

Inteligência de Segurança Pública em Seis Países

Mandatos Legais e Estrutura Organizacional ¹

Marco Cepik ²

Neste trabalho descrevo a legislação e a organização de inteligência em seis países (Estados Unidos, Canadá, Alemanha, Itália, Israel e África do Sul), com especial atenção para a área de inteligência de segurança pública (ISP). O objetivo deste levantamento preliminar é destacar a importância dos mandatos legais e criar algum parâmetro comparativo para o debate brasileiro sobre doutrina e implementação do SISP (Subsistema de Inteligência de Segurança Pública) nos estados. Estabelecido formalmente pelo Decreto Executivo 3.695/2000, o SISP a discussão pública sobre seus contornos concretos nos diversos estados da federação, bem como sobre o seu papel na reforma do sistema de justiça criminal e nos padrões de policiamento no Brasil poderia beneficiar-se do exercício descritivo oferecido no presente trabalho.

Antes de passarmos prosseguir, vale alertar o leitor quanto à diferença entre as duas áreas de inteligência interna, a chamada inteligência de segurança (*security intelligence*), mais voltada para as ameaças potenciais contra a segurança do Estado, e a inteligência criminal (*criminal intelligence*), voltada para o apoio das funções de policiamento, provimento de ordem pública e justiça criminal. Esta segunda área é que estamos chamando no Brasil de Inteligência de Segurança Pública (ISP).

A primeira área abarca as ameaças decorrentes da 'subversão', terrorismo e espionagem, praticados por Estados e/ou grupos nacionais e/ou estrangeiros. No jargão da literatura especializada anglo-saxã, esta área é chamada então de inteligência de segurança (*security intelligence* para os britânicos, canadenses e australianos e

¹ CEPIK, Marco. "Inteligência de Segurança Pública em Seis Países: Mandatos Legais e Estrutura Organizacional". In: RATTON Jr, José Luiz; BARROS, Marcelo. (Org.). *Pólicia, Democracia e Sociedade*. 01 ed. Rio de Janeiro: Lumen Juris, 2006, p. 101-149.

² Professor do Departamento de Ciência Política da UFRGS, pesquisador do GEE/COPPE/UFRJ e do NERINT/ILEA/UFRGS.

domestic intelligence nos Estados Unidos). A segunda área – e a que interessa mais diretamente aqui – é chamada inteligência criminal, ou policial (*criminal intelligence*), a qual tem como foco as ameaças resultantes de dinâmicas criminais mais ou menos complexas.

Considerando a confusão terminológica que isto tudo pode gerar, adotarei neste texto esta diferenciação entre o sentido mais geral (*security intelligence*) e o sentido mais específico (*criminal intelligence*), a despeito do fato de no Brasil haver a tendência para que a chamada inteligência interna abarque as duas coisas. Creio que esta solução é preferível e começa a ser reconhecida a especificidade doutrinária, funcional e organizacional da inteligência criminal ou policial, a qual tem recebido a designação nos regulamentos administrativos e legais de inteligência de segurança pública (ISP), justamente para diferenciá-la da chamada inteligência de Estado.

Em termos organizacionais, vale lembrar que *security intelligence* é o que o *Security Service* britânico (conhecido popularmente como MI-5) faz. No Brasil, isto corresponde em parte ao que historicamente a ABIN considera ser a sua missão central, embora formalmente esta agência brasileira também seja responsável pela chamada inteligência externa de Estado, o que no caso britânico corresponde à área de atuação de um órgão separado, o *Secret Intelligence Service* (ou popularmente conhecido como MI-6). Para não acrescentar confusão desnecessária a uma terminologia ainda pouco padronizada em termos internacionais e nacionais, neste texto não serão feitas maiores considerações sobre inteligência externa, seja ela civil ou militar.³

Por sua vez, e de novo em termos organizacionais e administrativos, *criminal intelligence* é o que as 53 forças policiais inglesas fazem nesta área, embora

³ Para um comentário adicional sobre a área militar, ver: CEPIK, Marco A. C. (2003a). “Inteligência Militar e Política de Defesa”. In: REBELO, Aldo [org.]. *Política de Defesa para o Século XXI*. Brasília, Câmara dos Deputados. Páginas 111-123.

coordenadas desde 1992 por um modelo nacional de inteligência policial e um serviço nacional de inteligência criminal, o *National Criminal Intelligence Service* (NCIS).⁴

Segundo Peter Gill (2000:77-91), entretanto, mesmo no caso do Reino Unido são bastante evidentes as dificuldades de delimitação de mandatos, limites tecnológicos, doutrinários, culturais, orçamentários e de pessoal para o estabelecimento efetivo, nacionalmente coordenado, de um modelo de policiamento ‘liderado pela atividade de inteligência’.⁵

No Brasil, o que existe atualmente em termos organizacionais corresponde em parte ao que a Diretoria de Inteligência Policial da Polícia Federal faz e ao que as polícias estaduais fazem na área de inteligência. Entretanto, pode-se dizer que no Brasil ainda há pouca inteligência criminal e muita ênfase na componente de segurança estatal (*security intelligence*), mesmo nas polícias. Isto não ocorre apenas por razões históricas inerciais, mas também em função das dimensões do país, da natureza de nossa inserção internacional e da ausência de uma problematização específica sobre o papel do conhecimento sistemático no trabalho policial. Além das imposições práticas decorrentes de ameaças mais ou menos agudas ligadas ao terrorismo, narcotráfico e crime organizado, as intersecções entre inteligência de segurança e inteligência criminal (ISP) são forjadas também pela necessidade de se buscar eficiência sistêmica e coordenação, ao mesmo tempo em que são aperfeiçoados os controles externos.

Feitas estas considerações iniciais, o restante deste trabalho será dividido em três partes. A seção I destaca a importância dos mandatos legais para a garantia de eficiência e de responsividade dos organismos de inteligência em geral e da área de

⁴ Para uma diferenciação bem clara entre os papéis das duas áreas (*criminal intelligence* e *security intelligence*) no caso britânico, veja-se: <http://www.police.uk/nim>, <http://www.ncis.co.uk/> e <http://www.mi5.gov.uk/>. Creio que em nenhum outro país a especialização entre as duas áreas é tão clara. Mesmo nos Estados Unidos, onde a separação é bem clara no nível local, nos âmbitos estadual e federal a situação ainda é mais parecida com o Brasil do que com o Reino Unido. Embora o Reino Unido não tenha sido incluído sistematicamente nesta pesquisa, recomenda-se a leitura do *Regulation of Investigatory Powers Act 2000* (RIPA) daquele país. Ver: <http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm>. Para contextualizar a situação da ISP no governo britânico, ver também: www.homeoffice.gov.uk/crimpol/index.html.

⁵ GILL, Peter (2000). *Rounding Up the Usual Suspects?*. Aldershot, Ashgate Publishers. Ver especialmente o capítulo sobre “development of Intelligence-Led Policing”.

inteligência interna em particular (tanto de segurança estatal como criminal). Como as duas subáreas da inteligência doméstica representam riscos potenciais para as liberdades dos próprios cidadãos que elas visam a proteger, isto também nos força a pensar de maneira integrada os desafios colocados pelos mandatos legais.

Embora a **seção I** do presente trabalho mencione exemplos da Austrália e Reino Unido para destacar a necessidade e os limites dos mandatos legais na área de inteligência doméstica (especialmente na chamada área de *security intelligence*), estes dois países não foram incluídos no levantamento realizado, o qual se limitou aos casos dos Estados Unidos, Canadá, Alemanha, Itália, Israel e África do Sul.

Na **seção II** é apresentada de maneira breve e seqüencial a legislação de cada um dos seis casos nacionais. A maior parte do material disponível na Internet refere-se à área de *security intelligence* e não de *criminal intelligence* (relativa ao trabalho próprio das polícias), mas nos casos em que foi obtido material específico ele encontra-se citado e comentado segundo uma lógica que vai dos ordenamentos legais mais abrangentes para os mais específicos. Na **seção III**, por sua vez, são descritas as organizações de inteligência de cada um dos seis países selecionados para este levantamento.

Finalmente, nas considerações finais do trabalho são mencionados os problemas e desafios da construção de um Subsistema de Inteligência de Segurança Pública no Brasil à luz da experiência de outros países em que se verifica desenvolvimento semelhante.

I – A Importância dos Mandatos Legais na Área de ISP:

A própria idéia de que as agências de segurança nacional deveriam ter uma regulamentação legal mais detalhada de suas funções, mandatos e missões é

relativamente recente e creio ser útil reforçá-la, ainda que brevemente, mesmo que o mesmo argumento já tenha sido desenvolvido em outro local.⁶

Note-se ainda que a demanda por mandatos legais não é algo recente apenas nas democracias recentes. Como observa Peter Gill (1996:313-333), no Reino Unido passaram-se mais de oitenta anos entre a criação dos serviços de inteligência exterior e interna (originalmente uma única organização fundada em 1909) e a promulgação das leis que regulam o funcionamento, as missões e os mecanismos de prestação de contas das principais agências de inteligência daquele país (a saber, o *Security Service Act* de 1989, o *Intelligence Services Act* de 1994 e o *Regulation of Investigatory Powers Act* promulgado em 2000).⁷

A importância central da delimitação desses mandatos, do ponto de vista dos mecanismos de controle público, é que eles fixam expectativas normativas associadas ao desempenho de papéis sociais até então desconhecidos para o público. Quando uma lei ou uma diretriz executiva pública delimita os objetivos, os meios, as responsabilidades e as condutas esperadas de cada agência de um sistema nacional de inteligência, isso fornece uma base mínima a partir da qual alguém poderia avaliar os desempenhos desses sistemas do ponto de vista da sua efetividade e eficácia, além de sua legitimidade.

Porém, uma limitação óbvia para que essa avaliação seja feita pelos cidadãos individualmente é que muitas das diretrizes e regulamentos mais importantes (sobre requerimentos informacionais, alocações de recursos, operações específicas e produtos de inteligência, por exemplo) são necessariamente secretas. Ainda assim, os contornos mais gerais das atividades de inteligência e segurança podem e devem ser fixados em

⁶ O texto desta seção corresponde, com adaptações e atualizações, ao trecho compreendido pelas páginas 164-167 de meu livro. Cf. CEPIK, Marco. (2003). *Espionagem e Democracia*. Rio de Janeiro, FGV.

⁷ Cf. GILL, Peter. (1996). "Reasserting Control: Recent Changes in the Oversight of the UK Intelligence Community". *Intelligence and National Security*, Volume 11, number 2, April. Pages 313-331. Do mesmo autor, ver: GILL, Peter. (1994). *Policing Politics: Security Intelligence and the Liberal Democratic State*. London, FrankCass.

leis e diretrizes executivas públicas. As diretrizes executivas tendem a ser mais detalhadas do que as legislações aprovadas pelo parlamento.

Os mandatos legais são necessários tanto para estabelecer parâmetros para os governantes controlarem o grau de eficiência e efetividade das agências de segurança nacional (agilidade), quanto para auxiliar os cidadãos a controlarem o grau de compatibilidade entre a atuação desses mesmos serviços e as regras institucionais democráticas (transparência), legitimando por este mecanismo as práticas estatais neste setor. Um aspecto pouco notado a respeito dos mandatos é que, do ponto de vista das agências de segurança pública, esses funcionam também como uma forma de proteção das próprias agências contra eventuais pressões políticas de chefes de governo. Tais pressões poderiam dar-se, por exemplo, para forçar a realização de missões impróprias e que, diante da existência de mandatos codificados legalmente, seriam apenas irregulares, mas não propriamente ilegais e passíveis de responsabilização administrativa e penal.

Em nenhuma outra área os mandatos legais são mais necessários do que no caso da inteligência interna. Como salientam Lustgarten & Leigh (1994: 374-411), a maioria dos serviços de inteligência interna do mundo forjou sua cultura organizacional e seus hábitos operacionais no contexto da repressão aos movimentos de esquerda ou, de modo mais geral, combatendo a dissidência política e os críticos dos governos. A forte orientação ideológica anticomunista dos serviços de inteligência dos países capitalistas e a forte orientação repressiva contra os dissidentes nos países do chamado Socialismo Real tornaram-se substitutos de uma delimitação mais precisa, politicamente deliberada e legalmente consistente, dos conteúdos de termos como “subversão”, “terrorismo” e “sabotagem”.⁸

Analisando os mandatos legais atualmente em vigor para os serviços de inteligência de segurança da Grã-Bretanha, Canadá e Austrália, Lustgarten & Leigh (1994) também observaram que as missões de contra-espionagem e as medidas

⁸ Cf. LUSTGARTEN, L. & LEIGH, Ian. (1994). *In From the Cold: National Security and Parliamentary Democracy*. Oxford-UK, Clarendon Press.

defensivas de segurança (tanto no plano operacional quanto informacional) tendem a ser menos ambíguas e implicam menos riscos para as liberdades civis dos cidadãos dos países democráticos.⁹

Já no caso da obtenção de inteligência sobre ameaças terroristas, sabotagem e subversão, há recorrentes denúncias sobre a falta de proporcionalidade entre as ameaças e as medidas de segurança com as quais os governos tendem a responder, bem como denúncias sobre a caracterização arbitrária de dissidentes políticos como 'terroristas'.

