2009-04 | 책임연구보고서

디지털 범죄수사와 기본권에 관한 연구

(영장제도를 중심으로)

치안정책연구소
POLICE SCIENCE INSTITUTE

2009-04 | 책임연구보고서

디지털 범죄 수사와 기본권에 관한 연구

(영장제도를 중심으로)

치안정책연구소 생활안전대책연구실

연구관 김 학 신

<목 차>

제1장 서 론

제1절 연구목적

최근의 디지털 기술은 급변하게 약진하고 있다. 이러한 디지털 기술을 통한 정보의 변화는 새로운 형태의 디지털 범죄를 생산해 내고 있다. 20세기와 21세기를 통틀어서 인간이 가장 획기적으로 발명한 것으로 내세우는 것이 인터넷이다. 인터넷 웹(web) 환경은 디지털 정보를 수집하여 보여주고 전달하던 시대인 웹 1.0 시대를 지나, 현재는 누구나 손쉽게 디지털 정보를 생산· 공유할 수 있도록 한 사용자 참여 중심의 웹 2.0의[1] 시대로 들어왔다. 앞으로는 인터넷이 인간처럼 스스로 지능을 갖는다는 웹 3.0의[2] 시대를 바라보면서 인터넷을 통한 디지털 기술의 환경은 지속적으로 가속화하여 발전할 것이다.

인터넷 사용자가 네트워크나 컴퓨터를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 유비쿼터스(Ubiquitous)의 환경으로 사회가 진화하면서 컴퓨터 사용자의 편리성이 증대되고, 우리의 여가활동 방법과 비즈니스 방식, 지식의 습득 방법 등이 다양하고 편리하게 변화되었다. 또한 모든 산업 사이의 장벽이 무너지고 여러 기술과 성능이 하나로 융합되는 '디지털 컨버전스'[3] 현상도 도래하였다.

---

1) 이에 대한 대표적인 것이 블로그를 자신의 취향대로 만들거나 게시판에 댓글을 쓰고, 동영상(UCC)을 제작해서 올리는 활동이 웹 2.0의 특징이다.

2) 최근 미국의 CNN은 정보기술(IT)업계에 '웹 3.0'이 화제가 되고 있다. 신생 검색 업체 트와인(Twine)의 창립자 노바 스파이백은 "우리는 현재 웹 3.0 시대에 있다. 이는 우리가 세 번째(third) 인터넷 시대에 접어들었음을 의미한다"고 말했다. 전자신문, '웹 3.0' 시대 오긴 왔나?, 2009. 5. 27.

3) 디지털 컨버전스(convergence)라 함은 디지털 기술이 발전함에 따라 유선과 무선, 방송과 통신, 통신과 컴퓨터 등 기존의 기술·산업·서비스·네트워크의 구분이 모호해지면서 이들 간에 새로운

현재 디지털 기술의 발달로 인한 순기능과 발맞추어 필연적으로 역기능도 급속하게 증가하고 있는 실정이며 컴퓨터를 통한 새로운 범죄 방법·기술들은 언제, 어디서나 쉽게 인터넷을 이용하여 범죄자에게 악용되고 있다. 그 결과 신종 범죄들이 쏟아지고 있는 실정이다. 더구나 이러한 범죄 기술과 신종 범죄에 대처하는 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 관련 법제가 미비하기 때문이라 하겠다. 또한 네트워크 정보와 시스템들은 디지털 기반으로 되어 있고 디지털 증거의 특성상 조작·삭제·위·변조, 전송 등이 용이하다는 것도 또 하나의 중요한 원인이 되고 있다.

최근 경찰 및 검찰 등의 수사기관은 디지털 범죄를 수사함에 있어 컴퓨터 포렌식 기법[4]을 통하여 디지털 증거를 수집하고 있다. 그러나 이러한 수사기법을 사용하여 수사함에 있어 이에 필요한 적법한 절차를 규정한 관련 법률은 미비한 상태이다.[5]

이러한 법률 미비로 인하여 디지털 범죄 수사시에 압수 · 수색을 통한 증거수집 과정에서 발생할 수 있는 헌법상 적법절차 위반, 영장제도를 위반한 증거수집, 타인의 사생활 침해 등 헌법상 개인의 기본권 침해 문제가 너무 많이 발생하고 있다. 수사기관에 의한 디지털 범죄 수사에서 기본권 침해 문제가 많이 발생하고 있지만, 수사를 하는 수사기관이나

형태의 융합 상품과 서비스들이 등장하는 현상을 말한다. 이에 대한 예로 휴대폰은 이동전화의 기능과 디지털카메라, MP3, 방송 시청, 금융 업무의 기능을 융합하였다. www.naver.com 참조.

4) 디지털 증거는 복사가 쉽고, 원본과 복사본의 구분도 어려우며, 조작 및 생성, 전송, 삭제가 매우 용이하다. 따라서 디지털 증거가 법적으로 증거능력을 갖게 하기 위해서는 수집·보관·분석·보고에 이르는 전 과정에 특별한 절차와 방법이 따라주어야 한다. 이렇게 디지털 증거가 법적으로 증거능력을 갖도록 하는 절차와 방법을 '컴퓨터 포렌식(Computer Forensics)' 이라고 한다.

5) 현재에는 2006년 12월 말에 경찰청에서 '디지털 증거 처리 표준 가이드라인' 과 검찰청에서 2006년 11월 21일 대검예규로 '디지털증거수집및분석규정' 을 근거로 시행하고 있는 실정이다.

수사를 받는 당사자도 이에 대하여 전혀 인식을 하고 있지 못하고 있는 것도 문제이다.

따라서 위와 같은 문제점을 해결하기 위하여는 수사기관이 디지털 증거를 수집함에 있어 디지털 범죄, 증거, 절차 등 관련 법률을 제정하거나 기존 관련 법률을 개정할 필요가 있다. 그리고 수사기관은 이 법률 규정에 근거하여 엄격한 절차에 따라 디지털 증거를 수집함으로써 헌법상 보장된 개인의 사생활 보호 및 국민의 기본권이 침해되지 않도록 최대한 존중해서 수사를 해야 할 것이다. 또한 수사에 필요한 최소한의 범위내에서 압수· 수색을 실시해야 할 것이다.

이러한 추세에 따라 이 논문은 수사기관이 디지털 범죄를 수사함에 있어, 특히 컴퓨터를 비롯하여 디지털 기기들에 대한 압수· 수색을 통하여 디지털 증거를 수집하는 과정에서 발생할 수 있는 문제점인 영장제도와 관련하여 기본권 문제를 고찰하고자 한다.

제2절 연구 범위와 방법

수사기관이 압수· 수색을 집행하여 디지털 증거를 수집하는 과정에서 발생할 수 있는 헌법상 적법절차 위반의 문제, 특히 영장제도와 관련된 문제점에 관하여 고찰하고 이에 대한 해결책을 제시하고자 한다. 이에 대한 구체적인 범위는 다음과 같다.

제1장은 서론으로 이 논문을 쓰게 된 목적을 제시하고, 문제를 제기함으로써 연구방향 및 연구 범위와 방법을 제시하였다.

제2장에서는 디지털 범죄의 개념과 유형을 설명하고자 한다. 현재 사이버 공간에서 발생하는 범죄를 컴퓨터 범죄, 사이버 범죄, 인터넷 범죄, 정보범죄, 하이테크 범죄, 디지털 범죄 등 다양한 형태로 불리고 있

는데 이에 대한 개념을 정의하고, 디지털 범죄의 특성인 익명성, 비대면성, 시간과 공간의 무제한성, 고도의 전파성, 정보의 집약, 정보전달의 신속성 등 디지털 범죄의 특성을 설명하고, 더불어 디지털 범죄의 유형을 설명하고자 한다.

디지털 범죄는 한 가지 수법에 의한 범행보다는 여러 가지 수법이 결합된 형태로 범죄 행위가 일어나는 경우가 많다. 현재 디지털 범죄의 유형을 구체적으로 구분한 규정이나 근거가 없어 이를 구체적으로 분류하기는 매우 어렵다고 할 수 있다. 경찰청에서는 디지털 범죄를 다음과 같이 분류하고 있다. 디지털 범죄를 크게 과거 현실세계의 범죄가 단지 컴퓨터 시스템을 이용한 형태의 일반화된 디지털 범죄와 사이버 공간 고유의 범죄 즉, 대규모 피해를 야기시키는 해킹, 바이러스 제작· 유포 등의 사이버 테러형 범죄로 구분하고 있다. 이에 대한 내용을 구체적으로 살펴보고자 한다.

제3장에서는 디지털 범죄에서 신체의 자유 보호를 위한 절차적 보장으로서 적법절차와 영장주의에 대한 개관과 현행 형사소송법상 영장에 의하여 디지털 증거의 압수· 수색이 가능한지의 여부를 중점적으로 고찰하고자 한다. 특히 일본의 판례를 인용하여 심도있게 살펴볼 것이다.

현재 우리 사회는 모든 범죄가 디지털화 되어가고 있고 디지털 범죄가 급속도로 증가하고 있다. 따라서 디지털 증거의 압수· 수색의 가능성에 관하여 다양한 형태의 문제점들이 앞으로 제기될 것이다. 이러한 문제점들을 적절하게 대처하기 위하여는 미리부터 연구가 필요하리라 본다.

제4장에서는 수사기관에 의한 디지털 범죄 수사시에 발생할 수 있는 기본권 침해문제로 특히 수사시관이 디지털 증거를 수집함에 있어 야기되는 적법절차 위반, 영장주의 위반에 따른 신체의 자유 침해 문제에 대하여 고찰하고자 한다. 현재 우리나라에서는 수사기관이 디지털 범죄와 관련하여 개인의 기본권 침해 문제에 관하여 논의 및 관련된 사례가 없

는 실정이다. 이러한 기본권 침해 문제를 해결하고자 다양한 형태의 미국의 사례들을 예로 들 것이다. 미국의 경우는 기존 전통적인 범죄사례와 판례에서 이를 도출하여 디지털 범죄에 적용하고 있다. 따라서 우리의 수사기관은 이에 대한 구체적인 검토가 필요할 것이라 본다.

이상과 같이 이 논문의 연구 목적을 달성하기 위하여 다음과 같은 방법으로 연구하고자 한다.

우선 디지털 범죄는 기존의 전통적인 범죄와는 디지털이라는 증거의 특성상 많은 차이점이 있다. 이러한 디지털 증거의 특성에 맞추어 새로운 수사기법을 일찍이 적용하고 있는 미국의 최근 문헌들을 구체적으로 분석하는 방식으로 연구하고자 한다.

두 번째로 위와 같은 문헌분석 방식을 통해 수사기관이 디지털 범죄를 수사함에 있어 발생하는 기본권 침해 사례를 분석하고자 한다. 우리나라는 현재 디지털 범죄에 있어 기본권이 침해되는 사례가 미비한 상태이고, 이에 반해 미국은 이와 관련된 사례가 많이 존재하고 있다. 이를 해결하기 위해 미국은 기존 전통적인 범죄사례 특히, 미연방 대법원 판례와 하급심 판례를 통해 디지털 범죄에 적용할 수 있도록 관련 부분을 도출해 내고 있다. 이러한 방법을 우리 수사기관에서도 인용을 하여 문제점을 찾고 앞으로 수사에 지침이 될 수 있도록 관련 미국 판례들을 심도있게 검토· 분석하고자 한다.

세 번째로는 전통적인 범죄와는 달리 디지털 범죄에 관한 증거문제는 법학적인 문제와 함께 기술적인 수사기법 문제도 혼합되어 있으며, 특히 이에 대한 연구가 부족한 상태이다. 이에 대한 미국의 문헌분석과 비교법적인 분석방법을 통하여 연구 및 개선방안을 구체적으로 제시하고자 한다.

제2장 디지털 범죄의 개념과 유형

제1절 디지털 범죄의 개념

1984년 William Gibson이라는 미국의 과학소설 작가가 'Neuromancer'라는 소설에서 '사이버 공간'[6]이라는 용어를 사용하였으며, 이는 현실적·물리적 세계와는 구분이 되며 이러한 사이버 공간의 출현은 인터넷[7]이 있기에 가능했다.[8] 그러나 1876년에 미국의 알렉산더 그레햄 벨(Alexander Graham Bell)이 오늘날 대중화된 통신장치의 하나인 전화를 발명하였을 때 이미 사이버 공간은 조성이 되었다.[9]

현재 사이버 공간에서 발생하는 범죄를 부르는 용어가 혼용되어 쓰이고 있는데, 보통 컴퓨터 범죄, 사이버 범죄, 인터넷 범죄, 디지털 범죄[10], 정보 범죄, 하이테크 범죄 등으로 다양하게 호칭이 되고 있다.

---

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

7) 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.

8) 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.

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

10) 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 명

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

1. 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.[11]

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.[12] 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.[13]

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

확하고, 데이터를 압축·조작하여 효율적인 전송이 가능하여 정밀도를 높일 수 있다는 특징이 있다.

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

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

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

를 저지르고 그 범죄를 조사하는데 있어서 컴퓨터 지식이 관련되어 있는 사건' 으로 정의하고 있다.[14] 현재 컴퓨터 범죄라는 용어는 상당히 보편화된 용어중의 하나이다. 보통 컴퓨터 범죄라 함은 컴퓨터를 대상으로 하거나 또는 수단으로 하여 행하는 범죄행위를 말한다.[15]

컴퓨터 범죄를 '컴퓨터와 관련한 정보처리과정에 불법적으로 개입하는 모든 범죄행위'[16] 또는 '컴퓨터의 데이터와 관련하여 형법적으로 처벌할 가치가 있는 범죄 행위의 총체'[17]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.[18]

2. 사이버 범죄와 인터넷 범죄

IT(Information Technology)의 발전으로 인하여 컴퓨터를 대상으로 하는 범죄가 지나가고 네트워크(Network)로 연결된 공간이 생기게 되었

14) 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.

15) 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.

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

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

18) 朴相基,「刑法各論」, 博英社, 1999, 9면 참조.

다. 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.[19] 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.[20]

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.

3. 정보범죄와 하이테크 범죄

정보화촉진기본법 제2조 1호에서 정보의 정의를 다음과 같이 규정하고

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

20) 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.

있다. “정보라 함은 자연인 또는 법인이 특정목적을 위하여 광 또는 전자적 방식으로 처리하여 부호·문자·음성·음향 및 영상 등으로 표현한 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 총칭하는 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.[21] 정보화촉진기본법 제2조 제3호에서 ‘정보통신’ 이라 함은 “정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 이에 관련되는 기기·기술·역무 기타 정보화를 촉진하기 위한 일련의 활동과 수단을 말한다” 고 규정하고 있다. 사실 ‘정보’ 가 무엇인가라는 문제에 대하여는 정보화촉진기본법 제2조의 정의 이외에도 정보의 정의를 다양하게 정의하는데 정보라 함은 ‘현실세계로부터 단순한 관찰이나 측정을 통해서 수집한 사실, 개념, 값을 표현한 것’[22] 또는 ‘특정한 사람이나 사항에 대하여 의미 있는 상태로 가공한 것’[23], ‘필요하고 적절한 자료를 활용이 가능한 형태로 처리한 것’[24]과 같은 정의를 내리고 있다.

이와 또 다른 용어로 하이테크 범죄(Hi-Tech Crime)[25]란 용어를 사용하는데 이는 과학기술 중에서도 컴퓨터 기술 및 정보통신기술 또는 양자의 결합으로 형성되는 가상세계와 직접 관련이 있는 범죄유형만을 하이

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

테크 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.[26]

4. 디지털 범죄

현재 우리가 사용하는 대부분의 전자기계들은 디지털의 방식으로 이루어져 있다. 컴퓨터를 비롯하여 휴대폰, 디지털 카메라, USB, 캠코더, PDA 등 다양한 기기들이 디지털의 방식으로 이루어져 있으며, 그 결과 디지털 혁명, 디지털 세대, 디지털 기술 등 디지털이란 용어가 대중화되었다. 이러한 디지털 기기의 발달은 우리나라를 정보화 선진국으로 견인하는 주요한 원동력이 되었다. 이와 더불어 모든 분야가 유비쿼터스[27]환경으로 진입하게 되고, 모든 생활은 전자 매체를 통하여 이루어지고 있다.

또한 수사기관의 범죄 수사 분야에서도 전자 매체를 통한 디지털의 활용은 필수불가결한 요소로 등장하였다. 현재 우리나라에서 CCTV(closed-circuit television)는 광범위하게 활용되고 있으며, 휴대전화 사용 내

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

27) 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.

역 및 위치 추적 확인 기능 등은 범죄 수사에서 중요하게 활용되고 있다.

최근에는 이동식 저장장치(USB Memory),[28] PMP(portable multimedia player),[29] 전자수첩, 내비게이션(Navigation),[30] 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 범죄를 발생케 하는 원인이 되었다. 이처럼 다양한 디지털 기기로 인하여 발생하는 모든 범죄를 디지털 범죄라 할 수 있을 것이다.

5. 소결

인터넷 네트워크를 이용하여 발생하는 범죄에 적절하게 대응하기 위해서는 이를 명확히 정의할 수 있는 적절한 용어가 필요하다. 앞에서 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 전통적인 범죄와는 수사방법이나 증거수집 및 조사 등에서 달리 취급해야 할 필요성이 있다. 그리고 정보통신 기술의 환경이 급속히 변화되기 때문에

---

28) 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.

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

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

법적 안정성을 중시하는 우리의 법제도를 위해서라도 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 기기들은 다양하게 범죄에 사용되고 있다.

이 논문에서는 디지털 기기에서 생성되는 디지털 증거[31]의 압수· 수색과 관련된 부분이 논문의 핵심적인 부분이기 때문에 여기에서는 디지털 범죄로 통일되어 쓰기로 하겠다. 물론 디지털 범죄와 가장 관련이 많은 부분은 인터넷임을 부정하지는 않기에 주된 대상은 컴퓨터와 관련된 인터넷임을 밝힌다.

제2절 디지털 범죄의 특성과 유형

1. 디지털 범죄의 특성

디지털 범죄는 기존의 전통적 범죄인 살인· 강도· 절도· 사기 등의 범죄와는 다른 특성을 가지고 있는데, 이는 정보통신 기술과 컴퓨터의 결합으로 조성되는 특수한 환경을 갖기 때문이다. 이는 시간과 공간의 제약을 받지 않으며, 익명성과 비대면성이 보장되고, 손쉽게 다량의 정보

31) 디지털 증거(Digital Evidence)라는 용어에 대하여는 아직 개념이 정의되지 않았다. 전자증거(Electronic Evidence) 또는 컴퓨터 관련 증거로 언급되기도 하며 어떠한 경우에는 여기서처럼 디지털 증거라는 용어로 사용하기도 한다. 현재 형법 및 우리의 기타 법률에서는 전자기록이라는 용어로 정의하고 있다.

를 처리할 수 있다. 또한 과거 국가나 공공기관이 아니면 구축할 수 없는 대형 용량의 컴퓨터 시스템을 이제는 개인도 쉽게 사용할 수 있게 되었다. 이러한 변화는 수사기관의 범죄 대응에도 중요한 도전이 되고 있으며, 특히 인권이나 사생활의 보호 측면에서도 새로운 변화가 일어나고 있다. 인터넷을 통한 디지털 범죄의 특성으로는 익명성, 비대면성, 시간·공간의 무제한성 내지 동시성 및 국제성, 높은 전파성과 재산피해, 정보의 집약, 정보전달의 신속성, 즉시성 등이 있으며 이에 대하여 좀 더 구체적으로 살펴보겠다.

가. 익명성(anonymity)

인터넷 온라인 세상에서는 익명을 이용하여 사이버 침입·절도·사기·자금세탁,[32] 파괴적인 디지털 범죄,[33] 인터넷 도박, 범죄 공모 등을 할 수 있다. 익명성은 인터넷 공간을 범죄 수행의 공간으로 만드는 중요한 요인이며, 가장 대표적 디지털 범죄의 특성 중 하나이다. 이와 같은 익명성(anonymity)을 이용하여 범죄자는 죄의식 없이 범행을 저지르는 경우가 많게 되고 이는 결국 범죄를 증가시키는 한 원인이 되고 있다. 이러한 인터넷의 익명성으로 야기되는 대표적인 범죄로는 인터넷 사기, 언어폭력과 허위사실 유포로 인한 명예훼손, 타인의 개인정보 유출[34] 등

32) 사이버 자금세탁은 부정한 방법으로 모은 자금의 출처를 인터넷을 통해 감추는 것을 의미하는데 자금 세탁은 아주 오래된 범죄이며, 인터넷의 익명성은 불법적인 자금을 적법한 자금으로 쉽게 바꿀 수 있도록 했다.

33) 파괴적인 디지털 범죄는 네트워크에 침입해서 데이터나 프로그램 파일을 삭제하거나, 웹 서버에 침입해서 웹 페이지를 지우는 행위, 네트워크나 컴퓨터로 바이러스, 웜, 기타 악성 코드를 주입시키는 행위, 서비스 거부(Dos)공격을 하여 서버를 다운시키거나 정당한 사용자가 네트워크를 사용할 수 없게 하는 행위 등을 의미한다.

34) 2008년도 주요 개인정보 침해사고 사례를 살펴보면,「옥션」고객 1,081만명 개인정보가 해킹에 의하여 유출(2008. 2),「GS 칼텍스」고객 1,100만명 개인정보가 내부자에 의해 유출(2008. 9),「다음」고객 53만명 개인 이메일 정보가 관리소홀로 노출(2008. 7),「하나로텔레콤」고객 600만명 개인정보가 무단 제공되 유출(2008. 4).

을 들 수가 있다. 또한 익명성을 이용한 악성댓글[35], 이로 인한 자살문제[36]와 ID 등의 허위표시가 가능하다는 점은 청소년이 음란 사이트에 가입하기가 보다 쉬워져 청소년 문제가 제기되기도 한다.

특히 최근에는 인터넷을 통한 쇼핑이 활성화 되고, 익명성을 이용한 쇼핑 사기 범죄가 꾸준히 증가하고 있다[37]. 이에 관련된 가장 대표적인 범죄 사례를 보면, 범죄자는 인터넷 쇼핑몰이나 물건을 거래하는 사이트에 광고를 낸다. 그리고 그 광고를 보고 물건을 구매하고자 하는 자는 인터넷 뱅킹이나 은행을 이용하여 온라인 입금 등의 방법으로 결재를 하면 물건 판매자 또는 쇼핑몰 운영자는 입금된 금액을 확인하고 바로 쇼핑몰이나 광고를 낸 사이트를 폐쇄하고 잠적을 한다. 이는 인터넷상 가장 전형적인 사기 범죄의 한 예로 범죄자는 인터넷 쇼핑의 구조적인 특성과 인터넷 환경에서의 익명성을 교묘하게 이용한 것이라 볼 수 있다.

이러한 인터넷상 익명성으로 인한 폐해가 증가하자 이에 대한 대책의 일환으로 인터넷 실명제가 추진되었다.[38] 인터넷 실명제라 함은 인터넷 이용자의 실명과 주민등록번호가 확인되어야만 인터넷 게시판에 글을 올릴 수 있는 제도를 말한다.[39] 이는 인터넷의 역기능을 해소함으로써 인

35) 2007년 7월 미국의 CNN 보도에 의하면, 한국의 인터넷 게시판의 댓글 7개 중 1개가 악성 댓글이라고 하였다.

36) 악성댓글 및 루머로 인한 연예인 자살 등으로 인터넷의 안전성· 유해성의 논란이 증폭되고 있다. 특히 연예인의 자살문제로 故 유니· 정다빈('07.1), 안재환 · 최진실('08.8) 등 악성 댓글은 연예인 자살에 동기를 제공하였다고 한다.

37) 인터넷 사기 발생 건수 2006년 26,711건, 2007년 28.081건(전년도 대비 5.1%↑증가), 2008년 29,290건(전년도 대비 4.3% 증가)으로 해마다 4-5% 정도씩 증가하고 있다.

38) 물론 익명성을 계속 주장하는 의견도 있는데 그 이유는 실명제를 도입하면 스토킹, 개인정보 유출, 인권침해 문제가 더 심각해질 수 있다는 것이다. 또한 익명성은 사회적으로 억압받는 약자와 소수자에게 헌법에서 보장한 표현의 자유를 보장하고 내부 고발자를 보호하기 위한 최소한의 장치이기 때문에 익명성은 보장되어야 한다는 주장이다. 최경진,「인터넷 실명제와 토론문화」, 매일신문, 2007. 7. 4.

39) 2004년 개정된 '공직선거및선거부정방지법' 에 규정된 개념으로 인터넷 언론사의 게시판에 선거에 관한 의견을 게시할 때 게시자의 실명과 주민등록번호의 일치 여부를 확인한 후 의견을 게시할 수 있도록 한 기술적 조치를 말한다. 그러나 인터넷 언론사의 범위에 대한 불명확성, 익명 표현의 자유에 대한 침해, 주민등록정보의 노출에 따른 개인 인권의 침해, 국민의 정치참여 제한 등 여러 가지 문제점이 제기되었다.

터넷 공간의 신뢰를 높이고, 책임 있는 글쓰기를 통해 올바른 여론을 형성하자는 취지에서 나온 것이다. 이에 따라 정부에서는 '인터넷주소자원관리법' 등을 통해 2002년 이후 공공기관이나 인터넷 포털사이트 등의 게시판에 글을 올릴 때는 본인 확인을 거치도록 하는 인터넷 실명제의 도입을 계속 추진해 왔다.

그 결과 인터넷 실명제와는 조금 차이는 있지만, 2007년 7월 28일부터 '제한적 본인 확인제'를 시행하고 있다. 이는 인터넷 이용자가 게시판에 게시물을 올릴 때 본인 여부를 확인해야 하는 제도로, 하루 평균 방문자수가 20만명 이상인 인터넷 언론사와 30만명 이상인 포털사이트, 사용자제작콘텐츠(UCC)[40]에 적용되고 있다. 완전 인터넷 실명제는 실명으로 모든 인터넷 서비스를 이용해야 하는 반면, 제한적 본인 확인제는 실명 이외에 ID, 별명 등을 사용할 수 있다는 차이점이 있다.[41]

나. 비대면성

인터넷 온라인상에서 또 다른 특성은 비대면성으로 이는 앞에서 설명한 익명성과도 관련이 깊다. 비대면성이라 함은 사람들이 사회생활, 경제생활을 영위하면서 일일이 서로 만나지 않아도 된다는 것이다.

인터넷을 통한 전자상거래에서도 판매자와 구매자가 서로 대면할 필요가 없이 물건을 사고 팔 수 있게 되었고, 국제간의 무역거래, 은행업무, 사람들간에 인터넷 메신저(Messenger)[42]를 통해 서로 대화를 하면서 굳

40) UCC(User Created Content)라 함은 사용자가 직접 상업적인 의도없이 제작한 콘텐츠를 온라인상 나타낸 것을 말한다. 미국에서는 일반적으로 창작의 개념이 강조된 UGC(User Generated Content)로 쓰고 있다.

41) 디지털 타임스, 2007. 8. 7일자.

42) 인터넷에서 실시간으로 메시지와 데이터를 주고받을 수 있는 소프트웨어로 인스턴트 메신저라고도 한다. 1996년 미국의 아메리카온라인(AOL)에서 처음 시작하였고, 우리나라에는 1998년 디지토 닷컴이 처음 소개하였다.

이 만날 필요가 없게 되었다. 이러한 비대면성은 편리하고 경제적인 상거래를 가능하게 하고 있지만 반면 쉽게 범죄에 악용되기도 한다. 인터넷 사기의 많은 경우가 직접 대면하지 않는데서 오는 책임의식의 결여와 범행 후 도주가 용이하여 쉽게 범죄로 연결되는 것으로 파악되고 있다. 또한 명예훼손이나 협박과 같은 경우도 얼굴을 서로 마주보면 쉽게 할 수 없는 언행도 비대면성으로 인해 과격해지고 대담해지는 경우가 많다. 또한 인터넷상에서는 확인되지 않은 사실을 받아들이며 이를 전파하고 동조하는 속도가 굉장히 빠르기 때문에 억울하게 명예가 훼손되어 피해자에게 심각한 피해를 입힐 수도 있다. 반면 피해자는 상대방을 볼 수 없기 때문에 더욱 피해의식이나 공포감이 큰 것으로 파악되고 있다. 인터넷에서는 비대면성을 이용하여 자신을 은폐시키고 범죄를 실행하기 때문에 죄의식이 박약해지며 보다 대담하게 행동하기 쉽다는 특성을 가지게 된다.[43] 이런면에서 익명성과도 매우 관련이 깊다.

다. 시간과 공간의 무제한성

인터넷의 또 다른 특성은 시간과 공간의 제약이 없다는 것이다. 최근 인터넷 네트워크에서 행위의 속도는 전파나 빛의 속도보다도 빠르다고 한다. 인터넷을 이용한 범죄행위는 시간제약 없이 24시간 가능하기 때문에 언제나 위험성이 존재한다. 음란물을 전송하거나 바이러스의 제작·유포, 해킹행위 등 인터넷상에서 언제나 손쉽게 범죄행위를 할 수가 있다. 또한 정보통신기술의 발달은 원격으로 인터넷에 접속이 가능케 하였으며, 지구 반대편에서도 실시간으로 같은 공간에서 동시에 대화할 수 있는 화상회의도 가능하게 만들었다. 그리고 인터넷을 이용해 언제든지 본인이 원하는 곳으로 갈 수 있으며, 산업스파이 활동을 위해 남몰래 신

43) 백광훈, 전게서, 41면.

분을 위장하고 외국에 갈 필요도 없고, 다른 회사에 위장 취업할 필요도 없다. 수십 개국의 국경선을 넘나들며 범죄 행위를 할 수도 있다.

