정보기관 감독 도구 모음

Edited by Hans Born and Aidan Wills

DCAF
a centre for security, development and the rule of law

Ministry of Foreign Affairs of the Netherlands

정보기관 감독
도구 모음

한스 본(Hans Born)/에이단 윌스(Aidan Wills) 편집

김영찬 연구원 부분감수

군의 민주적 통제(DCAF)를 위한 제네바 센터는 국제 사회의 굿 거버넌스 추구와 안보 부문 개혁을 돕는 것을 사명으로 하는 국제 재단이다. 이 센터는 규범과 표준을 개발하고, 맞춤형 정책 연구를 수행하며, 민주적인 안보 부문 거버넌스를 증진하는 모범 관행과 권고 사항을 파악하고, 국내 자문 지원 및 실용적 지원 프로그램을 제공한다.

DCAF 발행,
Geneva 11 Rue de Chantepoulet
Geneva – 1201 스위스
www.dcaf.ch

디자이너: Alice Lake-Hammond, www.alicelakehammond.com 언어 편집: Agincourt Press
표지 사진: Hans Kouwenhoven

본 간행물은 네덜란드 외무부의 물심양면의 지원에 힘입어 간행되었다.

ISBN: 978-92-9222-222-2

목차

표 및 상자 목록

DCAF 서문

정보 부문은 민주화와 안보 부문 개혁 과정의 마지막 전선에 해당한다. 여러 정착된 민주주의 체제가 보여준 것처럼 민주적 거버넌스와 법의 지배는 국가의 다른 분야에서 확실히 자리 잡고 난 한참 후에야 정보 부문에까지 미친다. 정착된 여러 민주주의에서 정보기관 감독 체계가 싹트는 과정은 공통적이다. 정보기관의 특정 활동들이 정당한 민주적 과정과 인권 및 기본적 자유의 행사를 침해한다는 우려를 불러일으켰고, 이로 인해 한동안 조사와 규명을 하다가 그 결과 새로운 감시 메커니즘이 만들어진 것이다.

신생 민주주의는 이런 반응적 방식에 따를 필요가 없다. "전환(transition)"은 이들 민주주의에 정보기관을 감독하기 위한 견고한 법적, 제도적 기초를 닦을 수 있는 천금 같은 기회를 제공한다. 그러나 이런 기초의 구축은 정보기관으로 하여금 국가 안보, 공공 안전, 인권을 효과적으로 보호하는 데 그치지 않고 법의 지배와 민주적 관행도 존중하도록 하는 지난하고 끝없는 과정의 작은 한걸음이라는 것을 명심해야 한다. 이들 목표의 장기적 달성에는 감독에 관련된 이해 관계자들의 지속적인 관심, 경계, 헌신뿐 아니라 감독 체계를 평가하고 개선하려는 끊임없는 노력이 필요하다. 이 도구 모음이 이 작업을 뒷받침하는 중요한 자원이 될 수 있다고 확신한다.

의원들에게는 감독을 위한 법적, 제도적 틀을 개발하는 것과 동시에 주요 외부 감시자로서 감독이 앞서 말한 목표를 달성하도록 해야 할 막중한 책임이 있다. 다른 어떤 분야보다도 이 분야에서는 의원들이 소속 정당의 정치적 이해보다 민주적 헌정 질서 보호라는 더 큰 목표를 우선시하려 노력해야 한다. 그럼에도 불구하고 의원들에게만 모든 외부 감독 책임을 떠넘겨서는 안 된다. 의원들은 시간과 전문성, 필요한 독립성이 부족하기 십상이기 때문이다. 이를 감안해 의원들은 최고 감사 기구, 옴부즈맨 기관, 전문 감시 기구 등의 독립적인 법정 감독 기구에 해당 권한 분야에서 중추적 역할을 해 주도록 요청해야 한다.

정보기관 감독에 초점을 맞춘 간행물은 많이 있었지만 감독 기구의 법적, 제도적 틀에 중점을 둔 것이 대부분이었다. 이 도구 모음은 이 방식을 바탕으로 의사 결정권자들이 감독 체계의 고안, 수정, 통합에서 비롯되는 여러 도전과 난제를 헤쳐 나갈 수 있도록 할 것이다. 그러나 기고 저자들은 외부 감시자들이 정보기관의 구체적 업무 영역 조사라는 어려움에 어떻게 맞설 수 있는지에 관해 명확하고 실용적인 지침을 제공함으로써 감독 체계 설계의 문제를 과감히 넘어선다. 이 도구 모음이 정보기관 감독의 다양한 측면들이 갖는 중요성에 대한 시민 사회와 언론의 인식을 제고하고 이들이 이 통찰을 활용하여 의원 및 기타 독립적 감시자들에게 정보기관 조사(또는 조사의 결여)의 책임을 물을 수 있기를 희망한다.

정보기관 감독 체계 개발과 관련된 의사 결정권자, 최근에 설립된 감독 기구의 구성원과 직원들 및 시민 사회 조직들이 아마 이 도구 모음에 가장 흥미를 가질 것이다. 이들 중 대다수는 전환기 국가(transition state)에 속할지 모르지만 정착된 민주주의 체제에서 정보기관 감독과 직간접적으로 관련되어 있는 그들에 대한 저자들의 통찰의 가치를 폄하해서는 안 될 것이다. 사실 필자는 이 도구 모음이 이들 정치 체제에서 가능한 감독 확장 또는 강화에 관한 논의를 불러일으킬 사례와 주장을 제공한다고 굳게 믿는다.

DCAF는 신생 민주주의뿐 아니라 민주주의가 정착된 국가에서도 정보기관 감독 역량을 강화하려는 노력을 10년 이상 지원해 왔다. DCAF는 정보기관 감독 체계의 개혁이 전환기 안보 부문 개혁의 필수적 부분이라고 본다. 일부 원조국이 (효과적인 운영 협력국을 만들기 위해) 전환기 국가 정보기관의 운영 역량 강화에 자원을 상당량 지원하고 있지만 가장 중요한 것은 원조국과 수혜국이 모두 지속적이고 효과적인 감독 체계의 개발과 유지에 투자하는 것이다. 필자의 바람은 이 도구 모음이 안보 부문 개혁 집단 내에서 정보기관 감독의 불가결성에 대한 인식을 높임으로써 운영적 효율과 거버넌스 사이의 이와 같은 균형을 바로잡도록 일조하는 것이다.

테오도르 H. 빙클러(Theodor H. Winkler) 대사 DCAF 국장

서문

어린 시절 나는 만화경에 빠져 있었고 성인이 된 지금도 그렇다. 손에 쥔 것이라고는 한쪽은 불투명 유리로 막혀 있고 다른 쪽에는 작고 둥근 구멍이 나 있는 조그만 통에 불과한데 말이다. 조심스럽게 통을 흔들면 보통 부드러운 딸랑딸랑 소리가 들린다. 하지만 그 안에 무엇이 있는지는 모른다.

작은 구멍을 통해 들여다봐도 아무것도 보이지 않는다. 하지만 빛이 불투명 유리를 통과하도록 통을 쥐면 갑자기 복잡한 모자이크가 나타난다. 이제 통을 돌리면 모자이크가 바뀌는 패턴을 보게 된다. 얼마나 매혹적인가.

어떤 면에서 이 책은 만화경과 좀 닮았다. 어쨌든 정보기관의 세계는 그 안을 들여다보려면 일정한 방식으로 다뤄야 하는 블랙박스이기 때문이다. 게다가 시각 또한 계속 바뀌는 것 같으니 말이다.

그럼에도 불구하고 관찰력이 더 뛰어난 관찰자들은 자신이 얻은 통찰을 다른 이들과 나누고 싶을 정도로 항상 가치 있고 흥미로운 무엇을 보게 된다. 그 점에 있어 이 일은 보기만큼 쉽지는 않은데, 정보기관의 세계가 들어 있는 통의 비밀을 그리 간단히 밝힐 수는 없기 때문이다.

이 책의 목표는 감독 기구들이 빛이 통과할 수 있도록 통을 제대로 들고 난 후에 충분한 근거를 바탕으로 관찰한 내용을 보고할 수 있게 해주는 도구를 제공하는 것이다.

저자들은 이들 도구를 설명할 때 감독의 다양한 측면을 조명하고, 상이한 감독 체계들을 나란히 비교함으로써 감독의 유형이 하나 이상 존재한다는 사실을 제대로 보여 주고 정보 업무의 놀라운 세계를 참신하고 비판적인 관점에서 지속적으로 바라볼 수 있도록 안내하는 만화경 같은 이미지를 만들어낸다.

따라서 이 책은 외부인들에게 흥미를 줄 뿐 아니라 내부자들(감독 기구 및 감독 대상)도 이 책을 공부함으로써 분명 이익을 얻을 수 있을 것이다.

베르트 반 델덴(Bert van Delden)
네덜란드 정보 보안 기관 심의 위원회 위원장

감사의 글

편집자들은 이 도구 모음이 가능하도록 재정 지원을 아끼지 않은 네덜란드 외무부에 감사를 표하고 싶다. 특히 이 도구 모음 개발 내내 귀중한 지원과 협력을 제공한 안보 국방 정책부의 야코 보스(Jacco Bos), 하인 크넥트(Hein Knegt), 미카엘 스티베(Michael Stibbe), 프랑크 반 베우닝겐(Frank van Beuningen), 욥 위즈난즈(Joep Wijnands)에게 감사한다.

네덜란드 정보보안기관심의위원회(CTIVD)와 특별히 베르트 반 델덴 위원장과 닉 페어호에벤(Nick Verhoeven) 전 간사, 힐데 보스-올러만(Hilde Bos-Ollerman) 현 간사의 기여에도 감사를 전하고 싶다. CTIVD는 이 프로젝트 착수에 필수적인 지원을 제공했고, 이 도구 모음 개발 기간 내내 아낌없이 전문적인 조언을 해주었다. 또한 이 프로젝트의 성공에 없어서는 안 될 지원을 DCAF에 해 준 윔 반 이클렌(Wim van Eekelen) 네덜란드 전 국방장관이자 상원의원에 대한 고마움도 기록해 두고자 한다.

나아가 편집자들은 도구 모음 대부분의 행 편집과 교열을 맡아 준 Agincourt Press 직원들에게 감사한다. Agincourt Press 직원들은 이 도구 모음을 비전문가 독자들도 최대한 쉽게 읽을 수 있게 만들었을 뿐 아니라 언어와 스타일이 일관성을 갖추도록 지대한 노력을 기울였다. 또 뛰어난 디자인 작업을 보여주고 도구 모음의 레이아웃과 식자에 고도로 전문적인 솜씨를 발휘한 앨리스 레이크-해몬드(Alice Lake-Hammond)에게 감사를 전한다.

끝으로 입문 도구를 공동 집필했을 뿐 아니라 도구 모음의 개념 정립과 개발에 크게 기여한 우리의 전 동료 가브리엘 가이슬러 메세바게(Gabriel Geisler Mesevage)에게도 감사한다.

한스 본/에이단 윌스
제네바, 2012년 7월

도구 1

정보기관 감독의 소개

한스 본/가브리엘 가이슬러 메세바게

1 정보기관 감독의 소개

한스 본/가브리엘 가이슬러 메세바게

1. 머리말

이 도구는 독자에게 정보기관 감독이라는 주제를 소개하고 누가, 무엇을, 언제, 어떻게, 왜라는 기본적 질문에 대한 간결한 대답을 제공한다. 또한 독자들에게 이 도구 모음에 있는 정보기관 감독에 관한 다른 도구들을 소개한다. 다른 도구들은 종합적으로 이 질문들과 그 밖의 질문들에 대해 더 자세한 대답을 제공한다.

이 프로젝트의 목표는 정보기관 감독 분야의 세계 최고 전문가들을 모아 비전문가들도 이해할 수 있게끔 이들의 전문 지식을 설명하는 것이다. 이 도구 모음은 구체적으로 관련 쟁점에 대한 독자들의 이해를 강화하고, 감독과 관련된 책임이 있는 사람들을 다양한 비교적 관점에 비추어 보는 것을 목표로 한다.

이 입문 도구는 관련 기관 및 "정보기관 감독 주기(intelligence oversight cycle)"에 대한 설명을 포함하여 정보기관 감독 과정의 개관으로 시작한다. 그 다음 정보기관 감독이 개인의 인권과 기본적 자유 보호에 왜 중요하며 개인의 안보 증진에 왜 중요한지를 설명한다. 그런 다음 대부분의 전문가가 인정하는 모범 관행에 초점을 맞추어 정보기관 감독의 현재 표준과 관행을 살펴본다. 이 도구는 정보기관 감독 강화를 위한 권고 사항으로 끝맺는다.

1.1 정보기관 감독 도구 모음이 왜 중요한가?

이 도구 모음은 신생 민주주의(및 정착된 민주주의)가 정보기관에 대한 민간 감독을 구축(및 개선)하는 것을 돕기 위해 만들어졌다. 도구 모음의 4가지 주요 목표는 다음과 같다.

1. 기존 정보기관 감독 체계의 검토와 개선 및 새로운 정보기관 감독 체계의 창설과 통합에 관한 정책 관련 지침 제공.

2. 정보수집, 개인정보 사용, 정보공유 등 정보기관의 특정 활동 분야에 대한 감독 지침 제공.
3. 정보기관 감독의 중요성에 관한 시민 사회 및 언론의 인식 형성.
4. 다양한 정보기관 감독 방식, 표준, 관행의 파악 및 분석을 통한 국가 간 학습 및 규범의 전수 증진.

따라서 이 도구 모음에서는 추상적인 학문적 분석이 아니라 정보기관 감독 체계를 감시하고 정기적으로 이 체계와 상호작용하는 사람들에게 실용적인 지침 제시에 중점을 둔다. 우리가 실제적 사례와 세계 각지의 관행이 반영된 구체적 권고 사항에 초점을 맞춰 이런 도구 모음 형식을 사용하기로 한 것은 이런 이유에서다.

1.2 이 도구 모음에서 다루는 문제

이 도구 모음의 9개 도구는 정보기관 감독의 중요 쟁점들에 대한 자족적 입문서 역할을 한다(표 1 참조). 각 도구는 독립적으로 읽을 수 있도록 쓰였다.

1.3 목표 독자층

이 도구 모음은 주로 정보기관 감독과 직간접적으로 관련된 사람들을 대상으로 만들어졌다. 이러한 독자들에는 행정, 입법, 사법부 구성원과 그 직원, 정보 관리, 시민 사회 구성원, 언론 구성원이 포함된다.

우리는 광범위한 대중이 이 도구 모음의 내용에 흥미를 가질 것으로 확신한다. 하지만 이 도구들을 특히 유용하게 여길 특정 고객층이 있다. 예를 들어 이 도구들이 의회 및 전문가 감독 기구가 하는 역할을 면밀히 검토하고 있기 때문에 이들 기관의 구성원과 직원들은 이 도구 모음의 정보가 각별히 의미 있다고 여길 것이다. 마찬가지로 업무에 정보기관 분석이 포함되는 언론인과 시민 사회 구성원, 현재 정보기관 감독 체계 창설 또는 개혁과 관련된 정부 관리들도 도구 모음에서 유용한 정보를 많이 찾을 수 있을 것이다.

표 1: 도구의 개관		
도구	제목	다루는 주요 질문
1	정보기관 감독의 소개	▪ 정보기관 감독이란 무엇인가? ▪ 정보기관 감독이 왜 중요한가? ▪ 정보기관 감독과 관련된 다양한 기관의 책임은 무엇인가?
2	효과적인 정보기관 감독 체계의 구축	▪ 정보기관 감독에 대한 다양한 제도적 접근법의 장단점은 무엇인가? ▪ 효과적 감독의 장애물은 무엇이며, 어떻게 해결할 수 있는가? ▪ 정보기관 감독을 위한 법적, 제도적 틀을 고안할 때 주요 고려사항은 무엇인가?
3	민주주의에서의 정보 투명성, 비밀주의, 감독	▪ 민주주의에서 정보기관의 비밀주의와 투명성 간의 적절한 균형은 무엇인가? ▪ 정보 보호 및 접근 입법과 관련된 모범 관행은 무엇인가?x ▪ 의회, 전문 감독 기구, 대중의 정보기관 정보 요구는 무엇인가?
4	감독 시행	▪ 감독 기구는 정보기관에게 책임을 묻기 위해 어떤 접근 방식과 방법을 사용하는가? ▪ 감독 기구가 정보기관의 관행을 효과적으로 조사할 수 있는 방법은 무엇인가? ▪ 감독 기구가 조사 결과를 보고할 수 있는 방법은 무엇인가?
5	정보수집 감독	▪ 정보수집 과정의 감독이 왜 중요한가? ▪ 감독 기구가 정보수집 과정을 효과적으로 감시할 수 있는 방법은 무엇인가? ▪ 정보수집 과정의 효과적 감독을 가로막는 장애물은 무엇이며, 어떻게 해결할 수 있는가?
6	개인정보 사용 감독	▪ 개인정보 사용 감독이 왜 중요한가? ▪ 정보기관이 개인정보를 합법적으로만 사용하도록 감독 기구가 보장할 수 있는 방법은 무엇인가? ▪ 개인정보 사용을 효과적으로 감독하는 데 있어서 장애물은 무엇이며, 어떻게 해결할 수 있는가?
7	정보공유 감독	▪ 정보공유 감독이 왜 중요한가? ▪ 정보공유와 관련하여 감독 기구가 해야 할 역할은 무엇인가? ▪ 국내 및 국제적 정보공유의 효과적 감독을 가로막는 장애물은 무엇이며, 어떻게 해결할 수 있는가?
8	정보기관에 대한 재정 감독	▪ 정보기관 재정 감독이 왜 중요한가? ▪ 정보기관에 재정적 책임을 물으려면 무엇이 필요한가? ▪ 정보기관 재정 감독과 관련된 다양한 기관들의 역할과 책임은 무엇인가?
9	정보기관에 대한 민원 처리	▪ 민원 처리 메커니즘이 왜 중요한가? ▪ 어떤 종류의 민원 처리 제도가 존재하는가? ▪ 민원 처리 제도를 개선할 방법은 무엇인가?

2. 정보기관 감독이란 무엇인가?

본 절은 정보기관 감독의 범위와 맥락을 개관하고 관련 기관들을 논의한다. 간결성과 명확성을 위해 이 도구 모음에서는 "보안 기관," "보안 정보기관/조직," "정보국" 등으로 다양하게 불리는 독립체들을 지칭할 때 일반적 용어인 정보기관(intelligence service)을 사용한다.[1] 관할권마다 정보 업무의 체계화 방식이 다르기 때문에 이 도구 모음에서는 정보기관의 정의에 대해 기능적 접근법을 취한다. 구체적으로 이 도구 모음에서는 *정보기관*을 국가 안보 위협과 관련된 정보를 수집, 분석, 유포하는 국가 조직으로 정의한다.

이러한 정의는 국내외의 군 정보기관, 경찰 정보기관, 민간 정보기관 등 다양한 조직을 망라한다. 또한 테러리스트 자금 조사나 돈세탁 방지를 담당하는 기관들처럼 흔히 재무성과 재무부에 소속되어 종종 간과되는 조직들도 포함된다. *안보 부문 개혁에 관한 OECD DAC 핸드북(OECD DAC Handbook on Security Sector Reform)*의 설명처럼 "대부분의 국가에는 경우에 따라 중첩되는 특정 임무를 지닌 다수의 정보 조직이 있다. 여기에는 내부/외부 정보수집 기관, 전술적/전략적 정보수집 기관, 범죄 정보수집 기관(예를 들어 통신, 인적 정보 및 사진), 민간/군 정보 당국, 전략 평가 당국이 포함된다."[2] 이들 기관이 모여 "정보 공동체(intelligence community)"를 구성한다.

정보기관은 또 통신 감청 권한, 잠복 감시 권한, 비밀 정보원 활용 권한, 몰래 주거지에 들어갈 권한 등 정보수집을 위해 보유하고 있는 특별한 권한에 의해 다른 국가 기관과 구별될 수 있다. 일부 국가(덴마크, 말레이시아, 러시아, 스웨덴 등)에서는 정보기관이 경찰권도 가지고 있어서 "경찰 보안부(police security service)" 또는 "특수 경찰(special branch)"로 불리기도 한다. 경찰 업무가 정보기관 업무와 완전히 분리되어 있어 정보기관이 경찰권(예: 용의자 체포권, 구금권, 취조권)을 전혀 갖고 있지 않은 나라들도 있다.

우리가 사용한 정의가 정보기관을 국가 조직으로 한정하기는 하지만 정보 업무 수행을 위해 정부가 민간 계약업체를 고용하는 나라들도 있다.[3] 민간

계약업체의 감독은 공공 서비스의 감독과는 상당히 다르므로 이 도구 모음에서는 논의하지 않는다.

2.1 정보기관 감독의 범위

*감독(oversight)*은 평가와 조사뿐 아니라 사전 감독, 지속적 모니터링, 사후 심사를 아우르는 포괄적 개념이다. 감독은 정보기관 내 관리자, 행정부 관리, 사법부 구성원 및 의회 구성원, 독립적 옴부즈맨 기관, 감사 기관, 전문 감독 기구, 언론인, 시민 사회 구성원들에 의해 수행된다.

감독은 *통제(control)*와는 구별되어야 하는데, 후자는 (관리처럼) 조직의 정책과 활동의 방향을 정하는 권한을 의미하기 때문이다. 따라서 *통제*는 일반적으로는 행정부와, 구체적으로는 정보기관의 고위직과 연관된다. 정보기관에 대테러 업무 같은 새로운 우선 과제를 채택할 것을 요구하는 행정 명령은 감독과 상반되는 통제의 예가 될 것이다. 그러나 독자들은 모든 정부가 감독과 통제를 명확히 구별하지는 않는다는 점에 유념해야 한다. 이런 이유에서 이 도구 모음에서 감독 기구로 설명되는 일부 기관은 여러 가지 통제 책임도 가지고 있을 수 있다.

감독의 주된 목표는 정보기관에 합법성, 적절성, 효과성, 효율성 측면에서 그 정책과 행동에 대한 책임을 묻는 것이다.[4] 감독 기구가 정보기관에 책임을 묻는 과정은 보통 다음 세 단계로 구분된다.

1. 감독 기구가 정보기관에 관한 정보를 수집한다.
2. 감독 기구는 이 초기 정보를 바탕으로 정보기관과 대화한다.
3. 감독 기구는 감독 결과와 권고 사항을 내놓는다.

따라서 감독 기관이 효과적으로 기능하기 위해서는 관련 정보를 평가하고, 정보 관리들에게 질문하며, 알게 된 것을 근거로 그 결과와 권고 사항을 공표할 능력을 가지고 있어야 한다. 이 세 가지 권한 없이는 진정한 책임(accountability)이 있을 수 없고, 감독은 실패할 가능성이 높다.

감독은 정보기관 활동의 적절성과 합법성뿐 아니라 정보기관의 효과성과 효율성도 포괄할 수 있다. 이 맥락에서 *적절성(propriety)*은 정보기관의 행동이 도덕적으로 정당한지 여부를 가리키는 반면 *합법성(legality)*은 이러한 행동이 준거법을 준수하는지 여부를 가리킨다. *효과성(effectiveness)*은 정보기관이 그 목표를 실현하는 정도를 측정하며, *효율성(efficiency)*은 정보기관이 그 목표를 얼마나 효율적으로 추진하는지를 측정한다. 정보기관 감독 기구가 합법성에만 관계하는 나라들(예컨대 네덜란드 정보보안기관심의위원회)이 있는가 하면 법률로 감독 기구가 효과성과 효율성에만 주력하도록 하고 있는 나라도 있다(예를 들어 영국의 정보보안위원회).

2.2 기관 책임

효과적인 정보기관 감독에는 국가 기관들의 조율된 활동뿐 아니라 정부의 행위에 대한 시민 사회 구성원과 언론의 적극적 비평도 필요하다. 이 기구들 모두가 중요한 역할을 하지만 이 도구 모음에서는 주로 의회 및 전문가 감독 기구에 초점을 맞추고 있는데, 이들은 정보기관이나 행정부의 지시를 받지 않아서 독립적으로 민주적 책임을 보호하고 법의 지배와 인권을 존중하기에 더 유리하기 때문이다.

표 2는 감독 과정에서 공공 기구와 민간 기구가 일반적으로 지게 되는 책임을 개관한다. 다만 독자들은 이들 책임의 관리 방식이 나라마다 다르며, 특정 국가의 감독 체계가 표에 명시된 모든 책임을 다루지 못할 수 있음에 유의해야 한다.

표 2: 감독 기구 및 주요 책임	
감독 기구	주요 책임
정보기관의 고위 관리층	▪ 내부 통제 시행 및 준수 모니터링 ▪ 법의 지배와 인권에 대한 존중을 증진하는 기관 문화 조성 ▪ 특별 권한 사용 요청을 심사하고 필요한 허가를 외부 조직에 요청 ▪ 내부 및 외부 감독 기구와의 협력 ▪ 불법 명령을 금하는 규칙 집행 및 불법 명령을 거부하는 정보관 지원 ▪ 내부 고발자 보호 절차의 시행 및 모니터링
행정부	▪ 정보기관 고위 관리직 지명 ▪ 정보기관 정책 및 우선 과제 수립 및 지침 공표 ▪ 정보기관의 활동에 관해 의회에 보고 ▪ 정보기관과 다른 정보기관 감독 기구의 협력 보장 ▪ 정보기관 예산 편성 및 지출 조사 ▪ 정보기관과 다른 국내외 기관의 협력 승인 ▪ 특별 권한 사용 요청 승인 ▪ 민감한 첩보 활동 승인
의회 및 전문가 감독 기구	▪ 정보기관 및 그 감독을 위한 포괄적인 법적 틀 채택 및 수정 ▪ 정보기관 활동의 적절성, 합법성, 효과성, 효율성 평가 ▪ 정보기관 예산 승인 및 심사
사법부	▪ 정보기관의 특별 권한 사용에 대한 사전 승인 및/또는 사후 심사 ▪ 정보기관의 활동과 관련된 형사, 민사, 헌법, 행정 소송 판결 ▪ 전문가 감독 기구 및 독립적 특별 조사의 구성원 역할(개인 자격으로)
옴부즈맨 기관	▪ 정보기관에 대한 민원 접수 ▪ 정보기관 활동에 대한 주제별 조사 착수
최고 감사 기구	▪ 재정 관리 개선을 위한 권고 및 재정 관리의 합법성, 효율성, 효과성의 문제를 밝힘 ▪ 정부 계정의 정확성과 합규칙성을 의회에 확인시킴으로써 행정부가 의회의 의지에 따르도록 도움 ▪ 국민의 돈이 합법적이고 적절하게, 효율적, 효과적으로 사용되고 있음을 국민에게 확인시킴
시민 사회와 언론	▪ 정보기관과 정보기관 감독 기구의 정책 및 활동 조사 ▪ 정보기관의 부적절하거나 불법적이거나 비효율적이거나 비효과적인 행위 폭로 ▪ 정보기관의 정책, 활동 및 그 감독과 관련하여 대중에게 알림 ▪ 정보기관의 정책과 활동 및 정보기관 감독 기구의 업무에 관한 공공 논의 장려

2.2.1 정보기관의 고위 관리층

효과적인 정보기관 감독은 효과적인 내부 통제로부터 시작된다. 정보기관 고위 관리층이 해이하거나 비협조적이라면 행정부 관리, 의회 위원회, 전문가 단체 모두 감독 책임 달성에 어려움을 겪게 될 것이다. 반면 고위 관리층이 업무에 충실하고 협력적이라면 정보기관 내부 통제 관리 체계는 권한 남용과 인권 침해를 막는 중요한 안전장치를 제공할 수 있다.

내부 통제 시행 및 준수 모니터링

고위 관리층은 내부 통제의 발달 및 지속적 준수에 직접적 책임이 있다. 베니스 위원회는 내부 통제를 "수단과 정책이 제대로 승인되도록 고안된 의사결정 구조"로 정의한다.[5] 달리 표현하면 내부 통제는 기관의 법적 의무, 행정부가 기관에 대해 정한 우선순위, 기관 고위 관리층이 수립한 정책과 규정 내에서 정보관들에게 그 행동에 대한 책임을 지운다. 내부 통제에는 적절한 예산 편성과 기록 유지 절차도 포함된다.

법의 지배와 인권에 대한 존중을 증진하는 기관 문화 조성

정보기관이 법의 지배와 인권을 존중하는 기관 문화를 조성하고 유지해야 할 필요성은 널리 인정되고 있다.[6] 따라서 이러한 문화를 증진하는 법규가 중요하지만 충분치 못하다. 기관 고위 관리층은 직원들에게 합헌성, 합법성, 책임성, 청렴성에 대한 이해를 심어 줄 프로그램도 개발하고 실시해야 한다.

특별 권한 사용 요청의 심사 및 필요한 허가를 외부 기구에 신청

대부분의 나라에서 정보기관의 특별 권한은 인권에 영향을 미칠 수 있기 때문에 궁극적으로 장관 및/또는 사법부에게 그 사용 승인을 받아야 한다. 다만 기관 고위 관리층은 이들 외부 기구로 전달할 만한 승인 요청인지를 결정할 때 중요한 역할을 한다. 고위 관리층은 이런 결정을 내릴 때 업무의 침해성과 위협의 성격을 균형 있게 비교해야 한다. 인권 침해의 위험이 클수록 내부 인가 계층도 높아져야 한다.

내부 및 외부 감독 기구와의 협력 보장

기관 고위 관리층은 모든 내부 감독 기구가 효과적으로 기능하도록 할 책임이 있다. 이 책임에는 기관 직원들이 내부 감독 기구 및 외부 감독 기구와 충분히 협력하도록 할 책임도 포함된다. 나아가 고위 관리층은 감독 기구가 민원 처리 메커니즘으로서 효과적으로 기능할 수 있도록 (특히 내부) 감독 기구에 대한 행정부의 압력을 차단해야 한다.

불법 명령을 금하는 규칙의 집행 및 불법 명령을 거부하는 정보관 지원

고위 관리층은 불법적 명령이 내려지는 일이 없도록, 그리고 불법적 명령이 내려지는 경우에는 그에 따르지 않도록 필요한 모든 조치를 취해야 한다. 이는 정보기관 인력이 정해진 내부 또는 외부 감독 기구에 불법 행위 관련 정보를 밝힐 수 있도록 하는 내부 고발자 보호법을 통해 강화할 수 있다. 일부 국가의 경우, 의심스러운 정보활동을 정보기관 책임자나 관련 관료에게 보고할 수 있는 법적 절차가 마련되어 있다. 보스니아 헤르체고비나에서는 의심스러운 활동을 기관 감찰관에게 보고한다(상자 1 참조). 다른 나라들의 경우, 주무장관에게 보고한다.[7] 또한 (불가리아 등의[8]) 일부 국가의 법은 정보기관 직원의 불법 행위 및/또는 공식적 의무 위반에 대해 직원 개인에게 책임을 묻는다.

상자 1: 보스니아 헤르체고비나의 정보관 불법 행위 보고 의무

"불법적 명령을 받았다고 생각하는 직원은 명령을 내린 자에게 그 불법성에 대한 자신의 우려를 충분히 전달해야 한다. 명령을 내린 자가 명령을 반복하는 경우, 직원은 그러한 명령의 확인서를 요구해야 한다. 계속 의심되는 경우, 직원은 명령을 내린 자의 직속상관에게 명령을 전달하고 감찰관에게 사안을 보고해야 한다. 직원은 명령 수행을 거부할 수 있다."[9]

2.2.2 행정부

장관 책임주의(doctrine of ministerial accountability)는[10] 각 장관은 자신의 권한과 직무의 행사에 대해 국가수반, 내각, 의회에게 설명할 책임이 있다고

규정하고 있다.[11] 이 주의에 따르면 정보기관의 정책을 정하는 행정부는 정보기관의 행위에 대해 정치적 책임이 있다.

일반적으로 정보기관은 정보기관이 적절하고 합법적이며 효과적이고 효율적으로 운영되도록 할 책임이 있는 정부 장관의 지시를 받는다. 예를 들어 독일에서는 해외, 국내, 군 정보기관들이 각각 연방수상실장, 내무부 장관, 국방부 장관의 지시를 받는다.[12]

행정부가 행사하는 통제의 정도는 국가마다 다르다. 정보 업무의 복잡성 때문에 행정부가 정보기관의 행동을 감시하고 통제하기 어려울 수 있다. 실제로 베니스 위원회는 "기관이 보유한 전문 지식의 독점 자체가 실제로는 기관에게 정부의 통제로부터 상당한 정도의 자율성을 부여한다"고 지적했다.[13]

행정부 관리들은 정보 실패(intelligence failure) 방지에 지대한 관심을 갖고 있지만 정보 실패가 발생할 경우 이를 공개하는 데는 소극적이다. 정보기관의 사고나 불법 행위의 공개는 정치적 낭패를 초래하고 관련 장관의 경력에 부정적 영향을 미칠 수 있다. 이런 이유로 일부 전문가는 정보기관을 제대로 감독할 행정부의 능력을 불신하며, 그 대신 행정부의 의사 결정에 대한 의회, 사법부, 시민 사회의 검토와 비판에 의존한다.

이런 우려에도 불구하고 행정부는 책임성의 연쇄(chain of accountability)에서 중요한 고리를 상징한다. 표2에 열거된 책임들은 행정부에 정치적 책임 외에 정보기관, 특히 정책 집행과 관련된 운영 책임도 있음을 분명히 보여 준다. 이런 이유에서 까다롭거나 민감한 운영상 결정과 관련된 정보를 행정부 구성원에게 감추지 않는 것이 중요하다. 오히려 행정부에는 항상 알려야 한다.

2.2.3 의회 및 전문가 감독 기구

행정부가 효과적인 보안 정보활동 감독을 확립하고 유지하는 것이 중요한 것처럼 독립적인 의회 및 비의회 감독 체계를 갖추는 것 역시 필수적이다. 정보 업무의 비밀주의, 사법적 심사와 비판의 부재, 과도한 감시에 따른 인

권 위협, 과거 불법 행위의 전력은 모두 현 정부에서 독립된 기구에 의한 효과적인 정보기관 감독의 필요성을 가리키고 있다.[14]

일반적으로 가장 효과적인 감독을 제공하는 외부 기관은 의회 감독 위원회와 전문가 기구이다. 전자를 광범위한 권한을 갖는 일반 위원회(국방 및 외무 위원회 등)와 정보 공동체에만 주력하는 특별 위원회로 나눠 보면 도움이 된다. (특히 예산 및 재정 관련 분야의) 일반 위원회는 정보기관과 관련된 특별한 감독 책임이 있을 수 있지만 정보기관 감독의 대부분은 특별 위원회가 수행하는 것이 일반적인데, 그 구성원의 경험과 전문성이 더 뛰어날 뿐 아니라 이를 통해 의회의 모든 구성원이 아니라 위원회 구성원에게만 특정 지식 정보 집합이 한정되기 때문이다.

전문가 정보기관 감독 기구(때때로 "전문 감독 기관" 또는 "전문 비의회 감독 기구"로 불린다)는 행정부, 의회 및 감독 대상인 정보기관과 독립적으로 설립, 운영된다. 전문가 감독 기구도 그 구성원의 전문성과 주력 분야의 명확성 면에서 유리하다는 점은 비슷하다. 대부분의 국가에서 이러한 기구는 전·현직 판사, 검사, 경찰 간부 등의 정보 전문가들로 채워진다.[15] 실제로 전문가 감독 기구 구성원들은 의회 전문 위원회의 구성원들보다 경험과 전문성에서 뛰어날 때가 많다. 뿐만 아니라 전문가 기구의 구성원들은 정보기관 감독에만 전념할 여유가 있는 반면 의원들은 여러 위원회의 자리를 맡고 있어서 여러 가지 책임을 관리해야 한다. 전문가 감독 기구의 또 다른 장점은 그 구성원들이 직업 정치인이 아니고 일상적 정치 활동에 직접 참여하지 않기 때문에 의원들에 비해 그 행동이 정치적 논란거리가 될 가능성이 훨씬 적다는 점이다. 그렇다 하더라도 전문가 감독은 항상 의회 감독의 대체재가 아닌 보완재로 보아야 하는데, 민주적 거버넌스의 원칙상 모든 정부 업무에 대해 의회가 직접 심사해야 하기 때문이다.

일부 국가(호주 등, 상자 2 참조)는 독립적인 감찰관을 창설함으로써 정보기관 감독을 강화했다. 이 직위의 명칭, 의무, 권한, 직무는 나라마다 상당히 다르지만(도구 2 참조) 그 핵심 임무에는 정보기관이 헌법, 성문법 및 행정부

가 정한 운영 정책을 준수하도록 하는 임무가 포함된다. 그 밖의 공통적 직무는 다음과 같다.

- 정보기관 인력에게 그 권리와 책임에 관해 교육
- 특히 낭비, 부정, 남용 탐지와 예방을 위해 내부 감사 및 조사 실시
- 효과적인 보안 정책과 절차의 유지 보장
- 기관 직원이 제기하는 민원 접수 및 조사
- 정보 자유법에 의해 일반 대중이 알 권리가 있는 정보의 공개
- 정보기관의 기록 관리가 관련 입법과 정책을 준수하도록 함[16]

상자 2: 호주 정보보안감찰관

호주의 정보보안감찰관은 호주 정보기관과 기타 보안 기관들이 합법적이고 적절하게 운영되고 있음을 독립적으로 수상, 선임 장관, 의회에 보장한다. 감찰관은 정보기관과 보안 기관의 조사와 그 활동에 관한 보고를 통해 이를 보장한다. 감찰관의 의무에는 정보기관과 보안 기관이 효과적으로 운영되고 있는지 여부 및 인권에 대한 존중을 보여주고 있는지 여부를 감시할 책임도 포함된다.

이 의무를 이행하기 위해 감찰관에게는 주무장관의 요청에 따라 또는 감찰관 자발적으로 조사를 실시할 권한이 호주 법률에 따라 부여된다. 또한 감찰관에게는 정보기관 활동의 영향을 받는 자가 제기하는 민원을 접수하고 조사할 권한이 있다. 이러한 조사에는 정보기관 구내(구금 지역 등) 조사, 선서를 한 증언 청취, 문서 접근도 포함될 수 있다. 각 조사가 마무리될 때 감찰관은 주무장관에게 보고서를 제출하며, 그 요약본은 보통 감찰관의 연례 의회 보고서에 포함된다. 관련 정보기관 책임자와 주무장관은 감찰관 보고서에 포함된 권고 사항의 이행에 관해 감찰관에게 보고할 법적 의무가 있다.[17]

의회 감독 위원회와 전문가 감독 기구의 위임 사항은 나라마다 다르다. (의회 정보기관 감독 위원회가 있는 미국처럼) 적절성, 합법성, 효과성, 효율성 전부를 망라하는 위임 사항을 제정한 나라도 있고, (네덜란드와 스웨덴처럼)

위임 사항이 합법성으로만 국한된 나라도 있다.

이 위임 사항을 이행할 수 있도록 의회 감독 위원회와 전문가 감독 기구에게는 종종 폭넓은 권한이 부여되는데, 여기에는 다음 목록 일부 또는 전부가 포함될 수 있다(목록은 예시적임).

- 기밀 정보 접근 권한
- 정보기관이 작성한 연례 보고서 및 기타 보고서 수령, 심의 권한
- 선서 후 증언을 위한 간부 및 정보관 소환 권한
- 선서 후 증언을 위한 외부 전문가 및 일반 대중 초청 권한
- 주무장관 및/또는 기관 책임자와 정기적 회의를 가질 권한
- 정기 및 특별 조사 실시 권한 및 정보기관 구내 방문 권한

2.2.4 사법부

정보기관은 법 위에 존재하는 것이 아니므로 법원의 관할에 속한다. 정보 업무와 관련된 법원의 역할은 여기 설명된 것보다 더 자세히 다뤄야 마땅하지만 다음과 같은 간략한 언급도 도움이 될 수 있다.

사법부는 법의 지배를 유지하고 인권이 존중되도록 할 책임이 있지만 전통적으로 판사들은 국가 안보 문제와 관련해서는 두 가지 이유로 행정부의 의견에 따라 왔다. 첫째로, 헌법과 준거법은 국가 안보 문제를 행정부의 독점적 권한 내에 두는 경우가 많다. 둘째, 많은 판사들은 법정이 기밀 정보가 공개되기에는 적절치 않은 장소라고 본다.[18] 그럼에도 일부 법원 제도는 정보기관 감독에서 적극적 역할을 하기도 한다. 예를 들어 미국에서는 형사 피고인의 적법 절차 권리가 확대되면서 판사들이 정부의 행위를 그 어느 때보다 상세히 검토했으며, 의회 또한 사법 심사의 증가에 기여한 정보 관련 법률을 통과시키는 경우가 늘어났다.[19] 특히 행정부가 국가 안보를 명목으로 과도하고 고압적인 주장을 해 온 다른 나라들에서는 판사들이 헌법과 인권 옹호에서 더욱 적극적인 태도를 띠게 되었다.[20]

정보기관에 대한 사법적 감독은 크게 네 가지 방식으로 이루어지는데, 이 중 세 가지는 통제 영역에 대한 감독을 넘어서는 것이다. 첫째, 준거법에서는 특별 조사 수단(통신 감청 등)을 사용하기를 원하는 정보기관이 판사에게 사전 승인을 구하거나 사후 사법 심사를 받도록 하는 요건을 두고 있는 경우가 많다. 이런 요건은 침해적인 기관 활동의 합법성을 독립적으로 조사하는 것이기 때문에 중요하다. 둘째, 판사들은 정보 업무 관련 위법 행위가 관련된 형사 재판을 주재할 수 있고, 정보 관련 문제가 연루된 헌법, 민사 또는 행정 청구에 대해 판결할 수 있다. 셋째, (프랑스 같은) 일부 국가에서는 안보 문제를 전문으로 다루는 수사판사(investigating magistrate)에게 정보기관 조사에 대한 감독권을 줄 수 있다. 넷째, 판사들은 경우에 따라 감독 기구의 구성원이 되거나 특별 조사 위원회 위원장을 맡을 수 있다.

이 역할들 중 처음 세 가지는 판사들에게 관련 정보기관의 활동을 지휘할 권한을 주기 때문에 통제 수단으로 부족함이 없다. 이에 비해 네 번째 역할은 보다 한정적이며, 구속력 있는 권고를 할 수 있는 권한은 없는 것이 보통이다.

2.2.5 옴부즈맨 기관

옴부즈맨 기관과 정보 공동체 간의 가장 일반적인 상호작용은 정보기관을 상대로 한 일반 대중의 민원 처리이다. 예컨대 네덜란드의 경우, "관련 장관, [정보] 기관의 수장, 조정관, 정보기관 및 조정관을 위해 일하는 자의 행위 또는 행위 혐의"와 관련된 문제에 관해 누구나 국가 옴부즈맨에 민원을 제기할 수 있다.[21] 민원을 제기하는 자는 먼저 주무장관에게 알려야 하며, 그 후 주무장관은 정보보안기관심의위원회(CTIVD)의 자문을 구한다. 그 다음 네덜란드 국가 옴부즈맨이 민원을 조사하여 "민원을 제기한 자에게 서면으로 민원에 관한 결정을 내리고, 안보 또는 그 밖의 중요한 국가 이익상 부득이한 경우가 아닌 한 결정 사유를 적시한다."[22]

옴부즈맨 기관은 대체로 독립성이라는 장점과 조사 관련 정보에 접근하는 데 필요한 법적 권한을 모두 갖고 있다. 불행히도 옴부즈맨 기관은 정보 공동체뿐 아니라 군, 경우에 따라서는 정부 전체가 포함되기 일쑤인 광범위한 관할 분야

를 효과적으로 다루기에는 인력이 부족한 경우가 많다. 따라서 옴부즈맨 기관은 정보기관 감독에 전문성과 자원을 충분히 투입하지 못하는 어려움이 있다.

2.2.6 최고 감사 기구

옴부즈맨 기관처럼 최고 감사 기구(SAI)도 정보기관의 행위에 대한 독립적인 외부 견제를 제공한다. 구체적으로 최고 감사 기구는 정보 업무의 재정적 측면을 감시하며 정보기관의 기록 관리가 공정하고 정확한지, 지출 내부 통제가 제대로 작동하고 있는지, 정보기관의 지출이 주요 규정을 준수하는지를 평가한다(도구 8 참조). 최고 감사 기구는 이런 책임 외에도 의원들과 행정부 구성원들이 정보기관 예산과 우선순위를 편성하기 위한 최선의 방안에 관해 현명한 결정을 내릴 수 있도록 효율성 평가(value-for-money assessment)를 하기도 한다.

2.2.7 시민 사회와 언론

애매한 개념이기는 하지만 *시민 사회(civil society)*는 일반적으로 국가 기관과 개인 및 공동체의 사적 생활 사이에 있는 공적 공간에 존재하는 자율적 조직을 망라하는 것으로 이해되고 있다. 이런 정의에는 예를 들어 학계, 비정부 조직(NGO), 시민 단체, 종교계가 포함된다. 정보기관 감독 수행에 있어서 시민 사회 조직의 큰 장점은 정부 정책을 제약 없이 분석하고 비판할 수 있다는 점이다.

시민 사회 조직처럼 언론 기관도 독립적 (즉 비정부적) 전문성을 활용하여 정보기관의 행위에 관한 지속적 피드백을 제공한다. 특히 탐사 보도 기자들은 부적절하고, 불법적이며, 비효과적/비효율적인 정보기관 행위를 밝혀내는 데 결정적 역할을 한다. 이런 실패 사례나 부정행위는 일단 밝혀지고 나면 의회 위원회나 전문가 감독 기구, 옴부즈맨 기관 또는 최고 감사 기구(SAI) 등의 그 밖의 독립적 감독 기구가 주도하는 공식적 조사 대상이 되는 경우가 많다. 언론 보도가 관심을 촉구하지 않는다면 이런 사안들은 결코 조사되지 않을 수도 있다.

불법 행위의 폭로든 행정부 정책에 대한 단순한 책임 규명이든 간에 언론 보도는 특정 쟁점을 공공 논의의 주제로 삼음으로써 이를 정부 의제에 올려놓는 경우도 많다. 예를 들어 워싱턴포스트지의 Top *Secret America* 시리즈는 2001년 911 테러 공격 후 10년 사이 미국 정보 공동체의 놀라운 성장을 공개함으로써 이러한 투자의 비용 대비 효과에 관한 격렬한 공공 논의에 불을 붙였다.[23] 그러나 지나친 정치 쟁점화를 일삼거나 편향된 언론은 정보기관 감독에 해로울 수 있다는 점은 인정해야 한다.

2.3 정보기관 감독 주기

감독은 몇 가지 시점에 이루어질 수 있다. 제안되었지만 아직 수행되지 않은 업무가 시작될 때 감독이 이루어질 수도 있고(사전 감독), 업무 진행 도중 이루어질 수도 있고 중도 감독), 업무가 종결된 후 이루어질 수도 있다(사후 감독).

2.3.1 사전 감독

가장 일반적인 사전 감독 활동에는 정보기관과 정보기관 감시 기구를 위한 포괄적인 법적 틀 마련, 정보기관 예산 편성 및 승인, 일정한 민감성 임계치(threshold of sensitivity)를 넘는 정보 업무의 승인이 포함된다.

법적 틀이 효과적이려면 정보기관이나 감독 기구의 위임 사항과 정보기관 또는 감독 기구에게 부여되는 권한을 명확히 기술해야 한다. 전통적 의미에서는 감독이 아닐 수도 있지만 이러한 입법 활동은 모든 유용한 감독 체계의 출발점(이자 필수요소)이다. 위임 사항과 권한이 명확히 규정되지 않으면 정보기관과 감독 기구가 제대로 기능할 수 없다. (법적 틀의 창설은 도구 2에서 폭넓게 논의된다).

정부 기관은 자금 없이는 운영될 수 없다. 따라서 민주주의에서 공공 자금 사용을 통제하는 의회는 정보기관을 포함한 모든 정부 기관의 연간 예산을 편성해야 한다. 예산안은 보통 주무장관이 정보기관의 고위 관리층, 재무부, 그리고 경우에 따라서는 최고 감사 기구와 협의하여 관련 의회 위원회에 제출한다. (예산 과정은 도구 8에서 더 자세히 다룬다.) 그러면 의회 위원회 위

원들이 현재 행정부의 정보 정책을 기준으로 예산안을 평가한다. 놀랄 것 없이 의원들은 예산 과정을, 행정부가 수립한 정보기관 정책과 우선 과제를 비판하는 기회로 삼는 경우가 비일비재하다.

사전 승인을 요하는 정보활동은 주로 개인 통신의 전자 감청 같이 개인의 권리를 침해하는 특별 권한의 사용과 관련된다. 흔히 이런 형식의 사전 감독은 판사가 수행하지만 특정한 상황에서는 독일연방하원의회 G10 위원회(우편 및 통신 프라이버시와 관련된 독일 기본법 10조에 따라 명명)처럼 비(非)사법 또는 준(準)사법 감독 기구가 수행할 수도 있다. (도구 5 참조).

2.3.2 중도 감독

중도 감독에는 정보기관과 감독 기구 자신의 활동에 관한 조사, 현장 조사, 주기적 청문회, 정기 보고가 포함될 수 있다. 또한 일부 국가에서는 판사들이 도청 등 진행 중인 정보수집 업무를 주기적으로 심사하여 업무의 지속이 정당성을 갖는지 결정한다.

2011년에 네덜란드 정보보안기관심의위원회(CTIVD)는 중도 감독 활동에 정보기관 도청, 정보기관 보안 심사, 정보기관 파일에 대한 접근 요청 처리에 대한 정기적 심의가 포함된다고 보고했다. 또한 해당 심의 위원회는 정보기관이 특별 조사 조치의 대상이 되는 개인들에게 법적 통보 의무를 이행했는지에 관해서도 조사했다.[24] 중도 감독을 실시할 구체적 권한이 있는 또 다른 정보기관 감독기구는 노르웨이의 의회정보감독위원회이다(상자 3 참조).

상자 3: 노르웨이 의회정보감독위원회

노르웨이 의회정보감독위원회(EOS 위원회)의 활동은 1995년 2월 3일자 정보, 감시, 보안 기관의 모니터링에 관한 법(Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services)에 명시되어 있다. 이 법률은 EOS 위원회를 "순전히 모니터링을 위한(purely monitory)"[25] 기관으로 규정하고 있다. 따라서 "위원회는 모니터링 대상 기구들에게 지시하거나 그 기구들이 협의를 위해 이용할 수 없다."[26]

이 법의 3조는 EOS 위원회가 "공공 및 군사 행정 내 정보, 감시, 보안 기관의 관행을 정기적으로 모니터링 한다"고 규정하고 있다. 4조는 위원회가 그 위임 사항을 이행하기 위한 부지 출입을 허가하고 있으며, 5조는 위원회가 청문회에 증인을 강제 출석시킬 수 있도록 하고 있다.

나아가 8조는 위원회에 접수되는 일체의 민원에 응하여 비밀로 분류되지 않는 보고서를 발행하고, 위원회 활동을 기술한 연례 보고서를 노르웨이 의회(Storting)에 제출할 의무를 위원회에 부과하고 있다. 또한 위원회는 "의회에 즉시 알려야 하는 요소들이 밝혀지는"[27] 경우, 특정 주제에 관한 정기 보고서를 발행할 수 있다. EOS 위원회는 이 후자의 권한을 통해 노르웨이 정보기관 활동에 대한 중요한 중도 감독을 수행할 수 있다.

2.3.3 사후 감독

가장 일반적인 사후 감독의 형태는 주제별 심사, 사례 심사, 지출 심사(도구 8 참조), 연례 심사이다. 하지만 불법 행위 혐의가 드러나는 경우처럼 상황에 따라서는 특별 조사의 형태로 사후 감독이 이루어질 수 있다. 이러한 조사는 특정 사건과 관련해 조사 및 권고를 하기 위해 이루어지는 것이 일반적이다.

일례로 2004년에 캐나다 정부는 캐나다 시민 마헤르 아라르(Maher Arar)가 미국에 의해 시리아로 송환된 뒤 고문을 받은 사건(마헤르 아라르 사건)에서 캐나다 왕립 기마경찰대(RCMP)가 한 역할에 관한 특별 조사에 착수했다(도

구 7 참조). 이 조사는 사실 심사와 정책 심사라는 두 가지 측면을 지니고 있었다. 사실 심사의 목표는 "마헤르 아라르에게 일어난 일과 관련하여 캐나다 관리들의 조치를 조사하고 보고하는 것"이었다.[28] 정책 심사의 목표는 "RCMP의 국가 안보 활동과 관련하여 독립적이고 공정한 심사 메커니즘을 위한 제안을 하는 것"이었다.[29] 이 두 가지 방식이 결합된 사후 조사 체계는 유용한데, 일어난 사실을 확정하는 동시에 적절한 정책 대응을 마련할 기회도 제공하기 때문이다.

사후 감독의 또 다른 중요한 분야인 민원 처리는(도구 9 참조)[30] 다양한 제도적 방식으로 관리할 수 있다. 흔히 민원은 사법부가 처리하지만 옴부즈맨 기관(예: 세르비아)이나 의회 위원회(예: 헝가리) 또는 전문가 감독 기구(예: 노르웨이)처럼 비사법적으로 처리될 수도 있다.

2.4 정보기관 감독 평가

정보기관 감독 기구는 정보기관의 업무 수행을 평가하지만 감독 체계의 업무 수행은 누가, 어떻게 평가하는가? 정보기관 감시자들과 학계는 최근에야 이런 질문을 하기 시작했는데, 여러 이유가 있지만 무엇보다도, 많은 나라에서 1990년대까지는 정보기관 감독 체계가 갖춰져 있지 않았기 때문이다.

몇몇 나라는 정보기관 감독 체계를 외부 평가에 맡겼다. 캐나다의 경우, 하원 특별 위원회가 캐나다보안정보국법(Canadian Security Intelligence Service Act)의[31] 5년 심사의 일환으로 이렇게 하고 있으며, 네덜란드에서는 CTIVD의 요청에 따라 독립적인 전문가가 정보보안국법(Intelligence and Security Services Act)의[32] 유사한 심사를 실시했다. 또한 일부 국가는 정보기관의 실패 또는 불법 행위 혐의에 대한 의회 조사나 독립적 조사의 일환으로 감독 체계를 평가했다. 이러한 예에는 미국의 911 위원회와 캐나다의 아라르 조사가 포함된다.

아래 소개된 원칙들은, 그 복잡다단한 내용을 이 도구 모음에서 모두 설명할 수는 없지만 향후 이 중요한 주제를 연구하는 데 지침이 될 수 있다.

- 준거법은 정보기관 감독 체계가 여전히 그 목적에 적합한지 결정하기 위해 감독 체계에 대한 주기적 심사를 의무화해야 한다.
- 이 주기적 심사에는 정보기관 고위 관리층, 행정부, 의회, 사법부, 독립적 감독 기구, 시민 사회, 언론을 비롯하여 전체 감독 체계가 포함되어야 한다.
- 이러한 심사는 전체적으로 평가했을 때 정보기관 감독 기구의 위임 사항이 정보기관 활동의 가장 중요한 측면을 포함하고 있는지 판단해야 한다. 특히 위임 사항이 정보기관 활동의 합법성과 효과성을 모두 다루고 있는지 평가해야 한다.
- 특정 감독 기구에 대한 평가는 감독 대상 기관에 책임을 물을 수 있는 감독 기구의 능력에 초점을 맞춰야 한다. 다시 말해 감독 기구의 권한과 자원이 위임 사항 집행에 충분한가? 구체적으로 감독 기구가 행정부와 정보기관으로부터 충분히 독립적인가, 기밀 정보에 충분히 접근할 수 있는가, 필요한 조사 권한을 가지고 있는가, 충분한 전문 인력을 보유하고 있는가?

3. 정보기관 감독이 왜 중요한가?

각국이 정보기관 감독 체계를 마련하는 세 가지 주요 이유는 (유권자에 대한 책임을 포함해) 정보기관에 대한 민주적 거버넌스를 강화하고, 법의 지배를 옹호하며, 정보기관 활동의 효과성과 효율성을 보장하기 위해서이다.

3.1 민주적 거버넌스와 책임

민주적 거버넌스의 근본적 원칙 중 하나는 유권자에 대한 국가 기관의 책임이다. 나아가 정보기관은 공공 자금을 사용하기 때문에 대중은 이 자금이 적절하고, 합법적이며, 효과적이고, 효율적으로 사용되는지를 알 권리가 있다.

많은 정보 업무가 비밀성을 띠기 때문에 정보기관이 완벽히 투명해질 수는 없다. 따라서 사회는 유권자를 대신하여 정보기관의 행위를 감시하는 (공공 감시 이외의) 대체 메커니즘을 만들어야 한다. 가장 일반적인 메커니즘은 모든 정부 기관을 통제하기 위해서는 적절한 견제와 균형이 존재하도록 해야

한다는 의회의 의무를 이행하기 위해 의회가 만든 의회 위원회와 전문가 감독 기구다.

이러한 견제와 균형을 통해 특히 정보기관이 현 정부의 안보가 아닌 국가 안보의 방어를 위해 행동하도록 보장해야 한다. 사실 정보기관들은 정당의 도구 역할을 해서는 안 되며, 오로지 공공의 봉사자 역할만을 해야 한다.

일반 대중이 그들의 대표자인 의회와 그 밖의 정보기관 감독 기구에 의해 정보기관이 적절히 감독 되고 있음을 알게 된다면 민주적 거버넌스 정보기관의 업무에 대한 대중의 신뢰를 강화할 수 있다.

3.2 법의 지배 옹호

정보기관은 여타 정부 기관처럼 법의 지배를 존중하고 옹호할 의무가 있다. 국가 안보에 대한 위협의 존재도 정보기관이 법을 위반할 충분한 이유가 되지 못한다. 정보기관의 불법적 행위는 정보기관이 보호해야 하는 법의 지배를 위배할 뿐 아니라 정보기관과 정부는 그로 인해 국내외적으로 오명을 뒤집어쓰게 될 것이다. 특히 정보기관의 특별 권한의 사용은 인권 침해 가능성이 존재하기 때문에 면밀히 감시해야 한다.

역사적으로 정보기관이 법률 위반 및 인권 남용과 관련되었던 나라에서는 불법 행위 재발 방지뿐 아니라 정보기관과 정부에 대한 대중의 신뢰 구축을 위해서도 면밀한 감독이 특히 중요하다.

3.3 효과성과 효율성

정보기관은 국가 안보 보호에서 중요한 역할을 하며, 그 자원이 한정되어 있기 때문에 이러한 자원을 목적 없이 낭비하지 않고 효과적, 효율적으로 사용하는 것이 중요하다. 따라서 잘 고안된 정보기관 감독 체계는 정보기관이 행정부가 설정한 우선 과제를 달성하는 한편 사용된 세금으로 최대의 가치를 얻을 수 있도록 그 자원을 사용하고 있는지 감시해야 한다.

일반적으로 정보기관의 효율성은 의회가 예산 공청회에서 심사하고 또한 최고 감사 기구가 정기 지출 심사에서 심사한다. 정보 업무의 비밀성 때문에 정보기관은 (다른 정부 기관과 비교할 때) 부정과 낭비 사례를 감추기가 더 용이하다. 그러므로 감독 기구는 공공 자금 사용을 특히 면밀히 검토해야 한다(도구 8 참조).

4. 모범 관행

모든 국가는 정보기관이 UN 헌장과 시민적·정치적 권리에 관한 국제 규약(International Covenant on Civil and Political Rights)에 명시된 것을 포함한 국제법상 의무에 일관되게 행동하도록 해야 한다. 정보기관의 위임 사항에 따라 경찰권의 사용에 관한 국제 조약도 적용될 수 있다.
이들 의무를 관리하는 한 가지 방법은 모범 관행에 따르는 것이다. 이 도구 모음에서 *모범 관행*은 효과적인 정보기관 감독을 증진하는 국가 제도적 체계, 절차 및 모델뿐 아니라 국내 및 국제법 조항을 의미한다.

정보기관 감독에는 만병통치약 모델은 없으므로 단 하나의 표준이나 관행이 이론의 여지없이 최고라는 주장은 타당하지 않다. 그보다는 전 세계 국가에서 동일하게 훌륭한 다양한 모델과 접근 방법을 찾을 수 있다. 법, 정치, 문화 체제의 차이로 인해 한 나라의 모범 관행을 다른 나라에 적용하기는 어려울 수 있으며, 그것이 가능하더라도 유의미한 적용에 앞서 관행을 적절히 수정하는 과정이 필요한 것이 보통이다. 그럼에도 불구하고 효과적인 정보기관 감독에 기여하는 공통적인 표준과 관행을 파악하는 것은 가능하다.

2010년에 DCAF는 인권과 기본적 자유의 증진 보호 및 테러 반대에 관한 UN 특별 보고관(UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism)을 위해 50개국 이상의 헌법, 법률, 법령, 의회 결의안, 독립적 조사, 법원 판결의 비교 분석을 바탕으로 정보기관 감독 모범 사례 카탈로그를 작성했다. (상자 4 참조).

상자 4: 정보기관 감독 모범 관행에 관한 UN 요약 보고서

2010년, 인권과 기본적 자유의 증진 보호 및 테러 반대에 관한 UN 특별 보고관은 DCAF의 연구를 바탕으로 정보기관 및 감독 모범 관행 요약 보고서를 내놓았다.[33] 이 요약 보고서에는 법적 근거, 감독 및 책임, 인권에 대한 존중, 정보 기능과 관련된 35개 모범 관행이 포함되어 있지만 아래 나열된 내용에서는 정보기관 감독과 관련된 모범 관행만 언급한다.

관행 6. 정보기관은 공개된 법률에 근거하여 위임 사항과 권한을 부여받은 내부, 행정부, 의회, 사법부 및 전문 감독 기관이 복합적으로 감독한다. 효과적인 정보기관 감독 체계에는 정보기관과 행정부로부터 독립적인 민간 기관이 적어도 하나 이상 포함된다. 감독 기관들의 소관을 모두 합치면 법률 준수, 활동의 효과성과 효율성, 재정, 행정 관행 등 정보기관 업무의 모든 측면이 포괄된다.

관행 7. 감독 기관들은 위임 사항 이행에 필요한 정보, 관료, 시설에 대한 제약 없는 완전한 접근뿐 아니라 자체 조사를 시작하고 수행할 수 있는 권한, 자원, 전문성을 갖추고 있다. 감독 기관들은 기록 및 기타 증거 획득은 물론 증언 청취에 있어서도 정보기관과 법 집행 당국의 전면적 협조를 받는다.

관행 8. 감독 기관들은 업무 도중 접하게 되는 기밀 정보와 개인정보를 보호하기 위해 필요한 모든 조치를 취한다. 감독 기관 구성원이 이러한 요건을 위반하는 경우 처벌이 규정되어 있다.

5. 권고 사항

- 효과적인 감독 체계는 정보기관 고위 관리층, 행정부, 사법부, 의회 위원회, 전문가 단체, 옴부즈맨 기관, 최고 감사 기구, 시민 사회, 언론 등 내부 기구와 외부 기구를 모두 활용한다.
- 정보기관 감독 체계를 구성하는 기구들의 위임 사항을 다 합치면 전체 정보 공동체의 적절성, 합법성, 효과성, 효율성이 포함되어야 한다.
- 정보기관 감독 체계 중 적어도 하나의 기구는 정보기관과 행정부 외부의 독립적 민간 기구여야 한다.

- 정보기관에 해당하는 것이 정확히 무엇인지는 기능적으로 정의되어야 한다. 즉, 주요 업무가 국가 안보 정보의 수집, 분석, 유포인 국가 조직은 정보기관이다.
- 정보기관 활동의 감시는 사전, 중도, 사후 감독으로 이루어지는 정보기관 감독 주기 전체를 포괄해야 한다.
- 정보기관 감독 체계의 효과성은 독립적 기구가 정기적으로 평가해야 한다.
- 정보기관 감독 기구는 모범 관행의 파악과 공유를 위해 해외의 정보기관 감독 기구들과 정기적으로 연락을 주고받아야 한다.

후주(後註)

1. 이 도구 모음에서는 공공 서비스 수행을 강조하기 위해 *정보국(intelligence agency), 정보 기구(intelligence body)* 대신 *정보기관(intelligence service)*이라는 용어를 사용한다.

2. Organisation for Economic Co-operation and Development, OECD DAC *Handbook on Security System Reform: Supporting Security and Justice* (Paris: OECD, 2007), p. 140.

3. 민간 계약업체에 관한 정보는 Tim Shorrock, Spies for *Hire: The Secret World of Intelligence Outsourcing* (New York: Simon & Schuster, 2008) 참조.

4. 공공 기관에 대한 책임 추궁의 의미에 관한 더 자세한 논의는 Mark Bovens, "Public Accountability," in The *Oxford Handbook of Public Management,* eds. Ewan Ferlie, Laurence E. Lynne Jr, and Christopher Pollitt (Oxford: Oxford University Press, 2005) 참조.

5. Council of Europe, European Commission for Democracy through Law (Venice Commission), *Report on the democratic oversight of the security services,* CDL-AD(2007)016 (2007), Paragraph 73.

6. 예컨대 Ronnie Kasrils, "To spy or not to spy? Intelligence and democracy in South Africa," in *To spy or not to spy? Intelligence and democracy in South Africa,* ed. Lauren Hutton (Pretoria: Institute for Security Studies, 2009), pp. 9–20 참조.

7. 예컨대 United States, Department of Defense, "Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))," Directive No. 5148.11, 21 May 2004 참조.

8. Bulgaria, Law on State Agency for National Security, 40th Session of the National Assembly, Article 88.

9. Bosnia and Herzegovina, Law on the Intelligence and Security Agency, 22 March 2004, Article 42.

10. South Africa, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10 September 2008), p. 77.

11. 네덜란드에서는 이미 1848년에 장관 책임의 헌법상 기초가 마련되었다. A. D. Belinfante, Beginselen van Nederlands Staatsrecht [Principles of Dutch Constitutional Law] (Alphen aan de Rijn: Samson Publishers, 1981), pp. 64 - 66 참조.

12. Christian Heyer, "Parliamentary Oversight of Intelligence: The German Approach," in *Intelligence and Human Rights in the Era of Global Terrorism*, ed. Steve Tsang (Westport, CT: Praeger Security International, 2007), p. 69.

13. Council of Europe, European Commission for Democracy through Law (Venice Commission), *Report on the democratic oversight of the security services*, CDL-AD(2007)016 (2007), Paragraph 78.

14. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (McDonald Commission), First Report: Security and Information (October 9, 1979), p. 425.

15. 일부 국가들은 독립적 전문가와 전직 의원이 위원으로 참여하는 혼합식 감독 기구를 활용한다.

16.United Kingdom, Intelligence and Security Committee, *Annual Report 2001 – 2002,* CM 5542 (2002), pp. 46 – 50 참조.

17.더 자세한 내용은 Australia, Inspector-General of Intelligence and Security Act 1986, Act No. 101 of 1986 as amended 및 정보보안감찰관 웹사이트(http://www.igis.gov.au/) 참조.

18.Ian Leigh, "National courts and international intelligence cooperation," in *International intelligence cooperation and accountability,* eds. Hans Born, Ian Leigh, and Aidan Wills (London: Routledge, 2011), p. 232.

19.Frederic Manget, "Another system of oversight: intelligence and the rise of judicial intervention," in *Strategic intelligence: A window into a secret world,* eds. Loch Johnson and James Wirtz (Los Angeles: Roxbury, 2004), pp. 407 – 409.

20.Ian Leigh, "National courts and international intelligence cooperation," in *International intelligence cooperation and accountability,* eds. Hans Born, Ian Leigh, and Aidan Wills (London: Routledge, 2011), p. 232.

21.The Netherlands, Act of 7 February 2002, providing for rules relating to the intelligence and security services and amendment of several acts (Intelligence and Security Services Act 2002), Article 83, Paragraph 1, p. 31.

22.Ibid., Article 84, Paragraph 1, p. 31.

23.Dana Priest and William M. Arkin, "Top Secret America: A Washington Post Investigation," *The Washington Post,* four-part article series, July – December 2010
(available at http://projects.washingtonpost.com/top-secret-america/;

accessed 18 November 2011).

24.The Netherlands, Review Committee on the Intelligence and Security Services (CTIVD), *Annual Report: 2010–2011,* pp. 8–9.

25.Norway, The Act relating to the Monitoring of Intelligence, Surveillance and Security Services, Act No. 7 of 3 February 1995, Section 2.

26.Ibid., Section 2.

27.Ibid., Section 8, Paragraph 2.

28.Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), p. 17.

29. Ibid., p. 17.

30.일반적으로 민원은 이미 발생한 사건과 관련되지만 때로는 진행 중이거나 계획 단계에 머무른 업무와도 관련될 수 있음에 유의할 필요가 있다.

31.Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" in *Accountability for Criminal Justice: Selected Essays,* ed. Philip C. Stenning (Toronto: University of Toronto Press, 1995).

32.Cyrille Fijnaut, *Het Toezicht op de Inlichtingen- en Veiligheidsdiensten: de noodzaak van krachtiger samenspel* [The oversight of security and intelligence services: the need for closer cooperation] (The Hague, April 2012) (in Dutch).

33.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,* United Nations Document A/HRC/14/46 (17 May 2010).

도구 2

효과적인 정보기관 감독체계 구축

스튜어트 파슨(Stuart Farson)

2 효과적인 정보기관 감독체계 구축

스튜어트 파슨(Stuart Farson)

1. 머리말

이 도구에서는 안보 부문 개혁의 주요 주제 중 하나인 전환기 국가에서의 효과적인 정보기관 감독 및 책임 메커니즘(특히 입법부의 메커니즘)의 구축에 관해 검토한다. 당장 떠오르는 질문은 정착된 민주주의에서 사용되는 메커니즘이 아직 민주적 거버넌스 방식을 발전, 확대시키고 있는 국가들에게 적절한 모델인가이다. 그 대답은 전환기 국가의 특징에 따라 달라지는데, 전환기 국가의 정보기관이 수행해야 하는 업무, 활동의 범위와 규모, 그리고 전환기 국가가 처한 구체적 위협 환경 등을 고려해야 한다. 이러한 요인들을 분석할 때 더 광범위한 문제, 특히 민주적 정치 문화의 발전 정도 및 널리 인정되는 민주적 관행의 편입 정도 또한 고려해야 한다.

정부 제도를 민주적 통제 하에 두고 책임을 지게 만드는 일은 민주주의의 가장 중요한 과제 중 하나이다. 하지만 민주국가들이 이를 달성하는 방식은 다양하다. 정부에 책임을 묻는 일을 의회에 의존하는 나라들도 있고, 다양한 전문가 기구들이 통합된 혼합형 제도를 갖고 있는 나라들도 있다. 흔히 감독이라고 불리는 이 과정의 효과성은 무엇을 어디서, 언제, 얼마나 자주 면밀히 검토할지를 결정할 수 있는, 법률과 헌법에서 비롯되는 권한뿐 아니라 감독 기구가 입수할 수 있는 정보의 범위에도 좌우된다. 지식을 획득하고 제도적 기억(institutional memory)을 유지할 능력 없이는 어떤 감독 기구도 목표 달성을 위해 어디를 살펴봐야 하고 어떤 질문을 해야 하는지 아는 데 필요한 전문성을 발전시킬 수 없을 것이다.

