국외 전기통신 서비스 감청제도 시행 동향

박소영* 김성혜** 강신각***

공공안전과 국가보안의 확보를 위한 방안으로, 여러 국가에서 통신 서비스에 대하여 감청을 집행하고 있다. PSTN 기반 유선전화 서비스와 이동전화 서비스에 대하여 큰 어려움 없이 감청을 집행했던 것과 달리, 2000 년대 들어 IP 기반 통신 서비스가 발달함에 따라 기존의 감청제도 및 기술로는 효과적인 감청 수행이 어려워지게 되었다. 이에 따라, 독일, 네덜란드 등 주요 유럽 국가들과 미국 등에서는 다양한 통신 서비스에 대한 감청을 효과적으로 수행하기 위한 감청제도를 정비하였거나 추진 중에 있으며, 관련하여 감청 기술표준과 솔루션을 개발 및 도입하고 있다. 이에, 본 고에서는 미국, 영국, 독일, 네덜란드, 호주 등 감청제도가 잘 발달된 것으로 알려진 국가들에 대하여 감청제도 수립 및 시행 동향을 분석하고자 한다. ▨

목 차

* ETRI 통합망표준연구팀/연구원
** ETRI 통합망표준연구팀/선임연구원
*** ETRI 통합망표준연구팀/팀장

Ⅰ. 서 론

감청(Lawful Interception: LI, 監聽)은 합법적인 형태의 도청을 의미하며, 통신비밀보호법에서는 감청을 “전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다”고 정의하고 있다[1]. 공공의 안전과 국가의 안보를 확보하기 위하여 미국과 유럽을 비롯하여 많은 국가에서 통신 서비스에 대한 감청을 제도화하여 시행하고 있다. 그러나, 당사자의 동의 없이 이루어지는 감청은 개인의 사생활을 침해할 소지가 있기 때문에 대부분의 국가에서 꼭 필요한 경우에 한하여 제한적으로 감청이 이루어지도록 하고 있으며, 감청의 오남용을 막기 위한 제도적·기술적 방안을 마련

하여 적용하고 있다. 특히 2000 년대 초반 IP 를 기반으로 하는 멀티미디어 서비스가 확대됨에 따라, 기존의 감청제도 하에서는 효과적으로 감청을 수행하기가 어려워졌다. 이에 따라, 미국, 네덜란드, 독일, 영국 등의 국가에서 IP 기반 통신 서비스 등 다양한 통신 서비스에 대한 감청을 수행하기 위한 제도적 기반을 마련하였으며, 한국, 중국, 호주 등에서는 이와 같은 통신시장 환경의 변화를 고려하여 감청제도를 재정립하고 있다.

II. 국외 감청제도 동향

1. 미국의 감청제도

가. 감청 의무 부과

미국에서는 이동통신과 IP 기반 통신 등 다양한 통신기술의 발달에 대응하여 효과적인 감청을 수행하기 위하여, 1994 년 10 월 통신사업자에게 감청 수행을 위한 기능구비 의무를 부과하는 것을 주요 골자로 하는 CALEA(Communications Assistance for Law Enforcement Act, 법집행을 위한 통신지원법)를 제정하였다.

CALEA 에서는 전기통신사업자(Telecommunications Carrier)로 하여금 전기통신의 감청을 수행하기 위한 능력을 갖추도록 규정하고 있다. 여기에서 전기통신사업자란 PSTN 기반 유선전화 서비스 제공업자와 PCS 서비스, 셀룰러 서비스, 위성이동통신 등을 포함하는 상업용 무선통신 서비스(Commercial Mobile Radio Service: CMRS) 제공업자, 호 부가 서비스 제공업자 및 일부 재판매 통신사업자를 포함한다. 그러나, 자가용 무선통신 서비스(Private Mobile Radio Service) 제공업자, 정보 서비스 제공업자, 사설 네트워크 제공업자 및 FCC 가 제외하는 전기통신사업자에 대해서는 해당 의무를 부과하지 않는다[2]. 인터넷 접속 서비스와 인터넷전화 서비스의 경우 정보 서비스로 분류되어 해당 서비스 제공업자가 전기통신사업자에 포함되지 않았으나, FCC 가 2005 년 9 월에 설비기반 광대역 인터넷 접속 서비스 제공업자(Facilities-based Broadband Internet Access Providers)와 상호연동 인터넷전화 서비스 제공업자(Providers of Interconnected VoIP Service)를 전기통신사업자로 재해석함에 따라 CALEA 의 준수 의무를 가지게 되었다. 상호연동 인터넷전화 서비스란 구체적으로 실시간 양방향 음성 통신을 가능하게 하며, 사용자가 광대역 접속을 필요로 하며, IP 와 호환되는 가입자 장치를 필요로 하며, 서비스 이용자가 PSTN 으로부터 호를 받고 PSTN 으로 호를 종료시킬 수 있는 인터넷전화 서비스를 말한다. FCC 는 해당 사업자들이 CALEA 요구사항을 준수하는 데 필요한 시간으로 18 개월의

