Documento de trabalho 2a

2 A finalidade das medidas de vigilância

2.1 Generalidades

Uma vez que num Estado de Direito a violação do direito fundamental ao respeito pela vida privada apenas é admissível se for considerada necessária, importa de antemão esclarecer quais os fins que se afiguram legítimos para justificar uma tal violação. Poderão invocar-se, essencialmente, razões como a aplicação da lei (ver ponto 2.2), a garantia da ordem e da segurança interna (ver ponto 2.3), bem como a garantia da segurança externa (ver ponto 2.4).

Numa segunda fase, cumpre especificar mediante leis nacionais (já que a admissibilidade e o alcance das medidas de vigilância são da competência exclusiva dos Estados-Membros[1]) as condições em que é permitido efectuar medidas de controlo e/ou interceptar comunicações. Os cidadãos têm de poder prever em que condições este tipo de intromissões na vida privada podem ocorrer legalmente. Por esse motivo, não é admissível proceder a uma escuta de todas as comunicações com o objectivo de uma posterior utilização do seu conteúdo para outros fins que não os estabelecidos na lei.

Tal aplica-se, pelo menos, nos casos em que as escutas visam comunicações que apresentam alguma ligação com o território nacional, ou seja, que se encontram indubitavelmente abrangidas pela protecção jurídica do Estado. Quando as medidas de vigilância visam processos que se encontram fora do núcleo protegido e quando se coloca, por conseguinte, a questão do âmbito de aplicação territorial dos direitos fundamentais não existe, na maioria dos casos, qualquer tipo de controlo. Uma vez que os eleitores não se insurgem contra esta realidade, ela também não tem suscitado o interesse dos órgãos de controlo parlamentar nacionais. Trata-se de uma zona cinzenta do direito que é fomentada pelo velho provérbio «Quem cala, consente». Neste domínio, os limites são traçados não tanto pelo direito, mas antes por aquilo que é tecnicamente viável, considerando os meios disponíveis.

2.2 As medidas de vigilância ao serviço da aplicação da lei e da prevenção da criminalidade

2.2.1 As regulamentações nacionais relativas à admissibilidade e ao alcance das medidas

Qualquer ordem jurídica nacional dispõe de legislação na qual estão previstas determinadas medidas de vigilância, passíveis de serem aplicadas pela polícia ou por outras autoridades de segurança pública para fins relacionados com a aplicação da lei. Quando autorizada, a violação do direito fundamental à vida privada é, geralmente, bastante radical, uma vez que é mesmo permitido violar o segredo das telecomunicações. Aos olhos dos legisladores nacionais, este tipo de violação afigura-se legítima na medida em que só é autorizada em caso de suspeita suficiente de crime (por vezes, especialmente qualificado, ou seja, de maior gravidade) e que, nessas circunstâncias, o interesse da sociedade na aplicação efectiva de sanções e, por conseguinte, na

[1] Cf. ponto 2.2.2.1 infra.

produção de provas prevalece sobre a protecção da vida privada do indivíduo. Nesses casos, as medidas de vigilância são aplicadas individualmente, ficando salvaguardada a protecção das pessoas não visadas. Para não dar azo a estados policiais, o legislador limitou os poderes de intervenção das autoridades de segurança pública, sujeitando-os, em cada caso concreto, à autorização de um juiz ou de um grémio competente. Não são concedidas autorizações gerais, pelo que fica excluída a possibilidade de, legalmente, realizar escutas integrais.

2.2.2 A cooperação entre os Estados-Membros com vista à execução técnica das medidas de vigilância ao serviço da aplicação da lei

2.2.2.1 A limitação das competências da UE a regulamentações técnicas

A opinião pública manifesta-se frequentemente preocupada com a possibilidade de a União Europeia estar a desenvolver um projecto de vigilância supranacional das telecomunicações no âmbito da cooperação no domínio da justiça e dos assuntos internos. Porém, este tipo de preocupações não tem qualquer fundamento. Ninguém está a preparar um sistema de escutas e de vigilância sistemática na UE[1].

