2022년 8월

박사학위 논문

역외 디지털 증거 압수·수색의 범위와 한계에 관한 연구

조선대학교 대학원

법 학 과

손 수 지

역외 디지털 증거 압수·수색의 범위와 한계에 관한 연구

A Study on the Scope and Limitations of Extra-territorial Search and Seizure for Digital Evidence

2022년 8월 26일

조선대학교 대학원

법 학 과

손 수 지

역외 디지털 증거 압수·수색의 범위와 한계에 관한 연구

지도교수 김 종 구

이 논문을 법학 박사학위 신청논문으로 제출함

2022년 4월

조선대학교 대학원

법 학 과

손 수 지

손수지의 박사학위논문을 인준함

위원장 남부대학교 교 수 정 병 곤 (인)

위 원 조선대학교 교 수 권 순 민 (인)

위 원 조선대학교 교 수 이 원 상 (인)

위 원 전남대학교 교 수 문 덕 민 (인)

위 원 조선대학교 교 수 김 종 구 (인)

2022년 6월

조선대학교 대학원

목 차

ABSTRACT

A Study on the Scope and Limitations of Extra-territorial Search and Seizure for Digital Evidence

Son, SuJi
Advisor : Prof. Kim Jong Goo, Ph.D.
Department of Law,
Graduate School of Chosun University

Today, with the very rapid development of information and communication technology(ICT), cyber crimes crossing over the countries are increasing, and collecting digital information from abroad is becoming more significant day by day. However, in the case of the extra-territorial seizure and search through the network connection, issues such as infringement of jurisdiction under international law, search and seizure procedures and breach of personal information related to digital data have been raised.

Therefore, in order to effectively secure the extra-territorial digital information, it is necessary to obtain cooperation from service providers through the criminal justice coordination process. However, the objective and neutral operation of digital evidence that guarantees the integrity of the evidence shall achieve the purpose of protecting the people's fundamental rights as stipulated in the Constitution and laws.

Digital forensic technology is advancing day by day to respond to crimes using various information and communication technologies. Due to the characteristics of the significance, diversity, and complexity of evidence analysis, new restrictions

are needed in addition to the existing principle of warrants. Therefore, it is necessary to strengthen the provisional control over the right to participate in addition to the court's pre-and post-control over the trial process through the 'Act on the Exclusion of Evidence from Illegal Collection.'

The dazzling advances in cloud computing create challenges for remote seizure and search. Although major foreign countries are addressing the issue legislatively, no explicit provision exists in the Criminal Procedure Act of Korea. Remote seizure and search are permitted in the interpretation of the Criminal Procedure Act of Korea. However, it is desirable to legally resolve the remote search and seizure regulations of the Criminal Procedure Act to protect the people's fundamental rights. Furthermore, it is necessary to actively consider joining the European Cyber-crime Convention and signing an administrative agreement with the United States.

For the search and seizure of e-mail that can be carried out in a place other than the place where the subject of the search and seizure exists without the intervention of the information storage server administrator, it is necessary to prepare legal regulations suitable for the characteristics or establish a separate regulatory system for digital evidence based on the current search and seizure regulations.

In addition, the protection of the digital evidence data subject's right to self-determination of personal information and the protection of the suspect's right to defend are key legal interests to be protected in extra-territorial digital information seizure and search procedures. We have no choice but to examine whether digital information is subject to seizure and search, whether it is possible to seize and search digital information through access means using information and communications networks, and whether it is appropriate according to legal interpretation in our criminal law. The Supreme Court also believes that it is legal only when an investigative agency uses digital information obtained legally to

access a server and that legislative measures are necessary as it does not allow any form of seizure and search.

The right to unconditionally participate in the search and seizure is guaranteed not only in the execution of the search and seizure, but also throughout the execution of the search and seizure warrant of the investigative agency, such as the seizure of storage media and video recording. It is necessary to specify the reasons for excluding the right to participate in cases of search, duplication, printing or destruction of evidence, leakage of investigation secrets, and obstruction of the investigation. It should be borne in mind that the principle of extra-territorial seizure, search, and just guarantee in the Internet and digital era is illegal if an investigative agency does not comply with even one procedure stipulated in the law in the course of a compulsory investigation, such as the execution of a warrant.

제1장 서 론

제1절 연구의 목적

오늘날의 현대사회 범죄들은 흔히 컴퓨터 및 스마트폰을 통해 이루어지고 있으며, 이러한 범죄들은 수사기관이 디지털 증거를 확보하여야만 수사가 가능하다. 디지털 데이터는 데이터자료가 해외에 있을 수도 있고 해당서버를 알 수 없는 경우도 있다. 따라서 국경을 초월한 인터넷 서비스의 사용이 확대되어 범죄와 관련 디지털 증거물에 대해 압수・수색의 필요성도 크다.

현재 일상생활에서 이용하고 있는 전자제품 모두에 저장이 되고 있는 데이터는 여기저기 분산이 되어 있지만, 사물인터넷(Internet of Things)을 통해 수집 또는 저장 되어 버린 데이터 이력은 오직 하나의 온전한 데이터로 결합되어 가치 있는 증거로써 사용할 수 있다. 증거는 사물인터넷에도 남아 있다. 인터넷을 이용해 활용해오던 전자제품기계는 PC, 휴대전화, 태블릿 PC 등의 IT 관련된 디바이스였지만, IoT의 시대에는 에어컨, 세탁기, 공기청정기, 로봇청소기 등의 가전제품에서부터 GPS 기능이 있는 모든 전자제품인 무선기기와 CCTV, 병원의 곳곳을 돌아다니며 공기살균을 해주는 공기청정기 로봇, 식당의 빈 그릇 치워주는 로봇에 이르기까지 제어하는 것이 모두 간단한 조작버튼 하나로 이루어진다. 사물인터넷 기술이 중첩된 가전제품이나 로봇에는 모두 원격조종을 통한 작동 데이터 및 센서 반응을 통한 작동 데이터 등의 이력이 남아 있게 되고, 이 정보들은 기기에 연결을 통해 모두 기록된다. 이처럼 사물인터넷의 편리함과 효율성에 반해, 이용자의 모든 사생활 이력이 증거자료로 남아 있다.

요즘에는 자신의 행적이 파악하기 쉬운 디지털 데이터가 많기 때문에, 자신의 행적과 관련된 모든 디지털 데이터를 찾는 것은 문제도 아니다. 이처럼 디지털 증거는 새로운 형태의 가치 있는 증거로써 수사기관의 입장에서는 핵심 증거가 되기 때문에 더 많은 문제가 된다. 특히 컴퓨터와 스마트폰 사용이 일상화되면서 문서파

일이나 e-메일, Facebook, Twitter, 인스타그램 등을 통해 서로 주고받았던 메시지 등 디지털 증거를 어떻게 추적할 것인지 복원 및 분석해 낼 수 있는가의 유무가 수사의 성패를 가르는 핵심 키포인트로 작용하고 있다. 현실적으로 해외 서버에 있는 디지털 증거를 확보하기 위해 많은 시간이 소요되어 신속하게 증거를 확보하기에는 많은 한계가 있다. 이러한 문제는 네트워크를 이용하여 해외 서버의 역외 압수·수색을 통해 제한적으로나마 해결할 수 있을 것이다.

그러나 역외 디지털 정보에 대한 압수·수색은 해외 서버를 직접 압수·수색하는 것이어서 국가관할에 대해서 문제를 야기할 수 있으므로, 기존의 압수·수색 절차방식대로 적용하기는 어렵다. 사법적 정의를 지키는 수사기관의 입장에서는 구시대 법률에 따라 새로운 형태의 증거물에 대한 수사 활동이 어려운 실정인 것이다. 특히 범죄와 네트워크의 초국가적 특성과 암호화 기술의 발달로 인해 역외 데이터에 대한 법 집행 기관의 접근 문제는 국경을 넘어 위치한 데이터에 대한 액세스 지연으로 인해 국가별 데이터 확보 노력의 실효성을 보장하기는 어렵다. 최근 디지털 데이터 수집의 맥락에서 적법성 및 집행 가능성에 의문이 있는 내용의 영장이 발부되고 있으며, 특히 집행방법의 기재가 문제되고 있다. 적법하게 발부된 영장의 집행방법 기재는 실제 압수·수색현장에서 사실상의 강제력을 가질 위험이 있고, 사후통제를 통해 이를 바로잡는 것은 결코 쉽지 않다. 따라서 이러한 위험을 제거하기 위해서도 영장의 효력을 다툴 절차를 인정할 필요가 있다.

이에 본 논문에서는 역외 압수·수색의 개념과 관련된 사례 및 그 특성을 확인하고 관련된 논의를 검토하면서, 역외 압수·수색이 해당국가의 주권침해를 적게 하면서도 목적을 향해 나아갈 수 있는 방안으로 국내 입법적 해결방안을 통한 제도화와 국제 협력의 필요성을 강조하고자 한다. 또한 역외 압수·수색에 적합한 집행과정의 공정성 확보방안과 참여인 제도를 통한 인권 보장도 살펴보고자 한다. 법원의 사전통제(영장심사)와 사후통제(공판절차)에 및 당사자 참여권(준항고)을 매개로 한 중간단계 통제를 강화할 필요성이 있기 때문이다. 이러한 공적 이익과 프라이버시(Privacy)의 보호를 조화할 수 있는 검토를 통하여 파악된 문제점 등을 바탕으로 개선방안을 모색해 볼 것이다.

제2절 연구의 범위와 방법

1. 연구의 범위

각종 정보통신기술을 이용하여 디지털 포렌식 기술들이 범죄에 대처하기 위해 나날이 발전하고 있지만 현재는 국내·외적 온라인 수색에 대해서 명시적으로 규정이 완비되어 있지 않다. 특히 역외 디지털 데이터의 압수·수색에 관해 실무에서 수권규정의 필요성이 대두되어 있으면서도 우리나라는 IT 강국으로써 자료가 국외에 있다는 이유로 수사가 힘들어지고 국외에 있는 서버 등에 대해 역외 압수·수색을 손쉽게 하여 사법정의를 실현이 가능한 장치가 마련되어야 할 것으로 보인다.

국제적 차원의 논의를 전제로 온라인 수색은 법관이 발부했던 영장에 의해 이뤄지고, 반드시 개인 프라이버시(Privacy) 또한 이헌 처분권한을 부여하는 법률에 보장되어야 한다. 디지털 데이터 수집의 맥락에서 적법성 및 집행 가능성에 의문이 없어야 적법절차의 실질적 내용을 보장할 수 있기 때문이다. 따라서 본 논문에서는 역외 디지털 데이터의 압수·수색의 범위와 한계를 살펴보며 그것이 우리 형사법 체계에 미치는 영향과 의미를 검토해 볼 것이다.

본 논문은 다음과 같이 6개의 장으로 구성하였다.

제1장 서론에서는 연구의 목적 및 범위와 방법에 대하여 기술하였다. 제2장에서는 디지털 증거의 일반적 고찰로서 디지털 증거의 의의과 특성 및 증거능력을 서술하고, 증거로 사용되기 위한 수집 절차의 적법성을 보장받는 디지털 증거의 증거능력의 요건과 확보방안을 살펴보았다. 그밖에 증거능력 확보를 위한 압수·수색의 실효적 방안을 찾아보며, 디지털 증거에 관련된 역외 압수·수색의 범위와 한계에 대해 모색해보았다. 제3장에서는 디지털 증거에 대한 역외 압수·수색의 개략적 특성을 확인하고, 유형과 문제점을 살펴보았고, 제4장에서는 본 논문의 연구대상인 역외 디지털 데이터의 압수·수색에 관한 미국과 유럽 등 해외 법제와 관련된 우

리나라의 주요 판례를 살펴보았다. 제5장에서는 역외 디지털 증거에 관련된 압수·수색의 적법성 확보방안에 대하여 역외 디지털 증거의 압수·수색의 특성과 허용성, 역외 디지털 증거의 압수·수색의 실효성과 영장주의 및 실효성 확보를 위한 영장주의 개선방안에 대해 살펴보았고 외국계 e-메일 계정에 대한 압수·수색의 문제와 현행법상 외국계 e-메일에 대한 압수·수색의 적법성 문제를 살펴보았다. 그리고 역외 디지털 증거 수집과 국제공조를 통해 국제형사규범의 발전을 위한 국제협력과 우리 형사법이론과 실무의 방향에 대해 논의하였다. 또한 역외 디지털 증거수집과 인권보장에서 디지털 증거수집과 정보인권보호, 참여권보장, 별건수사 금지와 관련하여 살펴보았다. 마지막으로 제6장에서는 본 논문의 결론으로 전체의 내용을 요약하여, 역외 디지털 데이터 압수·수색절차에서 역외서버에 대한 원격 압수·수색에 대한 입법적 해결과, 피압수자의 협력의무 규정, 유럽 사이버범죄협약 가입에 대한 고찰, 미국과의 행정협정체결 등을 강조하였다.

2. 연구의 방법

본 논문의 연구방법은 주로 문헌적인 연구를 통하여 학설 및 판례를 검토하는 방향에서 출발하였다. 범죄수사에서 형사재판에서 증거를 규율 중인 형사소송법이 디지털 증거에 대해 과연 적절한 해석을 할 수 있는지 자세히 살펴봐야 한다. 현행 형사소송법의 압수·수색 절차는 유체물 관점에서 제정되어 디지털 데이터의 특성이 유체물과 본질적으로 다르기 때문에 이를 디지털 환경에 맞추어 해석하는 것이 필요하다. 먼저, 국내·외 관련서적 및 논문 등을 조사하여 역외 디지털 데이터의 압수·수색에 대한 발전 연혁과 그 연구결과를 분석하였다. 이어서 인터넷 웹사이트와 관련 보고서도 조사하여 최근 논의되고 있는 문제에 대해 살펴보면서 그것이 우리 형사법에 미치는 영향과 의미를 검토하였고, 미국, 영국 등 외국의 입법례와 판례 및 국내의 판례를 검토하여 비교법적 방법 및 실제 사례를 중심으로 고찰하는 방법을 활용하였다.

제2장 디지털 증거와 디지털 증거 압수·수색 일반

제1절 디지털 증거 일반

1. 디지털 증거의 의의와 특성

가. 디지털 증거의 의의 및 개념

일반적으로 디지털 관련 증거 데이터가 법정에 제출되면서부터 '데이터'와 '정보'의 개념이 혼합적으로 사용되고 있는데 연구 및 조사 등의 바탕으로 되는 재료를 말하는데 자료를 잘 정리해보면 정보가 되므로 혼용되지 않도록 할 필요가 있다.[1] 전자적 방식, 자기적 방식, 일반 사람의 지각에 의해 그 존재 또는 상태를 인식할 수 없는 방식으로 작성된 디지털 신호의 집합체로서 컴퓨터에 의해 정보처리의 용도에 제공됨을 말한다.[2]

형사재판이 진행되려면 범죄에 대한 사실관계가 먼저 확정되어야만 공정한 절차로써 진행된다. 근래 사용되는 증거의 대부분은 디지털 저장매체에 저장된 또는 그 자체가 전송되는 '정보'[3] 즉, 이는 디지털 증거를 말하는 것이고, 많은 정보는 전자 데이터 형식으로 되어 있다. 이처럼 디지털 기기는 현대인들의 생활 속에 밀접하게 관여되어 개인에 대한 상당한 범위의 기록을 디지털 데이터로 남겨진다.

이처럼 디지털 증거는 그 작성주체와 성격 및 공소사실과의 관계 속에서 가지는 의미가 다양하기 때문에, '디지털'이라는 형식에 주목해서 이를 일률적으로 취급해선 안 될 것이다. 현대사회의 범죄, 특히 경제범죄 수사의 성패는 디지털 증거의

1) 이관희·이상진, 디지털 증거법, 박영사, 2022, 3면.
2) 이은모, 기본강의 형사소송법(제3판), 박영사, 2020, 375면.
3) 이순옥, "디지털 증거의 압수·수색절차에 관한 판례 연구", 중앙법학 제19집 제2호, 2017, 124면.

수집 여하에 많은 영향을 미친다 해도 지나치지 않다. 중요 사건 수사기록에는 전자문서, e-메일, 전자장부는 물론 로그기록, 스마트폰의 수·발신 내역 및 기지국 데이터, 금융거래내역 등 다양한 디지털 증거와 그 출력물들이 등장한다. 스마트폰에 저장된 데이터와 CCTV영상이 증거로 제출되는 방법도 급증했다.

오늘날 현대사회는 특히 컴퓨터나 서버 등 정보처리시스템이 없이는 모든 업무가 유지되기에는 역부족이다. 그렇기 때문에 압수·수색영장 발부 사유로 된 디지털 데이터가 저장된 저장매체는 범죄혐의와 연관되지 않은 기업경영에 대한 정보라던가 개개인의 일상생활 하나하나 많은 부분을 차지하고[4] 있어서 대부분 아주 큰 용량이 매우 크다.[5] 범죄혐의와 관련성 있는 정보와 관련 되지 않은 별건정보가 합쳐져 저장된 경우 과잉금지원칙을 견지하며 피압수자 등의 법익침해를 방지하기 위해서는 압수·수색절차 방법제한 또는 피압수자 등의 참여권 보장이 필요할 것이다.

디지털 증거는 전자정보만을 일컫는 것이 아니라 각종 정보저장매체, 통신매체, 디지털 매체를 모두 통틀어 일컫는 용어로 볼 수 있다. 디지털 증거에서 전제되는 개념은 '디지털'이라는 기술적 개념이며, 법에서는 친숙하지 않은 개념으로 '전자' 또는 '전자적', '컴퓨터 관련' 등으로 표현되기도 하며, 비교법적으로 독일[6]과 일본[7]에서 '전자적'이라는 용어를 쓰기도 한다. 하지만 많은 선행연구들은 '전자증거' 또는 '전자정보'[8]라는 용어보다 '디지털 증거'라는 용어를 즐겨 사용하므로 본 논문에서는 다른 문헌에서 다루는 전자증거, 전자적 증거, 컴퓨터

4) 대법원 2011모1839 전원합의체 판결, 다수의견; 장석준, "임의제출된 정보저장매체에 저장된 전자정보의 증거능력", 사법발전재단 제1권 제59호, 2022, 828면.
5) 이기리, "'유동적 위법' 개념을 통한 영장, 임의제출에 의한 디지털 증거의 압수·수색과 증거능력의 이해", 사법발전재단 제1권 제54호, 2020, 403면.
6) 독일 형사소송법 제 110조 3항: "수색 당사자에게 있어서 전자적 저장매체의 열람은 그것의 열람이 가능한 한 당사자와 공간적으로 떨어져 있는 저장매체에도 확대될 수 있지만,....."
7) 일본 형사소송법 제219조 제2항: "원격지 압수·수색을 위해 영장청구서에는 디지털 데이터의 범위에 대한 내용을 기재해야 하며, 이를 위해 원격지 서버의 서비스 종류(메일 서버, 파일 서버 등), 접속을 위한 ID 등을 기재해야 하는데, 다만 수사의 진전 상황에 따라 어느 정도의 개괄적 기재는 허용된다.; 일본형사소송법에서 전자적이라는 용어를 사용한다."
8) 대법원 2017. 11. 29. 선고 2017도9747 판결에서는 e-메일에 대하여 '전자정보'로 명칭하고 있다.

관련하여 가리키는 바를 ‘디지털 데이터’ 또는 ‘디지털 증거’라 통칭하기로 한다.

디지털 증거(digital evidence)는 디지털 데이터가 디지털 형태로 저장되거나 전송되는 와중에 증거로서의 가치 있는 정보,[9] 디지털형태로 저장 또는 전송되는 증거가치가 있는 정보[10]로서, “컴퓨터 또는 기타 디지털 저장매체에 저장되거나 네트워크를 통해 전송 중인 자료로서 법정에서 신뢰할 수 있는 저장되거나 전송되는 이진수 형태의 정보(IOCE)”[11]나, “범죄와 피해자 및 범죄와 가해자 사이를 연결하는 모든 디지털 데이터”,[12] 또는 “각종 디지털 저장매체에 저장되거나 네트워크 장비 또는 유·무선 통신상으로 전송되는 정보로서 그 신뢰성이 보장되어 증거가치를 가지는 것”을 의미하고 있다.[13]

법령의 검찰청예규 제991호 디지털 증거의 수집·분석 및 관리규정[14] 제3조 제1호에서 “디지털 증거란 범죄와 관련하여 디지털 형태로 저장되거나 전송되는 증거로서의 가치가 있는 정보”라고 정의하고 있고, 경찰청 훈령 제845호 디지털 증거의 수집 및 처리 등에 관한 규칙[15] 제2조 제3호에서 “디지털 증거란 형사소송법 제106조 및 제215조 ~ 제218조까지의 규정에 따라 압수한 디지털 데이터“라고 정의하고 있다.[16]

---

9) 이원상, “디지털 증거의 증거능력, -관련성과 전문증거에 대한 최근 판례 견해를 기반으로-”, 국민대학교 법학연구소 주최 학술회의 발표논문, 2016, 608면.
10) 손지영·김주석, “디지털 증거의 증거능력 판단에 관한 연구”, 대법원 사법정책 연구원 연구보고서, 2015, 24면.
11) International Organisation on Computer Evidence: 미국, 호주, 홍콩, 영국 등 여러 국가의 실무자들 중심으로 만들어진 디지털 증거에 관한 국제기구.; 손지영·김주석, 앞의 보고서, 21면.
12) 박석훈, “제3자 보관 디지털 증거에 대한 원격지 압수·수색 체계에 관한 연구”, 고려대학교 박사학위논문, 2016, 17면.
13) 전현욱·윤지영, “디지털 증거 확보를 위한 수사상 온라인 수색제도 도입 방안에 대한 연구”, 한국형사정책연구원 연구보고서, 2012, 6면.
14) 디지털 증거의 수집·분석 및 관리 규정<개정 대검예규 제1151호, 2021. 1. 1. 시행 및 일부개정> 참조.
15) 경찰청은 훈령을 제정하여 2015년부터 시행하고 있으나 디지털 저장매체에 대한 압수·수색과 사후처리절차와 관련된 규정이 세부적으로 되어있지 않아 아직은 미비한 실정이다.
16) 이주호·김호, 판례로 본 디지털 증거법, 북랩, 2020, 14면.

나. 디지털 증거의 특성

디지털 데이터의 특성들의 대부분이 디지털 증거의 증거능력에 영향을 미친다. 특히 디지털 데이터의 원본성・진정성・무결성・신뢰성 등은 증거능력에 절대적인 영향을 미치므로 디지털 데이터의 증거능력의 유・무를 판단함에는 선결요건이 되기 때문에 이러한 특성을 고려하지 않을 수 없다. 디지털 데이터의 일반적 특성으로서는 분리가능성[17], 수집・보관・분석의 용이성[18] 외에, 구체적으로 매체독립성, 비가시성, 비가독성, 사본 및 원본 구별의 난이성, 대량성, 취약성, 네트워크의 관련성, 전문성 등을 들 수 있다.[19]

(1) 매체독립성 및 원본과 사본 구분의 곤란성

디지털 값에는 아날로그 신호가 가지는 미세한 차이가 없으므로, 이진수로 구성된 디지털 데이터는 어떤 매체에도 동일하게 복제가 가능하고 수회에 걸쳐서 복제를 하더라도 데이터의 질이 떨어지는 경우가 없다.[20] 즉, 원본과 사본의 데이터 값의 가치가 같다. 그래서 디지털 증거는 매체와 정보의 분리가 어려운 기존의 증거들과 다르게 매체와 분리되었던 데이터 자체에 대한 압수 및 수색이 가능하게 되었고, 대량의 데이터라도 매체를 옮겨서 수집, 보관, 분석하는 것이 매우 쉽다. 이러한 특성을 '매체독립성'이라고 하는데 디지털 데이터의 매체독립성[21]에서는 예외로 정보저장매체 전체압수를 허용한다.[22]

---

17) 이기리, 앞의 논문, 389면.
18) 디지털 데이터는 수집이 용이하여 저장되어 있던 매체에 대해서 접근이 가능하면, 아무리 수많은 정보라도 소수인원으로 매우 간단한 장비를 이용해 복사하면 된다. 또한 아주 큰 용량의 많은 정보도 휴대 가능한 USB나 하드디스크 저장장비에 보관이 가능하고, 이를 수사기관의 아주 큰 용량 저장장치에 복사하게 되면 또 다른 저장매체가 전혀 필요치 않다.; 이기리, 앞의 논문, 390면.
19) 이순옥, "디지털 증거의 역외 압수・수색 -대법원 2017. 11. 29. 선고 2017도9747 판결을 중심으로-", 중앙법학 제20집 제1호, 2018, 125면.
20) 이관희・이상진, 앞의 책, 68면.
21) 형사소송법 제106조 제3항 참조.
22) 한성훈, "디지털 증거의 압수・수색의 합리화 방안에 관한 연구", 홍익법학 제16권 제3호,

또한 유체물인 저장매체와 구분이 가능한 무체물로써 매체독립성을 지니고, 디지털 증거는 값만 동일하면 반복된 복사과정에서도 질이 떨어지는 일이 없어 원본의 변경 없이도 그대로 복사가 가능하며 원본과 사본의 구별이 어렵다.[23]

(2) 비가시성, 비가독성

디지털 데이터는 전자매체에 이진수로 기록이 되어 있기 때문에 육안으로 식별이 어려운 0과 1이 합체된 디지털 형태로 무형의 정보이다.[24] 육안으로 식별하는 것이 어렵기 때문에 선별과정에서 무관정보까지 함께 가져오게 될 가능성이 높아진 것도 있다.[25] 그 자체 상태로는 사람의 식별이 불가능하므로 바로 인식할 수 없어, 법정에 현출하기 위해서는 반드시 일정한 판독절차를 거쳐 많은 시간과 노력이 필요하다.[26] 다시 말해, 디지털 데이터는 프린터를 통한 인쇄된 상태 또는 모니터 화면으로 출력되어야 비로소 가시성과 가독성을 갖게 되는 것[27]이다.

이처럼 디지털 데이터를 증거로 사용되려면 일정한 판독절차를 거쳐야 되고, 디코딩(Decoding) 및 암호 복호(Decrypt) 또는 압축 해제(Decompress)의 과정이 필요하다. 이러한 판독절차에 전문가들이 개입하는 경우와 적절한 변환 및 출력장치, 소프트웨어를 통과하게 되는데 이로 인한 논란의 소지가 발생할 수도 있다.[28] 이처럼 디지털 데이터의를 확보하는 과정에서 기술적이고 논리적인 방법들이 동원되며, 이런 측면은 디지털 증거의 증거능력 검토 과정을 통해 포렌식 도구의 신뢰성이나 분석관의 전문성 검증과 연결될 것이다.

2015, 348면.
23) 손지영・김주석, 앞의 보고서, 26면.
24) 이관희・이상진, 앞의 책, 67면.
25) 최윤정, “전자정보 압수・수색에 적용되는 영장주의 원칙과 그 예외에 관한 법적 검토”, 저스티스 통권 제153호, 2016, 113면.
26) 이관희・이상진, 앞의 책, 68면.
27) 정성남, “경찰 수사현장에서 디지털 증거의 압수・수색에 관한 연구 -스마트 폰을 중심으로-”, 인천대학교 박사학위논문, 2020, 21면.
28) 정성남, 앞의 논문, 21면.

(3) 변조의 용이성 및 취약성

수사기관은 디지털 증거를 수집하여 공판정에 증거로 제출할 때까지 이 디지털 증거가 위조·변조되지 않았다는 것을 증명할 수 있는 절차 및 기술, 이른바 '무결성을 확보하기 위한 절차와 기술'이 필요하다. 이러한 무결성 확보를 위한 최소한의 요건으로 관리연속성(Chain of custody)을 강조하여 ① 고유의 증거 식별자, ② 증거에 접근한 인물, 그리고 접근한 시간과 장소, ③ 증거 보존 시설 안으로 증거를 가지고 들어오거나 가지고 나간 인물 및 발생 시간, ④ 증거를 가지고 나간 이유, ⑤ 적절한 권한이 있었는지 여부를 들 수 있다.[29]

디지털 데이터가 전자적 방식으로 저장매체에 저장되어 있는 경우 쉽게 노출되거나 충격 등으로 인해 쉽게 손상 내지 변조 가능성에 노출되어 있다.[30] 만약 조작되었다면 누군가에 의해 조작되었는지 판별이 불가능하고 컴퓨터 작업이 끝나거나 전원이 갑자기 차단되면 정보가 날아가 버리는 불상사가 나타나기도 한다.

한편, 디지털 증거의 복제가 쉬운 용이성 등으로 인해서 압수·수색에 있어 혐의와 연관 되지 않은 개인정보들이 무작위로 수집이 가능한 위험성과[31] 개인의 정보침해 위험성이 커서 압수·수색 절차에서 참여권을 충실하게 보장하여 관련 데이터 저장매체 및 디지털 증거의 특수성을 고려하고 절차적 적법성을 확보하여 조치가 취해져야 할 것이다. 이를 위해, 압수·수색 영장 사본 교부 도입, 피압수자의 참여권 강화, 압수목록 교부제도 강화 등을 통해서 디지털 증거 압수·수색에 대해 절차적 규제를 강화해야 될 것이다.

이처럼 디지털 데이터는 변조의 용이성으로 간단한 명령 및 조작만으로도 아주 큰 용량자료 등 모든 정보 전체까지도 삭제·변경 등이 간단한 명령어 입력으로도 컴퓨터 하드디스크에 기록되어있던 정보를 변경할 수 있거나 온도, 습도 등 주변의 환경에도 쉽게 영향을 받을 수 있다.[32] 때문에 피압수자의 증거인멸 가능성도 높

29) 노명선, "전자적 증거의 수집과 증거능력에 관한 몇 가지 검토", 형사법의 신동향 통권 제16호, 대검찰청, 2008, 78면.
30) 이관희·이상진, 앞의 책, 67~68면.
31) 조광훈, "디지털 증거의 압수·수색의 문제점과 개선방안", 서울법학 제21권 제3호, 2014, 704면.

아[33] 수사기관은 이를 방지하기 위한 신속한 증거보전절차를 마련하여야 한다.

(4) 저장정보의 대량성

디지털 증거는 개인이 사용 하고 있는 컴퓨터에서 기업의 전산회계자료에 이르기까지 여러 종류의 응용프로그램에 의하여 생성된 수천수백만개 자료가 저장된 경우가 대부분이다. 최근 저장기술의 발달로 수많은 정보가 정보저장매체에 저장되고 정보통신망을 통해 대량으로 유통되고 있다.[34]

아주 작은 usb같은 정보저장매체에 저장된 디지털 정보는 어마어마한 아주 큰 용량인 경우가 대부분이고, 광범위한 분량의 정보까지도 저장가능하며, 저장매체를 압수함에 있어 범죄혐의와 관련된 정보뿐만 아니라 기업의 영업비밀이나 개인의 사생활과 같이 범죄혐의와 관련이 없는 내용도 함께 저장되어 있다는 특색이 있다. 무엇보다 디지털 데이터에 대한 압수・수색에 있어서는 그 대상자의 기본권이 침해되지 않도록 다른 강제처분보다 더욱 신중을 기하여야 할 필요가 있는 것이다.[35]

특히 여러 사람들이 공동으로 사용하는 서버 중 하나의 저장매체나 시스템에 범죄와 관련이 없는 많은 사람들의 개인정보가 저장 및 전송되는 경우가 통상적인 현상이므로, 범죄와 관련된 정보를 탐색하는 과정에서 개인의 사생활이 연관된, 범죄와는 관련이 없는 별건정보를 수사기관이 취득할 가능성이 제기되고 있고, 이러한 특성으로 인해 압수・수색의 범위, 방법 등을 제한할 필요가 있다.[36] 이러한 디지털 데이터의 방대한 양과 관련하여 디지털 데이터의 압수・수색을 위한 영장의 신청에 있어서는 영장의 내용이 과연 어떤 정도로 특정되어야 하는지, 영장의 집행범위가 어디까지[37] 허용될지가 중요한 문제이다.

---

32) 이인곤, “형사절차상 디지털 증거 압수・수색에 대한 문제점과 개선방안”, 한국경찰연구 제15권 제4호, 2016, 182면.
33) 손지영・김주석, 앞의 보고서, 73면.
34) 박민우, “디지털 증거 압수・수색에서의 적법절차”, 고려대학교 박사학위논문, 2016, 14면.
35) 이창현, 형사소송법(제6판), 정독, 2020, 445면.
36) 박병민・서용성, “디지털 증거 압수・수색 개선방안에 관한 연구 -법률개정에 관한 논의를 중심으로-”, 사법정책연구원 보고서, 2021, 17면.
37) 김범식, “경찰현장수사에서 디지털 증거에 대한 압수・수색의 개선방안”, 외법논집 제38권

(5) 전문성

디지털 데이터를 수집·분석하기 위해서는 특수한 방법과 전문적 기술이 필요한데 이를 '전문성'이라고 한다.[38] 변조의 용이성·취약성 등에 따라 증거의 무결성을 확보하기 위한 전문적이고 특수한 증거수집·보관·이송 등의 방법이 요구되는 것이다.

디지털 데이터를 분석할 경우에는 삭제되어버린 데이터 복구나 아주 큰 용량 데이터 중에서 범죄혐의를 입증할 때 필요한 정보만을 찾아내는 검색기술 등의 전문적인 기술이 필요한데[39], 디지털 증거의 수집과 분석을 위해 디지털 포렌식 센터, 경찰청의 사이버테러대응센터, 국가정보원의 국가사이버안전센터와 같이 전문적인 조직이 설치된 것도 이 때문이다. 따라서 만약 위법하게 증거를 취급하다가 증거가 훼손이라도 된다면 무결성이 보장되지 않아 증거로 절대 사용할 수 없게 되는 경우도 있다.[40]

(6) 네트워크 관련성

정보통신망의 고도화로 인한 관련 데이터의 저장 및 전송 등 그 유통환경의 발전은 이미 네트워크를 통해서 물리적 장소의 개념을 초월하고 있는 실정이다. 따라서 제대로 된 가치 있는 디지털 데이터를 수집하려면 네트워크를 통한 시스템 자원의 접근을 해야 하는 경우도 발생하는데, 이러한 특성을 '네트워크 관련성'이라 칭한다.[41] 네트워크는 일상생활의 수단이자 범죄의 수단이 되기도 한다. 따라서 디지털 증거를 수집하려면 네트워크를 통해야 하므로, 웹하드 및 파일공유 네트워크 또는 클라우드 서비스 등으로 네트워크상에 대량의 정보가 저장, 공유되기도 한

제4호, 2014, 172면.
38) 박민우, 앞의 논문, 14면.
39) 김범식, 앞의 논문, 172면.
40) 이인곤, 앞의 논문, 182면.
41) 김범식, 앞의 논문, 172면.

다.[42]

법집행기관 입장에서는 시스템에 대한 접근 권한을 획득하는 방법으로 원격으로 증거를 수집할 수 있는데, 다만 이 경우에는 원격 접속 데이터 다운로드 방식이 영장 집행 방법으로써 유효한 것인지, 시스템이 해외에 있어 과연 우리형사소송법 적용이 가능한 지에 대한 논란은 아직도 많다.[43]

2. 디지털 증거의 증거능력

가. 디지털 증거의 증거능력 요건

(1) 의의

디지털 증거의 증거능력은 컴퓨터용 디스크 등 정보저장매체에 저장된 내용이 음성이나 영상을 녹음 또는 녹화한 파일인지 또는 문자정보를 기록한 파일인지의 유무에 따라 그 판단이 달라진다.[44] 또한 피의자의 범죄혐의를 입증하는 증거로 사용되기도 하지만 피의자의 혐의가 없음을 밝혀주는 증거로 사용되기도 한다. 인간의 모든 생활에서 컴퓨터가 보편적으로 사용되고 있는 현실에서 각종 범죄가 컴퓨터와 밀접한 관련이 있고 인간의 행동을 기억매체인 디지털 데이터에 낱낱이 기억되어 굳이 형사사법 절차가 아니더라도 디지털 데이터는 일상생활에서도 그 중요한 역할을 담당하고 있다.

수사기관이 압수・수색영장의 집행으로 확보한 디지털 데이터를 증거로 사용하기 위해서는 증거능력이 있어야 한다. 정보기술의 발달로 인하여 형사법정에서 다양한 형태의 디지털 증거가 제출되고 있는 사례가 증가하며, 이에 따라서 디지털 증거의 증거능력 인정 여부가 문제되고 있다. 위법수집증거 배제법칙, 전문법칙 등

42) 강미영, “디지털 증거의 증거능력”, 외법논집 제43권 제3호, 2019, 153면.
43) 이관희・이상진, 앞의 책, 70면.
44) 이은모, 앞의 책, 375면.

종래의 증거능력에 관한 규정을 디지털 증거에 적용함에 있어서 그 특성을 어느 정도 고려할 것인지도 문제이며, 디지털 증거의 특성에 착안해 다른 증거와 다르게 특유한 증거능력 요건을 인정할 수 있을 것인지도 문제이다.[45]

일반 증거와 관련된 증거법의 원칙들은 주로 유체물인 증거, 사람에 의한 진술증거 등을 상정하고 있다. 그런데 디지털 증거는 그 고유한 특성 때문에 다른 증거들과 달리 형사소송상 의미 있는 증거로 사용하기 위해 해결되어야 할 문제들이 발생하고, 이러한 문제가 해결되지 않으면 디지털 증거는 증거능력으로 인정받을 수 없게 된다.[46] 이렇듯 디지털 증거는 유체물인 증거물과는 다르게 매체독립성, 취약성, 전문성 등의 특성으로 증거능력이 인정되는 선결요건으로 강조된다.

(2) 증거능력 요건

(가) 원본성

디지털 증거는 그 자체로는 가시성이 없으므로 가시성 있는 인쇄물로 출력하여 법원에 제출할 수밖에 없다. 아주 큰 용량 시스템에서 증거를 수집할 때에는 원 매체에 있는 증거를 다른 저장 매체에 복사하게 된다. 이러한 이유로 실제 법정에 제출되는 증거는 원본 증거와는 다른 형태를 취하게 되는 경우가 많으므로, 증거원본이 제출되어야 하는 증거법상의 원칙상 제출되는 사본 증거, 그리고 가시성 있는 상태로 증거가 변환되었는데 원본으로써 인정할 수 있는가의 유무는 법적으로 문제가 있을 수 있다. 즉 디지털 증거는 일반적 증거와는 달리 유체물이 아닌 정보이므로 매체독립적이고 원본과 사본을 구별하기 힘들어 원칙적으로 원본에 의한 입증을 요구한 데에 따라 그 원본성 문제가 논의되는 것이다.

디지털 증거는 원본에 대한 복제가 토시하나 틀리지 않게 가능해서 특별한 사정이 없으면 원본과 사본이 정확하게 일치하고, 그 출력물도 원본과 다를 바가 없

45) 손지영・김주석, 앞의 보고서, 11면.
46) 장상귀, “디지털 증거의 증거능력에 관한 연구”, 법학교수・검찰 실무연구회 발표자료집(Ⅰ), 대검찰청, 2009, 233면.

다.[47] 우리나라의 경우 2007년 개정 형사소송규칙 제134조의7에서 컴퓨터용 디스크 등에 기억된 문자정보 등에 대한 증거조사 방법에 관한 규정을 신설하여 디지털 증거의 제출방법에 대해 읽을 수 있도록 출력하여 제출하도록 하는 등의 조치로, 기존에 종종 문제되었던 저장매체에서 출력된 문건의 원본성 문제가 입법적으로 해결되는 듯하였다.[48]

이러한 원본성과 관련하여 대법원은, 원본의 성립의 진정 및 원본의 존재에 관하여 다툼이 있고 사본을 원본의 대용으로 하는데 대해 상대로부터 이의가 있을 때에는 사본으로 원본을 대신할 수는 없고, 반면에 사본을 원본으로서 제출하는 경우에는 그 사본이 독립한 서증이 되는 것이지만 그 대신 이에 의해 원본이 제출된 것으로 되는 것은 아니고, 이때는 증거에 의하여 사본과 같은 원본이 존재하고 또 그 원본이 진정하게 성립하였음이 인정되지 않는다면 그와 같은 내용의 사본이 존재한다는 것 이상의 증거가치는 없다고 하였다.[49]

(나) 진정성

증거의 진정성 증명이란 디지털 증거의 원본성 및 성립의 진정을 증명해 주는 법적 요건으로서, 무결성과 뒤섞여서 쓰이고 있으며, 일부 견해에 따라서는 무결성에 진정성이 포함되는 개념으로 보기도 한다.[50] 디지털 증거의 경우에는 주장하려는 반대로 해당 증거가 특정된 사람이 특정된 시점에 생성하고 난 후 특정시점에 특정인에게 전송된 것이 맞는 지를 증명한다.

진정성과 무결성에 대하여, 진정성은 특정한 사람의 행위결과가 정확하게 표현되고 그로 인한 생성된 자료임이 인정되어야 한다는 것이고, 동일성 또는 무결성은 최초 증거가 생성되었을 때 법정제출이 되기까지의 변경 및 훼손이 전혀 없었다는

47) 박혁수, “개정 형사소송법상 디지털 증거의 증거능력 -관련성, 신뢰성, 진정성, 원본성을 중심으로-”, 해외연수검사 연구논문집 제25집, 2010, 77면.
48) 정웅석, “개정법상 진술서 등의 증거능력에 관한 고찰”, 저스티스 통권 제158권 제3호, 2017, 832면.
49) 대법원 2002. 8. 23. 선고 2000다66133 판결.
50) 무결성에 진정성을 포함시켜 설명하고 있는 예로, 독고지은, “디지털 증거 압수·수색에 대한 개정 형사소송법의 규제와 집행에 관한 연구”, 고려대학교 박사학위논문, 2013, 32면.

것을 의미[51]한다. 현재 검찰에서도 대검찰청과 각 고등검찰청 및 지방검찰청에 교육훈련 등 별도의 기구로 적합한 자격을 갖춘 디지털 포렌식 수사관으로 구성된 전담 팀을 구성하여 수사 일선현장에서 그들의 지원을 받아 압수·수색 및 분석 또는 현출, 법정증언, 기술적 자문 등 디지털 증거의 수집 및 분석과 연관된 수사 및 공소유지 업무의 여러 과정에 압수한 디지털 증거의 수집과 보존만을 다루고 있는 실정이다.[52]

그럼에도 불구하고, 진정성과 무결성은 디지털 데이터의 수집과 보존을 포함해 분석하는 등의 여러 과정에 걸쳐진 문제로 보는 견해가 있다.[53] 즉, 디지털 증거의 진정성은 특정인에 의해서 해당 파일이 특정시간에 생성한 사실이 맞는지 증거가 되는 파일이 여부이며, 해당 증거파일의 진정성이 인정된 그 파일이 수집 및 분석 과정에서 변경되었는지 여부를 판단하는 것은 무결성의 문제이다.

일반적으로 디지털 증거는 데이터의 대량성과 삭제·변경의 용이성이 있고 누구나 복제·복사가 가능하기 때문에 디지털 증거를 분석·보존할 때는 그 훼손이나 조작가능성을 방지하여야 할 필요성이 제기된다. 따라서 디지털 증거가 증거 수집 이후 보관단계에서 위조 및 다른 파일로 바꿔질 염려가 있어 디지털 증거 수집 단계부터 법원으로 제출 단계까지 연계보관 로그(Log)를 기록해야 한다.

(다) 무결성

디지털 증거의 무결성이란, 원본의 디지털 증거가 수집되고 나서 보관 또는 분석하는 과정에서 훼손·수정·변경·손상 등이 없게끔 유지[54]되어야 하며, 이러한 수정·변경·손상이 발생하지 않았음을 검증이 가능하다 한다는 것을 말한다. 즉, 디지털 데이터의 특성상 위·변조가 용이하고 의도하지 않게 변경될 가능성이 발생하므로, 수집한 증거가 변경되지 않았다는 것을 담보하는 것이 무결성의 원칙이다.

51) 정웅석, 앞의 논문, 838~839면.
52) 정웅석, 앞의 논문, 839면.
53) 정웅석, 앞의 논문, 839면.
54) 장응혁, “디지털 증거의 압수·수색에 있어서 전문가 참여의 법적 성격 검토”, 디지털 포렌식연구 제15권 제1호, 2021, 118면.