이러한 시간·공간의 무제한성으로 인하여 국경 없는 범죄 행위에 대한 입증, 증거수집, 국가간 수사 공조 및 재판관할권 등 새로운 문제점이 등장하였다. 이러한 현상들은 세계 선진 국가도 이러한 문제점을 인식하여, 이에 대한 대책의 일환으로 2001. 11. 23. 헝가리 부다페스트에서 사이버범죄 방지조약(the Convention on Cybercrime)을 체결하였다. 이 조약은 인터넷을 이용한 모든 범죄행위에 대하여 상세한 규정을 두고, 이를 처벌하도록 한 최초의 국제조약이며 '부다페스트조약'이라고도 한다. 이 조약은 유럽연합(EU)의 45개 회원국과 미국 등 의결권 없는 5개 회원국으로 구성된 유럽 평의회(Council of Europe)에서 테러·컴퓨터 해킹·자금세탁 방지·아동포르노[44] 유포 등에 공동 대응하기 위해 만들었다.[45] 이 조약은 국제사회가 사이버 범죄에 공동으로 대처하고 국가간 공조를 긴밀히 하기 위하여 핫라인(hot line)[46] 설치 등이 명시되어 있다. 그리고 컴퓨터 시스템이나 데이터에 대한 불법 접속, 지적재산권 침해, 컴퓨터 바이러스 제작· 유포, 아동 포르노의 배포 등을 범죄행위로

44) 미국은 아동포르노 광고를 하거나 그 광고를 받아보는 것은 연방법(18 U.S.C §2251과 §2252) 상 범죄로 규정되어 있다. 1996년의 아동포르노 방지법(Child Pornography Prevention Act, CPPA)은 아동포르노의 범위를 미성년자가 등장하는 모든 포르노 영상물로 확대하였다. 그 영상물의 출현이 실제로는 미성년자는 아니지만 미성년자처럼 보이거나, 또는 그렇게 광고를 했을 경우에도 아동포르노에 해당된다. 자유언론협회(Free Speech Coalition)에서는 그 법이 위헌이라는 소송을 제기했고, 연방 항소법원에서는 그 법을 위헌으로 판결했다. 2002년 4월 미 연방 대법원은 컴퓨터로 합성하여 아동이 성행위를 하고 있는 이미지 즉, 가상 아동포르노를 금지하고 있는 조항(U.S.C §2256)이 너무 광범위해서 위헌이라는 판결을 내렸다. www.cyber-rights.org.

45) 2006년 7월 26일 미상원 외교위원회(FRC)는 사이버 범죄와의 전쟁을 수행하기 위해 유럽 평의회의「사이버 범죄 방지조약」가입에 찬성하였다. 이에 따르면 참여 국가들간에는 네트워크에 대한 승인을 받지 않은 침입, 웜, 컴퓨터 바이러스 및 아동 포르노 유포 등의 조사와 처벌을 요구할 수 있도록 했다. 그러나 ISP들은 정부기관의 인터넷 검색 및 몰수에 협력해야 하고, FBI는 실시간으로 전자감시를 할 수 있고, 미국 기업은 시스템의 로그나 기타 데이터를 일상적으로 삭제하지 못하게 하는 보존 명령을 받을 수도 있게 돼 있다는 점들이 대표적인 독소조항으로 꼽힌다. 전자신문,「사이버방지조약은 무소불위」, 2006. 8. 8.

46) 1963년 3월 미국의 워싱턴과 소련의 모스크바 사이에 개통된 양국 정부간의 긴급연락용 직통 통신선을 말한다.

규정하고 조약 참가국들이 국내법으로 이를 금지하도록 의무화하였다. 또한 동 조약은 가맹국에 대해서 경찰의 필요에 따라 보존 데이터의 수사, 압수, 비밀리에 행해지는 인터넷 도청, 국경을 넘는 지원, ISP의 기록 보존을 의무화하는 법률을 도입하도록 권고하였다. 이처럼 시간·공간을 넘는 디지털 범죄에 대응하기 위한 국제공조는 2009년 현재에도 계속되고 있다.

라. 고도의 전파성

인터넷은 네트워크로 연결되어 있기 때문에 접근하는 데에 거의 아무런 제약이 없으므로 누구라도 쉽게 해당 정보를 전송, 입수할 수 있는 특성을 가지며 이러한 정보전달이 순식간에 이루어지게 되는 고도의 전파성도 가진다.[47]

인터넷을 통한 고도의 전파성에 대한 대표적인 사례로 1999년 멜리사 바이러스(Melissa Virus)[48]는 불과 4일 만에 미국과 유럽의 수 백개 기업의 컴퓨터 10만대 이상을 감염시켰으며[49], 1년중 단 하루(4. 26)만 발생하는 CIH바이러스(Virus)[50]는 우리나라에서만 수십만대의 컴퓨터에 피해를 입힌 것으로 추정되었다.[51] 이처럼 신속하고 광범위한 전파성에

47) 강동범,「사이버범죄와 형사법적 대책」, 형사정책연구 제11권 제2호, 2000, 71면; 백광훈,「정보통신범죄의 개념과 유형 및 분류」, 사이버범죄연구회 제23회 세미나, 2001. 10. 13면; 윤상균,「사이버 범죄의 특징과 수사방향」, 수사연구, 2000. 6, 16-17면.

48) Melissa Virus는 1999. 2. 26. 유럽에서 처음 발견되었는데, 미국 뉴저지에 사는 David Smith가 유포시킨 컴퓨터 바이러스로, 멜리사는 MS의 빌게이츠의 부인 이름이다. 이는 '긴급메시지' 라는 제목의 전자우편 첨부파일을 클릭 하는 순간 감염되며, 감염된 컴퓨터의 e-mail 주소목록을 이용해 50명의 상대편 주소로 자동 전달되는 방법이다. 인터넷 흑사병으로 표현할 정도로 순식간에 전 세계 컴퓨터로 전파되었다. www.naver.com.

49) 한겨레신문, 1999. 3. 31.

50) CIH바이러스는 개인용 PC에 저장된 데이터를 삭제하거나 본체를 파괴할 수도 있는 바이러스로 1998. 4. 26. 대만인 첸잉하오가 만들었다. 우크라이나의 체르노빌 원전사고 13주년에 맞추어 출연하도록 고안됐다. 이는 전세계를 휩쓸어 약 60만대의 컴퓨터에 피해를 준 것으로 언론은 집계하였다. www.naver.com 이하 참조.

따라 범죄피해가 무한정 확산될 수 있으며, 컴퓨터 운영체계에 대한 완벽한 보안조치가 이루어지지 않는 경우 비밀의 누출이나 시스템의 파괴 등이 가능해진다. 위의 사례처럼 디지털 범죄의 강력한 전파성은 결국 국가 또는 개인에게도 엄청난 재산적 피해를 주고 있다.

마. 정보의 집약, 정보전달의 신속성

인터넷이 발달하면서 각종 정보는 대형 DB(Database)에 집중관리 되고 있으며 정보의 전달도 신속하다. 한 예로 현재 주요 언론사에서 운용하고 있는 홈페이지의 인물정보란을 보면 사회 저명인사들의 프로필이 저장, 입력되어 제공되고 있다. 지난 신문기사를 찾기 위해 신문사 및 도서관을 뒤지며 돌아다닐 필요도 없이 DB에 저장된 자료를 이용하여 바로 찾을 수 있다. 또한 네티즌이라면 누구라도 인터넷 신문을 통해서 기자들이 쓴 기사를 즉각적으로 받아 볼 수도 있다.

이처럼 정보의 집약과 정보전달의 신속성은 순기능적인 면에서는 우리에게 신속하고 정확한 정보를 제공하지만, 이렇게 집약된 개인정보들이 해킹 등을 통해 범죄행위에 이용된다면[52] 이로 인한 국민 개개인의 피해는 당연히 증가할 수 밖에 없을 것이다. 과거에는 개인정보 침해가 주로 국가나 공공기관에서 운용하는 대형 DB에서 발생하였으나, 현재는 어느 누구나 인터넷만 사용할 줄 알면 쉽게 집약되어 있는 개인정보를 수집할 수 있고, 이를 상업용으로 판매하는 사건도 자주 발생하고 있다.[53] 특히 기업들은 고객의 상세한 개인정보를 입수하여 무단으로 도

51) 동아일보, 1999. 4. 27.

52) 이에 대한 최근의 한 사례로 2008년 2월 「옥션」고객 1,081만명 개인정보가 해킹을 당하여 유출이 되었다.

53) 2004년 10월에는 인터넷을 통하여 637만명의 개인정보를 매매한 자들을 사이버 수사대에서 검거하였다. 동아일보, 2004. 10. 14; 2007년 2월에는 금융감독위원회 산하 '불법대부광고 사이버감시단'에서 인터넷에 개인신용정보를 판매한 업자들을 수사기관에 통보하여 검거하

용하기도 하며, 특히 보안시설이 취약한 인터넷 쇼핑몰의 경우에는 해킹이나 도청과 같은 범죄행위에 의하여 집약된 고객의 개인 신용정보 유출의 위험성이 높다.[54]

위에서 설명한 인터넷 공간에서의 디지털 범죄의 특성은 수사기관이 디지털 범죄를 수사하는데 많은 어려움이 되는 주된 이유이다. 또한 범죄를 증가하게 하는 원인이 되기도 하며, 다양한 신종 범죄를 야기하게 만든다. 이러한 디지털 범죄의 특성으로 인하여 최근에는 UCC에 의한 음란물 제작·유통 또는 은밀한 사생활을 담은 동영상이 인터넷을 통해 공공연히 전파되고 있다. 더불어 목욕탕, 화장실, 모텔과 같은 곳에 설치된 몰래 카메라에 의해 제작된 동영상이 인터넷에 유포되어 사생활 침해 및 초상권 침해 등 돌이킬 수 없는 인권침해를 발생시키고 있어 앞으로 인터넷 공간에서의 인격권 보호문제도 심도 있게 논의되어야 할 것이다.

2. 디지털 범죄의 유형

디지털 범죄는 한 가지 수법에 의한 범행보다는 여러 가지 수법이 결합된 형태로 범죄 행위가 일어나는 경우가 많다. 예를 들면 해킹의 경우 단순 침입, 사용자 도용, 파일의 삭제· 변경, 폭탄 스팸메일, 자료유출 등의 다양한 수법이 결합되어 해킹을 하며 또한 바이러스의 유포, 사기, 프로그램의 불법복제, 개인정보침해 등의 방법들이 결합된 형태로 범죄 행위가 일어나는 경우가 많아 그 유형을 구분하기가 매우 곤란하다.[55]

였다. 한국정책방송(KTV), 2007. 2. 21 방송 참조.

54) 2007년 8월 KT와 하나로 텔레콤이 인터넷 가입 고객 730만명의 개인정보를 무단 도용, 돈을 받고 제3자에게 유출하였다. 고객의 신용정보를 유출한 것은 결국 범죄단체의 손에까지 흘러가 제2·3 범죄를 일으키고 있다. 이런 고객정보 유출 실태는 카드회사, 게임업체, 대출정보회사 등 모든 업종에서 일어나고 있다. 매일경제신문,「기업들 도를 넘는 개인정보 유출」, 2007. 8. 9.

55) 조병인 외3,「사이버범죄에 관한 연구」, 한국형사정책연구원, 2000, 27면.

현재 디지털 범죄의 유형을 구체적으로 구분한 규정이나 근거가 없어 이를 구체적으로 분류하기에는 매우 어렵다고 할 수 있다.[56]

경찰청 사이버테러대응센터에서는 디지털 범죄를 다음과 같이 분류하고 있다.[57] 디지털 범죄를 크게 과거 현실세계의 범죄가 단지 컴퓨터 시스템을 이용한 형태의 일반화된 디지털 범죄와 사이버 공간 고유의 범죄 즉, 대규모 피해를 야기시키는 해킹, 바이러스 제작· 유포 등의 사이버 테러형 범죄로 구분하고 있다.

사이버 테러[58]라 함은 인터넷 네트워크 공간에서 수행, 계획, 조정되는 테러를 의미한다. 여기에는 폭력적 행위에 대한 정보를 공유하기 위해 e-mail로 정보를 주고 받는 것과 웹 사이트를 통해 테러리스트를 모집하는 등의 행위를 모두 포함한다. 그리고 항공 제어 컴퓨터 시스템을 파괴해서 비행기를 서로 충돌하게 하거나, 상수도 컴퓨터 시스템을 공격해서 물을 오염시키는 것, 병원 데이터베이스(DB)를 해킹해서 환자들에 대한 정보를 수정·삭제함으로써 환자들에게 잘못된 처방을 하게 하는 것, 전력 장치를 파괴함으로써 인공 호흡장치를 사용하고 있는 사람이 숨을 쉬지 못하게 하는 것 등을 사이버 테러에 포함하고 있다.[59]

디지털 범죄의 유형에 대하여 국가나 학자의 견해에 따라 다양한 기준으로 분류하지만, 이 논문에서는 경찰청의 분류기준에 따라 범죄 유형을 분류하고자 한다.

---

56) 제10차 UN회의에서는 디지털 범죄를 2가지로 분류하여 정의하고 있다. 좁은 의미로는 컴퓨터 시스템의 보안과 컴퓨터 시스템에서 처리하는 데이터를 대상으로 한 범죄행위라고 하며, 넓은 의미로는 컴퓨터 시스템 또는 네트워크와 관련된 모든 위법행위로 시스템이나 네트워크를 사용해서 정보의 유출, 유출정보의 타인 제공·배포하는 행위가 포함된다. Debra Littlejohn shinder(강유 譯), 前揭書, 17면; www.uncjin.org/Documents.

57) 경찰청, 사이버테러대응센터 홈페이지, www.ctrc.go.kr. 이하 참조.

58) 미국 국무부에서는 테러를 '계획적이고 정치적인 목적에 의해 비밀 그룹이나 요원이 전투능력이 없는 대상에 가하는 폭력행위'로 정의하고 있다.

59) Debra Littlejohn shinder(강유 譯), 前揭書, 19면.

가. 일반화된 디지털 범죄

사이버상에서 일반화된 디지털 범죄의 대표적인 분류의 예는 아래와 같다.

① 전자상거래 사기 또는 인터넷 사기로 인터넷을 통하여 물건을 賣買하는 과정에서 발생하는 범죄로 초고속 인터넷의 보급이 확대됨에 따라 그 규모는 날로 증가하고 있다. 인터넷으로 주문에서 결제, 배송까지 확인 할 수 있는 편리성 때문에 인터넷 쇼핑몰의 이용자들이 급증하는 추세이다. 앞서 디지털 범죄의 특성부분에서도 익명성을 이용한 인터넷 사기를 설명하였듯이 현재 다양한 형태의 인터넷 사기 사건이 증가하고 있다.[60] 특히 최근에는 10대 청소년들 사이에서 주로 발생하는 게임사기가 해마다 증가하고 있다. 인터넷 게임인구가 늘어나고 게임시장이 확대됨에 따라 게임사이트에서 실제 현금으로 게임머니를 충전해 주거나 인터넷 온라인상에서 통용되는 게임머니나 게임아이템 등이 실물처럼 거래되고 있다. 이처럼 게임머니나 아이템을 거래하기로 하는 과정에서 사기피해의 발생이 증가하고 있다.[61] 인터넷 게임에 관련된 사기는 일반화된 디지털 범죄중 경찰청에 가장 많은 신고접수가 되는 사례이며, 요즘의 청소년의 인터넷 게임 사기문제는 자살, 폭행의 결과로 이어지는 등 문제가 심각하게 제기되고 있다.

② 불법복제행위로 이는 저작권법 및 컴퓨터프로그램보호법상의 창작물에 대한 저작권을 침해하는 범죄 행위이다. 인터넷의 발달로 불법복제(illegal copy)가 쉬워지면서 과거 오프라인에서 거래되던 컴퓨터프로

60) 2007년도 8월 광주경찰청 사이버 수사대의 통계에 의하면 사이버 범죄 74%가 10-20대이며, 그 중 인터넷 상품매매로 인한 사기가 68%, 인터넷 게임 아이템을 이용한 사기가 25%나 차지하여 전체 93%가 인터넷 사기를 차지하고 있다. 국민일보, 2007. 8. 17.

61) 2006년 전북지방경찰청 사이버 수사대의 통계에 의하면 10대의 사이버 범죄 85%가 통신·게임 사기라고 하였다. 연합뉴스, 2006. 2. 1.

그램·영화·음반 CD 등의 불법복제물들이 최근에는 인터넷을 이용하여 유포되거나 판매되는 것이 증가하고 있다. 특히 소프트웨어의 불법복제를 막기 위하여 회사마다 불법복제방지 시스템을 구축하고 있으나 이를 완벽하게 막을 수 있는 방법이 없거나, 완벽하게 방지하면 소비자의 프로그램 사용이 불편하게 되므로 불법복제를 근절시키기가 어렵다. 소프트웨어의 불법복제는 도덕적인 문제일 뿐만 아니라 소프트웨어 산업 발전의 큰 저해요인이 되고 있다.[62] 또한 자신의 컴퓨터에 관련 프로그램만 설치하면 동일한 프로그램을 사용하는 다른 사람의 컴퓨터에 보관되어 있는 자료를 공유할 수 있는 P2P(peer to peer)[63] 방식의 인터넷 자료공유 서비스가 확산되면서 자료공유를 원하는 네티즌들 사이에 범죄의식 없이 불법복제된 컴퓨터 프로그램이나 영화 및 음악들이 유포되고 있다.

현재 이러한 불법복제 행위로 인한 문제점을 해결하기 위한 일환으로 정부는 저작권법을 시행하고 있다. 동 법은 저작권 산업 보호를 위하여 불법파일 다운로드를 막는 필터링 장치를 설치·운영하지 않는 온라인서비스제공자(OSP)에 대해 최고 3,000만원의 과태료를 부과하고 있다.

③ 불법·유해사이트를 운영하는 행위로 공공의 안녕·질서 또는 미풍양속을 해하는 등 반사회적 내용을 담고 있는 사이트 개설로 목적 자체가 법률에 위반되거나 범죄수단으로 사용되는 위법사이트를 포함하는 범죄이다. 특히 자살사이트나 마약거래 사이트, 위조 졸업장 및 각종 자격증 등을 만들어주는 증명서 관련 사이트, 청부살인이나 폭력을 의뢰하는 사이트까지 생겨나 인터넷으로 정보를 주고받음으로써 오프라인 범죄의 모

62) 이러한 불법복제는 컴퓨터프로그램 보호법 제29조, 제46조에 근거하여 프로그램의 지적재산권을 침해하는 경우에는 5년 이하의 징역, 5천만원 이하의 벌금형이 적용된다.

63) P2P(Peer to Peer)이라 함은 인터넷을 통해 각자의 컴퓨터 안에 있는 음악·문서·동영상 파일 등을 공유할 수 있게 해주는 기술을 말한다. PC와 PC를 직접 연결해 서버 없이도 인터넷에 접속한 개개인의 PC를 직접 검색, 저장된 자료를 1:1로 주고받는 방식이다. 이러한 서비스로 대표적인 것이 음악파일(MP3)들을 인터넷을 통해 공유할 수 있게 해주는「냅스터(Napster)」, 국내의「소리바다」등이 있다. www.naver.com. 이하 참조.

태가 되기도 한다. 인터넷 공간에 이러한 유해정보를 제공하는 것은 청소년이나 기타 일반 네티즌 등에게 범죄의 유혹을 제공함으로써 결과적으로는 범죄를 양산시키는 원인이 된다.

④ 인터넷을 통한 명예훼손에 관한 범죄로 이는 인터넷 게시판에 타인의 명예를 훼손하는 글이나 사진 또는 동영상 등을 게시하거나 전자우편, 메신저 등을 통해 유포하는 범죄행위를 말한다. 인터넷의 특성상 인터넷 게시판 등에 명예훼손 내용이 일단 게재되면 시·공간의 제한 없이 단시간내에 급속도로 유포될 수 있기 때문에 그로 인한 피해가 심각하다. 이러한 이유로 정보통신망이용촉진및정보보호등에관한법률 제70조에서는 인터넷상에서의 명예훼손죄를 형법 제307조의 명예훼손죄보다 더 무겁게 처벌하도록 규정하고 있다.[64]

⑤ 최근 대규모의 개인정보유출 및 오· 남용 등 개인정보침해 사건이 사회의 큰 이슈로 자주 등장 함에 따라 국민 대다수의 사회적인 관심은 과거의 어느 때보다도 개인정보의 보호에 대한 필요성을 절실히 인식하게 되었다. 정보통신의 발달에 따른 유비쿼터스 기술은 우리 사회 전체에 급속도로 전파되고, 더불어 디지털 기술에 의해 수집된 정보의 유통은 빠른 속도로 확대되고 있어 개인정보의 유출 가능성도 빠르게 증대하고 있다.

개인정보침해 범죄의 심각성은 단순히 개인정보가 유출된 것으로 끝나는 것이 아니라 유출된 개인정보가 다른 범죄에 사용될 수 있다는 것에 있으며 이러한 개인정보는 범죄의 표적이 되고 있다. 현재 우리 사회는 금융·교육·행정·쇼핑 등 생활 전반이 인터넷을 통해 이루어지고 있다. 따

64) 형법상 명예훼손에 관한 죄는 사실 유포의 경우 2년이하, 허위사실을 유포한 경우는 5년이하의 징역에 처하지만, 인터넷을 통한 명예훼손에 관한 죄는 사실 유포의 경우 3년이하, 허위사실을 유포한 경우는 7년이하의 징역에 처하고 있다. 이는 인터넷의 특성인 시·공간적 무제한성, 고도의 신속성과 전파성 등으로 인해 현실세계에서의 발생되는 명예훼손보다 훨씬 큰 피해를 줄 수 있기 때문에 형법규정보다 그 형을 무겁게 한 것이다.

라서 인터넷에서 개인의 성명·주민등록번호·주소 및 전화번호 등과 같은 개인정보의 중요성은 점점 커지고 있다. 개인정보는 재화로서의 가치를 갖고 유통되기도 하기 때문에 법에서는 정보통신서비스제공자가 이용자의 동의 없이 개인정보를 수집하는 경우나 개인정보를 취급하거나 취급하였던 자가 개인정보를 타인에게 누설하거나 제공하는 경우 등과 같은 조직적인 개인정보침해행위도 규제하고 있다.[65]

⑥ 스토킹(Stalking)에 관한 범죄로 이는 상대방 의사와 상관없이 의도적으로 계속 따라다니면서 편지, 전화, 팩스, 미행, 감시, 집과 직장 방문 등을 통하여 정신적·신체적 피해를 반복적으로 주는 행위라고 정의할 수 있다. 최근에는 인터넷을 이용하여 게시판, E-mail, 메신저, 문자 등 정보통신망을 통하여 상대방이 원하지 않는 접속을 지속적으로 시도하거나 욕설, 협박, 모욕 등의 내용을 지속적으로 송신하는 행위를 말한다. 우리나라에서는 현재까지 사이버스토킹을 범죄로 규정하지 않고 사이버 성폭력의 한 사례로 분류하고 있으나, 외국에서는 사이버 스토킹을 독립된 하나의 범죄로 중요하게 취급하고 있다.[66]

현재 정보통신망을 통하여 스토킹을 하는 행위에 대한 처벌조항으로는 정보통신망법 제44조의7(불법정보의 유통금지 등) 제1항의 3호, 제74조 제1항 3호로 “정보통신망을 통하여 공포심이나 불안감을 유발하는 말·

---

65) 이러한 추세에 부응하여 행정안전부는 2008년에 들어와 적극적으로 개인정보보호 강화라는 국민의 시대적인 요구를 반영하고자 개인정보보호에 관한 법률을 제정하기에 이르렀다. 2009년 5월 말 현재 국회에 계류중에 있다. 이 법률 안은 공공기관 및 민간기관 등을 포괄적으로 규율하는 개인정보보호의 원칙과 이에 대한 처리기준을 정립함으로써, 개인정보의 활용을 보장하고 부당한 침해로부터 정보주체의 권익을 보호하는 것을 목적으로 하고 있다. 이를 위해 개인정보의 수집·이용·제공 등의 처리기준 정립, CCTV 등 영상정보처리기기의 설치·운영의 제한, 정보주체의 열람·정정·삭제 요구권 보장 등을 규정하여 국내 개인정보보호 법제의 획기적인 전환점이 되고자 하였다.

66) 미국은 1990년 California 州를 시작으로 모든 주가 스토킹 법을 제정했고, California 州法 제646.9조에서 “의도적이고 악의를 가지고 타인에 대해 반복적으로 추근대거나 괴롭히는 것(willfully, maliciously and repeatedly following and harassing of another person)”이라 스토킹을 정의하고 있다. 1998년 제정된 연방 스토킹법은 사이버스토킹도 처벌대상에 포함시켰다. 일본은 2000. 5. ‘스토커행위등의규제에관한법률’이 제정되었다.

음향·글·화상 또는 영상을 반복적으로 상대방에게 도달하게 한 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다"고 규정하고 있다. 그러나 최근 우리나라도 스토킹에 대한 범죄가 증가되고 있는 실정이며 이에 대하여 구체적인 입법이 절실히 요구된다.

나. 사이버테러(Cyber Terror)형 범죄

현재 정보통신 시스템은 행정, 금융, 산업, 교통, 군사, 의료 분야 등 국가사회 전반에 보급되어 활용되고 있다. 따라서 이 정보통신 시스템의 기능을 마비시키거나, 파괴, 무력화시키는 것은 개인, 기업 뿐 아니라 국가적으로 엄청난 손상과 피해를 입히고, 국가의 안위도 위협을 받게 된다.[67]

사이버테러라 함은 최첨단 정보통신기술을 이용해 정보통신망 자체를 공격의 대상으로 하여 파괴하는 불법행위를 말한다. 즉, 해킹, 바이러스 제작· 유포, 메일폭탄 등을 이용하여 컴퓨터 시스템과 정보통신망을 공격하는 행위를 말한다.

사이버테러의 대상은 개인적인 자산의 손실과 사생활의 침해를 주는 개인적인 테러[68]와 기업이 운영하고 있는 정보시스템의 파괴나 기능마비 등을 통해 기업이 소유하고 있는 기술, 회계정보 등의 유출로 피해를 주는 기업테러가 있다. 마지막으로 사이버테러의 위험도가 가장 높은 것이 국가에 대한 사이버테러이다. 이는 국가간 또는 국제적인 차원에서 행해지는 테러로써 인터넷을 이용하여 통제도 없고, 국경도 없이 이루어

67) 이에 대한 대표적인 사례가 2001. 9. 11 테러로 당시 테러리스트들이 플로리다의 공공 도서관에서 테러에 필요한 자료 조사와 도서관 컴퓨터를 이용하여 E-mail 교신을 통해 9. 11 테러를 모의하였다.

68) 이는 금융정보나 신용카드, 보험, 납세, 자동차등록자료 등 개인정보에 관한 절도, 변조, 파괴, 유출, 삭제 등을 통한 사생활 침해를 의미한다.

지는 테러이기 때문에 그 피해정도가 사회경제 질서를 붕괴시킬 수 있는 정도로 규모가 크다고 할 수 있다.[69]

우리나라의 사이버테러 대응체계는 국가정보원이 총괄 지원하고 국방부가 국방 정보통신을 담당하고, 방송통신위원회가 민간 방송통신을 담당하는 등 각 분야별로 예방 및 대응체계를 구축· 운영하고 있다.[70]

또 경찰청, 검찰청 등이 각각의 사이버테러 대응 업무를 수행하고 있다. 그리고 국가 차원의 종합적이고 일원화된 대응체계를 위해 2004년 2월 '국가사이버안전센터'가 본격 가동에 들어갔다.[71]

사이버테러형 범죄로 대표되는 것이 해킹과 바이러스 제작· 유포이다. 첫째, 해커에 의한 해킹은 일반적으로 다른 사람의 컴퓨터 시스템에 무단 침입하여 정보를 절취하거나 프로그램을 파괴하는 전자적 침해행위를

69) 대표적인 예로 1990년 걸프전에서 미국이 이라크 방공망에서 바이러스를 유포시켜 방공 시스템을 교란시켰던 경우와 1999년 코소보 전쟁에서 유고가 나토는 물론 미국과 영국에 해커를 침입시켜 백악관과 국방부 전산망을 다운시킨 것은 물론 영국 기상국을 마비시켜 나토의 공습에 필요한 기상정보의 전달을 막아 공습이 취소되는 전과를 올렸던 경우 등을 들 수 있다. 南孝淳·丁相朝, 前揭書, 156면.

70)

부처별	대응분야	보호 기관
국정원	공 공	국가기관·공공기관 및 안보관련시설 사이버침해 대응
행안부	행 정	전자정부통신망, 정부통합전산센터, 지방자치단체(246개)
국방부	국 방	국방부 및 각 군 침해사고 대응
외교부	외 교	해외공관(153개)
국토부	국토해양	국토해양부, 소속기관(13) 및 산하기관(16)
복지부	보건의료	국·공립병원 등(65개)
교과부	교육·연구	시·도교육청(16개), 과학기술분야 연구기관(33개)
지경부	에너지	한국전력 등 산하기관(28개)
방통위	방송통신	방송 및 정보통신망
금융위	금 융	은행(18개), 증권사(16개)
경찰청	치 안	경찰청·지방경찰청(89개)

71) 국가사이버안전센터의 역할은 사이버테러 감시, 예방, 경고이며 국가기관의 정보통신망을 직접 모니터링 하는 동시에 국내·외 사이버보안 또는 침해사고 대응기구들과 협력해 각종 위협정보를 종합적으로 분석하고 공격징후를 탐지해 각 기관에 안전대책을 제공하고 있다. 국가정보원, www.ncsc.go.kr 參照.

의미한다.[72] 해킹은 사용하는 기술과 방법 및 침해의 정도에 따라서 다양하게 구분된다. 경찰청에서는 해킹에 사용된 기술과 방법, 침해의 정도에 따라서 단순침입, 사용자 도용, 파일 등 삭제·변경, 자료유출, 폭탄·스팸메일, 서비스 거부공격으로 구분하고 있다.[73]

우선 해킹에 관하여 먼저 살펴보면, ① 단순침입이란 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입 하는 것을 말하며, 여기서 '접근권한' 이라 함은 '행위자가 해당 정보통신망의 자원을 임의로 사용할 수 있도록 하는 권한' 을 말한다. '정보통신망에 침입한다' 란 의미는 '행위자가 해당 정보통신망의 자원을 사용하기 위해서 거쳐야 하는 인증절차를 거치지 않거나 비정상적인 방법을 사용해 해당 정보통신망의 접근권한을 획득하는 것, 즉 정보통신망의 자원을 임의대로 사용할 수 있는 상태가 되었을 때 침입이 이루어진 것이라고 할 수 있다.

② 사용자 도용이라 함은 '정보통신망에 침입하기 위해서 타인에게 부여된 사용자계정과 비밀번호를 권한자의 동의없이 사용하는 것을 말한다. 개념상으로는 단순침입의 한 가지 유형이지만, 사용자 도용이 많은 부분을 차지해 별도로 구분하였다.

③ 파일 등 삭제와 자료유출로 이는 정보통신망에 침입한 자가 행한 2차적 범죄 행위로 일반적으로 정보통신망에 침입행위가 이루어진 뒤에 가능하다.