Neste contexto, importa esclarecer que a regulamentação da questão da admissibilidade de medidas de escuta se inscreve nas competências nacionais dos Estados-Membros. Em conformidade com o princípio da delegação limitada de poderes, a UE só pode intervir nos domínios em que os Tratados lhe confiram competências. O título VI do TUE "Disposições relativas à cooperação policial e judiciária em matéria penal" não prevê, no entanto, quaisquer competências nesse sentido. No domínio da cooperação policial (artigo 30º, nº1) só está prevista uma acção em comum no tocante aos aspectos operacionais, ou seja, aqueles relacionados com os moldes em que se processa a actividade policial. No domínio da cooperação judiciária, a alínea c) do artigo 31º prevê, em termos muito gerais, que a acção em comum tem por objectivo «assegurar a compatibilidade das normas aplicáveis nos Estados-Membros», mas apenas «na medida do necessário para melhorar a referida cooperação», ou seja, visa sobretudo regulamentações específicas de cooperação. Por último, a «aproximação das disposições de direito penal dos Estados-Membros», nos termos do disposto no último travessão do artigo 29º, limita-se ao estabelecimento de regras mínimas quanto aos elementos constitutivos das infracções penais (alínea e) do artigo 31º). Em suma, pode dizer-se que a competência para regulamentar a questão relativa às condições em que é admissível efectuar medidas de vigilância continua a estar reservada ao direito nacional. O relator não tem conhecimento de que algum Estado-Membro tenha alguma vez envidado esforços no sentido de alterar esta situação.

Por conseguinte, a cooperação entre os Estados-Membros ao abrigo dos Tratados da UE só poderá realizar-se no tocante à execução das medidas de vigilância consideradas admissíveis à luz do direito nacional, ou seja a um nível inferior. Nos casos em que a intercepção das telecomunicações é permitida pela ordem jurídica nacional, está previsto que o Estado-Membro interessado possa recorrer à ajuda dos outros Estados-Membros para fins de execução técnica das medidas de vigilância. Se a pretendida simplificação técnica, que certamente contribuirá para uma maior eficácia das escutas transfronteiras no âmbito do procedimento penal, sobretudo no que respeita à criminalidade organizada, deverá ou não ser considerada positiva, dependerá em larga medida da confiança de cada um no seu próprio Estado de direito. Em todo o caso,

[1] Cf. resposta de Karl Schlögel, Ministro dos Assuntos Internos austríaco, à pergunta oral dos deputados Barmüller, Kier et al nº 4317/J, de 16 de Abril de 1998.
http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/AB04014_.html.

convém salientar uma vez mais o seguinte: mesmo que a uniformização técnica permita simplificar, em termos técnicos, a intercepção de comunicações transfronteiras e atendendo a que não será certamente possível evitar abusos num ou noutro caso, tal não afecta de forma alguma as condições em que é admissível realizar escutas, já que esta questão é regulamentada pela legislação nacional.

2.2.2.2. As iniciativas de carácter transnacional no domínio da intercepção de comunicações: definições e explicações

Os diferentes grupos de trabalho constituídos no domínio da intercepção de comunicações têm gerado alguns equívocos, inclusive na imprensa especializada. Atendendo a que no debate realizado em comissão também se verificaram algumas inseguranças nesta matéria, o relator considera pertinente explicar alguns dos conceitos empregados.

ILETS (International Law Enforcement Telecommunications Seminar)

Os seminários ILET surgiram na sequência de uma iniciativa do FBI. Em 1993, o FBI convidou as autoridades responsáveis pela aplicação da lei e os serviços de informações de países amigos a assistir a uma conferência subordinada ao tema da intercepção de telecomunicações, em Quantico. Nessa conferência participaram grande parte dos actuais Estados-Membros da UE, bem como a Austrália e o Canadá[1]. Desde então, têm-se realizado encontros periódicos para debater os requisitos necessários a uma vigilância eficaz das comunicações internacionais.

Por ocasião de uma reunião realizada em Bona, em 1994, os membros do ILETS aprovaram um documento que estabelecia orientações políticas e cujo anexo incluía uma lista de "international user requirements" (IUR 1.0 ou IUR 95). Esta lista continha os requisitos que deveriam ser impostos aos vários operadores de telecomunicações, a fim de simplificar as operações de intercepção. Embora não oficialmente, estas IUR 1.0 serviram de base à resolução do Conselho, de 17 de Janeiro de 1995, relativa à intercepção legal das telecomunicações (ver ponto 2.2.2.3.1 infra). Posteriormente, realizaram-se ainda outras reuniões de peritos para debater as IUR e a sua possível aplicação e adaptação aos modernos sistemas de telecomunicações.