군대의 민주적 통제를 위한 제네바 센터(DCAF) 같은 독립적 기관은 최근 들어 특히 정보기관 감독과 관련된 안보 부문 개혁을 위한 법적 표준과 모범 관행을 개발하기 위해 많은 일을 해 왔다.[1] 동시에 학자들은 정보기관 감

독 기구에 관한 연구 결과를 내놓는 것 외에도 비교 관점에서 정보기관의 기능과 감독을 분석하려 시도해 왔다.[2] 그러나 감독 모델들의 효과성을 통시적으로 파악하려 시도한 연구는 대체로 드물다.[3] 이와 관련해서는 영국과 미국의 사례에 관한 연구만 나와 있는 실정이다.[4]

감독 효과성 연구의 수적 부족은 감독 제도들을 비교해 그 중 어느 하나를 추천하려 할 때 제약 요소가 된다. 첫째, 통시적 평가가 포함되지 않은 감독 체계 검토는 비교 가치를 제한했다(감독 체계의 가치는 연구되는 감독 방식에서 발견되는 문제에 있을 공산이 크다). 둘째, 통시적으로 연구된 영국과 미국의 감독 체계가 전환기 국가들에게 최선의 모델이 아닐 수도 있다. 예를 들어 미국의 정보 조직의 범위와 규모, 많은 예산, 그리고 민간 부문의 참여 정도 때문에 미국 정보기관 감독에 대한 검토는 그 상황이 아예 다른 전환기 국가에는 그다지 가치가 없다.

이 도구의 다음 절에서는 다양한 민주적 거버넌스 형식을 구분하면서 전환기 국가들의 성격을 살펴본다. 세 번째 절에서는 효과적 감독의 특징을 논의한다. 네 번째 절에서는 다양한 국가에서 개발된 감독에 대한 제도적 접근 방식을 확인하고, 그 장단점에 주목한다. 다섯 번째 절에서는 효과적 감독의 장애물을 분석하고, 여섯 번째 절에서는 감독 기구가 작동하기 위해 필요한 법적 위임 사항에 관해 논의한다. 마지막으로 이 도구는 몇 가지 주요 권고 사항으로 끝맺는다.

2. 전환기 국가

민주적 거버넌스 방식을 발전시키는 과정에 있는 나라들을 흔히 전환기 국가(transition state)라고 한다. 이 나라들은 민주화 경험을 공유하고 있다는 점에서는 공통적이지만 출발점은 물론 선택하는 민주주의 형식에서도 달라 그 나머지는 공통점이 거의 없을 수 있다. 중간에 전체주의를 경험하기 전에 한때 민주주의 국가였던 나라도 있고, 국가 분열로 새로 세워진 신생국가들도 있을 것이며, 부족 지배, 심각한 민족 분열, 심지어 내전을 경험한 나라도 있을 수 있다. 부분적으로는 이들의 다양한 역사에 따라 그 민주주의가 취할

방향도 달라질 것이다. 단일 국가를 세우는 나라도 있을 것이고, 연방 국가를 세우는 나라도 있을 것이다. 어떤 나라는 행정부 권력에 대한 견제와 균형이 뚜렷한 대통령제를 세울 것이고 어떤 나라는 입법부와 행정부가 합쳐진 의원 내각제를 선택할 것이다. 입헌 군주제가 되는 나라도 있겠고, 공화국이 되는 나라도 있을 것이다. 단순 다수 대표제 선거 제도를 갖는 나라도 있는가 하면 비례 대표제 형식을 취하는 나라도 있을 것이다. 단원제 의회를 갖는 나라가 있는가 하면 양원제 의회를 택하는 나라도 있을 것이다. 뿐만 아니라 사법 체계도 다르기 십상이다.

각각의 전환기 국가의 이 모든 선택이 합쳐져 그 나라가 발전시키는 정치 문화의 유형에 직접적 영향을 미칠 것이다.

민주주의 국가의 정치 문화, 특히 대중이 민주적 이상을 수용하는 정도는 이러한 이상을 실현하는 방식을 결정한다. 예를 들어 어떤 나라의 행정부 구성원들은 다른 나라의 행정부 구성원들보다 그들의 행위에 대한 공적 책임을 받아들이는 데 더 적극적일 수 있다. 마찬가지로 입법부 책임의 발전 정도도 나라마다 다르다. 많은 경우, 민주적 거버넌스를 향한 이러한 발전에 영향을 미치는 것은 탈 민주화(de-democratization)를[5] 향한 움직임인데, 국가의 도구를 자신의 권력 유지에 사용하려는, 권력자들의 고질적 성향과 더 일반적으로는 부패가 그 원동력이 된다.

민주적 거버넌스라는 용어조차 나라마다 의미가 다를 수 있는데, 정보기관 감독이라는 구체적 맥락에서 사용될 때 특히 그렇다. 예를 들어 *책임(accountability)*은 일반적으로 해명을 하는 과정을 뜻하는 것으로 이해되며, 더 막연하게는 투명성을 의미한다. 그러나 웨스트민스터 모델에 따르는 영연방 국가들에서 *책임*은 내각의 주무장관이 해당 장관직에 속한 조직의 행위(또는 부작위)에 대해 의회 내에서, 또 의회를 상대로 정직한 해명을 할 구체적인 헌법적 의무도 가리킨다. 그 밖에 다양한 의미를 갖는 용어들로는 *위협, 위험, 국가 안보, 독립성, 재량, 권능, 보안, 정보 및 감독* 자체가 포함된다.

3. 효과적 감독

모든 입법부는 정보기관 감독 체계 설립에 앞서 그 체계가 과연 효과적일지 판단하고 싶을 것이다. 지금은 이 주제에 관해 새로 나온 문헌이 워낙 많아서 이런 판단이 쉬우리라고 생각할지도 모른다. 그러나 몇 가지 경고를 해둬야겠다. 몇몇 학자가 특정 감독 기구의 기능을 설명하는 유용한 연구를 최근에 내놓기는 했지만 이들 기구의 효과성을 충분히 자세하면서도 유의미한 결론을 내릴 수 있을 만큼 충분히 긴 기간에 걸쳐 검토한 연구는 극히 드물다. (안타깝게도 충분히 긴 기간을 고려한 극소수의 연구들마저 효과성을 판단할 만한 유용한 기준을 내놓지 못했다.)

더욱 난감한 것은 행정부와 입법부가 추구하는 감독 목표가 상이한 경향을 띤다는 점이다. 그 결과 많은 민주국가들은 복수의 감독 기구들이 그에 상응하는 조사 형식을 통해 다양한 목표들을 아우르는 혼합형 체계를 발전시켰다. 이런 체계에서는 입법부 감독 기구가 전문가 감독 기구와 나란히 존재하면서 상호 조정이 이루어지기도 하고 그렇지 않기도 한다.

어떤 체계가 존재하건 의원들이 감독 기구의 활동에 관해 알고, 제때 정보를 받으며, 이러한 기구의 보고서에 쉽게 접근할 수 있는 것이 중요하지만 늘 그렇지는 못했다. 가장 중요한 것은 의원들이 정보기관 감독을 통해 달성해야 할 목표를 늘 염두에 두어야 한다는 것이다. 그렇지 않을 경우, 현실적이기보다는 상징적인 접근 방식이라는 수렁에 빠질 수 있다.[6] 이 목표는 분명 간단한 것이며, 다른 모든 정부 기관에게도 마찬가지다. 정보기관이 하는 일을 통제하는 것이 아니라[7] 대중이 알 수 있고 이해할 수 있는 방식으로 정보기관과 행정부가 그들의 행위와 부작위에 대해 책임을 지도록 하는 것이다. 그렇기는 해도 정보기관 활동비용 충당을 위한 공공 자금 집행의 검토와 승인 및 이에 관련된 법의 채택 또는 수정이라는 의회의 최소 두 가지의 주요 책임에서 통제의 요소가 비롯될 수 있다.

의원들은 감독 책임을 이행하기 위해 그들의 역량, 성향, 한계를 평가해야 한다. 시간 부족, 한정된 전문성과 부족한 자원은 모두 현실적으로 달성 가

능한 성과에 영향을 미칠 수 있다. 따라서 의원들은 그들이 달성하고자 하는 것과 이를 의회의 업무 주기 내에 달성할 수 있는 방법을 고심해야 한다. 특정 감독 업무는 어쩌면 전문가 감독 기구가 더 적합할 수도 있다. 그 경우, 의회와 해당 기구와의 관계는 어떻게 될 것인가?

일반적으로 의회는 두 가지 특정 방식으로 정보기관 감독에 관여해야 하는데, 하나는 준수(compliance)와 관련되고 다른 하나는 효능(efficacy)과 관련된다. 구체적으로 의회는 정보기관과 그 계약업체들이 법률과 기관 규정 또는 정부 정책을 위반하지 않도록 해야 한다. 또한 공공 자금이 적절하고 효과적으로 사용되도록 해야 한다.

의원들은 너무도 자주 그들의 가장 중요한 책임이 정보기관의 활동을 소급 심사하는 것, 다시 말해 사후에 조사를 수행하는 것이라고 가정한다. 이것은 부분적으로만 옳다. 조사가 상당 부분 사후에야 가능하고 그래야 하는 것은 맞지만 그럼에도 불구하고 의원들은 정보 업무가 이루어지기 전과 이루어지고 있는 동안에 일부 조사를 수행할 책임이 있다. 예를 들어 의원들은 업무가 이루어지기 전에 필요한 규정과 정부 정책이 제대로 갖춰져 있는지 확인할 책임이 있다. 마찬가지로 효능은 사후에만 판단이 가능하지만 역량과 성과 기준은 사전에 또 도중에 평가되어야 한다.

4. 감독에 대한 접근 방법

본 절에서는 다양한 민주주의 국가에서 현재 시행 중인 세 가지 감독 방식을 분석한다. 이들은 각각 다음과 같다.

- 입법부 위원회 방식
- 감찰관 방식
- 외부 감독 기구 방식

여기서 *입법부 위원회(legislative committee)*라는 용어는 의회 위원회뿐 아니라 스스로를 의회로 칭하지 않는 입법 기관의 위원회를 총칭하는 것으로 사용된다.

4.1 입법부 위원회

입법부 위원회는 유형과 지위가 다양하다. 웨스트민스터 모델을 따르는 국가처럼 일부 국가의 입법부 위원회는 입법부의 선출직 구성원과 행정부가 일정 정도 혼합 또는 중첩될 수 있다. 전혀 중첩되지 않는 나라들도 있다.[8]

먼저 의회 제도에 존재하는 입법부 위원회와 의회 민주주의에서 볼 수 있는 입법부 위원회를 구별하는 것이 중요하다. 가장 중요한 것은 책임성에 대한 접근 방식의 차이이다. 권력 분립이 3부의 상호 견제를 장려하는 미국에서는 어떤 정보를 받을 것이고, 위원회 증언에서 어떤 사안을 검토할지를 의회 단독으로 결정한다. 의회에 독점적으로 부여되는 공공 자금 지출 승인 및 법률 제정 권한은, 몇몇 주목할 만한 예외는 있지만, 의회의 의지가 존중되도록 한다. 따라서 미국의 의회 위원회는 전체 행정부 고위 관료들로부터 정기적으로 증언을 청취하는데, 여기 포함되는 정보기관의 관리 책임자도 정책 및 관리에 관한 질문에 충분히 답하게 되어 있다. (미국 행정부의 선출직 구성원, 즉 대통령과 부통령은 의회에서 증언하지 않는다.)

반면 대부분의 의원내각제에서는 어떤 기밀 정보를 입법부 위원회와 공유할 것인지에 대한 최종 결정권이 행정부에게 있는데, 단순하게 집권당이 당연히 의회의 다수파를 장악하기 때문이다. 누가 위원회에 출석하고 어떤 주제에 관한 질문에 답할지에 관해서도 뚜렷한 차이가 있다. 일부 의원내각제 국가에서는 행정부의 선출직 구성원이 정책 사안에 관해 답변하기 위해 입법부 위원회에 출석하기도 하고 다른 행정부 관료들은 행정 사안에 관한 발언을 위해 재량에 따라 출석할 수 있다.

4.1.1 미국과 브라질의 의회식 접근법

미국에서는 1970년대의 처치 위원회와 파이크 위원회 조사의 결과로 의회는 하원과 상원에 상임 정보 위원회를 두기로 결정했다. 이들 위원회는 모든 미국 정보활동을 효능뿐 아니라 적절성까지 감안해 조사하는 일을 맡았다. 안전한 장소에서 회의를 갖고, 기밀 취급 인가된 광범위한 보좌진의 도움을 받는 이 위원회들에게는 사전, 중간, 사후에 감독을 실시할 권한이 부여된다. 미국

국내 정보활동을 조사할 책임은 현재 법무부와 국토안보부 업무를 감독하는 의회 위원회에 있다. 여당과 야당이 공동으로 지명하는 위원회 보좌진은 소속 정당 구성원에게 다양한 서비스를 제공한다. 이를 보완하는 것은 의회조사국과 회계감사원 같은 중요한 의회 지원 기관이 제공하는 서비스이다.

의회 제도의 또 다른 예가 브라질에 있는데, 브라질은 최근에 군부 통치에서 연방 민주주의로의 전환을 이뤄냈다. 1985년의 민정 전환 후 적어도 10년 동안은 브라질 새 행정부의 관심이 경제와 막대한 해외 부채 같은 시급한 문제에 쏠려 있었다. 여기에 브라질에는 외적이 없다는 광범위한 인식이 더해져 정보 부문을 개혁해야 할 절박함이 없었던 것이다.[9] 그러나 보다 최근에 들어 브라질 의회는 시스템을 개편했을 뿐 아니라 정보기관을 통제하기 위한 일련의 의회 위원회들을 설립했다. 1999년, 브라질 의회는 합동정보활동통제위원회(CCAI: Joint Commission for the Control of Intelligence Activities)를 설립했다. 브라질 의회는 그 이후로 상하 양원에 국방 위원회를, 하원에 조직범죄방지공공안보위원회(Commission of Public Security against Organized Crime)를, 상원 헌법정의시민위원회(Senate Commission of Constitution, Justice, and Citizenship)에 상임 공공 안보 소위원회를 설립하는 등 4개의 위원회를 신설했다. 비록 CCAI가 초기에 의회의 관심 부족으로 위원회 내규 합의에 실패하고 기술 자원과 인력이 충분히 제공되지 않아 어려움을 겪긴 했지만[10] 이 위원회들은 모두 투명성을 높이는 데 성공을 거두었다.

4.1.2 의원 내각제식 접근법

정보기관 감독에 대한 의원 내각제식 접근법은 의회식 접근법과도 다르지만 같은 내각제식 접근법 안에서도 차이가 있다.[11] 주요 차이점은 기밀 정보에 대한 접근, 인력 및 기타 자원의 가용성, 위원회의 위임 사항, 구성원 지명 방식과 관련된다.

현재 의원 내각제에서 시행되고 있는 정보기관 감독 방식은 최소한 다음 다섯 가지이다.

- 기밀 취급 그룹(secrecy loop) 외부의 의회 위원회

- 법정(法定) 의원 위원회
- 법정 의회 상임 위원회
- 법정 특별 심의 위원회
- 혼합형 위원회 및 체계

비밀주의 그룹 외부의 의회 위원회

일부 내각제 민주주의(캐나다, 아일랜드 등)의 경우, 행정부는 의회 위원회가 기밀 정보를 볼 수 있도록 하는 특별한 제도를 두고 있지 않다. 따라서 기밀 정보 취급 허가를 받은 기밀 취급 그룹 내부자가 이러한 정보를 의회 구성원에게 "누출"할 경우, 형사상 범죄가 될 수 있다. 그 결과 이들 민주주의의 의회 위원회는 정보 업무에 관한 어떠한 "내부" 지식도 없이 운영되어야 한다. 그러나 이들 위원회가 완전히 무력한 것은 아니다. 여전히 전면적 조사 권한과 사용 가능한 의회 자원이 있기 때문에 유용한 조사를 실시할 수 있고 중요한 쟁점에 대한 정부의 관심을 촉구할 수 있다.[12]

이 접근법과 관련하여 유의할 점이 두 가지 더 있다. 첫째, 충분히 다룰 수 없는 사안들이 분명 있다. 예를 들어 전문가 감독 기구가 특정 사안을 제기하는 경우, 의회에 이를 쉽게 알릴 수 없다. 둘째, 위임 사항이 확실히 규정되어 있지 않으면 위원회가 다룰 사안이 다소 비체계적으로 선정될 것이다. 위원회의 지도부가 바뀌면 의제와 관행, 제도적 기억도 바뀔 것이다.

법정 의원 위원회

영국에서 시행되고 있는 두 번째 접근법은 의원들로 이루어진 법정 위원회와 관련된다.[13] 의회의 특권이 아닌 입법에 의해 창설된 영국 정보보안위원회(ISC)는 하원과 상원의 의원들로 구성되며, 의회 위원회의 경우처럼 정당이 선정하는 것이 아니라 ISC가 보고를 올리는 총리에 의해 선정된다. 그 이유는 ISC가 실제로는 의회 위원회가 아니기 때문이다. 예컨대 ISC는 의회 위원회에 있는 조사 권한이 없으며, 일반적인 의회 자원과 특전을 활용할 수 없다. ISC는 오히려 의원 위원회(committee of parliamentarians)에 가깝다.

ISC의 주요 장점은 기밀 취급 그룹 내부에서 운영되며, 기밀 취급 인가를 받은 보좌진과 함께 보안이 유지되는 환경에서 회의를 갖는다는 점이다. 또 다른 장점은 연속성이다. 상원에서 뽑힌 위원회 위원들은 하원에서 뽑힌 동료들과는 달리 재선을 추구할 필요가 없다. 따라서 연속성이 향상되고 제도적 기억이 발전될 가능성이 높다.

반면 ISC의 법정 위임 사항은 제한적이어서 주요 정보기관의 지출, 행정, 정책만을 포함한다. 조사 자원 또한 제한된다. 최근에 보강되기는 했지만 여전히 바람직한 수준에는 못 미친다. 결과적으로 영국식 접근법은 이론의 여지는 있지만 감독의 중요한 측면인, 사건들의 지속적 모니터링에 걸림돌이 되기 쉽다.

ISC를 의회의 통제 하에 두려는 노력은 지금까지는 실패했지만 정당들의 역할은 커졌다. 현재 정당들은 ISC 위원의 선정에 강력한 영향력을 행사하며, 의회에서 ISC 보고서의 수정 (공개) 버전에 관해 논의할 시간이 정기적으로 따로 책정된다.[14]

법정 의회 상임 위원회

법정 의회 정보 상임 위원회는 실제로 의회 위원회라는 점에서 영국식 방식과 다르다. 위원들은 정당이 지명하며, 의회의 자원을 필요에 따라 활용할 수 있다.

직원들이 행정부의 뜻에 따라 직무를 수행하는 ISC와는 달리 의회 상임 위원회는 어떤 직원(기밀 취급 인가가 있는)을 고용할 것인지는 물론 (보안 장소임을 전제로) 어디서 회의를 가질 것인지 등 위원회의 행동 대부분을 스스로 결정할 수 있다.

위원 자격 요건은 나라마다 다르다. 예컨대 남아공은 비례 대표가 원칙이며, 위원회에서 모든 주요 정당이 대표되어야 한다. 뉴질랜드의 경우, 총리와 야당 지도자 모두 위원회 위원이어야 한다. 호주에서는 연방 의회의 양원에서 위원을 뽑아야 한다.

이런 의회 상임 위원회를 설립하는 법률은 일반적으로 위원회가 어떤 조직을 조사할 수 있는지 명시한다. 특정 행위가 제외되는 경우도 있지만 소관 사항은 상당히 광범위할 수 있다. 예를 들어 호주의 경우, 의회 정보보안합동위원회(PJCIS: Parliamentary Joint Committee on Intelligence and Security)는 호주의 주요 정보 조직 모두를 조사할 권한이 있다. 다만 이 위원회가 조사할 수 없는 활동 역시 많다(상자 1 참조).

상자 1: 호주 의회 정보보안합동위원회의 위임 사항의 한계

위원회의 직무에는 다음이 포함되지 않는다.

a. 호주 안보정보원(ASIO: Australian Security Intelligence Organisation), 호주 비밀정보국(ASIS: Australian Secret Intelligence Service), 국방화상지형국(DIGO: Defence Imagery and Geospatial Organisation), 국방정보원(DIO: Defence Intelligence Organisation), 국방암호이사회(DSD: Defence Signals Directorate) 또는 국립평가원(ONA: Office of National Assessments)의 정보수집 및 평가 우선순위의 심의

b. ASIO, ASIS, DIGO, DIO, DSD 또는 ONA가 사용 가능한 정보 출처, 기타 운영 지원 또는 운영 방법의 심의

c. ASIO, ASIS, DIGO, DIO 또는 DSD가 수행했거나 수행 중이거나 제안한 특정 업무의 심의

d. 외국 정부가 공개에 동의하지 아니하는 경우, 해당 정부나 그 기관이 제공하는 정보의 심의

e. 호주 국민에게 영향을 미치지 아니하는 ASIO, ASIS, DIGO, DIO, DSD 또는 ONA 활동 측면의 심의

f. 이 법의 15조에 따라 만들어진 규칙의 심의

g. ASIO, ASIS, DIGO, DIO, DSD 또는 ONA의 활동에 관한 개별적 민원에 대한 조사의 실시

h. DIO 또는 ONA가 하는 평가나 보고의 내용 또는 평가나 보고에서 도달한 결론의 심의 또는 그러한 평가나 보고의 근거가 되는 정보 출처의 심의

i. ONA가 수행하는 조정 및 평가 활동의 심의.[15]

법정 의원 위원회와 법정 의회 상임 위원회 사이의 중요한 차이는 권한과 특전이다. 후자는 위원회의 요청, 특히 문서 및 기록 제출 요청에 불응하는 당사자를 의회 모독죄로 고발할 수 있다. 또한 호주 법률은 상원이나 하원은 주요 정보기관과 관련된 "일체의 사안"을 심의를 위해 PJCIS(의회 정보보안 합동위원회)에 회부할 수 있다고 명시하고 있다.[16]

법정 특별 심의 위원회

적어도 한 국가(캐나다)에서 몇 년간 정보 법률이 시행된 후 정보 법률 검토를 맡을 법정 심의 위원회의 설립을 장래 의회의 의무로 규정했다. 1984년 캐나다 보안정보국법 및 안보범죄처벌법 채택 시 특별히 내건 조건은 이 법들이 제정된 지 5년 후에 의회가 이들 법을 심의할 위원회를 설립하는 것이었다.[17] 2001년에 채택된 캐나다 테러방지법도 유사하게 3년 후 의회가 심의 위원회를 설립할 의무를 규정했다.[18] 각 경우, 위원회의 위임 사항은 법 조항과 운영을 검토하고, 위원회가 필요하다고 보는 변경 관련 권고 사항을 의회 보고서에 포함시키는 것이었다.

임시적 성격을 갖는 이 위원회들의 존속 기간 중 1년은 보고 기한으로 고정되어 있었다. 이들 위원회는 기밀 취급 그룹 내에 있는 것으로 인식되지 않았기 때문에 역시 이들 법령에 의해 설립된 전문가 감독 기구로부터 거의 지원을 받지 못 했다.[19]

혼합형 위원회 및 체계

많은 나라에서 입법부 구성원이 아닌 자뿐만 아니라 행정부나 입법부에 속하지 않는 자들을 포함하는 혼합형 위원회를 설립했다.

스웨덴의 보안 및 무결성 보호 위원회

가령 스웨덴에서는 보안 및 무결성 보호 위원회(SAKINT)의 위원장과 부위원장은 판사로 재직했거나 그에 상당하는 법조인으로서의 경험이 있어야 한다. 최대 10명에 이르는 위원회의 나머지 위원들은 스웨덴 의회(Riksdag) 내 정당 그룹이 추천하는 후보자 중에서 지명되는데, 현직 의원일 수도 있고 아닐 수도 있다.

SAKINT의 두 가지 주요 책무는 범죄 수사 기관의 비밀 감시, 신분 위조 및 관련 특별 수사 기법의 사용을 감독하고, 스웨덴 보안국(Swedish Security Service)의 개인정보 처리를 감독하는 것이다. SAKINT는 주로 조사를 통해 이 책무를 이행하는데, 조사의 목적은 스웨덴 법규 준수를 보장하는 것이다.

SAKINT는 활동 과정에서 정부가 임명한 책임자가 이끄는 보좌진의 지원을 받는다. SAKINT를 설립하는 법률은 이 위원회에 위원회 감독 대상인 행정부 기관으로부터 정보와 지원을 얻을 권한을 부여하고 있다. 이 위원회는 또 감독 대상이 아닌 기관에서도 정보를 얻을 수 있다. SAKINT는 매년 정부에 보고할 의무가 있다. 스웨덴 의회와 관련해서 그러한 의무는 없다.

독일의 혼합형 체계

독일의 정보기관 감독 체계도 혼합형이라는 점에서 비슷하다. 함께 운영되는 몇 개의 기구로 구성되어 있기 때문에 일각에서는 이를 "다자형(multilateral)"이라고 불렀다.[20] 주요 기구는 독일 연방 의회 하원(Bundestag)의 상임 정보기관 감독 패널인 PKG(Parliamentary Control Panel)이다. PKG는 법률에 의해 분기마다 최소 1회 회의를 가져야 한다. PKG의 구성은 연방 의회의 정당 구성을 반영하고 있지만 의장직은 매년 여당과 야당이 번갈아 맡는다. 위원회 위원들의 업무는 7인으로 구성된 사무국이 보조한다. 이들은 3개 연방 정보기관의 활동에 초점을 맞추어 비공개로 심의한다. 위원회는 정보기관 인력을 소환해 증언을 청취할 수 있고, 필요 시 문서를 요구할 수 있으며, 언제든 정보기관 부지에 출입할 수 있다. PKG는 선거 기간 도중 및 종료 시 연방 의회에 보고해야 한다.

두 번째 기구인 기밀위원회(Confidential Committee)는 정보기관 예산 조사를 담당한다(예산안에 포함시키기 위해 연방 의회 예산위원회에 제출하는 총액). 중요한 것은 PKG와 기밀위원회가 예산 논의 시 합동 회의를 가질 때가 있다는 점이다. (자세한 내용은 도구 8 참조).

독일의 혼합형 체계의 마지막 구성 요소인 G10 위원회는 독립적인 준사법 기구로 그 결정은 정보기관과 정부에 구속력을 갖는다. PKG가 선정하는 G10 위원회 위원 4명은 연방 의회 하원 의원일 수도 있지만 꼭 그래야 하는 법은 없다.

G10 위원회는 처음에는 정보기관에 의한 우편 및 통신 감청을 인가하고 감독하기 위해 설립되었다. 그러나 2007년에 채택된 테러방지법 개정으로 정보기관에 새로운 권한이 부여되면서 G10 위원회의 역할도 바뀌었다. 이제 정보기관들은 통신 서비스 공급자에게 작동 중인 휴대전화 위치, 일련 번호 또는 카드 암호를 밝힐 수 있는 데이터를 요청하기 전에 G10 위원회로부터 사전 승인을 받아야 한다.

4.2 감찰관

본 절에서는 입법을 통한 감찰관(IG) 설립에 대한 세 가지 상이한 접근 방식을 검토한다.[21] 첫 번째 방식은 미국에서 개발된 이후 다른 두 방식의 모델 역할을 해 왔다. 그렇지만 이 방식들은 IG 고용 주체, IG의 보고 대상, 보고 관련 주제 면에서 상당히 다르다. 다양한 IG의 실제 경험 역시 달라서 핵심 인력과 필요한 정보에 대한 접근의 정도도 상이하다.

4.2.1 미국 중앙정보국 감찰관

1978년 감찰관법에서는 미국 정부의 모든 주요 부처에 감찰관을 두도록 규정하고 있지만 이미 자체 전담 감찰관이 있었던 중앙정보국에는 적용되지 않았다. 1952년에 처음 창설된 CIA 감찰관(IG-CIA)은 1978년에도 여전히 CIA 국장에 의해 임명되었고, 독립성이 부족하다는 것이 다수 의견이었다. 1989년이 되어서야 IG-CIA는 마침내 법적 근거와 더 큰 독립성을 갖게 되었다. IG-CIA는 여전히 CIA 직원이며, CIA 국장에게 계속 보고하지만 이제는 대통령이 지명하고 상원이 확정하는 자가 이 직위에 오르며, 대통령만이 해임할 수 있다.

IG-CIA의 역할은 주로 CIA 내부의 경제성, 효율성, 효과성, 책임성을 증진하는 것이다. 감찰관은 CIA 프로그램과 운영에 대한 독립적 감사, 검사, 조사,

검토를 통해 이 역할을 수행한다. IG-CIA는 또 부정행위, 낭비, 남용, 관리 부실을 적발하고 방지할 책임이 있다. 보고와 관련하여 IG-CIA는 조사 결과와 권고 사항을 CIA 국장과 의회 정보 위원회에 신속히 알려야 한다. 조사 결과가 법률 위반 혐의와 관련이 있는 경우에는 법무장관에게도 알려야 한다.[22]

4.2.2 캐나다 보안 정보기관 감찰관

자신이 감독하는 기관의 직원인 IG-CIA와는 달리 캐나다 보안 정보기관 감찰실(OIG-CSIS: Office of the Inspector General of the Canadian Security Intelligence Service)은 정보기관의 직원이 아니라 내각이 지명하는 공공안전부 소속으로 공공안전차관에게 보고한다. 1984년 캐나다 보안정보국법에 따라 창설된 OIG-CSIS의 위임 사항은 IG-CIA보다 훨씬 제한적이어서 캐나다 법률, 규정, 정책의 준수에 전적으로 초점이 맞춰져 있다. OIG-CSIS는 12개월마다 CSIS 국장이 기관의 운영 활동에 관해 주무장관에게 제출하는 보고서를 검토해야 한다. OIG-CSIS는 보고서를 확인하고 CSIS법에서 승인하지 않거나 장관의 지시에 반하는 일체의 행위를 파악해야 한다. 또 OIG-CSIS는 CSIS 권한의 불합리하거나 불필요한 사용과 관련된 활동도 파악해야 한다.

준거법은 OIG-CSIS가 의무 수행에 필요하다고 생각하는 일체의 정보, 보고, 설명을 CSIS 국장과 그 밖의 CSIS 직원들로부터 받을 권한을 명시적으로 부여하고 있다. 하지만 실제로는 감찰관들이 CSIS 국장과 만나기 어려웠다.

OIG-CSIS는 규정 불이행 사안과 관련해서도 의회와 직접 연락하지 않는다. 사실 의회 의원들은 이 정보를 세 가지 방법으로만 알 수 있다. 즉, 주무장관이 자발적으로 의원들에게 알려주는 경우, 의회 의원들이 정보접근법(Access to Information Act) 요청을 통해 정보를 획득하는 경우 또는 행정부 외부에서 운영되는 전문가 기구인 보안정보심의위원회(SIRC: Security Intelligence Review Committee)가 작성하는 연례 보고서 중에 해당 정보가 포함되어 있는 경우에만 가능하다(아래 4.3절 참조).[23]

4.2.3 호주 정보보안감찰관

호주 정보보안감찰관(AIGIS)은 법적 근거가 있다는 점에서 미국과 캐나다 감찰관과 유사하다. 1986년 정보보안감찰관법에 의해 설립된 이 직위는 어느 부처나 기관의 일부가 아니라 총리직 내에 독립적으로 존재한다.

총독이 지명하는 AIGIS의 소관 사항은 미국과 캐나다의 감찰관보다 훨씬 광범위하다. 호주 감찰관은 하나의 기관만을 조사하는 것이 아니라 전체 호주 정보 공동체를 담당한다. AIGIS가 수행하는 기능은 대상 정보기관에 따라 어느 정도 다르기는 하지만 주요 의무는 다음 네 가지이다.

1. 다양한 기관의 활동에 적용되는 법률, 지시, 지침 준수 모니터링
2. 이들 활동의 적절성 평가
3. 이들 활동의 효과성 평가
4. 이들 활동이 인권에 부합하지 않거나 위배되는지 여부 결정

어쩌면 당연하게도 전통적으로 AIGIS는 대부분의 조사 자원을 호주 안보정보원(ASIO) 문제에 집중시켜 왔는데, ASIO가 주로 국내를 관할하므로 호주의 대외 및 국방 정보기관들보다는 호주 시민의 권리를 침해할 가능성이 더 높기 때문이다. (최근 추정에 따르면 AIGIS 자원의 60 - 70%가 사전 조사 프로그램에 사용된다.[24]) AIGIS는 전면 조사를 실시할 때 왕립 조사 위원회에 주어지는 것과 동일한 조사 권한을 사용할 수 있으며, 또 사용한다. 즉, AIGIS는 증인의 청문회 출석과 정직한 증언을 강제할 수 있다. AIGIS는 문서 제출 강제 권한과 기관 부지 출입 권한도 가지고 있다. 한편, AIGIS는 타당한 사유를 근거로 해서만 해임이 가능하다는 사실에 의해 임기가 보장된다.

준거법에서는 AIGIS가 총리에게 연례 보고서를 제출하며, 총리는 양원에 보고서를 상정해야 한다고 규정하고 있다. 이전에 AIGIS로 재직했던 사람들은 일반적으로 AIGIS를 실질적 변화를 가져올 능력이 있는 감독 기구로 보지 않지만[25] 그럼에도 불구하고 정보기관과 해당 장관들은 AIGIS의 권고 사항을 진지하게 받아들인다.[26]

마지막으로 호주 정보기관들은 AIGIS와 PJCIS(위에서 논의)의 심의 외에도 호주 감사원의 조사도 받는다는 점에 유의해야 한다.

4.3 전문가 감독 기구

전문가 감독 기구는 보통 법령에 의해 설립된다. 전문가 감독 기구를 구별하는 특징은 수행하는 기능, 행정부와 의회로부터의 독립성 정도, 보고 대상, 구성원 선정 방식, 자격 요건 유무 등이다.

4.3.1 캐나다의 보안정보심의위원회(SIRC)와 통신보안국 위원(OCSEC)

캐나다에는 이러한 전문가 감독 기구가 2개 있다. SIRC(Security Intelligence Review Commission)와 OCSEC(Office of the Communications Security Establishment Commissioner Canada)가 그것이다. 행정부와 입법부 외부에서 운영되는 SIRC는 최대 5명의 위원으로 구성되며, 이들은 모두 추밀원 고문이어야 하므로 비밀 서약의 적용을 받는다. 또한 SIRC 위원은 현재 의회 구성원이어서는 안 된다.[27] 원래 기대하던 바는 주무장관 재직을 통한 추밀원 고문 경험이 있는 사람 중에서 SIRC 위원을 뽑는 것이었다. 하지만 늘 그렇지는 않았다. SIRC는 보안 환경에서 회의를 가지며, 기밀 정보 취급 허가가 있는 보좌진을 보유하고 있다. SIRC는 OIG-CSIS의 적합 증명서(certificate of compliance)를 받는 것에 그치지 않고 기관에 대한 민원 조사 권한 등 CSIS 규정 이행을 보장할 자체 위임 사항이 있다(상자 2 참조). 이 점에서 SIRC는 OIG-CSIS 또는 정보기관 자체에서 특정 활동의 심의를 실시하도록 지시할 수 있다.

상자 2: 캐나다 보안정보심의위원회의 위임 사항

이 심의위원회의 직무는 다음과 같다.

a. 일반적으로 기관의 의무와 직무의 수행을 검토하고 그와 관련하여,
   i. 33(3)관에 따라 위원회에 송부된 국장의 보고서와 감찰관의 증명서를 검토
   ii. 6(2)관에 따라 장관이 내린 지시 검토
   iii. 13(2), (3)관 및 17(1)관에 따라 기관이 체결한 약정 검토 및 이러한 약정에 따른 정보 및 첩보 공급의 모니터링
   iv. 20(4)관에 따라 위원회에 제공된 일체의 보고서 또는 의견 검토
   v. 16(3)(a)항에서 언급된 기관에 대한 요청 일체를 모니터링
   vi. 규정 심의
   vii. 기관의 운영 활동에 관한 통계 수집 및 분석
b. 40절에 따라 실시할 심의 준비 또는 심의 실시
c. 다음과 관련한 조사 실시
   i. 41, 42절에 따라 위원회에 제기된 민원
   ii. 시민권법 19절에 따라 위원회에 제출된 보고서
   iii. 캐나다 인권법 45절에 따라 위원회에 회부된 사안[28]

심의 실시에 있어 SIRC는 보고와 설명 등 SIRC가 그 의무와 직무 수행에 필요하다고 생각하면 OIG-CSIS 또는 CSIS 통제 하에 있는 어떠한 정보에도 접근할 권한이 있다. SIRC는 재량에 따라 주무장관에게 보고서를 제출할 수 있지만 주무장관이 의회에 상정할 수 있는 연례 보고서는 항상 제출해야 한다. SIRC가 연례 보고서의 내용을 달리 결정할 수는 있지만 연례 보고서에서 기밀 정보가 공개되어서는 안 된다.

원래는 SIRC의 연례 보고서가 효과적인 정보기관 감독 수행에 필요한 정보를 의회에 제공해 줄 것으로 기대되었다. 하지만 실제로 SIRC가 늘 협조적인 것은 아니었다.[29]

CSIS법 및 안보범죄처벌법 심의에 관한 하원 특별 위원회(위의 4.1.2절 참조)가 SIRC와 OIG-CSIS 각각의 역할을 검토하기 위한 회의를 열었을 때, 위원들은 OIG-CSIS의 기능을 왜 SIRC의 기능 안에 포함시킬 수 없는지 이해하지 못해 당황했다. 당시 주무장관은 특별 위원회에게 OIG-CSIS가 중요하고 두 기구가 모두 필요하다는 점을 설득하느라 진땀을 흘렸다. 그 결과 특별 위원회는 방침을 바꿔 OIG-CSIS 해체를 권고하는 입장에서 물러섰다. 그러나 몇 년 후 차기 정부는 재임자의 사직을 받아들였고, 1년 이상 이 직위를 공석으로 방치했다. 아주 최근에 들어서 정부는 이제 OIG-CSIS의 역할을 SIRC에 통합시킬 계획임을 시사했다. 정부가 밝힌 표면적 이유는 행정 비용 절감이었지만 감독이 개선될 것이라는 주장도 빼놓지 않았다.[30]

행정 명령으로 OCSEC가 설립된 1996년까지 캐나다의 신호 정보국인 통신보안기구(CSE: Communication Security Establishment)는 외부 감독을 받지 않았다. 5년 후 의회는 일괄 형법안의 일부로 테러방지법을 채택했고, 이 법을 통해 OCSEC와 (CSEC처럼 행정 명령에 따라 운영되어 온) CSE에 법적 근거가 마련되었다. 테러방지법은 CSE가 캐나다법을 준수해서 운영되도록 하는 제한적 위임 사항을 OCSEC에 부여했다. OCSEC는 또 기관에 대한 민원을 청취할 권한도 가지고 있다. 이 직위의 요건에는 선임 법원 판사로서의 경험이 포함된다. 일단 재직하게 되면 OCSEC는 정당한 사유가 있어야만 해임될 수 있다.

OCSES는 OIG-CSIS나 SIRC와 마찬가지로 기밀 취급 그룹 내에서 운영되며, 보안 시설과 제한적인 기밀 취급 인가 보좌진을 두고 있다. 또한 OCSEC는 심문법(Inquiries Act)에 따라 모든 위원과 동일한 조사 권한을 갖는다. SIRC처럼 OCSEC는 주무장관이 의회에 상정할 수 있는 연례 보고서를 제출해야 한다.

이 두 가지 연례 보고서가 제공하는 정보는 캐나다 의회가 OCSEC와 SIRC로부터 직접 받는 유일한 정보다. 어느 경우든 정부가 보고서의 권고에 따른 조치를 취할 의무는 없다.

4.3.2 벨기에의 상임 정보기관심의위원회

벨기에의 경우, SIRC와 유사한 전문가 기구가 정보기관 감독을 수행한다. 그러나 벨기에 상임 정보기관심의위원회(Committee I라고 함)는 몇 가지 중요한 점에서 캐나다의 사례와 다르다. 첫째, 그 위임 사항에는 2개의 정보기관(민간 기관인 국가보안국[State Security]과 국가보안국에 상응하는 군 정보기관인 일반정보보안국[General Intelligence and Security Service])과 위협평가조정단(Coordination Unit for Threat Assessment)이 포함된다.[31] 둘째, Committee I의 위임 사항은 법률 및 규정 준수 보장에 그치지 않고 기관의 효율성 및 기관 간 조정에 관한 사안까지 확장된다. 셋째, Committee I의 세 명의 위원(모두 기밀 취급 인가가 있어야 하고, 법학 학위를 보유해야 하며, 관련된 전문적 경험이 있어야 한다)은 (캐나다에서처럼 내각이 아니라) 벨기에 상원이 지명한다. 끝으로 위원회 위원장은 치안판사여야 한다.

Committee I 위원은 의원이 될 수 없지만 위원회의 수권법(enabling legislation)은 상하 양원에 Committee I의 업무를 모니터링하고 그 보고서를 검토할 상임 위원회를 설립할 책임을 부과한다. 이 법은 나아가 의회 위원회 위원들이 적절한 보안 예방 조치를 취할 것을 요구하며, 직위에서 물러난 후에도 이들이 받는 정보의 비밀을 유지할 의무를 부과하고 위반시 법적 처벌을 받도록 하고 있다.

5. 효과적 감독의 장애물

전환기 국가에서는 효과적인 정보기관 감독을 가로막는 여러 가지 요소가 있을 수 있다. 본 절에서는 가장 흔한 장애물들에 관해 논의한다.

5.1 행정부에 책임 묻기를 꺼림

효과적 감독의 가장 기본적 장애물은 의원들이 행정부에 책임을 물을 수 있는 수단을 제정하고 활용하기를 꺼린다는 점이다. 행정부에 책임을 물은 전례가 없는 전환기 국가의 경우, 의원들은 보통 어떤 방법이 최선인지 결정하기에 앞서 다양한 방식을 시험해 봐야 한다. 효과적인 감독을 위해 위원회

청문회에만 의존하는 것으로는 아마 부족할 것이다. 경험에 따르면 조직적 관리, 조사 연구, 현장 방문, 비공개 청문회 또한 필요할 것이다.

5.2 가파른 학습 곡선

보안 및 정보활동은 거의 모든 부처에 영향을 미치고 관여한다는 점에서 정부의 대부분의 다른 기능과 다르다. 적절한 감독을 위해서는 정보기관의 기능과 관행 및 정보기관과 다른 정부 기관 간의 복잡한 상호 작용 방식을 속속들이 알고 있어야 하는 등 학습 곡선이 가팔라서 시간과 주의를 쏟을 곳이 많은 의원들에게는 쉽지 않다. 필요한 전문성 개발은 시간이 걸리며, 특히 정보관들이 상세한 지식을 공유하기를 꺼린다는 점을 감안하면 더욱 그렇다.

5.3 신뢰 부족

정보기관과 정보기관 감독 기구가 서로를 신뢰하지 않으면 솔직한 논의, 의미 있는 정보 교환, 효과적 감독은 불가능하다. 신뢰 관계를 구축하려면 외부 감독 기관(특히 입법부 위원회)은 준수에만 초점을 맞추는 행태를 지양해야 한다. 감독을 이런 식으로 한정하면 대립적인 편가르기 환경이 조성되고, 정보 인력들은 감독 과정이 자신들에게 득이 될 것이 없다고 생각하게 될 것이다. 이들은 오히려 적어도 초기 단계에서는 상당한 어려움만 보게 될 것이다.

감독이 효과적이기 위해서는 정보기관들이 감독의 장점도 경험할 필요가 있다. 예를 들어 효능이 강조되면 행정부가 기관에 더 많은 자원을 제공할 것을 독려하는 권고 사항을 통해 기관에 이익이 될 수 있다. 정보기관 구성원의 비행을 잘못 비난하거나 그 효과성에 관해 의문을 제기하는 잘못된 언론 보도를 입법부 위원회나 전문가 감독 기구가 바로잡는 경우에도 기관은 감독의 장점을 경험할 수 있다.

5.4 사람, 장소, 서류, 기록에 대한 접근 거부

효과적인 감독의 가장 중요한 장애물은 사람, 장소, 서류, 기록에 대한 접근 거부다. 이에 접근할 수 없으면 감독 기구는 제 기능을 할 수 없다(도구 3도 참조). 감독 기구는 행정부로부터 얻은 정보가 정확한지 확인할 수 없을뿐더

러 특정 사안에 대한 조사를 제대로 발전시킬 수도 없다. 오로지 들은 이야기와 공개 출처에서 얻을 수 있는 것에만 의존해야 한다.

5.5 시간적 압박과 그것이 조사에 미치는 영향

의원들이 느끼는 시간적 압박은 그들이 수행하는 조사의 유형에 악영향을 미칠 수 있다. 미국 의회 감독 위원회에 관한 연구에 따르면 의원들은 스스로 문제점을 찾기보다는 이미 대중의 관심이 높은 쟁점을 받아들일 가능성이 더 높은데,[32] 그럴만한 이유가 있다. 의원들은 (자신의 재선을 포함한) 여러 가지 책임으로 바쁜 사람들이기 때문에 개인적인 정치적 이득을 안겨 줄 가능성이 가장 큰 사안을 추구하는 경향이 있다. 정보기관 조사가 공개적으로 이루어지는 경우가 드물다는 것은 이들에게 정치적 이득을 안겨줄 가능성이 거의 없음을 의미한다.

입법부 자체의 성격도 정보기관을 감독하는 의원들의 능력에 걸림돌이 된다. 감독에 쓸 수 있는 시간 역시 모든 의원이 수행해야 하는 업무는 물론 의회 회기로 인해 제한된다. 대부분의 국가에서 회기 중이 아닌 때와 선거 기간에는 의회 업무가 중단된다. 이 문제의 부분적 해결책은 감독 책임을 전문가 기구에 맡기는 것이다.

5.6 당파 갈등

감독 과정은 당파 갈등으로 너무도 쉽게 방해를 받을 수 있다. 예를 들어 미국의 경우, 당파 갈등이 과도해지면 의회 감독 위원회 업무를 지연시키거나 장악함으로써 야당의 정보기관 조사 노력을 좌절시킬 수 있다.[33] 마찬가지로 대부분의 내각제 국가에서 집권당은 다수 대표를 통해 모든 입법부 위원회의 의제를 좌지우지한다. 일반적 원칙인 이러한 다수 지배에 대응하기 위해 일부 국가에서는 정보기관 감독 기구의 위원장을 야당 소속이 맡도록 한다.

이렇게 교대로 위원장직을 맡고 정부와 야당 간의 적절한 균형을 토대로 위원회 위원을 선정하는 것은 당파 갈등을 최소화하고 협력을 증진할 수 있는

중요한 방법이다. 일반적으로 감독 위원회 위원들이 국가 이익에 기여하는 결과를 집단적으로 추구하고 협력할 때 감독이 최고의 성과를 낸다.

5.7 전문가 감독 기구의 보고 지연

선제적이고 일상적인 다양한 형태의 조사를 위해 전문가 기구를 설립하는 경우, 이들의 보고와 분석이 의원들에게 제때 전달되는 것이 매우 중요하다. 의원들이 정보기관의 어떤 측면을 직접 조사하든 상관없이 공공 기금 책정, 기존 법률 검토 같은 보다 폭넓은 책임을 이행하기 위해서는 최대한 광범위한 맥락을 인식할 필요가 있다. 의원들이 적시에 보고를 받을 수 없고 전문가 기구의 권고 사항에 관해 그 구성원들에게 질문할 수 없다면 의원들의 직무 이행 능력이 크게 손상될 것이다.

5.8 부족한 자원

의원들이 효과적인 감독을 수행할 수 있는 능력은 가용 자원에 크게 의존한다. 이와 관련하여 가장 중요한 자원은 보좌진과 접근권이다. 앞서 언급했듯이 의원들은 광범위한 책임을 지닌 바쁜 사람들이다. 정보 공동체에 관해 방대한 지식을 지니고 있고 고도로 숙련된 비당파적인 상임 지원 보좌진의 도움이 없으면 의원들은 기껏해야 조사 업무보다는 위원회 청문회에 초점이 맞춰진 제한적 감독을 수행하게 될 가능성이 크다. 게다가 의원들은 효과적인 감독을 수행하기 위해 조사 서비스, 감사 역량을 포함한 광범위한 정보에 접근할 수 있어야 한다.

비당파적인 상임 지원 보좌진의 창설도 제도적 기억의 개발과 지속에 도움이 될 수 있다. 정보 전문성 개발에는 긴 시간이 걸리기 때문에 의원들의 교체(일부 관할권에서는 상당한 수준이다)로 인해 지식과 경험이 손실되는 경우가 많다. 비당파적인 상임 보좌진이 존재하면 이러한 효과적 감독의 장애가 확실히 줄어든다.

6. 감독 체계를 위한 법적, 제도적 틀 설계

감독 위임 사항은 최대한 광범위해야 한다. 특정 감독 기구의 위임 사항은 주로 전체 감독 체계 내에서의 위상에 따라 달라지겠지만 이들 위임 사항을

다 합치면 행정과 운영부터 정책과 예산에 이르기까지 폭넓은 정보기관 문제가 포괄되어야 한다.

효과적인 감독 체계를 위해서 감시 대상 정보기관들이 관련 법률, 규칙, 정책을 준수하고, 효과적으로 업무를 수행하도록 해야 한다. 규정 준수 감시는 비교적 간단할 수 있지만 효능 평가는 전체 보안 정보 체계에 대한 종합적 평가를 요구하므로 훨씬 더 복잡하다. 이를 위해서는 단순히 정보수집 기관들을 조사하는 것으로는 부족하다. 조사뿐만 아니라 정보기관의 전략 및 책임을 결정하고, 현재의 위협과 기회에 부합하는 정보 요건을 설정하며, 따라야 할 우선순위를 확정하고, 정보 체계의 다양한 구성 요소들이 이러한 우선순위를 따르도록 하는 데 선출직 지도자들이 적극적, 일상적으로 관여하는지 여부를 검토할 필요가 있다.

보안 정보 체계를 전체적으로 살펴볼 때, 국가 안보에 도움이 되기 위해서는 정보기관이 가능한 "최선의 진실"을 언제든 정부에 제공해야 한다는 점은 명확해 보인다. 그러나 정보 업무는 완벽한 과학이 아니며, "최선의 진실"은 때로 심각한 결함이 있을 수 있다. 업무의 성격이 그러하기 때문이다. 그럼에도 불구하고 정보기관이 실패라는 결과에 상관없이 "권력에 진실을 말하는 것"이 매우 중요하다. 정보 공동체 내에서 이런 태도를 증진하고 유지하기 위해서는 정보기관에 대한 모든 정당의 전폭적인 지원과 그에 못지않은 공정한 비판이 필요하다. 문제는 입법부가 정치적 기구이며, 입법부에서 차기 정부는 대안적 입장을 제시함으로써 집권당을 난처하게 만들려고 하는 것이 일반적이라는 점이다. 따라서 당파적 이익을 추구하고자 하는 유혹이 협력하려는 의지를 꺾는 경우가 다반사다. 이런 이유로 행정부나 입법부와 직접적으로 연결되지 않은 전문가 감독 기구가 정보기관 감독을 흔히 더 효과적으로 수행한다. 이런 방식으로 정보 감독 업무에서 정치 요소를 제거할 수 있다.

정보기관의 법률 준수와 관련하여 전문가 감독 기구는 사후에 기관의 업무를 심의하는 것뿐 아니라 관련 법률, 규칙, 정책이 제대로 기능하고 있는지 아니면 개정이 필요한지를 지속적으로 검토할 권한이 있어야 한다. 또 이들 기구

에는 침해적이거나 강압적인 권한을 가진 정보기관에 대한 민원을 조사하거나 자격을 갖춘 재결 기관을 통해 민원을 충분히 조사하게 할 의무가 있어야 한다(도구 9 참조). 나아가 모든 관계 당국에 정기적으로 보고서를 제출해야 하며, 이 보고서에는 적절한 경우 시정을 위한 권고 사항이 포함되어야 한다.

전문가 감독 기구는 정보기관의 효능과 관련하여 역량과 성과를 모두 측정해야 한다. 흔히 이 측정은 사후에 이루어지지만(교훈 습득) 정보기관의 현재 역량이 정부가 예측하는 미래의 요구를 충족할 가능성이 있는지를 살펴보는 지속적 요소 또한 갖춰야 한다. 최고 감사 기구(SAI)는 보통 이러한 측정을 개발하는 데 필요한 기술을 갖고 있지만(도구 8 참조) 통상적으로 정부 운영의 전체 범위를 담당하고 있기 때문에 정보 부문에만 정기적으로 관심을 쏟기 어려울 수 있다. 따라서 입법부가 SAI에 특별 허가를 부여하거나 이 요구를 충족시킬 새로운 감사 기구를 창설할 필요가 있을 수도 있다.

의원들은 감독 기구의 위임 사항을 설정할 때 수권법에서 감독자에게 보안 정보 기반 시설의 모든 구성 요소에 대한 충분한 접근 권한을 부여하도록 해야 한다. 이렇게 하면 감독 기구가 정보 공동체의 전체적 역량에 접근할 수 있다. 이러한 광범위한 소관 사항이 없다면 행정부는 면밀한 조사를 피하기 위해 책임을 쉽게 이리저리 옮길 수 있다. 광범위한 소관 사항을 통해 감독 기구는 관련 조직 간의 구조적 관계와 이들 관계의 실제 운영 방식, 그리고 이들 관계가 공동 업무 비용에 미치는 영향을 조사할 수도 있다.

그뿐만 아니라 행정부가 감독 기구의 의사 결정에 영향을 미칠 가능성을 줄이기 위해 수권법은 감독 기관 구성원에게 어느 정도의 임기 보장을 해 주어야 한다. 즉, 감독 기구는 조직상으로는 행정부일 수는 있지만 행정부 내에 있어서는 안 된다.

그렇다면 입법부가 정보기관 감독을 수행할 전문가 기구를 창설할 경우, 입법부에는 어떤 감독 업무가 남는지 물어 볼 수 있을 것이다. 그 대답은 내각제 민주주의에서 입법부가 갖는 다음 세 가지 중요한 책임과 관계가 있다.

- 법률 토론 및 채택
- 정부 부처와 기관의 공공 자금 지출 승인
- 정부의 행위 또는 부작위에 대해 정부에 책임을 물음

이 모든 책임은 의원들이 정보기관 감독 업무에 적극적으로 참여할 것을 요구한다. 의원들이 법률 제정, 예산 심의, 책임성과 관련된 의무를 이행하기 위해서는 입법부 위원회 위원들이 전문가 감독 기구의 보고를 적시에 접할 수 있어야 하는 것은 물론 감독 기구가 제출하는 보고서에 관해 감독 기구 구성원에게 질문할 수 있는 능력도 갖춰야 한다. 또한 의원들은 정보기관에 대한 공공의 신뢰가 손상될 사안이 대두되는 경우, 자체 조사를 수행해야 할 수도 있다. 의원들은 또 정기적으로 전문가 감독 기구의 활동을 조사하여 이들이 효과적으로 운영되고 적절한 자원이 갖춰지도록 해야 한다.

끝으로 5.4절에서 논의했듯이 사람, 장소, 서류, 기록에 대한 접근 없이는 효과적 감독은 불가능하다. 따라서 감독 기구의 가장 중요한 권한은 접근을 강제할 권한이다. 입법부에 일반적인 접근 권한이 있더라도 입법부 위원회가 기밀 정보, 인력 또는 업무 환경에 접근하지 못할 수 있는데, 이런 접근이 성문법에 확실히 규정되어 있지 않기 때문이다.

7. 권고 사항

정보기관 감독 체계를 설립하는 법률에는 특히 다음 사안들이 포함되어야 한다.

사람, 장소, 서류, 기록에 대한 접근이 보장된 입법부 위원회 설립

이런 위원회를 설립하는 법률은 소환장 발부, 선서 또는 확약 하의 증언 강제, 정보기관 부지 출입 및 수색 권한 등 접근에 관한 위원회의 권한을 명시해야 한다. 또 위원회 위원이 될 수 있는 자격과 위원회가 사용할 자원도 명시해야 한다. 법률에 규정되는 위원회의 두 가지 목표는 보안 정보기관에 의한 남용의 방지와 그 운영의 효과성, 효율성, 경제성 증진이어야 한다. 또한 위원회는 적당한 기간 안에 완료하고 보고해야 하는 프로젝트처럼 위원회가

추진할 역량이나 시간이 없는 감독 프로젝트를 지원 기구에게 맡겨 수행하도록 지시할 수 있어야 한다.

위원회에 부과되는 의무에는 보안 환경에서 감독을 수행한다는 요건이 포함되어야 한다. 위원회 위원과 보좌진은 모두 기밀 취급 인가가 있어야 하며, 기밀 정보를 밝히지 않겠다는 선서를 해야 한다.[34] 또 위원회는 재량에 따라 공개 보고서를 발행할 수는 있지만 입법부에 상정되어 공개되는 보고서를 적어도 일 년에 한 번 작성해야 한다. 정보기관들은 기밀 정보가 부적절하게 포함되어 있는지 파악하기 위해 이러한 모든 보고서를 심사해야 하지만 어떤 주제를 포함할지에 관한 최종 결정권은 위원회에 있다.

아울러 국가 안보 법률이 의도대로 운영되고 있는지, 그리고 현재의 위협과 기술 환경을 계속 반영하고 있는지 판단하기 위해 위원회가 법률에 대한 정기적 검토를 수행하도록 법률에서 규정해야 한다. 정보를 누설하는 위원회 위원과 보좌진에 대한 구체적 처벌도 법률에 포함되어야 한다. 끝으로 외부 전문성이 필요하거나 당파성이 높은 사안일 경우, 법률에서 임시 조사 위원회를 설립할 권한을 위원회 위원들에게 부여해야 한다.

정보기관에 대한 민원을 청취할 독립적 기구 설립

이러한 기구는 정보기관에 대해 민원을 제기하는 사람이 제일 먼저 접촉하는 창구여야 한다. 해당 수권법은 내부 고발자에 대한 구체적인 보호를 제공해야 한다. 내부 고발자가 이전에 공개된 적이 없는 기밀 정보를 밝히지 않았고, 선의에서 폭로를 한 것이라면 보호받아야 한다. 또한 폭로가 이후에 공공의 이익에 기여하는 것으로 판결된다면 보호가 적용되어야 한다. 나아가 이 기구는 개별 사건들을 판결 후 검토하여 내부 고발자가 고용과 관련하여 부적절한 피해를 받지 않도록 해야 한다.

감독이 주 업무이지만 감독만을 수행하지 않고 예방적 성격을 갖는 하나 이상의 감독 기구 설립

이들 기구는 서로, 또 입법부 위원회와 자유롭게 회의와 대화를 할 수 있어

야 한다. 단, 이러한 회의는 보안 환경에서 이루어져야 한다. 이 기구들은 행정부의 요구에 따를 수도 있지만 주된 목적은 의회를 도와 권한 남용을 방지하고 효능을 증대하는 것이어야 한다. 이 감독 기구들은 자체 업무 계획과 일정을 개발할 수 있어야 하지만 입법부 위원회와 행정부로부터 지시도 받아야 한다. 이들의 조사는 검토 대상 사건의 발생 전, 발생 도중, 발생 후에 이루어질 수 있다.

후주(後註)

1. 예컨대 Hans Born (ed.), *Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices (Geneva: DCAF, 2003); and Hans Born and Ian Leigh, Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Geneva: DCAF, University of Durham, and Parliament of Norway, 2005) 참조.

2. 비교 연구는 Jean-Paul Brodeur, Peter Gill, and Dennis Tollborg (eds.), *Democracy, Law, and Security: Internal Security Services in Contemporary Europe* (Aldershot, UK: Ashgate, 2003); Thomas C. Bruneau and Steven C. Boraz (eds.), *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007); Stuart Farson, Peter Gill, Mark Phythian, and Shlomo Shpiro (eds.), *PSI Handbook of Global Security and Intelligence: National Approaches,* (Westport, CT: Praeger Security International, 2008); Greg Hannah, Kevin O'Brien, and Andrew Rathmell, *Intelligence and Security Legislation for Security Sector Reform,* Technical Report TR-288-SSDAT (RAND Europe, 2005) 참조.

3. 몇몇 연구는 일정 기간에 걸쳐 특정 감독 기구의 효과성을 살펴봤다. 여기에는 Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" in *Accountability for Criminal Justice: Selected Essays,* ed. Philip C. Stenning (Toronto: University of Toronto Press, 1995), pp. 185–212; Loch Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* (Lexington: University Press of Kentucky, 1985); Kathryn S. Olmsted, *Challenging the Secret Government: The Post-Watergate Investigations of the CIA and FBI* (Chapel Hill: University of North Carolina, 1996); and Kent Roach, "The Parliamentary Review of the Anti-Terrorism Act," *Criminal Law Quarterly* 52 (May 2007), pp. 281–4가 포함된다.

4. Anthony Glees, Philip H.J. Davies, and John L. Morrison, *The Open Side of Secrecy: Britain's Intelligence and Security Committee* (London: Social Affairs Unit, 2006); Frank J. Smist Jr., *Congress Oversees the United States Intelligence Community, 1947–1994, 2nd Edition* (Knoxville: University of Tennessee Press, 1994).

5. Charles Tilly, *Democracy* (Cambridge: Cambridge University Press, 2007) 참조.

6. Peter Gill, "Symbolic or Real? The Impact of the Canadian Security Intelligence Review Committee, 1984–88," *Intelligence and National Security* 4, No. 3 (1989) pp. 550–575 참조.

7. 내각제 민주주의에서 정보기관 통제는 보통 행정부의 책임이다. 그러나 정보기관 자금을 승인하고 정보기관 관련법을 제정하는 의회의 권한에서 의회 통제의 요소가 발생할 수 있다.

8. 권력 분립이 존재하는 몇몇 정부 체계에서는 입법부 위원회가 행정부 선출직 구성원을 불러 증언하게 할 수 없다.

9. Thomas C. Bruneau, "Intelligence Reforms in Brazil: Contemporary Challenges and the Legacy of the Past," *Strategic Insights* VI, No. 3 (May 2007) (available at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA485122) 참조.

10. Marco Cepik, "Structural Change and Democratic Control of Intelligence in Brazil," in Thomas C. Bruneau and Steven C. Boraz (eds.), *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007) pp. 149–169 참조.

11.EU 의회 감독 체계들의 비교 분석은 Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (Brussels: European Parliament, 2011), 특히 pp. 92–95의 차트 참조.

12.콜린 케니(Colin Kenny) 위원장 시절의 캐나다 상원 국가안보방위위원회는 광범위한 주제를 다뤘으며, 일부는 비공개 운영에 기초한 몇몇 중요한 보고서를 내놓았다.

13.캐나다는 이 방식을 고려했지만 아직 채택하지는 않았다.

14.이 보고서들은 원래 국무조정실에서 작성되었다. 그러나 국무조정실은 이해 상충의 가능성이 있는 것으로 인식되었기 때문에 지금은 더 독립적이라고 간주되는 보안 환경에서 작성된다.

15.Australia, Intelligence Services Act 2001, Section 29(3).

16.Ibid., Section 29(1)(b).

17.Canada, Special Committee on the Review of the CSIS Act and the Security Offences Act, In Flux But Not In Crisis (September 1990) 참조.

18.Kent Roach, "The Parliamentary Review of the Anti-Terrorism Act," *Criminal Law Quarterly* 52 (May 2007), pp. 281–4 참조.

19.Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" in *Accountability for Criminal Justice: Selected Essays, ed. Philip C. Stenning* (Toronto: University of Toronto Press, 1995), pp. 185-212 참조.

20.Shlomo Shpiro, "Parliamentary and Administrative Reforms in the Control of Intelligence Services in the European Union," *Columbia Journal of European Law 4* (1998), pp. 545–578 참조.

21.Geoffrey R. Weller, "Comparing Western Inspectors General of Intelligence and Security," *International Journal of Intelligence and CounterIntelligence 9,* No. 4 (1996), pp. 383–406 참조.

22.Frederick M. Kaiser, "The watchers' watchdog: The CIA inspector general," *International Journal of Intelligence and CounterIntelligence* 3, No. 1 (1989), pp. 55–75 참조.

23.오랫동안 SIRC에 OIG-CSIS 준수 확인서 전달이 지연됨으로써 CSIS 준수 문제에 관한 의견을 제시하고 그럼으로써 의회에 이 문제에 관해 알릴 위원회의 연례 보고가 불가능했다.

24.Ian Carnell and Neville Bryan, "Watching the watchers: How the Inspector-General of Intelligence and Security helps safeguard the rule of law" (paper presented at the Safeguarding Australia 2005 conference, 12–14 July 2005) (available at http://www.igis.gov.au/public_statments/conference_papers.cfm) 참조.

25.웨스트민스터 모델에 따르는 일부 관할권에서는 행정부 구성원들이 심의와 감독을 구분한다. 이들은 *심의(review)*를 단순한 조사의 의미로 사용하고, *감독(oversight)*은 변화를 가져올 권한이 동반되는 조사의 의미로 사용한다. 따라서 정보기관 활동에 대한 조사에서 심의 기구는 변화를 위한 권고만을 할 수 있는 반면 감독 기구는 변화를 강제할 수 있다.

26.Ian Carnell and Neville Bryan, "Watching the watchers: How the Inspector-General of Intelligence and Security helps safeguard the rule

of law" (paper presented at the Safeguarding Australia 2005 conference, 12 – 14 July 2005) (available at http://www.igis.gov.au/public_statments/conference_papers.cfm) 참조.

27.원래 바람은 전직 주무장관들이 SIRC 위원이 되는 것이었지만 늘 그랬던 것은 아니다.

28.Canadian Security Intelligence Service Act, R.S.C., 1985, Chapter C-23, Section 38.

29.Stuart Farson, "The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" in *Accountability for Criminal Justice: Selected Essays,* ed. Philip C. Stenning (Toronto: University of Toronto, 1995), pp. 185 – 212 참조.

30.Bruce Cheadle, "Conservatives use budget bill to cut spy agency inspector general's office," *Canadian Press,* April 26, 2012.

31.Committee I는 위협평가조정단이 테러와 극단주의에 관한 정보를 관련 경찰, 행정, 사법 당국에 전달하도록 할 책임도 있다.

32.예컨대 Mathew D. McGubbins and Thomas Schwartz, "Congressional Oversight Overlooked: Police Patrols versus Fire Alarms," *American Journal of Political Science* 28, No. 1 (February 1984), pp. 165 – 179 참조.

33.Marvin C. Ott, "Partisanship and the Decline of Intelligence Oversight," *International Journal of Intelligence and CounterIntelligence* 16, No. 1 (2003), pp. 69 – 94.

34.보안 기관이 의원 및 기타 특정 공직자들(판사 등)을 심사하는 것은 권력 분립의 관점에서 볼 때 헌법적 문제가 될 수 있다. 즉 행정부 구성원이 입법부나 사법부 구성원의 적격성에 관해 결정하는 것은 일반적으로 부적절하다. 일상적으로 기밀 정보를 취급하게 되는 사람의 경우, 일정한 형식의 심사가 필요한 이유는 명백하다. 다행히도 헌법적 문제를 우회할 수 있는 방법은 많다. 입법부와 사법부는 장관 지명 시 이루어지는 것과 유사한 자체 비공식 심사를 수행할 수 있다. 또는 보다 공식적인 심사 과정을 수행할 외부 보안 회사를 고용할 수도 있다. 이러한 심사는 세 가지 중요한 장점이 있다. 첫째, 정보기관은 구성원이 이런 심사를 받은 감독 기구를 신뢰하고 협력할 가능성이 크다. 둘째, 해외 파트너들은 공유 정보가 심사를 받지 않은 감독 기구에 의해 공개되지 않을 것으로 확신할 경우, 정보를 공유할 가능성이 높다. 셋째, 엘리트 일탈에 관한 연구에 따르면 “모든 통에는 썩은 사과가 있게 마련이다.” 판사들의 부패는 예전부터 있었던 일이고, 감독 기구 구성원들도 이해 충돌로 사임해야 했으며, 의원들이 반역죄를 범하기도 했다. 심사는 지나친 해를 끼치기 전에 이런 “썩은 사과들”을 제거할 수 있다.

도구 3

민주주의에서의 정보 투명성, 비밀주의, 감독

로리 네이선(Laurie Nathan)

3. 민주주의에서의 정보 투명성, 비밀주의, 감독

로리 네이선(Laurie Nathan)[1]

1. 머리말

민주국가에서 정보기관의 존재는 정치적 역설을 낳는다. 한편으로 정보기관들은 국가, 시민 및 국가 관할 하에 있는 그 밖의 사람들과 민주적 질서를 보호하기 위해 설립되며, 이를 위해 특별한 권한과 능력이 주어진다. 일반적으로 정보기관들은 감시, 통신 감청 및 기타 프라이버시권을 침해하는 방법을 통해 기밀 정보를 획득하고, 국가 안보에 대한 위협에 맞서기 위한 비밀 업무를 수행하며, 극비리에 운영할 권리를 법률로 부여 받는다.

다른 한편 정보기관과 행정부 구성원들은 이 권한과 능력을 남용하여 개인의 안보를 훼손하고 민주적 과정을 전복시킬 수 있다. 이들은 법을 위반하여 인권을 침해하고, 합법적 정치 활동을 방해하며, 정당이나 지도자의 편을 들거나 해를 끼칠 수도 있다. 이들은 정부 반대자들을 위협하고, 공포 분위기를 조성하며, 정부의 의사 결정과 여론에 영향을 미치기 위해 정보를 가공하거나 조작할 수 있다. 또 정보기관 자금과 절차를 개인적 이익을 위해 남용할 수 있다.

이런 위험성을 볼 때 민주국가는 불법 행위 및 권한 남용 가능성을 최소화하고 정보기관들이 헌법과 법률에 따른 책임을 이행하도록 할 규칙, 통제, 감독 메커니즘을 구축해야 하는 과제에 봉착해 있다.

이 목표들은 다른 국가 기관을 관할하는 통제 및 감독 기구에도 똑같이 적용되지만 정보기관과 그 업무가 고도의 비밀주의로 둘러싸인 정보기관의 세계에서는 이를 달성하기가 매우 어렵다. 비밀주의는 감독 기구의 모니터링과 심의를 방해하고, 공공의 감시를 억제하며, 정보관들이 비행을 쉽게 은폐할 수 있게 한다.

이 도구는 정보기관 감독 기구와 관련하여 정보 비밀주의, 정보 개방성, 정보 제공에 초점을 맞춘다. 이런 기구에는 의회, 의회 정보 감독 위원회, 사법부, 최고 감사 기구(SAI), 독립적 정보감찰관(호주, 뉴질랜드, 남아공의 경우), 전문가 정보기관 감독 기구(네덜란드의 정보보안기관심의위원회 등)가 포함된다. 이 도구는 정보 비밀주의와 투명성을 둘러싼 정치적, 개념적 논쟁을 개관하고, 정보 보호 및 접근 관련 입법의 모범 관행을 제시하며, 의회와 기타 감독 기구가 필요로 하는 정보기관 정보에 관해 논의한다. 이 도구는 일련의 권고 사항으로 끝맺는다.

정보 비밀주의에 관한 논의는 주로 공개하지 말아야 할 것에 초점을 맞추지만 이 도구에서는 효과적 감독과 민주적 거버넌스를 위해 공개되어야 할 정보 분야를 보다 적극적으로 살펴본다.

아울러 우선 과도한 비밀주의가 정보 조직에 대한 의심과 두려움을 낳고, 이들에 대한 대중적 지지를 잃게 만든다는 점을 강조해야겠다. 경찰국가와는 달리 민주주의에서 정보기관의 성공은 강압과 공포가 아닌 공공의 협력에 의존한다. 정보기관에 관한 정보를 더 많이 제공하면 정보기관의 이미지가 긍정적으로 바뀌고, 비밀주의로 인한 우려와 두려움이 줄어들며, 정보기관과의 협력이 증진되어 기관의 효과성도 증대된다.