④ 폭탄메일이라 함은 '메일서버가 감당할 수 있는 한계를 넘는 다량의 메일을 일시에 전송하여 전산망에 장애를 발생시키거나 메일 수신자의 PC에 과부하를 일으킬 수 있는 실행코드 등을 삽입하여 전송하는 것으로 서비스거부공격(Dos: denial of service attack)[74]의 한 유형이다.

---

72) 컴퓨터에 미친 사람을 뜻하던 것이 정보통신의 발전에 따라 타인의 컴퓨터 시스템에 접근하여 프로그램이나 정보를 훔쳐가는 사람들로 그 의미가 바뀌었다. 김강호,「해커의 사회학(해커를 해킹한다)」, 개마고원, 1997. 9 26면.

73) CTRC, www.ctrc.go.kr 이하 참조.

⑤ 스팸메일은 상업적인 내용의 메일을 불특정 다수에게 전송하는 것으로 쓰레기나 다름없다고 하여 정크메일(junk mail)이라고 한다. E-mail이 광고의 주요한 수단으로 부상하면서 이를 이용한 상업적인 목적의 광고가 많이 늘어나고 있다. 특히 기업광고, 특정인 비방, 음란물 및 성인사이트 광고, 컴퓨터 바이러스 등을 담은 이메일을 대량으로 발송하여 사회적인 문제를 일으키고 있다.

다음으로 사이버테러의 또 다른 유형으로 바이러스 제작· 유포를 살펴보겠다. 바이러스 또는 악성프로그램 이란 일반적으로 컴퓨터 바이러스 또는 인터넷 웜(worm)[75]을 의미하며 '정보시스템의 정상적인 작동을 방해하기 위하여 고의로 제작· 유포되는 컴퓨터 프로그램'이다. 보통 각자의 특징에 따라 컴퓨터 바이러스, 웜, 트로이 목마[76] 등으로 구분하고 있으며 법에서 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조 또는 그 운용을 방해할 수 있는 프로그램을 악성프로그램으로 규정하고 이를 유포하는 행위에 대하여 처벌하고 있다.[77]

이상과 같이 경찰청에서 분류하는 디지털 범죄의 유형을 살펴보았다. 이외에도 디지털 범죄의 유형을 ① 사이버스페이스의 범죄(컴퓨터중심범죄, 네트워크범죄 혹은 사이버스페이스 범죄)와 ② 실정법상의 범죄(형법상의 범죄, 특별법상의 범죄)로 대별한 사례도 있으나, 사실 큰 차이는 없다.

---

74) 서비스거부공격(Dos: denial of service attack)이란 '정보통신망에 일정한 시간 동안 대량의 데이터를 전송시키거나 처리하게 하여 과부하를 야기시켜 정상적인 서비스가 불가능한 상태를 만드는 일체의 행위'를 말한다.

75) Worm은 '컴퓨터에 근거지를 둔 지렁이와 같은 기생충' 이라는 뜻의 부정 프로그램으로 컴퓨터 바이러스와는 달리 다른 프로그램을 감염시키지 않고 자기 자신을 복제하면서 통신망 등을 통해 널리 퍼진다.

76) 프로그램에 미리 입력된 기능을 능동적으로 수행하여 외부의 해커에게 정보를 유출하거나 원격제어로 기능을 수행하여, 트로이목마처럼 유용한 유틸리티로 위장하여 확산되기 때문에 감염사실을 알아채기 어렵다.

77) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제71조 제9호에서 '악성프로그램을 전달 또는 유포한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다'고 규정하고 있다.

제3장 디지털 범죄 수사에서 적법절차에 의한 영장주의

제1절 신체의 자유 보호를 위한 절차적 보장

1. 신체의 자유 발달과 의의

신체의 자유는 근대헌법이 보장하는 가장 기본적인 자유로서 모든 사회적·경제적·정신적 자유의 근간이 되는 것이며, 신체의 자유[78]는 개인의 자유와 권리를 향유하기 위한 원시적 권리로서 인간의 존엄과 민주주의의 존립을 위한 최소한의 조건이기도 하다. 신체의 자유에 관한 보장은 영국에서 1215년 Magna Carta에서 비롯하여 1628년의 권리청원을 거쳐 1679년 Habeas Corpus Act,[79] 1689년의 권리장전에 의하여 완성되었다. 미국의 Virginia 권리장전과 연방헌법, 그리고 프랑스의 인권선언에서도 이를 선언하고 있다. 제2차 세계대전 후의 헌법은 거의 예외없이 기

78) 헌법 제12조에서「모든 국민은 신체의 자유를 가진다」고 하고 있는데, 여기에서 신체의 자유가 무엇인가가 문제가 되는데, 헌법 제10조·제36조 3항과 관련하여 볼 때 독일과 같이 신체의 자유는 신체활동의 자유만을 뜻한다고 할 것이다. 이에 대하여 丘秉朔 교수는 신체의 자유에는 생명의 자유, 신체안전의 자유, 신체자율의 자유가 포함된다고 본다(丘秉朔,「新憲法原論」, 博英社, 1989, 467면). 權寧星 교수는 생명권과 신체를 훼손당하지 않을 권리가 헌법 제10조와 제12조 1항 그리고 제37조 1항에 의하여 보장되는 것으로 보고, 이를 신체의 자유와 함께 人身의 자유에 포함시키고 있다. 權寧星,「憲法學原論」, 法文社, 2007. 2, 412면.

79) habeas corpus 제도는 영국의 보통법에서 발전되어 1679년의 Habeas Corpus Act에 의하여 확립되었다. 이 제도는 그 후 미국헌법에 규정되었고, 일본에서도 人身保護法으로서 도입되었다. 우리나라에서는 1948년 미군정법령 제176호에 의하여 구속적부심사제도로 도입되어 제3공화국에 규정되어 오다가 제4공화국 헌법에서 삭제되었던 것을 제5공화국 헌법에서 부활시켰고, 제6공화국 헌법에서는 법률유보조항을 삭제하여 그 범위를 확대하여 보장하고 있다. 金哲洙, 前揭書, 471면.

본권으로서 신체의 자유를 규정하고 있다.[80]

헌법재판소는 신체의 자유에 대하여「정신적인 자유와 더불어 헌법 이념의 핵심인 인간의 존엄과 가치를 구현하기 위한 가장 기본적인 자유로서 모든 기본권 보장의 전제 조건이다」라고 판결하고 있다.[81] 이를 정리하면 신체의 자유라 함은 법률과 적법절차에 의하지 아니하고는 신체의 안전성과 자율성을 제한 또는 침해당하지 아니하는 자유를 말한다고 할 수 있다.

2. 신체의 자유의 내용

현행 헌법은 신체의 자유를 제12조에서 상세히 규정하고 있는데, 제1항에서는 죄형법정주의와 체포·구속 등의 법률주의와 적법절차, 제2항에서는 고문금지와 묵비권의 보장, 제3항은 영장제도와 적법절차, 제4항은 변호인의 조력을 받을 권리, 제5항은 체포 또는 구속의 이유 등을 고지받을 권리, 제6항은 구속적부심사제, 제7항은 자백의 증거능력의 제한을 각각 규정하고 있다.

이 헌법 제12조 3항의 규정에 근거하여 컴퓨터 또는 디지털 저장장치에 있는 정보나 자료를 압수· 수색함에 있어서는 적법한 절차[82]에 따라 영장을 제시해야 한다. 컴퓨터 또는 디지털 저장장치에 보관되어 있는 자료, 정보 및 프로그램을 수사상·재판상 증거로 활용하기 위해서는 그 자료 및 프로그램이 저장되어 있는 디지털 기록을 직접 증거로 사용할 수도 있지만, 일반적으로는 조서재판이 중심이 되고 있는 우리나라의 형

80) 金哲洙, 上揭書, 437면.

81) 憲裁 1992. 4. 14. 선고, 90 헌마 82, 憲裁判例集 第4券, 194면 이하 (206면).

82) 適法節次라는 용어가 처음으로 사용된 것은 Edward 3세 하에서 제정된 1354년의 법률 제29장으로 그 조항의 내용은 "누구든지 그 지위나 환경을 묻지 않고 적법절차에 의한 심문을 받음이 없이는 토지나 가정으로부터 추출 또는 수용 당하지 아니하며, 투옥·상속권의 박탈 또는 사형을 당하지 아니한다" 고 선언하였다. 따라서 영국에서 14세기까지는 어느 정도 군주에 의한 자의적 지배를 배제하고 일정한 신체적 자유를 누리 수 있게 되었다. 尹明善, 前揭書, 10면.

사재판 실무관행에 비추어 이를 프린트를 통해 인쇄하여 가시적인 형태의 문서로 변형시켜 제출해야 할 것이다. 이처럼 컴퓨터나 디지털 기기들에 저장된 자료 기타 디지털 증거들을 압수· 수색함에 있어서도 헌법 제12조 3항의 영장주의와 형사소송법 제215조의 강제처분 법정주의의 원칙이 적용되어야 한다는 점에 대하여는 이론이 있을 수 없다.[83]

우리 헌법 제12조 ③은 "압수· 수색을 할 때에는 적법한 절차에 따라 영장을 제시해야한다" 고 규정하고 있는데 컴퓨터 관련 증거 및 기타 디지털 증거에 관한 압수· 수색에 관해서는 당연히 헌법 제12조의 규정에 의거 영장주의 요청에 따라 범죄를 명시한 정당한 이유와 수색장소, 압수 대상물 등이 영장에 명시되어야 하는데 컴퓨터 관련 디지털 증거에 관한 압수방법과 대상의 특정이 가능한가 하는 점에서 몇 가지 특수한 문제점이 제기된다.

첫째는 컴퓨터와 관련된 디지털 증거 자체는 무체정보에 해당한다고 할 수 있는데 이러한 무체정보인 데이터에 대한 압수가 가능한가 하는 문제이고, 둘째는 이러한 디지털 증거들을 압수· 수색하기 위해서 헌법과 형사소송법상 적법절차에 의한 영장주의의 원칙이 어떻게 적용될 수 있는가 하는 문제이다.

셋째는 데이터에 대한 압수· 수색의 범위와 관련된 요증사실과의 관련성 요건, 압수· 수색의 물리적인 범위, 넷째는 컴퓨터에 입력된 자료 및 기타 디지털 증거를 출력하기 위해 압수· 수색영장과는 별도로 영장이 필요한지 여부 및 압수· 수색영장에 의해 컴퓨터 관련증거의 보관자에게 그 자료의 출력을 강제할 수 있느냐 하는 문제 등이 제기될 수 있다.[84]

이러한 문제들을 해결함에 있어 전통적인 형사소송법 규정을 무리하게

83) 吳奇斗, 前揭論文, 70면.
84) 安富 潔,「刑事手續とコンピュータ 犯罪」, 慶應義塾大學 法學硏究會叢書(52)(平成 4年, 1992. 2. 20), 62면.

유추해석하여 적용하려는 태도는 지나치게 안이한 법해석이며 위험한 생각이라고 말할 수 있다. 왜냐하면 형사소송법은 형법과 더불어 피의자와 피고인의 시민적 자유를 보장하는 마그나 카르타이어야 하기 때문이다. 또한 수사기관의 강제력 사용에 관한 형사소송법 규정을 검토 없이 마음대로 유추해석 하는 것은 개인의 자유를 침해할 뿐만 아니라 형사소송법에 의한 시민의 자유제한과 새로운 강제처분의 허용여부는 국회가 결정해야 한다는 권력분립의 원칙에도 반하는 태도이다.[85]

3. 적법절차

가. 적법절차의 개념

적법절차의 기원은 1215년 영국의 대헌장에서 비롯되었으며,[86] 대헌장이 제정될 당시 제39장에서 '국가의 법' (law of the land)에 의하지 아니하고는 체포·구금당하지 아니하며, 재산·법익을 박탈당하지 아니하며, 추방당하지 아니한다고 선언하였다.[87] 여기에서는 적법절차 대신 국가의 법이란 용어를 사용하였고, 적법절차에 관한 명문 규정은 없었다. 그러나 분명히 대헌장 제39조의 주된 목적은 어떠한 자유인도 형집행 이전의 재판, 동료에 의한 재판, 그리고 영국법에 따른 재판에 의하지 아니하고는 생명, 자유, 재산을 박탈당하지 아니한다는 것을 확인하는데 있었다.[88] 17세기에 들어서면서 적법절차 조항은 에드워드 코크

85) 李 哲,「컴퓨터 犯罪의 法的規制에 대한 硏究」, 慶熙大學校 大學院 博士學位論文, 1991. 6, 213면 參照.

86) 金啓煥,「大憲章의 適法節次, 公法의 諸問題」, 海巖文鴻柱博士 華甲紀念論文集, 해암사, 1978, 225면.

87) No freeman shall be seized, or imprisoned, or dispossessed, or exiled, or in any way destroyed; nor will we condemn him, nor will we commit him to prison, excepting by the legal judgment of peers, or by the law of the land.

(Edward Coke)의 저서 '영법원론(Institutes of the Law of England)'에서 적법절차, 합법적인 영장, 영장의 합법적 발부, 합법적 구금, 구금 이유 명시 등의 내용을 구체적으로 명시하였다.[89] 이 코크의 기초 아래 적법절차는 1628년 영국의 권리청원에서 "자유인은 국법에 의하거나 적법절차에 의해서만 체포 또는 구금되고 아무런 이유 없는 왕의 특명에 의해서는 체포·구금당하지 아니한다"[90]고 선언되었다. 그 후 1679년 인신보호법(Habeas Corpus Act)에서는 권리청원에 규정된 인신보호영장의 실효성을 확보하기 위한 방법으로 이를 절차화하였고, 이어 1689년 권리장전에 이르러 근대 헌법 이전에 신체의 자유보장은 완성을 보았다. 영국에서의 적법절차는 신체의 자유보장을 위한 원칙이며, 실체적 내용까지 포함하는 것이 아닌 순수한 절차적 개념으로서 확립되었다.[91]

미국 최초의 헌법인 1776년의 버지니아 헌법에서는 적법절차의 두 요소로서 '자연권'과 '형사권'을 채택하였다. 즉, 생명·자유·재산의 향유를 인간의 생래적 권리로 선언하는 한편, 형사피의자의 권리로서 형사절차상의 고지, 대질심문, 증인, 신속한 재판, 자기부죄의 금지, 공정한 배심 등을 열거하였다. 그 이후 채택된 주 헌법들은 약간의 차이점은 있지만, 거의 예외 없이 적법절차에 관한 조항을 규정하게 되었다.[92]

이처럼 '적법절차(due process of law)' 조항은 국가권력의 자의적인 행사로부터 개인의 기본권을 보장하기 위한 제도적 장치로 출연한 것이며, 미국 수정헌법 제5조와 제14조에서 규정하여 인권신장을 위한 가

88) Edward Keynes, Liberty, Property, and Privacy, The Pennsylvania State University Press University Park, 1996, p.11; 權寧卨,「美國憲法上 適法節次의 法理와 그 展開」, 美國憲法研究 제1호, 1999, 163면.

89) Edward Coke, Second part of the Institutes of the Law of England, 4th ed., London, 1671, pp.46-50; 鄭鎭洪,「人身의 自由保障에 있어서의 適法節次에 관한 硏究-美國의 判例分析을 통한 그 適用實態와 法理理解를 中心으로-」, 漢陽大學校博士學位論文, 1993, 61면 참조.

90) 文鴻柱,「美國憲法과 基本的 人權」, 裕豊出版社, 2002, 757면.

91) 安京煥,「民主法治主義의 實質化를 위한 適法節次」, 法制硏究 第3號, 1992, 92면.

92) 尹明善, 前揭書, 12면.

장 중요한 헌법적 도구로 사용되었다. 그러나 적법절차의 개념에 관하여 법원은 사실상 그 정의를 포기하고 판례를 통해서 그 내용을 형성·확대하였다.[93),94)]

적법절차의 내용은 판례를 통해 발전되어 왔으며, 1819년 Bank of Columbia 사건[95)]에서 적법절차의 원칙이란 국가권력의 자의적 행사로부터 개인을 보호하며, 나아가 확립된 사적 권리와 배분적 정의의 원칙을 준수할 것을 요구하였다. 또한 1884년 Corfield 사건[96)]에서 Washington 대법관은 "적법절차에는 생명·자유·재산의 향유와 행복과 안전의 추구를 그 내용으로 하는 실체적 측면과 인신보호영장과 형사재판에 접근·향유할 수 있는 절차적 측면이 포괄된다" 고 판시하였다.

결론적으로 적법절차라 함은 국가권력의 자의적인 행사를 금지하고 개인의 생명·자유·재산을 보장하기 위한 '자유와 정의의 일반원칙' 으로서 이들 가치를 제한하는 경우에는 '적당한 법의 절차' 를 거쳐 행함으로써 궁극적으로 인간의 존엄성을 실현하기 위한 법의 지배 내지 입헌주의의 기본원칙을 말한다.[97)] 우리 헌법은 제12조 제1항과 제3항에서 적법절차의 제도를 명문으로 규정하고 있다.

---

93) Henry Abraham, The Pascinating World of Due process of Law; in Freedom and the Court(Oxford Univ. Press), 1977, pp.107-108; 尹明善,「美國 基本權 硏究」, 慶熙大學校出版局, 2004. 12, 7면.

94) 이에 대한 가장 대표적인 판례는 1884년 Hurtado v. People of the state california 사건으로 여기서 Harlan 대법관은 '적법절차' 란 자유와 정의의 원칙들을 유지하기 위한 법적절차로서 국가권력의 행사에 있어서 공정성(fairness)의 원리를 성취시키기 위한 '공정한 처우의 원칙(a standard of fair dealing)' 이라고 정의하였다. 이 정의는 이후 판결들에 있어 하나의 모델로 제시되었고, 특히 1937년의 Palko v. Connicticut 사건에서 다수의견으로 수용되었다. 이 사건에서 Cardozo 대법관은 '적법절차' 란 '우리들의 전통과 양심속에 근본적인 것으로 자리 잡고 있는 자유와 정의의 원칙' 이며, 나아가 '우리들의 모든 시민적·정치적 제도의 기반이 되는 자유와 정의의 기본원칙' 이라고 정의하였다. 尹明善, 上揭書, 9면.

95) Bank of Columbia v. Okely, 17 U.S. 235 (1819).

96) Corfield v. Coryell, 6 Fed. Cas. at 552-53.

97) 尹明善, 前揭書, 9-10면 參照.

나. 적법절차의 내용

이러한 적법절차의 법리를 우리나라는 1987년 개정 헌법 제12조①, ③항에서 적법절차를 신설하여 이를 수용하게 되었는데,[98] 이에 대한 직접적인 계기는 보안처분의 재발문제에서 비롯되었다.[99] 결과적으로는 처벌·강제노역과 체포 · 구속 · 압수 · 수색 모두에 적법절차의 헌법적 보장이 명문화 되었다.[100]

적법절차의 원리는 입법·사법·행정 등 모든 국가작용은 절차상의 적법성을 갖추어야 할 뿐 아니라 공권력의 행사의 근거가 되는 법률의 실체까지도 합리성과 정당성을 갖추고 있어야 한다는 헌법상의 일반원칙이다. 적법절차의 적용범위로서 행정절차와 사법절차에 적용된다는 견해와 입법·행정·사법절차 모두에 적용된다는 견해가 있으나, 헌법재판소는 1992년 형사소송법 제331조의 단서 규정에 대한 위헌심판사건에서 “헌법 제12조 제3항 본문은 동조 제1항과 함께 적법절차의 일반조항에 해당하는 것으로서, 형사절차상의 영역에 한정되지 않고, 입법·행정 등 국가의 모든 공권력의 작용에는 절차상의 적법성 뿐만 아니라 법률의 구체적 내용의 합리성이 있어야 한다는 적법절차의 원칙을 헌법의 기본원리로 명시하고 있는 것”[101]이라고 하여 적법절차의 원칙은 헌법조항에 규정된 형사절차상의 제한된 범위내에서만 적용되는 것이 아니라 모든 입법·행정·사법작용에 걸쳐 광범위하게 적용되고 있다.[102]

---

98) 金炯盛,「大韓民國 憲法學」, 일진사, 2005, 110면.
99) 金哲洙,「美國憲法이 韓國憲法에 미친 影響序說, 美國憲法과 韓國憲法」, 韓國公法學會, 大學出版社, 1989, 66면.
100) 吳桃洙,「美國憲法上 刑事節次에서의 基本權保護에 관한 硏究-Undercover와 Confidential Informant 제도의 적법절차 위반 여부를 중심으로-」, 成均館大學校 碩士學位論文, 2004, 80-81면 참조.
101) 憲裁 1992. 12. 24. 92 헌가 8; 憲裁 1993. 7. 29. 90헌마35; 憲裁 1994. 12. 29. 94 헌마 201; 憲裁 1994. 7. 29. 93 헌가 3 참조.
102) 權寧星, 前揭書 421면.

헌법상 적법절차에 관하여 우리 헌법 제12조 1항은 그 후문에서「누구든지 법률에 의하지 아니하고는 체포· 구속· 압수· 수색 또는 심문을 받지 아니하며, 법률과 적법한 절차에 의하지 아니하고는 처벌과 보안처분 또는 강제노역을 받지 아니 한다」라고 규정하여 형사사건에 관한한 적법절차에 의할 것을 분명하게 하였다.[103] 이는 근대형법의 기본원리인 죄형법정주의를 선언하고 있다.[104] 동법 제3항에서는「체포· 구속· 압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다」고 규정하고 있다. 이는 영미법상 '적법절차' 의 원칙을 도입하였다고 볼 수 있다.

이처럼 우리 헌법은 적법절차조항을 명문으로 채택하였지만, 여기에는 해석상 많은 문제점을 내포하고 있다. 원래 적법절차의 법리는 미국 헌정사에 있어서 법원의 판례를 통해 점진적으로 형성·확대되어 왔기 때문에 이를 포괄적으로 정의하는 것 자체가 곤란하다. 또한 우리 헌법은 그 표현방식, 인권구조와 법문화·전통이 영미법계 국가와는 다르기 때문에 그 해석방법과 의미, 내용은 동일할 수 없는 것이다. 따라서 우리 헌법해석론으로서 적법절차의 개념과 법적인 성격, 그 내용과 적용 대상·범위 등이 검토되어야 할 것이다.[105]

---

103) 愈熙一,「憲法學의 諸問題-憲法上 適法節次 規定」, 實甫金榮秀敎授華甲紀念論文集, 學文社, 2000, 212면.

104) 憲裁는 죄형법정주의에 대하여 다음과 같이 판시하고 있다.「헌법 제13조 1항 전단은 모든 국민은 행위시의 법률에 의하여 범죄를 구성하지 아니하는 행위로 소추되지 아니한다고 규정하고, 제12조 1항 후문은 누구든지 법률과 적법한 절차에 의하지 아니하고는 처벌·보안처분 또는 강제노역을 받지 아니한다고 규정하고 있다. 이 원칙은 법률이 처벌하고자 하는 행위가 무엇이며 그에 대한 형벌이 어떠한 것인지를 누구나 예견할 수 있고, 그에 따라 자신의 행위를 결정할 수 있게끔 구성요건을 명확하게 규정할 것을 요구한다. 그런데 처벌법규의 구성요건이 어느 정도 명확하여야 하는가는 일률적으로 정할 수 없고, 각 구성요건의 특수성과 그러한 법적 규제의 원인이 된 여건이나 처벌의 정도 등을 고려하여 종합적으로 판단하여야 한다」憲裁 1997. 3. 27 선고, 96 헌가 17, 헌법판례집 제9권 1집, 219면 이하; 憲裁 2001. 1. 18 선고, 99 헌바 112, 憲裁判例集 제13권 1집, 85면; 憲裁 2002. 2. 28. 선고, 99 헌가 8, 憲裁判例集 제14권 1집, 87면.

105) 尹明善,「美國 基本權 硏究」, 慶熙大學校 出版局, 2004. 12, 21면.

다. 디지털 범죄에서 적법절차

국가권력에 의한 인권침해의 사례는 형사사건에서 가장 빈번하게 발생하므로 적법절차의 원리는 형사소추와 형사재판절차에서 특별히 존중되어야 한다. 헌법도 제12조 제1항 제2문 후단에서 형사절차상의 적정한 절차보장을 하기 위한 일반적·총칙적 규정을 두는데 그치지 아니하고, 제12조 제2항 이하에서 형사절차의 내용적 적정을 요구하는 개별적 적법절차 조항들까지 규정하고 있다. 예컨대, 현행 헌법에 규정된 개별적 적법절차조항으로는 첫째 형사소추절차 중 범죄수사절차와 관련하여 ㉮체포·구속에 있어서의 영장주의(§12③), ㉯구속 이유등 고지제도(§12⑤), ㉰영장발부에 관한 적법절차(§12③), ㉱주거에 대한 압수, 수색에 있어서의 영장주의(§16), ㉲고문의 금지(§12②)등이 있고, 둘째, 형사재판절차와 관련하여 ㉮신속한 공개재판을 받을 권리(§27③), ㉯변호인의 조력을 받을 권리(§12④), ㉰불리한 진술거부권(§12②), ㉱임의성이 없는 자백의 증거능력제한(§12⑦), ㉲소급처벌의 금지(§13①), ㉳이중처벌의 금지(§13①) 등이 있다.

정보통신의 발달로 최근에는 디지털 범죄가 증가하고 있고, 전통적인 범죄도 디지털 범죄와 혼용되어 나타나고 있다. 최근에는 온라인과 오프라인 범죄의 경계가 무너지고 있는 현상이 나타나고 있다.

형사소추절차 중 디지털 범죄 수사절차와 관련하여 특히 디지털 증거를 압수· 수색하는 경우에도 헌법 제12조 제1항과 제3항의 규정에 의거하여 적법절차가 적용이 되는 것은 당연하다 하겠다.

최근 위법하게 수집된 컴퓨터와 관련된 디지털 증거에 대하여 유죄의 증거가 되지 않는다는 대법원의 판결이 있었다.[106] 대법원은 범죄 증거물의 압수물을 수집하는 과정에서 절차조항이 엄격하게 준수되어야 한다

는 점을 분명히 제시하였다.

그러나 디지털 범죄에서 디지털 증거의 특성상 기존의 형사절차법상으로 해결하기에는 많은 문제점을 내포하고 있다. 첫째로 적법절차를 준수하기 위한 관련 법률이 미비하다는 것이고, 둘째는 기존의 형사절차법은 디지털 범죄를 전혀 고려하지 않았다는 것이다. 따라서 현행 형사절차법의 개정과 관련 법률의 입법문제도 심각하게 고려해봐야 할 것이다.

4. 영장제도

가. 영장제도의 의의

영장주의란 법원 또는 법관이 발부한 적법한 영장에 의하지 않으면, 형사절차상의 강제처분을 할 수 없다는 원칙을 말한다. 법관의 공정한 판단에 의하여 수사기관에 의한 강제처분권한의 남용을 억제하고 시민의 자유와 재산의 보장을 실현하기 위한 제도이다.[107] 이처럼 적법절차 보장을 위한 영장제도는 영미법에서 발생·발달한 것이며, 강제처분에 있어서 인권보장을 도모하려는 것이 주된 목적이다.

우리나라에 있어서 영장주의는 1948년 미군정 법령 제176호 「형사소송법의 개정」에 의하여 도입되었다. 미군정법령 제176호는 미국 수정헌법 제4조의 영장주의를 우리 법체계에 수용시키는 가교가 되었다.[108] 이러한 영장제도는 인권의 보장적 측면에서 도입된 뒤 헌법에까지 규정되었다. 수사기관에 의한 부당한 인권침해와 신체의 자유에 대한 침해를 막도록 하는데 그 의의가 있다. (구)형사소송법 제255조에서는 검사의

106) 경향신문,「위법수집증거 불인정 판결의 의미」, 2007. 11. 20.
107) 李在祥,「刑事訴訟法 第6版(補訂版)」博英社, 2007, 201면.
108) 신동운,「형사소송법」, 法文社, 2007, 103면.

예심판사에 대한 강제처분청구권만을 인정하였을 뿐 현행범인의 경우를 제외하고는 수사기관에 독자적 강제처분권을 인정하지 아니하였다. 동법 제123조, 제129조에서는 검사가 독자적으로 구인장·구류장을 발부할 수 있는 예외를 광범위하게 인정하였으며, 특히 일제말기에는 행정검속이란 명목으로 부당한 인신구속이 자행되었다.

영장의 법적 성격에 대해서는 법관이 수사기관에게 일정한 강제처분을 행할 권한의 행사를 허가하는 허가장이라고 하는 학설과 영장을 법관이 스스로의 권한으로서 행하는 강제처분에 대하여 수사기관에 발하는 명령장이라는 학설로 나뉘어지는데, 이에 대하여 헌법재판소는 법원이 직권으로 발부하는 영장은 명령장으로서의 성질을 갖지만, 수사기관의 청구에 의하여 발부하는 영장은 허가장으로서의 성질을 갖는다고 보고 있다.[109]

신체의 자유를 최대한 보장하려는 헌법정신, 특히 무죄추정의 원칙[110]으로 인하여 수사와 재판은 불구속을 원칙으로 한다. 그러므로 구속은 예외적으로 구속이외의 방법에 의하여서는 범죄에 대한 효과적인 투쟁이 불가능하여 형사소송의 목적을 달성할 수 없다고 인정되는 경우에 한하여 최후의 수단으로 사용하여야 하기 때문에 신체를 구속함에 있어서는 영장제도에 의한 보장이 요청된다.[111]

헌법재판소는 영장주의 제도에 대하여 다음과 같이 판시하고 있다.

---

109) 憲裁 1997. 3. 27. 선고, 96 헌바 28·31·32(병합), 형사소송법 제70조 1항 違憲訴願 등, 憲裁判例集 제9권 1집, 321면 參照.

110) 憲裁는 무죄추정의 원칙을 다음과 같이 설명하고 있다.「무죄추정의 원칙은 형사절차와 관련하여 아직 공소가 제기되지 아니한 피의자는 물론 비록 공소가 제기된 피고인이라 할지라도 유죄의 판결이 확정될 때까지는 원칙적으로 죄가 없는 자로 다루어져야 하고, 그 불이익은 필요최소한에 그쳐야 한다는 원칙을 말한다. 이 원칙은 언제나 불리한 처지에 놓여 인권이 유린되기 쉬운 피의자나 피고인의 지위를 옹호하여 형사절차에서 그들의 불이익을 필요한 최소한에 그치게 하자는 것으로서 인간의 존엄성을 궁극의 목표로 하고 있는 헌법이념에서 나온 것이다」. 憲裁 1997. 5. 29. 선고, 96 헌가 17, 憲裁判例集 제9권 1집, 517면 이하.

