「法과 政策」第19輯 第1號, 2013. 2. 28.
濟州大學校 法과政策硏究所

디지털증거 압수수색에 관한 연구

A Study on search and seizure of digital evidence

박 봉 진* · 김 상 균**
Park, Bong-Jin · Kim, Sang-Kyune

목 차

국문초록

사이버공간에서 발생하는 각종 사이버범죄에 대한 정책적 대응은 사이버범죄의 성격과 디지털증거에 따라 체계적이고 구체적으로 이루어져야한다. 사이버범죄의 새로운 인터넷사기 수법으로 보이스 피싱의 경우 피해자가 계속증가하고 있고 매스컴에 자주 보도되고 있는 상황이며, 사이버음란물, 사이버성매매, 소프트웨어불법복제, 사이버도박 등이 지속적으로 문제되고 있다. 사이버세계에서의 비대면성·익명성은 죄의식을 감소시키고, 수많은 불법적이고 유해한 정보를 수집, 변형, 유통함으로써 공공의 안녕과 사회질서를 혼란스럽게 하는 결과를 야기하고 있다. 본 연구에서는 사이버범죄의 개념과 유형, 그리고

논문접수일 : 2012.12.24
심사완료일 : 2013.01.22
게재확정일 : 2013.01.24
* 법학박사, 백석대학교 법정경찰학부 강사(주저자)
** 법학박사, 백석대학교 법정경찰학부 교수(교신저자)

최근 5개년간 우리나라의 사이버범죄 현황의 추이를 살펴보고자 한다. 사이버범죄는 정보적, 국가적, 세계화적, 네트워크적 특성, 특히 현재성으로 인해 수사 및 형사사법절차에 있어, 개인의 안전과 프라이버시의 보호 등 많은 법적 어려움이 발생하고, 정보화 사회가 되어가면서 컴퓨터에 저장된 정보는 형사소송에서 증거로서 더욱 중요한 역할을 하고 있다. 2011.7.18 공포되어 2012.1.1부터 시행되는 형사소송법은 디지털증거에 대한 압수수색제도를 명문의 규정으로 제시하였다. 그러나 디지털증거의 압수수색에 대한 부분적인 형사소송법의 규정이 그 증거조사방법과 증거능력과 관련하여 충분한 근거조항이 되지 못하고 있으므로 이에 대한 문제점과 개선방향(보완입법)을 제시해 본다.

주제어 : 사이버범죄, 디지털증거, 공공의 안녕과 사회질서, 압수수색제도, 증거조사방법과 증거능력

Ⅰ. 문제제기

정보화 사회에서 정보의 흐름이 그 성격상 익명화, 대량화, 가속화됨에 따라 이에 부수된 각종의 위험요소, 예컨대 타인의 인격권이나 재산권등의 침해가 커지게 되었다. 이러한 위험이 사회적으로 용납될 수 있거나, 또는 민사법이나 행정법 등에 의해 충분히 방지되거나 극복될 수 있으면, 형사법상의 대책은 무용한 일인 것이다.[1] 우리나라에서도 1995년 형법일부개정을 통해 컴퓨터범죄에 대처하기 위한 것으로서 1990년 중반이후 본격적으로 등장한 사이버범죄에 대처하기에는 미흡한 부분이 있었다. 이에 정부는 정보통신방법을 개정하여 사이버범죄에 관한 규정을 삽입하였고, 사실상 이법이 사이버범죄에 대처하기 위한 기본법으로서의 위치를 가지게 되었다.[2] 그러나, 개방성·신속성을 위주로 한 인터넷의 발전은 사회가 인터넷이 유발시킬 수 있는 잠재적 위험

1) 허일태, "사이버범죄의 현황과 대책", 「동아법학」 제27호, 2000, 66면.
2) 이정훈, "사이버범죄학의 동향과 전망", 「경찰법연구」 제9권 제2호, 2011, 196면.

성에 대해 충분히 대비하지 못한 상태에서 지나치다 싶을 정도로 급속하게 진행되었다. 더구나 이러한 상황에 대해서 정부나 전문가들은 인터넷의 잠재적 위험성의 원인을 도외시한 채 최종적인 사회적 결과물, 즉, '자살', '채팅', '게임중독', '엽기', 등에만 주목하여 양적인 실태파악과 규제에만 집중함으로써 정보사회에서 인터넷으로 인한 역기능 문제가 근본적으로 해결되지 않은 채 새로운 형태의 문제들을 생산해 내고 있는 상황이 발생하게 되었다.[3] 정보사회를 실현함으로써 금세기 최대문명의 이기로 각광을 받게된 컴퓨터도 사회편익의 증진이라는 밝은 면과 함께 컴퓨터의 오용과 남용을 통해 인류에게 피해를 주는 어두운 면도 있는데, 그 가운데 하나가 컴퓨터의 급속한 보급과 정보통신기술의 발달을 악용하는 사이버범죄가 증가한다는 것이다.[4] 정보화사회로의 전환이 가속화됨에 따라 컴퓨터관련 범죄가 급증하게 되면서 워드프로세스파일과 전자메일 같은 전자기록이 형사소송에서 중요한 증거로 활용되는 사례가 빈번해지고 있고, 이러한 전자증거의 수집가능성 여부가 수사의 성패를 좌우하게 될 정도에 이르렀다.[5] 그러나 디지털증거에 대한 압수수색은 압수수색의 대상이 유체물이 아니라 무체물인 정보이며, 눈으로 보이지 않아 한정을 하거나 특정을 하기 어렵고 제3자로부터 목격될 가능성이 낮아 이러한 증거가 있는지 사전에 미리 알기 어렵다. 범행현장도 한군데로 특정하기 어려우며 국제적인 경우도 있다. 증거가 범행이 일어난 곳에 반드시 있지 않으며 많은 곳에 분산되어 있을 가능성이 높으며, 다른정보와 함께 혼재되어 있어 특정하는데 많은 시간과 노력이 필요하며, 증거취득과정에서 오염될 가능성이 높아 그것을 취득하는데 특별한 기술이 필요하며, 유체물에 비하여 쉽게 멸실될 가능성이 있어 사전에 강력한 보존조치가 필요하다. 또한 전송 또는 이동 중에 있는 경우도 많다. 따라서 이러한 디지털증거의 특성에 적합한 압수수색제도를 마련하는 것이 필요하다.[6]

3) 정완, "사이버범죄의 현상", 「형사정책」 제19권 제2호, 2007, 10면.
4) 우제태, "사이버범죄의 대응방안에 관한 연구", 「경찰연구논집」 제1호, 2007, 171면.
5) 박수희, "전자증거의 수집과 강제수사", 「한국공안행정학회보」 제29호, 2007, 128면.
6) 조석영, "디지털정보의 수사방법과 규제원칙", 「형사정책」 제22권제1호, 2010, 7. 76면.

Ⅱ. 사이버범죄의 실태

1. 사이버범죄의 개념

사이버범죄는 불법적 활동에 관여하기 위한 컴퓨터기술의 사용을 나타내는 용어의 하나이다. 컴퓨터범죄(Computer Crime), 하이테크범죄(HiTech Crime), 그리고 정보시대범죄(information-age crime), 등도 또한 이러한 현상을 표현하기 위해 사용된다.[7] 컴퓨터범죄는 보편화된 용어로써 컴퓨터를 대상으로 하거나 수단으로 하여 행하는 범죄행위를 말한다. 여기에는 컴퓨터부정조작, 데이터의 부정입수 내지 컴퓨터스파이, 컴퓨터파괴 내지 컴퓨터 업무방해, 컴퓨터 무권한 사용 내지 시간절도 등을 볼 때, 독립적인 컴퓨터시스템에 중점을 둔 용어라고 할 수 있다.[8]

사이버범죄는 사이버공간상에서 범죄자와 피해자의 대면없이 컴퓨터를 이용하여 접촉함으로써 비대면성과 익명성을 가짐에 따라 피해자가 가해가 누구인지를 정확히 알 수 없으며 타인의 인적사항이나 ID를 도용하면 완벽하게 자신의 익명성을 보장받을 수 있다.[9] 또한, 시간과 공간의 제약을 받지 않고 24시간 내내 어디서든 사용할 수 있다. 이로 인한 심각한 문제는 범죄행위장소와 범죄발생장소의 불일치, 또는 국가간에 발생하게 되는 범죄는 범죄수사의 한계를 나타나게 된다.[10] 그러므로, 컴퓨터프로그램조직을 통한 재산취득, 바이러스제작 및 유포, 해킹과 같은 사이버범죄는 고도의 점문적인 지식과 기술을 갖추고 있어야 가능한 범죄가 대부분이다.[11]

사이버공간에서 벌어지는 범죄는 현실공간에서 일어나는 범죄보다 평균적

7) 권오걸, "사이버범죄와 대응전략", 「법학연구」 제36집, 2009, 11, 197면.