No contexto pós-Guerra Fria, digamos até 2001, havia uma tendência moderada nesses três países (mais acentuada no caso australiano) para uma definição legal mais estrita de subversão, apontada como a "utilização organizada e continuada de meios violentos para fins de transformação da ordem política constitucionalmente estabelecida". Isso excluía do mandato legal dos serviços de segurança (*security intelligence*) a vigilância física e eletrônica de ativistas, manifestantes ou participantes de organizações de oposição ao governo, mesmo nos casos em que os cidadãos engajam-se em atos de desobediência civil. Por outro lado, essa tentativa de definição legal mais neutra do ponto de vista ideológico resultava também do crescimento da violência politicamente motivada e do terrorismo perpetrados por organizações de extrema-direita, tais como as milícias norte-americanas ou os grupos racistas e

⁹ Um ponto decisivo dos mandatos legais concedidos aos serviços de inteligência e segurança em relação à contra-espionagem é a concretização do princípio de soberania popular e de auto-governo; tentativas de governos ou organizações estrangeiras para influenciar os resultados políticos internos de uma nação soberana são considerados crimes graves porque violam os direitos democráticos dos cidadãos e devem ser prevenidos através do monitoramento por parte dos serviços de contra-inteligência. No caso dos Estados Unidos, mesmo o *lobby* regular de empresas, governos ou ONGs estrangeiras é monitorado, principalmente através da exigência de registro de atividades de estrangeiros. Ver: U.S. CODE. Section 951 of title 18. *Agents of Foreign Governments*. Ver também o: *Foreign Agents Registration Act of 1938 "as amended" [FARA]*. In: U.S. CONGRESS. (1998). *Compilation of Intelligence Laws and Related Laws and Executive Orders of Interest to the National Intelligence Community*. Washington-D.C., GPO, 1998. Páginas 421-435.

xenófobos existentes em quase todos os países mais industrializados e de renda *per capita* mais elevada.¹⁰

Claro está que os mandatos legais não resolvem os problemas políticos resultantes da interpretação sobre as áreas, os métodos e a intensidade da atuação das agências de inteligência. Tampouco as definições contemporâneas dos termos ‘subversão, terrorismo e sabotagem’ estão isentas de viés político ou ideológico, mesmo nas poliarquias institucionalizadas.¹¹ Entretanto, considerando-se que existem realmente ameaças que exijam a manutenção de organizações de *security intelligence*, os mandatos legais tornam-se imprescindíveis para ao menos estabelecer parâmetros a partir dos quais se possa julgar as ações e prioridades desses órgãos.

Além disso, os mandatos legais tornam-se mais importantes diante dos resultados recentes de estudos institucionais como o de Amy Zegart (1999:01-53), que concluiu que o fator mais importante na determinação da trajetória das agências de segurança nacional (dentre as quais incluem-se os serviços de inteligência) são as escolhas estruturais feitas no momento da criação dessas agências. Essas escolhas estruturais envolvem não apenas o desenho organizacional, mas principalmente o conjunto de regras formais e costumes quase-legais que delimitam suas missões e métodos de atuação.¹²

¹⁰ Para uma avaliação dos desdobramentos mais recentes ver: CEPIK, Marco. (2001). “Terrorismo, Inteligencia y Brasil”. *Argentina Global: Boletín On-Line sobre Relaciones Internacionales*. Numero Especial 2, Diciembre 2001. [<http://www.geocities.com/globargentina>].

¹¹ Um exemplo desse tipo de viés: não obstante a legislação australiana vetar o engajamento do serviço de segurança (*Australian Security Intelligence Organization – ASIO*) em operações que violem os direitos dos cidadãos manifestarem-se livremente contra o governo, o mandato do ASIO prevê o uso de medidas preventivas contra o crime de “sedição”, ou seja, a promoção de “hostilidade entre diferentes classes de súditos de Sua Majestade”. As implicações dessa relíquia da lei criminal britânica no contexto contemporâneo, na medida em que “classes de súditos” sejam entendidas como categorias “sócio-econômicas” representadas por organizações e partidos, vão desde uma autorização potencial para a vigilância de sindicatos e grupos socialistas, até a expectativa absurda de que todos os conflitos distributivos sejam igualmente acompanhados pelos serviços de inteligência de segurança. Cf. LUSTGARTEN e LEIGH (1994: 405-410).

¹² ZEGART, Amy. (1999). *Flawed by Design: The Evolution of the CIA, JCS and NSC*. Stanford-CA, Stanford University Press.

Ao avaliar os desafios relacionados ao controle do público sobre as atividades de inteligência em contextos de transição e consolidação democrática, Thomas Bruneau (2000:01-36) destacou três tipos de escolhas que seriam decisivas e que deveriam constar do mandato legal do setor: 1) A primeira escolha envolveria determinar em quais áreas de especialização da atividade de inteligência o governo deveria investir (*humint, sigint, imint, análise, contra-inteligência, operações encobertas etc.*), quantas organizações deveriam ser criadas para as diferentes missões e qual o volume de recursos que o país deveria dedicar para a montagem de um sistema nacional de inteligência. 2) A segunda escolha estaria relacionada ao peso relativo (nas esferas de produção e de consumo) das organizações militares e das organizações civis de inteligência, bem como o grau de controle ou autoridade formal que os militares terão sobre os recursos humanos, tecnológicos e orçamentários do setor. 3) O terceiro tipo de escolha refere-se à relação considerada desejável entre inteligência e políticas governamentais (*policymaking*).¹³

Enfim, os três tipos de escolhas têm conseqüências para o controle externo das atividades de inteligência e, uma vez traduzidos em ordenamentos legais e mandatos, tendem a durar no tempo ainda que sejam sujeitos a interpretações políticas ou até mesmo judiciais.

II – Dispositivos Legais Presentes nos Seis Países:

Embora os seis países pesquisados apresentem algum tipo de regulamentação legal das atividades de inteligência praticadas pelos seus respectivos governos, o grau de detalhamento e a abrangência organizacional dos mandatos legais variam muito em cada caso. De modo geral, entretanto, estes regulamentos (leis, decretos executivos, portarias administrativas etc.) chegam, no máximo, a tratar dos problemas associados à chamada inteligência de segurança (*security intelligence*). Especialmente no que diz

¹³ Cf. Thomas C. Bruneau, "Controlling Intelligence in new democracies," *International Journal of Intelligence and CounterIntelligence* 14, no. 3 (Fall 2001): 323-341.

respeito aos limites da atuação dos serviços de inteligência interna contra os cidadãos do próprio país quando não há suspeita razoável de envolvimento destes cidadãos em atividades que ameacem a segurança do Estado ou de seus concidadãos.

Em relação à componente da inteligência interna que nos interessa mais diretamente aqui (a chamada *criminal intelligence* ou inteligência de segurança pública – ISP), foi muito difícil identificar alguma regulamentação legal específica. Com a exceção parcial do Canadá e da África do Sul que contam com serviços nacionais de ISP, as capacidades dos outros países nesta área é parte integral do aparato policial e não recebe o mesmo tipo de atenção que a outra grande componente do sistema de inteligência atuando no âmbito interno dos países. Esta limitação é muito mais evidente quando se vai do nível central de governo para os níveis estaduais / provinciais e/ou locais.

No restante desta seção foram descritos brevemente os resultados obtidos a partir de pesquisa bibliográfica, documental e nas páginas institucionais na Internet. Para o caso dos governos locais e/ou estaduais / provinciais, um maior detalhamento dependeria de trabalho de campo direto e entrevistas com os dirigentes das unidades de ISP em diferentes países. De todo modo, na tabela ao final da seção foram sistematizados de forma comparativa os resultados a que se pode chegar até aqui.

Estados Unidos

A principal base legal para as atividades de inteligência do governo dos Estados Unidos é o *National Security Act of 1947*, cujos contornos básicos vêm sendo atualizados por meio de emendas ao longo de mais de cinquenta anos. Este ato, que corresponde também ao título 50 do *U.S. Code*, estabelece genericamente que inteligência significa o conjunto de “*informações relativas às capacidades, intenções e atividades de governos, organizações ou indivíduos estrangeiros*”. Ele fixa então como mandato da CIA a coleta de inteligência a partir de “*fontes humanas e outros meios apropriados, sendo que a agência não terá poderes de polícia, subpoena ou de*

imposição da lei, assim como não deveria exercer funções de segurança dentro do país”.

Apenas depois de 1981, como resultado de longas disputas sobre o significado e a abrangência desse mandato, a *Executive Order 12333* estabeleceu os tipos de informações que a CIA deveria coletar, analisar e disseminar sobre alvos estrangeiros, além de explicitar pela primeira vez que a agência também era encarregada das operações de contra-inteligência no exterior e das operações encobertas (chamadas nessa *executive order* de *special activities*). Além de detalhar os objetivos, tipos de informações e técnicas de coleta passíveis de serem utilizadas pela CIA, a *Executive Order 12333* também explicita as funções e alvos que são vedados à atuação da agência. Mais importante do que esse detalhamento, no entanto, foi o fato de que essa *executive order* pela primeira vez especificou publicamente as missões e áreas de atuação de uma série de outras agências de inteligência norte-americanas que não haviam sido criadas por lei, mas por decisão administrativa secreta do poder executivo.¹⁴

Dentre a legislação mais recente introduzida pelo Congresso, destaca-se o USA *Patriot Act of 2001*, a lei anti-terror aprovada logo depois dos atentados de 11 de Setembro de 2001 e que ampliou enormemente os poderes das agências federais de imposição da lei (*law enforcement*) e de obtenção de inteligência. Juntamente com a criação do novo ministério da segurança do território (*Department of Homeland Security* – DHS) e a reorganização do FBI, CIA e Departamento de Defesa, o PATRIOT Act tem sido encarado pelo governo americano como um importante instrumento para superar um conjunto persistente de barreiras doutrinárias e operacionais entre investigação criminal e inteligência.¹⁵

¹⁴ U.S. CONGRESS. (1998). *Compilation of Intelligence Laws and Related Laws and Executive Orders of Interest to the National Intelligence Community*. Washington-D.C., GPO, 1998. Páginas 03-45 (*National Security Act of 1947*) e páginas 729-740 (*Executive Order 12333 of 1981*).

¹⁵ Ver: www.fas.org/irp/offdocs/laws/index.html.

Canadá

O diploma legal mais importante regulamentando as funções de inteligência do Canadá é o *Canadian Security Intelligence Service Act* (1984). O mesmo ato também instituiu o *Security Intelligence Review Committee* (SIRC), um comitê independente, ligado ao poder executivo e não diretamente ao parlamento, mas que tem a missão de supervisionar as atividades do CSIS. O SIRC tem autoridade para acessar quaisquer informações manejadas pelo CSIS que sejam relevantes para sua função de supervisão, com exceção de casos especiais de investigações solicitadas pelo Conselho de Estado da Rainha. Como resultado de sua atividade, o SIRC deve apresentar um relatório anual ao Parlamento, além de relatórios eventuais em casos específicos. Ainda no âmbito do controle externo, o Ato de 1984 estabeleceu outro órgão interno ao governo para fiscalizar a comunidade de inteligência: o escritório do Inspetor-Geral do CSIS (IG-CSIS). O IG-CSIS responde institucionalmente perante o *deputy solicitor general* e tem como atribuição elaborar um relatório anual ao *solicitor general*, que por sua vez deverá apresentá-lo como documento público ao Parlamento.¹⁶

Mais recentemente, na sequência dos atentados de 11 de setembro de 2001 nos Estados Unidos, o Parlamento do Canadá adotou uma nova legislação referente ao papel da inteligência no combate ao terrorismo. Esta legislação, conhecida como *Anti-Terrorism Act*, foi sancionada pela Rainha em 18 de dezembro de 2001. Dentre outras medidas, esta lei permite a prisão (sem mandado judicial) de suspeitos por até 72h sem acusação formal, amplia o tempo de interceptação telefônica autorizada judicialmente para 12 meses, autoriza a interceptação de fluxo telefônico e de *e-mails* entre canadenses e estrangeiros suspeitos de terrorismo, além de flexibilizar as exigências de “plausibilidade e imediaticidade da ameaça” até então existentes para que os oficiais de

¹⁶ A lei de criação do CSIS e dos demais órgãos está reproduzida como anexo ao final do texto.

inteligência e autoridades policiais possam vigiar e monitorar os suspeitos de atividades terroristas.¹⁷

No mesmo período o governo canadense também aumentou significativamente seu orçamento de segurança nacional. Dentre as organizações que se beneficiaram destes novos recursos orçamentários estão justamente a Real Polícia Montada do Canadá (RCMP) e o Serviço de Inteligência Criminal (CISC). No caso da RCMP, vale notar o uso destes recursos para, dentre outras iniciativas, criar os novos 'times integrados' de segurança nacional e de fronteira: os *Integrated National Security Enforcement Teams* (INSETS) e os *Integrated Border Enforcement Teams* (IBETS). Estes novos desdobramentos legais e operacionais são coerentes com a atual doutrina canadense de policiamento 'liderado' pela inteligência.¹⁸

Alemanha

As três leis ordinárias federais alemãs mais importantes na regulamentação das atividades de inteligência em geral e de ISP em particular são a lei de criação da polícia federal (BKA), promulgada em 1951, a lei de criação da guarda de fronteiras (BGS), também promulgada em 1951, e a lei de criação do Serviço Federal de Proteção à Constituição (BfV), promulgada em 1950. Dentre os poderes concedidos ao BfV por esta lei, está o de investigar pessoas suspeitas de atos violentos contra as autoridades, prédios, conjuntos informacionais e operações do governo federal, proteger as informações governamentais contra tentativas de espionagem, sabotagem e terrorismo, bem como apoiar as organizações policiais no combate ao crime organizado.¹⁹

¹⁷ Disponível em inglês e francês: http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_4/90168bE.html#1.

