미국의 통신감청기간 및 연장에 관한 법제 현황 및 내용

정보신청기관 : 법무부

Ⅰ. 머리말

지난 해 말 많은 논란을 일으키며 통신비밀보호법이 개정되었고, 올 정기국회에서 정부여당은 다시 개정을 추진하고 있다. 추진하는 새로운 개정의 내용을 보면 스마트폰을 비롯한 모든 통신수단에 대한 감청을 의무화하고 있고,[1] 통신사업자로 하여금 통신설비에 감청설비 구비를 갖추도록 하여 휴대전화뿐 아니라 요즘 널리 사용되는 스마트폰은 물론 메신저와 P2P 등 거의 모든 통신수단에 대한 감청[2]을 합법화하여 논란이 예상된다. 또한 법안은 모든 통화내역과 인터넷의 IP주소 보관을 의무화하고 이를 위반하면 3천만 원의 과태료를 부과하도록 규정하고, 국가정보원에 대해서 '직접 감청'을 허용하는 규정을 두고 있어 국가정보원의 감청권한을 확대하고 있다.[3] 그동안 전화와 인터넷 등 전기통신기기의 발달로 이러한 과학기술의 발전

1) 한나라당 이성언 의원의 통신비밀보호법 개정안을 보면 제15조의2 제2항은 "전화서비스를 제공하는 전기통신사업자, 그 밖에 대통령령으로 정하는 전기통신사업자는 이 법에 따른 검사 · 사법경찰관 또는 정보수사기관의 장의 통신제한조치 집행에 필요한 장비 · 시설 · 기술 및 기능을 갖추어야 한다"고 의무화하였다.

2) 일반적으로 감청은 도청과는 구별되는 개념으로 도청이 타인간의 통신 혹은 대화를 청취하는 일반적인 행위인 반면, 감청은 이러한 도청행위 중에서 법적인 근거를 가지는 행위로서 정보통신상의 검열행위를 말한다. 현행 통신비밀보호법은 제2조 제7호에서 '감청'이라 함은 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 말한다고 규정하고 있다.

3) 현재 우리나라에서 실시되는 모든 감청 가운데 국가정보원의 감청이 98%에 달하고, 비공식적인 국가정보원의 직접 감청까지 더한다면 그 수치는 더 커진다. 지난해에는 국가정보원이 인터넷 회선을 통째로 감청하는 일명 패킷 감청을 실시해 왔으며, 직접 패킷 감청 장비를 운용해 왔다는 사실이 밝혀졌다.

을 이용한 범죄, 특히 마약범죄와 조직범죄 등이 은밀하게 진행되고 있어서 효과적인 범죄예방을 위하여 경찰, 검찰 등 법집행기관에게도 첨단시설을 이용한 감청, 녹음 및 녹화 등과 같은 과학적인 수사방법이 필요하게 되었다. 또한 국가의 안보차원에서도 대내적인 국가안보유지뿐만 아니라 대외적으로 국가적 이익을 위하여 일정부분 통신과 대화에 대한 감청과 제한이 필요하다. 실제로 세계 각국은 자신의 주권과 이익을 지키기 위해서 정보를 수집하고, 자국의 정보를 보호하는 수단으로 통신감청과 제한을 해오고 있다.

문제는 그 남용을 억제하기 위해서 일정한 통제수단이 강구되어야 한다는 점인데, 특히 범죄수사와 관련하여 피고인의 인권보장과 적법절차가 강조되는 형사소송절차에서 피의자의 유죄확정을 위한 증거수집의 방법으로 감청 등 과학적인 수사가 필요하나 이러한 과학적 수사에 의해 헌법상 보장된 인간의 존엄과 프라이버시권 등 개인의 기본권이 침해될 소지가 크다. 이하에서는 통신감청과 관련하여 미국의 통신감청 실태와 관련 법률을 개관하고, 특히 통신기간 및 기간연장에 관한 법제 현황 및 내용에 관하여 검토한다.