8) 김용현 · 황영구, "사이버공간에서의 범죄대응시스템 문제점과 대응방안에 관한 연구", 「한국치안행정논집」 제4권 제1호, 40면.

9) 강동범, "사이버범죄와 형사법적대책", 「형사정책연구」 제42집, 2000, 41면.

10) 박창욱, "사이버범죄에 대한 효율적인 경찰대응 방안에 관한 연구", 한국컴퓨터정보학회 제37차 동계학술발표논문집 제15권 제2호, 2007, 12,, 141면.

11) 김용현 · 황영구, 전게논문, 41면.

으로 높은 암수범죄(hidden crime)가 발생하고 있다.[12] 피해를 당하는 사람이나 기업들이 자신들의 이미지손상과 자체보완장치의 부재가 노출되는 점을 우려해서 피해사례를 기피하고 자체적으로 해결하려는 경향이 크기 때문에 형사문제로 노출되는 경우가 적다.[13] 더구나, 수많은 컴퓨터가 네트워크화되고 인터넷을 통해 시공을 초월하는 사이버공간을 형성함에 따라 특히 바이러스와 해킹에 의한 시스템작동불능은 시스템에 연결된 모든 컴퓨터의 작동을 멈추게 함으로써 업무전반을 마비시키는 심각한 결과를 초래하여 천문학적 재산피해를 야기한다.[14]

2. 사이버범죄의 유형

사이버범죄의 유형으로는 사이버테러형범죄와 일반사이버범죄로 다음과 같이 나누어볼 수 있다. 해킹, 바이러스 유포와 같이 고도의 기술적인 요소가 포함되어 정보통신망자체에 대한 공격행위를 통해 이루어지는 것을 사이버테러형범죄라고 하며 전자상거래 사기, 프로그램불법복제, 불법사이트운영, 개인정보침해 등과 같이 사이버공간이 범죄의 수단으로 사용되는 유형을 일반사이버범죄로 구분한다.[15]

가. 사이버테러형범죄

(1) 해킹

해킹(hacking)이란 타인의 컴퓨터 시스템에 무단으로 침입하여 수록된 정보를 빼내거나 시스템을 파괴하는 행위를 말한다.[16] 또한 해킹범죄는 DDoS 공격과 함께 국가기밀 탈취와 시스템파괴 등을 위한 사이버테러의 가장 강력

12) 김상균, "사이버범죄에 대한 경찰의 수사력강화방안", 「법학연구」, 한국법학회, 2001, 405면.
13) 우제태, 전게논문, 177면.
14) 정완, "사이버범죄의 현상", 「형사정책」 제19권 제2호, 2007, 13면.
15) 경찰청 사이버테러 대응센터, 2012.
16) 최영호, "정보범죄의 현황과 제도적 대처방안", 한국형사정책연구원, 1998, 61면. 재인용.

한 수단으로 활용되고 있다. 경쟁하거나 분쟁중인 국가간에 경제적· 군사적 타격을 위해 공격을 감행하고, 외교적 분쟁으로 이어지거나 실제 정보전의 수단으로도 이용되고 있다.[17]

(2) DDoS(분산서비스거부공격)

DDoS공격은 유명한 사이트의 접속을 마비시킴으로써 많은 사람들에게 공격사실을 홍보할 수 있고, 범행준비에 많은 비용이 소요되지 않으며 대외적으로 들어나지 않는다는 장점 때문에 테러분자에게는 매우효과적인 사이버테러 수단으로 인식되고 있다.

(3) 악성프로그램

바이러스를 제작하여 유포시킴으로써 컴퓨터에 의해 처리되는 타인의 업무를 방해하는 행위도 컴퓨터손괴 등 업무방해죄를 구성한다. 즉 타인의 컴퓨터의 프로그램이나 자료화일을 삭제하게 만드는 바이러스는 '전자적 기록의 손괴'에 해당하기 때문이다.[18] 악성프로그램을 바이러스, 웜, 악성코드, 불법적인 스파이웨어 등을 모두 포함하는 개념으로 시스템을 파괴하거나 오작동을 일으키고, 이메일이나 파일을 자동으로 유출하게 하는가 하면 피싱을 비롯 좀비 PC를 통해 대출, 성매매, 바이러스 무료진단 등과 같은 팝업 광고를 하는데도 활용된다.

(4) 피싱

피싱(phishing)이란 금융기관이나 정보통신서비스회사 등의 위장홈페이지를 만들어 개인에게 메일을 보내 이들로 하여금 위장홈페이지를 접속하도록 한 후 신용카드번호, 계좌정보 등을 입력하도록 하여 개인정보를 빼내 불법적으로 이용하는 사기수법이다.[19]

보이스 피싱은 무작위로 전화를 걸기보다는 인터넷 사이트등에서 입수한

17) 장윤식 · 김기범, 「사이버범죄수사론」, 경찰대학, 2011 , 17면.
18) 강동범, "사이버범죄와 형사법적대책", 「형사정책연구」 제42집, 2000, 50면.
19) 강동범, "사이버범죄 처벌규정의 문제점과 대책", 「형사정책」 제19권 제2호, 2007, 44면.

개인정보를 기초로 범행이 이루어지고, 이러한 보이스 피싱에 의하여 많은 사람들이 피해를 입게 되는 바, 중요한 문제는 보이스 피싱을 통해 '고객의 현금'을 인출당하는 피해자가 속출하고 있다는 점이다.[20]

우리나라에서 피싱범죄는 포털사이트에 광고글을 게시하거나, 전자우편을 발송하여 경품 이벤트, 신용대출, 게임 아이템 충전 등을 미끼로 이름, 주민등록번호, 전화번호, ID, 패스워드를 알아내는 범죄가 많이 일어나고 있다. 피싱으로 확보한 개인정보나 금융정보는 사기성전화, 스팸메일발송, 물건구매를 통한 결제대납에서부터 금융기관 예금인출까지 광범위하게 사용된다.

(5) 스팸메일

스팸메일(spam mail)이란 수신자가 원하지 않는 정보를 영리목적으로 반복하여 전송하는 메일을 말하며, 정크메일(junk mail)·벌크메일(bulk mail)이라고도 한다.[21] 스팸메일은 가상공간내의 자신의 사적공간에 대해 간섭받지 아니할 사생활 보호권의 침해내지 원하지 아니하는 정보를 받지아니하는 정보를 받지 아니할 정보프라이버시권의 침해로 볼 수 있다.[22] 스팸범죄는 정보통신 인프라의 발달에 따라 새롭게 등장한 범죄로 일반전화, 팩스, 전자우편, 휴대폰을 통해서 이루어지는 범죄로 스팸발송 그 자체로 범죄를 구성할 뿐만 아니라 개인정보 탈취와 금융사기를 위한 피싱과 DDoS 공격을 위한 악성코드 유포의 수단으로도 활용되고 있다.

나. 일반사이버범죄 유형

(1) 사이버스토킹

사이버스토킹은 정보통신망을 이용하여 행위가 이루어져야 하고, 공포심이나 불안감을 유발하는 행위가 있어야 하며, 이러한 행위가 최소한 2회이상 발생하여야만 처벌될 수 있다. 통상적으로는 하나의 일죄로만 끝나는 것이 아니

20) 정완, "사이버범죄의 실태와 동향 및 대응책", 「홍익법학」 제10권 제1호, 2009, 202면.
21) 강동범, "사이버범죄 처벌규정의 문제점과 대책" 「형사정책」 제19권 제2호, 2007, 43면.
22) 국방부과학수사연구소, 「사이버범죄수사」, 230면.