유예기간을 부여하였다[3]. 이와 같은 FCC 의 명령에 따라, 설비기반 광대역 인터넷 접속 서비스 제공업자 및 상호연동 인터넷전화 서비스 제공업자는 2007 년 5 월까지 CALEA 준수를 위한 감청 기능 구비를 완료해야 하나, 2007 년 말 기준, 표준 및 기술 개발 등의 문제를 이유로 감청 기능의 구비가 완료되지 않은 것으로 파악되고 있다.

나. 비용 보전

전기통신 서비스 제공업자가 CALEA 에 근거하여 감청 기능을 구비하는 데 소요되는 비용의 보전과 관련하여, 미국에서는 CALEA 발효일인 1995 년 1 월 1 일을 기준으로 그 이전에 도입된 장비, 설비 및 서비스에 대해서는 소요 비용을 국가가 부담하도록 규정하고 있다. 그러나, 1995 년 1 월 1 일 이후에 도입된 장비, 설비 및 서비스의 경우 원칙적으로 전기통신사업자가 소요 비용을 부담하는 것으로 규정하고 있다. 전기통신사업자가 1995 년 1 월 1 일 이후에 도입된 부분에 대하여 비용보전을 청원할 경우 심사를 통하여 비용을 보전 받을 수 있으나, FCC 는 이 규정이 매우 제한적으로 적용되는 것이라고 밝히고 있다. 1995 년 1 월 1 일 이전에 도입된 장비, 설비 및 서비스에 대하여 국가가 비용을 보전하는 범위는 감청을 위한 기능 등의 개발을 위한 직접비용, 지원능력의 제공을 위한 직접비용, 관련 인력의 훈련비용, 감청 기능 등을 설치하는데 소요되는 직접비용으로 정하고 있다[4]. 감청 기능 구비 비용을 국가로부터 보전 받지 못하는 부분에 대해서는 해당 비용을 통신 서비스 요금에 반영하여 서비스 이용자로부터 간접적으로 보전하는 것이 가능하다. 또한, 감청기능 초기 구축비용이 아닌 감청 수행에 소요되는 비용은 수사기관으로부터 감청비(Intercept Charge)를 받아 보전할 수 있다[5]. 미국에서는 1995 년 1 월 1 일 이전에 도입된 장비 등의 감청기능 구비를 위하여 2001 년까지 약 5 억 달러의 예산을 마련하여 대부분 집행한 것으로 밝히고 있다.

다. 감청 보안 관리

승인되지 않은 사람이 감청 관련 정보에 접근하는 것을 차단하고, 불법적인 감청의 수행을 방지하는 등의 감청에 대한 보안 관리는 매우 중요한 사안으로, 각 국가에서는 감청의 보안성을 높이기 위한 정책적, 기술적 대책을 수립하여 시행하고 있다. 미국에서는 감청 설비나 장비가 법적 승인을 받은 경우에만 감청 수행과 통화식별 정보에 접근이 가능하도록 하는 능력을 가지도록 하고, 전기통신사업자로 하여금 시스템 보안과 무결성을 위한 적절한 조치를 취하도록 하고 있다. FCC 는 이러한 감청 보안 요구사항을 만족시키기 위하여 전기통신사업자들이 준수해야 하는 규칙을 담은 시스템 보안 및 무결성 규칙(System Security and Integrity Regulation)을 제

정하였다. 이는 감청 보안 관리 측면에서 전기통신사업자가 직원의 감독과 관리를 위한 정책 및 절차 수립을 위하여, 그리고 감청과 정보 접근에 대한 안전하고 정확한 기록 보관을 위하여 지켜야 할 사항들을 명시하고 있다.