111) 憲裁 2003. 11. 27. 선고, 2002 헌마 193, 憲裁公報 제87호, 56면 이하(60면).

「영장주의라 함은 형사절차와 관련하여 체포· 구속· 압수 등의 강제처분을 함에 있어서는 사법권 독립에 의하여 그 신분이 보장되는 법관이 발부한 영장에 의하지 않으면 아니 된다는 원칙이고, 따라서 영장주의의 본질은 신체의 자유를 침해하는 강제처분을 함에 있어서는 중립적인 법관이 구체적 판단을 거쳐 발부한 영장에 의하여만 한다는 데에 있다고 할 수 있다」.[112]

나. 형사소송법상 영장제도

헌법상 영장주의 원칙 규정을 따르는 우리 형사소송법은 수사상의 압수· 수색에는 제215조의 사전영장에 의한 압수, 제216조 제3항의 사후영장에 의한 압수· 수색, 제216조 제1항, 제217조, 제218조의 영장없이 행할 수 있는 압수· 수색 등 세 가지 형태로 규정되어 있다.[113]

그리고 형사소송법 제113조는 공판정외에서 압수· 수색을 함에는 영장을 발부하여 시행하도록 하고 있고, 동법 제114조는 압수· 수색영장에는 피고인의 성명, 죄명, 압수할 물건, 수색할 장소, 신체, 물건, 발부연월일, 유효기간과 그 기간을 경과하면 집행에 착수하지 못하며 영장을 반환하여야 한다는 취지, 기타 대법원 규칙으로 정한 사항을 기재하도록 하고 있다. 이는 같은 법 제219조에 의해 검사 또는 사법경찰관의 압수· 수색에 준용되고 있다. 이는 일반영장금지 원칙을 천명한 것으로서 특정 피의사건에 있어서 수사기관이 압수 권한을 남용하여 권한 외의 물건을 압수함으로써 처분을 받은 자의 물건소지에 대한 안전을 해하지 않도록 하며, 다른 한편으로는 수사기관이 압수를 함에 있어서는 압수영장을 상대방에게 제시하도록 하고(동법 제118조), 피고인, 피의자 및 변호인을

112) 憲裁 1997. 3. 27. 선고, 96 헌바 28·31·32(병합), 憲裁判例集 제9권 제1집, 313면 이하.
113) 申東雲,「刑事訴訟法Ⅰ」, 法文社, 1996, 220면.

참여할 수 있게 하여(동법 제121조), 수사기관에 부여된 압수 권한을 넘어 권한외의 물건까지 불법으로 압수하는 경우 즉시 이의를 제기 할 수 있게 하거나 또는 형사소송법 제417조에 의해 법원에 대해 위법한 압수처분을 취소해 줄 것을 청구할 수 있게 하여 그 재산권을 방위할 수 있게 하려는 규정이라고 하겠다.[114] 이와 같은 형사소송법상의 영장주의 규정은 디지털 범죄에 있어서도 엄격하게 적용되어야 한다. 이는 영장제도라는 적법절차를 통하여 국민 개개인의 기본권을 최대한 보호하고 수사기관의 권한외 남용을 방지하기 위해서 반드시 필요하다.

1) 영장제시의 원칙

형사소송법 제219조 및 제118조에 의하여 수사기관은 압수· 수색의 강제처분을 함에 있어 법관이 발부한 영장을 반드시 제시하여야 한다. 이는 영장의 제시라는 일정한 형식을 거치도록 함으로써 수사기관이 행하는 강제처분의 적법성을 국민에게 납득시킴과 동시에 수사기관의 강제처분 남용을 심리적으로 견제하는 효과를 꾀하려는 규정이라 하겠다. 이러한 점을 강조하여 형사소송법은 영장을 '반드시' 제시하여야 한다고 규정하고 있다.[115] 이 경우 제시되는 영장은 반드시 정본이어야 하며 사본의 제시는 허용되지 않는다.[116]

---

114) 日本 刑事訴訟法의 해석에 관하여 동일한 견해를 취하고 있는 下級審 判決로 東京地方裁判所 昭和 33(1958년). 6. 12., 1審刑集 1卷 追錄, 2367면 參照, 安富 潔, 前揭書, 147면; 吳奇斗, 前揭論文, 92면 재인용.

115) 헌법 제12조 제3항에 의하여 법관이 발부한 영장의 제시가 있어야 함에도 불구하고 동행명령장을 법관이 아닌 지방의회 의장이 발부하고 이에 기하여 증인의 신체의 자유를 침해하여 증인을 일정 장소에 인치하도록 규정한 지방의회 조례는 헌법 제12조 3항 규정을 위반한 것이다. 大法院 1995. 6. 30 93추83 (법원공보 1995-997 이하); 신동운,「형사소송법」, 法文社, 2007, 105면.

116) 1997. 1. 24. 96다40547, 법률신문 1997. 2. 3. 5면 참조. 수사기관이 구속영장 정본이 아닌 사본을 제시하고 피의자를 연행한 사안에 대하여 대법원은 불법연행임을 이유로 국가가 위자료를 지급해야 한다고 판시하였다.

현행 형사소송법에 의하면 검사 또는 사법 경찰관이 체포영장(제200조의 2)이나 긴급체포규정(제200조의 3)에 의해 피의자를 체포하는 경우(제200조의 5) 체포영장을 소지하지 않았고, 긴급을 요하면 피의자에 대하여 피의사실의 요지와 체포영장이 발부된 경우 그 사실을 고지하고 체포할 수 있다(제209조, 제85조 제3항). 그러나 체포 후에는 체포영장이 발부되었으면 체포영장, 피의자를 긴급체포하였으면 사후에 발부받은 구속영장을 신속히 피의자에게 제시해야 한다. 그러나 체포영장을 집행함에 있어 인정되는 긴급집행의 예외, 즉 수사기관이 체포영장이나 구속영장을 소지하지 아니한 경우에 긴급을 요하는 때에는 영장을 제시하지 않고도 체포 또는 구속할 수 있는 예외가 압수· 수색· 검증 영장의 집행에 있어서는 인정되지 않고 있다. 따라서 압수· 수색 영장의 집행에 있어서는 반드시 영장을 제시하여야 한다(제219조, 제118조).[117] 그러므로 디지털 증거를 압수· 수색함에 있어서도 법관으로부터 발부받은 영장을 피의자나 피처분자에 대해 반드시 제시하여야 한다.

2) 영장주의의 예외

현행 헌법 제12조 3항 단서는 영장제도의 예외로 현행범인인 경우와 장기 3년 이상의 형에 해당하는 죄를 범하고 도피 또는 증거인멸의 염려가 있을 때에는 사후영장을 청구 할 수 있다. 이에 대한 대표적인 예로 1975년의 긴급조치 사건으로 법관의 영장없는 체포· 구속· 압수· 수색을 할 수 있게 한 긴급조치 제2호 12항이 위헌이라는 주장에 대하여 대법원은 대통령에게 (구)헌법 제53조에 의하여 국민의 자유와 권리를 잠정적으로 정지조치를 할 권한이 부여되어 있다 하여 이를 배척하였다.[118]

헌법 제77조 3항에 근거하여 비상계엄선포지역에서는 이 영장제도의

117) 申東雲, 前揭書, 124면.
118) 大判 1975. 4. 8. 74 도 3323, 緊急措置違反.

시행에 특별한 조치를 할 수 있다고 규정하고 있다. 이 비상계엄하에 특별한 조치가 무엇인가에 대하여 많은 논란이 있는데, 제1공화국 헌법위원회는 비상계엄하에 있어서도 영장제도를 배제하는 것은 아니라는 결정을 한 바 있다.

검사 또는 사법경찰관은 형사소송법 제200조의 2의 체포, 제200조의 3의 긴급체포, 제201조의 구속, 제212조의 현행범인 체포의 각 규정에 의해 피의자를 체포 또는 구속하는 경우에 필요한 때에는 영장없이 타인의 주거나 타인이 간수하는 가옥, 건조물, 항공기, 선거내에서 피의자를 수사할 수 있고, 피의자나 피고인을 체포한 현장에서 압수· 수색· 검증을 할 수 있다. 범행 중 또는 범행 직후의 범죄 장소에서 긴급을 요하며 법관의 영장을 발부 받을 수 없는 때에는 영장없이 압수· 수색· 검증을 할 수 있다. 이 경우에는 사후에 지체없이 영장을 발부 받아야 한다(제216조).

검사 또는 사법 경찰관은 긴급체포의 규정에 의거하여 체포할 수 있는 자의 소유, 소지 또는 보관하는 물건에 관하여는 긴급체포시 영장청구기간 규정(제200조의 4)에 정해진 기간내에 한하여 영장없이 압수· 수색 또는 검증할 수 있다(제217조). 이러한 현행 형사소송법 규정은 디지털 증거에도 당연히 적용할 수 있다. 그러나 디지털 데이터 자체의 압수가능성에 관해서는 혐의를 받고 있는 범죄 사실과 관련성을 기준으로 그 허용여부를 판단하지 않으면 안된다고 하겠다.[119]

다. 디지털 범죄에서의 영장제도 적용

헌법상 신체의 자유를 보장하는 방법은 다양하지만, 그것은 대체로 실체적 보장, 절차적 보장, 형사 피의자·피고인의 형사절차상의 권리보장

119) 吳奇斗, 前揭論文, 94면.

등으로 구체화 된다. 아무튼 신체의 자유는 헌법이 지향하는 궁극적인 이념인 인간의 존엄과 가치를 구현하기 위한 기본적인 자유로서 기본권 보장의 핵심이 된다.[120]

우리 헌법 제12조 제3항은 “체포· 구속· 압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다. 다만, 현행범인인 경우와 장기 3년 이상의 형에 해당하는 죄를 범하고 도피 또는 증거인멸의 염려가 있을 때에는 사후에 영장을 청구할 수 있다”고 규정하고 있다. 이는 우리 헌법도 영장주의를 천명하고 있는 것이다. 또한 헌법 제16조는 주거의 자유에 관하여 “모든 국민은 주거의 자유를 침해받지 아니한다. 주거에 대한 압수나 수색을 할 때에는 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다”고 규정하여 주거의 불가침과 영장에 의한 보호를 규정하고 있다. 주거의 불가침이라 함은 개인의 사생활을 공권력으로부터 보호하며 개인의 프라이버시를 보호하기 위한 것이다.[121]

위와 같은 우리 헌법규정은 ① 죄를 범하였다고 의심할 만한 상당한 이유가 존재하여야 하며 이때 압수· 수색의 구체적인 필요성이 있음을 의미한다. ② 그 범죄를 입증할 수 있는 개연성이 높은 증거나 압수 대상물의 특정, ③ 당해 압수 대상물이 존재할 개연성이 높은 장소 등과 같은 실체적인 요건과 중립· 공평한 입장에 있는 제3자인 법관에 의한 사전심사라는 절차적인 요건을 충족하여야 압수· 수색 등이 가능하며 ④

120) 신체의 자유는 모든 기본권 보장의 전제가 되는 것으로서 신체활동을 자율적으로 할 수 있는 신체 거동의 자유와 함께 신체의 안전성이 외부로부터의 물리적인 힘이나 정신적인 위협으로부터 침해당하지 아니할 자유를 포함한다. 이와 같이 신체의 자유는 헌법상 모든 기본권 보장의 종국적 목적이나 기본이념이라 할 수 있는 인간의 존엄과 가치에 밀접하게 관련되어 있으므로 그 침해여부는 헌법 제37조 제2항에 따라서 엄격하게 심사되어야 한다. 따라서 수용시설내의 안전과 질서를 유지하기 위하여 일부 제한이 불가피하다 하더라도 그 본질적인 내용을 침해하거나, 목적의 정당성, 방법의 적정성, 피해의 최소성 및 법익의 균형성 등을 의미하는 과잉금지의 원칙에 위배되어서는 아니되는 것이다. 憲裁 2003. 12. 18 2001 헌마 163; 憲裁 2002. 7. 18. 2000 헌마 327, 憲裁判例集 제14권 제2집, 63면.

121) 金哲洙,「憲法學新論」, 博英社, 2004, 409면.

동일한 영장에 의하여 수많은 수색할 물건이나 장소를 기재하는 일반영장(general warrant)은 금지된다.[122] 법관이 발부하는 영장은 그 내용이 특정되어야 한다. 범죄사실과 피의자는 물론 인치구금할 장소 등도 특정되어야 한다. 압수· 수색의 대상도 구체적으로 특정되어야 한다. 다만 통신비밀보호법은 통신의 특수성에 비추어 일정기간에 걸쳐 포괄적으로 통신제한조치를 허가하는 영장발부를 인정하고 있다.[123]

이러한 헌법 규정에 근거하여 디지털 증거에 대한 압수· 수색에 관한 규정도 당연히 영장제도를 따라야 하며 법률에 규정되지 않은 수단에 의해서 디지털 증거가 수집· 분석된다면 이는 위법수집증거에 해당되어 증거능력이 부정된다.[124]

그러나 디지털 증거를 압수· 수색하는데 현행 우리의 법률체계가 어느 정도 적용될 수 있는가 하는 것에는 상당한 의문이 있을 수 밖에 없다. 왜냐 하면 디지털 증거는 매체독립적인 정보성, 네트워크성, 초국경성, 대규모성 등의 디지털만이 갖는 고유한 특성을 가지고 있기 때문이다.[125]

디지털 증거와 관련하여 이러한 현행 법률의 문제는 전반적으로 현재의 정보통신, 과학기술 환경을 법률규정이 따라가지 못해서 생기는 현상이다. 우리나라의 법률제도, 특히 형사법규의 경우 생활환경의 변화를 반영하는 면에서는 상당히 소극적이다. 여러 가지 문제가 재판과정에서

122) 吳奇斗, 前揭論文, 91면 參照.
123) 신동운,「형사소송법」, 法文社, 2007, 105면.
124) 違法蒐集證據排除法則(exclusionary rules) 이라함은 위법한 수사로 인하여 획득된 증거와 그 증거를 원인으로 하여 얻어진 부수적 증거들에 대하여 증거능력을 부인함으로써 이를 유죄인정의 증거로 삼을 수 없도록 하는 원칙을 말한다. 위법수집증거배제법칙이 나오게 되는 계기는 수사기관이 범인의 유죄입증을 위한 증거를 수집하려는 목적에서 위법수사를 행하는 일이 많다는 사실에서 찾을 수 있다. 위법수집증거배제의 법칙은 이러한 경험적 사실에 주목하여 위법수사로 인한 증거의 증거능력을 전면적으로 부인함으로써 수사기관의 위법수사에 대한 유혹이나 동기형성을 처음부터 차단하자는 것이다. 신동운,「형사소송법」, 法文社, 2007,128-129면.
125) 梁根源, 前揭論文, 129-130면.

제기되고 사회적인 이슈로 등장하게 되면 당연히 이에 대한 논의가 활발해지겠지만, 우리의 형사재판제도에서 디지털 증거 분야와 관련된 문제가 제기된 적은 거의 없는 실정이다. 그나마 최근 2007년에 들어서 조금씩 디지털 증거에 관하여 학계와 수사기관에서 관심을 갖고 있으며, 이에 대한 입법적인 필요성도 서서히 제기되고 있는 추세이다.

우리 헌법규정의 영장제도는 디지털 증거의 압수· 수색에 있어서도 당연히 지켜지고 적극적으로 도입함으로써 헌법상 보장된 국민의 기본권이 최대한 보장되도록 해야 할 것이다. 따라서 헌법규정에 근거하여 관련 하위법령들의 정비가 조속히 이루어져야 할 것이다.

제2절 영장에 의한 디지털 증거의 압수·수색의 가능성

1. 문제제기

우리 헌법은 영장주의(令狀主義)를 헌법적 차원에서 규정하고 있는데, 영장주의라 함은 법관이 발부한 적법한 영장에 의하지 않고서는 수사상 필요한 강제처분을 할 수 없다는 원칙을 말한다. 이에 따라서 우리 헌법 제12조 3항도 체포, 구속, 압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다고 규정하고 있다. 영장주의는 헌법상 신분이 보장되고 직무활동의 독립성이 담보되는 법관이 발부한 영장을 제시하지 아니하고는 수사에 필요한 강제처분을 하지 못한다는 원칙을 말한다.[126] 이것은 수사상 필요한 경우 일정한 자유를 제한할 수 있다는 권한에 대한 법치국가적 제한을 의미한다. 다시 말하면 권한을 행사하는 수사기관의 입장에서 보면 영장 없이

126) 1993. 12. 23. 93헌가2, 헌집 5②, 578(596).

강제처분을 해서는 안 된다는 '금지' 에 해당하고, 수사대상인 피의자의 입장에서 보면 영장에 의한 강제처분을 요구할 수 있는 권리를 규정하고 있는 것이다. 따라서 영장주의는 수사기관을 위한 것이 아니라 국민의 기본권을 보장하기 위한 제도이다.[127]

헌법 제17조에 '모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다' 는 헌법상의 요청을 달성하기 위하여 디지털 증거에 대하여도 영장주의가 적용되어야 한다는 것은 헌법상의 원칙이다. 따라서 일반적· 탐색적 압수· 수색을 금지하여야 한다는 것을 의미한다.[128]

디지털 증거를 압수· 수색함에는 헌법상 적법절차 준수와 영장제도에 근거하여야 함에도 현행 형사소송법 규정은 디지털 증거의 압수· 수색이 가능한지에 대하여 구체적인 규정을 명시하고 있지 않다. 현행 우리 형사소송법 제219조, 제106조는 압수의 대상으로서 '증거물' 또는 몰수할 것으로 사료되는 '물건' 으로 규정하고 있다. 여기서 '증거물' 또는 '물건' 이라 함은 유체물을 의미한다고 할 것이다. 따라서 데이터나 프로그램을 기록한 자기테이프나 하드 디스크 등이 그 자체로는 증거물이 되는 경우에는 이를 압수· 수색의 대상으로 하여 그 점유를 취득할 수 있다는 견해에 대해서는 이를 긍정해야 할 것이다.[129] 이는 유체물이기 때문에 현행 형사소송법 규정으로 충분히 가능하다.

그러나 이러한 디지털 증거를 압수· 수색할 때는 그 유체물을 압수· 수색하는 것이 주된 목적이 아니고, 그 안에 내장되어 있는 정보를 압수· 수색하는 것이 주요한 목적이다. 따라서 압수· 수색 대상으로 무체정보인 디지털 정보를 유체물을 압수· 수색의 대상으로 하고 있는 우리

127) 裵鍾大·李相暾, 「刑事訴訟法」, 弘文社, 2006. 8, 215면.
128) 이훈동 「컴퓨터 관련 범죄와 형사절차」, 桂山成時鐸教授 華甲紀念論文集, 1993, 958면; 吳寄斗, 前揭論文, 82면.
129) 的場純男, 「コンピュータ 犯罪と捜査」, 松尾浩也·井上正仁 編, 刑事訴訟法の 爭點(新版), ジュリスト 增刊, 有斐閣, 1991, 94면.

형사소송법의 규정을 적용할 수 있는지가 문제가 된다.[130] 이에 대하여 디지털 증거에 대하여 압수· 수색의 가능성의 여부를 좀 더 구체적으로 살펴보자 한다.

2. 학설대립

가. 압수·수색이 가능하다는 견해

현재 우리 수사기관은 디지털 범죄에서 디지털 증거의 압수· 수색에 관하여 문제점은 인식하고 있지만, 실제로 이에 대한 구체적으로 문제를 제기한 적은 거의 없다. 이에 대해 미국은 압수· 수색을 유체물에 한정하지 않는다는 판결이 있는데, 미연방 형사소송규칙 제41조 제(h)항은 압수· 수색의 대상이 되는 물건(property)을 문서(documents), 장부(books), 서류(papers) 기타 유체물을 포함한다고 정의하고 있다. 위 규정대로 하면 디지털 증거는 압수· 수색의 대상이 아니라고 보아야 할 것이지만, 미연방 대법원은 United States v. New York Telephone Co. 판결[131]에서 위 규정은 한정적 열거규정이 아니어서 압수대상이 될 수 있는 사항(items)을 전부 열거하고 있는 규정도 아니므로 위 규정이 압수 대상물

130) 참고로 독일 형사소송법 규정을 보면, 동법 제94조는 압수의 목적물(Gegenstand der Beschlagnahme)이라는 표제하에 '공판심리에 의미가 있는 증거방법이 되는 목적물은 이를 유치하거나, 다른 방법에 의해서 이를 이용 가능하도록 취득해야 한다'(같은 조문 제1항), "어떤 사람이 압수목적물을 보관하고 있고, 그가 이를 임의로 제출하지 않는다면 이를 압수해야 한다"(제2항), "전2항은 몰수에 해당하는 운전면허증에도 적용된다"(제3항)고 규정하고 있다. 따라서 '목적물'의 해석에 관해 독일형사소송법상으로도 우리와 같이 무체정보를 포함하는 개념인지 여부에 관한 문제가 있다고 생각된다. 이에 대해 독일 형사소송법 제95조에 의해 압수대상물의 제출의무를 지는 은행이나 상인 등은 보관하고 있는 전자기억매체를 읽을 수 있는 형태로 출력하거나 복제하여 제출해야 한다고 해석하고 있다. Kommentar zur Strafprozeßordnung,(Knut Amelung), Band 2/Teilb and 1, Luchterhand, 1992, S. 20; 吳寄斗, 前揭論文, 72면 재인용.

131) United States v. New York Telephone Co., 434 U.S. 159, 98 S.Ct. 364, 54 L.Ed. 2d 376 (1997).

을 유체물에 한정하고 있는 것은 아니라고 판시하였다.[132] 이 밖에 압수· 수색영장에 기록과 문서(records and documents)만을 압수· 수색 목적물로 기재하고 있다고 하더라도 컴퓨터 디스크까지 압수할 수 있다고 한 판례도 있다.[133]

이에 대하여 일본의 安富 潔 교수는 데이터의 압수가능성에 대하여 다음과 같이 주장하고 있다. 일본 헌법 제35조에서 규정하고 있는 '주거, 서류 및 소지품에 관하여', '침입· 수색 및 압수를 당하지 않을 권리'는 영미법상 Common Law의 전통을 계수하여 미연방 수정헌법 제4조에 표현된 개인의 프라이버시권을 보호하기 위한 권리라고 해석된다. 따라서 주거 등에 대한 물리적인 지배권이나 이용권 등 만이 아니고 가시성, 가독성 없는 무체정보라고 할지라도 프라이버시 보호의 범위에 포함된다고 보아야 할 것이므로 압수대상이 된다고 볼 수 있다. 그런데 무체정보인 디지털 기록도 전자저장매체에 기록되어 있거나 일정한 용지에 프린트를 이용하여 인쇄하면 물리적으로 관리가능한 형태인 유체물로 되기 때문에 이것을 일체로 파악하면 무체정보에 대한 압수는 결국 유체물의 압수와 동일하게 볼 수 있다는 것이다.[134]

독일은 디지털 범죄와 관련된 증거를 압수· 수색함에 있어 이를 강제

---

132) 이와 관련된 사례로 United States v. Horowitz, 806 F.2d 1222(4th Cir. 1986)이 있다. 위 판결은 피고인을 고용하고 있는 고용주의 경쟁 상대방에게 피고인이 가격정보를 누설한 사건으로 FBI가 압수수색영장을 집행하면서 "그 가격정보가 위 경쟁 상대방의 컴퓨터 기억장치에 저장되어 있다고 생각할 때 컴퓨터 자기디스크, 자기테이프, 펀치카드, 프린트 아웃 등을 포함한 물건을 압수하기 위해 당해 건물내부를 수색하는 것"을 인정한 영장을 유효하다고 한 판결이다. 이 사건에서 피고인은 위 수색은 건물의 수색이 아니라 피고인 사무실의 연장인 컴퓨터에 대한 수색이었고, 컴퓨터 디스크나 테이프에 기록된 동영상이나 음성이라고 하는 무체물에 대해 행해진 수색이었으므로 당해 수색을 위한 별도의 영장을 발부받지 않고 행해진 위 수색은 영장없이 행해진 수색이며, 이와 같이 압수한 자기테이프의 재생으로 피고인의 프라이버시가 침해되었다고 주장하였다. 그러나 법원은 피고인의 주장을 받아들이지 않았다. 安富 潔, 前揭書, 36면.

133) United States v. Munson, 650 F. Supp. 525(D. Colo. 1986. Cynthia K. Nicholson, Robert Cunningham, "Computer Crime", American Criminal Law Review, vol. 28, 1991, p.400, fn 56.

134) 安富 潔, 前揭書, 150面.

수사로 인정하여 영장주의를 적용하고 있다. 그러나 강제수사는 언제나 피의자의 기본권을 침해할 수 있기 때문에 비례성 원칙에 의하여 그 허용범위가 결정되어야 한다. 즉 컴퓨터를 비롯하여 디지털 정보기술의 발전에 따른 정보제공 및 표현의 자유 보장이라는 측면과 디지털 범죄로 인하여 발생하는 부정적인 측면을 고려하여 디지털 범죄가 국민의 기본권을 침해하는 심각성이 인정되는 경우에 한하여 디지털 기록의 압수·수색을 인정할 수 있다고 한다. 따라서 수사기관이 디지털 기록에 대해 강제수사를 하기 위해서는 인터넷에 따른 공공의 이익이 존재하는가의 여부를 우선적으로 검토해야 한다.[135]

나. 압수·수색이 불가능하다는 견해

현재 대부분의 디지털 증거는 유체물이 아닌 무체물로 전통적인 형사소송법상의 강제적 증거수집 절차규정에 의거하여 압수· 수색이 가능한지에 대하여는 의문을 제기하지 않을 수가 없다.

일본에서는 무체정보 그 자체는 압수대상이 되지 않지만, 그 정보가 서류나 장부 등과 같은 유체물에 화체되어 있는 경우는 그 서류 등을 압수할 수 있으므로 디지털 정보가 컴퓨터의 하드 디스크에 기록되어 있는 경우도 그와 동일한 방법으로 무체정보를 압수 할 수 있다는 견해도 있다.[136] 그러나 일본에서는 근본적으로 무체정보의 압수가능성을 부정하고 있는 입장이다. 이에 대하여 1998년도 일본에서 디지털 증거에 관한 압수를 부정한 하급심 판례를 살펴보고자 한다.

---

135) Meier/Böhm, Strafprozessuale Probleme der Computerkriminalität, Wistra 1992, p.168; 원혜욱,「전자증거의 압수·수색」, 한국비교형사법학회 2003년 하계국제학술대회자료, 한국비교형사법학회, 2003. 8, 117-118면.

136) 柳俊夫,「捜索, 差押ぇ」, 三井誠=中山善房=河上和雄, 刑事手續上, 1988, 306면; 安富 潔, 前揭書, 154면, 註15; 吳奇斗, 前揭論文, 76面 재인용.

1) 일본 판례의 입장[137)]

일본에서 컴퓨터와 관련된 디지털 증거의 압수에 관하여 동경지방법원의 하급심 판례로 수사기관은 외설 홈페이지를 개설한 피의자의 데이터를 압수하기 위해 압수영장을 발부 받았다. 그러나 발부된 영장에 기하여 ISP가 관리하는 피의자 이외의 고객 데이터가 압수되었다. 법원은 피의자 이외의 고객 데이터의 압수가 피의사실과 관련성이 없다하여 압수의 필요성이 인정될 수 없다고 판결한 사례이다. 자세한 내용은 아래와 같다.

2) 범죄 사실의 개요

본 사건의 피의자는 ISP가 관리하는 서버 컴퓨터 내에 사진을 포함한 음란물을 홈페이지에 저장시켜 인터넷을 이용하는 불특정 다수인에게 위 홈페이지상의 외설 화면을 재생, 열람 가능한 상태를 만들었다. 수사기관은 외설 도화를 공연· 전시하였다는 피의사실을 이유로 압수· 수색영장이 발부되었다. 피의자는 홈페이지 및 이메일에서 morokin이라고 하는 계정을 사용하고 있었다. 수사기관은 압수영장을 근거로 하여 서버(server)컴퓨터[138)], 하드 디스크, 라우터(router)[139)] 등 통신기기 그리고 데이터가 저장된 디스크, 데이터를 출력한 서면, 로그 파일(log file)[140)]등 전자적 기록 매체, 개인용 컴퓨터, 전자게시판 광고자료,

137) 東京地方法院 判決, 1998. 2. 27 선고, 판례시보 1637-152.

138) 서버(server)라 함은 근거리통신망(LAN)에서 집약적인 처리기능을 서비스하는 서브시스템을 말한다. 일반적으로 서버 프로그램이 실행되고 있는 컴퓨터 하드웨어를 서버라고 부르며 다른 프로그램에게 서비스를 제공하는 컴퓨터 프로그램을 말하기도 한다.

139) 라우터(router)라 함은 네트워크 장비로 근거리통신망을 연결하여 정보를 주고 받을 때 송신정보(packet)에 담긴 수신처의 주소를 읽고, 가장 효율적인 경로를 선택하여 패킷을 다른 통신망으로 전송하는 장치이다.

고객 명부, 전자메일란, 신청서류, 개인전화부, 주소록, ID, 예금통장 등을 압수하였다.

3) 판결

본 사건의 인터넷 회사(ISP)는 피의자가 아니기 때문에 당연히 범죄와 관련이 없는 고객의 사생활을 보호해야만 한다. 따라서 ISP에 대한 압수· 수색의 적법성을 판단함에 있어서는 압수· 수색의 필요성과 고객 이용자의 사생활 보호를 충분히 고려할 필요가 있다. 또한 압수 영장에 의거하여 압수해야 할 물건들은 앞에서와 같이 포괄적이어서 구체적 압수처분에 있어서는 압수의 필요성을 엄격히 해석할 필요가 있다.

본 건에서 인터넷 회사의 고객 명부는 인터넷 서비스의 계약을 체결한 회원 중 성인장르를 선택한 고객 428명의 자료이고, 이 고객 명부도 압수되었다. 그러나 이 중에 morikin 계정을 사용하여 본 사건 외설 홈페이지를 개설한 피의자에 대하여는 범죄 사실과의 관련성, 압수의 필요성은 분명하다. 그러나 피의자 이외의 회원에 관한 데이터에 관하여는 본 범죄사실과 관련성을 인정하기 어렵고, 압수의 필요성은 인정되지 않는다고 판결하였다.

본 건의 디지털 증거에 관한 압수· 수색에 있어서 피의자의 범죄사실과 관련 없는 플로피 디스크 1매가 압수되었다. 법원은 범죄와 관련 없는 데이터의 압수를 인정하지 않는다고 판결 하였다.