¹⁸ Cf. http://www.rcmp-grc.gc.ca/index_e.htm e também <http://www.sgc.gc.ca>.

¹⁹ Conhecido como BverfSchG, esta lei pode ser encontrada na página da Federação dos Cientistas Americanos (FAS). Ver: <http://fas.org/irp/world/germany/docs/bverfg.htm>.

A legislação alemã referente ao controle parlamentar das atividades de inteligência (*Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes – PKK Gesetz*) foi introduzida pelo parlamento alemão em 1978. Regulações sobre a atuação do BND e do MAD foram introduzidas em 1990.²⁰

Em dezembro de 2001 o Parlamento alemão aprovou nova legislação que permite ao governo a suspensão das garantias constitucionais para as organizações suspeitas de “promover o extremismo ou ideais que possam ser relacionados com o terrorismo”. A nova lei permite ao governo monitorar as comunidades islâmicas participantes de mesquitas ou grupos de oração. No mesmo mês, uma segunda lei antiterror foi aprovada visando a aumentar o poder das agências de inteligência e melhorar as trocas de informações entre elas, bem como para melhorar o controle de fronteiras e a capacidade dos órgãos governamentais localizarem terroristas vivendo na Alemanha ou em trânsito pelo país. A mesma lei, segundo HENDERSON (2003:72), permitiu a presença de seguranças armados nas aeronaves comerciais alemãs.²¹

Itália

Na Itália, a Lei 801, de 24 de outubro de 1977, dispõe sobre a instituição e ordenamento dos serviços de inteligência e de segurança do país e disciplina o segredo de Estado. A legislação de 1977 criou o Serviço para a Informação e a Segurança Militar (SISMI), subordinado ao Ministério da Defesa e encarregado da produção de inteligência de defesa e também da contra-espionagem. Também foi criado o Serviço para a Informação e Segurança Democrática (SISDE), cujo objetivo é assegurar a ordem constitucional, contra qualquer atentado e forma de subversão. Este serviço está subordinado ao Ministro do Interior.

²⁰ A legislação completa sobre a inteligência alemã encontra-se disponível (apenas em alemão) no seguinte *site* não oficial: <http://www.geheimdienste.org/recht.html>.

²¹ Cf. HENDERSON, Robert. (2003). *International Intelligence Yearbook*. Washington, Brassey's.

No tocante ao controle externo, a lei 801 determina, no artigo 11, que o governo deverá apresentar semestralmente ao Parlamento um informe escrito com a política de inteligência e de segurança. A supervisão às atividades de inteligência é prevista, pela lei, para ser exercida por uma comissão parlamentar composta de quatro deputados e quatro senadores. Esta comissão pode requerer do Presidente do Conselho de Ministros e da Comissão Interministerial para a Informação e Segurança informações a respeito das linhas essenciais da estrutura e da atividade dos serviços, bem como pode formular propostas. As solicitações podem ser recusadas pelo Presidente do Conselho de Ministros se consideradas lesivas à atividade dos Serviços.

No combate ao crime organizado, a Itália conta com a Lei 410/1991, que aprova decreto do Presidente do Conselho de Ministros que dispõe sobre condições de emergência para a coordenação de inteligência e de investigações contra o crime organizado. Esta é a legislação que mais se aproxima de um mandato legal italiano no caso de ISP. A legislação dispõe, ainda, que a colaboração entre o SIDE e o SISMI deverá ser sempre recíproca, bem como entre todos oficiais e agentes da polícia judicial.

Além disso, o governo italiano tem a obrigação de informar semestralmente ao Parlamento, através de uma relação escrita, a sua política de informação e segurança, bem como os resultados obtidos com a mesma. O controle externo dos organismos de inteligência da Itália ocorre de três formas: político, parlamentar e ministerial. Os segredos de Estado são considerados como todas as informações que podem prejudicar o Estado democrático. Portanto, existe legislação que obriga os oficiais, agentes e os delegados do serviço público a se absterem de depor e de serem interrogados nos assuntos que digam respeito a temas ligados à segurança nacional.

Desde 1995, o SISDE possui como mecanismo de transparência a revista *Per aspera ad veritatem*, que é distribuída a vários órgãos, universidades, organismos

internacionais e nacionais, contendo ensaios, entrevistas e artigos sobre serviço de inteligência de segurança.²²

Mais recentemente, a Lei 25/1997 forneceu uma moldura institucional para a unificação e a racionalização da busca de inteligência de sinais eletrônicos por parte da agência militar de *sigint*. E a Lei 78/2000, por meio da qual foi acelerada a reforma do corpo de Carabinieri, colocou esta força constabular no mesmo nível das outras forças armadas do país, concedendo mandato mais amplo no uso de capacidades de inteligência para a garantia de 'segurança interna'.²³

Israel

A estrutura de inteligência criminal de Israel corresponde ao Departamento de Inteligência da Polícia Israelense, subordinado ao Ministério da Segurança Pública. Criado em 1997, o Departamento de Inteligência realiza a coleta, avaliação e distribuição de inteligência relativa ao combate ao crime organizado, à manutenção de ordem pública e à segurança interna. O Departamento de Inteligência elabora um relatório anual acerca do trabalho de inteligência da Polícia Israelense com o objetivo de planejar e conduzir operações em todos os territórios controlados por Israel. O Departamento de Inteligência da Polícia tem por missão prover aos dirigentes da polícia israelense e os comandantes de operações informações sobre atividades criminais de todos os tipos, como ameaças à ordem pública e atividades terroristas. Entretanto, não foi possível identificar uma legislação específica de ISP no caso israelense.²⁴

Em termos de mandato legal, a Lei sobre Segurança das Organizações Públicas, de agosto de 1998, regulamenta a atividade do MALMAB, o serviço de segurança que opera sob a direção do Ministério da Defesa. Embora vinculado ao Ministério da

²² Para maiores detalhes sobre a legislação e a jurisprudência italiana na área de inteligência, basta seguir os links correspondentes no site oficial da Revista do SISDE: <http://www.sisde.it>.

²³ Cf. HENDERSON (2003:105).

²⁴ Cf. http://www.police.gov.il/english/AboutUs/Structure/04_en_inteli.asp.

Defesa, o Malbad também realiza investigações criminais sobre desvios de conduta dos membros das forças armadas e, em decorrência, os produtos do seu trabalho são relevantes para as capacidades de contra-inteligência e de ISP de Israel. Vale lembrar que em Israel a condenação por traição pode implicar a sentença de pena de morte.

Em fevereiro de 2002 foi aprovada a Lei sobre o Serviço de Segurança Geral (SHIN BET), a primeira lei do tipo em mais de cinquenta anos do funcionamento do sistema de inteligência israelense. Por meio desta lei foi fixado um mandato de cinco anos para o diretor do serviço (o qual pode ser estendido no máximo por mais um ano) e definiu-se pela criação do subcomitê de inteligência da comissão de defesa e relações exteriores do Knesset.²⁵

África do Sul

A principal regulamentação da atividade de inteligência na África do Sul é dada pelo *Intelligence Services Act 1994*, que criou a *National Intelligence Agency* (NIA) e o *South African Security Service* (SASS), substituindo o aparato nacional de inteligência do regime de Apartheid. Complementarmente ao *Intelligence Service Act 1994*, o *National Strategic Intelligence Act 1994* (conhecido como NSIA) estabeleceu as funções dos membros da comunidade de inteligência, criando também o *National Intelligence Coordinating Committee* (NICOC).²⁶

Em matéria de ISP, a definição adotada pela África do Sul, nos termos do *National Strategic Intelligence Act 1994* (Seção 1, parágrafo vii), a caracteriza como “inteligência utilizada na prevenção ao crime ou na condução de investigações

²⁵ A seção mais controversa desta lei, permitindo o uso de “pressão física moderada” em interrogatórios de suspeitos de terrorismo, foi retirada pelo governo depois de uma avalanche de protestos. Formalmente, a tortura foi banida dos interrogatórios israelenses desde 1984, mas esta prática continua até hoje, mesmo depois da Suprema Corte de Israel ter proibido qualquer tipo de tortura ou pressão física em decisão tomada em 1999. Ref. *Financial Times*, London, February 12, 2002.

²⁶ O texto completo destas duas leis está disponível em: <http://www.fas.org/irp/world/rsa/index.html>.

criminais, bem como para preparar evidências com o objetivo de garantir o cumprimento da lei e processar judicialmente os violadores da lei”.

O NSIA confere mandato legal ao *South African Police Service* para promover a coleta, processamento, validação, análise e emprego da inteligência criminal em apoio às funções do Serviço, em conformidade com a seção 215 da Constituição. O NSIA também atribui ao SAPS a função de contra-inteligência para proteger as capacidades de inteligência da polícia contra as tentativas de infiltração do crime. Finalmente, o mesmo estatuto atribui ao SAPS a tarefa de prover inteligência sobre crime e ordem pública para o NICOC. Em 2002, o Parlamento sul-africano aprovou um *National Strategic Intelligence Amendment*, o qual expandiu algumas missões do SAPS na área de contra-inteligência fora do território do país, mas que não alterou substantivamente o desenho atual do sistema nacional de inteligência sul-africano.

Quanto ao controle externo, a supervisão à atividade de inteligência é prevista pelo *Committee of Members of Parliament and Inspectors General of Intelligence Act* de 1994. Este ato instituiu um comitê parlamentar de acompanhamento, o *Joint Standing Committee on Intelligence* (JSCI). Formado por 11 parlamentares, o Comitê pode ter acesso ao orçamento destinado aos serviços de inteligência e pode também ter acesso a certos documentos classificados. O Comitê pode convocar para testemunhar-lhe seja um Ministro, seja algum diretor de algum Serviço da comunidade de inteligência.²⁷

²⁷ Cf. TODD, Paul & BLOCH, Jonathan. (2003). *Global Intelligence: The World's Secret Services Today*. London, Zed Books. Especialmente o capítulo 7 (“Intelligence in the South: the growth of the virtual state”). Páginas 165-206.

Tabela 1: Comparativo da Legislação nos Seis Países:

| | Estados Unidos | Canadá | Alemanha | Itália | Israel | África do Sul |
|--|--|--|---|---|--|---|
| Existe mandato legal | Sim | Sim | Sim | Sim | Sim | Sim |
| Lei atinge intel interna e externa | Sim | Não | Sim | Sim | Não | Sim |
| Lei regula intel criminal (ISP) | Não | Parcialmente | Não | Não | Não | Parcialmente |
| Mandato legal definido em lei e/ou apenas por decisões do Executivo | Definido em lei e especificado por decisões executivas | Definido em lei e especificado por decisões executivas | Lei Aprovada no Parlamento | Lei Aprovada no Parlamento | Decisão Executiva | Definido em lei e especificado por decisões executivas |
| Definição da missão de Inteligência Interna (<i>security e criminal</i>) | FBI (CI, Anti-Subversão, CT e ISP) | CSIS (CI, anti-subversão e CT) e CISC (ISP e CT) | BfV (CI, anti-subversão e CT) e BKA (ISP, CT e Intel Financeira) | SISDE (CI, anti-subversão e CT) e Polizia di Stato (ISP, CT e Intel Financeira) | SHIN BET (CI, anti-subversão e CT) e Polícia Nacional (ISP, CT e Intel Financeira) | NIA (CI, anti-subversão e CT) e SAPS (ISP e CT). |
| Mecanismos de controle externo | Comitês Parlamentares (HPSCI, SSCI) e comissão presidencial (PFIAB) e Inspetorias. | Comissão Independente (SIRC) e Inspetor-Geral | Comissão Parlamentar Bundestag (PKK) e Comissão Interceptações (G-10) | Comitê Parlamentar (CoPaCo) | Sub-comitê seletor dos serviços secretos (Knesset) | Comitês Parlamentares (JSCI, JSCD) e Inspetoria Geral de Intel (IGIS) |
| Poder do órgão avaliador externo ²⁸ | alto | médio | alto | médio | Baixo | médio |
| Avaliação do desempenho das agências? ²⁹ | intensa | Média | fraca | fraca | Fraca | média |

²⁸ Por exemplo: aprova orçamento; aprova nomes dos dirigentes; solicita/avalia relatórios; convoca depoimentos; autoriza operações *ex ante*; julga ações *ex post*; requisita qualquer informação etc.