디지털 증거는 변개의 용이성 내지 취약성으로 최초의 증거가 저장된 매체에서 법정에 제출되는 동안 변경이나 훼손이 없었다는 것이 입증되어야 하는데 과연 어떻게 무결하게 확보하는가의 문제는 디지털 증거능력의 유지측면에서 관련된 파일의 선별만큼 중요하다.[55] 사실 디지털 증거자료에 대한 처리 및 법정제출 과정에서 많은 사람들의 손을 거쳐 갈 수 있는데 이 경우 그 각각의 행위마다 원본이 훼손되지 않고 유지되고 있다는 절차적 보증이 요구된다.[56] 디지털 데이터 원본을 압수할 때부터 관련 문건을 출력할 때까지 변경되지 않았다는 사실을 무결성이라고 의미하고 무결성은 관리 연속성으로 의미하는 것으로 이해된다.[57]

무결성 문제는 디지털 증거 영역에서 처음 제기되었는바, 여기에서의 무결성이란 디지털 데이터가 오직 관련된 사람들에게만 개방되어서 그들에 의해서만 수정될 수 있다는 것을 보장하는 것이다.[58] 즉, 허가된 자한테만 정보를 개방하여 수집된 디지털 데이터의 원본으로부터 보관・분석 과정에서 부당하게 수정・변경・손상이 생겨 1비트라도 변화가 되었고 결과적으로 해쉬값이 변경되었다면 무결성이 훼손되었다고 볼 수 있다.[59] 디지털 포렌식 분야에서는 수학적 해쉬 함수를 이용하여 원본과 분석된 복사본의 결과 값이 동일함을 증명한다. 수집 당시 하드디스크의 해쉬 값과 법정제출 당시 하드디스크의 해쉬 값이 같다면 해쉬 함수의 특성에 따라 무결성이 입증되는 것이다.

디지털 증거의 무결성 보장조치는 디지털 증거가 수사기관이 제3자에 의해서 위조되어 법정에 제출되는 경우에 검증과정에서 위조 사실의 적발이 가능할 수 있어야 하며, 디지털 증거가 실제로는 위조되지 않았어도 용의자 및 피고소인이 디지털 증거가 위조되었을 경우를 대비해 증거능력을 무력화시키려 시도하는 경우에도 모조건 디지털 증거의 신뢰성을 입증할 수 있어야 할 것이다. 디지털 포렌식 과정에서도 당연히 자료의 무결성을 입증할 수 있는 기술적인 방법들이 사용되어야 한다.[60]

---

55) 정웅석, 앞의 논문, 835면.
56) 정웅석, 앞의 논문, 835면.
57) 서울고등법원 2007. 8. 16. 선고 2007노929 판결.; 이관희・이상진, 앞의 책, 129~130면.
58) 장응혁, 앞의 논문, 118면.
59) 정웅석, 앞의 논문, 836면.

(라) 신뢰성

디지털 증거는 변조가 쉽고 의도적 또는 비의도적이던 일단 조작에는 취약하기 때문에 신뢰성이 보장되어야 할 것이다.[61] 여기서 신뢰성이란 증거 데이터의 분석 등 처리 과정에서 디지털 증거가 위·변조되거나 의도되지 않았던 오류를 포함하지 않았다는 것을 말한다. 분석 도구의 신뢰성 확보를 위해 신뢰성이 검증된 분석 장비와 소프트웨어를 사용하고 공개된 알고리즘을 사용하여[62] 증거가치를 확보해야 한다. 디지털 포렌식의 과정에서는 필연적으로 소프트웨어와 장비들을 사용하게 되는데 이러한 장비와 소프트웨어에 대한 신뢰성이 검증되지 않는다면, 그 결과물을 보증할 수 없는 것은 당연하다.

신뢰성이 인정되기 위해서는 절차적으로 '보관의 연속성'이 보장되어야 하며, 이를 위해선 디지털 포렌식 전문가의 신뢰성은 물론 디지털 포렌식 도구 및 방법의 신뢰성이 필요하다.[63] 디지털 증거의 신뢰성은 디지털 증거 자체의 특성이 아닌 디지털 증거를 취급하는 인력 및 도구, 분석실, 절차 등과 같은 주관적·객관적인 요소들의 신뢰성 증명을 통해서 간접적으로 증명된다.

(마) 판례의 입장 및 검토

디지털 데이터 저장매체로부터 출력한 문건의 증거능력에 대하여, 대법원은 소위 '일심회 사건'[64]에서 디지털 데이터 저장매체인 압수물로부터 출력한 문건을 증거로써 인정받기 위해서는 원본에 저장되어 있던 내용과 출력했던 문건이 동일한 것인지 인정되려면 디지털 데이터 저장매체 원본이 압수시점부터 문건 출력시점까지 변경되지 않아야한다고 하였다. 특히 디지털 관련 데이터가 저장된 원본

60) 정웅석, 앞의 논문, 836면.
61) 정웅석, 앞의 논문, 836면.
62) 현재 우리나라의 수사기관은 통합 포렌식 프로그램으로 미국의 신뢰성이 입증된 인케이스(EnCase)를 사용하고 있는 것으로 보여진다.; 손지영·김주석, 앞의 보고서, 33면.
63) 정웅석, 앞의 논문, 839면.
64) 대법원 2007. 12. 13. 선고 2007도7257 판결.

대신 저장매체에 저장되어 있던 데이터를 ‘이미징’ 또는 ‘하드카피’한 매체로부터 출력한 문건을 디지털 원본인 저장매체와 ‘이미징’ 또는 ‘하드카피’한 매체 사이에 자료의 동일성 인정이 요구된다. 물론, 이를 확인하는 차원에서 사용한 컴퓨터의 기계적 정확함과 신뢰성, 입력 및 처리 또는 출력의 각각의 단계에서 전문적인 감식기술능력과 정확성이 담보되어야 할 것이라 하였다. 또한 디지털 저장매체로부터 압수했던 출력한 문건을 진술증거로 사용할 때, 그 기재된 내용이 진실한 가에 대해서는 전문법칙이 적용되기 때문에 형사소송법 제313조 제1항에 따라 그 작성자 또는 진술자의 진술에 의해 그 성립의 진정성이 증명된 경우에 한해 이를 증거로 사용할 수 있다고 하여 디지털 증거로부터의 출력물에 대하여 작성자의 진술로 성립의 진정성이 인정되지 않을 경우 증거능력을 부정하였다.[65]

또한 대법원은 소위 ‘왕재산 사건’[66]에서도 디지털 증거의 경우 피압수자가 해쉬값이 동일하다는 취지의 서면을 교부하지 않더라도 압수절차에 참여한 수사관 등의 증언 등에 의하여 원본과의 동일성 및 무결성을 입증할 수 있도록 요건을 완화하였다. 압수된 저장매체를 복제하여 해쉬값을 생성하고 봉인을 한 후 증거를 찾기 위해 해당 파일을 열어 재탐색을 하는 경우 해쉬값 변동으로 동일성 상실의 문제가 발생하기 때문에 실무에서는 저장매체의 파일을 이미징 또는 복제한 후 대검찰청 서버에 그대로 업로드하고, 감사 및 수사관은 위 서버에 저장된 파일을 컴퓨터에 다운로드 받은 다음 범죄사실과 관련이 있는 증거를 찾는 방식을 사용하게 된 것이다.[67]

이렇듯 대법원은 데이터저장매체의 원본과 ‘하드카피’, ‘이미징’한 매체 사이에 데이터의 동일성과 함께, 이를 확인하는 과정에서 이용한 컴퓨터 기계의 정확성, 프로그램 신뢰성, 입력 및 처리 또는 출력의 각 단계마다 조작하는 사람의 전문적인 기술력과 정확성에 대해서 디지털 증거의 동일성·무결성을 인정하기 위해서는 철저히 담보되어야 한다고 판시했다. 또한, 변조되거나 삭제가 쉬운 취약성

65) 김윤섭·박상용, “형사증거법상 디지털 증거의 증거능력 -증거능력의 선결요건 및 전문법칙의 예외요건을 중심으로-”, 형사정책연구 제26권 제2호, 2015, 202면.
66) 대법원 2013. 7. 26. 선고 2013도2511 판결.
67) 이순옥, 앞의 논문, 126면.

때문에 검사가 출력된 문건과 디지털 데이터 저장매체의 원본에 저장되어 있던 내용 사이의 동일성을 증명해내야 하지만 동일성은 엄연히 소송법적 사실에 불과하기 때문에 엄격한 증명이 아닌 자유로운 증명에 의하도록 하고 있다.

그러나 실무상 법원에서는 증거의 동일성 증명에 대해 엄격하게 심사하며, 현행 형소법 제313조를 엄격히 해석해 작성자의 구두 진술에 의해서 진술서의 증거능력을 인정하던 종래의 입장을 재확인하고 있다. 제315조의 적용가능성을 배제하고 있다.[68]

판례가 '일심회 사건'과 '왕재산 사건'에서 제시하는 요인을 중심으로 디지털 데이터의 증거능력을 평가함에 있어 결국 디지털 데이터를 출력한 문서에 증거능력을 부여하기 위해서는 원본과 출력물 사이에 '동일성(identity)' + '무결성(integrity)' + '신뢰성(reliability)'이 유지되어야 하고 전문법칙의 예외를 규정한 형사소송법 제311조 이하의 각각의 요건을 갖추어야 할 것이다.

나. 디지털 증거의 증거능력 확보방안

(1) 형사 증거법의 기본원칙 준수

디지털 증거가 증거능력을 인정받기 위해서는 압수·수색에서부터 증거로 제출할 때까지의 적법절차가 철저히 준수되고 형사법에도 저촉되지 않아야 한다. 디지털 증거가 출현하기 전에는 우리 형사사법은 조서 재판에 치중한 나머지 전문법칙에 관심이 많았고 물적 증거에 대해서는 위법하게 수집한 경우에도 성질형상불변론에 입각하여 증거능력을 넉넉하게 인정해 주는 태도를 취했었다.[69]

기존 방식의 증거능력은 자칫 위법수집증거배제법칙의 논란에 휩싸이고 심지어는 민사상 불법행위를 부담 할 위험도 고스란히 질 수도 있다. 이렇게 형사사법절차에서 수사기관이 어렵게 확보한 디지털 데이터가 피의자에 대한 혐의를 인정하

68) <http://news.koreanbar.or.kr> 노명선, [판례평석] 디지털 증거의 증거능력(가칭 '일심회 사건'); 법조신문 (2022. 06. 30. 검색)
69) 이관희·이상진, 앞의 책, 111면.

거나 혐의 없음을 밝혀주는 증거로 외형상으로는 완벽한 증거의 형태를 갖추고 있을지라도 디지털 데이터를 획득하는 압수·수색절차에서 적법절차를 준수하지 않았다면 증거능력을 인정받지 못하게 된다. 어렵게 확보한 디지털 데이터가 증거로 사용할 수 없다면 압수·수색은 모두 수포로 돌아가고 오히려 비난만 자초하기 쉽다. 이러한 점에서 디지털 데이터의 증거능력을 검토하는 것이야말로 형사증거법에서 차지하는 비중이 결코 적지 않고, 디지털 데이터의 증거능력을 둘러싼 각 쟁점들에 대한 적절하고 조화로운 해석론이 절실히 요구된다고 할 것이다.

(2) 디지털 포렌식을 통한 범죄 과학 수사

범죄와 관련되어 있는 디지털 데이터가 디지털 형태로 전송 또는 저장되는 증거로서 가치 있는 증거로 인정받으려면 '기본적으로 원본이 변경되거나 손상 없는 상태로 디지털 데이터를 수집 및 삭제한 디지털 증거를 복구했을 경우에 원래 압수되었던 증거랑 같은 것이다.' 라고 증명할 수 있어야 되는데, 이러한 과정을 보장하기 위해서 이용할 수 있는 것이 바로 디지털 포렌식(Digital Forensics)[70]이다.

디지털 포렌식에 관해서 아는 사람들은 거의 없다. 디지털 포렌식을 알기 위해서는 많은 교육 및 컴퓨터 공학 또는 법학적 지식을 습득해야 한다. 죄의 유무를 가리는 법관의 경우 법에 관해 전문가일 수는 있지만 디지털 데이터 혹은 그 수집절차에 대해 잘 알지 못하는 경우가 많을 수 있다. 또한 컴퓨터 공학이란 것이 상당히 전문적인 분야이기 때문에 일반 사람들이 직관적으로 이해하기에 어려울 수 있다. 때문에 전문가가 법정에 나와 청중 혹은 관련자가 이해하기 쉽게 설명해주는 과정이 병행되어야 할 필요성이 있다.

디지털 포렌식은 디지털 기기에 적용하는 법의학 혹은 컴퓨터나 노트북, 스마트폰 등 각종 저장 매체 또는 네트워크상에 남아 있는 각종 디지털 데이터를 분석해서 범죄 단서를 찾아 내는 수사 기법을 말한다.[71] 기술의 발전으로 대부분 모든 사

70) 디지털 포렌식이란 용어는 1991년 미국 Portland에서 열린 'International Association of Colloid and Interface Scientists' (IACIS)에서 처음 사용되었다.; 최재민·신대민·이상진·임종인, "물리적 복구방법을 활용한 디지털 포렌식 기술", 한국방송공학회, 2007, 146면.

람들의 삶이 디지털화 되어 사이버장소에서 일어나는 범죄들 뿐만 아니라 일반 범죄에 대한 단서도 생활에서 쓰이는 모든 전자기기들을 통해서 찾아낼 수 있는 경우가 많아지면서 디지털 포렌식 기술이 요구되는 일이 늘어나고 있다.[72] 디지털 범죄가 급증하면서 검찰의 수사에서 디지털 포렌식은 선택이 아닌 필수가 되었다.

진정성이나 신뢰성을 얻으려면 체계적인 디지털 포렌식 수사절차가 확립되어야 될 것이고 해당 기술교육을 통해 지속적인 발전이 필요하다.[73] 그리고 디지털 증거의 중요성이 큰 만큼 우리형사소송법 영역에서 디지털 증거능력에 대한 요건과 입법이 독립해서 체계적으로 정비되어야 할 것이다.[74] 현재 디지털 증거 관련해서 국가디지털포렌식센터에서 범죄수사에 잘 활용되고 있지만, 압수・수색 및 검증까지 모두 한 장소에서 이루어지고 있으므로, 검증을 할 때에는 검증만을 전문으로 해줄 수 있는 전문기관이 검증하는 것이[75] 옳을 것이다.

각종 증거를 과학적으로 분석해 범죄사실을 규명하는 분야를 법과학(forensic science)라고 하는데 이는 범죄수사과정에서 뿐만 아니라, 법정에서 응용과학 또는 법정과학이라고도 말하며, 수사방법 개선을 위해 과학적으로 행하는 모든 수사 및 과학적 방법을 이용하는 수사는 과학수사라고 한다.[76] 과학수사라는 것은 이론이 말해주듯 합리적으로 사물의 추이를 풀어내기 위해 범죄 현장에서 수립되는 증거물이 항상 적정한 것이어야 할 것을 요구한다.[77] 법적 수사에서 재판에 도움이 되는 과학적 증거를 수집 및 분석 또는 보존하는 과정을 말하는데 이것은 “범죄 과학 수사의“라는 의미로써 법정에서 증거에 대한 진위여부를 가리기 위해 증거물을 과학적으로 조사하고 정보를 찾아내기 위한 과정 혹은 작업 정도라 생각할 수 있

71) 디지털 포렌식이란 범죄에 사용되거나 범죄현장에 남아있는 디지털 기기에서 범죄자 혹은 범죄에 대한 단서 및 증거를 수집 전자증거물 등을 사법기관에 제출하기 위해 데이터를 수집・분석・보고서를 작성하는 작업을 말한다.; 정병곤, “디지털 증거의 수집과 증거능력에 관한 연구”, 조선대학교 박사학위논문, 2012, 19면.
72) 강미영, 앞의 논문, 154면.
73) 강미영, 앞의 논문, 155면.
74) 강미영, 앞의 논문, 149면.
75) 강미영, 앞의 논문, 166면.
76) 윤신규, “수사 단계에서 확보한 법과학 증거의 요건과 질적 수준”, 한국과학수사학회지 제16권 제1호, 2022, 44면.
77) 정해상, 과학수사와 범죄, 일진사, 2020, 100면.

다.

포렌식 분야는 무궁무진하기 때문에 디지털 포렌식 기술이 과거에 컴퓨터와 인터넷 환경에만 제한되었지만 현재는 이미 클라우드 컴퓨팅과 모바일 SNS 환경까지 확대되었고, 조만간 데이터기술이 융합된 사물인터넷과 핀테크 환경까지 확대될 것으로 보인다.

(3) 디지털 증거 추적의 적법성 확보

범죄와 관련된 디지털 증거를 수집하려고 할 때 유의해야 할 점이 몇 개 있다. 그것은 디지털 증거의 특징을 이해하고 디지털 증거가 법정에서 증거능력을 인정받기 위해서 어떠한 절차를 거쳐야 하는가이다. 위·변조 등이 용이해서 증거훼손이 쉬운 디지털 증거를 법정에서 용의자의 범죄를 증명하기 위해서는 수사기관이 수집한 증거가 위·변조되지 않고 원본과 동일한 상태인지 판사에게 증명할 필요가 있다. 만약 이를 증명하는 절차 없이 증거로 사용 할 수 있다면 제3자 혹은 수사기관에 의해 증거가 변조되어 유·무죄 판별에 영향을 끼칠 수 있기 때문이다. 또한 정식 수색 기관의 모든 증거가 그러하겠지만 디지털 증거는 적법한 절차에 따라 수집되어야 할 필요성이 있다. 권한이 없는 사람 또는 권한이 없는 기관이 수집한 증거에 대해서는 절대 증거능력을 인정받지 못한다.

최근 디지털 증거에 관한 압수·수색 과정에서 가장 큰 쟁점이 되고 있는 것은 당사자의 참여권 보장 범위와 관련된 문제다. 특히 소셜 미디어를 통해 주고 받은 메시지나 포털사이트에 게재된 글 등에 대한 증거확보작업이 빈번해지면서 서버 압수·수색 과정에서 피의자 등의 참여권 보장 문제가 자주 논란이 되고 있다. 압수·수색 현장에 피의자를 참여시킬 수 없다 하더라도 수사기관이 해당 디지털 증거를 확보한 후 이를 정리하는 과정에서는 피압수·수색자를 참여시켜야 당사자의 참여권을 보장하는 일반적인 디지털 포렌식 원칙에 부합한다고 생각된다. 저장매체에 있는 디지털 증거를 압수·수색 장소에서 복제하고 추후 이를 재복제하는 과정까지 당사자를 참여시켜야 할 것이다.

그러나 대법원[78]은 수사기관이 데이터저장매체에 기억된 정보 중에 키워드 및

확장자 등을 통해 협의사실과 관련된 정보를 검색하여 선별하고 나서 비트열 방식으로 복제한 이미지파일을 제출받아 데이터 저장매체와 동일하게 압수했다고 한다면 이로써는 압수물에 대해서는 압수·수색 절차는 종료되어 마무리 된 것이므로 수사기관이 수사기관 사무실에서 압수되었던 이미지 파일을 탐색 및 복제 또는 출력하는 과정에서도 피의자 등에게 참여기회를 보장해야 되는 것은 아니라고 하였으며, 대법원은 이 사건에서 전원합의체 결정을 통해 디지털 데이터의 압수·수색 방법과 합법성의 기준을 처음으로 제시하였다.

즉, 압수·수색은 수사기관이 디지털 데이터에 대해서 원칙적으로 영장 발부 사유로 된 범죄혐의 관련 있는 부분만 문서 출력물로 수집 또는 복제를 수사기관이 휴대한 저장매체에 하는 방식으로 엄격한 기준을 세웠다. 다만 압수·수색 할 컴퓨터 등 데이터저장매체를 직접 반출하거나 거기에 들어있던 저장매체의 파일 전체를 이미징 또는 하드카피 등의 형태인 복제본으로 압수·수색하는 경우 압수·수색 영장 혐의 사실과 연관된 데이터만 추출하기에는 시간이나 기술적으로 제약이 많기 때문에 예외적인 경우에만 허용된다는 것이다.

무엇보다 수사기관은 압수·수색한 저장매체에서 영장 혐의와 상관없는 별도의 범죄혐의와 관련된 디지털 데이터를 발견하더라도 피압수자 측에 적정한 참여권 등을 보장하지 않으면 적법하게 그 내용을 압수할 수 없고, 압수한 디지털 데이터를 수사기관으로 가져와 복제하고 재복제하는 등 순차적인 압수·수색 과정에서 한 차례라도 정보소유자의 참여권을 보장하지 않았다면 해당 압수·수색 전체가 위법하므로 이 과정에서 획득한 증거는 증거능력이 부인된다고 했다.

그러나 이처럼 판결에만 의존해서는 디지털 증거 추적 등의 적법성 문제를 해결할 수 없다는 지적이 많다. 디지털 증거의 특성이 반영된 종합적이고 체계적인 법률체계가 구축돼야 한다는 것이다. 현행 형사소송법은 정보가 압수 대상인지에 대해서조차 규정돼 있지 않아 이 같은 기본적인 부분부터 명문화하는 작업이 필요하다. 원거리 압수·수색 등 디지털 시대에 맞게 도입돼야 할 제도들도 많고, 민사관계에서도 증거법칙이 필요하므로 민·형사를 불문하고 증거법의 새로운 체계를 만

78) 대법원 2018. 2. 8. 선고 2017도13263 판결.

들 필요가 있다. 임시방편적 제도가 아닌 기본 구조와 골격부터 체계적으로 새로 만들어야 할 필요가 있다.

제2절 디지털 증거 압수·수색 일반

1. 디지털 증거에 대한 압수·수색의 의의와 특성

가. 압수·수색의 개념 및 요건

(1) 압수·수색의 개념

물건의 점유를 취득하는 강제처분이 압수이고, 압수할 물건이나 체포할 피의자·피고인을 발견할 목적으로 사람의 신체, 물건 또한 주거 기타의 장소를 뒤져서 찾는 강제처분을 수색이라 하는데,[79] 압수와는 영장발부에 있어 불가분의 편의성을 띄는 경우가 잦기에 편의상 하나의 영장으로 발부되는 경우가 다수이지 완전히 다른 처분이다. 수색은 주로 압수를 위하여 행하여지며 실무상으로는 양자를 합친 압수·수색영장이라는 단일 영장이 보통 사용되고 있다.[80]

압수에는 압류, 영치, 제출명령의 3가지의 유형[81]이 있는 반면, 압류는 강제력을 사용하여 유체물의 점유를 점유자 또는 소유자의 의사에 반하여 수사기관 또는 법원에 이전하는 강제처분이고, 영치는 소유자 등이 임의로 제출한 물건이나 유류한 물건을 계속하여 점유하는 것이다. 제출명령에 의해 물건이 제출되었을 경우 압수의 효력이 발생하지만 이에 응하지 않았다면 압류가 가능하므로 제출명령도 압수의 일종으로 본다는 견해가 있다.[82]

---

79) 이주원, 형사소송법, 박영사, 2019, 140면.
80) 이주원, 앞의 책, 140면.
81) 이은모, 앞의 책, 152면.
82) 이은모·김정환, 형사소송법(제7판), 박영사, 2019, 307면.

한편, 압수・수색의 용어에 대해 재검토 할 필요가 있다. 수색의 압수에 선행되기 때문에 미국에서는 search and seizure 라고 표현을 하는데 우리는 압수수색이라는 용어를 사용함으로써 압수에 방점을 두고 수색이 가지는 문제점에 대한 생각은 뒷전인데 디지털 데이터에 대한 압수수색이 일상화 되면서 수색이 가지는 문제점에 대해 생각해 봐야 한다.[83]

(2) 압수・수색의 요건

일반적으로 압수・수색이 허용되고 적법하기 위해서는 피의자에게 범죄혐의가 있어야 하며, 압수・수색이 범죄의 수사에 필요하여야 하며, 압수・수색할 대상이 해당 사건과 관련이 있어야 하며, 압수・수색영장의 집행에 있어 비례성의 원칙[84]이 요구된다.[85]

압수・수색영장이 발부되려면 범죄의 혐의가 소명되어야 하는데, 범죄소명의 개연성에서 구속은 '구체적' 개연성을 요하지만 압수는 '낮은' 수준의 개연성으로 족하다. 다만 혐의에 대해서는 구체적 입증을 요한다. 압수와 수색은 별개의 수사 활동이지만, 대개의 경우 수색은 압수를 하기 위해 하게 되므로 병행되는 것이 보통이다. 물론 압수・수색은 강제수사 방법이므로 영장주의의 원칙에 따라 법원의 압수・수색 영장을 얻어서 행하여진다.

따라서 제출명령을 제외하고는 압수・수색에 있어 반드시 사전에 영장이 필요하다. 단, 예외적으로 체포 현장, 현행 범인의 범죄 장소, 그리고 긴급 체포 시에 피체포자가 소유・소지・보관하는 물건에 대하여는 영장 없이 압수・수색할 수 있고, 현행 범인의 체포를 위하여 필요한 경우에는 수색 영장 없이 타인의 주거를 수색할 수 있다. 또 수사 기관은 피의자나 다른 사람이 범죄 현장에 남긴 물건이나 이들이 영장 없이 임의로 제출했던 물건에 대해서 압수가 가능하다.[86] 이를 '임의

83) 이관희, 범죄수사입문, 박영사, 2021, 242~243면.
84) 비례성의 원칙이란 강제처분의 필요성 및 상당성과 기본권 보장 사이에 적정한 비례가 유지되어야 한다는 것으로 협의로는 과잉금지의 원칙이라고 한다.
85) 이관희, 앞의 책, 243면.
86) 형사소송법 제218조 참조.

제출물 압수’라고 하는데, 실무상 대부분이 이런 방식에 의하여 물건이 압수되고 있다.

역외로 수집한 데이터 관련 집행 관할권 행사의 허용범위를 국제법적으로 명확하게 할 필요가 있는데 특히 형사소송법 제215조 압수・수색 규정은 바로 범죄혐의의 정황 존재, 해당사건과의 관련성, 범죄수사의 필요성 및 비례성을 들고 있다.[87]

첫째, ‘범죄혐의에 대한 소명’이 있어야 한다. 형사소송법에서는 ‘범죄수사에 필요한 때’라는 어절을 통해 이를 말하고 있다.[88] 압수・수색은 신체의 구속에 비해 기본권 침해가 덜하다는 이유로 압수・수색을 위한 범죄 혐의의 정도는 구속에 비하여 완화되어 최초의 혹은 단순한 혐의로 족하다고 볼 수 있다.

둘째, ‘필요성의 원칙’이란 압수・수색은 ‘범죄수사에 필요한 때’에 할 수 있다는 것으로 수사를 위해서 필요할 뿐 아니라 강제처분으로 압수를 안하면 수사의 목적을 달성하지 못할 때를 말한다.[89] 이는 범죄의 태양, 경중, 압수물의 증거로서의 가치, 압수물의 은닉, 인멸, 훼손될 위험, 수사나 공판수행상의 지장 유무, 압수에 의하여 받는 피압수자 등의 여러 사정을 검토하여 종합적으로 판단하여야 할 것이다.[90]

셋째, ‘관련성의 원칙’이란 사건과 관련성이 인정되는 것에 한하여 압수・수색을 할 수 있다는 것[91]이다. 이 원칙은 과잉 압수・수색과 프라이버시(Privacy) 침해 등을 방지하기 위한 증거수집의 허용범위를 정하고 있다는데 그 의의가 있다. ‘증거의 관련성 원칙’이란 영미 증거법에 따라 증거능력을 인정받기 기본 요건을 말한다. 일반영장을 금지하는 영장주의 원칙상 대상이 특정되지 않은 영장의 압수・수색에 의해 수집된 증거는 위법수집증거로서 증거능력이 부정되므로, 압수・수색의 허용범위를 결정할 때는 범죄행위와의 ‘관련성’이 있어야 한다.[92] 즉, 사법부

87) 정성남, 앞의 논문, 27면.
88) 형사소송법 제215조 제1항과 제2항 참조.
89) 이주원, 앞의 책, 142면,
90) 신동운, 간추린 신형사소송법(14판), 법문사, 2022. 416면.
91) 형사소송법 제106조 제1항 참조.
92) 박석훈, “전자증거의 압수・수색 및 임의제출 과정에서의 데이터 범위 한정가능성”, 법조 제64권 제6호, 2015, 42면.

는 위법성 판단의 핵심요소로서의 ‘관련성 원칙’을 활용하고 있다. ‘관련성 원칙’은 실질적인 영장주의의 구현을 위한 것으로 압수·수색 집행의 범위를 한정하여 수사기관의 탐색적 수색, 일반 수색을 막기 위한 핵심적인 원칙으로 기능한다. 압수·수색의 관련성은 그 정도의 측면에서도 집행 현장의 상황에 비추어 피의사실과의 관련성이 확실한 때에 한정되지 않고 관련 개연성이 있는 정도면 충분하다.

넷째, ‘비례성의 원칙’은 압수·수색은 수사의 목적을 달성하기 위한 ‘필요한 최소한의 범위’ 안에서 하여야 한다는 것으로[93], 비록 수색의 필요성과 관련성이 충족되더라도 목적과 수단의 적정한 비례성의 요건이 추가로 필요하다는 것이다. 이러한 비례성은 범죄의 형태나 경중, 압수물에 대한 증거가치 및 그 중요성, 증거인멸의 유무, 압수로 인해 피압수자가 받는 불이익 등의 총체적으로 여러사정을 고려해 판단하여야 한다.[94] 즉, 기본권 침해의 정도와 혐의의 중대성 및 수사상 필요성을 비교형량 하여 그 허용여부 및 허용범위를 결정하여야 한다는 것을 의미하는 것이다.

나. 디지털 증거에 대한 압수·수색의 의의

디지털 증거는 그 작성주체와 성격, 공소사실과의 관계에서 가지는 의의가 다양하며, 현대사회는 범죄, 특히 경제범죄 수사의 성패는 디지털 증거의 수집 여하에 달려있다 하여도 지나치지 않는다. 중요 사건의 수사기록에는 전자문서, e-메일, 전자장부는 물론 ROG기록, 스마트폰의 수신·발신내역 또는 기지국 정보, 금융거래내역 등 각종 다양한 디지털 증거와 그 출력물들이 등장하며, 스마트폰에 저장되어 있던 정보들과 CCTV영상들이 법정증거로 제출되는 경우가 많아졌다. 요즘엔 컴퓨터나 서버 등 정보처리관련 시스템 없이는 유지되기 어렵다.[95] 또한 디지털 데이터가 저장된 저장매체 역시 대부분 아주 큰 용량이라 압수·수색의 영장 발부의 이

93) 형사소송법 제199조 제1항 참조.
94) 김현수, “적법한 압수·수색의 요건에 관한 고찰”, 인권과 정의 통권 제490호, 2020, 12면.
95) 이기리, 앞의 논문, 403면.

유가 되었다면 개인정보 및 기업관련 데이터가 어마어마하게 포함되어[96] 있게 마련이다.

그만큼 현재 우리나라의 형사소송법 분야에서 가장 활발하게 논의되는 주제의 하나가 디지털 증거의 압수·수색이라 할 것이다. 이후 이러한 상황을 반영하여 중요한 판례가 계속해서 나오고 있고, 실무 현장에서는 다양한 대응이 이루어지고 있다.[97] 그러한 대응의 대표적인 사례로 수사기관은 디지털 증거의 압수·수색에 전문가를 참여시키고 있다.

다. 디지털 증거에 대한 압수·수색의 특성

현대사회의 디지털화로 인해 범죄의 환경이 변화했고 이로 인해서 압수·수색을 통하여 디지털 범죄 관련 증거의 확보는 통상적인 수사기법의 하나가 되었을 뿐만 아니라 수사의 성패를 좌지우지하는 중요한 역할을 수행하고 있다. 디지털 증거의 압수·수색과 증거분석은 디지털 범죄수사에서 핵심절차에 속한다. 디지털 증거에 대한 압수·수색은 통상의 압수·수색과는 달리 독특한 특성으로 압수·수색과 증거분석에 전문성이 요구된다.

형사소송법 제106조(압수) 제3항은 디지털 데이터의 압수·수색과 관련하여 명문으로 규정하고 있지만 압수·수색 대상물 특정과 그 범위가 모호해서 이로 인해 야기되는 문제점들을 해결하지는 못하고 있다.[98] 매체 자체를 압수하는 것이 원칙이 아닌 그 안에 있는 관련데이터의 범위만을 출력 · 복제하는 것을 원칙으로 규정하였음에도 압수를 통해 개인정보 침해를 최소화되기는 어려워 보인다. 수사기관은 데이터저장매체의 압수를 원칙으로 하여 수사의 효율성을 높이려 하는 경향이다.[99]

디지털 증거에 관련된 압수·수색의 가장 큰 문제는 압수·수색 대상물의 특정 및 그 범위의 모호성으로 인해 광범위한 과잉 압수·수색이 이루어지고 이 때문에

96) 장석준, 앞의 논문, 822면.
97) 장응혁, 앞의 논문, 115면.
98) 이인곤, 앞의 논문, 177~178면.
99) 이인곤, 앞의 논문, 177면.

개인 프라이버시(Privacy)가 과도하게 침해될 수 있다.[100] 따라서 디지털 증거에 대한 압수·수색을 개선하려면 수사기관의 디지털 데이터의 압수·수색에 대해 올바르게 이해하고 압수·수색 절차에서 비례성·상당성을 준수하며, 증거의 무결성을 유지하기 위해서 많은 노력을 해야 한다.[101]

디지털 증거 압수·수색에서 수사기관은 비례성 및 상당성을 준수함, 법치국가의 원리와 적법절차의 이념과 동시에 선별적인 압수·수색으로 문제점을 극복해 나가야 한다. 무엇보다 디지털(digital) 증거의 수집과 연관되는 제도적인 보완책도 필요하다.[102]

압수·수색영장의 범죄사실과 연관되지 않은 데이터가 수집된 경우 수사기관이 이것을 그대로 놔두거나 반환하지 않고, 반환을 하더라도 사본은 남겨 놓는 방법으로 다른 범죄 수사할 때의 단서로 사용하며, 또 다른 법익침해를 가져올 가능성이 크다. 예를 들어, 갑의 A범죄 수사를 위해 대량의 디지털 데이터를 압수·수색하였는데, 그 중 A범죄사실과는 관련 되지 않은 디지털 데이터가 수년 후 을의 B범죄의 증거가 되는 경우, 또는 위 디지털 데이터를 바탕으로 갑의 B범죄에 관련하여 증거가 확보가 가능한 경우이다.

이처럼 수집된 B범죄에 관한 증거에 대해서는 새로운 압수·수색영장을 발부받아서 다시 압수하지 않는 한 위법한 증거로서 증거능력이 없다. 하지만 A범죄의 수사를 위해 압수·수색에서 확보되었던 데이터를 바탕으로 B범죄에 대해 압수·수색영장을 청구하여서 발부된 영장으로 B범죄의 증거를 입수한 경우 해당 증거는 증거능력의 유무는 용이하게 판단하기엔 문제가 있다.

2. 디지털 증거에 대한 압수·수색의 대상 및 장소

가. 압수·수색의 대상 및 장소

100) 이인곤, 앞의 논문, 199면.
101) 이인곤, 앞의 논문, 177면.
102) 이인곤, 앞의 논문, 177~178면.

일반영장의 폐해를 방지하기 위해 압수·수색 영장에 압수할 물건과 수색할 장소 등을 적도록 규정하고 있는 것은 그 입법취지가 있으므로, 압수할 물건은 구체적, 개별적으로 표시하고, 수색할 장소는 지역적으로 특정지어야 할 것이다. 형사소송법은 압수·수색 영장에 '수색할 장소'를 기재하도록 규정(제219조, 제114조)하고 있는바, 법원에서는 영장기재 장소에 관하여 압수·수색 장소의 내부구조를 사전에 명확히 알 수는 없는 경우에는, "통상적으로 보아 압수·수색 영장에 기재된 장소와 동일성이 인정되는 범위 내에서는 영장기재 장소"라고 판시하고 있다.[103] 이는 압수·수색할 장소는 특정되어야 하며 그 장소와 동일성이 인정되지 않는 장소에 대해서는 압수·수색이 허용되지 않는다는 것이다.

현행 형사소송법은 체포·구속 목적의 피의자 수색(제216조 제1항 제1호), 체포현장에서의 압수·수색(제216조 제1항 제2호), 범죄 장소에서의 긴급 압수·수색(제216조 제3항), 긴급체포 시의 압수·수색(제217조 제1항), 유류물 또는 임의제출물의 영치(제218조, 제108조) 등 영장주의의 예외를 인정하고 있다. 그러나 긴급 압수·수색 할 경우라도 압수·수색의 장소는 체포·구속 현장, 범죄 장소에 국한되어야 한다. 또한 제216조 제1항 제1호, 제218조의 경우를 제외하고는 모두 지체 없이 사후영장을 받아야 하므로, 사전영장주의의 예외라고 볼 수 있다. 하지만 디지털 데이터에 대한 압수·수색에 있어서는 그 대상자의 기본권이 침해되지 않도록 다른 강제처분보다 더욱 신중을 기하여야 할 필요가 있다.

나. 디지털 증거에 대한 압수·수색의 대상

수사기관의 디지털 데이터에 대해 압수·수색은 영장 발부의 근거로 된 범죄혐의사실과 연관된 부분만 수사기관이 간편·용이한 휴대용 저장매체에 해당 문서출력물로 수집하거나 파일을 복제하는 방식으로 이뤄져야하는 것이 원칙이다.[104] 직

103) 광주고법 2008. 1. 15, 선고, 2007노370 판결.
104) 이주원, 앞의 책, 154~155면.

접 데이터 저장매체 자체를 반출하거나 데이터저장매체에 있는 데이터 전부를 하드카피[105]나 이미징 등 형태로 외부로 반출하여 압수·수색하는 것은[106] 디지털 데이터의 대량성으로 관련된 정보를 획득하는데 긴 시간이 걸리거나 전문 인력에 의해 기술적 조치가 필요할 때 범위를 정해 출력·복제하는 방법이 불가능해서 현저히 곤란하다 인정되는 때에 한하여 예외적으로 허용된다.[107]

디지털 증거에 있어서 압수·수색의 대상에 대하여 형사소송법 제106조 제3항은 마치 '정보저장매체'가 압수·수색의 대상이라는 것임을 명시한 것으로 보이나, 동조 제4항에서는 제3항에 의거하여 데이터를 제공받았을 경우의 통지를 해야 한다고 의무를 규정하였고, 압수·수색하는 방법으로는 출력이나 복제에 의하도록 원칙을 정하고 있다. 이처럼 제106조 제3항 전단에도 불구하고 압수·수색의 대상은 '디지털 증거'라는 해석이 된다.

다. 디지털 증거에 대한 압수·수색의 장소

(1) 원격지에 저장된 정보에 대한 압수·수색

피의자의 e-메일 계정에 대해 접근권한에 갈음하여 발부받은 압수·수색 영장에 따라 원격지의 데이터 매체에 적법하게 접속하여 내려받거나 현출된 디지털 데이터를 대상으로 하여 범죄 혐의 사실과 관련된 부분에 대하여 압수·수색하는 것은 대물적 강제처분 행위로서 허용되며 압수·수색영장의 집행에 필요한 처분에 해당된다.[108]

압수대상인 디지털 데이터는 압수·수색을 개시할 때부터 압수·수색이 종료되기 전까지 수색장소에 확보되면 족하므로 수색장소에 있어야 하는 것은 아니다. 범죄와 연관된 디지털 데이터를 영장에 쓰인 수색장소에서 해당 서버에 접속해 수색

105) 일심회사건의 판결과 왕재산사건의 판결에서 '하드카피' 용어가 사용되었는데 그 화면을 인쇄물로 출력한 것을 의미한다.; 이관희·이상진, 앞의 책, 131면.
106) 이인곤, 앞의 논문, 188면.
107) 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정.
108) 이주원, 앞의 책, 158면.

장소에 있는 PC 등에 출력하거나 다운로드 받으므로써, 해당 디지털 데이터가 수색장소에 존재하여 이 같은 방법으로 압수·수색을 할 경우에는 영장에서 허용하는 범위를 넘는가의 유무는 실제로 발생하지 않는다.

그러나, 영장이 압수·수색의 대상을 '특정 장소에서 저장 되어 있는 디지털 데이터'로 특정하고 있는 경우에는, 문언해석상 압수·수색영장의 집행에 착수하여 네트워크를 통하여 다운로드 받음으로써 그 장소에 존재한 정보까지 포함한다고 보기는 힘들다.[109]

이와 관련하여 '제주도지사 선거법위반 사건'[110] 에서는, 평소 도지사실에서 보관하던 서류를 도지사 비서관이 압수·수색 당시 압수·수색 영장에 기재된 장소로 가져갔다가 압수된 경우에, 이는 영장에서 압수대상으로 적시하고 있는 '특정 장소에서 보관 중인 서류'로 볼 수 없다 하여 그 서류의 증거능력을 부정한 바 있다. 현재의 실무는 수사기관이 '압수·수색장소에 있는 컴퓨터에서 해당사이트에 접속해 디지털 데이터를 다운로드하고 이를 출력하거나 복사한 후 화면을 촬영하여 압수한다.[111]' 고 영장청구서에 기재한 후에야 압수·수색영장을 발부받게 된다.

이와 같은 취지가 쓰인 압수·수색영장이 발부된다면 이는 형사소송법 제120조에서 정한 '압수·수색영장의 집행에 필요한 처분'이라는 범위에 포함되므로 수사기관은 피압수자에게 해당 웹 사이트에 접속이 가능한 아이디 및 패스워드 등의 제공을 요구하는 것이 가능하며, 피압수자가 행여나 아이디와 패스워드를 임의로 제공하지 않을 경우, 수사기관은 피압수자가 해당 사이트의 접속할 때 사용하던 PC를 수색해서 남겨져 있던 데이터 속의 아이디 및 패스워드 정보를 취득하는 방법 등으로 범죄 관련 데이터가 저장되어 있는 서버에 접속하는 것이 형사소송법 제120조의 '압수·수색영장의 집행에 필요한 처분'인지 아닌 지에 대해 문제될

109) '제주도지사 선거법위반 사건'에서, 평소 도지사실에서 보관하던 서류를 도지사 비서관이 압수·수색 당시 압수·수색 영장에 기재된 장소로 가져갔다가 압수된 경우, 이는 영장에서 압수대상으로 적시하고 있는 '특정 장소에서 보관 중인 서류'로 볼 수 없다 하여 그 서류의 증거능력을 부정하였다; 대법원 2007. 11. 15. 선고 2007도3061 전원합의체 판결.

110) 대법원 2007. 11. 15. 선고 2007도3061 전원합의체 판결.

111) 손창현, "사이버테러에 대한 대응방안으로서의 디지털 증거 압수·수색", 비교형사법연구 21권 3호, 2019, 193면.

수 있을 것이다.

사안의 경중이나 대체가능한 수단(인터넷서비스제공자에 대한 압수・수색)이 있는지의 유무, 긴급성 등 개별적이거나 구체적 상황에 따라서 각각 달라지겠지만, 유형물에 대해 압수・수색에서 잠금장치가 설정된 문이나 금고를 열려고 열쇠기술자를 부르거나, 금고의 잠금장치를 손괴하는 것이 허용될 수 있다는 점에 비추어 보면, 필요성을 인정하여야 할 경우가 있을 것으로 여겨진다.[112]

(2) 국외의 서버에 보관 중인 정보의 압수・수색

우리나라에 지사를 두지 아니한 외국 포털사의 경우 압수・수색영장을 발부하더라도 이를 현실적으로 집행할 방법이 없을 것이다. 반면, 우리나라에 지사를 두고 있는 외국 포털사라면, 앞에서 원격지 서버에 위치한 정보의 압수・수색의 경우와 같이 한국 내에 소재한 동사의 컴퓨터로 외국의 서버에 접속하여 해당 정보를 한국 내에 존재하게 한 다음 압수하는 것은 이론상 가능하다고 할 것이다.

피의자가 Google 등 외국에 서버를 둔 인터넷서비스제공자의 e-메일을 사용하는 경우, 위 회사에 대하여 압수・수색영장이 발부되는 경우가 있으나, 실무상 자료를 제공받지 못하는 예가 있다. 이러한 경우에도 피의자의 집이나 사무실을 수색하여 그가 사용하는 컴퓨터 등에서 해당 포털사의 아이디나 패스워드 정보를 취득한 후에 외국에 있는 서버에 접속하여 e-메일 정보를 가져와 이를 압수하는 것은 가능하다고 할 것이다.