2. 정보기관 감독에서의 투명성과 비밀주의 문제

정보기관에 대한 민주적 거버넌스와 관련된 가장 중요하고도 골치 아픈 문제는 비밀주의다. 이것이 가장 중요한 문제인 이유는 비밀주의가 심할수록 정보기관의 특성과 성과에 대한 파악과 평가가 더 어려워지기 때문이다. 충분한 정보 없이는 정보기관의 역할과 지향, 정보기관 개혁의 필요성, 그리고 정보기관이 안보와 국가 관할 하의 시민 및 그 밖의 사람들의 자유를 보호하고 있는가 아니면 훼손하고 있는가라는 중대한 질문을 감독 기구가 유의미하게 규명하고 논의하기란 불가능하다.

이 주제가 골치 아픈 이유는 서로 경쟁하는 강력한 압력들을 특징으로 하기 때문이다. 한편으로 보면 정보 공동체와 그 활동의 일부 측면은 정보기관 운영 및 정보관과 정보 제공자의 생명을 위태롭게 하지 않기 위해 비밀이 유지되어야 한다. 다른 한편으로는 비밀주의는 민주적 거버넌스와 상반된다. 비밀주의는 전적인 책임을 가로막으며, 권력 남용, 불법성, 면책 문화(culture of impunity)의 온상이 된다.

본 절에서는 정보기관의 투명성과 비밀주의에 관한 논쟁을 살펴보고, 민주적 접근법을 설명한다. 이 문제는 의회와 관련성이 크다. 의회는 비밀주의와 정보 접근에 관한 법률과 정책의 입안 및 승인에 관여함으로써 정보 체제가 공공의 감시에 열려 있거나 닫혀 있는 정도를 결정하는 데 중요한 역할을 한다. 게다가 의회는 행정부와 국가 기관에게 책임을 물을 뿐 아니라 스스로도 공공에 대해 책임을 지며, 시민들에게 정보 공동체에 관한 정보를 제공할 의무가 있다. 따라서 정보 법률, 정책, 예산에 관한 의회 논의는 공개된 회의에서 이루어져야 한다.

2.1 정보기관 비밀주의의 동기

비밀주의는 정보기관의 본질적이고 필수적인 특징인데, 이는 정보기관의 위임 사항과 기능의 성격 때문이다. 정보기관들은 국가 안보에 대한 전통적 및 비전통적 위협, 적성국과 테러리스트 및 범죄 조직, 정부 지도자와 국가 시설의 물리적 보호, 국가 기밀 정보의 보호에 관여한다. 비밀주의는 이런 문제와 맞서는 데에서 정보기관에 경쟁 우위를 제공하지만, 극단적 투명성은 정보기관에 명백하고 위험한 단점이 될 것이다.

더 구체적으로 비밀주의가 필요한 이유는 다음과 같다.

- 첩보 활동의 목표물이 감시 받고 있음을 눈치 채는 것을 방지
- 목표물과 적들이 정보기관이 사용하는 방식에 관해 알게 되는 것을 방지
- 정보관과 정보 제공자의 생명 보호
- 정보기관이 보호하는 요인(VIP)의 안전 확보

- 외국 정보기관이 제공하는 정보의 기밀 유지
- 경쟁 정보기관으로 인한 다양한 피해 방지

이러한 비밀주의의 요건은 합리적이지만 정보기관들은 비밀주의에 대해 지나치고 때로는 강박적인 태도를 갖는 경향이 있다. 이들은 민감하지 않은 분야의 투명성은 필연적으로 민감한 분야의 개방성으로 이어져 끔찍한 결과를 가져올 것이라고 주장한다. 그래서 정보기관들은 비밀주의와 관련한 조금의 느슨함이나 유연성도 허용치 않는 내부 체계와 절차, 규칙을 개발한다. 비밀주의가 어느 정도의 신비감과 엘리트 지위를 부여하기 때문에 정보기관들이 비밀주의를 중시하는 것 또한 사실이다.

정보기관들은 때때로 정보를 받을 권한이 있는 의회 감독 기구에게도 정보를 공개하기를 꺼린다. 정보기관들은 의원들이 기밀 유지 훈련을 받지 않았기 때문에 인가 받지 않은 사람들에게 민감한 정보를 누설하고 당파적인 정치적 목표를 위해 정보기관 정보를 오용할 위험이 있다고 주장한다. 그러나 아래에서 논의하듯 정보 무단 공개 위험은 다양한 수단을 활용해 최소화할 수 있다.

2.2 표준이 아닌 예외로서의 비밀주의

위에서 언급한 정보기관 비밀주의의 동기가 합리적이기 때문에 정보기관에 대한 민주적 거버넌스에 관한 많은 논문은 “비밀주의와 투명성의 적절한 균형을 유지해야 한다”고 못 박고 있다. 그러나 이 표현은 너무 두리뭉실해서 그리 가치도 없고, 출발점도 옳지 않다. 출발점은 민주주의의 근본 교리여야 한다. 이들 교리에는 투명성과 국가 보유 정보에 접근할 수 있는 권리가 포함된다. 이 교리들은 의회 및 기타 감독 기구에 대한 행정부의 책임, 이들 기구에 의한 효과적 감독, 정치적·개인적 자유, 민주적 권력 경쟁, 활발한 사상 논쟁과 사상 교환, 시민권의 완전한 행사, 권력 남용 방지의 전제 조건이기 때문에 필수적이다.

정보의 자유가 다른 권리와 자유의 필수적 근간이라는 생각이 표명된 1946년 UN 총회 결의안 59(1)호는 "정보의 자유는 기본적 인권이며, UN이 헌신하는 모든 자유의 시금석"이라고 선언하고 있다. 비슷한 생각이 남아공의 2002년 정보접근증진법(Promotion of Access to Information Act of 2002)에도 분명히 나타나 있는데, 이 법은 "남아프리카 국민이 모든 권리를 보다 충실히 행사하고 보호할 수 있도록 정보에 효과적으로 접근할 수 있는 사회를 적극적으로 증진"하는 것을 목표로 한다.

개방성은 민주적 거버넌스와 인권 보호의 필수 조건이므로 정보기관 세계에서의 과제가 "비밀주의와 투명성 사이의 적절한 균형 찾기"로 규정되어서는 안 된다. 그보다 비밀주의는 *모든 경우에 있어 설득력 있는 정당화를 요하는 예외*로 간주되어야 한다. 전 세계 정보 공동체에서는 일부 예외가 포함된 비밀주의에 중점을 두지만 민주주의 사회에서는 개방성을 원칙으로 하고 일부 예외를 두어야 한다. 이것은 원칙의 문제이자 실천적 요청의 문제이다. 개방된 정치적 환경에서보다 비밀주의 환경에서 권력 남용과 인권 침해 가능성이 높다는 역사적 증거는 많다. 개방성을 통해 의회가 효과적으로 감독을 하고 언론 및 경계를 늦추지 않는 시민 사회 집단이 감시를 할 수 있으므로 불법 행위와 비행을 적발할 근거를 마련함으로써 면책 문화의 출현을 방지한다.

2.3 명시적 피해의 위험

그렇다면 개방성의 예외로서 정보기관 비밀주의의 적절한 근거는 무엇인가? 민주주의 국가와 권위주의 국가 모두 공통적 대답은 "국가 안보"이다. 이는 부적절하고 위험한 접근 방식인데, "국가 안보" 개념의 신축성과 모호성 때문이다.[2] 국가 안보를 넓게 해석하여 인간 안보의 모든 면을 아우를 경우, 이런 확대된 기초에 근거하는 비밀주의는 과도하고 비논리적인 기밀 정보 분류로 이어질 수 있다. "국가 안보"를 보다 협소하게 정의하는 경우에도 인권을 침해하는 예외적 수단을 국가가 정당화하는 구실로 이용되기 일쑤다. 예를 들어 조지 W. 부시 행정부의 고위 관료들은 국가 안보를 위한 고문의 사용을 지지했다.[3]

1971년 미 연방 대법원의 판결은 언론 자유의 제한과 관련하여 "국가 안보" 개념의 이러한 모호성에 관한 우려를 제기했다.

> *'안보'라는 단어는 광범위하고 모호한 일반론(generality)이다. 그 형체(contour)를 [언론의 자유를 다루는] 수정 헌법 제1조로 구체화된 기본법을 폐지하는 구실로 삼아서는 안 된다 . 대의 정부에게 정보를 주지 않으면서 군사 및 외교 기밀을 보호한다고 하여 우리 공화국의 실질적 안보가 지켜지는 것은 아니다.*[4]

민주주의에서 "국가 안보"라는 개념은 국가와 정부제도, 국가의 가치, 그리고 국가 관할 하에 있는 모든 사람의 안보를 포괄해야 한다. 따라서 국가 안보는 비밀주의가 아닌 개방성의 설득력 있는 근거가 된다. 인권 및 자유와 균형을 맞춰야 하는 성질의 것이 아니다. 국가 안보에 대한 민주적 접근 방식은 인권과 자유를 포함하고 수용한다.

정보 공동체와 관련한 비밀주의의 동기는 형체 없는 "국가 안보" 개념에 기초를 두기보다는 정보의 공개에서 비롯될 수 있는 *구체적이고 중대한 피해(specific and significant harm)*와 관련되어야 한다. 비밀주의는 정보 공개가 개인들의 생명, 정보기관, 국가 전체에 중대한 피해를 초래할 수 있는 분야로만 국한되어야 한다. 이러한 분야들은 다음과 같다.

- (정보기관 수장이 아닌) 정보관들의 신원
- 정보 제공자들의 신원
- 업무 방식의 기술적 세부 사항
- 요인 보호 세부 사항
- 현재 작전 및 수사
- 감시 대상 개인들의 신원과 개인정보

상황에 따라 위에 열거한 분야의 정보 공개로 인한 피해를 공개에 따른 공공의 이익과 비교해야 할 수도 있다. 예컨대 정보기관이 불법적으로 정치인을 겨냥해 작전을 벌인 경우, 요인 보호가 지나치게 허술한 경우, 혹은 정보기관 고위 관료들이 부끄러운 개인적 행위를 한 경우 공공의 이익을 위한

공개가 적절할 수 있다. 일반적으로 민주 정부는 민감한 정보의 공개로 인해 발생할 수 있는 피해를 모두 피할 수는 없다. 일부 피해는 감수해야 하는데, 비밀주의로 인한 위험이 민주적 질서 자체를 위태롭게 할 수 있기 때문이다.

정보 공동체 관련 정보에 대한 의회의 공개적, 개방적 접근은 의회 감독 위원회와 독립적 정보기관 감찰관 같은 전문 정보기관 감독 기구의 접근보다는 더 제한되어야 한다. 이들 기구는 위임 사항 이행을 위해 공공 영역에서 입수할 수 있는 것보다 많은 정보를 필요로 한다. 이들 기구가 필요로 하는 정보는 아래에서 논의한다.

2.4 정보기관 개방성의 실제적 이익

앞의 논의에서는 민주적 거버넌스, 인권 존중, 권력 남용 방지 측면에서 정보기관 개방성의 필요성에 초점을 맞췄다. 게다가 비밀주의를 줄이고 정보기관에 관한 정보 제공을 늘리면 기관 자체에도 이익이 된다. 지나치게 많은 정보를 기밀로 분류하는 기밀 구별 체계는 신뢰성을 잃고, 유지 및 집행이 어려우며, 비용도 많이 들고 비효율적이다. 무해한 정보를 기밀로 분류하고 보호하는 데 너무도 많은 시간과 노력이 들어갈 뿐 아니라 정작 진짜 민감한 정보의 보호에는 소홀해질 가능성도 있다.

유명한 1971년 미 연방 대법원의 국방부 비밀 보고서 (Pentagon Papers) 판결에서 포터 스튜어트(Potter Stewart) 판사는 이와 관련해 다음과 같이 말했다.

> *모든 것이 기밀로 분류되면 아무것도 기밀이 아닌 셈이 되어 냉소적이거나 경솔한 자들은 무시하고, 자기 보호나 자기 과시에 열중하는 자들이 조작할 수 있는 체제가 된다.*[5]

또한 머리말에서 지적했듯이 정보기관 투명성의 증대는 이들 조직에 대한 대중의 의심을 줄이고 공공의 신뢰를 높이는 데 일조할 것이다. 민주주의에서 이 점은 대단히 중요한데, 정보기관들이 공포와 강압이 아니라 협력적 관계를 통해 개인과 공동체로부터 정보를 얻어야 하기 때문이다.

3. 정보 보호 및 접근에 관한 입법

민주국가에서 위에서 개관한 정보기관의 비밀주의와 투명성에 관한 논쟁이 확실하고 항구적으로 해결되는 일은 없다. 특히 정보기관의 위기와 추문이 있을 때는 격렬한 다툼의 장이 될 수 있으며, 국가의 정치 및 안보 상황, 정보기관의 행위, 행정부와 의회 및 대중의 시각에 따라 개방성이 확대되거나 반대로 비밀주의가 강화되는 쪽으로 힘이 실릴 수 있다.

그럼에도 불구하고 이 논쟁은 국가 보유 정보에 대한 접근과 보호를 다루는 입법을 통해 공식적으로 해결된다. 이 법률에서 일반적으로 다루는 주제는 다음과 같다.

- 기밀 분류 및 공개의 원칙과 기준
- 기밀 분류 및 기밀 해제의 권한과 절차
- 기밀 분류에 대한 사법부 또는 기타 고위급 심의
- 국가 보유 정보에 접근할 개인 및 공공 이익 단체의 권리
- 이러한 접근 신청 절차 및 접근 거부 시 이의 제기 권리
- 기밀 분류와 접근에 관한 분쟁 판결에서 법원의 역할
- 불법적 정보 공개에 대한 처벌

정보기관에는 일반적으로 국가 보유 정보의 기밀 분류와 기밀 정보 보호 시스템 설계 및 유지의 책임이 있다. 또 법안 작성에도 참여할 수 있다. 이는 법률이 과도한 비밀주의로 경도될 위험을 초래한다. 정보기관들은 비밀주의를 선호하고 개방성에 반대하는 기능적 편향을 지니고 있기 때문에 법안 작성은 법무부 또는 헌법부 소관이어야 한다.

헌법 문제 및 정보기관을 다루는 의회와 의회 감독 위원회는 법률이 민주적 규범에 일치하도록 하는 데 결정적 역할을 한다. 이들은 행정부에 입법의 공적 동기와 논란이 되는 법 조항을 제시해 달라고 요청하고, 정당 간 활발한 논쟁을 촉진하며, 개인, 언론 및 기타 이익 집단들이 법안에 대한 의견을 낼 수 있는 공청회를 개최하고, 법안을 수정함으로써 법률의 질과 민주적 성격을 향상시킬 수 있다. 최종적으로 법률의 승인은 의회의 소관이다.

신생 민주주의에서 의원들은 모범 관행을 파악하기 위한 국제적 비교 검토를 통해 이익을 얻을 수 있다.[6] 다음은 정보 접근 및 보호 법률과 관련된 모범 관행에 해당된다고 할 수 있을 것이다.

- 투명성과 정보 접근이 인권과 자유, 굿 거버넌스, 공공 책임성, 정보 기반 논쟁을 증진하는 민주주의의 기본 원리로서 중요함을 법률로써 명시적으로 인정해야 한다. 정보의 기밀 분류는 결과적으로 사용을 자제해야 하는 예외적 수단임을 법률로써 명시해야 한다.
- 정보 접근에 대한 부적절한 제한을 방지하도록 법률로써 명시해야 한다 (상자 1).
- 기밀 정보 분류의 기준은 정보가 공개될 경우, 상당한 정도의 확실성을 가지고 중대한 피해가 발생할 수 있음을 보여 주어야 한다. "국가 안보"나 "국가 이익"이라는 모호한 근거로 비밀주의에 의존하는 것을 법률로써 허용하지 말아야 한다.
- 정보 공개와 비공개의 기준은 정부 관료들의 건전하고 일관성 있는 의사 결정을 촉진하고 개인들이 국가 보유 정보를 획득할 권리를 어떻게 행사할 수 있는지 이해할 수 있도록 정확하고 간결해야 한다.
- 법률로써 기밀 분류된 정보의 상황을 정기적(예: 5년마다)으로 검토하도록 규정해야 하며, 담당 관리들은 이 검토의 결과를 일반에 알려야 한다.
- 국가 보유 정보에 대한 개인 요청이 거부되는 경우, 담당 관리가 요청자에게 비공개 사유와 기밀 분류 기간을 알려 주어야 한다. 개인 또는 공공 이익의 증진을 위해 요청자가 관련 관리에게 정보 기밀 해제를 요청할 수 있음을 법률로써 규정해야 한다. 관리가 요청을 거부하는 경우, 요청자는 그 결정에 이의를 제기할 수 있어야 한다. 이의는 판사가 심리해야 한다.
- 법률에서 *문서*의 분류보다는 정보의 분류를 규정해야 한다. 이렇게 하면 정부 관리들은 전체 문서를 기밀로 분류하지 않고도 문서 내의 민감한 정보를 기밀로 분류할 수 있다. 그 다음 이러한 문서를 편집된 형태로 공개할 수 있다.
- 기밀 분류된 정보가 법정 소송과 관련된 경우, 정보를 비공개로 조회

할지 공개 법정에서 조회할지에 관한 결정은 행정부가 아닌 판사가 내려야 한다.

- 법률로써 기밀 정보의 불법 공개로 기소되는 자가 "공공의 이익"을 위한 공개라고 변론할 수 있도록 해야 한다. 이런 경우는 예를 들어 신문이 정보기관에 의한 불법 도청의 세부 사항을 폭로할 때 발생할 수 있다. 공공 이익 변론의 타당성은 사건을 심리하는 판사가 결정해야 한다.
- 아래에서 논의되는 것처럼, 법률로써 행정부가 정보기관 관련 정보를 포함한 국가 보유 정보에 대해 공공의 접근을 증진하고 촉진하기 위한 조치를 취하도록 할 의무를 설정해야 한다.

입법 모범 관행의 요소가 나열된 이 목록은 실질적 문제만큼 절차적 문제와도 관계가 깊으며, 정보 공동체에 관한 정보 등 국가 보유 정보와 관련된다. 다음 절들에서는 다양한 감독 기구에 제공되어야 하는 정보의 실질적 측면에 초점을 맞춘다.

상자 1: 부적절한 정보 분류 예방

미국의 기밀 정보 분류에 관한 행정 명령은 법률 위반이나 비효율성 또는 관리 실수의 은폐, 개인이나 조직 또는 기관을 난처하게 만들 소지의 예방, 국가 안보상 보호가 필요하지 않은 정보 공개의 방해나 지연을 목적으로 정보를 기밀로 분류할 수 없다고 명시하고 있다. 마찬가지로 슬로베니아 기밀정보보호법은 범죄와 관련된 정보의 기밀 분류를 금하고 있다. 멕시코와 페루의 경우, 관련 입법으로 인권 침해 및 국제법 위반과 관련된 정보의 기밀 분류를 금지한다.[7]

4. 의회의 정보 수요

민주주의에서 행정부와 국가 부처의 행동을 감독할 일차적 책임이 있는 기관은 의회다. 정보 공동체와 관련하여 의회는 이 책임을 이행하기 위해 정보 우선순위, 정보 관련 행정부 정책과 규정 및 행위, 정보 평가와 예산 및 재정 보고서, 정보기관에 관한 최고 감사 기구의 보고서, 전문가 정보기관 감

독 기구의 활동 및 조사 결과, 그리고 정보기관 행위에 대한 일체의 조사에 관한 정보를 필요로 한다. 본 절에서는 공개 의회 총회에서의 이러한 정보의 필요성을 다루며, 이와 대조되는 의회 정보기관 감독 위원회는 이후에 논의한다.

4.1 국가 정보 우선순위

주로 해마다 행정부는 다음 기간의 정보 우선순위가 무엇인지 결정해야 한다. 이는 정보기관들이 자체적으로 우선순위를 정해서는 안 되고, 위협과 정보 역점 분야의 우선순위가 고위 정책 사안이기 때문이다. 행정부의 정보 우선순위 결정은 정보기관들에 정치적 방향을 제시하며, 계획, 예산, 자원 배분, 운영 및 책임성의 기초가 된다.

행정부의 국가 정보 우선순위(NIP)는 기밀 정보로 분류되어서는 안 된다. NIP에 관한 의회의 논의는 국가 관할 하에 있는 사람들의 안전과 안녕에 심대한 영향을 미치는 국가 정책적 측면에 관한 책임과 민주적 의사 결정을 심화시킨다. NIP 공개로 국가 안보가 손상되지는 않을 것이다. 특정 개인과 조직을 거명하는 대신 “조직범죄,” “테러리즘,” “핵 확산” 같은 범주만을 언급하여 NIP를 의회에 제공할 수 있기 때문이다.

의회에 제공되는 NIP 버전에서는 민감한 정보를 제외하고, 의회 정보기관 감독 위원회에는 비밀이 유지되는 상태로 민감한 정보를 제공할 수도 있다.

4.2 행정부 정책, 규정, 행위

정보기관에 관한 행정부 정책과 규정은 민주주의가 뿌리내린 체제에서도 비밀인 경우가 많다. 이는 책임성이라는 기본적 원칙에 위배되기 때문에 비정상적이며 바람직하지 않다. 특히 헌법적 권리를 침해하는 수사 방식과 관련하여 정보기관에 적용되는 주요 규칙들은 의회의 논의와 심의의 대상이 되어야 한다. 운영 방식에 관한 민감한 기술적 세부 사항이 드러나기 때문에 비밀로 해야 할 부처의 규칙 및 절차와, 민주적 거버넌스에 필수적이기 때문에 공공의 영역에 있어야 할 행정부 규정 및 정책은 구별해야 한다.

행정부는 정보기관 입법에 근거하여 다음 주제에 관한 행정부 정책과 규정을 의회에 제출해 검토와 조언을 받아야 한다.

- 헌법적 권리를 침해하는 권한을 포함한 정보 조직의 기능과 권한의 행사
- 민감한 기술적 세부 사항을 제외한 운영 정책
- 장관의 통제 및 정보기관과 국가수반, 내각, 정보기관 주무장관과의 관계
- 다양한 정보 기구들 간의 관계와 책임의 분배, 정보의 조정, 국가 정보 조정 메커니즘의 기능
- 외국 정보기관과의 관계 및 외국 정부와 개인정보공유 기준과 규칙
- 정보기관의 징계 제도와 헌법 및 법의 지배 존중을 보장할 내부 메커니즘

의회는 국가 기관뿐 아니라 행정부를 감독할 책임도 있다. 따라서 정보기관과 관련된 행정부의 중요 행위에 관한 정보가 필요하다. 관련 행위에는 고위직의 임명과 해임, 고위직에 대한 징계 행위, 법적 요건인 경우 침해적 업무에 대한 장관의 승인(도구 5 참조), 정보 공동체의 체계 및 운영과 관련된 주요 개혁과 혁신이 포함된다. 공공 영역에 두기에는 너무 민감한 정보는 의회의 정보기관 감독 위원회에 제출해야 한다.

4.3 정보기관의 연례 보고서

민주주의에서 정부 부처와 기타 국가 기관의 연례 보고서 발행은 의회와 일반 대중에 대한 책임성을 보장하는 필수적 수단이다. 연례 보고서는 정부의 우선순위와 정책이 준수되고 있는지, 납세자들이 납부한 세금만큼의 가치를 돌려받고 있는지를 의회가 판단할 근거가 된다. 이 관행에서 정보기관을 제외할 타당한 이유는 없다. 네덜란드 일반정보보안국(AIVD)의 연례 보고서는 국가 안보 훼손 없이 포괄적이고 유용한 정보를 제공하는 훌륭한 예이다.8

정보기관의 연례 보고서는 (민감한 세부 사항을 누설하지 않고) 정보기관의 연간 목표 및 우선순위, 주요 안보 위협의 평가, 정보 정책과 체계 및 운영

상 주요 개혁, 기관의 보고 및 책임 기능 이행, 정보 자유 입법에 따른 정보 요청에 대한 기관의 대응과 같은 사안을 다뤄야 한다.

4.4 정보 평가

많은 경우, 개인과 조직에 대한 정보 공동체의 평가는 정보 업무와 범죄 수사를 훼손할 위험이 있으므로 의회에 제출하기에는 부적합하다. 그러나 안보와 안보 위협 범주를 다루는 정보 평가는 피해의 위험 없이 수시로 공개될 수 있다.

일례로 캐나다 보안정보국(CSIS)은 경제 안보, 무기 확산, 테러 방지 등의 주제에 관한 배경 문서, 캐나다 안보 관련 문제에 초점을 맞춘 이른바 *Commentary* 간행물, 공개 출처 정보에 관한 CSIS의 검토에 기초한 일련의 연구 보고서 등 다양한 자료를 발간한다.[9] 네덜란드 일반정보보안국의 연례 보고서에는 더 나아가 이름이 명시된 급진 조직과 테러 조직들에 관한 설명까지 포함된다.[10]

의회와 의회 정보기관 감독 위원회에 이러한 평가를 제출하는 것은 책임성의 중요한 형식으로서 의원들, 학계, 비정부 조직들이 정보기관의 정치적 관점과 안보관을 논의할 수 있게 한다. 시간이 지남에 따라 정보에 기초한 의회 및 공공의 논의를 통해 이 관점들이 개선될 수도 있다.

4.5 예산, 재무 보고서, 최고 감사 기관의 보고서

민주국가에서 의회는 정부 기관의 연간 예산과 재무 보고를 받고, 심의하며, 논의한다. 이는 불가결한 책임성의 형태이며, 선출된 국민의 대표들이 법률, 정부 정책, 의회 자체 우선순위 및 선호에 따라 공공 자금 사용을 감독하고 승인할 수 있도록 해 준다. 그러나 정보기관의 완전한 재무 보고 및 예산은 비밀이 유지되는 상태에서만 의회 감독 위원회에 제공되는 것이 일반적이며, 전체가 의회에 상정되지는 않는다(도구 8 참조).

정보 조직들은 외국 정보기관에 유리해질 수 있다는 논리로 예산 공개에 반대한다. 이 주장은 과장된 것이다. 외국 정보기관이 다른 나라 정보기관이 얼마나 예산을 쓰는지 안다고 해서 이득을 볼 일은 없다. 사실 인력, 운영 경비, 자본 지출로 나뉜 지출 내역을 공개한다 하여 아무런 이득이나 피해는 없다. 공개를 통해 안보가 훼손될 수 있는 경우는 목표물, 방식, 출처, 운영 결과 및 제약과 관련된 훨씬 더 세부적인 사항이 공개될 때뿐이다(상자 2 참조).

상자 2: 정보 예산 및 재무 보고 공표

2006년, 남아공의 장관정보심의위원회(Ministerial Review Commission on Intelligence)는 정보기관들이 의회 정보 감독 위원회에 매년 제출하는 기밀 예산, 재무 보고서, 전략 계획을 조사했다. 위원회는 이들 문서의 공개가 정보활동이나 국가 안보를 전혀 위태롭게 하지 않는다고 결론 내렸다. 위원회는 정보 예산과 재무 보고를 의회에 공개해야 한다는 재무부의 견해에 동의했다. 민감한 정보의 경우, 감독 위원회 비공개 회의에서 심의하는 문서로 제한할 수 있을 것이다.[11]

마찬가지로 정보기관에 관한 최고 감사 기구의 연례 보고서도 의회에 제출되는 공개 보고서와 의회의 관련 감독 위원회에 제출되는 더 상세한 기밀 보고서라는 두 가지 버전이 있어야 한다. 감사관 보고서 준거법은 민감한 정보의 보호에 관해 규정해야 한다(상자 3 참조).

상자 3: 재무 감사에서의 민감 정보 보호

남아공의 2004년 공공감사법에는 민감한 정보의 보호에 관한 몇 개 조항이 포함되어 있다. 이 법에서 감사관은 감사 과정에서 획득한 비밀 또는 기밀 정보가 공개되지 않도록 예방 조치를 취해야 한다고 명시하고 있다. 감사관은 기밀 보안 계정에 관해 보고할 때 "계정의 특별한 성격을 참작하여, 관련 장관의 서면 조언에 기해, 국가 이익을 근거로, 비밀 또는 기밀 분류된 세부 사항이 제외되었음을 감사 보고서에 명시하는 경우에 이러한 세부 사항을 감사 보고서에서 제외할 수 있다."

4.6 정보기관 스캔들 처리

앞의 논의에서는 의회가 감독 책임 이행 과정에서 필요로 하는 정보기관 정보에 초점을 맞췄다. 정보기관과 관련된 위기(예: 정치인 사찰의 폭로)가 있는 경우, 의회는 조사 위원회를 설립하거나 전문 정보기관 감독 기구에 조사를 시행하도록 요청할 수 있다. 조사 결과는 의회에서 공개적으로 설명되고 논의되어야 한다. 이것이 공개적으로 이루어지지 않으면 조사에 대한 공공의 신뢰도, 어떠한 범법 행위도 제대로 처리된다는 공공의 확신도 없을 것이다.

5. 전문적 정보기관 감독 기구의 정보 요구

전문적 정보기관 감독 기구(가장 중요한 것은 의회 정보기관 감독 기구, 독립적 정보 감찰관, 그리고 네덜란드의 정보보안국심의위원회 같은 전문가 정보기관 감독 기구)가 필요로 하는 정보는 이들 기구의 위임 사항과 기능에서 도출된다. 위임 사항과 기능은 나라마다 다르지만, 다음이 포함될 수 있다.

- 정보기관의 헌법, 법률, 규칙, 정부 정책 준수
- 법적 위임 사항 및 기능과 정부가 정한 우선순위에서의 정보기관의 성과와 성공
- 불법 행위 예방, 적발, 처리를 위한 내부 시스템과 방법
- 내부 재정 시스템과 지출

본 절에서는 이런 감독 기능을 고려하여 의회 정보기관 감독 위원회, 독립적 정보 감찰관 및 기타 옴부즈맨 기관, 사법부가 필요로 하는 정보를 검토한다. 그다음 부주의나 고의에 의한 기밀 정보 공개 위험을 최소화하는 방법을 살펴본다.

5.1 의회 정보기관 감독 위원회

의회 전체에 제출되는 모든 정보기관 관련 정보는 당연히 의회 정보기관 감독 위원회도 받게 된다. 위원회가 먼저 이 정보를 받게 되는 것이 일반적인데, 의회 논의에 앞서 신중한 조사와 숙의, 정보기관 고위층 및 행정부의 정보기관 담당 구성원과의 대화 기회를 주기 위해서다. 그러면 집단으로서의 위원회와 상이한 정당을 대표하는 위원들은 정확한 정보를 바탕으로 보다 폭넓은 의회의 논의에 조언을 제공할 수 있다.

또한 감독 위원회는 전체 의회에 제출되는 것보다 더 상세하고 더 민감한 정보를 비밀이 유지되는 상태로 받아야 한다. 위원회가 상세 정보를 받아야 하는 주제는 다음과 같다.

- 행정부의 국가 정보 우선순위
- 정보 관련 행정부 정책, 규정, 행위
- 정보기관의 연례 보고서
- 정보기관의 안보 및 위협 평가
- 정보기관의 연간 예산 및 재무 보고서
- 정보기관에 관한 최고 감사 기구의 보고서
- 전문가 정보 감독 기구(있는 경우)의 활동 및 조사 결과

중요하면서 어려운 질문은 감독 위원회에 제공하는 정보가 어느 정도 상세해야 하고 민감도는 어느 정도여야 하느냐다. 한편으로 위원회 위원들은 비밀 유지 훈련이 되어 있지 않으며, 국가와 소속 정당 모두에 충성할 의무가 있다. 그뿐만 아니라 비밀 정보를 보유한 사람들이 많아질수록 정보가 비밀로 유지될 가능성은 더욱 작아진다. 그러므로 정보기관들은 그들의 운영, 방식, 인력에 관한 민감한 상세 정보를 제공하기 꺼린다. 다른 한편으로 의회 위원회는 감독 기능을 제대로 수행하기 위해서 충분히 상세한 정보를 받아야 한다. 정보기관이 내주지 않는 정보가 너무 많으면 감독은 피상적이게 되며, 불법 행위나 성과 불량 또는 자금 남용을 제대로 적발하거나 조사할 수 없다.

의회 감독 위원회에 얼마나 상세하고 얼마나 민감한 정보를 제출해야 하는지는 의회와 정보기관 또는 의회와 행정부 간의 오해와 분쟁 가능성을 최소화하기 위해 법률에서 최대한 정확하게 규정해야 한다. 입법에서 이런 규칙과 지침을 명시하는 방식은 나라마다 다르다(몇 가지 예는 상자 4 참조).

상자 4: 의회 감독 위원회의 정보 접근에 관한 법률 조항

루마니아에서 정보기관들은 정보 제공이 진행 중인 업무, 요원의 신원, 방법 또는 출처를 위태롭게 하지 않는 한 합당한 기간 안에 의회 정보 감독 위원회의 정보 요청에 응해야 한다. 의회 위원회는 예고 없이 기관을 방문할 수 있으며, 인력, 데이터 및 시설에 대한 전면적 접근권이 부여된다.[13] 반면 영국에서는 의회 감독 위원회의 현재 위임 사항이 정보 보안 기관의 "지출, 행정, 정책"으로 제한돼 위원회 소관 범위에서 암묵적으로 업무가 배제되어 있어 정보에 대한 접근 또한 제한된다.[14]

법률에서는 의회 위원회의 정보 접근과 관련된 분쟁 해결 수단도 명시해야 한다. 예컨대 남아공의 경우, 관련법에서 정보 장관, 정보기관 수장, 의회 감독 위원회 위원장, 정보 감찰관으로 구성된 특별 위원회가 분쟁을 해결한다고 명시하고 있다.[12]

정보기관 관련 정보를 획득할 수 있는 의회 감독 위원회의 권한은 나라마다 다르다. 일상적으로 위원회는 정보 담당 행정부 구성원(들), 정보기관, 최고 감사 기구, 침해적 업무 승인을 담당하는 판사 또는 행정부 구성원, 존재하는 일체의 전문가 정보 감독 기구로부터 정기 보고를 받아야 한다. 위원회는 또 이들 기구에 보고서를 요청할 권한도 가져야 한다. 그뿐만 아니라 조사, 증인 소환, 정보기관 부지 조사 권한도 가질 수 있다.

5.2 정보 감찰관 및 기타 옴부즈맨 기관

정보기관을 둘러싸고 있는 비밀주의는 효과적 감독에 상당한 어려움을 준다. 따라서 특별한 권한과 전문성을 지닌 정보 감독 기구가 필요하다. 이런 기구 중 하나가 독립적 정보 감찰관(IG)이다.[15] 비밀이 유지되는 환경에서 효과적 감독을 수행하기 위해서는 IG가 다음과 같은 특징을 가져야 한다.

- IG는 임기가 보장된 독립적 관리여야 한다.
- IG는 정보기관의 헌법, 법률, 정부 정책 준수를 감시하고 불법 행위, 위법 행위, 권력 남용에 대한 민원을 조사할 법적 위임 사항과 권한을 가져야 한다.

- IG는 정보 주무장관뿐 아니라 의회 정보 감독 위원회, 그리고 중대한 조사의 경우, 의회 전체에 보고해야 한다.
- IG와 그 보좌진은 정보 분야에서 고도의 전문성과 경험이 있어야 한다.

또한 IG 관련 법률에서 감찰관과 그 보좌진이 정보기관 통제 하의 첩보나 정보 또는 부지에 접근하는 것이 거부되어서는 안 된다고 규정해야 하며, 그러한 접근 거부는 형사상 범죄가 된다고 규정해야 한다. 이것은 독립적 감독 기구가 비밀 업무와 시스템을 조사할 때 필수적인 요건이다.

IG에 관한 앞선 지적은 정보 감찰관이 없는 나라에서 인권 위원 등의 그 밖의 옴부즈맨 기관에도 똑같이 적용된다. 전문 IG 방식의 큰 장점은 감찰관과 그 보좌진이 정보 전문성을 갖추고 있어 비밀스러운 환경에서의 부정행위를 적발하는 동시에 그들이 접근한 기밀 정보를 적절히 보호할 수 있다는 점이다.

정보기관의 지출, 예산 배정, 수입(있는 경우), 재정 시스템을 감사할 때 최고 감사 기구는 정보기관의 비밀 업무와 비밀 자금에 관련된 모든 정보에 접근할 수 있어야 한다(더 자세한 내용은 도구 8 참조). 따라서 최고 감사 기구에는 기밀문서를 다루는 훈련이 되어 있고 기밀 취급 인가를 받은 전문가 팀이 있어야 한다. 아니면 독립적 정보 감찰관 직이 최고 감사 기구와 공동으로 재정 감사를 수행하는 것이 적절할 수도 있을 것이다.

5.3 사법부

정보기관과 법 집행 기관들은 통신 감청, 수색, 체포 같은 침해적 업무를 수행할 때 프라이버시권을 침해하게 된다. 따라서 대부분의 민주국가에서는 정부기관이 이러한 업무를 수행하려면 사법부의 승인을 얻어야 한다(자세한 내용은 도구 5 참조). 나라에 따라 기관들이 어느 판사에게나 승인을 요청할 수 있는 경우도 있고 모든 감청 신청을 심리하는 전담 판사가 있는 경우도 있다.

판사가 필요로 하는 정보는 보통 통신 감청에 관한 법률에 명시되어 있다. 신청인은 감청이 범죄 행위 또는 국가 안보나 공공 안전에 대한 위협에 관

한 정보를 수집하기 위해 필요하고도 정당한 수단임을 판사에게 입증할 수 있는 충분한 사실관계를 제시해야 한다. 법률에서 통신 감청을 최후의 수단으로 간주할 수도 있는데, 이 경우 신청인은 비침해적 방법으로는 부족하거나 부적절하다는 점도 판사에게 납득시켜야 한다.

감청 문제 외에도 정보 공동체와 관련된 형사 또는 민사 사건이 법정에서 다뤄질 수도 있는데, 예컨대 정보관이 위법 행위로 기소되거나 정치인이 자기 사무실이 불법 도청되었다고 주장하는 경우가 그렇다. 행정부 입장에서는 이런 사건들의 일부 또는 전부를 비공개로 심리하기를 원할 수 있다. 민주주의 국가들은 이 문제를 다루는 방식이 서로 다르다. 입법부가 다룰 수도 있고 재판장의 판단에 맡길 수도 있다(상자 5).

또한 IG 관련 법률에서 감찰관과 그 보좌진이 정보기관 통제 하의 첩보나 정보 또는 부지에 접근하는 것이 거부되어서는 안 된다고 규정해야 하며, 그러한 접근 거부는 형사상 범죄가 된다고 규정해야 한다. 이것은 독립적 감독기구가 비밀 업무와 시스템을 조사할 때 필수적인 요건이다.

IG에 관한 앞선 지적은 정보 감찰관이 없는 나라에서 인권 위원 등의 그 밖의 옴부즈맨 기관에도 똑같이 적용된다. 전문 IG 방식의 큰 장점은 감찰관과 그 보좌진이 정보 전문성을 갖추고 있어 비밀스러운 환경에서의 부정행위를 적발하는 동시에 그들이 접근한 기밀 정보를 적절히 보호할 수 있다는 점이다.

정보기관의 지출, 예산 배정, 수입(있는 경우), 재정 시스템을 감사할 때 최고 감사 기구는 정보기관의 비밀 업무와 비밀 자금에 관련된 모든 정보에 접근할 수 있어야 한다(더 자세한 내용은 도구 8 참조). 따라서 최고 감사 기구에는 기밀문서를 다루는 훈련이 되어 있고 기밀 취급 인가를 받은 전문가 팀이 있어야 한다. 아니면 독립적 정보 감찰 관직이 최고 감사 기구와 공동으로 재정 감사를 수행하는 것이 적절할 수도 있을 것이다.

5.3 사법부

정보기관과 법 집행 기관들은 통신 감청, 수색, 체포 같은 침해적 업무를 수행할 때 프라이버시권을 침해하게 된다. 따라서 대부분의 민주국가에서는 정부기관이 이러한 업무를 수행하려면 사법부의 승인을 얻어야 한다(자세한 내용은 도구 5 참조). 나라에 따라 기관들이 어느 판사에게나 승인을 요청할 수 있는 경우도 있고 모든 감청 신청을 심리하는 전담 판사가 있는 경우도 있다.

판사가 필요로 하는 정보는 보통 통신 감청에 관한 법률에 명시되어 있다. 신청인은 감청이 범죄 행위 또는 국가 안보나 공공 안전에 대한 위협에 관한 정보를 수집하기 위해 필요하고도 정당한 수단임을 판사에게 입증할 수 있는 충분한 사실관계를 제시해야 한다. 법률에서 통신 감청을 최후의 수단으로 간주할 수도 있는데, 이 경우 신청인은 비침해적 방법으로는 부족하거나 부적절하다는 점도 판사에게 납득시켜야 한다.

감청 문제 외에도 정보 공동체와 관련된 형사 또는 민사 사건이 법정에서 다뤄질 수도 있는데, 예컨대 정보관이 위법 행위로 기소되거나 정치인이 자기 사무실이 불법 도청되었다고 주장하는 경우가 그렇다. 행정부 입장에서는 이런 사건들의 일부 또는 전부를 비공개로 심리하기를 원할 수 있다. 민주주의 국가들은 이 문제를 다루는 방식이 서로 다르다. 입법부가 다룰 수도 있고 재판장의 판단에 맡길 수도 있다(상자 5).

상자 5: 법정 소송에서의 민감 정보 처리

2008년 남아공 헌법재판소가 심리한 사건에서 한 신문사는 국가정보국(NIA)이 연루된 사법 절차 기록 중 제한된 일부의 공개를 강제하는 명령을 신청했다. 이 신청의 근거는 재판의 공개(open justice)에 대한 권리였다. 정보장관은 국가 안보를 근거로 공개에 반대했다. 헌법재판소는 자료 일부의 공개를 명하면서 국가 안보상 타당한 비공개 근거가 없다고 판결했지만 외국 정보기관과의 관계, NIA 내 지휘 계통, NIA 정보원들의 신원과 관련된 그 밖의 정보는 계속 기밀로 유지해야 한다고 판결했다. 소수 의견은 특정 정보원의 이름을 제외한 모든 자료를 공개하는 것이 공공의 이익에 부합한다는 것이었다.[16]

5.4 감독 기구의 책임성 강화

민주국가에서 의회와 독립적 기구의 정보기관 감독은 비교적 강력할 수 있지만 감독 기구의 공공 책임성이 부족할 수 있다. 감독 기구 자체가 너무도 비밀스러운 것이다. 이는 감독 기구와 정보기관에 대한 공공의 신뢰를 모두 떨어뜨린다. 따라서 의회에 유의미한 보고서를 제출하고, 정보기관의 보고서뿐 아니라 자체 보고서도 자신의 웹사이트에 공개하는 것이 감독 기구의 의무이다. 이런 관행의 모범은 네덜란드 정보보안기관심의위원회인데, 위원회의 감시와 조사에 관한 종합적 보고서를 매년 공개한다.[17]

5.5 기밀 정보 공개 위험 최소화

앞서 언급했듯이 정보기관들은 의회 감독 위원회 위원들이 정치인이고 일반적으로 기밀 정보 보호 규율 및 관행과 관련된 훈련을 받지 않는다는 이유로 의회 감독 위원회에 민감한 정보를 공개하는 데 반대하는 경우가 있다. 민감한 정보가 고의 또는 부주의로 공개될 위험이 있다는 것이다. 이런 위험을 최소화하기 위해 취할 수 있는 조치는 다음과 같다.

- 정보 보호에 관한 법률로 기밀 정보의 무단 공개를 형사 범죄로 규정한다.
- 의회 감독 위원회 위원 임명 전에 정보기관의 심사를 받게 한다.[18]
- 위원회가 비공개 회의를 주최할 권한을 법률로 부여한다.
- 정보 전문가들이 감독 위원회 사무실, 컴퓨터, 전화, 서류 정리 체계가 감시로부터 보호되는지 확인한다.
- 정보 전문가들이 위원회 위원과 보좌진에게 교육과 훈련을 제공한다.
- 위원회와 정보기관이 공동으로 기밀 정보의 수령, 보유, 사용, 파기에 관한 규칙과 절차에 합의한다.

위의 조치들은 다른 전문가 감독 기구 전체 또는 일부와도 관련된다. 그러나 이들 기구가 정치인이 아닌 전문가로 구성되는 경우에는 기밀 정보가 공개될 위험이 더 적을 수 있다.

6. 권고 사항

- 국가 보유 정보의 투명성과 접근성은 민주적 거버넌스, 인권 보호, 권력 남용 방지의 필수 조건이다. 따라서 비밀주의는 예외적이어야 한

다. 정보 공동체와 관련하여 비밀주의는 정보 공개에서 발생할 수 있는 구체적이고 중대한 피해에 근거해야 한다. 비밀주의는 공개가 개인들의 생명, 정보기관, 국가 전체에 심각한 피해를 입히는 분야로 한정되어야 한다. 공개로 인해 발생할 수 있는 피해와 공개에 따른 설득력 있는 공공의 이익을 비교 형량해야 할 수도 있다.

- 정보 보호와 접근에 관한 법안 작성의 책임은 정보기관이 아니라 법무부 또는 헌법부의 소관이어야 한다. 의회는 법률이 민주적 규범에 부합하도록 노력해야 한다.
- 법률로써 정보의 투명성과 접근성이 민주주의의 기본 원칙이고, 정보의 기밀 분류를 남용하지 않아야 함을 강조해야 한다. 기밀 정보 분류 기준에서는 비공개가 정당화되기에 충분한 정도의 피해와 확실성을 명시해야 한다. 법률로써 기밀 정보의 불법 공개로 기소된 자가 공공의 이익을 위한 것이라는 변론을 제기할 수 있도록 해야 한다. 행정부에는 정보기관에 관한 정보를 포함한 국가 보유 정보에 대한 공공의 접근을 증진하고 촉진할 의무가 부과되어야 한다.
- 의회는 정보 우선순위, 정보 관련 행정부 정책과 규정 및 행위, 정보 평가와 예산 및 재무 보고서, 정보기관에 관한 최고 감사 기구 보고서, 전문가 정보 감독 기구의 활동과 조사 결과, 정보기관의 행위에 대한 일체의 조사에 관한 정보를 필요로 한다. 의회 정보 기구 감독 위원회는 이들 주제에 관한 더 상세하고 더 민감한 정보를 기밀이 유지되는 상태로 받아야 한다. 정보는 위원회가 적절히 감독 기능을 수행하기에 충분해야 한다. 이와 관련된 세부 사항은 법률에 명시해야 한다.
- 정보 감찰관 또는 전문가 정보 감독 기구에 적용되는 법률에서 정보기관 통제 하의 첩보, 정보 또는 부지에 대한 이 기구들과 직원의 접근이 거부되어서는 안 되며, 그러한 접근 거부는 형사 범죄에 해당한다고 규정해야 한다.
- 정보기관이 연루된 형사 또는 민사 사건에서 사건의 일부 또는 전부를 비공개로 심리할지 여부의 결정은 재판장이 내려야 한다.
- 감독 기구는 의회에 유의미한 보고서를 제출해야 하며, 정보기관의 보고서뿐 아니라 감독 기구의 보고서도 감독 기구 웹사이트에 공개해야 한다.

▪ 의회 정보 감독 위원회 위원들이 고의 또는 부주의로 기밀 정보를 공개할 위험을 줄이기 위한 조치를 취할 수 있다. 정보기관이 위원들을 심사하거나 위원들이 기밀 정보 보호 훈련을 받거나 위원들의 사무실, 컴퓨터, 전화, 서류 정리 시스템을 감시로부터 보호할 수 있다.

후주(後註)

1. 이 도구는 2006년 남아공 정보장관이 설립한 장관정보심의위원회 위원으로서의 필자의 경험에 기초한 것이다. 이 도구는 또 L. Nathan, *Lighting up the Intelligence Community: A Democratic Approach to Intelligence Secrecy and Openness,* Policy Paper (Birmingham, UK: Global Facilitation Network for Security Sector Reform, 2009)에도 기초한다.

2. 이 점에 관한 상세한 논의는 A. Wolfers, "'National Security' as an Ambiguous Symbol," *Political Science Quarterly* Vol. 67, No. 4 (1952), pp. 481 – 502 참조.

3. American Civil Liberties Union, *The Torture Report web site* (available at www.thetorturereport.org).

4. *New York Times Co vs United States* 403 US 713 (1971) at 719.

5. *New York Times Co vs United States* 403 US 713 (1971).

6. 이러한 검토의 예로는 D. Banisar, "Public Oversight and National Security: Comparative Approaches to Freedom of Information," in *Democratic Control of Intelligence Services: Containing Rogue Elephants,* eds. H. Born and M. Caparini (Aldershot, UK: Ashgate, 2007), pp. 217 – 235 참조.

7. 이 상자의 정보는 Banisar, "Public Oversight"에서 가져온 것이다.

8. 이들 보고서는 네덜란드 일반정보보안국 웹사이트에서 볼 수 있다 (https://www.aivd.nl/english/). 2010년 보고서는 https://www.aivd.nl/english/publications-press/@2827/annual-report-2010/ 참조.

9. 캐나다 보안정보국 웹사이트 참조 (www.csis-scrs. gc.ca).

10.Banisar, "Public Oversight" 참조.

11.South Africa, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10 September 2008) (available at www.ssronline.org/document_result. cfm?id=3852).

12.South Africa, Intelligence Services Oversight Act, Act No. 40 of 1994, Section 4(2)(b).

13.C. Matei, "Romania's Transition to Democracy and the Role of the Press in Intelligence Reform," in *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness,* eds. T. Bruneau and S. Boraz (Austin: University of Texas Press, 2007), p.227.

14.P. Gill, "Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the 'War on Terror,'" Intelligence and National Security Vol. 22, No. 1 (February 2007), pp. 14 - 37.

15.독립적 법정직인 정보 감찰관(호주, 뉴질랜드, 남아공의 경우)과 정보 조직 내에 속하는 감찰관(미국 중앙정보국의 경우)을 구별해야 한다.

16.*Independent Newspapers (Pty) Ltd vs Minister for Intelligence Services* CCT 38/07 [2008] ZACC 6 (South Africa).

17.이 위원회의 연례 보고서는 http://www.ctivd.nl/에서 볼 수 있다.

18.의회 감독 위원회 위원 심사에 관한 더 자세한 내용은 H. Born and I. Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Geneva: DCAF, University of Durham, and Parliament of Norway, 2005), pp. 88–90 참조.

도구 4

감독 시행

모니카 덴 보어(Monica den Boer)

4. 감독 시행

모니카 덴 보어(Monica den Boer)

1. 머리말

신생 민주주의에서는 개방성, 투명성 같은 특정 민주적 가치와 정보 업무 사이에 존재하는 고유의 긴장 때문에 정보 공동체에 대한 효과적 감독이 매우 중요하다. 국가 정보기관을 민간의 통제 하에 두려고 한다면 민간인들이 정보 업무에 관한 교육을 받아야 한다. 그렇지 않으면 기관의 전문가들이 계속 업무를 독점하게 될 것이다. 폐단을 방지하면서도 민주주의 사회에서 정보기관의 정당한 역할을 계속 지지하는 새로운 정치 문화 또한 발전해야 한다.

이 도구는 감독 기구가 정보기관의 활동을 어떻게 조사하는지 설명한다. 특별 조사부터 장기 조사까지 최대한 광범위하게 감독을 살펴본다. 또한 복수의 상설 기구들이 감독 책임을 맡는 상황과 상설 조직이 없고 임시 조직을 창설해야 하는 상황도 살펴본다.

아울러 이 도구의 목표는 정보 감독을 시행하는 방법에 관한 실용적 지침 역할을 하는 것이다. 여러 나라의 감독 기구들이 비슷한 여러 가지 난관에 당면해 있기 때문에 기본적 방법론을 이해하면 신설 감독 기구들이 공통적인 함정을 피하고 효과성을 극대화하는 데 도움이 될 수 있다.

2. 정보기관 감독 시행의 이유

정보 책임성에는 여러 계층이 있다. 이 중 일부는 내부적으로는 정보기관 관리들이, 외부적으로는 행정부 구성원들이 행하는 정보기관 통제와 관련된다. 다른 일부는 의회, 사법부, 전문가 감독 기구가 수행하는 감독과 관련된다(도구 1 참조). 정보기관 감독의 근본적 목표는 국가 정보기관의 부적절한 행위를 막는 것이다. 기관을 직접 관리하는 것을 가리키는 *통제(control)*와는 달리 *감독(oversight)*에는 감시, 평가, 검토, 심의가 포함된다. 감독 기구는 개방성과 투명성 증진을 통해

기관 내의 권력 남용 경향을 억제하고 의회와 행정부 구성원들(및 그 밖에 통제 책임을 행사하는 자)에게 유용한 정보와 전문성을 제공할 수 있다.

2.1 인권 침해

정보기관에 의한 인권 침해의 가능성은 언제나 일반 대중이 우려할 만한 사유가 된다. 예를 들어 1960년대와 1970년대에 미국 정부 기관들은 시민권 운동 및 반전 운동을 상대로 한 비밀 첩보 작전을 승인했다. 보다 최근에는 테러 방지에 협력하고 있는 국가 정보기관들이 특별 송환, 비밀 수감 시설 운영, 고문으로 얻은 정보 사용 같은 관행을 활용했다. 인권을 명백히 위협하는 이런 관행들은 모두 적절한 감독 사안이다.

감독 기구는 종종 언론, 특히 휴먼 라이츠 워치(Human Rights Watch), 국제사면 위원회 같은 비정부 조직의 제보를 바탕으로 취재하는 탐사 보도 기자들을 통해 부적절하거나 불법적인 행위에 주목하게 된다. 마리나 카파리니(Marina Caparini)에 따르면,

> *"언론은 개인과 단체를 정부와 연결하는 연결 조직에 해당하며, 여론과 정책 선호의 변화에 관한 정보를 전달하는 데 결정적 역할을 한다. 대중이 정보를 얻고 정부의 결정, 행위, 권력 남용에 대한 공공의 감시를 통해 정부에 책임을 물을 수 있는 것은 주로 자유로운 언론을 통해서다."*[1]

2.2 의회의 질의

의원들은, 감독 위원회 소속이 아니더라도 정보기관의 활동에 관해 질의할 수 있다. 질의는 위협 수준과 기관 우선 과제에 관한 일반적 질문부터 비밀스러운 방식과 특정 집단과의 상호 작용에 관한 구체적 질문까지 다양하다. 경우에 따라서는 감독 메커니즘이 아직 존재하지 않는 새로운 업무가 시작될 때 나타나는 법적 공백을 질의를 통해 밝힐 수도 있다. 예를 들어 2003년에 네덜란드 의원들은 이라크 사담 후세인 전(前)정부가 보유했다는 대량 살상 무기와 관련된 정보수집에 관해 질의했다.[2] 이 질의는 네덜란드 이라크조사위원회의 설립으로 이어졌다.

3. 감독 위임 사항

정보기관들은 그들이 봉사하는 정부의 법률, 명령, 인가, 정책을 준수해야 한다.[3] 정보 기관 감독 기구도 마찬가지로 그 조사 권한을 창설하고 제한하는 법률이나 위임 사항을 존중해야 한다. 정치적 논란을 피하기 위해 감독 위임 사항은 최대한 중립적으로 작성되는 것이 보통이다. 이는 특정 사건에 관한 특별 조사처럼 감독 기구가 일시적인 경우에 특히 중요하다. 그럼에도 불구하고 위임 사항은 구체적이고 명확해야 하며, 감독 대상 기관(들)의 권한, 방식, 자원에 적합해야 한다.

감독 기구들의 위임 사항은 상호 보완적이거나 서로 중첩될 수 있다. 후자의 경우가 바람직한데, 일반적으로 하나의 감독 메커니즘으로는 부족하다고 보기 때문이다. 이런 이유로 이탈리아에서는 최근 헌법 재판소에 의한 사후 감독에 그치던 정보기관 감독 체계를 확대해 내부 관리 기구(감찰국)와 외부 정치 기구(의회공화국안보위원회[COPASIR])라는 2개의 새로운 메커니즘을 포함시켰다.[4] 캐나다 보안정보국(CSIS)에는 중첩되는 감독 메커니즘이 네 가지가 있는데, CSIS의 운영 정책 준수를 감시하는 감찰관, CSIS 활동을 심의하고 기관에 대한 민원을 조사하는 보안정보심의위원회(도구 2 참조), 특별 조사 수단 사용을 허가할 권한이 있는 유일한 기구인 캐나다 연방 법원,[5] 그리고 공공안전부 장관의 연례 국가 안보 보고서(Annual Statement on National Security)와 CSIS 공공 보고서(Public Report) 형식의 공개 보고가 그것이다.[6]

COPASIR 같은 의회 감독 위원회의 위임 사항에는 지원 부서 및 관료를 포함한 국가 정보 공동체 전체가 망라되어야 한다.[7] 위임 사항은 정보기관의 합법성, 효능, 효율성 및 예산 회계 관행, 인권 기준의 준수, 기타 정책/행정 측면을 감시하는 데 필요한 모든 권한을 위원회에 부여해야 한다. 그렇지 못한 위임 사항은 개정되어야 한다. 일례로 호주의 경우, 감독 위임 사항의 제한으로 인해 국방화상지형국(DIGO)에 책임을 충분히 물을 수 없다는 것이 특별 조사를 통해 드러나자 호주의 모든 정보기관이 포함되도록 관련 의회 감독 위원회의 위임 사항을 확대할 것을 권고했다. 특별 조사에서는 또

DIGO 감시가 포함되도록 정보보안감찰관의 위임 사항을 확대할 것을 권고했다(도구 1 참조).[8]

3.1 위임 사항의 유형

위임 사항의 범위는 넓을 수도 좁을 수도 있다. 예를 들어 어떤 감독 기구의 위임 사항은 어느 한 정보기관의 활동의 합법성을 검증하는 것뿐일 수도 있다. 또 다른 감독 기구의 위임 사항은 정보관들의 실적과 예산 과정의 운영을 포함하여 여러 기관들의 효과성을 심의하는 것일 수도 있다. 위임 사항이 광범위할수록 단편화되거나 기타 불완전한 감독을 피하는 데 일반적으로 도움이 된다.

감시 시행에 정확히 필요한 정도를 넘는 권한이 감독 위임 사항에 포함되는 경우도 있다. 가령 체포 및 재판 전 구금 권한, 치명적 무기 사용 권한이 포함될 수도 있다. 또한 외국 기관으로의 정보 이전 통제와 행정부의 최고 정보직 임명에 대한 승인도 위임 사항에 포함될 수 있다.[9]

비밀 활동, 특히 개인정보수집을 위해 특별 조사 수단을 이용하는 활동과 관련하여 감독 위임 사항에 예방적 또는 사전적 권한이 포함되는 경우가 있다. 예를 들어 벨기에의 경우, 특별정보법으로 상임정보기관심의위원회(Committee I - 전문가 감독 기구)에 특별 조사 수단의 사용에 관해 정보기관에 조언할 권한을 부여하고 있다. 이 조언이 부정적이더라도 기관은 이의를 제기할 수 없다. 나아가 이 위원회는 특별 조사 수단 사용을 감시하는 과정에서 불법적 관행을 확인할 경우, 이를 중단시킬 수 있다.[10]

감독 위임 사항에 예산 심사도 포함될 수 있다. 예컨대 영국의 경우, 정보기관은 감사원의 회계 감사를 받고, 의회 정보보안위원회의 회계 심사도 받는데, 이 위원회의 연례 보고서는 정보기관 자금과 지출의 세부 내역 중 일부를 공개한다.[11] 마찬가지로 남아공 정보합동위원회는 남아공 정보기관들의 재정 관리를 심사하며,[12] 폴란드에서는 의회 감독 위원회가 정보기관 예산 초안을 심사하고 그 집행을 감시한다. 감독 기구의 위임 사항에 예산 통제까지

포함시키는 국가들도 있다. 예를 들어 아르헨티나의 양원 합동 정보 기구 활동 감독 위원회(Bicameral Committee for the Oversight of Intelligence Bodies and Activities)와 미국의 의회 정보 위원회가 이런 권한을 가지고 있다.

3.2 위임 사항의 변경

정보기관 감독 기구의 위임 사항이 고정불변이어야 할 이유는 없다. 가령 정보기관의 위임 사항이 확대되면 그 활동을 감독하는 기구의 위임 사항도 개정되어야 한다.[13]

정치적으로 중대한 악영향을 미치는 전략적 사건도 정보기관 감독 기구 위임 사항의 변화를 초래할 수 있는데, 정보 실패와 관련된 사건의 경우가 특히 그렇다. 예를 들어 미국의 정보 공동체가 911 공격을 탐지, 예방하지 못하면서 정보공유 메커니즘에 대한 재검토가 이루어졌다. 이러한 메커니즘의 변화는 감독 기구의 업무에 영향을 미쳤고 위임 사항 변경 또한 필요하게 만들었다.

때로는 감독 기구가 업무 과정에서 위임 사항에 필요한 변경 사항을 스스로 파악하기도 한다. 이런 이유로 일부 감독 기구는 이러한 변경 필요성을 파악하고 권고하기 위해 정기적인 전략 검토를 수행한다. 이를 통해 감독 기구들은 결함에서 정보 부문 개선을 위한 긍정적이고 건설적인 제안으로 변모시킬 수 있다.

4. 감독 권한

정보 감독 기구에 부여되는 권한은 천차만별이다. 아래 설명된 것은 가장 일반적인 경우이다. 예를 들어 일부 위임 사항에는 감독 기구가 알아낸 위법 행위를 징계를 위해 (감찰관 같은) 내부 기구에, 또는 형사 기소를 위해 외부 기구에 이첩할 수 있는 이첩 권한이 포함된다. 폭로 권한(power of exposure)은 감독 기구가 규정 불이행, 판단 착오 또는 법률 위반을 감찰관에게 보고하는 것을 넘어 미국의 법무장관 같은 해당 국가의 최고 당국자에

게 폭로할 수 있는 권한이다.

4.1 정보 권한

감독 기구가 정보에 접근할 수 있는 정보 권한은 수동적일 수도 능동적일 수도 있다. 수동적 정보 권한을 가진 감독 기구는 정보기관 활동에 관한 정보를 문서 형식 및 브리핑을 통해 받는다. 이러한 브리핑의 내용이 최신이고 종합적이면 좋겠지만 시행 법률에 따라 예산 문제와 비밀 업무 같은 고도로 민감한 정보가 포함되지 않을 수도 있다.

수동적 정보 권한만 가진 감독 기구가 받는 정보의 폭과 정확성은 감독 대상 정보기관에 전적으로 의존한다. 이런 이유로 감독 기구는 수동적 정보 권한과 능동적 정보 권한을 모두 갖는 것이 바람직하다. 능동적 정보 권한이 있는 감독 기구는 가령 관리들에게 정보 제공을 강제하거나 기관 부지를 예고 없이 방문하는 등의 방법으로 필요한 정보를 찾을 권한이 있다.

감독 기구가 의무를 이행하기 위해서는 필요한 모든 정보에 제약 없이 접근할 수 있어야 하지만 늘 그렇지는 못하다. 예를 들어 대부분의 감독 기구는 기밀 정보에 접근할 수 있지만 그렇지 못한 감독 기구도 있다. 반면에 정보원의 신원 보호처럼 일부 정보 접근 제한은 합리적일 수 있다. 이러한 제한은 예컨대 남아공 합동상임정보위원회가 이러한 정보에 접근할 때 적용된다. 아르헨티나, 캐나다, 미국의 일부 감독 기구는 정보 접근에 제한이 없다.

4.2 조사 권한

정보기관 감독 기구들에게는 제공되는 정보를 단순히 조사할 수 있는 능력을 넘어 조사에 착수할 수 있는 권한이 필요하다. 네덜란드 정보보안기관심의위원회(CTIVD)를 예로 들면 정보기관에 대해 접수된 민원을 근거로 조사에 착수할 수 있는 권한을 지니고 있다. 다른 감독 기구들의 위임 사항에서는 민원 접수 없이도 자체 조사에 착수할 권한을 감독 기구에 부여한다. 구체적인 조사 권한에는 관리들이 감독 기구에 출석해 답변하도록 요청 및 (또는) 강제할 수 있는 권한이 포함된다.

4.3 승인 권한

일부 위임 사항에서는 감독 기구에 전략적 정보 프로그램, 기관 예산 및 (또는) 최고위직 임명을 승인하거나 인가할 권한을 부여한다. 이런 승인 권한을 하나 이상 보유한 감독 기구는 이를 활용해 감독 대상 기관, 특히 정보기관의 우선순위 설정에 유의미한 영향력을 행사할 수 있다. 예를 들어 미국의 의회 정보 위원회가 행사하는 "재정권(power of the purse)"은 위원회가 자금 배정을 통해 정보 및 정책 우선순위를 시사할 수 있기 때문에 강력한 감독 및 통제 도구로 간주된다.

5. 감독 방법

감독 기구의 위임 사항은 권한뿐 아니라 조사 수행에 사용할 수 있는 방법도 규정해야 한다. 가장 흔히 사용되는 것은 점검, 청문회, 문서 분석이다. 그 밖의 방법에는 면담, 증인 진술, 데이터베이스 직접 접근이 포함된다(마지막 방법은 벨기에와 네덜란드 관리들이 주요 감독 방법으로 여기는 것이다). 이 모든 방법은 감독 목표 추진을 위해 개별적으로, 병행하여, 순차적으로 사용된다.

5.1 점검

일부 감독 기구는 감독 대상 기관의 부지를 정기적으로 점검한다. 이런 방문은 매년, 분기별 또는 심지어 월별로 이루어질 수 있다. 감독 기구가 예정된 방문을 정보기관에 통보하는 경우가 대부분이지만 많은 감독 기구가 불시 점검 권한도 가지고 있다. 방문 시 감독 기구 구성원들은 직원들을 면담하거나 무작위 추출 같은 방법을 이용해 컴퓨터 데이터베이스를 검사할 수 있다. 노르웨이의 경우, 의회 정보기관 감독 위원회(EOS 위원회라고 한다)가 매년 여러 차례 점검을 시행하며, 네덜란드의 CTIVD의 위임 사항도 이와 비슷하다. 뉴질랜드의 정보보안감찰관은 기관 부지 출입 권한을 가지고 있지만 기관장에게 사전 통지가 된 경우에 한한다.[14]

5.2 청문회

청문회는 감독 기구가 정보 관료, 독립적 전문가, 기타 청문회 출석인들로부터 정보를 얻는 일반적 방법이다. 비록 힘이 많이 들고 민감하기는 하지만 청문회는 문서 기록상 취약하거나 모호한 서술을 재구성하는 데 필수적일 수 있다. 청문회는 또 정보기관과 그 관리들이 내리거나 시행한 결정에 대한 정치적 및 (또는) 행정적 책임을 밝히는 데도 도움이 될 수 있다. 존 칠콧(Sir John Chilcot)이 위원장을 맡아 현재 진행되고 있는 영국의 이라크전 개입에 관한 조사에서 여러 차례 공청회를 개최했고, 모두 실시간으로 방송되었다.[15] 네덜란드의 이라크조사위원회도 비슷한 청문회를 열었지만 공개되지는 않았다.

5.3 문서 분석

감독 기구는 기밀 및 非기밀 보고서와 정보기관이 작성한 기타 문서를 정기적으로 검토한다. 이 문서들은 종종 유용한 정보를 제공하고 일부 질문에 대한 답변을 포함하기도 하지만 동시에 다른 방식의 답변을 요하는, 정보기관 업무와 관련된 다른 질문들을 제기할 수도 있다.

문서 분석이 정보기관이 작성한 문서로 국한될 필요는 없다. 네덜란드의 이라크조사위원회를 예로 들면 도움이 될 수 있는 그 밖의 문서들을 얻기 위해 공개 웹 사이트를 만들었다.

6. 감독 시기

감독은 업무 또는 정책 관련 결정이 내려지기 전이나 시행 도중 혹은 시행 이후에 이루어질 수 있다. 감독 시기는 감독 기구의 위임 사항에 따라 달라진다(도구 1 참조).

6.1 사후 감독

가장 일반적 형식의 감독은 사후 감독이다. 그 기본적 논거는 감독 기구가 정보기관의 관리 결정을 심의해야지 간섭해서는 안 된다는 것이다.[16] 계획 단계이거나 진행 중인 업무에 관한 감독 기구 브리핑이 사후 감독에서 반드시

배제되는 것은 아니지만 감독 기구가 소급적 관점을 취하여 이미 발생한 사건만을 조사한다는 뜻이 강하게 내포되어 있다.

6.2 사전 감독

일부 감독 기구의 위임 사항에는 사전 감독 수행이 포함된다. 사전 감독은 감독 체계의 권한 강화 방법으로 간주된다. 이는 정보기관 활동이 시작되기 이전의 점검 및 (또는) 승인을 의미한다. "정보기관의 정책 또는 업무가 실행되기 전에 감독 기구가 그 정책이나 업무를 금하거나 변경할 수 있도록 하는 위임 사항"으로[17] 정의되는 "사전적 위임 사항"을 이야기할 수도 있다. 많은 감독 기구는 관련 정보기관의 정책과 전략을 조사하는 입장에 있으므로, 특정 정보활동이나 비밀 업무가 시작되기 전에 내부심의 기구에 조사 수행을 요청 또는 지시할 수 있다.

인권과 기본적 자유의 보호 증진 및 테러 방지에 관한 UN 특별 보고관(UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism)은 사전 감독을 권장하는데, 테러와의 싸움 와중의 정보기관에 의한 인권 침해를 예방하는 데 유용하다고 보기 때문이다. 마찬가지로 국내 정보기관과 해외 정보기관 간의 협력 협정도 협정 서명 전에 감독 기구가 사전 검토하는 것이 권장된다(도구 7 참조).[18]

반면 사전 감독을 수행하는 감독 기구들은 경우에 따라 승인해 준 활동으로 인해 발생하는 정보 실패와 법률 위반의 책임을 지게 될 수도 있다. 또 감독 기구가 사전 감독을 할 수 있게 되면 감독 기구에 기밀 정보가 공개되는 것을 꺼리는 해외 협력 기관들과의 관계에 걸림돌이 될 수 있다.[19]

많은 국내 정보기관들이 운영 정보의 사전 공개와 관련하여 비슷한 보안 우려를 갖고 있는데, 사전 공개에 의원들이 관여되는 경우에 특히 그렇다. 이런 이유에서 정보기관 감독 위원회에 참여하는 의원들은 보안 심사를 받아야 하는 경우가 많다. 때로는 이런 예방 조치조차 충분치 않다고 간주된다.

6.3 주기적 감독

감독은 주기적으로 이뤄질 수도 있다. 정보기관 위임 사항에서는 고위 관리직이 행정부나 의회 또는 행정부와 의회 모두에 제출할 기관 활동에 관한 정기(일반적으로 연례) 보고서 작성을 요구하는 경우가 많다. 마찬가지로 감독 기구는 간헐적이 아니라 주기적으로 조사를 시행할 수 있다. 캐나다의 SIRC는 역량이 제한되어 있음을 인정하여 3년에서 5년 주기로 정보기관들에 대한 전면적 감독을 규정한 계획을 채택했다. 호주 정보기관 특별 조사 보고서(위에서 논의)도 이와 유사하게 5-7년마다 정보 공동체를 심사할 것을 권고했다.[20]

7. 감독 조사

감독 조사는 다양한 방법으로 시작할 수 있다. 의원이나 행정부는 공식적으로 이를 요청할 수 있다. 언론도 조사를 촉구할 수 있다. 벨기에와 캐나다 같은 일부 국가에서는 일반 대중이 제기한 민원으로도 조사가 시작된다. 감독 기구들은 자체 조사에 착수할 권한이 있는 경우가 많다. 그러나 대부분의 경우, 특정 사안을 다룰지 말지 여부에 관한 최종 결정권은 감독 기구에 있다.