결론적으로 디지털 증거에 관한 압수· 수색의 범위는 헌법의 요청에서 보아도 필요 최소한도의 그치는 것을 요구하고 있기 때문에 위 東京地方法院의 판단은 타당하다.

---

140) 로그(log)란 시스템에 접속한 사용자들의 행위들을 저장해 놓은 기록들을 말한다. 즉 시스템에서 작동된 모든 현상들을 저장하고 보여주는 것이 바로 로그이다.

3. 소결

디지털 증거의 압수· 수색의 가능성 여부는 디지털 증거의 특성상 부정적인 면이 있다고 해석된다. 현행 형사소송법은 압수의 대상을 유체물에 한정하고 있기 때문이다. 따라서 유체물이라고 할지라도 컴퓨터 하드디스크 자체보다도 그 안에 저장된 디지털 자료 자체를 현행 우리의 형사소송법상으로 압수· 수색 규정에 적용하는 것은 문제가 있다.

그러나 현재 이에 대한 구체적인 문제점을 아직 제기하고 있지는 않고 있는 실정이다. 다만 디지털 증거가 정보를 저장하고 있는 유체물인 경우 그 압수· 수색의 필요성이나 적법성을 일률적으로 부정할 수는 없으므로 현행법의 해석상 디지털 데이터의 압수가 결국 유체물의 압수로 볼 수 있는 경우에 한하여 그 유체물의 압수를 긍정해야 할 것이다.

디지털 범죄에서 컴퓨터와 관련된 디지털 증거를 저장하고 있는 유체물은 큰 의미가 없고, 그 안에 저장되어 있는 디지털 자료의 내용이 중요하다. 따라서 유체물만을 대상으로 하고 있는 우리 형사소송법 규정을 디지털 저장매체에 대한 압수· 수색에 적용하기 위해서는 디지털 저장매체의 특수성을 고려하여 보다 신중한 입법적인 검토가 필요할 것이다.

현재 우리 사회는 모든 범죄가 디지털화 되어가고 있다고 보아도 무리가 없을 정도로 디지털 범죄가 급속도로 증가하고 있다. 현행 형사소송법은 이러한 디지털 증거의 압수· 수색 문제가 관하여 세부적이고 구체적인 규정이 마련되어 있지 않다. 따라서 디지털 증거의 압수· 수색의 가능성에 관하여 다양한 형태의 문제점들이 앞으로 제기될 것이다. 이러한 다양한 문제점들을 제기되고 이를 해결하기 위해서는 우선적으로 형사소송법 규정을 구체적으로 디지털 증거의 특성에 맞게 개정해야 함이 하나의 해결방안이라고 생각한다.

제4장 디지털 범죄 수사에서 영장제도의 내용과 예외

제1절 한국 헌법상 영장제도의 내용

1. 영장의 필요성

우리 현행 헌법 제12조 3항은 “체포· 구속· 압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다”고 규정하여, 영장주의의 대원칙을 천명하고 있다. 즉, 수사기관의 입장에서 보면 영장없이 강제처분을 해서는 안된다는 것이고, 피의자의 입장에서는 영장에 의한 강제처분을 요구할 수 있는 권리를 규정하고 있는 것이다. 결국 영장주의는 수사기관을 위한 것이 아니라 국민의 기본권을 보호하기 위한 제도이다.[141]

이러한 기본권을 보호하기 위한 취지에 따라 수사기관이 디지털 범죄에서 관련 증거를 수집함에 있어서도 적법한 절차에 따라 영장주의 규정에 따라야 함은 당연하다. 그리고 영장은 검사나 경찰관이 디지털 범죄 수사에 필요성에 의거하여 지방법원판사에게 청구하여 발부 받아야 한다. 또한 디지털 증거의 압수· 수색 뿐 아니라 증거의 수집· 보존· 분석도 법률의 규정에 의하여야 하며 이를 위반시에는 위법한 증거가 되어 증거능력을 인정받지 못한다. 그러나 현행법상 디지털 증거의 수집· 보

141) 裵鍾大·李相暾, 前揭書, 215면.

존· 분석 등에 관한 법률 규정이 미비하여 이에 대한 문제가 있고, 디지털 증거에 대한 압수· 수색시에도 일반 전통적인 증거의 압수· 수색에 의한 형사소송법 규정이 디지털 증거에도 완벽히 적용이 될 수 있는지에 대하여는 디지털 증거의 특성상 많은 문제점을 내포하고 있다.

디지털 증거를 강제처분에 의하여 압수· 수색할 경우에도 우리 헌법상 영장주의의 원칙이 적용됨은[142] 위에서도 설명하였다. 적법절차의 원리에서 나온 영장주의는 압수· 수색 여부도 헌법 제103조에 의해 헌법과 법률에 의하여 양심에 따라 재판하고, 사법권 독립의 원칙에 의하여 신분이 보장된 법관의 판단에 의하여만 결정되어야 한다는 것까지 의미한다.[143]

따라서 이러한 영장주의 원칙은 수사기관에 의해 디지털 증거를 압수· 수색함에도 헌법상 국민의 기본권 보호의 필요성에 의거 반드시 지켜져야 한다.[144] 디지털 증거를 임의 제출하는 경우에도 영장주의의 원칙은 적용되어야 한다.

2. 영장발부의 요건

142) 憲裁에 의하면 영장주의란 헌법상 신분이 보장되고(헌법 제106조), 직무활동의 독립성이 담보되는(헌법 제103조) 법관이 발부한 영장을 제시하지 아니하고는 수사에 필요한 강제처분을 하지 못한다는 원칙을 말한다. 憲裁, 1993. 12. 23. 고지 93헌가2, 憲裁判例集, 제5권 제2집, 596면.

143) 憲裁, 1992. 12. 24. 고지 92헌가8 결정; 1993. 12. 23. 고지 93헌가2 결정, 憲裁判例集, 제5권 제2집, 596면.

144) 憲裁는 영장주의의 의의에 대하여 다음과 같이 설명하고 있다. “영장주의란 형사절차와 관련하여 체포· 구속· 압수· 수색 등의 강제처분을 함에 있어서는 사법권 독립에 의하여 그 신분이 보장되는 법관이 발부한 영장에 의하지 않으면 아니 된다는 원칙이고, 따라서 영장주의의 본질은 신체의 자유를 침해하는 강제처분을 함에 있어서는 중립적인 법관이 구체적 판단을 거쳐 발부한 영장에 의하여만 한다는 데에 있다고 할 수 있다” 憲裁 1997. 3. 27. 선고, 96 헌바 28·31·32(병합), 형사소송법 제70조 1항 위헌소송 등, 憲裁判例集 제9권 1집, 313면.

우리 헌법 제12조 3항은 영장주의의 대원칙을 천명하고 있음은 앞에서도 설명하였다. 수사기관의 압수· 수색은 형사소송법에 있어서 가장 중요한 강제처분이므로 헌법상 보장된 국민의 기본권을 보호하기 위하여 영장주의는 반드시 지켜져야 한다.

수사기관에 의한 영장의 발부는 검사의 청구에 의하여 판사가 발부하며, 사법경찰관은 검사에게 신청하여 검사의 청구로 판사가 발부한다. 따라서 수사기관은 강제처분을 행할 경우에 반드시 법관이 발부한 영장을 제시하여야 한다. 그리고 이 경우에 제시되는 영장은 반드시 정본이어야 하고, 사본 제시는 허용되지 않는다.[145]

법원이 공판정에서 압수· 수색을 행할 때에는 영장을 요하지 않는다. 이는 법원이 공판정에서 직접하는 처분이므로 영장주의의 예외가 아니다.[146] 그러나 공판정 외에서 압수· 수색을 행할 때에는 영장을 발부하여야 한다고 규정하고 있다.

이러한 영장발부 요건은 디지털 증거의 압수· 수색에 관하여도 반드시 지켜짐으로써 헌법상 보장된 국민의 기본권이 침해되지 않고 보장될 수 있도록 해야 한다.

3. 일반영장 금지

헌법상의 영장주의 원칙에 근거하여 형사소송법 제113조는 공판정외에서 압수· 수색을 함에는 영장을 발부하여 시행하도록 하고 있다. 동법

145) 대판 1996. 8. 8, 95나54753. 급속하게 연행하여야 할 필요가 없음에도 불구하고 피의사실 요지의 고지 및 구속영장 정본의 제시없이 영장표지의 사본 제시만으로 강제 연행한 것은 불법연행이다. 또한 수사기관이 압수· 수색 영장없이 공항의 보안구역내에서 피의자의 수하물을 임의로 개봉·수색한 행위는 비록 그것이 관세청 직원의 입회하에 이루어졌다 하더라도 영장주의에 반하는 위법한 행위이다.

146) 李在祥, 前揭書, 273면.

제114조는 압수· 수색영장에는 피고인의 성명, 죄명, 압수할 물건, 수색할 장소, 신체, 물건, 발부연월일, 유효기간과 그 기간을 경과하면 집행에 착수하지 못하며 영장을 반환하여야 한다는 취지 기타 대법원 규칙으로 정한 사항을 기재하도록 하고 있고, 동법 제219조에 의해 검사 또는 사법경찰관의 압수· 수색에도 준용되고 있으며, 이것은 일반 영장 금지원칙을 규정한 것이다.[147] 이는 수사기관에 부여된 압수· 수색의 범위를 명확히 하여 이를 남용하여 권한 외의 물건을 압수· 수색하지 못하도록 하며 처분 받은 자의 물건소지에 대한 안전을 해하지 않도록 하기 위함이다. 다른 한편으로는 수사기관이 압수· 수색을 함에 있어 영장을 제시하도록 하고, 피고인, 피의자 및 변호인을 참여할 수 있게 하여 수사기관에게 부여된 압수· 수색권한을 넘어 권한 외의 물건까지 불법으로 압수· 수색하는 경우, 즉시 이의를 제기나 취소 할 수 있게 하여 재산권을 방위할 수 있게 하려는 규정이다.[148]

이러한 일반영장금지의 원칙은 컴퓨터와 관련된 디지털 범죄에 있어 디지털 증거를 수집함에 있어서도 당연히 적용이 되어야 함은 물론이다. 특히 디지털 범죄의 경우에는 수사기관에 의한 포괄적인 압수· 수색이 이루어지는 것이 현실이다. 결국 이는 수사기관에 의하여 압수· 수색범위를 초과하여 수사하는 결과를 낳고, 또한 국민 개인의 기본권인 사생활이 침해되는 것을 야기한다. 따라서 디지털 범죄의 경우는 수사시에 구체적인 영장의 기재로 기본권이 침해되지 않도록 각별히 주의해야 할 것이다.

4. 영장의 특정

147) 申東雲,「刑事訴訟法Ⅰ」, 法文社, 1996, 220면.
148) 吳寄斗, 前揭論文, 92면.

디지털 증거에 대한 압수· 수색의 경우 피의자가 소지하는 컴퓨터에 저장될 수도 있고, 원격지에 있는 서버시스템에 저장될 수도 있어 특정이 쉽지는 않다. 파일이 암호화되어 있을 수도 있다. 따라서 이러한 불확실성 때문에 압수· 수색영장 신청시 상당한 이유를 제시하기 어렵고 필요한 파일이 무엇이고, 어디에서, 무엇을 검색해야 할지를 특정하기 어려운 점이 있으므로 담당 수사관은 수색대상 시스템에 대한 가능한 한 많은 정보를 알아내야 하지만 이는 개인의 사생활을 침해할 우려가 있다. 이런 이유로 압수· 수색 영장을 신청할 경우에는 개인정보보호법, 정보통신망법, 형사법 등을 고려해야 한다. 이와 같은 점을 고려하여 압수· 수색 방법을 결정해야 한다.[149]

디지털 증거에 있어서 영장에 의하여 압수· 수색이 허용되는 범위는 원칙적으로 영장에 명시된 압수· 수색의 대상에 대해 상당한 이유가 인정되는 장소나 물건에 한정된다. 특히 유죄를 입증할 만한 증거로 컴퓨터 관련 디지털 자료 및 정보, 저장· 기억매체, 출력물 그리고 범죄와 관련된 디지털 관련 부품들이 될 것이다.[150] 영장에 의거하여 수색할 장소 및 물건의 특정· 명시라는 요건은 그 대상이 어느 정도로 특정되어야 충족되는 것인지 문제가 될 수 있는데, 이는 구체적인 사안에 따라서 합리적으로 판단되어야 한다.[151]

디지털 범죄에 있어 증거의 범위를 영장에 특정하는 경우에 있어서 범위가 개괄적이고 포괄적인 기재방법이 허용되는 경우에는 압수· 수색시 디지털 증거의 특성상 개인의 사생활이 침해되는 문제가 발생할 수 있다. 또한 압수· 수색의 대상이 특정되지 않는 영장에 의하여 수집된 디지털 증거라면 일반영장을 금지하는 영장주의의 원칙에 비추어 위법한

149) CCIPS, Ibid, p.58.; 梁根源, 前揭論文, 69면.
150) 吳寄斗, 前揭論文, 95면.
151) 일본 최고재판소는 압수물의 특정정도에 관해 압수할 물건을 예시한 후 “기타 본건에 관계가 있다고 생각되는 일절의 문서 및 물건이라고 기재하는 영장이 특정성을 결하고 있는 것은 아니다”라고 판시하고 있다. 이훈동, 전게논문, 943; 원혜욱, 전게논문, 122면.

절차에 의해 수집된 증거로서 그 증거능력을 부정해야 할 것이다.[152]

디지털 범죄에 있어 수사기관의 청구에 의해 법관이 영장을 발부 할 때에는 디지털 기록으로부터 출력된 서면 또는 출력할 만한 서면으로서, 그것이 당해 '범죄와 관련되고 구체적으로 특정되어 있을 때 압수나 출력을 허가한다' 는 문구를 영장에 기재하도록 하는 것이 타당할 것이다.

그러나 영장자체에 압수· 수색이나 출력대상인 컴퓨터와 관련된 디지털 증거물을 특정하기에는 현실적으로 디지털 증거의 특성상 어려움이 많을 것이다. 즉 영장기재의 특정성 정도에 관해 처음부터 디지털 저장매체의 종류 및 명칭, 압수목적인 파일의 명칭 및 그 특징, 처리목적의 프로그램의 명칭 및 특징, 시스템의 명칭, 컴퓨터 하드웨어의 형식 등을 특정해야 한다는 견해도 있으나,[153] 수사의 초기단계에서는 구체적인 범죄내용이 판명되지 않는 경우가 많아 범행현장에 임하여 비로서 압수 필요성이 있는 물건의 구체적인 내용 및 범위가 판명될 것이므로, 영장청구의 단계에서 미리 위와 같이 압수하고자 하는 정보의 특정, 명시를 요구하는 것은 무리가 있다 하겠다. 따라서 영장의 기재는 지나치게 포괄적이지 않는 경우에는 어느 정도 개괄적으로 기재되어도 무방하다고 하겠다. 특히 디지털 범죄와 관련된 증거의 경우에는 명시성, 특정성의 요건을 어느 정도 완화하는 것이 상당하다고 하겠다.[154] 그러나 디지털 범죄에 관련된 압수· 수색을 함에 있어서 현행법상 어떠한 명문 규정이 존재하지 않는 이상 수사기관의 필요성에 의해 특정을 인위적으로 하는 것은 헌법상 적법절차에 위반된다고 볼 것이며, 이러한 문제는 입법을 통하여 현행 법률의 개정 및 새로운 법률의 제정을 통해 개선· 해결해야 할 것이다.

152) 吳寄斗, 前揭論文, 105면.
153) 安富 潔, 前揭書, 146면.
154) 吳寄斗, 前揭論文, 107면.

제2절 영장주의의 예외

1. 법률상 영장주의의 예외 규정

현행 헌법 제12조 3항의 단서는 '현행 범인인 경우와 장기 3년 이상의 형에 해당하는 죄를 범하고 도피 또는 증거인멸의 염려가 있는 때에는 사후영장을 청구할 수 있다' 고 규정하여 영장제도의 예외를 규정하고 있다. 또한 가택 수색시에는 헌법 제16조에 의거하여 영장의 제시가 필요하며, 압수· 수색영장에는 압수할 물건과 수색할 장소가 구체적으로 명시되어야 한다.

우리 형사소송법에서의 영장은 사전영장임을 원칙으로 하지만, 긴급체포, 현행범인의 체포, 체포목적의 수색, 체포현장에서의 압수· 수색· 검증, 범죄현장에서의 압수· 수색에서 보는 것처럼 긴급성에 대처하기 위하여 영장주의의 예외가 인정되고 있다. 이러한 영장주의의 예외에는 범죄장소에서의 압수· 수색처럼 사후에 영장을 요하는 경우와 임의제출물의 압수, 체포목적의 수색, 체포현장에서 압수· 수색처럼 사후에도 영장을 요하지 아니하는 경우가 있다.[155]

특히 디지털 증거들은 일반 증거와 비교하여 증거를 위조· 변조· 삭제· 수정· 조작이 쉽기 때문에 증거 인멸의 가능성이 매우 높다. 그래서 디지털 증거 압수· 수색에 있어서도 영장제도의 예외는 당연히 인정된다고 할 수 있을 것이다. 이에 근거하여 현행 형사소송법 규정 제200조의3 제1호에서 '피의자가 증거를 인멸할 염려가 있을 때', 동법 제212조 '현행 범인은 누구든지 영장 없이 체포할 수 있다' 고 규정하여 영장없이 피의자나 피고인을 체포한 현장에서 압수· 수색할 수 있다.

---

155) 정웅석,「형사소송법(제2판)」, 大明出版社, 2005, 186-187면.

이러한 형사소송법 규정에 근거하여 체포된 피의자가 소유, 보관하는 컴퓨터 관련 디지털 증거에 대하여 현재에는 적용을 하고 있지만, 디지털 증거의 특성상 완벽하게 적용하기에는 문제점이 많이 있다고 하겠다.

2. 디지털 범죄와 영장주의의 예외

디지털 범죄에 있어서 디지털 증거만의 특성을 전혀 고려하지 않고, 영장없이 디지털 증거를 수집하는 요건과 방식, 범위 등에 대하여 현재는 구체적인 법률 규정이 없어 문제가 제기될 수 있다. 이는 결정적으로 헌법상 보장된 국민의 사생활 비밀과 자유를 침해하고, 적법한 절차를 위반하는 결과를 초래한다고 본다. 수사기관이 실체적 진실을 발견하기 위하여 수사상, 재판상의 편의만을 위해 위법한 절차에 의해 수집된 디지털 증거의 증거능력은 당연히 배제되어야만 할 것이다.

디지털 범죄와 관련된 디지털 증거에 관하여 현재 우리 나라에서는 영장제도와 관련하여 문제가 제기된 사례도 없고, 거의 논의가 되지 않았다. 그러나 앞으로는 디지털 증거와 관련된 영장제도에 있어 현행 형사소송절차에 의해 해결을 하고자 한다면, 많은 문제점이 제기될 것으로 예상된다.

따라서 다음절에서 미국의 경우에는 컴퓨터와 관련된 디지털 증거를 영장없이 압수 · 수색을 어떠한 방식으로 하며, 이에 대하여 어떠한 견해를 갖고 이 문제를 해결하는지 영장주의의 내용과 예외 사항을 구체적으로 살펴보고자 한다.

미국의 사례들을 심도있게 고찰하여 우리의 영장제도와 관련된 법률 개정에도 참고를 해야 할 것이며, 디지털 범죄의 해결에도 또 다른 해결책을 제시하리라 본다.

제3절 디지털 범죄에 관한 미국의 영장주의

1. 요건

미연방 수정헌법 제4조[156]는 수사기관에 의한 부당한 압수· 수색과 일반 영장을 금지하고 있다. 이 조항에 의하여 압수· 수색을 하기 위해서는 첫째, 죄를 범하였다고 의심할 만한 상당한 이유가 존재하고, 둘째, 그 범죄를 입증할 수 있는 개연성이 높은 증거나 압수 대상물의 특정 셋째, 압수대상물이 존재할 개연성이 높은 장소에 한하여 수색의 제한 등과 같은 실체적인 요건과 중립, 공평한 입장에 있는 제3자인 법관에 의한 사전심사라는 절차적 요건을 충족하여야 만이 디지털 증거의 압수· 수색이 가능하다고 규정하고 있다.

이 헌법의 영장발부 요건은 수사기관에 의한 디지털 범죄 수사에 있어 디지털 증거의 압수· 수색에 관하여도 반드시 지켜짐으로써 국민의 기본권이 침해되지 않고 보장될 수 있도록 해야 한다.

이하 미국에서는 디지털 증거에 관하여 헌법상 영장 발부의 요건을 어떻게 보는지 살펴보겠다.

가. 상당한 이유(probable cause)

미국은 수사기관이 범죄 증거에 관하여 압수· 수색을 할 경우에는 미

156) 미연방 수정헌법 제4조(수색 및 체포 영장) 부당한 수색, 체포, 압수로부터 신체, 가택, 서류 및 통신의 안전을 보장받는 인민의 권리는 이를 침해할 수 없다. 체포, 수색, 압수의 영장은 상당한 이유에 의하고, 선서 또는 확약에 의하여 뒷받침되고, 특히 수색될 장소, 체포될 사람 또는 압수될 물품을 기재하지 아니하고는 이를 발급할 수 없다.

연방 수정헌법 제4조에서 규정하는 선서나 서약에 의해 지지되는 '상당한 이유'를 압수· 수색영장의 합리성을 보장하는 요건이라고 본다.[157] 이를 논의하는 실익은 위법수집증거의 배제법칙 적용여부를 결정하기 위함이다. '상당한 이유'의 증명은 유죄 입증에 필요한 '합리적 의심을 넘는 정도의 증명(proof beyond a reasonable doubt)'까지는 필요하지 않지만, 전체사정을 종합하여 그 압수대상물이 증거로 될 수 있다는 개연성이 증명되는 정도면 족하다.

수사기관은 영장담당 법관에게 압수· 수색이 필요한 이유를 '증거'로서 증명하지 않으면 안되고, 법관은 범죄가 행하여졌다는 것, 범죄와 관련 있는 물건, 범죄의 증거 등이 당해 장소에 존재한다는 것에 관하여 전체적인 사정을 종합적으로 고려하여 판단해야 한다.[158]

영장발부의 근거가 되는 선서진술서에 허위의 사실이 포함되어 있고 그러한 사실을 영장청구자가 알고 있었거나 알 수 있었을 경우가 있다.

---

157) 미국 형사절차법에서 '상당한 이유'의 요건은 단순한 혐의 이상의 것으로 '합리적 인간(reasonable person)'의 기준으로 체포· 압수· 수색이 정당화되기에 충분한 증거가 있을 때 충족된다[Bringer v. United States, 338 U.S. 160 (1949)]. 통상 영장을 통한 체포· 압수· 수색의 경우는 경찰관이 영장 없는 체포· 압수· 수색의 경우는 치안판사(magistrate)가 '상당한 이유'의 판단자가 된다. '상당한 이유'는 경찰관의 직무질문을 위한 '정지'를 위해서는 필요하다[Terry v. Ohio, 392 U.S. 1(1968)]. 그러나 '정지'도 '막연한 혐의'로는 부족하고 '객관적 사실에 기초한 합리적 의심'이 필요하다[Brown v. Texas, 443 U.S. 47, 48 (1979); U.S. v. Sokolow, 490 U.S. 1, passim (1989)]. 조 국, 전게서, 22면, 각주6 참조.

158) Illinois v. Gates 이 사건은 경찰이 익명의 정보제공자 편지에 의하여 피고인들의 범죄행위에 대한 정보를 입수했고, 경찰에 의하여 그 편지 내용의 진실성이 입증되어 수색영장이 발부되었다. 수색의 결과 마약거래의 증거가 발견되어 유죄를 선고했다. 미 연방대법원은 상당한 이유가 제시되지 않았다는 피고들의 주장을 배척하면서 정보제공자를 이용하는 상황의 완전성(totality of the circumstances)을 채택했다. 상황의 완전성이란 정보제공자의 정보와 같은 전문이 체포 또는 수색영장을 발부하기 위한 상당한 이유를 입증하는데 충분히 믿을 수 있는 것인지 여부를 결정하는 기준을 말한다. 이 판결에서 렌퀴스트 대법관은 영장담당법관은 전문정보를 제공하는 자의 신용성(veracity)과 지식의 기초(basis of knowledge)를 포함하여 선서진술서에 진술되어 있는 전체 사정에 비추어 금제품이나 범죄의 증거가 특정장소에서 발견될 것이라는 '상당한 개연성'이 있는지 여부를 경험적으로 결정하게 된다고 판시하였다. Illinois v. Gates, 462 U.S. 213, S.Ct. 2317, 76 L.Ed.2d 257 (1983); 安富 潔, 前揭書, 23면.

이때에는 영장의 적법성에 대해 수사관을 신뢰하는 것이 객관적으로 합리적이라고 할 수 없기 때문에 그 선서진술서에 기초하여 잘못 발부된 영장에 기해 취득한 증거는 유죄인정의 증거로부터 배제되어야 한다.[159] 다만, United States v. Leon 판결[160] 및 Massachusetts v. Sheppard 판결은[161] 법관이 적법하게 영장을 발부하였다고 신뢰하고 수색을 행하였으면, 그 후 영장 발부에 하자가 있어 당해 영장이 무효가 되는 사정이 있었다고 하더라도 그 영장의 적법성을 신뢰하고 이루어진 압수·수색활동에 기해 수집한 증거에 대해서는 '선의의 예외법칙(good faith exception)'에 의해 증거배제법칙이 적용되지 않는다고 하였다. 이에 대한 구체적인 예로 위 판결들은 ① 영장청구자가 허위라는 점을 알고 있었거나 당연히 그 사실을 알 수 있었을 허위진술서에 기해 잘못된 영장이 발부된 때 ② 중립적이고 공평한 입장에 있는 법관이 날인하여 영장을 발부하였고 ③ 상당한 이유를 찾아 볼 수 없는 선서진술서에 기해 영장이 발부된 때 ④ 영장자체에 수색장소나 압수대상물을 특정하고 있지 않은 때 등을 들고 있다.[162]

나. 수색할 장소 및 압수할 물건의 구체적 명시

미연방 수정헌법 제4조에서 요구하고 있는 수색할 만한 장소 및 압수할 만한 물건의 명시는 이른바 일반영장을 금지하기 위해 필요한 요건이다. 그러나 미연방 최고법원은 Massachusetts v. Sheppard 판결에서 '기술적인 오류'에 대해서는 위 헌법규정에 의한 증거배제법칙이 적용되지 않는다[163]고 판시하였다.[164]

---

159) 吳奇斗, 前揭論文, 85면.
160) United States v. Leon, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed. 2d 677 (1984).
161) Massachusetts v. Sheppard, 468 U.S. 981, 104 S.Ct. 3424, 82 L.Ed. 2d 737 (1984).
162) Franks v. Delaware, 438 U.S. 154, 98 S.Ct 2317, 76 L.Ed 2d 257 (1983). 安富 潔, 前揭書, 24면; 吳奇斗, 前揭論文, 85면 재인용.

적법한 영장에 근거한 수사 활동 중 별개의 범죄에 관한 증거나 장물, 또는 범죄에 제공 되었다고 생각되는 물건을 발견한 경우에는 '상당한 이유' 가 있고, '특정성' , '긴급성' 의 요건을 갖추고 있으면, 영장 없이 그와 같은 물건을 압수 할 수 있다는 것이 미연방 최고법원의 판결이다.[165] '상당한 이유' 가 필요하다고 판시한 사례가 Arizona v. Hicks 판결이다.[166] 1984년 4월 제임스 토마스 힉스(James Thomas Hicks)의 방에서 발사된 총알이 계단 밑에 있는 사람에게 명중되어 부상을 입었다. 이 사건을 수사하기 위해 경찰관이 피고인 Hicks의 방에 들어가서 총과 마스크를 압수하였다. 그러나 그 방에는 값비싼 입체음향 장비가 있었고 경찰관은 이것이 절도한 것이 아닌지 의심을 하였다. 그래서 음향 장비의 제조번호를 조사하기 위해 그 입체 음향 장비를 이동시켰다. 압수· 수색대상이 된 총기 범죄와는 관련 없는 별건의 물건에 대해 압수· 수색을 하기 위해서는 압수 대상물의 현재성, 명확성이 인정되는 경우 영장주의 예외 원칙인 plain view doctrine이 적용되지 않는다.

위 사건에서 제조번호를 조사하기 위해 고가의 입체 음향 장비를 이동하고 범죄를 범하였을 것이라는 의심이 든다는 것만으로는 부족하고, 특정범죄를 범하였다고 의심할 만한 '상당한 이유' 가 필요하다고 판시하였다.[167]

---

163) 경찰이 합리적으로 생각할 수 있는 모든 절차를 밟아 두었고, 또한 영장의 유효성에 관하여 영장담당 판사의 확신(affirmation)도 있었다면 경찰의 행동은 객관적으로 보아 합리적이었다고 할 수 있기 때문에 이러한 경우 수정헌법 제4조에 근거한 증거배제법칙은 수사관에 대한 제지효과를 주지 못할 것이므로 이때는 '선의의 예외법칙(good faith exception)' 이 적용되어야 한다고 판시하였다.

164) Maryland v. Garrison, 480 U.S. 79, 107 S.Ct. 1013, 94 L.Ed. 2d 72 (1989). 사건에서 경찰은 한 아파트를 수색하는 영장을 가지고 있었으나, 그와 인접해 있는 다른 아파트를 수색할 필요가 발생했고, 그 다른 아파트를 수색하여 마약을 발견했다. 미 연방대법원은 '수색의 기초가 된 영장은 비록 경찰이 두 주거지역 사이에 명확한 경계가 존재하지 않는 인접한 아파트를 수색했을지라도 무효로 되지 아니 한다' 고 판시했다.

165) Coolodge v. New Hampshire, 403 U.S. 443, 91 S.Ct. 2022, 29 L.Ed. 2d 564 (1971); South Dakota v. Opperman, 28 U.S. 364, 96 S.Ct. 3092, 49 L.Ed.2d 1000 (1976). 安富 潔, 前揭書, 31면.

166) Arizona v. Hicks, 480 U.S. 321, 107 S.Ct. 1149, 94 L.Ed.2d 347 (1987).

컴퓨터와 관련된 디지털 범죄에서의 디지털 증거는 그 특성상 자체로는 가시성, 가독성이 없으므로 컴퓨터의 모니터를 이용하지 않으면 그 내용을 알 수 없다. 따라서 컴퓨터에 의해 작성된 디지털 기록의 내용을 밝히기 위해서는 영장에 수색할 장소가 명확해야 하며, 또한 압수할 디지털 증거물의 구체적인 명시가 기재되어야 할 것이다.

