2010-26 | 책임연구보고서

디지털 범죄에서 프라이버시(Privacy) 보호에 관한 연구

치안정책연구소
POLICE SCIENCE INSTITUTE

2010-26 | 책임연구보고서

디지털 범죄에서 프라이버시(Privacy) 보호에 관한 연구

치안정책연구소 생활안전대책연구실

선임연구관 김 학 신

<목 차>

Ⅰ. 서 론 ·····1

Ⅱ. 디지털 범죄의 개념과 유형 ·····3

1. 디지털 범죄의 개념 ·····3

2. 디지털 범죄의 유형 ·····6

가. 컴퓨터 범죄 ·····6

나. 사이버 범죄와 인터넷 범죄 ·····7

다. 정보범죄와 하이테크 범죄 ·····9

라. 소결 ·····10

3. 디지털 범죄에서의 사생활 침해 ·····11

Ⅲ. 미국의 디지털 범죄 수사에서 사생활(privacy) 보호 ·····13

1. 미국 헌법상 사생활(Privacy) 보호에 관한 원칙 ·····13

2. 사생활(Privacy) 보호의 발전과 의의 ·····17

3. 디지털 저장장치 수색을 통한 사생활 침해 ·····19

4. 제3자 소유의 디지털 정보유출에 의한 사생활 침해 ·····21

5. 디지털 증거 수집에 의한 사생활 침해 ·····23

6. 인터넷에 공개된 자료에 의한 사생활 침해 ·····26
7. 경찰이 보유한 디지털 증거 수색에 의한 사생활 침해 ·····28

Ⅳ. 한국에서 디지털 범죄와 사생활의 보호 ·····30
1. 사생활 보호에 관한 헌법 규정 ·····30
2. 사생활의 보호의 요구 ·····31
3. 디지털 범죄에서 사생활 침해 가능성의 증대 ·····32

Ⅴ. 디지털 범죄에서 사생활 보호를 위한 법제 정비 ·····34
1. 헌법상 사생활 보호를 위한 입법 원칙 ·····34
2. 디지털 범죄 범위 규정을 통한 사생활 보호 ·····35
3. 디지털 범죄에서 사생활 보호를 위한 입법제정의 필요성 ·····38
4. 사생활 보호를 위한 입법절차 안(案) ·····40

Ⅵ. 결 론 ·····53

【參 考 文 獻】 ·····55

Ⅰ. 서 론

독일의 IT 전망 분석기업인 트랜드 원(Trend One)사의 CEO인 닐스 뮬러(Lils Muller)는 '기술과 인간이 하나가 되는(technology and human become one)' 시대가 빠르게 다가오고 있다고 하였다. 현재의 인터넷 웹(web) 환경이 인간처럼 스스로 지능을 갖는다는 웹 3.0의[1] 시대를 거쳐 앞으로 인간이 기술의 연장으로 업그레이드되면서 언제나 온라인과 연결되어 웹과 대화하는 웹 4.0시대를 바라보면서 인터넷을 통한 디지털 기술의 환경은 빠르게 발전하고 있다.

그리고 이러한 디지털 기술의 급속한 발달과 발맞추어 필연적으로 이에 대한 역기능도 급속하게 증가하고 있는 실정이며 컴퓨터, 스마트 폰 등을 비롯한 다양한 디지털 기기를 통한 새로운 신종 범죄의 방법과 기술들은 언제, 어디서나 쉽게 범죄자에게 악용되고 있다. 그 결과 인터넷과 스마트 폰 등을 통한 신종 범죄들이 쏟아지고 있는 실정이다.

더구나 이러한 범죄 기술과 신종 범죄에 대처하는 경찰을 비롯한 수사기관은 범죄자를 따라잡지 못하는 것이 현실이다. 이는 무엇보다 급속도로 증가하는 신종 범죄에 비하여 이에 대처하는 디지털 범죄 전문 수사관의 부족과 신속하게 디지털 범죄를 해결할 수 있는 기술력 및 관련 법제가 미비한 것도 그 하나의 원인이다.

정보통신기술의 발달이 급속히 진행되면서 과거 그 어느 때보다도 개인의 사생활의 자유가 침해될 위험성과 가능성은 더욱 커지고 있다.[2]

---

1) 웹 3.0의 예로 미국 국방부 산하 방위고등연구계획국(DARPA)은 2007. 11. 대(對) 테러전에 대비하여 컴퓨터를 이용하여 인공지능으로 운전하는 무인자동차를 개발·발표하였다. 조선일보, 2007. 11. 29.

2) 桂禧悅, 憲法學(中), 博英社, 2007, 391면.

이러한 배경에 의하여 현재는 컴퓨터 및 디지털 기기에 집적되는 정보의 양이 많아지고 있으며, 그 부작용으로 인한 개인 사생활의 침해 문제가 심각한 사회문제로 등장하고 있다.

컴퓨터를 통한 인터넷과 스마트 폰 등 다양한 디지털 기기들이 현재에는 통신 뿐 아니라 디지털 자료 및 정보의 저장 창고 역할도 하고 있다. 이러한 디지털 자료들이 범죄자들의 해킹 등을 통해 누설되는 경우에 개인의 사생활의 비밀이 유출되는 일이 발생하게 된다. 또한 경찰이 디지털 범죄를 수사함에 있어 그에 따른 일환으로 범죄행위를 한 용의자 및 혐의자와 관련된 컴퓨터, 휴대용 전화기, USB 등 관련 디지털 저장매체에서 디지털 증거 자료를 수집함에 있어 컴퓨터 서버나 공용으로 쓰는 컴퓨터에서 범죄와 관련이 없는 타인의 개인 정보 및 중요한 자료들이 공개되거나 유출이 되어 사생활의 침해가 발생하고 있다. 이러한 개인의 디지털 자료들이 경찰을 비롯한 수사기관이 범죄를 수사함에 있어 침해되는 경우를 방지하기 위하여는 헌법이나 관련 법률에 근거를 두고 사생활의 침해가 최소화 될 수 있도록 해야 할 것이다.

우리 헌법 제17조에「모든 국민은 사생활의 비밀과 자유를 침해받지 아니 한다」또한 헌법 제18조에「모든 국민은 통신의 비밀을 침해받지 아니 한다」고 규정하고 있음에도 불구하고, 현재 제정되어 있는 관련 법률 하에서는 경찰 수사기관이 디지털 범죄를 수사함에 있어 범죄와 관련이 없는 타인의 개인정보를 비롯하여 사생활이 유출·공개되는 부분에 대하여 하위 법률에서 구체적으로 규정되어 있지 않아 헌법상 보장된 국민의 사생활이 침해되는 문제가 제기될 수 있다.

따라서 위와 같은 디지털 범죄를 수사함에 있어 사생활 침해 문제점을 해결하기 위하여는 관련 법률을 제정하거나 기존 관련 법률을 개정할 필요가 있다. 그리고 경찰은 이 법률 규정에 근거하여 엄격한 절차에 따라 디지털 범죄를 수사함으로써 헌법상 보장된 개인의 사생활이 침해되지

않도록 해야 할 것이다.

현재 우리나라에서는 경찰을 비롯한 수사기관이 디지털 범죄를 수사함에 있어 발생하는 사생활 침해 문제에 관하여 관련된 사례가 거의 없는 실정이며, 더불어 이에 대하여 국내에서 선행되어진 연구가 거의 없다고 보여진다. 따라서 국가적, 사회적, 정책적으로 디지털 범죄 수사에서 발생하는 사생활 침해 문제에 대한 연구 및 이에 대한 대응책이 시급하다 할 수 있다.

이에 반해 미국의 경우는 기존 전통적인 범죄사례와 판례에서 사생활 침해 문제를 도출하여 디지털 범죄에 적용하여 해결하고 있으며, 이에 대한 관련 법률 및 지침서도 어느정도는 정비되어 있다.

따라서 이러한 미국의 관련 사례 및 판례에 대한 구체적이고 심도있는 검토를 통하여 현재 뿐만 아니라 앞으로 경찰이 디지털 범죄에서 발생할 수 있는 국민의 사생활 침해 문제점과 대응에 관하여 고찰하고자 한다.

물론 개인의 사생활이 침해되는 부분은 다양하게 나타나고 있지만, 여기에서는 경찰에 의한 디지털 범죄 수사와 관련하여 미국 헌법상 보장된 개인 사생활의 침해에 한정하여 살펴보고자 한다.

Ⅱ. 디지털 범죄의 개념과 유형[3)]

1. 디지털 범죄의 개념

3) 김학신, 디지털 범죄 수사와 기본권에 관한 연구(영장제도를 중심으로), 치안정책연구소, 2009. 5, 6-13면; 김학신,디지털 범죄 수사와 기본권, 한국학술정보(주), 20-28면.

1984년 William Gibson이라는 미국의 과학소설 작가가 'Neuromancer'라는 소설에서 '사이버 공간'[4]이라는 용어를 사용하였으며, 이는 현실적·물리적 세계와는 구분이 되며 이러한 사이버 공간의 출현은 인터넷[5]이 있기에 가능했다.[6] 그러나 1876년에 미국의 알렉산더 그레햄 벨(Alexander Graham Bell)이 오늘날 대중화된 통신장치의 하나인 전화를 발명하였을 때 이미 사이버 공간은 조성이 되었다.[7]

현재 우리가 사용하는 대부분의 전자기계들은 디지털의 방식으로 이루어져 있다. 컴퓨터를 비롯하여 스마트 폰, 디지털 카메라, USB, 캠코더, PDA 등 다양한 기기들이 디지털의 방식으로 이루어져 있으며, 그 결과 디지털 혁명, 디지털 세대, 디지털 기술 등 디지털이란 용어가 대중화 되었다. 이러한 디지털 기기의 발달은 우리나라를 정보화 선진국으로 견인하는 주요한 원동력이 되었다. 이와 더불어 모든 분야가 유비쿼터스(Ubiquitous)[8]환경으로 진입하게 되고, 모든 생활은 전자 매체를 통하

---

4) 尹明善,「美國憲法과 統治構造」, 유스북, 2006. 2, 432면 이하 참조.

5) 인터넷(Internet)은 최초의 대륙간 해저 통신망으로 1858년 설치된 Atlantic Cable이 그 시초로 기록되고 있다. 1969년 미 국방성의 지원으로 미국의 4개 대학을 연결하기 위해 구축한 알파넷(Advanced Research Project Agency NETwork:ARPANET)으로 군사적·학술적 부문에 제한되었을 뿐 일반인의 사용은 허용되지 않다가 1991년에 음성과 정지화상, 동영상을 동시에 전달 할 수 있는 World Wide Web(www이라 함)이 개발되면서 비로소 일상화 되었다. Michaael Rustad & Cyrus Daftary, E-Business Legal Handbook, 2002 ed., pp.3-5; 朴宣映,「가상공간에서의 성표현의 자유와 법적 제한」, 한국법제연구원, 2002. 12, 5면.

6) Cees J. Hamelink, The Ethics of Cyberspace, 2000, Sage Publications, London, p.9; David R. Koepsell, The Ontology of Cyberspace, Open Court, Chicago, 2000, p.16; G. David Garson, Social Dimensions of Information Technology: Issues for the new Millemium, Idea Group Pu. Hershey, 2000, p.88; 백광훈,「인터넷범죄의 규제법규에 관한 연구」, 한국형사정책연구원, 2000. 12. 35면.

7) Gina De Angelis, "ARPANET, HACKERS, CRACKERS, AND PHREAKS", Cyber Crimes, Philadephia (Chelsea House Publishers), 1999, pp.13-21.

8) 유비쿼터스(Ubiquitous)란 '언제, 어디에나 있는' 뜻의 라틴어로 누구나 장소에 상관없이 자유롭게 네트워크에 접속 할 수 있는 환경을 말한다. 이 용어는 1988년 미국의 복사기 회사인 제록스 팰로알트 연구소의 마크 와이저(Mark Weiser)가 '유비쿼터스 컴퓨팅' 이라는 용어를 처음으로 사용하면서 등장하였다. 그는 이 용어를 '어디에서든 접속이 가능한 컴퓨터 환경(computing acess will be everywhere)'으로 정의하였다. 정준현,「유비쿼터스 컴퓨팅과 프라이버시보호」, 成均館法學, 第16券 第1號, 2004, 465면.

여 이루어지고 있다.

또한 경찰을 비롯한 수사기관의 범죄 수사 분야에서도 전자 매체를 통한 디지털의 활용은 필수불가결한 요소로 등장하였다. 현재 우리나라에서 CCTV(closed-circuit television)는 광범위하게 활용되고 있으며, 휴대전화 사용 내역 및 위치 추적 확인 기능 등은 범죄 수사에서 중요하게 활용되고 있다.

최근에는 스마트 폰, 이동식 저장장치(USB Memory),[9] PMP(portable multimedia player),[10] 전자수첩, 내비게이션(Navigation),[11] 디지털 카메라(digital camera), 디지털 캠코더(digital camcorder) 등 다양한 디지털 기기에 중요한 디지털 정보가 저장되고 있어 이러한 기기들을 통하여 범죄 수사에 활용할 수 있는 가치가 점점 증가하고 있다.

이러한 다양한 종류의 디지털 기기들은 새로운 형태의 신종 범죄를 발생케 하는 원인이 되었다. 이처럼 다양한 디지털 기기로 인하여 발생하는 모든 범죄를 디지털 범죄라 할 수 있을 것이다.

현재 사이버 공간에서 발생하는 범죄를 부르는 용어가 혼용되어 쓰이고 있는데, 보통 컴퓨터 범죄, 사이버 범죄, 인터넷 범죄, 디지털 범죄[12], 정보 범죄, 하이테크 범죄 등으로 다양하게 호칭이 되고 있다.

---

9) USB 메모리 등 이동식 저장장치를 통한 악성코드 전파가 2007년 6월 25건, 7월 33건, 8월 38건 등으로 증가하고 있다. USB를 매개로 한 대표적 악성코드는 'VBS/Solow'이며, 이는 사용자들이 PC에 USB를 연결해 실행시킬 경우 자동으로 USB에 감염된다. 이를 다른 PC에서 실행시키면 해당 PC를 감염시키는 방식으로 전파된다. 매일경제신문, 2007. 9. 3.

10) PMP라 함은 '음악 및 동영상 재생, 디지털카메라 기능까지 모두 갖춘 휴대용 멀티미디어 재생장치'를 말한다.

11) Navigation은 항공기 또는 선박을 어느 한 지점으로부터 일정의 다른 지점으로 소정의 시간에 도달할 수 있게 유도하는 방법을 말한다.

12) 디지털이라 함은 데이터(data)나 물리적인 양을 0과 1이라는 2진 부호의 숫자로 표현하는 것을 말한다. 즉 소리, 영상, 문자 등 모든 정보를 0과 1의 숫자로 바꾸어서 저장, 재생되는 것을 말한다. 디지털은 원본과 100% 동일한 복제가 가능하며, 정보저장의 단위와 용량이 명확하고, 데이터를 압축·조작하여 효율적인 전송이 가능하여 정밀도를 높일 수 있다는 특징이

따라서 여기에서 이 부분에 대하여 간단히 용어에 대한 개념을 정리하고자 한다.

2. 디지털 범죄의 유형

가. 컴퓨터 범죄

컴퓨터 범죄에서 말하는 컴퓨터의 정의는 어디까지나 법률적인 개념으로 자연과학적인 컴퓨터의 개념과 반드시 일치하는 것은 아니다. 특히 형법에 의한 보호의 필요성이 있는 것으로 한정되어야 하는데, 범죄 유형에 따라 그 대상이 되는 컴퓨터의 범위가 다를 수 있다.[13]

컴퓨터 범죄에 대하여 광의와 협의로 보는 견해가 있는데, 광의설은 처벌 필요성을 이유로 들어 처벌법규가 없다 하더라도 컴퓨터를 이용한 위법행위를 컴퓨터 범죄로 보는 견해이다. 미국 변호사협회의 정의에 따르면 컴퓨터 범죄는 '컴퓨터를 절도, 사기, 횡령 등을 쉽게 하는 수단으로 이용하는 범죄(computer as a tool of crime)', '컴퓨터 자체를 범죄의 대상으로 하는 범죄(computer as an object of crime)'로 구분하고 있다.[14]

협의설은 컴퓨터 범죄란 컴퓨터가 범죄행위의 수단 또는 목적인 고의의 재산적 침해행위만을 의미한다는 견해이다. 최협의설은 협의의 컴퓨터 범죄의 범위 내에서 현금지급기에 사용하는 현금인출카드와 각종 신용카드를 이용한 범죄는 따로 분리시키고, 나머지 부분을 컴퓨터 범죄로 보는 견해이다.[15]

있다.