한편, Google처럼 관련 데이터가 하나의 서버에 저장이 되지 않고 임의적으로 분

112) 피고인들이 국가보안법상 국가기밀의 탐지, 수집 등의 혐의로 기소되었던 '일심회' 사건 항소심에서 피고인들은 국가정보원이 피고인들에게 진술거부권을 고지하지 않은 상태에서 강압적으로 디지털 저장매체의 암호를 획득하였으므로, 이러한 위법한 암호 획득에 따라 디지털 저장매체로부터 출력된 문건은 증거능력이 없다는 주장을 하였다. 이에 대하여 재판부는, 피고인들이 국가정보원이 자신의 진술 없이 암호를 알아내었다고 진술하였었던 점(암호는 '목련', '백유향', '천재왕', '이기자' 등이었다)과 수사관이 암호를 묻기에 능력이 있으면 풀어보라고 말했더니 15분 만에 암호(암호는 '투쟁'이었다)를 알아내 왔다는 점 등을 들어 피고인들의 위 주장을 배척한 바 있다. 즉, 국가정보원이 피고인들의 동의 없이(다만 피고인들에게 진술을 강제하지 아니하고) 상당한 방법으로 암호를 알아내어 이를 이용하여 문서파일을 열고 출력한 문서의 증거능력을 인정한 것이다.

산되어 저장하게 되는 클라우드 형식의 서비스의 경우, 사실상 서비스 제공자조차도 정보가 저장되는 곳을 잘 모르기에 수사기관으로서는 사전에 디지털 증거가 저장된 물리적 위치를 특정하여 압수·수색영장 청구가 어려울 뿐 아니라 디지털 증거가 어느 국가의 관할에 보관되어 있는지도 알 수 없기 때문에 클라우드에 저장된 e-메일 등 디지털 증거에 대한 압수·수색이 현실적으로 불가능하다.[113]

실무상 일부 국외 서비스제공자들은 수사기관에 홈페이지 또는 연락처 등을 개설하여[114], 압수·수색영장을 발부받아서 협력을 요청한다. 그리하여, 영장의 사본 등을 제시할 경우엔 해당된 디지털 데이터를 추출해 제공하는 경우 실무상 압수·수색 영장에 기재하는 압수·수색의 대상은 해외 본사가 보관하고 있던 정보로, 압수·수색의 장소 역시 외국에 소재한 본사의 주소로 기재하고 있는 것으로 보인다.[115] 따라서 외국계 서비스제공자가 보유한 디지털 데이터에 대한 압수·수색 영장청구서에 집행의 방법이나 집행 가능성에 대하여 소명이 부족하거나, 압수·수색 영장의 실효성에 의문이 있는 경우에는 수사기관으로 하여금 이에 대하여 추가적으로 소명하도록 할 필요가 있다.

정보의 보관자가 피의자인 경우도 문제가 된다. Google코리아가 스트리트뷰 서비스 준비를 위하여 와이파이(Wi-Fi)망에서 불특정 사용자들이 주고받은 통신정보를 무단 수집, 저장한 혐의로 압수·수색을 당한 적이 있다. 당시 위와 같은 정보를 저장한 서버가 미국에 설치되어 있는데, 우리 법관이 발부한 압수·수색영장에 의하여 증거를 수집할 수 있는지가 논란이 된 바 있다. 예를 들어 Google코리아가 미국에 있는 서버에 접속해서 해당 디지털 데이터를 임의로 제공할 경우에는 이를 압수하는 것에 대해 문제가 없다.[116] 임의로 제공하지 아니할 경우에는 압수·수색

113) 박석훈, 앞의 논문, 25~26면.
114) Google은 각 서비스 별로 본사의 e-메일계정을 통하여, Facebook은 홈페이지를 통해 협력요청을 수사기관에 각 본사에 자료제공을 할 수 있도록 창구를 개설하고 있는 반면, 한국지사에서는 자료제공 협조 등의 업무를 제공하지 않고 있는 것으로 보인다.
115) 조성훈, “역외 전자정보 수집과 국가관할권 행사의 합리성 이론 -미연방 ‘클라우드 법’의 제도적·법이론적 기원에 대한 분석을 중심으로-”, 형사정책연구 제32권 제1호 (통권 제125호), 2021,
116) 정대용·김기범·권헌영·이상진, “디지털 증거의 역외 압수·수색에 관한 쟁점과 입법론 -계정접속을 통한 해외서버의 원격 압수·수색을 중심으로-”,법조 제65권 제9호, 2016, 154면.

영장의 집행하는데 필요한 처분[117]에 의해 아이디 또는 패스워드를 알아내 국외 서버에 접속할 수 있다. 그러나 피의자가 자의적으로 데이터를 제공하지 않거나, 해당 서버에 접근이 가능한 아이디 또는 패스워드를 알려주려고 하지 않아, 보통 상식적인 방법으로는 엑세스가 불가능하여 국외 소재 서버에 있는 데이터를 우리나라의 영역으로 가져올 수 없다면, 압수・수색은 불가능하다 할 것이다.

피의자가 정보보관자인 경우 관련 데이터의 제출이나 증거수집에 협력할 의무를 부과할 수 있을까 의문이 든다. 이에 대해서는 헌법상 자기부죄금지원칙에 비추어 보면 피의자는 자신에게 불리하게 된 관련 증거의 수집에 상부상조하여야 할 의무를 줄 필요는 없다 할 것이다. 예를 들어 인터넷서비스제공자가 정보만 보관할 뿐 범죄혐의와 관련 되지 않은 제3자인 경우와 같은 이치이기 때문이다. 결론적으로 제출의무나 협력의무를 부과하거나, 또는 이런 의무 불이행을 이유로 제재를 가하는 것은 어렵다. 사이버범죄 방지조약 제31조, 제32조가 국경을 넘는 데이터 접근을 허용하는 조항을 두고 있는 점은 국경을 초월하여 저질러지는 사이버범죄에 대하여 각 회원국의 사법기관이 효과적으로 대응하기 위한 방안으로서 시사하는 바가 크다.

3. 디지털 증거에 대한 압수・수색의 방법과 절차

가. 디지털 증거에 대한 압수・수색의 방법

현대사회의 디지털 기술의 발전으로 기업 및 개인이 생성하거나 보관하고 있던 자료들의 데이터의 대부분이 디지털화 되었으며, 다양한 데이터들이 제3자에 의해서 대량으로 생성되거나 보존되는 실정에 이르렀다. 시대의 변화에 따라서 수사기관의 압수・수색 대상 또한 유체물에서 디지털 관련 데이터로 바뀐 것이다. 디지털 증거의 압수・수색에 대하여 종래 유체물에 대해서 압수・수색과는 다르게, 그 특징에 맞는 새로운 절차와 방식이 정립되어야 함에 불구하고 아직도 법률과 해석에

117) 형사소송법 제 120조(집행과 필요한 처분)

서 문제가 있다. 특히 정보의 집약체로 생겨난 스마트폰에 대한 압수·수색, 정보통신 서비스 업체의 감식을 통한 포렌식 활용도와 압수·수색의 중요성이 높아졌음에도 여전히 논란이 있어 그 범위와 한계에 도달한 상황이다.

고도의 첨단과학기술시대에 날로 발달하고 있는 지능적인 범죄수법에 대해 효과적으로 대응하기 위해서 과학기술시대에 다양한 디지털 증거를 추적하여 확보하고 필요한 부분을 수집하는 데에 집중적이고도 효율적인 포렌식 역량을 갖추고 증거능력 개선을 위한 방안을 강구하여야 한다. 현행 형사소송법상으로는 압수의 목적물이 컴퓨터용 디스크나 그와 비슷한 전자저장매체인 경우엔 기억된 데이터의 범위를 정해서 출력 또는 복제해서 제출받아야 하고, 다만 범위를 정해서 출력 및 복제하는 방법이 불가능할 경우나 압수의 목적을 달성하기에는 현저히 곤란하다고 인정되는 경우에는 전자저장매체 등을 압수할 수 있다.[118]

이처럼 수사기관의 디지털 데이터에 대한 압수·수색의 원칙에 대하여, 대법원은 범죄혐의사실과 연관된 부분만 문서로 된 출력물로 수집 또는 수사기관이 휴대한 데이터저장매체에 해당 파일을 복제하는 방식으로 이뤄져야 하고, 예외로 현장사정이나 디지털 데이터의 대량성으로 연관된 데이터획득에 긴 시간이 걸리거나 전문인력이 필요한 기술적 조치가 있어야 될 경우 등 범위를 정해서 출력 및 복제하는 방법이 전혀 불가능하거나 압수목적을 달성하기에는 곤란하다고 인정되는 때 한해, 직접 데이터 저장매체 자체를 반출, 데이터저장매체에 들어있던 데이터파일 전부 모두를 하드카피나 이미징 등의 형태로 복제본을 만들어 반출하는 방법으로 압수·수색하는 것이 허용되고, 다만 압수·수색영장에 이 방법의 그 취지가 기재되어 있어야 한다고 하였다.[119]

나. 디지털 증거에 대한 압수·수색의 절차

디지털 증거에 대한 압수·수색절차로는 먼저 사건의 개요와 압수·수색장소 및

118) 형사소송법 제106조 제3항, 제219조 참조.
119) 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정; 대법원 2012. 3. 29. 선고 2011도10508 판결; 대법원 2011. 5. 26.자 2009모1190 결정.

대상과 범위 수집정보의 특성 등 압수·수색계획을 치밀하게 작성하는 철저한 준비과정이 있어야 하고 압수의 목적을 정당한 절차적 방법으로 달성을 하기 위해서는 영장을 발부받아야 한다. 그리고 영장을 발부받기 전에는 압수·수색의 수사대상과 그 범위에 대해서는 세밀한 검토가 있어야 한다. 왜냐하면 압수·수색의 과정에서 대상과 범위와 관련하여 범죄의 관련성여부를 두고 시비의 소지가 있을 수 있기 때문이다. 디지털 데이터에 대한 수사권 행사나 재판권 행사의 기준이 바로 관련성이므로 그 의미를 깊이 이해하고 관련 있는 정보만을 취득하여야 할 것이다.

디지털 증거에 대한 압수·수색은 경우에 따라 다르지만 가장 대표적인 사례가 정보저장매체 자체를 외부로 반출할 경우를 보면, ① 압수·수색현장에서 데이터저장매체를 확보할 경우 ⇛ ② 원본을 압수할 때 데이터저장매체를 봉인해서 수사기관 사무실로 옮기는 경우 ⇛ ③ 데이터저장매체의 봉인을 해제한 후 이미징을 하는 경우 ⇛ ④ 이미징한 데이터를 업로드해서 저장하는 경우 ⇛ ⑤ 피압수자에게 데이터저장매체를 환부 및 가환부하는 경우 ⇛ ⑥ 수사기관의 분석관이 시스템에 접근해서 저장되어 있던 데이터사본에 대해 파일을 검색 및 탐색 또는 복제하는 경우 ⇛ ⑦ 수사기관의 분석관이 복제했던 파일에 대해서 분석 및 추출하는 경우 ⇛ ⑧ 분석이 완료된 데이터를 수사기관시스템에 업로드 등 하는 경우 ⇛ ⑨ 수사기관이 데이터를 검색하는 경우 ⇛ ⑩ 해당사건과 관련있는 디지털 데이터를 복사 및 출력하는 경우 ⇛ ⑪ 사건이 종결된 이후 데이터를 삭제 또는 폐기하는 경우로 나뉠 수 있다.[120]

압수·수색과정에서는 피의자 혹은 피고인측에 대한 고지 및 참여 등 적법절차를 철저히 준수하면서 디지털 증거를 온전하게 수집해야 한다. 수집단계에서 선별할 경우나 복제할 경우에는 현장에서 선별 및 복제과정을 거치게 되고, 현장사정상 압수의 목적을 달성할 수 없거나 현저하게 곤란한 경우에는 데이터저장매체 자체를 압수할 수 밖에 없다.[121] 이때 수사기관이 과잉 또는 위법한 수색을 하는 경우 피의자 혹은 피고인측이 과잉수색 내지 위법 수색을 하였다고 주장할 수 있으므로 수집과정에서 증거에 대한 무결성이 훼손되지 않도록 압수 전 과정을 전체와 세부

120) 조광훈, 앞의 논문, 75면.
121) 형사소송법 제 106조 제3항.; 권양섭, 앞의 논문, 141면.

로 나누어 촬영하여 차후에 문제가 될 수 있는 불법시비에 대비하는 등 세심하고 각별한 주의가 요구되는 바이다.

그러나, 일단 데이터저장매체 등에 대한 탐색 또는 복제가 완료된 후에 이루어진 수사기관의 활동에 대해서는 압수·수색이 아니기 때문에 참여문제가 나타나지 않는다. 대법원은 데이터저장매체에 저장되어 있던 정보 중에서 파일의 확장자 및 키워드 검색 등을 통해서 수사기관이 범죄 혐의와 관련된 정보만 선별한 다음 데이터저장매체와 같은 비트열 방식으로 복제해서 생성된 '이미지 파일'을 제출받아서 압수했다면, 그 때는 압수·수색절차가 이미 종료된 것이기 때문에, 그 후에 수사기관에서 압수된 이미지 파일을 탐색 및 복제 또는 출력 등의 과정에 피의자 등에게 참여의 기회를 무조건 보장해야 하는 것은 아니라고 판시[122]하였다.

4. 디지털 증거에 대한 압수·수색의 범위와 한계

가. 디지털 증거에 대한 압수·수색의 범위

압수·수색의 범위와 관련하여 대법원 판례는 정보저장매체 자체 또는 적법하게 획득한 복제본을 탐색하여 혐의사실과 관련된 디지털 데이터를 문서로 출력하거나 파일로 복제하는 일련의 과정 역시 전체적으로 하나의 영장에 기한 압수·수색의 일환에 해당하므로 그러한 경우의 문서출력 또는 파일복제의 대상 역시 정보저장매체 소재지에서의 압수·수색과 마찬가지로 혐의사실과 관련된 부분으로 한정되어야 함은 헌법 제12조 제1항, 제3항과 형사소송법 제114조(영장의 방식), 제215조(압수, 수색, 검증)의 적법절차 및 영장주의 원칙이나 비례의 원칙에 비추어 당연하다. 따라서 수사기관 사무실 등으로 반출된 정보저장매체 또는 복제본에서 혐의사실 관련성에 대한 구분 없이 임의로 저장된 디지털 데이터를 문서로 출력하거나 파일로 복제하는 행위는 원칙적으로 영장주의 원칙에 반하는 위법한 압수가 되는 것이라고 하였다.[123]

122) 대법원 2018. 2. 8. 선고 2017도13263 판결.

수사기관 또는 법원은 정보저장매체 등의 압수를 통하여 일정한 정보를 제공받은 경우에는 그 정보에 의해 알 수 있는 사람으로서 정보의 주체가 되는 사람에게 해당사실을 지체 없이 알려야 한다(법 제106조 제4항, 제219조, 개인정보보호법 제2조 제3호). 그리고 위와 같은 일련의 과정에서 피압수자나 변호인에게 참여기회를 보장하고(법 제219조, 제121조) 혐의사실과 관련 되지 않은 디지털 데이터의 임의적인 복제 등을 막기 위한 적절한 조치를 취하는 등 영장주의 원칙과 적법절차를 준수하여야 한다.

만약 그러한 조치가 취하지 않았다면 ① 피압수자측이 참여하지 않는다는 의사를 명시적으로 표시하였거나, 2 절차 위반행위가 이루어진 과정의 성질과 내용 등에 비추어 피압수자측에 절차 참여를 보장한 취지가 실질적으로 침해되었다고 볼 수 없는 경우에 해당한다는 등의 특별한 사정이 없는 이상 압수·수색이 적법하다고 평가할 수 없고, 비록 수사기관이 저장매체 또는 복제본에서 혐의사실과 관련된 디지털 데이터만을 복제, 출력하였다 하더라도 마찬가지이다.[124]

또한 판례는 수사기관이 데이터저장매체에 기억되어 있던 정보 중에서 키워드 및 확장자 검색 등을 통하여 혐의와 관련이 있는 데이터를 선별한 다음 정보저장매체와 동일하게 비트열 방식으로 복제하여 생성한 파일(이미지파일)을 제출받아 압수하였다면 이로써 압수의 목적물에 대하여 압수·수색 절차는 마무리된 것이므로 수사기관이 수사기관 사무실에서 위와 같이 압수되었던 이미지 파일을 탐색 및 복제 또는 출력하는 과정에서도 피의자 등에게 참여기회를 무조건 보장해야 되는 것은 아니라고 하였으며, 계속해서 수사기관은 압수 직후 현장에서 압수목록을 바로 작성하여 교부해야 하는 원칙에 따라 압수된 데이터의 상세목록에는 정보의 파일명세가 특정되어야 하므로 이를 출력하여 서면으로 교부 및 전자파일의 형태로 복사해주거나 e-메일을 전송하는 등의 방식으로 하여야 한다는 입장이다.[125]

한편 2011년 7월 19일 개정된 형사소송법은 디지털 증거의 압수·수색 관련 규

123) 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정; 대법원 2012. 3. 29. 선고 2011도10508 판결; 대법원 2011. 5. 26.자 2009모1190 결정.
124) 대법원 2019. 7. 11. 선고 2018도20504 판결; 대법원 2017. 9. 21. 선고 2015도12400 판결; 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정.
125) 대법원 2018. 2. 8. 선고 2017도13263 판결.

정을 제106조 제3항에 신설하였는바, 제219조(준용규정)는 제106조를 수사기관에 대하여 준용하고 있다. 이러한 점에서 우리나라는 압수·수색에 대하여 압수·수색의 대상은 원칙적으로 출력 또는 복제한 것이고 예외적으로 정보저장매체가 됨으로써 디지털 데이터자체가 대상이 아니라는 입장이다.[126]

또한 압수 가능한 디지털 데이터의 범위를 어떻게 정할 것인가 등 여러 쟁점이 있지만 디지털 증거의 압수·수색에 있어서 집행과정의 범위, 즉 정보저장매체를 반출한 후 처리과정을 어떻게 볼 것인지도 문제이다. 이는 이른바 관련성의 문제로, 디지털 증거의 압수·수색에서도 문제가 되지만 일반적인 압수·수색에서도 큰 쟁점이 되고 있다.

최근 피고인이 인터넷사이트(음란물유포)를 운영하면서 도박개장방조죄와 정보통신망이용촉진 및 정보보호 등에 관한 법률 위반(음란물유포)죄에 의해 비트코인을 취득한 사안에서, 가상자산은 국가에 의해 통제를 받지 않고 있으며, 블록체인 기술과 같이 분산원장에 의해 부여된 경제적인 가치가 디지털 형식의 정보로 나타나는 재산상 이익이라고 한 판례[127]를 주목해 볼 필요가 있다.

1심법원은 "현금과 달리 물리적 실체 없이 전자화 한 파일의 형태의 비트코인을 몰수할 수 없다"[128]면서 몰수 구형을 기각하였지만, 항소심과 대법원에서는 경제적인 가치를 디지털로 표상해 전자적으로 이전 및 저장 또는 거래가 가능해, 이른바 '가상화폐'의 일종인 비트코인, 피고인은 음란사이트를 운영할 때 사진 및 영상을 사용하는 사용자와 음란사이트에 광고를 원하는 광고주들로부터 비트코인을 대가로 지급받아 재산적 가치가 있는 것으로 취급한 점에 비추어 비트코인은 재산적 가치가 있는 무형의 재산이라고 보아야 하고, 범죄수익 은닉규제 및 처벌 등에 관한 법률은 몰수대상을 형법상 '물건'에 한정하지 않은 채 '재산'으로 규정하고, 동법시행령에서 '은닉재산'을 '재산적 가치있는 유형·무형의 재산'이라

126) 일본 형사소송법 제110조의2는 우리나라형사소송법과는 달리 정보저장매체를 원칙적인 압수의 대상으로 하고 출력 또는 복제물을 예외적인 압수의 대상으로 하고 있다.
127) 대법원 2018. 5. 30. 선고 2018도3619 판결; 대법원 2021. 12. 16. 선고 2020도9789 판결.
128) <https://weekly.cnbnews.com/news/article.html?no=144008> 한편 비트코인투자로 인해 일가족이 극단적 선택을 하거나 자살하는 사례가 이어지고 있다.(2022. 06. 30. 뉴스검색)

정의하며, 비트코인이 몰수대상으로 특정되어 있단 이유로, 피고인이 취득했던 비트코인을 몰수가능하다고 하였다.

위 사건은 가상자산도 경제적 가치를 갖는 재산상 이익으로서 형법상 보호할 가치가 있다고 한 것으로, 경찰은 피고인의 비트코인 '비밀키', '지갑주소'를 확인하여 피고인의 비트코인지갑의 별도 전자지갑으로 압수대상인 비트코인을 이체하는 방법을 통해 압수했다.

나. 디지털 증거에 대한 압수·수색의 한계

대법원[129]은 2011년 데이터저장매체 자체를 수사기관의 사무실 등으로 옮긴 이후 영장에 기재된 범죄혐의와 연관된 디지털 데이터를 탐색하여 당해 디지털 데이터를 문서인쇄 또는 파일복사과정 역시 압수·수색영장 집행의 일환에 전체적으로 포함되는 것이 당연하다 하였다. 그 후 대법원은 2015년 전원합의체 결정에서 데이터저장매체 자체 및 적법하게 얻은 복제본을 탐색해 혐의사실과 연관된 디지털 데이터를 문서출력 또는 파일복제 등의 일련의 과정 역시 하나의 영장에 전체적으로 기한 압수·수색의 일환에 해당한다고 했으나, 수사기관이 피의자의 데이터저장매체를 외부로 반출해서 복제본을 제작하고 그 복제본에 저장되어 있는 디지털 데이터를 피의자의 참여 없는 탐색 또는 선별하는 과정에서 별건 증거를 발견하고 나서 새로운 영장을 새로 발부받는 것은 위법하다고 하면서 당해 별건 증거의 증거능력을 부정하였다.[130]

대법원은 피압수자의 참여권 보장을 강조하며 변호인과 압수·수색의 집행과정에서 단순히 참여하는 것에 그치는 게 아니고, 저장매체를 압수 또는 이미징화, 탐색 및 복제와 출력 등 수사기관에서 전체적인 압수·수색영장의 집행과정에도 보장하여야 한다고 보고 있다.[131] 역외 디지털 데이터 압수·수색절차에서 정보주체

129) 대법원 2011. 5. 26.자 2009모1190 결정.
130) 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정.
131) 전명길, "디지털 증거의 압수·수색에 있어서 참여권에 관한 연구", 인문사회21, 제8권 제2호, 2017, 658면.

의 개인정보자기결정권 보호와 피의자의 방어권 보장은 보호되어야 할 핵심 법익이며, 그 수단은 당사자 참여권이므로 참여권 배제사유 역시, 증거인멸이나 수사기밀누설 또는 수사방해의 경우 등으로 구체화하는 것이 필요하다. 디지털 증거는 쉽게 변경·삭제할 수 있기 때문에 압수·분석 과정에서 수정이나 삭제가 없었는지 확인할 필요가 있음에도 형사소송법에 정보저장매체의 압수에 관한 규정만 존재할 뿐이다.

이렇듯 피압수자 등에게 참여권을 보장해야 한다는 것은 대검찰청과 경찰청에도 규정이 있다. 대검찰청의 '디지털 증거의 수집·분석 및 관리 규정' 제22조는 현장뿐만 아니라 현장 외의 장소에서 이미징 등을 통하여 디지털 증거를 압수하거나 디지털 증거의 분석이 필요한 경우에도 참여권이 피압수자 등에게 보장되어야 한다고 하고 있고, 경찰청의 '디지털 증거 수집 및 처리 등에 관한 규칙' 제12조는 디지털 증거에 관한 압수·수색의 집행에 있어서 정보저장매체의 원본 또는 복제본을 외부로 반출하는 경우 참여권을 고지해야 한다고 하고 있다.

5. 소결

대법원은 다른 범죄혐의와 관한 디지털 데이터를 발견한 경우에, 디지털 데이터에 대해 압수·수색에 있어서 데이터저장매체를 외부에서 데이터매체나 복제본에 대해 압수·수색이 허용된 예외경우라 하더라도 혐의사실과 관련 되지 않은 디지털 데이터를 탐색 또는 복제 및 출력하는 경우는 원칙적으로 위법 압수·수색에 해당하기 때문에 허용될 수 없다[132]고 하였다.

그러므로 디지털 데이터에 대한 압수·수색이 종료되기 전에 혐의사실과 관련된 디지털 데이터를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 디지털 데이터를 우연히 발견했다면, ① 수사기관에서는 추가 탐색을 더 이상 중단해야 할 것이고, ② 다만 법원으로부터 별도 범죄혐의에 대해서 압수·수색영장을 발부받은 경우라면 그러한 데이터에 대해서도 적법한 압수·수색을 할 수 있다.[133]

132) 대법원 2018. 4. 26. 선고 2018도2624 판결.

이런 경우에 최초 압수·수색 절차와 별도 압수·수색 절차는 구별이 되는 별개의 절차이며, 별도의 범죄혐의와 관련된 디지털 데이터는 최초 압수·수색영장에 의하여는 압수·수색의 대상이 아니다. 따라서 데이터저장매체의 원래의 소재지에서 별도 압수·수색영장에 기해 압수·수색을 진행한 경우랑 마찬가지로 피압수자는 최초 압수·수색 이전부터 해당 디지털 데이터를 보관해서 관리하고 있던 자라 볼 것이므로, 특별한 사정이 없는 경우 피압수자나 변호인에게 참여권을 보장하고(법 제219조, 제121조), 압수한 디지털 데이터 목록을 교부하는(법 제219조, 제129조) 등 피압수자의 이익보호를 위해서는 적절한 조치가 이뤄져야한다.[134]

디지털 증거는 네트워크를 통해서 시·공간을 초월하고 국경의 벽을 넘어서 저장·전송·처리되고 있는 특징이 있다. 따라서 증거가치 있는 디지털 데이터를 수집하려면 네트워크를 통해 시스템에 접근해야 하는 경우도 있다. 그 동안 압수·수색은 영장에 기재된 '압수·수색·검증할 장소'에 물리적으로 위치하는 물건만을 대상으로 하였으나, 온라인화 되어 있는 현재의 컴퓨터 네트워크 환경에서는 압수·수색 현장에서의 컴퓨터에 대한 압수·수색만으로는 압수·수색의 목적을 달성하기 어렵게 되었다.

점증하는 네트워크 환경의 디지털 증거에 대해 실무적으로 수색 대상 컴퓨터를 통해 원격지 컴퓨터에 접속하여 사건과 관련된 정보를 압수하는 방법이 나타나고 있다. 그러나 원격지 컴퓨터에 대한 압수·수색이 우리 법제 하에서 허용되는 것인지, 만일 허용된다면 어떠한 경우에 가능할 수 있는지, 또한 수색의 방법과 범위 및 프라이버시(Privacy)와 방어권의 보장은 어떻게 이루어져야 하는지 등 다양한 문제가 제기되고 있다. 원격서버에는 수많은 개인정보가 존재하고 개인의 프라이버시(Privacy)에 대한 기대수준이 높아서 신중한 접근과 다양한 사항에 대한 검토가 선행되어야 한다. 특히 압수·수색의 기본원칙의 철저한 준수, 허용범위의 제한, 수색의 범위특정은 물론, 집행의 방법도 피압수자의 통상적인 계정접속 방법으로 제한되어야 하며, 투명성 보장을 위한 피압수자의 참여와 집행과정의 방해배제도 고려

133) 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정; 대법원 2014. 1. 16 선고 2013도7101 판결.
134) 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정.

되어야 한다. 이러한 사항에 대한 진정한 노력을 통하여 인권침해의 예방과 프라이버시(Privacy)의 보호 및 사법정의 실현을 위한 효율적 수사제도의 구현이 가능할 것이다.[135]

135) 정대용・김기범・이상진, “수색 대상 컴퓨터를 이용한 원격 압수・수색의 쟁점과 입법론”,법조 제65권 제3호, 2016, 40~41면.

제3장 디지털 증거 역외 압수·수색의 특성과 유형 및 문제점

제1절 디지털 증거의 역외 압수·수색의 특성과 유형

1. 역외 디지털 증거에 대한 압수·수색의 특성

가. 개념

압수·수색의 당사자국이 아닌 제3국에 원격지 서버의 위치가 존재하는 경우를 일반적으로 '역외 압수·수색'이라고 한다. 이러한 역외 디지털 증거에 대한 역외 압수·수색은 해외 기반의 인터넷서비스사업자(ISP)가 보관하는 디지털 데이터에 대한 증거수집 방안으로, 수사과정에서 피수사 대상자의 해외 e-메일 또는 클라우드 서비스에 관한 계정 아이디 및 패스워드를 알게 된 경우, 수사기관 사무실 또는 그와 관련된 장소에서 역외서버에 접속해서 관련된 증거를 확보하겠다는 영장을 발부받아서 집행하게 되는 압수·수색 방법이다.[136]

그러나 아직까지 일관된 정의는 존재하지 않으며, 각 국가에서 집행하고 있는 실무상의 역외 압수·수색 또한 그 범주를 달리하고 있는 상황이다.[137] 그러나 구체적인 압수·수색의 유형이 다양하여 일관된 정의나 논의가 어렵기 때문에 특히 계정정보를 가지고 국내에서 해외 계정에 접속하여 e-메일을 압수·수색하는 경우로 범위를 제한하고 있다.

---

136) 정대용·김기범·권헌영·이상진, 앞의 논문, 136면.; 이수용·임규철, "역외 압수·수색의 절차적 위법성에 대한 비판적 소고", 비교법연구 제18권 2호, 2018, 81면.; 이관희·이상진, 앞의 책, 277면.

137) 정소연, "디지털 증거의 역외 압수·수색에 대한 법적 고찰", 디지털포렌식연구 제11권 제1호, 2017, 62면.

사이버범죄의 대부분은 국경을 초월하여 발생하여 특정 국가 단독의 노력으로는 대응이 곤란하다. 또한, Google, 트위터 등 여러 다국적 인터넷 기업들이 나타나게 되면서 수사기관이 이들에게 사용자정보 또는 접속기록 등을 요구하는 경우가 늘어나고 있다.[138] 이와 관련해서도 관할권 또는 집행방법 등에서 논란이 된다. 반면, 외국계 e-메일, 메시지 등의 관련 데이터를 확보하기 위해서는 형사사법공조절차를 거쳐야 하는데 많은 시간이 소요되기 때문에 절차 이행 중에 증거소멸 가능성이 크다.[139] 또한 국제공조에 있어서는 적극적으로 협력하는데 한계가 있어서[140] 이러한 문제가 해결되지 않는다면 범죄 그 피해를 받아들일 수밖에 없을 것이다.

외국의 법제를 살펴보자면, 미국에서는 저장통신법(SCA)에 이미 몇 년 전 원격지 압수・수색 규정을 도입했고, 이후 마이크로소프트와 이와 관련된 문제로 논란이 생기게 되자 2018년 클라우드법(CLOUD Act)을 제정하여 규정을 마련하였다.[141] 일본, 독일, 프랑스 형소법에서도 원격 압수・수색을 허용하고 있으며, 역외 압수는 유럽이사회(Council of Europe) 사이버범죄조약에서 이용자의 적법하고 자발적인 동의를 전제로 허용하고 있다. 현재 일본이나 유럽의 여타 국가들도 관련 규정을 두고 있다.

원격 압수・수색의 필요성이 인정된다고 하더라도 현행법상 허용되는지 여부에 관하여는 견해가 분분하고, 특히 역외 압수・수색의 경우는 주권의 문제까지 있어 논의가 더해지고 있다. 물론 최근의 대법원 판결[142]을 통하여 외국계 e-메일을 적법하게 압수할 근거는 마련되었다고 볼 수 있으나, 사이버 범죄에서 신속한 디지털 증거확보는 수사 성패와 직결되는 문제인 만큼 개인의 프라이버시(Privacy)를 보호하면서 수사의 효율까지 기할 수 있는 디지털 증거의 특성을 반영한 입법과 조약 체결 등 형사사법 공조를 위한 정부의 적극적인 행보가 필요해 보인다.

---

138) 정소연, 앞의 논문, 64면.
139) 정소연, 앞의 논문, 64면.
140) 정소연, 앞의 논문, 64면.
141) 이재윤・강민구, “ 디지털 증거 역외 압수・수색 쟁점 고찰”, 한국산업보안연구 제9권 제2호, 2019, 187면.
142) 대법원 2017. 11. 29. 선고 2017도9747 판결.

나. 특성

(1) 해외 서버에 관한 원격 압수・수색

디지털 데이터는 네트워크로 연결된 원격의 컴퓨터에 존재하면서 통신 프로토콜을 통해 접근・수정・저장할 수 있어 장소적 제한을 받지 않으므로 원거리 또는 타국에 있는 서버나 컴퓨터에 존재할 수가 있다. 그러므로 해외에 존재하는 서버나 컴퓨터라 할지라도 수사기관이 네트워크 접속을 통해 사건과 연관된 정보를 확인하여 이를 우리 사법관할권이 미치는 영역으로 다운로드 한 후 압수・수색하는 것이 가능하다. 이는 디지털 데이터의 네트워크성이라는 본질적인 특성에 따른 압수・수색이다.[143]

(2) 사건과 관련 되지 않은 장소에서의 집행 가능

통상 압수・수색이 집행되는 곳은 피의자를 체포하였던 장소나 사건과 연관된 컴퓨터가 있는 장소이지만 역외 압수・수색이 집행되는 곳은 피의자를 체포한 장소나 사건과 연관된 컴퓨터가 위치한 장소에 한정되지 않는다. 수색에 사용되는 컴퓨터 또한 사건과 연관성이 있어 수색대상이 된 컴퓨터에 국한되지 않는다.[144] 따라서 수사기관은 피압수자의 계정정보를 사전에 확인한 경우, 수사기관의 사무실 등 '사건과 관련이 없는 장소'에 있는 '사건과 관련이 없는 컴퓨터'를 이용하여 압수・수색을 집행하는 것이 가능하다.

(3) 선별 압수 및 계정수색을 통해 집행

해외 서버에 저장된 디지털 데이터는 역외 압수・수색의 대상이지만, 압수는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정되므로[145] 역외 압수・수색에 있

143) 정대용・김기범・권헌영・이상진, 앞의 논문, 141~144면.
144) 정대용・김기범・권헌영・이상진, 앞의 논문, 143면.

어서도 압수할 정보는 당연히 사건과 관련성이 인정되는 정보를 의미한다. 사건과의 관련성 여부는 해당 데이터를 열람하기 전까지는 모르므로 먼저 수색을 통해서 압수대상 관련데이터를 가려서 나눠야 한다.[146]

그런데 역외 압수·수색은 수색대상이 된 계정으로 접속하여 접근 가능한 정보만을 열람할 수 있고, 저장매체 자체에 대한 접근이 불가능하므로 '매체반출'은 물론, '하드카피 이미징'을 통해서 증거의 압수는 곤란하여 수색을 통해서 열람한 데이터를 직접 출력 및 수색할 때 컴퓨터의 하드디스크나 별도의 데이터저장매체에 다운로드 받아서 압수하는 방법으로 압수[147]할 수 있다.

2. 역외 디지털 증거에 대한 압수·수색의 유형

역외 디지털 증거에 대한 압수·수색의 유형으로 총 5가지 유형으로 분류될 수 있다.

첫째, 원격지 압수·수색에 의한 방법으로써, 원격지에 대하여 압수·수색 영장을 집행하는 과정에 용의자에게서 계정정보를 정당하게 획득해서 역외에 존재하고 있는 컴퓨터 데이터에 접근하는, 당사자로부터 적법한 방법으로 취득한 계정정보를 이용하여 역외에서 존재하는 컴퓨터의 데이터에 직접 압수·수색 영장을 집행해서 관련 데이터를 취득하는 방법이다.[148]

둘째, 합법적으로 획득한 계정정보를 이용한 방법으로써, 수사기관이 계정정보를 정당한 방법으로 획득해서 네트워크를 통해 국외서버에 접속하여 사관과 관련된 증거를 압수·수색하는 것으로[149] 불법정보 또는 유죄의 증거데이터가 저장되어 있는 역외 컴퓨터 관련 데이터에 접속하는 것이다.[150] 수사기관이 적법하게 계정정보

145) 형사소송법 제106조 제1항 참조.
146) 정대용·김기범·권헌영·이상진, 앞의 논문, 144면.
147) 정대용·김기범·권헌영·이상진, 앞의 논문, 143~145면.
148) 정대용·김기범·권헌영·이상진, 앞의 논문, 141면.
149) 정대용·김기범·권헌영·이상진, 앞의 논문, 170면.
150) 이정민, "외국계 이메일 계정에 대한 압수·수색의 정당성- [대상판결1] 서울고등법원 제12부 2017.6.13. 선고 2017노23, [대상판결2] 서울고등법원 제8형사부 2017.7.5. 선고 2017노146

를 취득하여 이를 정보통신망을 통해 역외에 있는 컴퓨터 데이터에 접근하는 합법적으로 취득한 계정정보를 이용한다.

셋째, 전문 소프트웨어의 기술적 방법을 활용하는 것으로써, 이는 온라인수색 또는 감청 등과도 개념상 유사한 측면이 있기 때문에 수사기관이 컴퓨터 시스템에 대해 직접적으로 접근한다는 측면에서 그 법익 침해의 정도가 크다. 앞의 두 가지 방법과 다르게, 소프트웨어나 기술적 방법을 활용하는 경우에는 차원이 다르다. 해킹프로그램인 키로거(key loggers) 및 스니퍼(sniffers) 같은 전문 소프트웨어의 기술적 방법을 이용한다.[151]

넷째, 당사자 동의를 얻어 역외에 있는 컴퓨터에 접근하는 동의에 의한 방법으로써, 범죄 사실의 입증함에 있어 중요한 증거가 될 수 있는 컴퓨터 관련 데이터가 다른 사법관할권 안에 존재할 경우에, 정당한 방법과 자발적 동의에 의해 수사기관이 집행하는 방법이다.[152]

다섯째, 인터넷서비스제공자(ISP)로부터 관련 데이터를 공급받는 방법으로, 이는 수사기관이 용의자와 관련된 기술적 정보를 인터넷서비스제공자(ISP)로부터 획득하는 것[153]이다.

3. 소결

클라우드 컴퓨팅[154]의 눈부신 발달은 원격 압수・수색의 문제를 야기한다. 해외

-", 비교형사법연구 제19권 제3호, 2017, 123면.

151) 이순옥, 앞의 논문, 129면.

152) 사이버범죄방지조약 제32조(Article 32) b. 만약 당사국이 데이터를 공개할 법적 권한을 가진 자의 적법하고 자발적인 동의를 얻었다면, 자국 영토내의 컴퓨터 시스템을 통하여 다른 당사국에 위치한 컴퓨터에 저장된 데이터에 접속하거나 이를 수령할 수 있다.;이순옥, 앞의 논문, 129~130면.

153) 마이크로소프트사건에서 2016년 수사기관은 마이크로소프트에게 아일랜드 서버에 저장된 이용자의 e-메일 데이터를 제출하도록 명하자 2차 순회법원(Second Circuit)은 마이크로소프트가 수사기관에 아일랜드에 데이터를 제공할 의무는 없다고 하였고, Google사건은 2017년 2월 펜실베니아 법원이 미국 연방수사국(FBI)의 압수・수색영장에 응하라고 하였다.;이순옥, 앞의 논문, 130면.

154) 클라우드란 데이터를 인터넷과 연결된 중앙컴퓨터에 저장해서 인터넷에 접속하기만 하면

주요국가에서는 이를 입법적으로 해결하고 있으나, 우리 형사소송법은 아직도 역외 서버에 대한 원격 압수・수색이 허용되는지 여부는 논란이 많다.[155] 사이버 범죄는 나날이 진화해가고 국경을 초월하는 역외에 존재하는 컴퓨터 데이터 및 관련 디지털 증거에 대해 집행하는 압수・수색의 필요성이 커지고 있다.[156]

해외 입법례 등을 살펴보면 미국의 CLOUD Act, 유럽 사이버범죄 협약, 영국의 PCA, 독일, 프랑스, 호주, 일본의 형사소송법 등에서 원격 압수・수색의 문제를 입법적으로 해결하고 있다. 국내에서는 원격 압수・수색의 허용 여부에 대해 다양한 견해가 있지만, 우리 대법원은 e-메일 압수・수색과 관련, 피의자의 아이디와 패스워드 입력을 통해 정당한 접근권한에 따라 접속하여 해외 서버로부터 e-메일을 압수・수색하는 것도 허용된다고 보아 우리 형사소송법 해석상으로도 원격 압수・수색이 허용된다고 여겨진다.

적법하게 얻은 계정정보를 이용해서 역외 압수・수색을 할 때, 정보의 주체인 피의자 보호에 중점을 두고 있다는 점과, 실제로 압수・수색행위는 압수・수색 대상 PC에서 이뤄진다는 점을 종합해 보면, 피압수자는 피의자를 정보주체라고 보아야 하며, 영장의 집행을 위한 필요한 행위를 해외 서버에 접속한 행위라고 보는 대법원의 결론이 타당해 보인다.

나아가, 데이터사용자를 보호하기 위한 국제적 합의와 해결방안이 필요하고 개인정보를 보호할 수 있게 될 것이며 심각한 권리 침해가능성이 있지만, 인권보호 측

언제 어디서든 데이터를 이용할 수 있는 것으로, 인터넷 접속만 가능하면 고성능 기기가 아니어도 원격으로 작업을 수행할 수 있다. 클라우드 컴퓨팅은 클라우드라는 인터넷 서버에서 데이터 저장과 처리, 네트워크, 콘텐츠 사용 등 IT 관련 서비스를 한번에 제공하는 기술을 말한다. 클라우드 컴퓨팅을 도입하면 컴퓨터 시스템을 유지・보수・관리하기 위해 들어가는 비용과 서버의 구매 및 설치 비용, 업데이트 비용, 소프트웨어 구매 비용 등 많은 비용과 시간・인력을 줄일 수 있다. PC에 자료를 보관할 경우 하드디스크가 장애를 일으키면 자료가 손실될 수 있지만 클라우드 컴퓨팅 환경에서는 외부 서버에 자료들이 저장되기 때문에 안전하게 자료를 보관할 수 있다. 그러나 서버가 해킹 당할 경우 개인정보가 유출될 수 있고 서버의 데이터가 손상되면 백업하지 않은 정보는 되살리지 못한다는 단점이 있다. 출처: 다음백과 2022.06.29. 검색.

155) 긍정설, 부정설, 제한적 긍정설 등 적법성을 부정하는 견해 및 원격 압수・수색의 필요성을 인정하는 전제에서 입법을 통하여 제도화를 주장하고 있다.; 조성훈, “역외 전자정보 수집의 범위와 한계: 국가관활권의 확정과 위법수집증거배제 법칙의 적용을 중심으로”, 제11회 한국형사학대회 학술대회 발표문, 2022. 176면.

156) 정소연, 앞의 논문, 57면.

면에서 유럽 사이버범죄협약과 미국과의 행정협정에 대해 적극 검토해서 해결방안을 마련하여 역외디지털 증거관련 데이터에 접근할 수 있도록 하여야 한다.

제2절 역외 디지털 증거 압수·수색의 문제점

1. 역외 디지털 증거에 대한 압수·수색상의 적법성 문제

우리 형사소송법은 미국이나 영국과 달리 무체물에 해당하는 정보를 명시적으로 압수·수색의 대상으로 규정하지 않고,[157] 정보에 대한 압수·수색을 일반적인 유체물의 압수·수색과 함께 규율하고 있다. 또한 디지털 증거의 특성을 반영한 압수·수색절차가 형사소송법에 구체적으로 명시되어 있지 않고, 해외 서버나 원격지 서버에 저장된 디지털 증거의 압수·수색에 대한 직접적인 조항도 없다.[158]

수사 실무상 가장 어려움이 있는 사안은 해외에 서버를 두고 운영되는 e-메일과 클라우드 서비스의 경우라 할 수 있다. 이 경우 각종 통신제한조치는 물론이고 서버의 압수·수색도 어려운 상황이기 때문이다. 이는 전형적인 법적 관할의 문제로 다른 국가의 주권적 영역에 대해 타국의 법적 강제가 이루어질 수 없다는 근본적인 한계가 있다. 국내법상 영토고권이 미치지 않는 지역에 대해서는 더욱 더 수사 실무상 어려움이 있는 것이다. 더구나 최근 급격한 성장세에 있는 글로벌 IT산업 및 클라우드 산업은 향후 이러한 상황이 더욱 극단적으로 전개될 것이다.