Ⅱ. 미국의 감청의 실태와 관련 법률

1. 미국의 감청실태

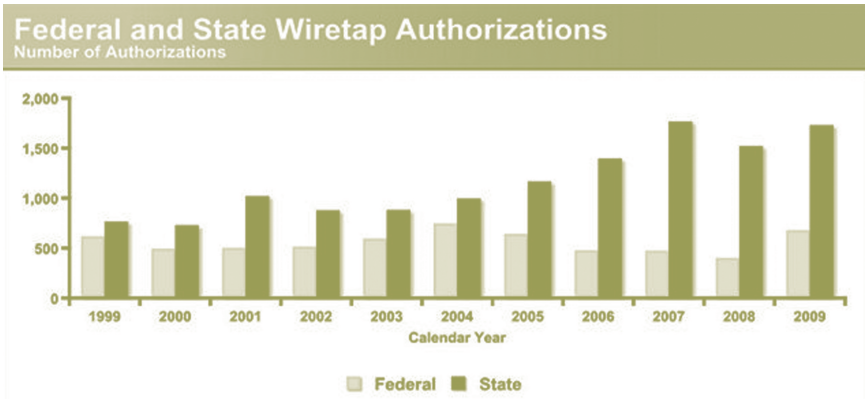
최근에 세계 각국은 국내적으로는 범죄와 치안유지를 목적으로, 국제적으로는 자국의 이익추구를 위한 정보수집과 관련하여 통신에 대한 도청과 통신제한을 하나의 수단으로 선택하고 있고, 미국 또한 예외가 아니다. 특히 2000년 2월 유럽의회가 미국이 주도하는 전 세계적 위성통신도청망인 '이셜론(ECHELON)'이 유럽 기업 등의 산업정보를 도청한 사실을 폭로하여 충격을 주기도 하였다.[4] 미국의 통신감청은 대외적인 면에서는 주로 정보기관에 의하여 이루어져 왔다.[5] 현재 미 연방정부 산하의 정보기관은 모두 15개의 조직으로 나누어져 있고, 이 가운

4) 이셜론(ECHELON)은 미국 NSA가 중심이 되어 앵글로색슨 국가들 사이에서 운영하고 있는 전 세계 통신 감시 및 감청 협력체제로 1947년 미국과 영국 간 협정으로 출발했다. 그간 3차에 걸쳐 가입국을 확대했다. 에셜론은 당초 공산국가와의 정보전을 대비해 구축되었지만 냉전 종식 후에는 국제범죄 및 테러방지 등을 목적으로 운영되고 있으며, 최근 미국 등이 이를 자국 기업을 위한 상업적 목적의 도감청 등에 활용하고 있는 것으로 드러나면서 비판을 받고 있다. 에셜론은 1차 가입국과 2차 가입국에 대해 무제한의 정보 제공을 허용하고 있는 데 반해 3차 가입국에 대해서는 제한된 정보만 제공해 주고 있다. 그 이전까지 미국과 영국은 이셜론의 존재 자체를 부인해 왔으나, 1999년 11월 영국의 BBC방송이 이셜론에 대해 집중 보도한 것을 계기로 미국 국가안보기록보관소에 의해 관련 비밀문서가 공개되었다.

5) 정보기관이 수집하는 정보는 크게 '인간정보'(Human Intelligence)와 '신호정보'(Signal Intelligence) 그리고 '영상정보'(Image Intelligence)로 나뉜다. 이 가운데 CIA는 인간 정보를 주로 다루고, 법무부 산하 수사기관인 FBI는 미국 내 대공(Counter Intelligence)업무, 국방부 산하의 NSA는 '신호정보'를 총괄 담당한다.

데 국가안보국(NSA), 중앙정보국(CIA), 국방정보국(DIA), 국가정찰국(NRO) 그리고 국가 대기권정보국(NGA) 등 5개 기관을 묶어 '정보공동체(Intelligence Community : IC)'라고 불린다. 일반적으로 미국의 정보기관으로 거론되는 곳이 CIA(중앙정보국)이나 그보다 더 막강한 정보력을 갖춘 곳이 '국가안보국(National Security Agency : NSA)'[6]이다. 현재 미국의 군사전문가들은 이들 정보기관이 한 해에 사용하는 예산을 6백억 달러로 추정하고, 이는 전체 국방예산(2010년 기준 6,364억 달러)의 약 10%에 해당한다.

대내적으로는 범죄수사와 관련하여 미국연방수사국(FBI)이 주로 통신감청을 하여 왔고(모든 통신감청의 1/3), 그 대상도 종래의 국내 범죄수사와 미국 내에서 활동하고 있는 외국인들의 불법적 경제정보활동을 감시 및 단속하기 위한 것이었다. 미국에서도 통신감청의 효율성에 대해 일부 이견이 있지만 전자적 감시수단의 활용은 필수적인 것으로 받아들여지고 있고, 실제로 전화감청 등 전자적 감시수단은 조직범죄, 마약거래, 뇌물, 유괴 · 납치, 살인, 테러리즘 등 심각한 폭력적 범죄활동을 방지하는 데 필수적인 것이 되고 있다. 한편으로 이러한 현상은 개인의 사생활을 침해하는 통신감청이 다른 한편으로는 개인의 사생활과 재산권을 범죄로부터 보호하는 데 기여하고 있다는 것을 의미하기도 한다. 최근 인터넷의 발달로 인하여 인터넷을 이용한 범죄가 증가함에 따라 미국 연방통신위원회(FCC)는 광대역서비스 사업자와 인터넷전화(VoIP)업체들이 유사시 경찰이 감청을 할 수 있도록 기술적 조치를 취하도록 추진하고 있고,[7] 미 사법당국(법무부와 FBI)은 스마트폰이나 소셜네트워