13) 심원섭,「컴퓨터 신종범죄에 관한 연구 -인터넷 관련 범죄를 중심으로-」, 연세대학교 석사학위논문, 2004, 5면.

14) S. H. Kadish, Crime and Justice, p.219.

15) 南孝淳·丁相朝,「인터넷과 法律Ⅱ」, 2005. 12, 146면.

미국 법무부는 2002년 8월 FBI Law Enforcement Bulletin에서 컴퓨터 범죄에 대하여 다음과 같이 정의하고 있다.

컴퓨터 범죄라 함은 '범죄를 저지르고 그 범죄를 조사하는데 있어서 컴퓨터 지식이 관련되어 있는 사건'으로 정의하고 있다.[16] 현재 컴퓨터 범죄라는 용어는 상당히 보편화된 용어중의 하나이다. 보통 컴퓨터 범죄라 함은 컴퓨터를 대상으로 하거나 또는 수단으로 하여 행하는 범죄 행위를 말한다.[17]

컴퓨터 범죄를 '컴퓨터와 관련한 정보처리과정에 불법적으로 개입하는 모든 범죄행위'[18] 또는 '컴퓨터의 데이터와 관련하여 형법적으로 처벌할 가치가 있는 범죄 행위의 총체'[19]라고 정의하는 것이 컴퓨터의 속성을 잘 나타낼 수 있다고 생각된다.

현재 우리나라도 컴퓨터 등 정보처리장치를 이용한 사기, 비밀침해, 공·사전자기록의 위작·변작 및 동행사죄 등 컴퓨터 관련 범죄를 처벌하는 규정을 마련하고 있으며, 재물 손괴죄 등에 대해서도 전자기록 등 특수매체기록을 행위객체로 추가하여 처벌하고 있다.[20]

나. 사이버 범죄와 인터넷 범죄

16) 미국의 FBI의 National Computer Crime Squad(NCCS)에서는 컴퓨터 범죄를 다음과 같이 분류하고 있다. privacy 침해, 공중전화망(PSTN), 주요 컴퓨터 네트워크의 침입·무결성 위반, 산업 스파이, 소프트웨어 불법복제 등으로 분류하고 있다. 미국 법전 18권 47장 1030절에서는 컴퓨터와 관련하여 연방법으로 처벌할 수 있는 사기행위를 정의하고 있는데 데이터, 정부기관, 은행/재무 시스템, 전자상거래 등과 관련된 범죄이다. Debra Littlejohn shinder(강유譯),「사이버범죄 소탕작전 컴퓨터 포렌식 핸드북」, 에이콘출판사, 2003. 8, 16면.

17) 독일의 Wolfgang Heinz 교수에 따르면 '특별한 기술적 가능성을 이용하는 모든 범죄의 총체' 즉, 컴퓨터 특유의 범죄를 말한다고 한다. Wolfgang Heinz,「컴퓨터 범죄와 컴퓨터 형법(독일의 컴퓨터 범죄 현황과 대응)」, 한양대 법학연구소 컴퓨터 범죄 세미나, 2000. 10. 4, 발표논문 참조.

18) 강동범,「컴퓨터 범죄와 개정형법」, 법조 46권 8호, 1997. 8, 107-108면.

19) 임종률,「컴퓨터 범죄와 형법적 대응」, 숭실대학교 법학 논집 제5집, 1989. 12, 68면.

20) 朴相基,「刑法各論」, 博英社, 1999, 9면 참조.

IT(Information Technology)의 발전으로 인하여 컴퓨터를 대상으로 하는 범죄가 지나가고 네트워크(Network)로 연결된 공간이 생기게 되었다. 이를 사이버 공간이라고 하는데 사이버 범죄라 함은 이 사이버 공간에서 발생하는 범죄를 총칭하는 용어로 보면 될 것이다.

사이버 공간에 대한 정의는 다소 추상적이며, 이에 대하여 야후(Yahoo)의 설립자 제리 양은 '당신의 모니터와 내 모니터 사이'가 사이버 공간이라고 설명하였는데, 인터넷 통신망으로 구축된 정보교환의 장을 말한다. 이 공간은 사람의 말초감각으로는 감지되지 않으면서도 엄연히 현실적으로 존재하는 가상의 생활공간이 사이버 공간이다. 이는 물리적으로는 존재하지 않기에 만질 수는 없지만, 많은 사람이 감정을 나누면서 느끼고, 대화하고, 물건도 거래하는 그런 공간이다.[21]

결론적으로 사이버 범죄는 많은 인터넷 사이트와 그것들을 연결시켜주는 컴퓨터 네트워크 망을 범행의 수단, 목표로 이용한 범죄 행위를 말한다. 이러한 사이버 공간과 관련하여 일어나는 모든 범죄행위를 총칭하여 사이버 범죄 내지 인터넷 범죄라고 넓은 의미로 정의하고 있다.[22]

사이버 범죄와 인터넷 범죄의 용어간에 다소 차이가 있을 수는 있다. 사이버 범죄란 인공적·가상적인 공간을 무대로 일어나는 행위라고 한다면, 인터넷 범죄는 인터넷이라는 네트워크에 관련된 행위만을 의미 한다고 볼 수 있기 때문이다. 그러나 사이버 공간이 인터넷과 네트워크로 연결된 것을 고려한다면 현재로는 양자가 같은 의미로 보면 될 것이다.

---

21) 조병인 외3,「사이버범죄에 관한 연구」, 한국형사정책연구원, 2000, 18면.

22) 김종섭,「사이버 범죄 현황과 대책」, 한국형사정책학회(2000년 동계학술회의자료), 2000, 22면; 허일태,「사이버범죄의 현황과 대책」, 동아대학교 법학연구소 세미나 발표논문, 2000. 4. 28, 3면; 허만영,「사이버 범죄에 대한 국가의 정책적 대응방안 (21세기 도전과 사이버스페이스)」, 사이버커뮤니케이션학회 추계학술대회발표논문, 1999. 11. 26, 22면.

다. 정보범죄와 하이테크 범죄

국가정보화 기본법[23] 제3조(정의) 제1호에서 정보의 정의를 다음과 같이 규정하고 있다. “정보라 함은 특정목적을 위하여 광(光) 또는 전자적 방식으로 처리하여 부호, 문자, 음성, 음향 및 영상 등으로 표현된 모든 종류의 자료 또는 지식을 말한다”라고 정의하고 있다.

이를 근거로 정보범죄의 정의를 내리면 ‘정보처리장치 또는 정보를 이용하는 범죄 그리고 정보처리장치 또는 정보에 대한 범죄를 총칭’하는 의미라고 할 수 있다. 그러나 정보 범죄가 정보에 대한 범죄를 총칭한다고 하면 사이버 공간과 무관하게 일어나는 정보에 대한 불법적인 탐색·누설행위도 고려대상이 될 수밖에 없다는 문제점이 있다.[24] 국가정보화 기본법 제3조 제5호에서 ‘정보통신’이라 함은 “정보의 수집·가공·저장·검색·송신·수신 및 그 활용, 이에 관련되는 기기(器機)·기술·서비스 및 그 밖에 정보화를 촉진하기 위한 일련의 활동과 수단을 말한다”고 규정하고 있다.

사실 ‘정보’가 무엇인가라는 문제에 대하여는 국가정보화 기본법 제3조의 정의 이외에도 정보의 정의를 다양하게 정의하는데 정보라 함은 ‘현실 세계로부터 단순한 관찰이나 측정을 통해서 수집한 사실, 개념, 값을 표현한 것’[25] 또는 ‘특정한 사람이나 사항에 대하여 의미 있는 상태로 가공한 것’[26], ‘필요하고 적절한 자료를 활용이 가능한 형태로 처리한 것’[27]과 같은 정의를 내리고 있다.

이와 또 다른 용어로 하이테크 범죄(Hi-Tech Crime)[28]란 용어를 사용

23) 정보화촉진기본법에서 국가정보화기본법으로 2009. 05. 22 법률 제9705호 전부개정.
24) 최영호,「정보범죄의 현황과 제도적 대처방안」, 한국형사정책연구원, 1998, 19면; 백광훈,「사이버범죄에 대한 ISP의 형사책임에 관한 연구」, 한국형사정책연구원, 2003, 40면.
25) 김문일,「컴퓨터 범죄론」, 법영사, 1992, 18면.
26) 유인모,「법학연구와 교육을 위한 컴퓨터 활용」, 영남법학, 제1권 제2호, 1994, 65면.
27) 전지연,「전자적 정보의 형사법적 보호에 관한 연구」, 한림법학 FORUM 제8권, 1999, 53면.

하는데 이는 과학기술 중에서도 컴퓨터 기술 및 정보통신기술 또는 양자의 결합으로 형성되는 가상세계와 직접 관련이 있는 범죄유형만을 하이테크 범죄라고 하는 경향이 있다. 그러나 하이테크 범죄라는 말의 사전적인 의미에는 고도의 과학기술 내지 첨단과학기술을 사용하는 범죄라는 의미가 들어있다. 그렇다면 하이테크 범죄라는 용어에는 사이버스토킹, 인터넷상의 명예훼손 행위 또는 도박행위 등과 같이 정보통신상에서 일어나는 범죄행위이지만 고도의 과학기술이 필요하지 않은 범죄들을 포함하기에는 적절하지 못한 측면이 있다.[29]

라. 소결

인터넷 네트워크를 이용하여 발생하는 범죄에 적절하게 대응하기 위해서는 이를 명확히 정의할 수 있는 적절한 용어가 필요하다.

위에서 설명한 것처럼 사이버 공간에서 발생하는 범죄들을 부르는 명칭은 컴퓨터 범죄, 사이버 범죄, 인터넷 범죄, 디지털 범죄, 정보 범죄, 하이테크 범죄 등 다양한 용어로 사용되고 있다. 이들의 특성 차이가 큰 것은 아니지만 다양한 용어로 불리워지다 보니 다소 혼란을 야기할 수 있다.

또한 기존의 전통적인 범죄와는 수사방법이나 증거수집 및 조사 등에서 달리 취급해야 할 필요성이 있다. 그리고 정보통신 기술의 환경이 급속히 변화되기 때문에 법적 안정성을 중시하는 우리의 법제도를 위해서

---

28) 영국에서는 사이버 범죄를 하이테크 범죄로 부르고 있으며, 하이테크 범죄 유형을 9개로 나누고 있다. ①데이터 절도 ②Denial of Service(DOS)공격 ③바이러스 공격 ④스푸핑(Spoofing) 공격 ⑤무단접근 또는 악용 ⑥해킹을 통한 접근·자료 획득 ⑦금융사기 ⑧데이터나 네트워크 공격 ⑨인터넷의 범죄 악용. 이용완,「유럽(영국, 프랑스, 독일)의 사이버 범죄 수사 및 디지털 증거분석 연구」, 경찰청 수사국, 2004. 12, 29면.

29) 조병인,「하이테크범죄의 실태와 대책」, 한국공안행정학회 국제범죄 세미나 발표논문, 1999. 9. 17, 11면 이하 參照.

라도 새롭게 등장하는 범죄현상을 신속하게 포착하여 개념을 명확하게 하는 작업은 필요하다. 그러나 새롭게 등장하고 있는 범죄현상을 명확하게 표현하는 것은 쉬운 일이 아니며, 많은 사람이 공감할 수 있는 시간적 여유가 필요할 것으로 보인다. 사이버 범죄라는 개념은 상당히 넓은 의미로 사용되고 이 용어가 현재에는 가장 많이 쓰이고 있다.

그러나 최근에는 새로운 형태의 디지털 기기들이 출현하고 있으며, 이러한 디지털 기기들은 다양하게 범죄에 이용되고 결국 새로운 신종 범죄들이 나타나고 있다. 이러한 추세에 맞게 여기에서는 디지털 범죄로 통일되어 쓰기로 하겠다.

3. 디지털 범죄에서의 사생활 침해

최근 세계 각국의 경찰 수사기관은 디지털 범죄에 관한 증거를 수집하기 위하여 훈련과 연구 및 기술도입에 적극적이다. 왜냐하면 디지털 증거는 그 특성상 휘발성이 강하고, 삭제, 위·변조의 조작이 쉽기 때문에 각국의 경찰들은 이에 대비하고 있는 추세이다. 이러한 추세에 따라 경찰을 비롯한 수사기관에 의하여 개인의 사생활의 침해가 증가하고 있으며, 이에 따라 수사기관에 의한 압수·수색영장의 발부요건 및 증거의 수집과 방법, 기술 장비 등에 관한 제한이 엄격해지고 있다.

우리나라의 경우 현행 헌법 제17조와 제18조에서 사생활과 통신의 자유를 보장하고 있음에도 불구하고, 수사기관이 디지털 증거를 수집함에 있어 범죄와 관련이 없는 타인의 개인정보를 비롯하여 사생활이 유출·공개되는 부분에 대하여 구체적으로 규정되어 있지 않아 사생활의 침해 문제가 제기될 수 있다. 그러나 이러한 사생활이 절대적인 것은 아니며,

국가안전보장·질서유지·공공복리를 위하여 필수불가결한 경우에는 법률로써 제한을 할 수 있다.

특히 질서유지나 범죄수사의 목적으로 경찰관이 사진을 촬영하거나, 전화를 도청하거나, 수색하는 것이 문제가 되고 있다. 국가안전보장·질서유지·공공복리를 위한 경우에는 법률이 정하는 바에 의하여 어느 정도의 사생활의 자유에 대한 침해는 인정된다고 한다.

그러나 대법원의 판례에 의하면, 수사기관의 피의사실공표로 인하여 피의자의 명예가 훼손되거나 피의사실이 진실이라고 믿는 데에 상당한 이유가 없는 경우에는 보도 자료의 작성·배포에 관여한 경찰서장과 수사관 및 국가는 연대하여 배상책임을 진다고 판결하고 있다.[30] 이처럼 수사기관이 질서유지라는 명목 하에 범죄수사를 하면서 개인의 사생활이 침해되는 경우가 발생하고 있는데, 아직 우리나라에서는 이 문제에 대한 구체적인 문제점을 제기하고 있지 않고 더불어 관련된 사례도 거의 없는 실정이다.

미국의 경우는 수사기관에 의한 프라이버시 침해 문제와 관련하여 많은 사례가 있고 또한 이와 관련된 문제점들도 많이 제기되고 있다.

미국의 경우 미연방 수정헌법 제4조에서 수사기관의 부당한 압수·수색을 헌법으로 제한하고 있는데, 미국 연방수정헌법 제4조[31]는 '신체·가택·서류·재산의 안전을 위하여 부당한 수색과 압수(unreasonalbe searches and seizures)를 금지' 하고 또 '영장은 상당한 사유(probable cause)가 있어야 하며 이것도 선서 또는 공약으로 지지를 받아야 하고, 영장에는 수색할 장소와 체포될 사람, 압수할 물품을

30) 대판, 1996. 8. 20, 94 다 29928, 공 1996, 2776 이하.

31) FOURTH AMENDMENT [U.S. Constitution] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

기재하여야 한다’ 고 규정되어 있다.