7.1 특정 사건의 조사

감독 기구는 가령 제소인, 의원 또는 언론이 주장하는 혐의를 근거로 특정 사건에 대한 조사에 착수할 수 있다. 감독 기구는 정보기관과 관련된 특정 사건이나 혐의에 대한 조사를 시행할 수 있으며, 이 조사는 감독 기구가 시작할 수 있다. 정보기관은 관련 절차에 따라 예컨대 불법 행위, 보안 침해 또는 정보 누설과 관련된 심각한 사건에 관한 보고서를 감독 기구에 제공할 수 있다. 이들 보고서는 정기적으로 제출하거나 특별 조사에 제출할 수 있다. 이런 보고서 중 하나가 캐나다 왕립 기마경찰(RCMP)이 마헤르 아라르 관련 조사 위원회(Canadian Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar)를 위해 작성한 보고서다. 이 조사 위원회는 무엇보다도 개인정보를 다른 정보기관과 공유하기 전에 그 관련성과 신뢰성을 심사해야 한다는 RCMP 방침을 RCMP가 어겼기 때문에 설립되었다. 이 위원회의 25개항의 권고 사항 중에는 RCMP가 경찰 기관으로서 그 위임의 범위를 벗어나지 말아야 한다는 충고도 있었다.[21]

7.2 주제별 조사

주제별 조사는 구체적 사건보다는 광범위한 사안에 초점을 맞춘다. 때때로 구체적 사건 조사 결과 더 폭넓은 문제가 밝혀지는 경우에도 이런 조사가 이루어진다.

상자 1: 특별 조사 수단에 대한 네덜란드 의회의 조사: 주제별 감독 사례 연구

1993년에 한 마약 상에 관한 정보수집 업무를 맡은 네덜란드의 지역 간 범죄 수사 팀이 업무 수행을 위해 특별 조사 수단을 사용했다. 이 수단들 중에는 수사를 위해 마약을 시장에 유통시킨 불법 행위가 있었다고 한다. 불법 행위 혐의를 받게 된 이 팀은 해체되었고, 1994년 4월에 네덜란드 의회는 네덜란드 기관들의 특별 조사 수단 사용에 관한 공식 조사에 착수했다.[22]

조사는 문서 분석과 정치인, 정보 전문가가 참여하는 오리엔테이션으로 시작됐다. 또한 조사 위원회는 학계에 2건의 보고서(네덜란드 조직범죄의 성격, 심각성, 규모 평가 보고서와 특별 조사 수단 사용을 규제하는 입법에 대한 국제 비교 연구 보고서) 작성을 의뢰했다.

한편 조사 위원회 직원들(모두 보안 심사를 받았다)은 6개월간의 비공개 청문회를 열었다. 이 청문회의 목적은 네덜란드에서의 특별 조사 수단 사용에 관한 정보와 식견을 모으는 것이었다. 비공개 청문회는 직접 방송된 일련의 공개 청문회의 준비 작업 역할도 했다.

1996년에 종료된 이 조사는 6,700페이지에 달하고 129개 권고 사항이 포함된 꼼꼼한 보고서를 내놓았다. 2년 후 의회는 이들 권고 사항의 이행을 평가하기 위한 새로운 임시 위원회를 만들었다. 새로운 위원회는 경찰과 세관 내 마약 관련 부패 증거 등 새로운 많은 정보를 발굴했다. 이런 정황이 드러나면서 벵크 코르탈스(Benk Korthals) 법무장관은 물러나기 직전까지 갔지만, 의회 논쟁에서 겨우 살아남을 수 있었다.

8. 감독 체계화

가장 효과적인 감독은 체계적 감독이므로 감독 과정을 구별되는 순차적 단계로 나누는 것이 유익하다.

8.1 쟁점의 파악과 선택

정보 업무는 다수의 행위자, 절차, 정책이 관련되는 복잡하고 역동적인 분야다. 이 때문에 다양한 쟁점이 정보기관 감독의 주제가 될 수 있다. 감독 과정을 시작하는 가장 좋은 방법은 가능한 모든 쟁점의 목록을 집대성해 이 목록을 감독 기구의 법적 위임 사항과 비교하는 것이다. 서로 겹치는 분야는 적절한 조사 대상임을 가리킨다.

8.2 기밀 취급 인가 획득

감독 기구 구성원과 직원들이 기밀 정보를 다루려면 기밀 취급 인가를 획득해야 하는 것이 보통이다. 주목할 만한 예외는 의회 감독 위원회 위원들로, 자신들의 사생활을 조사받는 것을 반대하는 경향이 있다. 특히 배경 조사를 하는 정보기관이 역설적으로 감독 위원회가 심사 또는 조사하는 기관과 동일 기관인 경우에 더 그렇다. 그럼에도 불구하고 정치인을 보안 심사에서 배제해야 하는가는 논란이 매우 큰 문제이다.

8.3 감독 기구 사무실 보안

감독 기구의 사무실은 보안이 유지되어야 한다. 예를 들면 정기적으로 전자 감시 장비를 찾아 제거해야 한다. 또한 컴퓨터와 기타 정보 통신 장비는 비밀번호로 보호되고 암호화되어야 한다. 마찬가지로 구내 출입이 가능한 모든 지원 인력(비서, 통역사, 출장 요식업체, 청소부 등)도 보안 확인을 거쳐야 한다.

8.4 문서 및 기타 자료 보안

감독 기구 구성원은 문서와 메모 취급에 엄격해야 한다. 클린 데스크(clean-desk) 정책을 준수해 기밀 정보는 금고에 보관하는 것이 관례화되어야 한다. 종이에 인쇄된 것이든 컴퓨터나 플래시 드라이브에 디지털로 저장된 것이든 기밀문서는 적절한 승인 없이는 절대 사무실 밖으로 반출되어서는

안 된다. 기밀 정보원, 증인 및 기타 핵심 출석인과 관련된 내부 기록은 익명으로 보관해야 한다. 끝으로 이 모든 요건들을 적절한 절차가 규정된 내부 매뉴얼에 명시해야 한다.

8.5 계획 수립

일부 감독 기구는 규정이나 시행 요강 또는 상세한 조사 계획까지 작성해야 하며, 감독 활동 시작 전에 이를 승인받아야 한다. 이렇게 하는 것은 감독 기구와 감독 대상 정보기관의 권리와 권한에 관한 오해를 방지하기 위함이다. 이러한 문서에 최소한으로 포함되는 구체적 사항들로는 조사 대상 단위나 임무의 정체성, 관련된 기술, 조사 대상이 될 파일 등이 있다.

상자 2: 기본적 조사 계획의 요소

- 조사 일자
- 조사의 법적 근거
- 조사의 목적
- 조사의 목표
- 조사를 수행할 감독 인력의 이름
- 조사 대상 기관 단위의 명칭
- 면담 대상 기관 인력의 이름
- 면담 요건
- 조사 대상 문서 목록
- 조사 전 문서 요청
- 자원
- 행정 지원
- 보고 기한[23]

상자 3: 상세 조사 계획을 위한 추가 과제

- 조사 시간표 작성.
- 피조사자 명단 작성.
- 잠재적 피조사자에게 초청장 작성 및 피조사자 증언을 재가할 관리자에게 요청서 작성.
- 외교관 지위(특권 및 면책)를 지닌 피조사자 관리를 위한 시행 요강 개발.
- 시행할 면담의 유형 (기밀, 익명, 기록 등) 결정.
- 면담 시행 요강을 개발하고 다음과 같은 쟁점을 처리: 피조사자에게 질문을 사전에 알려줄 것인가? 피조사자가 면담 도중 문서나 기타 기억 보조 자료를 활용할 수 있도록 할 것인가? 피조사자가 면담 사본을 검토 또는 편집할 권한이 있는가?
- 기밀 출처와 정보 처리를 위한 시행 요강 개발.
- 필기록 및 번역 지원 마련.
- 면담에서 얻은 정보 공개 시행 요강 개발.

감독은 복잡할 수 있기 때문에 감독 기구 구성원들은 아무런 요건이 없더라도 감독 활동 시작 전에 공통적 시나리오를 개발해 합의하는 것이 보통 도움이 된다. 특히 상세한 조사 계획은 관련 이해 관계자들이 감독 과정에 전념할 수 있게 해 준다. 게다가 미리 상세한 절차를 개발해 두면 조사가 시작된 후 감독 기구 구성원들이 내용에 집중하기가 더 쉬워진다.

9. 감독 기구의 전문성과 신뢰성

민주주의 사회에 사는 사람들은 정부 기관들이 국가의 법률을 지키고, 만약 지키지 않을 때는 감독 기구가 그 책임을 물을 것을 기대한다. 정보기관이 가진 특별한 권한(인권을 제한하거나 침해할 수 있는) 때문에 정보기관을 감독하는 기구들에도 그에 상응하는 큰 책임이 따른다. 따라서 업무와 공적 처신에 있어 최고 수준의 감독 전문성을 보여 줄 의무가 있다. 그렇지 않을 경우, 감독 과정의 신뢰성이 훼손되고 대중은 정부 기관에 대한 신뢰를 잃게 될 것이다.

9.1 감독 기구의 독립성

감독 기구의 독립성과 자율성이 법률에 의해 절대적으로 보장되지 않는다면 감독 기구가 전문적이라고 간주될 수 없다. 또한 전문성은 감독 기구가 철저히 비당파적일 것, 다시 말해 정당 정치의 압력, 행정부의 간섭, 언론의 압력으로부터 자유로울 것을 요구한다.

실제로 정치적 압력이나 언론의 압력으로부터 보호하는 최선의 방법은 이에 유념하는 것이다. 이 때문에 감독 인력들은 무엇보다도 정치인이나 언론으로부터 예상치 못한 질문을 받을 경우에 대비하는 언론 대응 훈련을 받으면 도움이 될 때가 많다. 특히 이 점은 이러한 질문에 답하는 과정에서 기밀 정보가 뜻하지 않게 공개되는 경우를 방지할 필요가 있다는 점을 감안할 때 중요하다.

9.2 감독 직원들의 전문성

이상적으로는 감독 기구 구성원과 직원들이 경찰, 군 기관, 외국 및 국내 정보기관 등 다양한 보안 기관과 관련된 사전 지식과 경험을 갖고 있어야 한다. 이런 지식과 경험이 없는 사람들은 최대한 일찍 훈련을 받아야 하며, 관련 규정의 숙지와 정기적인 교육 세미나에 지속적 참석을 요구 또는 장려해야 한다.

9.3 기밀 정보

감독 기구 인력에게 가장 까다로운 전문적 딜레마 중 하나는 어떻게 하면 투명성과 비밀주의라는 서로 경합하는 요구가 가장 잘 균형을 이루게 할 수 있느냐다(도구 3 참조). 일부 기밀 정보는 공개될 경우, 정말로 국가 안보가 위태로워질 수 있기 때문에 각국 정부는 이런 정보를 일반 대중에게 비밀로 할 정당한 권리가 있다. 감독 기구 직원들이 기밀 정보 취급에 앞서 먼저 기밀 취급 인가를 받아야 하는 것도 이 때문이다. 그러나 지나친 비밀주의도 바람직하지 않은데, 특히 정치적으로 곤란해질 행위를 감추기 위해 과도한 기밀 분류가 사용되는 경우가 그렇다(예를 들어 미국에서의 비밀 구금, 취조, 송환 프로그램의 설립). 국가 기밀 보호법의 남용은 정부에 대한 시민들의

신뢰를 잃게 하고, 모든 정부 제도의 정당성을 훼손한다. 뿐만 아니라 과도한 기밀 분류는 효과적 감독을 방해한다. (일부 관할권에서는 특정 문서가 적절하게 기밀로 분류되었는지 심사할 권한을 사법부에 부여하는 법률을 통해 이 문제를 개선하고 있다.)

10. 감독 기구의 처신

감독 기구의 처신도 그 효과성에 상당한 영향을 미칠 수 있다. 감독 기구 스스로가 투명성과 일관성 같은 가치를 받아들이지 않으면서 정보기관들에게 이를 기대하는 것은 정당하지 못하다.

10.1 투명성

감독 기구의 효과성에 가장 좋은 것은 최대의 투명성이다. 특히 감독 기구가 항상 그 행위를 해명할 수 있고 감독 대상 정보기관에게서 기대하는 책임성을 보여 주기 위해서는 합의된 표준과 규칙에 따라 행동하는 것이 필수적이다. 특정 조사를 위해 참조한 정보 출처에 관한 정보와 사용된 권한을 보고서에 포함시키면 감독 기구의 투명성이 보강될 수 있다.

10.2 일관성

충격적 사건이나 스캔들이 일어나면 정보기관 감독이 한바탕 집중적으로 이루어진 후 엄격한 감시가 한동안 이어지는 것이 보통이다. 하지만 문제가 생길 때마다 대응하는 것뿐 아니라 감독이 지속적으로 이루어지는 것이 중요하다. 정보기관 감독 기구는 감시 및 조사 패턴을 개발함으로써 업무의 일관성을 높일 수 있다. 이런 방법은 감독 소홀이나 새로운 감독 공백을 방지하는 데 도움이 되며, 궁극적으로는 정보 실패의 재발 가능성을 줄인다.[24]

10.3 정보기관과의 상호 작용

정보기관이 폐쇄적이고 배타적인 관료 체제로 보일지 몰라도 대부분은 외부의 지적을 받아들여 자신들의 결함을 기꺼이 시정하고자 하는 조직이다. 이런 이유로 감독 기구는 정보기관과 우호적이고 시의적절하며 유용한 상호작용을 하는 것이 좋다. 예를 들어 시정 권고는 정보기관이 자신의 조직에

맞는 구체적인 지침, 시행 요강, 절차, 시간표로 구체화할 수 있도록 제시되어야 한다.

감독 인력이 그들의 조사 결과가 개별 정보관에게 징계, 때에 따라서는 해임 등 나쁜 영향을 미칠 수 있음에 유념하는 것 역시 중요하다. 이런 이유로 감독 기구 구성원들은 조사 결과 보고에 앞서 이런 문제를 해당 정보기관의 고위층과 논의하는 것이 일반적으로 바람직하다.

11. 보고

정보기관 감독 기구가 따르는 보고 절차는 다양하지만 보편적인 의무는 조사 결과를 알리는 것이다. 거의 모든 경우에 감독 기구가 정기 (일반적으로 연례) 보고서를 제출하도록 법률로 규정하고 있다. 이러한 보고서에는 수행된 조사에 대한 설명과, 감독 기구의 위임 사항에 속하는 경우, 예산 분석이 포함되는 것이 보통이다. 보고서에는 정보기관 책임성, 투명성, 합법성, 효과성 개선을 위한 정보기관 및 (또는) 행정부에 대한 권고 사항도 포함될 수 있다.

감독 기구는 연중 내내 특별 보고서도 작성할 수 있다. 이런 보고서는 주제별 보고서이거나 특정 조사를 설명하는 것일 수도 있다. 예를 들어 의심스러운 정보활동을 감독 기구가 인지한 경우, 이 활동을 적절한 때에 관련 당국에 보고해야 하는 것이 일반적이다.

에이던 윌스(Aidan Wills)에 따르면 “감독 기구는 흔히 두 가지 버전의 보고서를 작성한다. 첫 번째 버전은 행정부와 정보기관을 위한 것으로서 기밀 정보가 포함될 수 있으며, 두 번째 버전은 일반 대중을 위한 것으로 기밀 정보가 포함되지 않는 것이 일반적이다. 감독 기구는 공개 보고서 발표 전에 행정부 및 정보기관과 협의한다. 이 협의는 보고서에 민감한 정보가 포함되는 문제에 관한 정보기관의 우려를 전달할 기회가 된다.”[25]

11.1 보고서 제출

제출 절차는 나라마다 다르다. 벨기에의 경우, Committee I이 상하 양원 의

장과 주무장관에게 연례 보고서를 보낸다. 하지만 특별 보고서는 먼저 주무장관에게 제출되고 난 후에야 상원 의장에게 보낸다.[26] 또 의회에 제출되는 보고서에는 기밀 정보가 포함되지 않는다. 보고 규정이 다른 캐나다에서는 SIRC가 행정부에 연례 보고서를 보내면 행정부는 15일 이내에 의회에 보고서를 송부해야 한다. SIRC는 또 법률에 의해 보고서 공개 전에 CSIS 국장과 협의하도록 되어 있다.

11.2 보고서 소유권

감독 기구는 보고서 내용과 시기를 포함해 보고서의 완전한 소유권을 가져야 한다. 경우에 따라서는 절차법이나 규칙에서 기밀 정보의 특별 취급이나 보고서 공개 유예 기간을 정할 수 있다. 네덜란드의 CTIVD는 주무 장관에게 6주의 시간을 준다. 이 6주 이내에 주무장관의 공식적 답변서가 제출되지 않으면 CTIVD의 기본 보고서가 공개된다.

11.3 정치적 고려 사항

정치적 합법성의 경계선에서 이루어지는 정보활동은 큰 논란거리가 될 수 있다. 외국 관할 내에서의 정보수집, 개인 인권을 침해하는 특별 조사 수단의 이용 등이 그 예다. 따라서 감독 기구의 조사는 종종 조사 결과를 자신들에게 정치적으로 유리하게 이용하려 드는 열성 당원들을 끌어들인다. 이런 압력에 대처하는 가장 좋은 방법은 이를 예측하는 것이다. 예를 들어 정치 일정과 그것이 언론의 관심에 미치는 영향에 유의하라. 보고서 이후 따라올 법한 정치적 결과를 잘 생각해 보면 어떻게 대비해야 하는지도 알 수 있다. 반면 보고서 공개를 조율하는 데 지나치게 신경을 쓰면 감독 기구가 독립적이고 객관적이기보다는 정치적으로 공모하는 것처럼 비치게 된다.

11.4 보고서 이행

보고서 자체는 끝이 아니다. 보고서의 목표는 의회와 정부 및 더 넓은 영역 내에서 보고서에 제시된 문제에 관한 토론을 불러일으키는 것이다. 이렇게 할 때에만 보고서의 내용을 권고 사항 이행으로 연결시킬 수 있다.

특정 사건 관련 보고서이건 정기 보고서이건 모든 감독 보고서는 결론과 시정 권고 사항을 분명히 나열해야 한다. 결론과 권고 사항은 표현이 정확해야 하며, 번호가 매겨져야 한다. 또한 감독 기구는 보고서를 관련 당국에 제출한 후 이들 당국과 협력하여 이행 일정을 수립해야 한다. 그 후 감독 기구는 각각의 정보기관이 권고 사항을 얼마나 이행했는지에 관한 후속 보고서를 작성해 제출해야 한다.

11.5 보고서의 접근성

이제는 감독 기구도 인터넷 같은 현대 기술을 이용해 광범위한 일반 대중에게 보고서를 공개한다. 영국의 이라크전 조사 위원회(칠콧 위원회)는 최종 보고서 발간을 앞두고 그 준비 작업으로 이미 필기록, 증인 진술 및 기타 기밀 분류되지 않은 문서를 위원회 웹사이트에 공개했다.

감독 기구의 보고서는 내각이나 의회 웹사이트처럼 감독 기구가 통제하지 않는 웹사이트에 게시될 수 있다. 일반 대중이 보고서를 볼 수 있도록 감독 기구는 보고서 삭제 결정이 이루어질 때마다 사전에 통보해 줄 것을 주장해야 한다. 그러므로 감독 기구에 보고서 및 기타 문서에 쉽게 접근할 수 있는 항구적인 공개 웹사이트가 있는 것이 바람직하다.

12. 잠재적 조사 결과

정보기관 감독 기구가 심의하는 다양한 사안 중에는 (기관의 법률 체계와 같은) 일반적인 사안도 있고 (특정 사건에 대한 조사 같은) 구체적인 사안도 있다. 다음은 감독 기구 조사에서 나올 수 있는 세 가지 잠재적 조사 결과의 예다. 각 조사 결과마다 그 이후 따라올 수 있는 개선 권고 사항을 논의한다.

12.1 정보기관이 외국 협력 기관이 제공한 정보를 검증하지 않은 경우

정보기관들은 특히 외국 협력 기관과 협업 시 외부 출처로부터 받은 정보를 적절히 검증하지 못할 수 있다. 가령 네덜란드에서는 2009년에 CTIVD가 일반정보보안국(GISS)의 외국 정보사용에 관해 조사한 결과, GISS가 법률에서 요구하는, 외국 정보기관이 협력 상대로 적절한지 여부에 관한 판단을 종종

그르쳤음을 발견했다. CTIVD 최종 보고서에 따르면 "체계적인 의사 결정 과정을 발견할 수 없었다." 보고서는 계속해서 그보다는 "결정이 종종 임시방편 식으로 이루어졌다"고 지적하면서, 이를 "지나치게 제한적"이고 "바람직하지 않은" 것으로 비판했다. 이에 따라 CTIVD는 GISS에게 협력 관계를 체결할 때는 물론 기존에 구축되어 있는 관계와 관련해서도 철저한 평가에 착수할 것을 권고했다.[27]

제공된 정보에 기초해 행동하기 전에 이러한 평가를 하는 것은 제공된 정보가 고문을 통해 획득됐을 가능성이 있는 경우에 특히 중요하다. 이런 이유로 캐나다의 마헤르 아라르 관련 조사 위원회는 모든 연락 협정(liaison agreement)이 감독 기구의 정기적 조사를 거치도록 권고했다.[28] UN 특별 보고관도 비슷한 취지로 각국이 정보공유 협정에 이러한 협정의 적용이 각국 심의 기구의 조사를 받도록 하고 이 심의 기구들이 양측 또는 어느 한쪽의 성과를 평가할 때 서로 협력할 자격이 있음을 선언하는 조항을 포함시킬 것을 권고했다.[29] (정보공유에 관한 자세한 논의는 도구 7 참조).

12.2 정보기관의 행위가 위임 사항의 한계를 벗어난 경우

감독 기구는 정보기관의 행위가, 특히 특별 권한을 이용한 정보수집과 관련하여 그 위임 사항의 한계를 벗어나는지 여부를 정기적으로 검토해야 한다 (도구 5 참조). 정보기관이 정말로 권한의 법정 한도를 준수하지 않은 경우에는 감독 기구가 기관에 책임을 물어야 한다. 이는 관련 당국에 위반을 보고하고, 감독 기관 자체 위임 사항에 속하는 경우에는 정보기관이 사용하는 하나 이상의 특별 권한을 해제함으로써 달성할 수 있다.

아라르 위원회는 RCMP가 위임 사항의 한계를 벗어났음을 밝힌 후에 차후 RCMP가 캐나다 정보 공동체 내에서의 CSIS의 분명한 역할을 존중할 것을 권고했다.[30]

12.3 정보가 정치화된 경우

정보가 정치화되는 방식은 여러 가지가 있고, 정보를 생산하는 정보기관과

무관하게 정치화되기도 한다. 하지만 가장 흔하게는 행정부와 지나치게 친밀한 관계에 있는 정보 관료가 유력한 행정부 직위를 지원하기 위해 의식적으로나 무의식적으로 정보를 가공할 때 정치화가 이루어진다("고위직 영합 정보[intelligence to please])." 연관된 정치화 형태로는 정부 관료가 정적에게 피해를 입힐 수 있는 정보를 획득하기 위해 정보기관을 이용하는 것도 포함된다. 정보기관 내에서 출세를 목적으로 즉각 사용 가능한 정보를 생산하려 경쟁하는 라이벌 분석가들로 인해 정치화가 발생할 수도 있다.

정치 정보화의 증거를 발견한 감독 기구는 의회에서 대외 정책과 국방 정책의 적절한 목표에 관해 공개적으로 토론할 것을 권고해야 한다. 또 차후에 정보를 정치 도구로 이용하는 것을 방지하기 위해 어떤 안전장치를 도입할 수 있는지도 검토해야 한다.[31]

13. 권고 사항

- 정보기관 감독 기구의 위임 사항은 공식적이고 상세하게, 가능하다면 모든 정보기관에 대한 감독을 다루는 포괄적인 법률 체계의 일부로 규정되어야 한다.
- 정보기관의 위임 사항이 바뀌면 그 감독 기구의 위임 사항도 그에 따라 개정되어야 한다.
- 한 나라의 정보기관 감독 기구들의 위임 사항을 다 합치면 민간 및 군 기관과 지원부서 및 관료를 포함한 전체 정보 공동체가 망라되어야 한다.
- 정보기관 감독 기구 위임 사항에 포함된 접근권, 조사권, 수사권, 승인권은 감독 대상 정보기관의 권한에 상응해야 한다.
- 정보기관 감독 기구는 현장 조사 권한, 공개 및 비공개 청문회를 개최할 권한, 문서, 데이터베이스 및 기타 컴퓨터 파일 내의 기밀 정보에 접근할 권한을 가져야 한다.
- 정보기관 감독 기구는 사후 감독을 실시할 수 있어야 한다. 정보기관 감독 기구가 예외적으로 사전 감독을 수행하는 경우에는 정보원의 신원과 기타 운영 정보를 보호하기 위해 구성원들이 보안 기관의 심사

를 받아야 한다.

- 감독 업무를 체계화하고 관련 이해 관계자들의 동참을 장려하기 위해 정보기관 감독 기구는 항상 감독 계획을 수립해야 한다.
- 정보기관 감독 기구는 수준 높은 전문성을 유지해야 한다. 이는 감독 기구의 정당성뿐 아니라 간접적으로 감독 대상 정보기관의 정당성도 강화한다.
- 정보기관 감독 기구는 투명하고 일관되며 책임성 있는 처신을 해야 한다.
- 정보기관 감독 기구는 그 활동과 감독 결과를 설명하는 주기적 (연례) 보고서를 발간해야 한다. 또 적절한 경우, 특정 조사를 설명하는 사건 보고서도 발간해야 한다.
- 정보기관 감독 기구의 보고서는 일반 대중이 접근할 수 있어야 한다.
- 정보기관 감독 기구는 조사 결과 초안을 정보기관 고위층에 제출하여 법적으로 규정된 기간 내에 그에 대한 답변을 받아야 한다.
- 정보기관 감독 기구의 보고서에는 관련 정보기관들이 이행할 수 있는 권고 사항이 항상 포함되어야 한다.
- 정보기관 감독 기구는 권고 사항 이행을 적극적으로 감시하고 후속 보고서를 펴내야 한다.

후주(後註)

1. Marina Caparini, “Controlling and Overseeing Intelligence Services in Democratic States,” in *Democratic Control of Intelligence Services: Containing Rogue Elephants,* eds. Hans Born and Marina Caparini (Aldershot, UK: Ashgate, 2007), p. 12.

2. Committee on Foreign Affairs, 26 September 2003, 03-BuZa-61.

3. 정보기관들은 사회적 정당성을 위해 공익에 부합하게 행동해야 한다. 특히 정보기관은 근거 없고 지나치며 불법적인 방식으로 시민 개인의 프라이버시를 침해하는 것을 지양해야 한다.

4. Tommaso F. Giupponi and Federico Fabbrini, “Intelligence agencies and the State secret privilege: the Italian experience,” *International Constitutional Law Journal* Vol. 4, No. 3 (Fall 2010), pp. 443‑466 (available at http://www.internationalconstitutionallaw.net/download/53c4319b67f44d52a392c655f17245a3/Giupponi_ Fabbrini.pdf; accessed 19 July 2011).

5. 특별 조사 수단에는 통신 감청, 정보원 및 잠입 요원 운영, 위장 구축이 포함된다

6. Canadian Security Intelligence Service web site, “Accountability and Review” (available at http://www.csis-scrs.gc.ca/bts/ccntblt-eng.asp; accessed 17 August 2011).

7. 일반적으로는 한 나라의 전체 정보 공동체가 적어도 하나의 의회 위원회의 감독을 받는 것이 권장된다.

8. Australian Department of the Prime Minister and Cabinet web site, *Report of the Inquiry into Australian Intelligence Agencies, Chapter4* (available at http://www.dpmc.gov.au/publications/intelligence_inquiry/chapter4/oversight.htm; accessed 17 August 2011).

9. Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Quarterly Journal* Vol. 3, No. 4 (December 2004), p. 6 (available at http://www.pfpconsortium.org/file/1645/view; accessed 19 July 2011).

10. Guy Rapaille, "Le Comité permanent R dans un rôle d'organe juridictionnel: Le nouveau rôle du Comité belge dans le cadre du contrôle des methods particulières de recueil de données" (speech at the 6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States, Brussels, 30 September - 1 October 2010) (available at http://www.parlement-eu2010.be/pdf/30sep-1okt-Thema0-Guy-Rapaille.pdf; accessed 18 July 2011).

11. 예로서 United Kingdom, Intelligence and Security Committee, *Annual Report 2010 - 2011,* Cm 8114 (2011) (available at http://www.cabinetoffice.gov.uk/sites/default/files/resources/isc-annualreport1011.pdf; accessed 13 October 2011) 참조.

12. Sandy Africa, "The South African Intelligence Services: A Historical Perspective," *in Changing Intelligence Dynamics in Africa,* eds. S. Africa and J. Kwadjo (Birmingham, UK: Global Facilitation Network for Security Sector Reform/African Security Network, 2009), pp. 61 - 94.

13.이에 관한 논의는 Paul Robinson, *Eyes on the Spies: Reforming Intelligence Oversight in Canada,* Centre for International Policy Studies (CIPS) Policy Brief No. 1 (Ottawa: CIPS, University of Ottawa, November 2008) (available at http://www.sciencessociales.uottawa.ca/cepi-cips/eng/documents/CIPS_PolicyBrief_Robinson_Nov2008. pdf; accessed 17 August 2011) 참조.

14.Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), p. 351 (available at http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf; accessed 17 August 2011).

15.Iraq Inquiry web site, "About the Inquiry" (available at http://www.iraqinquiry.org.uk/about.aspx; accessed 18 August 2011).

16.이 방식을 취하는 노르웨이의 정보기관 감독 체계에 관한 논의는 Trygve Harvold, "Norwegian Parliamentary Oversight: an 'effective remedy'?" (speech at the 6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States, Brussels, 30 September‐1 October 2010) (available at http://www.parlement-eu2010.be/pdf/30sep-1okt-Thema1-Trygve%20Harvold.pdf; accessed 18 July 2011) 참조.

17.Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Quarterly Journal* Vol. 3, No. 4 (December 2004), p. 9 (available at http://www.pfpconsortium.org/file/1645/view; accessed 19 July 2011).

18. United Nations Human Rights Council, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, United Nations Document A/HRC/10/3 (4 February 2009), p. 24 (available at http://www.unhcr.org/refworld/pdfid/49b138c32.pdf; accessed 18 August 2011).

19. Hans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Quarterly Journal* Vol. 3, No. 4 (December 2004), p. 3 (available at http://www.pfpconsortium.org/file/1645/view; accessed 19 July 2011).

20. Australian Department of the Prime Minister and Cabinet web site, *Report of the Inquiry into Australian Intelligence Agencies*, Chapter 8, Recommendation 22 (available at http://www.dpmc.gov.au/publications/intelligence_inquiry/chapter8/1_findings.htm; accessed 17 August 2011).

21. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), Chapter 9 (available at http://www.sirc-csars.gc.ca/pdfs/cm_arar_rec-eng.pdf; accessed 19 October 2011).

22. 이 조사에 관한 논의는 Parlement & Politiek web site, "Parlementaire enquête opsporingsmethoden, IRT (1994-1996)" (available at http://www.parlement.com/9291000/modulesf/g8pdkcx4; accessed 19 July 2011) 참조.

23.이 요약은 United States Army Inspector General School, *Intelligence Oversight Guide* (February 2008), Appendix D (available at http://www.fas.org/irp/doddir/army/ioguide.pdf; accessed 15 July 2011)에 제시된 견본 계획에서 발췌한 것이다.

24.Loch K. Johnson, *Secret Spy Agencies and a Shock Theory of Accountability,* Department of International Affairs Occasional Papers (University of Georgia, School of International and Public Affairs, 2006) p. 2.

25.Aidan Wills, Guidebook: *Understanding Intelligence Oversight,* Toolkit－Legislating for the Security Sector (Geneva: DCAF, 2010), p. 40.

26.Ibid., p. 37.

27.Bert van Delden, "Partners in Business?" (speech at the 6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States, Brussels, 30 September－1 October 2010), p. 4 (available at http://www.parlement-eu2010.be/pdf/30sep-1okt-Thema3-Bert%20Van%20 Delden.pdf; accessed 18 July 2011).

28.Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006) (available at http://www.Sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf; accessed 17 August 2011).

29.United Nations Human Rights Council, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including*

the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, United Nations Document A/HRC/10/3 (4 February 2009), p. 21 (available at http://www.unhcr.org/refworld/pdfid/49b138c32.pdf; accessed 18 August 2011). In reference to C. Forcese, *The Collateral Casualties of Collaboration: the Consequence for Civil and Human Rights of Transnational Intelligence Sharing* (conference paper for the DCAF workshop on accountability of international intelligence cooperation, Oslo, 17 October 2008).

30. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), p. 312 (available at http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf; accessed 17 August 2011).

31. 자세한 논의는 Monica den Boer, "Keeping 'Spies & Spooks' on the Right Track: Ethics in the Post 9/11 Intelligence Era," in *Ethics and Security,* eds. Monica den Boer and Emile Kolthoff (The Hague: Eleven, 2010), pp. 57 - 83 참조.

도구 5

정보수집 감독

로렌 허튼(Lauren Hutton)

5. 정보수집 감독

로렌 허튼(Lauren Hutton)

1. 머리말

이 도구의 목적은 정보기관의 정보수집 기능을 감시하는 데 있어서 감독 기구가 하는 역할을 살펴보는 것이다. 정보 생산은 여러 단계에 걸친 과정으로서 과제 선정, 계획, 정보수집, 분석, 유포가 필요하다. 하지만 이 모든 단계 중 적어도 일반 대중이 생각하기에 여전히 정보기관의 특징을 규정하는 것은, 특히 비밀스러운 수단을 통한 정보의 수집이다. 정보수집은 정보 업무에서 가장 논란이 되는 측면 중 하나이며, 민주적 이상을 옹호할 책임이 있는 감독 기구에게는 이례적인 어려움을 안긴다.

이 도구의 첫 부분에서는 정보기관들이 정보를 수집하는 몇 가지 방법을 살펴본다. 그런 다음 민주국가에서 비밀스러운 방법이 사용될 때에도 항상 인권이 존중되게끔 입법, 승인, 감독을 활용할 수 있는 방법을 살펴본다.

2. 정보수집 출처 및 방법

첩보의 기초는 다양한 출처에서 수집한 정보이다. 어떤 특정 사안을 완전히 이해하기에 충분한 정보를 어느 하나의 출처에서 제공받기는 어렵기 때문에 정보기관들은 사태의 가장 정확한 진상에 이르기 위해 복수의 출처를 이용한다. 이들 출처는 보통 유형별로 분류할 수 있다.

- 정보원 등의 인간 정보(HUMINT)
- 통신 감청 등 신호 정보 (SIGINT)
- 언론 보도 등 공개 출처 정보 (OSINT)
- 위성사진 등 화상 정보 (IMINT)

정보수집 방법은 공개적일 수도 비밀스러울 수도 있다. 공개적 방법은 OSINT 수집에 가장 흔히 사용되는데, 이 정보는 공개되어 있어 입수 가능하

기 때문이다. 비밀스럽거나 은밀한 정보수집 방법은 비밀성을 이용해 대상 몰래 대상에 관한 정보를 수집한다. 비밀스러운 방법에는 정보원, 전자적 감시, 통신 감청, 물리적 감시, 원격 수집 화상의 사용이 포함될 수 있다. 이런 방법을 개인의 프라이버시권을 침해하는 방식으로 사용하는 경우, "침해적 조사 방법"이라고 한다. 이런 기법 자체는 "특별 조사 수단" 또는 "특별 조사 기법"이라고 부른다.

유럽 회의는 특별 조사 기법이 "중대 범죄와 용의자의 탐지 및 조사를 목적으로 범죄 수사의 맥락에서 관계 당국이 대상 몰래 정보를 모으기 위해 활용하는 기법"을[1] 의미한다고 정의했다. 이 맥락에서 관계 당국은 정보기관이나 법 집행 기관을 의미할 수 있다. 중요한 것은 많은 나라의 정보기관들이 범죄 수사뿐 아니라 예방적 차원의 국가 안보 조사의 맥락에서도 이러한 수단을 사용한다는 점이다. 일반적으로 정보수집에 사용되는 방법은 필요한 정보의 유형, 정보수집의 목적과 정보기관이 운용되는 운영적, 법적, 정치적 맥락에 기초해야 한다.

3. 정보수집이 인권에 미치는 영향

정보기관들은 행정부 관리들의 정책 수립 및 전략적, 운영적 결정을 돕기 위해 정보를 수집한다. 정보기관의 정보수집 방법은 정보기관이 봉사하는 사회의 우선순위 및 가치관에 부합해야 한다.[2] 민주주의 국가에서 정보기관들은 인권, 법규 및 책임성, 투명성, 참여적 의사 결정 등의 민주적 거버넌스의 원칙을 존중해야 한다. 과제 선정부터 유포에까지 이르는 정보 과정은 이러한 한계 내에서 운영되어야 한다.

안보 위협에 관한 정보수집은 개인의 기본권에 직접적 영향을 줄 수 있다.[3] 남아공 국가정보국의 권한 남용 혐의를 조사한 남아공 장관정보심의원회의 2008년 보고서에 따르면 "침해적 조사 방법은 범죄 행위와 음모를 적발하는 데 결정적 역할을 할 수 있지만 오용될 경우에는 민주적 과정을 전복시키고, 합법적인 정치적, 사회적 활동을 방해하며, 일부 정치인과 정당에게 부당 이득을 줄 수 있다."[4]

국가의 침해적 방법 사용도 늘 헌법적, 정치적으로 민감한 문제지만 정보기관이 사용할 경우에는 특별히 주의해 다뤄야 한다. 그 이유는 장관심의위원회 보고서[5] 에 열거되어 있으며 다음을 포함한다.

- 조사 대상자가 침해적 방법의 사용에 관해 전혀 모를 수 있으므로 법정에서 그 효력에 이의를 제기하거나 다툴 수 없을지 모른다.
- 침해적 방법이 고도로 비밀스럽게 사용되므로 감독 기구가 그 사용을 감시하고 발생 가능한 남용과 불법성을 탐지할 능력이 줄어든다.
- 침해적 방법은 필요하거나 의도한 정도보다 개인의 프라이버시권을 훨씬 더 크게 침해할 수 있다.
- 침해적 방법은 대상자의 프라이버시를 침해하는 것을 넘어 대상자와 접촉하는 개인들(이들은 조사 대상자가 아님에도 불구하고)의 프라이버시권을 침해할 때가 많다.
- 대상자 및 대상자와 접촉하는 사람들에 관한 민감한 정보를 조사 기간이 지난 후에도 정보기관이 기록, 유지하고, 때로는 다른 목적에 사용하기도 한다.

감청 기술의 경우, 국내사용과 국외사용을 구분할 때가 있는데, 국내에서는 행정부가 정적 감시 등의 당파적 목적으로 비밀 감청 시스템을 사용할 위험이 있기 때문이다. 반면 외국 통신의 감청은 일반적으로 국내의 민주적 질서를 위태롭게 하지 않는다.

민주국가에서 정보기관 감독 기구는 정보기관들이 헌법 질서에 부합하게 행동하도록 할 정당한 권리를 가지고 있으며, 이를 법적 책임으로 못 박은 경우도 많다. 감독 기구들의 책임 범위는 일반적으로 정보 과정 전체에 미치지만 정보수집 분야는 비밀스럽고 침해적인 방법이 민주적 가치에 가하는 위험 때문에 특별한 주의가 필요하다. 구체적으로 감독 기구들은 정보기관이 법률의 한계 내에서 행동하도록 하기 위해 이러한 방법의 사용을 면밀히 감시해야 한다.

3.1 프라이버시권의 보호

정보기관에 의해 가장 자주 제한되거나 침해되는 권리는 프라이버시권이다. 따라서 정보기관 감독 기구의 중요한 기능은 정보기관이 정보수집시 프라이버시권에 관한 국내법과 국제법을 준수하도록 하는 것이다.

인권과 기본적 자유의 보호 증진 및 테러 방지에 관한 UN 특별 보고관은 프라이버시권을 "개인들이 자율적인 발전, 상호 작용, 자유의 영역, 즉 타인과의 상호 작용이 있건 없건 국가의 개입으로부터 자유로우며 초대받지 않은 다른 개인들에 의한 청하지 않은 과도한 개입으로부터 자유로운 '사적 영역(private sphere)'을 가져야 한다는 추정"으로[6] 정의했다.

비슷한 취지로 시민적·정치적 권리에 관한 국제 규약17조는 다음과 같이 명시하고 있다.

1. *누구도 사생활, 가족, 가정 또는 서신 교환에 대한 자의적이거나 불법적인 방해 또는 그 명예와 평판에 대한 불법적 공격을 받아서는 아니 된다.*
2. *모든 이에게는 이러한 방해나 공격으로부터 법의 보호를 받을 권리가 있다.*

167개국이 조인한 시민적·정치적 권리에 관한 국제 규약은 프라이버시권의 국제법상 근거를 형성한다. 이 규약이 프라이버시를 기본적 인권으로 옹호하고 있기 때문에 이 권리를 제한하는 정부의 행위는 구체적이고 정당한 목적을 위한 것으로 국법에 의해 승인되어야 한다.

유럽인권재판소가 밝힌 것처럼 국가 안보 보호는 프라이버시권 등의 인권을 제한할 수 있는 정당한 목표이다. 그러나 이 재판소에 따르면 이러한 일체의 제한은 국내법에 따라 부과되어야 하며, 그럼에도 불구하고 제한의 남용이 이뤄지는 경우에 대비한 방지책과 구제책이 법에 포함되어야 한다.[7]

정보기관의 비밀스럽고 침해적인 정보수집 방법의 사용은 프라이버시권의 제한에 해당한다. 따라서 이러한 모든 사용은 국내법의 승인을 받아야 하며,

구체적이고 정당한 목적을 위해서만 사용되어야 한다. 남아공의 전직 정보기관 감찰관은 이 원칙을 다음과 같이 해석했다.

> *권리의 제한은 국가 안보에 대한 위협을 근거로 정당화될 수 있다. 이러한 제한은 권리의 본질과 제한 목적의 중요성이 포함된 비례의 기준(test of proportionality)을 충족해야 한다. 따라서 정보를 수집할 수 있는 자격은 시민의 헌법적 권리를 보호하며 개방적이고 민주적인 사회를 지탱하는 대등하게 강력한 안전장치와 짝을 이뤄야 한다.*[8]

3.2 기술이 정보수집에 미치는 영향

현대 정보 통신 기술을 통해 전 세계의 개인들은 즉각 서로 통신할 수 있으며, 정보는 순식간에 엄청난 거리를 이동할 수 있다. 그러나 동시에 각국 정부는 이 기술을 이용해 전례 없는 정도의 감시를 수행할 수 있게 된다. 정보기관들은 첨단 기술 장치를 이용하여 대규모로 정보를 수집할 수 있고 자신들이 받아들이고 분석할 수 있는 것보다 훨씬 많은 정보를 모을 수 있다. 이 정보수집은 그 본질상 무차별적이므로 인권을 침해할 가능성이 있으며, 프라이버시권을 보호하는 법률 체계 내에서만 시행되어야 한다.

에셜론 감청 시스템(ECHELON Interception System)이 좋은 예다. 미국, 영국, 호주, 캐나다, 뉴질랜드가 집단 안보 협약의 일환으로 공동 운영하는 이 시스템은 궤도 위성과 주고받는 신호를 가로챈다. 2000년에 유럽 의회는 ECHELON 시스템이 유럽연합법 하의 개인의 권리에 미치는 잠재적 영향을 조사하기 위한 임시 위원회를 만들었다. 이 위원회의 최종 보고서는 ECHELON 같은 대규모 감청 시스템은 침해적 방법의 사용에 관한 비례의 원칙을 준수하지 않기 때문에 프라이버시권을 침해할 가능성이 있다고 결론내렸다. 위원회는 이러한 감청 시스템이 국가 안보를 근거로 정당화될 수 있음을 인정하면서도 그 사용을 명확하고 이해하기 쉬운 법률로 통제할 것과 EU 회원국들이 엄격한 감독 체제를 구축할 것을 권고했다.[9]

4. 정보수집을 위한 법률 체계

대부분의 민주국가에서 정보기관의 정보수집은 책임성과 투명성을 보장하는

법률 체계에 의해 통제된다. 이는 주로 행정부의 독점적 권한에서 승인 및 감독 책임을 제거하여 이를 (다양한 정도로) 의회, 사법부 및 기타 비행정 조직과 공유함으로써 이루어진다.

국제법은 국내법의 발전에 영향을 미칠 수 있다. 예를 들어 2005년에 유럽회의는 범죄 수사에서의 특별 조사 기법의 사용에 관한 국내법 제정을 위해 다음과 같이 권고했다.[10]

1. *회원국들은 유럽 인권 규약(ETS No. 5)의 요건에 따라 관계 당국이 특별 조사 기법 사용에 의지할 수 있는 상황과 조건을 국가 입법에서 규정해야 한다.*
2. *회원국들은 1항에 따라 관계 당국이 민주적 사회에서 필요하고 효율적인 범죄 수사와 기소에 적합한 것으로 간주되는 범위까지 특별 조사 기법을 사용할 수 있도록 이를 허용하는 적절한 입법 조치를 취해야 한다.*
3. *회원국들은 사법 당국이나 기타 독립적 기구가 사전 승인, 수사 중 감독 또는 사후 심사를 통해 특별 조사 기법의 시행을 적절히 통제할 수 있도록 적절한 입법 조치를 취해야 한다.*

일반적으로 비밀스럽고 침해적인 정보수집 방법에 관한 국가 입법은 다음을 명시해야 한다.

- 언제 그러한 방법을 사용할 수 있는가
- 의심이 어느 정도 확실해야 하는가
- 어떤 제약과 제한이 적용되는가
- 어떤 승인이 필요한가

비밀스럽고 침해적인 정보수집 방법의 국내사용을 규제하는 구체적인 국가 입법의 예에는 호주의 통신감청접근법(Telecommunication Interception and Access Act), 호주의 법집행 통신지원법(Communications Assistance to Law Enforcement Act), 미국의 해외정보감시법(Foreign Intelligence Surveillance Act), 영국의 수사권한규제법(Regulation of Investigatory Powers Act) 등이

있다. 이러한 법은 다음 세 가지 핵심 사안을 다뤄야 한다.

- 허용 가능한 목표
- 비례성
- 승인 및 감독

더 일반적으로 이런 법률에는 비밀스럽고 침해적인 방법을 통해 원하는 정보를 산출할 수 있음을 관계 당국이 합리적으로 확신할 수 있어야 한다는 규정이 있어야 한다.

4.1 허용 가능한 목표

비밀스럽고 침해적인 정보수집 방법의 사용이 허용될 수 있는 목표는 나라마다 상당히 다르다. 일부 국가에서는 유럽 회의의 권고대로 범죄 수사의 수행이 허용 가능한 목표이다.[11] 국가 안보와 민주적 질서의 보호도 허용 가능한 목표인 나라들도 있다. 독일의 서신 교환, 우편, 통신 프라이버시 제한법(Act Restricting the Privacy of Correspondence, Posts, and Telecommunications) 3(1)절은 누군가가 다음에 대한 범죄를 "계획 중이거나 저지르고 있거나 저질렀다는 의심을 불러일으키는 구체적 징후가 있는 경우," 개인의 프라이버시권에 대한 제한을 명할 수 있는 권한을 독일 정부(즉 경찰과 정보기관을 포함한 보안 기관)에게 부여하고 있다.

- 평화
- 민주적 질서
- 국가 안보
- 독일 주둔 군대의 안보

*구체적 징후(concrete indications)*라는 용어는 비밀스럽고 침해적인 방법 사용에 앞서 충족되어야 하는 높은 기준치를 설정한다. 침해적 조사 방법을 사용해야 할 상당한 이유가 있음을 보증하려면 승인 신청에 이와 같은 정당한 사유가 포함되어야 한다.

4.2 비례성

비밀스럽고 침해적인 정보수집 방법 사용의 준거법은 침해의 정도가 조사의 목적과 비례 관계일 것을 요구해야 한다. 이와 관련하여 유럽 회의는 다음과 같은 경우에만 특별 조사 기법을 사용할 것을 권고했다.

- 심각한 범죄를 저질렀거나 계획 중이라고 믿을 만한 상당한 이유가 있을 때
- "특별 조사 기법 사용의 효과와 확인된 목표 사이의 비례성"을 충분히 고려한 경우[12]

유럽 회의는 나아가 회원국들이 "그러한 (덜 침해적인) 방법을 통해 충분히 효과적으로 범죄를 탐지, 예방 또는 기소할 수 있는" 경우에는 항상 그러한 방법을 사용할 것을 권고했다.[13] 이와 같은 지침은 정당한 목표를 위해 침해적 방법을 사용하면서도 남용과 인권 침해를 최소한으로 줄일 수 있다.

국가 안보 위협과 관련해서는 비례성의 원칙을 적용하기가 더 까다롭다. 비례성 원칙 적용의 중요한 목적은 침해적 방법을 통해 수집되는 정보가 덜 침해적 방법을 통해서는 얻을 수 없었을 것이고, 침해적 방법의 사용을 통해 원하는 정보를 산출할 수 있음을 분명히 하는 것이어야 한다. 예를 들어 독일에서는 프라이버시권을 제한하는 수집 방법을 사용하라는 명령은 "사실을 조사하기 위한 다른 방법의 사용이 무익하거나 조사를 한층 더 어렵게 만들 경우"에만[14] 발할 수 있다.

4.3 승인과 감독

비밀스럽고 침해적인 정보수집 방법의 남용을 방지하기 위해서는 법률 체계에 (정보기관 고위층과 사법부가 참여하는) 승인 절차와 (의회와 전문가 감독기구가 참여하는) 감독 메커니즘이 모두 포함되어야 한다. 적절한 승인 및 감독 체계는 다음 두 절에서 자세히 논의한다. 이러한 승인과 감독의 단계는 상호 배타적이지 않으며, 포괄적이고 탄탄한 책임성 및 투명성 시스템에는 하나 이상의 승인 단계와 하나 이상의 감독 메커니즘이 포함될 수 있다.

5. 정보수집 업무 승인

서로 다른 정보수집 업무 유형에 따라 필요한 승인의 정도도 다르다. 가령 물리적 감시는 비밀스럽기는 하지만 침해의 정도가 크지 않다. 따라서 보통은 정보기관 내부 승인으로 충분하다. 하지만 전화 도청이나 우편물을 가로채는 것은 프라이버시에 대한 합리적 기대를 더 크게 침해하므로 정보기관 주무장관 및 (또는) 판사 등 더 높은 단계의 승인이 필요하다. 수집 업무의 기간을 연장할 때는 원래의 요청 때와 동일한 단계의 승인을 요해야 한다.

5.1 내부 승인

특별 조사 기법의 사용을 정보기관 고위층이 승인하도록 하면 기관 내부의 책임성이 확립되고, 위법 행위 억제에도 효과가 크다. 이 요건 자체만으로 남용을 방지하기에는 부족할 수도 있지만 개인의 프라이버시권을 제한하는 선택은 심각하고 중대한 결정이며 가볍게 받아들여서는 안 됨을 의미한다. 기관 내에서는 프라이버시 침해가 클수록 필요한 승인 단계도 높아지게끔 의사 결정 권한이 구성되어야 한다.

5.2 행정부 승인

정보기관들은 행정부의 통제를 받으며, 행정부는 정보기관의 우선순위를 정하고 활동을 지휘한다. 이것은 주로 주무장관의 책임이다. 주무장관은 또 특정 정보수집 업무의 승인도 담당할 수 있다. 내부 승인 요건이 기관 고위층에게 특별 조사 기법 사용에 대한 책임을 물을 수 있게끔 하는 것처럼 행정부 승인 절차도 특정 수단 승인 결정에 대해 장관에게 책임을 물을 수 있도록 한다.

장관 수준에서 남용이 이루어지는 가장 흔한 경우는 정보기관의 정보수집 장치를 이용해 정부의 정치적 반대파에 관한 기밀 정보를 수집하는 것이다. 이 때문에 비밀 정보수집 방법의 국내사용과 관련된 법률 체계에는 다음과 같은 승인 절차가 포함되어야 한다.

- 장관들이 기관에 요청할 수 있는 사항에 대한 한계를 설정
- 침해적 정보수집 방법의 사용 시 장관 승인 외에 사법부의 승인도 요구

- 정보관들이 위법 행위를 보고할 수 있는 메커니즘 창설
- 이러한 업무의 수행을 심의할 독립적인 감독 기구의 설립 또는 지정

5.3 사법부 승인

대부분의 민주국가에서 사법부의 전통적 책임은 개인의 인권을 보호하는 것이다. 이 역할을 감안하면 판사들이 인권 보호와 정보기관의 정보수집 필요성을 비교 형량할 책임을 갖는 것이 이치에 맞다. 그러므로 국법에서 개인의 프라이버시권을 침해하기 전에 사법부의 승인(보통 영장 형식)을 얻도록 규정하는 것이 일반적 관행이다. 이러한 영장은 공정한 평가의 산물이므로 잠재적 남용의 중요한 억제책으로 간주된다.[15] 나아가 민주적인 보안 기관 감독에 관한 베니스 위원회 보고서에서 지적했듯이 사법부 승인 요건은 보안 문제를 법률에 종속시킴으로써 법에 대한 존중을 제도화한다.[16]

준거 입법에서 사법부 승인을 요하는 업무의 유형과 판사가 업무의 범위, 기간, 대상을 제한하기 위해 가질 수 있는 권한을 명시하는 것이 좋다. 입법에서는 영장 신청의 최소 정보 요건도 정해야 한다(상자 1 참조).

상자 1: 캐나다의 사법부 승인 신청 요건

캐나다 보안정보기관법은 정보기관의 통신 감청 영장 신청에 다음 정보를 포함하도록 규정하고 있다.[17]

- 국가 안보에 대한 위협이 존재한다는 믿음을 정당화하는 데 필요한 사실 관계
- 덜 침해적인 기법을 시도해 보았으나 실패했거나 성공할 가능성이 적다는 증거
- 감청할 통신의 유형
- 획득할 정보의 유형
- 조사 대상 사람들의 신원 또는 계층
- 통신이 감청될 사람들의 신원(알려진 경우)
- 영장이 집행될 장소에 대한 일반적 설명(알려진 경우)
- 영장이 요구되는 기간
- 현재의 신청에 명시된 자와 관련하여 이전에 이루어진 신청의 세부 사항(이전 신청 일자, 이전에 신청을 받은 판사의 이름, 그에 대한 판사의 결정 포함)

많은 나라에서 통신 감청에 사법부 영장이 필요하다. 가령 아르헨티나의 국가정보법(National Intelligence Law)은 아르헨티나 정보기관들이 유형을 불문하고 사적 통신을 감청하기 전에 사법부 승인을 얻도록 규정하고 있다.[18]

경우에 따라 준거법에서 정보기관의 신청을 전문 판사가 심리하도록 규정하기도 한다. 캐나다, 프랑스, 남아공, 스페인 등이 이런 관례에 따르는 나라들이다. 또는 사법부 승인을 발급하는 특별 법원을 만든 나라들도 있다. 미국의 해외정보감시법원(FISC)이 그중 하나인데, 1978년 해외정보감시법에 의해 설립되었다. 임기는 7년으로 재임할 수 없으며 교차 재직하는 11명의 연방 지방 법원 판사로 구성된 FISC는 국가 안보 문제에 관한 영장 신청을 심리한다. 해외정보감시법에 따라 FISC 결정에 대한 정부의 항소를 심리하는 해외정보감시재심법원도 설립되었다.[19]

때때로 이들 전문 판사와 법원들이 진행 중인 정보수집 업무를 심리할 권한을 갖기도 한다. 남아공의 경우, 2002년 통신감청규제 및 통신 관련 정보 제공법(Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002)에서 판사들이 영장에 기술된 목표 달성을 위한 진행 상황에 대해 중간 서면 보고서를 요구할 수 있도록 하고 있다.[20] 이렇게 함으로써 의도하지 않은 대상에 대한 부수적 침해를 제한하고, 비밀스럽고 침해적인 방법을 필요 이상 오래 사용하지 않도록 할 수 있다.

6. 정보수집 업무의 감독

승인과 중요한 짝을 이루는 감독에는 정보기관의 업무가 제대로 승인되었는지 확인하기 위한 심의가 포함된다. 승인과 감독이라는 이러한 두 가지 안전장치가 모두 존재할 때에만 정보수집 활동이 효과적으로 규제된다고 볼 수 있다. (감독 기구의 정보기관에 대한 민원 처리에 관한 논의는 도구 9 참조).

감독은 다양한 기구에 의해 수행될 수 있다. 최고 감사 기구와 국가 옴부즈맨 지구 같은 일부 조직은 위임 사항이 폭넓으므로 감독과 관련이 있다. 감찰관과 전문가 감독 기구 같은 조직은 특정 위임 사항을 뒷받침하는 전문성을 갖추고 있다. 대부분의 나라에서는 감독 업무를 몇 개 조직에 분담시켜 관할이 다양한 정도로 서로 중첩되도록 한다.

6.1 의회 감독 기구

민주 정부 체제 내에서 의회는 정부 기구가 운영되는 법률 체계를 수립할 책임이 있다. 의회는 의회가 제정하는 법률의 준수를 감시할 책임도 있다. 이런 책임은 여느 정부 기관과 마찬가지로 정보기관에도 적용된다.

그러나 정보기관은 다른 정부 기관과 여러 면에서 다르기 때문에 의회는 정보기관 활동을 감시하고 정보기관이 운영되는 법률 체계의 개정을 권고하는 감독 위원회를 설립하는 것이 보통이다. 정보수집 업무와 관련하여 이들 위원회는 보통 다음과 같은 업무를 맡는다.

- 비밀스럽고 침해적인 방법의 사용 감독
- 예산 및 자금 사용 감시
- 충분한 인권 보호 장치가 포함되도록 법률 체계 검토
- 정보기관의 법률 체계 준수 보장

그뿐만 아니라 준거법으로 의회 위원회에 비밀스럽고 침해적인 정보수집 업무를 심사할 권한을 줄 수도 있다. 특히 의회 감독 위원회는 승인 절차가 제대로 적용되었는지 확인하는 데 있어 중요한 역할을 할 수 있다. 예를 들어 아르헨티나 국가정보법은 정보기관 및 활동 감독 공동 위원회(Joint Committee for the Oversight of Intelligence Agencies and Activities)에 "주어진 기간 동안 수행된 감청과 도청"의[21] 목록이 실린 보고서 작성(과 위원회에 대한 제출)을 강제할 수 있는 권한을 부여하고 있다. 그다음 위원회는 이 목록을 이용해 승인받은 사항과 비교해 특별 조사 기법의 사용을 검토할 수 있다. 이렇게 함으로써 승인 절차가 제대로 운영되고 있는지 확인할 수 있다. 이에 관한 예는 아래의 상자 2를 참조하라.

상자 2: 독일 의회의 정보수집 활동 감독

독일에서는 의회 컨트롤 패널(Parliamentary Control Panel)이 침해적 정보수집 방법의 사용을 감독한다.

법률에서는 행정부가 침해적 방법의 사용에 관한 보고서를 "6개월을 넘지 않는 간격을 두고" 컨트롤 패널에 제출하도록 규정하고 있다. 컨트롤 패널은 이 정기 보고서를 바탕으로 법률에 따라 사용된 침해적 방법의 성격과 범위에 관한 연례 연방 의회 보고서를 작성한다.[22]

이 법은 이런 감시 기능 외에도 컨트롤 패널에게 승인 역할도 부여하고 있다. 연방정보국(대외 정보기관)은 "일괄 묶음 형식(bundled form)"으로 전송되고 독일 또는 독일 국민과 관련이 있을지 모르는 국제 통신을 감청하기 전에 컨트롤 패널의 승인을 얻어야 한다. 이것은 주제어에 기초한 감청으로 특정 통신을 대상으로 삼지 않는다.[23]

의회 감독 위원회 자격으로 정보 전문성을 요구하지 않는 것이 보통이다. 하지만 미국의 한 의원이 지적했듯이 위원회 위원들은 적절한 판단에 도달하기 위해서는 생산되고 있는 정보와 그 생산에 사용되는 방법을 잘 알아야 한다.[24]

6.2 전문가 감독 기구

전문가 정보기관 감독 기구는 그 구성원과 보좌진이 특정한 정보 전문성을 갖추고 있는 독립적 조직이다(도구 1 참조). 가장 일반적인 전문가 감독 기구의 유형은 감찰관이다. 기능과 책임은 나라마다 다르지만 감찰관은 보통 정보기관 행위의 합법성과 관련된 민원을 접수하고 그에 대한 조치를 취할 권한이 있는 독립적 기구이다. 감찰관의 위임 사항에는 특별 조사 기법과 비밀 정보수집 방법의 사용을 조사할 권리가 포함된다. 미국과 캐나다 같은 일부 국가는 정보기관 내에서 감찰관을 운영한다. 남아공 같은 나라에서는 감찰관이 정보기관으로부터 독립되어 있다.

남아공 정보 감찰관은 다음과 같은 주요 감독 책임을 지니고 있다.[25]

- 정보기관의 행위가 합법적이고 업무 수행이 효과적인지 파악하기 위한 정보기관 활동 심사
- 행정부와 남아공 국민을 상대로 정보기관 활동의 합법성을 입증
- 정부 관리와 일반 대중이 정보기관을 상대로 제기하는 민원과 관련하여 옴부즈맨 기관 역할 수행

반면 벨기에(상자 3 참조), 독일(상자 4 참조), 노르웨이, 네덜란드는 정보기관 감독에 전문가 기구를 활용한다. 이들 전문가 기구는 정보수집 업무와 관련하여 다음의 기능을 수행한다.

- 업무가 법률 체계, 기관 내부 절차, 행정부 정책을 준수하도록 보장
- 운영 효과성 모니터링 및 개선을 위한 권고
- 정부 관리 및 일반 대중이 특별 조사 기법의 불법적 사용과 관련하여 제기하는 민원 처리

상자 3: 벨기에 상임 정보기관 심의위원회

전문가 감독 기구의 한 가지 예인 벨기에의 상임 정보기관 심의 위원회는 경찰 및 정보기관과 위협 평가 조정단의 심의에 관한 법률(Act Governing the Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment)에 의해 설립되었다. 이 위원회의 위임 사항은 벨기에의 2개 정보기관과 위협 평가 조정단의 운영을 감독하는 것이다. 위원회의 감독은 정보기관 활동의 합법성과 효과성 및 정보 보안 공동체의 조정에 초점을 맞춘다. 이런 책임을 이행할 수 있도록 위원회에는 정보기관이 정보를 수집하는 방법을 포함한 "정보기관의 활동과 방법을 조사"할[26] 권한이 부여된다.

2010년에 위원회에는 정보기관들이 새로 획득한 침해적 정보수집 방법을 사용하는 것을 감독하는 과제가 주어졌다. 위원회는 각각의 침해적 감시 업무를 평가해 법률에 부합하지 않을 경우, 종료(및 수집된 정보의 파기)를 명할 수 있다.[27] 그뿐만 아니라 위원회는 정보기관의 업무, 개입, 행동 또는 행동의 실패와 관련된 민원과 고발"을[28] 처리할 권한도 가지고 있다.

상자 4: 독일의 G10 위원회

독일에서 정보수집을 감시하는 전문가 감독 기구는 G10 위원회다. 이 위원회는 판사 1명이 포함된 4명의 위원으로 구성되며, 의원도 포함될 수 있다. 위원들은 의회 컨트롤 패널이 지명하지만 법률에 의해 직무의 독립성이 보장된다. 위원회의 주요 기능 중 하나는 정보기관의 침해적 수집 방법의 사용이 허용 가능하고 필요한 것인지 결정하는 것이다. 따라서 법률에서는 독일 정부가 침해적 조사 방법의 사용이 예정된 업무에 관해 위원들에게 매달 보고하도록 규정하고 있다. 위원들이 이들 방법 중 어느 하나라도 불필요하거나 허용할 수 없는 것으로 선고하는 경우, 정부는 업무 승인을 철회해야 한다.[29]

G10 위원회는 민원 처리 기능도 맡고 있다. 특히 침해적인 정보수집 방법의 사용에 관한 민원을 심리할 수 있고, 이러한 민원이 정보기관이 그러한 방법을 사용할 능력을 제한할 만한 것인지 결정할 수 있다.[30]

효과적인 정보수집 감독을 위해 전문가 감독 기구는 사전 대책을 취할 수 있는 권한이 있어야 한다. 특히 전문가 감독 기구는 자발적으로 조사를 수행할 수 있는 권한이 있어야 하며, 기밀 여부를 불문하고 정보기관의 방대한 정보에 접근할 수 있어야 한다. 결국 전문가 감독 기구는 권리 침해를 주장하는 사람들에게 의지가 되어야 한다. 또한 정기 의회 보고서도 작성해야 한다. (이 보고서의 수정본은 투명성 증진을 위해 공개되어야 한다.)

7. 결론

이 도구에서는 정보기관이 보안 목표 달성을 위해 언제 어떻게 인권을 제한할 수 있는지 검토했다. 다시 말해 이 도구에서는 개인의 권리를 제한하기 위해 언제 공적 자원을 사용할 수 있는가라는 질문을 살펴봤다. 이 질문의 근본에 놓인 것은 시민과 정부 사이의 관계다. 사회가 도달하는 답이 무엇이건 간에 정보기관으로 하여금 준거법의 한계 내에서 행동하게 하기 위해서는 엄격하고 명확히 규정된 승인 및 감독 체계가 항상 필요하다.

민주국가에서 효과적인 정보수집은 기관의 정당성, 신뢰할 수 있는 거버넌스, 그리고 궁극적으로는 공공의 신뢰에 의존하므로 정보수집 업무에 대한 감독이 특히 중요하다. 이러한 조건들은 정보기관의 활동이 인권을 보호하고 개방성, 투명성, 책임성이라는 민주적 원칙을 수용하는 법률 체계에 뿌리박고 이를 준수할 때에만 달성할 수 있다. 이런 기초 위에서 그리고 오직 이 기초 위에서만 비밀스럽고 침해적인 방법의 정당한 사용이 보장될 수 있다.

8. 권고 사항

- 프라이버시권 등 인권을 제한하는 조사 방법 사용이 허용되는 경우는 정보기관이 운영되는 법률 체계에 명확히 규정되어야 한다.
- 법률 체계에서 비밀스럽고 침해적인 정보수집 방법 사용의 적절한 근거를 명시해야 하며, 이러한 방법은 추구하는 목표와 비례하고 다른 어떤 방법으로도 충분하지 않을 때에만 사용되어야 함을 인정해야 한다.
- 법률 체계에서 비밀스럽고 침해적인 정보수집 방법의 사용을 규제하는 명확한 승인 절차를 설정해야 한다. 침해의 정도가 커질수록 승인 단계도 높아져야 한다.
- 법률 체계에서 비밀스럽고 침해적인 정보수집 방법의 국내사용에 대한 사법부의 승인을 요구해야 한다. 또한 이러한 허가를 내 줄 권한이 있는 판사들을 지정하는 절차를 확립하고, 이들이 정부의 신청을 평가할 때 어떤 기준을 사용해야 하는지 결정해야 한다.
- 법률 체계에서 의회 위원회나 전문가 감독 기구 또는 이 두 가지를 통해 비밀스럽고 침해적인 정보수집 방법을 감시할 효과적인 감독 메커니즘을 설정해야 한다.

후주(後註)

1. Council of Europe, Committee of Ministers, *Recommendation Rec(2005)10 of the Committee of Ministers to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism* (20 April 2005), Rec(2005)10, Chapter I (available at https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM).

2. 이에 관한 더 자세한 논의는 Ronnie Kasrils, *"To spy or not to spy? Intelligence and democracy in South Africa,"* in To spy or not to spy? Intelligence and democracy in South Africa, ed. Lauren Hutton (Pretoria: Institute for Security Studies, 2009), pp. 9–22 참조.

3. 이에 관한 더 자세한 논의는 Marina Caparini, "Controlling and Overseeing Intelligence Services in Democratic States," in *Democratic Control of Intelligence Services: Containing Rogue Elephants,* eds. Hans Born and Marina Caparini (Aldershot, UK: Ashgate, 2007), pp. 3–24 참조.

4. South Africa, Ministerial Review Commission on *Intelligence, Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10 September 2008) (available at http://www.ssronline.org/document_result. cfm?id=3852; accessed 11 July 2011).

5. Ibid., pp. 158–159.

6. United Nations Human Rights Council, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering*

terrorism, United Nations Document A/HRC/10/3 (4 February 2009), p. 6–7 (available at http://www.unhcr.org/refworld/pdfid/49b138c32.pdf; accessed 14 February 2012).

7. Council of Europe, European Commission for Democracy through Law (Venice Commission), *Report on the democratic oversight of the security services*, CDL-AD(2007)016 (2007) (available at http://www.venice.coe.int/docs/2007/CDL-AD%282007%29016-e.asp; accessed 22 October 2011).

8. South Africa, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10 September 2008), p. 157 (available at www.ssronline.org/document_result. cfm?id=3852).

9. European Parliament, Temporary Committee on the ECHELON Interception System, *Draη document on the existence of a global system for intercepting private and commercial communications (ECHELON interception system)* (2001) (available at http:// cryptome.org/echelon-ep.htm; accessed 16 July 2011).

10. Council of Europe, Committee of Ministers, *Recommendation Rec(2005)10 of the Committee of Ministers to member states on "special investigative techniques" in relation to serious crimes including acts of terrorism* (20 April 2005), Rec(2005)10, Chapter II (a) (available at https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=CM; accessed 2 February 2012).

11. Ibid., Chapter II (b) (4).

12.Ibid., Chapter II (b) (5).

13.Ibid., Chapter II (b) (6).

14.Germany, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (June 26, 2001), *Federal Law Gazette* I, p. 1254, revised 2298, last amended by Article 1 of the Act of July 31, 2009, *Federal Law Gazette I,* p. 2499, Section 3 (2).

15.이에 관한 더 자세한 논의는 Gregory Rose and Diana Nestorovska, "Terrorism and National Security Intelligence Laws: Assessing Australian Reforms" in *LAWASIA Journal* (2005), pp. 127 - 155 참조.

16.Council of Europe, European Commission for Democracy through Law (Venice Commission), *Report on the democratic oversight of the security services,* CDL-AD(2007)016 (2007), pp.44 - 45 (available at http://www.venice.coe.int/docs/2007/CDL-AD%282007%29016-e.asp;accessed 22 October 2011).

17.Canadian Security Intelligence Service Act (31 August 2004), R.S.C., 1985, Chapter C-23, Section 21 (2) (available at http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).

18.Argentina, National Intelligence Law, Law 25520 of 2001, Title VI, Article 18.

19.Federal Judicial Center web site, "Foreign Intelligence Surveillance Court" (available at http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html).

20.South Africa, Regulation of Interception of Communications and Provision of Communication- Related Information Act, Act No. 70 of 2002,*Government Gazette,* Vol. 451, No. 24286 (22 January 2003), Section 24 (available at www.info. gov.za/gazette/acts/2002/a70-02.pdf; accessed 2 February 2012).