2. 영장의 적용

미연방 수정헌법 제4조는 “부당한 압수· 수색· 체포로부터 신체, 주거, 서류 및 재산의 안전을 보장받는 국민의 권리를 침해하여서는 아니 된다. 그리고 선서 또는 서약에 의하여 상당한 이유가 인정되고 수색할 장소 및 체포할 사람, 압수할 물건 등이 구체적으로 기재되지 아니한 영장은 발부하면 아니 된다”고 하여 압수· 수색에 대한 영장주의의 원칙을 규정하고 있다.

본래 수정헌법 제4조는 FBI와 州 경찰과 같은 수사기관이 미국 국민들에 대하여 압수· 수색을 하는 경우 이에 대한 제한을 규정한 것이었다.[168] 따라서 이러한 미연방 수정헌법 제4조는 디지털 범죄에서 디지털 증거에 관한 압수· 수색 절차에도 당연히 이 조항이 적용이 된다.[169]

---

167) 安富 潔, 前揭書, 31면.

168) Jefferson L. Ingram, Criminal Procedure: Theory and Practice, 2005, p.2.

169) 미국 연방대법원은 1914년 Weeks v. United States, 232 U.S. 383 (1914) 판결에서 형사사건의 증거가 수정헌법 제4조 규정에 위반하여 취득된 것일 경우 피고인의 유죄를 인정하기 위하여 사용될 수 없다고 판시함으로써 개인의 프라이버시를 침해한 압수· 수색으로 수집된 증거의 배제를 선언하는 위법수집증거배제법칙이 도입되었다. 따라서 프라이버시를 침해하거나 영장주의 예외에 해당하는 사항을 위반하여 수집된 증거는 위법수집증거로서 증거능력이 없다고 할 수 있다. 우리나라의 판례는 압수절차가 위법하더라도 증거 자체의 성질·형상에 훼손이 없을 경우 증거로 사용할 수 있다고 하여 증거능력을 인정하고 있었다. 대법원 1996. 5. 14 자96초88 결정; 대법원 1987. 6. 23. 선고 87도705 판결; 1994. 2. 8. 선고 93도3318 판결 참조. 그러나 2007년 11월 20일 대법원은 기존의 원칙을 바꾸는 판결을 하였는데, 위법하게 수집된 증거는 유죄증거로 사용할 수 없다고 판결하였다. 대법원 2007도3061.

이처럼 디지털 범죄와 관련된 수사가 형사절차상 새로운 문제들을 야기하자, 미국 법원들은 수정헌법 제4조와 연방 법률들을 디지털 범죄와 관련된 사건에 어떻게 적용할 것인가를 해석하고 연구하기 시작하였다.

결국 판례를 통해 수정헌법 제4조의 범위 안에서 디지털 기록이 포함될 수 있다고 해석하게 되었고[170] 연방형사소송규칙 제41조의 압수대상으로 명시된 유체물을 예시에 불과한 것으로 해석함으로써 정보에 대한 압수를 긍정하기에 이르렀다.[171]

나아가 미국에서는 이러한 논란의 여지를 감안, 연방 형사소송규칙을 개정하여 현행 미연방 형사소송규칙 제41조 제(a)항 정의 편에서는 압수· 수색 대상인 '물건(property)'의 개념 속에 '정보(information)'을 포함시킴으로써 논란의 소지를 없애고 입법적으로 해결하였다.[172]

미연방 수정헌법 제4조는 수사기관의 부당한 압수· 수색으로부터 개인의 자유를 보장하기 위한 규정인데, 이 수정헌법 제4조에 근거하여 미연방 형사소송규칙 제41조 (b)항은 ① 범죄행위의 증거가 되는 물건 ② 금제품, 범죄에 의해 획득한 물건, 기타 불법적으로 소지한 물건 ③ 범죄행위의 수단으로 이용되거나 이용될 수 있는 물건 ④ 체포할 만한 상당한 이유가 있거나 불법적으로 구속되어 있는 등의 요건을 충족하는 물건 등에 대하여 압수· 수색 영장을 발부 할 수 있도록 하고 있다.

미국에서는 수사기관이 영장을 청구할 때 결정해야 할 가장 중요한 사항은 영장 안에 압수· 수색의 대상을 특정함에 있어서 압수할 수 있는

170) 탁희성,「형사절차법상 digital evidence에 관한 연구(압수· 수색을 중심으로)」, 한국형사정책연구원, 2002. 12.

171) United States v. New York Telephone Co. U.S. 159, 169, 98 S.Ct. 364, 54 LEd. 2d 376 (1997).

172) [Federal Rules of Criminal Procedure Rule 41]. Search and Seizure (a) Scope and Definitions. (1) Scope. This rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances. (2) Definitions. The following definitions apply under this rule: (A) "Property" includes documents, books, papers, any other tangible objects, and information.

대상이 컴퓨터 하드웨어 그 자체인가 아니면 하드웨어에 저장된 디지털 자료인가의 여부라고 할 수 있다.

따라서 하드웨어 자체가 압수· 수색의 대상이라면 영장에 하드웨어 자체를 기술해야 하는데 반해서 압수· 수색의 근거가 되는 상당한 이유가 단지 디지털 데이터에만 관련되어 있다면 영장에는 물리적인 저장장치 보다는 해당 데이터 또는 파일 내용을 기술해야 한다. 압수· 수색의 대상으로서 '기록(record)'과 '정보(information)'라는 용어는 모든 전기적, 전자적 또는 마그네틱 형태를 포함해서 어떠한 형태로 어떠한 수단에 의하든 그것이 만들어지거나 저장되어진 증거와 관련된 모든 항목을 포함한다. 따라서 영장 작성시 가능한 한 이 범위를 제한해야 하지만 구체적인 사안에 따라 합리적으로 판단되어야 한다.[173]

제4절 미국에서 디지털 범죄에 관한 영장주의 예외

미국에서는 영장주의 예외[174]로 수사기관은 영장 없이도 압수· 수색이 가능한 경우로 긴급성이 인정되는 경우(exigency circumstance exception),[175] 압수· 수색에 대한 동의가 있는 경우,[176] 적법한 체포에 부수된 수색(search incident to a lawful exception),[177] 피처분자가 임의로

173) 탁희성, 전게논문, 76면; 원혜옥, 전게논문, 124면.

174) 미국 헌법에서 영장없이 체포· 수색· 압수할 수 있는 경우는 다음과 같다. ① '체포'에 관해서 현행범은 영장없이 체포할 수 있고, 중죄에 관해서는 피의자가 범죄를 범하였다고 믿을 만한 상당한 이유가 있는 경우에는 체포할 수 있다. ②모든 범죄에 있어서 영장 발부 전에 도피할 우려가 있는 경우에는 영장없이 체포할 수 있다. ③피의자가 합법적으로 체포된 경우 범죄의 수단 또는 범죄의 결과물을 압수· 수색하는 경우에는 영장이 필요 없다. 그것은 범인이 소유하고 직접 점유하고 있는 장소와 물건에 한하며 그 압수· 수색의 시간도 체포와 함께 이루어지는 경우에 한한다.

175) Warden v. Hayden, 387 U.S. 294, 298-99, 87 S.Ct. 1642 18 L.Ed. 2d 782 (1967).

176) Schneckloth v. Bustamonte, 412 U.S. 218, 93 S.Ct. 2041, 36 L.Ed. 2d 854 (1973).

디지털 증거를 제출한 경우, 명확성이 인정되는 Plain-view 원칙,[178] 자동차 수색(automobile exception),[179] 압수 대상물의 현재성, 일시정지 후 즉시검문(stop and frisk exception),[180] '긴급성의 예외'가 인정되는 경우 등은 영장을 발부 받을 만한 시간적 여유가 없고, 증거인멸의 우려가 높기 때문에 영장 없이도 압수· 수색 할 수 있도록 허용하고 있다.[181]

이하의 사례에서는 기존의 전통적인 범죄 판례들이 디지털 범죄와 관련된 디지털 증거에서는 어떠한 방식으로 도출이 되어 적용이 되는지 다

177) United States v. Robinson, 414 U.S. 218, 234-36, 94 S.Ct. 467, 38 L.Ed. 2d 427 (1973).

178) Plain View에 해당하여 영장 없이 압수할 수 있는 경우는 다음과 같다. ①경찰관이 합법적으로 압수할 수 있는 장소에서 압수의 대상을 발견한 경우 ②범죄에 연루된 물건임이 명백한 경우 ③경찰관이 수정헌법 제4조에 위반되지 않고 물건에 대한 지배와 관리 권한을 획득할 수 있는 경우이다.

179) United States v. Ross, 456 U.S. 798, 809, 102 S.Ct. 2157, 72 L.Ed. 2d 572 (1982). 미국법상 체포에 수반하여 행해지는 차량에 대한 압수· 수색의 경우는 차량 전체 내부, 트렁크 등을 영장 없이 수색이 허용된다. 이 사건은 경찰관이 마약이 숨겨져 있을지도 모르는 상당한 이유를 가지고 피의자의 자동차 내부와 트렁크를 영장없이 수색을 하였다. 경찰관은 피의자(Ross)가 판매하기 위하여 보관하고 있던 마약을 발견했다. 이에 대하여 미 연방대법원은 '경찰이 자동차를 수색할 상당한 이유가 있는 경우에 목적물이 숨겨져 있을 자동차 내부에 대하여 합법적으로 수색할 수 있다' 고 판시했다. 오범석,「미국의 압수· 수색제도에 관한 연구」, 법무부, 2006, 33면; 이러한 영장 없는 '자동차 수색의 예외(automobile search warrant exception)'는 우리 법상으로는 경찰관직무집행법상의 불심검문이나 형사소송법 제216조 1, 3항이나 제217조의 요건에 해당될 경우 인정될 것이다. 조 국,「위법수집증거배제법칙」, 博英社, 2005, 354면.

180) 불심검문의 원류인 미국 Terry v. Ohio, 392 U.S. 1, 88 S.Ct. 1868, 20 L.Ed. 2d 889 (1968) 판결은 불심검문을 위해서 '상당한 이유'가 필요하지는 않지만. '막연한 혐의(vague suspicion)'로는 부족하고 '객관적 사실에 기초한 합리적 의심(reasonable suspicion based on objective facts)'이 필요하다[Brown v. Texas, 443 U.S. 47, 48 (1979); U.S. v. Sokolow, 4901 U.S. 1, passim (1989)]. 조 국, 上揭書 332면.

181) ① 美國判例: 긴급한 경우에 영장 없이 타인의 주거, 피의자의 신체 등을 수색하는 것까지도 정당시되는「긴급수색」에 대하여, 미연방대법원은 Coolidge v. New Hamphshire, 403 U.S. 443 (1971); Vale v. Louisiana, 399 U.S. 305 (1970); Chimel v. California, 395 U.S. 752 (1969)사건에서 "영장을 발부받기 위하여 지체함으로써 경찰관을 위태롭게 하거나 증거인멸을 초래할 경우에는 영장 없는 수색이 허용된다" 고 판시하였다.
② 日本判例: 마약단속관이 피의자를 긴급체포하기 위하여 그 자택에 갔던 바, 피의자가 외출중이므로 가택 수색을 개시하여 마약을 압수하고, 수색이 끝날 즈음에 귀가한 피의자를 긴급체포한 경우, 위의 압수· 수색은 체포에 선행된 것이기는 하나, 시간적으로 체포와 밀착하고 장소적으로 체포의 현장과 동일하기 때문에 위헌·위법이라고 할 수 없다. [最大判 1961 (昭和 36). 6. 7. 刑集 15권 6호 915면; 權寧星,「憲法學原論」, 法文社, 2007. 2, 459면.

양한 사례를 들어 구체적으로 살펴보고자 한다.

1. 긴급한 상황(exigency circumstance)

미국의 수사기관은 경찰관 또는 시민들의 신체적인 손상(physical harm)을 방지할 필요가 있거나, 증거와 관련된 것을 인멸할 우려가 있는 경우, 용의자가 도주의 우려가 있는 경우, 적법한 법집행을 방해할 현저한 우려가 있는 경우 등 긴급한 상황에 의거하여 영장주의의 예외로서 영장없이 수색할 수 있다.[182]

긴급한 상황의 여부를 판단하기 위해 수사기관이 고려해야 할 사항은 다음과 같다. ①긴급한 상황의 정도(the degree of urgency involved),[183] ②영장을 발부 받기 위해 걸리는 시간(the amount of time necessary to obtain a warrant) ③증거의 인멸(removed or destroyed)이 임박한 경우,[184] ④사건 현장의 위험 발생 가능성(the possibility of danger at the site) ⑤밀수품 또는 증거들을 소지한 자가 경찰관이 추적하는 정보를 인지 한 경우 ⑥밀수품 또는 증거들을 폐기 또는 파괴할 수 있는 준비가 된 경우이다.[185]

특히 긴급한 상황은 컴퓨터와 관련된 디지털 범죄 사건에 있어서도 자

182) United States v. McConney, 728 F.2d 1195, 1199 (9th Cir. 1984).

183) 미국의 O. J. Simpson 사건에서 경찰은 피고인의 집에 새벽 5시경 도착하여 집 앞에서 세워져 있는 자동차에 핏자국이 있음을 발견하였다. 경찰은 초인종을 눌렀으나, 응답이 없자 약 1.5m 가량의 담장을 넘어 집안을 수색하여 피 묻은 장갑 등의 증거물을 찾았다. 재판과정에서 피고의 변호인들은 위 증거들은 영장없이 수집된 것으로서 증거능력을 부인해야 한다고 주장하였으나, 법원은 급박한 상황을 내세워 이를 받아들이지 않았다.

184) Cupp v. Murphy, 412 U.S. 291 (1973). 피고인은 처의 사망에 대하여 진술하기 위해 경찰서에 자진출석하였는데, 경찰관은 피고인의 손가락에서 혈액으로 보이는 흔적을 발견하였다. 경찰관은 피고인에게 그 흔적을 채취할 것을 요구하였고, 피고인이 이를 거절하자 강제로 이를 채취하여 피해자의 피부조직을 발견하였다. 법원은 위 수색이 증거인멸의 급박한 우려에 의한 것으로 영장을 요하지 않는다고 판시하였다.

185) United States v. Reed, 935 F.2d 641, 642 (4th Cir. 1991).

주 발생하는데, 그 이유는 디지털 자료들은 간단한 컴퓨터 키보드의 작동이나 명령으로 순식간에 증거를 인멸· 삭제할 수 있고,[186] 또한 습기, 온도, 진동, 물리적인 훼손, 강력한 자성물체를 통과시켜 디지털 증거를 훼손시킬 수 있기 때문이다.[187] 따라서 이러한 경우에는 다른 전통적인 증거방법보다는 긴급한 상황의 원칙이 적용되어 영장없는 압수· 수색이 정당화 될 여지가 많다.

예를 들어 압수대상의 컴퓨터 모니터 스크린 상에 저장되지 않은 정보가 있는 경우 멸실될 위험이 있다고 믿을 만한 상당한 이유가 있다면, 긴급한 상황의 원칙이 적용되어 영장없이 그 정보를 저장하고 압수하는 것이 가능하다는 것이다. 특히 디지털 범죄의 증거 또는 범행의 도구가 되는 디지털 데이터가 피의자의 컴퓨터에 저장되어 있지 않고, 온라인으로 다른 지역에 연결된 보조기억장치로부터 온 것이라면 수사기관이 현장에 있는 대상 컴퓨터를 압수하더라도 그 정보가 저장되어 있는 컴퓨터를 통해서 또는 네트워크를 통하여 연결되어 있는 제3의 컴퓨터를 이용하여 얼마든지 데이터의 인멸 또는 변조가 가능하다.

만약 이러한 사실을 수사기관이 미리 알고 있다면 각 컴퓨터를 대상으로 각각의 수색영장을 발부받아야 하는 것이 원칙이다. 그러나 이러한 것을 미리 예측하지 못하는 경우에는 긴급한 상황의 원칙을 적용하여 영장없이 압수· 수색이 가능한지를 판단하여야 한다.

이를 판단하기 위하여는 다음과 같은 요소를 고려하여야 한다. (1) 긴급성의 정도와 영장을 얻는데 소요되는 시간 (2) 증거물이 파괴될 우려가 있다고 믿을 만한 상당한 이유가 있는지 여부 (3) 압수물의 소유자가

186) United States v. Doe, 61 F.3d 107, 110-11 (1st Cir. 1995). 긴급한 상황의 예외에 해당하는 경우라도 수사기관으로 하여금 증거인멸을 방지하기 위한 행위 이상을 허용하는 것은 아니며 긴급 상황이 종료하면 영장 없이 수색하는 행위도 종료되어야 한다고 한다.

187) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, *op. cit,* p.19.

수사가 진행되고 있는 사실을 알고 있는지 여부 (4) 증거물 자체의 성질상 파괴 및 멸실이 용이한 것인가 등 이다.[188]

이와 관련된 사례로 David 사건에서 수사관은 피의자가 컴퓨터 메모북(computer memo book)에서 파일을 지우고 있는 것을 목격하고 컴퓨터를 즉시 압수하였다. 이에 대하여 지방법원은 수사관이 메모북을 압수하는 데는 영장이 필요 없다고 판결하였다. 왜냐하면 피고의 행위는 긴급한 상황에 해당하기 때문이다. 이러한 경우에 영장 없는 압수· 수색을 인정하지 않게 되면 디지털 증거의 속성상 사후에 증거를 확보할 수 있는 방법이 없기 때문이다.[189]

이와 유사한 또 다른 사례로 Romero-Garcia 사건에서 지방법원은 수사관이 긴급하게 피의자가 소지한 호출기의 디지털 정보에 엑세스 한 것은 정당하다고 했는데, 그 이유는 증거의 인멸을 막을 필요성이 있다고 믿을 만한 합리적인 이유가 있었다고 판결하였다. 왜냐하면 호출기에 저장된 디지털 정보는 쉽게 파괴· 삭제· 멸실될 수 있으며, 호출기에 새로운 메시지가 들어옴으로써 기존에 저장되어 있던 디지털 자료 또는 정보들이 삭제될 수 있으며, 또한 배터리가 방전되면서 정보들이 삭제되거나, 피의자가 인위적으로 삭제할 수도 있기 때문에 수사관이 영장없이 호출기의 정보 및 디지털 자료들을 수색한 것은 정당하다고 판결하였다.[190]

또 다른 사례로 Gorshkov 사건으로 러시아 사람의 컴퓨터 내부 안에 디지털 범죄와 관련된 증거가 존재하고, 지금 당장 이 디지털 증거를 수색하지 않으면 증거를 인멸할 수 있는 상당한 이유가 존재하므로, 이 컴퓨터의 디지털 자료에 대하여 영장없이 수색함은 긴급한 상황에 비추어 정당하다고 판결하였다.[191] Ortiz 사건에서는 수사관이 피의자를 체포

188) U.S. v. Rubin, 474 F. 2d 262 (3d Cir. 1973).
189) United States v. David, 756 F. Supp. 1385 (D. Nev. 1991).
190) United States v. Romero-Garcia, 991 F. Supp. 1223, 1225 (D. Or. 1997).

하고, 이에 수반하여 피의자의 주머니에서 호출기 찾아 번호들을 검색한 행위는 정당하다고 판결하였는데, 그 이유는 호출기에 있는 디지털 정보들은 파괴· 삭제· 멸실되기 쉽기 때문이라고 판결하였다.[192]

그러나 Reyes 사건에서는 수사관이 호출기의 수색에 관한 긴급 상황은 정당화되지 못하였는데, 그 이유는 수사관이 불법적으로 호출기를 켜서 긴급한 상황을 만들었기 때문이다.[193]

디지털 증거와 관련하여 긴급한 상황의 필요성은 디지털 증거의 삭제 또는 멸실되는 것을 막는 것까지이며 그 이상에 대하여는 영장없는 압수· 수색은 허가하지 않았고, 긴급한 상황이 종료되었을 때는 영장없는 수색도 더불어 종료가 된다. 따라서 디지털 증거가 삭제되는 것을 막는 단계를 밟아야 할 것이며, 수사기관은 더 이상 영장 없이 수색을 할 수 있는 권한이 없다.[194]

David 사건에서 수사기관이 컴퓨터에 저장된 디지털 정보의 멸실과 훼손을 막기위해 컴퓨터 하드웨어의 압수는 가능하지만, 영장없이 계속적으로 컴퓨터의 디지털 정보를 수색하는 것은 불가능하다고 판결하였다.[195]

2. 동의(同意)가 있는 경우

수사기관이 피의자에 대한 범죄혐의를 갖고 있으나, 법률상 강제처분을 할 근거가 없는 경우에 피의자의 동의는 증거수집에 결정적인 역할을 할 수 있다. 그리고 피의자의 동의는 자신의 헌법상의 권리에 대한 침해

191) United States v. Gorshkov, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001).
192) United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996).
193) United States v. Reyes, 922 F. Supp. 818, 835-36 (S.D.N.Y. 1996).
194) United States v. Doe, 61 F.3d 107, 110-11 (1st Cir. 1995).
195) United States v. David, 756 F. Supp. 1382(D. Nev. 1991).

를 용인하겠다는 것이므로 헌법적 문제도 발생하지 않는다.

동의의 문제에 있어 유효한 동의가 되기 위해서는 첫째, 동의는 자발적으로 이루어져야 한다. 수사기관이 영장을 발부 받지 않고 또는 상당한 이유도 없이 주택이나 물건을 대상으로 수색을 할 때 권한 있는 사람이 자발적으로 동의를 했다면 영장없이 수색할 수 있다.[196] 이러한 동의는 명시적일 수도 있고 묵시적일 수도 있다.[197] 동의가 자발적인지 아닌지에 대한 문제점은 사실 법원이 종합적으로 주위 환경을 고려하여 결정해야만 한다. 미연방 대법원은 자발적인 동의에 대해 적법성을 증명하기 위해서 고려하여야 할 요소로서는 동의를 한 사람의 나이, 교육, 사고력, 육체적 · 정신적 상태[198]와 그 사람이 체포되어 있었는지, 또한 동의에 대하여 거부할 수 있는 권리를 알려주었는지 등을 중요한 요소로 보고 있다.[199] 그리고 수사기관이 동의를 받기위해 기망이나 협박이 있는 경우에 동의의 임의성을 인정할 수 없다. 또한 수사기관은 동의가 자발적이었다는 것을 입증하는데 책임을 져야 한다.[200]

이에 대한 대표적인 사례로 경찰관은 영장이 없으면서도 영장이 있다고 속이고 동의를 받은 경우,[201] 혈액채취의 목적으로 강간현장에서의 혈흔과의 일치 여부를 확인하기 위한 것임에도 이를 음주운전 검사용이

196) Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

197) United States v. Milian-Rodriguez, 759 F.2d 1558, 1563-64 (11th Cir. 1985). 이 사례는 묵시적인 동의에 의한 영장 없는 수색을 인정한 사건으로 경찰관에게 수색장소에 대한 열쇠가 있는 곳을 가르쳐 주는 것은 묵시적인 동의라고 판시하였다.

198) 만약 피의자가 동의를 할 수 있는 정신능력이 부족한 상태였다면, 그 동의에 기초한 강제처분은 허용될 수 없다.

199) Schneckloth v. Bustamonte, 412 U.S. 226 (1973). 이 사건에서 경찰관은 전조등이 파손된 자동차를 발견하고 탑승자 중 한명의 동의를 받은 후 자동차를 수색하여 트렁크에서 절취된 수표를 발견하였다. 법원은 동의를 한 자가 동의를 거부할 수 있느냐를 알았는지의 여부는 동의가 적법한 것인지를 결정하는데 고려하여야 할 요소중의 하나이기는 하지만 반드시 필요한 것은 아니라고 판시하여 동의의 적법성을 인정하였다

200) United States v. Matlock, 415 U.S. 164, 177 (1974); United States v. Price, 599 F.2d 494, 503 (2d Cir. 1979).

201) Bumper v. North California, 391 U.S. 543 (1968).

라고 속이고 동의를 받은 경우,[202] 그리고 차량 수색에 동의하지 않으면 차량을 압수하겠다고 고지하고 동의를 받은 경우[203] 등이다.

둘째, 동의의 주체는 본인이거나 수색할 장소에 대한 공통의 권한을 갖고 있는 제3자이어야 하며, 통상 부부나 동거인은 거주의 수색에 대해 서로 동의할 수 있을 것이다. 반면 건물주는 임차인의 방에 대한 수색에 동의할 수 없고, 호텔 직원은 호텔의 객실 수색에 동의할 수 없다.

셋째, 동의는 명시적으로 표명되어야 하며 또한 동의가 있었다 하더라도 그 동의의 범위를 넘는 압수· 수색은 불법이며, 피의자가 수사기관에 수색에 관한 동의를 하였다 하더라도 이후 그 동의를 철회할 수 있다.

넷째, 수사기관은 피의자에게 동의를 거부할 권리가 있음을 고지해 주어야한다. 이러한 요건을 충족하지 못한 강제처분은 위법이며, 이를 통하여 수집한 증거는 반드시 배제되어야 할 것이다.[204]

수사기관의 영장없는 수색이 프라이버시를 침해함에 있어 만약 영장요구의 예외적인 사항에 해당할 때에는 미연방 수정헌법 제4조의 규정에 위반되지 않는다.

컴퓨터 및 디지털 기기를 포함한 디지털 범죄에서는 이 동의(同意)문제를 어떻게 볼 것인지에 대하여 다양한 문제가 제기 될 수 있다.

특히, 디지털 범죄에 있어 수사기관이 피의자의 자발적인 동의를 받는 경우에는 범죄의 장소, 물건에 대하여 수색을 할 수 있다. 그러나 현재는 컴퓨터의 시스템이 대용량화 되고, 다수의 사용자가 공동으로 컴퓨터를 이용하는 현상이 일반화되고 있다. 이러한 환경에서 문제가 되는 것은 동의의 범위가 어디까지인가 하는 점과 수사기관의 수색에 동의할 수 있는 적법한 당사자가 누구인가 하는 점이다.

---

202) Graves v. Beto, 424 F. 2d 524 5th Cir. (1970).
203) State v. Williams, 772 P.2d 112 (1973).
204) 조 국, 전게서, 357-361면 참조.

먼저 동의에 기한 수사기관의 수색의 범위는 일반적으로 표현된 대상에 국한되고 동의한 내용에 의하여 제한된다. 컴퓨터 관련 사건에서 장소나 품목을 수색하는 것에 동의를 한 경우, 수색과정에서 접하게 된 디지털 저장매체까지 수색할 것을 묵시적으로 동의 하였다고 볼 수 있느냐의 문제가 자주 발생한다.

이에 대해 법원은 수사기관이 동의를 구할 당시 명시적이건 묵시적이건 수색의 유형, 범위, 기간 등에 대하여 한계를 설정하였는지 여부를 그 판단기준으로 삼고 있다. 이에 관한 판례로 수사기관이 성범죄와 관련된 범죄 사건의 증거를 찾기 위해 건물과 재산에 대한 수색 동의서를 받아 범죄 관련 컴퓨터를 수색하는 도중에 피의자의 컴퓨터에서 아동음란물을 발견하였다. 수사기관이 이 피의자를 아동음란물 소지혐의로 기소한 경우에는 수색에 관한 동의의 범위를 벗어난 것이며 아동음란물을 증거로 채택할 수 없다고 판시하고 있다.[205]

동의의 주체는 본인이거나 수색할 장소에 대한 공통의 권한을 갖고 있는 제3자이어야 한다. 여러 사람이 공유 컴퓨터를 함께 사용하는 상황에서 그 중 한 명이 수사관에게 디지털 자료나 정보에 대한 수색에 동의한 경우, 그 사람이 해당 컴퓨터에 대한 사용권한이 있는 자라면 일반적으로 그 동의에 기하여 컴퓨터 수색을 할 수 있다.[206] 이 경우 모든 사용자들은 본인 이외의 사용자가 공유 컴퓨터에서 모든 정보들을 볼 수 있고, 수사기관에게 사용자의 공동 영역에 대한 수색을 동의할지도 모른다는 생각 갖고 있는 것으로 보기 때문이다.[207] 그러나 다수가 공동으로

205) United States v. Turner, 169 F.3d 84, 1st Cir (1999).

206) Computer Search & Seizure Working Group, U.S. Dep't of Jusiice, Federal Guidelines for searching and Seizing Computer 13 (1994).

207) United States v. Matlock, 415 U.S. 164 (1974). 이 판결에서 연방대법원은 부동산이나 동산에 대하여 공동의 권한을 가지고 있는 사람은 다른 공동 사용자가 반대하더라도 그 물건에 대한 수색에 동의할 수 있다고 판시하였다. 이 판례에 의해 컴퓨터의 공동사용자의 경우에도 일반적으로 컴퓨터 파일 수색에 대한 동의권한을 가지고 있다고 하고 있다.

사용하는 컴퓨터라 할지라도 패스워드를 설정하거나, 다른 공동 사용자가 사용하지 못하도록 암호 조치 등을 한 경우에는 동의의 효력이 미치지 못한다.[208] 또한 배우자 및 동거인, 부모의 경우에도 일반적으로 동의를 할 수 있는 권한이 있다. 그러나 자녀가 성년이고 컴퓨터에 별도의 제한조치를 한 경우에는 동의에 대한 권한이 없다고 한다.[209]

3. 디지털 증거에 관한 플레인 뷰 원칙(Plain View Doctrine)

Plain View Doctrine 이라 함은 수사기관이 공공의 장소나 적법하게 출입이 허용된 장소 또는 영장을 집행하고 있는 현장에서 발견한 증거로서 범죄의 증거임이 명백한 경우에는 영장 없이도 이를 압수할 수 있다는 원칙을 말한다.[210] 이 원칙이 적용되기 위해서 수사관은 증거를 관찰하고 접근하기 위한 적법한 지위에 있어야 하고, 그 증거는 범죄와의 관련성이 명백하여야 한다.[211]

Plain View의 원칙은 개인의 프라이버시를 침해하지 않으며 수사기관

208) Trulock v. Freeh, 275 F.3d 391, 403-04, 4th Cir (2001).

209) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, *op. cit,* p.22.

210) 參照 判例로는 Arizona v. Hicks, 480 U.S. 321 (1987).