2. 네덜란드 감청제도

가. 감청 규제

네덜란드는 1970 년대부터 PSTN 기반의 유선전화 서비스에 대하여 감청을 수행하였다. 감청 수행 초기에는 가장 단순한 형태의 전화통화에 대해서만 감청이 가능하였으나, 감청 방식이 액세스 기반에서 서비스 기반으로 발전함에 따라 2003 년부터 호 전환이나 메일박스 등의 지능형 전화 서비스에 대한 감청이 가능하게 되었다. 이동전화의 경우 1990 년대 초부터 아날로그 네트워크에 대하여, 1990 년 중반부터는 GSM(Global System for Mobile Communication)에 대하여 감청을 수행하고 있다. 이메일을 비롯한 IP 서비스에 대한 감청은 2001 년부터 수행하고 있으며, 인터넷전화에 대한 감청은 2004 년도부터 시작한 것으로 파악된다.

네덜란드에서는 형사소송법(Code of Criminal Procedure), 국가보안법(State of Security Acts), 통신법(Telecommunication Act 1998) 등에서 감청 수행과 관련된 사항들을 규정하고 있으며, 이 법들은 감청 집행에 대하여 상호 보완적인 역할을 수행하고 있다. 형사소송법에서는 주로 감청 요청에 따른 감청의 시행 및 운용과 관련된 사항을 규정하고 있으며, 통신법에서는 주로 감청 수행과 관련한 통신사업자의 책임을 규정하고 있다. 감청이 공공안전 및 국가보안을 위하여 필요성이 인정되고는 있으나 개인의 사생활을 침해할 수 있는 수사방법인 만큼, 형사소송법에서는 감청을 수행할 수 있는 상황에 대한 조건을 다음과 같이 엄격하게 규제하고 있다.

- 대상 범죄가 4 년 구금 이상을 받을 것으로 예상되는 중범죄일 경우
- 생명을 위협하는 상황일 경우
- 수사가 감청을 통하여 마무리될 수 있으며, 감청 결과가 혐의 대상자의 유죄 또는 무죄 판단에 사용될 수 있을 것으로 여겨지는 경우

위와 같은 조건을 만족하는 중대한 범죄에 대하여 감청하고자 할 경우, 수사기관은 법원의 심사를 거쳐 영장을 발급받아 감청을 수행할 수 있다. 영장 심사 시 법원은 범죄의 수사를 위하여 감청보다 감청 대상자의 사생활을 덜 침해할 방법이 없는지의 여부와 감청 필요성과 사생활 침해의 경중을 비교하여 감청 허가 여부를 판단하게 된다. 이 밖에도, 감청 결과의 활용 및 감청 사실의 통보 등과 관련하여 감청의 오남용과 부작용을 줄일 수 있는 방안들을 법에서 명시하고 있다.

나. 감청 의무 부과

네덜란드 통신법에서는 감청 수행과 관련한 통신사업자의 책임을 규정하고 있는데, 인터넷 서비스를 포함하여 모든 전기통신 네트워크(Telecommunication Network) 및 전기통신 서비스(Telecommunication Service) 제공업자들로 하여금 서비스 개시 시점에 감청이 가능하도록 규정하고 있다. 그러나, 이와 같은 의무는 공공전기통신 네트워크 및 공공전기통신 서비스 제공업자에게만 적용되며, 사설 네트워크에는 적용되지 않는다. 공공전기통신 네트워크 및 공공전기통신 서비스 제공업자는 통신법의 규정에 따라, 수사기관에게 그들의 네트워크와 서비스에의 접속을 제공하고, 당국이 법적 권한을 행사하기 위해 필요한 모든 정보를 제공할 의무 등을 가진다. 통신법에 따라 감청 수행과 관련한 비용 중 감청 시스템의 구축 및 유지를 위한 구조적 비용과 임시 비용은 통신사업자가 부담하고, 수사기관으로의 감청 정보 전달과 관련된 관리 비용 및 인력 비용 등 감청 수행과 관련된 비용은 수사기관이 부담한다.