6) 인력 면에서도 NSA는 석사급 이상의 학력을 가진 3만 8천여 명의 요원들이 근무하고, 1년 예산도 400억 달러에 이르고 있어, 미 정보기관 중 최대 규모의 정보기관이다.

7) 법무부와 연방수사국(FBI)은 이미 2003년부터 미국 연방통신위원회(FCC)에 VoIP 감청권을 계속 요구해 왔고, FCC도 마약과 테러, 국제적인 조직범죄의 범죄의 효과적인 예방을 위해서는 필요한 조치로 받아들이고 있다.

크서비스(SNS) 등 모든 종류의 통신 서비스 제공 업체가 반드시 감청과 암호 해독 시스템을 갖추도록 의무화하는 법안을 현재 추진 중이다.[8] 이 법안이 통과되면 사법당국이 사실상 모든 통신업체에 대해 언제든지 감청할 수 있게 된다. 미연방법원에서는 매년 감청에 대한 리포트를 작성하고 있는데 2009년 자료를 보면, 2009년에 정부 및 주에 의해 승인된 도청 건수는 2,376으로 감청 장비가 설치되어 운영되는 평균 기간은 42일이며 2008년 41일에 비해 비슷한 수치이다. 또한 감청을 통해 4,537명이 검거되었다고 한다. 감청되는 범위는 일반 전화 및 모바일 통화 등 전화를 이용한 감청이 98%이며, 이 중 대부분은 휴대전화 통신이다.[9]

감청에는 적지 않은 비용이 소요되는데 2009년 감청을 위한 장비설치비용으로 건당 평균 $52,200이 들었으며, 이는 2008년에 비해 10% 증가한 수치다.

2. 통신감청에 대한 법적 근거

미국의 경우 감청은 수정헌법 제4조에서 규정하고 있는 압수 · 수색에 해당하며, 프라이버시의 침해가 되므로 원칙적으로 허용되지 않는다. 미국에서 감청을 최초로 규제한 법은 「연방통신법」[10]이다. 동법 제805조에서는 어떠한 자에 대해서도 전화감청을 금지하였으나 1967년의 연방대법원 판결에서 ① 범죄에 관한 정보를 전달하기 위하여 전화가 이용되거나, ② 감청의 목적이 위법한 내용의 통화에 한정되고 그 범위와 기간이 명확한 경우, ③ 감청을 피고인의 회화에 한정한다는 최대의 주의가 할애되고, ④ 하급판사가 감청을 허가하는 범위, 필요성과 상당성, 그에 수반하는 침해의 명확성을 판단하여 허가한 경우 등의 일정한 요건을 충족한 경우에는 전화감청이 적법하다는 판결을 내리게 되면서 동법은 현실을 규제하는 효력을 상실하게 되었다.[11]

8) 2010년 9월 27일, 뉴욕 타임즈. 백악관과 연방수사국(FBI) 등이 내년도 의회에 제출을 위해 검토 중인 이 법안에 따르면 통신 업체는 감청이 가능한 시스템을 갖춘 뒤에야 서비스를 제공할 수 있고, 소프트웨어 개발업자도 개발 단계에서부터 감청이 가능하게 만들어야 한다. 미국에서 영업하는 외국업체도 마찬가지이고 이를 위반하면 벌금 등 제재가 가해진다.

9) http://www.uscourts.gov/library/wiretap.html.

10) 연방통신법은 1934년에 제정되었고, 1996년에 대폭적인 개정을 하였다. 최근에 다시 급변하는 통신기술의 발전에 따라 연방통신법의 개정이 미 상 · 하원에서 추진되고 있다. 1934년 법에서는 " … 송신자에 의하여 허락받지 아니한 자는 누구라도 통화내용을 가로채고 다른 사람에게 이러한 가로챈 통화의 존재, 내용, 요지, 목적, 효과, 의미를 폭로하거나 공표하지 못한다"라고 규정하였다. 동 규정은 사인은 물론 주정부 또는 연방정부 공무원에 의한 감청에도 적용되고, 같은 주(州안)의 통신은 물론 주간의 통신에 대하여도 적용되는 것으로 해석된다. 그러나 동법의 금지규정에도 불구하고 연방수사요원 등은 상당한 양의 감청을 계속하였는데, 이는 동 법률이 국가이익을 위하여 행하여진 외국정보감청을 전부 금지하지는 않는다고 해석하여 행하여지거나, 또한 법무성과 FBI는 동법의 규정이 감청 자체를 금지하는 것이 아니라, 감청된 것을 폭로하는 것만 금지한다는 것으로 보았다.

11) Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967) 판결 참조.

1967년의 판결에 근거하여 1968년 제정된 「범죄단속및가두안전종합법(Omnibus Crime Control and Safe Street Act)」에 감청을 허용하는 새로운 규정을 두게 되었다. 특히 동법의 제3편이 연방 및 주(州)의 법집행기관에 의한 전자적 감시를 다루고 있기 때문에 동법을 감청과 관련하여 칭할 때 흔히 Title III라고 약칭되어 왔다. Title III는 모든 사적인 감청을 금지하고, 다만 법집행기관이 감청장치를 사용하는 것은 허용하면서 감청장치가 사용될 수 있는 시기와 방법, 감청허가를 신청할 수 있는 자, 신청서에 명시되어야 하는 내용, 감청허가를 위한 법관의 심사사항, 감청의 허가기간 및 연장 등에 관하여 규정하고 있다.

또한 Title III는 주 또는 지방의 법관이 전자감시를 허가했더라도 당해 주가 법관에게 그러한 명령을 발할 권한을 위임하는 법률을 두고 있지 않으면, 연방법하에서 불법이라고 규정하였다. 따라서 주가 권한을 위임하는 법률을 제정하지 않은 경우에는 어떠한 전자적 감시도 허용될 수 없다.[12] 그러나 이러한 Title III에 의하면 전신이나 팩시밀리 같은 통신수단에 대한 법적 보호 장치가 없어서 문제점이 제기 되었고, 이에 대한 새로운 법안이 통신서비스기업을 중심으로 적극적으로 추진되어 제정된 법이 1986년의 「전기통신및프라이버시법(The Electronic Communications and Privacy Act: ECPA)」이다.[13]

ECPA의 효력이 발생한 이후에 법집행기관이 전화와 대화 이외에 통신이 전송되는 도중에 그 내용을 채록하려면 전화와 대화에 대한 감청영장과 거의 동일한 절차에 의한 전기통신감청영장을 발부 받아야 한다. 이는 ECPA가 전기적 수단에 의하여 전달되는 전화와 대화 이외의 모든 통신을 전기통신으로 정의하고 있기 때문이다.[14]

따라서 전자메일을 포함하는 컴퓨터통신, 전화이용기록장치, 전화의 착발신추적기 등에 대한 감청도 동법이 규정한 일정한 절차에 의하여야 한다. 그 밖에 휴대전화와 관련하여 1998년 연방통신위원회는 범죄 수사를 위해 FBI와 경찰당국이 법원의 허가를 얻어 휴대전화를 감청할 수 있도록 휴대전화회사들이 수사당국의 요청이 있을 때는 휴대전화 소유자들의 통화내용과 장소 등의 자료를 제공토록 하는 방안을 채택하였다.[15]

그 밖에 인터넷전화 업체들이 유사시에 경찰들이 감청할 수 있도록 기술적 조치를 취해야 하는 방안을 합법화하기 위한 규제안을 준비하고 있다. 이는 인터넷 등 정보통신기술의 발달로 인

12) 김성돈(역), 미국형사소송법, 길안사 1999년, 337쪽.

13) http://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act.

14) 1986년 전기통신 및 프라이버시법, sec.101 참조.

15) 이에 대해 미국의 인권단체들은 사생활의 침해를 우려하고 있다.

하여 범죄수법도 발전하고 있어서 수사기관의 원활한 범죄수사를 위해서는 전문가인 인터넷 전문업과 감청을 위한 기술적 체제를 갖추는 것이 필요하다는 판단에서이다.

미국은 해외 정보활동에 대한 감청은 해외정보감시법(FISA)[16]이 규정한 절차를 따른다. 동 법률은 감청허가를 해외정보감시법원(Foreign Intelligence Surveillance Court : FISC)을 설립하여 감청허가여부와 기간연장을 담당하도록 하고 있다.[17] 통상 미국의 FBI도 범죄정보를 다루지만 국내 범죄관련 업무의 집행기관이고, CIA가 해외정보활동 기관이기 때문에 해외정보감시법원(FISC)은 처음에는 CIA의 업무와 관계있는 기관이었다. 그러다 2002년 11월 18일 미 항소심 재판부가 1심 판결을 뒤집고 "정보기관과 범죄수사기관 사이의 협력을 방해하는 것은 국가안보에 위협이 될 수 있다"며 FBI가 일반법원 대신 해외정보법원의 영장을 받아 감청 및 압수수색을 할 수 있도록 하였다.

