韓國 컴퓨터情報學會 論文誌
第11卷 第4號, 2006. 9.

2006-11-4-3-3

우리 사이버범죄 대응 절차의 문제점에 관한 연구
- 미국의 사이버범죄대응절차법을 중심으로 -

임병락*, 오태곤**

A Study on the Problems of Procedural Law Against Cyber Crimes in Korea
- On the Trend of Procedural Law Against Cyber Crimes of U.S -

Byoung-Rak, Lim*, Tae-Kon, Oh**

요 약

최근 정보통신시설에 대한 사이버공격을 보면 추적회피기술, 방어우회기술 등이 급속도로 발전하고 있고 전 세계에 있는 다수의 취약시스템을 경유지로 사용하기도 하며 또한 새로 개발된 사이버공격 도구들을 보면 취약점 공격·추적회피·증거훼손 등 완전범죄를 노리는 기술들이 패키지형태로 개발되어 유포되고 있다. 따라서 단순 예방기술로는 한계가 있으며 사안에 따라서는 실시간 추적 등 특별한 절차를 통해서 대응할 수밖에 없다. 나아가 국경을 넘어서는 사이버범죄의 특성상 세계가 공동으로 대응할 수 있는 국제적인 협력과 관련된 절차법적 정비가 요구된다. 특히 미국은 사이버범죄대응절차법의 제정으로 이에 대응하고 있다. 그러나 우리 현행법은 단순히 침해행위에 대한 처벌규정 등 실체법 등의 규정만 있고 절차상으로는 오프라인 범죄인 일반 형사사건과 동일한 절차를 밟아 대응하는 수준에 머물러 있다. 따라서 본 논문에서는 미국의 사이버범죄에 대한 절차법을 살펴보고 우리나라의 현실적 문제점과 대응방안을 제시한다.

Abstract

When current cyber attacks to information and communication facilities are examined, technologies such as chase evasion technology and defense deviation technology have been rapidly advanced and many weak systems worldwide are often used as passages. And when newly-developed cyber attack instruments are examined, technologies for prefect crimes such as weakness attack, chase evasion and evidence destruction have been developed and distributed in packages. Therefore, there is a limit to simple prevention technology and according to cases, special procedures such as real-time chase are required to overcome

• 제1저자 : 임병락 • 교신저자 : 오태곤
• 접수일 : 2006.08.29, 심사일 : 2006.09.12, 심사완료일 : 2006.09.20
* 조선대학교 사회과학대학 외래교수 ** 전남도립남도대학 초빙교수

cyber crimes. Further, cyber crimes beyond national boundaries require to be treated in international cooperation and relevant procedural arrangements through which the world can fight against them together. However, in current laws, there are only regulations such as substantial laws including simple regulations on punishment against violation. In procedure, they are treated based on the same procedure as that of general criminal cases which are offline crimes. In respect to international cooperation system, international criminal private law cooperation is applied based on general criminals, which brings many problems. Therefore, this study speculates the procedural law on cyber crimes and presents actual problems of our country and its countermeasures.

▸ Keyword : 컴퓨터범죄(Computer Crime), 지능화(Intelligent techniques), 첨단화(Advanced techniques) 수사절차(Investigation Procedure), 네트워크 환경(Network Environment)

Ⅰ. 서 론

최근 인터넷이 널리 보급되고 생활에 없어서는 안 될 필수품이 되면서 사이버범죄가 날로 증가하고 있으며, 이에 대한 대응으로 사이버공간에서의 각 기관의 활동도 활발하게 이루어지고 있다. 일례로 경찰청의 '사이버테러대응센터'는 불법 복제물 판매, 불법 사이트 운영, 온 라인 명예훼손과 성폭력 등의 업무를 담당하고 있으며[1], 대검찰청산하에 있는 사이버범죄 대응기관인 '인터넷범죄수사센터'는 해킹, 컴퓨터바이러스 유포와 이용한 사기, 개인정보침해 등에 중점을 두고 활동하고 있고[2], 국가정보원의 '정보보안 119'는 정부산하 각급 기관이 운영하는 시설에서 발생하는 해킹·바이러스 등 각종 보안사고를 처리하고 조사하며[3], 정보통신부의 '개인정보침해신고센터'는 개인정보 침해에 대한 조사 및 시정조치 등의 업무를 담당하고 있다[4]. 그러나 이러한 각 기관들의 노력에도 불구하고 최근 사이버범죄의 공격기술을 보면 추적회피기술, 방어우회기술이 급속도로 발전하고 있고 전 세계에 있는 다수의 취약시스템을 경유지로 사용하기도 한다[5]. 또한 새로 개발되어 공개되는 사이버공격 도구들을 보면 기본적으로 취약점 공격·추적회피·증거훼손 등 완전범죄를 노리는 기술들이 패키지형태로 개발되어 유포되고 있다[6]. 따라서 단순 예방기술로는 한계가 있을 수밖에 없으며 최소한 사안에 따라서는 실시간 추적 등 특별한 절차를 통해서 대응할 수밖에 없다.

또한 더 나아가 국경을 넘어서는 사이버범죄의 특성상 세계가 공동으로 대응할 수 있는 국제적인 협력과 관련된 절차법적 정비가 요구된다. 그러나 우리의 현행법은 단순히 침해행위에 대한 처벌규정 등 실체법 등의 규정만 있고 절차상으로는 오프라인 범죄인 일반 형사사건과 동일한 절차를 밟아 대응하며 국제적인 협력체제도 일반형사사범을 기반으로 한 국제형사사법공조법을 적용하고 있어 많은 문제를 내포하고 있다.

정보통신시설에 대한 범죄가 국가적, 사회적 혼란을 야기할 수 있는 성격의 범죄라는 것이 통상적 인식이고 보면[7], 이를 예방하고 대응하기 위해 그 중요성에 맞는 특별한 절차법 규정이 필요할 것이다.

이에 본 논문에서는 9.11 테러사건 이후 사이버안전을 위한 수사와 관련된 효과적인 수단들을 마련하고 있는 미국의 경우를, 그 중에서도 사이버범죄대응절차법을 중심으로 살펴보고 우리 법제에 있어서의 시사점을 제시하고자 한다.

Ⅱ. 미국의 사이버범죄대응 절차법

2.1 서설

미국의 사이버공간상의 범죄 수사를 위한 절차법규로는 1986년에 발효된 전기통신프라이버시법(Electronic Communications Privacy Act of 1986, 18 U.S.C. §§2701-2712 : ECPA)을 비롯하여 통신감청을 위한 감청법(Wiretap Statute, 18 U.S.C. §§2510~2522), 네트워크 모이터링 및 추적을 위한 펜트랩법(Pen/Trap Statute, 18 U.S.C. §§3121~3127)등이 있다[8].

