Vigilância Vídeo, Interceção Preventiva de Comunicações e Contraterrorismo

Júlio Pereira

Exerce atualmente funções de Procurador-Geral Adjunto no Supremo Tribunal de Justiça, tendo desempenhado, entre outros, o cargo de Diretor-Geral Adjunto do Serviço de Informações de Segurança, Diretor-Geral do Serviço de Estrangeiros e Fronteiras e Secretário-Geral do Sistema de Informações da República Portuguesa.

Resumo

Este artigo aborda a estratégia nacional de combate ao terrorismo nas suas múltiplas dimensões. É dado especial enfoque às questões relacionadas com a vigilância vídeo, interceção preventiva de comunicações e contraterrorismo. Para o autor, a estratégia nacional corresponde, grosso modo, à estratégia europeia neste domínio. Como é sublinhado, o problema da videovigilância é sempre o do equilíbrio entre o valor da segurança e o respeito pelos direitos constitucionais, particularmente no que respeita ao direito à privacidade e direito à imagem.

Abstract

Video Surveillance, Preventive Interception of Communications and Counterterrorism

This article addresses the national counter-terrorism strategy in its multiple dimensions. Particular focus is given to issues related to video surveillance, preventive interception of communications and counterterrorism. For the author, the national strategy corresponds to the European strategy in this area. As is emphasized, the problem of video surveillance is always that of the balance between the value of security and respect for constitutional rights, particularly with regard to the right to privacy and the right to image.

A Estratégia Nacional de Combate ao Terrorismo, aprovada pela Resolução do Conselho de Ministros n.º 7-A/2015, de 20 de fevereiro, aponta como objetivos estratégicos detetar, prevenir, proteger, perseguir e responder, assim procurando combater o terrorismo em todas as suas manifestações:

– Detetar, identificando precocemente potenciais ameaças terroristas, mediante a aquisição do conhecimento essencial para um combate eficaz, tanto na perspetiva do seu desmantelamento isolado, quanto da deteção de outros focos de ação terrorista. A recolha, tratamento e análise de dados e informações e a sua disponibilização recíproca entre entidades responsáveis neste domínio, no território nacional e no estrangeiro, permite antecipar o conhecimento e a avaliação de ofensivas em preparação.
– Prevenir, conhecendo e identificando as causas que determinam o surgimento de processos de radicalização, de recrutamento e de atos terroristas. O domínio dos factos que potenciam a sua expansão permite a adoção de medidas que obstem ao seu surgimento e desenvolvimento.
– Proteger, fortalecendo a segurança dos alvos prioritários, reduzindo quer a sua vulnerabilidade, quer o impacto de potenciais ameaças terroristas. A proteção concretiza-se no aumento da segurança das pessoas, das fronteiras, da circulação de capitais, das mercadorias, dos transportes, da energia e das infraestruturas críticas, nacionais e ou europeias.
– Perseguir, desmantelando ou neutralizando as iniciativas terroristas, projetadas ou em execução, e as suas redes de apoio, impedindo as deslocações e as comunicações e o acesso ao financiamento e aos materiais utilizáveis em atentados e submetendo os fenómenos terroristas à ação da justiça.
– Responder, gerindo operacionalmente todos os meios a utilizar na reação a ocorrências terroristas. A capacidade de resposta permite limitar as suas consequências, quer ao nível humano, quer ao nível das infraestruturas. A resposta incide ainda na assistência, tendo em consideração as necessidades especiais das vítimas e das testemunhas.

O mesmo documento indica como linhas de ação para prossecução do primeiro objetivo estratégico (detetar), entre outras as seguintes:

– Robustecer as estruturas responsáveis pela produção e coordenação e partilha de informações relevantes na identificação da ameaça terrorista;
– Reforçar os meios de produção, tratamento e análise de informações.