라 수개의 범죄행위와 결부되어 복합적으로 발생하는 경우가 많다. 정보통신망법상 사이버스토킹과 별개로 인터넷카페·블로그 또는 게시판 등에 해악을 고지하는 내용을 올리는 경우에는 형법상 협박죄(제283조), 모욕하는 경우에는 형법상모욕죄(제311조), 명예를 훼손하는 경우에는 정보통신망법상 사이버명예훼손죄(제70조) 등으로 처벌할 수도 있다.

(2) 사이버음란물

미국연방법원은 2007년 3월 미성년자의 사이버음란물 접근을 허용한 음란사이트운영자를 처벌하는 내용의 아동온라인보호법(Child Crime Protection Act, 1998)이 헌법상 표현의 자유를 침해한다고 판결하였다. 인터넷포르노금지법에 대하여 표현의 자유를 규정한 헌법을 위반하였다는 판결을 통해 알수 있듯이 사이버공간상의 음란물에 대한 정부차원의 대응은 매우 힘든 것이 사실이다.[23]

사이버공간에서 유통되는 음란물의 내용은 대체로 정상적인 성관계가 아닌 폭력과 변태, 엽기로 흐르고 있고, 이성과의 성관계를 쉽게 생각하고 나아가 강간범죄를 정당화 시킬 우려가 있다. 오프라인상 음란물 유포에 대해서는 형법상 음란죄, 공연음란죄로 처벌하고, 온라인상 음란물 유포행위에 대해서는 정보통신망법상 음란물 유포죄로 처벌하고 있다.

(3) 사이버명예훼손

사이버세계의 비대면성과 익명성 그리고 시공을 초월할 수 있는 기능 때문에, 타인에 대한 비방이나 언어폭력은 현실세계와는 비교도 되지 않을 정도로 많이 발생한다. 그뿐만 아니라 타인의 ID를 훔쳐 음란물을 판매하는 등의 방식으로 타인의 명예를 훼손하는 경우도 적지않다.[24] 우리나라는 명예훼손의 경우 '정보통신망이용촉진 및 정보보호 등에 관한 법률'에서 처벌하고 있지만, 모욕의 경우 처벌조항이 없어 법개정이 요구된다.[25]

23) 정완, "사이버범죄의 실태와 동향 및 대응책", 「홍익법학」 제10권 제1호 2009, 203면.
24) 허일태, 전게논문, 73면.
25) 조호대, "사이버범죄에 대한 경찰 수사전문화 방안", 「한국경찰학회보」 13권 5호, 2011, 244면.

(4) 사이버도박

사이버도박이란 사이버공간에서 일정한 재물을 걸고 우연성이 기초하여 블랙잭·포커와 같은 카드게임이나 슬롯머신·룰렛 등 각종 도박을 즐길 수 있도록 고안된 프로그램을 이용한 도박행위를 말한다.[26]

2008년 10월에 도박사이트 운영자, 장애인바지사장 알선책, 도박사이트개별관리업체 대표, 관련조직폭력배등이 한꺼번에 구속된 사건이 발생하였는데, 이들은 태국(파타야)과 중국연길에 설치한 콜센터(가맹PC방에 대한 사이버머니 충전 및 자금정산)를 이용, 불법으로 인터넷 도박사이트인 엠비게임 등을 운영하면서 경기지역에 수백개의 PC방을 모집, 도박사이트의 사이버머니를 환전하게 해주면서 손님의 배팅금액당 일정액을 수수료로 공제, 가맹PC방 및 총판과 배분하는 방법으로 도박을 개장해 수억원의 이익을 챙겼다고 한다.[27]

(5) 사이버사기

사이버 사기행위는 지능범들이 행하는 범죄인 화이트칼라의 한 범죄로 분류한다. 사이버사기는 전자상거래와 관련하여 사이버공간에서 이루어지는 사기행위의 한 유형을 말한다.[28] 전자상거래 등에서의 소비자보호에 관한 법률(이하 전자상거래법)에서는 사이버쇼핑몰을 운영하는 사업자 신원에 관한 정보게시와 통신판매업자 신고를 의무화하고 있고, 허위과장광고를 통한 소비자 유인 등 금지행위에 대해서 위반사실에 대한 조사와 감독권을 부여하여 관리감독 등 예방활동을 벌이고 있다.

3. 사이버범죄의 현황

사이버범죄의 최근 5년간 발생건수는 2007년도에 8만8천여건, 2008년도에 13만6천여건, 2009년도에 16만4천여건으로 꾸준히 증가하다가 2010년도에 12만2천여건, 지난해 2011년도에 11만6천여건으로 감소추세를 보이고 있다.

26) 김연수, 「사이버범죄 총람」, 법률미디어, 2002, 754면. 재인용.
27) 정완, "사이버범죄의 실태와 동향 및 대응책", 「홍익법학」 제10권 제1호, 2009., 205면.
28) 조호대, 전게논문, 244면.

〈표 1〉 사이버범죄의 최근 5년간 유형별 발생현황

구분 / 연도	총계		사이버테러형 범죄		일반사이버 범죄	
	발생	검거	발생	검거	발생	검거
2007	88,847	78,890	17,671	14,037	71,176	64,853
2008	136,819	122,227	20,077	16,953	116,742	105,274
2009	164,536	147,069	16,601	13,152	147,935	133,917
2010	122,902	103,809	18,287	14,874	104,615	88,935
2011	116,961	91,496	13,396	10,299	103,565	81,197

* 사이버대응대응센터(http://www.ctrc.go.kr)

주) 내사종결도 사이버범죄의 변화추이를 분석할 수 있다는 점에서 포함

사이버범죄의 발생에 따른 유형별 검거인원도 마찬가지로 2007년도에 7만9천여명, 2008년도에 12만2천여명, 2009년도에 14만7천여명으로 꾸준히 증가하다가 2010년도에 10만4천여명, 2011년도에는 9만1천여명으로 감소추세를 보이고 있다.

〈표 2〉 사이버범죄의 최근 5년간 유형별 검거현황

구분	총계	해킹·바이러스	인터넷 사기	사이버 폭력	불법사이트운영	불법복제판매	기타
2007	78,890	14,037	28,081	12,905	5,505	8,167	10,195
2008	122,227	16,953	29,290	13,819	8,056	32,084	22,025
2009	147,069	13,152	31,814	10,936	31,101	34,575	25,491
2010	103,809	14,874	35,104	8,638	8,611	17,885	18,697
2011	91,496	10,299	32,803	10,354	6,678	15,087	16,275

* 사이버테러대응센터(http://www.ctrc.go.kr)

2011년 사이버범죄의 연령별통계는 20대가 40.2%로 가장 높게 나타났고, 30대의 경우 27.2%, 10대 17.6%, 40대이상은 14.4%순으로 나타났다. 이러한 통계를 보면 알 수 있듯이 컴퓨터와 인터넷의 이용빈도가 높은 연령대에서 사이버범죄가 높게 나타난다.

〈표 3〉 사이버범죄의 최근 5년간 연령별현황

구분	10대	20대	30대	40대 이상	기타
2007	15.1%	39.2%	26.3%	17.7%	1.7%
2008	26.6%	39.0%	21.8%	11.8%	0.8%
2009	19.4%	34.0%	29.6%	16.5%	0.5%
2010	19.5%	39.5%	25.4%	14.4%	1.2%
2011	17.6%	40.2%	27.2%	14.7%	0.3%

* 사이버테러대응센터(http://www.ctrc.go.kr)
주) 내사종결사건은 제외함

Ⅲ. 디지털증거의 압수 · 수색 문제점

1. 디지털증거의 의의

사이버범죄에 있어서 증거란 주로 디지털증거(Digital Evidence)와 관련된 것을 말하며 디지털증거란 범죄를 증명할 수 있는 가치를 지닌 이진형태로 저장되거나 전송될 수 있는 정보로서 범죄와 피해자 또는 범죄와 가해자 사이의 연결고리를 제공할 수 있는 모든 디지털 데이터를 말하는 것이다. 디지털 증거를 다루는데 있어 고려되어야 할 점이 여러 가지가 있는데 그 중 디지털 증거의 증거능력에 대한 문제와 증거법상 전문법칙의 적용여부에 관한 문제이다. 디지털증거에 대해서도 그 진정성, 동일성 및 원본성이 인정되는 경우에는 증거로서 사용될 수 있다.[29]

2. 디지털증거물의 진정성과 동일성을 증명하기 위한 조치[30]

가. 압수된 디지털증거물을 명확하게 특정한다.