미국은 9.11 테러사건이후 패트리어트법(USA Patriot Act 2001)을 의회에 제출, 10월 26일 발효되었는데 이 법

은 기존의 사이버수사절차와 관련된 법률들인 전기통신프라이버시법, 감청법, 팬트랩법등의 규정을 개정하여 한층 강화된 권한을 행사할 수 있도록 하는 내용을 포함하고 있다.

한편 지난 2002년에는 「사이버안전확장법(Cyber Security Enhancement Act)」이 제정되었는데 기존의 처벌규정 및 수사절차상의 일부 규정들이 개정되었다.

미국에서 통신공간의 수사를 위해서 마련된 제도는 다양하다. 먼저 전기통신프라이버시법상에서 각종 증거를 수집할 수 있는 제도로 제출명령(subpoena), 법원명령(court order), 수색영장(search warrant)이 규정되어 있으며[9], 감청법(TittleⅢ)에서는 전기통신의 내용을 지득할 수 있는 감청명령(TittleⅢ order)이 규정되어 있고[10], 펜트랩법에서는 네트워크상의 실시간 추적을 위한 펜트랩명령(Pen/Trap order)을 규정하고 있다[11]. 물론 다른 점은 많이 있지만 우리나라의 제도와 비교한다면 제출명령은 행정기관의 자료제출요청 공문과 성격이 비슷하며 법원명령, 펜트랩명령은 통신비밀보호법상의 통신사실확인자료요청과 유사하다. 수색영장은 압수·수색영장과, 감청명령은 통신비밀보호법상의 통신제한조치(일명 '감청영장')와 유사하다.

2.2. 정보통신수사절차법

펜트랩법은 특정 전화에 의해서 전화 연결된 전화번호와 같은 통신과 관련된 내용이 아닌 소통정보의 수집을 관장한다. 관련규정들은 아래와 같은 3가지 중요한 방식에서 개정되었다.[12]

따라서 미 연방법전 제18권의 제3121조, 제3123조, 제3124조, 제3127조를 개정하여 대상통신기술에 휴대전화번호와, 인터넷사용자 계정 또는 이메일주소, IP주소, 포트번호 또는 유사한 컴퓨터네트워크 주소 또는 주소의 범위를 포함할 수 있게 했다. 나아가 수정안은 펜트랩명령(Pen/Trap Order)으로 유선과 전자통신의 진행과 전송에서 이용되는 정보들 즉 통신내용이 아닌 모든 다이얼링, 라우팅, 주소할당 및 신호정보 등을 획득할 수 있도록 하고 있다. 그렇지만 통신의 내용을 감청하는 것을 허락하는 것은 아니다. 나아가, 전화이용상황기록장치와 함정과 추적 장치는 종종 물리적으로 목적설비에 부착될 수 없는 소프트웨어인 경우도 있기 때문에 '목적설비에 부착되거나 적용되어'지는 장치로 개정되었다.

2.3. 사이버범죄수사절차법

패트리어트법(Patriot Act)에서 제정된 컴퓨터범죄 및 전자증거와 관련된 새로운 내용들을 살펴보면 다음과 같다[13].

2.3.1 음성메일 및 저장된 음성통신 획득

이전의 법조항에서는 전기통신프라이버시법(ECPA)에 의해 저장된 이메일과 같은 전자통신에 대한 접근은 수색영장을 통해서 가능했지만, 저장된 음성메일과 같은 유선통신은 감청영장을 사용하도록 되어 있었다.

2.3.2 컴퓨터 해킹수사에서의 감청 권한

이전법률에 의하면, 수사관들은 컴퓨터사기와남용에관한 법률(18 U.S.C. §1030) 위반 사항에 대하여 음성을 포함하는 유선통신내용을 지득하기 위한 감청영장을 발부 받을 수 없었으나 유선통신에 대한 감청영장을 발부받을 수 있는 대상범죄를 나열하는 구절에 미 연방법전 제18권의 제1030조의 중대범죄 위배를 추가하였다.

2.3.3 전자적 증거에 대한 제출명령의 범위

이전의 법률인 전기통신프라이버시법(ECPA) 제2703조(c)항은 법집행기관이 제출명령으로 고객의 이름, 주소, 서비스의 기간, 지불수단과 같은 제한된 등급의 정보를 획득할 수 있도록 하였으나 고객의 실제 신원을 결정하는 것과 관련된 특정 기록들(예컨대 통신서비스를 사용하기 위한 신용카드 숫자 또는 다른 형식의 지불수단)을 포함하지 않았기 때문에 사용자들이 가짜 이름을 사용하여 인터넷서비스 제공자에 등록하게 되는 점을 간과했다. 더군다나, 제2703조(c)항의 많은 정의들이 기술 특정적이었으며, 주로 전화통신과 관련되어졌기 때문에 '세션시간과 기간의 기록들'과 같은 컴퓨터 네트워크상에서의 통신에 관한 대등한 문구를 포함하지 않았다[14].

따라서 제2703조(c)항을 수정하여 법집행기관이 제출명령을 가지고 얻을 수 있는 기록들의 목록을 확장했다. 즉 구체적인 목록에 '어떠한 일시적으로 할당된 네트워크 주소' 뿐만 아니라, '세션시간과 기간의 기록들'과 '지불의 수단과 원천'에 관련된 정보도 포함시켰다.

2.3.4 케이블 법률 범위의 명확화

이전의 미국법률은 전화 및 인터넷 서비스에 관해서는 ECPA, 감청법 등이 적용되었고 케이블 서비스에 대해서는 케이블법(47 U.S.C. §551)이 관장하고 있었는데 케이블법률은 케이블회사에 의해서 소유되는 대부분의 기록에 대한 법집행기구의 접근을 극도로 제한하고 있었다. 예를 들어, 케이블법률은 접속기록들을 얻기 위한 제출명령 또는 심지어는 수색영장의 사용마저 허락하지 않았다. 대신에, 케이블회사는 고객들에게 미리 고지를 해야 했으며 정부는 고객으로 하여금 법정에 변호사와 함께 나타나도록 하고 법정에

그 기록을 얻기 위한 필요성과 정당성을 인정받아야 했다. 그러나 의회가 케이블법을 통과시켰던 1984년도와는 달리[12], 많은 케이블회사들이 전통적인 케이블 프로 서비스뿐만이 아니라 인터넷라인과 전화서비스까지 제공하기 때문에 범죄수사에서 중대한 어려움을 야기했다[15].