Grupo TREVI

Antes da entrada em vigor do Tratado de Maastricht (que, com o TUE, veio introduzir as disposições relativas à cooperação no domínio da justiça e dos assuntos internos), era no quadro do grupo TREVI que os ministros da Justiça e dos Assuntos Internos dos Estados-Membros da Comunidade Europeia debatiam as questões de segurança interna. Entretanto, o grupo TREVI deixou de estar activo, já que os temas debatidos no seu seio transitaram para os grupos de trabalho específicos do Conselho (GTC).

Para efeitos da presente análise, importa sobretudo referir dois GTC: o GTC "Auxílio judiciário mútuo em matéria penal" que, no âmbito da cooperação no domínio da justiça e dos assuntos internos, estudou a convenção relativa ao auxílio judiciário mútuo em matéria penal e o grupo de trabalho do Conselho "Cooperação policial" que tratou das questões relacionadas com a intercepção legal das telecomunicações, incluindo a intercepção dos novos sistemas de comunicação (telemóveis, Internet, correio electrónico). Este último também tratou da aproximação das legislações no que respeita aos requisitos impostos pelos serviços de controlo legalmente autorizados aos operadores de rede e prestadores de serviços.

---

[1] Sobre o conteúdo, cf. resposta escrita do Ministro dos Assuntos Internos austríaco, Karl Schlögel, à pergunta parlamentar do deputado Van der Bellen ; 4014/AB XX. GP.
http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/AB04014_.html.

"ENFOPOL"

Contrariamente ao que muitos autores pensam, o "ENFOPOL" não é um grupo de trabalho ou uma organização, mas sim uma abreviatura que designa os documentos de trabalho em matéria de acções penais e policiais, inclusive da autoria do GTC "Cooperação policial"[1]. O ENFOPOL não figura no título dos respectivos documentos, mas estes são classificados segundo o mesmo.

EUROPOL

Por «Europol» entende-se o Serviço Europeu de Polícia, com sede em Haia, instituído pela Convenção Europol.[2] Actualmente, as funções da Europol limitam-se ao intercâmbio de dados entre os Estados-Membros, à realização de estudos de criminologia e à prestação de consultoria em resposta a pedidos dos Estados-Membros. Não obstante estar previsto na alínea a) do n.º 2 do artigo 30º que o Conselho irá adoptar, até 1 de Maio de 2004, as medidas que permitam a realização de "acções operacionais de equipas conjuntas em que participem representantes da Europol com funções de apoio", a Europol ainda não possui, até à data, quaisquer competências operacionais.[3] Assim sendo, a Europol não pode ser considerada como uma entidade policial no sentido técnico, mas antes como uma base de dados europeia ao serviço da aplicação da lei. A Europol não está, por isso, habilitada a efectuar operações de intercepção.

2.2.2.3. Trabalhos no domínio da intercepção das telecomunicações no quadro da UE

Em matéria de intercepção das telecomunicações, apenas foram adoptados, até à data, dois actos jurídicos comunitários: a resolução do Conselho, de 17 de Janeiro de 1995, relativa à intercepção legal de telecomunicações, cujo teor deveria ter-se estendido a países terceiros mediante a celebração de um memorando nesse sentido e relativamente à qual estava também prevista uma proposta de actualização (ambos foram preparados em documentos ENFOPOL), e a convenção relativa ao auxílio judiciário mútuo em matéria penal.

2.2.2.3.1 Resolução do Conselho, de 17 de Janeiro de 1995, relativa à intercepção legal de telecomunicações[4].

Ao que parece, a resolução do Conselho, de 17 de Janeiro de 1995, relativa à intercepção legal de telecomunicações será fruto da cooperação entre os peritos no âmbito dos seminários ILET (ver ponto 2.2.2.2 supra) e corresponde, essencialmente, aos IUR (international user requirements) elaborados nesses mesmos seminários.