다. 감청 정보 처리

감청 능력을 갖추어야 하는 전기통신 네트워크 및 전기통신 서비스 제공업자는 당국이 전기통신을 기록 및 도청하는 것에 대한 그들의 법적 권한을 행사하기 위해 필요한 모든 정보(이름, 주소, 전화번호, 제공되는 전기통신 서비스의 종류 등)를 전달해야 한다. 그러나, 당국이 필요로 하는 정보 외의 이용자 데이터(이용자 및 가입된 서비스에 대한 정보) 또는 트래픽 데이터(통신서비스의 실제 사용에 대한 정보)를 저장해야 할 의무는 없다. 다만, 선불 전화카드와 같이 제공업자가 당국이 필요로 하는 정보를 얻어내지 못할 경우, 제공업자는 트래픽 데이터 등 다른 데이터를 보관해야 할 수도 있다. 또한, 제공업자들은 당국이 운영하는 중앙정보지점에서 24 시간 접근할 수 있도록 그 정보를 보관해야 한다.

제공업자가 당국으로 감청 정보 전달 시 제공업자의 네트워크 혹은 서비스와 당국의 설비 간 연결 구성이 사람들로 하여금 전기통신의 내용을 알아챌 수 있게 되어 있다면, 전기통신은 당국이 제공업자와 협의하여 결정한 방식에 따라 암호화되어야 한다. 감청 및 전달 포맷에 대한 기술 규격(Technical Specifications)을 결정하는 것은 당국의 몫이며, 이 때 당국은 해당 제공업자와 이에 대하여 상의하여야 한다[6].

라. 감청 보안 관리

네덜란드는 2003 년 10 월에 전기통신의 감청을 통하여 습득한 정보에 대하여 공공전기통신 네트워크 및 공공전기통신 서비스 제공업자가 취해야 하는 보안 조치를 담은 법령(Decree on

security of data on telecommunication lines tapped)을 발효하였다. 이 법령이 담고 있는 주요 내용은 다음과 같다.

- 제공업자는 지정된 데이터 및 정보에의 승인되지 않은 접근을 막기 위하여 모든 필요한 보안 조치를 마련해야 함
- 보안 조치가 기본적으로 포함해야 하는 사항 명시
- 제공업자는 보안 조치를 취하기 위하여, 제공업자의 의무를 이행하는 방법을 구체화하는 보안 계획을 준비해야 함
- 당국으로부터 그 결과에 대한 요청을 받을 경우, 제공업자는 보안 계획에 대한 당국의 검사를 허락해야 함
- 제공업자는 지정된 종류의 데이터 또는 정보의 기밀과 관련하여 승인되지 않은 위반이 발생하였을 때, 즉시 관련 당국에 알려야 함
- 제공업자는, 감청과 관련하여 특정한 임무를 맡은 직원들이 그 임무 및 그들이 취득하는 데이터와 정보에 대한 기밀을 지키도록 해야 함
- 제공업자가 작업 수행을 위해서 제 3 자와 계약을 맺고, 제 3 자가 감청 관련 데이터 및 정보를 습득할 수 있을 경우, 제공업자는 그 제 3 자로 하여금 정해진 보안 수칙을 지키도록 해야 함[7]

이 밖에도, 이 법령에서는 승인되지 않는 자가 감청 관련 정보에 접근하는 것을 막기 위한 보안조치로서 포함되어야 하는 구체적인 방법들을 부록에서 규정하고 있다.

3. 독일 감청제도

가. 감청 규제

독일에서는 전기통신법(Telecommunication Act), 전기통신감청령(Telecommunications Interception Ordinance) 및 시행규칙(Technical Directive)에 기반하여 감청의 기술적인 부분을 규제하고 있다. 전기통신법은 통신시장의 모든 부분을 관할하는 법으로, 제 110 조에서 감청의 기술적 수행에 대한 사항들을 다루고 있다. 전기통신감청령은 감청 관련 의무를 가지는 주체의 범위와 기본 요구사항을 명시하고, 시행규칙을 만드는 절차와 승인절차 등에 대하여 기술하고 있다. 전기통신법과 전기통신감청령은 의회 입법을 통하여 제·개정이 이루어지며, 경제부를 중심으로, 국방부, 재무부, 내무부 등의 정부부처가 전기통신법 초안을 작성하는 데 참여한다. 연방 네트워크 중개소(Federal Network Agency)는 감청에 대한 기술적 요구를 담당하는 정부

기구로서, 해당 당국 및 산업체와 협의를 통하여 시행규칙을 제정하는 데 책임을 맡고 있다.