따라서 그 법률을 개정하여 고객이 케이블 회사로부터 인터넷 연결과 전통적인 케이블 TV 서비스 모두를 같이 수신하고 있는 경우에, 정부주체는 전기통신프라이버시법(ECPA)하에서 그 회사로 하여금 인터넷서비스와 연관된 고객의 기록들만을 공개하도록 강요할 수 있도록 하였다.

2.3.5 통신회사에 의한 긴급공개

통신회사에 의한 자발적인 공개와 관련된 이전의 법률은 부적절한 측면이 있었다. 즉 이전의 법률은 회사로 하여금 비상시에 고객의 기록 또는 통화내역 등을 공개하도록 허용하는 특별조항을 포함하고 있지 않았다. 예를 들어 한 ISP가 독립적으로 자신의 고객 중의 한 사람이 현저한 테러리스트 공격을 수행하는 조직의 일원이라는 것을 알게 되었을 경우에, 법집행기관에 대해 그 계정정보를 공개하게 되면 생명들을 살릴 수도 있으나 이러한 정보를 제공하는 근거규정이 없었기 때문에 공개를 하는 ISP는 민사소송을 당할 수 있었다[16].

따라서 이 부분을 개정하여 미 연방법전 제18권의 제2702조(b)(6)항에 서비스제공자로 하여금 긴급한 살인의 위협 또는 어떠한 사람에 대한 심각한 신체적인 상해를 포함하는 비상시에 그 내용 또는 내용이 아닌 고객기록을 법집행기구에 공개하는 것을 허용하도록 했다.

2.3.6 컴퓨터 투입자의 통신내용 감청

감청법은 자신들의 권리와 재산을 보호하기 위해서 컴퓨터시스템 소유자가 자신의 시스템상에서의 행위를 감시하는 것을 허용하고 있지만 그런 감시를 수행하는 경우에 법집행기구의 지원을 받을 수 있는지의 여부가 불분명했다. 따라서 법집행기구가 피해자들이 자연적이고 합리적인 조처를 취하는 것을 지원하는 것에 어려움이 있었다. 실제로, 서비스제공자들이 종종 그들 스스로 공격을 감시하기 위해서 필요한 기술자와 장비 또는 금전적인 자원이 부족하기 때문에 그들은 일반적으로 허가받지 않은 공격자들로부터 그들을 방어하기 위한 그들의 권리를 행사하기 위한 어떠한 효과적인 방법도 가지고 있지 않는 경우가 있다. 즉 '컴퓨터 해커의 부당한 사생활 권리가 해킹 피해자의 합법적인 사생활권리를 이겼다'는 '결과'를 만들어낸 것이다.

이 문제를 수정하기 위해서, 개정법률은 컴퓨터 공격의 피해자로 하여금 법집행기구가 자신의 컴퓨터 시스템상에서 무단침입자들을 감시하는 것을 인가해주도록 허용한다. 즉 법집행기구는 보호되는 컴퓨터로 전송되는 무단침입자의 통신을 감청할 수 있는 것이다. 그러나 다음과 같은 네 가지의 요구 조건이 충족되어야 한다. 첫째, 보호되는 컴퓨터의 소유자 또는 운영자가 침입자의 통신 감청을 인가해야 한다. 둘째, 통신을 가로채는 개인은 법적으로 수사에 종사해야 한다. 셋째, 감청되는 통신의 내용이 진행되는 조사와 관련되어 있다는 합리적인 근거를 가지고 있어야 한다. 넷째, 조사관들은 침입자에 의해서 보내어지거나 또는 수신되는 통신만을 감청할 수 있다.

2.3.7 이메일 수색영장에 전국적 효력

과거에는 법집행기관이 개봉되지 않은 이메일을 공개토록 할 때 6개월 짜리의 수색영장을 사용했으며, 이 영장은 발부하는 법원의 관할구역내에서만 유효하기 때문에, 몇몇 법원들은 다른 구역에 위치한 이메일에 대한 제2703조(a)항의 영장을 발부하기를 거절했다. 이런 문제는 수사중인 범죄행위와 아무 관계도 가지고 있지 않을 지라도 주요 ISP들이 위치한 지역에 대한 엄청난 행정적인 짐을 지우게 되었을 뿐만 아니라 수사관들로 하여금 원격관할에서 영장을 얻도록 요구함으로써 수사에 많은 장애를 초래하였다.

따라서 개정법은 제출명령, 명령과 동일하게 수사관들이 법원이 위치한 지역 외에서 기록을 획득하기 위해서도 수색영장이 사용될 수 있도록 하였다. 즉 수사에 대한 관할을 가지고 있는 법원들이 주요한 ISP들이 위치한 지역에 있는 요원, 검찰 그리고 판사들이 간섭을 요구하는 것 없이 직접적으로 증거를 요구하도록 허용하는 것이다.

2.3.8 사이버테러의 抑制와 防止

그 외 미 연방법전 제18권의 제1030조, 컴퓨터사기와남용에관한법률에서 보호되는 컴퓨터를 훼손한 해커들에 대한 형벌을 최고 10년형에서 최고 20년형으로 강화했으며, 해커는 단지 훼손의 고의만 필요하지, 특정한 유형의 훼손이 필요한 것이 아니다는 것을 명백히 하기 위해서 그러한 공격에 대하여 요구되는 범의를 명확히 하고, 국가안보 또는 사법정의에 사용되는 컴퓨터의 손괴에 대한 새로운 범죄를 추가했다. 법률의 효력범위를 미합중국의 각주 연합 또는 외국상업에 대한 영향이 있는 한, 외국 나라에 있는 컴퓨터들을 포함하도록 확장했다.

2.4 사이버안전확장법

미국은 2002년 3월 사이버안전확장법(Cyber Security Enhancement Ace)을 제정했다[17] . 이 법은 사이버 보안을 강화하기 위한 다양한 조항들을 가지고 있는데 제1030조를 개정하여 해커들이 범죄를 저지르기 위해 컴퓨터를 도구로 사용하여 고의로 생명 또는 신체에 중대한 위해를 일으켰거나 일으키려고 한 경우 보다 무거운 형을 선고하도록 규정하고 있으며 국가기반구조보호센터(National Infrastructure Protection Center : NIPC)가 정부차원의 위협측정, 경보, 수사, 중요기반시설에 대한 공격 대응의 초석으로서의 역할을 다 할 수 있도록 규정하고 있다. 또한 패트리어트법(Patriot Act)에 의해 '긴급시의 예외' 규정에 의해 ISP가 사람의 생명 또는 신체에 대한 중대하고 급박한 위험이 관련된 긴급한 상황에서 지체 없는 정보 제공이 필요한 때에 법원의 감독이나 사용자에 대한 고지 없이 법집행기관과 이메일 컨텐츠 및 전기통신의 내용을 공유할 수 있도록 한 것에서 한걸음 더 나아가 예외 규정의 범위를 더 넓혀 법원의 감독이나 사용자에 대한 고지 없이 'ISP'가 선의로(in good faith) 사람의 생명 또는 신체에 중대한 위험이 관련된 긴급상황시 지체 없는 정보의 공개가 요구된다고 믿는 때에 정부기관에 대하여' 관련 정보를 제공할 수 있도록 하고 있다.