A resolução visa alcançar que em todos os Estados-Membros sejam criadas as condições técnicas necessárias para que, no exercício dos seus poderes no plano nacional, as autoridades competentes possam efectivamente ter acesso aos dados, ou seja, que possam exercer, na prática, as competências que lhe foram atribuídas ao abrigo do direito nacional.

---

[1] Cf. resposta oral do Ministro dos Assuntos Internos austríaco, Karl Schlögel, à pergunta parlamentar do deputado Van der Bellen; 4739/AB XX. GP http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/040/AB04014_.html, bem como o relatório Campbell :ILETS, a mão invisível por detrás do ENFOPOL 98, http://heise.de/tp/deutsch/special/enfo/6396/1.html.

[2] Acto do Conselho, de 26 de Julho de 1995, que estatui a Convenção elaborada com base no artigo K.3 do Tratado da União que cria um Serviço Europeu de Polícia (Convenção Europol), JO C 319 de 27 de Novembro de 1995, p. 1.

[3] Nem a recomendação do Conselho de 30 de Novembro de 2000 aos Estados-Membros, relativa ao apoio da Europol às equipas de investigação conjuntas criadas pelos Estados-Membros (JO C 357 de 13 de Dezembro de 2000, p. 7) veio alterar esta situação, visto que também só trata das questões da recolha, do tratamento e da transmissão de informações.

[4] JO C 329 de 4 de Novembro de 1996.

Para este efeito, a resolução inclui um anexo que assume «requisitos» bastante pormenorizados dos Estados-Membros, relativamente aos quais o Conselho «toma nota» de que «representam uma síntese importante das necessidades das autoridades competentes na execução técnica da intercepção legal, designadamente nos modernos sistemas de telecomunicações». Estes requisitos incluem, por exemplo, o acesso, em tempo real, a dados associados à chamada (2) ou a possibilidade de os operadores de rede transmitirem as comunicações interceptadas ao serviço de controlo (3.4) Na sua resolução, o Conselho considera que «na definição e execução de medidas [...] devem ser tidos em conta os requisitos» e insta os Estados-Membros e os ministros responsáveis «a cooperar [...] na aplicação dos requisitos relativos aos operadores de rede e aos prestadores de serviços».

Neste contexto, cumpre assinalar que o tipo de acto jurídico escolhido, isto é, a resolução, não assume qualquer carácter vinculativo, ou seja, dela não resultam direitos nem obrigações para os Estados-Membros. A agitação gerada em torno desta resolução e dos documentos associados à mesma não se deveu tanto ao seu conteúdo, mas antes às condições em que foram elaborados.

2.2.2.3.2 Memorando de Entendimento

No subsequente Memorando de Entendimento[1] convidavam-se os países terceiros a transpor os requisitos técnicos contidos na resolução do Conselho de 17 de Janeiro de 1995. Além disso, pretendia-se que as inovações técnicas e os novos requisitos daí resultantes fossem comunicados ao FBI e ao Secretariado do Conselho. A razão desta medida prendia-se com o facto de, muitas vezes, a produção das telecomunicações estar nas mãos de empresas multinacionais, tornando assim imprescindível a cooperação com as autoridades competentes dos países terceiros onde esses centros de produção se encontram sediados.

O memorando foi assinado, em 23 de Novembro de 1995, pelos Estados-Membros da UE e por um único país terceiro, a Noruega. Os Governos dos Estados Unidos da América, do Canadá e da Austrália apenas informaram, por escrito, que iriam providenciar a transposição dos requisitos para a ordem interna dos seus países.

Lamentavelmente, até à data, o texto ainda não foi publicado, tendo dado azo a inúmeras especulações na imprensa.

2.2.2.2.3.3 O projecto de resolução do Conselho relativa à intercepção legal de telecomunicações no que respeita às novas tecnologias

Como o relator já teve oportunidade de referir no seu relatório de 23 de Abril de 1999[2], o «projecto de resolução do Conselho relativa à intercepção legal de telecomunicações no que respeita às novas tecnologias» constitui uma «actualização» da resolução de 1995. Pretende esclarecer que os "requisitos", aos quais são acrescentados alguns novos, também se aplicam às novas tecnologias, por exemplo, as comunicações por satélite e a Internet e que os termos técnicos utilizados actualmente devem ser entendidos por analogia no sector das novas tecnologias (por exemplo, o número de telefone é equivalente ao código de identificação para

[1] Sobre o conteúdo, cf. resposta escrita do Ministro dos Assuntos Internos austríaco, Karl Schlögel, à pergunta parlamentar do deputado Van der Bellen; 4739/AB XX. GP.
http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/AB04739_.html.