미국 연방대법원에 의하면 영장 없는 수색은 다음 두개의 조건에서 한 가지만 해당하는 경우에는 수정헌법 제4조에 위반되지 않는다고 한다. 첫째로 국가기관의 행위가 개인의 ‘프라이버시에 대한 합리적인 기대(reasonable expectation of privacy)’를 침해하지 않는 경우에는 영장 없이도 수색이 가능하며,[32] 둘째로 수사기관의 영장 없는 수색은 개인의 프라이버시를 침해하지만, 영장요구의 예외에 의한 수색은 ‘합리적일 경우에는 수색이 가능하다’ 고[33] 판시하고 있다.

그러므로 경찰을 비롯한 수사기관은 디지털 범죄와 관련하여 컴퓨터 및 디지털 저장장치를 수색할 경우 범죄와 관련 없이 개인의 프라이버시를 침해하는지 그리고 프라이버시가 침해되었다면 수사에 있어 그것이 합리적인 이유가 있는지 등을 고려해야만 한다.

Ⅲ. 미국의 디지털 범죄 수사에서 사생활(Privacy) 보호

1. 미국 헌법상 사생활(privacy) 보호에 관한 원칙

경찰을 비롯한 수사기관의 수사권의 남용은 개인의 사생활의 비밀과 자유에 대한 중대한 위협이 될 수 있다. 수사권의 발동으로 예를 들어 범죄수사를 위한 사진촬영이나 도청 등으로 말미암아 사생활의 비밀과 자유가 제한될 수 밖에 없는 경우에도 헌법상의 요건에 따라야 하고 필

32) Illinois v. Andreas, 463 U.S. 765, 771 (1983).
33) Illinois v. Rodriguez, 497 U.S. 177, 185 (1990).

요 최소한의 제한이어야 한다.[34]

미국에서 부당한 압수·수색은 개인의 사생활을 보장하기 위한 것인데 그것이 초창기에는 유형물의 압수만을 의미하는 것으로 해석되었다. 예를 들어 남의 집 창 밑에서 엿듣거나, 열쇠구멍으로 실내를 들여다보는 것은 부당한 압수·수색이 아니라고 하였다. 또한 피고인 소유의 공개된 장소에서의 양주병의 발견도 압수·수색에 해당되지 않는다고 하였다.[35] 그리하여 수색은 실질적인 침입이 있어야 하고 압수는 유형물을 대상으로 하는 것이기 때문에 통화자 모르게 전화를 도청하는 것은 압수·수색이 아니며 따라서 이것은 수정헌법 제4조가 말하는 '부당한 압수·수색'에 해당되지 않는다고 하였다.[36]

이에 대한 사건이 아래의 1928년 Olmstead 사건[37]이다. 1920년대에는 정부가 전화도청장치를 사용하여 통화내용을 도청함에 따라 도청에 의한 정부의 비물리적 침해에 대해서도 수정헌법 제4조가 적용될 수 있는가의 문제가 제기되었다.

미국 연방대법원은 1928년 Olmstead 사건에서[38] 최초로 도청문제를

34) 일본판례: 범죄수사를 위한 피의자의 사진촬영은 현재 죄를 범하였다고 의심할 상당한 이유가 있을 경우, 범죄가 막 행해지려고 하는 경우 및 긴급성이 인정되고 그 방법이 일반적으로 허용된 상당성을 갖추었을 경우에는 피의자의 의사에 반해서도 행할 수 있다고 해석하여야 한다. 이러한 경우에 행하여진 경찰관에 의한 사진촬영은 그 대상 가운데 범인의 얼굴 외에 범인의 신변 또는 근처의 제3자인 개인의 모습 등을 포함하고 있더라도 헌법 제13조, 제35조에 위반되지 아니한다. 最大判, 1969[昭和 44]. 12. 24. 刑集 23卷 12號, 1625면.

35) Hester v. United States, 265 U.S 57 (1924).

36) 文鴻柱,「美國憲法과 基本的 人權」, 裕豊出版社, 2002, 521면.

37) 동 사건은 연방 금주단속 수사요원(federal prohibition agent)이 영장없이 대량 밀주제조 음모에 관한 전화내용을 도청한 사건이다. 위와 같은 전화도청은 아무런 물리적 침입이 없었으므로 압수수색에 관한 영장주의를 규정한 수정헌법 제4조나 적법절차 및 사유재산보장을 규정한 수정헌법 제5조를 위반한 것이 아니라고 대법원은 판시하였다. Olmstead v. United States 277 U.S. 438 (1928).

38) 이 Olmstead 사건 원칙은 1942년의 Goldman v. United States, 316 U.S. 129 사건에 적용되었는데, 이 사건의 내용은 옆방의 말을 비밀도청기로 엿듣는 것은 부당한 압수수색이 아니라고 하였다. 또 이 원칙은 1952년의 Oh Lee v. United States, 343 U.S. 747 사건에서 재확인되었다. 文鴻柱, 前揭書, 521면.

다루면서 ‘물리적 침해론’(physical intrusion)으로 불리는 법원칙을 확립하였는데,[39] 연방대법원의 다수의견은 감청은 수정헌법 제4조에 해당되는 압수·수색이 아니라고 판시하였다. 국가기관에 의한 전화감청에는 물리적인 불법침해가 없으므로 ‘수색(search)’에 해당되지 않고, 유체물이 포함되어 있지 않으므로 ‘압수(seizure)’도 이루어진 것이 아니라고 주장하였다.[40]

이에 반해 소수의견은 수정헌법 제4조가 보호하고자 하는 것은「주거·서류·재산 또는 인간관계에 있어서의 사생활 그 자체이며, 그 수단이 무엇이든 간에 개인의 사생활에 대한 정부의 모든 부당한 침해로부터 보호하는데 있다」고 주장하였다. 이 소수의견은 수정헌법 제4조의 해석은 물론 프라이버시 권리 승인의 이정표가 되었다.[41]

이후 1937년 Nardone 사건[42]에서 연방대법원은 연방정부 공무원에 의한 전화도청의 내용은 부당한 압수·수색으로서 도청은 위법이며, 위법한 도청에 의해 얻은 증거는 증거능력이 없다고 판시하였다. 또한 1939년 제2차 Nardone 사건[43]에서는 전화도청의 결과로 발견된 증거도 불법의 과실로서 증거능력을 인정하지 않았다.[44]

1960년대 후반에 들어 전자도청장치를 설치한 사안에서 프라이버시 침해를 이유로 위헌이라고 판시한 이래,[45] 1968년 미국 의회는 일정한 요

39) 동 판결에서 확립된 물리적 침해 이론는 1967년 Katz 사건 판결에서 파기될 때까지 40여년 동안 도청에 관한 판례의 기초이론으로 유지되었다. Denise A. Hill, Telecommunications, Creighton Law Review v13, 1980, p.1279.

40) David M. O’Brien, Privacy, Law, Public Policy Praeger Publishers, 1979, pp. 51-54; 尹明善, 前揭書, 137면.

41) 尹明善, 前揭書, 137면.

42) Nardone v. United States, 302 U.S. 397 (1937).

43) Nardone v. United States, 308 U.S. 338 (1939).

44) Athan Theoharis, FBI Wiretapping: A case study of Bureancratic Autonomy, Political Science Quaryerly V1077, Spring, 1992, p.104.

45) 이 사건에서 피고인 Katz는 연방법령(USC 18-§1084)을 위반하여 Los Angeles로부터 마이애미와 보스톤까지 공중전화 부스(telephone booth)를 이용하여 도박에 관한 정보를 전달하였다. 이에 연방수사관은 그 공중전화 부스 바깥쪽에 전자 도청장치를 부착하여 증거를 확보하

건아래 도청을 허용하는 법률인 옴니버스범죄통제및안전도로법(The Omnibus Crime Control and Safe Street Act, 1968)을 제정하게 되었다.

미연방 수정헌법 제4조는 개인의 프라이버시를 침해하지 않는 수색의 경우에는 헌법에 위배되지 않는다고 판결하고 있다.[46] 여기에는 두 가지의 문제가 있는데 첫째는 프라이버시에 대한 개인의 주관적인 기대가 반영된 것인지, 둘째는 프라이버시에 대한 개인의 주관적 기대가 사회에서 합리적으로 받아드릴 인식이 되어 있는지가 문제가 된다.[47]

미국에서 프라이버시에 대한 기대가 헌법적으로 합리적인지 아닌지 명확한 규정은 없다. 예를 들어 미 연방대법원은 개인이 그의 집안에 있는 재산에 대하여,[48] 닫혀진 공중전화 박스 안에서의 대화,[49] 가정집의 여러 개의 방에서 나온 열(heat)과 관련된 것을 열영상 카메라를 사용한 경우,[50] 빛이 들지 않는 컨테이너(opaque containers)의 내용물에 대하여[51] 프라이버시에 대한 합리적인 기대가 있다고 판시하였다.

이와는 반대로 개인의 프라이버시에 대한 합리적인 기대가 없는 경우는 공개된 장소에서의 활동하는 행위,[52] 가정집 앞에 버려진 쓰레기,[53]

였다. 피고인은 California 지방법원 및 항소심까지 유죄판결을 받았다. 그러나 본 사건에서 문제가 된 것은 검찰측이 증거로 제시한 전화내용 수집 방법이다. 즉, 전화내용이 공중전화실 밖에 전자 수신기록장치를 설치하여 획득한 증거는 전화 사용인의 프라이버시(privacy)의 권리를 침해하여 획득한 것이며, 이는 수정헌법 제4조에서 금지하는 수단으로 수색하고 압수하였다고 하여 연방대법원은 항소심을 파기하였다. 개인의 프라이버시에 대한 권리는 미국헌법에 의해 보호되는 자유(liberty)보다도 우월한 것이고, 연방수사관은 도청장치를 사용하기 전에 선행적으로 법원의 허가를 얻지 않았으므로 그러한 도청에 의해 얻어진 증거는 받아들일 수 없는(inadmissible) 불법적으로(illegally) 얻어진 증거라고 판시하였다. Katz v. United States, 389 U.S. 347 (1967).

46) Katz v. United States, 389 U.S. 347, 362 (1967).

47) O' Connor v. Ortega, 480 U.S. 709, 715 (1987).

48) Payton v. New York, 445 U.S. 573, 589-90 (1980).

49) Katz v. United States, 389 U.S. 358 (1967).

50) Kyllo v. United States, 533 U.S. 27 (2001).

51) United States v. Ross, 456 U.S. 798, 822-23 (1982).

52) Oliver v. United States, 466 U.S. 170, 177 (1984). 수사기관은 대마초가 재배되고 있다는 정보에 의하여 피고인의 집을 조사하러 갔는데 출입이 금지 되었다. 집 옆길로 갔더니 대마초를 재배하는 밭을 발견하였다. 그곳도 출입이 금지 되었지만 밭은 공개되어 있다는 원칙(open

타인이 절도를 하기 위하여 집 주인의 동의 없이 가택에 들어오는 경우[54]에는 개인의 프라이버시에 대한 합리적인 기대가 없다고 본다.

2. 사생활 보호(privacy)의 발전과 의의

미국에서는 헌법상 프라이버시 권리[55]에 관한 명문 규정이 없었다. 이처럼 '프라이버시권'을 구체화하지 않았다 할지라도, 내재적으로 이미 프라이버시가 보장된다는 이념은 19세기말로 거슬러 올라간다. 프라이버시에 관한 가장 최초의 언급은 1880년 Thomas Cooley 판사의 불법행위에 관한 저서에서 나타나는 바, 그에 따르면 이는 '혼자 있을 권리'를 포함한다고 하였다.[56]

프라이버시 권리가 처음 독자적인 권리로 주장된 것이 1890년의 Samuel Warren과 Louis Brandeis에 의하여 쓰여진 '프라이버시권(the right to privacy)'이란 논문에서 독립된 권리로 인정되었는데,[57] 미국에서는 판례법상 인정하게 되었다.[58]

---

field doctrine)에 의하여 밭에 대한 조사는 영장이 없어도 위헌이 아니라고 판결하였다.

53) California v. Greenwood, 486 U.S. 35, 40-41 (1988). 수사기관이 집 밖에 버려진 쓰레기 속을 수색함에는 영장이 필요 없다고 판결한 사건이다. 수사관은 버려진 쓰레기 속에서 마약 포장지를 발견하고, 수색영장을 발부 받아 가택을 수색한 결과 피고인의 집에서 마약을 발견하였다. 수사관이 쓰레기통을 뒤지는 것는 영장이 필요 없으며, 이는 미연방 수정헌법 제4조의 위반이 아니라고 판결하였다.

54) Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978).

55) 프라이버시(privacy)란 말은 '사람의 눈을 피하다'라는 의미의 라틴어 'privatue'에서 유래한다. 權寧星, 私生活權의 意義와 역사적 변천, 言論仲裁委員會, 1983. 6, 13면; 梁邵英, 「犯罪報道로 인한 프라이버시권 侵害에 관한 硏究(韓·日 比較)」, 成均館大學校 大學院 碩士學位論文, 2007. 8, 1면.

56) Thomas C. Cooley, Laws of Torts, 1880, p.29.

57) Samuel D. Warren and Louis D. Brandeis,「The Right to Privacy」, Harvard Law Review, Vol. 4, 1890, p.193; 徐柱實,「Warren·Brandeis의 The Right to Privacy」, 美國憲法硏究 第6號, 美國憲法硏究所, 1995, 45-84면.

58) 1905년 Pavesich v. New England Life Insurance co., 122 Ga. 1901, 50 S. E. 68 (1905). 이 판결이 미국에서 프라이버시 권리를 사법적으로 승인한 최초의 판례이다. 프라이버시 권리가 법원칙으로 승인된 판례는 Melvin v. Reid, 112 Cal. App. 285, 297 (1931) 사건이다. 尹明善, 美國 基本權 硏究」, 慶熙大學校 出版局, 2004. 12. 135면.

이 이후로 프라이버시 권리가 최초로 법원에서 논의되기 시작한 것은 1902년에 뉴욕 州에서 제소된 Roberson v. Rochester 사건[59]이었다. 이 사건에서 원고인 Roberson은 그녀의 동의없이 자기의 초상을 광고에 이용한 밀가루 회사를 상대로 하여 소송을 제기하면서, 정신적 고통을 구제 받기 위해 손해배상을 청구하였다. 원심 법원은 원고의 프라이버시 권리를 인정하였고, 뉴욕주 의회는 이 판결 이후 1903년에 '프라이버시법'[60]을 제정하였다.

그리고 1965년 연방대법원은 수정헌법 제4조에서 보장되는 것과는 명백히 다른 헌법상 프라이버시권을 인정하였다. 이러한 권리는 Griswold v. Conneticut[61]에서 연방대법원에 의하여 처음으로 인정되었다. 그리고 1973년의 Roe v. Wade[62]사건에서 연방대법원은 수정헌법 제14조의 적법절차조항에 의해 명시적으로 프라이버시권이 보장된다고 판시하였다.

위에서 언급한 것처럼 브랜다이스(Brandeis) 판사는 헌법상 프라이버시권을 혼자 있을 권리로서 가장 포괄적인 권리이며 가장 중요시되는 권리라고 하였다.[63] 미국 수정헌법 제4조의 법리에 의해서 프라이버시는 신성한 공간인 자기 가정에서 실제로 고독을 향유할 권리이며, 자주적인 의사결정권을 의미하는 것으로 이해할 수 있다.[64]

프라이버시의 의의에 대하여 다음과 같은 다양한 입장을 검토할 수 있는데, 첫째, L. Brandeis는 개인의 '혼자 있을 권리'(right to be left alone)로 이해하여 민주주의에서 가장 중요한 자유로서 헌법에 반영되어

59) Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (1902).
60) N.Y. Sess. Laws 1903, ch. 132, § 50-51에 규정되어 있다.
61) Griswold v. Connecticut, 381 U.S. 479 (1965).
62) Roe v. Wade, 410 U.S. 113, (1973).
63) Laurence H. Tribe, American Constitutional Law (Second Edition), The Foundation Press Inc., 1988, p.1302.
64) 정영화,「현대헌법학에서 프라이버시 법리의 재검토」, 사이버커뮤니케이션 학보 통권 제7호, 2001, 217면.