²⁹ Por exemplo, relatórios periódicos de atividades; declaração formal de satisfação dos usuários; indicadores qualitativos ou quantitativos de produção; verificações de qualidade analítica.

III – Organização de Inteligência e ISP em Seis Países:

Obviamente, o grau de complexidade organizacional de cada sistema nacional de inteligência varia muito, indo desde sistemas com dezenas de agências, como os Estados Unidos e a Rússia, até países como Canadá e Itália, que têm um número bem menor de agências principais. Não existe um “modelo ideal” de organização dos sistemas nacionais e dos subsistemas setoriais de inteligência, mas sempre se pode aprender algo da observação das semelhanças e diferenças entre os casos nacionais.

Estados Unidos

Nos Estados Unidos, a *U.S. Intelligence Community* (IC) abrange quatorze organizações principais, além das instâncias de coordenação que estão ligadas ao escritório do Diretor Central de Inteligência (DCI).³⁰

O *Director of Central Intelligence* (DCI) ocupa legalmente o vértice do "sistema" e desempenha três papéis principais: coordena a IC, dirige a CIA e assessora o Presidente e o Conselho de Segurança Nacional na área de inteligência. O DCI possui dois adjuntos, um para a direção da CIA e, desde 1996, outro para o gerenciamento da comunidade. Estão ligadas também ao DCI quatro instâncias colegiadas superiores da IC: o *National Intelligence Council* (NIC), o *National Foreign Intelligence Board* (NFIB), o *Intelligence Community's Executive Committee* (IC/EXCOM) e o *Community Management Staff* (CMS). Pode-se dizer que o NIC e o NFIB dão suporte ao DCI no seu papel de principal assessor governamental de inteligência, enquanto o CMS e o EXCOM apóiam o DCI na sua função gerencial de coordenador do sistema.

³⁰ Para uma visão geral mais detalhada do sistema nacional de inteligência dos Estados Unidos, ver: RICHELSON, Jeffrey T. (1999). *The U.S. Intelligence Community*. Cambridge-MA, Ballinger Publishing. Quarta edição revisada e ampliada. Os sites oficiais das agências são listados com links atualizados em: <http://www.loyola.edu/dept/politics/intel.html>.

A principal componente da IC é formada por quatro agências nacionais de busca e coleta de inteligência externa (*foreign intelligence*), a saber, a *Central Intelligence Agency* (CIA) para as áreas de operações encobertas e *humint*, a *National Security Agency* (NSA) na área de *sigint* e segurança de informações, a *National Imagery and Mapping Agency* (NIMA) na área de *imint* e o *National Reconnaissance Office* (NRO), responsável pelo desenvolvimento e aquisição de satélites de *sigint*, *imint* e outras plataformas e sistemas especializados para uso das forças armadas e das agências nacionais de coleta. A instância nacional para o trabalho de análise e produção de inteligência para o governo norte-americano é o diretório de inteligência (análise) da CIA. Relatórios anuais sobre temas e áreas vitais (*estimates*) são produzidos colegiadamente no *National Intelligence Council* (NIC) dirigido pelo DCI. No âmbito “ministerial”, o trabalho de análise é feito por escritórios de inteligência nos departamentos de Defesa, Estado, Tesouro, Justiça, Energia, Comércio e Transportes. Esses escritórios participam das instâncias colegiadas da IC e respondem administrativamente aos titulares dos órgãos aos quais eles servem.

O caso do Departamento de Defesa necessita um comentário adicional. Além de subordinar três das quatro agências nacionais de inteligência (NIMA, NSA e NRO), o Pentágono conta ainda com a *Defense Intelligence Agency* (DIA), que contém um diretório de espionagem, o *Defense Humint Service* (DHS). Além da DIA, o Pentágono tem ainda o *Defense Airborne Reconnaissance Office* (DARO), a *Defense Threat Reduction Agency* (DTRA), a *Defense Information Systems Agency* (DISA) e o *Defense Security Service* (DSS). Todas essas são consideradas agências de suporte ao combate, mas enquanto a DIA e o DARO têm missões primárias na área de inteligência, a DTRA, a DISA e o DSS têm suas missões primárias na área de segurança. Além dessas organizações centrais do departamento de Defesa, o subsistema militar de inteligência é formado ainda pelo *Army Intelligence and Security Command* (INSCOM) do exército, pelo *Office of Naval Intelligence* (ONI) e pelo *Naval Security Group Command* (NSGC) da marinha, pela *Air Intelligence Agency* (AIA) da aeronáutica e a *Marine Corps Intelligence Activity* (MCIA) dos fuzileiros navais. Capacidades orgânicas são também articuladas em torno dos *Joint Intelligence Centers* (JIC's) dos nove comandos centrais unificados (Atlântico, Central, Europeu, Pacífico,

Sul, Espaço, Operações Especiais, Estratégico, Transportes), além de instituições de treinamento e formação acadêmica (nível de graduação e mestrado) em inteligência e segurança nacional, tais como o *Joint Military Intelligence College* (JMIC), a *National Defense University* (NDU) e a *Naval Post-Graduate School* (NPS).

A principal agência norte-americana nas áreas de contra-inteligência e de inteligência de segurança é o *Federal Bureau of Investigation* (FBI), por meio de sua divisão de segurança nacional (anteriormente chamada de divisão de inteligência). As forças armadas, a guarda costeira e o secretário de defesa possuem suas próprias organizações de segurança e contra-inteligência. No âmbito dos Departamentos de Justiça, de Segurança do Território (*Homeland Security*) e dos departamentos de polícia estaduais e locais nota-se a formação de um subsistema de inteligência policial ou criminal, cujo contorno será especificado logo depois desta descrição geral do sistema.

Finalmente, o controle externo da IC é exercido pelo próprio presidente da República, através do *Presidential Foreign Intelligence Advisory Board* (PFIAB), mas principalmente pelos comitês de inteligência do Senado (*Senate Select Committee on Intelligence* - SSCI) e da Câmara (*House Permanent Select Committee on Intelligence* - HPSCI).

Os gastos do governo federal dos Estados Unidos com inteligência (definida *stricto sensu*) comprometeram 1,6% do orçamento nacional no ano fiscal de 1999. Mas esta porcentagem representa um valor absoluto enorme segundo qualquer parâmetro internacional. De maneira inédita e que não se repetiria nos anos seguintes, a Casa Branca divulgou oficialmente em 1997 que o agregado orçamentário das atividades de inteligência para o ano fiscal de 1998 havia sido fixado pelo Congresso em 26,7 bilhões de dólares. Estima-se extra-oficialmente que, para o ano de 2003, tenham sido aprovados gastos federais da ordem de mais de 30 bilhões de dólares. Os gastos estaduais e locais com inteligência não são estimados, mas, considerando-se a existência de 15 mil forças policiais diferenciadas organizacionalmente nos Estados Unidos, é razoável supor que o gasto público total com atividades de inteligência naquele país seja bem maior do que o agregado federal.

Voltando então ao tema específico do subsistema de ISP, no caso dos Estados Unidos, embora ISP seja algo menos coerente e regulamentado em termos legais do que o sistema nacional (*Intelligence Community* – IC) é cada vez mais evidente o peso deste subsistema nos últimos anos.

No plano federal, tanto para a área de ameaças internas (*security intelligence*) quanto para a área de inteligência sobre crime (*criminal intelligence*) destacam-se os componentes subordinados ao diretor do FBI (*Federal Bureau of Investigation*), subordinado ao Departamento de Justiça. Na atual configuração institucional do FBI, estes componentes são atualmente descritos na página do Bureau na Internet (www.fbi.gov) como sendo o *Office of Intelligence* e as divisões de Contra-Inteligência e de Contra-Terrorismo. No quadro atual de atuação do governo federal dos Estados Unidos, as fronteiras entre ameaças externas e internas são cada vez mais tênues, especialmente nas áreas de combate ao terrorismo, narcotráfico e crime organizado, que são as três áreas prioritárias dos organismos de inteligência doméstica naquele país.

Ainda no âmbito do Departamento de Justiça, tanto o *Bureau of Prisons* (BOP), por meio da unidade de inteligência do seu *Correctional Services Branch*, quanto a *Drugs Enforcement Administration* (DEA) são decisivos na estruturação de um subsistema de ISP para aquele país. No entanto, a DEA não deve ser considerada primordialmente uma agência de inteligência, mas sim uma polícia especializada com uma divisão de inteligência para apoiar suas missões. ³¹

Cabe destacar aqui o papel de dois centros federais especializados que são integrados por centenas de funcionários de várias agências e que prestam serviços para todo o sistema, não apenas no âmbito federal, mas também no estadual e local: 1) O primeiro é o *National Drug Intelligence Center* (NDIC), criado em 1993 e situado em Johnstown-PA. 2) O segundo centro é o *El Paso Intelligence Center* (EPIC), criado em 1974 e situado no Texas. Enquanto o NDIC trabalha com análise estratégica do narcotráfico, violência de gangues e fluxos logísticos das drogas, a missão central do

³¹ Cf. www.bop.gov e também www.usdoj.gov/dea.

EPIC é relacionar tráfico de drogas, violações nas leis de imigração, tráfico de armas e explosivos, suspeitos fugitivos e roubos de veículos, barcos e aviões.³²

Criado em 2002, o Ministério da Segurança do Território (*Homeland Security Department* - DHS) não tem funções diretas de coleta de inteligência, mas como parte de suas atribuições e por força do Patriot Act ele centraliza e analisa todas as informações sobre ameaças terroristas. Assim, por meio de seu componente de *Information Analysis & Infrastructure Protection* são analisadas as informações sobre ameaças provenientes de agências nacionais (FBI, CIA, NSA etc), internacionais e locais, são emitidos alertas e são planejadas as respostas integradas.³³

Apesar do peso enorme das agências federais na montagem de um subsistema de ISP nos Estados Unidos, o componente propriamente criminalístico deste subsistema também foi sendo impulsionado pelas necessidades de cada departamento de polícia e pelas redes mais ou menos informais de cooperação entre as polícias.

Dentre os departamentos de polícia metropolitanos com componentes de inteligência criminal mais forte, pode-se mencionar o de Nova York (NYPD) e o de Los Angeles (LAPD), sendo que Los Angeles conta com um *Criminal Intelligence Group* para supervisionar as capacidades de busca e análise de informações por parte das divisões de crime organizado, narcóticos e antiterrorismo.³⁴

Uma rede estadual de inteligência sobre crime naquele país pode ser exemplificada com o caso da *Law Enforcement Intelligence Network* (LEIN) do estado de Iowa, criada em 1984. Embora a rede seja coordenada pelo Bureau de Inteligência do Departamento de Segurança Pública do governo estadual, desde 1994, todos os membros das polícias locais de condados e cidades e também das demais agências estaduais de imposição da lei [*law enforcement*] que passam por um curso de duas

³² Cf. www.usdoj.gov/ndic e também www.usdoj.gov/dea/programs/epic.htm .

³³ Cf. www.dhs.gov.

³⁴ Cf. www.nyc.gov/html/nypd e também <http://www.lapdonline.org>.

semanas são certificados como membros da LEIN e podem submeter relatórios de inteligência para alimentar o sistema de inteligência daquele estado.³⁵

Este modelo de organização da atividade de inteligência policial por redes colaborativas é bastante comum nos Estados Unidos em função do próprio sistema federal. As três redes mais abrangentes e importantes de inteligência criminal/policial nos Estados Unidos são: o programa RISS (ao qual estão ligados vários arranjos regionais), a FINCEN e a LEIU. No âmbito da inteligência nacional (de Estado como se diz no Brasil), destaca-se a rede INTELINK, sobre a qual também vale a pena mencionar algo. Entretanto, enquanto a FINCEN e o INTELINK são iniciativas federais coordenadas, respectivamente, pelo Departamento do Tesouro (USTREA) e pelo Diretor Central de Inteligência (DCI), o RISS é um programa muito maior e mais complexo em termos de gestão, programa este financiado pelo governo federal e que envolve mais de 6.600 agências de imposição da lei (*law enforcement*). Por sua vez, a LEIU é uma iniciativa das agências locais e estaduais, organizada de maneira horizontal, apoiada e parcialmente financiada pelo governo federal, mas não coordenada diretamente por nenhuma agência federal de governo e sim administrada de maneira cooperada pelos órgãos participantes. Vejamos então alguma informação adicional sobre o RISS, a FINCEN, a LEIU e o INTELINK.