Por esta breve alusão aos objetivos estratégicos e algumas das respetivas linhas de ação é desde logo possível verificar a importância quer da videovigilância quer da intervenção preventiva de comunicações no prosseguimento da estratégia nacional de combate ao terrorismo, nomeadamente no que diz respeito à proteção das pessoas e das infraestruturas críticas e na capacidade de reposta no caso de um incidente terrorista.

A estratégia nacional corresponde *grosso modo* à estratégia europeia neste mesmo domínio, se bem que entre nós, no que diz respeito à prevenção, se tenha operado um desdobramento para dois objetivos estratégicos: por um lado a deteção e por outro a prevenção. Não creio que tenha havido nisso qualquer vantagem e receio mesmo que isso se tenha ficado a dever a uma mais fácil e menos quezilenta repartição de competências entre forças e serviços de segurança, na concretização de cada um dos pilares da estratégia. Falo assim por ter na memória o conturbado processo que levou à aprovação do plano de coordenação, controlo e comando operacional das forças e serviços de segurança, que se arrastou durante anos, precisamente por causa das disputas corporativas em matéria de competências, particularmente no que diz respeito à gestão dos incidentes tático-policiais, que viriam a ser ultrapassadas pela perspetiva da criação do cargo de secretário-geral do sistema de segurança interna e por uma postura mais assertiva do então responsável da tutela.
No conjunto das medidas que um pouco por todo o mundo foram sendo adotadas em matéria de contraterrorismo, destaca-se o reforço de capacidades e de meios dos serviços de informações e a partilha de informações entre forças e serviço de segurança, tanto a nível nacional como no plano internacional. É verdadeiramente impressionante o avanço que neste domínio se fez sentir, particularmente no âmbito internacional, já que a temática das informações foi sempre encarada como matéria de soberania sujeita a especiais medidas de sigilo e a cooperação só existia no âmbito de questões pontuais e específicas e entre países que partilhavam interesses convergentes ou de manifesta proximidade.
Quando Portugal, em fins dos anos 90, por iniciativa do então diretor do Serviço de Informações de Segurança (SIS), Dr. Rui Pereira, propunha a criação de uma Eurointel, um serviço de informações de segurança interna dos países da União Europeia, a proposta foi encarada com espanto e manifesta animosidade. Todavia, com os acontecimentos de 11 de Setembro, subsequentes atentados de Madrid e Londres e posterior disseminação do terrorismo jihadista o realismo apoderou-se das mentes dos líderes americanos e europeus e hoje, para além de um INTCEN – EU Intelligence and Situation Centre –, que produz informação de natureza estratégica no âmbito da Comissão Europeia, temos um grupo de contraterrorismo no seio do Clube de Berna – organização informal que reúne representantes dos serviços internos de Estados-membros da União Europeia – e ainda uma estrutura sedeada em Haia, que partilha em tempo real informação sobre ameaças e atentados terroristas, na qual estão representados todos os serviços internos dos países da UE, que constitui uma verdadeira unidade europeia de prevenção e combate ao terrorismo.
No que diz respeito aos meios e capacidades dos serviços registou-se uma evolução semelhante. Os serviços, muito centrados durante o período da Guerra Fria nas questões associadas ao conflito leste/oeste, particularmente na espionagem e ameaças terroristas de cariz ideológico e independentista, que na generalidade dos

casos espelhavam também esse conflito, foram perdendo terreno e chegou mesmo a ser questionada a sua utilidade após a falência da União Soviética. Com a emergência do terrorismo de cariz islamista e quando a respetiva ação se fez sentir nos Estados Unidos e na Europa, ganharam necessariamente novo fôlego e rapidamente se reajustou o seu dispositivo para poderem enfrentar esta nova ameaça. Na generalidade dos países europeus foi alterada a sua estrutura, criaram-se instâncias de coordenação, alargaram-se os seus poderes e ampliaram-se os seus meios materiais e humanos.

Compreende-se a razão deste processo evolutivo. As ameaças deixaram de ser nacionais, luta-se contra um inimigo invisível e os caminhos que conduzem à realização de atentados são percorridos, em cerca de 90% do seu percurso, na penumbra ou na sombra. Neste contexto reconhece-se que o trabalho dos serviços de informações é essencial para se poder evitar, ou pelo menos para reduzir a ocorrência de atentados ou para limitar os respetivos efeitos.