야 한다고 주장하였다.[65]
둘째, Alan Westin은 프라이버시는 어떠한 환경에서든지 자신의 신체, 태도와 행위를 타인에게 얼마만큼 노출시킬 수 있는가는 자신이 자유롭게 선택할 수 있는 자유라고 파악하였다.[66] 셋째, Edward Bloustine은 프라이버시란 인간의 인격권으로 인격의 침해, 개인의 자주성, 존엄과 안전성을 보호하는 것이라고 한다.[67]
넷째, Ruth Gavison은 프라이버시의 3가지 요소로서 비밀, 익명성, 고독을 들고, 그것이 자신의 선택에 의해서 또는 타인의 행위에 의해서 상실될 수 있는 상태를 말한다고 한다.[68]
프라이버시에 관한 이러한 다양한 견해들은 결국 그 실체를 명확하고 구체적으로 파악하기는 여전히 어려움이 있다.[69]

3. 디지털 저장장치 수색을 통한 사생활 침해

미연방 수정헌법 제4조는 수사기관이 영장 없이는 컴퓨터 및 디지털 저장장치에 저장된 정보를 탐색 및 액세스를 금지하고 있다. 디지털 범죄에 있어서 가장 기본적으로 문제가 되는 것은 개인이 관리하고 있는 컴퓨터 및 다른 디지털 저장장치 안에 저장된 디지털 정보에 대하여 프라이버시에 대한 합리적인 기대를 적용할 수 있는지 문제가 된다.

예를 들어 개인의 컴퓨터, USB, 플로피디스켓, 디지털 카메라, 노트북, PDA 등에 저장되어 있는 정보 및 자료에 대하여 개인의 관리가 가능

65) Samuel D. Warren and Louis D. Brandeis,「The Right to Privacy」, Harvard Law Review, Vol. 4, 1890, pp.193-220.
66) Alan F. Westin, "*Privacy and Freedom*", Atheneum(N.Y), 1967, p.7.
67) Edward Bloustine, "Privacy as an Aspect of Human Dignity", 39 *New York Univ. Law Review*, 1964, p.971.
68) Ruth Gavison, "Privacy and the Limits of Law", *Yale Law Journal* 421, 1980, p.428.
69) Jerry Kang, "Information Privacy in Cyberspace Transaction"s, Stanford Law Review Vol. 50, 1998, p.1204.

하고 프라이버시에 대한 합리적 기대가 있다면 수사기관은 그러한 디지털 저장 장치 안에 있는 정보나 자료에 접근하기 위해서는 반드시 수색 영장을 발부 받아야 한다.[70]

연방 대법원은 디지털 저장장치 안에 저장된 정보를 액세스 할 때는 잠금 장치가 된 저장장치와 유사하게 보는데, 그 이유는 잠금장치가 되어있는 디지털 자료에는 개인의 프라이버시가 있기 때문이다.[71] 따라서 디지털 저장장치 안에 있는 정보나 자료에 대하여는 그 소유자에게 프라이버시가 있다고 할 수 있다.[72]

미연방 제10순회 재판소는 영장 없는 또는 영장요구의 예외사항 없이 컴퓨터 하드디스크의 수색은 허용하지 않는다고 판결하였는데, Carey 사건에서 경찰관이 마약을 판매한 증거를 찾기 위해 용의자의 컴퓨터를 수색하던 중 그 컴퓨터에서 아동 포르노를 발견하였다. 경찰관은 마약판매 관련 증거 수색을 중단하고, 그 대신에 5시간 동안 그 컴퓨터 안에 있는 아동포르노에 관한 증거를 수색한 것은 수색의 범위를 초과한 것이라 하여 프라이버시를 침해하였다고 판결하였다.[73]

현재의 대부분의 사람들은 컴퓨터가 많은 디지털 정보를 저장하고 있고, 수사에 필요한 증거자료나 정보들이 같이 혼합되어 있다 보니 경찰 수사기관이 디지털 증거를 수색할 때 개인의 사생활 침해가 필연적으로 발생하고 있다고 보았다.[74]

---

70) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations”, 2002. 7, p.2.

71) United States v. Ross, 456 U.S. 798, 822-23 (1982).

72) United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998). 이 사건은 개인용 컴퓨터의 하드드라이브에 저장된 파일은 프라이버시에 대한 합리적인 기대가 있다고 판결하였다; United States v. Reyes, 922 F. Supp. 818, 832-33 (S.D.N.Y. 1996). 이 사건은 개인용 호출기(pager)안에 저장된 데이터(data)에도 프라이버시에 대한 합리적인 기대가 있다고 판결하였다; 같은 판례로는 United States v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995); United States v. Blas, 1990 WL 265179, at *21 (E.D. Wis. Dec. 4, 1990).

73) United States v. Carey, 172 F.3d 1268, 1273-75 (10th Cir. 1999).

보통 개인이 컴퓨터를 사용할 때 프라이버시를 갖고 있지만, 특수한 상황에서는 프라이버시에 대한 기대를 갖지 못하는 경우도 있는데 예를 들면 우리나라의 PC방이나 공공기관의 휴게실, 병원, 공공 도서관 등에 설치되어 누구나 사용할 수 있는 컴퓨터처럼 공개적으로 사용하는 컴퓨터들은 프라이버시에 대한 합리적인 기대를 갖을 수 없다.

또한 경찰관이 피의자의 어깨 너머로 피의자가 입력하는 비밀번호를 스크린을 통하여 목격한 경우[75]에는 프라이버시를 침해하지 않았다고 판결하였다.[76] 또한 개인이 자기의 집이나 사무실을 의도적으로 공개한 경우,[77] 절취한 컴퓨터내의 디지털 자료나 정보에 대하여는 사생활의 보호를 받지 못한다고 하고 있다.[78]

4. 제3자 소유의 디지털 정보유출에 의한 사생활 침해

개인의 관리 하에 있는 디지털 자료나 정보에 대한 소유를 제3자에게 양도하였을 경우, 미연방 수정헌법 제4조는 저장된 디지털 정보에 대한 프라이버시를 보호하지 않는다.

예를 들어 개인의 고장 난 컴퓨터를 제3자가 운영하는 A/S센터에 가지고 가거나, E-mail이나 인터넷 메신저를 이용하여 디지털 자료를 제3자에게 보내는 경우처럼 디지털 정보를 제공하여 소유권이 제3자에게 넘어간 경우에는 미연방 수정헌법 제4조에 의하여 사생활을 보호 받지 못한다. 경찰은 제3자가 디지털 범죄에 대한 디지털 증거를 소유하고 있다는 것을 알았을 때 그 정보를 조사할 수 있다. 이처럼 제3자에 의한 소유는

74) United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).
75) United States v. David, 756 F. Supp. 1385 (D. Nev. 1991).
76) Id, 1389.
77) also Katz v. United States, 389 U.S. 347, 351 (1967).
78) United States v. Lyons, 992 F.2d 1029, 1031-32 (10th Cir. 1993).

사생활 보호를 받을 수 없으며, 수정헌법 제4조는 이 경우에는 영장의 발부를 요구하고 있다.[79]

제3자의 소유문제에 관하여 살펴보면, 지정된 수령자에게 전달되는 과정에서 운반자의 소유와 그 후의 지정된 수령자의 소유를 구분하는 것이 좋다.

예를 들면, A는 물건을 운반하기 위하여 B를 고용하였다. B가 C에게 물건을 운반하는 동안에 그 물건의 내용물에 대하여 A의 프라이버시는 C가 그 물건을 받은 후에는 다를 수 있다. 물건의 내용물에 대하여 운송중에는 일반적으로 미연방 수정헌법 제4조의 보호를 받지 못한다. 경찰은 운송중인 물건의 내용물에 대하여는 영장 없이 수색하지 못한다.

경찰이 물건의 내용물에 대하여 불법적으로 점유하거나 검사를 하는 것은 발송자와 수령자 양 당사자의 프라이버시를 침해하는 것이다.[80]

그러나 Walker 사건에서는 범죄계획에 의하여 가명으로 보내는 소포물은 프라이버시 보호를 받지 못한다고 판결하였다.[81] 이는 운송인이 수사기관인지 개인회사인지 관계없이 적용이 된다.[82]

디지털 범죄에 있어서도 개인이 본인의 디지털 저장장치를 관리할 수 있는 권한을 잃을 경우에는 프라이버시에 대한 보호도 받을 수 없다.

일단 지정된 수령인이 물건을 받는 후에는 발송인의 프라이버시에 대한 합리적인 기대는 발송인의 물건과 그 내용물에 대한 통제의 유무에 따라 차이가 있다.

---

79) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, op. cit, p.4.
80) United States v. Villarreal, 936 F.2d 770, 774 (5th Cir. 1992).
81) United States v. Walker, 20 F. Supp. 2d 971, 973-74 (S. D. W. Va. 1998).
82) Parte Jackson, 96 U.S. (6 Otto) 727, 733 (1877) 이 사건은 국가기관에 의한 운반 판결이고, Walter v. United States, 447 U.S. 649, 651 (1980) 사건은 개인에 의해 운반된 판결이다.

예를 들면 공공장소에서 물건을 잠시 제3자에게 보관을 시켰을 때에는 그 물건에 대하여 계속 유지할 수 있는 권한이 있기 때문에 물건에 대한 프라이버시를 갖는다 할 것이다.

이에 대한 대표적인 사례로 Walter 사건이 있는데, 외설영화 우편물이 잘못 우송되어 제3자에게 배달되었다. 우편물을 받은 제3자가 이것을 개봉해보니 외설영화 필름이므로 이것을 미연방수사국(FBI)에 전달하였다. 미연방수사국(FBI)은 수색 영장을 발부 받을 의사도 없이 이 외설영화 필름을 영사해보고 외설물이 주간(州間) 우송이라는 이유로 하여 기소하였다. 이 사건에 대하여 하급법원에서는 유죄판결을 받았지만, 연방대법원은 이 사건을 미연방수사국(FBI)에 의한 프라이버시 침해라고 하여 파기·환송한 사건이다.

5. 디지털 증거 수집에 의한 사생활 침해

미연방 수정헌법 제4조는 개인이 디지털 정보 및 자료를 관리할 수 있을 경우에는 사생활의 보호를 받는다고 하고 있다. 그러나 e-mail처럼 일단 메일이 수신자에게 도착하면 그 자료에 대한 관리가 불가능하기 때문에 프라이버시에 대한 보호를 받을 수가 없다.

예를 들어 개인이 자기의 가방을 제3자에게 맡겨두고 잠시 자리를 이탈하였더라도 가방에 대한 소유권은 계속하여 갖고 있기 때문에 프라이버시는 있다고 본다.

Most 사건에서 식품 매장 매니저에게 플라스틱 가방과 그 안의 물건을 맡기고 떠났더라도 프라이버시에 대한 합리적인 기대는 있다고 판결하였다.[83] 그리고 Presler 사건에서 여행객의 잠금장치로 잠겨진 여행용 가

83) United States v. Most, 876 F.2d 191, 197-98 (D.C. Cir. 1989).

방이 공항의 수화물 카운터에 있는 경우에도 이에 대한 프라이버시는 있다고 판결하였다.[84] Barth 사건에서는 고장 난 컴퓨터를 수리하기 위하여 컴퓨터 수리 전문가에게 컴퓨터 하드 드라이브의 수리를 맡긴 경우에도 이 컴퓨터 하드 드라이브에 대한 프라이버시의 합리적 기대는 있다고 판시하고 있다.[85]

제3자의 소유에 관한 논쟁을 분석하면, 이에 대한 판단은 그 물건 및 내용물에 대하여 발신인이 계속하여 관리능력을 가지고 있는지 여부에 달려 있다. 즉, 발신인이 물건을 제3자에게 임시적으로 보관만 시킨 것이라면 발신인의 프라이버시에 대한 합리적인 기대는 그대로 유지된다.

예컨대, 피의자가 자기 회사의 영업비밀인 상품 가격정보를 경쟁회사에게 이메일로 보낸 것을 미연방수사국(FBI)이 상대 경쟁회사의 컴퓨터를 수색하여 상품 가격정보 자료를 찾았다. 이에 대하여 피의자는 사생활이 침해되었다고 주장하였으나, 법원은 피의자가 상대 경쟁회사에게 상품의 가격정보 자료를 보낸 것은 그 소유와 통제를 포기하였다고 판결하였다.[86]

또 다른 비슷한 사례로 인터넷을 통한 채팅과 관련된 사건에서 피의자가 아메리카 온라인(America Online) 채팅방을 통해 이메일 메시지를 보내고 그 메일을 채팅방에 있는 참석자들이 수령을 한 이후에는 메시지 내용에 대한 프라이버시의 합리적인 기대가 없다고 판결하였다.[87]

결과적으로 발신인에 의하여 발송된 물건을 제3자가 소유하고 있다면 발신인의 관리능력이 없다고 판단되며 물건에 대한 발신인의 프라이버시에 대한 합리적인 기대는 더 이상 인정될 수 없다.

---

84) United States v. Presler, 610 F.2d 1206, 1213-14 (4th Cir. 1979).
85) United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998).
86) United States v. Horowitz, 806 F.2d 1222 (4th Cir. 1986).
87) United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997).

예를 들어 Kevin Poulsen 사건[88]에서 컴퓨터 해커인 케빈 폴센(Kevin Poulsen)이 렌트 비용은 지불하지 않고 시정 잠금장치가 되어있는 상업용 디지털 저장설비에 디지털 자료들을 저장하였다. 경찰은 이 디지털 저장설비에 대하여 영장 없이 수색을 하여 케빈 폴센의 디지털 자료들을 찾았다. 이에 대하여 미연방 제9 순회재판소(The Ninth Circuit)는 경찰이 케빈 폴센(Kevin Poulsen)의 프라이버시를 침해하지 않았다고 판결하였는데, 그 판결 이유는 렌트 비용을 지불하지 않았기 때문에 케빈 폴센(Kevin Poulsen)이 디지털 저장 설비에 액세스할 수 있는 권리는 소멸했다는 것이다.[89]

미연방 대법원과 지방법원들의 의견은 개인이 디지털 정보를 제3자에게 전송하였을 때는 그 디지털 정보에 대하여는 프라이버시권을 기대할 수 없다는 것이 일반적인 견해이다.

만약 개인이 제3자에게 보낸 정보들이 본인의 주관적인 생각으로는 제3자가 그 정보의 비밀을 지켜줄 것이라고 생각하더라도 정보는 제3자에게 소유를 이전했다고 보아 프라이버시에 대한 보호를 받을 수 없다는 것이다.

이에 대한 대표적인 사례로 Miller 사건이 있는데 이는 다음과 같다. 경찰에 의해 압수된 은행발행의 수표, 저금통장 등은 피고인의 개인사물로 볼 수 없기 때문에 프라이버시는 존재하지 않는다. 이는 제3자인 은행 업무상 은행직원에 의하여 공개가 가능하기 때문이다.

따라서 은행은 고객이 소지하고 있는 은행 계좌의 누설에 관하여 계좌정보를 보호하지 않는다고 법원은 판결하였으며, 이는 미연방 수정헌법 제4조에 위반되지 않는다고 판결하였다.[90]

---

88) United States v. Poulsen, 41 F. 3d. 1330 (9th. Cir 1994).
89) id. 1337.
90) United States v. Miller, 425 U.S. 435, 443 (1976).

개인이 디지털 자료나 정보를 인터넷 네트워크를 이용하여 전송을 하고 이것이 수신자에게 도착한 이후부터는 프라이버시에 대한 보호를 받지 못한다.

Meriwether 사건에서[91] 호출기를 이용하여 디지털 메시지를 보낸 경우, 또한 e-mail 메시지를 이용하여 상대방에게 메시지가 완벽하게 전송된 경우에는 프라이버시에 대한 보호를 받지 못한다.

6. 인터넷에 공개된 자료에 의한 사생활 침해

일반 네티즌에게 공개된 인터넷 자료도 관련 포털업체나 서버운영자와 그 가입자간의 동의나 승인이 없으면 당연히 법관의 영장이 있어야 취득이 가능하다고 해야 할 것이다.