III. 미국의 사이버 수사 절차법

3.1 전기통신프라이버시사법상의 증거수집절차

전기통신프라이버시법(ECPA)은 네트워크 서비스 제공자로부터 정부기관이 어떠한 절차로 사용자(subscriber) 계정정보를 취득할 수 있는지를 규정하고 있다. 동법은 기본적으로 어떠한 정보가 서비스사용자의 프라이버시의 핵심에 더욱 근접한가를 기준으로 절차를 구분하고 있다[18] . ECPA에 따르면 수사기관은 관련 자료를 수사상 취득할 때 첫째, 네트웍서비스의 유형, 둘째, 자료 및 정보의 유형, 셋째, 자료 및 정보요청의 방법을 고려하여야 한다. 네트워크 서비스의 유형은 다음과 같다.

3.1.1 전기통신서비스

전기통신서비스(Electronic Communication Service : ECS)란 사용자에게 전기통신이 가능하도록 하는 서비스로서 전화서비스, 이메일서비스 등이 이에 해당한다. 이 때 전자적 저장공간(Electronic storage)이라는 개념이 등장한다[19] . 이는 '데이터 전송과정에서 부수적으로 존재하는 전자통신상의 임시적 · 중간적 저장공간', 또는 ECS에 의해 생성되는 저장공간'을 의미한다. 여기서 '임시적 저장공간'이라는 표현이 핵심이며, 즉 아직 당해 서비스의 최종 목적지에 도달하지 않은 중간상태를 의미한다. 실무적으로는 관련 서비스가 ECS인지 여부는 이 전자적 저장공간의 유무로 판단하게 된다.

3.1.2 원격컴퓨팅서비스

원격컴퓨팅서비스(Remote Computing Service : RCS)란 '전자통신시스템을 이용하여 컴퓨터 저장공간 또는 데이터 처리를 사용자에게 제공하는 서비스'이다[20]. 전자통신시스템이란 '회선·전자 통신의 전송을 위한 유선, 무선, 전자석, 광학, 광전자학적 설비' 또는 '그러한 통신의 전자적 저장 공간장치를 위한 컴퓨터 장치'라고 한다[21] .

ECS의 경우에는 사용자의 파일이나 통신이 제3자에게 전송되기 전 ECS의 필요에 의해 전자적 저장공간에 임시로 저장되는 반면, RCS는 계정을 가지고 있는 사용자의 필요에 의해 파일이나 자료가 보관되거나 처리된다. 따라서 RCS의 저장 장치는 전자적 저장공간과는 개념이 다르다. 또한 RCS는 유료든 무료든 누구나 계정을 발급받을 수 있는, 이른바 일반에 공개된 서비스만을 의미하며, 특정한 부류의 사람들만이 계정을 발급받을 수 있는 경우는 RCS에 해당하지 않는다.

3.2 자료 및 정보의 유형

3.2.1 사용자 기본정보

ECPA의 사용자 기본정보(Basic Subscriber Information)에는 첫째, 사용자의 신원과 관계된 정보, 둘째, 사용자와 서비스 제공업자와의 관계에 관한 정보, 셋째, 기본적인 접속기록의 세가지가 있다. 보다 구체적으로는 이름(name), 주소(address), 전화접속기록, 또는 접속유지시간[22], 서비스 사용기간(서비스 개시일시 포함)과 제공되는 서비스 유형, 전화번호, 장비번호, 기타 사용자번호 또는 신원, 일시적으로 부여된 네트웍 주소 등, 서비스 이용 지불방법(신용카드 번호 또는 은행계좌번호 포함)이 해당한다. 즉 이는 기존의 사용자 기본정보에 2001년 Patriot Act에 의해 접속유지시간, 유동 IP주소(서비스에 접속하는 소스어드레스 또는 소스전화접속번호가 포함된 것임)[23], 서비스비용 지불방법이 추가된 것이다. 우리나라 전기통신사업법상의 통신자료와 비교해 볼 때 그 범위가 상당히 넓음을 알 수 있다.

3.2.2 사용자에 관한 기록 또는 기타 정보

사용자에 관한 기록 또는 기타 정보(Records or Other Information Pertaining to a Customer or Subscriber)는 사용자 기본 정보와 통신 콘텐츠 그 자체를 제외한 서비스 사용자와 관련된 정보를 의미하며[24] , 통신 또는 데이터 전송과 관련된 정보들로서 계정사용내역 로그파일, 사용자가 이메일을 주고받은 상대방의 이메일 주소 등이 그 예이다. 이는 사용자의 온라인 접속에 관하여 전반적이고 보다 자세한 내용을 담도 있는 정보를 단순한 사용자 기본 정보와 구분하기 위해 따로 규정한 것이다.

3.2.3. 콘텐츠

콘텐츠(Contents)는 사용자 계정에 저장되어 있는 파일 또는 통신내용 그 자체를 의미한다.[25] 이는 앞서 살펴본 ECS의 전자적 저장 공간에 저장되어 있는 것, RCS 의 저장 장치에 저장되어 있는 것, ECS나 RCS 모두에 해당되지 않는 서비스의 저장 공간에 저장되어 있는 것 모두를 지칭한다.

3.3 자료 및 정보요청의 방법

ESPA에서 규정하고 있는 강제수사 절차는 아래와 같으며 수사기관이 사용자 프라이버시의 핵심에 가까운 정보를 요구할수록 보다 엄격한 법적 요건이 요구된다.