역외서버에의 일반적인 접속 방법으로는, ① 피압수자가 계정정보를 제공할 때, 2 제3자가 계정 정보를 제공할 때, ③ 압수·수색 과정에서 서면 등을 통해 확인할 때, ④ 자동접속 기능을 통해 접속할 때, ⑤ 수사기관이 피의자에 관한 정보를 바탕으로 추측하여 반복적인 시도로 인해 알아낼 때, ⑥ 프로그램을 이용해 계속적인 접속을 시도할 때(Brute Force Attack), ⑦ 시스템의 보안 취약성을 이용하여 침입할 때, ⑧ 프로그램을 설치해서 일정시간 피의자가 타이핑 하였던 내용을 확보하고

157) 손지영·김주석, 앞의 보고서, 26면.
158) 이순옥, 앞의 논문, 131면.

이를 분석해 비밀번호를 유추할 때를 들 수 있다.[159]

위의 8가지 방법 중 ①에서 ④까지의 방법은 수사기관이 접속권한을 얻기 위하여 별도의 추가적 행위를 하지 않지만 ⑤이하의 방법은 접속권한에 관한 추가적 조치가 필요한 경우이다. 따라서 수사기관의 추가적 노력이 필요한 ⑤의 방법부터는 '일반적인 접속'이라고 보기 어려워 ④까지의 방법만을 합법적 접근권한을 이용한 일반적 접속의 범위로 보는 것이 타당하다.

역외 압수·수색은 "최초 압수·수색 장소의 수색 대상 컴퓨터와 네트워크로 연결된 다른 컴퓨터에 사건관련 정보가 저장되어 있을 가능성이 확인되고 해당 컴퓨터를 통해 접근·이용이 가능한 경우 다른 컴퓨터를 수색하여 관련된 정보를 압수하는 행위"[160]로 현행 형사소송법은 역외 압수·수색의 방법을 명문으로 하는 규정이 없다. 따라서 수사기관이 정당한 방법으로 접근 권한을 취득하였더라도 e-메일 사용자의 동의를 받지 않은 e-메일 계정 접속이 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조 제1항[161]의 정보통신망 침해행위로 위법한 수사인지 또는 당초 형사소송법이 예정한 압수·수색의 방법인지가 문제된다.

이와 관련하여 과거 국가정보원의 소위 RCS(Remote Control System)활용에서 결국 해킹 프로그램을 통한 합법적인 감청이 인정될 수 있을 것인지가 쟁점이 되었다. 이에 대하여 항소심[162]은 e-메일 압수·수색의 성격이 통신비밀보호법상 '전기통신'의 압수·수색과 유사하다고 보여 e-메일 서비스 제공자에 대한 강제처분의 방식으로 이루어지지 않은 압수·수색은 법이 예정한 방식의 강제처분이 아니라고 판단하였고, 상고심 대법원[163]은 e-메일 계정 사용자를 디지털 데이터의 소유자로 보아 인터넷서비스 제공자가 아닌 사용자를 피처분권자로 하는 대물적 강제처분의 방법을 인정하였다. 즉 대법원은 서버의 관리권한자인 인터넷서비스 제공자의 의사는 형식적으로 접근권한을 가진 자를 대상으로 한 서비스제공의 의사이므

159) 김기범·이관희·장윤식·이상진, "정보영장 제도 도입방안 연구", 경찰학연구 제11권 제3호, 2011, 108면.
160) 정대용·김기범·이상진, 앞의 논문, 46면.
161) 제48조(정보통신망 침해행위 등의 금지) 제1항 참조.
162) 서울고등법원 2017노23 판결.
163) 대법원 2017도9747 판결.

로 접근권한 있는 수사기관의 접속을 불허하려는 의사는 없다고 본 것이다. 결과적으로 대법원은 형사소송법이 명문으로 규정하고 있지 않으나 현행법의 해석상 디지털 데이터의 원격 압수·수색을 적법한 강제수사의 방법으로 인정하고 있는 것이다.

수사기관이 정상적으로 취득한 계정정보를 이용하여 e-메일 계정에 접근하는 자체를 위법한 압수·수색으로 보는 견해는 확인되지 않는다. 다만 e-메일이 인터넷서비스제공자의 제3자 보관물이라는 점에서 인터넷서비스제공자의 의사가 문제되는데 타인의 계정정보를 이용한 계정 접근이 인터넷서비스제공자를 기망하거나 그 의사에 반하는 접근이라고 생각되지 않는다. 외관상 적법한 접근 또는 처분권한을 가진 자가 서비스를 이용하는 경우에는 서비스제공자의 의사에 반하는 것은 아니다. 영장 집행절차의 준수를 전제로 한다면 적법하게 얻은 계정데이터를 이용해 서버에 접속하는 것은 형사소송법 제120조상의 영장 집행에 필요한 사전행위로서 적법성이 인정되기 때문이다.[164]

즉 e-메일을 제3자 보관물로 보아 인터넷서비스제공자의 의사를 고려하더라도 인터넷서비스제공자는 계정정보에 관하여 실질적인 심사가 아닌 형식적 정확성만을 확인하여 서비스 이용을 허용하기 때문에 합법적으로 취득한 계정정보를 활용하는 것은 기망이라 할 수 없다. 대법원 판결[165]로 인하여 계정정보를 이용한 e-메일 접속과 그 내용의 압수·수색은 현재 합법성이 인정된 강제수사방법이라 할 수 있으며 남은 문제는 이렇게 취득한 e-메일 내용의 증거능력 인정 문제라 할 수 있다. 다만, 역외 압수·수색에 대해 대법원 판례로만 인정하는 것은 논란의 여지가 있다.

현행 형사소송법은 제106조 제1항에서, 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다고 하였고, 동조 제2항에서는 압수할 물건을 지정하여 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다고 하여 '유체물'의 압수를 전제로 하는 절차를 규정하고 있다.

---

164) 이순옥, 앞의 논문, 136~138면.
165) 대법원 2017. 11. 29. 선고 2017도9747 판결.

디지털 데이터의 압수·수색 방법에 대해서는, 동조 제3항에서 압수의 목적물이 컴퓨터용 디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 하며, 다만 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체 등을 압수할 수 있고, 제3항에 따라 정보를 제공받은 경우에는 개인정보보호법 제2조 제3호에 따른 정보주체에게 해당 사실을 지체 없이 알려야 한다는 2개의 조항이 따로 규정되어 있을 뿐이다.

위 제106조 제3항, 제4항은 컴퓨터 등 저장장치에 저장된 디지털 데이터의 압수·수색을 염두에 두고 개정된 것임에도 불구하고 정보 자체가 압수·수색의 대상물로 특정되지 않아 유체물인 디지털 데이터 자체를 압수·수색의 대상물로 볼 수 있는지 여부에 대하여 견해의 대립이 있다.[166] 이에 대해 대법원은 압수·수색의 대상을 '정보' 자체로 보고 영장에 기재된 범죄와 관련된 정보만 압수하여야 하는 것으로 판시하고 있다.[167]

e-메일은 디지털 데이터의 일종으로서, 이용자가 삭제하거나 용량이 초과되지 않는 한 송·수신자 모두에 의해 변형 없이 보존되고, 송수신이 완료된 e-메일은 대부분 이용자 개인이 아닌 인터넷서비스제공자가 관리하는 서버에 저장·보관된다.

지금까지 e-메일 압수·수색에서 문제되는 사실은 대개 e-메일이 압수되었다는 사실을 이용자, 즉 송·수신자가 모르는 경우였다. 즉 e-메일의 내용은, 일반적으로 사용자가 계정을 개설한 인터넷서비스 제공자(Internet Service Provider, ISP)의 서버에 저장되기 때문에, e-메일에 대한 압수·수색의 경우에는 일반적인 유형물에 압수·수색과 달리 '압수처분을 받는 자'와 '압수의 실질적인 대상인 정보의 소유자'가 분리되게 된다.[168] 그 결과 정보주체는 '현실적으로 압수·수색을 당하고 있는 자로서 압수할 물건 또는 장소를 실제로 지배하는 자'가 아니어서 형사소송법 제118조에 정한 영장제시의 상대방인 '처분을 받는 자'가 될 수 없어

166) 정대용·김기범·권헌영·이상진, 앞의 논문, 168면.
167) 대법원은 일명 종근당 사건(대법원 2015. 7. 16. 자 2011모1839 전원합의체 결정) 등에서 디지털 관련 데이터 자체를 압수·수색 대상으로 보고, 혐의사실과 관련 되지 않은 데이터까지 문서로 출력 및 파일로 복제할 경우 영장주의에 반하여 위법하다고 판시하였다.
168) 이정민, 앞의 논문, 121면.

영장제시를 통하여 그 집행 사실을 알릴 수 없기 때문에, 형사소송법 제122조 본문의 규정에 의한 사전통지가 아니고서는 그 집행사실을 사전은 물론 사후적으로도 통지받을 수 없게 되는 문제점이 있었다.

결국 우리 형사소송법은 디지털 데이터 그 자체가 압수·수색의 대상인지 여부, 디지털 데이터가 원격지의 서버에 존재하는 경우에도 정보통신망을 이용한 접근방법으로 압수·수색이 가능한지 여부, 그리고 그 절차에 대하여 별도의 규정을 두고 있지 않기 때문에 법리적 해석에 의해 이러한 압수·수색의 가능성 및 압수·수색 영장 집행방법의 적정성 여부를 검토해야 한다. 따라서 '원격 압수·수색' 방법에 따른 역외 디지털 증거 수집의 적법성은 일률적으로 판단할 문제는 아니며, 개별 사건의 구체적 사실관계를 고려하여 '수색'과 '압수'의 목적론적 해석에 따라 그 적법성 여부를 판단할 수밖에 없다. 따라서 이러한 디지털 증거의 특성과 역외 압수·수색이라는 특성을 반영한 압수·수색의 적법성을 확보하는 방안의 마련이 필요할 것이다.

2. 역외 디지털 증거 수집과 국제공조 문제

나날이 진화하는 디지털 범죄를 뿌리 뽑기 위해 오늘날 '국제공조'는 선택이 아닌 필수가 되었다. 범죄 관련물 공유 사이트가 해외에 서버를 둔 경우, 우리나라 수사기관이 이를 직접 수사할 방법은 없기 때문이다. 접속한 IP주소와 가입자 추적이 어려운 해외 메신저 프로그램을 사용하는 사례가 점차 증가하는 것도 문제다.

오늘날 인터넷 디지털사회에서 수많은 사이버범죄의 발생은 부득이한 현상이지만, 범죄 발생을 줄이기 위한 당국의 온갖 노력에도 불구하고 전혀 줄어들지 않고 단속과 수사를 어렵게 만드는 이유 중 하나는 범죄 관련물 공유 사이트가 해외에 서버를 둔 경우이다. 국가관할권은 한 국가가 사람, 물건, 행동 등에 행사할 수 있는 권한의 총체를 의미하는데[169] 이에 문제는 국제법상 논해지는 개념인 바, 이러한 국가관할권은 일반적으로 입법관할권, 집행관할권, 재판관할권으로 세분할 수

169) 김대순, 국제법론(제20판), 삼영사, 2019, 451면.

있다. 입법관할권은 국가가 자국법을 설정하는 권한을 말하고, 재판관할권은 사법기관이 그의 재판관할의 범위를 정하고 국내법령을 적용하여 구체적인 사안을 심리하고 재판을 선고하는 권한을 말하며, 집행관할권은 법원 또는 행정기관이 체포, 강제조사 등의 물리적인 강제조치에 따라 국내법을 집행하는 권한을 말한다.[170]

일반적인 형사절차에서는 위법수집증거 배제법칙에 따라 불법취득증거의 경우 증거능력은 부정되지만, 재판관할권 자체가 부정되지는 않는다. 따라서 국가관할권의 문제는 결국 재판관할권의 문제라 할 수 있다. 최근 재판관할권의 범위를 판단함에 있어 국제예양 또는 국제관계의 존중을 중시하기는 하지만, 형사사건의 경우 우리 형법이 적용되기 때문에 우리가 재판관할권을 갖는다는 것이다.[171]

역외 집행관할권을 행사하려면 다른 국가의 영역 내에 물리적으로 현존하거나 유형력 행사를 수반해야 하므로 현실적으로 광범위한 제약을 받는다. 그러나 이러한 상황은 가상공간의 맥락에서는 달라질 수밖에 없다. 가상공간에서의 국가관할권 행사는 영토적 제약의 굴레를 벗어날 여지가 많기 때문이다.[172] 즉, 역외 디지털 데이터의 압수・수색에 있어 실행국가의 수사기관이 대상국가에 물리적으로 현존하지 않아도 증거수집이 가능하기 때문에 일방적 집행의 가능성이 높다.[173]

일반적으로 범죄는 국내에서 일어나는 범죄 또는 범죄자가 머물렀던 국외에서도 발생되므로 해당 지역의 수사당국은 이들 범죄자를 자국의 수사관할권 하에서 신속히 적발하고 단죄할 수 있다. 하지만 사이버범죄는 국경이 없는 사이버공간을 이용하여 발생되는 특성상 해당 범죄자가 어디에 있든 상관없이 지구 어느 곳에서나 범죄를 저지를 수 있어 문제를 해결하기가 어렵다.[174]

다시 말해서 일반범죄는 자국의 수사관할권 하에 수사할 수 있음에 반하여, 사이버범죄는 범죄의 내용이 담긴 서버가 자국 영토 내에 있지 않으면 직접수사가 불가능한 것이다. 예컨대 사이버음란물을 유통시킨 범죄자가 해당 서버를 국내에서 운영하였다면 철저한 수사가 가능하므로 적발이 가능하지만, 미국이나 유럽 혹은

170) 조성훈, 역외 전자정보 압수・수색 연구, 박영사, 2020, 229면.
171) 조성훈, 앞의 책, 226면.
172) 김대순, 앞의 책, 450면.; 조성훈, 앞의 책, 231면.
173) 조성훈, 앞의 책, 243면.
174) 조성훈, 앞의 책, 242면.

동남아에 서버를 두고 있다면 해당 국가에 있는 서버를 직접 수사할 권한이 없으므로 당해 국가의 경찰에 협조를 구하거나 인터폴에 수사를 의뢰할 수밖에 없다.

이러한 사정은 사이버음란물 범죄 이외에도 각국에서 시도되는 보이스 피싱, 해킹과 사이버공격, 랜섬웨어, 도박사이트, 인터넷사기 등 수 많은 사이버범죄의 수사에 있어서도 동일하다. 이처럼 범죄자가 타국에 있거나 관련 서버가 타국에 존재할 경우라도 국내 수사기관이 관할권을 넘어 직접 수사할 수 있는 방법으로 가장 좋은 방법은 해당 국가와 형사사법공조 조약을 체결하는 것이다. 조약에는 양자간 조약과 다자간 조약이 있는데, 현재 사이버범죄 분야에서 양자간 조약이 체결된 사례는 없지만, 다자간 조약의 사례로는 유럽 '사이버범죄조약'을 들 수 있다.[175]

디지털 범죄와 관련해 국제공조 수사의 필요성이 점차 커지고 있지만 정작 이를 위한 '다자간' 국제 조약에 아직 우리나라는 가입하지 않은 상황이다. 지금껏 국제공조 수사는 사건에 따라 해당 국가에 개별적으로 요청하는 데 그쳤다. 현재 우리나라 국제공조 수사는 대부분 '국제형사경찰기구'(ICPO・인터폴)에 의존하고 있다.

특히 디지털 범죄에 관해서는 '소라넷', '텔레그램' 등 이슈화가 된 사건에 한해 단발적으로 공조를 요청해 왔다. 일반 외교 채널을 통한 공조보다는 빠르고 효율적이지만 갈수록 복잡하고 교묘해지는 사이버 공간에서의 수사에는 한계가 있다. 그렇다고 무턱대고 역외 디지털 증거 수집이 모두 적법성을 인정받는다는 것은 아니다. 여기에 국제적인 형사사법공조 절차가 필요한 것이다.[176] 사법공조 절차를 거치지 않고 수사기관이 해외에 저장・보관된 정보에 직접 접근하는 것은 대상국가의 영토주권을 침해하고, 사법공조 관련규범을 무의미하게 만들기 때문이다.

물론 국제공조 절차를 위반하여 취득한 데이터라 하더라도 바로 증거능력이 배제되는 것은 아니지만, 다른 국가가 증거사용에 반대하거나 국제공조절차에 따른 협력을 거부하는 경우에 그 데이터를 증거로 사용할 수 없는 경우가 있다. 따라서 역외 디지털 데이터 취득을 실효성 있게 담보하기 위해서는 특히 국제형사사법공조절차를 통한 서비스 제공자(ISP)의 협조를 얻어야 하는데 이는 시간과 절차상의 제약이 있으므로 수사기관이 당사자의 계정 정보를 알게 되었을 경우 서버에 직접

175) 조성훈, 앞의 발표문, 202면.
176) 조성훈, 앞의 논문, 138면.

접속하여 압수・수색하는 방법이 가능해야 할 것이다.

주권 및 개인정보보호 침해 가능성 등 우리나라가 조약 가입을 미루고 꺼려하는 여러 이유는 있으나 보안 강화, 사이버 전 방어 및 공격 능력 확충과 함께 사이버 침해나 공격 대응에 많은 효과를 보이고 있기 때문에 향후 우리나라 인터넷 영토를 안전하고 청결하게 만드는 대안으로 고려해 볼 필요가 있다.[177] 이처럼 역외 디지털 증거의 압수・수색에는 현실적으로 국제공조절차를 통해 상대국가의 협조를 구하는 것이 가장 필요한 절차 중 하나이므로 이에 관한 방안의 마련이 중요하다.

3. 역외 디지털 증거수집과 정보인권보호의 문제

압수・수색을 통한 수사의 최대 목적은 실체적 진실의 발견이지만, 본 논문에서 다루는 역외 디지털 증거에 대한 압수・수색의 범위와 한계를 논함에 있어서 역시 최대의 한계는 인권보호가 될 수밖에 없다. 비록 역외 디지털 데이터라 하더라도 그 안에는 수사대상자의 개인의 프라이버시(Privacy)가 많이 포함되어 있을 것이므로 국내수사에서만 인권문제를 관심 가져야만 하는 것이 아니라 역외수사에 있어서도 그 대상이 내국인이든 외국인이든 당연히 인권은 최우선으로 보호되어야 하는 것이다.

형사소송법은 실체적 진실 발견과 피고인 인권 보호라는 두 축 사이에서 형성된다. 그만큼 실체진실의 인식은 기본적 인권 보장을 위한 '합리적일 형사절차' 안에서만 가능한 것이다. 위법수집증거 배제법칙, 적법절차 원칙도 결국은 기본적 인권 보장을 위한 것이다. 실체적 진실을 찾는 과정은 형사소송법에서 가장 중요한 이념이라고 할 수 있다.[178] 진실한 범죄자를 찾아서 처벌하는 것이 무고한 피해자들 발생을 막고, 나아가 범죄의 예방이라는 형법의 궁극적인 목적을 달성하는 것이기 때문이다.[179]

177) 이상호, "한국 사이버 안보 취약성 개선 대책 모색; 사이버범죄조약 가입 효용성 평가", 세계지역연구논총 34권 4호, 2016, 169면.
178) 이수용・임규철, 앞의 논문, 95면.
179) 이수용・임규철, 앞의 논문, 95면.

인권은 인간이라면 누구나 누려야 할 가장 기본적인 권리이다. 따라서 인권은 일반인은 물론 범죄인을 포함한 피의자·피고인에게도 동일하게 보편적으로 향유하는 것이다. 수사의 목적인 실체적 진실의 발견은 법원에 의해 최종적으로 확인되는 것이지만, 이미 수사단계에서 피의자의 자백과 참고인의 진술, 유죄의 증거 등이 확보된다는 점에서 실체적 진실 발견의 유무는 사실상 수사단계에서 결정된다고 보아도 과언은 아니다.

실체적 진실 발견은 형사법적 판단의 목적이면서 동시에 책임주의라는 형법의 대원칙을 실현하기 위한 필요불가결한 수단이다. 그러나 실체적 진실의 발견에만 집중하다보면 수사의 효율성이 우선시 되고 그 과정에서 수사기관의 부당한 인권침해나 적법절차가 무시될 수도 있다. 수사대상자의 인권을 보호하고 존중하는 것은 실체적 진실의 발견 못지않게 중요하다. 종래의 비합법적이고 편법적인 수사관행에서 탈피하여 적법절차에 따른 수사의 투명성과 공정성을 제고하고 이를 통한 인권 친화적인 수사절차를 모색해야 한다는 것은 너무도 자명한 일이다. 특히 역외 디지털 증거의 압수·수색에 있어서도 수사의 효율성을 위해 인권보호의 측면이 간과될 수 있으므로, 압수·수색에 있어서 실체적 진실발견과 인권보장을 조화시키는 방법을 강구할 필요가 있다.

제4장 역외 디지털 증거의 압수·수색에 관한 입법례와 국내 판례

제1절 역외 디지털 증거의 압수·수색에 대한 외국 입법례

1. 서설

정보통신망의 발달로 컴퓨터 기기와 실제 디지털 데이터가 저장된 서버가 있는 장소가 서로 다른 경우가 많다. 디지털 데이터의 압수·수색시 영장에 기재된 장소에 대해서만 영장집행이 허용이 된다고 해석한다면, 서버가 원격지에 있는 경우 영장에 기재된 장소와 서버가 있는 장소가 다르므로 원격지 압수·수색영장을 별도로 발부받아 집행해야 한다.[180]

역외 디지털 데이터 압수·수색의 문제는 국가관할권의 범위를 확정하는 문제라 할 수 있다. 즉 압수·수색의 맥락에서 역외 데이터수집이 문제되는 바, 이는 우리 법제에서는 수사단계에서 제출명령이 인정되지 않고 있기 때문이다. 반면 미국에서는 수사단계의 자료 수집을 위해 '제출명령'(subpoena)이 적극적으로 활용된다. 제출명령이란 그 명령을 송달 받은 사람에게 자신이 보관·소지하는 것으로서 현재 계속 중인 절차의 쟁점과 관련성을 가진 특정한 문서·물건의 제출을 명령하는 것이다.[181] 제출명령(subpoena)은 연방 형사소송규칙(Federal Rules of Criminal Procedure) 제17조 및 연방 민사소송규칙(Federal Rules of Civil Procedure) 제45조가 이를 규율하고 있으며, 민사절차에서의 제출명령은 증거개시제도(discovery)의 구체적인 실현방법 중 하나로 인정된다.[182]

주권국가들 사이의 이익을 조정하여 정보접근에 대한 일관되고 안정된 규칙을

180) 입법조사처, "정보저장매체에 관한 압수·수색제도의 문제점과 개선방안", 2015, 31~32면.
181) 조성훈, 앞의 논문, 253면,
182) 조성훈, 앞의 논문, 254~255면.

발전시키기 위한 국제적 논의가 활발히 진행되고 있지만, 국제적으로 일원화된 만족스러운 조약으로 이러한 목표를 달성하는 것은 서로의 가치관을 달리하는 개별 주권국가들의 이해관계를 모두 충족하기에는 어렵다.[183]

디지털 증거 역외 압수·수색에 대해서는 미국의 경우 마이크로소프트사 사건이 있고, 국내에서는 외국계 e-메일 압수·수색사건으로 시나닷컴 사건이 있다. 우리 대법원은 수사과정에서 피의자의 해외 e-메일 계정의 아이디와 패스워드를 모두 취득하고 법원의 영장에 따라 로그인하여 실시한 압수·수색은 합법이라고 판단했으나, e-메일 계정만 알고 있는 경우에 대해서도 해외 인터넷사업자에 대한 압수·수색영장이 효력이 있을지에 대해서는 아직 판단된 바 없다.

대법원은 역외는 아니지만 원격지 서버에 저장돼 있는 정보라도 영장에 기재된 수색장소에서 해당 서버 또는 웹사이트에 접속하여 범죄와 관련된 e-메일 등 디지털 데이터를 복제하거나 출력하는 방법의 압수·수색이 가능하다는 입장이다.[184] 또한 대법원은 피의자의 e-메일 계정 아이디와 패스워드를 입력해서 역외에 있는 원격지 서버의 e-메일을 압수·수색하는 것도 적법하다고 판단하고 있다.[185]

인터넷과 디지털 시대에 역외 압수·수색과 적법한 영장주의 문제는 계속하여 많은 논란이 있을 것이다. 우리의 경우도 미국의 판례도 이에 관한 많은 시사를 주는 것으로 판단된다.[186] 그러나 어떤 경우에도 수사기관은 영장집행 등 강제수사 과정에서 법규에 규정된 한 가지 절차라도 준수하지 아니하면 위법한 법집행이 된다는 원칙은 명심해야 한다.

이러한 추세에 따라 우리 형사절차에 대한 논의에 있어서도 해외 선진국들 대부분은 원격 압수·수색의 문제를 이미 입법적으로 해결하고 있기에, 역외 디지털 데이터의 수집방법에 대한 검토가 필요하고, 비교법적 관점에서 제출명령 제도의 구체적인 내용을 의미 있게 살펴볼 필요가 있다.

---

183) 조성훈, 앞의 논문, 128면.
184) 대법원 2015. 7. 16.자 2011모1839 결정.
185) 대법원 2017. 11. 29. 선고 2017도9747 판결.
186) 김종구, “과학기술의 발달과 영장주의의 적용범위 -미연방대법원 판례의 변천과 관련하여-”, 전북대학교 법학연구소 법학연구 통권 제61집 2019, 205~206면.

2. 미국의 입법례

가. CLOUD(Clarifying Lawful Overseas Use of Data) Act

(1) 배경

미국은 2018. 3. 23. 시행된 연방법인 이른바 ‘CLOUD Act’를 통해 원격 압수·수색에 대한 법률적 근거를 마련하였다. 즉, 인터넷서비스제공자가 보유하고 있는 이용자 관련 데이터에 대해 그 정보의 위치를 불문하고 이를 제공할 의무가 있음을 명시한 것이다. 이는 ‘데이터의 위치’와 관계없이 데이터 ‘보유·관리자의 위치’에 초점을 맞춘 것이라고 볼 수 있다.

타국 서버에 저장된 자국 기업의 데이터를 미국 정부가 열람할 수 있도록 한 일명 ‘CLOUD Act’의 공식 명칭은 ‘합법적 해외 데이터 활용의 명확화를 위한 법(The Clarifying Lawful Overseas Use of Data Act, CLOUD Act)’으로, 제정당시부터 제기되었던 개인정보 및 인권 침해 논란이 미·호주 간 클라우드법 행정협정 체결 과정에서 재부상 되었다.[187]

CLOUD Act의 입법 배경은 미국 연방 정부와 Microsoft(마이크로소프트) 간 소송이 문제가 되었기 때문인데 이른바 ‘Microsoft(마이크로소프트) 사건’[188]에서 미국 연방 정부는 마약사건 수사를 위해 특정 e-메일 계정에 대한 수색영장(Search Warrant)을 발부받아 Microsoft(마이크로소프트)를 상대로 집행하려 하였고, 이에 대해 Microsoft(마이크로소프트)는 ‘해당 정보가 미국 내에는 없고 아일랜드에 위치한 서버에 저장되어 있으므로 기존 저장된 통신법(Stored Communication Act, SCA)에 기반하고 있는 수색영장의 효력은 아일랜드 서버에까지 미치지 않는다.’는 취지로 영장 집행의 적법성을 다투었다. 이러한 태도는 결국 기존 법률인 “저장된 통신법(Stored Communication Act, SCA)”의 입장을 수정한 것이라고 할 수 있다.[189]

187) 조성훈, 앞의 논문, 267면.
188) United States v. Microsoft Corp. 584 US 2018.
189) 송영진, 앞의 논문, 152~156면.

이에 대해 뉴욕 남부 연방지방법원은 Microsoft(마이크로소프트)가 아일랜드 서버에 접근 권한을 보유한 미국 내 법인이라는 점을 근거로 Microsoft(마이크로소프트)는 해당 정보를 제공하여야 할 의무가 있다고 판시하였음에 반하여,[190] 연방 항소법원은 국내 전기통신 서비스 제공자에게 해외 저장 정보를 공개하도록 강제하는 것은 법률의 불법적인 역외 적용으로서 허용될 수 없다는 취지로 1심과는 다르게 판단하였다.[191]

이 사건이 연방 대법원 계류 중, 미연방 법무부는 해외 저장 데이터에 대해서도 영장 집행이 가능할 수 있도록 SCA를 개정하는 법안을 제출하여 이런 개정안이 포함된 CLOUD Act(클라우드법)가 통과할 수 있게 되었으며, 이에 따라 미국 연방 정부는 개정된 법률에 따라 영장을 집행하게 되었고, 결국 연방 대법원은 소의 이익이 없음(Moot)을 이유로 기각 결정을 하였다.

이처럼 CLOUD Act는 2013년 미국 법무부가 Microsoft(마이크로소프트)의 아일랜드 데이터 센터에 저장된 전자메일을 요청하는 영장을 발부하였으나, Microsoft(마이크로소프트)가 이를 거부하면서 발생한 소송(일명 Microsoft Ireland Case)을 계기로 제정되었던 것이다. 2018년 종합세출법안(omnibus appropriations bill)에 포함되어 일괄 처리된 “합법적인 해외 데이터 활용의 명확화를 위한 법률(Clarifying Lawful Overseas Use of Data Act)”의 약칭으로, 미국 정부와 행정협정(executive agreement)이 체결된 타국의 서버에 저장된 메일, 문서, 기타 통신 자료 등을 압수·수색 영장 없이 열람할 수 있는 권한을 확보할 수 있는 집행 근거를 마련하였다.

미국과의 CLOUD Act 행정협정 최종 단계를 추진할 때는 호주의 통신법 개정 과정에서 시민사회와 관련 글로벌 기업들의 반발이 이어졌다.[192] 미국 CLOUD Act는 수사기관에게 CLOUD 기업의 해외 서버에 저장된 메일, 문서, 기타 통신 자료 등을

190) In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, No. 13 Mag. 2814, 2014 WL 1661004(S.D.N.Y. Apr. 25, 2014).

191) Microsoft v. United States, No. 14-2985 (2d Cir. 2016); In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., Case No. 14-2985 (2d Circuit July 14, 2016).

192) 한국인터넷진흥원, “미-호주 간 클라우드법 행정협정 체결 이슈 -미국 클라우드법의 주요 내용 및 전망-”, 2018, 425면.

열람할 수 있는 권한을 부여하여 미국의 법집행기관은 법원의 압수·수색 영장을 발부 받지 않고 전 세계 모든 국가에 저장된 온라인 정보에 대한 액세스를 요구할 수 있게 되었다.

이에 애플, 페이스북, Google, 마이크로소프트 등 미국 내 주요 IT 기업들이 2018년 2월 이 법안을 지지하는 공동 서한을 작성하는 등 CLOUD Act를 환영하고 있으나 시민권 옹호 단체 등을 중심으로, 법안 통과에 앞서 개인정보보호와 관한 충분한 토론이 이루어지지 않은 것과 개인정보보호에 대한 CLOUD Act의 부정적 영향에 대한 우려가 제기되었다. 이하에서는 역외 디지털 데이터 수집과 관련하여 다양한 내용이 규정되어 있는 저장통신법 법률인 CLOUD Act의 내용을 구체적으로 살펴보기로 한다.

(2) CLOUD Act의 주요 내용

CLOUD Act가 제정되기 전에는 정부가 서비스제공자에게 해외에 저장·보관된 데이터의 제출을 요구할 수 있는 규정이 명시되어 있지 않아서, 마이크로소프트 아일랜드 사건 등에서 역외 데이터의 제출을 강제할 수 있는지가 논란이 되었다. 이는 저장통신법의 적용 범위가 문제된 사안으로, 저장통신법에 의한 영장을 집행하여 '해외에 저장되어 있지만 국내에서 접근 가능한 정보'의 제출을 강제할 수 있는지가 쟁점이었다. 이에 대해 연방 제2항소법원은 마이크로소프트사에 미국 외에 저장된 데이터의 제출을 요구하는 영장 집행은 법률의 역외적용에 해당되므로 허용할 수 없다고 판시하였다.

이에 미연방 의회는 이를 입법적으로 해결하기 위해 연방 법률 제18장 제2713조를 신설하였다.[193] 제2713조는 서비스제공자는, 해당 통신 또는 정보가 미국 내에 저장되어 있는지 여부와 상관없이, 해당 제공자가 소유(소지), 또는 관리(통제, 보관)하는 통신의 내용과 가입자 관련 정보를 보존, 백업, 또는 공개할 법적 의무를 준수하여야 한다고 규정하여 서비스제공자에게 해외에 저장·보관된 데이터를 제

193) 기존 저장통신법은 미국 연방 법률 제18장 제2701조부터 제2712조까지 규정되어 있었으나, 여기에 제2713조를 추가한 것이다.

출할 의무가 있음을 명시한 것이다.

한편 CLOUD Act는 서비스 제공자가 영장 등의 효력을 다툴 수 있도록 하는 절차로, 연방 법률 제18장 제2703조 (h)(2)(A)는 가입자 등의 통신 내용을 공개하라는 요청을 받은 서비스 제공자는, ① 가입자 등이 미국인이 아니고 미국 내에 거주하지도 않고, ② 통신내용 공개로 인하여 외국 정부의 법률을 위반할 실질적 위험이 있는 경우에는 영장의 무효 또는 변경을 신청할 수 있으며, 이 신청은 정보공개 요청을 송달받은 날로부터 14일 이내에 하여야 한다고 규정하였다.[194]

또한 CLOUD Act는 초국경적 정보제공 요청을 위한 행정협정(executive agreement)과 관련하여, 연방 법률 제18장 제2523조 (b)(1)는 외국 정부의 국내법과 그 집행이 데이터수집과 관련된 개인의 프라이버시(Privacy)와 시민적 자유를 실체법・절차법적으로 강력하게 보장하는 등 법률에서 정한 요건을 충족하는 경우, 해당 외국 정부와 행정협정을 체결할 수 있다고 규정하였다.[195]

행정협정을 체결할 때 고려할 사항에 대하여도, 연방 법률 제18장 제2523조 (b)(1)(B)는 ① 외국 정부가 사이버범죄 및 디지털 증거에 관한 적절한 실체법과 절차법을 가진 경우, ② 법의 지배와 차별금지원칙에 대한 존중, ③ 국제 보편적 인권의 존중, ④ 데이터수집, 보유, 활용, 공유의 절차 및 그러한 활동의 효과적 통제에 대한 분명한 법적 권한과 절차, ⑤ 데이터수집 및 사용과 관련하여 책임성 및 적절한 투명성을 제공하는 메커니즘, ⑥ 세계적인 정보의 자유로운 이동과 인터넷의 공개되고 분산되고 상호 연결된 특성을 촉진하고 보호하겠다는 의지 등을 규정하고 있다.

한편 CLOUD Act는 제2702조 (b)(9)를 신설하여 행정협정 대상국 정부의 요청이 있는 경우 서비스제공자가 자발적으로 통신 내용을 제공할 수 있도록 하였다.[196] 이는 타국 정부에 대한 봉쇄조항(blocking statute)을 제거하는 것으로, 일정한 요건을 갖추어 행정협정을 체결한 경우에는, 해당 국가는 국제형사사법공조 절차를 거치지 않고서도 바로 미국에 근거한 서비스제공자(ISO)에게 통신 내용의 제출을 요

194) CLOUD Act, H.R. 1625, 115th Cong. div. V, § 103(b) 2018. (18 U.S.C. § 2703(h)).
195) CLOUD Act, H.R. 1625, 115th Cong. div. V, § 105(a) (18 U.S.C. § 2523).
196) CLOUD Act, H.R. 1625, 115th Cong. div. V, § 104 (2)(A)(i)(II) (18 U.S.C. § 2702 (b)(9)).

구가 가능할 수 있다. 이는 국제형사사법공조 절차의 비효율성을 극복하고, 신속한 정보공유를 가능하도록 하는 것으로서 CLOUD Act의 핵심적 내용이다.[197]

하지만 CLOUD Act는 기존의 국제데이터 공유 방법을 보완하는 것이지 그것을 대체하는 것이 아니다. 따라서 행정협정이 없는 경우라도 여전히 기존의 국제형사사법공조 절차를 통해 공조 요청이 가능하다.[198] 그러므로 행정협정이 체결된 국가라 하더라도 CLOUD Act의 범위를 넘어서는 정보에 대해서는 국제형사사법공조 절차를 적극 활용하여야 한다.

또한 행정협정을 체결하려면 추가 요건을 충족해야 하는데, 행정협정은 서비스제공자에게 암호해제(decryption) 능력을 갖출 의무를 부과하거나 서비스제공자가 복호화를 할 수 없도록 하는 제한을 포함하면 안 된다. 더불어 '의도적으로 미국인이나 미국 내에 거주하는 사람을 대상으로 하는 것'도 안 되고, 미국인이나 미국 내에 거주하는 사람과 관련된 데이터를 획득할 목적으로 미국 밖의 미국인이 아닌 자를 대상으로 할 수도 없다. 따라서 테러리즘을 포함한 '중대한 범죄'(serious crime)의 수사 등과 관련된 정보에 한정되며, 표현의 자유를 침해하기 위한 목적으로 이용해서는 안 된다.

한편 CLOUD Act는 통신에 대한 실시간 감청의 법적 근거도 제공하고 있다.[199] 즉, 제2511조 (2)(j)에서는 서비스제공자가 미국과 행정협정을 체결한 외국 정부의 명령에 따라 통신의 내용을 감청하거나 공개하는 것은 위법하지 않다는 명시적 예외규정을 두고 있다. 다만 실시간 감청은 '정해진, 제한된 기간'에만 할 수 있고, 보다 덜 강제적인 방법으로는 같은 정보를 확보할 합리적 기대가 없는 경우에만 허용된다.[200]

(3) CLOUD Act의 특징 및 주요 문제

197) 조성훈, 앞의 논문, 273면.
198) 조성훈, 앞의 논문, 137면.
199) CLOUD Act, H.R. 1625, 115th Cong. div. V, § 104 (18 U.S.C. § 2511 (2)(j)).
200) 조성훈, 앞의 논문, 274면.

미국 CLOUD Act의 핵심은 행정협정을 체결한 상대국이 보유한 자국 기업의 데이터에 양국 정부의 법집행기관이 상호 접근 가능하도록 하는 것이다. CLOUD Act는 범죄 조사에 필요한 데이터가 미국이 아닌 타국 소재 서버에 저장되어 있을 경우 이를 안정적으로 확보할 수 있는 방안 마련을 위해 제정되었으며, 고객의 정보를 비공개로 유지할 의무가 있는 기술기업 입장에서는 개인정보보호법을 준수해야 할 의무와 법집행기관이 요청하는 자료를 제공하여 수사에 협조할 의무 사이에서 모순을 겪지 않고 데이터를 제공할 수 있는 법적 근거와 프레임워크를 제공한 것이다. 이러한 CLOUD Act는 행정협정을 체결한 상대국의 법집행기관이 영장 없이도 미국의 기술 기업에게 개별사용자에 대한 데이터를 생성하도록 요구할 수 있도록 허용하고, CLOUD 컴퓨팅 시대의 전자(electronic) 증거 확보 과정에서 기존의 법 집행 도구 및 개인정보보호법이 지닌 한계를 넘어서기 위한 방안이다.

또한 CLOUD Act는 저장통신법(Stored Communications Act, SCA)에 따라 발부된 미국의 법집행명령이 타국에 저장되어 있는 특정 데이터에 도달할 수 있도록 한 것이 특징이다. 개인정보보호 및 시민의 자유를 침해할 수 있다는 우려를 고려하여, 법 집행 요청 시 SCA에서 규정한 대상과 데이터 유형에 대해서만 CLOUD Act를 적용한다. SCA가 전자 통신 및 CLOUD에 저장된 메일, 문서, 전송 기록, 사용자 계정 정보 등의 통신 관련 데이터에 대한 접근만 허용할 뿐 다른 유형의 개인 데이터 혹은 비즈니스 데이터에 대한 접근은 허용하지 않으며, 타국 서버에 저장된 데이터에 대해서 미국 정부의 요구에 따라 공개하도록 함으로써 전자통신 서비스 제공업체의 의무를 강화하였다.

그러나 범죄 증거 등의 수집을 위한 법 집행 과정이 상세하고 구체적인 표준 및 절차에 따라 진행될 수 있다는 CLOUD Act의 긍정적 측면[201]에도 불구하고, 동법의 개인정보 침해 및 정부의 감시 강화 가능성에 대한 우려가 있다. 개인정보보호 옹

201) 국제 협약을 통해 자국민에 대한 프라이버시(Privacy)를 공유함으로써 법적 모순 문제는 해결된 것으로 보인다. 외국의 수사기관이 영장 없이 데이터를 수집할 수 있고 판사의 검토 없이 사생활 데이터를 외국정부가 요구할 수 있다. 또한 타국과 협정을 맺음으로써 사생활 보호법을 준수하지 않고 데이터를 무단으로 수집가능하다. 국적에 상관없이 국가에 상관없이 데이터수집이 가능하다. <https://brunch.co.kr/@keepit/4> 미국의 클라우드법 파헤치기. (2022. 06. 30. 검색)

호 단체들은 CLOUD Act가 4차 수정헌법의 통신 개인정보보호 원칙에 위배되는 것은 물론 해외 정부가 시민 감시에 개입할 가능성이 있다며 반발하고 있으며, 미 의회는 시민들의 개인정보와 관련한 사항을 정부가 의회를 배제한 채 행정협정을 통해 해외 국가들과 협력할 수 있다는 점에 대해 우려를 표명하고 있다.[202]

(4) CLOUD Act의 의미

CLOUD Act[203]는 전자 형태로 해외 서버에 저장된 범죄 증거에 대한 '초국경적' 접근문제에 대한 해결 방안으로서 구체적인 프레임워크를 제공하고 있으나, 실제 국가 간 협력과정에서는 추가적인 검토가 필요하다. 영국은 The Crime(Overseas Production Orders)Act(COPOA)를 2019년 10월에 통과시켰고, 최초로 미국과 데이터 공유 행정협정을 2019년 10월 3일 체결한 나라이지만, 국내법과 국제법의 충돌 문제, 영국의 브렉시트 및 EU의 외부로 개인의 데이터를 전송하는 GDPR(유럽연합 개인정보보호법) 금지 사항문제가 아직도 남아 있는 상황이다.

EU와의 행정협정은 CLOUD Act가 GDPR 준수를 위한 충분한 조건을 갖추지 못하여 아직 체결되지 않은 상태이며, 이 사안과 관련하여 EDPB와 EDPS가 공동으로 발표한 법률 검토 결과에서도 유럽시민의 데이터를 미국으로 이전하기 위한 충분한 법적 근거가 CLOUD Act는 없다. 또한 호주의 경우는 구체적인 법률적 토대 확보 과정에 개인정보보호 기준과 비즈니스 환경에 대한 고려가 요구된다.

국내에서 미국과의 CLOUD Act 행정협정 체결이 논의될 경우, CLOUD Act의 상호주의 원칙에 대한 대비 및 호주 등의 선례를 참조하여 데이터 열람 사실의 투명

202) 조성훈, 앞의 논문, 275~276면.

203) 미국의 클라우드법은 인터넷 통신 서비스 업체가 보유한 데이터에 대해 신속하게 접근할 수 있는 증력은 공공의 안전을 도모하고 테러를 포함해 다른 중범죄에 대처하기 위한 정부의 노력에서도 반드시 필요한 요소이고, 미국정부는 해외에 저장된 데이터에 접근이 불가능하므로, 미국의 사법제도 관할 하에 있는 인터넷 서비스공급자의 데이터에 대해서는 미국정부가 보호권, 통제권, 소유권을 가지므로 외국 정부 또한 중범죄에 대처하기 위한 목적으로 미국에 위치한 인터넷 통신 업체가 보유한 데이터에 대해 접근이 가능한 방법을 찾기 위해 모색한 방법을 찾은 것이다. <https://brunch.co.kr/@keepit/4> 미국의 클라우드법 파헤치기. (2022. 06. 30. 검색)

한 공개와 기업의 책임 범위 등에 대한 논의가 필요할 것으로 보인다.