특히, 인터넷 게시판의 경우 송신자와 수신자간에 흐르고 있는 정보는 그 성질상 압수·수색 범위를 특정하기 어려우므로 이를 압수하기 위해서는 보통 일반 범죄보다 그 요건을 완화하여 압수할 수 있다고 보아 디지털 범죄와 관련성만 인정되면 압수할 수 있다는 견해가 있다.[92]

물론 인터넷 게시판과 같이 다수의 이용자에게 광범위하게 정보를 제공하고자 할 목적을 갖고 있는 것에 관해서는 컴퓨터 시스템의 이용자에 대해 헌법이 보장하는 사생활의 보호정도가 축소된다고 보아도 좋을 것이다. 그러나 인터넷 게시판이 다수에게 개방되어 있다고 하여도 비밀번호나 ID에 의해서 그 이용이 제한되어 있는 경우에는 이용이 허용된 자 이외의 누구에게나 자유롭게 액세스 할 수는 없다.

---

91) United States v. Meriwether, 917 F.2d 955, 959 (6th Cir. 1990).

92) 安富 潔,「刑事手續とコンピュータ 犯罪」, 慶應義塾大學 法學研究會叢書(52)(平成 4年, 1992. 2. 20), 217면.

따라서 인터넷 게시판 이용자는 프라이버시에 대한 합리적 기대를 갖고 있다고 보아야 하며, 이에 따라 인터넷 게시판의 통신비밀도 보호되어야 한다.

그러므로 경찰은 법관이 발부한 영장에 의하지 않고는 인터넷 게시판 또는 자료실을 무단으로 수색할 수 없다. 즉 경찰이 컴퓨터 시스템 이용자의 동의를 얻어 비밀번호나 ID를 확보한 경우 이외에 인터넷 게시판에 게시된 정보를 무단 취득하는 것은 위법한 도청이나 위법한 컴퓨터 수색이라고 해야 한다. 또한 경찰이 디지털 기록에 대해 정당하게 접근할 수 있는 권한이 없이 위법하게 취득한 ID나 비밀번호를 이용하여 수색행위를 하는 것은 위법한 수색행위에 해당한다고 보아야 한다.[93]

다만 인터넷 게시판에 접근 할 수 있는 권한을 갖고 있는 공동 이용자는 경찰의 수색에 동의할 수 있다고 하겠다. 그러나 그 접근 권한은 무한정한 것이 아니며, 당해 게시판의 특정파일에 메시지를 남길 수 있을 뿐 그곳으로부터 정보를 읽어내는 것이 허용되어 있지 않다면 그 파일에 접근 할 수 없다고 해야 한다.

따라서 공동 이용자의 접근 권한에 일정한 제한이 있는 경우 경찰의 수색범위는 제한될 수 밖에 없는 것이다. 특정기록에만 접근 할 수 있는 이용자는 그 외의 전자기록에 대한 수색에 동의할 수 있는 권한이 없다고 해야 할 것이다.[94]

이때에도 경찰은 범죄수사를 위해 법관이 발부한 영장에 근거하여서만 수색할 수 있으며, 이를 위반하여 수색할 경우에는 당연히 헌법상 보장된 타인의 사생활이 침해된다 할 것이다.

93) 吳奇斗,「刑事節次上 컴퓨터관련 證據의 蒐集 및 利用에 관한 硏究」, 서울大學校 博士學位論文, 1997, 196-197면.
94) 安富 潔, 前揭書, 211면.

7. 경찰이 보유한 디지털 증거 수색에 의한 사생활 침해

경찰은 보통 범죄자에게서 압수한 물건을 보관한다. 이때 그 압수물을 수색하는 경우가 있는데, 이는 합리적이며 영장없이 가능하다.

이처럼 영장없이 가능한 경우에는 다음 두 가지 조건이 있는데 첫 번째는 경찰은 피의자를 구금하고 있는 동안 피의자가 소지하고 있던 물건을 보관하는데, 이때 그 보관물의 위험으로부터 경찰관을 보호할 수 있는 물건, 훔친 물건, 파괴될 수 있는 물건은 영장없이 수색이 가능하다. 이러한 물건들에 대한 합법적인 수색은 개인의 사생활의 권리를 침해하지 않는다고 하였다.[95] 두 번째로 수색은 적법한 절차를 따라야 한다.[96]

디지털 범죄에서 컴퓨터와 관련하여 경찰관서에 보관되거나 압수되어 있는 컴퓨터, 디스켓, 핸드폰, 디지털 카메라 등 디지털 증거에 관해서는 영장없는 수색이 허용되지 않는다.[97]

이는 오프라인에 관한 범죄 증거에 대하여는 경찰관서에서 보관하는데 큰 문제가 없지만, 컴퓨터에 저장 되어 있는 디지털 정보나 증거 자료는 디지털 증거의 특성상 경찰관서에서 보관하게 되는 경우에 증거의 삭제나 변경이 가능할 수 있기 때문이다.

따라서 경찰관서에 보관되어 있는 디지털 증거들에 대하여 수색을 할 경우에 있어서는 반드시 수색영장을 발부 받아야 할 것이다.[98] 이를 위

95) Illinois v. Lafayette, 462 U.S. 640, 644 (1983); South Dakota v. Opperman, 428 U.S. 364, 369-70 (1976).
96) Colorado v. Bertine, 479 U.S. 367, 374 n.6 (1987); Florida v. Wells, 495 U.S. 1, 4-5 (1990).
97) United States v. O' Razvi, 1998 WL 405048, at *6-7 (S.D.N.Y. July 17, 1998); United States v. Flores, 122 F. Supp. 2d 491, 493-95 (S.D.N.Y. 2000).
98) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, op. cit, p.23.

반하여 수색 영장없이 디지털 증거를 경찰이 수사하는 경우에도 헌법상 사생활 침해의 문제가 제기될 수 있을 것이다.

또한 디지털 범죄의 정보를 얻기 위하여 경찰관이 보유한 최첨단 기술(Use of Technology to Obtain Information)을 사용할 경우에 사생활이 침해되는지 여부와 관련하여 문제가 제기될 수 있다.

이에 관하여 미연방 대법원은 Kyllo 사건[99]에서 피고인이 집안에서 마리화나를 재배한다는 혐의가 있어 경찰이 보유한 열영상 카메라(Thermal Imager)[100]로 집에서 방출되는 열의 양을 측정하였다. 그 결과 집안에서 마리화나를 재배하는 것을 밝혔고, 이를 근거로 기소하였다. 그러나 경찰이 수색영장 없이 개인 주택에 대하여 열영상 카메라를 사용한 것은 불법적인 수색으로 사생활을 침해한 것이라고 판결하였다.

특히, 연방 대법원은 수사기관이 일반적으로 사용하는 않는 장비를 사용하여 수색하는 것과 물리적인 침입없이 이전부터 알려지지 않았던 방법으로 집안을 세심하게 수색하는 것은 영장이 필요하다고 판시하였다.[101] 경찰이 컴퓨터와 네트워크를 통하여 전송되는 디지털 정보나 자료를 얻기 위하여 일반적으로 사용되지 않는 최첨단 기술 장비를 사용하는 경우에는 당연히 수색 영장이 요구된다.[102]

따라서 영장없이 수사기관이 보유한 최첨단 기술로 디지털 증거를 수색 하는 것은 당연히 헌법상 보장된 개인의 사생활이 침해된다 할 것이다.

---

99) Kyllo v. United States, 533 U.S. 27 (2001).
100) 열영상 카메라(Thermal Imager)라 함은 마리화나를 자라게 하는 고온의 조명을 사용하는지를 측정하기 위하여 집안으로부터 새어 나오는 열을 측정하는 기구를 말한다.
101) Id. 40.
102) Id. 34 & 39 n.6 參照.

Ⅳ. 한국에서 디지털 범죄와 사생활의 보호

1. 사생활 보호에 관한 헌법 규정

우리나라의 사생활 보호에 관한 권리는 인간의 존엄과 가치·행복추구권의 한 내용으로서 주장하게 되었으며,[103] 현행 헌법은 제17조에「모든 국민은 사생활의 비밀과 자유를 침해 받지 아니한다」는 규정을 두어 이를 명문화하고 있다.

우리의 헌법 규정에 근거하여 이를 보장하고 있는 공공기관의개인정보보호에관한법률(1994년 1월 7일 제정)은 컴퓨터에 의해 처리되는 개인정보의 보호를 위한 법으로서 현저한 기본권의 침해의 우려가 있는 개인정보의 수집 등을 원칙적으로 금지하고 있다. 그러나 그 보호대상을 컴퓨터에 의해 처리되는 개인정보에 한정하고 그 규제대상도 공공기관으로 한정하고 있다는 문제점이 있다.[104]

최근 첨단과학기술 변화에 따른 헌법상 기본권인 사생활의 보호에 관하여 새로운 보호 필요성이 강하게 제기되어 헌법을 개정 하고자 하는 견해가 제기되고 있는데,[105] 정보사회 발전으로 인한 사생활과 개인정보의 적극적인 보호는 당연한 귀결이라고 할 수 있다.

앞으로 우리 사회는 더욱더 첨단 정보화 사회로 진입할 것이며, 이에 따른 사생활의 침해 또한 다양한 방식으로 발생할 것으로 예상된다. 따

---

103) 金哲洙, 前揭書, 518면.
104) 金哲洙, 前揭書, 519면.
105) 金日煥,「憲法上 私生活關聯 自由의 改正方向과 內容에 관한 考察」, 憲法學硏究, 第12券 第4號, 2006. 11, 164면.

라서 헌법상 사생활 보호에 관하여 정보화 시대에 맞추어 기능, 역할, 보호 내용 등을 충분히 검토할 필요성이 있다 할 것이다.

2. 사생활의 보호의 요구

현대는 정보통신기술의 발전으로 디지털 정보화가 빠르게 이루어지고 특히 인터넷상에서 개인의 사생활이 공개 또는 유출, 누설되는 경향이 많아지고 있어 사생활의 보호가 요구되기 시작하였다.[106] 물론 우리나라에서는 헌법에 명시적으로 규정하고 있지만, 정보통신 기술의 발전에 따른 사생활 침해에 대한 보호의 필요성은 날로 증대되고 있다. 이에 따라 이를 법제화할 필요성이 끊임없이 학계에서 제기되어 왔고, 또한 정보화로 인한 폐해는 우리 앞에 있는 현실이기도 하다.[107]

사생활의 비밀과 자유의 개념은 다양하게 이해되고 있다.[108] 사생활의 자유라 함은 개인이 사적인 생활을 영위할 수 있는 자유를 말하는 것이고, 사생활의 비밀이라 함은 사생활의 부당한 공개로부터의 자유라고 할 수 있겠다. 이 권리는 외국에서 말하는 프라이버시의 권리들 뜻하는 것이라고 하겠다. 이러한 프라이버시의 권리는 정보통신이 발달한 오늘날 소극적으로 '사생활의 평온을 침해받지 아니하고 사생활의 비밀을 함부

106) 金哲洙,「憲法學 新論」, 博英社, 2007. 4, 518면; 성낙인,「개인정보보호법제의 현황과 재정립 방향」, 인터넷과 法律Ⅱ, 法文社, 2005, 62면.

107) 성낙인, 전게서, 62면.

108) 이에 대하여 구병삭 교수는 사생활의 비밀은 사생활의 부당한 공개로부터의 자유를 말하고, 사생활의 자유란 개인의 사생활을 영위하는 자유를 말한다고 한다. 丘秉朔,「新憲法原論」, 博英社, 1995, 489-490면. 다른 의견으로 권영성 교수는 사생활의 내용을 공개당하지 아니할 권리, 사생활의 자유로운 형성과 전개를 방해받지 아니할 권리 그리고 자신에 관한 정보를 스스로 관리·통제할 수 있는 권리 등을 내용으로 하는 복합적인 권리라고 한다. 權寧星,「憲法學原論」, 法文社, 2007, 445면. 또 다른 의견으로는 프라이버시 권리는 개인 또는 단체가 그 의견에 반하여 자기의 성명·초상·행동·사상·문서 기타 징표를 탐지·공개 또는 이용당하지 아니할 권리 및 자기 또는 자기의 지배하에 있는 자의 정보가 타인에 의하여 취득·개시될 정도를 결정할 수 있는 권리라고 한다. 변재옥,「정보화 사회에 있어서 프라이버시 權利」, 서울대학교 박사학위논문, 1979, 257면.

로 공개당하지 아니 할 권리’에서 그치는 것이 아니고, 적극적으로 ‘자기에게 관련된 정보의 전파를 컨트롤 할 수 있는 권리’로 파악하려는 경향이 있다. 이는 오늘날의 정보화 사회에서 개인의 존엄을 보장하기 위하여 필수적인 것으로 인정되어야 할 것이다.[109]

헌법재판소는 ‘사생활의 자유’란 시민공동체의 일반적인 생활규범의 범위 내에서 사생활을 자유롭게 형성해 나가고 그 설계 및 내용에 대해서 외부로부터의 간섭을 받지 아니할 권리이며, 사생활에 관련된 사사로운 자신만의 영역이 본인의 의사에 반해서 타인에게 알려지지 않도록 할 수 있는 권리인 ‘사생활의 비밀’과 함께 헌법상 보장되고 있는 것이라고 한다.[110]

사생활의 비밀과 자유는 넓은 의미로는 인격적 이익의 총체를 포괄하게 된다. 이렇게 사생활의 비밀과 자유를 넓은 의미로 이해하는 미국의 판례에 비추어 본다면 그것은 대체로 프라이버시권(Privacy Right)으로 이해될 수 있다.

3. 디지털 범죄에서 사생활 침해 가능성의 증대

최근 들어 디지털 범죄에서 경찰을 비롯한 수사기관의 수사에 의한 개인의 민감한 정보, 통신이나 이메일을 감청 또는 유출하는 일이 늘어나고 있다. 이는 범죄와 무관하게 헌법상 보호하고 있는 개인의 사생활이 침해되고 있다고 말할 수 있다.

이에 대한 대표적인 최근 사례가 2007년 9월 신정아의 가짜 학위를 이

109) 金哲洙, 前揭書, 519면

110) 憲裁 2001. 8. 30. 선고, 99 헌바 92 당, 憲裁判例集 제13권 2집, 174면 이하(203면); 憲裁, 2003. 10. 30. 선고, 2002 헌마 518, 憲裁判例集 제15권 2집(하), 185면 이하; 헌재공보 제86호, 100면 이하(109면).

용한 교수직 획득과 광주비엔날레 총감독 등 형법상 업무방해죄와 관련된 사건이다. 그러나 한 언론사에 의해 이 여성의 누드 사진이 본인의 동의 없이 유출되어 본인에게는 심각한 사생활이 침해가 되었고,[111] 결국 당사자는 관련 언론사를 상대로 손해배상 및 정정보도 청구소송을 제기하였다.

이는 최근들어 이슈가 된 언론사에 의한 개인의 사생활 침해의 대표적인 사례라 할 수 있다. 우리나라에서 아직까지는 경찰을 비롯한 수사기관에 의하여 범죄와 관련이 없는 개인의 사생활이 유출, 공개되어 문제가 제기된 사례는 거의 없지만, 매년 기하급수적으로 증가하는 디지털 범죄에서 사생활 침해의 개연성이 범죄와 같이 증가할 가능성은 충분히 있다고 보여진다.

따라서 경찰을 비롯한 수사기관은 이에 대한 사생활 보호의 필요성을 인식하고 수사에 임해야 할 것이며, 무엇보다도 중요한 것은 디지털 범죄에서 사생활 침해 문제에 대하여 이를 보호할 수 있는 입법적인 방안이 제정되어야 한다고 생각한다.

111) 서울여성회,「여성,뉴스 클리핑」, 2007. 9. 13.

Ⅴ. 디지털 범죄에서 사생활 보호를 위한 법제 정비

1. 헌법상 사생활 보호를 위한 입법 원칙

우리 헌법 제12조는 신체의 자유에서 제1항은 ‘누구든지 법률에 의하지 아니하고는 체포··구속·압수·수색을 받지 아니하며’, 제3항에서 ‘체포·구속·압수·수색 을 할 때에는 적법한 절차에 따라서 영장을 제시해야 한다’고 규정하고 있다.