3.3.1 제출명령

제출명령(subpoena)은 가장 법적 요건이 약하며 발부절차가 간소한 강제수사 절차이다. ECPA에서 인정되는 제출명령에는 정부기관발부 제출명령(administrative subpoena), 연방·주 대배심 발부 제출명령(administrative subpoena), 연방·주 대배심 발부 제출명령(federal or state grand jury subpoena), 법원제출명령(trial subpoena)이 있다.[26]

3.3.2 사용자 고지 후 제출명령

사용자 고지 후 제출명령(subpoena with prior notice to the subscriber or customer)은 서비스 제공자에게 제출명령을 제시하기 전에 관련 정보의 당사자인 사용자에게 그 사실을 미리 고지하여야(prior notice)한다. 앞의 제출명령으로 취득할 수 있는 정보, RCS에 보관 중인 사용자의 콘텐츠, ECS의 전자적 저장 공간에 보관 중인 사용자의 콘텐츠 중 180일이 초과된 것을 요구할 수 있다. 이러한 선고지 의무는 특별한 경우에 감독기관의 증명이 있는 경우 후통보로 대신하여 집행 가능하다.[27]

3.3.3 법원명령

법원명령(court order)이란 연방치안판사(federal magistrate), 연방지방법원(district court), 주법원(state court) 판사가 증거 확보 등을 위해 발하는 명령이다.[28] 이를 발부받기 위해 수사관은 통신 콘텐츠나 관련 기록 정보 등이 진행 중인 범죄의 수사에 본질적으로 관련되어 있다는 특정적·명시적 사실을 제시하여야 한다. 제출명령보다는 그 발부 요건이 까다롭다.

법원명령으로는 제출명령으로 요구할 수 있는 모든 자료, 콘텐츠를 제외한 사용자에 관한 기록 또는 기타 정보를 요구할 수 있다.

3.3.4 사용자 고지 후 법원명령

사용자 고지 후 법원명령(court order with prior notice to the subscriber or customer)은 서비스 제공자에게 법원명령을 제시하기 전에 관련 정보의 당사자인 사용자에게 그 사실을 미리 고지하여야 한다.[29]

이로서는 사용자에 의해 열람되지 않은, 즉 전자적 저장 공간의 이메일 중 보관 일수 180일 이내의 콘텐츠를 제외한 모든 정보를 요구할 수 있으며, 구체적으로 법원명령으로 요구할 수 있는 모든 자료, RCS에 보관 중인 사용자의 콘텐츠, ECS의 전자적 저장공간에 보관 중인 사용자의 콘텐츠 중 180일이 초과된 것이 있다. 이 또한 제출명령과 마찬가지로 후통보로 집행 가능하다.

3.3.5 수색영장

수색영장(search warrant)은 법원의 치안판사(magistrate)에 의해 발부된다. 수사기관은 법원에 수색영장을 신청할 때 선서진술서(affidavit)와 발부 받고자 하는 수색영장의 원본(warrant itself)을 제출한다. 선서진술서에는 수사기관이 수색이 정당하다고 믿는 상당한 이유(probable cause)를 명시한다. 원본에는 수색의 장소, 압수의 대상이 특정된다. 증거를 취득하는 절차들 중 가장 법적 요건이 엄격하다. 수색영장을 통해 수사기관은 ECS의 전자적 저장공간의 콘텐츠 중 보관 일수 180일 이내의 콘텐츠를 포함, 사용자와 관련된 모든 자료와 정보를 취득할 수 있다.

3.3.6 임의적 공개

일반에 공개되지 않은(not available to the public) 서비스의 제공자는 저장되어 있는 콘텐츠를 비롯하여 모든 정보를 수사기관에 제공할 수 있다. ECPA는 원칙적으로 일반에 공개된(available to the public) 서비스 제공자의 임의적 정보제공(voluntary disclosure)만을 규제하고 있으나, 다음과 같은 예외가 있다[30] .

첫째, 콘텐츠가 제공의 대상인 경우 서비스의 제공, 또는 서비스 제공자의 권리와 재산의 보호에 필수적인 경우, 콘

텐츠가 서비스 제공업자에 의해 우연한 기회에 확보되었으며, 범죄의 실행과 관련이 있는 것으로 보여 수사기관에 제출되는 경우, 서비스 제공자가 합리적으로 판단컨대, 정보의 공개가 사람의 생명, 신체의 위해에 급박한 위험을 초래하여 긴급성이 요구되는 때, 아동보호와 성폭력에 관한 법률(Child Protection and Sexual Predator Punishment Ace)에서 규정하는 경우[23] , 의도된 수신자 또는 발신자의 동의가 있거나, 법원명령이나 법정절차에 의하여 의도된 통신의 수신자에게 공개하는 경우, 서비스 제공자의 임의적 공개를 허용한다.

둘째, 콘텐츠가 아닌 사용자 정보가 그 대상인 경우 서비스의 제공, EH는 서비스 제공자의 권리와 재산의 보호에 필수적인 경우, 서비스 제공자가 합리적으로 판단컨대, 정보의 공개가 사람의 생명, 신체의 위해에 급박한 위험을 초래하여 긴급성이 요구되는 때, 의도된 수신자 또는 발신자의 동의가 있는 경우, 또는 법원명령이나 법정절차에 의하는 경우에 서비스 제공자의 임의적 공개가 허용된다.

3.4 펜트랩법 및 감청법상의 증거수집절차

미국은 우리의 통신비밀보호법이 감청의 대상이 통신 중인 내용인지, 통신이 완료된 후 저장되어 있는 내용인지 특별히 규정하고 있지 않고 단지 '통신의 음향•문언•부호•영상'이라고만 규정하고 있는 것과는 다르게 통신이 완료되어 보다 엄밀하게 이야기하면, ECS의 전자적 저장공간에 보관되어 있는 경우는 통신이 완료되어 ECS에 일시적으로 보관되어 있거나 또는 RCS에 저장되어 있는 경우는 ECPA가 규제하는 한편, 통신 중의 실시간 모니터링(real-time electronic surveillance)에 관해서는 펜트랩법과 감청법(Title Ⅲ)으로 규제한다[24] .

펜트랩법은 전기통신의 접속정보 등 콘텐츠 이외의 정보를 실시간으로 취득하는 절차를 규정하고 있는 반면, Title Ⅲ는 콘텐츠 그 자체를 획득하는 절차를 규정하고 있다. 전자와 후자에 이용되는 툴의 기능부터 명확히 구분된다. 전자의 경우는 접속정보 등이 기록되어 있는 패킷 또는 이메일의 헤더만을 캡춰하도록 설계되어 있는 반면, 후자는 패킷전체(entire packet)나 이메일 자체를 스니핑할 수 있도록 되어 있다.[31]

3.4.1 펜트랩법

이 법에 의해 검사(government attorney)나 수사기관은 법원에 추적장비(pen register and/or trap and trace device)의 설치를 허가하는 명령(pen/trap order)의 발부를 신청할 수 있다[32] . 이 장비에 의해 취득될 정보가 현재 진행 중인 범죄의 수사에 관련이 있다는 사실이 명시되어야 한다. 명령의 신청시 또는 집행시 이 장비가 설치될 서비스 제공자가 모두 특정될 필요는 없다.