Para chegar a esse inimigo invisível, é essencial a sua deteção nos meios onde desenvolve a sua ação preparatória, desde a fase de doutrinação, passando pela radicalização, recrutamento e treino e posterior preparação para a ação terrorista, o que implica um vasto conjunto de ações e de disponibilização de recursos, sendo indispensável uma grande cooperação no plano internacional, que passa essencialmente pela troca ampla e célere de informações e atividades operacionais conjuntas e, no plano nacional, por uma empenhada cooperação entre forças e serviços de segurança e também forças armadas, indispensável para acompanhar indivíduos, locais e comunidades de risco e detetar indícios técnicos que apontem para o envolvimento individual ou de grupos em atividades suspeitas.

As interceções de comunicações constituem, no elenco dos meios ao dispor das forças e serviços de segurança, imprescindíveis para tal finalidade. Até porque é no universo da internet, com a imensidão dos fornecedores desse serviço, com a possibilidade de ocultação e multiplicação de identidades e de recurso a redes de acesso condicionado ou interdito, que grande parte das coisas acontecem e em geral onde elas começam.

Cremos que em Portugal as polícias dispõem no plano legal de capacidades equivalentes ao que ocorre em grande parte dos países da União Europeia em matéria de videovigilância. Poderão não dispor dos mesmos meios em termos técnicos, dada a constante evolução da tecnologia e custos que lhe estão associados, mas no plano legal não sofrerão mais limitações do que em outros países do espaço europeu, até porque esta matéria tem o essencial das suas regras fixadas em instrumentos jurídicos da União Europeia.

O problema da videovigilância é sempre o do equilíbrio entre o valor da segurança e o respeito pelos direitos constitucionais, particularmente no que respeita ao direito à privacidade e direito à imagem. E este equilíbrio será cada vez mais difícil

à medida que se vão sofisticando os instrumentos de vigilância, designadamente com a maior capacidade de definição de imagem e o *software* que lhe está associado para reconhecimento de voz, reconhecimento facial e identificação pelos diversos elementos biométricos. Ou seja, quanto mais sofisticado o equipamento mais eficaz se torna para a respetiva finalidade mas simultaneamente maior é a sua capacidade de devassa e mais difícil é conciliar a videovigilância com os diversos direitos constitucionais que serve ou com que contende.

Deve dizer-se que não é unânime a opinião sobre a mais-valia da videovigilância, tanto em matéria de contraterrorismo como de prevenção da criminalidade comum. Se em geral se reconhece a sua eficácia, por exemplo na preservação dos centros urbanos contra ações de vandalismo, ou para a proteção de locais procurados para a prática de crimes por carecerem de vigilância ou mais afastados de instalações policiais, alude-se por outro lado ao facto de as câmaras de videovigilância empurrarem o crime para outros locais e até de estigmatizarem certas zonas. Há mesmo quem acuse o uso de câmaras de constituírem um fator de radicalização terrorista, nomeadamente quando direcionadas para a vigilância de certas comunidades étnicas ou religiosas. Há, no entanto, que reconhecer que a maioria destas críticas vem de sectores que privilegiam a proteção das liberdades individuais em detrimento do vetor segurança.