Ⅲ. 통신기간 및 기간연장에 관한 법률 내용

1. 1968년 제정된 「범죄단속및가두안전종합법 (Omnibus Crime Control and Safe Street Act)」

범죄와 관련하여 통신감청을 허용하는 규정을 두고 있으며, 특히 동법의 제3편이 연방 및 주(州)의 법집행기관에 의한 전자적 감시를 다루고 있기 때문에 동법을 감청과 관련하여 지칭할 때 흔히 Title III라고 약칭되어 왔다. Title III는 도청 및 전자적 감시(WIRETAPPING AND ELECTRONIC)라는 표제하에 챕터 제119에서 통신감청과 대화의 감청(WIRE INTERCEPTION AND INTERCEPTIONOF)에 관하여 규정하고, 이를 세부적으로 2510조에서 2520조까지 나누어 규정하고 있다. 법률조항을 개관하면 제2510조에 정의규정을 두어 동법에 규정된 용어를 정의하고, 제 2511에서 통신과 대화에 대한 도청 및 공개 금지(Interception and disclosure of wire or oral communications prohibited)에 관한 규정을 두고 있다.

제2512조에서는 도청장치의 제조, 유통, 소유, 광고의 금지(Manufacture, distribution, posses-

16) 미 의회는 해외거주 외국인에 대한 감청을 합법화하는 해외정보감시법(FISA:Foreign Intelligence Surveillance Act) 개정안을 상정, 찬성 69표, 반대 28표로 통과시켰다. 당시 이 법안에 대해 신중한 입장을 보였던 민주당의 대선 후보 버락 오바마(Obama) 상원의원도 '해외정보감시의 중요한 수단을 만들 기회'라는 이유에서 찬성하였다.

17) 우리나라의 현행 통신비밀보호법은 통신제한조치와 관련하여 일반적 범죄수사의 경우에는 관할법원, 국가안보를 위한 경우에는 대통령과 고등법원 수석부장판사가 이 문제를 관할하도록 되어 있다. '승인'은 대통령이, '연장'은 고등법원 수석부장판사의 허가 또는 대통령의 승인을 받도록 규정하고 있다(통신비밀보호법 제6조와 제7조).

sion, and advertising of wire or oral communication intercepting devices prohibited)를 규정하고, 제2513조에서 도청장치의 압수(Confiscation of wire or oral communication intercepting devices)에 관한 규정을 두고 있다. 제2514조에서 증인 면책(Immunity of witnesses)에 관한 조항을 두고, 제2515조에서 도청에 의한 증거사용금지규정(Prohibition of use as evidence of intercepted wire or oral communications)을 두고 있다.

제2516조에서는 통신과 대화의 도청허용에 관한 규정을 두고, 제2517조에서 도청된 내용의 공개와 사용에 관한 규정을 두고 있다. 그리고 제2518조에서 도청절차(Procedure for interception of wire or oral communications)에 관하여 규정하여 감청장치가 사용될 수 있는 시기와 방법, 감청허가를 신청할 수 있는 자, 신청서에 명시되어야 하는 내용, 감청허가를 위한 법관의 심사사항, 감청의 허가기간 및 연장 등에 관하여 규정하고 있다. 마지막으로 제2519조에서 허가 받은 도청의 결과 보고(Reports concerning intercepted wire or oral communications)에 관한 규정을, 제2520조에서 감청으로 인하여 발생한 피해에 대한 손해배상(Recovery of civil damages authorized) 규정을 두고 있다.

미국에서 도청허가신청은 법무장관, 또는 법무장관이 특별히 지명한 법무장관 보좌관(Assistant Attorney General)이 관할권이 있는 연방판사에게 도청허가를 신청할 권한이 있고, 신청을 받은 판사는 동법 제2518조의 규정에 따라 통신과 대화에 대한 도청허가를 도청허가 신청서를 제출한 FBI나 기타 범죄조사를 담당하는 다른 연방기관에 발부한다.[18] 도청허가의 대상이 되는 범죄는 우리나라의 통신비밀법과 유사하게 규정하고,[19] 살인, 납치, 도박, 강도, 뇌물, 강탈죄를 저지른 증거를 수집하기위한 도청을 하는 경우 이를 실행하는 담당자가 신청된 범죄조사에 대한 책임이 있음을 규정하고 있고(동법 제2516조(2)), 이것은 고위직의 집행기관으로 하여금 정치적 책임을 물을 수 있도록 하여 도청영장 신청의 남용을 억제하는 효과적인 안전장치가 되고 있다. 물론 도청이 실행되는 기간을 한정하여 허가하여야 한다.[20]

도청허가신청서에는 조사하거나 법률을 집행하는 공무원의 신원과 실행하는 공무원의 권한,

18) 동법 제 2516조(1) 참조.