21.Argentina, National Intelligence Law, Law 25520 of 2001, Title VI, Article 34II.

22.Germany, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (June 26, 2001), Federal Law Gazette I, p. 1254, revised 2298, last amended by Article 1 of the Act of July 31, 2009, *Federal Law Gazette* I, p. 2499, Section 14.

23.Ibid., Section 5.

24.L. Britt Snyder, *Sharing Secrets with Lawmakers:Congress as a User of Intelligence* (Washington: Central Intelligence Agency, February 1997) p. 49(available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sharing-secrets-with-lawmakers-congress-as-a-user-of-intelligence/toc. htm; accessed 14 February 2012).

25.Imtiaz Fazel, "Who shall guard the guards? Civilian oversight and the Inspector General of Intelligence," in *To spy or not to spy? Intelligence and democracy in South Africa,* ed. Lauren Hutton (Pretoria: Institute for Security Studies, 2009), pp.35–36 참조.

26.Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991); See also the Belgian Standing Intelligence Agencies Review Committee web site (available at www.comiteri.be).

27.Belgium, Loi relative aux méthodes de recueil des données par les services de renseignement et de sécurité (4 février 2010).

28.Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Article 34.

29.Ibid., Section 15.

30.Germany, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (G10 Act), (June 26, 2001), *Federal Law Gazette I,* p. 1254, revised 2298, last amended by Article 1 of the Act of July 31, 2009, *Federal Law Gazette* I, p. 2499, Section 15.

도구 6

개인정보 사용 감독

이안 리(Ian Leigh)

6. 개인정보 사용 감독

이안 리(Ian Leigh)

1. 머리말

이 도구에서는 감독 기구가 어떻게 하면 정보기관들이 기관 준거법에 따라 개인정보를 사용하도록 할 수 있는지 살펴본다. 이 도구의 목표는 정보기관들이 개인정보를 어떻게 저장, 접근, 이전하는지 검토하는 데 있어 감독 기구가 하는 역할을 설명하는 것이다. 정보기관에 의한 개인정보수집(도구 5에서 다룸)이나 국내 및 해외 협력기관과의 정보공유(도구 7에서 다룸)는 다루지 않는다.

이 도구에서 살펴보는 주제는 정보기관에 의한 개인정보 사용으로 인한 위험, 이러한 사용을 규제하는 적절한 법률 체계, 이러한 사용을 감독할 수단 등이다. 이 도구는 정보기관의 개인정보 사용에 관한 법률 제정의 주요 원칙을 간략히 요약하면서 끝맺는다.

국제적으로 널리 퍼진 법적 관행에 따라 이 도구에서는 개인정보*(personal data)*라는 용어를 "확인되거나 확인 가능한 개인('정보 주체')과 관련된 일체의 정보"의[1] 의미로 사용한다.

2. 정보기관에 의한 개인정보 사용의 위험

정보기관들은 법적 위임 사항과 관련하여 개인정보를 수집, 저장, 처리, 공개할 정당한 이유를 가지고 있다. 정보와 관련된 개인들이 가령 스파이 행위나 테러 연루 혐의로 인해 정당한 관심 대상일 수 있다. 이러한 정보를 수집할 필요성은 나라마다, 또 기관의 정확한 법적 책임에 따라 기관마다 달라질 것이다.

하지만 지나치게 광범위한 개인정보수집의 위험성이 상존한다. 가령 어떤 용의자가 테러 활동과 관련이 있는지 규명하는 과정에서는 수집된 정보가 부

정적 결론으로 이어질 가능성을 고려한다. 분명 이런 상황에서는 초기의 정보수집을 부적절하다고 할 수는 없다. 하지만 해당 개인이 무관하다는 것을 정보기관이 확인하고 나면 정보를 계속 수집해서는 안 된다(또는 이론의 여지는 있지만 수집한 정보를 계속 보유, 사용해서도 안 된다). 게다가 이렇게 할 경우, 기관은 점점 더 넓은 범위에서 정보를 얻으려는 유혹, 예컨대 용의자의 동료들이나 이들이 속한 시민 사회 조직에 관한 정보를 수집하려는 유혹을 느낄 위험이 있다. 이는 냉각 효과를 일으켜 개인들이 노동조합, 분리주의 정당, 환경 단체나 반핵 단체 같은 합법적 시민 사회 조직에 참여하는 것을 두려워하게 될 수 있다. 또 정보기관의 파일에 저장된 개인정보가 오용될 수 있는 더 일반적인 위험(예컨대 전환기 국가의 관리들이 정적을 협박하거나 언론인들을 압박하기 위해 이용하는 경우)도 존재한다.

정보기관에 의한 정보의 단순한 저장, 분류, 분석, 보유는 해롭지 않다고 주장하는 경우도 있다. 개인정보의 수집은 이보다 확실한 위협이 되지만(도구 5 참조) 개인정보는 개인의 자율성과 밀접히 연관되기 때문에 개인정보의 저장 또한 잠재적으로 해롭다. 정부 기관들이 복수의 출처에서 얻은 개인정보를 짜 맞추는 것이 허용될 경우, 개인들이 자신의 삶에 대해 갖는 통제권, 특히 상세한 개인정보와 관련된 선택권(누구에게 어느 정도로 어떤 목적으로 공개할 것인지에 관한 선택)은 무너지게 된다.

정보기관들은 개인들에 관한 정보를 축적하면서 해당 정보의 주체에 대한 통제 수단을 얻게 된다. 최악의 경우, 정보기관이 보유한 개인정보가 정치인이나 언론인에게 압력을 가할 목적으로 부적절하게 사용될 수도 있다. 피해가 될 만한 공개가 전혀 이루어지지 않은 경우에도 정보기관이 개인정보를 보유하고 있다는 것을 아는 것만으로도 해당 개인은 심리적으로 불안해질 수 있다. 마찬가지로 특정 형태의 정치적, 산업적, 사회적 활동이 보안 파일로 보유되고 있음을 알게 되면 (혹은 그런 의심을 떨쳐버릴 수 없는 경우) 시민 사회 참여가 위축될 수 있다.

자주 언급되는 보안 정보의 장기적 보유의 필요성을 염두에 둔다면 언제 피해를 당할지 모른다는 예상은 개인들에게 수년 또는 수십 년 동안 영향을 미칠 수 있다. 예컨대 어떤 개인의 젊은 시절 활동과 관련된 정보가 경우에 따라서는 그 개인의 노년기까지 보유될 수도 있다(그 사람의 노년기의 삶을 보면 보안 위험으로 취급될 이유가 하등 없음에도 불구하고).

그뿐만 아니라 정보기관이 보유한 개인정보가 부분적이거나 부정확하거나 낡은 것일 수도 있다. 극단적인 경우, 개인적 반감이나 질투심 때문에 해당 개인에게 피해를 주고 싶어 하는 정보원에게서 얻은 정보일 수도 있다. 마찬가지로 금전적 보상을 동기로 하는 정보원은 사람들에 관한 정보를 제공할 때 과장하거나 윤색할 유인이 있을 수 있다.

개인정보 저장과 관련된 그 밖의 위험에는 평소 같으면 별도의 법 집행 기관, 의료, 조세 관련 데이터베이스에 나뉘어 있을 한 개인의 정보를 특권적 접근을 통해 연계할 수 있는, 일부 정보기관의 전례 없는 능력이 포함된다.

물론 위험은 개인정보의 저장, 분류, 분석으로 끝나지 않는다. 그 사용에 수반되는 위험도 있다. 일부 사용은 합법적이지만(보안 심사 등) 신용하기 힘든 경우도 있다(인종적 또는 종교적 정보 자료 수집이나 한 개인에 대한 눈에 보이지 않는 영향력 행사). 예를 들어 출처가 특정되지 않은 개인정보가 언론에 공개될 경우, 정보와 관련된 개인이 피해를 입거나 기회를 잃을 수도 있다. 기밀 정보 취급 인가를 상실하거나 거부당하는 등 직업적 위상이 영향을 받을 수도 있고, 더 일반적으로는 평판이 손상될 수 있다. 마찬가지로 근거가 없거나 부정확한 정보를 외국 정부에 공개할 경우, 입국이 거부되거나 그보다 더 안 좋은 상황에 처할 수 있다(도구 7 참조).

정보기관들은 합법적 대상에 관해 그들이 보유한 정보가 공정하고, 정확하며, 최근의 정보임을 보장하는 데 강한 이해관계를 가지고 있다. 잘못되거나 불완전하거나 오래된 정보를 공개하거나 이를 바탕으로 조언하거나 조치를 취할 경우, 정보기관의 효과성과 평판에 나쁜 영향을 미칠 수 있기 때문이

다. 그럼에도 불구하고 정보 업무에는 정보 취급 절차의 외부 통제와 감독이 필요하다는 주장에 힘을 실어 주는 몇 가지 내재적 위험이 있다. 특히 장래의 안보 위험을 예측해야 한다는 정보기관들의 압박감은 점점 더 많은 개인들에 관해 지나치게 방대한 정보를 수집하려는 태도를 부추긴다. 데이터 마이닝(data mining) 발전 같은 기술적 변화도 이메일 트래픽, 웹 검색, 항공편 예약, 재정 거래 등 방대한 양의 개인정보수집과 저장을 조장한다.

3. 정보기관에 의한 개인정보 사용의 법률 체계

프라이버시권은 주요 국제 조약들에 의해 확립된 인권법에 따라 보호된다.[2] 하지만 이 도구에서는 관련성 및 실용성을 감안하여 유럽 내에서 적용되는 인권, 특히 가장 앞서 있는 유럽 인권 규약(ECHR)에 명시된 인권을 집중적으로 다룬다. 이 도구는 프라이버시권에 초점을 맞추고 있지만 정보기관에 의한 개인정보의 수집과 사용은 표현의 자유권이나 결사의 자유권 같은 다른 인권에도 간접적인 영향을 미칠 수 있다.

유럽 회의 47개국에 적용되는 ECHR 8조는 다음과 같이 명시하고 있다.

1. *모든 이에게는 개인 생활과 가족생활, 가정, 서신 교환을 존중받을 권리가 있다.*
   [유럽 인권 재판소(ECtHR)는 전화 통화 및 기타 전자 통신 수단이 포함되는 것으로 이 조항을 해석했다.]
2. *민주주의 사회에서 국가 안보, 공공 안전 또는 국가의 경제 복지를 위해 무질서나 범죄의 방지, 보건 또는 도덕의 보호 또는 타인의 권리와 자유의 보호를 목적으로, 법률에 합치하며 필요한 경우를 제외하고 공공 당국이 이 권리의 행사를 방해해서는 안 된다.*

유럽 연합(EU) 회원국들에게 구속력을 갖는 명시적인 개인정보 보호 조항이 포함되어 있다는 점에서 EU 기본권 헌장도 중요하다. 8조는 다음과 같다.

1. *모든 이에게는 자신과 관련된 개인정보를 보호 받을 권리가 있다.*
2. *이러한 정보는 명시된 목적을 위해 관련 당사자의 동의나 법률에 규정된 그 밖의 정당한 근거에 기초하여 공정하게 처리되어야 한다. 모든*

이에게는 자신과 관련하여 수집된 정보에 접근할 권리와 수정을 요구할 권리가 있다.

3. *이들 규칙의 준수는 독립적 기관에 의해 통제되어야 한다.*

뿐만 아니라 헌장 52.1조에 따르면,

본 헌장에서 인정하는 권리와 자유의 행사에 대한 모든 제한은 법률로 규정하되 이러한 권리와 자유의 본질을 존중해야 한다. 비례성의 원칙에 따라 제한이 필요하면서도 유럽 연합이 인정하는 공공복리의 목적 또는 타인의 권리와 자유를 보호할 필요성을 진정으로 충족시킬 수 있는 경우에만 제한이 가해질 수 있다.

그러나 기본권 헌장의 이 조항들이 아직 법제화되지 않았기 때문에 이 도구에서는 주로 유럽 인권 규약에 초점을 맞춘다.

유럽인권재판소는 개인정보가 포함된 정부 보안 파일이 유럽 인권 규약 8조에 명시된 사생활의 보호 범위에 분명히 속한다고 판결했다. 이 재판소는 또 몇몇 사건에서 정보기관에 의한 개인정보의 수집, 저장, 배포는 사생활을 존중받을 권리의 "간섭"에 해당하며, 이런 방해는 8.2조에 명시된 엄격한 기준 하에서만 허용된다고 판결했다. 유럽인권재판소의 판결은 다른 정부 기관에 대한 정보의 공개뿐 아니라 내부 심사 및 기밀 취급 인가에도 적용된다.[3] 루마니아 정보기관들이 보유한 보안 파일과 관련된 Rotaru v. Romania (2000) 사건에서 재판소는 다음과 같이 판결했다.

공공 기관에 의한 개인 사생활 관련 정보의 저장과 사용 및 그에 대한 반박 기회의 거부는 규약의 8.1조에 보장된 사생활을 존중받을 권리의 간섭에 해당한다.[4]

3.1 허용 가능한 프라이버시권 제한

정보기관의 개인정보 저장과 사용이 유럽 인권 규약에 부합하려면 8.2조에 명시된 기준을 충족해야 한다. 즉 사용이 "법률에 합치하고," "민주주의 사회에서 필요하며," "국가 안보를 위한" 것이어야 한다.

"법률에 합치" 기준은 가장 엄격한 기준을 부과한다. 이 기준이 충족되지 않으면 아무리 광범위한 이익이 걸려 있더라도 상관없이 8조 위반이 된다.

따라서 합법성 요건은 의원들이 정보기관의 개인정보 사용에 대한 견고한 법적 근거를 마련할 것을 촉구한다.

유럽인권재판소는 "법률에 합치"를 프라이버시권의 제한은 "국내법상 일정한 근거"가 있어야 하며, 재판소의 정의에 따르면 "관련 당사자가 이해하기 쉽고, 나아가 자신에게 닥칠 결과를 예상할 수 있어야 하며, 법의 지배와 양립하는"[5] "사법 제도의 품질(quality of law)" 기준을 충족해야 한다는 의미로 해석했다.

유럽인권재판소는 정보기관에 적용되는 법률이 존재하지 않거나 개인정보의 수집 및 저장을 규제하는 조항이 법률에 포함되지 않은 경우, 이 기준들을 적용하여 8조 위반으로 판결했다.[6] 나아가 "사법 제도의 품질" 기준에 따라 이러한 법률은 "[법률이 적용될 수 있는] 상황에 관해 시민들이 적절히 알 수 있도록 그 용어에 있어 충분히 명확해야 한다."[7] 또 "실제로는 비밀 통신 감시 수단의 집행이 관련 개인들이나 일반 대중이 조사할 수 있도록 공개되어 있지 않기" 때문에 개인정보수집에 관한 법률은 "행정부나 판사에게 부여되는 법적 재량이 규제 받지 않는 권한의 형식으로 표현되는 것"을 허용해서는 안 되며, 따라서 "자의적인 간섭으로부터 개인을 적절히 보호하기 위해서는 부여되는 그러한 재량의 범위와…행사 방식을 충분히 명확하게 적시"해야 한다.[8]

재판소는 이러한 법률을 고려할 때 특히 획득된 정보의 조사, 사용, 저장 시 따라야 할 절차, 정보를 다른 당사자에게 전달할 때 취해야 할 주의 사항, 감시를 통해 획득한 기록을 파기할 수 있거나 파기해야 하는 상황이 법률에 충분히 명확하게 명시되어 있는지 확인한다.[9]
러시아 정부와 관련된 최근의 사건은 이 원칙들을 잘 보여준다.[10] 재판소는 비밀 감시 데이터베이스에 인권 운동가들을 등재한 것은 유럽 인권 규약 8

조 위반이라고 판결했다. 이 데이터베이스는 일반 대중이 접근할 수 없었던 비공개 부령(部令)에 따라 만들어졌기 때문에 일반 대중은 특정 개인들이 데이터베이스에 등재된 이유, 저장되는 정보의 유형, 저장 방식, 저장 기간, 사용 방법, 통제 주체를 알 수 없었다.

다만 "사법 제도의 품질" 기준은 정당한 안보 우려를 감안한다. 예를 들어 보안 심사의 맥락에서 이 기준의 "예상 가능성(foreseeability)" 부분은 신청인이 과정을 완전히 예측할 수 있을 것을 요구하지 않는다(이를 요구할 경우, 심사의 회피가 쉬워질 것이다). 오히려 수권법은 관례에 관한 일반적 설명만 제공하면 된다.[11]

상자 1: 실제에서의 '사법 제도의 품질' 기준

Rotaru v. Romania[12] 사건에서 유럽인권재판소는 루마니아 정부가 보유한 보안 파일의 규제에 관한 루마니아 법률을 검토했다. 재판소는 보안 파일이 사용될 수 있는 상황(구체적으로는 파일에 포함된 개인정보의 사용)에 관한 법률의 설명이 충분히 명확하지 않을 뿐 아니라 정보의 사용을 감시할 메커니즘도 설정하지 않았다고 판결했다.

재판소는 또 이 법률이 루마니아 정부에 부여되는 재량의 범위를 합리적인 정도로 명확하게 "적시"하지 않았기 때문에 결함이 있다고 판결했다. 다시 말해 이 법률은 개인정보를 수집, 기록하고 비밀 파일로 보관하는 정부의 권한 행사를 제한하지 못했다는 것이다. 특히 이 법은 기록될 수 있는 정보의 종류, 감시 조치를 취할 수 있는 대상자의 범주, 그러한 조치를 취할 수 있는 상황, 따라야 할 절차를 규정하지 않았다. 게다가 정보를 보유할 수 있는 제한 기간도 전혀 포함되어 있지 않았다.[13]

혁명 전 정보기관들이 보유하고 있던 비밀 기록 보관소와 관련하여 이 법은 이들 기록 보관소를 참고하는 것은 허용했지만 "파일을 참고할 권한이 있는 사람들, 파일의 성격, 따라야 할 절차 또는 그렇게 얻은 정보를 사용할 수 있는 용도에 관한 명시적이고 상세한 조항들"은[14] 포함되어 있지 않았다.

유럽 인권 규약은 "사법 제도의 품질" 기준의 명확성, 접근 가능성, 예상 가능성 요건이 충족되고 난 후 사생활 간섭의 목적과 필요성에 대한 검토를 요구한다. 여기에는 비례성의 평가가 수반되는데, 다시 말해 국가 안보 보호라는 정당한 목표를 감안하더라도 간섭이 지나치지 않은지 평가한다. 예를 들어 최근 사건에서 유럽인권재판소는 스웨덴 정부가 30년을 넘는 기간 동안 개인정보를 비밀 파일로 보관한 것은 유럽 인권 규약 8조 위반이라고 판결했다. 재판소는 정보의 성격과 오래된 정도를 감안할 때, 정보를 계속 저장하기로 한 결정이 국가 안보라는 적절하고 충분한 이유로 뒷받침된다는 변론을 받아들이지 않았다.[15]

재판소는 사생활 간섭이 "민주주의 사회에서 필요"한지 검토할 때 개인정보의 저장과 사용을 감독하는 어떤 안전장치(특히 독립적 기구가 포함되는 안전장치)가 만들어졌는지 고려한다.[16] 개인이 자신의 사생활에 대한 권리를 보호할 수 있도록 해 주는 안전장치가 존재하지 않는다면 재판소는 8조 위반으로 판결할 것이다. 예컨대 *Turek v. Slovakia* (2006) 사건에서 청구인이 전(前) 체코 공산당 정보기관의 협력자로 등재된 것과 그러한 취지의 기밀 취급 인가가 발급된 것, 그리고 등재에 항의하는 청구인의 제소가 기각된 데 대해 이의를 제기하였으며 재판소는 청구인이 사생활에 대한 권리의 보호를 구할 수 있는 절차의 부재는 8조 위반이라고 판결했다.[17]

법률상 이러한 절차가 존재하더라도 일반 대중이 자신의 정보에 대한 접근 신청을 했을 때 응답이 지나치게 지연되면 위반으로 간주될 수 있다(안전장치가 효과적이지 않기 때문에). 예를 들어 *Haralambie v. Romania* (2009) 사건에서 재판소는 이전의 공산 체제하에서 만들어진 청구인의 보안 파일에 대한 접근 신청 허가를 루마니아 정부가 6년간 지연시킨 것은 유럽 인권 규약 8조에 따른 권리를 침해했다고 판결했다.[18]

따라서 정보기관에 의한 개인정보의 수집과 사용에 대한 명확한 법적 제한이 존재할 필요가 있으며, 감독 기구는 정보기관이 이러한 정보의 관리를 규제하는 법률을 준수하도록 보장해야 한다. 인권과 기본적 자유의 증진 보호

및 테러 방지에 관한 UN 특별 보고관은 UN 인권 위원회에 제출한 2010년 보고서에서 이런 필요성을 거듭 제기했다.

> *공개적으로 이용 가능한 법은 정보기관이 보유할 수 있는 개인정보의 유형과 이 정보의 사용, 보유, 삭제, 공개에 어떤 기준이 적용되는지를 개략적으로 설명한다. 정보기관은 그들의 위임 사항 이행이라는 목적에 필수적인 개인정보를 보유할 수 있다.*[19]

3.2 정보 보호 원칙

유럽 회의 개인정보 자동 처리 관련 개인 보호 협약[20](“데이터 보호 협약”)은 데이터 보호 분야에서의 회원국들의 최소 원칙을 규정한다(표 1 참조). 데이터 보호 협약에 따라 각 조인국은 “데이터 보호의 기본 원칙을 시행하는 국내법상 필요 조치를 취하고,”[21] “데이터 보호의 기본 원칙을 시행하는 국내법 조항의 위반에 대한 제재와 구제책을 수립”하기로[22] 약속한다. 또한 이들 원칙의 측면들(특히 공정한 처리, 동의, 합법적 권한, 주체 접근, 수정과 관련된 측면)은 유럽 인권 규약 8.2조에서 찾을 수 있다.

표 1: 유럽 회의의 개인정보보호 원칙	
데이터 보호 원칙	요건
데이터의 품질 (5조)	자동 처리되는 개인정보는, a. 공정하고 합법적으로 획득, 처리되어야 한다. b. 명시된 정당한 목적으로 저장되고, 이러한 목적과 양립하지 않는 방식으로 사용되어서는 안 된다. c. 저장 목적과 관련하여 적절하고 관련성 있으며 과도하지 않아야 한다. d. 정확하며, 필요할 경우 최신의 정보여야 한다. e. 데이터 주체의 식별을 허용하는 형식으로 보존하되 정보 저장 목적에 필요한 기간 이상 보존해서는 안 된다.
데이터 보안 (7조)	자동화된 데이터 파일에 저장된 개인정보를 무단 접근, 변경 또는 유포 및 우연적 파기나 무단파기 또는 우연적 손실로부터 보호하기 위해 적절한 보안 조치를 취해야 한다.
개인정보의 존재를 확인할 권리(8조)	누구나 자동화된 개인정보 파일의 존재와 그 주요 목적 및 파일 통제자의 신원과 상거소 또는 주 사업장을 확인할 수 있어야 한다.
접근 권리 (8조)	누구나, • 합리적인 시간 간격을 두고 과도한 지연이나 비용 없이 자신과 관련된 개인정보가 자동화된 정보 파일에 저장되어 있는지 여부를 확인하고, 그러한 정보를 이해하기 쉬운 형식으로 전달받을 수 있어야 한다. • 그러한 정보가 본 협약의 5조와 6조에 명시된 기본 원칙을 시행하는 국내법 조항에 반하여 처리되었다면 경우에 따라 그러한 데이터를 수정 또는 삭제할 수 있어야 한다.
구제 받을 권리	누구나 확인 요청, 또는 경우에 따라 본조의 b항과 c항에 언급된 전달, 수정 또는 삭제 요청이 받아들여지지 않는 경우, 구제를 받을 수 있어야 한다.

데이터 보호 협약은 (11조에서) 협약에 포함된 원칙들은 최소 기준이며, 더 폭넓은 보호 수단으로 보완될 수 있다고 명시하고 있다.

데이터 보호 협약이 데이터 보호 원칙에 대한 제한을 다루는 방식은 유럽 인권 규약이 프라이버시권에 대한 제한을 다루는 방식(위에서 논의)과 비슷하다. 제한은 "[조인국의] 법률에 의해 규정"되어야 하며, 국가 안보나 정보주체의 권리 같은 정당한 이익의 보호를 위해[23] "민주주의 사회에서 필요한 수단"에[24] 해당되어야 한다.

3.3 국가 입법의 관련성

정보기관의 개인정보수집, 취급, 공개로 인해 잠재적으로 심각한 인권 침해가 발생할 수 있기 때문에 이러한 데이터의 관리 및 사용 지침을 공개적으

로 접근 가능한 입법을 통해 민주적으로 제정하는 것이 합당하다. 이러한 관행은 몇 가지 장점이 있다. 즉 적절한 정보기관 활동 범위에 관한 반성적인 정치적 논쟁을 장려하고, 결정권을 정보기관이나 행정부의 재량에 속하지 않게 하며, 인권을 침해할 수 있는 행동에 관해 명확한 위임 사항을 정보기관들에 제공한다.

정보기관의 개인정보 사용에 적용되는 입법은 다음 주제 중 하나 이상을 다룰 수 있다.

- 개인정보 처리가 허용되는 사유 및 허용되지 않는 사유
- 개인정보 공개의 한계
- 저장되는 데이터 유형의 공개
- 정보 주체에 의한 개인정보 접근
- 개인정보가 수집되었다는 통지
- 개인정보의 검토, 수정, 삭제

3.3.1 개인정보 처리가 허용되는 사유 및 허용되지 않는 사유

이런 종류의 입법에서는 개인정보가 포함된 파일을 공개할 수 있는 때와 수집 및 보유할 수 있는 개인정보의 유형을 명시할 수 있다(상자 2 참조). 독일의 법률은 비례성의 원칙을 명시적으로 인정하여 정보수집의 필요성을 상응하는 위협의 심각성과 연계시킨다. 구체적으로 이 법에서는 독일 국내 정보기관(연방헌법수호청)에 원하는 정보를 공개 출처에서 얻을 수 있는지 혹은 프라이버시권을 덜 침해하는 수단을 이용해 얻을 수 있는지 고려하도록 요구한다.[25] 이러한 입법은 또한 인종이나 종교적 특징 또는 정치적 견해를 기초로 개인을 표적으로 삼는 등의 특정 행위를 금지함으로써 정보기관이 인권을 침해할 가능성도 줄일 수 있다.

상자 2: 일부 관할권에서의 개인정보 처리의 제한

이 상자에는 허용 불가 기준에 근거해 정보기관의 개인정보 처리를 제한하는 네덜란드와 아르헨티나의 법률 조항이 포함되어 있다.

네덜란드[26]

"일반정보보안국은 다음과 같은 자에 관련된 개인정보만을 처리할 수 있다.

a. 민주적 법률 제도나 국가 안보 또는 기타 중요한 국가 이익에 위험하다고 심각히 의심할 만한 자
b. 기밀 취급 인가 조사를 허락한 자
c. 다른 나라들이 연관된 조사와 관련하여 개인정보 처리가 필요한 자
d. 다른 정보기관 또는 보안 기관이 관련 정보를 획득한 적이 있는 대상자
e. 기관 임무의 적절한 수행을 지원하기 위해서 개인정보가 필요한 자
f. 현재 기관에 고용되어 있거나 고용된 적이 있는 자
g. 6조 2항의 e에서 언급된 위협 및 위험 분석 작성의 맥락에서 관련된 개인정보 처리가 필요한 자"

아르헨티나[27]

"어떤 정보기관도...인종, 종교, 사적 행위, 정치 이념을 이유로, 혹은 당파, 사회, 조합, 공동체, 협동, 지원, 문화 또는 노동 조직 가입을 이유로, 혹은 분야를 막론하고 수행된 법적 행위를 이유로 개인들에 관한 정보를 보유해서는 안 된다."

3.3.2 개인정보 공개의 제한

개인정보 공개에 대한 법적 제한은, 특히 당파적인 정치적 이유로 인한 정보 누출 방지를 위해서라도 일반적으로 바람직하다. 이런 종류의 제한은 특히 전환기 국가에서 중요한데, 보안 기관의 중립성에 대한 신뢰 구축이라는 쉽지 않은 노력이 당파적 행위로 인해 심각하게 훼손될 수 있기 때문이다. 많은 나라에서 합법적 권한 없이 혹은 인가되지 않은 목적으로 개인정보 등

정보기관 파일의 정보를 공개하는 정보관에게는 형사상 책임이 부과된다(상자 3 참조).

상자 3: 루마니아의 개인정보의 부적절한 공개 금지

루마니아 법률의 이 조항은 정보관에 의한 부적절한 공개로부터 개인정보를 어떻게 보호할 수 있는지 보여 준다.

"국가 안보에 필요한 데이터를 얻는 과정에서 우연히 알게 된 개인의 사생활, 명예 또는 평판에 관한 정보는 공개되어서는 안 된다. 1항에 규정된 데이터의 정보를 정보기관 직원들이 법적 체계를 벗어나 공개 또는 활용할 경우, 범법 행위로 간주하고 2~7년의 징역형에 처한다."[28]

3.3.3 저장되는 정보 유형의 공개

일부 국가의 데이터 보호법은 정보기관 등의 국가 기관이 보유하는 개인정보의 유형, 정보를 수집한 목적, 공개가 가능한 목적, 정보가 보관된 데이터베이스의 설명, 데이터베이스에 적용되는 조건 및 통제에 관한 세부 사항을 공개하도록 요구한다. 이런 정보의 공개는 투명성과 책임성의 강화에 도움이 된다. 정보 주체 접근권과 수정권을 행사하고자 하는 개인들은 이 정보를 통해 어떤 국가 기관들이 자신의 개인정보를 가지고 있고 그러한 정보 보유의 범위와 이유는 무엇인지 알 수 있다.

원칙적으로 개인정보 보유를 공개할 의무를 정보기관에 부과하는 것이 바람직한데, 기관의 정당성을 강화하고 정보기관 업무에 관한 부정확한 추측을 줄이는 데 도움이 되기 때문이다. 이런 공개는 정보기관의 개인정보 보유 여부를 해당 개인에게 알려주지 않을 만한 국가 안보상의 타당한 사유가 있는 경우에도(예컨대 정보 주체 접근 신청에 대한 "긍정도 부정도 않는" 답변이 정당할 경우) 도움이 된다.

상자 4: 캐나다 법률상의 데이터뱅크 관련 정보 공개 의무

캐나다 법률의 이 조항은 개인정보 데이터베이스에 관한 정보를 공개할 일반적 의무를 보여 준다.

"정부 기관의 장(長)은 (a) 행정 목적으로 사용되었거나 사용 중이거나 사용이 가능하거나 (b) 개인의 이름이나 식별 번호, 기호 또는 개인에게 할당된 기타 사항에 의해 체계화되거나 검색할 수 있도록 되어 있는 정부 기관 통제하의 모든 개인정보가 개인정보 뱅크에 포함되도록 해야 한다."[29]

3.3.4 개인정보에 대한 정보 주체의 접근

많은 나라가 정부 기관이 보유한 자신의 개인정보에 접근할 수 있는 정보 주체의 권리를 인정하는 정보 보호법 또는 프라이버시법을 제정했다(상자 5 참조). 일부 정보 보호법에서는 추가로 정보 주체가 정보를 수정할 권리, 정보의 정확성에 이의를 제기하는 진술을 정보에 포함시킬 권리 또는 정보를 파기시킬 권리도 인정한다. 이러한 법들은 하나같이 국가 안보의 이유에서 정보기관 보유 정보에 관한 특별 조항을 두고 있다. 이런 조항들의 형태는 다양하다.

일부 국가의 정보기관들의 경우, 정보 보호법이 *면제*되어 이들이 보유하는 정보에는 정보 보호법이 적용되지 않는다. 이러한 경우에는 정보 주체의 권리가 존재하지 않는다. 이 방식은 단순성이라는 장점은 있지만 특정 정보를 알려주지 않는 것이 국가 안보상의 이유로 왜 정당한지 정보기관들이 설명할 의무가 면제를 통해 없어지기 때문에 부당한 것으로 비칠 수 있다. 이 방식은 예컨대 프라이버시 위원회의 관할을 제한하는 등 정상적인 외부 감독과 통제가 작동하지 못하도록 할 수도 있다.

이 방식의 한 가지 변형은 정보기관들에 정보 입법의 자유만 면제해 주는 것이다. 이 경우, (정보 주체의 접근 권리를 포함한) 정보 보호법은 적어도 원칙적으로는 계속 적용되지만 실제로는 사례별로 심사 대상이 된다.

상자 5: 네덜란드 법률상의 정보기관 보유 개인정보에 대한 접근 권리

네덜란드 법률의 이 조항들은 정보기관이 보유한 개인정보에 대한 정보 주체의 조건부 접근 권리를 보여 준다.[30]

"47조

1. 주무장관은 누구든 요청할 경우, 그 사람과 관련된 개인정보가 기관에 의해 혹은 기관을 위해 처리되었는지, 처리되었다면 어떤 개인정보인지 가능한 한 빨리, 늦어도 3개월 이내에 알려주어야 한다."

"48조

1. 기관에 의해 또는 기관을 위해 처리된 자신에 관한 정보를 47조에 따라 조사한 자는 이와 관련된 진술서를 제출할 수 있다. 이 진술서는 관련 정보에 추가된다."

"53조

1. 47조에 언급된 요청은 다음의 경우에 예외 없이 기각된다.
   a. 일체의 조사와 관련하여 요청하는 자와 관련된 정보가 처리되었을 때, 다만,
      i. 관련 정보가 처리된 지 5년이 넘은 경우,
      ii. 그 이후 관련 정보 처리와 연관된 조사와 관련하여 요청하는 자에 관해 어떤 새로운 정보도 처리되지 않았고, 이 정보가 현재의 어떤 조사와도 관련이 없을 때는 그렇지 아니하다.
   b. 요청하는 자와 관련하여 어떤 정보도 처리된 바 없는 경우."

다른 나라들은 그 대신 정보 보호법에 국가 안보에 근거한 *예외 조항*을 포함시킨다. 이 조항들은 면제보다 더 협소하고 더 구체적인데, 정보 보호법하에서 왜 개인의 권리가 적용되어서는 안 되는지 그 이유의 타당성을 사례별로 보여줄 책임을 정보기관에 지우기 때문이다.

이러한 입법은 단순히 행정부 감독 기구에 신청함으로써 행사되되 진행 중인 조사를 보호하고 출처와 방법을 보호하기 위해 고안된 제한 역시 적용되

는 직견적 (prima facie) 접근 권리를 개인들에게 부여할 수 있다.[31] (이러한 모든 제한은 준거법에 부합해야 하고, 위협과 비례 관계가 있어야 하며, 독립적 심사의 대상이 되어야 한다.[32]) 문제가 되는 인권과는 별개로 이러한 접근 방식은 잘못된 처리와 부패를 막는 안전장치 역할을 할 수 있다.

흔히 이런 종류의 예외 조항을 통해 정보기관은 추측에 근거한 요청 및 기관이 보유하고 있는 정보의 범위를 밝혀내려는 의도로 잠재적인 위협이 되는 요청을 막기 위해 "긍정도 부정도 않는" 답변을 내놓을 수 있다.

실제로는 예외의 적용으로 대부분의 요청이 거부될 수 있다. 따라서 예외 방식의 결과는 면제 방식의 결과와 별로 달라 보이지 않을 수 있다. 하지만 중요한 차이점이 있다. 예외 방식은 기관이 공개에 우호적인 법률상의 추정에 맞서 비공개를 정당화할 것을 요구하는 반면 면제 방식은 그렇지 않다. 또한 예외 주장은 면제 주장과는 달리 독립적 기관의 심사가 가능하다. 캐나다의 1982년 정보접근법과 프라이버시법의 시행에 관한 실증적 조사는 정보기관의 정보 취급 과정을 독립적 기구에 의한 외부 조사의 대상으로 삼는 것이 유익하다는 점, 특히 정보 및 프라이버시 문제에 관한 내부적 인식을 제고한다는 점을 확인시켜 준다.[33]

또 다른 방식은 특정 데이터뱅크만을 "면제"로 지정함으로써 원칙적으로는 다양한 감독 메커니즘의 대상으로 삼되, 실제로는 개인의 요청에 대해 상세하게 답변할 정보기관의 의무를 완화하는 것이다. 캐나다는 이 모델을 예외 방식의 보완 장치로 사용하고 있다.

또는 준거법에서 심의 대상 장관에게 포괄적 면제 증명서(영국 정보보호법의 경우처럼[34])를 발급할 권한을 줄 수도 있다. 이렇게 하면 정보기관은 정보기관의 파일이, 가령 협력자나 정보원에게 한 약속과 어긋나게 공개되지 않을 것이라고 확신할 수 있다. 반면 이런 증명서는 일반적으로 지나치게 광범위해서 외부의 감시는 물론 기관의 적합성에 대한 공공의 신뢰 등 외부 감시에 수반되는 이익까지 없애버린다. 정보 보안과 관련된 정당한 우려는 포괄

적 면제보다는 구체적 예외를 통해 더 잘 해결된다. 그뿐 아니라 정보 주체의 접근 및 수정 외에도 데이터 품질 및 데이터 보안과 관련된 정보 보호 원칙 역시 정보기관과 분명 관련이 있으며, 따라서 기관들을 정보 보호법의 관할에서 면제해 주지 않는 또 다른 사유가 된다.

상자 6: 정보기관 보유 개인정보에 대한 접근: UN 특별 보고관이 인정한 모범 관행

"개인들은 정보기관이 보유한 그들의 개인정보에 대한 접근을 요청할 수 있다. 개인들은 관계 당국에 요청서를 보내거나 독립적인 정보 보호 기관 또는 감독 기구를 통해 요청함으로써 이 권리를 행사할 수 있다. 개인들은 자신의 개인정보에서 부정확한 것을 수정할 권리가 있다. 이러한 일반적 규칙의 모든 예외는 법률로 규정되고, 엄격하게 제한되며, 정보기관의 위임 사항 이행에 필요하면서 비례해야 한다. 개인정보를 공개하지 않기로 하는 결정의 타당성을 독립적 감독 기구에 설명할 의무는 정보기관에 있다."[35]

3.3.5 개인정보가 수집되었다는 통지

일부 국가(네덜란드와[36] 독일[37] 등)는 (특히 감시에 의한) 개인정보수집 대상들에게 사후 통지하고, 그들에 관한 정보수집에 일정한 제한을 두도록 요구한다(상자 7 참조). 이론상 이 관행은 소급적 이의 제기의 가능성을 허용하며, 정보기관이 정보수집 대상에 관한 파일을 공개하려는 결정을 억제한다. 하지만 진행 중인 업무와 정보원의 신원을 보호하기 위해 통지받을 권리를 제한하는 것은 많은 경우, 권리를 허상으로 만든다. 이런 이유로 현재 네덜란드에서는 이 관행을 검증하고 있다.[38]

그 대신 통지 또는 수정의 권리가 없는 경우에는 정보기관에 의한 개인정보 사용의 위험이 악화될 것이 뻔하며, 다른 통제의 필요성이 그만큼 더 커진다.

상자 7: 독일 법률상의 정보 대상에 대한 통지 의무

독일 법률의 이 조항들은 통지 원칙을 보여 준다.

"정보 주체는 3절에 따라 제한적 조치의 종료 후 그에 관해 통지받아야 한다. 정보 주체에 대한 통지가 제한의 목적을 위태롭게 할 가능성을 배제할 수 없거나 연방 또는 연방국의 이해관계에 대한 전반적 불이익이 예상되는 동안은 이러한 통지를 보류해야 한다. 조치가 종료된 지 12개월 후에도 이러한 통지가 (문장 2에 따라) 계속 보류되는 경우, 계속 통지를 연기하려면 G10 위원회의 승인을 얻어야 한다. G10 위원회는 계속되는 연기의 기한을 결정해야 한다."[39]

"2관(款) 및 1관에 따른 정보수집과 관련하여 그 성격과 중요성이 특히 은밀한 기술적 수단을 이용한 사적 대화의 도청과 기록으로 이루어지는 서신, 우편 및 통신 프라이버시의 제한에 상당하는 경우,

1. 조치의 목표가 위태로워질 가능성을 배제할 수 있게 되는 즉시, 조치의 종료 후 정보 주체에게 조치에 관해 알려야 한다.
2. 의회 컨트롤 패널에게 통지해야 한다."[40]

3.3.6 개인정보의 검토, 수정, 삭제

정보 보호 원칙을 시행할 수 있는 또 다른 방법은 정보기관의 개인정보 파일이 정확하고, 최신이며, 위임 사항과 관련이 있는지를 주기적으로 심사할 의무를 정보기관에 부과하는 것이다.[41] 일부 국가에서 이 의무는 부정확하거나[42] 더 이상 관련성이 없는[43] 정보를 수정 또는 파기할 보완적 의무와 연계된다.

정보기관들은 보고서가 정확한 정보에 기초할 수 있도록 개인정보가 최신이고 완전한지 검토하고 수정하는 절차를 수립해야 한다(그것이 기관의 합법적 활동과 관련이 있다는 전제하에). 낡은 정보는 오도할 소지가 있으므로 아예 모르는 것보다 더 위험할 수 있다. 게다가 정보 주체의 관점에서 보면 개인정보가 정확하고 최신이어야 기밀 취급 인가 거부나 불리한 이민 심사 결정

같은 부당한 처우를 받을 가능성이 훨씬 낮아진다.

상자 8: 정보기관 보유 정보의 정기적 평가: UN 특별 보고관이 인정한 모범 관행

"정보기관들은 그들이 보유한 개인정보의 관련성과 정확성에 대한 정기적 평가를 수행한다. 이들은 부정확하거나, 위임 사항이나 감독 기구의 업무 또는 발생할 수 있는 법적 소송과 더 이상 관련이 없다고 평가되는 모든 정보를 삭제하거나 업데이트해야 할 법적 의무가 있다."[44]

정보기관에 의한 위협 평가는 예방적이고 예측적인 성격을 갖기 때문에 일부 개인들은 그들이 더 이상 적절한 정보수집 대상이 아님을 입증하는 추가 정보가 수집되기 전까지 정보기관의 정당한 정보수집 대상이 될 수 있다. 예를 들어 정당한 정보수집 대상의 동료이지만 공모자가 아닌 것으로 밝혀지거나 단순히 정당한 조사 대상과 이름이 비슷할 수도 있는 것이다. 정보기관으로 하여금 이러한 대상에 관한 정보수집을 종료시키도록 하면 가능한 남용을 방지할 수 있을 것이다.

마찬가지로 업무 과정에서 수집된 별로 관계없는 개인정보는 삭제해야 한다. 연방헌법수호청의 활동에 관한 독일 법률에는 이 문제와 관련된 몇 가지 조항이 포함되어 있다. 예를 들어 정보수집은 "목표가 달성되는 즉시, 또는 목표를 전혀 달성할 수 없거나 이 정보를 이용해서는 달성할 수 없다는 징후가 있을 경우"[45] 끝내야 한다고 규정하고 있다. 이 법은 또 이전에 수집된 데이터를 정기적으로 (5년마다) 검토해서 부정확한 데이터를 수정하고(부정확하거나 다툼이 있는 데이터는 관련 파일에 그렇게 기록하고[46]) 더 이상 필요하지 않은 데이터를 삭제할 의무를 부과한다(상자 9 참조). 이 의무는 정보주체의 보호를 넘어 감독 업무에도 도움이 된다.

상자 9: 독일 법률상의 개인정보 심의, 수정, 삭제 의무

독일 법률의 이들 조항은 검토, 수정, 삭제의 원칙을 보여 준다. "(1) 파일로 저장된 부정확한 개인정보는 연방헌법수호청이 수정해야 한다.

(2) 파일로 저장된 개인정보는 저장이 허용되지 않거나 더 이상 연방헌법수호청의 과제 수행을 위해 해당 정보를 알고 있을 필요가 없는 경우, 연방헌법수호청이 삭제해야 한다. 삭제로 인해 정보 주체의 정당한 이익이 손상될 것이라고 믿을 만한 이유가 있는 경우에는 정보를 삭제해서는 안 된다. 이 경우 정보를 차단해야 하며, 정보 주체의 동의가 있을 때에만 이전할 수 있다.

(3) 연방헌법수호청은 특정 사건을 다룸에 있어 늦어도 5년 후에 주어진 기간 내에 저장된 개인정보가 수정 또는 삭제되었는지 확인해야 한다."[47]

4. 감독 기구의 역할

본 절에서는 감독 기구가 정보기관의 개인정보 오용 여부를 감시할 수 있는 방법을 논의한다. 본 절에서는 주로 외부 감독에 초점을 맞추고 있지만 내부 메커니즘의 중요성도 간과해서는 안 된다. 여기에는 파일을 언제 공개하거나 종결해야 하는가, 파일에 접근할 수 있는 관리는 누구인가, 그 내용을 언제 검토해야 하는가, 비밀을 유지할 방법은 무엇인가를 결정하는 구체적 절차가 포함된다.

반면 효과적인 외부 감독은 위임 사항을 이행할 수 있는 적절한 법적 권한과 자원을 가진 독립적 기구의 존재에 좌우된다(표 2 참조). UN 특별 보고관은 "정보기관들이 보유한 모든 파일에 접근할 수 있고, 관련 개인들에게 정보를 공개하라는 명령을 내리고, 파일 또는 개인정보의 파기를 명할 권한을 가진"[48] 독립적 기구의 필요성을 강조한 바 있다. 유럽 인권 규약은 정보보호 규정의 준수를 "독립적 기구에 의한 감독 대상"으로[49] 삼고 있다. 국가 차원에서는 스웨덴의 법률이 스웨덴 보안 및 무결성 보호 위원회의 자율성

과 자원을 보장하며,[50] 헝가리 법률은 정보기관의 개인정보 사용과 관련하여 독립적 감독 기구와 협력할 의무를 정보기관에 부과한다.[51]

표 2: 독립적 외부 감독 기구의 특징				
기관	독립성	소관	방법	결과물
옴부즈맨 기관	자율적	개인의 민원	조사	권고
정보 보호 위원	자율적	정보 보호 법률 준수	조사, 표본 추출	보고서, 지시
심판 위원회	자율적	개인의 민원	당사자간 절차	구속력 있는 결정
의회 위원회	당파적	이첩, 자발적 보고	의회 청문회	보고서

전환기 국가와 탈분쟁국의 경우, 새롭게 민주화된 기관들이 이전 정권에서 수집된 정보가 포함된 방대한 보안 파일을 관리할 때가 많다. 이런 파일의 관리는 특히 (건전한 민주적 이유로) 국가의 보안 및 정보 부문의 규모가 대폭 축소되었을 때 특별한 어려움이 될 수 있다. 이런 상황에서 독립적 감독 기구는 다양한 수단을 통해 파일 관리 관행을 감사하는 데 유용한 역할을 할 수 있다.

일반적으로 개인정보와 관련된 독립적 감독 기구의 기능은 부분적으로는 인권법에 명시된 기준에 의해 지배된다. 예를 들어 유럽 인권 규약 13조는 사후 구제에 관해 "권리와 자유가…침해된 모든 사람은 국가 기관 앞에서 실효적 구제를 받아야 한다"고 규정하고 있다. 유럽인권재판소는 *Segerstedt-Wiberg v. Sweden* (2006) 판결에서 13조의 기준은 일반적으로 8조의 "법률에 합치" 및 "민주 사회에서 필요성" 기준에 종속되지만 국가 입법에서 구제 조항의 부재는 결과적으로 규약을 위반하는 것이 될 수 있다고 판결했다. 한편 이 재판소는 국가 안보와 관련된다 할지라도 13조가 요구하는 구제 절차는 법률상으로뿐 아니라 실제에서도 효과적이어야 한다고 판결했다.[52]

8조 및 13조 위반이 주장된 통신 감청 사건인 *Association for European Integration and Human Rights v. Bulgaria* 사건에서 동 재판소는 규약의 요건을 충족하는 독립적 구제의 몇 가지 예를 언급하며 이에 동의했다. 여기에는 독일의 전문가 감독 기구(G10 위원회)와 헌법재판소에 이의를 제기할 권리,

룩셈부르크 국무원에 항소할 권리, 영국의 특별 재판소에 상소할 권리, 노르웨이 전문가 감독 기구에 이의를 제기할 권리가 포함되었다.[53] (민원 처리에 관한 자세한 논의는 도구 9 참조).

정보기관의 개인정보 사용과 관련된 주요 감독 문제는 법적 기준의 문제, 즉 데이터 수집, 데이터 저장, 주체 접근, 통지, 검토, 수정, 삭제 문제와 흡사하다. 이들 문제의 범위가 방대하기 때문에 감독 기구의 관할도 똑같이 방대해야 한다. 예컨대 독일 G10 위원회의 권한은 "정보 주체에게 통지 결정을 포함하여 이 법에 따라 연방 정보기관들이 획득한 개인정보의 수집, 처리, 사용의 전체 범위"에[54] 미친다.

이런 종류의 감독은 정보기관들이 위에서 논의한 개인정보 기준을 준수하도록 하는 데 필요하다. 정보 업무의 비밀스러운 성격을 염두에 둘 때, 이러한 감독은 일반 대중의 민원 제기나 남용 주장에 그때그때 대응하는 식보다는 지속적(또는 적어도 주기적)일 때 더 효과적이고 대중으로부터 존중받을 가능성이 더 높다. 이에 따라 많은 나라가 정보기관 감독을 담당하는 독립적 기구의 위임 사항에 지속적 조사를 위한 조항을 포함시켰다. 가령 노르웨이의 경우, 의회 정보 감독 위원회(전문가 감독 기구)는 매년 여섯 차례 노르웨이 경찰 보안국을 조사할 법적 의무가 있다. 이 조사에는 적어도 10회의 문서 보관소 무작위 점검과 현재 이루어지고 있는 모든 감시 사건에 대한 최소 연 2회의 심사가 포함되어야 한다.[55] 덴마크의 군 및 경찰 정보기관 통제 위원회(초대 위원장인 A.M. Wamberg의 이름을 따 웜버그 위원회로 명명)도 비슷한 역할을 한다(상자 10 참조).

상자 10: 덴마크의 경찰 및 군 정보기관 통제 위원회(웜버그 위원회)

웜버그 위원회의 일차적 업무는 덴마크 보안정보국(PET)에 의한 개인정보 등재와 유포를 감독하는 것이다. 어떤 사람이나 조직이 정보 조사의 대상이 되면 PET는 그 사람이나 조직에 관한 파일을 등록하고자 할 것이다. 이러한 파일들은 웜버그 위원회의 심의 대상이 되며, 위원회가 덴마크인과 덴마크에 거주하는 외국 국적자들에 관한 새로운 파일 등재를 승인해야 한다.

이 위원회는 위원장 1명과 나머지 위원 3명으로 구성된다. 위원장과 위원들은 일반적으로 신뢰와 존경을 받기 때문에 지명된다. 또 위원장과 위원 각자는 정파와 관련 없는 것으로 간주되어야 한다.

위원회는 PET 사무실에서 1년에 6~10차례 회의를 갖고 사건들을 심사해서 그 등재 기준이 충족되었는지 결정한다. 이와 동시에 위원회는 무작위로 낡은 파일의 표본 조사를 실시해서 삭제 마감 기한이 지켜졌는지 확인한다. 위원회는 법무부와 정기적으로 등재 원칙에 관해서 논의하기도 한다.

다수의 국가에서 정보기관이 자신의 개인정보를 취급하는 방식에 민원이 있는 개인은 정보기관의 파일을 조사하여 정보 오용 여부를 독자적으로 판단할 권한이 있는 독립적 기구에 민원의 심리를 청구할 수 있다(도구 9 참조). 예를 들어 스웨덴 법에 따르면 보안 및 무결성 보호 위원회는 민원에 응답할 경우 개인정보 사용과 관련된 보안 기관 활동의 합법성을 심사할 권한이 있다(상자 11 참조). 이 위원회는 또 개인정보 공개 시 인권 기준 및 비례성 원칙을 비롯하여 스웨덴 법령과 헌법을 준수하도록 보장하기 위해 다양한 경찰 및 보안 등록부의 개인정보 공개를 심사한다.[56]

상자 11: 스웨덴의 보안 및 무결성 보호 위원회

스웨덴 법률의 이 조항들은 보안 및 무결성 보호 위원회(전문가 감독 기구)의 책임을 설명한다.

"1. 보안 및 무결성 보호 위원회(이하 위원회)는 범죄 수사 기관에 의한 비밀 감시와 제한적 위조 신원의 사용 및 관련 활동을 감독해야 한다.

위원회는 경찰정보보호법, 특히 동 법 5절과 관련하여 스웨덴 보안국에 의한 정보 처리도 감독해야 한다.

감독은 특히 1항과 2항의 활동들이 법률 및 기타 규정에 부합하게 수행되도록 보장하는 것을 목표로 해야 한다.

2. 위원회는 검사 및 기타 조사를 통해 감독을 시행해야 한다. 위원회는 확정된 상황에 관해 성명을 발표하고 활동 변경의 필요성에 관한 의견을 표명할 수 있으며, 법률과 기타 규정의 결함이 수정되도록 노력해야 한다.

3. 개인의 요청이 있을 경우, 위원회는 해당 개인이 비밀 감시의 대상 혹은 1절에 규정된 개인정보 처리의 대상이었는지 여부와 비밀 감시 및 연관 활동 또는 개인정보의 처리가 법률과 기타 규정에 부합했는지 확인할 의무가 있다. 위원회는 확인이 실시되었음을 해당 개인에게 통지해야 한다."[57]

5. 권고 사항

본 절에서는 정보기관의 개인정보 사용이 인권 의무에 부합하게 하기 위한 적절한 법률 체계 구축에 있어 특히 의원들이 따를 수 있는 원칙들을 권고한다.

- 각 정보기관의 법적 위임 사항은 개인정보를 합법적으로 수집하고 파일을 합법적으로 공개할 수 있는 목표를 명시해야 한다.

- 정보기관의 준거법은 개인정보의 사용 방법과 보유 기간에 대한 효과적 통제 수단을 확립해야 한다. 이러한 통제 수단은 국제적으로 인정되는 정보 보호 원칙을 준수해야 한다. 이러한 법률은 또한 통제 수단이 진정으로 효과적일 수 있도록 독립적 인력(즉, 정보 공동체 외부의 감독자)에 의한 견제도 규정해야 한다.

- 정보기관 준거법은 국내 프라이버시 및 정보 보호 법률의 적용에서 정보기관을 면제해 주어서는 안 된다. 그보다는 정보기관의 위임 사항과 관련이 있는 경우, 정보기관들이 제한적 국가 안보 개념에 근거해 공개 규정의 예외를 활용할 수 있도록 허용해야 한다.

- 이러한 예외가 올바로 적용되었는지 여부는 정보기관 파일에 있는 관련 정보에 적절히 접근할 수 있는 독립적 감독 기구가 결정해야 한다.

- 정보기관에 의한 자신의 개인정보의 저장, 사용 또는 공개가 자신의 프라이버시를 침해했다고 민원을 제기하는 개인들은 독립적 기구 앞에서 실효적 구제를 받을 권리가 있다.

- 정보기관의 개인정보 저장 결정은 정보 주체의 접근 요청 및 개인정보의 보유, 이전, 삭제 결정과 마찬가지로 독립적 감독 기구에 의해 심사되어야 한다.

후주(後註)

1. 이 정의는 유럽 회의 개인정보 자동 처리 관련 개인 보호 협약 2(a)조와 경제개발협력기구(OECD) 프라이버시 보호 및 개인정보의 국제적 유통에 관한 지침 1(b)절에 등장한다. 비슷한 정의가 EU Directive 95/46/EC 2(a)조에도 나오지만 이 지침은 국가 안보 활동에는 적용되지 않는다(3.2조 참조).

2. 시민적 정치적 권리에 관한 국제 규약 17조는 "1. 누구도 사생활, 가족, 가정 또는 서신 교환에 대한 자의적이거나 불법적인 간섭 또는 그 명예와 평판에 대한 불법적 공격을 받아서는 아니 된다. 2. 모든 이는 이러한 방해나 공격으로부터 법의 보호를 받을 권리가 있다"고 명시하고 있다. 세계 인권 선언 12조는 "누구도 사생활, 가족, 가정 또는 서신 교환에 대한 자의적 간섭이나 명예와 평판에 대한 불법적 공격을 받아서는 안 된다. 모든 사람은 그러한 간섭이나 공격으로부터 법의 보호를 받을 권리가 있다"고 명시하고 있다.

3. *Leander v. Sweden,* No. 9248/81, European Court of Human Rights (ECHR), 1987.

4. *Rotaru v. Romania,* No. 28341/95, ECHR, 2000, Paragraph 46.

5. *Weber and Saravia v. Germany,* No. 54934/00, ECHR, 2006, Paragraph 84.

6. R. V. v. *The Netherlands,* No. 14084/88, ECHR, 1991.

7. *Weber and Saravia v. Germany,* No. 54934/00, ECHR, 2006, Paragraph 93.

8. Ibid., Paragraph 94.

9. 예컨대 German G10 law in *Weber and Saravia v. Germany,* admissibility decision, No. 54934/00, ECHR, 2006의 상세한 분석 참조.

10.*Shimovolos v. Russia,* No. 30194/09, ECHR, 2011.

11.*Leander v. Sweden,* No. 9248/81, ECHR, 1987.

12.*Rotaru v. Romania,* No. 28341/95, ECHR, 2000.

13.Ibid., Paragraph 57.

14.Ibid.

15.*Segerstedt-Wiberg and Others v. Sweden,* No. 62332/00, ECHR, 2006.

16.*Leander v. Sweden,* No. 9248/81, ECHR, 1987, Paragraphs 52–57; see also *Rotaru v. Romania,* No. 28341/95, ECHR, 2000, Paragraph 59.

17.*Turek v. Slovakia,* No. 57986/00, ECHR, 2006.

18.*Haralambie v. Romania,* No. 21737/03, ECHR, 2009.

19.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,* United Nations Document A/HRC/14/46 (17 May 2010), p. 21 (Practice 23).

20.Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108 (Strasbourg, 28.I.1981). 이 협약은 광범위한 영향을 미친 프라이버시 보호 및 개인정보의 국제적 유통에 관한 OECD 지침 (23 September 1980) (available at http://www.oecd.org/document/18/0,33

43,en_2649_34255_1815186_1_1_1_1,00. html#part2)에 기초한 것이다. OECD 지침은 수집 제한, 데이터 품질, 목표 명시, 사용 제한, 보안 안전장치, 공개성, 개인의 참여, 책임성과 관련한 8대 정보 보호 기본 원칙을 확립했다.

21.Ibid., Article 4.

22.Ibid., Article 10.

23. *필요한 수단* 이라는 용어는 EU 기본권 헌장에 천명된 비례성의 원칙의 맥락 내에서 이해되어야 한다.

24.Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing

of Personal Data, ETS No. 108 (Strasbourg, 28.I.1981), Article 9.

25.Germany, Federal Act on Protection of the Constitution (20 December 1990), *Federal Law Gazette* I, p. 2954, 2970, last amended by Article 1a of the Act of 31 July 2009, *Federal Law Gazette I,* p. 2499, 2502, Section 9.

26.The Netherlands, Intelligence and Security Services Act 2002, Article 13.

27.Argentina, National Intelligence Law 2001, No. 25520, Article 4.

28.Law on the National Security of Romania, Article 21.

29.Canada, Privacy Act, R.S.C., 1985, Chapter P-21, Section 10. An overview of the personal information databanks maintained by the Canadian Security and Intelligence Services can be found at http://www.infosource.gc.ca/inst/csi/fed07-eng.asp.

30.The Netherlands, Intelligence and Security Services Act 2002.

31.예컨대 Netherlands, Intelligence and Security Services Act 2002, Article 47; Sweden, Act on Supervision of Certain Crime-Fighting Activities, Article 3; Switzerland, Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, Article 18 (1) 참조.

32.예컨대 Netherlands, Intelligence and Security Services Act, Articles 53–56; Croatia, Act on the Security Intelligence System, Article 40 (2) (3) 참조.

33.Ian Leigh, "Legal Access to Security Files: the Canadian Experience," *Intelligence and National Security* Vol. 12, No. 2 (1997), p. 126. 이 연구를 위해 캐나다 보안정보국 관리들, 정보 프라이버시 위원 및 보좌진, 법률 이용자들, 연방 법원 판사들 및 기타 전문가들과의 면담이 수행되었다.

34.United Kingdom, Data Protection Act 1998, Section 28.

35.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,* United Nations Document A/HRC/14/46 (17 May 2010), p. 23 (Practice 26).

36.2002년 정보보안기관법 34조에 따르면 정보기관이 특별 조사 권한을 행사한 지 5년 후부터(그 이후로는 매년) "주무 장관은 이 특별 권한을 적용받은 사람과 관련된 사건 보고서를 이 사람에게 제출할 수 있는지 여부를 검토한다. 가능할 경우, 최대한 빨리 제출이 이루어져야 한다."

37.Germany, Federal Act on Protection of the Constitution, Section 9.3.

38.The Netherlands, Review Committee on the Intelligence and Security Services (CTIVD), *Annual Report 2010 – 2011,* Chapter 4.

39.Germany, Act Restricting the Privacy of Correspondence, Posts and Telecommunications (G10 Act), (June 26, 2001), *Federal Law Gazette* I, p. 1254, revised 2298, last amended by Article 1 of the Act of July 31, 2009, *Federal Law Gazette* I, p. 2499, Section 12.1.

40.Germany, Federal Act on Protection of the Constitution, Section 9.3.

41.예컨대 Germany, Federal Act on Protection of the Constitution, Section 14.2; Germany, G10 Act, Sections 4.1 and 5; Switzerland, Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, Article 15 (1) (5) 참조.

42.The Netherlands, Intelligence and Security Services Act 2002, Article 43; Croatia, Act on the Security Intelligence System, Article 41(1).

43.Germany, Federal Act on Protection of the Constitution, Section 12.2.

44.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,* United Nations Document A/HRC/14/46 (17 May 2010), p. 22 (Practice 24).

45.Germany, Federal Act on Protection of the Constitution, Section 9.1.

46.Ibid., Section 13.

47.Ibid., Section 12.

48.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,* United Nations Document A/HRC/14/46 (17 May 2010), p. 22 (Practice 25).

49.European Union, Charter of Fundamental Rights of the European Union, Article 8.3.

50.Sweden, Ordinance containing instructions for the Swedish Commission on Security and Integrity Protection, Sections 4–8 (on management and decision making) and 12–13 (on resources and support).

51.Hungary, Act on the National Security Services, Section 52.

52.*Al-Nashif v. Bulgaria,* No. 50963/99, ECHR, 2002, Paragraph 136.

53.*Association for European Integration and Human Rights v. Bulgaria,* No. 62540/00, ECHR, Paragraph 100.

54.Hans De With and Erhard Kathmann, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Germany," in *Parliamentary Oversight of Security and Intelligence Agencies in the European Union,* Aidan Wills and Mathias Vermeulen (Brussels: European Parliament, 2011), Annex A, p. 220.

55.Norway, Instructions for Monitoring of Intelligence, Surveillance and Security Services, Sections 11.1 (c) and 11.2 (d).

56.Iain Cameron, "Parliamentary and Specialised Oversight of Security and Intelligence Activities in Sweden," in *Parliamentary Oversight of Security and Intelligence Agencies in the European Union,* Aidan Wills and Mathias Vermeulen (Brussels: European Parliament, 2011), Annex A, pp. 279–81.

57.Sweden, Act on Supervision of Certain Crime- Fighting Activities (2007); 또한 Sweden, Ordinance containing instructions for the Swedish Commission on Security and Integrity Protection (2007) Section 2 (available at http://www.sakint.se/dokument/english/ordinance_instruction_scsip.pdf) 참조.

도구 7

정보공유 감독

켄트 로치(Kent Roach)

7. 정보공유 감독

켄트 로치(Kent Roach)

1. 머리말

이 도구에서는 정보공유의 증가로 정보기관 감독과 국가 안보 정보를 수집, 분석, 배포하는 그 밖의 정부 부처가 당면하는 도전을 검토한다.[1] 여기서 정보공유라는 용어는 정보기관들과 해외 및 국내 협력 기관들 사이에서 교환되는 정보를 가리킨다. 이 도구는 주로 감독 기구에 초점을 맞추지만 정보공유의 증가가 인권과 프라이버시에 미치는 영향도 살펴본다(이는 사법부와 행정부, 언론, 시민 사회 같은 다른 조직들도 관심을 가질 만하다).

수집한 정보의 공유는 항상 정보기관의 업무 중 하나였다. 하지만 2001년 9월 11일 테러 공격 이후 정보기관 간 정보공유와 정보기관과 다른 국제 조직들 간의 정보공유가 한층 더 강조되었다. 정보공유의 양 및 관련되는 기관의 범위가 증가하면서 당연히 정보공유에 수반되는 문제도 늘어났다. 공유된 정보는 부정확할 수 있어 정보를 받은 측이 희소한 자원을 엉뚱한 곳에 쓰게 될 수도 있다. 그뿐만 아니라 정보를 수령한 기관이 정보를 부적절한 용도로 사용할 수도 있다. 몇몇 극단적인 경우에는 정보의 제공자나 수령자가 저지르는 고문 및 기타 인권 침해에 기관들이 연루될 수도 있다.

최근 드러난 리비아, 미국, 영국 정보기관들 간의 정보공유 사례가 보여준 것처럼 나쁜 정보공유 관행은 정보 공급 국가의 평판을 심각하게 손상시킬 수 있다.[2] 더욱 중요한 것은 부적절하게 공유된 정보가 개인의 평판에 지극히 해로운 영향을 미칠 수 있다는 점이다. 이런 유감스러운 결과 때문에 공유되는 정보가 극비 정보인 경우가 많다 하더라도 정보공유 관행을 효과적 감독 하에 두는 것이 특히 중요하다. 이러한 공유 활동이 일반적으로 비밀스럽게 수행되고, 그에 따라 법원이나 언론이 심사하기가 쉽지 않다는 점을 감안할 때 정보공유 관행의 감독은 특히 중요하다. 공유된 정보로 인해 피해를 볼 수 있는

사람들은 심지어 자신이 피해를 당했는지 모를 수도 있으며, 항의조차 하지 못할 수 있다. 일반적으로 감독 기구는 공유된 정보에 접근할 수 있어야 한다. 그렇지 않으면 감독 대상 정보기관의 정보공유 관행을 효과적으로 심사할 수 없을 것이다. 하지만 최근의 정보공유 강화와 공유되는 정보의 비밀성이 감독 기구에 제기하는 도전은 아무리 심각하게 보더라도 지나치지 않다.

이 도구는 911 이후의 정보공유에 대한 간략한 검토로 시작한다. 본문에서는 정보의 수령 및 유포와 관련하여 해외와 국내 순서로 정보공유 감독이 당면한 도전을 살펴본다. 이 도구는 정보공유 감독 개선을 위한 구체적인 권고사항으로 끝맺는다. 권고 사항은 감독의 정책, 조직, 관리 측면뿐 아니라 정보공유를 더욱 효과적으로 감독할 수 있는 법률 체계도 다룬다.

2. 정보공유

2.1 정보공유의 필요성

해외와 국내의 정보기관들이 당면한 복잡한 안보 위협에 효과적으로 대처하려면 정보를 공유할 필요가 있다는 점은 분명하다. 그러나 현재의 전환기적 환경에서는 정보공유가 훨씬 더 강화되어야 할 필요성이 자주 강조되어 왔다. 가령 UN 안전보장이사회는 결의안 1373호(2001년 9월 28일)를 통해 회원국 간 정보공유의 강화를 구체적으로 촉구했다. 유럽에서도 유로폴(Europol), 베른 클럽(Club of Berne), EU 군사 참모단, EU 상황 센터 같은 기구들이 정보공유 증대를 추진했다.[3] 그 결과 평소 같으면 공동 안보 작전에 동참하기를 꺼렸을 전통이 판이한 나라들이 이제는 테러 방지뿐 아니라 군사 및 평화 유지 작전, 무기 사찰, 전쟁 범죄 기소와 관련한 정보공유에 적극적인 태도를 보이고 있다.

현재 정보기관들 사이에서 이루어지는 정보공유의 범위는 가늠하기 어려운데, 정보 자체가 기밀이고 공유 협정 역시 마찬가지이기 때문이다. 하지만 입수 가능한 데이터로 어느 정도 규모를 파악할 수 있다. 캐나다와 호주의 국내 정보기관들을 예로 들면 각각 약 250개 해외 기관들과 정보를 교환한다. 미국 중앙정보국(CIA)은 전 세계 400개 이상의 기관들과 연계하고 있다.[4]

이러한 공유는 공식적으로, 또 비공식적으로 이루어진다.

현재의 안보 위협 환경이 다면적이기 때문에 인권을 존중하는 나라들은 이따금 인권 기록(human rights record)이 좋지 않은 국가들과 정보를 공유해야 한다는 점에 부담을 느낄 수도 있다. 정보기관은 테러 용의자가 입국했거나 입국을 계획하고 있는 국가에 이를 경고해야 한다고 생각할 수 있다(비록 정보를 받는 나라가 인권 억압의 전력을 가지고 있다고 하더라도). 정보를 제공하는 측이 정보를 받는 측으로부터 일정 정도의 보답을 당연히 기대하는 것 역시 사실이다.

911 이후 10년 간, 여러 나라 정부들은 보안 및 정보 업무를 담당하는 국내 기관들 간의 정보공유를 가로막는 법적, 조직적 장벽을 제거하기 위해 노력했다. 미국의 경우가 특히 그렇다. 미국의 정부 위원회는 정보 보안 기관들 간의 장벽 때문에 911 항공기 납치범 일부의 신원을 파악하지 못했을 수 있다고 판단했다.[5] 그 결과 정보공유의 열기가 테러 방지를 훌쩍 뛰어넘어 국경 경비, 이민, 밀수, 스파이 활동 등 광범위한 법 집행 기능까지 확대되었다.

2.2 정보공유가 초래하는 문제점

안보 증대를 위해 정보공유가 필요하다는 점에는 폭넓은 합의가 이루어져 있지만 최근에 정보공유가 확대되면서 주의 깊은 관리와 감독을 요하는 숱한 잠재적 문제들이 제기되었다. 예를 들면 이제 법 집행 기관들은 신뢰할 수 없는 공유 정보를 근거로 집행 활동을 펼치게 될 가능성이 커졌으며, 정보기관들이 공유한 정보가 이후의 법정 소송에서 공개될 위험도 더 커졌다. 개인들의 권리, 특히 프라이버시권이 침해될 위험성 역시 더 커졌다. 개인들은 공유된 정보의 정확성에 이의를 제기할 기회조차 얻기가 힘든데, 자신에 관한 정보가 공유되었다는 사실 자체를 모를뿐더러 공유된 정보에 대한 접근이 불가능하기 십상이기 때문이다.

많은 나라의 정보기관들은 경찰 및 기타 법 집행 기관과의 비밀 정보공유를 기피해 왔다. 캐나다의 한 조사 위원회는 이러한 기피가 1985년의 에어 인디

아 폭파 사건과 사건 후 조사에서 드러난 다양한 결함의 한 원인이었다고 결론 내렸다.[6] 정보기관들은 정보를 공유하면 결국은 공개되어 중요한 정보 출처와 방법을 노출시키고 향후 기관의 정보수집 능력을 위협할 것을 우려해 정보를 감추려는 경향이 있다. 게다가 법정 소송에서 채택될 수 없는 방법으로 획득한 정보를 법 집행 기관과 공유할 경우에는 더욱 큰 문제가 될 수 있다. 어쩌면 정보기관보다는 정보공유에 더 적극적일 경찰 역시 정보공유가 안보 위협을 수사하고 기소하는 경찰의 능력에 타격을 입힐 수 있다고 우려한다.