복잡하게 얽혀져 있는 네트웍을 통해 통신이 이루어지는 것이 보통이므로, 특정한 서비스 사업자를 대상으로 발부된 명령은 당해 통신과 관련된 모든 서비스 제공자들에게도 그 효력이 미친다. 수사의 효율을 기하기 위한 규정이다. 동 명령은 60일간 유효하며, 필요시 60일간 그 효력을 연장할 수 있다.

3.4.2 감청법

감청법(Title Ⅲ)에는 'intercept'라는 표현이 등장하는데 이는 통신 중인 내용의 실시간 취득(acquired contemporaneously)만을 의미하며, 앞서 살펴본 저장공간에 보관 중인 콘텐츠의 취득은 해당되지 않는다. 후자의 경우는 전기통신프라이버시법(ECPA)에 따르게 된다[33].

감청법(Title Ⅲ)의 구조는 간단하다. 원칙적으로 쌍방의 통신에 그 통신에 관여하고 있지 않은 제3자가 개입하는 것을 금지한다. 그리고 이러한 금지가 적용되지 않는 예외를 규정한다. 동법은 다양한 예외규정을 두고 있으며 특히 수사상 많이 적용되는 예외들은 다음과 같다. ① Title Ⅲ 명령에 의한 감청의 경우-Title Ⅲ 명령(Title Ⅲ order) 발부의 법적 요건은 상당히 엄격하다. 우선, 동 명령을 법원에 신청할 때 감청을 통해서 동 법에 열거된 중대한 범죄(felony)에 대한 증거가 확보될 수 있다는 상당한 이유(probable cause)가 명시되어야 한다. 또한 다른 일반적인 수사절차가 시도되었으나 증거를 취득할 수 없었다는 사실, 또는 그러한 방법으로는 증거의 취득에 성공할 수 없을 것이라거나 그 방법이 위험을 초래할 것이라는 합리적 근거, 당해 통신수단이 범죄에 이용되고 있다는 상당한 이유, 감청이 증거 취득 이외의 경우 필요 최소한도에 그칠 것이라는 사실이 명시되어야 한다. 동 명령은 법무부(Justice Department)의 허가(authorization)와 지방법원(US District Court) 또는 항소법원(US Court of Appeals) 법관의 승인을 거쳐야 발부된다[34]. ② 당사자의 동의 - 실제 통신에 참여하고 있는 양 당사자들 중 어느 일방의 동의를 득한 경우 수사기관은 감청을 실시할 수 있다. ③ 서비스 제공자의 권익에 관한 예외- 서비스 제공자가 자신의 권리와 재산을 보호하기 위해 실시하는 감청은 허용되며, 이 과정에서 취득한 증거를 수사기관에 제출할 수 있다. 그러나 이는 서비스 제공자 본인에 의해 직접 이루어져야 하며 수사기관이 대신 행할 수는 없다. 단, 서비스 제공자가 수사기관에 관련 증거를 제출한 이후에는 수사기관이 이어

서 감청을 실시할 수 있다. ④ 불법침입에 관한 예외 - 시스템 공격의 피해자들은 수사기관으로 하여금 당해 시스템이 목적지, 경유지, 또는 출발지인 불법침입자(computer trespasser)의 통신을 감청하도록 수사기관에 의뢰할 수 있으며[35], 이로서 수사기관에 감청권한이 부여된다. 반드시 피해자의 요청이 선행되어야 하며, 불법침입자의 통신 내용이 수사와 관련된 것이라고 믿을만한 합리적 근거가 있어야 한다.

III. 우리 현행 법제의 고찰

3.1. 서설

우리나라는 통신비밀보호법에서 당사자의 동의가 없는 감청과 검열을 규제하고 있으며 또한 각종 특별법에서 사이버범죄 대응 절차법을 마련하고 있으나 앞서 살펴본 미국의 경우에서처럼 체계적인 규정은 아직 완비하지 못하고 있는 현실이다. 그러나 미국과 같은 정도에 법규가 완비되어 있지 않다. 따라서 이하에서는 우리 현행법을 살펴본 후 그 문제점을 일별하고자 한다.

3.2.1 통신비밀보호법

우리나라는 통신비밀보호법(2005.05.26 법률 제7503호)에서 누구든지 법원의 허가 없이는 검열[36]과 감청[37]을 할 수 없도록 하고 있으며[38], 통신사실확인자료[39]는 통신비밀의 자유와 사생활침해의 우려가 많아 통신비밀보호법의 적용대상에 포함, 법원의 허가를 받도록 하여 이를 제한하고 있다.[40] 또한 통신제한 조치 후에는 대상자에게 사후통지를 하게 함으로서 그 남용을 방지하고 있다. 통신제한조치는 과학기술의 발달에 의하여 새로이 등장한 수사기법으로 「일정한 요건 즉 요건대상 범죄를 계획·실행하고 있거나 실행하였다고 의심할 만한 충분한 이유가 있고, 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거수집이 어려운 때에 한하여 대상자의 우편물을 검열하거나 전기통신을 감청하는 것」을 말하며 임의수사와 강제수사의 한계문제로 다루어지고 있으나, 당사자에게 직접 강제력을 행사하지 않고, 의무를 부과하지도 않는다는 점에서는 임의수사와 유사하나, 통신제한조치가 개인의 사생활(privacy)을 중대하게 침해한다는 점에서 강제수사로 보아야 한다. 따라서 통신비밀보호법이 통신제한조치를 행할 경우 일정한 요건하에 법원의 허가를 얻도록 규정하고 있다. 그 동안 제한조치의 범위가 너무 확대되어 남용이 여지가 많았으나, 통비법의 개정으로 대상범죄가 280개 범죄로 축소되었으며 , 통신제한조치의 대상범죄는 통신비밀보호법 제5조 제1항 각호에 상세하게 규정되어 있고, 이법에 의하여 규정되어 있지 않은 범죄는 당사자의 동의가 있어 비밀성이 보장되지 않는 예외적인 경우를 제외하고는 통신제한조치를 할 수 없다. 통신제한조치의 대상은 제5조 제1항 제1호의 요건에 해당하는 자가 발송·수취하거나 송·수신하는 특정한 우편물이나 전기통신 또는 그 해당자가 일정한 기간에 걸쳐 발송·수취하거나 송·수신하는 검열이나 우편물이나 전기통신을 대상으로 허가될 수 있다. 제한조치의 기간은 범죄수사를 목적으로 한 경우에는 2개월을 초과할 수 없고, 허가요건이 존속하는 경우에는 그 절차에 따라 2개월의 범위내에서 연장허가를 받아야 한다고 규정하고 있으나 이는 미국의 법제와 비교 했을때 그 기간이 너무 길다는 문제점이 있다.