29) 중앙경찰학교, 「사이버수사」, 2010, 113면이하.
30) 경찰대학, 「사이범죄수사론」, 2011, 98면.

(1) 디지털증거물 압수시 압수목록에 디지털증거물의 형상을 기재하거나 사진촬영을 한다.

(2) 전원이 꺼진 상태일 경우 압수현장 상태 그대로 피의자에게 확인시킨 뒤 봉인을 하고 피의자의 확인(간인 또는 서명)을 받는다.

(3) 전원이 켜진 상태일 경우 가능한 한 디지털 증거물의 파일명, 생성일시, 용량 등을 피의자에게 확인시킨 뒤 봉인을 하고 피의자의 확인(간인 또는 서명)을 받는다.

(4) 수사기관에 증거물을 가지고 와서 분석을 시작하기전 관계자를 입회시킨후 봉인을 뜯고 디지털 증거물의 내용을 확인시켜야 한다.

나. 내용을 출력할 경우는 출력물이 압수된 디지털증거물로부터 나온 것임을 명백히 해야 한다. 저장할 내용을 프린터 등을 이용해 출현하는 과정에서도 가능한 한 관계자를 입회시켜 그 출력의 진정성을 명확하게 해야 한다.

다. 증거물을 수집하는 단계별로 필요한 사항이나 특이사항 또는 이상한 점을 발견을 할 경우 반드시 기록을 유지한다.

3. 디지털증거의 압수수색 대상성

우리나라 형사소송법에서는 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다.[31] 현행 형사소송법에서 규정하는 증거물에 대하여 컴퓨터전자기록의 압수수색을 부정하는 견해는 물건의 범위를 유체물에 한정시키고 있다. 그런데, 압수대상을 유체물(tangible objects)로 명확히 규정하고 있는 미국법과 달리 우리 형사소송법은 단지 증거물 및 몰수물이라고만 규정하고 있는 점에 유의할 필요가 있다.[32] 문언상 형사소송법은 압수·수색의 객체를 증거물이라고 하고 있고,

31) 형사소송법 제106조(압수) 제1항(개정 2011.7.18).

32) 조석영, 전게논문, 80면.

증거물이란 강제적으로 점유이전의 처분에 당하여 대체성이 없고 물리적으로 가능한 유체물이라고 해석하고 있다. 따라서 문리적으로만 보면 무체정보로서의 기록내용은 유체물성을 결하고 있어 증거물이라고 할 수 없다. 그러나 전자적 기록과 자기테이프 등 전자적 기록매체와는 이론적으로는 구별할 수 없고 결국 일정한 프로그램에 의해 비로소 가시성·가독성이 있는 상태로 되는 것이기 때문에 양자간에 진정한 관계가 인정되는 한 이를 실질적으로 판단하여 증거물이라고 해석하는 것이 타당하다. 컴퓨터를 작동하여 전자적 기록을 아웃풋 하는 것은 압수에 '필요한처분'으로서 인정된다.[33] 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 피고인의 신체, 물건 또는 주거, 그 밖의 장소를 수색할 수 있다.[34]

형사소송법에서는 이 부분에 대해서 디지털증거에 대한 아무런 규정이 되어 있지 않기 때문에 디지털증거가 압수수색의 대상이 될 수 있는 지에 관해서 많은 논란이 되어왔다. 만일 디지털증거가 형사소송법의 압수수색의 대상이 될 수 없는 경우에는 현행 수사기관이 디지털 증거를 압수수색 하는 것이 불법이라는 결론에 도달하기 때문이다. 그러나 실무에서는 압수 수색되는 상당수가 디지털 증거이고 이런 논란과 상관없이 디지털 증거에 대한 압수수색이 행해지고 있다. 또한 이를 부정할 경우 수사자체가 불가능해진다. 그러므로 이와 같은 디지털증거의 압수수색에 대해서 그 근거를 헌법 제12조 제3항의 영장주의에서 찾기도 한다.[35] 특히 컴퓨터에 입력된 정보는 일정한 프로그램을 사용한 명령을 적절히 행하지 않으면 입수할 수 없는 특징을 지니기 때문에 프로그램지침서를 입수하거나 그 프로그램에 대한 전문가의 협력이 요구된다. 이러한 경우 수사과정의 지연이나 증거확보에 차질을 우려하지 않을 수 없다.[36]

33) 노명선, "사이버범죄의 증거확보에 관한 몇가지 입법적제안", 「성균관법학」 제19호 제2호, 2007, 8, 347면.

34) 형사소송법 제109조(수색) 제1항(개정 2011.7.18).

35) 탁희성, "전자증거의 압수수색에 관한 일고찰", 「형사정책연구」 제15권 제1호, 2004, 24면.

36) 김종세, "사이버범죄의 법적쟁점에 관한 고찰", 「경찰연구논집」 제2호, 2008, 241면.

4. 압수수색영장의 특정

디지털증거의 경우 그 정보의 양이 많기 때문에 이를 특정하는 문제가 발생하게 된다. 그 때문에 이를 압수수색하기 위해 특정하는 문제가 발생하게 된다. 영장주의는 일반영장의 금지를 그 내용으로 한다. 이는 현행 형사소송법 제114조(개정2011.7.18)에서는 압수·수색영장에는 피고인의 성명, 죄명, 압수할 물건, 수색할 장소, 신체, 물건, 발부연월일, 유효기간과 그 기간을 경과하면 집행에 착수하지 못하며 영장을 반환하여야 한다는 취지 기타 대법원규칙으로 정한 사항을 기재하고 재판장 또는 수명법관이 서명날인 하여야한다. 다만, 압수·수색할 물건이 전기통신에 관한 것인 경우에는 작성기간을 기재하도록 하고 있기 때문에 압수수색의 범위를 특정하고 있다.[37] 또한, 형사소송규칙 제107조는 압수수색영장 청구서에 기재하여야 할 사항을 나열하고 있으나 압수수색에 대한 구체적인 방법에 대하여는 현행법상 요청되고 있지 않다. 이를 현장에서 수색을 종료할 것인지 아니면 일단 캐비넷이나 서류, 컴퓨터 등 용기를 압수후 제3의 장소에 이전해서 수색할 것인지에 대하여도 아무런 기재가 없다.[38]

범인의 컴퓨터 내에서 관련 정보만을 압수수색하거나 원격지에 있는 서버에서 다른 범인과 관련되지 않은 일반인들의 정보로부터 범인의 정보만을 특정하여 압수수색하는 것은 거의 불가능에 가까울 정도이다. 이 때문에 특정성의 요건들이 어느 정도 완화되어 다소 포괄적이거나 일반적인 용어가 기술된 경우라고 하더라도 유효하다고 판단할 필요가 있다. 또한 압수수색 장소의 경우에도 다소간의 완화가 필요하다. 디지털증거가 존재하는 컴퓨터나 서버를 특정하는 것은 매우 어렵다. 특히 디지털정보는 쉽게 전송 및 이동이 가능하기 때문에 이를 통해서 압수수색 영장을 쉽게 무력화 시킬 수도 있다. 따라서 디지털증거가 압수수색의 장소에는 없다고 하더라도 그 장소에서부터 합법적으로 접속 가능한 네트워크 시스템에 존재할 경우 영장기재의 특정성을 어긴 것으로 볼 수는 없을 것이다.[39]

37) 이재상, 「신형사소송법」, 2008, 302면.
38) 노명선, 전게논문, 351면.