나. 연방 형사소송규칙 Rule 41

CLOUD Act의 경우 자국 기업 보유 정보가 해외 서버에 저장되어 있더라도 해당 기업은 미국 수사기관에 정보를 제공해야 하고, 미국과 행정협정을 체결한 국가라면 미국의 입장에서 그 외국 기업이 보유하고 있는 정보에 대해 정보제공을 요청할 수 있다는 것으로 기본적으로 피압수자가 전기통신 서비스 제공자인 형태를 띤다. 그런데 통상 우리가 논의하는 원격 압수·수색은 피압수자가 전기통신 서비스 제공자인 경우가 아닌 피의자 및 제3자를 피압수자로 해서 압수·수색영장을 발부받아서 그가 보유·관리하는 데이터가 원격지 서버에 있을 경우에, 압수·수색 장소에서 그 원격지 서버에 접속해서 관련 데이터를 압수·수색하는 것이 가능한지[204] 여부에 포커스가 맞춰져 있다.

미국은 우리나라와 같이 피압수자 측에 대한 참여권의 사전통지를 명시적으로 규정하고 있지는 않다.[205] 이러한 원격 압수·수색이 가능할 것인지에 관하여, 미국은 우리나라와 같이 피압수자 측에 대한 참여권의 사전통지를 명시적으로 규정하고 있지는 않지만,[206] 법무부(the Department of Justice)는 여러 관할(district)에 걸쳐있는 인터넷 범죄에 대한 수사에 장애가 되었던 연방 형사소송규칙(The Federal Rules of Criminal Procedure) Rule 41 개정을 통해 위치를 알 수 없는 컴퓨터의 원격 수색도 가능하도록 함으로써 이를 입법적으로 해결하였다. 또한 소위 'Dark Web(한정된 채널로만 접근 가능한 웹페이지)'을 이용한 범죄에 대해서는 인터넷 서비스제공자로부터 정보를 제공받는 것은 무의미하므로, 직접적 방식을 통한 원격 압수·수색의 필요성도 있어서 연방 형사소송규칙 Rule 41의 개정을 통해 가능하게 되었다고 한다.[207]

---

204) 서주연, "클라우드 컴퓨팅 환경에서의 디지털 증거 확보에 관한 논의", 전북법학 제64집 2020, 335면.
205) 박병민, "디지털 증거 압수·수색의 절차적 규제 개선방안 -참여권강화, 영장사본 교부제도 도입 등-", 2021 공동학술대회 디지털 증거 압수·수색 개선방안, 2021, 3면.
206) 박병민, 앞의 논문, 3면.

Rule 41은 치안 판사(Magistrate Judge)가 두 가지 경우 관할 구역 외에 위치한 디지털 데이터 저장매체에 대해서도 원격 수색과 전자적으로 저장된 정보의 압수 또는 복제가 가능하도록 하는 영장 발부 권한이 있다고 규정하고 있다.[208] 여기서 두 가지 경우란 ① 기술적 수단으로 저장 매체나 정보의 위치가 은닉되어 있는 경우, ② 컴퓨터 관련사기 또는 기타 범죄 수사에 있어 저장매체가 보호 대상 컴퓨터들로서 권한 없이 손상되었고, 그러한 컴퓨터들이 5개 이상의 지역에 위치하는 경우를 말한다.[209] 이 규정은 수색 대상 컴퓨터의 위치를 알 수 없는 경우 또는 수사기관이 다수 지역에 퍼져 있는 수많은 컴퓨터에 대해 수색을 하는 경우에 중요한 의미를 갖는다고 볼 수 있다.[210] 결국 피압수자가 전기통신 서비스 제공자가 아니더라도 해당 서버의 위치를 알 수 없는 경우 원격 압수·수색을 허용한 규정이라고 평가할 수 있을 것이다.

3. 유럽 사이버범죄 협약

사이버범죄의 국제형사사법공조를 위한 전치 단계에 해당하는 유럽 사이버범죄 협약(2001. 11. 23. 채택, 2004. 7. 1. 발효)은 사이버범죄관련 최초의 국제 협약으로서[211] 국가 간 공조를 통해 대응공백을 최소화하기 위한 것으로 유럽을 비롯해 현재 미국, 캐나다, 영국, 독일, 프랑스, 일본 등 66개국이 가입되어 있고[212], 조만간

207) Ahmed Ghappour, “Searching Places Unknown; Law Enforcement Jurisdiction on the Dark Web”, 69 Stanford Law Review 1075, 2017.
208) 서주연, 앞의 논문, 335면.
209) Rule 41(6).
210) Devin M. Adams, “COMMENT; The 2016 Amendments to Criminal Rule 41; National Search Warrant to Seize Cyberspace, “Particularly” Speaking”, Richmond Law Review Symposium Book volume 51, 745면.
211) 위 협약에 대한 연구들로는 이기수·민수현, “한국과 중국의 사이버범죄 형사사법공조 강화를 위한 법 개정 검토 -유럽 사이버 범죄협약을 기준으로-”,비교형사법연구 제19권 제4호, 2018, 538면.; 전현욱·이자영, “사이버범죄협약과 형사절차상 적법절차원칙: 저장된 데이터의 보존 및 일부 공개를 중심으로”, 형사정책연구 제25권 제2호, 2014, 81면.; 박희영·최호진·최성진, “사이버범죄협약 이행입법 연구”, 대검찰청연구용역보고서, 2015, 6면.; 이경렬·하건우, “유럽평의회 사이버범죄조약 가입·비준을 위한 국내 이행법률의 마련과 준비 비교”, 비교형사법연구 제19권 제4호, 2018, 503면.

더 늘어날 것이다. 위 협약 제2장 제1절은 실체적 요건으로 협약 가입국이 국내법상 범죄로 규정해야 하는 범죄 유형을 나열하고 있는데, ① 컴퓨터 데이터와 시스템의 기밀성・무결성・효용성을 침해하는 범죄(제1편),[213] ② 컴퓨터 관련 범죄(제2편),[214] ③ 콘텐츠 관련 범죄(제3편),[215] ④ 저작권 및 저작인접권 침해 관련 범죄(제4편)를 말한다.[216]

협약 제2장 제2절은 위 범죄들 및 컴퓨터 시스템을 이용한 범죄의 수사, 기타 일반 범죄의 디지털 증거 확보와 관련하여 협약 가입국이 갖추어야 할 절차를 규정하고 있고, 그 주요 내용으로는 ① 저장된 데이터의 신속한 보전(제16조), ② 트래픽 데이터[217]의 신속한 보전 및 일부의 제공(제17조), ③ 제출명령(제18조), ④ 저장된 컴퓨터 데이터의 수색과 압수(제19조) 등이 있다.

위 협약은 디지털 증거의 압수・수색과 관련하여 "① 자국의 법 집행기관이 특정 컴퓨터 시스템이나 그 일부를 수색함에 있어, ② 찾고자 하는 정보가 자국 영역 내에 있는 다른 컴퓨터 시스템 또는 그 시스템의 일부에 저장되어 있다고 믿을 만한 근거가 있고, ③ 그 정보가 처음의 시스템을 통해 합법적으로 접근 또는 이용 가능한 경우에 ④ 다른 시스템에 대한 수색이나 접근을 신속히 확대할 수 있도록 하는 입법적 조치"를 취하도록 협약 가입국에게 요구한다.[218]

---

212) <http://www.koit.co.kr/news/articleView.html?idxno=96077> 한편, 박주민 의원 2022. 04. 20. 우리나라도 유럽사이버범죄방지 협약 가입을 촉구하는 결의안을 대표 발의하였다. (2022. 06. 23. 검색)

213) 불법 접속(제2조), 불법감청(제3조), 데이터 침해(제4조), 시스템 방해(제5조), 장치 남용(제6조)을 열거하고 있다.

214) 컴퓨터 관련 위조(제7조), 컴퓨터 관련사기(제8조)를 규정한다.

215) 아동음란물 관련 범죄(제9조)이다.

216) 이에 더하여 부수적 책임 및 제재(제5편)에서는 미수・교사・방조범(제11조), 법인의 책임(제12조), 제재 및 조치(제13조)를 두고 있다.

217) 여기서 트래픽 데이터란 '통신의 발신지, 착신지, 통신 경로, 시간(GMT), 날짜, 크기, 기간, 이용한 서비스의 유형'을 말한다(협약 주석서 30).

218) 유럽 사이버범죄 방지협약 제19조(저장되어 있는 컴퓨터 데이터의 수색과 압수)
1. 각 회원국은 자국의 영토 내에서 컴퓨터 데이터가 저장될 수 있는 컴퓨터 시스템이나 컴퓨터 데이터 저장 매체를 검색하거나 접근하는 권한을 가진 권한을 부여하기 위해 필요한 입법 및 기타 조치를 취해야 한다.
2. 각 회원국은 소속 기관이 자국 영토 내의 다른 컴퓨터 시스템 또는 시스템에 의해 검색 또는 접근한 데이터가 다른 시스템으로 신속하게 확장될 수 있도록 입법 또는 기타 필요한 조치를 취해야 한다.

이러한 내용은 결국 협약 가입국에게 원격 압수·수색에 관한 의무를 부과한 것이라고 볼 수 있다.[219] 다만, '수색의 확대'에 관한 구체적인 절차나 방법을 명시하지는 않고 협약 가입국의 국내법에 위임하고 있는 것으로 해석된다.[220] 위 협약 내용 중 특히 원격 압수·수색을 허용하는 법률적 근거는 위 협약 제18조의 제출명령[221]이라고 할 수 있는데, 이 중 제18조 제1항 b호는 각 당사국에게 자국 영토 내에서 서비스 제공자가 보유 또는 관리하는 가입자 정보[222]를 제출하도록 명령할 권한을 부여하고 있다.

사이버범죄조약의 내용은 실체적 금지규정과 절차규정으로 구성되어 있는데 실체적 금지규정은 해킹범죄, 저작권침해범죄, 아동음란물범죄, 인터넷사기 등 네 가지가 주요한 내용이다. 구체적으로 컴퓨터 시스템이나 데이터에 대한 불법 접속(DDos 공격 및 해킹), 지적재산권 침해, 아동·청소년 성착취물 유포 등 인터넷에서 발생하는 여러 행위를 범죄로 규정한다. 이 조약에 가입한 국가들은 '핫라인'을 설치해 디지털 범죄에 공동으로 대응하고 있다. 범죄가 발생한 경우 서로 트래픽·데이터 자료 협조와 신속한 자료보존, 긴급상황시 도움 등을 요청할 수 있으며, 국제 공조수사를 위한 규정과 절차도 마련되어 있다.

사이버범죄방지협약 제16조[223]는 데이터저장매체와 상관없이 서비스제공자와 같

219) 이용, "디지털 증거 수집에 있어서의 협력의무", 서울대학교 법학연구소 법학연구총서 60, 2016, 228면.

220) 이인곤·강철하, "클라우드 컴퓨팅 환경에서 전자정보 압수·수색의 문제점과 개선방향", 형사법의 신동향 제54호, 2017, 331면.

221) 협약 제18조(제출명령)
1. 각 당사국은 관할 기관에게 다음 각 호의 명령을 내릴 권한을 관할 당국에 부여하기 위해 필요한 입법 조치 및 기타 조치를 취해야 한다. a. 자국 영토 내에 있는 사람이 보유 또는 관리하고 있는 컴퓨터 시스템 또는 보유 중인 컴퓨터 데이터 저장 매체에 저장된 특정 컴퓨터 데이터를 제출하도록 하는 것 b. 당사국의 영토 내 서비스 제공자가 보유 또는 관리하는 서비스와 관련된 가입자 정보를 제출하도록 하는 것

222) 협약 제18조(제출명령)
3. 여기에서의 가입자 정보는 트래픽 데이터나 콘텐츠 데이터를 제외한 서비스 사업자가 전산 데이터 또는 다른 형태로 보유한 서비스 이용자에 대한 모든 정보로서 다음 각호의 내용을 확인할 수 있는 정보를 말한다. a. 사용되는 통신 서비스의 종류, 서비스에 대해 제공되는 기술적 조치 및 서비스 이용 기간. b 가입자 신원, 주소, 전화 번호 및 기타 접속 번호, 서비스 계약 또는 약정으로 확인할 수 있는 청구 및 지불에 대한 정보. 서비스 계약 또는 약정을 통해 확인할 수 있는 통신 장치의 위치와 관련된 기타 정보.

223) 사이버범죄방지협약 제16조(저장된 컴퓨터데이터의 신속한 보전)

은 데이터보유자에 의해서 수집되어 저장되어 있는 데이터를 보호하는 것을 규정한 것으로, ‘보전’이란 데이터의 현재의 품질이나 상태를 변경시키는 모든 것으로부터 보호하는 것을 말한다.[224]

또한 본 협약은 제17조에서 트래픽 데이터의 신속한 보전 및 일부 공개와 관련하여 본 협약에서는 데이터 보전과 데이터 보존이라는 용어를 구별한다. 데이터보전이란 이미 저장된 형태로 존재하는 데이터를 보호하는 것을 의미하는 반면 데이터 보존이란 현재 생성되고 있는 데이터의 축적과 미래에 이를 소유 또는 보유하는 것을 의미한다.[225] 각 당사국은 하나 또는 둘 이상의 서비스 제공자(Service Providers)가 당해 통신의 전송과 관련되는 지에 관계없이 통신 자료를 신속히 보전하고, 당사국의 법집행기관 또는 동 기관이 지정한 개인이 서비스제공자와 통신의 전송 경로를 확인할 수 있도록 하는데 필요한 충분한 정도의 통신 자료를 신속하게 공개할 수 있도록 규정하고 있다.[226]

유럽평의회의 사이버범죄협약위원회는 이 규정에 대한 해설서[227]를 통해 원격 압

---

1. 컴퓨터시스템에 의해서 저장되어 있는 트래픽데이터를 포함하여 특정 전산정보가 분실 또는 변경될 수 있다고 믿을 만한 사유가 있는 경우에는 그 권한을 부여받은 기관이 그 자료를 신속하게 보존할 수 있도록 필요한 입법 및 그 밖의 조치를 취하여야 한다.
2. 어떤 자가 보유하거나 관리하고 있는 특정한 저장된 컴퓨터데이터를 보전하게 하는 명령을 통하여 당사국이 제1항을 실행한다면, 당사국은 필요한 만큼의 기간 동안, 최장 90일 동안 그 자가 이러한 컴퓨터데이터의 무결성을 보존·유지할 수 있도록 필요한 입법 및 그 밖의 조치를 하여야 한다.
3. 각 당사국은 국내법이 정하는 기간 동안 비밀리에 이러한 절차를 수행하기 위하여 관리인 또는 전산자료의 입수가 필요한 자에게 필요한 입법 및 그 밖의 조치를 취하여야 한다.
4. 이 조에 의한 권한과 절차는 제14조와 제15조의 규정을 따라야 한다.

224) 박희영, 앞의 논문, 49면.

225) 이용, “디지털 증거의 보전명령제도에 관한 고찰”, 법조 제64권 제12호 (통권 제711호), 2015, 14~15면.

226) 사이버범죄방지협약 제17조 - 교통 데이터의 신속한 보존 및 부분 공개
1. 각 당사자는 제16조에 따라 보존될 교통 데이터에 관하여 다음과 같은 사항을 채택해야 한다. 입법 및 기타 필요한 조치: 다음과 같은 신속한 보존을 보장한다. 트래픽 데이터는 하나 이상의 서비스 제공자가 관련되었는지 여부에 관계없이 사용할 수 있다. 해당 통신의 전송 및 충분한 양의 트래픽 데이터를 가진 당국 또는 해당 기관이 지정한 사람 서비스 공급자와 통신이 전송된 경로를 식별하는 당사자의 유능한 자에 대한 신속한 공개를 보장한다.
2. 본 조항에 언급된 권한 및 절차는 제14조 및 제15조의 적용을 받는다.

227) Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10 - Production orders for subscriber information(Article 18 Budapest Convention), T-CY(2015)16, 1 March 2017.

수·수색도 허용된다고 본다.[228] 즉, 가입자 정보를 보관하고 있는 서버가 다른 관할 지역에 있는 경우에도 서비스 제공자가 당해 정보를 보유하거나 관리하고 있다면 제18조 적용을 배제하지 않는다고 해석하고 있고, 여기서 '보유 또는 관리'라 함은 서비스 제공자의 가입자 정보에 대한 물리적인 보유는 물론, 원격지에 저장된 가입자 정보가 서비스 제공자의 관리 하에 있는 경우도 포함되는 것으로 설명하고 있다.[229] 이처럼 상호사법공조를 통한 사용자 관련 정보 요청 절차의 간소화를 통한 수사 효율성 강화, 타국 관할 서비스 제공 기업과 직접 협력을 통해 사용자 정보요청, 보존 요청, 긴급 요청 가능 등을 그 내용으로 하고 있다.

이 같은 해석의 근거로 예컨대, 제18조가 적용되는 상황에는 서비스 제공자의 본사는 특정 관할 지역 내에 두고 관련 정보들은 그 지역과는 다른 관할 지역에 저장하는 경우도 포함될 수 있고, 그 정보들은 서비스 제공자의 재량에 따라 서비스 이용자가 알지 못하거나 통제할 수 없는 상황에서 수 개의 관할 지역에 복제되어 저장되거나 각각의 관할 지역 간을 이동할 수도 있기 때문에 데이터의 위치는 관할을 결정함에 있어 결정적인 요소는 아니라는 점을 들고 있다.[230]

유럽평의회 사이버범죄방지협약(Convention on Cybercrime) 제32조는 협약당사국이 국제사법공조를 요청하지 않고도 다른 협약당사국의 영역 내에 있는 데이터에 접근할 수 있도록 하고 있는데,[231] 이에 의하면, 불특정다수인에게 공개된 경우와 데이터를 공개할 적법한 권한이 있는 자의 자발적인 동의가 있는 경우엔 다른 서버 소재국의 승인과 상관없이 데이터에 접속할 수 있고(32(a)), 만약 당사국이 데이터를 공개할 법적 권한이 있는 자에게 적법한 동의를 얻은 경우엔 자국의 영토 내 컴퓨터 시스템을 통해서 다른 당사국인 서버 소재국에 위치한 데이터에 접속하거나 자료를 받을 수 있도록 규정하고 있다(32(b)).[232]

위 규정은 역외 압수·수색이 가능하다는 것을 전제로 한 것이지만, 이런 역외

228) 2017. 6. 협약 당사국들은 클라우드 소재 디지털 증거 확보 등에 대한 제2선택의정서 초안 작업에 착수/ 2019. 12. 발표.
229) Article 18. 앞의 조약.
230) Article 18. 앞의 조약.
231) 김한균·김성은·이승현, "사이버범죄방지를 위한 국제공조방안 연구 -유럽사이버범죄방지협약을 중심으로-", 대검찰청, 2009, 43~44면.
232) Article 32.; 이순옥, 앞의 논문, 128면.

압수·수색의 경우에도 정보공개에 대해서 '적법한 권한이 없는 자' 및 '서버 소재국의 승인이 없는 경우'에 비공개된 데이터에 접근할 수 있는지에 대해서는 직접적인 규정이 없다.[233] 그러나, 사이버범죄방지협약위원회의 소위원회그룹은 사이버 공간에서의 범죄로부터 국민을 보호하기 위해 역외 압수·수색의 필요성을 강조하고 있다.[234]

즉, 위 조약 제32(b)의 이행을 위해서는 적법하게 획득한 계정정보에 의한 동의 없는 접근을 협약 당사국 내에서 제한 없이 허용하고, 관련 데이터가 어느 지역에 위치하는지 여부를 선의로 알지 못한 경우, 선의의 경우와 급박한 위험 등을 방지하기 위한 경우 등에는 동의 없는 접근을 허용하며, 데이터의 위치는 알 수 없으나, 데이터의 처분권한을 가진 자가 수색을 수행하는 국가의 영토 내에 있는 경우에는 수사기관의 수색을 허용하도록 하자는 등의 적극적인 대안을 제시하고 있다.[235]

유럽 사이버범죄협약 역시 미국의 CLOUD Act의 입법 취지와 그 맥락을 같이 하고는 있지만, 그 차이를 보면 첫째, 사이버범죄를 막기 위한 협약의 특성상 정보를 공유할 수 있는 범죄의 유형이 협약에 열거적으로 한정된 것으로 보이고, 둘째, 공유할 수 있는 정보 또한 트래픽 데이터나 콘텐츠 데이터는 제외되어서 그 범위도 제한되는 것으로 해석할 수밖에 없는 한계가 있다. 유럽에서도 한 회원국이 다른 회원국이나 EU 내에서 서비스를 제공하는 회사(SP)에 대해 직접 보전명령(European Preservation Order)과 문서제출명령(European Production Order)이 가능한 입법을 시도하고 있다고 한다.[236]

4. 기타 주요 국가의 입법례

233) 손진, "해외 서버 압수·수색에 대한 연구 -미국의 예-", 대검찰청 형사법아카데미 자료집, 2017, 11면.
234) T-CY, (Draft) elements of an Additonal Protocol to the Budapest Convention on Cybercrime regarding tranboder access to data(2013), -proposal prepared by the Ad-hoc Subgroup on tranboder access.; 이순옥, 앞의 논문, 129면.
235) 손진, 앞의 논문. 12면.
236) UNODC · CTED · IAP, 『Practical Guide for Requesting Electronice Evidence Across Borders』(e-book), 55면.

가. 영국

영국의 경찰 및 형사증거법(The Police and Criminal Evidence Act 1984, PACE83) 제19조는 제4항에서 전자정보(infomation which is stored in anyelectronic form)의 수집에 관한 조항을 두고 있다. 제19조 4항에서 경찰관은 자신이 수사한 범죄나 다른 범죄와 관련된 증거이거나, 범죄 실행의 결과물로 획득된 것이고, 이 정보의 은닉, 멸실, 변조 또는 파기를 방지하기 위하여 압수가 필요하다고 믿을 만한 합리적인 근거가 있는 경우에, 전자적 형태로 저장되고, 압수·수색 장소에 접근하여 가져갈 수 있는 형태로 만들어질 수 있고, 가시적이거나 읽을 수 있는 형태로 용이하게 만들어질 수 있는 정보를 요구할 수 있다고 규정하고 있다.

제20조는 '컴퓨터화된 정보에 대한 압수 권한 확대'라는 규정을 두고 있는데 이 섹션에 적용되는 법률에 의하여, 경찰에게 부여된 모든 압수·수색의 권한은 컴퓨터 내에 전자적 형태로 저장되어 있고, 압수 장소로부터 접근하여 가져갈 수 있는 형태로 만들어질 수 있고, 가시적이거나 읽을 수 있는 형태로 용이하게 만들어질 수 있는 정보를 요구할 수 있다고 규정하고 있다.

이와 같이 영국은 정보를 압수의 대상으로 하는 명문의 규정이 있고, 디지털 증거의 압수에 대하여 가시화를 할 수 있는 형태로 요구할 수 있다고 규정하여 해당정보의 관리자에 대하여 출력, 복제, 저장매체 자체의 제출까지 요구할 수 있음을 알 수 있다. 영국의 디지털 포렌식 절차는 The Association of Chief Police Officers(ACPO)에서 "Good PracticeGuide for Computer Based Electronic Evidence"라는 가이드를 제정하여 디지털 증거에 관한 절차에 적용하고 있다. 위 가이드는 디지털 포렌식 절차에 대하여 계획(Plan) ⇒ 수집(Capture) ⇒ 분석(Analysis) ⇒ 제출(Present)의 순으로 이루어진다고 안내하고 있다.

특히 영국은 대형 ICT기업이 없고 대부분의 ICT기업이 미국에 있기 때문에 개인정보의 국외 유출에 대해 민감하게 대응하고 있다. 영국은 원격지 압수에 대한 별도의 규정을 가지고 있지는 않지만, 유럽평의회(Council of Europe) 사이버범죄방지

협약(Convention on Cybercrime)에 가입하여 있기 때문에 이에 따른 범죄에 대한 원격지 압수가 가능하다.

즉, 영국은 경찰 및 형사증거법(Police and Criminal Evidence Act) 제19조 제4항[237]에서 디지털 데이터가 범죄수사를 위해 필요하거나 또는 범죄의 결과로 취득한 것인 경우에 그 정보에 접근이 가능한 장소에서 식별 가능한 형태로 당해 관련 데이터를 요구할 수 있다고 규정하고 있어 원격 압수·수색이 가능하다. 따라서 압수권한을 가지고 있는 경찰관이 적법하게 권한의 행사를 위해서 주거와 같은 장소에 들어간 경우에, 컴퓨터에 저장되어 있는 관련 데이터 또는 그 장소로부터 접근 가능한 데이터에 대해서는 그 형태를 불문하고 ① 그것을 취득할 수 있는 상태로, 또는 ② 가독성이 있는 형태로, ③ 가독성이 있는 형태로 쉽게 변경 가능한 상태로 제출을 할 것을 명령할 수 있다.[238]

이와 관련하여 영국 내무성 법률위원회는, 서버 관리자가 역외에 있거나, 서버 관리자는 국내에 있다 하더라도 서버는 역외에 있는 경우 수사는 한계에 부딪히게 되므로, 데이터의 물리적 장소에만 초점을 맞추는 것은 비효율적, 비현실적이라는 점을 강조하여 전기통신에 관하여는 그 정보의 물리적 저장 위치와 무관하게 일정한 요건 하에서 증거를 확보할 수 있도록 함이 상당하다는 입장이다.[239]

나. 독일

독일 형사소송법[240]은 법문상 압수의 대상(Gegenstand) 또는 인도(Herausgeben)라는 문구를 사용하고 있으나, 독일 연방 헌법재판소는 디지털 증거를 수사기관의 저장매체에 복제하여 압수하는 것도 적법한 압수방법으로 인정한 바 있다[241]. 디지털 데이터에 대한 수색에 대한 규정으로 형사소송법 제110조 제3항은 수색대상자

237) Police and Criminal Evidence Act, § 19(4)
238) 이인곤, 앞의 논문, 77면; 이윤제, “디지털 증거 압수·수색영장의 집행에 있어서 협력의 무”, 형사법연구 제24권 제2호, 한국형사법학회, 2012, 12면.
239) Law Commission, “Search Warrants”, Consultation Paper No235, 2018, 239면.
240) 독일 형사소송법 제94조(증거대상의 보전)
241) BVerhG 1, 126.

의 전자저장매체에 대한 수색은 수색대상인 데이터의 소실 우려가 있는 경우 당해 저장매체와 공간적으로 분리된 저장매체들에까지 확대될 수 있다. 조사에 중대한 의미가 있는 데이터는 이를 압수가 가능하다고 규정하고 있고, 형사소송법 제98조 a~c는 중대한 범죄에 대한 데이터 검색에 대한 규정을 도입하여, 열거된 중대한 범죄를 범하였다는 충분한 근거가 있을 경우, 데이터에 대한 비교조사를 하여 혐의자를 추적하는 조사를 할 수 있도록 규정하고 있다.

독일 형사소송법 제110조 제3항은 수색 대상인 자에 대해 필요한 경우 저장매체의 검열을 저장매체에서 도달할 수 있는 다른 저장매체로 확대할 수 있도록 규정한다. 검색대상자에 대해 수사기관이 접근한 데이터가 해외에 존재한다는 점이 나중에 알려진 경우에도 국제사법공조 절차에 따라서 요청하면 된다는 견해[242]가 있고, 수사기관의 선의만으로는 주권 침해에 해당하여 국제법 위반에 치유되지 않는다는 견해[243]도 있다.

'역외 압수·수색' 내지 '원격지 압수·수색' 및 '온라인 압수·수색'에 관해 실무에서 수권규정의 필요성이 대두돼 상당부분 법률로 규정되어 있다. 이처럼 독일은 원격지 압수·수색을 명문으로 규정하고 있는데 이는 최초의 압수·수색 대상인 컴퓨터에서 '적법하게' 접근·이용이 가능한 정보만을 대상으로 하는 것으로 국가기관에 의한 해킹이라 할 수 있는 은밀한 온라인 수색을 의미하지는 않는다.[244] 또한 독일 형사소송법 제110조 제3항은 디지털 데이터 저장매체 열람을 원격지에 있는 저장매체에까지 확장하는 것을 허용하고 있다. 이는 유럽 사이버범죄협약 제19조를 수용하여 원격 압수·수색을 법률로써 명확히 한 것이라 해석된다.[245]

협약 제19조 제4항에서 규정하고 있는 제3자에 대한 정보요구권(제3자의 협력의무)은 증인에게 적용되는 규정(형사소송법 제48조 이하[246]과 정보제공을 거부하는

242) Wabnitz/Janovsky (Hrsg), Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl., 2014, 27. Kap. Rn. 30
243) Meyer-Goßner/Schmitt, Strafprozessordnung, 61. Aufl., 2018, § 110 Rn. 7a
244) 손지영·김주석, "압수·수색 절차의 개선방안에 관한 연구", 사법정책연구원 연구보고서, 2016, 168면.
245) 이용, 앞의 책, 34면.
246) 형사소송법 제48조(증인의 소환), 제49조(연방대통령에 대한 신문), 제50조(정부각료 및 국회의원에 대한 신문), 제51조(불출석의 효과)

경우에 있어서 강제처분(형사소송법 제70조: 이유 없는 증언거부 또는 선서거부)에 의해서 가능하다. 이는 증인이 컴퓨터시스템에 대한 암호화기술, 보안체제 또는 그 밖의 접근권한에 관한 정보를 알고 있는 경우 이를 수사기관에게 제공해야 한다는 것이다. 게다가 증거수단(예컨대 암호)이 어디에 있고, 그것이 어떻게 평가되는가에 대한 정보가 질문을 통해서 확보되어야 한다. 이러한 인식을 토대로 하여 이후의 강제처분이 진행될 수 있다. 하지만 이러한 자에 대한 정보제공의무가 배제될 수 있는 자의 증인 묵비권(형사소송법 제52조 이하[247])은 협약 제15조 제1항에서 고려될 수 있다. 그리고 범죄를 저질렀다고 기소되거나 의심받는 사람이 형사상 본인에게 불리한 진술을 강요당하지 아니하는 권리를 말하는 자기부죄금지원칙에 의해서 피고인에게 그러한 정보제공의무는 부과될 수 없다.[248]

즉, 위 조항은 수색 대상인 저장매체에 대한 검열은, 검열 대상 데이터가 상실될 우려가 있는 경우 자료저장매체로부터 접근할 수 있는 한 당해 자료저장매체와 분리되어 있는 자료저장매체들에까지 넓혀질 수 있으며, 조사하는데 있어서 중요한 의미가 있는 데이터는 이를 압수할 수도 있다고 하고 있다.[249]

따라서 ① 수색 대상 정보가 원격 시스템에 존재하고, ② 수색 대상 정보 상실의 우려가 있으며, ③ 최초 접근한 시스템을 통해 원격 시스템에 정당하게 접근 가능한 경우라면 원격지 시스템에 대한 수색이 가능하게 된다.[250] 이 조항의 의미는, 수사기관은 공간적으로 떨어져 있는 전자적 데이터 저장매체까지 그 정보를 열람할 수 있을 뿐만 아니라, 그 열람을 통해서 수사상의미가 있는 정보를 발견한 때에는 그 데이터의 손실이 우려되는 등의 경우에 그 정보를 압수하는 것까지 가능하게 함으로써 원격 압수・수색을 허용하고 있다는 것이다.[251]

---

247) 형사소송법 제52조(인적 사유로 인한 증언거부권), 제53조(업무상증언거부권), 제53조a(보조자의 증언거부권), 제54조(법관과 공무원에 대한 증언허가), 제55조(정보제공거부권), 제56조(거부사유의 소명)
248) 박희영, “독일의 사이버범죄방지조약의 비준에 관한 법률(下)”, 법제, 2009, 58~59면.
249) 정대용・김기범・이상진, 앞의 논문, 64면.
250) 이인곤・강철하, 앞의 논문, 331면.
251) 박희영, 앞의 보고서, 57면.

다. 일본

일본은 우리나라와 같은 대륙법계의 법체계를 갖고 있다. 따라서 독일 법체계를 따라 유사한 편제로 법률을 규율하여 2011년 6월 형사절차법을 개정하면서 디지털 증거에 대한 절차를 갖고 있다. 즉 2011년 일본은 정보처리의 고도화 등에 대처하기 위한 형법 등의 일부 개정 법률을 통하여 디지털 증거에 관한 형사소송법 규정을 정비하면서 원격 압수・수색을 명문으로 규정하였다.[252]

우리나라의 형사소송법과 동일한 내용을 가지고 있던 개정 전 일본 형사소송법 제99조 제1항, 제2항은 개정 전 우리 형사소송법 제106조 제1항, 제2항과 같은 내용이다. 그리고 수사기관에 대해 준용규정인 제222조는 제99조 전체를 준용해서 조문상으로는 제99조의2의 제출명령도 준용이 되는 것처럼 규정되어 있었으나, 개정된 일본 형사소송법 제222조는 제99조의1만을 특정하여 준용했고, 제2항을 제외해 버렸다. 유체물에 대해 제출명령은 수사기관에 준용 되지 않는다고[253] 강조하였지만, 일본은 개정된 형사소송법에서 법원에 대한 규정인 제99조의2에서 기록명령부 압수제도를 신설[254]하고, 제110조의2에서 압수・수색영장의 집행방법으로 제출명령을 포함하게 한 뒤 제222조에서 제110조 제2항을 준용함으로써 디지털 증거에 대하여 드디어 수사기관에서도 제출명령을 인정하게 된 것이다[255].

일본 형사소송법 제99조 제1항의 ‘증거물 또는 몰수하여야 할 물건이라고 사료

252) 우지이에 히토시, “일본의 전자적 증거 압수에 관한 2011년 개정법 소개”, 형사법의 신동향 통권 제49호, 2015, 421~423면.

253) 이윤제, 앞의 논문, 15면.

254) 일본 형사소송법 제99조의2; 법원은 필요한 때에는 기록명령부압수(디지털 데이터를 보관하는 자 그 밖에 디지털 데이터를 이용하는 권한을 가지는 자에게 명령하여 필요한 디지털 데이터를 기록매체에 기록시키거나 또는 인쇄시킨 후 해당 기록매체를 압수하는 것을 말한다.)를 할 수 있다.

255) 일본 형사소송법 제110조의2; 압수하여야 하는 물건이 디지털 데이터에 관계된 기록매체인 때에는 압수영장의 집행을 하는 자는 그 압수에 대신하여 다음에 게재한 처분을 할 수 있다. 공판정에서 압수하는 경우에도 같다. ① 압수하여야 하는 기록매체에 기록된 디지털 데이터를 다른 기록매체에 복사, 인쇄하거나 또는 이전한 다음 당해 다른 기록매체를 압수하는 일. ② 압수를 받는 자에게 압수하여야 하는 기록매체에 기록된 디지털 데이터를 다름 기록매체에 복사시키거나 인쇄시키거나 또는 이전시킨 다음 당해 다른 기록매체를 압수하는 일.

되는 것’을 압수의 대상으로 명시한 규정에 의하면 압수의 대상은 당해 사건에 관련된 증거물 또는 몰수할 물건으로 사료되는 물건이므로 성질상 유체물에 한하며, 컴퓨터에 입력된 정보 그 자체는 유체물이 아니므로 압수의 대상이 되지 않는다.[256] 다만 정보가 전자기록매체에 입력되어 있는 경우나 용지에 출력되어 있는 경우 해당범죄와 내용적으로 개연성을 갖는 정보를 분별하여 압수할 수 있는 경우에는 그 부분의 정보를 출력하여 압수할 수 있고, 내용적으로 분별이 불가능한 경우에는 하드디스크, 자기디스크 또는 출력된 용지 그 자체를 압수할 수 있다고 하고 있다[257]

따라서 종래 일본의 입장은 우리 형사소송법과 마찬가지로 무체정보의 압수대상성을 부정하는 것으로 볼 수 있다. 이에 일본에서는 정보처리의 고도화에 따른 범죄에 대처하기 위하여 사이버범죄방지조약을 조약을 체결하고, 디지털 증거와 관련된「정보처리의 고도화 등에 대처하기 위한 형법 등의 일부 개정 법률」을 통하여 무체정보에 대한 압수・수색의 대상성 문제를 입법적으로 해결하였다.[258]

개정된 형사소송법 제99조 제2항 및 제110조의2에서는 디지털 데이터에 대한 압수・수색의 대상성을 인정하고, 디지털 데이터이 무체물인 정보인 점을 감안하여 구체적 압수방법을 규정하고 있다. 본 조항에 따르면 정보가 저장되어 있는 기록매체 등을 압수하는 경우 그 기록매체 등을 압수하는 대신 디지털 데이터을 ‘다른 기록매체’에 복사, 인쇄, 이전하여 그 ‘다른 기록매체’를 압수함으로서 디지털 증거를 확보할 것을 규정하고 있다.

2011년 6월 개정된 일본 형사절차법은 유체물 증거원칙을 일관되게 지키고 있다. 유체물인 저장매체를 압수의 대상으로 하는 것을 원칙으로, 복제・출력의 방법으로 정보를 압수하는 것은 예외로 하고 있으며[259] 기록명령부 압수제도를 도입[260]하여 디지털 데이터에 대한 압수절차를 마련하고 있다. 즉 압수할 물건이 디지털 데이터

256) 히라라기토키오 저・조균석 역, 일본 형사소송법, 박영사, 2012, 170면.
257) 히라라기토키오 저・조균석 역, 앞의 책, 171~172면.
258) 이경렬, “디지털정보 관련 증거의 압수・수색 규정의 도입방안 연구”, 홍익법학 제13권 제3호, 2012, 491면.
259) 일본 형사소송법 제110조의2, 앞의 조항 참조.
260) 일본 형사소송법 제99조 제2항.

에 관련된 기록매체인 경우, 압수영장을 집행하거나 공판정에서 압수하는 경우 압수할 기록매체에 기록된 디지털 데이터를 다른 기록매체에 복사 또는 인쇄하거나 옮긴 후에 그 다른 기록매체를 압수하거나, 피압수자에게 압수할 기록매체에 기록된 디지털 데이터를 다른 기록매체에 복사 또는 인쇄하거나 옮기도록 한 후 261)그 다른 기록매체를 압수하도록 하고 있는 것이다.

또한 법원은 필요한 경우 기록명령부를 압수(記録命令付差押え)를 할 수 있다고 하고 있는데 그러한 기록명령부 압수(記録命令付差押え)는 디지털 데이터 보관자나 그 밖의 디지털 데이터를 이용할 수 있는 권한을 가진 자에게 필요한 디지털 데이터를 기록매체에 기록하거나 인쇄하게 명하여 해당 기록매체를 압수하는 것을 말한다.262) 이는 일본이 '전자정보'를 압수의 대상으로 하지 않고, '매체'를 압수의 대상으로 하는 데서 비롯된 것으로, 유럽 사이버범죄협약 제18조의 제출명령에 대응하여 신설된 규정이다.263)

이어서 제107조 제2항264)은 일본도 형사소송법 제99조 제2항, 제218조에 따라 역외서버에 저장된 데이터에 대하여 압수・수색이 가능하도록 함으로써 원격 압수・수색의 문제를 입법적으로 해결하였다. 일본도 한국처럼 수사기관은 대인적 강제처분의 집행 여부에 따라 관련 없이 독립적으로 영장 없이 압수・수색을 집행하지 못하지만265) 일본 형사소송법에는 디지털 데이터의 정보매체 압수・수색과 관련된 규정이 한국에 비해 다양하고 구체적으로 상세하게 규정되어 있다.266) 우리 형사소

261) 손창현, "사이버테러 대응방안으로서의 디지털 증거 압수・수색에 대한 비교법적 고찰 -원격 압수・수색 및 제3자 보관 정보에 대한 압수・수색을 중심으로 한 정책 제언 -", 한국공안행정학회보, 제28권 제3호, 2019, 257면.

262) 정대용・김기범・권헌영・이상진, 앞의 논문, 169면.

263) 조성훈, 앞의 논문, 274면.

264) 일본 형사소송법 제107조 제2항; "제99조 제2항의 규정에 의한 처분을 할 때에는 전항의 압수장에 동항에 규정하는 사항 외에 압수할 전자계산기에 전기통신회선으로 접속해 있는 기록매체로서 그 디지털 데이터을 복사해야 할 범위를 기재해야 한다."

265) 加藤康榮, "無令状捜索差押えの許容範囲--「緊急捜索差押え」の可否を巡って" 日本法学 第76巻 第4号, 日本大学法学研究所, 2011年, 1296면.

266) 일본 형사소송법은 ① 원격 압수・수색(제99조 제2항, 제218조 제2항), ② 기록명령부차압(제99조의2, 제218조 제1항), ③ 디지털 데이터에 관한 압수의 집행방법(제110조의2, 제222조 제1항), ④ 피처분자에 대한 협력요청(제111조의2, 제222조 제1항), ⑤ 제3자에 대한 보전요청(제197조 제3항~제5항), ⑥ 디지털 데이터의 몰수에 관한 규정(제498조의2)을 2011년의 개정을 통해서 신설하였다.

송법에 없는 기록명령부차압을 통하여 디지털 증거 특성인 데이터의 대량성으로 유관정보의 선별 및 압수와 관련한 집행의 어려움을 많이 다운시킬 수 있을 것으로 예상된다.[267]

라. 러시아

러시아의 경우는 우리나라 형사소송법처럼 선별압수를 원칙으로 명시된 건 아니고, 형사소송법 제164.1조 제3항에서 정보저장매체 압수의 방법으로 정보를 복제할 수 있게 서술하고 있다.[268]

제164.1조 제1항에서는 경제범죄의 증거로 서버 등 정보저장매체를 처분할 필요가 있는 경우 매체 압수의 제한 및 그 예외 사유를 서술하고 있으며, 동조 제2항은 제1항의 예외에 해당하는 매체 압수가 이루어지는 경우 피압수자의 신청에 따라 전문가와 입회인의 참여하에 피압수자가 준비한 정보저장매체에 몰수대상인 정보저장매체 데이터를 복제할 수 있도록 규정하고 있어 피압수자에게 덜 침해적인 선별압수를 명시적으로 규정하고 있다.[269]

러시아 연방 헌법재판소는 수사기관이 검증과정에서 영장 없이 통신사실에 대한 자료나 메시지 등 대화 내용을 수집하게 되는 것은 헌법적 기본권인 통신의 자유를 침해한다는 취지의 헌법소원에 대한 판단사건에서, 법원 영장에 의해 합법적으로 압수된 스마트폰에 저장된 수사 단서를 찾기 위해 전문가 감정을 할 때 추가 영장을 받을 필요가 없다면서 절차상 청구인이 헌법적 권리가 침해되었을 경우에는 형사소송법 제125조에 따라 그 위법 여부에 대한 판단을 요청이 가능하다고 판시하고 있다.

---

267) 後藤昭＝白取祐司『新・コンメンタール刑事訴訟法』[第3版](日本評論社 丶 2018年) 233頁 °; 방경휘, “독립적 긴급 압수·수색 제도의 필요성에 관한 재고찰 -”, 숭실대학교 법학논총 제 50권, 2021, 117면.

268) 조미지・송영진, “형사절차상 디지털 증거 압수・수색 법제에 관한 비교법적 고찰 -러시아 형사소송법과의 비교를 중심으로-”, 입법과 정책, 제13권 제3호, 2021, 137면.

269) 조미지・송영진, 앞의 논문, 138면.

5. 소결

이렇듯 외국의 사례를 참고해보면 우리나라에서도 네트워크로 연결된 다른 장소의 컴퓨터에 압수·수색이 가능하게 유럽의회의 사이버범죄방지협약을 참고하여 압수·수색 법제를 개편하여 역외 압수·수색에 대한 법적 근거가 마련되어져야 한다.[270] 실무에서는 저장하고 있는 매체를 압수하거나 다른 매체에 정보를 복제하는 방법을 사용하며, 디지털 증거가 복제나 인쇄 등이 가능한 경우와 그렇지 않은 경우로 나뉘어 현실적으로 용이한 방향으로 디지털 증거에 적합한 압수·수색 절차를 마련해야 될 것이다. 클라우드 컴퓨팅 등 원격 압수·수색에 대해 각국의 입장을 보면, 영미법계나 대륙법계의 입장에는 명문으로 규정하고 있는지에 따른 차이는 있을 수 있으나 내용상 큰 차이를 발견할 수 없어 보이지만, 원격 압수·수색을 통한 디지털 증거를 확보함에 있어서 각국의 입장은 대체적으로 실효적인 입장을 취하고 있다고 볼 수 있다.