19) 대표적 범죄로 형량이 사형에 해당하거나 미 연방법전(the United States Code) title 42의 섹션 2274에서 섹션 2277의 규정에 의해 1년 이상의 유기징역에 처벌되거나, 이 법 제37장(스파이에 관한 처벌규정), 제105장(방해에 관한 처벌규정), 제115장(반역과 관련된 처벌규정), 또는 제102장(폭동에 관한 처벌규정), 미 연방법전 title 29 섹션 186 또는 섹션 501을 위반하거나 살인, 납치, 강도, 금전 갈취죄에 해당하는 범죄 등이 이에 해당한다.

20) 동법 제2518조 (4).

감청허가명령이 발부될 수 있을 정도의 감청 신청자의 사실과 상황에 대한 충분하고 완전한 설명이 요구되고,[21] 도청허가신청에 대해 판사는 법원이 관할하는 지역 내에 한정하여 신청된 내용을 그대로 또는 수정하여 통신이나 대화에 관한 도청을 허가하는 명령을 서면으로 발부한다. 판사는 신청자가 제출한 사실에 기초하여 도청허가여부를 결정하고, 각각의 도청허가 명령은 도청할 통신과 대화를 구체적으로 특정하여 허가하여야 한다. 즉, 도청 대상자의 구체적인 신원사항을 특정하고, 도청할 시설물과 장소를 특정하여 허가하여야 한다. 또한 도청할 대화는 구체적인 범죄와 관련이 있어야 하고, 대화의 유형을 특정하여 허가하여야 한다. 도청허가를 받은 신청인과 도청을 실행할 기관을 특정하여 허가하여야 한다.

감청기간에 관하여 동법 2518조(5)는 어떤 통신과 대화에 대한 감청허가도 객관적으로 필요한 감청기간을 초과하여 허가할 수 없고, 그 기간도 어떤 경우에도 30일을 초과할 수 없다고 규장하고 있다. 다만, 동조 (1)의 법적 요건[22]을 충족하면 감청기간의 연장이 가능하고 법원은 동조 (3)의 요건[23]을 충족하여 기간연장을 허가한다. 기간연장은 처음에 허가 받은 기간보다 더 장기로 연장할 수 없다. 판사가 목적달성에 필요하다고 판단하여 기간연장을 하더라도 역시 어떤 경우에도 30일을 초과 할 수 없다.[24] 따라서 모든 도청허가와 기간연장허가는 실행이 가능한 때 실행하고, 허가 받은 도청목적에 한정하여 최소한으로 실행한다. 그리고 어떤 경우에도 30일 이내에 허가받은 감청내용을 녹취하여 감청을 종료하여야 한다. 또한 동 법률에 의한 도청허가를 하는 경우 도청허가를 받은 대상에 대한 도청의 진행상황과 도청의 결과물에 대한 보고를 허가명령을 발부한 판사에게 하여야 하고, 도청을 계속할 필요가 있는지의 여부도 보고를 하여야 한다.[25]

감청된 통신과 대화의 내용은 테이프나 다른

21) 동법 제2518조(b)는 ① 실행되거나 모의되는 구체적인 범죄사실, ② 도청장소나 시설물의 구체적인 명시, ③ 도청되는 대화 유형의 구체적인 명시, ④ 도청 대상자가 공인인 경우 그 대상자의 신분과 누구의 대화가 도청되는지를 특정하여야 한다고 규정하고 있다.

22) 도청허가신청서에 기재할 사항.