Iniciado em 1973, o *Regional Information Sharing System* (RISS) foi criado por iniciativa de polícias locais e estaduais visando a compartilhar informações e promover a cooperação entre diferentes agências de combate ao crime organizado (<http://www.iir.com/riss>). Sua finalidade principal é fomentar a habilidade das agências estaduais e locais de justiça criminal para identificar, enquadrar (*target*) e remover conspirações e atividades criminais, para além dos limites jurisdicionais de cada agência. O programa RISS inclui troca de informações, análise conjunta e telecomunicações seguras. O RISS conta também com uma intranet para o trabalho em rede entre as agências de imposição da lei. Dentre os serviços opcionais prestados pelo

³⁵ Para a rede do estado de Iowa (LEIN), ver: www.state.ia.us/government/dps/intell/lein. Para uma visão mais detalhada sobre as redes estaduais de inteligência criminal/policial nos Estados Unidos, ver: <http://www.iir.com/Publications/SISMonograph.pdf>.

RISS estão incluídos fundos confidenciais, equipamentos para trabalho de investigação, assistência técnica e treinamento. O número de membros do programa RISS está em torno de 6.600 agências policiais de todo o território dos EUA, incluindo ainda algumas agências policiais no Canadá, Reino Unido e Austrália. O RISS é um dos programas mais importantes desenvolvidos atualmente pelo *Institute for Intergovernmental Research* (IIR), uma organização não-governamental de pesquisa e treinamento baseada na Florida, especializada em temas de segurança pública, justiça juvenil e questões de justiça criminal.³⁶

Financiado principalmente pelos departamentos de Justiça (DOJ) e de Segurança do Território (DHS), O IIR tem outros programas viabilizadores do próprio RISS, os quais são relevantes para um país como o Brasil conhecer e analisar neste momento em que se está definindo um modelo nacional de ISP. Cabe mencionar, por exemplo, o projeto relacionado com a regulação federal prevista pelo *Criminal Intelligence Systems Operating Policies* (28CFR23.1), a qual prevê que todos os programas de compartilhamento de inteligência entre agências locais, estaduais e federais financiados pelo governo federal sejam compatíveis com a privacidade e os direitos constitucionais dos indivíduos.³⁷ Vale mencionar também o trabalho do *Global Intelligence Working Group*, que elaborou em 2002, sob demanda da Associação Internacional de Chefes de Polícia (IACP), um conjunto de recomendações práticas para a formulação de planos nacionais, estaduais e locais de policiamento liderado por inteligência (*intelligence led policing*).³⁸ Estes dois projetos têm profundas implicações para se pensar o modelo brasileiro de ISP e a cooperação com outros países da América do Sul e de fora da região.

Estabelecida em abril de 1990, a *Financial Crimes Enforcement Network* (FINCEN) teve em princípio a missão de gerar inteligência de múltiplas fontes e manter uma rede analítica para apoiar mais diretamente a detecção, investigação e instrução

³⁶ Cf. www.iir.com.

³⁷ Cf. http://www.access.gpo.gov/nara/cfr/waisidx_03/28cfr23_03.html.

³⁸ Cf. <http://www.theiacp.org/documents/pdfs/publications/intelsharingreport.pdf>.

processual da acusação [*prosecution*] nos casos de lavagem de dinheiro levada a cabo no âmbito doméstico e no exterior, além de outros crimes financeiros e eletrônicos. Atualmente, além de prestar apoio às investigações das agências de imposição da lei e à cooperação internacional em matéria de combate aos crimes financeiros, a FINCEN produz avaliações de maior fôlego para os tomadores de decisões acerca das práticas, padrões e tendências da lavagem de dinheiro nos níveis doméstico e internacional. Além disso, cabe ao FinCEN, por exemplo, controlar os mais de 150 milhões de relatórios arquivados segundo as determinações do *Bank Secrecy Act* (BSA). Têm acesso a esses relatórios as agências locais, estaduais e federais de imposição da lei, as quais, através de um *Gateway Program*, acessam na base de dados autorizadas pelo BSA as informações relativas às altas movimentações financeiras em bancos dentro dos Estados Unidos, contas em bancos estrangeiros, atividades de cassinos etc. A FinCEN está integrada com a *Financial Action Task Force* (FATF) e com a *Caribbean Financial Action Task Force* (CFATF).³⁹

Finalmente, a *Law Enforcement Intelligence Unity* (LEIU) foi criada em 1956 com o objetivo de registrar e intercambiar informações criminais confidenciais sobre crime organizado, as quais antes não eram disponíveis pelos canais habituais de comunicação. Fontes extra-oficiais afirmam que a LEIU surgiu em um contexto em que o FBI era relutante em compartilhar informações sobre o crime organizado com agências de nível local. Nesse sentido, a LEIU veio a cumprir um papel de coordenação principalmente entre as agências locais e estaduais de imposição da lei (*law enforcement*) dos Estados Unidos e do Canadá, embora hoje em dia também inclua organizações policiais da África do Sul e da Austrália na cooperação. Focada, entretanto, nos dois países da América do Norte, a LEIU é dividida em quatro zonas geográficas: Ocidental, Central, Noroeste e Sudoeste, sendo em cada uma delas designado um diretor e um vice-diretor. A formulação da política da LEIU, bem como a admissão de novos membros passa pela alçada do seu *Executive Board*, o qual compreende oficiais nacionais, oficiais de zona, um ex-diretor, um conselheiro legal e um representante do *California Department of Justice* – sendo que esta secretaria

³⁹ Cf. www.ustreas.gov/fincen.

estadual de justiça e segurança pública do estado da Califórnia é que ocupa desde a criação da rede a função de Agência Central de Coordenação da LEIU e que é responsável por gerir o sistema informatizado da rede.⁴⁰

Estima-se que a LEIU contava com 250 agências pertencendo formalmente à rede no ano 2000. As agências estatais ou locais que pretendam nela ingressar devem ser dotadas de função de inteligência criminal e ter sua candidatura proposta por uma outra agência já integrante da rede. Além disso, é requerida a assinatura de três agências adicionais apoiando a nova adesão. Dos recursos compartilhados pela LEIU, pode-se mencionar um *pointer index* com nomes de fugitivos da justiça que pode ser consultado pelos membros da rede. Os analistas da LEIU podem checar informações solicitadas por seus membros acerca de indivíduos suspeitos e suas atividades. A LEIU realiza uma conferência anual e reuniões intermediárias por temas e/ou regiões.

Finalmente, cabe mencionar brevemente aqui o caso do INTELINK, a intranet da comunidade de inteligência (IC) dos Estados Unidos. O Intelink consiste numa arquitetura integrada de sistemas de serviços e de plataformas de disseminação dos produtos de inteligência das várias agências federais dos Estados Unidos⁴¹. Suas principais finalidades podem ser descritas como sendo a de interconectar produtores de inteligência e seus usuários, contribuir para a redução de trabalho duplicado entre diversas agências e serviços, fomentar a interoperabilidade e promover a modernização dos sistemas multimídia nos campos da computação e da comunicação. Reunindo as bases de dados de várias agências federais de inteligência (CIA, NSA, DIA, FBI, DEA etc), o INTELINK está organizado em cinco camadas de segurança e serviços com acesso hierarquizado (as camadas U, S, SCI, P e C). Assim, por exemplo, o INTELINK-S corresponde ao nível secreto da rede, justamente o que começou a se expandir mais rapidamente em termos de escopo e alcance. Segundo o *Intelink Service Management*

⁴⁰ Cf. <http://caag.state.ca.us/ag/aboutdoj.htm>.

⁴¹ Mesmo a página web central do INTELINK não é de acesso público. Para uma visão geral e não-oficial das funcionalidades, serviços, hierarquias de acesso e interfaces da intranet da comunidade de inteligência dos Estados Unidos, ver a página de Frederick Martin na Internet: <http://www.topsecretnet.com>. A referência completa do livro é: MARTIN, Frederick T. (1999). *Top Secret Intranet: How U.S. Intelligence Built Intelink*. Upper Saddle River-NJ, Prentice Hall.

Center, a rede Intelink compreende mais de 250 produtores distintos de inteligência e mais de 60 mil usuários com credenciais de acesso *top secret*, caminha para ter 250 mil usuários com credenciais de acesso no nível confidencial, além de reunir milhões de documentos e centenas de bases de dados acessíveis *online*.⁴²

Como foi possível notar até aqui, mesmo sem existir uma sistematização adequada sobre o conjunto de capacidades de inteligência nos Estados Unidos, especialmente no caso da chamada inteligência policial ou criminal, a especificação de um modelo brasileiro de ISP pode se beneficiar sobremaneira do conhecimento mais detalhado das inúmeras experiências federais, estaduais, locais e em rede existentes naquele país. Os outros cinco casos nacionais descritos a seguir são caracterizados por estruturas de inteligência (inclusive ISP) menos complexas e caras do que aquelas encontradas nos Estados Unidos, mas, ao menos em parte, é justamente por isso que o conhecimento destes casos nacionais é útil para o nosso país.

Canadá

O sistema nacional de inteligência do Canadá é formado por três componentes principais: o primeiro deles conformado pelas agências de inteligência militar, enquanto os outros dois componentes são formados por uma agência de inteligência interna (*security intelligence*) e um serviço de inteligência policial (*criminal intelligence*).⁴³

Os serviços de inteligência do Canadá são dirigidos política e operacionalmente pelo Comitê Interdepartamental de Segurança e Inteligência do *Privy Council Office* (PCO), órgão central de coordenação e formulação de políticas do gabinete de governo canadense. Integra também o PCO um *Intelligence Advisory Committee*. Este comitê é integrado pelos diretores das agências nacionais de inteligência, além de contar com

⁴² Cf. MARKS, Randy C. (s.d.). "*Intelink: The Intelligence Community's Classified Internet*". Material produzido pelo Intelink Service Management Center. Este material pode ser obtido em: <http://www.fas.org/irp/program/disseminate/docs/intelink.ppt>

⁴³ Para um detalhamento maior do papel de cada componente organizacional do sistema canadense, ver: http://www.pco-bcp.gc.ca/docs/Publications/si/si_e.pdf.

duas unidades internas: o *Security and Intelligence Secretariat* (SIS-PCO) e o *Intelligence Assessment Secretariat* (IAS-PCO). Ambas as unidades respondem a um vice-ministro do PCO para assuntos de segurança e inteligência (*Deputy Secretary to the Cabinet and Coordinator of Security and Intelligence*). Enquanto o SIS-PCO é responsável pela inteligência governamental e pela formulação da política de segurança, o IAS-PCO assessora e coordena a produção de avaliações em matéria política, econômica, estratégica e de segurança para o primeiro-ministro, para o Gabinete e para os oficiais seniores do governo.

Como em todos os países, as principais capacidades canadenses de obtenção e produção de inteligência estão sob controle do ministério da Defesa. A agência de *sigint* canadense é o *Communications Security Establishment / Centre de la Sécurité des Télécommunications* (CSE/CST), subordinada administrativamente ao Departamento de Defesa Nacional, embora responda politicamente ao PCO. O número de pessoal estimado da CSE é em torno de 1.000 oficiais, entre civis e militares. A agência tem quatro divisões: produção de *sigint*, desenvolvimento tecnológico, segurança de informações (INFOSEC) e serviços corporativos. O subsistema de inteligência militar do Canadá contém ainda uma divisão J-2 de inteligência para coleta e avaliação de inteligência para o Ministério da Defesa e para os comandantes das forças armadas, bem como para o Privy Council.⁴⁴

Embora o Canadá não possua uma agência própria separada para obtenção de inteligência externa, existem componentes analíticos voltados para a produção de análises e relatórios sobre temas de segurança nacional. Tais componentes estão situados principalmente no Departamento de Assuntos Internacionais e Comércio Exterior (DFAIT) e nos departamentos de imigração, alfândega e transportes.

A produção de inteligência doméstica na área de segurança do Estado é realizada pelo *Canadian Security Intelligence Service / Service Canadien du Renseignement de Sécurité* (CSIS/SCRS), criado na reforma de 1984. Esta reforma ocorreu depois de uma grande investigação sobre os abusos cometidos pelo serviço de

⁴⁴ Cf. www.cse.dnd.ca.

segurança da Polícia Montada (*Royal Canadian Mounted Police – RCMP*), quando então as funções de inteligência contra ameaças internas para a segurança do Estado e de contra-inteligência foram transferidas para uma organização civil submetida a controles externos mais estritos. Embora o CSIS não possua uma divisão ou departamento de inteligência externa, o órgão mantém pessoal de ligação com serviços semelhantes no exterior.⁴⁵

Na esfera da ISP, o *Criminal Intelligence Service of Canada / Service Canadien du Renseignements Criminels* (CISC/SCRC) é uma organização guarda-chuva que unifica as unidades de inteligência criminal das agências de execução penal do Canadá no combate ao aumento do crime organizado e outros crimes relevantes para o governo canadense. Criado em 1970, o CISC é dirigido por um funcionário civil com mandato de cinco anos, podendo se renovar por um período máximo de mais cinco anos.⁴⁶

O CISC possui dois níveis de participantes. O primeiro é restrito aos serviços permanentes de inteligência criminal das polícias municipais ou regionais, provinciais e federais, bem como às agências responsáveis pela execução dos estatutos provinciais e federais, tais como, por exemplo, a Polícia Montada, o Departamento de Defesa Nacional e a Alfândega. O segundo nível corresponde aos órgãos de execução legal dos estatutos federais ou provinciais que não possuem qualificações para o nível um de participação. O sistema possui uma agência central localizada em Ottawa, além de nove agências localizadas nas províncias. As unidades de inteligência fornecem às agências provinciais dados para futura análise e disseminação.