오늘날 인터넷 기술의 발전 속도에 따라 디지털 포렌식 분야에서도 원격 압수·수색이 적극적으로 인용되어져야 할 것으로 보인다. 온라인 디지털시대의 범죄는 국경이 없어 언제 어느 곳이든 일상적으로 벌어지고 있고, 범죄현장과 그 증거가 순식간에 인멸되기 일쑤이므로, 작금의 디지털 포렌식 수사는 원격 압수·수색으로 범죄현장이 신속하게 포착되어야 할 필요성이 절실한 시대적 환경적 상황에 놓여 있다. 물론 기본권이 침해되지 않고 적법절차에 따라야 하며 특히 최소 침해의 원칙과 비례의 원칙에 따라 과도하게 집행되지 않아야 함은 당연지사이다.

사이버범죄방지협약 중 제2절에서는 저장 데이터의 보존, 데이터 압수수색뿐만 아니라 제출명령 등에 관하여 규정하고 있다.[271] 디지털 증거의 확보를 위한 형사사법공조 절차의 문제점이나 이를 해결하기 위해서는 미국과 우리나라에서 논의중인 여러 문제들을 해결하기 위한 방안들을 종합적으로 고려할 때,[272] ISP(인터넷

270) 정대용·김기범·권헌영·이상진, 앞의 논문, 172면.
271) 이관희·이상진, 앞의 책, 348면.
272) 이동현, “디지털 증거의 수집 관련 국제 공조 방안 -형사사법공조 절차의 문제점과 이를 해결하기 위해 미국 실무상 논의되는 방안을 중심으로-”, 법과학의 신동향 통권 제1호, 2020, 354~355면.

서비스사업자)보관 자료에 대한 제출 절차는 제출명령으로 제도화하는 것이 보다 바람직하다. 제출명령은 그 명령을 송달을 받은 사람에게 자신이 보관하고 소지하고 있는 것으로 절차의 쟁점과 관련성 있는 문서, 물건 등을 제출하도록 하는 명령인데 미국에서는 불응하면 검사는 법원에 모욕에 의한 제재의 청구가 가능하다.[273] 즉 강제력이 인정되기 때문인데 우리 형사소송법에는 제106조 제2항에서 제출을 명할 수 있다고 규정하였으나, 제출명령에 응하지 않을 경우 별다른 제재수단이 없다.[274]

각각의 제도로 구분될 필요가 있음에도 불구하고 수사기관의 직접 집행 및 전기통신사업자[275]의 관련 증거 제출이 침해의 정도와 절차적인 측면에서 우리 법체계는 아직 이를 반영하지 못하고 있다.[276] 그러므로 우리나라도 유럽 사이버범죄방지협약상의 제출명령[277]제도와 일본의 형사소송법상 기록명령부 압수 제도처럼 정보를 갖고 있는 자에게 필요한 데이터를 기록하고 제출이 가능하도록 하는 제도를 도입할 필요성이 있다.[278] 법이 현실의 변화 속도를 쫓아가기 위해서는 해외에 나가지 않더라도 해외에 있는 서버 등에 대한 역외 압수・수색을 할 수 있어야 한다.

오늘날 국경 없는 디지털시대의 효과적 범죄수사를 위해서는 역외 디지털 정보에 대한 압수・수색에 있어 국제형사사법공조 절차를 통하는 국제협력체계가 최선의 방책인 것은 분명하다. 그러나 원격 압수・수색의 필요성이 절실한 시대적・환경적 상황에 능동적으로 대처하기 위해서는 나라마다 과학기술수준 및 국제적 이해관계가 다름으로 인한 국제형사사법공조 절차상의 비효율성을 극복하고, 신속한 정보공유도 가능할 수 있게 우리의 경우도 국제형사사법공조 절차를 거치지 않고서도 바로 서비스제공자(ISP)에게 통신한 내용에 대해 제출을 요구할 수 있는 가에

273) 연방 형사소송규칙 제17조(g); 조성훈, 앞의 책, 158~159면.
274) 조성훈, 앞의 책, 159면.
275) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 이하 정보통신망법 제2조 제2호에 따라 등록 또는 신고를 하고 전기통신역무를 제공하는 자를 의미한다. 인터넷서비스 제공자(ISP)라는 용어를 쓰기도 한다.; 조성훈, 앞의 책, 10~11면.
276) 전현욱 외, “사이버범죄의 수사 효율성 강화를 위한 법제 개선 방안 연구”, 경제인문사회연구회 협동연구 보고서, 2015, 162면.
277) Article 18;유럽 사이버범죄협약 제18조의 제출명령에 대응하여 신설된 규정이다.
278) 정대용・김기범・권헌영・이상진, 앞의 논문, 169면.

따라 법제도적 장치가 필요하다고 생각된다.

이를 위해 해외 사례를 참고하여 우리 형사소송법 제106조 제5항에 “법원은 제3항에 대하여 압수하여야 하는 물건이 국내가 아닌 국외에 디지털 데이터에 관련된 기록매체인 때에는 압수영장의 집행을 하는 자는 그 압수를 대신하여 제출을 명할 수 있다.”고 명문으로 규정하는 입법안을 제시해 보고자 한다. 다만 제출명령에 응하지 않을 경우, 즉 강제력의 인정문제와 관련해서는 타법과의 관계 및 개인정보 침해와 정부의 감시 강화 가능성에 대한 우려 등을 고려해야 하고, 설령 인정한다 하더라도 현행법상 직접강제(처벌) 규정이 가능한 것인지, 간접강제(배상)로 규정해야 하는 것인지 등의 논란이 있을 수 있으므로 이에 대해서는 좀 더 충분한 논의가 필요할 것으로 보인다.

현행 규정	개 정 안
형사소송법 제106조 (압수) ① 기재생략 ② 기재생략 ③ 기재생략 ④ 기재생략 ⑤ 신설	형사소송법 제106조 (압수) ① 기재생략 ② 기재생략 ③ 기재생략 ④ 기재생략 ⑤ 법원은 제3항에 대하여 압수하여야 하는 물건이 국내가 아닌 국외에 디지털 데이터에 관련된 기록매체인 때에는 압수영장의 집행을 하는 자는 그 압수를 대신하여 제출을 명할 수 있다.

제2절 역외 디지털 증거의 압수·수색 관련 판례

1. 서설

전자통신망이 활성화된 요즘은 시대변화에 상응하여 개인정보 유출이나 해킹 등

보안취약 요소 역시 증가하고 있다. 이에 따라 개인, 단체, 국가에서는 전자통신망 송수신시 암호화 절차를 거쳐 보안을 강화하고 있는 실정이다.

해외 서버에 저장된 e-메일에 대한 압수・수색 절차 관련하여 동일한 쟁점에 대하여 서로 다른 결론의 고등법원 판결이 나왔다. 디지털 증거와 관련하여, 국내에서 발부된 압수・수색 영장에 의해 해외 서버에 저장된 e-메일을 압수한 유사한 두개의 사건에서, 2017년 서울고등법원 제12형사부[279]와 제8형사부[280]는 서로 상반되는 판결을 내놓은 것이다.

2017노23 판결은 수사기관이 甲의 외국계 e-메일에 로그인하여 압수・수색한 행위가 압수・수색 장소 또는 대상물이 우리나라가 아닌 국외에 존재하므로 대한민국 사법관할권이 미치지 아니하여 영장의 효력이 없어서 이를 통한 증거는 증거능력이 없다고 봤으나, 2017노146 판결에서는 실제로 압수・수색 모든 과정이 사실상 국내 수색 장소에서 이루어졌으므로 역외 사법권의 침해나 국제관할 위반의 문제가 생긴다고 보기 어려워 증거능력을 인정하였다.[281]

이어진 제12형사부(2017노23 판결)의 상고심에서 대법원은 국내 영장에 기한 해외 소재 서버에 저장된 e-메일 압수를 적법한 것이라고 판단하였다. 즉, 고등법원에서는 상대국에 대해 사법관할권 침해라고 봤으나, 대법원[282]에서는 적법하게 국내에서 압수・수색 영장을 집행한 것이므로 사법관할권 침해가 아니라고 판시한 것이다.[283] 이는 미국의 마이크로소프트사건이나 Google 사건에도 중요한 쟁점이다.

고등법원 두 판결이 외국계 e-메일 계정에서 압수한 e-메일의 증거능력에 대하여 이렇게 서로 다른 결론을 내리게 된 이유는 네트워크로 연결된 e-메일 압수의 특수성 때문이다.[284] e-메일은 기존의 우편물과는 달리, 수신인이 우편물을 전달받았을 때 수신인에게 우편물에 대한 소유권 내지 점유권이 있는 것이 아니라, 서버

279) 서울고등법원 제12형사부 2017. 6. 13. 선고 2017노23 판결.
280) 서울고등법원 제8형사부 2017. 7. 5. 선고 2017노146 판결.
281) <www.lawtimes.co.kr>, 김경환, "해외 서버에 저장된 e-메일에 대한 압수・수색", 법률신문 2017년 9월 12일자 판례해설.
282) 대법원 2017. 11. 29. 선고 2017도9747 판결.
283) 이재윤・강민구, 앞의 논문, 187면.
284) 법률신문 2017년 7월 20일 4면.

에 있는 우편물을 볼 수 있는 권리와 삭제·전달 등 처분할 수 있는 권리, 그리고 특수한 이용권 내지 디지털 데이터에 대한 통제권을 가지는 것이다.

압수한 뒤에도 이용자는 다른 계정에 접속하였다가도 언제든지 메일에 로그인해서 열람할 수 있다. 압수한 후에 하는 환부의 의미도 일반 우편물과 다르므로, e-메일 압수의 특수성을 전제로, e-메일 압수의 목적과 침해되는 법익, 그리고 이용자의 e-메일에 로그인해서 압수·수색하는 방법이 과연 적법한 것인지 살펴볼 필요가 있다.[285]

2. 고등법원과 대법원 판례의 검토

가. 서울고등법원 판결의 분석

(1) 서울고등법원 제12부 2017. 6. 13. 선고 2017노23 판결

(가) 사실관계

피고인은 북한 공작원으로부터 지령과 1만8900달러의 활동비를 받았던 혐의로 국가보안법 위반으로 기소되었다. 국가정보원 수사관은 피고인의 차량에 있던 USB 안의 안티포렌식 처리가 된 파일이 있었는데 그 파일을 복호화 하였다. 그 후 중국 내 서버가 있는 시나닷컴의 피고인 e-메일 아이디와 패스워드를 취득하였다. 이후 수사기관에서는 서울중앙지방법원에 '시나닷컴의 e-메일 계정 안에 있던 편지함에 송신 및 수신이 완료되어서 저장되어 있던 모든 내용 등'을 압수하기로 하고 '한국인터넷진흥원 사무실 내 PC'를 수색할 장소로 특정하였다. 그 후 압수·수색 영장을 청구했고, 서울중앙지방법원은 피고인의 압수·수색 참여의 기회 부여를 조건으로 영장을 발부하였다. 수사기관은 한국인터넷진흥원 직원의 참여로 피고인의 e-메일 계정에 패스워드를 입력하고 로그인한 후 e-메일(북한 대남공작조

285) 이정민, 앞의 논문, 118면.

직 225국과의 메일) 15건을 빼서 출력・저장하는 방법으로 압수했다.[286]

이에 대하여 피고인은 ① 시나닷컴 서버는 대한민국의 형사재판관할권이 미치지 않아 영장의 효력이 미치지 않기에 수사관의 접속행위는 정보통신망법을 위반한 위법한 접근에 해당하고, ② 수사기관은 효력 없는 영장을 근거로 피고인의 개인정보를 수집하였는바 이는 개인정보보호법을 위반한 행위이며, ③ 외국계 e-메일 서버에 저장된 정보를 가져오기 위해 외국계 e-메일 서버 관리자의 의사에 반하여 피고인의 계정 및 패스워드를 입력한 것은 법질서 전체의 체계에 비추어 볼 때 위법한 것이므로, 결론적으로 외국계 e-메일 계정에 대한 압수・수색은 위법하고, 이를 통하여 취득한 e-메일의 내용은 증거능력이 없다고 주장하였다.[287]

(나) 판결요지

2017노23 판결에서는 형사소송법의 압수・수색은 대물적 강제처분으로, 디지털 데이터에 대한 통제권을 가지고 있는 e-메일서비스 이용자의 e-메일 계정에 대하여 접근수단인 아이디와 패스워드를 확보하였음을 기화로 그 디지털 데이터가 저장되어 있는 제3의 장소인 해외 e-메일 서비스 제공자의 서버에 대하여 압수・수색의 범위를 확장하는 것은 대물적 강제처분인 압수・수색의 효력을 아무런 근거 없이 확장한 것으로서 위법하다고 판단하였다.[288]

법원은 피압수자에 대하여 해외에 위치한 서버에 대한 압수・수색이 이루어진 것으로 파악하고 있는데, 이는 압수・수색 대상인 디지털 증거를 직접 보관하고 있는 자를 상대로 하지 않고, e-메일 서비스 이용자의 접근 수단을 이용하여 임의의 장소에서 해당 e-메일 계정에 접속하여 증거를 수집하는 방법의 압수・수색을 허용할 경우, 사실상 압수・수색의 처분을 받게 되는 e-메일 서비스 제공자의 참여를 배제한 채 압수・수색이 이루어지는 결과를[289] 낳게 하였다.[290]

---

286) 이정민, 앞의 논문, 119면.
287) 이수용・임규철, 앞의 논문, 91~92면.
288) 오경식, 김창우, “안보형사법상 증거재판주의와 자유 심증주의의 이론과 실제”, 형사법의 신동향 제70권, 2021, 194면.
289) 형사소송법 제121조, 제122조 참조.
290) 이수용・임규철, 앞의 논문, 91~92면.

그 근거로, ① 수사기관이 역외 e-메일 서비스 이용자로부터 e-메일 계정에 관한 접근수단을 확보하였음을 기화로 해당 e-메일 계정에 접근하여 자료를 확보하는 것은 형사소송법이 상정하고 있는 압수・수색의 방법은 아닌 점, ② 전기통신의 경우에는 해당 전기통신을 소지 또는 ,보관하고 있는 기관 등을 상대로 해당 전기통신에 대하여 이루어질 것을 정하고 있는 형사소송법 제107조의 규정에 저촉하는 점,[291] ③ 본 건과 같은 압수・수색을 허용한다면 압수・수색이 피고인 등의 주거지 외에서 이루어질 경우 해당 주거주 또는 간수자 등을 참여하도록 정하고 있는 형사소송법 제123조의 규정을 실질적으로 회피하는 점,[292] ④ e-메일 서비스 제공자의 참여를 배제한 채 이루어지게 됨으로써 수집된 증거의 원본성이나 무결성을 실질적으로 담보할 수 없는 점, ⑤ 형사소송법 제120조 제1항에서 '압수・수색영장의 집행에 있어서는 건정을 열거나 개봉 기타 필요한 처분을 할 수 있다'고 규정하고 있지만, 건정을 열거나 개봉하여 압수・수색하는 장소 또는 대상물이 해외에 존재하여 대한민국의 사법관할권이 미치지 아니하는 경우까지 영장의 효력이 미친다고 보기는 어렵다는 점을 들었다.

(2) 서울고등법원 제8형사부 2017. 7. 5. 선고 2017노146 판결

(가) 사실관계

피고인 등은 국가보안법 위반의 혐의로 기소되었다. 수사기관은 피고인 등의 수첩 메모에서 발견한 아이디와 패스워드를 이용하여 해당 e-메일 계정에 접속하여 범죄혐의와 관련된 파일을 빼서 디지털 포렌식 전문가로 하여금 저장하는 방법으로 압수하였다.

(나) 판결요지

291) 신도욱, "원격 압수・수색의 적법성 -해외에 존재한 서버에 저장된 이메일 압수・수색을 중심으로-", 법조 제67권 제3호, 2018, 489면.
292) 신도욱, 앞의 논문, 489면.

2017노146 판결에서는 국정원 수사관이 피고인들의 e-메일 계정에 접속한 것은 수사의 필요상 법원의 영장에 기재된 상당한 방법에 따라 채증활동을 한 것이므로, 이는 정당한 접근권한을 가지고 해당 e-메일 계정에 접속한 것에 해당한다는 점, 형사소송법 제120조 제1항에서 '압수·수색 영장의 집행에 있어서는 건정을 열거나 개봉 기타 필요한 처분을 할 수 있다' 고 규정하고 있고, 이는 검정영장을 집행하는 경우에 준용되는바, 수사관이 적법하게 알아낸 피고인들의 e-메일 아이디와 패스워드를 입력하는 것도 이러한 '기타 필요한 처분' 에 해당한다고 봄이 상당하다고 하여 해당 e-메일에 대한 압수·수색이 위법하지 않다고 판단했다.

적법하게 알아낸 아이디와 패스워드를 이용하여 법원의 영장에 기해 취득한 외국계 서버 저장 e-메일에 대한 증거능력을 인정한 것인데, 외국계 e-메일이라 하더라도 e-메일 서버 관리자의 의사는 정당한 권한을 가지고 아이디와 패스워드를 아는 자라면 세계 어디든지 접속할 수 있도록 하는 것으로 추정되므로, 법원의 영장에 기해 e-메일에 접근할 정당한 권한을 가진 국정원 수사관이 대한민국에서 e-메일에 접근했다고 하더라도 이는 어떠한 위법이 있거나 국제적인 관할권 문제가 생긴다고 볼 수 없는 것이므로 적법한 압수이며, 증거능력이 있다는 것이다.

그 근거로, ① 피고인이 역외 인터넷서비스제공자의 해외 서버에 접속하여 전자정보를 취득한 후 이를 수사기관에 임의로 제출하는 것은 법적으로 하자가 없는바, 수사기관이 피고인을 갈음하여 해외 서버에 접속·취득하여 압수·수색하는 것은 적법한 점, ② 실제 영장의 집행 과정에서 영장에 기재된 국내의 수색장소에서 해외 서버에 접속하여 e-메일 등을 취득하였는바, 역외 사법권 침해나 국제 관할위반 등의 문제가 발생한다고 보기 어려운 점, ③ 수사기관이 적법하게 알아낸 피고인들의 아이디 등을 입력하는 것은 형사소송법 제120조 제1항의 '기타 필요한 처분' 에 해당하고, 적법하게 취득한 아이디와 패스워드를 이용하여 디지털 데이터를 취득하는 것은 수단과 목적에 비추어 사회통념상 상당하므로 형사소송법 제120조 제1항의 '압수·수색영장의 집행에 필요한 처분' 에 해당한다는 점, ④ e-메일 계정의 이용자가 임의로 제3자에게 아이디와 패스워드를 알려 주어 해당 e-메일 계정을 사용하도록 할 수 있고 그것이 서비스제공자의 의사에 반하는 조치로 보기 어려운 점, ⑤ 해외 서버에 접속하여 취득한 e-메일 등의 압수 과정에서 피압수자 및

전문가 등의 참여 하에 봉인, 암호 설정, 해시값 산출 및 확인 등의 방법을 통해 동일성과 무결성을 확보할 수 있는 점을 들었다.

(3) 2017노23 판결과 2017노146 판결의 차이점

2017노23 판결과 2017노146 판결은 수사과정에서 외국계 e-메일 계정과 패스워드를 알게 된 경우, 수사기관 사무실 등에서 해외 서버에 접속하여 관련증거를 확보하겠다는 내용을 기재한 영장을 발부받아 집행하여 얻은 증거에 대한 증거능력의 유무가 문제되는 사안이었다.[293] 이는 국내 e-메일 압수・수색에서 사용해 왔던 서버자체에 대한 압수・수색이라 하지만, 제3자가 보관하는 정보를 제공해 달라는, 즉 인터넷서비스제공자에게 통신내용을 제출하라고 명령하는 통신내용 제출명령과는 구분된다.[294]

두 판결에서 사용된 역외 압수・수색은 서버에 대한 강제적 침입에 의하지 않고, e-메일 서비스 이용권을 이용하여 접근한 것이며, 개인의 프라이버시(Privacy) 침해 문제는 영장으로 해결하였다. 일반적으로 e-메일 수신자는 e-메일을 자유롭게 처리할 수 있고, 제3자의 접근을 막고 싶으면, 그 메일을 삭제하면 된다고 하였다.[295] 읽지 않은 e-메일과 읽은 e-메일은 보호정도가 다르고, 삭제된 e-메일과 삭제되지 않은 e-메일도 보호정도가 다르다. 한편, 외국계 e-메일 서버에 영장을 직접 집행하는 원격지 압수・수색에 비해서 역외 압수・수색은 이용자가 삭제해버린 메일 등에는 접근할 수 없기 때문에 프라이버시(Privacy) 침해정도는 약하다고 할 수 있겠다.[296]

두 판결에서 아이디와 패스워드를 알아낸 방법에 대해 적정성이 문제될 수 있지만, 2017노23 판결에서는 암호화된 파일을 복호화하는 과정에서, 2017노146 판결은 수첩의 메모에서 발견된 계정과 패스워드이다. 이는 진술을 강요하여 알아낸 것이

293) 이정민, 앞의 논문, 141면.
294) 이정민, 앞의 논문, 141면.
295) 이정민, 앞의 논문, 141면.
296) 이정민, 앞의 논문, 141면.

아니기 때문에 진술거부권의 문제가 없다.

그리고 아이디와 패스워드로 로그인한 행위에 대해 기망인지 여부가 문제될 소지가 있다. 이는 수사기관이 가스점검원이라고 말하고 집에 불쑥 들어간 행위를 기망으로 볼 것인가와 같은 것이라 할 수 있다.[297] 이러한 수사에 대해서는 범죄의 중대성, 증거가치의 중요성, 증거인멸의 우려, 보호하고자 하는 법익과 침해되는 법익 사이의 비례성 원칙에 따라 결정되어야 한다. 압수에서 필요한 처분은 집행보다 넓은 개념이므로 이용자 아이디로 로그인한 행위는 압수의 '필요한 처분'에 해당된다.

가장 문제가 되는 것은 외국계 e-메일함에 접근한 것이 관할 위반인지 여부이다. 원래 역외에 소재한 물건을 대상으로 압수를 하는 경우, 대한민국의 사법관할권이 적용되지 않아 형사사법공조 절차를 거치거나 관리자의 협조를 받아 물건을 제공받아야 한다. 그러나 e-메일은 네트워크로 연결되어 있고, 압수를 해도 점유의 이전은 일어나지 않는다. 즉 e-메일 이용자의 접근권한을 이용하여 서비스를 이용한 것이다. 따라서 e-메일은 유체물과 달리 장소적 제한이 의미가 없고, 그런 의미에서 수사기관이 이용자의 아이디로 로그인해 얻은 정보는 비례성의 관점에서 증거인멸의 위험성, 수색과 압수의 어려움, 긴급성 측면에서 볼 때 압수·수색에서 필요한 처분으로 얻은 증거로 볼 수 있는 것이다.[298]

이처럼 서로 다른 결론인 2017노23 판결과 2017노146 판결이 나오게 된 가장 큰 이유는 인터넷의 디지털 데이터의 특수성과 전문성에 따라 이에 대해 역외 압수·수색 등 수사기법의 허용 여부에 대한 가이드라인이 만들어져야 할 필요성이 더욱 커졌다고 볼 수 있다. 사이버 관련 법률의 가이드라인이 되는 사이버 범죄방지 조약의 국내법 이행 절차가 하루 속히 이루어지고,[299] 국제적인 공감대를 형성한 역외과의 조약체결로 외국계 e-메일에 대한 압수·수색을 가능할 수 있게 하여야 할 것이다.

297) 이정민, 앞의 논문, 147면.
298) 이정민, 앞의 논문, 142면.
299) 이정민, 앞의 논문, 146면.

(4) 판례분석

상반되는 판결이 존재하는 미국에서도 마이크로소프트 사건[300]의 경우 2016년 7월 제2순회 항소법원은 미국 정부가 아일랜드 소재 서버에 저장된 고객 e-메일 정보를 마이크로소프트에게 제출하도록 강제할 수 없다고 판단하여 영장의 집행은 법률의 불법적인 역외 적용에 해당한다고 판시하였다.[301] 하지만, 2017년 2월에 있었던 Google사건의 경우에는 펜실버니아 동부 주법원은 Google에게 해외 서버에 있는 고객의 e-메일에 대한 미국 연방수사국의 압수・수색영장에 응하라고 판단하였다. Google의 경우는 이용자도 모르는 사이에 정기적으로 이용자의 데이터를 해외의 한 데이터센터에서 다른 데이터센터로 옮기고 있으며, 이런 이동은 고객의 접근권이나 소유권을 둘러싼 이해관계를 침해하지 않는다는 점을 지적하면서 마이크로소프트 사건과 다른 결론이 가능하다고 보았던 것이다.

본 건은 미국의 사안과 비교하여, 압수・수색대상인 e-메일이 해외 서버에 존재한다는 점은 유사하나, 미국 사안은 e-메일서비스 제공자를 통하여 e-메일을 압수・수색하고자 한 반면, 서울고등법원의 두 판결은 이미 파악한 이용자의 아이디와 패스워드를 이용하여 압수・수색하는 점이 서로 다르게 해석을 하고 있다.

첫째, 이와 관련하여 직접적인 적용 조문인 형사소송법 제107조에 대하여, 2017노23 판결은, 압수는 해당 전기통신을 소지 또는 보관하고 있는 기관 등을 상대로 이루어져야 하는 것인바, 이와 같이 e-메일 서비스 제공자를 상대로 하지 않은 압수는 위법하다고 본 반면, 2017노146 판결은 피고인이 스스로 아이디 등을 입력하여 e-메일을 취득하여 임의로 제출하는 것이 가능하다면 본 건과 같이 수사기관이 전문가 참여하에 아이디 등을 입력하여 e-메일을 취득하는 것도 법적으로 하자가 없다고 보았다.

---

300) '미국 정부 vs 마이크로소프트' 사건인 이 재판은 2013년의 마약 수사가 발단이 되었는데, 수사를 하던 경찰이 마이크로소프트에 단서가 있을 것으로 추정된 e-메일 정보를 요구하였고, 수색영장을 받은 마이크로소프트는 서버에 저장돼 있던 관련 e-메일 정보를 경찰에 제출하였다. 하지만 아일랜드 서버에 저장돼 있는 e-메일 정보는 제출을 거부하였다. 수색대상 메일 중 일부가 해외 서버에 저장돼 있기 때문이다. 그러자 사법당국이 마이크로소프트를 제소했다. 1심 법원은 미국 정부 편을 들어줬지만 이 판결은 항소심에서 뒤집혔다.

301) 김재윤, 앞의 논문, 152면.

둘째, 역외 사법권 침해나 국제 관할위반 등에 대하여, 2017노23 판결은, 압수·수색은 대물적 강제처분이므로 압수·대상인 e-메일이 해외의 서버에 존재하는 경우 대한민국의 사법관할권이 미치지 않는다고 본 반면, 2017노146 판결은 온라인을 통해 해당 해외 서버에 접속하여 e-메일 등을 취득하는 등 전 과정이 국내의 수색 장소에서 이루어졌으므로 역외 사법권 침해 등의 문제가 발생한다고 보기 어렵다고 보았다.

셋째, 수사기관이 피고인의 아이디와 패스워드를 이용하여 e-메일을 취득하는 것이 형사소송법 제120조 제1항의 '건정을 열거나 개봉 기타 필요한 처분'에 해당하는지에 대하여, 2017노23 판결은 건정을 열거나 개봉하여 압수·수색 하는 장소 내지 대상물이 해외에 존재하여 대한민국의 사법관할권이 미치지 아니하는 해외 e-메일서비스 제공자의 역외서버에 대하여 까지 영장의 효력이 미친다고 보기는 어렵다고 본 반면, 2017노146 판결은 영장집행의 목적을 달성하기 위해서 최소한의 필요조치로서 그 수단과 목적에 비추어 사회통념상 상당하므로 형사소송법 제120조 제1항에 해당한다고 보았다.

넷째, 증거의 원본성·무결성 담보에 대하여, 2017노23 판결은 e-메일서비스 제공자의 참여를 배제한 채 이루어졌는바 원본성과 무결성을 실질적으로 담보할 수 없다고 본 반면, 2017노146 판결은 압수 과정에서 피압수자 및 전문가 등의 참여하에 봉인, 암호 설정, 해시값 산출 및 확인 등의 방법을 통해 동일성과 무결성을 충분히 확보할 수 있다고 보았다.

다섯째, 개인정보보호법 또는 정보통신망법 위반에 대하여, 2017노23 판결은 명시적인 판단을 하지는 않았다. 그러나 2017노146 판결에서는 임의로 제3자에게 e-메일 아이디 등을 알려 주어 e-메일 계정을 사용하도록 하는 것이 꼭 서비스제공자의 의사에 반하는 행위라고 보기 어려우므로 영장을 통하여 정당하게 접근 권한을 부여받은 수사기관(제3자)이 서버에 접속하는 것이 위법하다고 단정할 수 없다고 판단하였다.

2017노23 판결은 형사소송법 제107조 등의 조문에 보다 충실하게 법해석을 했지만, 오늘날 IT 현실에서는 2017노146 판결이 더 부합한다고 생각한다. 특히 형사소송법 제107조는 압수 처분의 상대방을 규정하는 것이 아니라 단지 압수물을 규정

한 것이고, 압수 처분의 상대방은 IT 상황에 따라 달라질 수 있다고 유연하게 해석할 여지도 있다.[302]

나. 대법원 2017. 11. 29. 선고 2017도9747 판결

(1) 판시사항

이 사건의 판시사항은, 피의자의 e-메일 계정에 대해 접근권한에 갈음해서 발부받은 압수·수색영장에 따라 원격지의 저장매체에 적법하게 접속하여 내려 받거나 현출된 디지털 데이터를 대상으로 하여 범죄 혐의사실과 관련부분에 대하여 압수·수색하는 것이 허용될 지 여부(적극)와, 형사소송법 제120조 제1항에서 정한 '압수·수색영장의 집행에 필요한 처분'에 해당할 지 여부(적극), 그리고 이러한 법리는 원격지의 저장매체가 국외에 있는 경우라도 마찬가지로 적용되는지 여부(적극)이다.

(2) 판결요지

인터넷서비스이용자는 인터넷서비스를 이용하여 개설한 e-메일 계정과 관련 서버에 대한 접속권한을 갖고, e-메일 등 디지털 데이터에 관한 작성 및 수정또는 열람이나 관리 등 처분권한을 가지며, 디지털 데이터의 내용에 관해 사생활의 비밀과 자유 등의 권리보호이익을 가지는 주체로서 해당 디지털 데이터의 소유자 내지 소지자라고 할 수 있다. 수사기관이 피의자의 컴퓨터 등 정보처리장치 내에 저장되어 있는 e-메일 등 디지털 데이터를 압수·수색하는 것은 디지털 데이터의 소유자 내지 소지자를 상대로 해당 디지털 데이터를 압수·수색하는 대물적 강제처분으로 형사소송법의 해석상 허용된다.

---

302) <https://blog.naver.com/humill/222675234148> 법률신문- 해외 서버에 저장된 이메일(E-Mail)에 대한 압수·수색, (2022. 03. 17. 뉴스검색)

수색행위는 원격지의 저장매체에서 수색장소에 있는 정보처리장치로 내려 받거나 현출된 디지털 데이터에 대하여 위 정보처리장치를 이용하여 이루어지고, 압수행위는 위 정보처리장치에 존재하는 디지털 데이터를 대상으로 그 범위를 정하여 이를 출력 또는 복제하는 방법으로 이루어지므로, 수색에서 압수에 이르는 일련의 과정까지 모두 압수·수색영장에 기재된 장소에서 행해지기 때문에, 그 수단과 목적에 비추어 사회통념상 타당하다고 인정되는 대물적 강제처분행위로서 허용되며, 압수·수색영장의 집행에 필요한 처분에 해당한다.

(3) 판례분석

그동안 계속해서 e-메일 압수는 인터넷서비스 제공자를 대상으로 이루어지는 경우가 많았지만, 외국계 제공자에 대하여는 영장의 집행이 용이하지 않을 뿐만 아니라 재판권의 문제까지 있다. 대상판결은 수사기관이 적법하게 취득한 인터넷서비스 이용자의 e-메일 주소와 암호를 이용하여 한국인터넷진흥원의 PC에서 이용자의 중국 e-메일 계정에 접속한 뒤 화면캡쳐나 내려받기의 방법으로 디지털 데이터를 압수·수색한 사안에 대한 것으로서, 원격 압수·수색과 역외 압수·수색이라는 두 가지 문제가 함께 있다.

대상판결은, 이용자는 디지털 데이터의 소유자나 소지자로서 압수·수색의 대상자가 되고, 이용자의 접근권한에 갈음하여 발부받은 영장에 따라 통상적인 방법으로 원격지 서버에 접속하여 압수·수색하는 것은 제공자의 의사에 반하지 아니하며, 압수·수색장소도 단말기가 있는 한국인터넷진흥원이라는 점을 들어 원격 압수·수색이 적법하다고 하면서, 원격지 서버가 국외에 있는 경우라도 달리 볼 것이 아니어서 역외 압수·수색도 적법하다고 하였다.

즉, 인터넷 서비스 이용자는 인터넷 서비스 제공자와 체결한 서비스 이용계약에 따라 그 인터넷 서비스를 이용하여 개설한 e-메일 계정과 관련 서버에 대한 접속권한을 가지고, 해당 e-메일 계정에서 생성한 e-메일 등 디지털 데이터에 관한 작성·수정·열람·관리 등의 처분권한을 갖고 있고, 디지털 데이터의 내용에 관하여 사생활의 비밀과 자유 등의 권리보호이익을 가지는 주체로서 해당 디지털 데이터

의 소유자 내지 소지자라고 할 수 있어서 인터넷 서비스 제공자는 서비스 이용약관에 따라 디지털 데이터가 저장된 서버의 유지·관리책임을 부담하고, 해당 서버 접속을 위해 입력된 아이디와 패스워드 등이 인터넷 서비스 이용자가 등록한 것과 일치하면 접속하려는 자가 인터넷 서비스 이용자인지 여부를 확인하지 아니하고 접속을 허용하여 해당 디지털 데이터를 정보통신망으로 연결되어 있는 컴퓨터 등 다른 정보처리장치로 이전, 복제 등을 할 수 있도록 하는 것이 일반적이므로, 수사기관이 인터넷 서비스 이용자인 피의자를 상대로 피의자의 컴퓨터 등 정보처리장치 내에 저장되어 있는 e-메일 등 디지털 데이터를 압수·수색하는 것은 디지털 데이터의 소유자 내지 소지자를 상대로 해당 디지털 데이터를 압수·수색하는 대물적 강제처분으로 형사소송법의 해석상 허용된다고 한 것이다.

이 사건에서 대법원은 두 가지 중요한 지적을 하고 있는데, 첫째, 원격 압수·수색이 우리 형사소송법 하에서 당연히 인정된다는 점을 재확인하였다는 점이다. 즉, 형사소송법 제109조 제1항, 제114조 제1항에서 영장에 수색할 장소를 특정하도록 한 취지와 정보통신망으로 연결되어 있는 한 정보처리장치 또는 저장매체 간 이전, 복제가 용이한 디지털 데이터의 특성 등에 비추어, 수색 장소에 있는 정보처리장치를 이용하여 정보통신망으로 연결된 원격지의 저장매체에 접속하는 것이 형사소송법의 규정에 위반하여 압수·수색영장에서 허용한 집행의 장소적 범위를 확대하는 것이라고 볼 수 없다고 하였다.

둘째로는 이와 같이 수사기관이 획득한 e-메일 계정 아이디와 패스워드를 입력하여 실행되는 원격 압수·수색을 형사소송법 제120조 제1항의 '기타 필요한 처분'으로 해석하고 있다는 점이다. 즉, 대법원은 피의자의 e-메일 계정에 대한 접근권한에 갈음하여 발부받은 압수·수색영장에 따라 원격지의 저장매체에 적법하게 접속하여 내려 받거나 현출된 디지털 데이터를 대상으로 하여 범죄 혐의사실과 관련된 부분에 대하여 압수·수색하는 것은, 압수·수색영장의 집행을 원활하고 적정하게 행하기 위하여 필요한 최소한도의 범위 내에서 이루어지며 그 수단과 목적에 비추어 사회통념상 타당하다고 인정되는 대물적 강제처분 행위로서 허용되며, 형사소송법 제120조 제1항에서 정한 압수·수색영장의 집행에 필요한 처분에 해당한다고 하여 원격 압수·수색이 우리 형사소송법 규정 해석으로 가능하다고

하였다.

다. 항소심과 대법원 판결의 주된 차이점

두 판결의 가장 큰 차이점은 수색행위를 해외 서버로 볼 것인지 아니면 실제 수사기관의 수색행위가 이루어지는 디지털 데이터를 다운로드 받아 저장한 PC로 볼 것인지의 문제와, 피압수자를 해당 정보를 보관 또는 저장하고 있는 ISP로 볼 것인지 아니면 정보의 소유 또는 소지자인 피의자로 볼 것인지의 문제이다.[303]

이에 대하여 항소심 법원은 e-메일이 저장된 시나닷컴의 서버를 수색장소를 보고, 피압수자를 정보의 보관자인 시나닷컴라고 보아 시나닷컴에게 참여의 기회를 배제한 것을 절차적 위법으로 보았다면, 대법원은 실질적으로 수색행위가 이루어진 해당 PC에서 수색행위가 이루어진 것으로 보고 정보의 소유자인 피의자를 피압수자로 보아 절차의 적법성을 판단하였다. 대법원의 이러한 태도는 수색장소를 데이터의 소재지인 미국으로 볼 경우에는 대한민국 법원이 발부한 압수·수색영장의 효력이 미국에까지 미치는지의 여부 즉 사법관할권의 문제가 발생하는 반면에, 수색장소를 데이터를 다운로드 받은 컴퓨터로 봤을 경우라면 이러한 문제가 발생하지 않는다는 점을 고려한 것으로 보인다.

3. 소결

인터넷서비스제공자(ISP)에 대하여 직접 디지털 관련데이터 제출을 요구하는 경우의 판례의 태도는, 결국 원격 압수·수색은 현행 형사소송법하에서도 원칙적으로는 허용된다고 보고 있지만, 그 원격지 서버에 정당한 접근 권한에 의해 접속하였을 것을 전제로 하고 있는 것으로 해석상 인정된다는 입장인 것이다. 다만, 모든 형태의 역외 압수·수색에 대해 허용하는 것이 아니며, 수사기관이 적법하게 취득하게 된 계정정보를 이용한 서버에 접속하는 경우에 한에서만 적법하다고 판시하

303) 이순옥, 앞의 논문, 124면.

고 있다.

마이크로소프트(MS)사건을 계기로 등장한 클라우드 법도 관련 정보를 보관하는 장소와 상관없이 영장을 집행이 가능하게 저장통신법을 개정하였으나 수색의 법적 위치를 관련정보의 위치를 기준으로 할 건지 관련 정보 장소를 기준으로 할 것인지 명확하지 않다.[304] 마이크로소프트 사건의 항소심 법원은 정보저장장소를 기준으로 역외 적용 여부를 판단했고, 구글 사건은 정보접근 장소를 기준으로 해서 명확한 차이를 보이고 있다.[305]

일본・독일・프랑스 형소법은 원격 압수를 허용하고 있다. 역외 압수는 유럽사이버범죄 조약이 이용자의 적법하고 자발적인 동의를 전제로 허용하고 있다. 특히 독일과 일본은 형사소송법에 원격 압수・수색을 명문으로 규정하고 있다. 독일 형사소송법 제110조 제3항은 공간적으로 분리된 저장매체까지 접속할 수 있는 한 수색이 확대될 수 있으며, 이를 통해 발견된 정보를 압수할 수 있다고 규정하고 있다. 한편 일본에서는 전기통신회선을 통한 데이터저장매체로부터의 압수 관련 규정에는 형사소송법 제99조 제2항, 제218조 제2항이 있다.[306] 이렇게 디지털 증거와 관련되어 적법절차원칙의 준수 및 증거능력 등과 관련하여 실무와 이론은 논의를 하고 있지만, 원격 압수・수색이 허용되는지 여부에 관하여 우리나라의 경우 원격 압수・수색의 문제는 오로지 판례가 큰 영향을 주고 있다.

304) 조성훈, 앞의 책, 34~35면.
305) 조성훈, 앞의 책, 35면.
306) 전현욱・윤지영, “디지털 증거 확보를 위한 수사상 온라인 수색제도 도입 방안에 대한 연구”, 한국형사정책연구원, 2012, 44면.; 전현욱 외, 앞의 보고서, 260면.

제5장 역외 디지털 증거의 압수·수색 적법성 확보방안

제1절 역외 디지털 증거 압수·수색의 특성과 허용성

1. 현황 및 평가

유체물은 압수의 의미가 점유의 이전을 의미하지만 e-메일 내용을 네트워크로 연결되어 있고 압수 이후에도 여전히 서버에 존재하고 있어 유체물에 관한 사법관할권의 적용과 동일하게 판단할 필요는 없다. 사법관할권의 의미 역시 네트워크 시대로의 변화에 맞추어 해석될 필요가 있으며 실질적인 관할권 침해의 위험성이 없는 범위 내에서는 유연한 해석이 가능할 것이다. 역외 e-메일 서비스 제공자에게 접근 권한을 요구하거나 저장 정보의 제출을 명하는 압수·수색의 유형이 아니므로 역외 e-메일 서비스 제공자는 이러한 접근을 허용할 것인지 여부에 한하여 이해관계가 있다고 보면 될 것이다. 이와 관련해서는 현금카드(결제수단)에 관한 대법원 판례의 논지를 원용해 볼 수 있다.[307]

ISP(Information Strategy Planning)[308]가 아이디 및 패스워드 등 계정 데이터를 가진 자 또는 처분권한을 가진 자 및 형식적 접근권한을 가진 자가 서비스를 이용가능하게 할 수 있도록 허용하고 실질적인 권한 유무를 심사하지 않는 경우, 즉 외관상 적법한 접근 및 처분권한을 가진 자가 서비스를 이용하는 경우에는 서비스 제공자의 의사에 반하지 않는다고 보아야 할 것이다.[309]

역외 e-메일 서비스 제공자의 의사는 형식적으로 접근권한을 가진 자에게 접근

307) 대법원의 '현금카드 소유자를 협박하여 현금을 절취한 것이라 하여 따로 절도죄로 처단할 수는 없다'고 본 판례; 대법원 1996. 9. 20. 선고 95도1728 판결; 대법원 2005. 9. 30. 선고 2005도5869 판결.

308) ISP(정보전략기획)란 인터넷 전용 신용카드 인증 및 결제서비스 회원이 전자상거래를 이용할 때 신용카드 번호, 패스워드 등을 입력함으로써 발생할 수 있는 개인정보 유출 가능성을 원천적으로 차단할 수 있는 인터넷 전용 신용카드 인증 및 결제서비스를 말한다.

309) 이순옥, 앞의 논문, 136면.

을 허용하는 것이므로 역외 수색이라 하여 이를 달리 볼 이유는 없다. 따라서 강제처분의 필요성과 비례성에 근거하여 역외 계정의 e-메일에 대한 확보가 필요한 경우, 영장을 발부받은 상태에서 접근권한을 이용한 e-메일 압수·수색은 허용되는 것으로 봄이 타당하다. 적법절차의 문제와 관련하여, 피압수자 등에 대한 사전 통지 등에 있어 그 범위를 확대하여 절차적 신뢰성을 제고하는 방안도 생각해 볼 수 있는데, 이는 실제 정보주체인 피의자를 포함시키는 방안이다.

최근 법원은 디지털 데이터의 경우 물리적으로 압수·수색을 받는 자, 즉 ISP를 피 압수자로 보지 않고, 정보의 소유자를 피압수자로 보는 경향이 있다. '세월호 참사 추모 침묵행진'을 기획한 용혜인[310]을 집회 및 시위에 관한 법률 위반 등으로 수사하면서 위 사람의 카카오톡 대화내용을 압수하였는데, 용혜인은 수사기관이 압수·수색 당시 카카오톡을 상대로 압수·수색영장 원본을 제시하지 않았고 정보주체인 자신에게 압수·수색의 사전 통보도 하지 않았기 때문에 위법한 압수·수색에 해당한다고 하였다. 그리하여 당해 압수·수색에 대한 취소를 구하는 준항고를 제기하였고, 서울중앙지방법원에서는 사전에 압류·수색을 통보할 필요가 없는 긴급한 사정이 없는 것은 물론 정보주체인 피의자에게도 참여권이 보장되지 않아 위법하다고 하여 압수·수색을 취소한 사건(서울중앙지방법원 2016. 2. 18. 2015보6 결정, 준항고 인용)이 있다.