23) 감청신청에 대해 판사가 이에 대한 결정을 내릴 때 고려할 사항으로 첫째, 감청의 대상이 되는 개인이 동법 제2516조에 규정된 범죄를 실행하였거나 실행 중이거나 착수하려고 한다는 확신에 대한 합리적인 근거가 있어야 하고 둘째, 도청에 의해 감청된 대화가 특정 범죄에 관련된 대화라는 확신에 대한 합리적인 근거가 있어야 한다. 셋째, 범죄에 대한 정상적인 조사 절차가 실시되었지만 성공할 것 같지 않거나 조사의 실행이 너무 위험하다는 합리적인 근거가 있어야 하고 넷째, 범죄관련자들이 통상적으로 사용하거나 범죄에 사용하려고 임대한 시설물, 나열된 이름 등 도청되는 시설과 장소가 범죄와 관련되고, 도청되는 통신이나 대화가 범죄와 관련되어 이용되고, 곧 이용될 것이라는 것에 대한 확신에 대한 합리적인 근거가 있어야 한다.

24) 동법 제2518조(5) 참조.

25) 동법 제2518조(6).

유사한 장치에 의한 기록 등 감청된 통신이나 대화의 내용이 편집이나 위조나 변조로부터 보호할 수 있는 방법으로 기록하여야 한다. 기록물의 관리는 판사의 명령에 의해 이루어지고 10년 동안 보존된다.[26]

2. 1986년의 「전기통신프라이버시법(The Electronic Communications and Privacy Act: ECPA)」

동법은 1968년 제정된 「범죄단속및가두안전종합법(Omnibus Crime Control and Safe Street Act)」 Title Ⅲ이 가지는 문제점을 시정하기 위해 통신서비스기업을 중심으로 추진되어 제정된 법률이다. 동법은 감청장치가 사용될 수 있는 시기와 방법, 감청허가를 신청할 수 있는 자, 신청서에 명시되어야 하는 내용, 감청허가를 위한 법관의 심사사항, 감청의 허가기간 및 연장 등에 관하여 규정하고 있고, 이는 1968년 「범죄단속및가두안전종합법(Omnibus Crime Control and Safe Street Act)」의 규정을 기초로 하고 있다. 다만, 30일의 감청허가기간과 관련하여 30일의 도청허가 기간의 시작은 법률집행기관이 도청허가명령에 따라 감청을 처음 실행한 날이나 도청허가명령이 발부된 날로부터 10일 후부터 기산한다는 내용을 새로이 규정하였다.[27]

또한 감청된 대화가 법률사항이거나 외국어인 경우에는 허가된 감청기간을 최소한으로 사용하여 그러한 내용의 감청이 있는 즉시 우수한 법률전문가나 통역전문가의 도움을 받도록 규정하고 있다. 그리고 감청의 실행주체와 관련하여 동 법률에서의 감청은 그 전부나 일부를 정부가 실시하거나 민간인 사인도 정부와의 계약에 따라 감청을 허가 받아 집행하는 공무원이나 조사관의 감독을 받아 감청을 실행한다고 규정하고 있다.

3. 1994년의 「감청통신지원법(The Communications Assistance for Law Enforcement Act : CALEA)」

IT기술의 발전으로 법집행기관이 전자적 수사를 위해 필요한 법적 권한을 규정한 1986년 'the Omnibus Crime Control and Safe Streets Act'를 개정한 법률로 전자통신(electronic communications)의 범위에 이메일, 데이터전송, 팩스 등을 추가하여 확대시켰다. 또한 정부의 유선, 음성(oral) 및 전자통신 등에 대한 감청을 위한 법률적 권한을 획득하기 위한 절차를 규정하고 있고, 법집행을 지원하기 위한 방법에 대한 많은 가이

26) 동법 제2518조(8) (a) (b).

27) the Electronic Communications and Privacy Act, 제 2518조 (5) 참조.

드라인을 통신 사업자들에게 제공하고 있다.

CALEA는 수사목적을 위한 통신감청시 통신사업자의 의무를 구체화하고(동법 제103조) 있어서 동법에 따라 조사관들은 필요시 네트워크 회사가 작동하는 스위치를 통해 통신을 감청할 수 있다. 또한 통신 사업자에게 수사당국의 요구 시 통신감청을 가능하게 하는 기기를 통신사업자의 설비 중에 설치하도록 규정하고,[28] 정보서비스(information services), 사적 네트워크(private network), 통신연결(interconnecting telecommunications)을 지원하는 장비, 시설 또는 서비스 등은 지원능력요구사항 시 명시적인 요구가 가능하도록 하고 있다.