이는 헌법상 경찰을 비롯한 수사기관의 범죄수사와 이에 부수되는 증거 수집에 관하여 국민의 기본권이 침해받지 않고 이를 보호하고자 최고 규범인 헌법에 규정하였다. 이러한 헌법의 규정에 근거하여 범죄에 관련된 현행 법률들은 헌법규정에 따라야 하며, 법률에 근거한 절차에 의하지 않고 수집된 증거들은 당연히 위법하게 수집된 증거로 배척되어야 할 것이다. 그러나 이러한 헌법 규정에 근거한 형사소송법을 비롯한 하위 법률들은 기존 전통적인 일반 범죄를 기준으로 하여 규정되어 있다 보니 과연 디지털 범죄에는 어느 정도 적용을 할 수 있을지 의문이 제기된다.

현재는 정보통신의 발달로 인하여 디지털 기기들이 우리 사회를 장악하고 있는 디지털 시대이며 이를 기반으로 하여 발생하는 새로운 디지털 범죄에 대응하기 위하여는 정보화 시대에 맞는 기존 법률의 개정 또는 새로운 법률의 제정이 필요하다.

특히 헌법상 국민의 기본권을 최대한 보호하기 위하여는 디지털 범죄의 특성에 맞게 형사소송법의 조문을 개정하여 기본권인 개인의 사생활

을 보호할 수 있고 더불어 새로운 디지털 범죄와 증거 수집에 대응하는 방법이 현재로서는 가장 무난하다 생각이 된다. 물론 디지털 범죄의 특성을 고려하여 특별법의 형식으로 새로운 입법을 제정하는 것도 배제하지는 않는다.

경찰이 디지털 범죄 수사를 통한 증거를 수집함에 있어 관련 법률 절차를 개정 또는 새로운 법률을 제정하지 않는다면 현행 법률로서는 다양한 방식으로 국민의 기본권인 사생활이 침해될 것이며, 또한 미비된 법률로 인해 범죄자도 처벌하기가 곤란할 것이다. 그러면 결과적으로 국가는 범죄로부터 개인 및 사회의 안녕과 질서를 보호하지 못하며, 헌법상 보장되어 있는 국민의 기본권도 보호하지 못하는 결과가 초래하게 된다.

따라서 이러한 법적인 수단이 미치지 않는 영역이 생기지 않도록 해야 할 것이며, 또한 국민 개개인의 기본권인 사생활 침해가 최소한도로 그칠 수 있도록 절차적인 요건을 명백히 하는 법률적 통제장치를 두는 것이 기본권 보호를 위해 합리적이라고 본다.[112]

2. 디지털 범죄 범위 규정을 통한 사생활 보호

현재 컴퓨터와 관련된 디지털 정보들은 디지털 저장매체에서 생성되는 정보 외에도 네트워크로 연결된 다양한 전산시스템들에 의해 많은 정보를 생산하고 또한 저장하고 있다. 이러한 많은 디지털 정보의 현실에서 수사기관에 의한 디지털 증거의 수집은 생각지도 않게 범죄와 전혀 관련 없는 물건, 데이터, 타인의 개인정보와 장소에 대한 수색으로 타인의 사생활을 침해하는 문제를 야기하게 된다.

특히, 현행 형사소송법은 수사기관에 의한 압수·수색이라는 강제처분

112) 梁根源, 前揭論文, 130면.

을 하기 위하여는 증거물 또는 피고인과의 관련성을 기본 요건으로 하고 있기 때문에 범죄 대상이 된 물건과 장소가 범죄와 관련되어 있다는 사실이 소명되어야 한다.[113] 따라서 피의자 또는 범죄와 관련 없는 물건, 데이터, 타인의 개인정보, 장소 등에 대한 압수·수색은 허용되지 않는다고 보는 것이 원칙이다.[114]

물리적 증거 및 장소와 관련해서는 범죄와의 관련성 여부는 어느 정도의 소명만으로도 판단이 가능하다. 소수의 개인들이 사용하는 컴퓨터를 비롯한 디지털 관련 장비를 압수·수색하는 경우에는 일반적인 범죄 관련성의 판단으로 충분하다.[115] 이런 경우에도 범죄행위와 관련성 있는 자료만 내장되어 있는 매체만을 압수할 수 있으며 컴퓨터 전체를 압수함으로써 범죄와 관련성 없는 자료까지 압수하는 것은 허용될 수 없다는 주장[116]도 있으나, 비록 범죄와 관련성이 약한 디지털 자료가 저장되어 있다 하더라도 논리적 구분이 용이하지 않은 점을 고려, 포괄적인 관련성을 인정하여 압수·수색을 허용해야 한다는 주장도 있다.[117] 이에 관하여 일본,[118] 미국[119]에서는 포괄적으로 인정한 사례들이 있다.

---

113) 裵鍾大·李相暾, 前揭書, 295면.

114) 원혜욱,「컴퓨터 관련 증거의 증거조사와 증거능력」, 수사연구 2000년 6월호, 수사연구사, 2000. 6, 122면.

115) 梁根源, 前揭論文, 148면.

116) Voss v. Bergsgaard, 774 F. 2d 402 (10th Cir. 1985) 사건에서 판례가 광범위하게 사기죄가 범하여졌다고 생각되는 상당한 이유가 인정되는 경우에도 당해 범죄와의 관련성 유무를 묻지 않고 수색장소에 있는 기록 전부를 압수한 것은 허용되지 않는다고 하고 있다. 吳寄斗, 前揭論文, 99면.

117) 이은모, 전게서, 163면.

118) 일본의 판례는 수색현장에 존재하는 디지털 매체 안에 범죄사실과 관련 있는 정보가 기록되어 있을 개연성이 인정되나 현장에서 피의사실과 관련성이 없는 데이터를 선별하는 것이 용이하지 않은 경우에는 관련성이 있다고 보아 포괄적으로 압수가 허용되는 경우도 있다. 大阪高判 平成 3年 11. 6. 判例 ハイテク 796号, 264面.

119) United States v. Sassani 1998 WL 89875 at *5(4th Cir. 1998). 사건에서 법원은 "컴퓨터의 하드디스크나 전자파일 등 전자적 매체기록을 사용한 범죄를 수사함에 있어서 압수·수색 영장을 발부하는 법원으로서는 어느 파일이 관련성 있는 파일인지 알 수 없으며 따라서 영장에 어느 파일 등을 압수할 것인지를 특정하여 기재할 수 없다"며 피고인의 컴퓨터와 382장의 플로피디스크에 대한 압수를 허용하였다.

그러나 지금처럼 다수의 사람들이 이용하는 인터넷 포털 업체의 대형 서버시스템이나 네트워크 시스템 저장매체의 경우에는 수많은 디지털 정보들이 혼재되어 있는 경우가 많다. 이러한 경우는 수사 대상자 뿐만 아니라 범죄와 전혀 관련 없는 다수인 제3자의 디지털 정보들도 포함되어서 ISP의 대형 서버시스템에 저장되어 있다. 그러한 대형 저장매체에 혼재되어 있는 것 중 어느 것이 증거물인지 매체에 저장되어 있는 정보를 구체적으로 확인하지 않고서는 알 수가 없다.

따라서 이에 대한 압수·수색은 범죄와 전혀 관련 없는 제3자의 개인적인 사생활을 침해할 수 있는 가능성이 충분히 있다. 하지만 개인의 사생활의 침해 가능성 때문에 디지털 증거의 압수·수색을 허용하지 않으면, 경찰을 비롯한 수사기관은 범죄의 증거를 획득할 수 없게 되는 결과를 초래한다. 따라서 범죄와 관련이 없는 제3자의 사생활을 보호하기 위해 압수·수색의 범위를 엄격하게 하는 것은 당연하다.

그러나 현실적으로 ISP의 대형 저장매체의 압수·수색 범위를 규정하는 것이 물리적·논리적으로 불가능한 경우가 많다. 이를 고려하여 대형 저장매체 및 네트워크 시스템에 대한 압수·수색은 기존의 물리적 증거, 물리적 공간에 대한 압수·수색과는 다른 형태로 디지털 범죄와의 관련성이 요구되어야 할 것이다.[120]

결국 경찰에 의한 디지털 증거의 압수·수색에 있어서 범죄와의 관련성은 범죄와 관련 없는 디지털 데이터 내지 제3자의 사생활 보호라는 측면과 형사소추 유지의 이익이라는 측면을 적절히 고려해서 관련성 범위를 명확하게 판단해야 할 것이다.[121] 경찰에 의한 합법적인 수집수단이 확보되어 절차적으로 문제가 없다 하더라도 그 수단으로 어느 정도의 범위까지 증거수집이 가능한 것인가 하는 문제가 항상 제기될 수 밖에 없

120) 안경옥,「정보화 사회의 새로운 수사기법과 개인의 정보보호」, 비교형사법연구, Vol. 5 No. 1, 한국비교형사법학회, 2003, 328면.
121) 탁희성, 전게서, 111면.

으며 따라서 헌법상 기본권인 사생활의 자유가 침해될 우려가 항상 존재한다. 따라서 디지털 증거수집에 있어 범죄와의 관련성 범위를 명확히 규정하는 것이 헌법상 사생활의 침해를 최소화하고 최대한 보호하는 바람직한 방향이라 생각된다.[122]

3. 디지털 범죄에서 사생활 보호를 위한 입법제정의 필요성

현재 경찰은 매년 디지털 범죄와 관련된 국제 세미나를 개최하여 선진국과의 수사기법 교류, 디지털 범죄 사례 발표를 통한 범죄 경향 분석 등 디지털 범죄를 예방 및 대처하고자 노력하고 있다. 올해 2010년 9월 13일 - 15일에도 '2010 국제 사이버범죄 대응 심포지엄(International Sympsium on Cybercrime Response 2010)'을 개최하였다.[123]

이처럼 우리의 경찰은 디지털 범죄에 대응하기 위하여 적극적인 노력을 하고 있다. 그러나 아직까지 입법, 사법기관의 수용 자세는 그에 따르지 못하고 있는 것이 현실이며, 이는 결과적으로 헌법상 보장된 국민의 기본권 침해로 계속 이어지고 있다.

따라서 디지털 범죄를 법적인 측면에서 바라보고 경찰이 범죄를 수사함에 있어 미비한 법률적 근거를 마련하여 헌법상 보장된 기본권이 침해

122) United States v. Carey 172 F.3d 1268, 1273(10th Cir. 1999) 사건에서 법원은 수사기관이 수색영장에 기록된 범위 외의 파일을 열어 증거로 제시한 경우 개인의 사생활에 대한 권리를 침해하여 위법하다고 판시하였다.

123) 2010 국제 사이버범죄 대응 심포지엄은 인터폴, 미국 국토안보부(HSI)·FBI 사이버부 조직범죄과, 뉴질랜드 경찰청, 네덜란드 포렌식 연구소(NFI), 프랑스 정보통신범죄대응센터, 싱가포르 첨단범죄수사과, 대만 경찰청 수사과, 일본 경찰청 하이테크 범죄과, 독일 경찰청 첨단범죄수사과 등 외국 수사기관 9개국과 국내 12개 기관이 참석한 가운데 심포지엄을 개최하였다.

되지 않도록 해야 할 것이다.

현행 형사소송법은 디지털 범죄를 수사함에 있어서 특히, 디지털 증거의 수집함에 있어 많은 부분이 법적으로 근거가 되지 못하는 것이 현실이며, 그 결과 수집된 증거는 법원에서 증거능력을 인정 받지 못하게 된다.

따라서 디지털 범죄에서 증거를 확보하기 위해서는 과학적, 기술적인 개발을 하는 한편 그에 맞추어 형사법 체계를 정비하든지 아니면 따로 형사특별법의 형식의 입법이 필요하다고 생각된다.

여기에서는 새로운 입법안으로 디지털 범죄에서 '디지털 증거 수집 및 분석 절차법안' 을 제시하고자 한다.

우리의 형사소송법이 디지털 증거를 비롯하여 새로운 과학기술과 관련된 증거법상의 문제를 심도있게 다루지 못했던 것은 그 동안의 제정, 개정작업 가운데서 공판시스템 운영을 위한 인적·물적 자원의 부족 문제를 이유로 당사자주의와 공판중심주의가 형해화 되고 증거법 관련 부분은 큰 개정없이 기본 골격을 유지하여 왔기 때문이다.[124] 형사재판을 둘러싸고 있는 환경 자체의 세계화, 국제화 추세는 세계적 표준 법률안을 제정하도록 요구하고 있고 증거법 부분에 있어서도 전근대적 방식을 더 이상 고수할 수 없게 하고 있다. 특히 과학기술의 발달은 새로운 형태의 증거수집 방법과 증거법상 취급방법을 마련하는데 필연적인 요청일 수 밖에 없다.

이러한 법적인 절차로 도입하기 위해서는 미국 법무부 사법 연구원이 제시한 절차방법, 미 공군 기술연구소에서 제안한 방법들을 참고하여 헌법상 국민의 기본권인 사생활의 침해가 최소화 될 수 있도록 해야 할 것이다.

---

124) 신동운,「향후 형사법 개정의 방향」, 서울대학교 법학 제46권 제1호, 서울대학교, 2005, 119면.

다음은 사생활 보호를 위한 입법적인 절차안으로서 '디지털 증거 수집 및 분석 절차법안' 을 제시하고자 한다.

4. 사생활 보호를 위한 입법절차 안(案)

수사기관에 의한 디지털 범죄 수사에 있어 사생활을 보호하고자 개인적으로 디지털 증거 수집 및 분석에 관한 절차법을 제시하고자 한다. 물론 이 입법안(案)이 사생활 보호에 중점을 두고 제안한 것이라기 보다는 사생할 보호와 더불어 헌법상 보장되어 있는 국민의 기본권을 보호하고자 하였다.

본 디지털 증거 수집 및 분석에 관한 절차법에 관한 구성은 다음과 같다. 본 법률은 총칙을 비롯하여 크게 제1장 총칙, 제2장 디지털 증거의 압수·수색, 제3장 디지털 증거의 분석, 제4장 디지털 증거의 분석보고 및 수집·분석 지원요청, 그리고 부칙으로 구성하였다. 이에 대하여 좀 더 구체적으로 각 장의 법률 내용을 살펴보고자 한다.

제1장 총칙부분에서는 이 법률의 최대 목표인 적법절차 준수와 이로 인한 국민의 기본권을 보호하는 제정목적을 언급하고, 동 법률에서 쓰이는 용어의 정의, 특히 디지털 증거, 증거 분석 등을 명확하게 하여 용어에서 오는 혼란을 없애고자 하였다. 그리고 적용범위와 적법절차의 준수를 명시하였다. 또한 수사기관이 신속하고 효과적인 디지털 증거를 수집하기 위하여 디지털 증거의 수집 계획의 내용과 이를 통하여 디지털 증거의 수집 절차를 명확히 규정하였다. 이는 디지털 증거의 진정성과 무결성을 확보하기 위한 것이다.

이 장의 마지막은 압수된 디지털 기기 및 저장매체들의 운반과 보관 규정을 두어 디지털 증거의 특성을 감안하여 증거가 손상이 되지 않도록

각별하게 주의를 주고자 하였다.

제2장에서는 수사기관에 의한 디지털 증거의 압수·수색을 규정하였는데, 이는 형사소송법의 압수·수색 규정에서 디지털 증거 부분만을 특화시켜 구체적으로 규정하고자 하였다.