이 사건 결정은 준항고 법원이 '수사기관의 수사의 필요성'과 '국민의 기본권, 즉 개인의 사생활 및 통신의 자유를 보장할 필요성'을 비교·형량하여 수사기관의 증거수집 과정에서 영장주의 등 절차의 적법성이 강조되고, 국민의 기본권 보장에 더 중점을 둔 결정이라고 할 것이다. 또한 수사기관이 압수·수색 집행과정에서 피의자에게 통지하지 아니하여 피의자 및 변호인 참여권을 침해하여 위법하게 된 이상

310) 용혜인(龍慧仁, 1990년 4월 12일~)은 대한민국의 정치인이자, 국회의원, 사회운동가로, 세월호 침몰 사고가 있고 며칠 뒤인 2014년 4월 28일 안산 단원고등학교 학생과 교사가 포함된 세월호 참사의 희생자를 추모하기 위해 〈가만히 있으라〉 침묵행진을 제안했다. 2014년 5월 18일, 6월 10일, 가만히 있으라 침묵행진 도중 경찰에 연행되었는데, 수사 과정에서 경찰이 용혜인의 카카오톡 메신저 대화내용을 압수·수색하였다. 경찰은 5월 10일부터 21일까지 열흘에 이르는 카카오톡 대화 내용과 대화 상대방의 개인정보, 주고받은 사진, 동영상 일체를 압수·수색 내용에 포함시켰다. 〈https://ko.wikipedia.org/wiki/%EC%9A%A9%ED%98%9C%EC%9D%B8〉 위키백과, (2022. 06. 30.검색)

압수・수색 영장집행 과정에서 원본의 제시 유무, 압수물 목록 교부 유무, 피의사실과의 관련성 등 나머지 주장에 대해 살펴 볼 필요 없이 이 사건 압수・수색의 취소는 면할 수 없다는 준항고 법원의 결정 내용에 주목할 필요가 있다.[311]

결국 이 사건 준항고 법원은 수사기관이 영장집행 등 강제수사 과정에서 법규에 규정된 한 가지 절차라도 준수하지 아니하면 위법한 법집행이 된다는 것을 분명히 밝힌 것으로, 앞으로 메신저 뿐만 아니라 포털, 앱 등 의 압수・수색에 있어서도 적법기준을 지키지 않은 수사는 재판에서 효력을 인정받기는 어려워 향후 수사기관이 압수・수색 영장 집행 등 강제수사를 할 경우 반드시 적법절차를 준수해야 한다는 것을 강조한 것이다.

최근 SNS(사회관계망 서비스) 및 포털사이트를 범죄에 이용하는 경우가 빈번해지고 있다. 따라서 최근 범죄의 경향에 맞게 압수・수색 영장집행 절차 규정을 세분화하는 등 이를 재정비할 필요가 있다. 앞 사건처럼 정보의 ISP를 피압수자로 보게 된다면, 정보주체의 경우 참여권 등을 행사할 수 없게 된다.[312] 절차의 명확성을 위해 이러한 경우 피압수자를 누구로 볼 것인지에 대하여 궁극적으로는 입법적 해결이 타당할 것이다.

또한 준항고 법원이 압수・수색 영장 집행의 절차 요건 중 한 가지의 요건이라도 갖추지 못하면 위법하다는 결정취지에 따라 향후 수사의 필요성뿐만 아니라 개인의 사생활보호 및 통신의 자유보호라는 국민의 기본권이 침해되지 않도록 사회관계망 서비스 및 포털사이트에 대한 압수・수색영장을 집행함에 있어 더욱 신중한 집행 절차를 진행하여야 할 것이다.

2. 개선방향

가. 원격 압수・수색 관련 규정 체계화

311) <http://awtimes.co.kr> 이태한, 판례해설 -카카오톡 서버에 대한 압수・수색 취소- (2022. 06. 10. 검색)
312) 이순옥, 앞의 논문, 140면.

(1) '증거'의 개념에 대한 패러다임 변화

그동안 우리나라의 새로운 증거 유형인 디지털 증거에 대하여 기존의 압수·수색 관련 규정에 별도의 조항 하나(형사소송법 제106조 제3항)를 추가하는 입법으로 대처하였다. 그러나 현행 형사소송법은 압수·수색의 목적물을 정보저장매체로 규정하고 있어 '정보' 그 자체에 대한 압수·수색이라는 개념조차 확립되지 않은 상황이다. 또한 형사소송법의 대원칙인 '적법절차의 원칙'을 보장하기 위한 각종 절차 규정이 유체물을 전제로 한 것이어서 법률의 해석만으로는 현실에 맞는 수사 실무 운영에 한계가 있다.

특히 압수·수색의 목적물이 존재하는 장소가 아닌 다른 장소에서 이루어 질 수 있고 정보 저장 서버의 관리자의 관여가 전혀 없이 이루어질 수 있는 e-메일의 압수·수색은 그 특성에 맞는 법적 규정이 마련되어야 한다. 따라서 현행 압수·수색 규정을 기본으로 하여 몇 가지 사항에 대하여 추가 변경하는 방식의 개정이 아닌 디지털 증거를 대상으로 한 별도의 규정 체계를 새롭게 정립할 필요가 있다.

(2) 디지털 데이터의 압수·수색 대상성 명시

형사소송법 제106조 제3항은 디지털 증거의 압수·수색 대상을 정보저장매체로 적시하고 있으나 '디지털 데이터' 그 자체를 압수·수색의 대상으로 보아 압수·수색의 물리적 장소라는 개념적 한계를 벗어날 필요가 있다.[313]

(3) 역외 압수·수색제도 도입

오늘날 수사실무에서 역외 압수·수색의 필요성은 날로 더 커져가고 있으며 수사의 비례성 측면에서도 일정 범위의 역외 압수·수색을 허용하는 방안이 필요하

313) 전현욱, 앞의 책, 403면.

다. 구체적으로 우리 형사소송법이 인정하는 강제수사 방법으로 어느 범위까지를 인정할 것이며 어떤 방법까지를 허용할 것인지에 관한 입법적 결단이 필요하다.

(4) 네트워크 환경을 고려한 영장 집행 절차 마련

현재 영장의 제시나 당사자 등의 참여에 관한 조문과는 별도로 네트워크 환경을 전제하여 영장 집행 절차를 규정할 필요가 있다. 집행과 필요한 처분(제120조), 영장 집행시의 책임자 참여(제123조), 야간집행 제한 규정(제125조) 등이 특히 클라우드 환경을 반영하여 조정되어야 한다. 특히, 당사자와 책임자의 참여가 동일성 및 무결성 확보의 측면에서도 중요한 역할을 하는 바, 디지털 포렌식의 전문성을 갖춘 공정성 있는 전문가의 참여를 고려하여야 할 것이다.

나. 수사실무를 위한 가이드라인 및 수사기관 관련 규정의 개정

(1) 실무 지침이 될 수 있는 가이드라인 또는 관련 규정의 정비

법률의 개정이 이루어지기 전이라도 판례에 의하여 인정된 역외 압수·수색으로 얻은 증거의 증거능력을 확보할 필요가 있다. 가이드라인을 제정하기 위해서는 수사현장에 대한 정확한 실태진단이 필요한데 현재 어떤 방식으로 디지털 증거가 수집되며 처리되고 있는지, 또한 일련의 절차에 애로사항은 무엇인지, 실태를 정확하게 진단해야 할 것이다.[314]

(2) 동일성 및 무결성 확보 방안의 다양화

역외 압수·수색에서 동일성 및 무결성은 기존의 해시값 추출만으로는 확보되기

314) 권양섭, “경찰의 디지털 증거 수집 및 가이드라인 제정을 위한 실태조사 연구”, 원광법학 제33권 제2호, 2017, 70면.

어려운 측면이 있으므로 영상 녹화의 방법 등 실무에서 활용 가능한 방법을 제시하여 준수하게 할 필요가 있다. 예를 들어 검찰청 내규과 경찰청 훈령 모두 압수·수색에 있어서 무결성 확보방안으로 해시값의 추출을 중심으로 제시하고 있으며 참여자의 경우도 피의자와 변호인의 참여권 보장을 중심으로 규정하고 있다.

제2절 역외 디지털 증거의 압수·수색과 영장주의

1. 압수·수색 영장주의의 요건

압수·수색영장은 대물적 강제처분의 일종으로, 수사기관이 증거물 또는 몰수해야 할 것으로 판단되는 물건을 수집·확보하기 위한 것으로, 검사의 청구에 의해 지방법원 판사가 발부받도록 하고 있다. 압수·수색영장 제도의 요건에는 피고인의 성명·죄명·압수하려고 하는 물건·수색하려고 하는 장소 및 신체와 물건 또는 발부 연월일과 유효기간 등 관련된 기타 사항을 기재하여야 하며, 발부일로부터 7일까지 유효하다(법 제114). 만약, 수사기관이 발부된 영장을 근거로 하여, 압수·수색을 집행하는 과정에서 영장에 적힌 범죄 혐의와 다른 별도의 범죄 혐의와 관련된 증거 등을 발견한 경우에는, 집행을 정지하고 별도로 법원으로부터 영장을 발부받아야 한다.[315]

최근 수사기관이 조사 과정에서 피의자에게 스마트폰이나 PC에 저장된 문자메시지 및 카카오톡, 사진, 동영상 등을 임의제출을 요구하거나 압수·수색하는 경우가 많아졌다. 스마트폰 PC 등 디지털 증거 압수·수색과 관련하여 형사소송법 제106조 제3항에 “압수의 목적물이 컴퓨터용 디스크 그밖에 이와 비슷한 정보 저장매체인 경우에는 기억된 정보의 범위를 정하여 출력 복제하여 제출받아야 한다.“ 고 규정되어 있어 원칙적으로 수사기관은 당해 범죄 혐의와 관련성이 있는 부분만을 출력하거나 복제하는 방법으로 디지털 증거에 대한 압수 절차를 진행해야 한다.

315) 방경휘, 앞의 논문, 126면.

특히 검찰이 삭제하지 않고 저장해 놓고 있는 디지털 데이터 데이터는 위법적인 별건 수사로 연결될 수 있다. 이 데이터에는 수사 중인 범죄 혐의와 관련없는 정보들까지 들어 있기 때문이다. 민감한 사생활 정보까지 검찰의 손에 넘어가게 되면 수사나 재판 과정에서 피의자가 겁을 먹고 방어권을 제대로 행사하지 못하게 된다. 수사기관이 해당 시스템의 패스워드를 알지 못하는 경우 또는 저장정보에 암호가 걸린 경우는 ISP가 패스워드 또는 암호해제조치를 하도록 의무를 부과할 필요가 있다지만, 피의자에게 패스워드를 제출 의무를 부과할 경우 진술거부권 침해가 될 수 있다.[316]

한편, 스마트폰은 인터넷이 결합된 통신수단의 기능을 가지고 있다. 스마트폰으로 주고받는 실시간 대화내용에 대한 감청과 패킷감청 등의 통신제한조치와 기지국 수사, 과거 및 장래의 위치정보수집 등 통신사실 확인 자료에 대한 제공요청은 새로운 수사기법으로 활용되고 있다. 그러나 이러한 과학 수사기법의 발달은 '강제처분의 팽창' 현상을 초래하고 있다. 범죄와 관련이 없는 정보, 범죄와 관련이 없는 개인들에 대한 정보까지도 수사의 그물망에 포섭되고 있다. 정보주체의 프라이버시(Privacy) 보호가 무력화될 수 있는 것이다.

독일의 경우 '역외 압수·수색' 내지 '원격지 압수·수색' 및 '온라인 압수·수색'에 관해 실무에서 수권규정의 필요성이 대두돼 상당부분 법률로 규정되어 있는 반면 우리나라는 최근 각종 정보통신기술을 이용한 범죄에 대해 대처하기 위해 디지털포렌식 기술이 나날이 발전하고 있지만 디지털 증거자료가 해외에 있어서 수사에 불편을 겪는 것보다 역외 압수·수색을 통해 보다 손쉽게 사법정의를 실현할 수 있어야 한다.

요즘의 정보통신기술(ICT)의 급속한 발전으로 각종 범죄가 주로 사이버 범죄는 국가를 초월하여 발생하므로 디지털 증거의 역외 압수·수색이 실제로 필요하지만 많은 논쟁을 야기시킨다. IT 강국인 우리나라에서 자료가 해외에 있다는 이유만으로 수사에 장애가 발생하는 것보다 해외에 나가지 않더라도 해외에 있는 서버 등에 대한 역외 압수·수색을 통해 보다 손쉽게 사법정의를 실현할 수 있어야 한다.

316) 이순옥, 앞의 논문, 130면.

다만 온라인 수색은 전적으로 법관이 발부한 영장에 의해 이뤄져야 하고, 이러한 처분권한을 부여하는 법률에는 반드시 개인 생활형성의 핵심영역을 보호하기 위한 장치를 마련해야 될 것이다.[317]

2. 압수・수색의 실효성과 영장주의

현대사회에서 디지털 증거의 적극적인 활용 없이는 범죄 혐의사실의 입증은 매우 어려운 일이 될 것이다. 디지털 증거는 어떻게든 확보되어 공판정에서 유죄입증을 위하여 제시되어야 하며, 디지털 증거에 대한 강제수사, 즉 압수・수색도 법치국가원칙에 따라 불필요한 기본권 침해를 최소화하는 가운데 어떻게든 이뤄져야한다. 그렇지만 혐의사실 관련성을 기준으로 압수・수색의 대상을 특정하는 방법은 현실적으로 디지털 증거에 관한 압수・수색 범위를, 즉 수사기관이 시민의 기본권을 제한할 수 있는 범위를 합리적으로 제한하기 어려울 뿐만 아니라 경우에 따라 합법적인 수사의 범위가 비합리적으로 축소됨으로 인해서 압수・수색의 실효성을 확보하기도 어려울 수밖에 없다.

그렇기 때문에 단순하게 유체증거를 기반으로 하는 압수・수색의 정당성 판단기준을 기계적으로 적용하는 것 보다, 디지털 증거의 특징에 적합한 압수・수색 절차를 만들고 물리적 특정보다는 정보의 성질이나 형식을 통하여 압수・수색의 범위를 필요한 범위 내에서 합리적으로 확대하거나 축소할 수 있는 방법을 모색할 필요가 있다.[318] 다만 이 때 압수하고자 하는 정보를 발견하기 위한 수색의 과정에서 폭넓게 피압수・수색인 또는 관련된 제3자의 개인정보가 노출될 수도 있는 우려가 있다. 이는 디지털 증거의 특성으로 인하여 혐의사실 대상성을 기준으로 수색의 범위를 명확하게 특정하기가 어렵기 때문이다.

유체물에 대한 수색의 경우에 비하여 디지털 증거에 대한 수색의 범위는 상대적

317) 신상미, “온라인수색의 법률적 문제점과 허용가능성”, 경찰학연구 제 20권 제3호, 2020, 184면.

318) 한국형사정책연구원(전현욱・이상미), “형사절차상 디지털 증거의 압수・수색 및 증거능력”, 형사정책연구원 대검찰청 법무・법제(형사법제 등) 전문검사 커뮤니티, 2014, 26면.

으로 그 폭이 넓을 수밖에 없다. 그렇기 때문에 혐의사실을 관련성을 기준으로 수색의 범위를 특정하지 않은 일반영장은 영장주의의 본질상 허용될 수 없다는 문제제기가 있다. 그러나 이러한 특징은 디지털 증거의 특성으로 인한 압수·수색의 본질적인 한계이다.

압수·수색의 실효성을 확보하려면 유체물에 비해 특정의 정도는 상대적으로 완화될 수밖에 없다. 그러나 이는 유체물을 기준으로 하는 특정 방법을 그대로 준용할 경우에 그러한 것이므로, 디지털 증거의 특성에 부합하는 보다 구체적인 특정이 가능한 방법을 모색해야 한다. 따라서 이러한 문제는 명시적으로 디지털 증거의 유체증거와의 차이점을 인정하고 압수·수색의 범위에 대한 특정 정도를 완화하는 절차규정을 마련하는 수밖에 없으며, 그 안에서 가능한 범위 내에서 디지털 증거의 특성에 맞도록 최대한 압수·수색 범위의 특정 가능성을 확보하고, 더 나아가 또 다른 제도적 장치를 마련하여 기본권 제한의 범위를 최소화하는 방법으로 대응해야 한다.

본래 유체물의 경우에도 압수할 물건을 발견하기 위한 수색은 증거물이 소재하고 있는 것으로 추정되는 장소 전체에 걸쳐서 인정되는 것으로 당연히 압수에 비하여 비교적 폭넓게 허용되는 것이며 이것이 수색의 본질에도 부합한다. 특히 디지털 증거의 경우 기술적 검색 방법을 활용하면 수색의 범위를 폭넓게 인정함으로써 압수의 범위를 보다 합리적으로 제한할 가능성이 넓어진다는 점에서 이는 오히려 기본권 보호에 관하여 디지털 증거 수색의 장점으로 보아야 할 것이다. 게다가 디지털 증거에 대한 수색도 여전히 혐의사실을 입증하기 위한 증거를 발견하려는 강제수사이며, 따라서 기본적으로 수색의 범위는 혐의사실에 관련된 내용으로 한정될 수밖에 없다.

수사기관은 형사소송법 제215조 제2항에 의하여 범죄수사에 필요할 경우 해당 사건과 연관이 되어 있을 때 인정한 것에 한해 압수·수색을 할 수 있다.[319] 따라서 영장 발부 단계에서 별도의 혐의 입증을 통하여 범죄수사에 필요한지 여부, 그리고 압수하려는 디지털 증거가 해당 사건과 관계가 있는지 여부를 법관에게 객관

319) 형사소송법 제215조 제2항.

적으로 소명할 수 있어야 한다. 그러므로 디지털 증거의 경우에도 영장을 발급받을 수 있을 정도로 해당 혐의와 필요성이 소명 가능하다면 필요한 증거의 범위와 이를 발견하기 위하여 수색해야 하는 정보처리장치의 범위를, 물리적(장소적) 특정의 요건만 제외하고, 구체적으로 영장에 특정하여 명시하는 것은 실무상 불가능하지 않을 것이다.

예컨대 형사소송법 제114조 단서[320]의 취지처럼 일차적으로는 디지털 데이터의 작성기간을 통하여 수색 범위를 특정하는 것도 가능할 뿐만 아니라, 더 나아가 정보의 작성주체를 기준으로 특정하거나 피고인 또는 피의자 등의 접근 가능성 또는 합리적인 근거로 압수·수색이 개시된 컴퓨터 시스템으로부터 논리적으로 접속 가능한 범위 등을 기준으로 특정할 수도 있다. 또는 수사하고자 하는 혐의 사실의 구체적인 내용에 부합하는 범위를 영장에 명시하여 특정하는 것도 가능할 것이다.

그럼에도 불구하고 해소되지 못하는 우려가 남는다면, 이에 대해서는 디지털 증거에 대한 압수·수색으로 인하여 확인된 불필요한 정보나 사생활의 내밀한 분야에 해당하는 정보는 즉시 삭제하도록 하고, 수사기관에 비밀엄수 의무를 부여하는 방법으로 2차적 보완제도를 마련하는 것도 방법이 된다. 오히려 이런 방법을 마련하는 것이 막연히 유체물 증거를 기준으로 하는 현재의 압수·수색 절차를 준용하는 것에 비하여 보다 합리적으로 기본권을 보장할 수 있을 것이다. 디지털 증거의 압수·수색은 결국 2차적 보완 절차를 마련하는 것을 통하여 상당한 범위로 수색 범위를 제한하고 수사기관의 공권력 남용을 통제하는 절차적 방법을 통해 그 정당성이 확보될 수 있을 것이다.

3. 압수·수색의 적법성 및 실효성 확보를 위한 영장주의의 개선방안

현재의 범죄는 날로 고도화되며 그 수법은 더욱 지능화되고 있다. 이에 컴퓨터, 스마트폰, 전자기기 등에 숨겨진 범죄 증거를 찾아내는 '디지털 포렌식' 은 수사와 재판 그리고 국민의 기본권보호에 있어 그 중요도는 아주 크다. 정보통신과 디지털

320) 형사소송법 제114조 1항.

기술의 발전에 따라 컴퓨터, 스마트폰 등 정보저장매체를 이용한 정보저장이 언제, 어디서든지 가능하게 되었고,[321] 각종 범죄의 증거들도 종이 문서가 아닌 디지털 데이터의 형태로 존재하는 경우가 상당히 많아지고 있다. 이제 범죄 수사에 있어 디지털 증거의 활용은 필수적이다. 이에 따라, 범죄 수사에 있어서도 디지털 증거를 적법하고 효과적으로 확보할 필요성이 높아지고 있다.

디지털 증거는 이를 출력하기 전까지는 일반인들의 눈으로 직접 확인하기 어렵다는 특징을 지니고 있으므로, 압수·수색 대상물을 특정하거나 압수·수색의 범위를 정함에 있어 모호함이 있다. 또한, 클릭 한 번만으로도 순식간에 다른 서버나 저장매체로 옮겨질 수도 있고, 규모가 매우 방대할 수도 있기 때문에 여러 정보들 가운데 실제로 수사에 필요한 증거가 어디에 숨어있는 지 찾아내는 일도 쉽지 않다. 때문에 자칫하면 범죄와 관련이 없는 정보에 대한 불필요한 압수·수색이 행해지고, 영장주의를 위반하거나 개인의 사생활의 비밀을 과도하게 침해할 가능성도 있다.

디지털 증거의 대량성, 복제 용이성 등의 특징으로 인해 압수·수색에 있어 혐의와 관련이 없는 개인 사생활의 프라이버시(Privacy)들이 무작위로 수집되는 위험성과 개인정보 자기 결정권의 침해 가능성은 더욱 커진 것이다.[322] 그만큼 과학기술의 발달에 따라 다양한 디지털 데이터저장매체를 포렌식 수사기법이 일반화되면서 광범위한 개인의 프라이버시(Privacy)의 침해가능성이 커지는 상황을 반영하는 것으로 보인다.[323] 위법하거나 과잉한 압수·수색이 발생할 수 있기에 수집 및 집행 절차에 관한 정교한 기준 마련이 무엇보다 중요하다.

최근 디지털 범죄 피해 영상물에 대한 영상물 압수 제도 개선 방안이 강구되고 있는 것도 그 이유가 크다. 여기에는 피해 영상물 원본을 복제해놓고 압수한 다음 원본을 삭제하는[324] 압수 방법 및 압수 영장 발부 전까지 압수 대상을 보전할 수 있도록 명령하는 제도를 명문화하는 것도 포함된다. 기존의 압수·수색 방법은 이

321) 정웅석, 앞의 논문, 359면.
322) 조광훈, 앞의 논문, 316면.
323) 김종구, 앞의 논문, 212면.
324) 서주연, 앞의 논문, 330면.

러한 특성을 반영해 변화해야 함에도 여전히 현행 형법, 형사소송법에는 그러한 변화가 제대로 이루어지지 않고 있는 것이다.

그만큼 디지털 증거의 경우 영장주의에 따라 압수 특정물을 사전에 기재하기란 실무적으로 어렵고 모호하다. 영장의 범위와 기준 밖에서 확보된 디지털 증거는 위법한 것으로 증거능력의 상실을 초래해 수사 실패로 이어질 위험성이 있고, 이로 인한 피해는 국민에게 돌아갈 것이므로 보다 정합성을 갖춘 제도 개선방안이 필요하다. 실체적 진실의 발견과 피의자, 피고인의 기본권 보호가 조화를 이룰 수 있는 적절한 방안에 대한 논의가 필요하다. 디지털 증거의 압수대상물 특정, 범위, 집행방법 등에 대한 다양한 고민들이 이뤄져야한다.

한편 스마트폰은 정보저장매체로 분류됨에도 불구하고 일반적으로 사후분석으로는 선별압수가 어렵기 때문에 먼저 매체압수를 하는 것이다. 사실상 이러한 방식이 현실적으로는 타당하긴 하나, 사후분석 과정에서 영장의 기재 범위를 넘나드는 과도한 수색에 대하여 우려 되는 것은 당연지사다.[325] 다른 전자증거보다 오히려 프라이버시(Privacy) 보호가 절실한 스마트폰의 압수방법에 있어서 그 침해의 정도가 더 클 수 있는 매체압수가 빈번하게 이루어진다는 것은 선별압수 원칙과 예외적 매체압수를 규정한 입법자의 취지에도 어긋난다.[326] 따라서 스마트폰의 압수・수색에 있어 참여권의 보완하거나 절차적으로 보충성 요건을 추가를 통해 매체압수에 대한 집행이 영장주의에 반하지 않아야 할 것이다.[327]

스마트폰에 대한 디지털 증거분석결과, 압수하여 증거로 사용할만한 새로운 디지털 데이터가 없었기 때문이라는 이유로 상세목록을 교부하지 않거나, 디지털 증거분석을 통하여 확보된 디지털 데이터 중 범죄사실과 관련 있는 부분에 대한 탐색・출력・복제 과정이 종료되어 보전의 필요성이 없어진 정보는 지체 없이 삭제・폐기되어야 하는데, 그 필요성이 없음에도 불구하고 통보받은 디지털 데이터를 삭제・폐기하지 않은 채 CD에 복제하여 사건기록에 첨부하는 경우 등도 문제이다. 즉 수사기관이 스마트폰을 압수하여 디지털 증거분석을 실시하였음에도 불구하고,

325) 박병민・서용성, 앞의 보고서, 230면.
326) 조미지・송영진, 앞의 논문, 139면.
327) 조미지・송영진, 앞의 논문, 139면.

형사소송법 제219조에 따른 상세목록을 교부하지 않고, 증거분석이 모두 종료된 후에도 장기간 스마트폰을 반환하지 않았다면 이는 적법절차원칙 위반이다.

스마트폰에는 혐의사실과 관련된 정보는 물론 그와 관련이 없는 다양하고 방대한 내용의 사생활 정보가 포함되어 있으므로, 스마트폰의 디지털 데이터를 수사기관이 적법한 절차에 의하지 않은 채 보유하게 된다면, 해당 디지털 데이터가 사건기록의 열람·복사 과정에서 관계인 등에게 유출될 가능성은 물론, 수사기관에 의해 다른 범죄의 수사 단서 또는 관련 증거로 위법하게 사용되는 등 새로운 법익침해를 초래하게 될 위험 가능성이 있다.[328] 따라서 어떠한 이유에서든 보전의 필요성이 있어 디지털 데이터를 CD 등에 복제하여 수사기록 등에 편철하였다면, 상세목록을 피의자에게 교부해야 한다. 통상 임의제출의 적법성과 관련하여 다툼이 있는 경우, 제출함에 있어 임의성이 존재한다는 점에 대하여는 수사기관이 합리적인 의심을 떨칠 수 있을 정도로 증명해야 한다.[329]

이에, 디지털 증거의 압수·수색 절차에 있어 적법절차를 준수하여 국민의 기본권을 불필요하게 침해하지 않도록 신중을 기해야 한다. 압수·수색 절차에서 당사자 참여권을 충실히 보장하여 절차적 적법성을 확보하고, 정보저장매체 및 디지털 증거의 특수성을 고려한 각종 조치도 마련되어야 한다. 사생활 침해의 우려가 매우 큰 디지털 증거의 압수·수색과 관련하여 국민의 기본적 인권 보호를 위해 가장 원칙적 한계로서 헌법에서 규정하고 있는 적법절차의 원칙과 영장주의를 준수하며 실체적 진실 발견과 개인의 인권보장을 조화롭게 실현할 수 있도록 하여야 한다.

또한 디지털 데이터의 대량성, 다양성, 증거분석의 복잡성 등의 특징 때문에 기존 영장주의 법리 외에 새로운 제한이 필요하다는 의견이 제시되고 있다. 영장에 구체적인 집행방법을 기재하는 '사전통제'는 이론상 받아들이기 어렵고 실효적인 방안이 되기도 어렵다. 위법수집증거 배제법칙을 매개로 한 공판절차의 '사후통제'도 시기적절한 대응이 되지 못하거나 위법한 수사 관행에 미흡한 대응이 될 우려가 있다. 따라서 법원의 사전통제(영장심사) 및 사후통제(공판절차)에 더하여

328) 전승수, "디지털 증거 압수절차의 적정성 문제 -피압수자 참여 범위 및 영장 무관 정보의 압수를 중심으로-", 형사판례연구 제24권, 2016, 638면.
329) 이기리, 앞의 논문, 420면.

당사자 참여권(준항고)을 매개로 한 '중간단계 통제'를 강화할 필요성이 있다. 특히 압수·수색영장의 맥락에서 영장 재판에 대한 불복을 허용함이 필요하다.

최근 디지털 데이터 수집의 맥락에서 적법성 및 집행 가능성에 의문이 있는 내용의 영장이 발부되고 있고, 특히 '집행방법'의 기재가 문제되고 있다. 적법하게 발부된 영장의 집행방법 기재는 실제 압수·수색현장에서 사실상의 강제력을 가질 위험이 있고, 사후통제를 통해 이를 바로잡는 것은 결코 쉬운 일이 아니다. 따라서 이러한 위험을 제거하기 위해서도 영장의 효력을 다툴 절차를 인정할 필요가 있다.

제3절 외국계 e-메일 계정에 대한 압수·수색의 적법성

1. 외국계 e-메일 계정에 대한 압수·수색의 문제

가. 외국계 e-메일 계정에 대한 압수·수색의 상황

2021. 1. 5. 통신비밀보호법 개정으로 제9조의3에서, 검사는 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우 그 사건에 관하여 공소를 제기하거나 공소의 제기 또는 입건을 하지 아니하는 처분을 한 때에는 그 처분을 한 날부터 30일 이내에 수사대상이 된 가입자에게 압수·수색·검증을 집행한 사실을 서면으로 통지해야하고 (제1항), 사법경찰관은 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우 그 사건에 관하여 검사로부터 공소를 제기하거나 제기하지 아니하는 처분(기소중지 또는 참고인중지 결정은 제외한다)의 통보를 받거나 검찰송치를 하지 아니하는 처분(수사중지 결정은 제외한다) 또는 내사사건에 관하여 입건하지 아니하는 처분을 한 때에는 그 날부터 30일 이내에 수사대상이 된 가입자에게 압수·수색·검증을 집행한 사실을 서면으로 통지하여야 하는 것으로(제2항) 2021. 3. 16. 개정하는 한편, 2011. 7. 18. 개정된 형사소송법 제107조 제3항에서는, 전기통신에 관한 물건의 제출을 명하거나 압수한 때에는 발신인이나

수신인에게 그 취지를 통지하도록 규정하였다. 이러한 입법개선에 의하여 e-메일상의 정보주체는 이 사건 법률조항에 규정된 사전통지의 예외에 해당하는 경우라도, 적어도 그 압수·수색 집행사실을 기소 또는 불기소처분 등이 있은 날로부터 30일 이내에 통지받을 수 있게 되었다.[330]

이처럼 우리나라는 e-메일 압수·수색할 때 송·수신자의 관여 없이 e-메일 관리자의 협조만 얻어서 해당 서버에 보관된 특정 e-메일 계정에 대한 압수·수색을 하여 왔다. 그러다 보니 송·수신자 관여 없이 e-메일 서버, 서비스제공자에 대한 압수·수색이 이루어져 정보의 자기결정권 측면에서 문제가 되고 있는 것이다. 그러나 외국계 e-메일 계정의 경우는, 원칙적으로 형사사법공조절차를 거쳐 역외 수사기관을 통하여 증거를 확보하거나, 관리서비스 제공자의 협조를 얻어 해외의 정보저장매체[331]로부터 데이터를 제공받아야 한다. 그러한 상황에서는 실무상 수사기관은 수사과정에서 합법적으로 획득한 수사대상자의 계정과 패스워드를 확보하였을 경우라도, 이를 근거로 다시 압수장소와 방법을 기재한 압수·수색영장을 발부받아 e-메일을 압수·수색하여야 한다.[332]

나. 외국계 e-메일 계정에 대한 압수·수색의 유형

(1) 서버소재지 역외 압수·수색

유럽평의회 사이버범죄방지 조약에서는 역외 압수·수색에 대하여, "적법한 방법으로 계정정보를 취득하여, 영장에 의하여 역외에 존재하는 컴퓨터 데이터에 접근한 것"이라고 정의하고 있다. 이러한 방법은 대개 서버의 소재지를 압수·수색 장소로 하여 서버를 수색하여 압수하거나 매체 자체를 압수하는 경우이다.[333]

330) 통신비밀보호법[시행 2022. 7. 1.] [법률 제18465호, 2021. 9. 24. 타법개정] , 형사소송법[시행 2022. 2. 3.] [법률 제18799호, 2022. 2. 3. 일부개정] , 법제처 국가법령정보센터
331) 정웅석·최창호, 형사소송법, 대명출판사, 2017, 186면.
332) 정소연, 앞의 논문, 66면.
333) 이정민, 앞의 논문, 123~126면.

(2) 합법적으로 획득한 계정정보를 통한 역외 압수・수색

합법적으로 획득한 계정정보를 이용하여 역외 컴퓨터 데이터에 접속하는 경우는 예를 들어, 국외에 위치한 서버인 경우, 수사기관이 피의자 계정과 패스워드를 확인할 수 있는 경우, 네트워크 접속을 통해 사건과 관련된 정보를 확인하고 국내 사법관할권이 미치는 영역으로 다운로드 하여 압수・수색하는 경우이다.[334]

(3) 전문적・기술적 방법을 통한 역외 압수・수색

전문 소프트웨어 혹은 기술적 수단을 이용하는 방법은 데이터가 저장된 서버 자체를 기술적으로 뚫고 그 데이터에 접근하는 수사방법인 온라인 수색[335]도 이에 해당한다. 그 예로, 미국의 Gorshkov 사건[336]이 있다. Gorshkov 사건은 FBI가 키로거(Key Logger)를 이용하여 계정과 패스워드를 확보한 뒤, 영장 없이 러시아 서버에 접근하여 해킹 툴 등 데이터를 다운받아 증거로 사용하였다.[337]

(4) 동의에 의한 역외 압수・수색

동의에 의한 방법은 범죄 사실의 입증에 중요한 증거가 될 수 있는 컴퓨터 데이터가 다른 사법관할권 내에 존재할 때, 수사기관이 정당한 방법과 자발적 동의에 의해서 집행하는 방법을 말한다. 사이버범죄 방지조약 제32조는 데이터의 역외 접

334) 이정민, 앞의 논문, 123~124면 참조.
335) 전현욱 외, 앞의 보고서, 217면.
336) United States v, Gorshkov, 2001 WL 1024026, U.S. Dist, LEXIS 26306(W.D. Wash, 2001) FBI가 미국의 ISP, 전자상거래, 은행 등에 대한 해킹에 대하여 러시아에 대한 수사를 착수하였다. FBI는 러시아인 용의자를 채용제안을 통해서 미국으로 유인한 후에 해킹기술 test를 실시했더니 용의자가 자신의 ID와 PASSWORD로 러시아 내 서버에 접속했다. FBI는 이 때 접속한 ID와 PASSWORD를 이용하여 해당서버에 접속해 해킹 도구와 공격하여 FTP를 통해 관련 파일을 다운 받고 긴급보전조치를 한 다음에 압수・수색영장을 발부받아서 증거로 사용한 것이다.; 정소연, “디지털 증거의 역외 압수・수색에 대한 법적 고찰”, 디지털포렌식 연구 제11권 제1호, 2017. 65면.
337) 이정민, 앞의 논문, 124면.

속동의에 의한 또는 공개되어 있는 저장된 컴퓨터 데이터에 대한 초국경적 접속 당사국은 다른 당사국의 승인을 얻지 않은 상태에서, a. 데이터의 지리적 위치에 관계없이, 공개적으로 사용 가능한 저장된 컴퓨터 데이터에 접속할 수 있고, b. 만약 당사국이 데이터를 공개할 법적 권한이 있는 자의 합법적이고 자발적인 동의를 얻었다면, 자국 영토내의 컴퓨터 시스템을 통해 다른 당사국에 위치한 컴퓨터에 저장된 데이터에 접속하거나 이를 수령할 수 있다고 규정하고 있다.[338]

(5) 관리자의 정보 제공

인터넷 서비스 제공자로부터 정보를 제공받는 방법은 수사기관이 용의자와 관련된 정보를 인터넷 서비스 제공자로부터 획득하는 것을 의미한다.[339] 이 경우, 통신자료요청에 해당하여 전기통신사업법 및 개인정보보호법 규정이 적용[340]될 수 있다. 사이버범죄 방지조약 제18조는 당사국에게 제3자가 보관하는 전자기록에 관련된 증거를 수집하기 위해 수사기관이 복잡한 컴퓨터시스템의 전문적인 조작을 해야 하는 상황을 피하고, 피처분자에게도 덜 침해적이 되도록, 전자기록의 보관자에게 전자기록을 제출하도록 하는 제출명령 제도를 둘 것을 규정하고 있다.[341]

흔히 역외서버 압수・수색이 문제되는 사건은 우리나라 국내 e-메일 압수・수색에서처럼 제3자에게 정보제공을 요구한 경우이다. 대표적인 경우로는 미국의 마이크로소프트사건과 Google사건이 있다. 마이크로소프트사건은 2016년 수사기관이 마이크로소프트에게 아일랜드 서버에 저장된 이용자의 e-메일 데이터를 제출하도록 하였으나, 2차 순회법원(Second Circuit)은 마이크로소프트가 아일랜드에 있는 데이터를 수사기관에 저장통신법을 근거로 제공해야 할 의무는 없다고 했다. 그러나 Google사건은 2017. 02.에 펜실베니아 법원이 미국 연방수사국(FBI)의 압수・수색영장에 응하라고 판단한 사례이다.

---

338) 이정민, 앞의 논문, 124~125면.
339) 정소연, 앞의 논문, 63면.
340) 이원상, “수사절차에서 통신자료 활용에 따른 쟁점 고찰”, 형사소송 이론과 실무 제7권 제1호, 2015, 77면.
341) 이정민, 앞의 논문, 125면.

2. 현행법상 외국계 e-메일 계정에 대한 압수・수색의 적법성 문제

가상공간의 맥락에서 영토주권 침해 여부는 ① 영토적 완전성에 대한 침해, ② 정부 고유 기능에 대한 개입 침탈을 기준으로 하지만, 개별 국가의 국내법을 함께 고려하여야 한다. 기존 국제규범과 개별 국가의 국내법의 내용을 종합적으로 검토할 때, '접근권한 없는 침입' 은 국제법 위반(영토주권 침해)을 구성할 가능성이 높다 할 것이다. 국제법 위반의 문제가 있는 경우 해당 증거의 증거능력 판단에 어떠한 영향을 미치는지는 실행 국가의 국내법에 의하여 판단할 문제이다. 따라서 국제법상 위법이라는 이유로 반드시 형사소송법 위반도 인정되고, 나아가 위법수집증거배제법칙의 적용대상인지의 문제에 대한 검토가 필요하다.

가. 견해의 대립

(1) 긍정설

긍정설은 e-메일과 같은 디지털 증거는 네트워크로 연결되어 있고, 압수를 한 경우에도 여전히 서버에 남아있어 유체물에 대한 압수와 달리 수사기관이 '접근권' 이라는 서비스를 이용했을 뿐 배타적인 점유권을 취득한 것이 아니며,[342] 원격압수・수색의 방법을 통해 압수・수색을 하는 경우에는 수색 장소에 있는 컴퓨터를 이용하여 원격지 서버에 접속하여 해당 컴퓨터로 다운로드 받은 디지털 데이터를 압수・수색하는 것이므로, 이러한 취지의 별도 영장을 발부받아 집행한 경우 형사소송법 제120조의 '압수・수색영장의 집행에 필요한 처분' 에 해당하는 것으로 별도의 입법 없이도 현행 형사소송법의 해석에 의하여 역외 압수・수색을 인정할 수 있다는 견해이다.[343]

342) 이정민, 앞의 논문, 133~134면.
343) 박봉진・김상균, "디지털 증거 압수・수색에 관한 연구", 법과 정책 제19집 제1호, 2013,

(2) 부정설

부정설은 현행법상 해외 서버에 대한 원격 압수・수색에 대한 명문의 규정이 없기 때문에 불가능하고,[344] 해당 정보가 저장된 정보저장장치의 소재지가 해외인 경우에도 압수・수색할 수 있도록 한다면, 서버 위치인 상대국의 관할권이나 주권을 침해할 수 있고, 이는 타국의 사법관할권을 침해하는 것이기 때문에 해외 서버에 저장된 e-메일을 압수・수색하려면 당사국간의 조약체결이 전제되어야 한다는 것[345] 등을 근거로 들고 있다.

나. 판례의 입장

고등법원은[346] 부정설의 입장으로 이 사건의 수색 장소가 역외에 위치한 서버이고, 피압수자는 해당 디지털 데이터를 보관하고 있는 해외 e-메일 서비스 제공자라고 가정하면, e-메일 계정정보를 이용하여 해외 서버에 존재하는 e-메일을 접속한 것이 외관상 형사소송법 제120조 제1항에서 규정하는 '압수・수색영장의 집행에 있어서는 건정(자물쇠)을 열거나 개봉 기타 필요한 처분'에 해당할 수는 있으나, 압수・수색 장소 또는 대상물이 해외에 존재하여 대한민국의 사법관할권이 미치지 아니하는 경우까지 압수・수색・검증영장의 효력이 미친다고 보기는 어렵다고 보았다. 즉 해외 e-메일 서비스 제공자의 해외 서버 및 그 해외 서버에 소재하는 저장매체 속 디지털 데이터에 접속하는 것은 관할권을 침해하여 영장을 집행한 것으로 형사소송법 제120조 제1항의 필요한 처분에 해당하지 않는다고 판단하였다.

이 견해에 따르면, 데이터 보관 서버가 해외에 존재한다면 국내 ISP의 서비스를 이용할 때도 피의자가 e-메일을 자발적으로 제출하지 않는 한 수사기관이 정보저

207면.

344) 이원상, "현행 디지털 증거 수집 관련 법률의 한계", 디지털포렌식연구 제11권 제3호, 2017, 32~33면.

345) 정대용・김기범・이상진, 앞의 논문, 57면.

346) 서울고등법원 2017. 6. 13. 선고 2017노23판결.

장매체에 물리적으로 접근할 방법이 없다.[347] 적법하게 압수한 메모 등을 통해 피의자의 해외 e-메일의 계정정보를 입수하더라도 국제사법공조절차 또는 해외 ISP의 협조 없이는 수사기관의 강제처분을 통한 e-메일을 취득하는 것 자체가 현행법상 허용될 수 없다고 보는 것이다.

그러나 대법원은[348] 긍정설의 입장에서, 압수·수색의 장소를 해외 서버가 아닌 정보통신망을 이용하여 서버에 접속하는 컴퓨터 및 그 컴퓨터의 소재지로 보고, 피압수자 역시 해외 ISP가 아닌 정보의 주체, 즉 e-메일 사용자인 피의자로 보았다. 즉, 이 사건 영장으로 원격지에 있는 저장매체 즉 서버 자체를 수색하거나 이에 저장된 정보를 압수한 것이 아니라, 정보통신망을 통하여 연결된 원격지의 저장매체에서 수색장소에 있는 컴퓨터 등 정보저장장치로 다운로드하여, 압수·수색 대상 컴퓨터에 저장된 디지털 데이터를 수색하여 압수하는 것으로서 처음부터 서버 소재국의 사법관할권 침해 자체가 발생하지 않는다고 본 것이다. 그리고 위와 같이 적법하게 취득한 계정정보를 이용하여 당사자 동의에 갈음하는 압수·수색영장을 별도로 발부받아 해외 서버에 접속하는 것 자체는 형사소송법 제120조 제1항에서의 '압수·수색·검증영장의 집행에 필요한 처분'에 해당하고, 따라서 이러한 행위는 비례성의 원칙에 비추어 보아도 적법하다는 것이다.