5. 영장의 집행

디지털 증거에 대한 인식이 수사기관에 확산되기 이전에는 사이버범죄에 대한 영장을 집행함에 있어서 많은 문제가 있었다. 기본적으로 컴퓨터 저장장치의 용량이 수백기가에서 테라(Tera)바이트를넘어가기 때문에 압수품을 선별하는 것에도 어려움이 있다. 압수품을 선별한 뒤에도 이처럼 거대한 저장용량 속에서 필요한 정보를 찾아내는 과정 역시 매우 힘들다.[40] 특히 디지털 증거가 오염되거나 훼손되는 문제들로 인하여서 디지털증거에 대한 증거능력이 부인되는 경우도 많이 발생하고 있다. 그러므로 압수수색 영장을 집행함에 있어서는 반드시 정형적인 절차를 정해놓고, 영장을 집행하는 자가 이를 준수할 필요가 있다. 일반적으로 압수수색 영장을 집행함에 있어서 다음의 사항이 고려되어야 한다. 첫째, 현장에서 압수수색영장을 제시한 후 사용자들이 현장의 컴퓨터 작업을 중지하도록 한다. 둘째, 해당 컴퓨터 수색시 그 사용자를 확인하여 참여시키며, 견출지 등으로 사용자 표시 및, 컴퓨터 시간을 확인한다. 셋째, 컴퓨터 본체 압수시 사용자가 보는 앞에서 컴퓨터의 케이스를 열어 내부 부품을 확인 시킨후 이를 사진으로 촬영한다. 넷째, 하드디스크만을 압수하는 경우 이를 본체에서 분리한 후 사용자에게 제조사, 용량, 제조번호 등을 확인시키며, 필요시에는 사진촬영한다. 다섯째, 하드디스크의 내용만을 복제시 복제전후에 사용자에게 이를 확인 시킨후, 확인을 받는다. 여섯째, 피의자가 사용하는 컴퓨터의 주변을 수색하여 기타의 저장장치 확인한다. 일곱째, 압수수색 목록 작성시 압수한 품명과 제조번호를 구체적으로 기술한다.[41] 또한, 영장없이 압수수색이 가능한 경우에는 첫째, 소유자 또는 보관자가 컴퓨터 또는 저장장치를 임의로 제출하는 경우이고 둘째, 수인이 공동으로 사용하는 컴퓨터 또는 저장장치를 사용자 중 1인이 임의로 제출하는 경우이며 셋째, 보관자에게 임의제출 권한이 있다고 인정되는 경우이다.[42]

---

39) 탁희성, "전자증거에 관한 연구", 이화여자대학교대학원, 박사학위논문, 2004, 107면.
40) 경찰수사연수원, 「2010 사이버범죄수사」, 56면.
41) 경찰수사연수원, 전게서, 62면.
42) 중앙경찰학교, 전게서, 109면.

다만, 압수수색 영장의 집행에 있어서 아직도 어려움을 겪고 있는 것이 SNS와 같이 원거리의 서버에 저장되어 있는 정보를 압수수색하는 절차이다. 실제로 외국에 있는 서버에 저장되어 있는 정보는 관련회사가 협조해 주지 않을 경우에는 집행이 불가능하게 된다. 따라서 이와 유사한 이메일 압수수색과 관련해서 실질적인 소송절차 확보를 위해서 국가간의 공조가 매우 필요하다는 견해가 제기되고 있다.[43] 또한 압수·수색의 대상인 컴퓨터가 네트워크로 다른 컴퓨터나 서버에 접속되어 있는 경우에는 원격지에 저장된 정보를 다운로드하거나 복사하게 한 후 압수하는 제도의 도입도 검토되어야한다.[44]

6. 압수·수색 문제점의 한계

디지털증거의 경우 무체물인 정보이므로 가시성이 없어서 특정하기 어렵고, 제3자로부터 목격될 가능성이 낮아 이러한 증거가 있는지 사전에 미리 알기가 어려울 뿐만 아니라 범행현장도 국제적인 경우가 많다. 더구나 증거가 범행장소가 아닌 많은 곳에 분산되어 있을 가능성도 크고, 다른 정보와 혼재되어 있는 경우도 많아서 그 대상을 특정함에 있어서 많은 시간과 노력이 필요하다.[45] 또한, 네트워크 기술을 이용한 데이터 저장방식은 사이버범죄 수사에 있어서 장애요인이 된다. 즉, 피의자가 사용하는 컴퓨터를 조사해 보지 않고서는 피의자가 어떠한 '네트워크 드라이브'나 '웹하드'를 사용하는지 알 수 없고, 따라서 사전에 적절한 압수수색의 대상을 특정하기 곤란하다.[46] 그리고 수사기관이 시스템관리자의 물리적 소재지를 대상으로 압수수색영장을 발부받아 이를 집행하더라도 실제 필요한 데이터가 물리적으로 멀리 떨어져있는 서버에 저장되어 있는 경우에 영장기재 장소인 시스템 관리자의 물리적 소재지에서 원격지 서버에 접속하여 범죄사실과 관련된 수색할 수 있는지 문제된다.[47]

43) 김성룡, "이메일 압수수색에 관한 독일 연방헌법재판소 결정의 주요내용과 그 시사점", 「법학논고」, 2012, 2, 221면.

44) 노명선, 전게논문, 354면.

45) 강동욱, "디지털증거 수집에 관한 형사소송법 개정안에 대한 검토", 「법학연구」 제18권 제3호, 2010, 12, 168면.

46) 중앙경찰학교, 전게서, 107면.

정보의 출력·복제 디지털증거압수는 증거의 종류나 현장의 상황에 따라 그 방법에 차이가 크며, 압수현장에서 저장매체 모두를 수색·검증하기 위해서는 장시간이 소요될 수 있고, 복제가 가능하더라도 정보의 양이 방대할 경우 시간상 현실적으로 복제가 불가능하며, 증거의 복제나 출력이 원본의 압수보다 대상자의 업무에 지장을 더욱 가중시킬 수 있다는 것이다.[48] 형소법 제106조 제3항의 "출력하거나 복제하여 제출받아야한다"는 규정이 제출명령을 표현한다고 할 수 있지만, 이를 가지고 출력과 복제를 법원이나 수사기관이 강제로 할 수 있다는 표현을 포함한다고 할 수 있느냐는 것이다. 입법과정에서 국회의원들이 그렇게 해석된다고 합의한 것을 무시할 수는 없겠지만 국어가 가지고 있는 일상적인 의미를 벗어나는 해석이 가능해지는 문제점이 있다.[49] 기록복사 명령후 압수에 대하여 수사기관으로서는 이러한 통신내역을 알거나 이를 보전하기 위해서는 통신내역이 기록된 통신사업자의 컴퓨터나 기록매체에 대하여 압수수색이나 검증을 하는 방법이 있을 뿐이다. 그러나 이는 통신사업자의 업무를 방해하거나 범죄와 관련이 없는 이용자의 권리나 이익을 많건 적건 침해하게 된다.[50] 그리고, 범죄관련성이 미미하고 과도하게 오래전에 생성된 기록들에 대해 압수수색이 이루어지고 있고 압수수색이 정보저장장치 전체에 대해 이루어지면서 범죄관련성이 없는 기록들까지 한꺼번에 압수수색이 되고 있어 포괄적 압수수색금지원칙에 위반된다는 것이다.[51]

7. 디지털증거의 압수수색제도와 관련된 형사소송법 개정법률

디지털증거의 압수수색제도와 관련하여 2009년부터 다양한 내용의 형사소송

47) 강철하, "디지털증거압수수색에 관한 개선방안", 성균관대학교 법학전문대학원 법학과 박사학위논문, 2012, 204면.

48) 손동권, "새로이 입법화된 디지털증거의 압수·수색제도에 관한 연구", 「형사정책」 제23권 제2호 2011, 12, 331면.