먼저 디지털 증거의 압수·수색 준비단계로 사건의 개요, 압수·수색의 장소 및 대상, 정보처리시스템의 유형과 규모, 네트워크의 구성, 디지털 기기의 보유현황 등 모든 사항들을 확인하고 철저하게 계획을 수립하는 조항을 삽입하였다. 이러한 준비과정을 거쳐 디지털 증거를 압수·수색할 수 있는 세세한 부분을 규정하였다. 그리고 헌법상 보호된 기본권의 침해를 방지하기 위하여 디지털 증거의 부당한 압수·수색은 당연히 금지하고 반드시 적법절차에 의하도록 규정하였다. 물론 디지털 증거의 특성상 압수·수색시에는 유의해야 할 사항이 있기에 이에 대한 유의사항도 첨부하여 규정하였다.

제3장에서는 수사기관에 의하여 압수·수색된 디지털 증거를 수사관 또는 디지털 증거 분석전문가에 의하여 분석시 지켜야 할 준수사항을 규정하였다. 먼저 디지털 증거의 분석시 지켜야할 기본원칙과 이를 통하여 디지털 증거를 분석하는 방법을 규정하였다. 그리고 수집된 증거의 보존을 위한 준수사항을 규정하였다.

제4장에서는 수사기관에 의해 압수·수색된 디지털 증거를 분석한 후, 이에 대한 분석보고서를 작성하는 방법과 디지털 증거의 수집 및 분석시 분석 전문가의 지원이 필요할 경우, 이를 요청할 수 있는 부분을 규정하였다.

먼저 수집된 디지털 증거에 대한 분석을 종료하였을 경우 이에 대한 분석보고서 작성방법을 명확히 하고 차후 이를 법원에 제출할 수 있도록 하였다. 또한 경찰 수사기관은 수사 또는 공소유지 등을 위하여 필요한

경우 상급 수사기관이나 컴퓨터 포렌식 전문가의 지원요청을 받을 수 있도록 하였다. 마지막으로 디지털 증거의 분석을 종료한 경우에는 그 분석결과를 수사기관의 최고 책임자에게 보고하도록 하였으며, 분석대상이 된 디지털 기기들을 분석후에는 반환할 수 있도록 규정하였다.

위와 같은 내용을 중심으로 하여 디지털 증거 수집 및 분석 절차 법률안을 구성하였다. 물론 많은 부분이 부족하다고 생각이 된다. 하지만 이를 계기로 하여 입법기관에서 보완해야 할 부분은 심도있는 검토 작업을 거쳐서 보완을 한 후, 조속한 시일안에 본 법률이 제정될 수 있도록 해야 할 것이다. 이 법률의 제안은 디지털 범죄에 있어서 경찰의 적법한 절차 준수로 인한 사생화 보호와 더불어 국민의 기본권이 침해되는 것을 방지하고, 헌법상 보장된 국민의 기본권을 최대한 보호하는 작은 밑거름이 될 것이라 생각한다.

이하에서는 법률안을 도표로 제시하였다.

【법률 안】

디지털 증거 수집 및 분석에 관한 절차법

법률 제 호

디지털 증거 수집 및 분석에 관한 절차 법률안

제1장 총칙

제1조 (목적) 이 법은 컴퓨터 등 디지털 기기로부터 적법절차에 따라 디지털 증거를 수집하거나 분석하는 과정에서 필요한 절차와 준수하여야 할 기본적 사항을 정함으로써 실체적 진실 발견에 기여하고 국민의 기본권을 보호하는 것을 그 목적으로 한다.

제2조 (용어의 정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. “디지털 증거”라 함은 컴퓨터 또는 기타 디지털 저장매체에 저장되거나 네트워크를 통해 전송중인 자료로서 조사 및 수사 업무에 필요한 증거 자료들을 말한다.
2. “디지털 증거 분석”이라 함은 컴퓨터 또는 기타 디지털 저장매체(네트워크를 통해 전송중인 자료를 포함한다)에 남아있는 자료에 대한 원본 보존과 사건 관련 증거를 과학적인 절차를 통하여 추출, 검증, 판단하는 조사 및 수사과정을 말한다.
3. “휘발성 증거”라 함은 컴퓨터 실행시 일시적으로 메모리 또는 임시파일에 저장되는 증거로 네트워크 접속상태·프로세스 구동상태·사용중인 파일 내역 등 컴퓨터 종료와 함께 삭제되는 디지털 증거를 말한다.
4. “비휘발성 증거”라 함은 컴퓨터 종료시에도 컴퓨터 또는 기타 디지털 저장매체에 삭제되지 않고 남아 있는 디지털 증거를 말한다.
5. “기타 디지털 저장매체”라 함은 플로피 디스크, 휴대폰, USB, 플래쉬 메모리 등 컴퓨터 하드디스크 외의 디지털 저장매체를 말한다.

제3조 (적용범위) 이 법은 디지털 증거를 적법절차에 따라 수집·분석·보관하는 등 디지털 증거 취급과 관련된 각종 조사 및 수사행위에 적용된다.

제4조 (적법절차의 준수) 수사기관은 수사 등에 필요한 한도 내에서 적법절차를 준수한 최소한의 증거수집을 원칙으로 하며, 형사소송법, 형사소송규칙 등의 법규 및 지침에 규정된 일반적인 원칙과 절차를 준수하여야 한다.

제5조 (디지털 증거의 수집 계획) 수사기관은 신속하고 효과적인 디지털 증거를 수집하기 위하여 다음과 같은 사항에 유의하여 증거수집 계획을 수립하여야 한다.

① 수사기관은 증거수집과 관련하여 아래와 같은 사항을 사전에 파악하여야 한다.

1. 컴퓨터 하드웨어, 운영체제, 소프트웨어, 저장매체, 데이터베이스
2. 네트워크 관련 정보
3. 시스템 또는 네트워크 책임자나 관리자
4. 수집해야 할 디지털 매체의 개수나 데이터의 분량

② 디지털 증거 수집 및 이송에 필요한 인원과 장비를 준비해야 한다.

③ 수사기관은 디지털 증거 수집의 필요에 따라 압수·수색영장을 신청한다.

제6조 (디지털 증거의 수집 절차) 수사기관은 디지털 증거를 수집하기 위하여 다음과 같은 절차에 유의하여 증거 수집을 하여야 한다.

① 컴퓨터 관련 디지털 기기들에 대한 사진촬영 및 현장을 스케치한다.

② 컴퓨터 네트워크 정보 등 휘발성 증거를 수집하여야 한다.

③ 컴퓨터 관련 디지털 기기들에 대한 수집 대상물의 전원을 확인한다.

④ 컴퓨터 본체의 수집을 원칙으로 하되, 부득이한 경우에는 컴퓨터 하드디스크만 분리하여 수집한다.

⑤ 외장형 하드 디스크, USB 메모리 등 기타 디지털 저장매체와 각종 소프트웨어, 주변장치, 케이블 등을 수집한다.

⑥ 디지털 증거물을 포장하고 상세한 정보를 기재하여 증거물에 부착한다.

⑦ 압수증명서를 작성하여 입회인에게 교부하고, 입회인으로부터 압수확인서 및 압수증거물 목록에 서명날인을 받는다.

제7조 (디지털 증거의 진정성·무결성 확보) 디지털기기 등을 압수·수색·검증하거나 디지털 자료를 수집·분석할 때에는 디지털기기 또는 디지털 자료를 수집한 때로부터 법정에 증거로 제출할 때까지 변경 또는 훼손되지 않도록 절차의 연속성을 유지하여야 하며 그 과정을 기록하여야 한다.

제8조 (디지털기기 및 저장매체 등의 운반 및 보관) 디지털 자료가 저장된 디지털기기 및 저장매체 등은 외부환경에 민감하고 파손되기 쉬우므로 운반 또는 보관할 경우에는 완충용 보호 박스 사용, 정전기 차단, 충격방지를 위한 개별포장 등의 조치를 취하여 그 기기 등이 파손되거나 저장된 디지털 자료가 손상되지 않도록 하여야 한다.

제2장 디지털 증거의 압수 · 수색

제9조 (디지털 증거의 압수·수색 준비) 컴퓨터 관련 기타 디지털기기 등을 압수·수색·검증하거나 디지털 자료를 수집하고자 할 경우에는 사전에 다음 각호의 사항을 확인하고 계획을 수립하여야 한다.

1. 사건의 개요, 압수·수색 장소 및 대상
2. 압수·수색대상자가 운영하고 있는 정보처리시스템의 유형과 규모
3. 압수·수색대상자가 운영하고 있는 네트워크의 구성 형태
4. 기타 디지털 기기의 보유현황 등

제10조 (컴퓨터 등 정보처리시스템의 압수·수색) ① 컴퓨터 등 정보처리시스템을 압수할 경우에는 가능하면 정보처리시스템으로부터 저장매체만을 분리하여 압수하는 것을 원칙으로 한다. 다만, 저장매체를 분리할 경우에 수사의 목적을 달성할 수 없거나 디지털 기기 또는 디지털 자료가 손상, 훼손될 우려가 있을 때에는 정보처리시스템 전부를 압수할 수 있다.

② 제1항과 같이 정보처리시스템 등을 압수할 경우에는 별지 제1호의 서식의 부전지를 작성하여 압수대상 정보처리시스템 또는 저장매체에 붙이고 압수·수색 대상자의 확인·서명을 받아야 한다.

③ 압수·수색·검증의 현장에서는 전산관리자 또는 책임자를 통하여 대상 정보처리시스템의 구성 및 주변장치의 연결 상태 등을 파악하고 특별한 사정이 없는 한 이를 사진 및 카메라, 캠코더로 촬영한 후 특이사항을 기록하여야 한다.

④ 정보처리시스템을 압수·수색·검증할 경우에는 대상 정보처리시스템의 설정시간을 한국 표준시간과 비교하여 기록하여야 한다.

⑤ 제1항의 방법으로 정보처리시스템을 압수하기 곤란한 사정이 있거나 또는 수사목적상 필요한 경우에는 대상 정보처리시스템에서 디지털 자료를 검색하여 이를 저장매체에 기록하는 방법으로 수집할 수 있다. 이때에는 압수·수색대상자 또는 전산관리자를 입회시키고 수색한 결과물이 대상 정보처리시스템내의 자료로부터 검색된 것임을 확인시킨 후 다음 각호의 사항이 포함된 별지 제2호의 서식을 작성하여 입회인의 확인·서명을 받아야 한다.

1. 압수·수색·검증 착수 시작과 종료시간
2. 정보처리시스템의 종류와 구성
3. 정보처리시스템의 설정시간
4. 검색도구와 방법
5. 수집된 디지털 자료에 대한 해쉬 값(Hash Value)

⑥ 데이터베이스(DB)가 구축된 정보처리시스템에 대하여 네트워크를 통해 다른 데이터베이스 시스템에 이식 가능한 형태의 파일로 변환(Export, Dump)하여 압수할 경우에는 압수·수색대상자 또는 전산관리자를 입회시키고 압수된 데이터베이스 자료의 해쉬 값(Hash Value)을 포함하는 프로파일을 생성하여 입회인의 확인·서명을 받아야 한다.

⑦ 정보처리시스템을 압수할 경우에는 해당 정보처리시스템의 사용자 또는 관리자의 인적사항을 파악하여 기록하고, 기타 정보처리시스템을 운영하는데 필요한 프로그램 매뉴얼, 설계도, 조직도, 개체관계도(ERD) 등을 함께 압수하여야 한다.

제11조 (부당한 압수·수색·검증 금지) 디지털기기 등을 압수·수색·검증하거나 디지털 자료를 수집·분석할 때에는 수사에 필요한 최소한의 범위에서 실시하고 전 과정에서 적법절차를 엄격히 준수하여야 한다.

제12조 (디지털 증거의 압수·수색시 유의사항) ① 컴퓨터 관련 디지털기기 등을 압수·수색·검증하거나 디지털 자료를 수집할 경우에는 대상 정보처리시스템으로부터 사용자를 격리하여 시스템 강제종료 등 임의적인 조작행위를 방지하여야 한다.
② 압수·수색·검증 대상 정보처리시스템이 네트워크에 연결되어 있고 압수·수색대상자가 네트워크로 접속하여 저장된 자료를 임의로 삭제할 우려가 있을 경우에는 네트워크 연결 케이블을 차단하여야 한다.
③ 디지털기기 등을 압수·수색·검증하거나 디지털 자료를 수집할 경우에는 대상 정보처리시스템내의 링크파일(link file)의 등록정보를 확인하는 등으로 휴대용 디지털 저장매체의 사용여부를 확인하고 그 사용 흔적이 발견된 경우에는 해당기기의 식별 값(Volume serial Number)을 특정하고, 이를 압수할 수 있도록 현장에서 적절한 조치를 취하여야 한다.
④ 디지털기기 등을 압수·수색·검증하거나 디지털 자료를 수집하는 현장에서 분석을 실시하는 경우에는 쓰기방지장치를 사용하는 등으로 그 자료가 변경 또는 훼손되지 않도록 하여야 한다.

⑥ 수사기관이 수사목적상 정보처리시스템의 사용자를 특정 하는 것이 필요한 경우에는 해당 정보처리시스템의 마우스, 키보드 등에서 지문을 채취하는 등 다른 수사방법으로 조치를 취한 후, 정보처리시스템을 압수·수색·검증 하여야 한다.
⑤ 디지털기기 등을 압수·수색·검증하거나 디지털 자료를 수집하는 현장에서는 정보처리시스템이나 프린터기 등의 임시 메모리(RAM, Cache Memory)에 기록된 디지털 자료에 대하여도 확인하고 필요한 경우에는 메모리 덤프(dump) 등의 적절한 방법을 사용하여 이를 수집하여야 한다.

제13조 (압수물의 관리 및 인수인계) 수사기관에 의해 압수된 디지털기기 등은 각 품목별로 별지 제3호 서식에 따라 관리번호를 부여하고, 이를 인수인계할 경우에는 별지 제4호의 서식에 따라 인수인계표를 작성하여야 한다.

제3장 디지털 증거의 분석

제14조 (디지털 증거의 분석의 기본원칙) 디지털 증거물의 분석시에는 다음의 기본 원칙을 준수하여야 한다.
① 디지털 증거 원본의 안전한 보존 및 무결성을 확보하여야 한다.
1. 디지털 증거분석은 원본에 대한 사본 이미지를 생성하여 수생하는 것을 원칙으로 한다. 단 신속한 분석을 요하거나 이미지 생성이 현저히 곤란한 경우에는 예외로 한다.
2. 디지털 증거 분석 전의 증거 원본과 이미지의 해쉬 값 동일성 여부를 확인해야 하며, 증거 분석으로 인해 증거가 변경되어서는 안된다.

3. 디지털 증거 분석 대상에 실행 파일이 포함되어 있는 경우는 별도의 운영체제 또는 운영체제를 가상으로 설치하는 프로그램에서 실행 및 분석하도록 하여 증거의 변경을 방지하여야 한다.

4. 디지털 증거물 접수 및 반환시 책임자, 관리자, 일시, 장소, 사유 등을 관리대장에 기재하여야 한다.

② 디지털 증거분석 기법과 도구에 대한 신뢰성을 국가기관이 검증해야하고, 검증에 통과된 소프트웨어 및 도구 리스트를 공개하여야 한다.

③ 디지털 증거분석 과정 및 분석자의 성명, 분석일자, 분석방법 등에 대한 상세한 기록을 하여야 한다. 또한 증거 분석시 주요한 장면은 사진 또는 카메라, 캠코더로 촬영하여 보관하여야 한다.

④ 디지털 증거물이 동일할 경우, 제3의 분석관이 다시 분석하거나, 다른 증거분석 도구 및 장비를 사용하여도 원래의 분석과 일치하는 결과가 도출되어 디지털 증거분석 결과의 신뢰성이 확보되어야 한다.

제15조 (디지털 증거 분석 방법) ① 수집된 디지털 자료의 분석에는 국가기관이 검증한 적합한 장비와 소프트웨어를 갖추고 신뢰할 수 있는 방법으로 하여야 한다.

② 수집된 디지털 자료를 분석할 경우에는 사본을 작성하여 그 사본으로 분석하여야 한다. 다만, 사본을 만들기가 현저히 곤란한 경우에는 원본으로 분석할 수 있으며, 이 경우에는 원본이 변경, 훼손되지 않도록 기술적 조치를 취하고 기술적 조치에 관한 사항 및 원본의 변경여부 등을 분석보고서에 반드시 기재하여야 한다.