정보기관 감독 담당자들은 가장 힘든 도전 중 일부에 봉착한다. 이들은 현재 공유되고 있는 방대한 양의 정보에 뒤처지지 않아야 하는데, 정보의 양이 워낙 많아서 그 중 일부만을 조사하는 감사에 자주 의존해야 하는 실정이다. 대부분의 감독 기구 역시 공유되는 비밀 정보에 접근하고 추적해야 하는 어려움에 봉착한다. 가령 경찰을 관할하는 감독 기구는 경찰이 정보기관으로부터 획득한 정보가 어떻게 수집되었는지 파악할 권한이 없을 수 있다. 정보공급자가 외국 기관일 경우에는 더욱 그렇다.

많은 관할권에서 여러 국내 및 해외 출처에서 공급되는 안보 위협 관련 정보를 집대성하기 위해 정보 보안 기관의 네트워크(경우에 따라 “융합 센터”라고도 함)가 만들어졌다. 이들 네트워크 중 일부에서는 심지어 외국 기관들의 상호 정보 교환까지 가능하다. 국내 감독 기구가 감독 대상 기관의 업무를 완전히 이해하려고 한다면 이들 네트워크가 수집하고 배포하는 정보에 접근할 필요가 있다. 특히 해당 기관이 이러한 지역, 국가, 초국가적 기관들과 정보를 주고받기 때문에 더욱 그렇다.

국내 기관 간 및 해외 기관과의 정보공유 증가에 대한 한 가지 대응은 복수 기관 간의 정보공유를 검토할 특별 관할권을 갖는 특별 조사 위원회를 임명하는 것이었다. 상자 1과 2에서는 캐나다와 영국의 이러한 특별 조사 위원회의 사례를 살펴본다.

정보기관들은 명백히 국내 및 해외 협력 기관과 정보를 공유할 필요가 있다. 정보를 공유하지 않고 단순히 수집만 하는 기관은 탐지한 보안 위협을 다른 기관들에 경고해야 하는 의무를 게을리 하는 것이다. 현재 많은 위협의 초국가적 성격으로 인해 국내적으로나 국제적으로도 정보공유의 증대가 필수적이다.

하지만 정보공유 증대에 단점이 없는 것은 아니다. 정보공유는 법적으로 허용되지 않고 윤리적으로도 정당화되지 않는 방식으로 프라이버시권과 그 밖의 인권 침해를 불러올 수 있다. 또한 민감한 출처에서 얻은 비밀 정보가 공개될 위험도 있다.

국내 및 초국가적 네트워크(융합 센터)를 통한 정보공유는 책임을 분산, 왜곡시킬 수 있다. 위임 사항상 관할이 단일 기관으로 국한된 의회 및 전문가 감독 기구는 정보기관들이 참여하는 네트워크의 기록에 접근할 수 없는 경우가 많은데, 이는 감독 업무에 심각한 걸림돌이 될 수 있다.

국경을 넘나드는 정보공유는 예컨대 인권이 잘 보호되는 나라들이 인권 상황이 좋지 않은 나라들과 정보를 교환해야 하는 압박을 받는 경우처럼 정책 갈등을 초래할 수도 있다. 이런 식의 정보 교환은 해당 국가를 정보공유 상대국에 의해 자행되는 고문과 같은 인권 억압의 공모국으로 만들 수 있다.

요컨대 정보기관은 정보공유를 아예 거부하고서는 그 기능을 할 수 없다. 하지만 정보공유의 증가는 여러 가지 위험을 초래한다. 개인들로서는 인권, 특히 프라이버시권이 침해될 위험이 있다. 정보기관의 경우, 정보기관의 평판을 손상시키고 희소 자원의 잘못된 할당을 초래할 수 있는 신뢰할 수 없는 정보 또는 부적절하게 획득한 정보가 유포될 위험이 있다. 감독 기구의 경우, 어떤 정보가 공유되고 있고 공유가 어떻게 이루어지고 있는지 이해할 능력이 새롭게 제한될 위험이 따른다.

상자 1: 캐나다의 정보공유 관련 특별 조사

캐나다의 다년간에 걸친 2개 조사 위원회(마헤르 아라르[Maher Arar] 관련 조사 위원회와 압둘라 알말키[Abdullah Almalki], 아마드 아부-엘마티[Ahmad Abou-Elmaati], 무아예드 누레딘[Muayyed Nureddin] 관련 내부 조사 위원회)의 보고서에 따르면 캐나다 경찰과 정보기관의 정보공유 관행은 테러 혐의로 시리아와 이집트에 구금된 캐나다 시민들에 대한 고문의 간접적인 원인이었다.[7] 두 위원회는 모두 일차적으로는 대중적 스캔들에 대한 대응 차원에서 정부가 임명한 임시 기구였지만 기존의 감독 기관들이 특정 기관에 매여 있어 광범위한 국제적 안보 문제에 대한 범정부적 대응 방식을 조사할 관할권이 없다는 인식이 높아진 이유도 있었다.

두 위원회는 미국, 이집트, 시리아 정부에 조사 협조를 요청했다. 세 나라 정부는 모두 협조하지 않았다. 또한 캐나다 정부는 두 위원회가 보유하게 된 비밀 정보를 공개할 권한도 제한했다. 그러나 이 제한은 사법 심사의 대상이었기 때문에 두 위원회는 경우에 따라 (승소 또는 소송 가능성을 통해) 정부가 원했던 것보다 많은 정보를 공개할 수 있었다. 두 위원회는 캐나다가 미국, 시리아, 이집트 관리들과 공유한 정보의 몇몇 세부 사항을 검토했다. 이 정보에는 다양한 캐나다인들을 테러 집단과 연관 짓는 첩보가 포함되어 있었다. 구체적으로는 테러 혐의로 시리아와 이집트에 구금된 캐나다 시민들에게 질문을 하기 위해 캐나다 관리들이 시리아와 이집트 관리들에게 보낸 질문 목록이 포함되어 있었다.

캐나다의 두 위원회는 이들 외국 관리들로부터 받은 정보도 검토했는데, 나중에 캐나다 내에서 유포되었고 적어도 한 건의 소송에 제출되었다. 두 위원회 모두 이 정보가 공유된 방식에 결함(비단 국내 경찰, 보안, 세관, 외무부서 인력 간 공유만이 아니라 외국 기관과의 공유에 있어서도)이 있음을 발견했다.

이 두 조사 위원회는 주로 정보공유의 적절성, 특히 정보공유가 고문을 당하지 않을 권리 및 프라이버시권 같은 인권에 가하는 위험에 초점을 맞췄다. 그럼에도 불구하고 두 위원회가 정보공유의 증대에 반대했다고 추론하는 것은 옳지 않다. 이들은 단지 통제의 강화와 심사의 보강을 원했을 뿐이다. 아라르 위원회는 "정보공유는 필수적이지만 신뢰할 수 있고 책임감 있는 방식으로 이루어져야 한다. 정보공유의 필요성이 정보를 통제 없이, 특히 단서 조항의 사용 없이 공유해야 함을 뜻하지는 않는다. 또 정보의 관련성, 신뢰성 또는 정확성을 고려하지 않거나 개인정보나 인권을 보호하는 법률을 고려하지 않고 정보를 교환하는 것을 뜻하지도 않는다"고[8] 결론 내렸다.

1985년 에어 인디아 폭파 사건을 조사한 세 번째 캐나다 조사 위원회는 다소 다른 관점에서 정보공유를 검토했다. 정보공유의 효능(적절성과 상반되는 의미)을 고려하여 에어 인디아 위원회는 공개의 위험 때문에 정보기관이 경찰 및 기타 법 집행 기관과의 정보공유를 꺼리는 태도를 개선하기 위한 권고 사항을 마련했다. 이 세 위원회 모두 정보공유의 근본적 딜레마, 즉 정보공유가 너무 적으면 안보에 위협이 되는 반면, 정보공유가 너무 많고 특히 공유에 규율이 서 있지 않으면 인권을 위협한다는 딜레마를 인정했다.

상자 2: 영국의 정보공유 관련 특별 조사

2010년에 영국 정부는 다른 나라에 억류되어 있는 사람들에 대한 학대에 영국이 얼마나 관련되어 있는지를 조사할 공식 조사 위원회(억류자 조사 위원회)를 출범시켰다.

처음에는 정보 제공이 기존의 기밀 유지 의무와 충돌하지 않는 한 정부가 모든 관련 정보를 조사 위원회에 제공하도록 규정한 프로토콜이 마련되었다.[9] 이 프로토콜은 또 어떤 자료를 공개해도 되는지는 궁극적으로 내각 장관이 결정하도록 할 계획이었다. 이 조항의 목적은 국가 안보, 국제 관계, 국방, 경제와 관련된 정보의 부적절한 공개를 통해 공공복리가 훼손되지 않도록 하는 것이었다. 이러한 과정은 여기 다른 곳에서 논의한 캐나다의 세 조사 위원회가 사용한 과정과 뚜렷이 다른데, 정부의 정보 공개 반대에 관한 사법 심사 조항이 빠져 있기 때문이다. 몇몇 인권 단체들은 이 점과 그 밖의 제한을 감안해 조사 위원회 참여를 거부했다.

2012년 1월에 영국 정부는 조사 위원회가 업무를 시작하기 전에 (조사 위원회가 조사해야 하는 활동의 일부에 관한) 범죄 수사 결과를 기다려야 하는 관계로 조사가 계속 지연되자 조사를 중단시켰다. 이 광범위한 특별 조사는 탁월한 감독의 행사가 될 가능성이 있었지만 영국 정부의 이러한 임의적이고 일시적인 조치는 항구적인 감독 체계의 한계를 부각시켰을 뿐이다.

3. 외국 기관과의 정보공유 감독

외국 기관과의 정보공유는 일반적으로 감독 기구에 가장 큰 난제이자 인권 측면에서도 가장 큰 위험이 된다. 외국 기관에는 정보기관, 경찰 및 그 밖에 외교 대화 채널이 있는 외국 정부 부서가 포함될 수 있다. 또 이들 기관 중 하나 이상이 참여하는 초국가적 네트워크도 포함될 수 있다. 한 평론가는 중앙 집중화된 통제를 받을 수 있는 국내 정보공유와는 달리 "혼돈스러운 국

제 사회에서는…모든 나라가 프라이버시 규범이나 그 밖의 기본적 자유를 준수하지는 않는다. 따라서 프라이버시권은 네트워크의 각 정보기관의 처분에 맡겨져 있다"고[10] 말했다.

위험에 처한 다른 권리들에는 고문이나 그 밖의 잔인하고 비정상적이거나 모멸적 처우를 받지 않을 권리도 포함된다. 캐나다의 아라르 위원회가 밝혔듯이 "캐나다에서의 조사로 얻은 정보를 다른 나라와 공유할 경우, 캐나다 국경을 넘어 캐나다 내에서는 그 결과를 통제할 수 없는 '파급 효과'가 발생할 수 있다." [11] 최악의 시나리오를 가정하면 외국 기관에 보낸 정보가 사법 절차를 거치지 않은 해당 기관의 구금, 고문, 심지어 살해를 뒷받침하는 데 사용될 수도 있다. 반대로 외국 기관에서 받은 정보가 고문이나 기타 부정한 방법을 통해 얻은 것일 수도 있다.

정보기관과 경찰이 외국 기관이 제공한 정보의 획득에 사용된 출처와 방법을 잘 모르는 것은 당연하다. 이는 문제가 되는데, 사용된 출처와 방법이 정보의 신뢰성과 정보 수령 기관의 인권 존중 의무에 영향을 미치기 때문이다. 마찬가지로 정보를 제공하는 측은 외국 기관이 제공받은 정보를 어디에 사용할지에 관해 잘 모르는 경우가 많다. 정보 제공 기관이 공유된 정보의 사용을 제한하는 단서 조항을 붙이는 경우도 있지만 외국 협력 기관들로 하여금 그러한 제한을 준수하도록 할 방법이 없다. 국제적 정보공유는 때때로 국가 주권에 포괄되거나 정보의 출처, 방법, 용도의 비밀성을 보호할 필요성에 포함되기도 한다. 국내 감독 기구는 정보를 보내는 기관이나 받는 기관에 대한 관할권을 행사할 수 있지만 이 중 하나가 외국 기관이라면 양측을 모두 감독할 수는 없다. 따라서 실제로는 정보 교환의 한쪽 당사자만을 감독할 수 있다.

3.1 국제적 정보공유의 나쁜 관행

최근에 있었던 국제적 정보공유의 나쁜 관행 중 가장 악명 높은 사례는 마헤르 아라르 사건이다. 911 테러 이후 캐나다 왕립기마경찰(RCMP)의 현장 수사관들은 미국 정부 관리들과 수사 데이터베이스의 내용을 공유했다. 어떠

한 정보도 사전에 신뢰성이나 관련성이 검증되지 않았고, RCMP는 정보의 사용에 어떠한 제한도 두지 않았다. 나중에 캐나다의 한 조사 위원회는 미국에 의해 아라르가 구금되고 그 이후 시리아로 인도되어 고문을 받은 일련의 사건에서 이 정보가 일정한 역할을 했을 가능성이 있다고 결론 내렸다. 중요한 것은 이 위원회가 확실한 조사 결과에 도달하지 못했다는 점인데, 미국 정부와 시리아 정부 모두 조사에 협력하지 않았기 때문이다. 국가 주권 주장에 맞닥뜨리면 감독 기구가 비밀스러운 국제적 정보공유의 깊은 내막을 파헤치기 위해 할 수 있는 일은 거의 없다. 그럼에도 불구하고 아라르 위원회와 더불어 시리아, 이집트에 의한 캐나다인 3명의 구금 사건에 관한 후속 조사는 RCMP와 캐나다 보안정보국에서 시리아와 이집트 당국에 보낸 질문들이 시리아, 이집트 정보 요원들에 의한 구금자 고문의 한 원인이었음을 밝혀냈다.

이와 같은 조사 결과는 무엇을 피해야 하는지에 관한 중요한 교훈을 전해준다. 그것은 급박한 상황에 처해 있더라도 정보기관은 외국 협력 기관에 정보를 제공하기 전에 적절성을 검증해야 한다는 것이다. 또한 필요할 경우, 정보에 단서 조항을 첨부하고, 용도를 제한해야 한다. 나아가 심문관들이 고문이나 기타 인권 억압 행위를 하는 것으로 알려진 외국 협력 기관들에 질문 목록 등 후속 조사 요청을 보내는 것도 삼가야 한다.

3.2 정보기관의 국제적 정보공유의 모범 관행

국제적 정보공유와 관련하여 모범 관행이란 무엇일까? 우선 공유 기관들은 정보 협력 기관들에 관해 잘 알아야 할 것이다. 인권과 기본적 자유의 증진 보호 및 테러 방지에 관한 UN 특별 보고관은 “정보기관들이 정보공유 협정을 체결하거나 임시로 정보를 공유하기 전에 상대측에 적용되는 법적 안전장치와 제도적 통제 장치뿐 아니라 인권 및 정보 보호 실적에 대한 평가를 수행한다. 정보기관들은 정보를 건네주기 전에 공유되는 모든 정보가 정보를 받는 측의 위임사항과 관련이 있고, 부가된 조건에 부합하게 사용되며, 인권을 침해하는 목적으로 사용되지 않을 것임을 확인한다[해야 한다]”고12 권고했다. 특별 보고관의 이 권고는 정보기관을 상대로 한 것이지만 모범 관행에 따르게 하고 그렇지 못할 경우 구제책을 제공해야 할 의무가 있는 감독 기구와도 관련이 있다.

아라르 위원회는 RCMP가 시리아와 이집트 보안 기관과 정보를 공유하기로 했을 때 이들 기관의 관행에 대해 충분한 정보를 갖고 있지 않았음을 알아냈다. 일반적으로, 국제적으로 정보를 공유하는 기관 중 경찰이 외국 협력 기관의 관행을 판단하는 데 있어 전문성이 가장 떨어진다. 따라서 국제적으로 정보를 공유하는 국내 기관들은 잠재적 외국 협력 기관에 관해 현재 알고 있는 것들을 공통 데이터베이스로 만들고 유지하는 것이 현명할 것이다. 이렇게 하면 국내 기관들이 특정 정보공유에 관해 현명한 결정을 내릴 수 있다. 이런 방식은 정보를 보내는 것뿐 아니라 받은 정보를 평가하는 것과 관련한 의사 결정도 개선할 것이다. 앞서 인용한 캐나다 사례에서 잔인한 취조를 통해 얻은 정보는 나중에 법 집행, 정보, 외교 정책 관료들 사이에 널리 배포되었다. 아라르 위원회의 결론처럼 "상이한 기관들이 외국 정부로부터 받은 정보에 대한 상이한 평가에 근거해 일하도록 하는 것은 말이 되지 않는다."[13]

또 앞서 논의한 것처럼 정보기관들은 외국 기관에 제공하는 정보에 그 사용을 적절히 제한하는 단서 조항을 붙일 필요가 있다. 외국 정부가 이 단서 조항을 존중하리라는 보장은 없지만 적어도 신경을 쓸 가능성은 높일 수 있는 모범 관행들이 있으며, 그렇지 않더라도 이런 관행은 약속 위반을 바로잡을 가능성도 높일 수 있다. 아라르 위원회는 이와 관련하여 몇 가지 권고를 했다. 첫째, 단서 조항의 문언은 최대한 명확하고 정확해야 한다. 예를 들어 정보를 받는 정부가 그 "정보 공동체" 내에서 정보를 공유하는 것을 허용할 경우, 이런 모호한 개념 안에 많은 기관이 포함될 수 있기 때문에 정보를 받는 측의 위임 범위가 지나치게 광범위해진다. 둘째, 정보를 받는 정부가 공유된 정보를 형사 소송이건 입국이나 본국 송환과 관련된 소송이건 법적 소송에서 사용하는 것이 일반적으로 금지되어야 한다. 나아가 정보 수령 정부가 단서 조항을 수정하거나 남용을 보고하려 할 경우, 정보 제공 정부의 특정 관리에게 연락하도록 하는 단서 조항이 부가되어야 한다. 이는 이런 사안 발생 시 연락 대상을 두루뭉술하게 정보 제공 기관이나 정부로 하는 현재의 나쁜 관행을 대체하게 될 것이며, 개인의 책임성을 증진하게 될 것이다. 아라르 위원회에 따르면 "단서 조항은 단서 조항이 적용되는 정보의 사용 및

배포에 관한 명확한 의사소통이 이루어지는 적절한 채널을 구축하는 데 도움이 될 수 있다."[14] 마지막으로 정보 수령 기관이 정보 수령 국가뿐 아니라 정보 제공 국가의 법률이 부과하는 개인정보에 대한 통제를 존중할 것을 요구하는 단서 조항이 항상 포함되어야 한다.[15]

정보기관이나 보안 기관이 단서 조항 중 하나가 위반되었음을 알게 되는 경우, 즉시 위반 기관에 이의를 제기해야 한다. 남용의 심각성에 따라 정보 제공 기관은 기본적인 정보공유 협정의 정당성을 재검토해야 할 수도 있다. 동시에 감독 기구는 각각의 위반 사례와 정보 제공 기관의 대응을 알아야 한다. 감독 기구는 감독 대상 기관들이 단서 조항 존중을 요구하고 필요할 경우 적절한 구제책을 취하도록 하는 데 중요한 역할을 할 수 있다.

아라르 위원회의 조사 결과가 시사하듯 외국 기관에 질문을 보낼 때는 특별히 주의해야 하는데, 이로 인해 가혹한 취조가 사용될 가능성이 있을뿐더러 단서 조항을 통해 제재하기 훨씬 더 힘든 방식으로 외국 기관이 이 질문을 사용할 수도 있기 때문이다. 아라르 위원회는 "정보 제공이 고문 사용을 초래하거나 그에 원인 제공을 할 것이라는 믿을 만한 위험이 있는 외국에는 절대로 정보를 제공해서는 안 된다"고[16] 결론 내렸다. UN 특별 보고관도 비슷한 권고를 통해 감독 기구는 인권을 침해할 수 있는 행위에 특히 유의해야 한다고 강조했다. 또 UN 특별 보고관은 인권 규범 위반 행위에 참여하라는 명령을 받은 정보기관의 직원들은 그러한 명령을 거부하고 감독 기구에 이의를 제기할 수 있도록 허용되어야 한다고 권고했다.[17]

외국 파트너와의 정보공유는 위험이 수반될 뿐 아니라 심사 및 감독을 용이하게 하기 위해서도 항상 철저히 문서화되어야 한다. 캐나다 보안정보국법 17절은 공공안전부 장관에게 (외무부 장관과 협의하여) 외국 기관 및 정부와 협력 협정을 맺을 법적 권한을 부여하고 있다. 이러한 협정이 없으면 CSIS는 외국 기관에 합법적으로 정보를 제공할 수 없다. (다만 정보를 받을 수는 있다.)[18] 추가 부령(部令)에서는 RCMP가 정보 협력 기관과 구체적인 서면 협정을 맺도록 요구하고 있다. 이들 협정은 법적 (및 외국 기관의 경우에는 외교

정책적) 조언으로 보완되어야 한다. 그럼에도 아라르 위원회는 RCMP가 이 부령을 일상적 정보공유에 적용하지 않았음을 발견했다. 위원회는 서면 협정이 "지나치게 형식적이거나 길 필요는 없지만" 정보를 공유할 때 단서 조항과 인권을 존중할 필요성에 대한 기관들의 인식을 높일 수 있다고 결론지었다.[19]

정보기관이 미심쩍은 인권 기록을 보유한 외국 파트너와 협력 협정을 체결할 때는 감사 증적(audit trails)이 특히 중요하다. 아라르 위원회는 이런 파트너에게 정보를 제공할 때는 정보 제공 기관이 공유되는 정보와 공유 결정의 근거를 설명하는 문서 기록을 작성할 것을 권고했다.[20] 위원회는 나아가 인권 기록이 미심쩍은 나라로부터 정보를 받을 때도 비슷한 방법을 사용하라고 권고했다.

> *책임성 측면에서 의사 결정 과정을 문서로 명확히 설명하고 결정의 책임자들을 파악할 수 있는 것이 중요하다. 그뿐만 아니라 인권 기록이 미심쩍은 나라들로부터 정보를 받으려는 결정은 적절한 심의 기구의 심의를 받아야 한다.*[21]

3.3 기관 간 국제적 정보공유에서 감독 기관의 모범 관행

감독 기구가 감독 대상 기관이 공유하는 정보(정보가 비밀주의 적용 대상인지 여부에 상관없이)에 접근할 수 있는 것이 대단히 중요하다. UN 특별 보고관이 권고하는 모범 관행 중에는 "독립적 감독 기관은 정보공유 협정 및 정보기관이 외국 기관에 제공하는 모든 정보를 검토할 수 있다"는[22] 관행이 포함된다. UN 특별 보고관에 따르면 사실 "국가 법률에서 정보기관이 독립적 감독 기관에 정보공유를 보고하도록 명시적으로 요구하는 것이 좋은 관행이다."[23]

효과적 감독의 잠재적 장애물은 제3자 규칙으로서, 공유된 정보를 다른 기관("제3자")에 배포하는 것을 제한하도록 공유 정보에 부가된 공통적 단서 조항이다. 독일 등 일부 국가는 감독 기구에 공유 정보에 대한 접근권을 부여하지 않는데, 감독 기구를 제3자로 간주하기 때문이다.

제3자 규정의 이런 해석에 대한 확실한 대응은 해외 정보공유와 관련하여 감독 기구가 외국 정보를 받는 정보기관의 일부로 간주되어야 한다고 스스로 주장하는 것이다. 정보기관들은 그렇게 되면 외국 기관들이 정보공유를 꺼릴 것을 우려해 이러한 입장에 반발할지 모른다. 하지만 많은 경우 정보 수령 기관과 동일한 비밀주의 절차에 따르는 감독 기구들과 협력할 책임에 관해 외국 협력 기관들에 알려주도록 정보기관을 독려할 수 있다.

감독 기구는 정보기관들이 때때로 정보공유를 국내의 활동 제한을 피하는 수단으로 사용한다는 점도 유념해야 한다. UN 특별 보고관은 이 문제에 관해 ECHELON 신호 정보 시스템에 관한 유럽 의회 보고서를 토대로 모범 관행을 제안했는데, 구체적으로 "정보기관이 외국 정보기관의 도움을 이용해 국가의 법적 기준과 그 활동에 대한 제도적 통제를 피하는 것이 명시적으로 금지된다."[24]

끝으로 감독 기구는 감독 대상 정보기관에 권고하는 것과 동일한 모범적 정보공유 관행을 채택하고 장려해야 한다. 예를 들어 감독 기구는 외국 협력 기관의 인권 기록에 관해 알아야 한다. 마찬가지로 감독 기구가 감독하는 기관들이 외국 협력 기관과 공식적인 서면 협정을 맺도록 촉구해야 한다.

상자 3: 네덜란드 정보보안기관 심의위원회의 해외 정보공유 감독

2002년에 네덜란드 정부는 몇몇 정보기관의 운영을 심사할 관할권과 이러한 심사에 필요한 비밀 정보에 대한 접근권을 비롯하여 광범위한 정보 사안의 감독 책임을 갖는 상설 기구를 설립했다. 2009년에는 이 정보 보안 기관 심의 위원회가 2002년부터 2005년 중반까지 네덜란드의 단일 정보기관의 정책과 관행을 중심으로 네덜란드와 외국 기관들의 협력을 다룬 방대한 보고서를 발간했다.

이 보고서에 따르면 네덜란드의 해당 정보기관과 외무부는 인권 기록이 좋지 않은 외국 기관들을 포함해서 외국 협력 기관들이 적절한 정보공유 기준을 충족하는지 여부에 충분히 주의를 기울이지 않았다. 보고서는 또 네덜란드 정보기관들이 외국 협력 기관에 개인정보를 제공함으로써 불법적 행위를 저질렀다고 밝혔다. 보고서는 이들 기관에 불법적 목적으로 정보를 사용할 것으로 의심되는 외국 협력 기관과의 정보공유를 중단할 것을 권고했다.[25] 보고서는 또 외국 기관과의 정보공유 협정 체결을 결정하기 위한 체계적 과정을 마련하도록 권고했다. 이러한 협정은 주기적 심사 대상이 되며, 공유된 모든 개인정보를 서면 기록으로 보관하도록 의무화하게 될 것이다.[26]

3.4 네트워크를 통한 국제적 정보공유에서 감독 기구의 모범 관행

국제적 정보공유는 양자 간뿐 아니라 다자간에서도 이루어지므로 감독 기구는 네트워크를 통한 정보공유에 수반되는 문제점을 최소화하고 기회를 극대화할 수 있어야 한다. 예를 들어 개별 회원 기관들의 자체 평가에 의존하는 것보다 바람직한 방법으로 정보공유 네트워크에서 협력 기관들에 대한 인권 평가를 수행할 수 있다. 네트워크는 또 여러 정보 교환에 부가되는 인권 및 프라이버시 단서 조항의 집행과 관련하여 개별 기관들보다 더 큰 영향력을 행사할 수 있다.[27] 끝으로 네트워크는 회원 기관들에 우수 사례 기관들이 정한 기준을 맞추도록 요구함으로써 정보 신뢰성과 감독에 관련된 모범 관행을 확산시킬 수 있다.

유로폴과 베른 클럽이 관리하는 네트워크 등 유럽의 일부 정보공유 네트워크들은 실제로 높은 기준을 부과하고 있으며, 이는 유익한 것으로 입증되었다. 하지만 이들은 일부 국가에는 덜 공식적인 (그리고 심지어 사안별로 이루어지는) 양자간 정보공유에 의존할 것을 장려하기도 했다.[28] 이런 경향에 맞서려면 감독 기구는 다자간 네트워크 내에서의 정보공유의 이점을 강조하는 것과 동시에 보다 불투명한 양자간 협정에 따라 이루어지는 정보 교환에 면밀히 주의를 기울이는 양면적 접근 방식을 취해야 한다. 국내 정보기관과 정보를 공유하는 외국 협력 기관에 관한 정보를 얻기는 어려울 수 있지만 감독 기구는 이 정보를 획득해서 해외 정보공유 협정과 관행을 감시해야 한다.

개도국의 경우, 국제 정보공유 네트워크 가입으로 얻을 수 있는 자원은 가입 시 요구되는 일정한 인권 기준 준수 의무에도 불구하고 강력한 가입 유인이 된다. 감독 기구는 충족되어야 할 기준을 파악하고 감독 대상 정보기관들이 이를 충족하도록 촉구함으로써 네트워크 가입을 증진하는 데 중요한 역할을 할 수 있다.

4. 국내 기관과의 정보공유 감독

앞서 논의한 것처럼 911 테러 이후 여러 국가 정부는 정보공유 확대가 장래의 테러 공격 방지에 도움이 될 것이라고 믿어 정보, 경찰, 국경, 세관, 운송 관리 등 국내 협력 기관 간의 정보공유를 늘렸다. 가령 영국의 2008년 반테러법(Terrorism Act) 19절은 영국 정보기관에 정보공유와 관련하여 폭넓은 자유를 부여하고 있다. 이 조항은 구체적으로 누구에게나 정보기관에 정보를 공개할 권한을 부여했다. 또 직무의 적절한 이행, 중대 범죄의 예방 및 탐지, 형사 소추의 목적을 위해 필요할 경우에 정보기관이 정보를 공개할 권한도 부여했다. 이렇게 최근의 정보공유 확대 압력은 잠재적 안보 위협뿐 아니라 범죄 예방 및 범죄 수사와 관련된 정보 공개의 확대를 가져 왔다.

4.1 국내 정보공유의 문제점

감독 관점에서 볼 때 국내 협력 기관에 정보를 공개할 경우, 위에서 국제적

정보공유와 관련해 논의한 것과 동일한 우려가 상당수 제기된다. 그러나 특별히 국내 정보공유와 관련된 추가적 우려 사항도 있다. 이들 중 가장 중요한 것은 관할권의 한계 때문에 관련 감독 기구가 관련된 국내 기관 전부를 심사할 법적 권한이 없어서 국내 정보공유에 대한 효과적이고 조율된 심사가 불가능할 수 있다는 위험성이다. 이처럼 감독 권한이 결여되면 책임성이 희석되고 적절한 심사 없이 정보 교환이 이루어지는 공백이 생긴다.

정보기관들은 특별한 권한을 가지고 있기 때문에 각국 정부는 일반적으로 법 집행 기관보다 정보기관을 더 엄격히 감독한다. 책임성의 공백이 발생하는 경우, 이런 강화된 감독이 약해질 수 있다. 예를 들어 캐나다 정부는 마헤르 아라르와 그 밖의 캐나다인들이 시리아와 이집트에서 고문을 당한 사건과 관련하여 캐나다 관리들의 행위를 조사하기로 했을 때, 상설 조직인 보안 기관 심의 위원회의 감독 관할권이 시리아 및 이집트와의 정보공유에 연루된 경찰, 세관, 외무, 이민국 관리들에게 미치지 않는다는 것을 알게 됐다. 이에 따라 캐나다 정부는 책임성 공백을 메우기 위해 비상설 특별 조사 위원회를 설립해야 했다.

연방 제도 역시 위험한 책임성 공백을 초래할 수 있다. 예컨대 911 이후 미국에서는 연방, 주, 지자체 기관들 간 정보공유 증진을 위해 융합 센터가 만들어졌다. 옹호자들은 융합 센터에 참여하는 각 기관에 기존의 감독 체계가 계속 적용되므로 새로운 감독 메커니즘이 필요 없다고 주장했다. 하지만 이 주장은 실제적으로 정부의 한 층위와 관련된 감독 기구는 정부의 다른 층위의 기관들의 행위를 심사하는 데 필요한 관할권을 갖고 있는 경우가 드물다는 점을 간과한 것이다.[29]

4.2 국내 정보공유의 나쁜 관행

911 이후 국내 정보공유에서 특히 나쁜 관행은 비폭력적인 시위자들을 테러 용의자로 오인한 것이었다. 미국에서 이런 관행은 몇몇 융합 센터의 잘못이었다. 연방, 주, 지방 기관들이 제공하는 다양한 데이터베이스가 테러 위협 및 취약성과 관련된 전략적 정보와 합쳐진 후에 이런 오인이 발생했기 때문

에 참여 기관들은 신뢰할 수 없는 정보에 대해 몰랐다고 주장하거나 다른 기관을 탓한다. 일부 융합 기관은 감독 기구에 정보가 어떻게 조합되었는지 설명하는 기록을 제공하기를 거부해 문제를 더 악화시켰다.[30] 이런 요인들이 합쳐져 융합 센터와 그 지원 기관에 행위의 책임을 묻기가 매우 어려워진다.

더 일반적으로 정보 네트워크와 네트워크에 속하는 기관들은 잠재적으로 신뢰성이 떨어지는 정보의 무차별적 공유를 줄일 필요가 있다. 캐나다에서는 외무부가 외국 기관으로부터 얻은 신뢰할 수 없는 정보가 그 신뢰성 문제를 간과한 채 이후 국내 정보기관 및 법 집행 기관에 유포되었다. 심지어 이 정보는 수색 영장 신청의 근거로도 사용되었다. 이렇듯 국내 정보공유의 나쁜 관행은 해외 정보공유에 내재한 위험을 증폭시킬 수 있다.

4.3 국내 정보공유의 모범 관행

모범적인 국내 정보공유 관행은 융합 센터와 정보 교환을 촉진하는 기타 기관들이 보유하고 공유하는 정보를 추적하는 영구적 기록을 관리하는 데서 시작된다. 이러한 기록 관리와 이를 통해 가능한 감사 증적 없이는 국내 정보공유의 감독이 불가능하지는 않더라도 어려워질 것이다.

국제적 정보공유에서처럼 국내 정보공유에서도 단서 조항은 좋은 관행인데, 특히 공유되는 정보가 법 집행과 관련해 사용되는 경우에 그렇다. 공유 기관은 공유되는 정보가 법 집행 목적에 사용될 수 있을 만큼 신뢰할 수 있는 정보인지, 또 해당 기관이 그러한 목적으로 정보를 공유할 법적 권리를 갖고 있는지 신중히 고려해야 한다. UN 특별 보고관은 각국이 국내 정보공유의 법적 근거를 제정할 필요성을 강조했다. 영국의 2008년 반테러법 19절은 그와 같은 사례 중 하나다.

법적 근거의 제정은 입법자들에게 현재 감독 메커니즘의 적절성을 검토할 기회를 주며, 어쩌면 현재의 감독 체계를 수정할 기회를 제공할 수도 있다. 일례로 캐나다 감독 체계의 법적 근거를 살펴본 아라르 위원회는 다양한 감독 기구가 국가 안보 활동을 검토할 때 비밀 정보를 공유하고 협력할 수 있

도록 하는 "법적 관문(statutory gateways)"을 만들 것을 캐나다 입법부에 권고했다. 이 위원회의 권고는 감독은 감독 대상 활동에 뒤처지지 않아야 한다는 건전한 원칙에 근거한 것이었다. 달리 말해 정보공유의 법적 승인이 확대된다면 심의 권한 또한 확대되어야 한다는 것이다.

평론가들은 감독 기구가 국내 정보공유 네트워크의 확산에 발맞추려면 명확한 형식의 "네트워크 책임성"이 필요하다고 주장했다. 권고 사항에는 모든 공유 정보의 기록 및 보존(감독 기구가 조작이 힘든 감사 증적을 수집할 수 있도록)과 융합 센터 내 시정 메커니즘의 구축(부정확한 정보의 유포와 프라이버시권 침해를 시정할 수 있도록)이 포함된다.[31] 다른 평론가들은 특히 미국의 감찰관들이 감독 대상 기관들의 정보공유 관행을 공동 조사할 필요성을 역설했다.[32] 캐나다의 아라르 위원회도 비슷한 취지에서 911 이후 중요한 새 보안책임을 맡게 된 다수의 정보기관들이 포함되도록 감독 기구의 관할권을 확대할 것을 권고했다.[33] 벨기에에서는 각각 경찰과 정보기관을 감독하는 별개의 기구들의 정보공유가 이미 허용되고 있고, 몇 건의 공조 수사가 시행되기도 했다.[34]

이러한 폭넓은 감독 체계가 없는 경우, 보안 정보공유에 관여하는 여러 국내 기관들의 행위를 조사하고자 하는 정부는 아라르 위원회 같은 특별 조사 위원회를 설립해야 하는데, 복수 기관의 행위를 심사하는 데 필요한 권한을 갖고 있는 기존의 감독 기구가 없기 때문이다. 하지만 특별 조사 기구의 임명은 재량적이고 예외적이기 때문에 의미 있는 심사를 수행할 충분한 권한을 보유한 상설 감독 기구를 대신하지는 못한다. 이런 이유에서 아라르 위원회는 캐나다 정보기관과 법 집행 기관의 행위를 심사하는 상설 감독 기구에 보안 정보를 공유하는 여러 기관의 행위를 심사할 권한을 더 크게 부여할 것을 권고했다. 안타깝게도 이 권고와 정부가 공동 감독을 위한 법적 경로를 만들어야 한다는 권고(두 가지 모두 2006년에 이루어진 권고이다)는 아직 이행되지 않았다.[35]

미국에서는 현재 보안 정보공유에 참여하고 있는 복수의 국내 기관들을 조사할 권한을 상설 책임 기구에 부여하기 위한 몇 가지 진전이 있었다. 일례로 국방부, 법무부, 중앙정보국, 국가안보국, 국가정보국의 감찰관들은 영장 없는 도청에 관해 공동 조사를 시행했다.[36]

상자 4: 호주 정보기관 국정 조사에 의한 국내 정보공유 심의

호주는 안보 문제 및 정보공유에 대한 새로운 범정부적 접근 방식에 맞는 정보기관 감독의 채택에서 중요한 진전을 이뤄냈다. 2006년에 호주의 한 정보기관 조사 위원회는 전문가 감독 기구인 감찰관 및 관련 의회 공동 위원회의 위임 사항을 확대해 모든 국내 정보기관들의 행위를 감독할 수 있도록 할 것을 권고했다.[37]

이 권고는 국내 정보기관들의 정보공유 확대까지는 인식했지만 국내 정보기관들과 다른 국내 기관들 간의 정보공유에는 상대적으로 관심이 부족했다. 이런 결함은 2010년에 호주 의회가 모든 연방 부서 또는 기관 내의 보안 및 정보와 관련된 모든 사안을 조사할 권한을 감찰관에게 부여하는 법률을 제정함으로써 시정되었다.[38] 하지만 한 가지 측면에서 새로운 법률은 기대에 못 미쳤다. UN 특별 보고관이 자체 심사에 착수할 수 있는 감독 기구의 권한의 중요성을 강조했음에도 불구하고 호주의 새로운 법률은 총리의 위임을 통해 감찰관의 권한을 확대하도록 하는 데 그쳤기 때문이다.[39]

한편 호주는 국가 안보 및 정보공유에 관련된 법 집행 기관의 행위를 심사할 새로운 의회 위원회를 설립했다. 또 정보기관 감독을 맡는 의회 공동 위원회의 규모도 늘렸다.

5. 권고 사항

다음 권고 사항의 목적은 국내 및 국제적 정보공유에 대한 감독을 촉진하는 것이다. 이 권고 사항들은 입법부와 행정부의 감독 기구만이 아니라 감독 대상 정보기관과 안보 위협에 대한 범정부적 대응에 관련된 그 밖의 다양한 조직들에도 적용된다.

정보공유는 이루어져야 하지만 법적으로 승인되고 프라이버시권 등 인권을 존중하는 가운데 이루어져야 할 것이다. 이를 보장하는 중요한 수단은 911 이후 더욱 증가하고 있는 국내 및 국제적 정보공유에 뒤처지지 않는 데 필요한 법률적 자원과 기타 자원을 감독 기구에 제공하는 것이다.

정보공유에 관한 내부 지침 개발

정보기관들은 정보공유 관행에 적용할 일련의 원칙을 고안해야 한다. 이 원칙들은 법률이나 정책의 형식으로 서면으로 명시되어야 한다. 이 원칙들은,

- 인권 존중(고문 공모 방지 포함)과 프라이버시 관련법 존중(개인정보 공유 포함)을 의무화해야 한다.

특히 이 원칙들은 정보 교환이 고문의 실행을 초래하거나 그에 원인을 제공할 믿을 만한 위험이 있을 때는 정보공유를 금지해야 한다.

- 공유된 정보(제공하는 정보건 받는 정보건)의 관련성, 신뢰성, 정확성 및 프라이버시와 인권에 미치는 영향에 대한 심사를 요구해야 한다.
- 제공되는 정보에 단서 조항을 부가할 필요성과 수령하는 정보에 다른 기관이 부가한 단서 조항을 존중할 필요성을 인정해야 한다. 이러한 단서 조항의 목적은 공유된 정보가 부적절한 목적으로 사용되거나 국내법 또는 국제법에 위배되게 사용되지 않도록 하는 것이다.
- 다른 기관에 보낸 잘못된 정보를 수정하고 다른 기관으로부터 받은 정보의 신뢰성에 대한 독립적 평가를 시행할 지속적 의무를 인정해야 한다.
- 공유 기관 내의 책임성과 감독 기구에 대한 책임성을 증진하는 방식으로 정보를 공유한다는 약속이 포함되어야 한다. 즉 공유된 정보는 서면으로 기록되어야 하며, 감사 증적에는 정보 교환의 인가 과정과 후속 조치의 설명이 포함되어야 한다. 정보공유가 이러한 인가 없이 가령 현장 차원이나 급박한 상황에서 이루어진 경우, 될 수 있는 대로 빨리 명확하게 해명해야 한다.

정보기관들은 이러한 원칙을 훈련 프로그램에 포함시키고 감독 기구와 이를 공유해야 한다. 또 국가 안보상 기밀 유지 관련 우려가 없다면 이를 일반에

공개해야 한다. 정보기관이 이런 원칙을 개발하지 못하는 경우, 감독 기구가 유사한 원칙을 개발해 감독 업무에 활용해야 한다.

정보에 입각한 정보기관 내 정보공유 방식 개발

정보기관들은 정보를 공유하는 상대국의 인권 기록을 추적하는 데이터베이스를 유지해야 한다. 이 데이터베이스는,

- 국제 및 지역 인권 보호 단체와 믿을 만한 시민 사회 단체가 제기한 인권 침해 혐의를 포함하여 광범위한 공개 정보를 포함해야 한다.
- 외무 부처와 협의하여 개발되어야 한다.
- 정보기관 인력 훈련에 사용되어야 한다.
- 국가 안보상 기밀 유지 관련 우려에 부합하게 일반에 공개되어야 한다.

감독 기구는 이러한 데이터베이스에 접근할 수 있어야 하며, 이를 검토하고 필요 시 보완, 업데이트해야 한다. 정보기관이 이런 데이터베이스를 만들지 않는 경우, 감독 기구가 만들어야 한다.

국제적 정보공유 협정 개발

정보기관은 외국 협력 기관과의 정보공유에 적용되는 서면 협정을 개발해야 한다. 이 협정에는 정보 제공 및 수령 양측의 인권 관련 의무를 명시해야 한다. 또 받은 정보를 기관의 주요 감독 기구 및 가능한 경우, 동일한 기밀 유지 보충 협약에 합의한 관련 감독 기구들과 공유할 수 있도록 하는 표준 조항도 포함되어야 한다. 이런 협정을 작성하는 과정에서 정보기관은 법률적 조언과 외교 정책적 조언을 얻어야 한다.

감독 기구는 이러한 모든 협정이 체결되거나 개정되는 시점에 협정의 사본을 받아야 한다. 감독 기구는 각각의 협정을 의무적으로 검토하되 가능한 경우에는 협정 조건의 준수를 측정하는 무작위 감사를 시행해야 한다. 이러한 감사는 이전의 관행들을 고려하여 협정을 개정할 필요가 있는지 결정하는 데 도움이 될 수 있다.

공유 정보에 부가된 단서 조항 위반 보고 및 해결

정보공유 협정에는 정보 제공자 측이 공유 정보에 부가한 단서 조항의 위반을 보고하고 단서 조항 위반으로 인한 분쟁을 해결하는 구체적인 절차가 포함되어야 한다. 정보 제공 기관이 위반 사실을 알게 되면, 정보 수령 기관에 정식으로 항의해야 한다. 정보 제공 기관은 또 이를 해당 정보공유 협정을 재검토하고, 가능하면 수정하는 기회로 삼아야 한다. 이러한 절차는 정보를 수정하거나 업데이트하고, 구체적인 사건별로 또는 시간 경과에 따라 단서 조항의 개정을 제안하는 데에도 사용될 수 있다.

위반이 발생하는 경우(또는 위반 혐의만 있는 경우에도), 정보기관은 감독 기구에 통보해야 한다. 이러한 통보에는 기관이 취했거나 제안하는 일체의 개선 조치 기록이 포함되어야 한다. 감독 기구는 모든 개선 조치를 검토하고 의견을 제시해야 하며, 위반이 위반 당사자와의 향후 정보공유에 어떤 영향을 미칠지 전반적인 문제도 고려해야 한다.

공유된 정보의 불법적 사용 보고 및 해결

정보기관들은 공유된 정보가 특히 인권 침해와 관련하여 불법적으로 획득되었거나 불법적으로 사용되었거나 불법적으로 사용될 수 있음을 알게 되는 경우, 감독 기구에 통보해야 한다. 이러한 통보에는 기관이 취했거나 제안하는 일체의 개선 조치 기록이 포함되어야 한다. 감독 기구는 모든 개선 조치를 검토하고 의견을 제시해야 하며, 불법성이 위반 당사자와의 향후 정보공유에 어떤 영향을 미칠지 전반적인 문제도 고려해야 한다.

국내 정보공유 협정 개발

정보기관들은 국내 협력 기관과의 정보공유 서면 협정을 개발해야 한다. 이러한 협정은,

- 명확한 법적 권한이 있어야 한다.
- 인권 준수뿐 아니라 단서 조항도 다뤄야 한다.
- 분명한 감사 증적을 규정해야 한다(공유된 모든 정보의 항구적 기록과 정보 제공 기관 및 수령 기관의 서면 승인 포함).

- 관련 감독 기구가 국내 정보공유를 어떻게 심사할지를 다뤄야 한다.

이런 협정을 구성할 때 정보기관은 특히 프라이버시 및 정보공유에 대한 기타 법적 제한과 관련하여 법률적 조언을 얻어야 한다. 법률 조언에서는 정보기관의 감독 기구가 갖고 있는 관할권이 정보공유 관행 심사에 충분한지도 다뤄야 한다.

이들 협정은 책임 문제를 다룰 때 정보 제공 기관과 정보 수령 기관이 서로 다른 감독 체제의 감독을 받을 경우에 발생할 수 있는 문제점을 예상하고 해결해야 한다. 감독 기구는 가능하면 항상 정보공유 관행의 효과적 심사에 필요한 모든 정보에 접근할 수 있어야 한다. 그러려면 국내 감독 기구들이 공동으로 심사를 수행하고 서로 정보를 공유할 수 있는 추가적인 법적 권한이 필요할 수 있다. 또 감독 기구들이 평소 관행보다 더 엄격한 보안 및 비밀 유지 조치에 따라야 할 수도 있다.

후주(後註)

1. 여기서 *정보기관*이라는 용어는 국가 안보 관련 정보를 수집, 분석하고 의사 결정권자에게 전파하는 것이 주 임무인 정부 기관을 의미한다. 이 정의는 Aidan Wills, *Guidebook: Understanding Intelligence Oversight,* Toolkit －Legislating for the Security Sector (Geneva: DCAF, 2010), p. 10에서 취한 것이다.

2. BBC News, "Libya: Gaddafi regime's US-UK spy links revealed," September 3, 2011 (available at http://www.bbc.co.uk/news/world-africa-14774533).

3. James Walsh, "Intelligence-Sharing in the European Union: Institutions Are Not Enough," *Journal of Common Market Studies* Vol. 44, Issue 3 (September 2006), pp. 625–643.

4. Elizabeth Sepper, "Democracy, Human Rights and Intelligence Sharing," *Texas International Law Journal* Vol. 46 (2010), p. 155.

5. Ernest R. May (ed.), *The 9/11 Commission Report* (New York: St. Martins Press, 2007), Section 3.2.

6. Commission of Inquiry into the Investigation of the Bombing of *Air India Flight 182, Air India Flight 182: A Canadian Tragedy* (2010).

7. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006); and Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (2008).

8. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), p. 331.

9. Detainee Inquiry, "Protocol for the Detainee Inquiry" (2011) (available at http://www.detaineeinquiry.org.uk/key-documents/protocol/).

10. Francesca Bignami, "Toward a Right to Privacy in Transnational Intelligence Networks," *Michigan Journal of International Law* Vol. 28, No. 3 (Spring 2007), p. 674.

11. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), p. 431.

12. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,* United Nations Document A/HRC/14/46 (17 May 2010), p. 46.

13. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), p. 349.

14. Ibid., p. 342.

15. Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practices for Oversight of Intelligence Agencies* (Geneva: DCAF, University of Durham, and Parliament of Norway, 2005), p. 45.

16.Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), p. 345.

17.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,* United Nations Document A/HRC/14/46 (17 May 2010).

18.Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (2008), p. 82.

19.Commission of Inquiry into the Actions of Canadian Officials in *Relation to Maher Arar, Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), p. 322.

20.Ibid., p. 347.

21.Ibid., p. 348.

22.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,* United Nations Document A/HRC/14/46 (17 May 2010), p. 48.

23.Ibid., p. 49.

24.Ibid., pp. 49 – 50.

25.The Netherlands, Review Committee on the Intelligence and Security Services (CTIVD), *Review Report on the cooperation of the GISS with foreign intelligence and/or security services,* CTIVD No.22A (12 August 2009) (available at http://www.ctivd.nl/?English), Section 14.2.

26.Ibid., Sections 14.6 and 14.15.

27.Francesca Bignami, "Toward a Right to Privacy in Transnational Intelligence Networks," *Michigan Journal of International Law* Vol. 28, No. 3 (Spring 2007), pp. 683 – 684.

28.Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (2008), p. 68.

29.Danielle Citron and Frank Pasquale, "Network Accountability for the Domestic Intelligence Apparatus," *Hastings Law Journal* Vol. 62 (2011), p.1441.

30.Ibid.

31.Ibid.

32.Philip Heymann and Juliette Kayyem, Preserving Liberty in the Face of Terror (Boston: MIT Press, 2005); Kent Roach, "Review and Oversight of National Security Activities and Some Reflections on Canada's Arar Inquiry," *Cardozo Law Review* Vol. 29, Issue 1 (October 2007), pp. 53 – 84.

33.Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006).

34. Ibid., pp. 333 – 334.

35.Kent Roach, *The 9/11 Effect: Comparative Counter- Terrorism* (Cambridge: Cambridge University Press, 2011), pp. 416 – 420 and 455 – 459.

36.Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and O ffice of the Director of National Intelligence, *Unclassified Report on the President's Surveillance Program* (10 July 2009).

37.Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies* (Canberra: Government of Australia, 2004).

38.Australia, National Security Legislation Amendment Act No. 127 of 2010, schedule 9; see also Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge: Cambridge University Press, 2011), pp. 354 – 356.

39.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,* United Nations Document A/HRC/14/46 (17 May 2010).

도구 8

정보기관의 재정 감독

에이단 윌스(Aidan Wills)

8. 정보기관의 재정 감독

에이단 윌스(Aidan Wills)[1]

1. 머리말

민주국가에서는 의회가 공공 기관들이 기능을 수행하고 법적 위임 사항을 이행할 수 있도록 재정 자금을 할당한다. 그 다음 의회는 다른 감독 기구들과 연계하여 이 자금의 사용이 합법적이고 효율적인지 감시한다. 모든 공공기관은 이 과정에 따라야 하며 정보기관도 예외는 아니다.

이 도구는 민주적 정치 조직이 예산 편성부터 지출의 사후 심사까지 정보기관의 재정을 어떻게 감독하는지를 비교해 개관한다. 그 목적은 모범 관행을 부각시키는 것이다. 이 도구에는 다음 여섯 개 절이 포함된다.

- *정보기관 재정 감독의 중요성*
  외부 감독이 중요한 이유 설명
- *정보 예산*
  정보 예산에 대한 상이한 접근 방식 개관
- *내부 재정 통제 및 감사 메커니즘*
  외부 감독을 보다 효과적으로 만드는 통제와 메커니즘 개관
- *의회의 감독*
  정보 예산 수립, 집행 감독, 기관 지출의 합법성과 효과성 심사에서의 의회의 역할 논의
- *최고 감사 기구*
  정보기관 재정 감사에서의 최고 감사 기구(SAI)의 역할 논의
- *권고 사항*
  정보기관 재정 감독과 관련된 모범 관행의 모음

지면상 제약으로 이 도구에서는 정보기관 재정 감독에서 행정부, 감찰관, 검찰, 사법부가 하는 역할은 다루지 않는다.

이 도구에서는 “재정 감독”을 폭넓게 정의하여 “통제”(도구 1 참조)의 행사로도 볼 수 있고 감독 대상 재정 활동 이전, 도중 또는 이후에 이루어지는 기능들까지 포함시킨다.

2. 정보기관 재정 감독의 중요성

정보기관 재정의 외부 감독은 다음 네 가지 이유에서 중요하다.

- 민주적 거버넌스의 원칙은 공공 자금의 할당과 사용을 면밀히 조사할 것을 요구한다.
- 재정 기록을 통해 정보기관의 행태와 성과를 잘 파악할 수 있다.
- 정보기관의 비밀주의는 기관 활동을 조사할 수 있는 일반 대중의 능력을 제한한다.
- 정보 업무의 성격으로 인해 공공 자금의 오용 위험 등 다양한 재정 위험이 생겨난다.

2.1 공공 자금 사용과 관련된 민주적 거버넌스

보편적으로 받아들여지는 민주적 거버넌스의 원칙은 공공 자금은 공공의 것이므로 그 지출은 선출된 국민의 대표(즉, 의회)에 의해 승인되어야 한다는 것이다. 의회는 예산권을 통해 공공의 의지가 반영된 정부 기관의 정책과 우선순위를 형성한다. 똑같이 중요한 것은 의회와 의회에 보고하는 독립적 기구(SAI 등)에 의해 공공 지출이 사후 심사되어야 한다는 것이다. 사후 심사의 목표는 무엇보다도 다음을 보장하기 위해서다.

- 원래 지출이 승인된 용도에 공공 자금이 사용되었다.
- 지출 시 관련법(공공 자금 관리에 관한 법, 공공 조달에 관한 법, 부패 방지법, 관련 기관[예: 정보기관] 활동의 준거법 등)을 준수한다.
- 지출이 정부 정책에 부합했다.
- 설정된 목표를 효과적으로 달성함으로써 지출에 상당하는 가치(value for money)를 제공했다.

이 원칙들은 정보기관을 포함한 모든 정부 기관에 똑같이 적용되지만 일부 국가의 경우, 정보기관을 공공 자금 지출을 규제하는 특정 법의 적용 대상에

서 명시적으로 배제하고 있다. 미국의 중앙정보국(CIA)이 그런 예이다.[2] 이런 경우 면밀한 검토가 특히 중요하다.

2.2 행태 및 성과 지표로서의 재정 기록

공공 기관의 재정은 일반적으로 기관의 활동과 성과에 관해 많은 것을 보여준다. 기관은 돈을 쓰지 않고서는 직무를 거의 수행할 수 없다. 따라서 기관의 재정 기록에는 감춰진 활동의 단서가 포함되어 있을 때가 많고 그 활동 중 일부는 불법적일 수도 있다. 정보기관의 경우, 비밀 구금 시설의 운영이나 국내 정당에 대한 비밀 자금 지원 같은 불법 활동이 기관의 재정 기록에서 드러날 수 있다. 마찬가지로 어떤 부서의 예산선(budget line)이 비정상적으로 높다면 해당 부서의 성과 부진을 나타내는 것일 수 있다. 그러므로 감독 기구는 기관의 재정 기록을 검토함으로써 기관의 업무 중 추가 조사가 필요할 수 있는 면면을 파악할 수 있다.

2.3 비밀주의와 공공 감시의 한계

정보 업무는 이례적으로 높은 수준의 비밀주의를 필요로 하기 때문에 정보기관 재정은 다른 정부 기관과 동일한 정도로 공개되지 않는다. 재화 및 용역 입찰 분야에서의 비밀주의는[3] 국가 보유 정보에 대한 공공의 접근을 규제하는 대부분의 법률에서 정보기관이 제외됨으로써 더욱 심화되는데, 그로 인해 언론과 그 밖의 시민 사회 조직이 획득할 수 있는 관련 정보의 양이 제한된다. 공공의 감시가 이렇게 제한됨을 감안하면 기밀 정보에 접근할 수 있는 외부 감독 기구가 정보기관의 재정을 면밀히 조사하는 것이 특히 중요하다.

2.4 정보 업무에서의 재정 위험 관리

정보 업무의 특정 측면들은 공공 자금이 비효과적이거나 부적절하게 사용될 위험을 고조시킨다. 이런 측면들의 상당수 역시 정보기관 감독을 매우 까다롭게 만드는 요소이다.

2.4.1 불확실한 결과

정보기관들은 정책 결정권자의 국가 안보 수호를 돕기 위해 정보를 수집한다.

기관들은 이 기능을 수행하기 위해 돈을 쓴다. 하지만 정보기관은 그렇게 쓰인 돈이 원하는 정보를 산출하리라고는 절대 확신하지 못한다. 가령 어떤 기관이 외국 정보원을 채용하는 데 많은 돈을 쓰고도 이 정보원이 가진 정보의 가치가 보잘것없음을 알게 될 수도 있다. 이러한 위험은 정보 업무에 고유한 것이지만 내부 통제와 외부 감독을 통한 관리로 공공 자금 낭비를 최소화할 수 있다.

2.4.2 무형의 편익

정보 업무의 재정비용은 유형적인 경우가 많지만 그것이 산출하는 편익은 무형적일 때가 많다. 캐나다 감사원이 밝혔듯이 "정보수집, 평가, 보고의 결과와 특히 그 궁극적 효과는 본질적으로 측정이 어렵다."[4] 업무의 목표가 테러 공격 같은 사건이 일어나지 않게 하는 것일 때는 더욱 그렇다. 지식과 경험이 충분한 감독 기구만이 정보 업무의 무형적 편익을 제대로 평가할 수 있고, 적절한 지출 상당 가치가 있는지 판단할 수 있다.

2.4.3 비밀주의와 공공 자금 남용

정보기관들이 업무 세부 사항과 정보원의 신원 같은 민감한 정보를 기밀로 유지하는 데 신경을 쓰는 것은 당연하다. 따라서 정보기관은 기관 직원들 사이에서도 가능한 한 소수의 사람만 알도록 이 정보에 대한 접근을 차단한다. 하지만 정보를 아는 사람이 적을수록 공공 자금이 잘못 사용될 위험은 커진다. 예컨대 정보원에 관한 정보가 정보원을 "운용(running)"하는 정보관으로 한정되는 경우, 정보관들이 존재하지 않는 "유령 요원들"을 만들어 이들에게 지급될 돈이라면서 자금을 횡령할 수도 있다. 정보원들이 실재하는 경우에도 비밀주의 규정 때문에 정보관들은 별로 들킬 염려 없이 정보원에 할당되는 돈을 착복하기가 더 쉬워진다.

2.4.4 이해 충돌

정보관들은 업무의 일환으로 정보 제공이나 감시를 위한 주택 사용에 대한 대가로 비밀리에 사람들에게 돈을 지불하는 경우가 있다. 누구에게 얼마의 금액을 지불할지는 대체로 정보관(그리고 아마도 상관)의 재량일 때가 많다. 이는 잠재적 이해 충돌을 초래하는데, 정보관의 결정은 정보 제공자의 공로

뿐 아니라 개인적 관계, 그리고 거래의 비밀스러운 성격을 감안할 때 정보 제공자에 대한 정보관의 신뢰 정도에 근거할 가능성이 높기 때문이다. 그 결과 일부 정보관은 단지 아는 사이라는 이유로 정보원을 쓸 수도 있다. 또 정보 제공자와 친하다는 이유로 과도한 액수를 지불할 수도 있다. 일부의 경우지만 정보관들이 뇌물을 받을 수도 있다(상자 1 참조).

상자 1: 카일 포고(Kyle Foggo) 사건

카일 포고는 한때 CIA 고위 정보관으로 일했다. 그가 맡았던 직무 중에는 비밀 해외 구금 시설 구축 등 매우 민감한 업무를 위한 재화와 용역의 조달이 포함되어 있었다. 포고는 이들 시설 일부의 자재 조달을 위해 CIA가 그의 친한 친구와 연계된 회사와 계약하도록 주선했다. 나중에 검찰은 이 회사와 여러 건의 계약을 맺게끔 포고가 조종했고, 제공된 재화와 용역에 부풀려진 가격을 지불하게 했음을 알아냈다. 그 대가로 포고는 호화판 휴가와 향후 채용 약속 등의 선물을 받았다. 포고는 동료들에게 이 관계를 숨기기 위해 자신이 신뢰할 수 있는 회사로부터 재화 및 용역을 구매해야 했으며, 관료주의적인 표준 구매 절차를 피하고 싶었다는 주장을 내세워 이 회사를 이용한 것을 정당화하려 했다. 결국 포고는 부패 혐의를 인정했고, 징역형을 선고 받았다.[5]

2.4.5 가처분 자산 및 수입과 관련된 위험

정보기관들은 업무의 일환으로 상당량의 가처분 자산을 구매한다. 예를 들어 작전 도중 부유한 목표물과 어울리기 위해 값비싼 차량을 구입하거나 비싼 호텔을 이용할 수 있다. 정보관들은 이런 값비싼 물건이 더 이상 필요 없어진 후에도 개인 용도로 보유하거나 아는 사람에게 넘기거나 팔아서 돈을 챙기는 등 이익을 보려고 할 수 있다. 이러한 자산이 비밀리에 조달되었다는 것은 그 위험성을 증가시킨다. 마찬가지로 일부 정보기관들은 비밀 활동을 은폐하기 위한 "유령" 회사를 설립할 수도 있다. 이런 회사 중 일부에서 수입이 발생할 수 있는데, 관련된 정보관들이 수입을 불법적으로 챙길 위험이 있다. 이런 위험 때문에 감독 기구는 정보기관의 지출뿐 아니라 기관 자산과 수입도 감시해야 한다.

2.4.6 정치적 목적을 위한 정보기관 이용

정보기관 자금의 남용은 정보기관을 담당하는 행정부 구성원에게도 미칠 수 있다. 이런 관료들은 때때로 공공 자금 지출과 관련된 불법적인 정치적 목적을 위해 기관의 자원을 사용해 왔다. 따라서 감독 기구는 기관 관료들의 행태뿐 아니라 이들과 행정부 관료들의 상호 작용에도 초점을 맞춰야 한다.

3. 정보 예산

*예산*이란 다음 기간(일반적으로 회계연도)의 수입과 지출을 상세히 밝힌 항목별로 분류된 문서이다. 따라서 예산은 공공 기관의 업무를 지휘하고 통제하는 주요 도구인데, 기관들이 일을 하려면 자금이 필요하기 때문이다. 민주국가에서 예산은 보통 입법의 일부로서 의회가 제정한다.

일부 국가의 정보기관은 조직적 자율성과 자체 예산을 가지고 있다. 정보기관이 부처 내에서 운영되는 나라들도 있는데, 프랑스 내무부 안에 있는 프랑스 정보기관(la Direction Centrale du Renseignement Intérieur)이 그런 예다. 후자의 경우, 정보기관이 자체 예산을 갖고 있지 않다. 그 대신 소속된 부처의 예산 하에서 자금을 받는다. 따라서 *정보 예산(intelligence budget)*이라는 용어에 혼동이 있을 수 있는데, 어떤 때에는 단일한 기관의 예산을 가리키기도 하고, 어떤 때에는 단일 부처 내의 복수 기관들의 예산을 가리키기도 하기 때문이다. 이 용어가 몇 개 부처에 걸쳐 있는 전체 정보 공동체의 예산을 모두 합친 것을 지칭할 수도 있다. 몇몇 나라에서는 정보기관과 관련된 모든 지출이 그 예산에 포함되지는 않는다는 점에도 유의해야 한다. 특히 연금 지출과 사무 용품 같은 항목은 국가 예산의 다른 부분에 포함될 수 있다. 이런 탓에 정보기관의 전체 예산을 계산하기가 어려울 수 있다.

기관의 조직적 위상은 예산 심사에 영향을 미치기 때문에 중요하다. 일반적으로 외부 감독 기구는 부처 내에서 운영되는 정보기관보다 자율적 기관으로 설립된 정보기관의 재정을 더 직접적이고 상세하게 검토할 수 있다. 자율적 기관의 재정은 다른 부처의 재정과 엮이지 않기 때문이다.

정보 업무 수행 여부에 상관없이 정부 기관의 예산은 "포괄적(comprehensive)"이어야 한다. 세계은행은 이 용어를 예산이 "모든 재정 운영을 포괄해야 한다"는[6] 의미로 사용한다. 다시 말해 정부 기관의 예산에는 해당 기관과 관련된 재정 활동 전부가 포함되어야 하는 것이다.[7] 특히 정보기관은 이 요건을 준수해야 하는데, 일부의 경우, 법률로 승인받지 않은 활동을 위한 자금 조성이나 지출의 전력이 있기 때문이다. 일례로 1980년대 중반에 CIA는 니카라과 콘트라 반군 지원을 위해 이란에 대한 무기 판매로 얻은 수입을 사용한 적이 있다.

3.1 예산 주기

*예산 주기(budget cycle)*라는 용어는 돈이 요청되고, 할당되고, 지출되는 완결적 과정을 가리킨다(그러한 지출에 대한 사후 심사 포함). 예산 주기에는 네 가지 주요 단계가 있다.

- 편성 - 주무부처, 정부 부서 및 기관들이 계획된 수입과 지출을 결정한다.
- 검토 및 승인 - 의회가 예산을 수정하고 제정한다.
- 집행 - 기관이 예산에 상세히 나와 있는 계획을 집행한다.
- 사후 심사 - 감독 기구가 기관의 자금 사용을 조사한다. 그 다음에 해당 연도 정부 계정의 "책임 해제(discharge: 승인 및 종결)"를 위한 의회 표결이 있을 수 있다.[8]

정보기관 예산도 편성 과정은 다른 정부 부처 및 기관의 예산과 동일하지만 검토 및 승인, 집행, 사후 심사(이 도구의 5-6절에서 논의) 과정은 다르다.

3.2 예산 방식

전통적인 예산에서 사용하는 품목별(line-item) 방식은 특정 액수(투입)를 정책 목표나 산출에 연결시키지 않고 비용 또는 예산선(budget line)에 할당한다. 이 투입 기반 방식과 대조적으로 여러 나라(프랑스 등)에서는 이제 자금 할당을 정책 목표와 궁극적으로는 기대성과(desired outcome)에 연결시키는 "성과" 또는 "결과 기반" 예산 방식을 사용하고 있다.[9] 예산 방식은 사후 감

독에 중요한 의미가 있다. 결과 기반 예산 방식에서는 투입과 산출이 연결되기 때문에 이후에 효율성과 지출 상당 가치 같은 요소를 포함하여 예산 집행을 평가하기가 더 용이하다. 반면 투입 기반 예산 방식은 예산 집행을 평가할 틀을 제공하지 않는다.

3.3 정보 예산 공개

필자가 알기로는 정보기관들의 예산 전부를 공개하는 정부는 없다. 대부분의 나라에서 기밀 분류된 예산 세부 사항은 일반 대중뿐 아니라 이 분야의 기밀 정보를 다룰 권한이 있는 위원회에 소속되어 있지 않은 의원들에게도 제공되지 않는다.

정보 예산의 비밀주의는 예산 정보 공개가 적국에 이로울 수 있다는 정보기관의 우려 때문이다. 하지만 공개되는 정보에 특정 목표물, 방법 또는 정보 출처와 관련된 세부 사항이 포함되는 경우에만 그럴 가능성이 크다. 대부분의 경우, 현재 공개되는 것보다 훨씬 많은 정보를 공개하더라도 국가 안보는 위태로워지지 않는 반면 투명성은 크게 높일 수 있다.

일반적으로 민주 국가들이 선택하는 정보 예산 공개 방식은 세 가지 중 하나다. (영국 같은[10]) 일부 국가는 국가의 전체 정보 공동체에 할당되는 총액만을 공개한다. (독일 등) 다른 나라들은 각 정보기관의 개별적 총액을 공개한다. 분명 이 두 방식 모두 (공공 토론에 유용한 정보가 될) 할당된 자원과 구체적 정책 목표 간의 관계는 공개하지 않는다. (예컨대 호주와 프랑스가 채택하고 있는) 세 번째 방식은 특정 목표에 할당되는 구체적 액수를 공개하는 것이다. 예를 들어 프랑스의 대외 정보기관인 DGSE(Direction Générale de la Securité Exterieure)의 공개 연간 예산은 승인된 인건비, 운영비, 투자 지출을 따로 열거하며, 승인된 특별 업무 활동*(les fonds spéciaux)* 총액도 공개된다.

(호주와 프랑스처럼) 성과 예산을 채택하는 정부들은 일반 대중이 예산과의 연관성을 알 수 있도록 정책 목표와 기대성과도 공개할 수 있다.[11] 예를 들어 2010년 DGSE 예산의 일반 공개 버전은 핵심 정책 목표를 "DGSE의 정보수

집 및 분석 능력 향상"으로 확정하고 이 목표를 달성할 수단으로 2009년부터 2015년까지 690명의 추가 직원 채용 계획을 꼽았다.[12]

최대한 많은 예산 정보의 공개(세 번째 방식이 다른 두 방식보다 낫다)는 몇 가지 이유에서 사회에 유익하다. 첫째, 자신의 돈이 어떻게 사용되는지 알 대중의 권리를 존중한다. 둘째, 투명성을 높임으로써 일반 의원(즉 이 분야의 기밀 정보에 접근할 권한이 있는 위원회 소속이 아닌 의원들), 언론, 심지어 일반 대중도 정보기관의 자금, 정책, 우선순위에 관한 공공 토론에 유의미하게 참여할 수 있게 된다. 활발한 공적 논의는 정부로 하여금 지출 우선순위를 정당화하지 않을 수 없게 만들며, 궁극적으로는 공공 자금의 보다 효율적인 사용을 증진할 수 있다. 끝으로 공개 토론은 정보기관에 대한 공공의 신뢰를 강화하여 정보 지출의 목적에 관한 근거 없는 믿음을 일소하고 경우에 따라서는 정보 자금의 증가를 가져올 수도 있다.

얼마나 많은 예산 정보를 공개할 것인지에 관한 결정을 행정부에게만 맡겨두어서는 안 된다. 의원들은 입법을 통해 어떤 재정 정보를 비밀로 할 것이며 공개해야 할 정보는 무엇인지 규제해야 한다. 얼마나 많은 예산 정보를 공개하느냐에 상관없이 정보 예산의 조사, 수정, 승인에 관여하는 의회 위원회가 예산의 기밀 부분을 포함한 모든 관련 정보에 접근할 수 있는 것이 중요하다(5.1절 참조).[13]

4. 내부 재정 통제 및 감사 메커니즘

이 도구는 정보기관 재정 감시에서 외부 감독 기구가 하는 역할에 초점을 맞추고 있지만 정보기관 내에 존재하는 내부 재정 통제에 관한 몇몇 논의가 없이는 설명이 불완전해질 것이다. 이러한 메커니즘 없이는 외부 감독이 효과적일 수 없다.