Na agência central existe um comitê, constituído de várias agências de nível um, que se reúne duas vezes ao ano para decidir as metas, prioridades e pontos de monitoramento. A agência central monitora o progresso das prioridades em cooperação com as nove agências provinciais que também se reúnem duas vezes ao ano com o diretor geral da CISC para discutir pontos relevantes acerca do crime organizado e recomendações ao comitê executivo. A agência central mantém um banco de dados

⁴⁵ Cf. <http://www.csis-scrs.gc.ca>.

⁴⁶ Cf. <http://www.cisc.gc.ca>.

computadorizado com atualizações em tempo real chamado ACIS (*Automated Criminal Intelligence Information System*). Todos os membros do CISC coletam, analisam e disseminam dados contribuindo para alimentar a base de dados do ACIS. As prioridades atuais do sistema canadense de ISP são o combate ao crime organizado asiático, o do leste europeu, o Italiano e as chamadas *outlaws gangs*, além desses também estão entre as outras prioridades o contrabando de cigarro e álcool, indústria de diamantes, tráfico de armas, crime tecnológico e exploração sexual. Como mecanismo de transparência e de controle de eficiência, o CISC publica anualmente um relatório sobre as dinâmicas criminais mais relevantes e em quais regiões elas se mostram mais ativas.⁴⁷

O controle externo sobre a inteligência no Canadá é exercido pelo *Security Intelligence Review Committee / Comité de Surveillance des Activités de Renseignement de Sécurité* (SIRC/CSARS), criado também em 1984 como um organismo governamental independente da comunidade de inteligência do país, com o objetivo de supervisionar as atividades do CSIS. Além do SIRC, dois outros organismos apresentam funções de supervisão interna e autofiscalização mais desenvolvidas. O escritório do Inspetor Geral do próprio CSIS fiscaliza a compatibilidade das atividades do CSIS com a legislação governamental, com as diretrizes ministeriais e com a política operacional do próprio CSIS.⁴⁸ Uma função semelhante de supervisão interna é exercida pelo Comissário interno do *Communications Security Establishment* (CSE).

Parte decisiva da explicação sobre por que o sistema de inteligência do Canadá é relativamente pequeno em relação ao seu território, PIB e gastos agregados com defesa é dada pela aliança formal nesta área com os Estados Unidos. Esta aliança se dá tanto por meio de acordos como o UKUSA (1947) e a NATO (1949), quanto por meio de uma comissão binacional de defesa permanente, em funcionamento desde 1940, ou mesmo em função da integração prática da defesa aérea dos dois países por meio do NORAD (1950) e do Comando Norte (2001).

⁴⁷ Cf. Para uma visão mais completa do trabalho recente do CISC, ver: <http://www.cisc.gc.ca/AnnualReport2003/Cisc2003/coverpage2003.html>.

⁴⁸ Cf. http://www.sgc.gc.ca/igcsis/index_e.asp.

Finalmente, vale observar que a divisão organizacional entre um serviço de inteligência criminal e outro de inteligência de segurança, verificada no caso canadense, representa uma tendência observada também no caso inglês.

Alemanha

Também no caso alemão o sistema nacional de inteligência é formado por três componentes principais. Mas, nesse caso, os componentes estão estruturados cada um em torno de uma ou duas agências principais para a inteligência civil externa (BND), para a inteligência militar (AfNBw / MAD) e para inteligência interna de segurança (BfV / BKA). Diferentemente dos casos britânico, canadense e sul-africano, não existe na Alemanha um serviço nacional de inteligência policial (*criminal intelligence*) separado organizacionalmente da agência de inteligência interna de segurança (*security intelligence*), embora este tipo de atividade seja exercido no âmbito da polícia federal daquele país.

O Serviço Federal de Inteligência (*Bundesnachrichtendienst* - BND) foi criado em 1956 e faz parte do Gabinete do Chanceler (chefe de governo da Alemanha), onde está subordinado ao Diretor de Inteligência do Gabinete, que coordena todas as agências federais de inteligência do governo alemão. O BND trabalha anualmente com um orçamento de cerca de 328 milhões de dólares e emprega cerca de 6.000 funcionários. Responsável pela espionagem internacional e pela produção analítica de relatórios sobre temas tais aspectos militares, políticas e econômicas de países relevantes para a Alemanha, além de análises sobre dinâmicas conflitivas internacionais (proliferação, narcotráfico, guerras, terrorismo etc.), o BND conta ainda com recursos para a interceptação de comunicações e sinais eletrônicos (as duas componentes da disciplina de *sigint*).⁴⁹ Ainda na área de inteligência externa, é relevante mencionar também o escritório federal de economia e controle de exportações (*Bundesausfuhramt* – BAFA), órgão subordinado ao Ministério da Economia e da Tecnologia, o qual entre outras

⁴⁹ Cf. www.bundesnachrichtendienst.de.

tarefas também coleta e analisa inteligência sobre proliferação de armas de destruição massiva, o contrabando de armas convencionais e outros ilícitos transfronteiriços.⁵⁰

O subsistema de inteligência militar da Alemanha tem sua organização principal localizada na 2ª Seção do Estado-Maior das Forças Armadas (*Amt für Nachrichtenwesen der Bundeswehr* (AfNBw)). Responsável pelo provimento de informações para o chefe do estado-maior e para os comandantes das grandes unidades, a AfNBw vem travando uma disputa burocrática com o BND na área de busca e coleta de inteligência externa sobre aspectos militares, a partir da criação (pela AfNBw) de um “comando de inteligência estratégica” que contaria com sua própria rede internacional de agentes independente do BND. A inteligência de sinais alemã é centralizada pelo *Amt für Fernmeldwesen Bundeswehr* (AFMBW), o escritório de monitoramento de sinais do Ministério da Defesa. Uma agência independente, o *Bundesamt für Sicherheit in der Informationstechnik* (BSI), que antes era parte do BND, é responsável pela segurança das comunicações e dos computadores contra ataques terroristas e espionagem eletrônica.

As funções de contra-inteligência militar são desempenhadas pelo *Militärischer Abschirmdienst* (MAD), o serviço de segurança das forças armadas que foi criado em 1956 e que recebeu sua atual denominação em 1984. Desde a promulgação da Lei de contra-inteligência militar em dezembro de 1990, o MAD é encarregado de monitorar e neutralizar as atividades dos serviços de inteligência das potências estrangeiras voltadas contra a Alemanha, bem como é encarregado de monitorar ameaças contra a Constituição do país. Além disso, o MAD interpreta informações para gerar avaliações da segurança do país e das forças armadas aliadas, e provê avaliações de segurança e precauções técnicas de proteção do material classificado. Organizacionalmente, o MAD é parte integrante das forças armadas, respondendo ao Inspetor Geral das Forças Armadas da Alemanha em relação aos temas de segurança orgânica militar. Finalmente, cabe mencionar que as forças armadas da Alemanha contam com

⁵⁰ Cf. www.bafa.de.

atividades de treinamento em inteligência por meio de uma escola dedicada exclusivamente ao treinamento em inteligência (SNBw).⁵¹

O terceiro pilar do sistema de inteligência da Alemanha tem como organização principal o Escritório Federal de Proteção da Constituição (*Bundesamt für Verfassungsschutz* - BfV), criado em 1950 para monitorar ameaças internas oriundas de organizações violentas de extrema direita e de extrema esquerda, bem como para combater a espionagem econômica contra a então Alemanha Ocidental, proteger os segredos de Estado e exercer as funções de contra-inteligência dentro e fora do país em coordenação estreita (nem sempre efetiva) com o BND. Subordinado ao Ministério Federal do Interior, atualmente o BfV conta com cerca de 2.200 funcionários e também é encarregado de identificar, vigiar e analisar as organizações criminosas e o narcotráfico. Entretanto, como o BfV não tem poderes de polícia, ele atua na área criminal fornecendo informações para a polícia federal alemã. A lei que dispõe sobre a cooperação entre os entes federados em matéria de proteção à Constituição regula o armazenamento, o processamento e utilização de dados relativos às pessoas, inclusive dos menores de idade. Mesmo que o BfV não possua poderes policiais, não podendo prender ou mesmo interrogar nenhum indivíduo, invadir propriedades e confiscar objetos, os dados obtidos por meio de vigilância, observação, escutas, agentes e fontes ostensivas servem muitas vezes em procedimentos legais como evidências importantes observados os limites legais e a necessidade de proteger fontes e métodos. Nos dezesseis estados alemães também existem escritórios estaduais de proteção à Constituição (*Landesamt für Verfassungsschutz* – LfV), cada qual subordinado ao governo do estado federado em questão.⁵²

Embora a Alemanha não tenha um serviço federal de inteligência criminal organizacionalmente separado da inteligência de segurança e/ou da polícia central (como ocorre no caso do Reino Unido e do Canadá), sua polícia federal (assim como o

⁵¹ Cf. <http://bundeswehr.de>. Ver também o *site* do Ministério da Defesa (*Bundesministerium der Verteidigung* - BNvG) localizado em: <http://www.bmvg.de>.

⁵² Cf. <http://www.verfassungsschutz.de>. Os relatórios anuais do BfV estão disponíveis neste *site* em alemão e inglês.

FBI dos Estados Unidos) possui responsabilidades e capacidades de inteligência voltadas especificamente para o combate ao crime. Criado em 1951, o *Bundeskriminalamt* (BKA) conta com cerca de 3.000 membros e investiga crimes federais ou incidentes que afetam dois ou mais estados (*Länder*). O BKA também é subordinado ao Ministério Federal do Interior e disputa jurisdição sobre vários temas com o BfV. Além de contar com seções especializadas para a proteção de autoridades e para a segurança do Estado, o BKA tem um esquadrão de investigações especiais com 600 efetivos, dedicado a investigar incidentes terroristas e outras formas de violência política. Em função da nova legislação sobre combate à lavagem de dinheiro e financiamento do terrorismo, introduzida pelo Parlamento alemão no começo de 2002, também foi criada recentemente no BKA uma unidade de inteligência financeira (FIU).

53

Além do BKA e do BfV, a Alemanha conta com unidades especializadas de combate clandestino e contra-terrorismo na sua polícia de fronteiras (*Bundesgrenzschutz* – BGS) e nas forças armadas (os comandos KSK do exército e os KFK da marinha).⁵⁴

Os três subsistemas de inteligência (externo, militar e de segurança) da Alemanha são supervisionados externamente por uma comissão parlamentar de controle criada pelo *Bundestag* (Parlamento da República Federal da Alemanha) em 1970. Esta comissão (PKK) de oito membros, representativa de todas as forças políticas presentes no *Bundestag*, deve enviar ao plenário do Parlamento um relatório no meio de cada legislatura e outro ao final de cada período. Comissões semelhantes existem em cada um dos legislativos estaduais. Além do PKK, o *Bundestag* ainda

⁵³ Cf. <http://www.bka.de>. Para um relatório anual da FIU/BKA em inglês, ver: http://www.bka.de/fiu/fiu_germany_annual_report_2002.pdf. Outros documentos relevantes estão disponíveis em alemão, inglês, francês e espanhol.

⁵⁴ Para uma visão geral da polícia federal de fronteiras do Ministério do Interior alemão (24.000 efetivos policiais e constabulares), ver: <http://www.bundesgrenzschutz.de>. O *site* de acesso às polícias estaduais da Alemanha é: <http://www.polizei.de>. Para informações sobre os antigos arquivos do Ministério da Segurança do Estado e da Polícia Política (STASI) da ex-Alemanha Oriental, ver inicialmente o *site* da chamada Comissão Gauck, subordinada ao Ministério do Interior da Alemanha e responsável pela guarda dos arquivos localizado em: <http://www.bstu.de>.

nomeia uma comissão independente (conhecida oficialmente como G-10), formada usualmente por oito membros que não são obrigatoriamente parlamentares, responsáveis por revisar e acompanhar as atividades de vigilância sobre telefones e e-mails levadas a cabo pelo BND, BfV e outras agências de inteligência alemãs.⁵⁵

Embora de maneira diferente do que o Canadá, também a Alemanha pode manter seu sistema nacional de inteligência relativamente pequeno durante a Guerra Fria em função de sua participação na OTAN e no Pacto de *Sigint* UKUSA (como 'terceira parte' e não como signatário direto). O afastamento diplomático entre os Estados Unidos e a Alemanha nos últimos dois anos em função dos contornos da guerra contra o terrorismo e da invasão do Iraque, apenas em parte foi compensado, e assim mesmo apenas na área de inteligência criminal, pelo aprofundamento da cooperação no âmbito da União Européia.

Itália

No caso da Itália, existem dois serviços de inteligência principais, resultantes da reforma do setor realizada em 1977, além de capacidades dispersas em vários departamentos ministeriais.

