(a)(7)(B), ou seja, prescinde da indicação prévia do fim a que se destina a informação, podendo a mesma ser utilizada fora do âmbito relativo da sua colheita (Poole, 2001).

A secção 206 prevê *a* vigilância *"roving"*[18] ao abrigo do *FISA, Foreign Intelligence Surveillance Act of 1978.*Ou seja, o Tribunal do FISA pode ordenar a terceiros, que forneçam informações ou prestem assistência e colaboração aos agentes de investigação, a fim de permitir a instalação de gravadores ou a recolha de informações relevantes para os serviços secretos. Estes "terceiros" são pessoas com determinadas actividades profissionais (informáticos, electricistas, serralheiros, etc...), senhorios, funcionários de lojas e outros, que devem ser identificadas na ordem judicial que autoriza a vigilância, porque a secção 206 permite:

---

17 O diploma legal que regula o e-governo "*the E-Government Act (P.L. 107-347)* fixa os requisitos legais que as agências governamentais devem seguir para garantir a sua privacidade no uso de informações pessoais identificáveis no sistema de informação governamental e estabelece manuais para a politica de privacidade dos Web sites federais.

18 A vigilância "roving" é a vigilância móvel, que vai atrás do alvo

a) Alargar a competência jurisdicional para instalar os dispositivos de intercepção de comunicações, e seguir o alvo da investigação onde quer que se encontre, mesmo que não seja possível indicar na ordem do Tribunal o destinatário da mesma.

b) Suprir o problema da identificação do alvo, na medida em que este pode a qualquer momento mudar de local, de número de telemóvel, de telefone, de conta de Internet, de IP.

Apesar do alvo sob vigilância electrónica dever estar identificado ou descrito na ordem judicial nos termos da lei em vigor, o tribunal pode emitir uma ordem genérica que pode ser apresentada a qualquer outra pessoa, independentemente da sua profissão exigindo a sua assistência para assegurar que a vigilância seja levada a cabo logo que seja tecnicamente possível. No fundo o que a secção 206 prevê são "os mandados ou ordens judiciais em branco" e a aplicação do mandado em várias jurisdições, o que levanta problemas com o princípio *ne bis in idem ou do double jeopardy.*

5. Conclusões

A intercepção das comunicações quer celulares, quer por via electrónica, de computador a computador, pela Internet ou outras redes nacionais e internacionais, é um meio insuprível na luta contra o terrorismo, e contra as outras as formas mais graves de criminalidade, porque o ciberespaço é o "*virtual criminal field"*,ou seja, o meio privilegiado da circulação da informação criminosa.

Por outro lado, é inegável que o crescimento da confiança e da fiabilidade relativamente à internet reside no estabelecimento de meios de comunicação seguros, sendo que é do interesses dos usuários, dos fornecedores de serviços IP e de toda a comunidade internacional da Internet, que a vigilância passe a ser concebida como um mecanismo de e-segurança (Watney,2007).

A internet é uma ferramenta muito poderosa e a vigilância do Estado, quer das autoridades de investigação criminal, quer da *intelligence* deve ser uma garantia e não uma fonte de violação dos direitos humanos porque as garantias de segurança não podem ser os instrumentos de destruição dos valores da internet (Poore, 2002).

Ao compararmos o regime legal das "escutas" português com o modelo americano podemos concluir que estão nos antípodas um do outro, e imediatamente distinguimos a realidade americana da nossa, mas a questão que se coloca é: - será que o nosso sistema permite obter efectivas condenações dos criminosos da rede?

Por outro lado, há ainda outro problema: -será que só se conseguem efectivas condenações dos criminosos se se violarem os direitos, liberdades ou garantias fundamentais do cidadão pelo Estado?

Não estamos já a falar do caso do "envelope 9" bastante simples (nem sequer nos ocupa a questão controversa da legalidade da busca e apreensão), mas da intercepção em tempo real de comunicações estalecidas entre várias pessoas situadas em vários países, ou mesmo vários continentes, e que simultaneamente se organizam numa dinâmica de grupo, planeando um ou vários atentados terroristas, vizando alvos diferentes, mais ou menos graves, sem que para isso tenham de dispôr de fundos ou recursos financeiros apreciáveis.