따라서 동법에 의해 기존의 전화망뿐만 아니라 디지털 음성과 이동 전화망을 포함하여 광케이블 전화 시스템에서부터 디지털 네트워크와 휴대폰까지 거의 모든 통신수단에 대한 정부의 감청이 가능하도록 되었다. 그리고 동법에 의해 요구되는 감청 협조 요청에 불응한 사업자나 감청관련 시설물을 갖추지 못한 서비스 제공 회사들은 벌금이나 다른 제제들을 받게 된다.[29] 다만, 동법은 특별히 인터넷 등 통신사업자들이 수행하거나 제공해야 할 감청기간에 대한 규정이 없다. 이는 동법에 의한 통신감청도 기본적으로 1968년 제정된「범죄단속및가두안전종합법(Omnibus Crime Control and Safe Street Act)」Title Ⅲ의 감청규정을 따르고 있는 것으로 해석된다. 최근 미국 연방통신위원회는 일반 통신망뿐만 아니라 인터넷 전화와 광대역 네트워크에 대한 합법 감청을 확대할 것을 강제화하였다. 또한 2005년에 합법 감청통신지원법을 개정하여 브로드밴드 인터넷 사업자와 인터넷 전화 사업자까지 그 적용이 확대되었으며, 2007년 12월까지로 준수 데드라인을 결정한 바 있다.

최근에 오바마 정부가 이를 더 강화하는 동법의 개정을 추진하고 있다. 이에 따르면 메시지를 암호화하는 통신 서비스 회사들은 이를 해독하는 방법을 갖추고 있어야 하고, 해외에 서버를 두고 미국 내에서 영업하는 회사들은 감청수행이 가능한 국내 기지를 세워야 한다. 또한 P2P 통신을 가능케 하는 소프트웨어 개발자들은 감청이 가능하게끔 이를 재설계하여야 한다.

28) 만약 감청대상이 자신의 컴퓨터와 서버를 오고가는 메시지를 암호화해놓을 경우에는 통신사에게 이를 해독하도록 명령을 할 수 있도록 규정하고 있다.

29) 동법 제2522조 (c)에 의하면 법원은 동법에 의해 요구되는 감청 협조 요청에 불응한 사업자나 감청관련 시설물을 갖추지 못하여 법률을 위반한 통신 사업자, 통신 전송 또는 스위칭 장비, 또는 통신 지원 서비스 공급자에게 매일 최고 1만 달러의 민사상의 제재금(civil penalty)을 부과하는 명령을 발하도록 규정하고 있다.

Ⅳ. 맺음말

선진국에서는 인터넷 전화를 포함한 대부분의 감청행위가 합법적 감청의 대상이 되고 있다. 국내에서도 합법 감청의 범위를 확대하기 위한 통신비밀보호법 개정이 현재 추진되고 있다. 이러한 통신감청이 국민의 프라이버시 보호와 국가의 수사권과 충돌하는 문제여서 개인의 기본권을 강조하면 감청의 적법성을 인정하기 어렵고, 감청을 허용하면 개인의 기본권이 침해될 소지가 있어서 어떻게 균형을 유지하게 하느냐의 문제가 발생한다. 오늘날 과학기술의 발달과 이를 이용한 범죄환경의 변화로 범죄양상이 지능화, 과학화, 국제화되고 있다. 따라서 현실적으로 검찰과 수사기관의 입장에서는 과학적 수사기법의 도입이 필요하고, 사법부도 이러한 사회현상을 해결을 위한 적극적인 법해석이 필요하다.

그러나 항상 고려해야 할 것은 감청 등의 전자감시가 오 · 남용되는 경우에는 시민의 모든 활동이 감시되는 경찰국가나 전체주의국가를 초래할 수도 있다는 점과 개인의 기본권이 침해될 수 있다는 사실이다. 결국 이 문제는 국가가 공익을 위해 어느 범위까지 개인의 사생활정보에 접근할 수 있는지에 대한 것으로 합법적 감청에 대한 명확한 법적 근거와 절차, 그에 따른 법적 책임, 감청기록의 보존, 감청으로 인한 피해구제 등을 명확히 하여 법제도의 운영이 국민의 프라이버시 권한을 보호하면서 사이버상의 범죄 행위를 막을 수 있도록 하여야 한다.

특히 감청기간과 관련하여 현행 통신비밀보호법이 제6조와 7조에서 감청기간을 범죄수사의 경우에는 2개월의 기간과 최장 2개월의 연장기간을 규정하고, 국가안보를 위한 경우에는 4개월의 기간과 최장 4개월의 연장기간을 규정하고 있다. 이는 현실적으로 우리나라보다 각종 전자적 장비가 발달되어 이에 대한 대비가 더 시급한 미국의 경우보다 2배 내지 4배의 기간이라는 점에서 문제가 있다. 또한 연장횟수에 대한 규정도 흠결되어 있는데 미국의 경우처럼 총 연장기간이 일정기간을 초과하지 않도록 하는 규정이 필요하다.

나 채 준

(한국법제연구원 초청연구원)