4.1 회계

법률은 일반적으로 정보기관을 포함한 모든 정부 기관이 재정 기록을 잘 정돈되고 정확하게 보관하고 모든 관련 규정을 준수하도록 보장하는 회계 담

당관을 지정할 것을 요구한다(상자 2 참조). 회계 담당관이 기관의 장일 때도 많은데, 그런 경우에는 기관의 모든 재정 거래를 기록하고 보고하는 일상적 업무를 처리하는 재무부서의 지원을 받는다. 재무부서 역시 자원이 적절히 사용되도록 하는 재정 통제를 구축하고 유지한다.

상자 2: 남아공의 회계 담당관 관련법

이 상자는 정부 기관(정보기관 포함)의 내부 재정 통제를 규율하는 남아공의 1999년 공공재정관리법의 몇몇 조항을 발췌한 것이다. 이 법에 따라 남아공 회계 담당관에게는 소속 기관이 모범 재무 관행을 채택하도록 할 광범위한 책임이 있다.

남아공 정부의 모든 기관은 다음을 책임지는 회계 담당관을 두어야 한다.

1. 기관의 효과적이고, 효율적이며, 투명한 재정 위험 관리 체계 및 관련 규정에 따라 운영되는 감사 위원회가 통제하는 내부 감사 제도 유지
2. 기관 자원의 효과적, 효율적, 경제적이고 투명한 사용
3. 기관 자산의 보호를 포함한 기관 자산과 부채의 관리
4. 기관 지출의 관련 예산 입법 준수

이 법은 나아가 회계 담당관에게 승인되지 않거나 변칙적이거나 낭비적인 기관 지출을 방지하고 필요할 경우, 그에 대응할 책임도 부과한다. 이러한 지출이 발견될 경우, 회계 담당관은 즉시 지출의 세부 사항을 재무부에 서면으로 보고해야 하며, 재화나 용역의 조달과 관련된 변칙적 지출의 경우에는 관련 입찰 위원회에 보고해야 한다. 또 회계 담당관은 기관의 재정 관리 체계를 손상시키거나 승인되지 않거나 변칙적이거나 낭비적인 지출을 한 (또는 하도록 허가한) 모든 관료에게 적절한 징계 조치를 취해야 한다.

회계 담당관은 기록 관리와 관련하여 규정된 규범과 기준에 따라 기관의 완전하고 적절한 재정 기록을 보존해야 한다.

외부 감독 기구의 업무에는 적절한 내부 회계가 필수적인데, 이것이 없이는 최고 감사 기구와 그 밖의 이러한 기구들이 거래와 관련 활동을 재구성하기가 극히 어렵기 때문이다. 일반적으로 정보기관의 회계의 질은 그 재정 기록이 공정하고 진실한지를 보여 주는 지표이다.

4.2 재정 관리 지침

모든 정부 기관처럼 정보기관들도 일련의 서면 지침을 통해 재정 관리와 회계 절차를 공식화한다. 보통 기관의 장이나 행정부가 공표한 후 외부 감독 기구가 평가하는 이 지침은 기관 직원들의 행위의 평가 기준이 되는 규제 체계의 일부를 구성한다.

일반적으로 재정 관리 지침에 포함되는 사안은 다음과 같다.

- 수입 발생 및 지출은 누구에 의해, 어떤 과정을 통해 승인되는가? 지침은 이 질문에 대한 답을 통해 재정 거래의 책임과 책임성의 한계를 명확히 해야 한다.
- 기관 자금의 허용 가능한 사용은 무엇인가? 이 질문에 대한 답은 관련 입법과 일치해야 한다.
- 재정 거래는 어떻게 이루어져야 하는가? 지침은 예컨대 정보 요원들이 현금을 사용할지 혹은 전자 지불을 해야 하는지에 관해 조언해야 한다.
- 어떤 재정 기록을 관리해야 하는가? 적절한 기록 관리는 차후에 사용할 수 있는 감사 증적을 구축하기 때문에 중요하다. 다만 미국 등 일부 나라에서는 정보기관이 몇몇 민감한 업무(예: 해외 정보 업무)와 연관하여 "무증명 계정(unvouchered account)"(행정부 구성원 1인의 확인서만으로 해명되고 완전한 영수증 일체로 뒷받침되지 않는 지출)을 사용하는 것을 법률로 허용한다.[14]

4.3 재정 보고

정보기관을 포함한 공공 기관은 보통 법률에 따라 그 재정 거래에 관한 상세한 연간 보고서를 작성해야 한다.[15] 이러한 보고서가 없으면 외부 감독 기구가 기관의 재정과 활동을 심사할 수 없다.

일반적으로 정보기관은 이 보고서를 행정부, 최고 감사 기구, 의회에 제출한다. 하지만 정보 예산과 마찬가지로 이들 보고서가 제공하는 세부 사항의 양은 달라질 수 있다.

공개할 예산 정보와 공개하지 않을 예산 정보를 행정부가 단독으로 결정하도록 해서는 안 되는 것처럼 재정 보고에 포함시키기에 적합한 정보가 무엇이고 비밀로 해야 할 정보가 무엇인지도 행정부가 결정하도록 해서는 안 된다. 그보다는 의회가 입법을 통해 어떤 재정 정보는 공개해야 하고 어떤 정보는 비밀을 유지해야 하는지를 규율하는 상세한 기준을 만들어야 한다(상자 3 참조).

정보 예산과 관련하여 호주와 프랑스는 이 점에서 모범 관행을 보여 준다. 이 나라들의 정보기관은 공개용으로 비교적 상세한 재정 보고서를 작성한다. 호주 안보정보원(ASIO)의 공개 보고서에는 인건비, 물품비(재화 및 용역 포함), 감가상각/할부 상환 비용 등의 지출 범주별 소계도 포함된다. 보고서에는 자체 수입, 자산 매각, 정부 수입 같은 소득 범주의 소계도 포함된다. [16] 프랑스 법에서는 정보기관의 재정 보고서에 각각의 기관 사명별로 상세한 부록을 포함시키도록 요구한다. 이 부록들에는 재정 데이터뿐 아니라 정책 목표와 예산 주기 시작 시 정한 기대성과에 대한 평가도 포함되어야 한다.[17]

상자 3: 뉴질랜드 법률상의 재무 보고

이 상자는 1984년 공공재정법과 1969년 보안정보기관법의 일부 조항을 발췌한 것으로서 이 두 법은 뉴질랜드 정보기관들의 재정 보고서 작성 방식을 규율한다. 여기서는 정보기관에 대한 요건과 다른 공공 기관에 대한 요건을 비교한다.

뉴질랜드의 공공 기관들(정보기관 포함)은 매 회계연도 종결 후 조속히 이전 회계연도의 재정 보고서를 작성해 주무장관에게 제출해야 한다. 보고서에는 기관 운영에 관한 정보 및 기관 성과 보고뿐 아니라 완전한 재정 데이터가 포함되어야 한다. 일반적으로 보고서는 이전 회계연도 동안의 기관의 성과, 특히 연초에 정한 기관의 목표, 지표 및 기준과 관련된 성과를 정확히 평가하기에 충분한 정보를 제공해야 한다.

대부분의 공공 기관과 관련하여 법률은 주무장관이 보고서를 수령한 다음 의회에 제출하고, 그 후 조속히 공개하도록 규정하고 있다. 하지만 정보기관의 보고서인 경우에는 달리 처리된다. 주무장관은 전체 보고서를 의회 본회의에 제출하는 것이 아니라 위원들이 기밀 정보를 조회할 수 있는 의회 정보보안위원회에만 제출한다. 의회 본회의를 위해 주무장관이 작성하는 수정판 보고서에는 총 지출 보고가 포함되어야 한다. 이후에 장관이 공개하는 보고서는 바로 이 수정판 보고서이다.

예산 정보와 관련해 위에서 언급한 것과 동일한 이유로(3.3절 참조) 정보기관들은 업무 기밀이나 국가 안보를 위험에 빠트리지 않는 한도에서 최대한 상세한 재정 보고서의 공개용 버전을 작성해야 한다.

5. 의회의 감독

이 절에서는 예산 주기의 마지막 세 단계, 즉 검토 및 승인, 집행, 사후 심사에서 의회가 하는 감독 역할에 초점을 맞춘다. 정보기관의 업무에는 민감한 사안들이 관련되어 있지만 의회는 정보기관 재정을 다른 공공 기관의 재정

과 동일한 수준으로 검토해야 한다. 유일하게 양보할 점이 있다면 감독 메커니즘을 더 신중하게 사용해야 한다는 것뿐이다.

정보기관에 대한 의회의 감독 대부분은 비공개로 이루어질 필요가 있다. 그러나 의원들이 공개 보고서와 공청회를 통해 감독 업무에 관해 일반 대중에게 알리는 것은 여전히 중요하다(도구 3 참조). 투명성은 의회의 감독에 대한 공공의 신뢰뿐 아니라 정보기관의 업무에 대한 신뢰도 증진하기 때문이다.

5.1 예산의 검토 및 승인

대부분의 민주 국가에서 의회는 행정부가 제안하는 기관 예산을 검토, 수정, 승인한다.

이런 과정에서 정보기관 예산이 제외되어야 할 타당한 이유는 없다.

의회는 기밀 정보를 보호하기 위해 예산의 기밀 부분을 검토할 특별한 메커니즘을 만들 수 있다. 하지만 어떤 메커니즘을 사용하건 항상 본회의에서는 정부 예산 승인의 일환으로 정보기관 예산 승인에 관해 표결이 이루어져야 한다. 본회의 표결은 예산 위원회나 정보 감독 위원회 또는 특별 기밀 위원회 또는 그 조합에 의한 전면적 검토에 추가되는 것이어야지 이를 대체해서는 안 된다.[18]

5.1.1 예산 위원회

일부 의회는 표준 예산 (또는 지출 승인) 위원회를 이용하여 정보기관의 재정을 검토한다. 이들 위원회는 조사 위원(rapporteur)이라고 하는 특정 기관, 부처 또는 임무를 담당하는 위원을 지명할 수 있다. 이런 조사 위원들은 보통 전체 위원회의 기관 예산 논의, 수정, 승인에 기초한 권고 사항이 담긴 보고서를 작성하는 것이 일반적이다.

예산 위원회는 전체 행정부 예산이라는 방대한 맥락 내에서 정보기관 예산을 평가하기가 여러 모로 유리하다. 하지만 전문 조사 위원이 없으면 위원회

위원들에게 정보기관의 예산을 제대로 검토할 수 있는 시간이나 주제별 전문성이 없기 십상이다. 예산 위원회는 기밀 정보에 충분히 접근할 수 없어 기관 예산 검토 능력이 더욱 제한되는 경향도 있다.

5.1.2 정보기관 감독 위원회

정보기관 감독 위원회는 보통 다른 의회 구성원들은 접근할 수 없는 기밀 정보에 접근할 수 있다(도구 2, 도구 3 참조). 이 위원회는 일반적으로 재정을 포함한 정보기관 활동의 사후 심사에 초점을 맞춘다. 하지만 일부 국가에서는 그 책임이 예산 검토 및 승인까지 확대된다. 헝가리 의회의 국가안보위원회는 정보기관 예산안을 검토하고 그에 관한 의견을 제시한다. 여기에는 의회 본회의에는 공개되지 않는 예산의 기밀 부분에 관한 검토도 포함된다.[19] 더 복잡한 미국 의회의 과정은 상자 4에 설명되어 있다. 다른 나라(예컨대 독일, 상자 5 참조)에서는 정보기관 감독 위원회가 부차적 역할을 하며, 주 책임이 예산 검토인 다른 위원회(예산 위원회 또는 지출 승인 위원회)에 조언한다.

정보기관 감독 위원회는 정보기관의 활동, 절차, 정책을 잘 알고 있기 때문에 정보기관 예산을 검토하고 이해하기에 유리하다. 하지만 이러한 검토의 효과는 다음과 같은 몇 가지 요인에 좌우된다.

- 위원회의 자원, 조사 권한 및 기밀 정보에 대한 접근 권한
- 위원회 위원들의 시간적 여유, 보좌진, 직무 수행 전문성
- 위원회 위원들의 직무 수행 의지
- 예산 과정에 영향을 미칠 수 있는 위원회의 능력(특히 그 역할이 조언인 경우)

상자 4: 미국 정보기관 예산에 대한 의회 심의 및 승인 [20]

미국 의회의 정보기관 예산 검토 및 승인 과정에는 무려 8개의 위원회와 소위원회가 관여한다. 이 과정은 승인(authorization)과 지출 승인(appropriation)이라는 두 가지 구별되는 측면을 가지고 있다.

승인

의회의 수권 법안은 대통령이 서명 시 예산을 포함한 정부 기관들의 활동을 규율한다. 정보기관 예산의 경우, 승인 과정은 행정부가 의회에 제출하는 예산안에서 시작된다. 예산안은 하원에서 정보특별상임위원회(Permanent Select Committee on Intelligence)와 군사위원회(Armed Services Committee)의 심사를, 상원에서 정보특별위원회와 군사위원회의 심사를 거친다. 이들 위원회는 예산 내에서 금액을 재할당할 수 있고, 특정 활동을 금지하고 새로운 사업을 포함시킬 수도 있다. 상하 각 원의 위원회들이 수권 법안을 최종 확정하면 본회의에 상정해 표결에 부친다. 상하 양원에서 승인된 수권 법안은 다시 원내에서 조정, 승인된 다음 대통령에게 보내 서명을 받는다.

각각의 정보 수권 법안에는 각 기관이 금액을 수령할 수 있는 활동의 범주와 자금을 사용해야 하는 목적이 열거된 기밀 분류된 부록이 포함된다. 이런 방식으로 수권 법안은 (법률로 가결되고 나면) 정보기관의 지출의 한계를 설정한다. 그러나 수권법은 승인된 프로그램이 정말로 자금 지원을 받게 될지 보장하지 않는다. 최종적인 자금 지원 결정은 지출 승인 과정에서 이루어진다.

지출 승인

지출 승인 입법은 다른 나라의 예산 입법과 유사하다. 즉 국고 자금을 기관이나 프로그램에 할당하는 것은 법률 문서다. 하원 세출위원회와 상원 세출위원회에는 거의 모든 미국 정보 공동체의 예산에 대한 관할권을 갖는 국방 소위원회가 있다. 이들 소위원회는 행정부로부터 받은 예산안을 기초로 정보기관 지출 승인 법안을 작성한다.

일반적으로 지출 승인 법안은 기존의 수권법을 준수해야 하지만 특정 정보 프로그램의 자금을 증액하거나 감액할 수 있다. 그러한 법률이 존재하지 않는 경우에는 지출 승인 법안에 모든 정보활동에 대한 포괄적 승인 조항을 포함시킬 수 있다.

수권 입법과 마찬가지로 지출 승인 법안도 복잡한 승인 과정을 거쳐야 한다. 소위원회의 승인을 받은 다음 전체 위원회의 승인을 받고, 그 다음에는 상하 각원의 본회의에서 가결되어야 하며, 그 후 다시 상하 각원에서 조정, 승인된 다음 최종적으로 대통령의 서명을 받아야 한다.

올바른 상황에서는 상당한 예산 책임을 가진 정보기관 감독 위원회가 (다른 관련 위원회와 협력 하에) 승인 권한을 이용하여 예산안에 기관의 효과성, 효율성, 법률 준수 개선에 관한 이전의 위원회 권고 사항이 반영되도록 할 수 있다.

5.1.3 특별 기밀 위원회

의회가 세 번째 메커니즘인 특별 기밀 위원회를 활용하여 정보기관 예산을 검토하는 경우도 있다. 이 메커니즘의 모범 사례는 독일 하원이 창설한 기밀 위원회(Confidential Committee)다(상자 5 참조).

상자 5: 독일 하원의 기밀 위원회 [21]

독일 의회의 하원인 Bundestag는3개 연방 정보기관과 관련된 예산 문제를 하원이 만든 특별 기밀위원회에 회부한다. 이 위원회는 하원의 예산공공회계위원회가 다른 공공 부서 및 기관과 관련해 수행하는 것과 동일한 기능을 한다. 즉 행정부의 예산안을 검토하고 수정할 수 있으며, 그 집행을 심사한다. 이 상자에서는 위원회의 검토 및 승인 기능에 초점을 맞춘다.

위원회 위원 선정

기밀 위원회의 위원 10명은 하원의 정당 의석수에 따라 비례적으로 배정된다. 후보자는 기밀 취급 인가가 필요 없지만 이른바 "총리의 과반수(chancellor's majority)"에 의해 선출되어야 하는데, 하원의 과반수 투표를 얻어 의회의 신뢰를 얻었음을 보여 주어야 함을 뜻한다.

정보기관 예산의 검토 및 승인

위원회의 정보기관 예산 검토 및 승인 과정은 다음과 같다.

1. 행정부가 각 정보기관의 상세한 예산을 위원회에 제출한다.
2. 위원회는 부처 관료 및 기관 고위층과 회의를 갖고 예산안을 논의한다.
3. 위원회는 하원 정보기관 감독 위원회와 협의한다.
4. 위원회는 행정부에 예산을 반환하기 전에 적절하다고 생각하는 수정을 하고, 행정부는 일반적으로 이런 변경을 받아들인다.
5. 위원회 위원장은 예산위원회에게 각 기관에 할당되는 총액을 알린다. 그러면 예산위원회는 이들 수치를 (토론 없이) 예산 권고안에 포함시킨다.
6. 의회 본회의는 전체 정부 예산에 관해 표결한다.

조사 권한 및 정보 접근

법률은 기밀위원회에게 정보기관 통제 하의 모든 파일과 문서를 심사하고 모든 기관의 부지를 점검할 수 있는 능력 등 강력한 조사 권한과 기밀 정보에 대한 광범위한 접근권을 부여한다. 위원회는 기관 관리와 행정부 구성원의 답변을 강제할 수 있으며, 필요할 경우, 외부 전문가들에게 업무 지원을 위탁할 수 있다.

5.2 예산 집행 감시

공공 기관의 예산이 승인되고 나면 의회는 예산이 적절히 집행되도록 기관의 지출을 감시할 책임이 있다. 정보기관의 경우, 감시는 보통 기밀 정보에 접근할 특권이 있는 의회의 정보기관 감독 위원회(또는 특별 기밀 위원회)에 의해 수행된다. 하지만 실제로는 특정 프로그램이나 활동과 관련된 위법 행위 혐의가 제기된 경우에만 정보기관 감독 위원회가 재정 정보를 요청하는 경향이 있다. 대부분의 의원들에게는 일 년 내내 방대한 재정 정보를 상세히 검토할 시간이나 자원이 없기 때문이다.

이런 한계 때문에 의회가 수행하는 집행 감독은 보통 행정부와 정보기관들이 선제적으로(즉 요청 없이) 공개하는 정보에 의존한다. 사실 많은 민주 국가의 관련 법률에서는 행정부 및 (또는) 정보기관들이 주기적으로 기관 재정을 공개하도록 규정하고 있다.[22] 가령 이탈리아는 총리가 6개월마다 정보기관 예산 집행에 관해 의회공화국안보위원회(COPASIR)에게 보고하도록 하고 있다.[23]

의회는 회계연도 도중 발생하는 추가 자금 요청도 고려해야 한다. 정보기관의 경우, 이 요청은 테러 공격 같은 예상치 못한 사건과 관련이 있을 수 있다. 다른 집행 관련 사안과 마찬가지로 이런 요청의 검토는 의회 정보기관 감독 위원회에 위임되는 것이 일반적이다. 예컨대 스페인에서는 추가 자금 요청을 비밀자금위원회가 심의하며, 그 의견은 본회의 표결에 영향을 미친다.[24]

5.3 재정의 사후 심사

공공 기관 재정의 사후 심사는 주로 각 기관의 내부 감사 메커니즘(4절 참조)과 국가 최고 감사 기구(6절 참조)가 담당한다. 그렇더라도 의회는 이 과정에서 감사관들의 업무를 검토하고 자체 조사를 수행함으로써 일정한 역할을 한다. 이 과정이 끝날 때 일부 의회는 예산 집행의 "책임 해제(discharge)" 법률을 통과시킨다(즉 주어진 기간 동안의 정부 계정을 공식적으로 승인).

5.3.1 의회의 사후 심사 메커니즘

공공 기관 재정의 사후 심사를 수행하는 의회의 공공 회계 또는 공공 감사

위원회(PAC)는 보통 정보기관 재정의 사후 심사는 담당하지 않는데, 사안의 민감성 때문이다. 그 대신 많은 의회는 정보기관의 재정을 심사하기 위한 특별한 장치를 두고 있다. 가령 영국의 경우, 정보기관에 관한 감사원(영국의 최고 감사 기구)의 보고서와 의견은 공공회계위원회 위원장에게만 제출된다.[25] 심사의 일차적 책임은 정보보안위원회에 있으며, 이 위원회의 위임 사항에는 정보기관 예산의 사후 심사가 포함된다(상자 6 참조). 독일 등(상자 5 참조) 다른 나라에서는 기밀 정보가 포함된 예산 및 계정과 관련된 의회의 업무를 수행하기 위한 전담 위원회를 두고 있다.

상자 6: 사후 심의에서 영국 정보 보안 위원회의 역할

영국 의회의 정보보안위원회(ISC)에는 양원의 의원들이 포함된다. 그 위임 사항은 정보 보안 기관들의 "정책, 행정, 지출"을 감독하는 것이다.[26]

ISC는 이 위임 사항에 따라 감사원(NAO)이 작성하는 감사 의견과 보고서를 주된 기초로 삼아 **기관** 재정의 사후 심사를 수행한다. 이 과정의 일환으로 ISC는 NAO 대표자 및 기관 고위 관리층과 함께 NAO 감사를 논의하는 청문회를 개최한다.

ISC는 자체 연례 보고서에 기관 재정 평가를 포함시킨다.[27] ISC는 먼저 보고서를 총리에게 제출하**지만 그** 후 보고서가 공개된다.[28] 뿐만 아니라 ISC는 중요한 재정적 영향이 있는 기관 활동 면면의 조사 업무에 언제든 배정될 수 있는 조사관을 채용한다.[29]

5.3.2 사후 심사 과정과 목표

정보기관 재정의 사후 심사는 보통 최고 감사 기구 보고서에 초점을 맞춘다. 사후 심사를 담당하는 의원들은 정보기관이 작성하는 연례 보고서와 재무제표도 검토한다.[30] 최고 감사 기구 감사관, 행정부 관료, 정보기관 관리층이 증언하는 청문회는 이 과정의 중요한 부분이다.

사후 심사의 주된 목표는 다음 사항을 파악하는 것이다.[31]

- 정보기관들이 예산 주기 시작 시 의회가 승인한 대로 예산을 집행했는가
- 관련 법률과 정책에 따라 공공 자금을 사용하고 내역을 설명했는가

- 정보기관들이 효과적이고 효율적으로 업무를 수행했는가
- 예산 주기 시작 시 설정한 정책 목표를 달성했는가(성과 예산을 사용하는 경우)

심사 과정이 끝날 때 심사를 수행하는 의원들은 기관의 재무 관행 및 통제 메커니즘 개선을 위한 권고 사항이 담긴 보고서를 발간할 수 있다. 법률에서 의회 전체 차원의 예산 책임 해제를 요구하는 나라들(예: 프랑스, 독일, 헝가리)의 경우, 이러한 보고서는 본회의 표결에 영향을 미칠 수 있다.

사후 심사는 장래 예산에 대한 의회의 승인에도 영향을 미친다. 사실 의원들은 사전 예산 권한을 이용해 행정부와 정보기관이 사후 권고를 받아들이도록 강제할 수 있다. 이 수단은 예산의 사전 승인과 집행의 사후 심사 간의 연계가 강한 경우에 가장 효과적이다. 이를 가장 잘 달성할 수 있는 방법은 의회 위원회 한 곳이 이 두 가지 기능을 모두 맡도록 하는 것일 것이다(독일의 경우처럼, 상자 5 참조). 또는 예산의 사전 검토를 담당하는 위원회와 예산의 사후 심사를 맡는 위원회 간 합동 위원회 회의나 그 밖의 정보공유 형식을 통해 조정을 강화할 수도 있다.

5.3.3 최고 감사 기구 보고서 요청

(프랑스, 미국 같은) 일부 나라의 의회는 최고 감사 기구에 특정 프로그램이나 지출의 조사 또는 특정 투자가 제공하는 지출 상당 가치의 평가를 지시할 수 있다.[32] 이런 방법으로 의회에 권한을 주면 최고 감사 기구의 업무가 의회 감독 위원회의 업무를 뒷받침하도록 하는 데 도움이 될 수 있다. 그 반면 최고 감사 기구에 과중한 부담을 주고 그 업무가 정치화될 가능성이 있다(예컨대 영향력 있는 의원들이 최고 감사 기구에 당파적 이유에서 사안의 조사를 지시하는 경우). 따라서 프랑스에서는 법률로 의회가 할 수 있는 요청의 건수를 제한하여 감사원(Court of Audit)이 한 건 이상의 요청을 거부할 수 있는 여지를 남겨 둔다. 마찬가지로 독일의 법률은 의회가 연방회계검사원(FCA)에게 요청하는 것은 허용하되 FCA의 조사를 강제할 수 있는 의회의 권한은 부인함으로써 FCA의 독립성을 보존한다.[33]

6. 최고 감사 기구

모든 민주 국가에는 정보기관을 포함한 공공 기관 감사를 담당하는 일정 형태의 자율적 최고 감사 기구가 존재한다. 최고 감사 기구는 정보활동의 재정적 측면에 주력하지만 정부 서비스의 다른 측면에도 감사가 확대될 수 있다. 다양한 유형의 최고 감사 기구에 관한 전면적 논의는 이 도구의 범위를 벗어나지만 간략하게 최고 감사 기구가 두 가지 넓은 범주에 속한다는 점은 지적할 수 있다. 즉 (프랑스 감사원 같은) "법원" 모형과 (영국 감사원과 미국 회계감사원 같은) "관청" 모형이다. 구체적인 형태야 어떻든 간에 최고 감사 기구는 정보기관 재정의 사후 심사를 담당하는 주요 외부 기구인 것이 보통이다. 이 절의 논점은 두 가지 형태의 최고 감사 기구에 모두 적용된다.

6.1 독립성

최고 감사 기구가 효과적으로 기능하기 위해서는 행정부와 모든 감사 대상 기관으로부터 완벽히 독립적이어야 한다. 실제로 UN 총회는 최고 감사 기구의 독립성의 중요성을 인정하는 결의안을 통과시켰다.[34] 구체적으로 최고 감사 기구는 다음을 필요로 한다.

- *조직적 독립성*
  최고 감사 기구는 법률에 의해 자체 예산이 있는 자율적 기관으로 설립되어야 한다.
- *운영상 독립성*
  최고 감사 기구는 감사 대상과 시기, 방법 및 그러한 감사에 근거한 결과와 권고 사항을 자유롭게 결정할 수 있어야 한다. 감사관의 업무는 어떠한 기구의 간섭으로부터도 보호되어야 한다.
- *인적 독립성*
  인적 독립성이란 감사관 자신들의 직위를 가리킨다. 최고 감사 기구의 고위 관료는 적절한 전문성을 갖추고 있으면서 감사관 직위를 손상시킬 수 있는 관계나 이해관계로부터 독립적인 사람이 선정될 수 있도록 임명되어야 한다. 이는 후보자가 의회와 행정부 모두의 지지를 받을 수 있는 투명하고, 포괄적이며, 성과에 기반을 둔 과정을 요한다. 임명된 감사관들은 고정된 임기를 보장하고 감사 결과가 현 행

정부에 호의적이지 않은 경우에도 보복으로부터 감사관들을 보호할 수 있는 그 밖의 수단을 통해 독립성이 보장되어야 한다. 끝으로 고위 감사관들은 독립성을 훼손하거나 이해 상충으로 인식될 수 있는 정치적 또는 경제적 활동을 지양해야 한다.

6.2 기능

최고 감사 기구의 주 기능은 다음과 같다.

- 재정 관리의 합법성, 효율성, 효과성 문제 및 일반적으로 인정되는 그 밖의 기준으로부터의 일탈 규명
- 내부 통제, 위험 관리, 회계 시스템 등 재정 관리 개선을 위한 권고
- 의회에 정부 계정의 정확성과 합규성을 확인시킴으로써 행정부가 의회의 의지에 따르도록 도움
- 일반 대중에게 세금이 합법적이고 적절하며, 효과적, 효율적으로 사용되고 있음을 확인시킴
- 공공 기관에 공공 자금 사용에 대한 책임을 물음

이 기능들 중 상당수가 사후적이지만 (재정 활동이 이루어진 후에 심사가 수반됨) 최고 감사 기구는 사전적 역할도 할 수 있다. 특히 최고 감사 기구(독일 연방회계검사원의 경우, 상자 7 참조)는 예산안에 관한 의견을 제시할 수 있는 권한이 있다.[35] 이것은 재정 문제가 발생하기 전에 문제를 파악하고 수정하기 위한 예방적 기능으로 볼 수 있다. 예를 들어 최고 감사 기구는 이전의 감사에서 특정 활동이나 지출 유형에 초과 지출이 있었음이 일관되게 확인된 경우, 그에 관한 추가 자금 할당을 권고할 수 있다.

부정부패 사건을 적발하는 것은 최고 감사 기구의 직무는 아니지만 그러한 관행의 증거가 발견되는 경우에는 행정부의 적절한 구성원 및 (또는) 적절한 법 집행 기관에 알려야 한다.

6.3 정보기관 감사

최고 감사 기구는 다른 공공 기관 감사에 적용하는 것과 동일한 기준을 사

용하여 정보기관을 감사하며, 최고 감사 기구의 관할권은 정보기관 재정의 모든 면에 미쳐야 한다. 행정부가 외부 재정 감독에서 면제시키는 정보기관 활동 분야가 있어서는 안 되는데, 최고 감사 기구의 독립성을 훼손할 뿐 아니라 불법적이거나 부적절한 자금 사용이 은폐될 수 있기 때문이다.[36]

(프랑스와 미국 같은) 일부 국가의 경우, 정보기관의 일부 운영 계정이 최고 감사 기구 감사에서 면제된다. 이런 경우, 모범 관행은 면제된 계정을 감사할 다른 독립적 기구를 지명하도록 한다. 예컨대 프랑스에서는 면제된 계정을 의원들과 감사관들로 구성된 특별자금위원회가 감사한다.[37] 미국의 경우, 면제되는 "무증명 계정"(행정부 구성원 1인의 확인서로만 해명되는 지출)은 회계감사원이 감사할 수 없지만 의회 정보기관 감독 위원회의 감사를 받을 수 있다.[38]

심사가 어떤 방식으로 이루어지건 정보기관의 모든 재정 활동은 정보 공동체와 행정부 외부의 기구에 의한 감사를 받아야 한다. 일반적으로 최고 감사 기구는 이런 감사를 수행하기에 가장 적합한 기구이다.

상자 7: 독일 회계검사원

독일 연방회계검사원(FCA)은 연방 정보기관을 포함한 모든 연방 정부 기관의 감사를 담당한다.[52]

기능

연방 정부 기관과 관련된 FCA의 기능은 다음과 같다.

- 연방 정부 기관들의 수입, 지출, 자산, 부채를 감사하고 재정적 영향이 있을 수 있는 기관들의 일체의 행위를 검사
- 예산안에 대한 의견 제시 등을 통해 기관 예산을 정하는 의회의 권한 행사를 지원
- 공공 자금 관리와 관련하여 행정부의 책임을 해제할지 여부에 대한 의회의 결정을 지원[53]

감사 범위

준거법은 FCA의 활동에 아무런 제한을 두지 않고 있다. 따라서 FCA는 감사할 기관, 감사 시기 및 방법을 단독으로 결정한다. 의회(이 맥락에서는 하원 기밀위원회)는 FCA 감사를 요청할 수 있지만 FCA의 행동을 강제할 수는 없다. FCA 감사는 기관들이 재정 활동과 관련된 법률과 규정을 준수했는지 파악한다. 특히 다음 사항을 파악한다.

- 예산법 조항들을 준수했는가
- 기관의 수입, 지출, 자산, 부채가 문서로 정연하고 적절히 입증되는가
- 공공 자금을 효율적으로 관리했는가
- 주어진 과제를 효과적으로 완료했는가

FCA가 제기하는 정보 사안들은 예산 책임 해제 과정 및 이후의 예산 토론의 일환으로 기밀위원회(상자 5 참조)에서 다룬다. 따라서 최고 감사 기구 대표자들은 종종 기밀위원회 회의에 참석하여 감사와 지출 승인 과정 사이의 유용한 연결 고리를 만들어낸다.[54]

구성

FCA는 검사원장 1명과 부원장 1명이 이끈다. 두 명 모두 행정부가 지명하고 의회에 의해 선출된다. 각자는 최대 12년 재임할 수 있다. FCA

는 각각 국장 1명과 차장 1명이 이끄는 주제별 국으로 나뉜다. 이 사람들은 모두 "법원의 구성원(members of the court)"인데, 사법적 독립성이 있음을 뜻한다. 대부분의 감사 관련 결정은 2명의 법원 구성원(주무 국장과 부문 책임자)으로 이루어진 "칼리지(college)"가 내리며, 의견이 일치하지 않을 때는 검사원장이 합류해 3인으로 이루어진 칼리지를 만든다.[55]

정보에 대한 접근

법률에서는 정보기관을 포함한 모든 정부 기관이 FCA가 업무 완료에 필요하다고 여기는 모든 문서를 제공하도록 규정하고 있다. 이 의무에는 아무런 제한이 없다.[56]

보고서

FCA 보고서는 일반적으로 공개되지만 정보기관에 관한 보고서는 공개되지 않는다. 그 대신 이 보고서는 하원의 정보기관 감독 기구인 기밀위원회와 관련 행정부 기구에 제출된다.[57]

6.4 감사 유형

최고 감사 기구가 수행하는 감사의 유형은 나라마다 다르지만 다음 세 가지 유형이 거의 보편적이다.

- *재정 감사*
  공공 기관이 작성한 재무제표의 정확성과 공정성을 파악한다.
- *준법 감사*
  기관의 수입과 지출이 연간 예산법 등 관련 법률과 규정을 준수하는지 파악한다.
- *성과 감사 또는 VFM(value-for-money) 감사*
  기관이 효과적, 효율적으로 위임 사항을 이행하고 목표를 달성했는지, 다시 말해 기관에 투자된 공공 자금에 상당하는 가치가 납세자들에게 돌아갔는지 파악한다.

최고 감사 기구는 정보기관과 관련하여 내부 재정 통제, 위험 관리, 회계 시스템에 초점을 맞춘 재정 감사와 준법 감사를 주로 실시한다.

최고 감사 기구가 기관의 모든 재정 거래를 심사할 수는 없기 때문에 대부분은 위험 기반 접근 방식을 이용해 감사 결과의 타당성을 평가한다. 구체적으로 말해 최고 감사 기구는 제출된 재무제표가 부정확할 위험을 평가한다. 그 방법은 기관의 회계 보고 절차, 내부 통제의 약점, 최고 감사 기구 자체의 탐지 절차의 약점을 평가하는 것이다.

정보기관 성과 감사는 이 도구의 2절에서 논의한 이유, 특히 정보 업무의 특징인 결과의 불확실성과 편익의 무정형성 때문에 매우 어려울 수 있다. 예컨대 최고 감사 기구는 성공이나 실패를 계량화하기 어려운 운영 활동(요원 운영, 감시 등)의 가치를 평가하기 힘들 수 있다. 따라서 일부 최고 감사 기구는 이들 분야의 성과 평가를 자제한다.

하지만 성과 감사는 재정 감사와 준법 감사로는 불가능한 감사 결과를 내놓을 수 있다. 가령 해명이 적절히 이루어지고 모든 관련 법규를 준수해서 재정 검열과 준법 검열을 통과한 대형 자본 프로젝트나 대규모 조달 프로그램을 생각해 보라. 그럼에도 이들은 사용된 돈에 상당하는 가치가 없을 수 있는데, 이것은 성과 감사로만 밝혀낼 수 있다.

최고 감사 기구가 정보기관의 성과 감사를 수행하는 경우에는 보통 정보 기술 시스템이나 기밀 취급 인가 절차 등 여러 기관에 걸친 구체적 사안이나 주제에(상자 8 참조) 초점을 맞춘다.

상자 8: 캐나다의 업무 감사

2004년, 캐나다 회계 감사관(AG)은 캐나다 정보보안국과 그 밖의 정보 관련 기관들에 대한 성과 감사를 실시했다. 이 감사는 "공공 안보 및 테러 방지 프로그램(Public Security and Anti-Terrorism initiative)의 전반적 관리, 부처 및 기관 간 정보 조정, 집행 인력에 대한 적절한 정보 제공 역량"을[39] 조사했다. 이 감사는 911 이후 캐나다 정부가 테러 방지에 상당한 투자를 한 후 이루어진 것이다.

최종 감사 보고서에서 AG는 무엇보다도 "정부는 투자, 관리, 개발 결정을 지도하고 개별적 기관들에서 보완 조치를 지휘할 수 있는 관리 체계를 갖고 있지 않았다"고[40] 결론 내렸다. 그뿐만 아니라 AG에 따르면 "정부 전체가 보안 정보 체계의 상호 소통 능력 개선을 달성하는 데 실패했다."[41] 보다 일반적으로 AG는 "정부 전반적으로 정보 관리 방식에 결함"이[42] 있었다고 판단했다.

6.5 정보에 대한 접근

최고 감사 기구는 고품질 감사의 전제 조건으로, 또 운영 독립성을 보장받을 수 있는 조건으로서 정보에 제한 없이 접근할 수 있어야 한다. 정보기관이 무단 공개로부터 기밀 정보를 보호하고 싶은 것은 당연하지만 최고 감사 기구가 여기에 구애되지는 않는다. 따라서 최고 감사 기구에 감사관들이 업무에 필요하다고 생각하는 모든 문서, 사람, 물리적 장소에 접근할 권한을 법률로 부여하는 것이 좋은 관행이다. 가령 남아공(상자 9 참조)과 독일(상자 7 참조)의 경우가 그런데, 현재 진행 중인 업무에 관한 정보에도 접근할 수 있다. 최고 감사 기구를 규율하는 법률에 접근 권한이 명시되는 것은 필수적이지만 그것만으로는 충분하지 않다. 입법자들은 정보기관과 기밀 정보에 관한 법률이 최고 감사 기구의 접근에 관한 이러한 단서와 모순되지 않도록 해야 한다. 정보 접근을 지원하는 각종 권한도 법률로 최고 감사 기구에 부여해야 한다. 이러한 권한에는 소환 권한, 수색 및 압수 권한, 선서 증언 또는 무선서 증언을 강제할 권한이 포함될 수 있다(상자 9 참조).

일부 국가의 법률은 최고 감사 기구의 정보 접근을 제한한다. 예를 들어 영국 감사원의 경우가 그런데, 정보 출처와 방법에 관한 정보에 대한 접근이 제한되었다. 이런 제한은 협소하고 명확히 규정되어 있어 감사원 업무를 방해하는 것으로 간주되지는 않는다. 하지만 다른 나라에서는 최고 감사 기구의 정보 접근에 대한 제한이 훨씬 광범위하다. 예를 들어 미국에서는 법률로 회계감사원과 공유할 정보를 사안별로 결정할 수 있는 상당한 재량을 정보 공동체에게 부여한다.[45] 게다가 회계감사원(GAO)은 "무증명 계정" 출처, 방법, 비밀 업무에 관한 정보에 접근하는 것이 차단된다.[46] 정보 접근 제한은 GAO와 다른 나라의 감사 기관들의 업무를 방해한다. 이는 독립적 재정 감독의 효과성과 포괄성을 줄이는 기능을 할 수 있다.

법률이 최고 감사 기구에 완전한 접근 권한과 강력한 집행 권한을 부여하는 경우에도 최고 감사 기구가 관련 있다고 여기는 모든 정보에 접근하기에는 부족할 수 있다. 많은 정보 관련 사안의 비밀스러운 속성 때문에 최고 감사 기구는 특정 유형의 정보에 접근하는 데 상당한 실제적 장애물에 봉착하게 된다. 특히 유급 정보원과의 면담, 비밀 작전에 관한 정보 획득, 비밀 요원들이 사용하는 자산의 존재 확인에서 어려움을 겪게 될 것이다.

상자 9: 남아공 감사원(Auditor General)의 권한 [43]

남아공 감사관(AG)은 필요한 정보에 접근하는 데 사용할 수 있는 강력한 권한을 가지고 있다. 이 상자에서는 이러한 권한들을 요약한다. 다만 실제로는 AG 법률 체계에 이러한 권한을 포함시킨다고 해서 반드시 비밀 정보기관들의 관련 정보가 공개되는 것은 아니라는 점에 유의해야 한다.[44]

정보에 대한 접근

법률은 감사를 수행하는 AG에게 모든 합리적인 시기에 다음에 대해 완전하고 제한 없이 접근할 권한을 부여한다.

- 피감사 기관의 사업, 재정 활동, 재무 상태 또는 성과를 설명하는 서면 또는 전자적 기록 방식의 피감사 기관이 보유한 일체의 문서나 정보
- 피감사 기관의 소유 또는 통제 하의 일체의 자산
- 피감사 기관의 대표자 또는 그 직원

감사 권한

AG는 감사를 수행함에 있어,

- 구두 또는 서면으로 기밀, 비밀 또는 기밀 분류 정보 등 감사와 관련된 정보를 선서 또는 무선서 하에 공개하도록 지시할 수 있다.
- 누구에게나 그러한 정보에 관해 질문할 수 있다.

또한 AG는 감사를 수행함에 있어 다음을 위한 영장을 판사 또는 치안판사에게서 받을 수 있다.

- 관련 정보가 있거나 감춰져 있다는 합리적 의심으로 구내, 부지 또는 차량에 출입
- 잠재적으로 관련성 있는 정보를 위해 구내, 부지 또는 차량 및 부지나 차량에 있는 자에 대한 수색
- 감사 완수를 위해 잠재적으로 관련성 있는 정보의 압수

일반적으로 필요한 정보에 대한 AG의 접근 권한은 정보기관의 기밀 유지 의무에 우선한다. 예를 들어 정보 사안에 관련된 정보를 공개하는 것이 일반적으로 금지되는 자라 하더라도 해당 정보를 AG에게는 공개해야 할 수 있다. 이러한 경우, AG의 요청에 따르는 것은 이 사람의 비공개 의무 위반으로 간주되지 않는다.

정보 접근에 대한 법적, 실제적 제한이 감사에 미치는 영향은 무엇보다도 실시되는 감사의 유형과 정보기관의 협조 정도에 좌우된다. 상황에 따라서는 정보 접근 제한이 최고 감사 기구의 업무 수행 능력을 유의미하게 손상시키고, 감사 과정의 무결성을 훼손해 기대에 못 미치는 수준의 감사를 초래할 수 있다. 실제로 감사의 결론을 바꿀 수도 있었던 정보가 은폐되었다는 것을 감사관들이 알지 못하는 경우, 특히 문제가 된다. 이러한 정보가 없으면 감사관들은 그릇된 보장 및 책임성을 제공하는 적정 의견(unqualified opinion)을 낼 수도 있다.

이런 종류의 문제는 최고 감사 기구의 권한과 독립성이 아직 완전히 자리잡지 못했거나 최고 감사 기구와 감사 대상 정보기관의 관계가 적대적인 나라에서 발생할 가능성이 매우 높다. 최고 감사 기구가 정보 접근 제한이 정확한 감사 의견을 낼 능력에 걸림돌이 된다고 판단하는 경우, 국제 감사 기준에서는 이 최고 감사 기구가 한정 의견(qualified opinion)을 낼 것을 요구한다. 이런 직업적 의무를 고수하면 정보 접근에 대한 어떠한 법적 또는 실제적 제한도 감사 의견과 보고서에 포함될 수 있다.

6.6 정보 보호

감사관들에게 공개하는 정보의 기밀 유지를 정보기관과 행정부에게 보장하기 위해 많은 최고 감사 기구는 정보기관 감사를 수행할 보안 시설과 기밀 취급 인가 인력을 갖춘 특별 부서를 설립했다. (일반적으로 정보기관 기록을 감사하는 최고 감사 기구 인력에게는 기밀 분류 정보 및 기타 기밀 정보의 비밀을 유지할 법적 의무를 포함하여, 동일 정보에 접근할 수 있는 기관 인력과 동일한 보안 기준이 적용되어야 한다.[47]) 전문가다운 방식으로 기밀 정보를 취급하면 최고 감사 기구와 정보기관 간 신뢰를 구축하고, 향후에 정보를 순조롭게 제공받을 가능성을 높인다.

6.7 보고서

보고서는 감사관들이 감사 결과와 권고 사항을 전달하는 주된 수단이다. 감사 보고서를 받는 사람들에는 정보기관 관리층, 행정부 관료, 의원, 일반 대

중이 포함된다. 종종 이 이해 관계자들은 주로 최고 감사 기구의 보고서에 근거해 조치를 취한다. 가장 중요한 것은 의원들이 최고 감사 기구 보고서를 정보기관 재정 감독의 기초로 사용한다는 점이다. 실제로 최고 감사 기구의 감사 결과와 권고 사항은 향후 예산에 대한 의회의 결정을 통해 정보기관과 행정부에 영향을 미칠 수 있다.

6.7.1 비밀주의

정보기관에 관한 최고 감사 기구의 보고서에는 기밀 정보가 포함되어 있기 때문에 수정되지 않은 버전은 보통 일반에 공개하지 않으며, 심지어 대부분의 의원들에게도 공개하지 않는다. 법률과 관행은 일반적으로 전체 (기밀) 보고서를 수령할 수 있는 사람을 기관 고위 관리층, 행정부 고위 관료, 의회 감독 위원회 위원, 그리고 경우에 따라 의회 재정/예산 위원회 위원들로 제한한다.

최고 감사 기구 보고서에 포함된 민감한 국가 안보 정보는 분명 "비밀주의의 고리(ring of secrecy)" 안에 남아 있어야 하지만 이들 보고서 중 많은 부분이 공개가 가능하며 또 공개되어 마땅하다. 이 점에서 남아공 감사관은 정보기관에 관한 그의 보고서에는 공개될 경우 기관에 해를 끼치거나 국가 안보를 훼손할 내용이 없으므로 공개되어야 한다고 밝힌 바 있다.[48]

정보기관 감사 공개의 포괄적 금지와 그 내용의 일률적인 기밀 분류는 투명성, 개방 정부, 정보의 자유라는 기본적인 민주적 원칙에 반한다. 이 문제와 관련해 남아공 헌법은 특히 진보적인데, 정보기관과 관련되고 민감한 정보가 제외되어야 하는 보고서를 포함하여 감사관이 작성한 모든 보고서의 공개를 규정하고 있다.[49] 일반적으로 기밀 분류는 공표라는 일반적 원칙의 예외로서 정당한 국가 안보 이익의 보호에 필요한 경우에만 허용되어야 한다.

정보기관이나 행정부의 구성원은 어떤 경우에도 공공 자금의 불법 사용을 은폐하기 위해 비밀주의 조항을 이용할 수 없어야 한다. 부정행위를 밝히는 데 필요할 경우 기밀 정보의 공개를 명시적으로 허용하는 우선 조항을 법률에 포함시키는 것이 좋은 관행이다. 남아공 공공감사법의 이 문구는 이러한

우선 조항을 설명한다.

(1)감사관은 비밀 또는 기밀 정보의 공개를 막기 위한 예방 조치를 취해야 한다.

(2)(1)관에 관해서 취한 조치는 무단 지출, 변칙 지출 또는 성과가 없거나 낭비적인 지출…또는 피감사 기관의 재정 문제와 관련된 그 밖의 변칙 또는 범죄 행위에 관한 감사관 또는 관계 감사인의 공개를 막을 수 없지만 그러한 공개에는 공개 시 국가 안보를 해칠 수 있는 사실 관계가 포함되어서는 안 된다.[50]

6.7.2 정보 공개

최고 감사 기구는 최소한 정보기관 감사/심사에 관한 다음 유형의 정보를 공개해야 한다.

- *최고 감사 기구가 실시했거나 실시할 감사의 목록*
  각각은 제목과 간략한 설명으로 간단히 언급할 수 있다.[51]
- *기관의 재무제표에 관한 기본 감사 의견*
  보통 아주 짧은 문서인 기본 의견은 정보를 거의 공개하지 않지만 기관과의 상호 작용이 있었음을 확인해 준다.
- *기밀 보고서의 공개 버전*
  최고 감사 기구는 정보기관에 대한 정기 감사와 성과 감사를 포함한 보고서의 공개용 버전을 발간해야 한다(예로 상자 8 참조). 이는 보고서의 기밀 버전에서 민감한 정보를 수정(제거)한 별도의 공개 버전을 만들거나 공개되지 않는 부록에 모든 기밀 정보를 포함시킴으로써 가능하다. 대부분의 의회 및 전문가 감독 기구들은 보고서의 공개 버전을 발간하지만 최고 감사 기구의 경우, 이 관행이 아직 널리 시행되지는 않고 있다.

6.8 최고 감사 기구 업무에서 투명성의 중요성

일반 대중은 민주적 거버넌스의 원칙에 맞춰 최고 감사 기구의 업무와 정보기관에 관한 최고 감사 기구의 보고서에 관해 최대한 많이(위에서 논의한 기밀 제한이 적용된다는 전제하에) 알 필요가 있다. 일반 대중에게 최고 감사

기구의 정보기관 감사를 알려 주는 것은 피감사 기관과 최고 감사 기구에 대한 신뢰와 지지를 형성하는 데 도움이 된다. 정보 공동체가 적절한 조사를 받는다는 것을 대중에게 확신시키는 것은 정보기관들이 전문가답게 행동하며, 공공 자금을 적절히 사용하고, 법률의 한계 내에서 운영된다는 유용한 인식에 기여한다.

나아가 투명성은 특히 공공 자금 사용과 관련된 정보기관에 관한 근거 없는 추측을 일소하는 데 도움이 된다. 이는 정보기관에 대한 신뢰 수준이 여전히 낮고 기관들이 자금을 잘못 사용한 전력이 있는 나라에서 특히 필요하다. 또 정보기관의 적절한 역할에 관한 공공 토론을 불러일으키고 그것에 영향을 미치는 역할도 한다. 이는 정부가 대규모 예산 적자에 봉착해 공공 서비스를 축소해야 하는 경우에 중요할 수 있다.

7. 권고 사항

정보기관의 재정을 감독하는 단일한 "최선"의 방법은 없지만 이 도구에서 논의한 법률, 제도적 모형, 관행에서 발췌한 다음의 권고 사항들은 여러 상이한 법률 및 제도 모형에 적합하게 수정 가능한 모범 관행들이다. 이들 권고 사항 대부분은 예산 및 감사의 법적, 제도적 틀이 이미 존재하고, 공공 자금 관리 및 사용의 법률 체계가 이미 구축되어 있다고 가정한다.

예산 및 재정 보고와 관련된 권고 사항

- 정보기관 예산은 "포괄적"이어야 한다. 즉 기관의 재정 활동 전부를 포괄해야 한다. 법률은 기관들이 그들의 예산에 포함되지 않은 재정 활동에 관여하는 것을 명확히 금지해야 한다.
- 정부는 공공 안전이나 국가 안보를 위험에 빠트리지 않는 한도 내에서 정보기관 예산을 최대한 많이 공개해야 한다. 최소한 정부는 한 기관에 할당되는 총액, 특정 비용 범주의 소계, 특정 지출과 관련된 목표를 공개해야 한다. 예산 정보는 정당한 국가 안보 이익을 보호하기 위해 엄격히 필요한 경우에만 기밀로 분류되어야 한다.

- 의회는 어떤 재무 정보(예산 및 재무제표 포함)를 공개해야 하고, 어떤 정보는 기밀로 유지하거나 특별 회계 및 감사 절차의 대상으로 삼을지 규정하는 법률을 제정해야 한다.
- 정보기관은 최대한 많은 정보가 포함된 재무제표의 공개 버전을 작성해야 한다.

내부 재정 통제와 관련된 권고 사항

- 정보기관은 공공 기관의 내부 재정 통제와 감사 메커니즘에서 면제되어서는 안 된다.
- 정보기관이 이따금 공공 자금의 관리 및 사용 관련 법규 적용 대상에서 벗어나도록 허용하려면 그러한 허용 권한이 법률에 근거해야 한다.

외부 재정 감독과 관련된 권고 사항

- 법률은 최고 감사 기구가 정보기관의 재정을 감사하여 기관의 재무제표가 정확하고 공정한지, 기관의 재정 거래가 관련 법규를 준수하는지, 공공 자금이 지출에 상당하는 가치를 제공하게끔 효과적으로 사용되었는지 파악할 것을 요구해야 한다. 최고 감사 기구는 이들 목표를 추구함에 있어 비밀 업무나 기타 민감한 업무와 관련된 특별 계정을 포함한 기관 활동의 모든 측면을 감사할 권한을 가져야 한다.
- 의회와 최고 감사 기구는 다른 공공 기관에 적용되는 것과 동일한 수준으로 정보기관 재정을 조사해야 한다. 이 조사는 예산안 기밀 부분의 전면 검사부터 시작하여 기관 재정 기록의 사후 심사 및 감사로 끝나는 예산 주기 전체에 걸쳐 이루어져야 한다.
- 법률은 외부 감독 기구가 업무의 완수에 필요하다고 여기는 모든 정보(그 정보를 감사 받는 정보기관이 보유하건 다른 공공 기관이 보유하건 상관없이)에 접근할 권한을 외부 감독 기구에 부여해야 한다. 이러한 접근은 공개를 강제하기에 충분하고 적절한 조사 권한으로 뒷받침되어야 한다.

- 기밀 정보에 접근할 수 있는 의회와 최고 감사 기구는 이 정보를 무단 공개로부터 보호하기 위한 조치를 취해야 한다. 이러한 조치는 해당 정보를 알 필요가 있는 자에게만 정보가 공개되도록 하고, 정보를 물리적, 기술적으로 보호하며, 무단 공개를 막는 제재 장치가 있도록 해야 한다.
- 재정 감독을 담당하는 의회 위원회 위원들은 정보기관 재정을 이해하고 의미 있는 조사를 수행할 수 있는 충분한 인적, 기술적 자원을 갖춰야 한다.
- 의회는 최고 감사 기구가 그 업무를 완수하는 데 필요한 권한과 자원을 갖도록 해야 한다. 나아가 정보기관이 최고 감사 기구의 권고를 이행하도록 독려해야 한다.
- 의회는 사후 심사 및 감사 결과를 후속 연도 예산안 검토에 활용할 수 있도록 외부 감독 기구들이 서로 적절히 연계되도록 해야 한다.
- 정보기관 재정 감독을 담당하는 의회 위원회는 최고 감사 기구와 적극적으로 교류해야 한다. 여기에는 최고 감사 기구 보고서 검토, 후속 회의 주최, 그리고 최고 감사 기구가 정보기관 감사에 적절한 권한과 자원을 갖도록 조치를 취하는 것 등이 포함되어야 한다.
- 의회와 최고 감사 기구는 정보기관 감독에 관해 일반 대중에게 알릴 책임이 있다. 의회와 최고 감사 기구는 조사 및 감사 결과의 공개 버전을 작성하고 그 활동에 관한 정기 보고서를 공개해야 한다.

후주(後註)

1. 이 도구는 정보기관 재정 감독에 관한 DCAF 워크샵 회의록과 제출된 문서에 기초한 것이다. 여러 나라의 최고 감사 기구 고위 구성원, 국회 대표자, 전직 정보 관료, 학자들이 여기 참여했다. 모든 회의록은 비공개였기 때문에 직접적으로 인용되지 않았다. 참가자들은 이 도구의 초고에 관한 유용한 의견도 제공했다. 필자는 이 그룹의 모든 구성원에게 감사를 표하며, 초기 원고에 귀중한 의견을 보태 준 DCAF 동료인 한스 본, 벤자민 S. 버클랜드, 가브리엘 가이슬러 메세바게에게 감사한다.

2. "지출 상당 가치(value for money)"는 조직이 책임 수행에서 자원을 활용하는 경제성, 효율성, 효과성을 가리킨다. "Performance Audit" in: International Organization of Supreme Audit Institutions, Financial Audit Guideline – Glossary of Terms to the INTOSAI Financial Audit Guidelines 참조.

3. United States, Central Intelligence Agency; appropriations; expenditures, U.S. Code 50 §403j (available at http://us.code.vlex.com/vid/central-intelligence-agency-expenditures-19266900).

4. 이러한 예외 사례는 United Kingdom, The Defence and Security Public Contracts Regulations 2011, No. 1848, Section 7 (available at http://www.legislation.gov.uk/uksi/2011/1848/made) 참조.

5. Auditor General of Canada, *Report of the Auditor General of Canada* (1996), "Chapter 27—The Canadian Intelligence Community—Control and Accountability," Section 27.107 (available at http://www.oag-bvg.gc.ca/internet/English/parl_oag_199611_27_e_5058.html).

6. 더 자세한 내용은 David Johnston and Mark Mazzetti, "A Window Into C.I.A.'s Embrace of Secret Jails," *New York Times,* August 12, 2009; David Johnston, "Ex-C.I.A. Official Admits Corruption," *New York Times,* September 29, 2008; Matthew Barakat, "Feds: Misconduct by CIA's Foggo spanned decades," *Associated Press,* February 25, 2009; and U.S. v. *Foggo and Wilkes,* U.S. District Court of Southern California, Grand Jury Indictment, June 2005 참조.

7. The World Bank, *Public Expenditure Management Handbook* (Washington: The World Bank, 1998), "Code of Practices on Fiscal Transparency," Annex J.

8. Todor Tagarev, (ed.), *Building Transparency and Reducing Corruption in Defence: A Compendium of Best Practices* (Geneva: NATO/DCAF, 2010), p. 64. 국가 법률의 예는 South African Public Finance Management Act, No. 1 of 1999, Section 38(2) 참조.

9. 다양한 예산 방식에 관한 더 자세한 논의는 The World Bank, *Public Expenditure Management Handbook,* pp. 12–16; Tagarev, *Building Transparency,* p. 59; and Organisation for Economic Co-operation and Development (OECD), "Performance Budgeting: A User's Guide," Policy Brief (March 2008) 참조.

10. 영국의 단일 정보 회계는 민간 정보기관 3곳의 예산을 합산한다.

11. 더 자세한 논의는 Nicolas Masson and Lena Andersson, *Guidebook: Strengthening Financial Oversight in the Security Sector* (Geneva: DCAF, 2012) 참조.

12. France, Mission Ministérielle Projets Annuels de Performances, "Annexe au projet de loi de finance pour Défense" (2010), pp. 36–37.

13.모든 예산 정보에 대한 의사 결정권자의 접근권의 중요성에 관해서는 The World Bank, *Public Expenditure Management Handbook*, pp. 1–2 참조.

14.United States General Accounting Office (GAO), "Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities," GAO-01-975T (July 2001), p. 10; and United States, Central Intelligence Agency; appropriations; expenditures, U.S. Code 50 §403j.

15.예컨대 Australia, Financial Management and Accountability Act 1997, Section 49 참조.

16.Australian Security Intelligence Organisation, Financial Statements, in *Annual Report 2010–11* (Canberra: 2011), pp. 133–151 (available at http://www.asio.gov.au/img/files/Report-to-Parliament-2010-11.pdf).

17.France, Loi organique n°2001–692 du 1 août 2001 relative aux lois de finances (LOLF), Article 54.

18.의회가 총액에 대해 투표하고 구체적인 자금 할당은 행정부의 재량에 맡기는 이탈리아 모형에 관한 논의는 Federico Fabbrini and Tomasso Giupponi, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Italy," in *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, Aidan Wills and Mathias Vermeulen (Brussels: European Parliament, 2011), Annex A, p. 245 참조.

19.Hungary, Act CXXV of 1995 on the National Security Services, Article 14(g).

20.Richard Best, The *Intelligence Appropriations Process: Issues for Congress* (Washington: Congressional Research Service, October 27, 2011); see also Richard Best and Elizabeth Bazan, *Intelligence Spending: Public Disclosure*

Issues (Washington: Congressional Research Service, February 15, 2007), p. 5; Frederick Kaiser, Walter Oleszeck, and Todd Tatelman, *Congressional Oversight Manual, Congressional Research Service* (Washington: Congressional Research Service, June 2011), pp. 16–19; Eric Rosenbach and Aki Peritz, *Confrontation or Collaboration? Congress and the Intelligence Community* (Cambridge, MA: Harvard, 2009), pp. 24–28; and James Saturno, *The Congressional Budget Process: A Brief Overview* (Washington: Congressional Research Service, 2004).

21. German Federal Budget Code, Article 10(a). See also Hans De With and Erhard Kathmann, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Germany," in P*arliamentary Oversight of Security and Intelligence Agencies in the European Union,* Wills and Vermeulen, Annex A, pp. 225–226.

22. 더 자세한 논의는 Wills and Vermeulen, pp. 129–131 참조.

23. Italy, Law 124/2007, Articles 33(8) and 29(2).

24. Spain, Ley 11/1995, Article, 2.2. See also Susana Sanchez Ferro, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in Spain," in *Parliamentary Oversight of Security and Intelligence Agencies in the European Union, Wills and Vermeulen,* Annex A, p. 271.

25. 공공회계위원회 위원장은 항상 야당 소속이다.

26. United Kingdom, Intelligence Services Act 1994, Section 10 (1).

27. 예컨대 United Kingdom, Intelligence and Security Committee, *Annual Report 2010–2011,* CM 8114 (2011), pp. 12–16 참조.

28.Ian Leigh, "Parliamentary and Specialised Oversight of Security and Intelligence Agencies in the United Kingdom," in *Parliamentary Oversight of Security and Intelligence Agencies in the European Union, Wills and Vermeulen,* Annex A, p. 298.

29.Ibid., p. 297; 조사관 업무의 예는 United Kingdom, Intelligence and Security Committee, *Annual Report 2010–2011,* pp. 7, 16, 17, and 79에서 논의되고 있다.

30.OECD, "Relations Between Supreme Audit Institutions and Parliamentary Committees," Sigma Papers, No. 33 (Paris: OECD Publishing, January 2002), pp. 19–20.

31.일부 국가에서는 의회의 사후 심사로 최고 감사 기구의 감사가 적절히 수행되었는지도 판단한다.

32.France, Ministry of Budget, Public Accounts and Civil Service, "Guide to the Constitutional Bylaw on Budget Acts" (2008) p. 32; France, LOLF, Article 54 and Article 58; United States, Government Accountability Office web site (available at http://www.gao.gov/about/index.html).

33.German Federal Ministry of Finance, "The Budget System of the Federal Republic of Germany" (Berlin: 2008) p. 47.

34.UN General Assembly Resolution, "Promoting the efficiency, accountability, effectiveness and transparency of public administration by strengthening supreme audit institutions," United Nations Document A/RES/66/209 (15 March 2012),.

35.Ibid., p. 18.

36.여전히 미국에서는 CIA의 몇몇 업무 분야에 대한 GAO의 감사가 실제적, 법률적으로 제한된다. Intelligence Community Directive, No. 114, June 30, 2011; Gene Dorado (US Comptroller General), Letter to Director of National Intelligence James Clapper regarding "GAO Comments on Intelligence Community Directive Number 114: Comptroller General Access to Intelligence Community Information," 28 April 2011; and US GAO, "Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities," GAO-01-975T (July 2001), pp. 4–8 참조.

37.France, Loi n° 2001–1275 du 28 décembre 2001 de finances pour 2002, Article 154; France, L'Assemblée Nationale, "Rapport fait au nom de la Commission des Finances, de l'économie générale et du contrôle budgétaire sur le projet de loi de finances pour 2012: Annexe n° 12, direction de l'action du gouvernement publications officielles et information administrative" (14 October 2009), pp. 25–27.

38.United States, Auditing Expenditures Approved Without Vouchers, U.S. Code 31 §3524.

39.Office of the Auditor General of Canada, *March 2004 Report of the Auditor General of Canada* (2004), Section 3.2.

40.Ibid., Section 3.3.

41.Ibid., Section 3.4.

42.Ibid., Section 3.5.

43.South Africa, Public Audit Act, No. 25 of 2004, Sections 15–16.

44.South Africa, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy: Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP* (10 September 2008), pp. 226 – 227.

45.Intelligence Community Directive, No. 114; and Gene Dorado, Letter to Director of National Intelligence James Clapper, 28 April 2011.

46.United States GAO, "Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities," pp. 4 – 8; Intelligence Community Directive, No. 114; and Frederick M. Kaiser, "GAO Versus the CIA: Uphill Battles against an Overpowering Force," *International Journal of Intelligence and Counterintelligence* Vol. 15, No. 3 (Fall 2002): pp. 345 – 353.

47.예컨대 Australian Auditor General Act 1997, Section 36; 31 U.S.C. 716; and OECD, "The audit of secret and politically sensitive subjects, comparative audit practices," Sigma Papers, No. 6 (Paris: OECD Publishing, 1996), p. 12 참조.

48.South Africa, Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy* (10 September 2008), p. 229.

49.Constitution of the Republic of South Africa, No. 108, 1996, Article 188(3).

50.South Africa, Public Audit Act, Section 18.

51.호주 감사원은 이 관행을 따른다. NAO 감사 계획의 예는 http://www.anao.gov.au/~/media/Files/Audit%20Work%20Programs/2011_Audit_Work_ Plan.PDF에서 볼 수 있다. 진행 중인 NAO 감사의 개요는 http://www.anao.gov.au/Publications/Audits-in-Progress에서 볼 수 있다.

52.German Basic Law, Article 114(2); Germany, Federal Budget Code of 19 August 1969, *Federal Law Gazette I,* p. 1284, as most recently amended by Article 4 of the Act of 31 July 2009, *Federal Law Gazette I,* p. 2580, Section 10a (3); Section 88.

53.German Basic Law, Article 114(2); Audit Rules of the Bundesrechnungshof (Germany's Federal Court of Audit), last amended by Senate decisions on 29/30 August 2005, Articles 3, 56 – 57.

54.Germany, Federal Budget Code, Section 10a (3) and Sections 89 – 90; Audit Rules of the Bundesrechnungshof, Articles 4 – 5; The Budget System of the Federal Republic of Germany, pp. 49 and 51.

55.German Federal Court of Audit Act of 11 July 1985 (BGBl. I 1985, p. 1445) as last amended by article 17, Act of 9 July 2001 (BGBI. I, p. 1510), Sections 3, 5, 6, 9 and 19.

56.Germany, Federal Budget Code, Sections 10a (3) and 95.

57.Germany, Federal Budget Code, Section 10a (3); Audit Rules of the Bundesrechnungshof, Article 50.

도구 9

정보기관에 대한 민원 처리

크레이그 포르체세(Craig Forcese)

9. 정보기관에 대한 민원 처리

크레이그 포르체세(Craig Forcese)

1. 머리말

이 도구에서는 정보기관 구성원이 제기하는 민원뿐 아니라 일반 대중이 제기하는 정보기관에 관한 민원 처리에서 감독 기구가 하는 역할에 초점을 맞춘다. 민원 처리 시스템은 특히 정보기관의 경우에 절실히 필요한데, 정보기관에는 "부당하게 또는 잘못 사용될 경우 개인들의 권리를 심각하게 침해할 위험이 수반되는 감시나 기밀 취급 인가 같은 예외적 권한이 맡겨져 있기"[1] 때문이다. 그러나 민원 처리 시스템이 필요한 이유는 권리 침해에 대한 구제 차원에 그치는 것이 아니다. 정보기관 민원 처리 메커니즘은 "관리 실패와 배워야 할 교훈을 부각시켜 책임성 또한 강화함으로써 성과 개선으로 연결될 수 있다."[2]

이런 이유와 그 밖의 이유에서 민원 처리 시스템은 정보 거버넌스의 필수적 부분으로 간주된다. 이런 점에서 UN 특별 보고관의 정보기관 및 그 감독 관련 "모범 관행" 편찬물은[3] 자신의 권리가 침해되었다고 믿을 때는 언제나 "민원을 법원 또는 옴부즈맨, 인권 커미셔너 혹은 국가 인권 기구 같은 감독 기구에 제기"할 수 있는 절차가 있어야 한다고 권고한다. 나아가 불법 행위의 피해자는 "겪은 피해에 대한 완전한 배상을 포함한 실효적인 구제를 제공할 수 있는 기관에 의지"할[4] 수 있어야 한다. 인권 침해의 시정을 구할 이 권리의 근거가 되는 국제 인권법은 "실효적 구제"를[5] 받을 권리 또한 있어야 한다고 요구한다. 이 맥락에서 "실효적 구제"는 확정된 권리 침해에 대한 보상 이상으로 해석되어야 함에 주목해야 한다. 실효적 구제에는 권리가 실제로 침해되었는지 판단할 수 있는 기관에 의지할 권리도 포함된다.[6]

특별 보고관의 보고서는 더 나아가 민원과 구제 청구를 처리할 수 있는 기관은 정보기관 및 정치 행정부(political executive)로부터 독립적이어야 하며,

“모든 관련 정보에 대한 완전하고 제약 없는 접근 권한, 조사 수행에 필요한 자원과 전문성, 구속력 있는 명령을 내릴 수 있는 자격을 갖춰야 한다”고[7] 주장한다.

가장 복잡한 문제를 제기하는 것은 이 마지막의 설계 문제이다. 지금은 정보 부문 민원 처리 기구의 설계와 범위에 관한 비교 데이터가 상당히 풍부하다. 본 프로젝트의 가용 자원으로는 이들 기구의 실제 운영을 평가하기가 불가능하지만 이들 시스템의 구조, 범위, 권한에서 몇 가지 결론을 도출할 수 있다. 이런 검토를 통해 확실해지는 것은 민원 처리 시스템의 필요성은 절실하지만 효과적인 시스템을 설계하는 일은 과학보다는 예술에 가까울 수 있다는 점이다. 각국은 전통적인 법원에 의존할지 아니면 특별한 민원 처리 기구를 설계할지 결정해야 한다. 후자를 선택할 경우, 각국은 정보 관련 민원이 제기하는 특유의 비밀주의 및 보안 문제를 다루는 특별한 정보 처리 체제를 설계할 수 있어야 할지 모른다. 동시에 전문 민원 처리 기구에 의지할 경우, 특히 관할권, 자격 요건, 구제 권한 등 그 밖의 설계 문제가 제기된다.

이 도구에서는 민원 제기, 민원 관할지, 민원 처리 절차 및 정보 통제, 민원 구제책 등 몇 가지 절로 나누어 이들 문제를 검토한다.

2. 민원 제기

누가 민원을 제기할 자격이 있는지는 현행 규칙이 결정한다. 정보기관과 관련된 민원은 두 가지 범주로 나눌 수 있다. 첫 번째는 “내부자” 민원이고 두 번째는 “공공” 민원이다. 이 도구의 목적상 “내부자” 민원은 정보기관의 일부 행위로 인해 피해를 입은 정보기관 직원 또는 기타 정부 직원들이 독립적 기구에 제기하는 민원이다. “공공” 민원은 정보 공동체나 정부와 관련이 없는 일반인이 제기하는 민원이다.

2.1 내부자 민원

일부 관할권의 정보기관 또는 기타 정부 직원들은 정보기관을 상대로 고충을 제기할 수 있다. 이런 내부자 민원은 때때로 민원 제기인에 대한 정보기

관의 처우와 연관되기도 한다. 예를 들어 캐나다에서는 캐나다 보안정보국(CSIS)이 정부 직원들에게 기밀 취급 인가를 부여할 목적으로 거의 모든 캐나다 정부의 보안 심사를 실시한다. 보안 심사 결과에 민원이 있는 직원은 보안정보심의위원회(SIRC)라는 독립적 행정 조직(또는 전문가 감독 기구)에게 민원을 제기할 수 있다.[8]

또 다른 경우, "내부자" 민원이 보다 일반적인 양상을 띠어 정보기관의 부정행위나 월권 신고에 이를 수도 있다. 예컨대 벨기에의 상임 정보기관 심의 위원회(Committee I이라고 함)의 조사국에게는 다음과 같은 권한이 부여된다.