허가절차 및 관할법원은 사법경찰관이 각 피의자별 또는 각 피내사자별로 통신제한조치허가를 신청, 검사의 청구로 법원에서 통신제한조치 허가서를 받아 이루어진다. 그러나 청구권자를 검사 및 사법경찰관으로 인정할 필요성이 있다. 검사·사법경찰관 또는 정보수사기관의 장은 국가안보를 위협하는 음모행위, 직접적인 사망이나 심각한 상해의 위험을 야기할 수 있는 범죄 또는 조직범죄의 계획이나 실행 등과 같은 긴박한 상황이 있고, 법원의 허가나 대통령의 승인에 필요한 절차를 거칠 수 없는 법 제8조의 규정에 의한 긴급처분을 할 수 있고, 사법경찰관이 긴급통신제한조치를 할 경우에는 미리 검사의 지휘를 받아야 한다. 다만, 특히 급속을 요하여 미리 지휘를 받을 수 없는 사유가 있는 경우에는 긴급통신제한조치의 집행착수 후 지체없이 검사의 승인을 얻어야 한다. 제6조에 규정하는 절차를 거칠 수 없는 긴급한 사유가 있는 때에는 그 통신제한조치를 집행한 때부터에 제6조 및 제7조 제3항의 규정에 의한 절차에 따라 법원의 허가 또는 대통령의 승인을 받아야 하며 법원의 허가를 받지 못한 때에는 즉시 그 통신제한조치를 중지하여야 한다(동법 제8조).

.집행사실 통지제도를 살펴보면 단시간 내에 종료되어 법원의 허가를 받을 필요가 없는 경우 그 종료 후 에(범죄수사규칙상'지체없이') 긴급통신제한조치통보서를 작성하여 지방검찰청 검사장에게 송부, 지검장은 다시 이를 법원장에게 송부해야 한다. 또한 통신제한조치를 집행한 사건에 관해 검사로부터 공소를 제기하거나 제기하지 아니하는 처분(기소중지 제외)의 통보를 받거나 내사사건에 관하여 입건하지 아니하는 처분을 한 때에는 그 날로부터 에 대상자에

게 통지해야 한다. 통지유예 승인을 받은 경우에는 그 사유가 해소된 날로부터 30일 이내에 통지하여야 한다. 기소(참고인)중지시에는 통지대상이 아니나 재기하여 종국처분시에는 역시 통지대상이다. 집행사실을 통지한 경우에는 지체없이 관할지방 검찰청 검사장 또는 지청장에게 보고하여야 한다. 통신제한조치와 긴급통신제한조치 모두 해당되며 통신제한조치를 집행한 사실, 집행기관 및 그 기간 등에 대해 통지해야 한다(구두 및 전화통지는 불가).

3.2.2 전기통신사업법등

전기통신사업법(2006.03.24 법률 제7916호, 정보통신부)은 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공연히 전시하는 내용의 전기통신, 사람을 비방할 목적으로 공연히 사실 또는 허위의 사실을 적시하여 타인의 명예를 훼손하는 내용의 전기통신, 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하게 하는 내용의 전기통신, 정당한 사유없이 정보통신시스템· 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 전기통신, 청소년보호법에 의한 청소년유해매체물로서 상대방의 연령확인·표시의무 등 법령에 의한 의무를 이행하지 아니하고 영리를 목적으로 제공하는 내용의 전기통신, 법령에 의하여 금지되는 사행행위에 해당하는 내용의 전기통신, 법령에 의하여 분류된 비밀 등 국가기밀을 누설하는 내용의 전기통신, 국가보안법에서 금지하는 행위를 수행하는 내용의 전기통신, 범죄를 목적으로 하거나 교사 또는 방조하는 내용의 전기통신을 이용행위를 하여서는 아니된다(동법 제53조)라고 규정하여 불법통신의 금지 등을 금지하고 있다. 또한 공익침해목적허위통신(제47조제1항)과 사익침해목적행위(제47조 제2항)등 허위통신행위를 규제하는 전기통신기본법, 전기통신업무종사의 비밀침해·누설(제69조, 제54조 제2항) · 일반 비밀침해·누설(제70조, 제54조 제1항) · 이용자 정보의 공개(제71조, 제34조의5 제1항, 제2항)등 비밀누설행위 및 전기통신설비의 손괴 등 소통방해를 처벌하는 전기통신사업법이 있으며, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2006.03.24 법률 제7917호, 정보통신부)은 사람을 비방할 목적으로 정보통신망을 통하여 공연히 사실을 적시하여 타인의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 2천만원 이하의 벌금에 처하고, 사람을 비방할 목적으로 정보통신망을 통하여 공연히 허위의 사실을 적시하여 타인의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처하도록 규정하고 피해자의 명시한 의사에 반하여 공소를 제기할 수 없다고 규정하고 있다(동법 제61조). 즉 개인정보의 훼손, 침해, 누설행위와 정보통신망 침해행위를 규제하는 정보통신망이용촉진및정보보호등에관한법률, 프로그램저작권 침해 · 프로그램 복제물을 업무상 사용하거나 통신망을 통해 전송, 배포하는 행위 · 직무상 알게된 프로그램저작권 비밀누설행위를 처벌하는 컴퓨터프로그램보호법(2005.12.29 법률 제7796호, 정보통신부), 공공기관의 개인정보를 변경, 말소한 행위 · 공공기관의 개인정보를 누설, 권한없이 처리 또는 타인의 이용에 제공· 허위 기타 부정한 방법으로 공공기관으로부터 처리정보를 열람 또는 제공받는 행위를 처벌하는 공공기관의개인정보보호에관한법률(1999.01.29 법률 제5715호, 행정자치부)이 있다.

3.3. 현황 및 문제점

우리의 통신비밀보호법이 감청의 대상이 통신 중인 내용인지, 통신이 완료된 후 저장되어 있는 내용인지 특별히 규정하고 있지 않고 단지 '통신의 음향 ·문언·부호·영상'이라고만 규정하고 있는 것과는 다르게 미국은 통신이 완료되어 ECS의 전자적 저장공간에 보관되어 있는 경우는 통신이 완료되어 ECS에 일시적으로 보관되어 있거나 또는 RCS에 저장되어 있는 경우는 ECPA가 규제하는 한편, 통신 중의 실시간 모니터링(real-time electronic surveillance)에 관해서는 펜트랩법과 감청법(Title Ⅲ)으로 규제한다.

우리나라의 제도와 비교한다면 제출명령은 행정기관의 자료제출요청 공문과 성격이 비슷하며 법원명령, 펜트랩명령은 통신비밀보호법상의 통신사실확인자료요청과 유사하다. 수색영장은 압수·수색영장과, 감청명령은 통신비밀보호법상의 통신제한조치(일명 '감청영장')와 유사하다.