Vivemos hoje numa sociedade cada vez mais urbanizada, com uma enorme mobilidade de pessoas, provenientes das mais diversas origens, de todas etnias, professando diferentes confissões religiosas. Está definitivamente ultrapassado o tempo em que a rotina uniforme dos dias permitia assinalar qualquer situação anómala. Hoje encontramo-nos em permanência com pessoas diferentes, em diferentes contextos situacionais, tornando-se praticamente inviáveis os velhos mecanismos informais de controlo, muito assentes na cooperação dos próprios cidadãos. É agora impossível policiar uma grande cidade, todos os locais de concentração de pessoas, sem recurso a meios técnicos, nomeadamente videovigilância, que de forma ativa ou passiva auxiliem a polícia no desempenho das suas tarefas, nomeadamente de prevenção da criminalidade. Ora, se em matéria de segurança, a colaboração ativa dos cidadãos é indispensável, como de resto é reconhecido em diversos países com apelos à vigilância cidadã, como acontece em França ou, para dar um exemplo mais radical com a China, onde a lei da segurança nacional faz menção expressa a essa participação, isso já não basta. A configuração das cidades e o *modus vivendi* de hoje não permitem que o tradicional controlo informal opere de forma eficaz, podendo mesmo dar origem a lamentáveis equívocos que, em termos de ofensa aos direitos individuais, podem até ser mais lesivos do que os apontados excessos de qualquer programa de vigilância vídeo.

A eficácia da videovigilância no âmbito do contraterrorismo, começou a ser amplamente reconhecida por altura dos atentados de 2005 em Londres, já que permitiu

identificar os terroristas da primeira vaga de atentados e deter os que se preparavam para uma segunda. Foi também reconhecida nos atentados mais recentes, como nos atentados de Paris em 2015 e de Bruxelas em 2016, se bem que neste último caso as imagens divulgadas tenham sido um bónus oferecido aos terroristas, permitindo-lhes ver aquilo que deviam evitar em atentados subsequentes. Daí que as autoridades francesas tenham reforçado o seu dispositivo de videovigilância e o atentado de Berlim, de dezembro de 2016, tenha removido as reservas que existiam na Alemanha, de enveredar por caminho semelhante.

Na verdade, à medida que vão sendo recolhidos mais elementos sobre agentes da ameaça terrorista, se vai partilhando a informação a nível europeu e se vão desenvolvendo novos mecanismos para tratamento inteligente dos dados obtidos, registam-se novas capacidades de prevenção de atentados ou de contenção subsequente dos respetivos efeitos.

Pelo que sei, a videovigilância em Portugal tem obtido resultados positivos, constituindo fator não negligenciável de redução da criminalidade urbana. Felizmente não temos tido oportunidade de avaliar as suas potencialidades na prevenção do terrorismo mas, não estando nós imunes a uma possível ocorrência dessa natureza, podemos pelo menos considerar que a sua importância não será menor do que a que tem tido em países que até agora têm sido fustigados pelo fenómeno.

Um outro fator importante a ter em conta é o contributo da videovigilância para o sentimento de segurança das populações. Não obstante as cautelas e as preocupações quanto ao uso deste meio de prevenção, a verdade é que a população, em toda a Europa, é favorável ao seu uso e sente-se mais segura com a sua utilização. Ora o sentimento de segurança é um importantíssimo fator de paz social. O sentimento de insegurança gera intranquilidade e em alguns países tem até contribuído para um desvio rumo a políticas não democráticas porque a segurança, não sendo o direito mais importante, é o palco onde se exercem todos os outros direitos. E é até mais relevante, mais impactante o sentimento de segurança do que real situação de segurança. Uma sociedade é mais tranquila se nela prevalecer a ideia entre as pessoas de que estão seguras, ainda que a real situação não lhe corresponda exatamente, do que, apesar de objetivamente desfrutar de um bom clima de segurança nela prevalecer um sentimento de insegurança. Nestas circunstâncias, a sociedade sofre daquilo que eu costumo designar por hipocondria securitária, que Kafka ilustrou magistralmente no seu conto "A toca".

Por outro lado e numa sociedade democrática, onde as forças e serviços de segurança atuam em conformidade com a constituição e a lei, os procedimentos de segurança acrescentam liberdade. Nos países fustigados pelo terrorismo e até pela criminalidade comum, em que as pessoas têm receio de frequentar determinadas zonas, de viajar para certos locais, elas sofrem uma efetiva restrição da liberdade. O habitante de uma grande cidade que a certas horas da noite não entra em deter-

minadas linhas do metropolitano, ou em certos bairros chama um táxi para se deslocar por escassas centenas de metros, vê reduzida a sua liberdade, só que não perceciona esse facto como tal. Para ele é apenas insegurança. Mas não, é efetiva restrição da liberdade. Ou seja, a segurança acrescenta liberdade.