독일에서는 1995~1997 년에 최초로 전기통신감청령을 만들어 통신 서비스에 대한 감청을 시작하였다. 1999 년에 ETSI 의 감청 규격인 ES 201 671(Telecommunications security; Lawful Interception(LI); Handover interface for the lawful interception of telecommunications traffic)이 출판되었는데, 2001 년에 ES 201 671 의 내용을 반영하고 인터넷 상의 전송 보안에 대한 내용을 포함하는 시행규칙(Technical Direct)을 제정하였다. 2007 년 말 현재 시행규칙 5.0 버전이 이용되고 있으며, 인터넷전화와 멀티미디어에 대한 요구사항 등을 반영한 시행규칙 5.1 버전이 머지않아 발효될 것이라고 밝히고 있다.

나. 감청 의무 부과

전기통신법에서는 공공전기통신 서비스(Publicly Available Telecommunications Services)를 제공하는 전기통신설비 운영자로 하여금 감청 수행을 위한 장비를 갖추도록 규정하고 있다. 이에 따라, PSTN 유선전화, GSM 과 UMTS 기반의 이동전화, 이메일, 인터넷접속, 인터넷전화 등의 공공전기통신 서비스를 제공하는 전기통신설비 운영자는 감청 기능 구비 등의 의무를 가지게 된다. 이 때, 감청 기능의 구비는 전기통신설비 운영자의 비용으로 이루어진다.

전기통신설비를 운영하지 않으면서 공공전기통신 서비스를 제공하는 자의 경우 자신이 서비스를 제공하는 가입자에 대한 감청이 누구를 통하여 수행될 수 있을지 등에 대하여 규제관청에 알리도록 하고 있다. 공공전기통신 서비스를 제공하는 전기통신설비 운영자라 하더라도 사설 네트워크, 인터넷으로의 연결에 이용되는 통신망연결점, 1,000 명 이하의 가입자를 가진 소규모 설비 등의 경우에는 감청 기능 구비 의무를 면제하고 있다. 또한, 단말기가 외국에 위치하고 있는 것으로 판단되는 전기통신의 경우도 법의 적용 범위에서 제외하고 있다.

다. 감청 보안 관리

전기통신감청령은 감청 집행을 위해 필요한 기술적 설비의 구성에 대한 기본적 요구사항 등에 대한 지침을 담고 있으며, 특히 감청 시스템의 보안 관리 및 오남용 방지를 위한 요구사항을 아래의 항목들에 대하여 상세하게 규정하고 있다.

- 기술설비 보호 요구사항: 협조의무자는 감청기능과 정보전달 접속지점 통제를 위한 기술설비를 기술의 발달에 맞추어 부정 사용되지 않도록 보호하는 조치를 취해야 함
- 감청사본 보호 요구사항: 권한 없는 자가 감청사본에 접근할 수 없도록 적절한 방법으로 보호해야 함

- 비밀 유지: 협조의무자는 권한 없는 자가 법적처분이 전기통신 시스템에 구현된 방식에 대한 정보에 접근할 수 없도록 해야 하며, 감청 조치와 관련된 정보 보호를 공고히 해야 함
- 설비 사용 기록: 감청설비를 사용할 때마다 데이터 입력 사항이 빠짐없이 자동으로 기록되어야 함. 기타, 접근 권한과 삭제 기능의 기술적 구현을 위한 요구사항에 대하여 규정
- 이 밖에 로그기록 데이터의 검사와 삭제, 서류의 파기와 관련된 절차 및 요구사항 등에 대하여 규정하고 있음