A principal instância coordenadora das capacidades de inteligência do Estado italiano é o Comitê Executivo para os Serviços de Informação e Segurança (*Comitato Esecutivo per i Servizi di Informazione e di Sicurezza – CESIS*), também instituído pela reforma de 1977. Este comitê funciona sob a presidência do conselho de ministros do governo italiano reunindo os chefes dos dois principais serviços e os diretores dos departamentos de inteligência dos principais ministérios envolvidos. Acima do CESIS, o arcabouço institucional italiano possui ainda um Comitê Interministerial para a Segurança e a Inteligência (CIIS), a máxima instância de coordenação de políticas de segurança nacional no país, dirigida pelo primeiro-ministro e composta pelos ministros da Defesa, dos Assuntos Exteriores, Justiça, Interior, Pesquisa Científica e pelo ministro

⁵⁵ Cf. http://www.bundestag.de/htdocs_e/orga/03organs/05othcomm/index.html.

das Finanças e Economia, além dos diretores dos dois serviços de inteligência e do secretário do CESIS. Ainda em termos de coordenação de políticas, é relevante mencionar o papel do Comitê Nacional para a Segurança e a Ordem Pública (CNOSP), criado em 1981 para coordenar o trabalho de todas as agências com responsabilidades no provimento de ordem pública, inclusive aquelas da área de segurança do Estado.⁵⁶

Na Itália, as áreas de inteligência externa e de inteligência militar são pouco diferenciadas organizacionalmente. A principal agência de inteligência externa do país é justamente o *Servizio per le Informazioni e la Sicurezza Militare* (SISMI), subordinado ao Ministério da Defesa. Além de prover informações sobre aspectos militares de outros países, ameaças transestatais e conflitos internacionais que afetam os interesses italianos, o SISMI também é encarregado de obter informações sobre aspectos políticos e econômicos de outros países, da contra-inteligência, da contra-espionagem e da busca de *sigint*. Além do SISMI, o Ministério da Defesa ainda controla uma agência de inteligência de defesa integrada por elementos das três forças armadas. Esta divisão de inteligência do Ministério da Defesa (chamada RIS) foi criada em 1998 e conta hoje com cerca de 2.000 funcionários. Também o Ministério dos Assuntos Exteriores tem uma unidade de análise e produção de relatórios de inteligência, mas esta unidade não está autorizada, como é o caso do SISMI, a realizar operações de *humint* e *sigint*.⁵⁷

Tampouco as áreas de inteligência de segurança e de inteligência criminal (ISP) são muito diferenciadas no caso italiano. A principal agência interna é o *Servizio per le Informazioni e la Sicurezza Democratica* (SISDE), criado em 1977 pela mesma lei que criou o SISMI. Com cerca de 1.500 funcionários, o SISDE é subordinado ao Ministério do Interior e tem como missões tradicionais a contra-inteligência, a contra-espionagem e o contra-terrorismo dentro do território italiano. De maneira semelhante ao BfV alemão, a principal justificativa para a manutenção do SISDE depois do final da Guerra

⁵⁶ Para uma visão mais detalhada das funções e da estrutura do CESIS, além de dados sobre o SISMI e o SISDE, ver: <http://www.serviziinformazione sicurezza.gov.it>.

⁵⁷ A página Internet do Ministério da Defesa da Itália é: <http://www.difesa.it>. O *site* do Ministério do Exterior é: <http://www.esteri.it>.

Fria é a defesa da democracia, das instituições e da comunidade, priorizando também a produção de relatórios sobre crime organizado, imigração ilegal e crimes na Internet.

O Ministério do Interior conta ainda com grupamentos de operações especiais anticrime e de vigilância nas principais forças policiais e constabulares do país. No corpo de *Carabinieri*, que tem um efetivo total de mais de 100.000 pessoas e é considerado como uma das quatro forças armadas do país, mas que ainda assim se reporta administrativamente ao Ministério do Interior, existe um grupo de operações especiais para vigilância dentro do país. Na polícia fiscal (*Guardia di Finanza*), uma força paramilitar de mais de 50.000 efetivos, o Ministério do Interior mantém uma *Direzione Investigativa Antimafia*. Finalmente, cabe mencionar que a Polícia Nacional (*Polizia di Stato*) italiana possui um departamento de antiterrorismo com funções operacionais e de inteligência.⁵⁸

O controle externo das atividades de inteligência na Itália é feito por um comitê parlamentar criado em 1969, o *Comitato parlamentare per i servizi di informazione e sicurezza e per il segreto di Stato* (CoPaCo). Este comitê é composto por quatro senadores e quatro deputados e tem poderes para convocar audiências e fazer perguntas ao governo sobre a conformidade das operações com a lei. Mas, salvo em situações extraordinárias, o comitê parlamentar não pode exigir documentos ou aprovação *ex ante* de operações de inteligência. O funcionamento do comitê está subordinado às regras legais sobre o segredo governamental da Itália.⁵⁹

Israel

O sistema de inteligência de Israel é caracterizado por um baixo grau de centralização da autoridade sobre as unidades do sistema, um baixo grau de integração

⁵⁸ Por meio de sua Direção de Segurança Pública, o Ministério do Interior italiano coordena e supervisiona o trabalho da *Polizia di Stato*, *Polizia Peninteziarica*, *Carabinieri*, *Guardia di Finanza* e outras agências policiais nacionais e das regiões administrativas. Cf. http://www.interno.it/sezioni/attivita/sicurezza/dip_ps/s_000000097.htm.

⁵⁹ Cf. http://www.camera.it/_bicamerale/sis.

analítica dos produtos de Intel das várias agências, um baixo envolvimento da atividade de inteligência com as instâncias de *policymaking*, um alto grau de responsividade das unidades do sistema aos governantes e, por fim, um grau médio de efetividade dos mecanismos de *accountability* e controle externo. Como no caso alemão, os três ramos principais da inteligência israelense são o externo, o militar e o de segurança. Também como no caso alemão, não existe em Israel uma agência específica para a área de inteligência policial ou criminal (ISP).⁶⁰

Na área externa a principal agência israelense é o MOSSAD (o acrônimo para o nome em hebraico do Instituto para Inteligência e Tarefas Especiais), criado em 1951 e até hoje responsável pela espionagem internacional (*humint*), pelas operações encobertas e de contra-terrorismo fora do território de Israel. Compõem o Mossad oito departamentos: coleta, ação política e ligação (com os países aliados), operações especiais (conhecido como *Metsada*), planejamento operacional e coordenação, pesquisa, tecnologia, operações técnicas, infra-estrutura (recursos humanos, logística, segurança e finanças) e treinamento. O diretor do MOSSAD é indicado pelo primeiro-ministro, mas o nome tem ser aprovado pelo parlamento israelense (*Knesset*). Além do MOSSAD, o governo de Israel mantém unidades de análise e produção de inteligência externa no Ministério de Relações Exteriores e no Conselho de Segurança Nacional (estabelecido em 1999).⁶¹

O subsistema de inteligência militar é dirigido pelo Chefe do Estado-Maior Geral das Forças de Defesa de Israel (IDF), que coordena os quatro principais organismos a ele subordinados e responde perante o Ministro da Defesa. O diretório de inteligência do Estado-Maior Geral tem como serviço principal o AMAN (*Agaf ha-Modi'in*),

⁶⁰ Neste sentido, Israel parece aproximar-se mais do que CEPIK (2003:112-113) chama de 'modelo europeu continental' de organização do sistema nacional de inteligência do que de um modelo 'anglo-saxão'. Para uma avaliação das mudanças recentes na inteligência israelense, ver: KAHANA, Ephraim. (2002). "Reorganizing Israel's Intelligence Community". *IJICI*, vol.15 (nº 03), Fall 2002. Páginas 415-428.

⁶¹ Embora não haja muita informação disponível no *site* oficial do governo israelense, seguem algumas URL's que podem ser úteis: www.info.gov.il / www.pmo.gov.il e www.mfa.gov.il. Informações semi-oficiais podem ser encontradas também no *site* do Centro de Informações de Inteligência e Terrorismo: <http://www.intelligence.org.il>.

encarregado de coleta, produção e difusão de inteligência militar nas disciplinas de *humint*, *sigint* e *imint* – esta última valendo-se do sistema israelense Ofek de satélites de reconhecimento lançado em 1995. O diretor do AMAN tem que produzir uma avaliação anual acerca de ameaças regionais à segurança de Israel, tratando também da balança estratégica nos países vizinhos. Além do AMAN, a inteligência estratégica de Israel conta com os serviços de inteligência de combate do exército, da aeronáutica e da marinha. Em abril de 2000, foi criado um novo serviço de inteligência tática: o *Hel Modi'in HaSadeh* (corpo de inteligência de campo), subordinado ao comando das forças terrestres das IDF. Além dos serviços de inteligência, o Ministério da Defesa de Israel conta ainda com um serviço de segurança operacional e informacional, o MALMAB, responsável também pela segurança de projetos secretos com outros países, além de unidades menores mencionadas por diferentes autores embora não esteja claro se tais unidades são ou não parte orgânica das agências e serviços maiores.⁶²

Na área de segurança e inteligência sobre ameaças internas, destaca-se o SHIN BET (também conhecido como SHABAK). Este Serviço Geral de Segurança (*Sheruth a Bitachon ha Klali*) foi criado em 1948 na fundação do Estado de Israel e foi renomeado em fevereiro de 2002 como Agência de Segurança de Israel. Segundo as informações disponíveis, o SHINBET tem três departamentos: assuntos árabes (contra-terrorismo e repressão contra a 'subversão'), assuntos não-árabes (contra-inteligência e contra-espionagem) e departamento de segurança e proteção (escolta de autoridades, proteção à infra-estrutura governamental, científica e industrial, segurança da empresa aérea nacional, a *El Al*). Este organismo tem poder de prisão e seu diretor é indicado pelo Primeiro Ministro (a quem ele se reporta diretamente), embora o nome do diretor precise ser aprovado pelo *Knesset*.

Na esfera de *criminal intelligence* (ISP), Israel conta com unidades departamentais especializadas na Polícia Nacional (onde a área de inteligência criminal foi criada em 1997), no Serviço Prisional e na Guarda Policial de Fronteiras (cuja unidade antiterror foi criada em 1974). A polícia, o serviço prisional e a guarda de

⁶² Cf. www.mod.gov.il e também www.idf.il. A página oficial do AMAN é: <http://www1.idf.il/aman/site/default.asp>. Ver ainda HENDERSON (2003:97-98).

fronteiras (constabular) reportam-se ambas ao Ministro da Segurança Pública. No âmbito do Ministério da Justiça foi criada, em 2002, uma nova unidade de inteligência financeira para apoiar o combate contra a 'lavagem' de dinheiro do crime organizado e o financiamento de atividades terroristas.⁶³

No caso da divisão de inteligência da Polícia Nacional, vale acrescentar que ela coordena e dirige o trabalho de ISP empreendido em todo o país, tanto no nível operacional e tático quanto estratégico. Os esforços estão concentrados no combate aos crimes mais sérios contra a pessoa e o patrimônio, especialmente o crime organizado. Todos os dados de inteligência são informatizados e armazenados centralmente, podendo ser facilmente recuperados. Além das funções mencionadas, a divisão é responsável por todo o trabalho relacionado com a repressão ao tráfico e consumo de drogas (*drug enforcement*), bem como pela cooperação internacional com as forças policiais de outros países. Israel é membro da INTERPOL desde 1949 e mantém cooperação operacional extensiva com outras polícias por meio desta organização. Diversos representantes da Polícia Nacional são postados no exterior (EUA, Alemanha, França e Países Baixos são alguns exemplos) para facilitar investigações internacionais.

A principal instância de coordenação do sistema nacional de inteligência de Israel é o VARASH (*Va'adat Rashei ha-Sherutim*), um conselho interagências formado em 1949 para planejar, coordenar e administrar conflitos jurisdicionais entre os serviços israelenses. O VARASH é coordenado pelo chefe do MOSSAD e reporta-se ao escritório do Primeiro Ministro. No âmbito do recém criado Conselho de Segurança Nacional (1999), existe ainda uma unidade de avaliação das atividades de contra-terrorismo e de planejamento de políticas de segurança, incluindo inteligência.

A principal instância de supervisão e controle externo dos serviços israelenses é o Comitê Permanente de Assuntos Exteriores e Segurança do *Knesset*. Este revisa as atividades das forças armadas, serviços secretos e polícia, aprova os respectivos orçamentos e aprova os nomes indicados pelo Primeiro Ministro para a direção do

⁶³ Cf. www.police.gov.il e também www.ips.gov.il.

MOSSAD e do SHIN BET. Por meio de um sub-comitê seletivo dos serviços secretos, o Comitê do *Knesset* revisa as atividades dos serviços secretos, especialmente do SHIN BET.