Se as polícias estão dotadas de meios legais condizentes com as necessidades da sua atuação no plano da prevenção da criminalidade, já o mesmo se não pode dizer relativamente aos serviços de informações que, agindo numa fase precoce, de prevenção antecipada, quando ainda não há elementos que permitam o início de uma investigação criminal, no âmbito da qual os órgãos de polícia criminal, com permissão da autoridade judiciária competente podem recorrer a meios intrusivos, têm que agir no maior sigilo. E aí, os instrumentos legais existentes, não estão manifestamente à altura das necessidades, nomeadamente para controlo de alvos determinados.

A Lei n.º 1/2005, de 10 de janeiro, regula a utilização de sistemas de vigilância por câmaras de vídeo pelas Forças e Serviços de Segurança em locais públicos de utilização comum, para captação e gravação de imagem e som. Um dos fins para que pode ser autorizada é a prevenção de atos terroristas – art.º 2.º, n.º 1 alínea *e*).

A instalação de câmaras fixas está sujeita a autorização do membro do governo que tutela a FSS – art.º 3.º, n.º 1 – precedida de parecer da Comissão Nacional de Proteção de Dados – art.º 3.º, n.º 2 – e, os locais objeto de vigilância é obrigatória a afixação, em local bem visível, de informação da existência e localização das câmaras, finalidade da captação da imagem e som, responsável pelo tratamento de dados e direitos de acesso e retificação que podem ser exercidos – art.º 4.º.

Um diploma com esta norma está talhado para a prevenção da criminalidade comum. Não tem sentido no âmbito da prevenção do terrorismo.

No que diz respeito à interceção de comunicações a situação portuguesa, no que concerne aos serviços de informações é deplorável, constituindo Portugal um fator de vulnerabilidade do Espaço Schengen. É o único país desse espaço que veda essa possibilidade aos serviços. Sem interceção de comunicações a prevenção do terrorismo chegará tarde de mais. Dificilmente se compreende que no âmbito da investigação criminal tal seja possível e que esse procedimento esteja banido para efeitos de prevenção, o que revela maior empenho na punição do delinquente do que na proteção das vítimas.

Diz-se que o problema decorre de limitações de ordem constitucional porquanto, nos termos do art.º 34.º, n.º 4 da Constituição da República Portuguesa "É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal". Porém, mais do que na norma, pode o problema situar-se na amplitude com que a mesma tem sido interpretada. Havendo boas razões para se entender que esta norma foi pensada tendo em vista o conteúdo das comunica-

ções, confiou-se na possibilidade de dela se fazer uma interpretação que a isso a reconduzisse, dados os riscos associados ao terrorismo, à espionagem e criminalidade altamente organizada.

Foi por isso ensaiada a possibilidade de dar aos serviços de informações o poder "de aceder aos dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar ou identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização" e nesse sentido foi aprovado na Assembleia da República, por larga maioria, o Decreto n.º 426/XII. Era uma inovação tímida, que dava essa possibilidade para fins determinados e desde que autorizada por uma comissão constituída por três juízes do Supremo Tribunal de Justiça, designados pelo seu Presidente.

O diploma foi sujeito pelo Presidente da República a fiscalização preventiva e a norma em causa foi considerada inconstitucional.

Portugal não tem lições a dar, em matéria de proteção dos direitos fundamentais, à generalidade dos países democráticos, onde a interceção preventiva de comunicações, em termos muito mais amplos do que os previstos na norma constitucionalmente vetada, era permitida. Ainda assim o Tribunal Constitucional, com um esclarecido voto de vencido, pronunciou-se pela inconstitucionalidade.