211) 이와 관련된 판결로 Horton v. California, 496 U.S. 1060 (1990) 사건에서 무장 강도인 피의자를 조사하던 경찰관은 절도한 물건과 무기가 피의자의 집에 있어서 그의 집을 압수· 수색할 상당한 이유가 있다고 판단하였다. 그러나 발부된 영장은 오직 장물만 수색하도록 기재 되었다. 경찰관이 피의자의 가택을 수색하는 도중에 장물은 발견하지 못하고 노출된(plain view) 무기를 발견하여 몇 가지 범죄 관련 물건과 함께 압수를 하였다. 이 무기로 인하여 제1심 법원에서 피고인은 유죄판결을 받았다. 그러나 피고인은 동 무기는 영장없이 압수한 증거물이기에 증거능력을 부인하였지만, California州 大法院은 “압수· 수색영장에 기재되지 않은 물건도 ‘plain view’ 원칙에 따라 압수할 수 있다. 왜냐하면 쉽게 노출된 물건을 압수· 수색하는 것은 사생활 침해가 되지 않기 때문이다” 라고 하였다. 文鴻柱, 前揭書, 460면.

은 수정헌법 제4조에 의거하여 디지털 증거를 수색할 수 있는 권한을 부여 받았다고 할 수 있다.

컴퓨터 관련 디지털 범죄 사건에서는 하드 드라이브에 대한 적법한 수색영장을 집행하던 수사관이 수색도중 영장과 관련 없는 범죄의 증거를 우연히 발견하였을 경우에 그 증거를 영장 없이 압수할 수 있다는 것으로 적용될 수 있다. 하지만 이 Plain View의 원칙은 컴퓨터 파일을 열어서 그 내용을 확인할 권한까지 부여한 것은 아니다. 즉, 비밀번호에 의하여 잠겨진 컴퓨터 파일을 인위적으로 열어서 확인한 것은 Plain View의 원칙에 위배되고 이 경우에는 반드시 수색영장을 발부 받아 수색을 해야 한다.[212]

이와 관련된 Villarreal 사건은 Plain View의 원칙이 적용되지 않았는데, 그 이유는 다음과 같다. 55갤런(gallon)의 드럼통은 라벨에 표시된 내용이 고정되고, 드럼통이 불투명하여 외부에서 내부의 내용물이 보이지 않아 수색이 불가능하며 결국 Plain View의 원칙 적용되지 않는다. 따라서 라벨에 표시된 것 이상으로 불투명한 드럼통 안의 내용물을 확인하고자 한다면, 수색영장을 발부 받아야 한다고 판결하였다.[213]

법원의 판례는 대체로 과외로 발견된 많은 디지털 파일 중에서 첫 번째 파일을 열어 보는 것은 허용하지만, 그 외의 다른 파일을 열어보는 것은 위법하다고 하기도 하지만, 최근의 판례에서는 광범위한 Plain View Doctrine의 적용을 인정하고 있는 추세이다.[214] 그러나 법원은 디

212) United States v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996).

213) United States v. Villarreal, 963 F.2d 770, 776 (5th Cir. 1992).

214) United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2001) 이 판결에서는 Plain View 원칙에 의하여 컴퓨터 또는 저장장치에서 한 개의 파일을 열어 보는 경우는 보다 광범위한 기초를 제공할 수 있으며 컴퓨터 또는 저장장치의 일부에 대한 영장 없는 수색이 적법할 경우 피의자로서는 더 이상 그 컴퓨터 또는 저장장치에 남아 있는 내용물들에 대하여 프라이버시에 대한 합리적인 기대를 가질 수 없다. 따라서 수사기관에 의한 광범위한 수색은 수정헌법 제4조를 침해하는 것이 아니고, 이 이론은 플레인 뷰 원칙에도 적용할 수 있다고 하여 그 범위를 광범위하게 인정하고 있다.

지털 범죄에서 컴퓨터에 저장된 개개의 파일은 각각 분리되어 취급되어야 한다고 판결하고 있다.

Carey 사건에서 법원은 수사관이 마약밀매에 대한 증거발견을 위해 적법한 수색영장을 발부 받아, 피고인의 컴퓨터를 수색하던 중 우연히 'jpg' 파일을 열었을 때 마약밀매에 대한 증거가 아닌 아동 포르노를 발견한 후, 그 즉시 수사관은 마약밀매에 관한 증거 수색을 포기하고 5시간에 걸쳐서 수백 개의 아동 포르노 파일인 'jpg' 파일을 검색하여 이를 압수하였다. 피고인은 수사기관이 수색영장의 범위를 넘은 압수에 대하여 아동 포르노는 증거에서 제외되어야 한다고 주장하였고, 이에 대하여 수사기관은 아동 포르노 파일을 수색한 것은 적법하다고 주장하였다. 그 이유는 아동포르노나 마약 밀매는 모두 불법적인 것이기 때문에 Plain View Doctrine이 적용된다고 주장하였다. 이에 대하여 제10 순회재판소는 이 사건에서 최초로 발견한 아동 포르노에 관한 'jpg' 파일은 마약에 관한 수색 영장에 의거하여 수색 중에 발견되었기 때문에 Plain View Doctrine에 해당하여 영장 없는 압수가 정당하다고 판시하였다. 이를 제외한 다른 모든 파일은 플레인 뷰 원칙에 해당되지도 않고, 수색영장의 범위를 초과하여 증거를 수색하였기 때문에 위법하다고 판시하였다.[215]

이와 유사한 사례로 Walser 사건에서 경찰관이 피의자들의 마약매매에 관한 디지털 기록을 찾기 위해 수색영장을 발부 받아 피의자의 컴퓨터를 수색하였다. 수사관이 피의자의 컴퓨터 파일 1개를 열자 아동 포르노 파일이 나왔고, 수사관은 수색을 중지하고 판사에게 두 번째 수색영장을 발부 받아서 수색한 행위는 미연방 수정헌법 제4조를 위반하지 않았다고 판결하였다.[216]

---

215) United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999).
216) United States v.Walser, 275 F.3d 981, 986-87 (10th Cir. 2001).

최근 판례인 United States v. Runyan 사건과 United States v. Slanina에서는 플레인 뷰 원칙을 넓게 적용하고 있다.[217] 이 두 사건에서 컴퓨터 저장장치의 일부에 대한 영장 없는 수색이 적법할 경우, 그 이상의 컴퓨터 저장장치에 남아 있는 내용물들에 대한 수색은 프라이버시의 침해가 되지 않는다고 판결하고 있다. 따라서 수사기관에 의한 보다 광범위한 컴퓨터 수색은 수정헌법 제4조를 위반한 것이 아니며, 이는 플레인 뷰 원칙을 기본보다 넓게 적용하고 있는 것이라 판단된다.[218]

4. 컴퓨터 시스템 관리자의 동의

일반적으로 모든 컴퓨터 네트워크는 시스템 관리자나 운영자들에 의하여 작동 또는 운영되는데, 그들은 컴퓨터 네트워크가 적절히 작동되게 하는 것과 모니터의 보안 및 수리, 네트워크 오류 및 문제점을 발견하여 이러한 것들을 해결하는 것이 주된 업무이다. 이러한 시스템 관리자들은 루트 권한 즉, 관리자 권한으로 모든 시스템에 접근할 수 있으며, 허가된 마스터 키(master key)로 어떠한 계정도 열어 시스템에 있는 파일을 읽을 수 있다. 수사기관이 컴퓨터 네트워크에서 용의자의 디지털 증거를 찾고자 한다면 시스템 관리자에게 수색에 관한 동의를 요청해야 가능할 것이다.

여기서 실제로 문제가 되는 것은 시스템 관리자의 동의에 관한 권한이다. 시스템 관리자의 동의에 따라 네트워크 계정을 수색함에 있어 최초의 장애물은 헌법이 아닌 법률이다. 시스템 관리자들은 원격 서비스를 제공하는 업체에 대하여 데이터를 요구할 수 있는 기본적인 제도가 전기

217) United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2001); United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002).

218) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, *op. cit,* p.21.

통신프라이버시법(Electronic Communications Privacy Act: ECPA)[219]에 규정되어 있다. 전기통신프라이버시법은 수사기관이 개인의 컴퓨터 계정을 수색하기 위하여 시스템 관리자에게 동의를 얻고자 할 때 적용된다. 그리고 시스템 관리자의 동의에 의한 수색은 전기통신프라이버시법(ECPA)에 근거를 둔다.[220]

보통 컴퓨터 시스템에 저장된 파일에 대하여 개인의 프라이버시가 인정되는 경우에 시스템 관리자가 그 파일에 대하여 접근할 수 있는 권한이 있다고 하더라도 수색에 동의할 수 있는 권한까지 부여한 것이라고 볼 수는 없다.

이와 관련된 사례로 1964년 Stoner 사건에서 미연방 대법원은 수사기관이 호텔의 객실을 수색하는 행위에 대하여 호텔 직원은 동의할 수 있는 권한이 없다고 판결하였다. 비록 손님이 호텔의 직원에게 호텔객실의 열쇠를 맡겨 직원이 직무의 수행을 위해 호텔의 객실에 들어가서 일을 할 수 있게 허가는 되었지만, 그 직원에게는 수사기관에게 호텔의 객실에 대한 수색에 동의할 수 있는 권한이 없다고 하였다. 또한 수사기관의 부당한 압수· 수색이 있다면, 호텔직원은 손님을 보호하기 위하여 수사기관의 동의를 거부할 수 있는지 여부는 그의 재량에 맡겨진다고 판결하였다.[221]

컴퓨터 시스템 운영자가 네트워크 계정을 엑세스하는 것과 호텔직원이 호텔의 객실을 열어보는 것이 유사한 것이라면 컴퓨터 시스템 운영자가 수사기관의 계정 파일의 수색에 대한 동의는 할 수 없다고 본다.[222] 물론 호텔 직원의 사례가 모든 상황에 적합하게 적용되지는 않는다. 가령,

---

219) Electronic Communications Privacy Act: ECPA), 18 U.S.C. §§ 2701-2712.
220) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, *op. cit,* p.16.
221) Stoner v. California, 376 U.S. 483 (1964).
222) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, *op. cit,* p.16.

회사의 직원과 그 회사 네트워크의 시스템 관리자와의 관계는 민간 인터넷 서비스 업체의 시스템 관리자와 고객과의 관계는 같지 않다. 전자의 경우에 회사는 직원의 모든 업무와 관련하여 회사의 네트워크 시스템 관리자에게 직원 계정들에 대한 모든 접근 권한이 있고, 회사 직원들은 회사 네트워크 시스템 관리자가 그러한 권한이 있다는 것을 안다. 이러한 경우에는 회사의 시스템 관리자는 직원들의 계정들에 대하여 수사기관에 의한 수색에 동의를 할 수 있는 권한이 있다.[223]

이와 관련된 사례들은 다음과 같다. Barth 사건에서 컴퓨터 수리전문가의 목적은 컴퓨터에 엑세스하여 수리하는 것이지 이를 수사기관의 수색에 동의할 수 있는 권한이 있는 것은 아니다.[224] 또 다른 사례로 1961년의 Chapman 사건으로 수사기관은 영장없이 임대인의 동의만으로 부재중인 임차인의 가택 창문을 통해 집안에 들어가 수색하여 주정증류기와 양조원액을 압수하고, 이때 마침 귀가한 임차인을 체포하였다. 임차인은 수사관의 수색이 영장없는 불법한 가택침입으로 이루어진 것이라 주장하고 증거물의 증거능력을 부인하였으나, 제1심· 제2심에서 모두 유죄판결을 받았다. 그러나 미연방 대법원은 수정헌법 제4조에 보장된 부당한 수색을 당하지 않을 권리의 침해라고 판결하였다. 즉 수색영장이 없는 가택 수색은 불법이며, 본 사건에 있어서는 충분히 수색영장을 발부받아 합법적으로 수색 할 수 있는데, 임대인의 동의만으로 영장없이 수색한 것은 불법이라고 대법원은 판결하였다.

보통법상 임대인은 본인의 주택 훼손 정도를 조사하기 위하여 임차해준 주택안에 들어갈 수 있다는 원칙이 있어서 임대인은 이 권리를 수사관에게 위임하였다고 볼 수 있다. 그러나 위 사건처럼 창문을 통해 들어가는 것까지를 의미하는 것은 아니며, 또한 수색의 목적이 주택의 훼손

223) Keeping Secrets in Cyberspace, Establishing Fourth Amendment Protection for Internet Communication, 110 Harv. L. Rev. 1591, 1602-03 (1997).
224) Barth, 26 F. Supp. 2d at 938.

을 조사하기 위한 것이 아니고, 술 냄새가 남으로 밀주제조사실을 탐지하기 위하여 들어간 것이니 이는 보통법상의 원칙이 적용되지 않는다. 또 州 법률은 임차인이 주택을 범죄의 목적으로 사용할 경우에는 주택 임차인의 권리가 상실된다고 되어 있어서 임차인은 주택을 밀주제조용으로 사용하였으니, 임차인의 권리를 상실하였다. 따라서 임차인의 동의없이 주택안에 들어 갈 수 있다고 하지만, 수사기관이 임차인의 주택 안에 들어갈 때에는 아직 그 주택이 밀주양조용으로 사용되고 있다는 것은 알지 못하였고, 가택에 들어가서야 주택이 밀주양조용으로 사용되고 있음이 발각되었던 것이므로 수사기관의 수색 당시 합법성에 관하여는 이것으로 치유되는 것은 아니라고 판결하였다.[225] 또 다른 Clarke 사례로 마약을 운반하기 위해 고용된 피고인은 잠겨진 공구박스 안에 있는 마약에 대하여 수사기관이 공구 박스에 저장된 내용물에 대한 수색에 동의할 수 있다고 판결하였다.[226]

5. 체포에 의한 디지털 증거 수색(search incident to a lawful exception)

원칙적으로 수사기관이 수색을 실시하려면 판사가 발부한 영장이 있어야 하는 것이지만, 피의자를 적법한 절차에 의하여 체포함에 따라 별도의 영장 없이도 피의자의 신체나 근접한 주변장소를 수색할 수 있다.[227]

225) 이 사건에서 수사관이 수색영장을 발부 받아서 정당하게 수색하여야 할 충분한 시간적 여유가 있었음에도 불구하고 임대인의 동의가 있으니 충분하다고 생각한 수사관의 행동은 과실이 있다. 또한 범죄사실을 충분히 입증할 만한 증거가 있음에도 불구하고 다만 그 첫 출발이 불법인 관계로 그로 인하여 얻은 모든 증거가 증거능력이 없게 되었다. 따라서 증거 이외에 또 다른 증거가 없다면 임차인은 범인인 줄 알면서도 무죄석방하지 않을 수 없는 사건이라고 할 수 있다. 文鴻柱, 前揭書, 449면.

226) United States v. Clarke, 2 F.3d 81, 85 (4th Cir. 1993).

227) James, A. Fagin, Criminal Justice, 2005, p.147.

이처럼 수사관이 적법한 체포에 의해 부수된 수색은[228] 불법 거래품이나 범죄의 다른 증거를 발견함에 있어서 합리적인 방법을 사용하여야 한다. 예를 들면 수사관이 공공의 장소에서 피체포자의 옷을 벗도록 강요할 수는 없다. 또한 항문이나 여성의 성기 등을 포함하는 광범위한 수색은 체포에 따르는 수색에 의하여 정당화 될 수 없다.[229]

이와 관련된 Chimel 사건은 체포에 부수되는 압수· 수색은 용의자의 지배하에 있는 공간, 예를 들어 지갑, 배낭, 옷, 개인 소지품 등은 압수· 수색이 가능하지만, 체포된 공간 이외의 가택을 수색함은 부당하다고 한 사례로 사건의 내용은 다음과 같다. 1965년 9월 13일 3명의 경찰관이 California 州 용의자의 집에 도착하였다. 그의 처에게 경찰서에서 왔으며, 남편은 강도죄의 용의자로 합법적인 체포영장을 가지고 왔다고 고지하고 용의자가 귀가하기를 기다렸다. 잠시 후 용의자가 귀가하자 경찰관은 영장을 제시하고 그를 체포하였으며 집안 내부를 둘러 볼 것을 요구하였다. 용의자는 거부하였지만, 경찰관은 체포영장이 있으면 수색영장이 없어도 가능하다고 말하고 50여분 뒤에는 절도한 다량의 물건을 발견하여 압수하였다. 이 물건들은 유죄증거로 제출되어 유죄판결을 받았다. 법원은 체포영장이 합법이라면 체포영장으로 범인을 체포하는 경우 수색영장이 없어도 체포에 수반되는 수색이나 압수는 가능하다고 판결하였다.[230]

그러나 이 사건에서 미연방 대법원 Stewart 대법관은 “본 사건에서 체포영장의 발부는 합법적이지만, 체포에 수반된 수색문제, 특히 수색범위

228) United States v. Robinson, 414 U.S. 218, 235 (1973). 경찰관이 교통법규를 위반한 자에 대하여 무기 또는 위험물 소지를 조사하기 위하여 옷 위로 몸을 더듬어 신체 수색을 하였는데, 그 때 용의자의 가슴 주머니에서 구겨진 담배 갑을 발견하였다. 경찰관은 담배갑 안의 내용물을 확인하기 위하여 열어보니 그 안에서 14개의 헤로인(heroin) 캡슐이 발견되었다. 이에 대하여 미연방 대법원은 경찰관이 담배갑을 확인한 것은 적법한 체포에 부수된 수사로 허용된다고 판결하였다.

229) Jefferson, *op cit,* p.91.

230) Chimel v. California, 395 U.S. 752, 762-63 (1969).

에 관하여 헌법상의 문제를 제기하였다. 종래의 판결은 체포에 따른 부수적인 수색은 합법적이라고 하였고, 체포된 장소에서 범죄에 관계있는 물건을 찾고 압수하기 위한 수색은 수색영장 없이도 가능하였다.[231] 그러나 수색 영장없이 체포에 부수되는 수색이 가능하다 함은 체포를 항거하기 위하여 무기를 사용할지 모르기 때문에 체포된 자의 몸을 수색하고 또한 은닉하고 파괴할 우려가 있는 물건을 압수하는데 영장없는 압수·수색의 진의가 있을 것이다. 즉 그의 직접적인 지배하에 있는 공간에서의 압수· 수색을 의미하는 것이다. 그러므로 위 사례에서 체포된 방이 아니고 다른 방 또는 떨어져 있는 차고까지 모든 주택을 수색할 수 있다는 것은 아니며, 이때에는 수색영장이 필요한 것이다.[232]

따라서 본 사건에서의 수색은 부당한 수색이라 할 수 있다. 즉 수색은 범인의 신체의 수색을 넘었으며, 범인이 직접 지배하고 있는 공간을 넘어서 모든 주택을 걸쳐 수색하였다고 볼 수 있다. 결국 법원은 이를 위헌적인 수색이라고 판결하였다. 그 뒤 Vale의 사례에서는 체포영장에 수반하여 현관 밖에서 범인을 체포하고 수색 영장없이 가택을 수색한 것은 불법이라고 판결하였다.[233]

최근 들어 디지털 범죄 수사에 있어서 컴퓨터와 디지털 기기들의 저장장치가 많이 사용되고 증가하면서 수사기관은 적법하게 용의자를 체포하고 그들이 소지하고 있는 노트북, 핸드폰, USB, PDA 등을 압수· 수색하는 경우가 많이 발생하고 있다. 여기서 체포된 용의자가 소지하고 있는 디지털 저장장치들을 영장없이 수색할 수 있는지에 대하여 문제가 될 수 있다. 각주의 Robinson 사례처럼 호출기의 저장장치의 경우는 항상 체포와 수반하여 수색이 가능하다고 법원은 보았다.[234] 현재 법원은 디지

231) United State v. Robi-nowitz, 339 U.S. 56 (1950).
232) Preston v. United States, 376 U.S. 364 (1964).
233) Vale v. Louisiana, 399 U.S. 30 (1970).
234) 이와 같은 견해의 사건으로는 United States v. Reyes, 922 F. Supp. 818, 833 (S.D.N.Y. 1996); United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993); United States

털 저장장치에 관하여 Robinson 사건에서처럼 영장없이 수색을 허가할 것인지 아닌지에 대하여는 견해를 밝히지 않았다. 과거 문서를 쓰던 때에는 체포에 따른 부수적인 수색을 넓게 해석하였다. 예를 들어 적법하게 체포한 용의자에 대하여는 그의 지갑 내용물을 모두 수색할 수 있도록 하였다.[235] 또한 피고를 적법하게 체포하는 동안 그의 주소록, 서류가방(briefcase) 등에 대하여는 영장없이 수색할 수 있다고 하여 부수적인 수색이 가능하다고 보았다.[236] 판례의 경향이 이러하다면 당연히 컴퓨터와 관련된 디지털 저장 장치도 적법한 체포에 수반하여서는 영장없이 수색할 수 있을 것이다. 이에 관하여 참고할 수 있는 사례로 수사관이 자동차 사고를 낸 피의자를 적법하게 발부된 영장에 의하여 체포하였다. 그리고 그에 수반하여 그의 자동차 안에서 Zip 디스크를 압수하였다. 그러나 수사기관은 디스크 안에 있는 아동 포르노 사진을 수색영장이 발부 되기전에 수색하였기 때문에 법원은 이를 기각하였다.

따라서 용의자 체포에 수반된 어떠한 수색도 합법적이어야 하며,[237] 체포에 수반하여 용의자의 신체 소지품을 수색할 때 항상 합리적이어야 한다. 수사관이 다른 환경에서 더 깊숙이 수색을 한다면 이는 미연방 수정헌법 제4조를 위반했다고 볼 수 있다.

이러한 수색은 컴퓨터와 관련하여 디지털 저장 장치에 항상 적용이 되는 것은 아니기 때문에 수사기관은 디지털 저장 장치에 포함된 많은 디지털 정보 및 자료를 수색할 경우에는 반드시 수색영장을 발부 받아서

---

v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995); Yu v. United States, 1997 WL 423070, at *2 (S.D.N.Y. Jul. 29, 1997); United States v. Thomas, 114 F.3d 403, 404 n.2 (3d Cir. 1997); United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996).

235) United States v. Castro, 596 F.2d 674, 676 (5th Cir. 1979); United States v. Molinaro, 877 F.2d 1341, 1347 (7th Cir. 1989).

236) 이와 유사한 판례로는 United States v. Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993); United States v. Johnson, 846 F.2d 279, 283-84 (5th Cir. 1988); United States v. Lam Muk Chiu, 522 F.2d 330, 332 (2d Cir. 1975)이 있다.

237) Swain v. Spinney, 117 F.3d 1, 6 (1st Cir. 1997).

수색해야 할 것이다.[238]

미국은 국가의 특성상 국경에서의 수색이 자주 발생하고 있다. 수사기관이 국경에서 발생하는 밀수품이나 금제품, 불법적으로 수출· 입하는 물건들을 통제하기 위해서는 영장주의 예외로 영장없이 수색을 할 수 있다. 국경에서는 범죄의 증거를 수색하기 위하여 영장의 필요성이나 합리적이고 상당한 이유에 관계없이 수색영장 없이도 수색할 수 있다고 미연방 대법원은 판시하고 있다. 특히, 국경지대에서 미국내로 반입되는 국제화물이나 국제우편은 그 내용물이 불법 반입물을 포함하고 있는지를 판단하기위해 영장없이 수색할 수 있다.[239] 그러나 밀입국에 관하여는 적어도 합리적인 의심정도는 요구하고 있다.[240] 위와 같은 판례는 미국을 출입하는 모든 사람들에게 적용이 되고 있다.[241]

디지털 범죄에 있어 컴퓨터와 관련하여 법원은 국경에서도 불법적인 내용을 담고 있는 컴퓨터 파일이나 디스크, 컴퓨터 하드 드라이브, 노트북 등에 대한 영장주의의 예외로 영장없이 수색하고 있다.[242]

---

238) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, *op. cit,* p.23.

239) United States v. Ramsey, 431 U.S. 606 (1977); United States v. Scheer, 600 F. 2d 5(3d Cir. 1979).

240) United States v. Montoya De Hernandez, 473 U.S. 531, 538 (1985).

241) United States v. Oriakhi, 57 F.3d 1290, 1297 (4th Cir. 1995).

242) United States v. Roberts, 86 F. Supp. 2d 678, 681. 682 (S.D. Tex. 2000). 로버트는 텍사스 휴스턴에서 프랑스 파리로 가는 비행계획을 갖고 컴퓨터 파일에 아동 포르노를 소지하고 공항에 도착하였다. 수사관은 불법적인 방법으로 자금, 기술, 자료를 해외로 유출되는 것을 막기 위해 검문한다고 고지하고 로버트를 검문하였다. 수사관은 로버트의 동의를 받아 그의 노트북과 Zip 디스켓을 수색하여 다량의 아동포르노 사진을 발견하였고, 이를 근거로 기소하였다. 이에 대해 피고는 항변을 하였지만 법원은 기각하였다. 그 이유는 수사관이 피고의 가방을 수색한 것은 공항에서 일상적으로 있는 수색이었고, 어떠한 혐의를 갖고 수색한 것이 아니었다고 판결하였다. 또한 수사관의 수색은 정당하게 동의를 구하였기 때문에 이는 미연방 수정헌법을 위반하지 않았다고 판시하였다. 이에 로버트는 항소하였지만, 법원은 기각하였다. 그 이유로 로버트가 소지한 아동 포르노에 대한 혐의는 처음 공항에서 수색을 본인이 동의하였고, 로버트의 컴퓨터를 압수· 수색한 것은 상당한 이유가 있다고 판결하였다. United States v. Roberts, 98 F. Supp. 2d at 688 (S.D. Tex. 2000).

6. 디지털 범죄 수사에서 제3자의 동의

가. 일반 원칙

요즘은 정보통신기기의 범람으로 대학교, 도서관, 공공기관 등에 있는 컴퓨터와 그 주변 디지털 장비들을 여러 사람이 사용하는 경우가 많이 있다. 그럴 경우 그들 중 한 사람이 컴퓨터에 대한 권한을 가지고 수사기관의 수색에 동의하여 컴퓨터 데이터를 수색하는 것이 허가되는 경우가 있다. 이 경우 모든 컴퓨터 이용자들은 다른 이용자가 그 공용 컴퓨터에 내장된 모든 이용자의 정보를 노출시킬 수 있고, 수사기관의 요청에 의하여 공동 영역(common area)에 대한 수색을 동의할지도 모른다는 것을 감수해야 할 것이다.

이에 대한 획기적인 사례로 United States v. Matlock 사건이 있는데, 미연방 대법원은 다음과 같이 판결하였다. 부동산이나 동산에 대하여 공동의 권한을 가지고 있는 사람은 다른 공동 사용자가 반대하더라도 그 부동산이나 동산에 대한 수색에 동의할 수 있다고 판결하였다. 제3자의 동의를 정당화할 수 있는 공동의 권한의 요건으로는 공동 접근권한과 관리권한을 가진 사람들에 의하여 그 재산이 공동 사용되고 공동 사용자의 누구라도 그 혼자만의 권한으로 그 재산에 대한 수색을 허락 할 권한이 있다고 인정하는 것이 합리적이다. 또한 다른 사람들이 공동 사용자 중 1인이 공동 영역을 수색할 것을 허락할 수도 있다는 것을 인정하고 있음을 요한다.[243] 이 판례에 의하면 컴퓨터를 공동으로 사용하는 경우

243) 예를 들어 갑과 을이 한 아파트에 거주하면서 응접실을 공동으로 사용하고 있다면 갑의 동

에도 일반적으로 컴퓨터 파일 수색에 대하여 동의할 수 있는 권한을 가지고 있다고 하고 있다.[244]

제3자에 대한 동의에 대하여 일반적인 원칙은 제3자에게 동의를 요구할 때, 수사기관이 수색을 시작하기 전에 수색할 물건에 대한 제3자가 관리할 수 있는 권한이 있는지 없는지, 접근권이 있는지 없는지에 대하여 반드시 물어봐야 할 것이다.

이에 대한 사례로 Block 사건이 있는데, 이는 다음과 같다. 나이가 23살이 된 아들의 방을 수사기관이 수색할 때 어머니가 동의할 수 있는가에 대한 문제로 아들의 방안 침대 밑에 있는 사물함(footlocker)이 잠금장치가 되어 있어 어머니는 수색에 동의하지 않았다. 왜냐하면 제3자인 어머니는 그 사물함에 대하여 관리 권한이 없기 때문이다.[245] 또 다른 사례로 아파트에 두 남녀가 동거를 하고 있는데, 수사기관의 아파트에 대한 수색의 동의 여부에 대하여 여자는 애인과 함께 동거하면서 모든 것을 공유하는 관계로서 비록 애인이 수색 동의에 거부를 하더라도 법원은 그 아파트에 대하여 수사기관의 수색에 동의할 권한이 있다고 판결하였다.[246]

디지털 범죄에 있어서 컴퓨터를 공용으로 사용하는 경우에도 일반적으로 수사기관의 수색에 대하여 공동 사용자는 수색을 동의 할 수 있을 것이다.

이와 관련된 사례로 한 여자가 그녀의 남자친구와 공동으로 함께 사용하는 컴퓨터에 대하여 수사기관의 수색에 동의할 수 있다고 하였는데, 이는 남자친구가 사용하는 컴퓨터 파일에 비밀번호를 이용한 잠금장치를

의만으로도 응접실에서 을의 범행에 대한 증거를 수색하는 것은 적법하다는 것이다. 다만 갑과 을이 응접실을 공동으로 사용하면서 침실을 각각 사용하고 있었다면 갑의 동의로 을의 침실을 수색하는 것은 동의의 범위를 넘어선 것이다.

244) States v. Matlock, 415 U.S. 164 (1974).

245) United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978).

246) United States v. Sumlin, 567 F.2d 684, 687-88 (6th Cir. 1977).

하지 않았기 때문에 가능하다고 판결하였다.[247] 그러나 비밀번호를 이용하여 잠금장치를 하였고, 이를 다른 사람들과 함께 비밀번호를 공유하지 않았다면, 수사기관의 수색에 대한 동의는 불가능하다고 판결하였다.