Concluimos que em relação às especificidades das "escutas" ou do "eavesdropping" da transmissão de dados (texto, som ou imagem) entre computadores ou à recolha de dados de tráfego, em particular do correio electrónico (e-mail), sem falar no voIP, questão que aqui nos motiva, o nosso Código do Processo Penal ficou aquém do que seria necessário.

Com isto não queremos dizer que devíamos adoptar o sistema americano, mas tão só que o nosso regime legal de "escutas" se devia adequar às novas tecnologias, preservando os direitos fundamentais dos cidadãos.

Na verdade, o uso de material interceptado obtido através de escutas ou de outros dispositivos de vigilância em tribunal é uma ferramenta que envolve vários riscos.

O uso do material interceptado implica desde logo um leque de riscos operacionais e organizacionais, que interferem directamente na capacidade para recolher, tratar, filtrar, decifrar, descodificar, transmitir em tempo útil as informações por parte das autoridades de investigação criminal ou dos serviços secretos *(intelligence)* orientadas para a defesa e manutenção da defesa nacional. Não podemos esquecer que os alvos que ameaçam a segurança nacional (incluindo terroristas, traficantes de armas e espiões) têm acesso às mesmas comunicações do que os criminosos em geral, ou seja, as capacidades técnicas usadas para a escuta de comunicações num e no outro tipo de crimes podem ser as mesmas, o que significa que os prejuízos que resultam da revelação das técnicas usadas nas intercepções não se limitam às investigações criminais, prolongando-se ao âmbito da actividade dos serviços secretos. Qualquer divulgação ou revelação das capacidades da intercepção pode ter um profundo impacto na segurança nacional, encorajando um amplo conjunto de alvos (não só criminosos, mas também terroristas e outros individuos muito inteligentes) a mudar o seu comportamento, dificultando as investigações no futuro.

Quanto aos riscos de carácter legal, devemos desde logo considerar que o regime jurídico aplicável às "escutas" deve ser compatível com a Convenção Europeia dos Direitos do Homem (CEDH). Em particular, deve garantir os direitos que o acusado tem a um julgamento justo, nos termos do artigo 6º, e simultaneamente o direito que qualquer pessoa tem à intimidade da vida privada, nos termos do artigo 8º. Apesar da acusação poder invocar o sigilo, e o interesse público, nomeadamente razões de segurança do Estado, para não divulgar os métodos e as técnicas sensíveis que usa na recolha de informações, este não é um direito absoluto, ou seja, em todo o caso o Juiz terá de garantir ao acusado o direito a um julgamento justo.

Bibliografia

Branch, P (2003) Lawful Interception of the Internet, *Australian Journal of Emerging Technologies and Society*, Vol. 1, No. 1.

Branch, P., Pavlicic, A. and Armitage, G. (2004) *Using MAC Addresses in the Lawful Interception of IP Traffic,* Australian Telecommunications Networks & Applications Conference 2004, Sydney, Australia, December 8-10, from http://caia.swin.edu.au/pubs/ATNAC04/branch-pavlicic-armitage-ATNAC2004.pdf

Brown, Tina (2005) Death by Error, *The Washington Post* from http://www.washingtonpost.com/wp-dyn/content/article/2005/05/18/AR2005051802083.html

Capeller, W. (2001) *Not such a Neat Net: Some Comments on Virtual Criminality*, Social and Legal Sttudies, 10; pp. 229-249

Centro de Estudos Judiciários (2003) *Contributos para a reflexão sobre o Sistema Penal Português*, Lisboa, Centro de Estudos Judiciários

Chemerinsky, E. (2004) *Losing Liberties, Applying a Foreign Intelligence Model to Domestic Law Enforcement*, 51 UCLA L. Rev. 1619 From http://eprints.law.duke.edu/ archive/00001136/01/ 51_UCLA_L._Rev._1619_(2003-2004).pdf

Comer, D. E (2000) *Internetworking with TCP/IP*, Volume 1: Principles, Protocols, and Architectures, Fourth Edition, Prentice Hall PTR, Upper Saddle River, NJ

Costa Andrade, M. (1992) *Sobre as Proibições de Prova em Processo Penal*, Coimbra, Coimbra Editora, pp. 272, 275, 281, 283 e 285.