Pode apontar-se para isso uma boa razão: Portugal tem sido imune aos atentados terroristas que têm afligido outros países da Europa e o grau de ameaça não tem ultrapassado o nível moderado. De facto, têm sido os atentados e os graus de ameaça que têm impulsionado a produção de legislação mais intrusiva neste domínio, como aconteceu por exemplo nos Estados Unidos ou com a França. Ou seja, não é apenas em Portugal que neste domínio tem prevalecido uma atitude reativa. Também em outros países as coisas evoluíram não por força da razão mas por impulso das bombas e do sangue das vítimas. Só que nesses outros países o que tem estado em causa não é a atribuição de poderes, como em Portugal, mas a sua ampliação.

Ora, não obstante a situação de risco moderado que temos tido em Portugal, há alguns sinais que merecem a devida atenção, designadamente alguns sinais de radicalização, casos de recrutamento para a militância terrorista e a possibilidade de vinda para Portugal de soldados de Alá, portugueses ou com ligações a Portugal e ainda outros que com eles se relacionaram.

Deparamo-nos também com um trauma que ainda não foi ultrapassado e que gera um sentimento de recusa num determinado espetro político, em conferir estes meios aos serviços de informações, sugerindo-se mesmo que seria de alargar os poderes da Polícia Judiciária por forma a abarcar a possibilidade de recurso a esse meio com vista à produção de informações. Todavia esta posição afronta a matriz do sistema de informações que foi estruturado com vista a uma separação nítida entre a atividade de polícia e a atividade de informações. O nosso legislador preten-

deu evitar a criação de polícia de informações, que era o paradigma existente até 25 de abril de 1974.

Próxima desta razão há uma outra que se prende com um alargamento progressivo da judicialização da atividade de segurança interna, aliada a um também alargamento do conceito de prevenção criminal o qual, no entendimento de alguns, poderia abranger a produção de informações no domínio do contraterrorismo, a cargo da Polícia Judiciária como órgão competente na investigação e prevenção dos crimes de terrorismo, sob supervisão do Ministério Público. Resulta esta posição, como disse, de um conceito alargado de prevenção criminal, que sob o ponto de vista da proteção dos direitos das pessoas é positivo mas que desequilibra em excesso a relação com o vetor segurança e gera o risco de tomada de assalto de competências de segurança interna, que não cabem nem ao Ministério Público nem em exclusivo à Polícia Judiciária.

Finalmente há que registar uma tendência para reconduzir a atividade de informações ao paradigma do processo penal e centrar a proteção dos direitos fundamentais em entidades judiciárias ou de natureza judiciária.

Não obstante todas estas dificuldades a possibilidade de acesso aos dados de tráfego foi consagrada na Lei Orgânica n.º 4/17, de 25 de agosto, embora num contexto excessivamente burocrático que não se sabe se alguma vez irá funcionar. No que diz respeito ao acesso a dados de tráfego os mesmos terão que se destinar exclusivamente à prevenção de atos de espionagem e terrorismo e a violação das disposições previstas nesta lei geram sanções criminais agravadas.

É efetuado um controlo judicial dos pedidos, por uma entidade constituída pelos presidentes das secções criminais do Supremo Tribunal de Justiça e por um conselheiro designado pelo Conselho Superior da Magistratura, entidade que é também a que autoriza. O pedido é dirigido pelo Secretário-Geral do Sistema de Informações da República Portuguesa à comissão judicial, com conhecimento ao Procurador-Geral da República e, uma vez dada autorização, a mesma pode ser cancelada em qualquer momento por esta entidade, que tem competência para fiscalizar a sua execução, poderes de fiscalização que competem também à Comissão de Fiscalização de Dados e ao Conselho de Fiscalização do Sistema de Informações da República Portuguesa.

As possibilidades de este regime merecer o aval do Tribunal Constitucional são escassas dados os precedentes acima mencionados. Tudo aponta no sentido de que, em matéria de meios de prevenção do terrorismo continuaremos a estar orgulhosamente sós, exibindo a bandeira de elo mais vulnerável do Espaço Schengen.