[2] A4-0243/99

acesso à Internet). Apesar de o Parlamento Europeu ter aprovado o projecto[1], o Conselho decidiu congelá-lo provisoriamente.

2.2.2.4 A convenção relativa ao auxílio judiciário mútuo em matéria penal[2]

O segundo acto jurídico é a convenção relativa ao auxílio judiciário mútuo em matéria penal. Os artigos 17º e seguintes da Convenção estabelecem as condições em que serão executados os pedidos de auxílio judiciário mútuo em matéria penal que envolvam a intercepção de telecomunicações. Sem querer entrar nos detalhes da regulamentação, fica apenas o apontamento de que a Convenção não limita de forma alguma os direitos das pessoas sujeitas a intercepção, uma vez que o Estado-Membro onde a pessoa em causa se encontra pode recusar-se a prestar auxílio judiciário, sempre que à luz da sua legislação nacional tal auxílio não seja admissível.

2.3 Medidas de vigilância destinadas a garantir a ordem democrática fundamental

No que respeita à garantia da ordem e a segurança interna, afigura-se insuficiente que a recolha de informações por parte do Estado se limite a investigações específicas em casos concretos de suspeita de crime. Para poder combater, pela raiz, eventuais movimentos extremistas ou subversivos, o terrorismo e a criminalidade organizada, o Estado tem de dispor de fontes de informação alternativas. Geralmente, existem bases jurídicas próprias que permitem determinadas operações de vigilância, incluindo a observação e a gravação de imagens e de sons, para fins de prevenção. A recolha de dados relevantes, bem como a respectiva análise, é levada a cabo por serviços de informações especiais a nível nacional, que normalmente também se dedicam à prevenção da espionagem e estão sob a tutela do ministro dos Assuntos Internos ou do ministro da Justiça (ver documento de trabalho 5). A actividade destes serviços está normalmente sujeita à fiscalização de um grémio parlamentar (para mais informações, ver o documento de trabalho 6). No combate à criminalidade internacional, existe uma colaboração estreita com os serviços de informações externos. Quando se trata da segurança de equipamentos militares, muitas vezes, é uma autoridade militar que detém a competência exclusiva na matéria.

Estas medidas de vigilância também não têm como alvo o público em geral, mas antes pessoas específicas ou determinados grupos de pessoas. Se fosse legalmente permitido vigiar de forma generalizada todos os cidadãos, isso traduzir-se-ia num esvaziamento do direito fundamental ao respeito pela vida privada e só por isso nunca poderia estar previsto em qualquer ordem jurídica nacional.

2.4 Medidas de vigilância destinadas a garantir a segurança externa

Uma parte significativa das medidas de vigilância é constituída por acções tendentes a garantir a segurança do Estado em relação a actividades desenvolvidas no estrangeiro. Trata-se, por um lado, de avaliar a situação estratégica militar (mesmo em tempos de paz) e de observar as crises a nível internacional. Por outro lado, trata-se de acompanhar a actividade de grupos

[1] Resolução legislativa que contém o parecer do Parlamento Europeu, de 7 de Maio de 1999, JO C 279, p. 498, de 1 de Outubro de 1999.

[2] Acto do Conselho, de 29 de Maio de 2000, que estabelece, em conformidade com o artigo 34º do Tratado da União Europeia, a Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia; JO C 197 de 12 de Julho de 2000, p. 1.

estabelecidos no estrangeiro e que aí se dedicam à prática de actos de criminalidade e/ou de terrorismo internacionais.

A recolha, o tratamento, a análise e o fornecimento de informações importantes para a segurança a partir do estrangeiro compete, geralmente, a um serviço de informações externo. Na maioria dos países, este trabalho é realizado pelas forças armadas, enquanto que noutros também envolve instituições da sociedade civil (ver documento de trabalho 5). Também aqui, a fiscalização compete normalmente a um grémio parlamentar (para mais informações, ver documento de trabalho 6).