라. IP 서비스 감청

인터넷전화 서비스는 서비스 제공 형태에 따라 단말간에 운용 장비 없이 통신이 이루어지는 peer-to-peer 형태의 서비스와 트래픽이 서버를 경유하는 형태의 서비스로 나눌 수 있다. P2P 형태의 인터넷전화 서비스 제공업자는 감청 기능 구비에 대한 의무를 가지지 않으며, P2P 형태의 인터넷전화를 감청하고자 할 경우에는 인터넷 접속 포인트에서 감청을 수행하는 것이 가능하다. 서버를 통한 인터넷전화 서비스의 경우 1,000 명 이상 가입자를 가진 제공업자는 감청 협조의무를 가지며, 10,000 명 이상 가입자를 가진 경우에는 인터넷전화 감청을 위하여 인터림 솔루션을 이용하도록 하고 있다. 인터넷전화 감청을 위한 인터림 솔루션에서는 인터넷전화 시그널링의 감청이 기술적으로 간단하기 때문에 이를 감청하도록 하고 있으나, RTP stream 형태의 통신 내용은 우선 감청하지 않기로 하고 있다. 그러나, 시행규칙 5.1 버전이 발효되면 통신 내용에 대한 감청이 이루어질 것으로 예상된다[8].

4. 영국 감청제도

가. 감청 규제

영국은 1985 년에 IOCA(Interception of Communications Act)를 제정하여 통신 서비스에 대한 감청을 시작하였다. 법 제정 당시에는 PSTN 기반 전화 서비스에 대해서만 감청을 집행하였으며, 이후 이동통신 서비스에 대하여 법을 적용하는 데도 큰 문제가 없었다. 그러나, IP 서비스가 발전함에 따라 IOCA 에 기반하여 감청을 집행하는 데 어려움이 있어, 1999 년에 국회위원, 시민, 수사기관 등의 관계자들이 모여 감청 정책 개정을 위한 협의절차(Consultation Process)을 시작하였으며, 그 다음 해에 RIPA 2000(Regulation of Investigatory Powers Act 2000)을 제정하였다. RIPA 2000 은 모든 종류의 감시/감독을 그 범위로 하고 있는데, Part 1 에서 감청에 대한 부분을 규정하고 있으며, 기술 중립적으로 제정되어 다양한 통신 기술에 대한 감청이 가능

하도록 하고 있다.

영국에서는 보안당국, 수사기관 등 9 개의 기관에 대해서 감청을 허가하고 있다. 또한, 감청은 국가의 보안 등 주요한 목적의 달성을 위하여, 그리고 최후의 수단으로 제한적으로 사용하도록 규정하고 있다. 또한, 감청 결과를 법원에서 증거로 사용할 수 없도록 하고 있다.

나. 감청 의무 부과

RIPA 2000 에 근거하여 공공우편 서비스 또는 공공전기통신 서비스 제공업자와 이러한 서비스 제공을 계획하고 있는 자는 소속장관이 발부한 통지서에 기술된 모든 감청 협조 조치를 강구할 의무를 가진다. 그러나, 전기통신 서비스가 아닌 서비스를 제공하는 수단에 불과하거나, 전기통신 서비스가 아닌 서비스를 제공하는데 필연적으로 수반되는 것에 불과한 경우에는 위 의무를 부담할 책임이 없다. 감청 협조 조치를 강구할 의무를 가지는 제공업자 중, 가입자 10,000 명 이상의 대규모 사업자는 직접 감청 기능을 구비해야 한다. 그러나, 소규모 사업자는 비용 부담을 줄이기 위하여 감청 기능을 직접 구비하지 않고 감청이 가능하도록 네트워크를 개방하도록 하고 있다. 이와 같은 의무 수행을 위하여 소요되는 비용 보전과 관련하여, 중소기업에 대해서는 정부가 비용을 전부 부담하고, 대기업에 대해서는 RIPA grant 를 이용하여 초기 감청기능 구축 비용의 상당 부분을 보전하지만 감청 능력의 업데이트에 소요되는 비용은 제공업자가 부담한다[9].