Costa, F.(1998) *Direito Penal da Comunicação*, Coimbra, Coimbra Editora, pp. 63 e ss., e 143 .

Davis, L. E (2002) *Organizing for Homeland Security*, from http://www.rand.org/pubs/issue_papers/IP220/index2.html

Doyle, C. (2001) *Best Intelligence and Law Enforcement cooperation: Countering Transnational Threats to the U.S*, CRS REP. Nº RL30252 from http://www. faz.org

Doyle,C. (2002) *Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations: Background and Proposed Adjustments*, CRS Report RL32880 from

www.fas.org/sgp/crs/natsec/RS22122.pdf

Doyle, C. (2006) *National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments*, RS22406, March 21, 2006, from http://www.fas.org/sgp/crs/intel/RS22406.pdf

Furnell, S.M and Warren, M.J. (1999) *Computer Haching and Cyber Terrorism: The Real Threats in the New Millennium? Computers & Security*, 18; Elsevier Science Ltd. pp.28-34

Garcia, F.P. (2008) *O que há de novo na "intelligence"?* from www.jornaldefesa.com.pt/conteudos/view_txt.asp?id=560 - 42k

Grabosky, P and Smith, R. (2001) Digital Crime in the Twenty-First Century, *Journal of Information Ethics*, 10; pp. 8-26

Jancsewski, L. and Colarik, A. (2005) *Managerial Guide for Handling Cyber-Terrorism and Information Warfare*, USA: Ida Group Publishing, pp.223–225.

Kerr, O. S. (2003), *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't* . Northwestern University Law Review, Vol. 97, from http://ssrn.com/=317501

Malik, I. (1996) *Computer Hacking: detection and protection*. Sigma Press, UK, ISBN 1-85058-538-5

Poole, P.S (2001) *Inside America's Secret Court: the Foreign Intelligence Surveillance Court*, from http://www.digits.com.

Poore, R.S. (2002) Computer forensics and privacy: at what price do we police the internet, in R. *Herold (Ed). The Privacy Papers Managing Technology, Consumer, Employee and Legislative Actions*, USA: CRC Press LLC, pp.33–34.

Privy Council (2008) *Review of Intercept as Evidence Report to the Prime Minister and the Home Secretary*, from www.tsoshop.co.uk

Ramasastry A.(2006) *The National Security Letter Provision of the USA Patriot Act: Why It Ought to Be Amended during the Reauthorization Debates* from http://writ.news.findlaw.com/ramasastry/20060109.html#continue

Silva, G.M. (2001) *Direito Processo Penal*, Tomo II, 2ª Edição, Lisboa, Verbo Editora, pp. 201-202

Smith, M. S. (2003) Internet Privacy: Overview and Pending Legislation, CRS, REP. Nº RL 31408 disponível em http://www. faz.org

Veiga, P. (2004) *Tecnologias e sistemas de informação, redes e segurança*, Porto, SPI – Sociedade Portuguesa de Inovação, Consultadoria Empresarial e Fomento da Inovação, S.A, ISBN 972-8589-39-5

Venâncio, P. D (2006) *Breve Introdução da Questão da Investigação e Meios de Prova na Criminalidade Informática*: 27, from http://www.verbojuridico.net/

Vitorino, A. (2007) "aqui tão perto", *Diário de Notícias* from http://dn.sapo.pt/2007/04/20/opiniao/aqui_perto.html

Zanini, M. and Edwards, J.A. (2001) The Networking of Terror in the Information Age in Arquilla, J. and Ronfeldt, D. (orgs.),*Networks and Netwars: The Future of Terror, Crime and Militancy*,Santa Monica, CA: RAND, 2001, MR-1382-OSD, p. 43.

Wall, D.S (2001) Maintaining order and law on the internet. In Wall, D. (Ed) *Crime and the Internet*, London: Routledge

Watney, M. (2007) 'State surveillance of the internet: human rights infringement or e-security mechanism?' Int. J. of Electronic Security and Digital Forensics, Vol. 1, No. 1, pp.42–54.

Wisniewski, D. J (2001) "Homeland Security: Under Organized and Over Involved", National Defense University, Nacional War College, Disponível em http://www. stinet.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA4451