우리 통신제한조치의 경우 엄격한 법원의 통제를 받도록 그 요건을 강화하고 있으나, 통신사실확인자료나 통신자료 대상이 명확하지 않는점, 핸드폰의 전파추적(호추적)을 통한 실시간 위치추적은 감청에 해당하므로 통신사실확인자료 요청으로는 가능하다는 점. 타인간의 상면대화 내용의 녹음이 필요한 경우에는 통신제한조치를 신청해야 한다. PC통신 인터넷 전자우편 비공개모임(Close User Group)의 게시내용 지득 또는 채록은 기본적으로 감청에 해당된다. 전화(컴퓨터 통신 포함)등 가입자의 대금결재(요금납부) 방법에 있어서의 자동이체 계좌의 번호를 알고자 하는 경우 감청절차가 아닌 압수수색영장에 의한다.

Ⅳ. 결 어

이상에서 살펴본 것과 같이 미국의 경우 사이버공간상의 범죄 수사를 위한 절차법규, 즉 패트리어트법, 전기통신프라이버시법, 감청법, 팬트랩법, 사이버안전확장법이 잘 정비되어 있으며, 동법률들의 개략적인 내용으로서 사용자에 관한 기록 또는 기타 정보의 예외를 인정한 점, ESPA에서 규정하고 있는 강제수사 절차는 수사기관이 사용자 프라이버시의 핵심에 가까운 정보를 요구할수록 보다 엄격한 법적 요건이 요구된다는 점, 제출명령이 가장 법적 요건이 약하며 발부절차가 간소한 강제수사 절차라는 점, 사용자 고지 후 제출명령제도, 판사가 증거 확보 등을 위해 발하는 법원명령제도, 증거를 취득하는 절차들 중 가장 법적 요건이 엄격한 수색영장을 통해 수사기관은 ECS의 전자적 저장공간의 콘텐츠 중 보관 일수 180일 이내의 콘텐츠를 포함, 사용자와 관련된 모든 자료와 정보를 취득한 점, 일반에 공개되지 않은 서비스의 제공자는 저장되어 있는 콘텐츠를 비롯하여 모든 정보를 수사기관에 제공할 수 있도록 한 점등이다. 우리나라의 사이버관련 법규, 즉 통신비밀보호법을 비롯한 전기통신기본법, 전기통신사업법, 정보통신망이용촉진및정보보호등에관한법률, 컴퓨터프로그램보호법, 공공기관의개인정보보호에관한법률이 있으나 위에서 지적한 내용들은 앞으로 우리 법제를 정비 하는데 필요하다.

참고문헌

〔1〕 http://www.ctrc.go.kr.; 2006.7.25.검색.
〔2〕 http://spo.go.kr/kor. ; 2006.7.1.검색
〔3〕 http://www.ncsc.go.kr. ; 2006.6.11.검색
〔4〕 http://www.mic.go.kr. ; 2006.7.2.검색
〔5〕 양근원, "사이버테러의 실태와 법적 대응에 관한 연구", 경희대학교 석사학위논문, 2003, 27-29면.
〔6〕 양근원, 상게논문, 17면
〔7〕 http://www.cybercrime.gov/PatriotAct.htm. ; 2006.7.2.검색
〔8〕 양근원, 전게논문 127 ~128면 127-129면.
〔9〕 http://www.cybercrime.gov ;2006 .8.2.검색
〔10〕 오기두, "형사절차상 컴퓨터관련증거의 수집 및 이용에 관한 연구", 서울대학교 박사학위논문, 2003, 43-49면.
〔11〕 「Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations」(미국 법무부 컴퓨터범죄지적재산과 http://www.cybercrime.gov 발간)
〔12〕 양근원, 전게논문, 78면
〔13〕 양근원, 상게논문, 89면
〔14〕 양근원, 상게논문, 91면
〔15〕 로어크 M. 리드 외, 정완 역, 미국의 형사절차, 서울: 한국형사정책연구원, 2000, 164면
〔16〕 로어크 M. 리드외, 정완 역, 상게서, 169면
〔17〕 정완, "국제조직범죄 및 하이테크범죄 대책을 위한 G8 장관회의", 「형사정책연구소식」, 제57호(2000.1)..278면
〔18〕 로어크 M. 리드 외, 정완 역, 미국의 형사절차, 서울: 한국형사정책연구원, 2000, 164면
〔19〕 정완, "하이테크범죄대책에 관한 국제동향", 「형사정책연구」, 제10권 제4호(통권 제40호, 1999·겨울호),212면
〔20〕 양근원, 전게논문, 78-79면.
〔21〕 오기두, 전게논문, 46-54면.
〔22〕 한봉조, "사이버범죄수사에 대한 국제적 협력문제", 「사이버범죄의 실태와 대책」, 제25회 형사정책세미나 자료(2000.5) 121면
〔23〕 한봉조, 상게논문, 127면
〔24〕 오기두, 전게논문, 40-42면
〔25〕 정완, 상게논문, 44면
〔26〕 Computer Crime and Intellectual Property Section (CCIPS), Field Guidance in New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001(http://www.cybercrime.gov/PatriotAct.htm2007. 6. 17 방문)
〔27〕 양근원, 상게논문, 23면
〔28〕 양근원, 상게논문, 25면
〔29〕 양근원, 상게논문, 26면
〔30〕 한봉조, 상게논문, 132면
〔31〕 한봉조, 상게논문, 141면
〔32〕 http://www.cybercrime.gov ;2006 .8. 3.검색
〔33〕 정완, 상게논문, 47면
〔34〕 정완, 상게논문, 52면
〔35〕 양근원, 상게논문, 43면
〔36〕 "검열"이라 함은 우편물에 대하여 당사자의 동의없이

이를 개봉하거나 기타의 방법으로 그 내용을 지득 또는 채록하거나 유치하는 것을 말한다.

〔37〕 "감청"이라 함은 전기통신에 대하여 당사자의 동의없이 전자장치·기계장치등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다.

〔39〕 "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다. 가입자의 전기통신일시. 전기통신개시·종료시간 . 발·착신 통신번호 등 상대방의 가입자번호 . 사용도수 . 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료 . 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료 . 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료를 말한다.

〔40〕 로어크 M. 리드외, 정완 역, 상게서, 172면

저 자 소 개

임 병 락

2005년 2월, 조선대학교
법학박사 과정
2005.~ 현재 :
조선대학교 사회과학대학
외래교수

오 태 곤

2005년 2월, 조선대학교
법학박사
2004.~ 현재 :
전남도립남도대학 초빙교수