5. 호주 감청제도

호주의 감청 규제는 크게 두 부분으로 나누어 이루어지고 있는데, 통신산업부는 일반적인 정책을 수립 및 운영하는 역할을 담당하며, 법무부는 검찰 및 사업자의 정책 이행, 각 주에서의 감청 관련 법률 적용, 정책의 적용을 위한 정부당국과 사업자와의 조율 등을 담당하고 있다. 호주에는 70 개 이상의 통신 서비스 제공업자와 100 개 이상의 ISP 가 서비스를 제공하고 있는데, 호주 내 모든 CSP 와 ISP 는 사업 허가의 조건으로 감청 기능을 제공해야 한다. 따라서, IP 기반 통신 서비스, 위성통신 서비스, 데이터통신 서비스 등 모든 종류의 공공전기통신 서비스가 감청의 대상이 될 수 있으며, 해당 서비스 제공업자는 다음의 의무를 가진다.

- 의무를 면제받지 않는 한, 해당 제공업자는 서비스 출시 시점부터 감청 기능을 갖추어야 함
- 수사기관이 정하는 전달 규격을 준수해야 함
- 감청 능력의 구비 비용은 제공업자가 부담하며, 수사기관이 협약된 규격 외의 기능을 요구할 경우 해당 기능에 대한 비용은 보전될 수 있음

위의 의무를 준수하지 않을 경우 해당 제공업자는 하루에 천만 달러까지 벌금이 부과되거나

사업권을 잃을 수도 있다. 이러한 결정에 대한 권한은 수사기관이 가지고 있다. 감청을 통하여 취득한 모든 정보는 감청을 수행한 제공업자가 저장하지 않고 실시간으로 수사기관에 전달되어야 한다. 그러나, 과금 및 서비스 기록 등 일부 데이터는 사업적 목적으로 보관될 수 있으며, 수사기관이 이러한 데이터에 접근할 권한을 가진다. Data retention 과 관련하여 해당 법안이 계류중에 있으며, 2008 년 중에 제정될 예정인 것으로 밝히고 있다[10].

III. 결 론

국내에서는 통신비밀보호법을 기반으로 통신 서비스에 대한 감청을 수행하고 있다. 그러나, 현재의 통신비밀보호법 하에서는 전기통신사업자들이 수사기관의 감청 요청에 대한 단순협조의 무만을 가지고 있어 PSTN 유선전화 서비스 이외의 통신 서비스에 대한 감청에는 어려움이 있다. 이러한 이유로, 전기통신사업자에게 감청 수행을 위한 기능 구비 의무를 부과하는 내용을 포함하는 통신비밀보호법 일부 개정법률안이 국회 본회의에 상정되어 있다. 법률 개정을 위하여 여러 가지 이슈가 검토되고 있으나, 특히 감청 오남용 방지를 위한 기술적 대책에 대한 논의가 활발하게 이루어지고 있다. 외국의 사례에서도 알 수 있듯이, 수사의 필요성에 의하여 통신 서비스의 감청을 수행하고 있으나 불법적인 형태의 감청을 차단할 수 있는 감청 보안 대책 수립을 무엇보다 철저히 하고 있다. 통신시장의 환경 변화를 고려하여 국내 감청제도가 재정립됨에 있어, 감청의 보안성 확보를 위한 제도적 기반 마련과 더불어 감청 보안관리 표준 및 기술의 개발이 중요한 것으로 생각된다.

<참 고 문 헌>

[1] 통신비밀보호법 제 2 조(정의), 2005. 5. 26.
[2] “Second Report & Order,” FCC 99-229, Aug. 31, 1999, pp.4~17.
[3] “First Report and Order AND Further Notice of Proposed Rulemaking,” FCC 05-153, Sep. 23, 2005.
[4] Communications Assistance for Law Enforcement Act, Sec.109. Payment of costs of telecommunications carriers to comply with capability requirements, “http://www.askcalea.net/calea.html”
[5] “Second Report and Order and Memorandum Opinion and Order,” FCC 06-56, 2006. 5. 12, pp.33~34.
[6] Koen Jaspers, “The LI Approach in the Netherlands,” 2007. 10.
[7] Decree on security of data on telecommunication lines tapped, Oct, 2003.

[8] Klaus Knab, “Lawful Interception – Regulation in Germany,” 2007. 10.
[9] Ian Cooper, “Lawful Interception – the UK Perspective,” 2007. 10.
[10] Alan Dubberley, “Telecommunication LI and DR – Australian Approach,” 2007. 10.

* 본 내용은 필자의 주관적인 의견이며 IITA 의 공식적인 입장이 아님을 밝힙니다.