Em regra, este tipo de intercepções não visa pessoas singulares, mas abrange, pelo contrário, determinadas áreas ou frequências. Consoante os meios e as atribuições legais dos serviços de informações externos, estes têm ao seu dispor um amplo espectro de possibilidades, abrangendo desde as operações de vigilância estritamente militares por intercepção de comunicações na gama de onda curta até à intercepção de todo o tipo de comunicações com o estrangeiro. Neste último caso, as mensagens podem ser seleccionadas com a ajuda de um filtro electrónico que as separa em função de determinadas ligações ou palavras-chave, sendo igualmente possível avaliar os respectivos resultados (ver documento de trabalho 3).

Comparativamente, os serviços de informações externos possuem poderes bastante amplos, o que se deve ao facto de visarem a intercepção de comunicações estrangeiras e, por conseguinte, afectarem apenas uma pequena minoria dos sujeitos jurídicos.

2.5 Espionagem de sinais eléctricos (SIGINT)

A espionagem de sinais eléctricos (SIGINT), propriamente dita, designa informações importantes sob o ponto de vista técnico e da segurança obtidas mediante a intercepção de sinais, em especial de telecomunicações, sem envolvimento do destinatário da mensagem. A SIGINT inclui, geralmente, informações resultantes de intercepções de sinais de localização, de navegação e de radar, enquanto que o conceito mais restrito COMINT (Communications intelligence) abrange exclusivamente informações relativas a comunicações. Os dois conceitos são, na maioria dos casos, utilizados como sinónimos.

Num sentido mais amplo, o conceito SIGINT é entretanto associado a um determinado processo de vigilância das telecomunicações, isto é, a intercepção mais ou menos sistemática de comunicações estrangeiras em todos os meios de transmissão ao alcance dos serviços de informações externos (feixe hertziano, satélite, cabo de cobre, cabo coaxial, cabo de fibra óptica).

A espionagem de sinais eléctricos começou com as escutas das comunicações diplomáticas. Conforme referido no ponto 2.1 supra, os organismos estatais não podem proceder à intercepção generalizada das comunicações no seu território, em virtude da protecção dos direitos fundamentais que assistem aos cidadãos nacionais. A intercepção a partir do exterior era, por sua vez até há bem pouco tempo, bastante difícil do ponto de vista técnico. Era, no entanto, usual interceptar as comunicações entre as embaixadas, que embora estabelecidas no território nacional não estavam sujeitas à sua jurisdição, e os respectivos países de origem. Para além das comunicações diplomáticas, também as comunicações militares começaram a ser cada vez mais alvo de escutas, o que se revelou ser uma tarefa particularmente fácil nas regiões fronteiriças. Com a evolução técnica também as comunicações assumiram novas formas, como, por exemplo,

a Internet, que originalmente foi concebida e utilizada para fins militares, ou as comunicações via satélite.

A tecnologia de vigilância acompanhou o ritmo de desenvolvimento das tecnologias de comunicação. Subitamente tornou-se possível escutar todas comunicações, mesmo aquelas realizadas longe do território nacional: as informações trocadas através da Internet entre duas cidades europeias começaram subitamente a passar pelos EUA; os dados transmitidos via satélite passaram a poder ser registados mesmo a grandes distâncias da estação terrestre interceptada. Uma vez que a comunicação civil utiliza os mesmos canais que a comunicação militar e diplomática, passou a ser possível interceptar também de forma generalizada as comunicações estrangeiras de carácter civil, quando inicialmente a vigilância só prosseguia fins militares e de segurança nacional. Atendendo à crescente internacionalização do comércio, tal oportunidade era bem-vinda, já que a recolha de informações sobre o estado da ciência e da tecnologia nos outros países começou a adquirir uma importância cada vez maior.
Acresce ainda que, simultaneamente, começaram a surgir grupos de criminalidade organizada que actuam a nível internacional, facto esse que obrigou muitos países a tomar medidas de vigilância.
Deste modo, também a sociedade civil reconheceu a necessidade de se recorrer à espionagem de sinais eléctricos, pelo que a sua utilização não é contestada.