> *정보기관의 개입과 직접적으로 관련된 개인들의 민원과 고발을 조사한다. 명령, 결정 또는 관련 규칙 및 방법 또는 조치와 직접적으로 관련되는 모든 공무원, 공적 기능을 수행하는 모든 자, 모든 군대 구성원은 … 상관의 승인을 요청하지 않고도 민원을 제기할 수 있다.*[9]

미국 법률에 따르면 CIA 직원이나 계약자는 의회 감독 위원회에 민원을 제기하기 전에 내부 통보 절차에 따라야 한다. 준거법에서는 또 "의회에 민원 또는 긴급한 우려와 관련된 정보를 보고하고자 하는" 그러한 개인은 "이러한 민원 또는 정보를 감찰관에게 보고할 수 있다"고[10] 규정하고 있다. 이 맥락에서 "긴급한 우려"는 다음을 의미한다.

- 심각하거나 명백한 문제점, 남용, 법률이나 행정 명령 위반 또는 기밀 정보 관련 정보활동의 자금 조달, 관리 또는 운영과 관련된 결함. 단, 공공 정책 사안에 관한 의견 차이는 포함되지 않는다.
- 정보활동의 자금 조달, 관리 또는 운영과 관련된 중요한 사실 문제에 관해 의회에 한 허위 진술이나 고의적인 은폐[11]

이런 종류의 내부자 민원은 일종의 "내부 고발"로서 정보기관 내의 정상적 지휘 체계 밖에서 부정행위를 폭로하는 것이지만 그렇다고 반드시 정부 기관이나 다른 승인된 감독 기구의 좁은 범위를 벗어나 비밀을 공유하는 것은 아니다. 이러한 민원 메커니즘을 이용할 수 있으면 직원이 언론 등 보다 극단적인 공개 형식에 의존할 가능성을 줄일 수 있다.

일부 관할권에서 이런 형태의 내부 고발에 의지할 것을 독려하는 것은 꽤 합리적이다. 예를 들어 일부는 이런 공인된 경로를 통해 민원을 제기하는 내부자에게 보호를 제공한다. 가령 뉴질랜드에서는 "정보 보안 기관의 직원이 [정보기관] 감찰관으로 하여금 어떤 사안에 주목하게 만드는 경우, 해당 직원은, 악의로 그런 것이 아닌 한 감찰관이 해당 사안에 주목하게 했다는 이유만으로 정보 보안 기관에 의한 어떠한 처벌이나 고용과 관련된 차별적 처우를 받아서는 안 된다."[12] 미국에서는 "허위임을 알면서 또는 그 진위를 고의로 무시하고 민원을 제기하거나 정보를 공개한 경우가 아닌 한 그러한 민원 제기에 대한 보복에 상당하는 조치 또는 보복 위협을 할 수 있는 직위에 있는 중앙정보국 직원은 그와 같은 조치를 취할 수 없다."[13]

일부 관할권의 경우, 내부자의 내부 고발은 보다 공적이고 외부적인 형태의 내부 고발의 전제조건이다. 예컨대 캐나다에서는 내부 경로를 통해 최초 공개가 이루어지지 않은 경우, 기밀 정보 무단 공개라는 형사 고발에 맞서 민원 제기자가 스스로를 성공적으로 변호하기 어렵다.[14]

2.2 공공 민원

공공 민원은 정부와 무관한 사람에 의해 개시되는 절차이다. 이런 종류의 민원은 내부자 민원과 토대 자체가 다르다. 우선 공공 민원 제기자는 문제의 부정행위를 어렴풋이만 알고 있을 수 있다. 예를 들어 불법 감시를 당하는 일반 대중은 이 문제를 우연히 알게 될 수 있고, 그럴 때에도 감시에 관여한 기관의 정확한 정체를 깨닫지 못할 수 있다. 이런 이유로 이 사람에게는 민원의 근거가 되는 구체적 정보가 거의 없을 가능성이 높다. 또 이 사람이 민원 제기를 꺼리거나 단념하는 사회적, 인종적 또는 종교적 집단 소속일 가능성도 있다. 이런 사람의 전형적 예로는 최근에 새로 이주한 사회의 제도와 관습이 익숙지 않은 이민자를 들 수 있다.

따라서 공공 민원 시스템은 불확실성을 수용하고 폭넓은 접근이 가능해야 한다. 이는 공공 민원의 근거는 폭넓어야 하며, 민원에 기한 조사 시작의 장애물은 낮아야 함을 의미한다.

일부 관할권은 민원을 제기할 수 있는 사람의 계층(class)에 어떠한 제한도 두지 않고, 민원 제기인이 광범위한 주제에 관한 우려를 제기하는 것을 허용함으로써 이런 관행을 채택하고 있다. 예컨대 네덜란드에서는 민원 제기인이 자신의 견해를 제시할 수 있도록 주무장관에게 통보한 후, "각자"가 보안 기관의 준거법 집행과 관련하여 국가 옴부즈맨 기관에 민원을 제기할 수 있다.[15] 아일랜드의 경우, 가르다 시오카나 옴부즈맨 위원회(Garda Síochána Ombudsman Commission)는 "가르다 시오카나(경찰) 구성원의 행위와 관련하여 일반 대중이 제기하는 민원을 접수"할 수 있다.[16] 마찬가지로 캐나다에서 공공 민원 제기인이 보안 정보기관을 상대로 제기할 수 있는 가장 일반적인 민원은 "기관이 한 일체의 행위 또는 일"과[17] 관련된다. 끝으로 미국에서 CIA 감찰관은 "법률, 규칙이나 규정의 위반 또는 관리 부실, 자금 낭비, 권한 남용 또는 공공 보건과 안전에 대한 실질적이고 구체적이 위험에 해당되는 행위의 존재에 관해 누구에게서나 민원 또는 정보를 접수하고 조사할 권한이 있다."[18]

이처럼 공공 민원을 제기할 자격을 폭넓게 규정하는 것은 민원 처리 모델의 목적이 정보기관 행위의 합법성과 청렴성을 규율하는 또 다른 수단들을 추가하는 것인 경우에 바람직한 것으로 보인다. 하지만 많은 다른 관할권은 광범위한 공공 민원 제기 자격 개념에서 벗어나 민원 제기 자격을 "모든 사람"보다 좁은 개인들의 계층으로 제한한다. 이런 제한 중 일부는 적당해 보이지만 범위가 상당히 불확실할 수 있다. 예컨대 케냐 민원위원회는 정보기관의 권한 행사나 기능 수행 과정에서 정보기관에 의해 "피해를 입은 자"의 민원을 접수할 수 있다.[19] 남아공에서는 "모든 일반인은" "자신이 믿기에 기관이 자신의 신체나 재산에 초래한 일체의 것에 관해"[20] 합동 상임 정보 위원회에 민원을 제기할 수 있다.

이 두 가지 접근 방식은 특정한 정보기관 관행에 대한 인식에서 촉발되는 선제적이거나 추측에 근거한 민원을 미연에 방지하는 것으로 보인다. 예를 들어 정보 조사에서의 소수 민족 프로파일링을 의심하는 소수 민족 협회는 그러한 관행을 개인적으로 경험한 민원 제기인 대표가 없는 경우, 민원을 제

기할 자격이 없을 수 있다. 민원 시스템의 목적이 정보기관의 합법성과 청렴성을 규율하는 것이라 할 때 이런 제한으로 어떤 부가 가치가 생성되는지 알기 어렵다.

관할권에서 일정 유형의 민원 제기인들에게 국적법을 부과하는 경우에는 더욱 문제가 된다. 예컨대 뉴질랜드 정보보안감찰관은 "뉴질랜드인"(시민 또는 영주권자) 또는 정보기관 중 하나에 의해 고용된 적이 있거나 고용되어 있는 자의 민원만을 접수할 수 있다.[21] 호주 정보보안감찰관(IGIS)은 호주 대외 정보기관과 관련된 민원을 "호주 시민이거나 영주권자인 자"로부터만 접수할 수 있다.[22] (하지만 이런 국적 제한은 호주 국내 보안 정보기관에 관한 민원과 관련해서는 적용되지 않는다.)

국적 (또는 국적/거주) 규칙은 민원에 대한 자의적 장벽이다. 그 결과 난민 민원 제기인 및 아직 영주권자나 시민이 아닌 그 밖의 외국 출신자 등 특별히 목표 집단이 될 가능성이 있는 집단에서 얻을 수 있는 정보기관의 업무 수행에 관한 정보 유통에 구멍이 생길 수 있다. 이 역시 민원 제기인이 부정행위의 조기 경보 지표 기능을 한다면 이런 식으로 자격을 제한해서 어떤 득이 있는지 알기 어렵다.

3. 민원 관할지

이 절에서는 민원을 제기할 수 있는 장소를 다룬다. 민원이 제기되는 기관은 다양하다. 일반적으로 이들 기관은 일반 관할지와 특수 관할지의 두 가지로 크게 나눌 수 있다. 이 도구에서 "일반 관할지"는 전문적인 보안 또는 정보 감독 위임 사항이 없는 기관을 의미한다. 일반 관할지의 예에는 법원, 옴부즈맨 기관, 국가 인권 위원회 및 정보 커미셔너 같은 그 밖의 규제 기구가 포함된다. 반면 "특수 관할지"는 보안 또는 정보 사안을 다루도록 특별히 위임 받은 기관들이다. 그 예에는 벨기에의 Committee I과 캐나다의 SIRC 같은 전문가 감독 기구가 포함된다.

3.1 일반 관할지

3.1.1. 일반 법원

일부 관할권에서는 민사상 권리 침해(다양한 형식의 불법 행위 포함) 형식으로 인정할 수 있음을 근거로 일반 민사 법원이 정보기관과 관련된 민원을 심리할 자격을 갖는다. 다른 관할권에서는 행정 법원이 정보기관의 행위와 관련된, 자체 사물 관할(즉 행정법) 내의 사건을 심리할 수 있다.[23]

실제로 적어도 일부 (어쩌면 대부분의) 관할권에서는 특정 유형의 법원들이 정보기관과 관련된 민원을 접수할 자격이 있는 유일한 관할지이다.[24] 민원을 접수할 권한이 있는 전문 정보기관 감독 기구가 없는 것이다. 이런 선택은 어려움을 제기한다. 아래에서 논의하겠지만 법원은 강력한 구제를 명할 권한이 있을 수 있지만 실제적 이유에서 민원 제기인이 그러한 구제를 받기는 불가능에 가까워서 때로는 정보기관에 관한 특별한 민원을 일반 법원의 전통적 관할 내에 억지로 밀어 넣거나(예: 소송 가능한 민사상 권리 침해) 심리 자체가 이루어지지 않기도 한다.

3.1.2. 전통적 규제 기구

또한 다른 정부 기관들처럼 정보기관도 공공 기관에 관한 민원을 처리할 일반적 위임 사항을 지니거나 정보기관에 한정되지 않는 사물 관할을 지닌 기관의 관할에 속한다는 점에 유의할 필요가 있다. 이들 기관에는 옴부즈맨 기관, 정보 보호 위원회, 인권 위원회가 포함된다. 가령 이들은 정보기관의 정보 사용 또는 보다 일반적으로는 인권 준수에 관한 민원을 심리할 자격이 있을 수 있다. 예를 들어 네덜란드에서는 특히 주무장관, 일반정보보안국 또는 국방정보보안국의 장 및 이들 기관에서 일하는 자들의 행위와 관련된 민원을 국가 옴부즈맨에 제기할 수 있다.[25] 마찬가지로 핀란드와 스웨덴에서는 보안 경찰과 관련된 민원을 의회 옴부즈맨 기관에 제기할 수 있다.[26] 벨기에, 핀란드, 캐나다에서는 프라이버시 (또는 정보) 커미셔너가 정보기관의 개인정보 취급과 관련된 민원을 접수할 수 있다 [27]

일부 관할권에서는 민원이 정보기관 및 (또는) 국가 안보 문제와 관련된 경우, 법률에 의해 주제별 규제 기구가 정보기관 감독 기구 및 다음절에서 논의할 민원 처리 기구와 협의해야 한다. 가령 캐나다에서는 캐나다 인권 위원회가 "캐나다 안보와 관련된 문제에 근거한" 관행과 관련된 민원을 SIRC에 회부해야 한다. 그 다음 SIRC가 조사해 위원회에 보고하면 위원회는 민원 처리를 계속할지 여부를 결정한다.[28] 이런 종류의 분리 심리(bifurcation)는 필연적으로 사건을 복잡하게 만들지만 기밀 정보를 취급하는 사람들의 수를 줄여 소수로 집중시키는 기능을 한다. 동시에 전통적인 규제 기구와 기밀 정보를 공유하기를 꺼리는 정보기관의 태도로 인해 민원 처리가 훼손될 가능성도 적어진다.

3.1.3. 일반 관할지의 단점

(법원이건 전통적인 규제 기구건) 일반 관할지에 관한 공통적 우려 사항은 기밀 정보에 대한 접근이다. 일부 관할권에서는 정보기관이 민사상 권리 침해를 범한 경우, 민사 법원이 원고에 대한 피해 보상을 명할 권한이 있지만 실제로는 정부의 비밀주의 주장 때문에 일반 법원에서의 민사 소송이 어렵다. 민사상 권리 침해의 입증 책임이 원고에게 있고 관련 사실 관계가 정부의 통제 하에 있다는 점을 감안하면 민사 소송에서 승소는 거의 불가능하다.[29] 마찬가지로 정보 및 국가 안보 문제를 전담하지 않는 전통적인 규제 기구는 정보기관과 관련된 민원을 조사할 때 기밀 정보에 접근하고 검토할 수 없어 곤란을 겪을 수 있다. 예를 들어 캐나다 경찰 관련 일반 공공 민원 처리 기구인 왕립 기마경찰은 비밀주의 때문에 경찰의 국가 안보 관련 활동을 입증할 수 없다는 불만을 거듭 표했다.[30]

일반 관할지가 지나치게 일반적일 수도 있다. 다시 말해 보안 정보기관을 다룰 만한 전문성이 부족하다는 것이다. 그 결과 정보기관 감독 경험이 많은 보다 전문적인 감독 기구보다는 정보기관의 비밀주의 주장이나 기타 특수한 상황 주장을 더 존중할 수 있다.

끝으로 정보기관에 관해 제기된 민원의 성격 때문에 전통적인 법원이나 규제 기구가 그러한 민원을 처리하기에는 부적합할 수 있다. 민원 제기인은 종

종 행위의 합법성이나 청렴성에 관한 민원을 표준적인 민사상 근거나 규제상 근거에 끼워 맞춰야 한다. 이것이 잘 맞지 않을 수 있고, 다른 경우라면 가치 있는 민원이 정보기관에 관한 실질적 의혹을 제기하지 않아서가 아니라 이러한 의혹을 일반적인 민원 처리 기구의 관할 언어(jurisdictional language)로 표현할 수 없어서 기각될 수 있다. 예를 들어 불법 감시는 일부 관할권에서는 민사상 권리 침해로 인정되지 않을 수 있으며, 따라서 전통적 법원의 권한에 속하지 않을 수 있다.

3.2 특수 관할지

일반 관할지의 단점에 대한 확실한 대응은 보다 전문화된 민원 처리의 장을 만드는 것이다. 특수 관할지는 보통 다음 세 가지 범주 중 하나에 속한다. 첫째는 행정부 내부에 있는 경우다(예: 일부 감찰관). 두 번째는 행정부와 의회로부터 독립되어 있는 경우다. 마지막은 의회 기구인 경우다.

3.2.1 내부 민원 처리 기구

일부 관할권이 두고 있는 내부 감시 기구는 정치 행정부가 정보기관을 감독하는 수단의 역할을 한다. 이들 기구는 단순히 개별 장관이거나 경우에 따라 감찰관이라고 부르는 특별 장관 대리일 수 있다. 하지만 일부 관할권에서는 감찰관이 진정으로 독립적 기구일 수 있다는 점에 유의해야 하는데, 감찰관의 임기가 보장되며 행정부와 정보기관의 명령과 통제보다 감찰관이 우선하는 운영상 독립성을 갖고 있다. 일부 경우에는 내부 기구가 공공 민원을 접수할 자격을 가질 수도 있다.[31] 행정부의 관점에서 보면 이러한 방식은 민원에서 쟁점이 될 수 있는 기밀 정보를 매우 협소한 영역 밖에서 공유해야 할 필요성을 최소화한다. 동시에 내부 민원 처리 기구는 정보기관을 담당하는 조직으로부터의 독립성과 자율성이 결여되어 있다. 일반 대중은 이러한 기구가 "고양이에게 생선 가게를 맡기는" 데서 비롯되는 이해 상충에 취약하다고 인식하고, 내부 민원 처리 절차의 정당성에 의심을 품을 수 있다.

3.2.2 독립적 민원 처리 기구

구조

보다 독립적이지만 여전히 제한적으로 전문화된 민원 처리 기구는 기밀 정보 유포를 제한할 필요성과 공적 정당성을 증진할 필요성 사이의 명백한 타협에 해당된다. 많은 관할권이 정보기관 및 여타 행정부로부터 인력과 운영이 독립되어 있는 전문가 감독 기구를 설립했다. 이들 기관은 독립적 운영에서 비롯되는 신뢰를 누린다. 하지만 그럼에도 불구하고 이 기관들은 그 구성원이 기밀 취급 인가를 받고 기밀 정보를 맡을 만큼 정부와 충분히 가까울 수 있다. 이것이 바로 기밀 정보의 유통에 대한 정보기관의 우려를 완화하기 위해 최초의 이러한 기구 중 하나인 캐나다의 SIRC에 적용되는 법률에 성문화된 관행이었다. SIRC 위원들은 연방 행정부가 임명하지만 의회에서 야당과의 협의를 거쳐야 한다. 위원들은 재임 가능한 5년의 실질적 임기 보장을 받으며, 비록 행정부 재정 관리 부처의 승인을 받아야 하지만 자신의 보좌진을 고용할 수 있다. 위원 각자는 비밀 서약을 하며, 캐나다 공무원 비밀 유지법의 적용을 받는다.[32]

캐나다 시스템에서는 특정 전문성을 가진 개인의 임명이 의무적이지 않지만 이와 다른 방식을 사용하는 관할권도 있다. 예를 들어 케냐의 정보기관 민원위원회는 판사인 위원장 1명과 4명의 다른 위원들로 구성되는데, 그 중 한 명은 7년 이상의 계속적 경력이 있는 "변호사(advocate)"고, 한 명은 "국가적 명성"이 있는 "종교 지도자"여야 한다. 위원장은 "사법제도위원회의 조언에 따라" 대통령이 임명하며, "3년 간 직을 유지해야 하고," 최고 두 번의 임기까지 재임용될 수 있다.[33] 벨기에의 Committee I은 상원이 임명하고, 임기는 6년으로 재임이 가능하며, 위원들은 법률 지식과 관련 경험 면에서 일정 기준을 충족해야 하고, 경찰이나 정보기관 구성원이어서는 안 된다.[34]

이러한 독립적 임명 시스템의 선의(bona fides)를 멀리서 평가하기는 어렵다. 하지만 그 원칙은 건전한 것이다. 게다가 자격 및 직업적 배경을 요구하는 임명 시스템은, 그것이 배타적인 피임명자 계급 제도를 만드는 효과만 없다

면 정당하다. 임명 기준이 지나치게 협소하고 까다로우면 적합한 후보자 집단이 정보기관 배경이 있는 사람들로 제한될 수 있는데, 이는 감독 기구가 감독 대상 정보기관에 의해 "포획(capture)"되었다는 인식으로 연결될 수 있다(실제로는 안 그렇더라도).

영국의 수사권재판소는 상당히 다른 직업적 요건의 예를 보여 주는데, 사법부 고위직이었거나 10년 이상 법조인이었던 사람들로만 충원된다.[35] 하지만 법조인과 전직 판사로만 구성되는 자격 요건 역시 극단적일 수 있다. 광범위한 공익에 봉사하는 기구는 다양한 시각과 직업 경력이 반영되도록 구성원을 임명하는 방식이 일정한 장점을 갖는다.

이것이 캐나다의 SIRC를 움직이는 것으로 보이는 철학이다. 즉, 전문 자격 요건이 없는 것이다. 위원 자격은 현재 연방 입법부에 속하지 않은 캐나다 추밀원 고문이기만 하면 된다. 실제로 잠재적 후보자에는 전직 고위 정치인, 지도적 판사, 이 명예를 위해 선발되는 "저명한" 개인들이 포함된다. 나중에 SIRC 위원이 될 목적으로 어떤 사람이 추밀원에 임명되는 것도 전적으로 가능하다. 바꿔 말하면 SIRC 위원 자격은 완전히 개방되어 있어 이 기구가 (적어도 원칙적으로는) 보다 폭넓은 대중을 대변한다는 것이다.

하지만 캐나다 방식의 유연성이 지나치면 잘못될 수 있다. 준사법적 기능을 갖는 민원 처리 기구를 완전히 非법조인으로 채운다는 것은 불성실해 보이며, 현재의 캐나다 SIRC를 보건대 결국 그럴 가능성도 있다. 위원들의 다른 자질이 무엇이건 간에 법률 훈련의 부족은 민원 처리 기구의 법률 보좌진에 대한 의존을 낳을지 모른다. 이는 다시 이런 법률 보좌진의 경력 경로와 정부 내에서의(잠재적으로는 정보기관도 포함하여) 이동을 신중히 평가해야 하는 상황으로 연결된다. 행정부에 들어가고 나오기를 반복하는 직업 공무원들에게 구성원을 의존하게 되면 민원 처리 기구의 독립성이 손상될 수 있다(혹은 손상된 것으로 인식될 수 있다). 이 점을 볼 때 이상적인 모형은 다양한 배경을 지닌 복수의 구성원으로 이루어지되 그 중에는 예컨대 법률 훈련을 받은 최소한의 인원 할당이 있는 민원 처리 기구일 수 있다.

기능

일부 관할권에서는 민원 접수와 조사만을 전담하는 감독 기구를 설립했다. 예컨대 영국의 수사권재판소는 "정보국 - 국내 정보국(MI5라고도 함), 대외 정보국(MI6라고도 함), GCHQ(정부 통신 본부)의 행위 혐의 또는 정보국을 대신한 행위 혐의에 관한 일체의 민원을 조사할 수 있다."[36]

이들 전문가 감독 기구의 주요 기능이 독립적인 정보기관 성과 심사 또는 장관이나 의원들을 대신한 심사인 경우도 있다.[37] 하지만 이들 기구가 감독을 위임 받은 정보기관과 관련된 민원을 접수(및 조사)할 권한을 가질 수도 있다.[38] 가령 노르웨이의 의회 정보감독위원회의 경우, 위원들은 의회에 의해 선출되지만 제도적으로는 입법부의 일부가 아니다. 이 위원회는 자발적으로 정보기관의 행위를 조사할 수 있을 뿐 아니라 일반 대중의 민원을 접수하고 조사할 수도 있다.[39] 마찬가지로 벨기에의 Committee I은 "정보기관, 위협평가조정단, 기타 지원 기관 및 그 인력의 운영, 개입, 행위 또는 부작위와 관련하여 접수한 민원과 고발을 다룬다."[40] 행정부에서 독립되어 있고 아래 언급하는 의회 감독 위원회에 책임을 지는 남아공 정보 감찰관(IGI)도 비슷한 기능을 수행한다. 감찰관은 "구성원의 행위나 부작위를 통한 행정 실책, 권한 남용, 헌법, 법률 및 [정보 및 방첩 관련] 정책의 위반, 부패, 부정 축재 혐의에 관한 일반인 및 기관 구성원의 민원을 접수하고 조사"할[41] 수 있다.

일부 관할권의 경우, 이들 감독 기구에 민원을 제기하기 전에 정보기관에 통보해야 한다. 예를 들어 캐나다에서는 공공 민원을 먼저 CSIS 국장에게 제기해야 한다. 그 다음 SIRC는 위원회가 합리적이라고 보는 기간 안에 국장이 응답하지 않거나 부적절하게 응답하는 경우, 경솔하지 않은 선의의 민원을 조사할 수 있다.[42]

3.2.3 의회의 민원 처리 기구

다수의 관할권이 정보기관을 감독하는 특별한 의회 기구를 두고 있다. 위에서 설명한 일부 전문가 감독 기구와 마찬가지로 이 의회 위원회들도 정보기관 활동에 관련된 민원을 접수하고 조사하는 일을 맡을 수 있다.[43] 예를 들어

독일에서는 의회 컨트롤 패널이 민원을 심리할 수 있다.[44] 남아공에서는 의회 합동 정보 상임 위원회(정보기관 감독을 수행하는 의원 15명으로 구성된 기구)가 민원을 직접 조사하지는 않지만,

> *일반인이 믿기에 기관이 자신의 신체 또는 재산에 입힌 일체의 피해와 관련하여 위원회가 그러한 일반인에게서 접수한 민원에 대해 기관의 장 또는 감찰관의 조사를 명하거나 기관의 장 또는 감찰관의 보고서를 받을 수 있다. 단 위원회는 그러한 민원이 사소하거나 소송 남용이거나 악의에서 이루어진 것이 아님을 납득해야 한다.*[45]

의회 위원회에게 감독 기능과 민원 처리 기능을 모두 맡기면 보안 부문 전문성이 단일 기구에 집중될 수 있는 동시에 기밀 정보의 유포를 제한할 수 있다. 그러나 의회 감독 기구에 민원 처리 기능을 부여할 경우 여러 가지 문제점이 수반된다. 첫째, 의원들은 민원을 조사하고 재결하기에 충분한 전문성이나 시간이 없을 수 있다. 둘째, 의원들은 정의상 당파적 행위자다. 이는 현 정부의 행위와 관련하여 특별히 민감한 문제를 제기하는 민원을 적절히 조사하고 재결할 능력을 손상시킬 수 있다. 셋째, 민원 처리에는 세부 사항의 면밀한 검토, 절차적 공정성의 규칙, 그리고 예컨대 증인의 신뢰성과 관련된 증거에 입각한 심사가 필요할 수 있으며, 이는 보다 준사법적인 환경에서 더 잘 다룰 수 있다. 끝으로 의회 위원회는 구성원 수가 많아서 명확한 판결에 도달하고 이를 명확히 표명하기가 어려울 수 있다.

4. 민원 처리 절차 및 정보의 통제

이 짧은 도구에서 민원 처리 절차를 상세히 설명하기는 불가능하다. 그래서 기밀 정보 보호에 사용되는 절차와 몇 가지 일반적인 절차적 고려 사항에 초점을 맞춘다. 보다 일반적인 위임 사항(정보기관에 한정되지 않는 위임 사항)을 갖는 기구들이 사용하는 절차는 매우 다양하기 때문에 이 절에서는 위의 3.2절에서 논의한 전문적 (정보 및 국가 안보 관련) 민원 처리 기구(CHB)가 활용하는 절차에 초점을 맞춘다.

4.1 일반적인 절차적 규칙

일부 관할권의 준거법에서는 민원은 서면으로 제기해야 한다고 규정하고 있다.[46] 민원 처리 기구에는 경솔하거나 소송 남용이거나 악의로 이루어졌거나 기타 조사를 촉발할 만한 최소한의 한계에 미치지 못한다고 판단되는 민원을 기각할 권한이 부여될 수 있다.[47] 이러한 제한은 폭넓은 자격 규칙의 효과를 명백히 제한하여 기구로 하여금 명백히 가치가 없는 민원을 기각할 수 있도록 해 준다. 물론 까다로운 사건을 피하기 위해 무차별적으로 적용될 경우, 이러한 규칙은 민원 처리 기구의 감독 기능과 민원 처리 기능의 효과를 저해할 수 있다. 궁극적으로 이런 여과 규칙이 적절히 사용되도록 할 안전장치는 기구 자체의 독립성에 있다. 정부로부터 충분히 독립적이며 신중하고 능력 있는 사람들로 적절히 기구를 충원하면 추정적인 절차상 근거를 들어 논란이 큰 사건들을 피해 갈 유인은 거의 없을 것이다.

민원 처리 기구가 "경솔하고 소송 남용인" 민원과 "충분한 세부 사항이 수반되지 않은" 민원을 혼동하지 않는 것이 매우 중요하다. 이미 지적했듯이 은밀하고 비밀스러운 정보기관의 행위에 항의하는 민원에는 보다 공개적인 소송에 수반되는 풍부한 세부 사항이 부족할 것으로 예상하는 것이 합리적이다. 마찬가지로 단지 까다로운 민원 제기인에 대한 대응으로 "악의"를 근거 삼아 민원을 기각해서도 안 될 것이다. 막강한 정보기관을 상대로 민원을 시작한다는 것은 가장 집요한 사람들을 제외하면 누구든 단념하기 십상인 어려운 일이다. 민원 제기인, 그리고 특히 내부 고발자는 지켜보는 사람들로 하여금 민원의 정당성에 의심을 품게 할 만큼 특이한 성격의 소유자일 수도 있다. 신뢰성에 관한 의심을 불러일으킬 수 있는 성격적 특징과 분리해 사실관계를 분석하려면 특별히 신중을 기해야 한다.

청문회나 조사가 이루어지는 경우에는 적어도 일부 민원 처리 기구에 적용되는 규칙에서는 절차적 공정성의 기준을 부과해 예컨대 관련 당사자의 행위를 비난하는 판결이 이루어지기 전에 이들의 입장을 청취하도록 요구한다.[48]

4.2 민원 처리 기구의 권한

일부 민원 처리 기구는 문서의 작성 및 증인 출석을 강제할 권한을 가지고 있다.[49] 경우에 따라서는 이러한 권한이 상당히 강력해 변호인-의뢰인 특권 같은 것에 우선할 수도 있다.[50] 예를 들어 SIRC는 비공개 각료 회의 정보(기본적으로 각료 회의의 기록)를 제외하고 정보기관이 보유한 모든 정보에 접근할 수 있다. 미국 같은 다른 나라의 경우, CIA 감찰관은,

> *감찰관의 의무 수행에 그 증언이 필요한 기관 또는 기관 계약업체의 모든 직원에게 접근할 수 있어야 한다. 또한 감찰관은…감찰관에게 관련 책임이 있는 프로그램 및 업무와 관련된…모든 기록에 직접 접근할 수 있어야 한다... 직원 또는 계약업체가 감찰관에게 협력하지 않는 경우, 고용 상실 또는 기존 계약 관계의 종료 등 국장의 적절한 행정 조치의 근거가 된다.*[51]

다른 민원 처리 기구의 경우, 정보에 대한 접근이 더 제한된다. 남아공의 경우, 준거법에서 의회 정보 합동 상임 위원회가 정보기관 정보원의 신원을 밝힐 수 있는 정보에 접근하는 것을 금지하고 있다.[52] (반면 남아공 정보 감찰관의 업무에는 제한이 적어서 첩보, 정보 또는 [보안 기관] 부지에 대한 감찰관의 접근을 "어떠한 근거로도" 막을 수 없다.)[53] 민원 처리 기구의 비밀 정보 접근 제한은 자발적이거나 우발적인 누출 가능성을 제한하려는 명백한 노력이다. 그러나 제한은 민원의 시비곡직을 철저히 평가하는 민원 처리 기구의 능력을 손상시킬 수 있다. 달리 말하면 처음부터 민원 처리 기구는 불리함을 떠안게 될 수 있다. 따라서 유의미한 민원 처리 기구를 만들고자 한다면 이 점은 우려되는 사항이다.

정보 보안 난제의 부분적 해법은 민원 처리 기구 준거법에 정보 취급 요건을 규정하는 것이다.[54] 가령 남아공 정보 감찰관은 "정보기관의 직원에 적용되는 모든 보안 요건을 준수해야 한다."[55] 캐나다의 경우, SIRC 위원들은 캐나다 공무원 비밀 유지법에 구속되므로 비밀 정보를 부당하게 공개할 경우 기소 대상이 된다.[56]

정보의 물리적 흐름을 통제하기 위한 프로토콜도 갖춰져 있다. 예컨대 SIRC 조사원들은 일반적으로 CSIS 자체 시설에 있는 보안 설비가 갖춰진 SIRC 사무실에서 기밀 정보를 조회한다. 하지만 특히 해당 정보가 SIRC의 재결 대상 민원에서 쟁점이 되는 경우에는 정보를 SIRC 자체 보안 시설로 옮기기도 한다. 이러한 정보 취급 기반 시설을 만드는 데는 상당한 투자가 필요할 수 있고, 지리적으로 넓은 나라(캐나다 등)에서는 SIRC의 업무 수행 장소가 제한될 수 있다.

4.3 국가 안보 기밀

위의 논의가 시사하듯 국가 안보 관련 정보의 전문적 취급은 모든 민원 처리 시스템의 가장 중요한 책무다. 여러 민원 처리 기구의 준거법에서는 조사 및 (또는) 청문회를 비밀리에 실시해야 한다고 규정하고 있다.[57] 또한 민원 처리 기구의 조사 결과는 수정하거나 유포를 제한할 수 있다. 예컨대 호주의 정보기관 감찰관(IGIS)은 "관련 [정보] 기관의 장과 감찰관이 제안된 조건에 따라 민원 제기인에게 조사 결과를 제공하더라도 안보, 호주의 국방 또는 호주의 대외 관계에 피해가 없다는 데 동의할 때까지"[58] 민원 제기인에게 조사 결과를 제공해서는 안 된다. 남아공에서도 정보 감찰관(IGI)은 정부의 사전 허가 없이 제한된 정보를 공개할 수 없다.[59] 마찬가지로 케냐의 민원위원회는 그 직무 이행에 있어 "국가 안보 요건을 고려"해야 한다. 이를 위해 위원회는 "국가 안보를 위해 조사 과정에 있거나 조사와 관련된 정보 또는 특정 정보가 공개되어서는 안 되는 상황을 결정할 때"[60] 국가안보정보국(및 장관급 국가안전보장회의) 국장과 협의해야 한다. 노르웨이에서는 민원 제기인에게 보내는 위원회의 진술서는 "기밀 정보를 밝히지 않는 한도에서 최대한 완전해야 한다."[61]

비밀주의가 민원 제기인의 성공적인 민원 제기 능력을 손상시키기 때문에 일부 관할권에서는 청문회의 비공개 부분의 특별 절차를 이용해 민원 제기인을 도울 수 있다. 예컨대 캐나다에서는 SIRC 변호인은 다음과 같은 책임이 있다.

> *비공개 자료에 포함된 정보의 비공개 결정에 대한 이의 제기와 비공개 절차에서 정부측 증인 반대 심문… 경우에 따라 업무량 때문에 내부 변호인이*

당사자간 절차에서 충분히 역할을 할 수 없을 때 외부 변호인(또는 '법률 대리인')을 고용할 수 있다. 또는 사건에 특별히 공격적인 CSIS 반대 심문이 필요하다고 내부 변호인이 판단하는 경우, 법률 대리인을 고용할 수 있다.[62]

5. 구제

위에서 언급한 것처럼 민원 처리 시스템의 중심적 목표는 "실효적 구제"다. 특히 정보기관 민원 처리 기구가 제공하는 구제는 가령 피해 보상과 관련된 법적 구속력이 있는 결정보다는 권고에 그치는 경우가 많다.[63] 이런 제한적 권한은 여러 민원 처리 기구의 이중적 위임 사항을 반영하는 것일 가능성이 크다. 다시 말해 민원을 심리하는 기구와 정보기관의 행위에 대한 자율적 감독을 수행하는 기관이 동일한 것이다. 이런 감독 과정은 보통 관련 정보기관과 행정부에 대한 정책 및 관행 개혁 권고로 이어진다. 감독이 민원 처리 기구의 주된 기능인 경우에는 이들 기관을 만든 입법자들이 민원에 대해 강제적 보상 권한을 부여하는 것이 효과적 감독에 필요한 덜 적대적인 특성에 부합하지 않는다고 보았을 가능성이 높다.

하지만 실제로는 민원 처리 기구의 권한을 권고로 제한하면 민원 처리 기구가 정보기관을 부끄럽게 만들어 권고에 따르게 만드는 것 이상을 할 수 있는 능력을 제한할 수 있다. 이런 방식은 특히 위에서 지적한 흔한 관행인, 민원 조사 결과 자체가 기밀인 경우에 더욱 힘들어진다. 이런 이유로 민원 처리 기구가 공개 연례 보고서나 기타 방식을 통해 조사 결과의 수정 버전을 작성하는 방식은 장점이 있다. 하지만 이조차도 의원들과 언론의 관심은 놀랄 만큼 적을 수 있다. 가령 캐나다의 SIRC가 내놓은 때때로 과오를 강력히 시사하는 요약 보고서도 지속적인 관심을 거의 불러일으키지 못했다.

최악의 경우에는 단순한 권고 권한이 민원 처리 기구가 가진 다른 장점들을 줄이는 효과를 낼 수 있다. 잠재적 민원 제기인이 자신의 행동이 의미 있는 대응, 변화 혹은 보상을 가져올 것을 의심하게 되면 민원 처리 기구에 민원을 제기할 이유를 거의 찾지 못할 수 있다. 따라서 민원 제기인은 다른 경로(민원을 다루기에는 불리한 일반 법원 등)를 통해 민원을 제기하거나 반응을

이끌어낼 수 있으리란 희망을 품고 언론에 공개하거나 그냥 노력을 포기할 수도 있다. 이 모든 반응은 정보기관의 부정행위를 밝혀내고 그에 대응한다는 민원 처리 기구의 존립 근거를 허문다.

더 "사법부 같은" 권한을 지닌 기구들도 있다. 민원 처리가 독점적 업무인 민원 처리 기구의 경우가 특히 그렇다. 따라서 영국의 수사권재판소 같은 준사법 기구는 "영장의 기각, 보유한 기록의 파기 또는 재정적 보상 같은 구제 조치"를[64] 부과할 권한이 있다.

6. 권고 사항

민원 처리 기구에 관한 이 조사에 기초한 다수의 권고 사항이 있다. 이들은 뒤에 나오는 논의에 요약되어 표 1의 "우수 관행"으로 제시된다.

- 각국은 내부자 민원 및 공공 민원의 접수와 조사를 담당하는 민원 처리 기구를 만들어야 한다.

내부자 민원 처리 시스템은 "내부 고발"을 가치 있는 민원에 대응하는 동시에 기밀 정보 보호와 관련된 정부의 우려도 해소할 수 있는 제도적 틀 안으로 유도하는 수단에 해당된다. 하지만 이 시스템은 그에 따르는 자들도 보호해야 한다.

- 효과적인 내부자 민원 시스템에는 직원이 선의의 청구를 관계 당국에 제기하는 경우, 보복이 없으리라는 보장이 포함되어야 한다.

이에 비해 공공 민원 시스템은 더 광범위하며, 일반적으로 모든 사람들에게 열려 있다. 일반적으로는 대외 정보 업무와 관련해서만 민원 제기 자격에 제한을 두고, 그보다 훨씬 적은 경우기는 하지만 민원 제기인이 민원의 쟁점에 의해 어떤 식으로든 개인적으로 영향을 받았을 것을 요구하는 경우도 있는 반면 몇몇 관할권은 국적 요건을 부과한다. 이런 식의 자격 제한에서는 어떤 장점도 찾아보기 힘들다.

- 민원 처리 기구는 일반 대중으로부터 민원을 접수할 수 있는 광범위한 권한을 가져야 한다.

민원 제기 자격과 관련한 광범위한 규칙은 더 많은 민원을 민원 처리 기구에 제기할 수 있음을 의미한다. 이러한 규칙은 또 해당 기구의 잠재적 부담도 확대한다. 이 민원들 중 가치가 있는 민원으로 한정해 처리하는 것이 적절할 수 있다. 그러나 이 결정을 내리는 방식에 있어서는 주의해야 한다.

- 경솔하거나 소송 남용인 민원에 관한 우려는 민원 처리 기구가 처리 과정에서 조기에 이러한 민원을 기각할 수 있도록 하는 규칙으로 해소될 수 있다. 그러나 까다롭거나 정치적으로 논란이 되거나 단순히 상대하기 힘든 사람들이 제기한 민원이라는 이유로 기각하지 않도록 주의해야 한다.

관할지와 관련하여 각국은 일반 법원이나 전통적인 규제 기구가 정보기관과 관련된 민원을 충분히 다룰 수 있는지 여부를 신중히 고려해야 한다. 실제로 이 기구들은 기밀 국가 안보 및 (또는) 정보 문건을 취급할 수 없어서 효과성이 손상되고 민원을 충분히 조사하지 못하는 결과를 초래할 수 있다. 게다가 일반적 기구들은 이러한 사안을 철두철미하게 조사하는 데 필요한 주제 전문성이 부족할 수 있다.

이에 비해 정보 전문 민원 처리 기구는 기밀 정보 보호에 관한 우려를 해소할 수 있는 구조를 갖추고 있을 수 있다. 그와 동시에 이러한 비밀 유지에 관한 우려가 민원 처리 기구로서의 신뢰성이 사라질 정도로 전문 민원 처리 기구의 기능을 저하시켜서도 안 된다. 투명성이 기본이어야 하며, 비밀주의는 정당한 상황으로 제한되어야 한다. 이 밖에도 정부와 민원 제기인의 변론 능력이 어느 정도 균형을 이루게 하려는 노력이 있어야 한다. 정부가 비밀주의를 통해 입장을 숨길 수 있는 경우에는 기구 자신이 심문 방식을 통해 반드시 사안을 조사해야 한다. 나아가 감독 기구 구성원들 자신이 기밀 취급 인가가 있어야 하며, 정부와 정보기관이 보유한 정보에 전면적으로 접근할 수 있어야 한다.

- 대부분의 경우, 정보기관과 관련된 민원의 조사에는 일반적 민원 처리보다 전문 민원 처리 기구가 선호되어야 한다. 이러한 기구는 기밀 정보에 접근할 수 있는 매우 광범위한 권한을 갖춰야 하고, 이 정보가 (자발적 또는 우발적으로) 누출될 가능성을 줄이기 위한 안전장치를 시행해야 한다. 이러한 안전장치의 예에는 특별한 정보 취급 프로토콜과 적극적인 기밀 취급 의무가 포함된다.

그렇더라도 민원 처리 기구는 정부로부터 독립적으로 충원, 유지되고 적절한 자원을 갖추는 경우에만 신뢰를 받을 수 있다. 민원 처리 기구가 특정 직업 경력(예: 법조인)을 가진 사람들로만 구성되어서도 안 되지만 구성원 중에는 적정수의 법조인이 있어야 한다. 독자적인 법률적 역량은 법률 훈련을 받은 (그리고 아마도 그리 독립적이지 않을) 보좌진에 대한 과도한 의존을 최소화할 수 있다.

- 민원 처리 기구는 정부로부터 독립적이어야 한다. 실제에 있어 이는 이들의 임명 방식이 현 정부에 의한 일방적 임명이 아니고, 정부로부터 자율적으로 운영할 자유가 있으면서도 임기가 보장되는 것을 의미한다. 민원의 재결에서 정보기관 직원들에게 과도하게 의존하는 것을 피하려면 적어도 일부 구성원은 법률적 훈련을 받은 자여야 한다.

구제 문제는 민원 처리 시스템에서 가장 어려운 쟁점이다. 일반적으로 말해 정보기관의 부정행위에 대한 보상을 명할 수 있는 강력한 권한을 가진 기구(법원)는 정보기관을 둘러싼 특수한 상황, 특히 비밀주의와 기밀 정보의 요구와 관련된 민원을 다루기에는 가장 적절하지 않다. 전문가 감독 기구는 비밀주의의 안개를 뚫고 들어가기에 더 유리한 경우가 많지만 일반적으로는 권고하는 것 이상의 권한을 갖고 있지 않다. 각국은 민원 처리 기능이 부여된 전문가 감독 기구에 부당한 대우를 받은 개인들에 대한 재정적 보상을 명할 수 있는 권한과 같은 준사법적 구제 권한도 부여할지 여부를 신중히 고려해야 할 것이다.

- 민원 처리 기구에 단순한 권고 권한만 부여하는 것으로는 부족하며, "실효적 구제"에 해당되지 않는다. 오히려 이들 기구에는 재정적 보상을 명할 수 있는 권한 등 준사법적 구제 권한이 주어져야 한다.

마지막으로 각국은 정보기관 책임성 보장을 위해 민원 기반 모형에만 의존하는 것을 지양해야 한다. 민원 처리는 이러한 책임성 보장 과정에서 분명 의미가 있지만 이 기능의 수행을 위해 민원 처리 기구에 전적으로 의존하는 일부 국가들의 경험은 긍정적이지 않았다. 예를 들어 캐나다에서 연방 경찰(RCMP)이 행사하는 국가 안보 기능에는 허약한 민원 기반 책임성 메커니즘만 적용된다. 911 이후 RCMP의 의심스러운 테러 방지 관행에 관한 사법적 조사 위원회는 민원 처리 기능의 강화와 성과를 감사하는 심사 시스템을 권고했다. 조사 위원회는 "자체적으로 착수되는 심사의 필요성은 RCMP의 국가 안보 활동 대부분이 비밀스럽게 수행되고, 사법적 심사를 거의 받지 않으면서도 개인의 권리와 자유에 상당한 영향을 미칠 수 있다는 사실에서 비롯된다"고[65] 판단했다.

민원 기반 책임성에 근시안적으로 집중하는 경우, 일종의 책임성 "극장"을 만들 위험이 있다. 즉, 기구의 존재가 겉보기에는 견제와 균형을 만들어내는 것 같지만 정보기관 활동을 둘러싸고 있는 비밀주의로 인해 효과적으로 운영될 수 없는 것이다. 이 비밀주의는 정보기관의 목표가 된 사람들로 하여금, 가령 프라이버시 무단 침해를 의식하지 못하게 만들 수 있다. 이런 이유에서 부정행위를 밝힐 수 있는 다른 형식의 심사 및 감독이 수반되지 않는 민원 처리 시스템은 정보 거버넌스에 대한 나쁜 접근 방식에 해당한다.

- 정보기관 책임성에 대한 민원 기반 모형에 전적으로 의존하는 것은 적절치 않다. 이러한 방식은 독립적 심사 및 (또는) 감독 시스템으로 보완되어야 한다.

표 1: 민원 처리에 관한 모범 관행 체크리스트	
관행	관행에 따르지 않을 경우의 결과
민원 처리 기구가 사안 및 법률 전문성을 적절히 갖추고 있는가?	그렇지 않다면 효과적이고 확실하게 민원을 재결할 민원 처리 기구의 능력에 의문이 제기될 수 있다.
민원 처리 기구가 정보기관의 비밀 정보에 전면적으로 접근할 수 있는가?	그렇지 않다면 민원 처리 기구가 실제로 민원의 시비곡직을 판단하고 기관의 행위를 평가할 수 없을 위험이 있다.
민원 처리 기구가 임명 과정, 임기 보장, 운영 관리 측면에서 정부와 정보기관으로부터 독립되어 있는가?	그렇지 않다면 민원 처리 기구는 신뢰성이 결여되기 쉽고, 사실상 독립적 결정을 내리지 못할 수 있다.
민원 처리 기구가 내부자 민원과 공공 민원을 모두 허용하는가?	그렇지 않다면 내부자는 내부 고발(예: 언론)에 의존하게 될 수 있으며, 일반 대중은 민원을 일반 법원이나 국가 안보 사안을 다루기에 부적합한 그 밖의 기구에 제기할 수밖에 없다.
내부자가 선의의 민원을 제기할 경우, 고용법 및 (또는) 공무원 비밀 유지법에 따라 보복으로부터 보호되는가?	그렇지 않다면 내부자는 민원 처리 기구의 절차에 따를 유인이 없거나 아예 부정행위를 밝히지 못하게 될 것이다.
공공 민원에 대한 관할 규정이 모든 일반인이 정보기관의 모든 행위에 관해 민원을 제기할 수 있도록 광범위하게 되어 있는가?	그렇지 않다면 정보기관의 행위에 대한 정당한 우려가 주목 받지 못할 수 있다.
가치 없는 청구를 기각할 권한은 적절하지만 민원 처리 기구가 이 권한을 민원의 정치적 함의 또는 사안과 관련 없는 민원 제기인의 특징 같은 무관한 사항을 고려하지 않고 신중하게 행사하는가?	그렇지 않다면 정보기관의 행위에 관한 정당한 우려가 너무 쉽게 기각될 수 있다.
민원 처리 기구가 재정적 보상 등 준사법적 구제 권한을 가지고 있는가?	그렇지 않다면 민원 처리 기구의 결정은 정보기관의 행위에 거의 영향을 미치지 못하고 민원 제기인은 애초에 민원을 제기하는 것을 단념할 수 있다.

후주(後註)

1. Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Geneva: DCAF, University of Durham, and Parliament of Norway), p. 105.

2. Hans Born and Ian Leigh, Democratic *Accountability of Intelligence Services,* Policy Paper No. 19 (Geneva: DCAF, 2006) p. 17.

3. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight* (henceforth Scheinin Report), United Nations Document A/HRC/14/46 (17 May 2010), p. 10.

4. Scheinin Report, p. 10.

5. Scheinin Report, p.11 (citing Article 2 of the International Covenant on Civil and Political Rights).

6. Klass v. FRG, A 28 (1979), 2 EHHR 214 at para. 64 (construing Art 13 of the ECHR).

7. Scheinin Report, p. 11.

8. Canadian Security Intelligence Service Act (31 August 2004), R.S.C., Chapter C-23, Section 42 (available at http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).

9. Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Articles 28 and 30 (available at http://www.comiteri.be/images/pdf/engels/w.toezicht - l.contrle - engelse versie.pdf).

10. United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e) (2) (available at http://codes.lp.findlaw.com/uscode/50/15/I/403q).

11. United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (d)(5)(G).

12. New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 18 (available at http://www.legislation.govt.nz/act/public/1996/0047/latest/whole.html - dlm392526).

13. United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e)(3)(B).

14. Canada, Security of Information Act (1985), R.S.C., Chapter O-5, Section 15 (available at http://laws. justice.gc.ca/eng/acts/O-5/).

15. The Netherlands, Intelligence and Security Services Act (7 February 2002), Article 83 (as amended) (available at http://www.ctivd.nl/?download=WIV2002 Engels.pdf).

16. Ireland, Garda Síochána Act 2005, No. 20 of 2005, Section 67.

17. Canadian Security Intelligence Service Act (31 August 2004), R.S.C., Chapter C-23, Section 41 (available at http://www.csis-scrs.gc.ca/pblctns/ct/cssct-eng.asp).

18.United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e)(3).

19.Kenya, National Security Intelligence Service Act (31 December 1998), Section 24 (available at http://www.nsis.go.ke/act.pdf).

20.South Africa, Intelligence Services Oversight Act (23 November 1994), Section 3 (1) (f) (available at http://www.acts.co.za/intelligence_services_oversight_act_1994.htm).

21.New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 11.

22.Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 8(available at http://www.comlaw.gov.au/Details/C2011C00349).

23.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum,* United Nations Document A/HRC/14/46/Add.1 (26 May 2010), p. 50 (핀란드 논의).

24.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum,* United Nations Document A/HRC/14/46/Add.1 (26 May 2010) Paragraph 121 (베냉의 민원 메커니즘을 헌법재판소로 거명); Paragraph 294 (에콰도르의 주요 민원 관할지를 헌법재판소로 거명); Paragraph 243 (동일, 코스타리카와 관련); Paragraph 307 (보안 기관의 감시로 피해를 입은 사람의 주요 민원 메커니즘으로 법원을 거명); Paragraph 353 (그루지야 정보기관이 저지른 민사상 권리 침해와 관련한 법원의 역할과 형사상 권리 침해와 관련한 검찰총

장의 역할 논의), Paragraph 482 (라트비아의 시스템 논의); Paragraphs 556 – 557 (마다가스카르의 시스템 논의).

25.The Netherlands, Intelligence and Security Services Act, Article 83.

26.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum,* United Nations Document A/HRC/14/46/Add.1 (26 May 2010), p. 49 (핀란드 논의); Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *International Models of Review of National Security Activities* (May 2005), p. 14 (available at http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/IntlModels_may26.pdf).

27.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum,* United Nations Document A/HRC/14/46/Add.1 (26 May 2010), Paragraphs 67, 75, and 82 (벨기에 논의); Paragraph 327 (핀란드 논의); Paragraph 374 (그리스 옴부즈맨 기관의 역할 설명); 또한 Canada, Privacy Act (1985), R.S.C., Chapter P-21, Section 29 (available at http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html) 참조.

28.Canadian Human Rights Act (1985), R.S.C., Chapter H-6, Sections 45 – 46 (available at http://laws-lois. justice.gc.ca/eng/acts/H-6/page-15.html).

29.정부의 비밀주의 주장이 민사상 구제를 받을 원고의 능력을 손상시킨 (혹은 적어도 복잡하게 만든) 법원 판례는 *Mohamed v. Secretary of State for Foreign and Commonwealth Affairs,* [2009] EWHC 152 (Admin) (UK);

Mohamed v. Secretary of State for Foreign and Commonwealth Affairs [2009] EWHC 2549 (Admin) (UK); *Canada (Attorney General) v. Almalki,* 2011, FCA 199 (Canada); *Mohamed v. Jeppesen Dataplan, Inc.,* 614 F.3d 1070 (9th Cir. Cal. 2010) (United States) 참조.

30. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (2006), pp. 492–3 (available at http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/EnglishReportDec122006. pdf).

31. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum,* United Nations Document A/HRC/14/46/Add.1 (26 May 2010), Paragraph 380 (헝가리 보안 기관 활동과 관련한 민원을 접수할 헝가리 주무장관의 권한 설명); Paragraphs 521–523 (마케도니아의 내부 통제 시스템 논의); and United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q.

32. Canadian Security Intelligence Service Act (31 August 2004), R.S.C., Chapter C-23, Sections 35–37.

33. Kenya, National Security Intelligence Service Act (31 December 1998), Section 25.

34. Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Articles 28 and 30.

35. United Kingdom, Investigatory Powers Tribunal web site (available at http://www.ipt-uk.com/ default.asp?sectionID=1).

36. United Kingdom, Investigatory Powers Tribunal web site, "About IPT: What the Tribunal can investigate" (available at http://www.ipt-uk.com/ sections.asp?sectionID=22&type=top).

37. The Netherlands, Intelligence and Security Services Act, Articles 64 and 78.

38. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum,* United Nations Document A/HRC/14/46/Add.1 (26 May 2010) Paragraphs 270 and 271 (크로아티아 보안정보기관시민감독위원회의 기능 설명); Paragraph 279 (키프로스의 경찰 상대 고발 및 민원 독립 조사국의 기능 설명); Paragraph 396 (아일랜드Garda Síochána 옴부즈맨 위원회의 기능 설명); Paragraph 410 (일본의 현[縣]공안위원회의 기능 설명); Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 8 (as amended).

39. United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum,* United Nations Document A/HRC/14/46/Add.1 (26 May 2010) Paragraph 585; Norway, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services (3 February 1995), Section 3 (available at http://www.eos-utvalget.no/filestore/EOSAct.pdf).

40. Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Article 34.

41. South Africa, Intelligence Services Oversight Act (23 November 1994), Section 7(7)(cA).

42.Canadian Security Intelligence Service Act (31 August 2004), R.S.C., Chapter C-23, Section 41.

43.United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum,* United Nations Document A/HRC/14/46/Add.1 (26 May 2010) Paragraph 270 (describing the role of the Croatian parliamentary Committee for Internal Policy and National Security); Paragraph 380 (헝가리 의회의 국가안보위원회의 역할 설명); and Paragraphs 609–611 (루마니아의 양원 합동 위원회 설명, 단 이 기구는 다른 의회 위원회들의 승인이 있어야만 민원을 조사한다고 시사); Larry Watts, "Control and Oversight of Security Intelligence in Romania," in *Democratic Control of Intelligence Services,* eds. Hans Born and Marina Caparini (Aldershot, UK: Ashgate, 2007), p. 60 (루마니아 의회 위원회들이 심리하는 민원 논의).

44.DCAF, Backgrounder: Parliamentary Oversight of Intelligence Services (2006) (독일 의회 "컨트롤 패널"이 시민 민원을 심리할 수 있음을 지적); Germany, Control Panel Act (29 July 2009), *Federal Law Gazette* I, p. 2346, Section 8.

45.South Africa, Intelligence Services Oversight Act (23 November 1994), Section 3(1)(f).

46.Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 10 (as amended); New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 16.

47.Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 11 (as amended); South Africa, Intelligence Services Oversight Act (23 November 1994), Section 3(1)(f); New Zealand,

Inspector-General of Intelligence and Security Act (1 July 1996), Section 17; Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Article 34.

48. Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 19 (as amended).

49. Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 18 (as amended); Norway, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services (3 February 1995), Sections 4 and 5; Germany, Control Panel Act (29 July 2009), *Federal Law Gazette I,* p. 2346, Section 5; New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Sections 20 and 23; Kenya, National Security Intelligence Service Act (31 December 1998), Section 26; Belgium, Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment (18 July 1991), Article 48.

50. Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 18 (as amended).

51. United States, Inspector General for the Central Intelligence Agency, U.S. Code 50, §403q (e)(2). See, also, paragraphs (4) and (5).

52. South Africa, Intelligence Services Oversight Act (23 November 1994), Section 5.

53. South Africa, Intelligence Services Oversight Act (23 November 1994), Section 7.

54.South Africa, Intelligence Services Oversight Act (23 November 1994), Section 7; Germany, Control Panel Act (29 July 2009), *Federal Law Gazette I,* p. 2346, Section 10.

55.South Africa, Intelligence Services Oversight Act (23 November 1994), Section 7; See similar strictures in Norway, Act Relating to the Monitoring of Intelligence, Surveillance, and Security Services (3 February 1995), Section 9; New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 13.

56.Canada, Security of Information Act (1985), R.S.C., Chapter O-5, schedule.

57.Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 17 (as amended); New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 19; Kenya, National Security Intelligence Service Act (31 December 1998), Section 26.

58.Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 23 (as amended).

59.South Africa, Intelligence Services Oversight Act (23 November 1994), Section 5.

60.Kenya, National Security Intelligence Service Act (31 December 1998), Section 26.

61.Norway, Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS), Issued pursuant to section 1 of Act No. 7 of 3 February 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services, Section 8; See also New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 25.

62. Craig Forcese and Lorne Waldman, "Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of 'Special Advocates' in National Security Proceedings" (study commissioned by the Canadian Centre for Intelligence and Security Studies, with the financial support of the Courts Administration Service) (August 2007), pp. 7 – 8.

63. Canadian Security Intelligence Service Act (31 August 2004), R.S.C., Chapter C-23, Section 52 (SIRC의 권한 설명); Netherlands, Intelligence and Security Services Act, Article 84 (국가 옴부즈맨의 권한 설명); United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Addendum*, United Nations Document A/HRC/14/46/Add.1 (26 May 2010) Paragraph 77(벨기에 프라이버시 커미셔너의 권한 설명); and Paragraph 585 (노르웨이 감독 위원회의 권한 설명); Australia, Inspector-General of Intelligence and Security Act (17 October 1986), Section 24 (as amended); Norway, Instructions for Monitoring of Intelligence, Surveillance and Security Services (EOS), Issued pursuant to section 1 of Act No. 7 of 3 February 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services, Section 8; New Zealand, Inspector-General of Intelligence and Security Act (1 July 1996), Section 25; Kenya, National Security Intelligence Service Act (31 December 1998), Section 26. 64. United Kingdom, Investigatory Powers Tribunal web site, "Complaints process: What happens to my complaint?" (http://www.ipt-uk.com/sections.asp?sectionID=4&chapter=0&type=top); United Kingdom, Regulation of Investigatory Powers Act 2000, Chapter 23, Section 67.

65. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the National Security Activities* (2006), p. 18.

기고자 명단

한스 본(HANS BORN)은 DCAF 선임 연구원이다. 현재 보안 부문 거버넌스에서의 의회 및 옴부즈맨 기관의 역할과 정보기관 감독에 주력하고 있다. 그의 전문 지역은 동남아시아(캄보디아, 인도네시아, 필리핀, 태국 등)다. UN, 유럽 안보협력기구, 유럽 회의, 유럽 연합 의회를 위해 인권, 책임성, 보안 부문 거버넌스 분야의 연구를 수행했다. 그는 동남아시아 보안 부문 거버넌스 국제 의원 포럼(www.ipf-ssg-sea.net)과 국제 군 옴부즈맨 기관 컨퍼런스(www.icoaf.org)를 공동 설립했다. 보안 부문 개혁과 거버넌스에 관한 다양한 간행물을 출판했다. 최근 간행물로는 *Governing the Bomb: Democratic accountability and civilian control of nuclear weapons* (Oxford University Press, 2011), *Accountability of International Intelligence Cooperation* (Routledge 2011), *Parliamentary Oversight of the Security Sector: ECOWAS Parliament-DCAF Guide for West African Parliamentarians* (ECOWAS, 2011) 등이 있다. 네덜란드 트벤테(Twente) 대학에서 행정학 석사 학위를, 틸부르프(Tilburg) 대학에서 사회 과학 박사 학위를 받았다.

에이단 윌스(AIDAN WILLS)는 DCAF 조사부의 프로젝트 코디네이터로 6년 동안 보안 및 정보 거버넌스 연구를 해 왔다. 그는 정보기관 및 그 감독에 관한 UN 편찬물 작성 작업에서 수석 컨설턴트였다. 최근에는 중요한 유럽 연합 의회 연구서인 *Parliamentary Oversight of Security and Intelligence Services in the European Union*을 공동 집필했고, *International Intelligence Cooperation and Accountability*를 공동 편집했다. 그는 유럽과 중동 전역에서 정보 보안 감독 기구들을 교육했으며, 다양한 입법 과정에도 기여했다. 에이단은 보안 부문 거버넌스 및 인권의 다양한 측면에 관해 유럽 회의, 유럽 연합 의회, UN 특별 보고관(인권 및 테러 방지)의 컨설턴트 역할을 해 왔다. 현재는 열린 사회 재단(Open Society Foundation)이 주도하는 *Global Principles on National Security and the Right to Information* 편찬서 개발에 참여하고 있다.

모니카 덴 보어(MONICA DEN BOER)는 네덜란드 경찰학교에서 직책을 맡고 있으며, 국제 문제 자문 회의 유럽 통합 위원회(Committee on European Integration of the Advisory Council on International Affairs) 위원이다. 유럽대학원대학(European University Institute)에서 박사 학위를 취득했고, 에든버러 대학, 네덜란드 형사 법 집행 연구 센터, 유럽 행정 연구소, 틸부르프 대학, 유럽 법 집행 협력 연구소에서 일했다.
2004년 3월부터 2012년 1월까지는 네덜란드 경찰학교를 대표해 VU 암스테르담 대학에서 비교 행정 교수로 일했다. 2009년에는 네덜란드 이라크 조사 위원회 위원이었고, 2009-2010년에는 국방 미래 조사 그룹에 참여했다. 그녀는 유럽 내부 안보 협력에 관해 다양한 저작물을 발간했고, 교육, 코칭, 감독에 전념하고 있다.

스튜어트 파슨(STUART FARSON)은 사이먼 프레이저 대학 정치학 객원 교수이다. 1989-90년에는 캐나다 보안정보기관법에 대한 최초이자 유일한 법정 의회 심사의 연구 책임자로 일했다. 그는 마헤르 아라르 조사 위원회의 전문가 증인이었다. 최근에는 레그 휘태커(Reg Whitaker)와 공동으로 "Accountability in and for National Security," IRPP Choices(2009)를 집필했다. 또 Praeger에서 간행된 Commissions of Inquiry and National Security(2011)와 PSI Handbook of Global Security and Intelligence: National Approaches(2008)를 공동 편집했다.

크레이그 포르체세(CRAIG FORCESE)는 오타와 대학 법학부(관습법) 부학장 겸 조교수이다. 그는 국제공법, 국가안보법, 행정법, 공법/입법을 가르친다. 그의 현재 연구와 집필 상당 부분은 국가 안보, 인권, 민주적 책임성과 관련되어 있다. 현재 캐나다 국제법 회의 의장이다. *National Security Law: Canadian Practice in International Perspective*(Irwin Law, 2008) 등을 집필했고, *Human Rights and Anti-terrorism*(Irwin Law, 2008)을 공동 편집했다.

가브리엘 가이슬러 메세바게(GABRIEL GEISLER MESEVAGE)는 국제 개발 연구 대학원에서 박사 과정을 밟고 있으며, 조교로도 일하고 있다. 그는

이 대학원에서 연구 조교로 민간 부문 부패를 연구했다. 2010-2011년부터 가브리엘은 DCAF 조사부에서 일했으며, 경찰 및 정보기관 거버넌스를 집중 연구했다. DCAF에서 일하는 동안 DCAF *Toolkit on Police Integrity*의 외부 감독 절에 기고하기도 했다. 세인트 앤드류스 대학에서 국제 관계와 사회 인류학 석사 학위(MA First Class Honours)를 받았고, 국제 개발 연구 대학원에서 국제 연구 석사 학위를 받았다.

로렌 허튼(LAUREN HUTTON)은 2005년 이후 아프리카 보안 부문 개혁과 분쟁 후 변화에 관한 연구원 겸 실무자로 일해 왔다. 현재는 남수단에서 덴마크 데밍 그룹과 덴마크 난민 자문 위원회의 고문으로 일하면서 분쟁 민감도 및 무장 폭력 감소에 주력하고 있다. 로렌은 세이퍼월드(Saferworld)와 안보연구원(ISS)에서 일한 바 있다. ISS에서 일할 때는 아프리카 정보기관의 민주적 거버넌스 관련 프로젝트를 개발했다. 이를 통해 그녀는 남아공의 2007년 정보 심사 과정과 2009년과 2010년의 입법 초안 작성 과정에 조언을 제공했고. 남아프리카와 동아프리카의 의원들을 상대로 정보기관 감독에 관해 교육했다. 또 이 기간 동안 남아공 정보기관과 민주주의에 관한 책인 *To spy or not to spy*를 편집했고, 정보 거버넌스에 관한 몇 편의 잡지 기사와 논문을 발표했다. 로렌은 (남아공) 웨스턴케이프 대학에서 정치학 석사 학위를 받았다.

이안 리(IAN LEIGH)는 더럼 대학 법학 교수이자 더럼 국제 안보 연구소 회원이다. 그의 저작으로는 로렌스 러스트가르텐(Lawrence Lustgarten)과 공동 집필한 *In From the Cold: National Security and Parliamentary Democracy*(Oxford University Press, 1994), 한스 본, 로크 존슨(Loch Johnson)과 공동 집필한 *Who's Watching the Spies: Establishing Intelligence Service Accountability*(Potomac Books, 2005), 한스 본, 에이단 윌스와 공동 집필한 *International Intelligence Cooperation and Accountability*(Routledge, 2011)가 있다. 그의 정책 보고서 *Making Intelligence Accountable*(한스 본 공저, Norwegian Parliament Printing House 2005)은 14개 언어로 번역되었다. 그는 *OSCE/DCAF Handbook on Human Rights and Fundamental Freedoms of Armed Forces Personnel* (Warsaw, 2008)도 공동 집필했으며, OSCE 민주 제도

및 인권 사무국, 유럽 회의 내 보안 정보기관의 민주적 통제에 관한 베니스 위원회, 안보 부문 개혁 UNDP의 컨설턴트 역할도 했다.

로리 네이선(LAURIE NATHAN)은 프레토리아 대학 중재 센터 원외 교수이다. 또 크랜필드 대학 객원 교수로서 정보 개혁 석사 과정을 가르치고 있다. 가장 최근 저작은 *Community of Insecurity: SADC's Struggle for Peace and Security in Southern Africa, Ashgate*(2012)이다. 남아공 정보장관심의위원회에서 일했으며(2006-2008년), 남아공 국방 백서 초안을 작성했다(1996년). 그는 휴먼 라이츠 워치 군대 부문 자문 위원회, 카터 센터 국제 분쟁 해결 회의, UNDP 민주적 거버넌스 관행 네트워크 전문가 자문 그룹 회원이었다. 현재는 UN 중재 인명부와 UN SSR 전문가 인명부의 회원이다.

켄트 로치(KENT ROACH)는 토론토 대학 법학 교수로 법학 및 공공 정책 프리차드 윌슨 체어(Prichard Wilson Chair)로 재직하고 있다. 그는 마헤르 아라르 조사 위원회 조사 자문위 위원이었으며, 에어 인디아 폭파 사고 조사 위원회의 조사국장이었다. 가장 최근 저작은 The 9/11 *Effect: Comparative Counter-Terrorism*(published by Cambridge in 2011)이다.

베르트 반 델덴(BERT VAN DELDEN)은 1966년부터 네덜란드 사법부에서 일했다. 그는 1990-2001년까지 헤이그 지방 법원장이었으며, 당시 사법위원회 수석위원으로 임명되었다. 사법부에서 은퇴한 후에는 네덜란드 정보보안기관 심의위원회(CTIVD) 위원으로 임명되었다. 2009년 이후 이 위원회 위원장으로 일하고 있다.

테오도르 빙클러(THEODOR H. WINKLER)는 2000년에 스위스 연방 평의회가 대사 직으로 승진시켜 새로 만들어진 군대의 민주적 통제를 위한 제네바 센터(DCAF) 책임자로 임명한 이후 DCAF 소장으로 재직해 왔다. 그는 1981년 후반에 국제 안보 전문가로서 스위스 국방부에 참여했다. 1985년에는 정치 군사 문제 참모총장 대리로 임명되었고, 1995년에는 신설된 국제 안보 정책부 책임자가 되었다. 그 후에는 안보 국방 정책 차장직으로 승진했다.

빙클러는 제네바 대학, 하버드 대학, 제네바 국제 연구 대학원에서 정치학과 국제 안보를 연구했다. 그는 1981년에 핵 확산에 관한 논문으로 정치학 박사 학위를 취득했다.

정보기관 감독

도구 모음

이 도구 모음은 정보 거버넌스에 관한 전 세계 주요 전문가들이 집필한 소책자들을 요약한 것이다. 이 도구 모음은 정보기관 감독 체계의 구축과 통합 및 정보수집, 개인정보 사용, 국내 및 해외 파트너와의 정보공유, 재정 등 구체적인 정보기관 업무 분야 감독에 관한 정책 관련 지침을 제공한다. 이 지침은 수많은 나라의 법률적, 제도적 틀과 관행에 기초하고 있다.

이 도구 모음은 의회 감독 기구와 독립적 감독 기구에 초점을 맞추고 있지만 행정부, 사법부, 언론, 시민 사회 및 정보기관 자신과도 관련되는 수많은 통찰도 포함하고 있다. 감독 기구 구성원과 보좌진, 감독 업무 감시에 관련된 행위자(예: 언론, 시민 사회 조직 및 의원들), 외부 감독 대상, 행정부 및 정보기관은 이 도구 모음에 특히 관심을 가질 만하다.

군대의 민주적 통제를 위한 제네바 센터(DCAF)는 국제 사회의 굿 거버넌스 및 안보 부문 개혁 추진을 지원하는 것을 사명으로 하는 국제 재단이다. DCAF는 규범과 기준을 개발, 증진하고, 맞춤형 정책 연구를 수행하며, 민주적 안보 부문 거버넌스 증진을 위한 모범 관행과 권고안을 파악하고, 국내 자문 지원과 실용적 지원 프로그램을 제공한다.

www.dcaf.ch