Além dos Estados Unidos, Israel mantém forte cooperação na área de inteligência com a Turquia, Rússia, Índia, China, Cingapura, África do Sul e Austrália e outros países num total de trinta e nove acordos secretos para a troca de informações e a garantia de segurança contra vazamentos de informação em projetos conjuntos.⁶⁴

África do Sul

Em 1994, como parte da transição do regime de *Apartheid* para uma democracia parlamentar multipartidária, o antigo *National Intelligence Service* (NIS) do regime racista foi extinto e começou a emergir uma nova institucionalidade para a área de inteligência e segurança nacional na África do Sul. Primeiro foram criados dois novos serviços de inteligência (especializados respectivamente em ameaças externas e internas) e, mais tarde, houve sucessivos aperfeiçoamentos dentre os quais destaca-se a criação de um ministério específico, de novas agências setoriais e o aumento da capacidade de controle externo por parte do Parlamento.⁶⁵

Na área externa, o governo da África do Sul conta com o *South African Secret Service* (SASS), criado pela reforma de 1994 e responsável pela busca e coleta de informações sobre ameaças e crises internacionais, alerta avançado e 'outras' atividades (possivelmente operações encobertas). No Departamento de Relações

⁶⁴ Cf. HENDERSON (2003:99).

⁶⁵ Ver, principalmente: McCARTHY, Shaun P. (1996). *Intelligence Services for a Democratic South Africa: Ensuring Parliamentary Control*. London, Research Institute for Study of Conflict & Terrorism. Para as mudanças mais recentes, ver: *Budget Vote Speech by Minister for Intelligence Services Ms. L. N. Sisulo* (Pretoria: Ministry for Intelligence Services, June 14, 2001).

Exteriores (DFA) existe um diretório de ligação de inteligência e um pequeno *bureau* de avaliação dos relatórios produzidos pelas várias agências do governo central.⁶⁶

No âmbito militar, destaca-se a divisão de inteligência do Estado-Maior da *South African National Defense Force* (NDFID/SANDF), que presta serviços para o chefe do Estado-Maior e para o Ministro da Defesa. Embora a NDFID procure obter inteligência sobre ameaças militares externas e também internas, o extenso envolvimento do antigo departamento de inteligência militar do regime de *Apartheid* na repressão interna gerou uma grande resistência nacional contra quaisquer abusos aos direitos humanos por parte das forças armadas e, portanto, isso levou a uma especialização crescente deste departamento na área militar externa (no plano estratégico) e no suporte operacional (em termos de inteligência tática). Além das divisões de inteligência nos respectivos estados-maiores do exército, marinha e força aérea, bem como das seções pertinentes nas unidades menores, também existe na *Special Forces Brigade* da SANDF um regimento de elite para reconhecimento em profundidade.⁶⁷

A principal agência de inteligência interna na África do Sul é a *National Intelligence Agency* (NIA), criada também em 1994 e responsável pelo acompanhamento de ameaças internas, operações de contra-inteligência e verificações de segurança para a concessão de credenciais de acesso à informação para os funcionários e membros do governo. Esta agência supre a nova e ampla definição de segurança nacional da Constituição de 1996, colhendo, analisando e distribuindo os relatórios de inteligência interna, referentes às ameaças contra a segurança da república e de seus cidadãos. A agência também auxilia no combate à criminalidade, prestando informações ao *South African Police Service* (SAPS) a respeito de atos 'subversivos' de extrema direita e de extrema esquerda, sabotagens, ações terroristas

⁶⁶ Cf. www.gov.za/ministry/intel. Ver tb. www.gov.za/dept/sass.php e ainda a página internet do *Department of Foreign Affairs* (<http://www.dfa.gov.za>).

⁶⁷ Cf. www.mil.za.

ou atos violentos contra as pessoas, instalações estratégicas e órgãos da república. O diretor da NIA reporta-se diretamente ao Ministro Chefe dos Serviços de Inteligência.⁶⁸

As capacidades de inteligência de segurança pública (ISP) presentes na administração pública sul-africana localizam-se principalmente no *Department of Safety & Security* (DSS), ao qual é subordinado o *South African Police Service* (SAPS). Por meio da divisão de *Crime Intelligence & Crime Detection*, uma das 13 divisões principais do SAPS, são coordenados os esforços de obtenção e análise de informações sobre crime com as divisões regionais e locais de inteligência das polícias, são padronizados procedimentos e treinamento, bem como são tomadas medidas de contra-inteligência em relação ao crime organizado. Principal responsável pelas informações criminais no país, *Divisional Commissioner para Crime Intelligence & Detection* tem sob seu comando uma força de cerca de 479 analistas e policiais especializados.⁶⁹

Ainda na área de ISP, em 1999 foi criado no âmbito da Promotoria Nacional (*National Prosecuting Authority of South Africa - NPA*) um Diretório de Operações Especiais (*Directorate of Special Operations - DSO*) também conhecido oficialmente como *Scorpions*. Basicamente, a função deste diretório é a de combater crimes como corrupção, crime organizado, lavagem de dinheiro e crimes financeiros e eletrônicos, contrabando de armas e narcotráfico. Para apoiar as investigações e a abertura de processos judiciais visando a condenação de criminosos, o DSO conta com recursos de inteligência para suporte estratégico de tomada de decisões sobre prioridades e também, em cooperação com as forças policiais do país, para suporte operacional durante as investigações.⁷⁰

Pode-se dizer que existem três instâncias principais de coordenação e supervisão das atividades de inteligência no poder executivo da África do Sul.

A primeira delas é o próprio *Ministry for Intelligence Services* (MIS), criado em 1996 e que subordina diretamente as duas principais agências sul-africanas do setor, a

⁶⁸ Cf. <http://www.nia.org.za>.

⁶⁹ Cf. <http://www.saps.gov.za/profile/pci.htm>.

⁷⁰ Cf. <http://www.npa.gov.za>.

National Intelligence Agency (NIA) e o *South Africa Secret Service* (SASS). Segundo Robert Henderson (2003:171), o orçamento destes dois serviços somava em 2000-2001 algo em torno de US\$ 140 milhões.

Dentre as medidas de reforma anunciadas pela ministra Lindiwe Nonceba Sisulu no final de 2001, destacava-se a criação de uma unidade analítica especial para atender a Presidência da República (*Presidential Intelligence Support Unity – PISU*), bem como a criação de um escritório de ligação para melhorar a responsividade dos serviços de inteligência às demandas dos usuários. Vale destacar ainda a exigência da ministra de que cada membro do MSI, da NIA e do SASS aprendesse pelo menos uma língua estrangeira, além das várias línguas faladas no país. Houve também uma série de iniciativas para aumentar o debate público com segmentos organizados da sociedade civil sul-africana sobre a legitimidade e a eficiência dos serviços de inteligência e, talvez a mais importante de todas as medidas anunciadas, a decisão de trabalhar para a criação de uma agência civil centralizando todas as capacidades de *sigint* do país.

Num segundo nível, o MIS coordena suas ações com os demais ministérios e supervisiona o sistema nacional de inteligência sul-africano por meio do *National Intelligence Co-ordinating Committee* (NICOC). Este NICOC é dirigido pelo Ministro dos Serviços de Inteligência e, na sua ausência, pelo Coordenador de Inteligência do Ministério. Do NICOC participam ainda os diretores da NIA e do SASS, o diretor da divisão de inteligência das Forças Armadas da África do Sul (NDFID/SANDF), o diretor da divisão de inteligência criminal do SAPS, o diretor do diretório de operações especiais da promotoria (DSO/NPA) e outras autoridades quando necessário. Nas províncias da África do Sul existem também instâncias de coordenação local e regional, chamados de *Provincial Intelligence Coordinating Committees* (PICOCs).

No terceiro nível que corresponde ao âmbito ministerial propriamente dito, há um comitê específico para a discussão e formulação de políticas em matéria de inteligência: o *Inter-Ministerial Committee on Intelligence* (IMCI). Este IMCI é dirigido pelo próprio Presidente da República e é integrado pelos Ministros da Justiça, da Inteligência, da Segurança & Proteção, da Defesa e por outros membros segundo a necessidade. O

Comitê Inter-Ministerial tem como uma de suas atribuições principais transmitir ao Ministério de Inteligência as demandas e prioridades do governo e dos poderes da República referentes à obtenção, análise e produção de inteligência.

O controle externo da atividade de inteligência é realizado pela Assembléia Nacional da África do Sul (o parlamento) por meio do *Joint Standing Committee on Intelligence* (JSCI) e do *Joint Standing Committee on Defence* (JSCD). Ambos os comitês são compostos por membros das duas casas, sendo apontados conjuntamente pelo presidente e pelo *speaker* da Assembléia Nacional. Além disso, existe a figura de um *Inspector General for Intelligence Services* (IGIS), o qual se reporta ao chefe do JSCI.

Considerações Finais

Como se pode observar a partir deste levantamento preliminar sobre a legislação e a organização dos sistemas de inteligência dos Estados Unidos, Canadá, Alemanha, Itália, Israel e África do Sul, a busca por um arranjo institucional adequado para a área de inteligência de segurança pública esta longe de ser uma exclusividade brasileira. Os problemas de doutrina, organização, equipamento, treinamento e controle externo destes arranjos institucionais tampouco são exclusividades brasileiras, embora seja forçoso reconhecer que o debate brasileiro a respeito destes temas ainda é muito escasso e os avanços tem se dado de maneira lenta e desigual.

Há, por trás do recorrente apelo a versões diferenciadas de modelos de policiamento liderado pelo conhecimento (ou 'Intelligence-Led Policing' no jargão dos ingleses) uma percepção internacionalmente compartilhada sobre o tipo de desafio a enfrentar. Este desafio esta associado a uma percepção de ameaça mais aguda da sociedade em relação ao crime, sobretudo violento. Mas também a uma percepção por parte das autoridades públicas de que as dinâmicas do crime tornaram-se mais complexas com o desenvolvimento tecnológico das comunicações e transportes, mais diversificadas e, portanto, associadas a fatores causais específicos cuja compreensão

adequada extrapolou há muito as possibilidades de uma abordagem puramente empírica e hedonista do trabalho policial tradicional.

Os estudos de caso realizados brevemente neste texto mostram claramente o peso crescente, não apenas nos países mais ricos e poderosos, da componente de inteligência criminal (ou de Segurança Pública) no âmbito dos sistemas nacionais de inteligência. Isto reflete em parte uma realidade na qual uma maior cooperação transfronteiriça entre os órgãos de segurança de diferentes países para lidar com ameaças de 'novo' tipo (tais como o terrorismo internacional, o crime organizado e a lavagem de dinheiro) tende a ser anulada se houver incapacidade de integração vertical entre os diferentes componentes nacionais do aparato estatal na área de segurança nacional. Especialmente as agências com responsabilidade local no policiamento, provimento de ordem pública e justiça criminal e as agências com responsabilidade nacional pelo planejamento estratégico, ligação internacional, validação de sistemas, análise e disseminação de tendências de longo prazo, integração de fluxos etc.

Por outro lado, os estudos de caso realizados não capturam uma dimensão importante da reflexão sobre as perspectivas de implantação do SISP no Brasil, a qual tem que ver justamente com a reforma das próprias polícias. Embora haja razoável consenso sobre os cuidados necessários em termos de incrementalismo na busca por maior integração, efetividade, eficiência, eficácia e legitimidade como desideratos para estas reformas, a resistência e a protelação na adoção de modelos de policiamento baseados em inteligência / conhecimento / informações nos seis países estudados deve constituir um alerta para as autoridades públicas e os estudiosos também no caso brasileiro.

Como observou corretamente Eduardo Estevez (1999) em seu estudo sobre inteligência criminal no âmbito da reforma policial após a extinção da *Bonaerense* na Província de Buenos Aires em 1997, a relação entre inteligência e polícia ainda é muito problemático entre nós.⁷¹

⁷¹ Cf. ESTEVEZ, Eduardo. (1999). "Modelos de Inteligencia y su aplicación en Policías en Proceso de Reforma". *Cuadernos IEPADES*, N.1, Ciudad Guatemala. Páginas 37-92.

O senso comum segundo o qual a componente funcional de coleta de informações em situações conflitivas é mais problemática do que a análise destas informações e sua integração ao ciclo do trabalho policial precisa, no caso de sistemas policiais como os nossos na América do Sul, levar em conta também o fato de que a coleta de informações no âmbito das investigações criminais (onde a inteligência constitui potencialmente um recurso penal e esta regulada pelas regras processualísticas de aceitabilidade das provas) tende a ser menos problemática do que a coleta de informações para fins de prevenção do crime, por parte das agências policiais responsáveis pelo patrulhamento ostensivo e provimento de ordem.

Ao lado de uma discussão sobre o desenho institucional adequado para os novos recursos de inteligência criminal previstos pelo SISP nos estados e prefeituras, as próprias normas federais que regulam a coleta de informações por parte das polícias precisam ser detalhadas, pelo menos em relação ao manejo de informações sobre a vida privada dos cidadãos, os procedimentos de aceitabilidade de informações em termos de sua qualidade e confiabilidade, o uso de infiltração policial em organizações criminosas e o que deveria constituir a área de contra-inteligência no caso da inteligência de segurança pública. Também no caso da reforma das polícias e da implementação do SISP, a participação do legislativo e da sociedade no debate público será decisiva para a efetividade e a legitimidade das estruturas que se estão criando neste momento no Brasil.