49) 이윤제, "디지털증거 압수·수색영장의 집행에 있어서의 협력의무", 「형사법연구」 제24권 제2호, 2012, 20면.

50) 노명선, 전게논문, 348면.

51) 박광현, "사이버공간에서의 법익침해에 관한 형사법적 고찰", 숭실대학교 「법학논총」 제28집, 2012, 7, 20면.

법 일부 개정법률안 등이 제출되어 논의되다가, 형사소송법 개정법률(법률 제10864호)이 2011. 7. 18. 공포되어 2012. 1. 1. 시행되게 되었다.[52]

디지털증거의 압수수색제도와 관련된 형사소송법 개정법률(법률 제10864호)의 주요내용은 다음과 같다.

첫째, 법원의 압수·수색의 요건에 피고사건과의 관련성을 추가하였다(제106조 제1항, 제107조, 제109조). 둘째, 정보 저장매체등에 관한 압수의 범위와 방법을 명시하고, 정보주체에게 해당사실을 알리도록 하며, 영장에는 작성기간을 기재토록 명시하는 등 전기통신관련 압수·수색제도를 보완하였다(제106조 제3항·제4항, 제114조 제1항). 셋째, 수사기관의 압수·수색·검증의 요건에 피고사건과의 관련성과 피의자가 죄를 범하였다고 의심할 만한 정황이 있을 것을 추가하였다(제215조). 넷째, 압수물의 소유자, 소지자 등의 신청이 있을 경우 수사기관이 압수물을 환부 또는 가환부할 수 있도록 하고, 기존의 준용규정을 정비하였다(제218조의2, 제219조).[53]

Ⅳ. 디지털증거의 압수 · 수색 개선방향

인터넷사용이 대중화된 사회에서 디지털증거는 간과할 수 없는 중요한 의미를 갖는다. 디지털증거의 압수·수색은 효율적인 증거수집 뿐만 아니라 적정절차원칙, 실체적진실주의 발견, 개인의 사생활비밀보호와 상충되는 가치조화를 이루어야 한다. 이를 위해서는 다음과 같은 내용의 보완입법방안이 도입되어야 하고 검토되어야 한다.

1. 디지털증거의 신속한 보전제도

수사기관이 원본은 그대로 두고 저장된 정보만을 출력 또는 복제해 갈 경우

52) 이주원, "디지털증거에 대한 압수수색제도의 개선", 「안암법학」 제37권, 안암법학회, 2012, 196면.

53) 이주원, 전게논문, 192면-193면.

원본소지자는 거기에 남아있는 정보의 내용을 얼마든지 쉽게 삭제·변경을 가할 수 있다. 이 경우에는 출력물 내지 복제물의 출처가 원본으로부터 나왔다는 사실여부에 관한 동일성 문제와 무결성 문제가 대두될 수 있고, 그 여파로 출력물 또는 복제물에 대한 증거물의 증거능력의 부여가 어려워질 수 있다. 이러한 문제를 해결하기 위해서는 데이터를 압축하여 하나의 형태로 출력하는 이미징 파일에 대해 원본동일성을 긍정하거나 미국의 입법례와 같은 보존명령제도를 도입하여 피처분대상자가 증거훼손을 할 경우 법률상 불이익을 부과하는 입법조치가 요구된다.[54]

디지털범죄에서 컴퓨터와 관련하여 수사기관에 보관되거나 압수되어 있는 컴퓨터, 디스켓, 핸드폰, 디지털카메라 등 디지털증거에 대하여는 영장이 없는 수색은 허용되지 않는다.[55] 이는 오프라인에 관한 범죄의 증거에 대하여는 경찰서에 보관하는데 큰 문제가 없지만, 컴퓨터에 저장되어있는 디지털정보나 자료는 디지털 증거의 특성상 경찰서에서 보관하게 되는 경우에 증거의 삭제나 변경이 가능할 수 있기 때문이다. 따라서 수사기관에 보관되어있는 디지털증거에 대한 수색에 있어서는 수색영장을 발부 받아야할 것이다.[56] 디지털증거의 변조용이·취약성 등의 특성으로 인해 신속한 증거보전절차마련이 필요할 뿐만 아니라 "관할지방법원 또는 지원의 허가를 받을 시간적여유가 없는 경우"에는 먼저 수사기관이 이른바 '긴급보전명령처분'을 하고 지체없이 법원의 허가를 받도록 할 필요가 있다. 이 경우 필요한 때에는 피처분자에게 비밀유지의무를 부과하여 범죄수사 관련정보의 누설로 인해 발생가능한 수사상 위험을 사전에 차단할 필요도 있다. 결국 보전명령제도는 결국 압수수색을 위한 사전처분이기 때문에 단지 이러한 보전명령만으로 압수수색하는 것은 불가능하다고 보아야 한다. 따라서 보전된 자료에 대해 압수수색을 하기 위해서는 별도의 압수수색영장을 발부받아야 할 것이다.[57]

---

54) 손동권, 전게논문, 343면.

55) United States v. O'Razvi, 1998 WL, 405048, at *6-7(S.D.N.Y. July 17, 1998): United States v. Flores, 122 F. Supp. 2d 491, 493-95(S.D.N.Y. 2000). 재인용.

56) Computer Crime and Intellectual Property, Section Criminal Division United States Department of Justice, op. cit, p23. 재인용.

57) 강철하, 전게논문, 218면-219면.

2. 기록명령후 압수제도

수사기관이 디지털정보를 출력하거나 파일을 복사하는 과정에서 그 정보의 소유자나 관리자의 당해 관련정보 또는 이를 저장하고 있는 컴퓨터디스크 등에 대한 접근을 강제로 배제하고, 그 의사에 반하여 관련정보를 획득하는 것이므로 반드시 정보 그 자체 또는 원본 파일의 수집만을 압수라고 그 의미 및 대상을 좁게 해석할 실질적인 이유가 없다고 한다. 따라서 출력물의 수집이나 파일복사의 방법으로 디지털정보에 대한 압수가 가능하며 압수집행에 대해서는 영장주의의 통제가 필요하다고 한다.[58] 대량의 정보를 보유한 기업의 서버를 무리하게 압수수색하는 경우, 기업의 정상적인 영업행위를 방해할 수 있고 관련 없는 제3자의 프라이버시를 부당하게 침해할 소지도 있다. 나아가 만일 필요한 정보를 보유하고 있는 사람이 범죄와 무관한 사람이라면 오히려 그 사람에게 필요한 정보를 기록케 하고 이를 압수하는 것이 피처분자의 재산권 보호 등에 더 유리할 수 있다는 점에서 '기록명령 후 압수제도'를 도입할 필요가 있다[59]

일본은 법관이 전자기록을 보관하고 있는 자 또한 이용권한이 있는 자에게 수사에 필요한 전자기록을 다른 매체에 기록하거나 출력하도록 명령하여 해당기록물이나 출력물을 압수할 수 있도록 하는 "기록명령첨부영장"제도를 신설하여 입법적인 해결을 시도하고 있다.[60]

3. 원격지 압수수색제도

최근 범죄의 국제화, 지능화로 인해 대부분의 중요한 증거들은 디지털로 처리 서버에 저장하고 있으며, 그것도 외부노출을 피하기 위해 해외서버에 저장해 두고 관리하고 있다. 나아가 별도 해외서버 없이도 중요한 의사소통을 국

58) 이경렬, "디지털정보 관련 압수수색규정 도입을 위한 전제적 고찰", 「성균관법학」 제21권 제2호, 2009. 8, 319면.

59) 강철하, 전게논문, 221면.