또한 법원은 컴퓨터 파일에 비밀번호를 설정하거나, 방안 침대 밑의 잠겨진 사물함에 대하여는 동의 권한 범위를 넘었다고 판결하고 있다. 반대로 용의자한테 컴퓨터의 비밀번호를 받은 상태라면 수사기관의 수색에 동의할 수 있는 권한이 있다고 판결하고 있다.[248] 또한 창고를 관리하는 직원은 잠겨진 창고에 대한 수색에 동의할 수 있는데, 왜냐하면 그 직원은 열쇠(key)를 가지고 있고 고용주가 열쇠를 맡긴 것은 창고내부를 볼 수 있도록 허락했고 보여지기 때문이다.[249]

실제적인 문제는 수사기관이 제3자의 동의를 얻어 수색을 할 때 정확히 제3자의 권한 범위가 어디까지인지 알기가 어렵다. 특히, 동의의 범위를 초과하여 수색을 했을 때이다. 예를 들어 수사기관이 컴퓨터를 수색하겠다고 동의를 구하였을 때 컴퓨터에 저장된 디지털 정보에 대한 검색의 권한을 어디까지가 동의에 범위인가가 문제이다. 또한 수사기관이 수색을 할 때 누가 동의에 적당한 사람인지 문제가 된다. 예를 들어 수사기관이 범죄자의 컴퓨터 파일을 수색할 때 친구, 부모, 룸메이트(roommates) 등이 동의할 수 있는 권한을 가지고 있는가이다. 그리고 제3자가 소유물에 대한 권한의 범위를 넘어서 수사기관에게 동의를 해줄 수도 있다. 이에 대하여 미연방 대법원이 판결하길 수정헌법 제4조는 수사기관이 권한이 없는 제3자의 동의에 의해 수집한 증거를 바로 기각하지 않는다고 하였다. 수사관이 권한 없는 제3자의 동의라도 일반적으로 권한을 가지고 있다는 합리적인 믿음이 있을 경우에는 그 사람의 동의로 영장없이 들어가서 수색· 체포할 수 있다고 판결하였다.[250]

---

247) United States v. Smith, 27 F. Supp. 2d 1111, 1115-16 (C.D. Ill. 1998).
248) Trulock v. Freeh, 275 F.3d 391, 403-04 (4th Cir. 2001).
249) United States v. Murphy, 506 F.2d 529, 530 (9th Cir. 1974).

이하에서는 대표적으로 제3자인 배우자, 동거인, 부모 등에 의한 동의를 살펴보고자 한다.

나. 배우자와 동거인의 동의

수사기관의 수색에 있어 배우자나 동거인의 동의에 의한 수색은 대부분 합법적이다. 법원은 남편의 부재시 부인이 집안 재산에 대한 접근 권한이 없더라도 수사기관의 수색에 동의할 수 있다고 판결하였다. 이와 관련된 Duran 사례에서 수사기관은 남편이 주로 사용하는 헛간(barn)에 대한 수색을 통하여 마리화나를 발견하였는데, 이에 대해 부인이 수색에 동의할 수 있다고 판결하였다. 남편은 평상시에 부인이 헛간에 들어오는 걸 거부한 적이 없기 때문에 수색에 동의할 권한이 있다는 것이다.[251] 또 다른 Long 사례가 있는데, 부인이 남편을 잠시 떠난 사이에 남편은 공동으로 소유하고 있는 집의 현관 열쇠를 바꾸어 버렸다. 하지만 수사기관의 가택 수색에 대하여 부인은 동의할 수 있다고 판결하였다.[252] 그러나 판례중에는 배우자의 소유물이 별도의 서랍에 보관되어 있는 경우,[253] 배우자 일방에 의해서만 사용되는 특별한 부분에 대하여 사용하지 않는 배우자가 동의를 한 경우, 배우자 일방이 다른 배우자에 대한 분노에서 동의를 한 경우 등에는 적법한 동의가 아니라고 한 사례가 있다.[254]

---

250) Illinois v. Rodriguez, 497 U.S. 177 (1990).

251) United States v. Duran, 957 F.2d 499, 504-05 (7th Cir. 1992). 법원은 결혼생활에 있어 가택은 배우자들 간에 공동으로 유지되고 관리되는 것으로 추정되는 것이고 이러한 추정은 수색대상인 가택에 대하여 동의를 하는 배우자가 실질적으로 접근이 허용되지 않는다는 증거가 있어야 부정될 수 있다고 판시하였다.

252) United States v. Long, 524 F.2d 660, 661 (9th Cir. 1975).

253) United State v. Evans, 372 P. 2d 365 (Haw. 1962).

254) United States v. mazurkiewicz, 431 F. 2d 839 (3d Cir. 1970) 이 판결은 일방 배우자에 대한 수색을 정당화하는 배우자의 동의는 조화로운 결혼관계에서 유래하므로 이러한 관계에 근거하지 않은 배우자의 동의는 적법하지 않다고 판시했다.

디지털 범죄 수사에 있어 동의에 의한 컴퓨터 수색이 가능한지에 관한 사례로 스미스(Smith) 사건이 있는데 이에 대한 내용은 다음과 같다.

스미스(smith)라는 남자는 그의 부인(Ushman), 그리고 2명의 딸과 함께 살았다. 스미스에 의하여 아동학대(child molestation) 범죄가 일어났고, 이어 수사기관의 수사가 시작되었다. 부인은 수사기관이 남편의 컴퓨터를 수색하는데 동의하였다. 수사기관의 수색 대상이 된 남편의 컴퓨터는 집안의 골방(alcove)에 있었다. 비록 부인은 남편 스미스의 컴퓨터를 거의 사용하진 않았지만, 지방법원은 부인에게 남편의 컴퓨터를 수사기관의 수색에 동의할 수 있는 권한이 있다고 판결하였다. 왜냐하면 부인은 평상시 골방에 들어가는 것이 남편에 의해 금지되지 않고 수시로 출입을 하였으며, 또한 남편이 사용하는 컴퓨터는 비밀번호가 설정되어 있지 않았기 때문에 부인은 수사기관에 의한 남편 컴퓨터의 수색에 동의할 수 있는 합리적인 권한이 있다고 법원은 판시하였다.[255]

다. 부모에 의한 동의

미국은 부모들이 자녀들의 범죄행위에 대하여 수사기관에 동의할 수 있는 범위를 통상 자녀들의 나이가 18세 미만인 경우에는 자녀들의 방에 대한 수색에 동의를 할 수 있다. 그러나 자녀들의 나이가 18세 및 그 이상일 경우에 부모들은 수사기관의 수색에 대한 동의가 가능한지 여부가 문제가 된다.

최근 청소년의 디지털 범죄는 컴퓨터 게임범죄를 비롯하여 다양하게 나타나고 있다. 이러한 청소년과 관련된 디지털 범죄에 있어서 범죄자들이 대부분 미성년자이고 그들은 보통 부모들과 같이 산다. 범죄자의 나

255) United States v. Smith, 27 F. Supp. 2d 1111 (C.D. Ill. 1998).

이가 18세 미만인 경우에 그 아이들이 소유하고 있는 물건이나 방에 대하여 수사기관이 수색하는 경우에 부모들의 동의에 의한 경우는 언제나 합법적이다.[256] 그러나 나이가 18세 이상의 자녀들이 부모들과 함께 거주하는 경우에는 더욱더 복잡해진다. 부모들은 자녀들의 범죄행위에 대하여 나이에 상관없이 같은 집에 거주하는 가족이라면 수사기관의 수색에 동의하는 것은 명백히 가능하다. 가령, 아들이 본인의 컴퓨터와 파일을 지하실에 있는 방에 은닉하였을 경우에 부모들은 수사기관의 수색에 동의할 수 있다.[257]

수사기관이 나이가 18세 이상 자녀들의 개인적인 공간이나 방을 수색하고 싶을 때는 항상 부모들이 수색에 대한 동의권 있다고 생각할 수 없다. 그래서 법원은 수사기관에게 3가지 요건을 제시하였다. 첫째는 용의자의 나이, 둘째는 용의자가 집세를 지불하는지, 셋째는 용의자가 그의 방이나 개인적인 공간에 부모들의 접근을 거부하는지 아니면 승낙하는지이다. 법원은 용의자가 나이가 많거나, 집세를 내거나, 부모의 접근을 거부할 경우에는 부모들이 동의를 할 수 없다고 판결하였다.[258]

이에 관한 Durham 사건에서 수사기관은 24살 된 아들의 방을 수색하는데 동의할 수 있는 권한이 없다고 판결하였다. 그 이유는 어머니에게 고지도 없이 아들은 본인의 방에 잠금장치를 하였고, 또한 어머니에게 집세도 지불하였기 때문이다.[259] 이와는 반대로 18세 이상의 자녀가 집세를 지불하지 않거나, 부모들이 자녀들의 개인적인 공간을 자유롭게 출입하는 경우에는 부모는 수사기관의 수색에 대하여 동의할 수 있는 권한이 있다. 이에 관한 Rith 사건에서 18세의 자녀가 집세를 내지 않은 경우에

256) 3 W. LaFave,Search and Seizure: A Treatise on the Fourth Amendment § 8.4(b) at 283 (2d ed. 1987).
257) United States v. Lavin, 1992 WL 373486, at *6 (S.D.N.Y. Nov. 30, 1992).
258) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, *op. cit,* p.15.
259) United States v. Durham, 1998 WL 684241, at *4 (D. Kan. Sept. 11, 1998).

는 수사기관의 수색에 대하여 부모는 동의를 할 수 있는 권한이 있다고 판결하였다.[260]

7. 수사기관의 압수·수색에 있어 동의 범위

수색에 대한 동의의 범위는 일반적으로 표현된 물건에 한정되고, 동의한 내용에 의하여 제한된다.[261] 미연방 수정헌법 제4조에 근거하여 동의의 범위를 측정하는 기준은 객관적으로 합리적이어야 하는데, 이 의미는 수사기관과 동의를 허가한 사람과의 사이에서 동의 내용에 대하여 합리적인 사람이라면 이해할 수 있어야 한다는 말이다.[262] 물론 수사기관의 수색 전이나 후에 동의의 범위가 명확히 주워졌을 경우, 그 범위안에서 수색을 해야만 한다.[263] 수사기관의 수색에 대한 동의를 허가했을 때, 그 범위는 각 사건들의 사실에 의존하고 있다.

컴퓨터와 관련된 디지털 범죄 사건에서 장소나 내용물에만 암시적으로 수색에 동의하는지 아니면 디지털 저장 장치인 메모리까지 수색하는데 동의할 수 있는지에 대하여 문제가 제기된다. 이러한 문제가 제기된 사건에서 법원은 수사기관이 동의를 구할 당시에 명시적이건 묵시적이건 수색의 형태, 범위, 기간 등에 대하여 한계를 설정하였는지 여부를 그 판단 기준으로 삼고 있다.[264]

수사기관의 수색에 있어 허가된 동의의 범위는 각각의 사례에 따라 다

---

260) United States v. Rith, 164 F.3d 1323, 1331 (10th Cir. 1999); United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978).
261) United States v. Pena, 143 F.3d 1363, 1368 (10th Cir. 1998).
262) Florida v. Jimeno, 500 U.S. 248, 251 (1991).
263) Vaughn v. Baldwin, 950 F.2d 331, 333 (6th Cir. 1991).
264) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, *op. cit,* p.11.

른데, 디지털 범죄의 사례에 있어서는 위치나 사물의 수색에 대한 동의가 디지털 저장장치의 기록에 대한 엑세스도 동의의 범위에 암시적으로 포함되는지 의문이 제기될 수 있다. 전통적인 기존의 일반 범죄에서는 동의의 범위를 어디까지 적용되는지 아래의 사례를 검토해 보면, Reyes 사건에서 법원은 '차량 안을 보라(look inside a car)' 고 말한 의미는 자동차 실내 뒷좌석에서 발견한 호출기의 내부에 저장된 번호들을 검색하는 것도 동의에 포함된다고 판결하였다.[265] 이와 비슷한 사례로 Blas 사건에서 법원은 '호출기를 보라(look at pager)' 고 말한 의미는 호출기를 켜고, 호출기 안의 번호들을 검색해라고 한 것은 동의에 포함되지 않는다고 판결했는데, 왜냐하면 '호출기를 보라' 는 의미는 어떤 기계이며, 얼마나 작은 것인지, 어느 회사 브랜드인지를 보라는 의미이다.[266] 일반적으로 자동차를 수색하는데 '동의 한다' 는 의미는 경찰관이 자동차 안에 있는 핸드폰의 메모리를 수색하는 것도 이 동의의 범위에 포함된다.[267]

수사기관은 컴퓨터와 관련된 디지털 증거를 수색을 함에 있어 하나의 증거 수색에 관하여 동의를 받았는데, 수색의 범위를 초과하여 그 이상에 대하여 수색행위를 하였을 때에 문제가 제기될 수 있다. 특히 수사기관은 컴퓨터 수색에 관한 기본원칙인 동의에 관한 신뢰성 문제에 주의해야 할 것이다.

이에 관한 Turner 사건은 수사기관이 범죄의 증거를 찾기 위해 피고에게 그의 가택과 재산을 수색하는 절차에 따라서 동의를 받고, 수색하던 중 피고의 컴퓨터 파일에서 숨겨 놓았던 아동 포르노 사진을 찾은 사건이다. 수사기관은 성폭행을 시도했던 자의 물리적인 증거를 찾기 위해 피해자의 이웃주민으로부터 수색 동의서를 받아 그의 재산과 이웃 주변

265) United States v. Reyes, 922 F. Supp. 818, 834 (S.D.N.Y. 1996).
266) United States v. Blas, 1990 WL 265179, at *20 (E.D. Wis. Dec. 4, 1990).
267) United States v. Galante, 1995 WL 507249, at *3 (S.D.N.Y. Aug. 25, 1995).

을 수색하였다. 그러나 수사관이 이웃주민에게 수색동의서에 사인을 받기 전에 그의 아파트안에서 큰 칼과 핏자국을 발견하였다. 수사관들은 그에게 성폭행 증거를 더 찾아야 한다고 설명을 하고 그 아파트에 남아 계속 수색을 하였다. 수사관들이 물리적인 증거를 찾기위해 수색하던 중 수사관 중 한명이 그 이웃주민의 개인용 컴퓨터에서 아동포르노 사진을 발견하였다. 그 이웃주민은 아동 포르노 소지죄로 기소가 되었다. 이에 대하여 제1 순회 재판소는 컴퓨터의 수색은 동의의 범위를 초과한 것이라고 하여 증거를 기각하였다. 성폭행의 물리적인 증거를 찾기 위해 동의를 받았는데, 개인용 컴퓨터 파일을 수색한 것은 동의의 범위를 벗어난 것이라고 판결하였다.[268]

수사기관이 디지털 범죄와 관련하여 컴퓨터와 기타 부수물에 관한 수색에 대하여 동의를 받게 되는 경우에 예상하지 못한 결과가 발생할 수 있다. 따라서 수사기관은 동의서에 '디지털 저장장치와 컴퓨터 수색을 포함한다' 라는 동의의 범위를 구체적이고 명확히 영장에 기재해야 할 것이다.[269]

---

268) United States v. Turner, 169 F.3d 84 (1st Cir. 1999).

269) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, *op. cit,* p.12.

제5장 결 론

현재 디지털 범죄가 고도화 되고 이로 인한 대량의 개인정보· 기업정보 유출[270]이 발생하고 뿐만 아니라 다양한 디지털 기기를 통한 새로운 형태의 신종 범죄들이 증가하고 있다. 이에 부가하여 이러한 신종 디지털 범죄에 대한 디지털 증거를 수집하기 위한 경찰 및 검찰 수사기관의 노력은 더욱 절실해지고 있다. 특히 최근에는 전통적인 일반 범죄에서도 범행의 예비, 음모, 시도나 과정에서 컴퓨터를 이용한 인터넷과 디지털 기기들이 다양하게 혼합되는 경향이 증가하고 있다. 예를 들어 살인· 절도· 마약거래· 성매매· 보험사기· 협박· 인터넷 사기 등의 범죄행위를 실행하기 위해 인터넷을 이용하여 E-mail, 개인 홈페이지 게시판, 메신저, 블러그, 휴대폰의 문자서비스 등을 이용하여 범죄행위를 예비· 공모하는 사례들이 자주 나타나고 있다. 이러한 추세라면 앞으로는 모든 범죄들이 디지털 범죄와 일반 범죄가 나누어지는 것이 아니라 벽이 없어져 하나로 융합 또는 혼합되어 나타날 것이라 예상된다.

일반 범죄 뿐만 아니라 디지털 범죄에서 수사기관이 디지털 증거를 수집하기 위해서는 헌법상 적법한 절차와 이에 따른 영장주의의 원칙이 적용되어야 함은 국민의 기본권 보호를 위하여 당연하다 할 것이다. 그러나 현행 형사소송법은 디지털 증거의 압수· 수색에 대해서는 명문의 규정이 없고, 해석상으로만 인정이 되고 있어 이것이 근본적인 해결방안은 아니라고 생각된다.

---

270) 2008년 한해 동안 발생했던 대표적인 대규모 개인정보 유출 사례를 살펴보면 ①해킹에 의한 「옥션」고객 1,081만명의 개인정보 유출사고(08. 2), ②내부자에 의한 유출로 「GS칼텍스」고객 1,100만명의 개인정보유출(08. 9), ③관리소홀로 인한 「다음」고객 53만명 이메일 정보 유출(08. 7), ④개인정보 오·남용으로 인한 「하나로 텔레콤」고객 600만명의 개인정보 무단 제공(08. 4) 등이 있다.

이러한 현행법의 근거규정 미비로 인하여 수사기관이 디지털 범죄를 수사함에 있어서 영장주의 위반, 적법절차 위반 등의 형태로 기본권 침해 행위가 다양하게 발생하고 있다. 그러나 우리의 수사기관과 수사를 받는 범죄인들은 이에 대하여 인식하고 있지 못하고 있다.

이처럼 부지불식간에 다양한 형태로 나타나는 기본권 침해 문제에 대하여 제기가 없다보니 현재 우리의 수사기관에서는 이에 대한 구체적인 대안을 제시하고 있지 못한 것이 현실이다. 물론 수사기관 뿐만 아니라 판사, 변호사, 피의자 등 범죄와 관련된 업무를 하는 이들 조차도 아직 기본권 침해에 관하여 구체적인 인식을 갖고 있지 않은 것이 현 상태이다. 따라서 수사기관은 이에 대한 대안을 준비해야 할 것이며, 이와 관련된 사례들이 증가하게 되면 입법적인 측면도 적극적으로 고려하여 대비를 해야 할 것이다.

앞에서 제시한 미국의 경우에는 컴퓨터와 관련된 디지털 범죄에서 디지털 증거를 영장없이 압수 · 수색을 함에 있어서 발생하는 영장주의 위반에 따른 적법절차 문제 등의 사례들을 일반 전통적인 범죄에서 도출하여 해결하고 있다.

이러한 미국의 사례들은 우리에게 많은 시사점을 주었고, 이러한 사례들은 차후 우리의 입법적인 모델이 될 수 있을 것이다. 그래서 앞으로 디지털 범죄에 관하여 관련 법률을 제정하거나 기존 형사절차법을 개정할 경우 다양한 형태의 사례들을 참고할 수 있도록 광범위하게 미국의 범죄 판례를 심도있게 검토·분석·고찰하여야 할 것이다. 이러한 미국 판례의 검토·분석은 차후 우리의 디지털 범죄 관련 법률을 개정하거나 제정할 경우 많은 참고가 되리라 확신한다.

결국 이것은 국민의 기본권 보호를 위해서이기도 하지만, 미래에 선진 일류 경찰이 되기 위해서이기도 하다.

【參考文獻】

Ⅰ. 國內文獻

1. 單行本

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

_____,「디지털증거분석지침」, 경찰청 사이버테러대응센터, 2004. 12.

桂禧悅, 憲法學(中), 博英社, 2007.

丘秉朔,「新憲法原論」, 博英社, 1989.

_____,「新憲法原論」, 博英社, 1995.

權寧星,「憲法學原論」, 法文社, 2007. 2.

김문일,「컴퓨터 범죄론」, 법영사, 1992.

金榮秀,「憲法學의 諸問題」, 實甫金榮秀敎授華甲紀念論文集, 學文社, 2000.

김일수·서보학,「형법총론(제10판)」, 博英社, 2005.

金哲洙,「憲法學新論」, 博英社, 2007. 4.

金炯盛,「大韓民國 憲法學」, 일진사, 2005.

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」, 한국형사정책연구원, 2000. 12.

백광훈,「사이버범죄에 대한 ISP의 형사책임에 관한 연구」, 한국형사정책연구원, 2003.

白亨球,「刑事訴訟法講義(第8 改訂版)」, 博英社, 2001.

成樂寅,「憲法學」, 法文社, 2005.

_____,「憲法學」, 法文社, 2007.

성선제 외2,「네티즌을 위한 e-헌법 Cyber Law」, 길벗, 2003. 11.

申東雲,「刑事訴訟法Ⅰ」, 法文社, 1997.

_____,「형사소송법[제4판]」, 法文社, 2007.

申洋均,「刑事訴訟法(제2판)」, 法文社, 2004.

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.

李在祥,「刑事訴訟法(第6版)」, 博英社, 2007.

정웅석,「형사소송법」, 大明出版社. 2005.

조 국,「위법수집증거배제법칙」, 博英社, 2005.

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

曺俊鉉,「刑法總論」, 法元社, 2004.

_____,「犯罪學」, 法元社, 2005.

차용석·최용성,「刑事訴訟法」, 세명출판사, 2004.

탁희성·이상진,「디지털 증거분석도구에 의한 증거수집절차 및 증거능력확보방안」, 한국형사정책연구원, 2006. 12.

許 營,「憲法理論과 憲法」, 博英社, 2001.

2. 論 文

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

權寧鳥,「美國 憲法上 適法節次의 法理와 그 展開」, 美國憲法硏究 第1號, 1999.

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

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

김귀남,「국내 디지털 포렌식 기술에 대한 고찰」, 수사연구, 수사연구사, 2005. 3.

金啓煥,「大憲章의 適法節次, 公法의 諸問題」, 海巖文鴻柱博士 華甲紀念論文集, 海巖社, 1978.

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

金哲洙,「美國憲法이 韓國憲法에 미친 影響序說(美國憲法과 韓國憲法)」, 韓國公法學會, 大學出版社, 1989.

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.

김형준,「현행 통신비밀보호법의 몇 가지 문제점: 통신제한조치와 대화감청을 중심으로」, 한국형사법학회 2005년 추계학술회의

자료집, 한국형사법학회, 2005. 10.

박문수,「미국의 컴퓨터에 대한 압수· 수색절차 연구」, 해외연수검사 연구논문집 제17집(I), 법무연수원, 2002.

박희영,「인터넷에서 링크제공자의 형사책임에 관한 연구」, 인터넷법률 통권 제21호. 2004.

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

백광훈,「정보통신범죄의 개념과 유형 및 분류」, 사이버범죄연구회 제23회 세미나, 2001.

成樂寅,「개인정보보호법제의 현황과 재정립 방향」, 인터넷과 法律 Ⅱ, 法文社, 2005.

_____,「通信에서의 基本權保護」, 公法硏究 제30집 제2호, 2001.

쉔케/ 박종수 번역,「通信의 基本權的 問題」, 公法硏究 제30집 제2호, 2001.

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

심희기,「아동포르노그래피와 한국의 청소년 보호법」, 비교형사법연구 제5권 제2호 특집호. 2003.

안경옥,「정보화사회의 새로운 수사기법과 개인의 정보보호」, 비교형사법연구 Vol.5 No. 1, 한국비교형사법학회, 2003.

安京煥,「民主法治主義의 實質化를 위한 適法節次」, 法制硏究 第3號, 1992.

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.

염동신,「독일 형사법상 인터넷 관련 범죄의 형사소추에 관한 연구」, 해외연수검사연구논문집 제16집(II), 법무연수원, 2001.

吳桃洙,「美國憲法上 刑事節次에서의 基本權保護에 관한 硏究 -Undercover와 Confidential Informant 제도의 적법절차 위반 여부를 중심으로-」, 成均館大學校 碩士學位論文, 2004.

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.

_____,「증거의 관련성과 컴퓨터 관련증거」, 저스티스 통권 제73호, 한국 법학원, 2003.

오범석,「미국의 압수· 수색제도에 관한 연구」, 국외단기개인훈련보고서, 법무부, 2006.

尹明善,「性的 프라이버시 權利」, 美國憲法硏究 제6호, 1995.

愈熙一,「憲法學의 諸問題-憲法上 適法節次 規定」, 實甫金榮秀敎授華甲紀念論文集, 學文社, 2000.

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

_____,「전자증거의 압수· 수색」, 한국비교형사법학회 2003년도 하계국제학술대회자료집, 한국비교형사법학회, 2003. 8.

李 哲,「컴퓨터 犯罪의 法的規制에 대한 硏究」, 慶熙大學校 博士學位論文, 1991. 6.

이훈동,「컴퓨터관련범죄와 형사절차」, 세명논총 제2집, 세명대학교, 1992.

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

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

정수봉,「유럽의회 사이버범죄 방지조약의 주요 내용 및 쟁점」, 해외연수검사연구논문집(I) 제19호, 법무연수원, 2004. 3.

정 완,「국제조직범죄 및 하이테크범죄 대책을 위한 G8 장관회의」, 형사정책연구 제57호, 한국형사정책연구원, 2000. 1.

_____,「컴퓨터관련증거의 증거조사와 증거능력」, 수사연구, 2004. 5.

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

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.

丁泰鎬,「個人情報自決權의 憲法的 根據 및 構造에 대한 考察」, 憲法論叢, 제14집, 2005.

최재호,「컴퓨터 범죄의 관할에 관한 연구(독일의 논의를 중심으로)」, 해외연수검사연구논문집 제17집(I), 법무연수원, 2002.

탁희성,「형사절차법상 digital evidence에 관한 연구(압수· 수색을 중심으로)」, 한국형사정책연구원, 2002. 12.

_____,「전자증거에 관한 연구」, 이화여자대학교 박사학위논문, 2004.

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

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

II. 外國文獻

Allan M. Gahtan, Electronic Evidence, 2000.

Carrie Morgan Whitcomb, “An Historical Perspective of Digital Evidence: AForensic Scientist’s View”, IJDE Spring 2002 Volume 1, Issue 1, 2002, <www.ijde.org>.

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>.

_____, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, 2002.

_____,Provisions of Section 225 (“The Cyber Security Enhancement Act”) of the Homeland Security Act of 2002, H.R. 5710, <www.cybercrime.gov>.

Curtis E. A. Karnow, The Encrypted Self : Fleshing Out The Rights of Electronic Personalities, Journal of Computer & Information Law Vol. XIII 1994.

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.

Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition, Academic Press, 2004.

FBI Academy, International High-Technology White Collar Crime Conference, 2000. 3.

Gary Palmer, "A Road Map for Digital Forensics Research", DFRWS, Nov. 2001.

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

Guidance Software, Inc., EnCase Legal Journal, 2005. 5.

James, A. Fagin, Criminal Justice, 2005.

Joseph N. Froehlich·Edward M. Pinter , COMPUTER VIRUSES: Making The Time Fit The Crime, <www.fmew.com>.

Mark M. Pollitt, Who is SWGDE and what is the history?, 2003. 1,

Michael G. Noblett·Mark M. Pollitt·Lawrence A. Presley, "Recovering and Examining Computer Forensic Evidence", Forensic Science Communications Volume 2 Number 4, October 2000, <www.fbi.gov>.

NIJ(National Institute of Justice), Forensic Examination of Digital Evidence: A Guide for Law Enforcement, NIJ, 2004. 4, <www.ncjrs.org>.

NIJ, Electronic Crime Scene Investigation : A Guide for First Responders, 2001. 7.

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

황과 대응), 한대 법학연구소 컴퓨터 범죄 세미나, 2000. 10.

的場純男,「コンピュータ 犯罪と捜査」, 松尾浩也·井上正仁 編, 刑事訴訟法の 爭點(新版), ジュリスト 增刊, 有斐閣, 1991.

貴志治平,「ハイテク犯罪の捜査に關する諸問題」, 警察學論集 51卷7号, 1998.

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.

長沼範良,「ハイテク犯罪と刑事手續法の整備」, ジュリスト No. 1257, 2003.

山口 厚,「サイバー犯罪に對する實態法的對應」, 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.

_____,「ハイテク犯罪と刑事手續」, 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.

石井徹哉,「サイベ-犯罪條約に關する覺書き」, 奈良法學會雜誌, 第15卷1·2号, 2002. 9.

園田壽/野村隆昌/山川健,「不正ハッカー vs. 不正アクセス禁止法」, 日本評論社, 2000.

III. 인터넷 웹사이트(Internet Web Site)

구 글, www.google.co.kr

네이버, www.naver.com

한국정보보호진흥원, www.kisa.or.kr

SANS사 홈페이지, www.sans.org

국제 법률·정책포럼, www.ilpf.org

국제 첨단범죄수사협회, www.htcia.org

국제 컴퓨터수사전문가 협회, www.cops.org

국제연합(UN), www.uncjin.org

디지털 증거에 관한 국제협회, www.ijde.org

디지털 포렌식 연구 워크숍, www.dfrws.org

미국 국립법과학센터, www.ncfs.org

미국 국방부 사이버범죄센터, www.dcfl.gov

미국 법무부 컴퓨터범죄지적재산, www.cybercrime.gov

미국 백악관, www.whitehouse.gov

미국 비밀수사국, www.ustreas.gov

미국 사법연구원, www.ojp.usdoj.gov

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

컴퓨터증거에 관한 국제조직, www.ioce.org

Ⅳ. 언 론

경향신문,「위법수집증거 불인정 판결의 의미」, 2007. 11. 20.

매일경제신문, 2007. 9. 3.

매일경제신문,「기업들 도를 넘는 개인정보 유출」, 2007. 8. 9.

매일신문,「최경진, 인터넷 실명제와 토론문화」, 2007. 7. 4.

보안뉴스,「데이터의 효과적 관리·보호 방안없나」, 2007. 11. 13.

서울경제신문,「디지털 증거분석 시장 급성장」, 2007. 6. 11.

서울디지털포럼 홈페이지, http://sdf.sbs.co.kr 참조.

와이티엔(YTN TV), 2007. 8. 22.

오마이뉴스,「서울디지털포럼 특별연설」, 2007, 5, 31.

전자신문,「사이버방지조약은 무소불위」, 2006. 8. 8.

조선매거진, 2007. 11. 19.

조선일보, 2007. 11. 29.

한겨레신문, 2006. 9. 11.

한국경제, 2006, 10. 17.

한국경제신문,「해킹등 각종 컴퓨터 범죄 디지털 포렌식으로 잡는다」,2007. 3. 14.

한국일보, 2007. 11. 16.

한국정책방송(KTV), 2007. 2. 21 방송.

책임연구보고서 2009-04

디지털 범죄 수사와 기본권에 관한 연구
(영장제도를 중심으로)

발행일 : 2009년 6월 30일
발행인 : 김 길 배
발행처 : **치 안 정 책 연 구 소**
경기도 용인시 기흥구 언동1길 29
홈페이지 : www.psi.go.kr

POLICE SCIENCE INSTITUTE