③ 제2항의 사본을 작성할 때에는 보존용 사본(이하 '보존사본'이라 한다.)과 분석용 사본(이하 '분석사본'이라 한다.)을 작성하여야 하며, 해쉬 값과 그 생성시간을 분석 보고서에 반드시 기재하여야 한다.
④ 데이터베이스(DB) 형태의 디지털 자료를 분석할 경우에는 '데이터베이스 분석 내역서'를 작성하여 분석에 이용된 데이터베이스, 테이블, 칼럼이름 및 용도 등 소정의 사항을 기재하여야 하며, 분석과정에서 작성된 질의어(SQL), 프로시저(PLSQL Procedure, Stored Procedure 등)에 대한 상세한 설명을 소스 코드(Source Code)와 함께 첨부하여야 한다.
⑤ 수집된 디지털 자료를 분석할 경우에는 분석과정을 사진 및 카메라, 캠코더로 촬영하는 등 객관성 유지에 필요한 조치를 취하여야 한다.

제16조 (디지털 자료의 보존 및 준수사항) ① 디지털 증거 자료는 온도와 습도 등 기후의 영향을 받지 않으면서 충격과 자기장, 먼지 등으로부터 보호될 수 있는 증거보관실을 설치·운영하여야 한다.
② 디지털 증거물은 쓰기방지처리가 된 상태로 충격방지용 보관함에 담아 분석이 끝날 때까지 증거본관실에 보관하여야 한다.
③ 디지털 증거분석을 위해 생성한 복제본과 분석과정에서 나온 결과물은 반영구적인 저장매체에 저장하여 증거 보관실에 보관하여야 한다.
④ 디지털 증거의 분석자료 검색 및 유사사건 분석 또는 처리에 도움을 제공하고자 증거물 데이터베이스(DB)를 구축하여 관리 및 운영하여야 한다.
⑤ 디지털 증거분석에 사용되는 도구 및 프로그램은 차후 수사 및 재판과정에서 재검증이 필요할 경우를 대비하여 제조사, 제작연도, 버전별로 구분하여 지속적으로 관리·보관하여야 한다.

제4장 디지털 증거의 분석보고서 작성 및 수집·분석 지원요청

제17조 (분석보고서 작성 및 준수사항) ① 수집된 디지털 자료에 대한 분석을 종료한 때에는 분석보고서를 반드시 작성하여야 한다.

1. 분석보고서는 추정을 배제하고 사실관계를 중심으로 작성한다.
2. 분석보고서는 객관적인 사실, 설명내용, 디지털 증거분석관의 의견을 구분하여 작성한다.
3. 디지털 증거의 발견방법, 증거물에 대한 작업 내용은 명확하게 문서화하여야 한다.
4. 디지털 증거 분석 및 처리과정을 사진 또는 화면캡처, 동영상 등으로 기록을 하여야 한다.
5. 디지털 분석에 사용된 하드웨어와 소프트 웨어의 정보를 반드시 기록한다.
6. 분석보고서는 수정이 불가능한 문서자료 형태로 부본을 작성하여, 관련 사건의 재판 종결시 또는 공소시효 만료시까지 증거보관실에 보관한다.

② 디지털 자료를 분석하는 과정에서 새롭게 획득하거나 생성된 자료가 있는 경우에는 그 자료의 사본을 CD, DVD, 하드디스크 등 디지털 저장매체에 저장하여 분석보고서에 첨부할 수 있다.

③ 분석보고서의 작성자는 서명하고, 보고서 작성내용에 대해 책임을 진다.

제18조 (디지털 분석 지원요청) ① 수사기관은 수사 또는 공소유지 등을 위하여 필요한 경우 상급 수사기관에게 다음 각 호의 지원을 요청할 수 있다.

1. 디지털기기 등의 압수·수색·검증
2. 디지털 자료의 수집
3. 수집된 디지털 자료의 분석

② 제1항의 지원을 요청할 경우에는 별지 서식에 따라 '지원요청서'를 송부하여야 한다. 다만, 긴급을 요하는 경우와 보안을 요하는 경우에는 구두 또는 전화로 요청할 수 있으며, 이 경우에는 사후에 요청서를 송부할 수 있다.

③ 제1항 제3호의 지원을 요청할 경우에는 디지털 자료가 저장된 디지털기기 등을 우송 기타 적절한 방법으로 상급 수사기관에게 송부하여야 한다.

제19조 (디지털 분석 지원 검토 및 방법) ① 상급 수사기관은 제18조 제1항의 지원을 요청받은 경우에는 즉시 지원의 타당성과 필요성을 검토하여 지원여부를 결정하여야 한다.
② 상급 수사기관은 제18조 제1항의 지원을 할 경우에는 디지털기기 등의 유형과 규모에 따라 적합하고 충분한 인원의 디지털 분석 전문수사관을 지정하여 지원하여야 한다.
③ 제2항에 의하여 지원을 지정받은 디지털 분석 전문수사관은 지원을 요청한 수사기관에 출장하여 지원함을 원칙으로 한다. 또한 지원을 종료한 때에는 상급 수사기관에게 보고한 후, 지체 없이 복귀하여야 한다.

제20조 (분석결과 통보) 수사기관은 수집된 디지털 자료의 분석을 종료한 때에는 분석결과를 최고 책임자에게 통보하여야 한다.

제21조 (디지털기기 등의 반환) 수사기관은 수집된 디지털 자료의 분석을 종료한 때에는 분석대상이 된 디지털기기 등을 수령해 가도록 통지하여야 한다.

부 칙 〈2011. 1. 1.〉
제1조 (시행일) 이 법은 공포한 날부터 시행한다.
제2조 (다른 지침의 폐지)
종전의 컴퓨터 등 압수·수색 기본지침(대검 61100-284호, 2003. 8. 11.), 디지털 증거 수집 및 분석규정(대검예규 제410호 2006. 11. 21)은 이 규정의 시행과 동시에 폐지한다.

Ⅵ. 결 론

최근 들어 디지털 범죄에서 수사기관의 수사에 의한 개인의 통신이나 이메일을 감청 또는 유출하는 일이 늘어나고 있다. 이는 범죄와 무관하게 헌법상 보호하고 있는 개인의 사생활이 침해되고 있다고 말할 수 있다.

이에 대한 최근의 우리나라 대표적인 사례가 2007년 9월 신정아의 가짜 학위를 이용한 교수직 획득과 광주비엔날레 총감독 등 형법상 업무방해죄와 관련된 사건이다. 그러나 한 언론사에 의해 이 여성의 누드 사진이 본인의 동의 없이 유출되어 본인에게는 심각한 사생활이 침해가 되었고,[125] 결국 당사자는 관련 언론사를 상대로 손해배상 및 정정보도 청구 소송을 제기하였다.

이는 최근에 이슈가 된 언론사에 의한 개인의 사생활 침해의 대표적인 사례라 할 수 있다. 우리나라는 디지털 범죄에 있어 아직까지 수사기관에 의하여 범죄와 관련이 없는 개인의 사생활이 유출, 공개되어 문제가 제기된 사례는 없지만, 매년 기하급수적으로 증가하는 디지털 범죄에서 사생활 침해의 개연성이 범죄와 같이 증가할 가능성은 충분히 있다고 보여진다.

앞에서 살펴본 바와 같이 미국의 경우는 디지털 범죄 수사에서 발생하는 사생활 침해문제를 일반 전통적인 범죄사례에서 도출하여 해결하고자 하였다. 이러한 사례들은 우리에게 많은 시사점을 주었고, 차후 우리의 입법 모델이 될 수 있도록 제시하였다.

앞으로 우리 사회는 더욱더 첨단 정보화 사회로 진입할 것이며, 이에

125) 서울여성회,「여성,뉴스 클리핑」, 2007. 9. 13.

따른 사생활의 침해 또한 다양한 방식으로 발생할 것으로 예상된다. 따라서 헌법상 사생활 보호에 관하여 정보화 시대에 맞추어 기능, 역할, 보호 내용 등을 충분히 검토할 필요성이 있다 할 것이다.

따라서 미국의 디지털 범죄 사례들을 심도있게 검토·분석하고, 우리의 수사기관은 이에 대한 사생활 보호의 필요성을 인식하고 수사에 임해야 할 것이며, 무엇보다도 중요한 것은 디지털 범죄에서 사생활 침해 문제에 대하여 이를 보호할 수 있는 입법적인 방안이 제시되어야 한다고 생각한다.

【參 考 文 獻】

Ⅰ. 國內文獻(單行本)

경찰청,「디지털 증거처리 표준 가이드라인」, 경찰청 수사국, 2006. 12.

桂禧悅, 憲法學(中), 博英社, 2007.

김문일,「컴퓨터 범죄론」, 법영사, 1992.

김일수·서보학,「형법총론(제10판)」, 博英社, 2005.

김학신, 디지털 범죄 수사와 기본권, 한국학술정보(주), 2009.

南孝淳·丁相朝,「인터넷과 法律Ⅱ」, 法文社, 2005. 12.

文鴻柱,「美國憲法과 基本的 人權」, 裕豊出版社, 2002.

朴相基,「刑法各論」, 博英社, 1999.

裵鍾大·李相暾,「刑事訴訟法(第6版)」, 弘文社, 2006.

백광훈,「인터넷범죄의 규제법규에 관한 연구」, 형정원, 2000. 12.

_____,「사이버범죄에 대한 ISP의 형사책임에 관한 연구」, 형정원, 2003.

尹明善,「美國憲法과 統治構造」, 유스북, 2006. 2.

_____,「美國 基本權 硏究」, 慶熙大學校 出版局, 2004. 12.

이용완,「유럽(영국, 프랑스, 독일)의 사이버 범죄 수사 및 디지털 증거분석 연구」, 경찰청 수사국, 2004. 12.

조 국,「위법수집증거배제법칙」, 博英社, 2005.

조병인 외3,「사이버범죄에 관한 연구」, 한국형사정책연구원, 2000.

Ⅱ. 國內文獻(論文)

權寧星,「私生活權의 意義와 역사적 변천」, 言論仲裁委員會, 1983. 6.

강동범,「컴퓨터 범죄와 개정형법」, 법조 46권 8호, 1997. 8.

_____,「사이버범죄와 형사법적 대책」, 형사정책연구 제11권 제2호, 한국형사정책연구원, 2000.

김종섭,「사이버 범죄 현황과 대책」, 한국형사정책학회(2000년 동계 학술회의자료), 2000.

김학신, 디지털 범죄 수사와 기본권에 관한 연구(영장제도를 중심으로), 치안정책연구소, 2009.

金炯盛·金學信,「Computer Forensics의 법적 문제 연구」, 成均館法學 第18券 第3號, 成均館大學校 比較法硏究所, 2006. 12.

朴宣映,「가상공간에서의 성표현의 자유와 법적 제한」, 한국법제연구원, 2002. 12.

徐柱實,「Warren·Brandeis의 The Right to Privacy」, 美國憲法硏究 第6號, 美國憲法硏究所, 1995.

심원섭,「컴퓨터 신종범죄에 관한 연구 -인터넷 관련 범죄를 중심으로-」, 연세대학교석사학위논문, 2004.

梁根源,「刑事節次上 디지털 證據의 蒐集과 證據能力에 관한 硏究」, 慶熙大學校博士學位論文, 2006.

吳奇斗,「刑事節次上 컴퓨터관련 證據의 蒐集 및 利用에 관한 硏究」, 서울大學校 博士學位論文, 1997.

유인모,「법학연구와 교육을 위한 컴퓨터 활용」, 영남법학, 제1권 제2호, 1994.

尹明善,「性的 프라이버시 權利」, 美國憲法硏究 제6호, 1995.

원혜욱,「컴퓨터관련증거의 증거조사와 증거능력」, 수사연구, 수사연구사, 2000. 6.

임종률,「컴퓨터 범죄와 형법적 대응」, 숭실대학교 법학 논집 제5집, 1989, 12.

전지연,「전자적 정보의 형사법적 보호에 관한 연구」, 한림법학 FORUM 제8권, 1999.

조병인,「하이테크범죄의 실태와 대책」, 한국공안행정학회 국제범죄학술세미나 발표논문, 1999. 9. 17.

조병인 외3,「사이버범죄에 관한 연구」, 한국형사정책연구원, 2000.

정영화,「현대헌법학에서 프라이버시 법리의 재검토」, 사이버커뮤니케이션 학보 통권 제7호, 2001.

정준현,「유비쿼터스 컴퓨팅과 프라이버시보호」, 成均館法學 第16券 第1號, 成均館大學校 比較法硏究所, 2004.

최영호,「정보범죄의 현황과 제도적 대처방안」, 한국형사정책연구원, 1998.

허만영,「사이버 범죄에 대한 국가의 정책적 대응방안(21세기 도전과 사이버스페이스)」, 사이버커뮤니케이션학회 추계학술대회발표논문. 1999. 11.

허일태,「사이버범죄의 현황과 대책」, 동아대학교 법학연구소 세미나 발표논문, 2000.

Ⅲ. 外國文獻

Allan M. Gahtan, Electronic Evidence, 2000.

Cees J. Hamelink, The Ethics of Cyberspace, 2000, Sage Publications, London

CCIPS(Computer Crime and Intellectual Property Section, U.S. D.O.J.), Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, <www.cybercrime.gov>.

David R. Koepsell, The Ontology of Cyberspace, Open Court, Chicago, 2000.

Debra little john shinder ed tittel; 譯 강유, Scene of the cybercrime computer forensics handbook, 에이콘, 2003.

Edward Bloustine, "Privacy as an Aspect of Human Dignity", 39 *New York Univ. Law Review*, 1964.

G. David Garson, Social Dimensions of Information Technology: Issues for the new Millemium, Idea Group Pu. Hershey, 2000.

Gina De Angelis, "ARPANET, HACKERS, CRACKERS, AND PHREAKS", Cyber Crimes, Philadephia (Chelsea House Publishers), 1999.

Jerry Kang, "Information Privacy in Cyberspace Transaction"s, Stanford Law Review Vol. 50, 1998.

Ruth Gavison, "Privacy and the Limits of Law", *Yale Law Journal* 421, 1980.

Wolfgang Heinz, 컴퓨터 범죄와 컴퓨터 형법(독일의 컴퓨터 범죄 현황

과 대응), 한대 법학연구소 컴퓨터 범죄 세미나, 2000. 10.

大橋充直,「ハイテク犯罪捜査入門」, 東京法令出版, 2004.

北村 篤,「ハイテク犯罪に對處するための刑事法の整備に關する要綱」, ジュリストNo. 1257, 2003.

安富 潔,「コンピユータ犯罪と刑事手續」, 慶應義塾大學法學研究會, 2000.

_____,「刑事手續とコンピュータ 犯罪」, 慶應義塾大學 法學研究會叢書(52)(平成 4年), 1992. 2. 20.

Ⅳ. 기타

한국정보보호진흥원, www.kisa.or.kr

국제 첨단범죄수사협회, www.htcia.org

국제 컴퓨터수사전문가 협회, www.cops.org

디지털 증거에 관한 국제협회, www.ijde.org

미국 국방부 사이버범죄센터, www.dcfl.gov

미국 법무부 컴퓨터범죄지적재산, www.cybercrime.gov

미국 사법연구원, www.ojp.usdoj.gov

미국 스탠포드대 안보전략연구소(CISAC), www.cisac.stanford.edu

컴퓨터증거에 관한 국제조직, www.ioce.org

매일경제신문, 2007. 9. 3.

서울여성회,「여성,뉴스 클리핑」, 2007. 9. 13.

조선일보, 2007. 11. 29.

책임연구보고서 2010-26

디지털 범죄에서 프라이버시(Privacy) 보호에 관한 연구

2010년 12월 30일 발행

발행인 : 김 영 식

발행처 : **치안정책연구소**
경기도 용인시 기흥구 언동1길 29

홈페이지 : www.psi.go.kr

POLICE SCIENCE INSTITUTE