60) 일본 형사소송법 개정안 제99조의2

내의 법집행력이 미치지 않는 구글, 야후 등과 같은 해외서버를 이용하는 경우도 포함한다.[61] 수사관이 네트워크에 연결된 다수의 컴퓨터에 압수수색대상인 동일한 데이터가 존재하거나 네트워크컴퓨터에 분산되어 있다고 판단한 경우, 해당 데이터가 금제품과 같은 것으로서 반드시 압수하여 파기하여야 할 경우에는 해당 데이터가 존재하는 각각의 컴퓨터가 있는 장소를 특정하여 영장을 발부받아야한다.[62] 영장에 특정된 입력장치에 대한 압수수색만이 허용된다면 입력처리장치와 저장장치가 서로 다른 공간에 위치해 있는 대상 디지털 정보를 압수수색하지 못하는 사태에 봉착할 수 있기 때문이다. 이러한 경우 압수수색 집행대상인 정보처리장치를 통하여 저장서버에 접속한 후 그 저장정보의 압수수색을 가능하게 하여야 한다는 것이다. 그러나 이러한 원격지 압수수색제도의 입법도입에 대해서는 수색장소는 특정되어야하고 소위 탐색적·일반적 영장은 허용되지 않는다는 영장주의가 침해된다는 반론이 제기될 수 있다.[63]

형사소송법상 원격수색에 관한 명문의 규정은 없고 종래의 이론상으로 형소법 제120조[64] 의 필요한 처분에 포함되는 것으로 해석된다.

4. 협력의무제도

피처분자가 압수수색영장의 목적달성에 필요한 조치를 집행기관에 적극적으로 제공하여야 하는 의무로서, 구체적으로 영장의 집행 전에 대상정보가 삭제되지 않도록 보전조치를 하는 의무(보전의무), 영장의 집행단계에서 압수의 대상인 정보를 제출하는 의무(제출의무), 암호화된 컴퓨터의 작동을 위한 패스워드의 제공, 암호화된 파일의 암호해제(복호화), 네트워크로 연결된 다른 컴퓨터의 접속에 필요한 조치의 제공 등 수사기관의 영장집행행위에 협력하

61) 조석영, 전게논문, 83면.
62) 노명선, 전게논문, 353면.
63) 손동권, 전게논문, 335면.
64) 형소법 제120조(집행과 필요한 처분) ① 압수·수색영장의 집행에 있어서는 건정을 열거나 개봉 기타 필요한 처분을 할 수 있다. ② 전항의 처분은 압수물에 대하여도 할 수 있다.

는 의무(기타 협력의무 또는 협의의 협력의무)가 있을 수 있다. 이를 법원과 수사기관의 입장에서 반대로 표현하면 보전명령, 제출명령, 협력명령이라고 부를 수 있다.[65] 수사기관이 복잡하게 얽혀있는 컴퓨터시스템에서 필요한 정보를 선별하여 압수수색하기란 쉽지 않은 일이며 이 경우 필요한 정보를 확인하는 과정에서 전문적인 기술이 요구될 수 있다. 나아가 압수수색하려는 데이터에 암호가 설정되어 있다거나 전문적인 프로그램을 사용해야 하는 경우라면 오히려 이에 대한 전문적인 지식을 가지고 있는 피처분자에게 협력을 요구하는 것이 보다 현실적인 해결방법이 될 수 있다.[66] 현재 정보처리시스템은 그 구성이 복잡할 뿐만 아니라 암호화 되어있는 경우가 많다. 그리고 통신업체의 서버에 데이터를 저장하는 '클라우딩(Clouding)은 자신의 데이터를 네트워크로 연결되어있는 통신업체 등 제3자의 서버에 저장하여 사용하는 경우를 말하는데, 이러한 경우 통신업체등 제3자의 협력없이는 수사가 진행될 수 없다. 특히 외국서버(예; 구글)에 보관하고 있는 메일에 대한 압수수색은 불가능하다. 이러한 문제점을 해결하기 위해서는 피압수자 내지 정보가 저장된 서버관리자 등의 협력의무를 규정할 필요가 있다는 입법보완론이 제시되고 있다.[67]

5. 현장가압수제도의 긴급처분(독립적 압수수색제도)

미국의 '명백한시야원칙(Plain View Doctrine)'이란 수사기관이 적법하게 위치할 수 있는 장소에서 시야 내에 보이는 물건에 대해서는 그 물건이 범죄와 관련되어 있다고 믿을 만한 상당한 이유가 있어 압수의 대상이 명백한 경우에는 영장없이 긴급압수할 수 있다는 것이다.[68]

마약사건을 위하여 영장을 발부받아 하드디스크를 수색하던 중 아동 포르노파일을 발견한 경우, 법원은 이에 대하여 plain view 법리[69]를 적용할 수

65) 이윤제, 전게논문, 5면.
66) 강철하, 전게논문, 226면.
67) 손동권, 전게논문, 338면.
68) 손동권, 전게논문, 339면.
69) 미국의 영장주의에 대한 합리적인 예외로서 1971년 Coolidge사건에서 구체화되었다. ①대상물을 발견한 장소에 수사기관이 적법하게 출입하였고 ②수사기관의 입장에서 대상물이 범

없다고 하였다. 영장을 발부받은 마약관련 파일만이 합법적이며 따로 영장을 발부받지 않고 수색한 다른 파일은 증거로 인정할 수 없다는 것이다. 우리 형사소송법은 압수수색에 대한 영장주의의 예외에 관하여 형사소송법 제216조 내지 218조에서 이를 규정하고 있고 영장주의는 헌법상 보장이므로 영장주의에 위반하여 수집된 증거의 증거능력을 부정하고 있는 것이 판례의 입장이기도 하다.[70]

그러나, 미국의 plain view 원칙이 적용되지 않는 우리 법제에 있어서는 적합한 압수수색 중에 타사건과 관련된 명백한 유죄의 증거를 발견한 경우에도 이를 압수할 수 없다. 이러한 경우 형식적인 영장발부 절차를 다시 밟아야 하기 때문에 그 기간 중에 증거가 인멸될 수 있고 신속한 범죄대응이 어렵게 될 것이다. 그러므로 우리법제도에 미국의 plain view 원칙과 유사한 현장임시압수제도를 도입할 필요가 있다.[71]

V. 결 어

정보화 사회가 되면서 컴퓨터와 인터넷사용이 일반화되고 있으며, 전세계적으로 생성되는 정보의 대부분이 디지털형태로 나타나고 있는 실정이다. 최근 범죄수사에 있어서도 범죄입증을 위해 디지털증거의 획득이 중요한 수사목적이 되어 있다는 것을 반영하여 새로운 수사방법으로서 디지털 포렌식의 활용이 크게 확대되고 있다.[72]

많은 이용자가 접속하는 대형시스템의 경우에는 그 전산시스템 자체를 압수하게 되면 선의의 이용자들이 피해를 입게 되므로 필요한 데이터를 추출하여 별도의 저장장치에 복제하거나 프린터로 출력하여 그 복제물 또는 출력물

죄의 증거물인 것이 명백하고 ③증거물의 발견이 우연한 것이어야 한다는 요건을 갖추고 있다면 영장없는 압수행위는 적법하다.

70) 이주원, 전게논문, 175면.

71) 강철하, 전게논문, 230면.

72) 강동욱, 전게논문, 185면.

을 압수하는 방법을 강구해야 할 것이다. 압수수색 대상의 컴퓨터에는 범죄와 관련없는 제3자의 전자기록이 포함되어 있을 수 있으므로 압수수색의 범위를 초과하지 않도록 유의하여야 한다.[73] 요구되는 보완입법의 내용으로는 원격지 압수수색제도, 협력의무제도, 정보분석 중 취득한 관련범죄 이외의 증거에 대한 긴급압수제도, 보존명령제도, 형사소송법 제106조의 압수대상에 정보를 직접 포함시키는 입법조치, 전자정보에 대한 전문법칙 규정의 명시화 등이 있다.[74] 디지털증거의 압수수색은 강제처분으로 개인의 프라이버시 및 권리의 침해를 수반하고 그 뒤에서는 과잉금지원칙, 비례성의 원칙 등을 넘어서는 안된다는 수사의 규제원리가 분명히 있고, 그 한계를 엄수해야한다고 본다. 이는 수사실무상의 편의만을 생각하여 각종 관련법규를 과잉해석을 금지한다는 점도 포함하고 있다. 그러나 이러한 기존 형사소송법의 해석상의 인정이 근본적인 해결방안은 아니라고 생각된다.[75]

압수수색은 기본권을 제한하는 강제처분이므로 강제처분법정주의와 영장주의의 적용을 받을 뿐만 아니라, 비례성원칙의 적용을 받음이 당연하다. 그럼에도 불구하고 대물적 강제처분인 압수수색은 대인적강제처분에 비하여 실무상 쉽게 영장이 발부되는 경향이 있었다. 특히 기업 등의 문서·컴퓨터에 대한 수사기관의 과도한 압수수색으로 수사목적에 필요한 범위를 넘어 기업활동이 위축되고 국민경제에 악영향을 미친다는 비판이 제기되기도 하였으며, 이메일 등 개인의 사생활과 직접 관련된 전기통신내용에 대하여도 빈번한 압수수색이 행해짐에 따라 그 규제의 필요성도 크게 대두되었다.[76] 사이버공간은 전파성이 강하여 불법유해정보가 게시되면 순식간에 전국적으로 확대되기 때문에 그 피해는 이루 말할 수 없이 커진다. 사이버공간이 이제 우리생활의 상당부분을 차지하는 오늘날 건전한 사이버문화를 조성하기 위해서는 규제를 강화해야 할 것이다. 특히 피해자의 심각한 정신적 공황을 가져오는 사이버범죄에 대해서는 새로운 입법을 통해서라도 이를 적극 규제함으로써 관련범죄의 발

73) 국방부과학수사연구소, 전게서, 242면.
74) 손동권, 전게논문, 344면.
75) 조석영, 전게논문, 95면.
76) 이주원, 전게논문, 196면,

생을 최소화할 필요가 있을 것이다.[77]

참고문헌

이재상, 「신형사소송법」, 2008.

김종세, "사이버범죄의 법적쟁점에 관한 고찰", 「경찰연구논집」 제2호, 2008.

김용현 · 황영구, "사이버공간에서의 범죄대응시스템 문제점과 대응방안에 관한 연구", 「한국치안행정논집」 제4권 제1호.

김상균, "사이버범죄에 대한 경찰의 수사력강화방안", 「법학연구」, 한국법학회, 2001.

김성룡, "이메일 압수수색에 관한 독일 연방헌법재판소 결정의 주요내용과 그 시사점", 「법학논고」, 2012, 2.

강동범, "사이버범죄와 형사법적대책", 「형사정책연구」 제42집, 2000.

강동범, "사이버범죄 처벌규정의 문제점과 대책", 「형사정책」 제19권 제2호, 2007.

강동욱, "디지털증거 수집에 관한 형사소송법 개정안에 대한 검토", 「법학연구」 제18권 제3호, 2010, 12.

강철하, "디지털증거압수수색에 관한 개선방안", 성균관대학교 법학전문대학원 법학과 박사학위논문, 2012.

권오걸, "사이버범죄와 대응전략, 법학연구", 「한국법학회」 제36집, 2009, 11.

국방부과학수사연구소, 「사이버범죄수사」, 2000.

경찰대학, 「사이범죄수사론」, 2011.

경찰수사연수원, 「2010 사이버범죄수사」, 2010.

경찰청 사이버테러 대응센터, 2012.

노명선, "사이버범죄의 증거확보에 관한 몇가지 입법적제안", 「성균관법학」 제19호 제2호, 2007, 8.

77) 정완, "사이버범죄의 실태와 동향 및 대응책", 「홍익법학」 제10권 제1호, 2009., 220면.

박광현, "사이버공간에서의 법익침해에 관한 형사법적 고찰", 숭실대학교「법학논총」제28집, 2012, 7.

박수희, "전자증거의 수집과 강제수사",「한국공안행정학회보」제29호, 2007.

박창욱, "사이버범죄에 대한 효율적인 경찰대응 방안에 관한 연구", 한국컴퓨터정보학회 제37차 동계학술발표논문집 제15권 제2호, 2007, 12.

손동권, "새로이 입법화된 디지털증거의 압수·수색제도에 관한 연구",「형사정책」, 제23권 제2호 2011, 12.

이경렬, "디지털정보 관련 압수수색규정 도입을 위한 전제적 고찰",「성균관법학」제21권 제2호, 2009, 8.

이정훈, "사이버범죄학의 동향과 전망",「경찰법연구」제9권 제2호, 2011.

이주원, "디지털증거에 대한 압수수색제도의 개선",「안암법학」제37권, 안암법학회, 2012.

이윤제, "디지털증거 압수·수색영장의 집행에 있어서의 협력의무",「형사법연구」제24권 제2호, 2012.

우제태, "사이버범죄의 대응방안에 관한 연구",「경찰연구논집」제1호, 2007.

허일태, "사이버범죄의 현황과 대책",「동아법학」제27호, 2000.

조석영, "디지털정보의 수사방법과 규제원칙",「형사정책」제22권 제1호, 2010, 7.

조호대, "사이버범죄에 대한 경찰 수사전문화 방안",「한국경찰학회보」제13권 제5호, 2011.

장윤식 · 김기범,「사이버범죄수사론」, 경찰대학, 2011.

정완, "사이버범죄의 현상",「형사정책」제19권 제2호, 2007.

정완, "사이버범죄의 실태와 동향 및 대응책",「홍익법학」제10권 제1호, 2009.

중앙경찰학교,「사이버수사」, 2010.

최영호, "정보범죄의 현황과 제도적 대처방안", 한국형사정책연구원, 1998.

탁희성, "전자증거에 관한 연구", 이화여자대학교대학원 박사학위논문, 2004.

탁희성, "전자증거의 압수수색에 관한 일고찰",「형사정책연구」제15권 제1호, 2004.

Computer Crime and Intellectual Property, Section Criminal Division United States Department of Justice.

United States v. O'Razvi, 1998 WL, 405048, at *6-7(S.D.N.Y. July 17, 1998); United States v. Flores, 122 F. Supp. 2d 491, 493-95(S.D.N.Y. 2000).

[Abstract]

A Study on search and seizure of digital evidence

Park, Bong-Jin
Ph.D in Law, Lecturer, Dept of police administration, Baekseok Univ.
Kim, Sang-Kyune
Ph.D in Law, Professor, Dept of police administration, Baekseok Univ.

Cybercrime is one of the terms used to denote the use of computer technology to engage in unlawful activity. Computer crime, high-tech crime and information-age crime. Most of the cybercrime we have seen so far is nothing more than the migration of real-world crimes into cyberspace

The other significant portion of cybercrime consists of specially defined cyber-offences-hacking, cracking and virus dissenmination-that are online version of real-world crimes. And Cybercrime are different to more conventinal crimes because of their mediation by computer technology. The mark of a true cybercrime is that it disappear once networked technology is removed characteristice of Informational.

We are living in the digital age. Lots of people in the world are using the Internet and so we are spending our lifetime in the Cyberspace through the Internet.

Digital evidence is difficult to treat, because digital information is easy to

forge, alter, delete and modify. So several digital evidence collection tools and forensic tools are developed. However there are many problem of composition which is whole due process from evidence collection to submitting to the court because existing digital evidence collection process and tools have a vulnerability of guaranteeing integrity.

Digital evidence of electronic evidence is probative information stored of transmitted in digital form. A party to a court case may use it at trial. Before accepting digital evidence, a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay-evidence, and whether a copy is acceptable or the original is required. Digital evidence tends to be easily eliminated modified and duplicated. Digital evidence is often attacked for its authenticity due to the ease with which it can be eliminated of modified. Digital evidence is often ruled inadmissble by court because it was obtained without authorization. The intangible information cannot be viewed in the eyes nor defined in any forms. Evidence may not remain at place where a criminal activity has occurred. It is therefore necessary to have the special knowledge and skills for efficient investigation.

In 2011, however, Korea Criminal Procedure was amended to include the duty to produce digital evidence. Nonetheless, the law enforcement demand to amend additionally the law to expand the scope of the duty to assist digital search warrant execution resulting in including duty to preserve digital evidence and duty to assist warrant execution. Some scholars and Judges have expressed different opinion over the additional revision.

Key words : Cybercrime, hacking, cracking and virus dissenmination, networked technology, Digital evidence, Korea Criminal Procedure