다. 소결

서버에 저장된 디지털 증거에 대한 압수·수색의 경우 주로 그 서비스 이용자가 e-메일 등 증거자료 자체를 복사, 출력하는 등의 방법으로 임의제출하지 않는 한 인터넷 서비스 이용자가 아닌 ISP에 대한 압수·수색을 통해서 정보를 획득하게 되는데, 이때 ISP의 경우 이용자의 정보를 관리하고 있을 뿐 그 내용에 대하여는 알지 못하며, 일반적으로 서비스 이용자를 위해 데이터를 어디에 저장하느냐는 중요한 고려사항이 아니기 대법원 입장이 타당하다고 본다.

---

347) 이순옥, 앞의 논문, 134면.
348) 대법원 2017. 11. 29. 선고 2017도9747 판결.

먼저 이용자는 데이터를 저장한 국가가 이용자의 정보에 접근 또는 이를 처분한 것을 허용하지 않았기 때문에 위 해외 ISP가 이용자의 데이터에 대한 처분권한을 가지고 있다고 보기 어렵다.[349] 특히 e-메일처럼 공개되지 않는 사적 통신의 경우 발신자와 수신자, 즉 서비스 이용자가 개인정보보호의 이익을 가지는 정보주체에 해당하고 이용자의 정보보호가 중요하므로,[350] 참여권을 보장할 대상은 ISP가 아닌 서비스 이용자라고 보아야 할 것이다.

해외 ISP나 서버 관리자는 정당한 권한으로 아이디와 비밀번호를 입력만하면 세계 어디서나 해당 e-메일을 접속하고 자료를 클라우드에 저장할 수 있도록 하고 있다.[351] 수사기관이 적법하게 계정정보를 취득하여 법관의 영장을 발부받아 e-메일을 압수한 것이라면, 인터넷 서비스 이용자가 통상의 방법에 따라 해당 서비스를 이용한 것과 그 접근방법이 동일한 점, ISP는 해당 계정 명의자가 직접 계정에 접속한 것인지, 제3자가 계정정보를 알고 접속한 것인지, 명의자가 제3자에게 계정을 빌려준 것인지 등에 대하여 실질적으로 심사하지는 않고 입력한 계정정보만 정확하다면 서비스 이용을 허용하고 있는 점 등을 고려하면, 위와 같은 압수·수색은 ISP의 의사에 반하는 처분이라고 보기 어려울 것이다.[352]

또한, 역외 인터넷 서버에서 접속하여 범죄와 관련된 데이터만 추출하여 국내에 접속한 컴퓨터로 데이터를 옮겼지만, 해당 데이터는 서버 자체에 지워지지 않고 그대로 남아 있다.[353] 유체물의 압수와는 달리 국내 수사기관이 압수대상인 정보의 점유를 배타적으로 취득하는 것도 아니고, 범죄 혐의와 관련된 검색어를 입력하여 관련 정보를 추출하고, 다운로드 또는 저장하는 등의 압수·수색행위는 국내에 소재한 압수·수색장소의 컴퓨터에서 이루어지는 것으로 실질적으로 압수·수색의 장소가 해외로 보기도 어렵다.[354] Google사건에서도 펜실베니아 동부지방법원은 '데이터를 해외 서버로부터 캘리포니아 소재 Google 데이터 센터로 전자적 방법

349) 이순옥, 앞의 논문, 135면.
350) 박경신, "E-메일 압수·수색의 제문제와 관련 법률개정안들에 대한 평가", 법학연구 13권 2호, 2010, 269면.
351) 이순옥, 앞의 논문, 136면.
352) 이순옥, 앞의 논문, 136면.
353) 이정민, 앞의 논문, 133~134면.
354) 이순옥, 앞의 논문, 137면.

으로 전송하는 것은 사용자의 데이터에 대한 점유 이익에 관한 유의미한 간섭이 없으므로 이는 압수에 해당하지 않고 따라서 역외에서의 압수에 해당하지 않는다.' 라고 보았다.

그 다음, 실무상 국내 ISP의 경우에는 계정접속을 통한 원격지 압수·수색에 응해주고, 해외 ISP의 경우에만 국제사법관할권의 문제로 삼아 압수·수색을 허용하지 않는다면, Google 등 해외 ISP 및 그 이용자의 경우에만 수사기관의 압수·수색을 거부할 수 있는 특례를 제공하는 것처럼 되어, 오히려 국내 ISP 및 그 이용자를 역차별 하는 결과가 될 수도 있다.[355]

마지막, 역외 압수·수색을 인정하더라도 형사소송법이 규정하는 참여권 등 영장집행절차를 모두 준수할 수 있고, 비례의 원칙에 비춰 보아도 적법하게 취득한 계정정보를 이용하여 해외 서버에 접속하는 것은 압수·수색행위 그 자체가 아닌 형사소송법 제120조상의 압수·수색·검증영장의 집행에 필요한 사전행위로서 적법하다고 볼 수 있다. 압수·수색의 절차 과정에서의 참여권 등 적법절차가 보장된다면 헌법 제12조 제1항에서 보장하는 적법절차 원칙에 어긋나는 것은 아닐 것으로 볼 수 있기 때문이다. 그러므로 집행과정에서 특별하게 위법사항이 있다고 볼 수는 없을 것이다.

제4절 역외 디지털 증거수집과 국제 공조

1. 국제형사규범의 발전을 위한 국제협력

가. 제도개선을 위한 국제적 협력

오늘날 국경을 초월하는 네트워크, 암호화 기술발전 등으로 인해 범죄행위에 관련한 역외 디지털 데이터의 수집은 날로 그 중요성이 커지고 있어, 이에 각국 정부

355) 박석훈, 앞의 논문, 25면.

는 다양한 방법을 동원하고 있다. 그러나 역외 디지털 데이터를 확보하기 위한 이러한 각 국가의 노력은 개인의 프라이버시(Privacy) 자유를 침해할 우려가 있지만 그 실효성을 담보하기는 힘들다. 즉, 규제와 회피의 악순환은[356] 국가 안보와 적법한 법 집행 등 공공의 이익을 저해하는 동시에 바람직하지 않은 정치·경제적 결과를 초래할 수 있기 때문이다.[357] 이에 따라 공적 이익과 프라이버시(Privacy) 보호의 조화를 위하여 역외 디지털 데이터 접근과 관련하여 법적 절차를 개선하려는 다양한 방법론이 제시되고 있는바, 이러한 국제적 가상공간 관련 범죄 현상에 대한 가장 대표적인 것으로 '사이버범죄방지협약' 이 있다.[358]

우리도 현재 형사사법공조를 위한 양자조약은 1992년 호주와 처음 조약을 체결하였고 2020년 9월말 기준으로 33개국과 체결한 상태이고, 국제사법공조법은 공조조약에 법과 다른 규정이 있을 경우에는 조약에 따른다고 규정하고 있다.[359] 뿐만 아니라, 2011년 12월 29일 형사사법공조에 관한 유럽협약을 체결하여 유럽평의회 47개국 회원국들과도 형사사법공조가 가능해졌으며 UN부패방지협약(2008년 4월 26일 발효), UN초국가적 조직범죄 방지협약(2015년 12월 5일 발효), 국제상거래에 있어서 외국공무원에 대한 뇌물제공방지를 위한 협약(1999년 12월 15일 발효)에 가입되어 있어서 형사사법공조가 가능하다.[360]

이렇게 국제형사사법 공조법의 활용하듯이 사이버범죄협약도 벤치마킹하여 적극 검토해 볼 문제이다. 국내 서버를 전제로 한 원격 수색의 경우와 달리 역외 수색은 우리나라의 관할권을 인정하더라도 ① 다른 나라의 관할권이 동시에 존재하거나 ② 현실적으로 해외에 소재한 서버의 압수·수색이 불가능하거나 ③ 타국의 주권 침해 문제를 야기할 가능성이 있는 등의 문제가 내재되어 있다.[361]

정보통신기술이 발전하고 이에 의존할수록 사이버범죄 발생 가능성도 높아져 수

356) 조성훈, "역외 디지털 증거의 수집과 국제형사규범의 발전", 단국대학교 법학논총, 제43권 제3호, 2019, 127면.
357) 조성훈, 앞의 논문, 274면.
358) 이에 관해서는 앞의 제4장 제1절 역외 디지털 압수·수색에 대한 외국 입법례 부분 참조.
359) 정영수, "역외 전자정보 수집의 범위와 한계: 국가관할권의 확정과 위법수집증거배제 법칙의 적용을 중심으로", 제11회 한국형사학대회 학술대회 토론문, 2022, 251면.
360) 정영수, 앞의 토론문, 251면.
361) 이인곤·강철하, 앞의 논문, 353면.

사 대응력을 강화할 필요가 있으며, 사이버범죄의 초국가적 성격상 신속하고 긴밀한 국제공조가 필수적이다. 이제는 협약 가입과 관련한 쟁점들에 대하여 결론을 내리고 국제사법공조, 사생활 보호, 기업의 부담 완화, 국가안보 등의 가치들이 조화롭게 달성될 수 있는 입법·정책적 방안을 모색할 필요가 있다.[362]

아직은 사이버범죄방지조약에 가입되어 있지 않지만 만일 가입하게 된다면 컴퓨터시스템을 공격한 자가 해외에 있는 경우라도 피해 시스템이 자국에 있다면 속지주의에 따라 관할권을 행사할 수 있다. 또한 자국민이 자국의 영토관할권 밖에서 클라우드시스템 등에 대한 공격행위를 할 때에도 속인주의에 따라 관할권을 행사할 수 있으며, 해당 범죄에 대해 2개 이상의 국가가 관할권을 주장할 경우에는 상호 협의하여 결정하게 된다. 개정 전 미연방 형사소송규칙(Federal Rules of Criminal Procedure)은 치안판사가 속한 법원의 관할권 내 지역에만 수색영장을 발부할 수 있도록 하고 있었지만[363], 관할 구역 내외를 불문하고 정보저장매체 수색과 디지털 데이터 압수·복제를 위한 원격접속을 할 수 있도록 허가하는 영장을 발부할 수 있다' 고 규정[364]되어 있다.

동 협약의 주요 내용은, '개별국가 차원의 조치(제2조-제22조)' 와 '국제협력(제23조-제25조)' 으로 나누어져 있고, 특히 국제협력과 관련해서는 비교적 상세한 규정을 두고 있다. 구체적으로 사이버범죄방지협약은 제2장에서 '개별국가 차원의 조치' 를 ① 형사실체법(제2조-제13조), ② 형사절차법(제14조-제21조), ③ 관할(제22조)로 구분하고, 제3장에서 '국제협력' 을 ① 일반원칙(제23조-제28조), ② 개별규정(제29조-제35조)으로 나누어 규정하고 있다.[365] 그러나 아직 국제형사사법공조 절차를 좀 더 효율적으로 개선하는 만족할 수준의 협력이 되도록 디지털 증거 수집 데이터관련 제도개선에 대한 적극적인 국제적 차원의 논의가 필요하다. 충돌하는 개별 주권국가들의 이익을 상호 조정하여 정부(수사기관)의 정보 접근에 대한

362) 신용우, "유럽 사이버범죄 방지 협약 체결 현황과 우리나라의 입법·정책적 대응방향", 국제관계 동향과 분석 제77호, 2020, 6면.
363) In re Warrant to Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013).
364) Federal Rules of Criminal Procedure Rule 41. Search and Seizure.
365) 조성훈, 앞의 논문, 275면.

일관되고 통일된 안정적인 규칙을 발전시켜 나가는 국제적 협력이 필요한 것이다.

나. 분권형 국제협력

국제적으로 일원화된 하나의 조약으로 관련 데이터 접근에 대하여 일관되고 안정적인 규칙을 만든다는 것은 어렵다. 서로 가치관을 다른 개별 각 국가의 이해관계를 모두 충족하는 경우는 매우 힘들고, 만든다 해도 실효성이 없는 최소한의 합의 수준에만 그치는 경우가 많다.[366] 개별 국가별로 서로 다른 법체계와 이해관계를 가진 상황에서 단일한 조약을 맺는다는 것은 쉽지 않다.

그 대안으로 분권화된 접근방법이 제시되고 있으며, 그 대표적인 것으로 미연방 '클라우드 법'이라 할 수 있다. 미연방 '클라우드 법', 즉 '합법적 해외 데이터 활용의 명확화를 위한 법(Clarifying Lawful Overseas Use of Data Act, CLOUD Act)'은 데이터에 대하여 국가기관의 통제범위라는 관점에서 새로운 도전이라 할 것이다. 이는 역외 데이터수집, 테러나 사이버보안 등의 국제범죄 대응, 국제적 차원의 정보공유와 같은 형사정책 및 절차법적인 사항에 대한 새로운 쟁점을 제시하며, 이에 대한 구체적인 검토도 이루어지고 있다.[367]

'클라우드 법'은 다음의 2가지 원칙을 기초로 한다.[368] 먼저, 동등 경쟁조건 원칙인데 서비스제공자의 데이터가 어떤 장소에 저장되어 있던 간에 동등하게 취급하는 것을 말한다. 동 원칙은 역외 데이터 접근에 대한 법적 절차를 형성함에 있어 데이터 저장 위치 등에 따라 서비스제공자를 차별하는 것은 타당하지 않다는 점에 착안한 것이다.[369]

다음으로, 상호주의 원칙이다. 클라우드 법은 해외의 수사기관이 미국 내에 저장되어 있던 범죄 관련 데이터에 접근하려면[370] 상호주의 원칙에 따라 해당 국가도

366) 조성훈, 앞의 논문, 102면.
367) 송영진, "미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점", 형사정책연구 제29권 제2호, 2018, 149면; 김재운, "미국의 클라우드법(CLOUD Act)상 대테러정책 연구", 한국테러학회보 제33호, 2018, 148면.
368) 조성훈, 앞의 논문, 276면.
369) 조성훈, 앞의 논문, 276면.

미국과 동등한 수준의 조치를 해결해 줄 것을 요구하고 있다.[371] 국제형사사법공조에 있어서 국제법의 일반원리인 상호주의란 역외 사법공조를 제공하는 만큼 자국도 역외 협조요청에 대해 동일하거나 유사한 범위 내에서 대응한다는 것으로, 대부분의 국가가 형사사법협력의 기본원칙으로 인식하고 있다.[372] 현재 상호주의에 따라 공조가 가능한 국가는 싱가포르, 대만 등으로 그 수는 적으나, 국제형사사법공조법 제4호에 의거하여 형사사법공조를 할 수 있다.[373]

2. 우리 형사법 이론과 실무의 방향

가. 협정(협약) 등을 검토한 역외 디지털 데이터 접근범위의 확대

우리 형사실무에 있어서도 양자 간 협의를 통하여 역외 디지털 데이터에 대한 접근범위를 확대해 볼 필요가 있다. 물론 데이터 수집과 관련된 국내 법률 및 사이버범죄방지조약의 규정과 관련된 국내법 등에 대해 이와 관련한 행정협정을 체결할지 여부에 대해서는 국제동향에 대해 신중히 검토해야 될 것이다.[374]

만일 '클라우드 법'은 행정협정을 체결할 것이라면 두 가지 사항을 요구한다. 먼저 데이터수집과 관련된 국내법이 실체법·절차법적으로 프라이버시(Privacy) 및 시민의 자유를 강력하게 보장하는 등 법률이 규정한 요건을 충족하여야 하며, 다음으로 사이버범죄방지조약 가입국이거나 국내법이 사이버범죄방지조약의 규정과 합치하는 등 사이버범죄·디지털 증거에 관한 적절한 실체법과 절차법이 있을 것을 요구한다.[375] 유럽의 사이버범죄협약에도 실체적 금지규정과 절차규정으로 구성되어 있는데 실체적 금지규정은 해킹범죄, 저작권침해범죄, 아동음란물범죄, 인터넷사

370) 조성훈, 앞의 논문, 276면.
371) 손창현, 앞의 논문, 256면.
372) 조성훈, 앞의 논문, 275면.
373) 정영수, 앞의 토론문, 251면.
374) 조성훈, 앞의 논문, 276면.
375) 조성훈, 앞의 논문, 277면.

기 등 네 가지가 주요한 내용이다.[376] 그러나 아직 우리나라는 사이버범죄방지조약에 가입되어 있지 않아 국내법이 조약의 내용과 완전히 합치되지는 않을 것이므로 개인정보보호법, 형사소송법을 비롯한 국가의 전반적인 정보관리 체계를 검토하고 재정비해야 한다.[377]

나. 역외 디지털 데이터관련 법제도의 정비

기존의 국제형사 규범의 2가지 중 하나는 먼저 다자간 조약을 통해 전통적 국제법 주체인 국가에 대한 제재를 넘어 국제범죄를 저지른 개인에 대한 처벌체계를 구축하는 것이다. 두 번째는 범죄인 인도로 대표가 되는 개별 각 국가의 협력체계인데, 이는 어떤 국제규범의 발전보다도 개별 각 국가가 형사사법권을 적절히 행사하는 것을 목표로 하는 것이다.[378]

그런데 디지털 증거에 관한 집행관할권 확장과 양자 간의 협력을 매개로 한 국제형사 규범의 발전은 위의 두 분야와는 성격이 다르다. 그 이유는 먼저, 국제형사규범의 발전이 다자간 조약보다는 양자 협정을 위주로 한 국제규범의 발전 과정이기에, 초국가적 사법기구의 성립을 전제로 하지 않는다는 점에서 전통적 의미의 국제형사법과 구별되며, 또한, 개별국가의 형사사법권 행사에 초점을 두지만 개별국가의 형사법의 내용을 실질적으로 수렴해 가는 성격을 갖는다는 점에서 범죄인 인도 절차와 구별된다.[379]

결국 국제적 협의를 통한 디지털 데이터의 공유를 확대하는 과정에서 개별 각 국가의 정보보호법제와 수사·증거의 핵심 내용이 융합되어 새로운 국제형사규범 개발이 촉진될 수 있고, 국가의 디지털 증거의 압수·수색시 정보수집 활동 유관정보 선별과정 관리차원에서 당사자의 참여권은 적법절차의 실질적 내용의 원칙으로 발전할 수 있을 것이다.[380]

376) <http://www.ltn.kr> 정완, 사이버범죄 방지 국제조약에 당장 가입해야 한다, 법조인 칼럼, 법률방송뉴스, (2019. 07. 05.)
377) 조성훈, 앞의 논문, 277면.
378) 조성훈, 앞의 논문, 278면.
379) 조성훈, 앞의 논문, 278면.

제5절 역외 디지털 증거 수집과 인권보장

1. 디지털 증거 수집과 정보인권보호

실체적 진실의 발견은 적정한 절차에 의하여 발견되어야 하므로 위법한 절차에 의하여 수집된 증거는 증거능력이 부정된다.[381] 역외 디지털 증거의 압수·수색에 대해서도 우선 그 수단이 실체적진실의 발견이라는 목적에 적합해야 될 것이고, 그 수단이 아니라면 실체적 진실발견이라는 목적을 달성할 수 없을 정도로 반드시 필요해야 될 것이며, 그로 인해 수사대상자의 프라이버시(Privacy)가 침해와 관련 당사자의 이익을 비교해 균형을 상실하지 않아야 할 것이다.[382]

테러범에 대한 대책으로 입법된 미국의 클라우드법도 개인정보보호와 인권보호의 측면에서 비판이 적지 않은 실정이다. 특히, 클라우드법(CLOUD Act)은 테러리즘이나 국가안보사범에 있어서는 매우 긍정적이지만, 우리나라의 경우 아직 사이버범죄방지협약은 가입하지 않았다. 데이터사용자를 보호하기 위한 국제적 합의와 해결방안이 필요하고 개인정보를 보호할 수 있게 될 것이며 심각한 권리 침해가능성이 있기 때문이다. 미국에서도 인권과 주요한 민주적 안전장치를 악화시키는 법안이라 평가하였다.[383]

2018년 11월 국내 금융그룹의 외국계 CLOUD 사용에 있어서 미국과 행정협정 체결시 국내 개인정보 침해에 대한 많은 우려가 있었다. 따라서 행정협정 체결 시, 상호주의 원칙에 따라 우리 기업이 저장 또는 관리하고 있는 데이터에 대해 미국이 영장 없이 제공 요청을 할 수 있게 되므로 이에 대한 대비가 필요하다는 것이다. 이처럼 외국의 현황을 보고 벤치마킹해서 개인 프라이버시(Privacy) 보호수준의

380) 조성훈, 앞의 논문, 280면.
381) 신호진, 형사소송법요론, 문형사, 2022, 15면.
382) 전현욱 외, 앞의 보고서, 424면.
383) <https://brunch.co.kr/@keepit/4> 미국의 클라우드법 파헤치기, (2022. 06. 29. 검색)

적정성에 관하여 구체적 기준을 마련해서 이를 충족한 때에만 개인정보를 이전할 수 있도록 관련된 규정을 마련할 필요가 있다.[384] 이로써 국민의 개인데이터를 역외에서 이전 및 활용하는 경우에도 국민의 개인 프라이버시(Privacy)를 안정적으로 보호 가능한 환경이 유지될 수 있도록 개인정보 관련 제도적 장치를 평가할 수 있는 관련 규정이 시급히 도입되어 적용되어야 할 것이다.[385]

더 나아가 인권보장의 역할을 충실히 할 때 수사의 효율성도 증대된다. 따라서 수사의 전문성을 강화하고 수사의 공정성을 보장한 인권보장과 국민 중심의 수사가 전개되어야 할 것이다. 앞으로 수사가 국민에게 전폭적인 신뢰를 얻기 위해서는 인권보장의 수사관행을 정착시키는 것 외에 전문성을 강화하는 것도 시급한 과제이다. 또한 검사의 기소를 보다 공정하고 정확하게 하여 국민의 신속한 재판을 받을 권리를 보장해야 할 것이다.

2. 피압수자의 정보인권과 참여권 보장

가. 서설

역외 디지털 데이터 압수·수색의 맥락에서 유관정보의 선별과정에 참여하는 당사자의 참여권이 '적법절차의 실질적 내용'의 핵심을 이루는 것은 극히 당연하다. 정보주체의 개인정보자기결정권 보호와 피의자의 방어권 보장이 디지털 데이터 압수·수색절차에서 보호되어야 할 핵심 법익이며, 그 수단은 당사자 참여권이기 때문이다. 당사자 참여권이 적법절차의 실질적 내용을 구성한다는 것은, 국제법 위반의 문제와도 맥락을 같이 한다.

오늘날의 개인정보보호는 단순한 사생활의 소극적 보호라는 차원을 넘어 헌법상 권리인 개인정보자기결정권의 중심으로 전개된다. 헌법재판소는 '십지지문날인제

384) 한정미, "미래산업 분야 법제이슈에 관한 연구(IV) -클라우드컴퓨팅 환경의 이용자 보호에 관한 법제연구-", 한국법제연구원, 2016, 41면.
385) 김형섭, 클라우드컴퓨팅에서의 개인정보 보호에 관한 법정책적 검토, 법과 정책연구, 제21권 제4호, 2021, 103면.

도에 대한 헌법소원' 사건에서 개인정보자기결정권을 '자신에 대한 정보가 언제 누구에게 어떤 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 권리'라고 정의한다.[386]

또한 흔히 '종근당 결정'으로 불리는 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정은 디지털 증거 압수·수색에 대한 절차적 통제 수단으로 참여권을 제시하였다. 유관정보 선별을 위한 저장매체 탐색 과정에서 피압수자의 참여권이 보장되어야 관련성 원칙(법 제106조 제1항, 제3항)이 준수될 수 있다는 취지이다. 아울러 참여권을 자백 강요에 대한 대응 수단인 진술거부권에 견주어, 저장매체를 대상으로 하는 디지털 증거의 압수·수색 과정에서 참여권이 보장되지 않으면 그 절차를 모두 위법하다고 보았다.

미국과 독일 등 선진국은 디지털 증거를 압수·수색할 때 수사기관에 영장 사본을 교부할 의무를 부여해 절차적 통제를 강화하고 있다. 미국 연방형사소송규칙은 "영장을 집행하는 수사관은 피압수자에게 영장 사본을 교부하여야 한다."고 규정되어 있다. 또한 독일 연방일반법원은 "수색영장은 형사소송법에 따라 관계인에게 원칙적으로 이유가 완전하게 기재된 정본 교부를 통해 고지되어야 한다. 관계인에게 수색영장 주문만 교부하고 이유가 기재된 완전한 영장을 교부하지 않는 행위는 헌법상 의문이 있다"고 판시하였다. 독일 연방일반법원은 압수가 비밀 처분이 아닌 공개 처분임을 근거로 예외를 두지 않고 영장 정본의 교부가 이루어져야 한다고 판시한 것이다.

나. 판례의 입장

(1) 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정

대법원은 수사기관의 디지털정보에 대한 압수·수색에 대하여, 원칙적으로 영장 발부의 사유로 된 범죄 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수

386) 헌법재판소 2005. 5. 26. 선고 99헌마513 등 결정.; 조성훈, 앞의 책, 106면.

사기관이 휴대한 저장매체에 해당 파일을 복제하는 방식으로 이루어져야 하고, 저장매체 자체를 직접 반출하거나 저장매체에 들어 있는 전자파일의 모든 정보를 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 반출하는 방식으로 압수·수색하는 것은 현장의 사정이나 디지털정보의 대량성으로 관련 데이터 획득에 긴 시간이 소요되거나 전문 인력에 의한 기술적 조치가 필요한 경우 등 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에 한하여 예외적으로 허용될 수 있을 뿐이라고 하였다.

따라서 문서출력 또는 파일복제의 대상은 반드시 혐의사실과 관련된 부분으로 한정되어야 하며, 혐의사실 관련성에 대한 구분 없이 임의로 저장된 디지털정보를 문서로 출력하거나 파일로 복제하는 행위는 원칙적으로 영장주의 원칙에 반하는 위법한 압수가 된다.

저장매체에 대한 압수·수색 과정에서 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란한 예외적인 사정이 인정되어 디지털정보가 담긴 저장매체 또는 하드카피나 이미징 등 형태를 수사기관 사무실 등으로 옮겨 복제·탐색·출력하는 경우에도, 그와 같은 일련의 과정에서 형사소송법 제219조, 제121조에서 규정하는 피압수·수색 당사자나 변호인에게 참여의 기회를 보장하고 혐의사실과 관련 되지 않은 디지털정보의 임의적인 복제 등을 막기 위한 적절한 조치를 취하는 등 영장주의 원칙과 적법절차를 준수하여야 한다.

만약 그러한 조치가 취해지지 않았다면 피압수자 측이 참여하지 아니한다는 의사를 명시적으로 표시하였거나 절차 위반행위가 이루어진 과정의 성질과 내용 등에 비추어 피압수자 측에 절차 참여를 보장한 취지가 실질적으로 침해되었다고 볼 수 없을 정도에 해당한다는 등의 특별한 사정이 없는 한 압수·수색이 적법하다고 할 수 없고, 비록 수사기관이 저장매체 또는 복제본에서 혐의사실과 관련된 디지털정보만을 복제·출력하였다 해도 다르게 볼 필요는 없다.

(2) 다수의견의 요지

이 사건에는 다음과 같은 쟁점이 문제되었다. 즉, ① 디지털정보에 대한 압수·

수색절차에서 당사자 참여권의 의미와 범위, ② 압수·수색 과정에서 나타난 위법이 중대한 경우 압수·수색 과정 전체를 하나의 절차로 파악하여 전체 압수·수색 처분을 취소하여야 하는지 여부, ③ 유관정보를 탐색하는 과정에서 우연히 별건의 무관정보가 발견된 때 수사기관이 그 무관정보를 적법하게 압수할 방법은 무엇인지에 관한 것이다.

(가) 디지털정보에 대한 압수·수색절차에서 당사자 참여권의 의미와 범위

다수의견에 의하면, 당사자 참여권은 혐의사실 관련성에 대한 구분 없이 이루어지는 디지털정보에 대한 복제탐색출력을 막는 중요한 절차이다.[387] 특히 저장매체에 대한 압수·수색 과정에서 예외적 사정이 인정되어 디지털정보가 담긴 저장매체 자체 또는 복제본을 수사기관 사무실 등으로 옮겨 복제탐색·출력하는 경우에도, 그 일련의 과정에서 참여권을 보장하고 혐의사실과 관련없는 디지털정보의 임의적 복제 등을 막기 위한 적절한 조치를 취하는 등 영장주의 원칙과 적법절차가 준수되어야 한다.[388]

나아가 다수의견은, 당사자 참여권이 실질적으로 보장되지 아니한 경우 그 흠결은 압수·수색절차를 적법한 것으로 평가할 수 없도록 하는 중대한 흠결에 해당하며, 설사 수사기관이 저장매체 또는 복제본에서 혐의사실과 관련된 디지털정보만을 복제출력하였다 해도 다르게 볼 필요는 없다고 판시해서 영장주의 원칙의 핵심 내용은 참여권 보장임을 확인하고 있다.

(나) 압수·수색 과정에서 나타난 위법이 중대한 경우 압수·수색 과정 전체를 하나의 절차로 파악하여 전체 압수·수색 처분을 취소하여야 하는지 여부

다수의견에 의하면, “압수·수색 과정 전체를 하나의 절차로 인식해서 그 과정에서 나타난 위법이 압수·수색절차 전체를 위법하게 할 정도로 중대한 경우 전체적으로 그 압수·수색 처분을 취소하여야 하고, 위법의 중대성은 위반한 절차조항

387) 대법원 2011모1839 전원합의체 결정.
388) 앞의 2011모1839 판례 참조.

의 취지, 전체과정 중에서 위반행위가 발생한 과정의 중요도, 그 위반사항에 의한 법익침해 가능성의 경중 등을 종합하여 판단한다.” 고 한다. 다수의견은 그 이유를 다음과 같이 설명한다.

즉, 디지털정보에 대한 압수·수색 과정에서 이루어지는 일련의 처분은 하나의 영장에 의한 압수·수색 과정에서 이루어지는바, 그러한 일련의 행위가 모두 진행되어 압수·수색이 종료된 이후에는 특정 단계의 처분만을 취소하더라도 그 이후의 압수·수색을 저지할 수는 없고 수사기관으로 하여금 압수·수색의 결과물을 보유하도록 할 것인지가 문제 될 뿐이라는 것이다. 달리 말하면, 수사기관이 위법하게 수집한 디지털정보를 보유할 일체의 법적 근거를 제거한다는 취지에서 전체적으로 압수·수색 처분을 취소한다는 취지로 이해된다.

(다) 유관정보를 탐색하는 과정에서 우연히 별건의 무관정보가 발견된 때 수사기관이 그 무관정보를 적법하게 압수할 방법

디지털정보에 대한 압수·수색이 종료되기 전에 혐의사실과 관련된 디지털정보(유관정보)를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 디지털정보(무관정보)가 우연히 발견된 경우에는, 수사기관은 더 이상의 추가 탐색을 중단하고 법원으로부터 별도의 범죄혐의에 대한 압수·수색영장을 발부받은 경우에 한하여 그러한 정보에 대하여 적법하게 압수·수색을 할 수 있다. 물론 포괄적인 압수·수색이라는 과잉금지의 원칙을 고려해야하지만 개별 구체적인 사건에 따라서는 범죄의 경중 또는 범죄혐의의 강도에 상응하게 맞는 적법한 절차에 따른 수사처분의 비례성원칙에 충족하여 판단해야 할 것이다. 최소한 압수의 적법성을 이를 가능하게 하는 수권규범의 존재만으로 인정되는 것이 아니라 당해 압수의 구체적인 집행이 형사절차의 법치국가적 정형성과 비례성의 원칙에 합치해야 하기 때문이다.[389] 또한, 이러한 별도의 압수·수색절차에서도 피압수자의 참여권을 보장하고 압수한 디지털정보 목록을 교부하는 등 피압수자의 이익을 보호하기 위한 적절한 조치가 이루어져야 한다.[390]

389) 이경렬, 앞의 논문, 508면.

(3) 판례분석

디지털정보나 정보저장매체를 외부로 반출한 이후의 실무상 제기되는 쟁점들로는 정보저장매체의 압수・수색의 종결시점, 외부로 반출한 이후의 행위의 법적성질, 참여권과 관련성의 상관성 등이 있다. 디지털정보나 정보저장매체의 외부로 반출한 이후의 각 단계별 참여권의 보장방법과 그 범위는 8단계로 구분하여 살펴볼 수 있다. 즉 외부장소에서의 정보저장매체의 봉인과 해제, 디지털정보에 대한 이미징의 단계, 디지털 포렌식 센터 증거사본 시스템에 저장 단계, 증거사본을 내려 받아 삭제 파일의 복구, 파일의 추출단계, 원격 디지털 공조시스템에 업로드 저장하는 단계, 디지털정보의 확인 단계, 디지털정보의 복사 또는 출력단계, 증거화 단계 중에서 봉인의 해제, 이미징의 단계, 삭제 파일의 복구, 파일을 추출하는 단계, 디지털정보의 탐색단계, 디지털정보의 복사 또는 출력단계에서는 피압수자의 참여권을 보장하여야 할 것이다. 특히 파일을 선별적으로 탐색하고 이를 출력하는 과정에서는 반드시 보장하여야 할 것이다.[391]

피압수자 참여권의 합리적 보장과 실체적 진실발견의 원활을 위한 모색방안으로는 피압수자 등이 참여권을 정당한 사유 없이 수사를 방해할 목적으로 일방적으로 연기한다든지 거절할 경우가 있을 수 있다. 이런 경우에는 수사기관은 종합적으로 판단하여 디지털 증거의 분석과 관련한 예규나 지침에서 각 단계별로 참여권을 신축적으로 보완하는 것도 필요하다. 피압수자 등은 수사기관이 연관이 없는 디지털정보를 탐색하는 경우라면 준항고 절차를 이용하여 다투어야 한다. 관련성 없는 디지털 데이터는 사건종결 후에는 즉시 폐기하도록 하고 이러한 사실을 피압수자 등에게 통보를 증명하는 확인서 등을 주는 방안도 있을 것이다.

390) 조성훈, “디지털 미란다 원칙 : 전자정보에 대한 압수・수색과 당사자의 참여권”, 사법 36호, 2016, 38면.

391) 조광훈, “정보저장매체 등을 외부로 반출한 이후의 절차에서 피압수자의 참여권을 둘러싼 실무상 쟁점과 해석론”, 영남법학 41권 0호, 2015, 195~196면.

다. 소결

당사자의 참여권 보장은 디지털 증거의 수집·분석 및 관리 규정 제21조[392]에 나와 있듯이 압수·수색·검증의 전 과정에 걸쳐 피압수자 등이나 변호인의 참여권을 보장해야 되고, 피압수자 등과 변호인이 참여를 거부하는 경우엔 신뢰성 및 전문성을 담보 가능한 상당한 방법으로 압수·수색·검증을 하여야 한다.[393] 공개된 강제처분은 수사기관의 무관정보에 대한 무분별한 접근을 막는 외에 적법한 권한 없는 정보접근을 막는 효과도 있을 것이다. 즉, 국제법 위반의 기준과 증거능력 판단의 기준은 일관성을 갖추고 상호 보완하면서 역외 디지털 데이터 압수·수색 과정의 적법성을 실질적으로 보장할 수 있을 것이다. 특히 디지털 증거에 대한 압수·수색 과정에서 당사자의 참여권을 어디까지 보장해야 하는 것인지 압수목록 교부 등 적법성을 확보할 수 있는지와 같은 법적 쟁점들이 중요하다.[394] 현재 대법원 판례 등에만 오롯이 의존해야 하는 상황이다 보니 선례가 없는 경우에는 확보된 디지털 증거의 증거능력에 대한 공방이 법정에서 치열하게 벌어지고, 결국 대법원 최종 판단이 나올 때까지는 적법성이 유동적인 상황에 직면하기도 한다.

3. 개인정보인권 보호와 별건수사 금지

독일 연방헌법재판소에서도 데이터저장매체에 대한 압수·수색 명령 효력을 다툰 2005년 결정에서 절차적 제한 수단으로 무관 정보의 환부를 들었는데, 독일형사소송법 제108조 제1항에서는 “수색을 하는 기회에 그 수사와는 관련이 없으나, 다른 범죄를 암시하는 대상물이 발견된 경우, 이를 임시로 압수할 수 있다.”라고 규정하며 ‘독립적 압수·수색’이라고 칭한다.[395] 여기서 디지털 증거 압수·수색에

392) 디지털 증거의 수집·분석 및 관리 규정 제21조 (참여권의 보장)
393) 권양섭, “디지털 증거의 증거능력에 관한 대법원 판례 분석 -위법수집증거와 증거능력을 중심으로-”, 디지털 포렌식 연구 제 13권 제1호, 2019, 6면.
394) 조성훈, 앞의 발표문, 176면.
395) 정찬욱, “형사절차상 범죄혐의에 관한 연구”, 전남대학교 박사학위논문, 2022, 128~129면.

도 독립적 압수・수색이 적용되기 때문에, 정보저장매체를 수색하면서 별거 범죄인 데이터를 우연히 발견한 경우에는, 수색이 본래의 범죄혐의와 관련성이 있다면 우연히 발견한 정보의 증거능력은 인정될 것이다.[396]

예시로 우편물 압수 중에 당해 사건 수사와 관련성은 없으나 다른 범행을 암시하는 우편물(Sendung)이 발견된 경우에는 제108조를 준용하여 우연한 발견물(Zufallsfunde)로 다루게 된다.[397] 또한, 증거와 관련된 서버가 해외에 있는 경우는 국외의 주권 침해 및 사법공조협약의 내용과 연관되므로 다양한 문제가 생겨날 소지가 있다.[398]

또한, 개인이 소지하고 있는 스마트폰의 경우, 그 사람의 인생 전부가 담겨 있다고 보아도 과언이 아니다. 뿐만 아니라 그 사람의 하루 일상, 시간대별 행적, 가는 장소, 매 순간마다의 언행 등 민감한 개인정보 거의 전부가 그 안에 다 들어있다. 이 정보들이 수사기관에 노출된다면 그 사람은 수사기관 앞에 거의 벌거벗은 상태가 된다. 특히 스마트폰 압수 후 이를 통한 원격 압수・수색이 허용될 경우 방대한 양의 정보를 수사기관이 수집할 수 있고, 이에 따라 개인의 프라이버시(Privacy) 침해 위험성뿐 아니라, 별건수사로 이어질 가능성도 더욱 커진다. 이러한 수사기관의 불가피한 기본권 침익적 행위는 적법절차(Due Process)의 원칙을 준수하여 디지털 증거는 엄격히 적법한 절차를 준수해 수사상 필요한 범위 내에서 수집과 분석 및 관리[399]되어야 하며, 개인의 프라이버시(Privacy) 보호라는 헌법적 가치를 이익 형량하여 필요 최소한의 범위 내에서 이루어져야 한다.

최근 형사소송법이 개정(시행 2022. 9. 10. 법률 제18862호, 2022. 5. 9. 일부개정)되었는데 특히 법 제196조(검사의 수사)의 제2항과, 법 제198조(준수사항) 제4항을

396) 박병민・서용성, 앞의 보고서, 140면.
397) BeckOK StPO(21 Ed., 2015)/Graf StPO § 100 Rn. 19.79) Allgayer, Die Verwendung von Zufallserkenntnissen aus Überw.; 김성룡, 전자정보에 대한 이른바 “‘별건 압수・수색’-대법원 2015. 7. 16. 선고 2011모1839 전원합의체 결정의 평석을 겸하여-”, 형사법의 신동향 제49호, 2015, 137면.
398) 김성룡, 앞의 논문, 137면.
399) 디지털 증거의 수집・분석 및 관리 규정 제4조 (적법절차의 준수)

보면, 제196조 제2항에서는 검사가 보완수사를 할 때는 “해당 사건과 동일성을 해치지 아니하는 범위 내에서” 수사할 수 있게 하였고, 제198조 제4항에서는 “수사 중인 사건의 범죄 혐의를 밝히기 위한 목적으로 합리적인 근거 없이 별개의 사건을 부당하게 수사하여서는 아니 되고, 다른 사건의 수사를 통하여 확보된 증거 또는 자료를 내세워 관련 되지 않은 사건에 대한 자백이나 진술을 강요하여서도 안 된다.” 고 하여 검찰을 포함한 모든 수사기관이 수사할 때 아예 별건수사를 하지 못하도록 법제화 하였다.

디지털 정보의 압수·수색과정에서 영장범죄 사실과 관련 되지 않은 범죄의 증거가 발견했다면 수사기관은 바로 별도의 압수·수색 영장을 발부받아야 되고 이를 집행하려면 피압수자 측의 참여권을 보장해야만 별건 범죄에 대한 증거가 수집된 증거가 적법하게 유죄의 증거로 사용이 가능하다고 볼 것이다.[400] 또한 디지털 증거의 처리 등에 관한 규칙에는 관련된 디지털 정보를 탐색하는 과정에서 별도의 범죄 혐의를 발견한 경우 별건 혐의와 연관된 추가 탐색을 중단해야 한다.[401] 고 규정되어 있고, 디지털 증거의 수집·분석 및 관리 규정 제22조에는 범죄혐의와 기본적인 사실관계가 동일하거나 동종·유사 범행과 연관있는 의심될 만한 상당한 이유가 있는 범위 내, 즉 필요한 범위 내의 전자정보[402]를 압수할 수 있다고 되어 있다. 결국 위법하게 수집된 증거에 기해 수집된 모든 증거의 증거능력은 부정하는 것이 타당하다.

400) <https://www.yulchon.com/mail/201605/newsletter/sub3.html> 김태균, ‘전자정보에 대한 압수·수색 과정 중 이루어진 이른 바 별건압수·수색에 관하여’, 율촌 뉴스레터, (2022. 06. 30. 검색)

401) 디지털 증거의 처리 등에 관한 규칙[시행 2021. 8. 30.] [경찰청훈령 제1030호, 2021. 8. 30. 타법개정.] 제20조 (별건 혐의와 관련된 전자정보의 압수)

402) 디지털 증거의 수집·분석 및 관리 규정 제22조 제1항 (관련성의 판단기준)

제6장 결 론

오늘날 정보통신기술의 급속한 발전과 함께 점증하는 사이버 범죄는 국가를 초월하여 발생하고 있어 역외 디지털 데이터 수집문제는 날로 중요해지고 있다. 디지털 데이터가 압수·수색의 대상인지 여부, 정보자체가 원격지의 서버에 존재하는 경우임에도 정보통신망을 이용해서 접근한 것도 압수·수색이 가능할 것인지 여부, 그 절차에 대하여 별도 규정이 없기 때문에 법률 해석에 의해 압수·수색의 가능성과 압수·수색영장의 집행방법에 대해 적정성 여부를 검토해야 한다.

대법원도 모든 형태의 역외 압수·수색의 허용이 아니라, 수사기관이 적법하게 얻은 계정정보를 이용해서 서버에 접속했을 경우에만 적법하다고 판단하고 있다. 그러나 계정 접속을 통해서의 역외 압수·수색은 허용성과 관련해서 계정의 취득과 관련된 개인정보 침해문제, 압수·수색 절차상의 문제 등이 발생된다. 각종 정보통신기술을 사용하여 데이터 범죄에 대처하기 위해서는 디지털 기술들이 서서히 발전하고 특히 역외 디지털 증거수집이 중요성을 더해가고 있는 상황에서, 역외 디지털 증거 압수·수색의 디지털 증거수집에 대한 적법성은 계속 문제될 수 있으므로 객관적인 적법성 확보를 위한 다양한 방안의 마련이 필요하다.

인권보호 측면에서도 유럽 사이버범죄협약과 미국과의 행정협정에 대해 적극 검토하여 역외디지털 증거에 접근할 수 있도록 하여야 한다. 현재 일본·독일·프랑스 형사소송법은 원격 압수를 허용하며, 역외 압수는 유럽이사회 사이버범죄조약이 이용자의 적법하고 자발적인 동의를 전제로 허용하고 있으며, 독일과 일본은 원격 압수·수색을 형사소송법에 명문으로 규정하고 있다. 해외 주요 국가는 이를 입법적으로 해결하고 있으나, 우리 형사소송법은 이에 대한 명문규정이 없기 때문에 유럽의 사이버범죄방지협약을 벤치마킹해서 방안을 마련함이 바람직하다.

더구나 e-메일의 압수·수색은 압수·수색의 목적물이 존재하는 장소가 아닌 다른 장소에서 이루어 질 수도 있고 정보저장서버 관리자의 관여가 전혀 없이 이루어질 수 있으므로 그 유럽 사이버범죄협약 제18조와 일본 형사소송법 제99조 제2

항에서 기록명령부 압수제도 및 제110조 제2항에서 제출명령을 참고하여 형사소송법 106조 제5항에 관련 규정을 마련하는 방안으로 입법안을 제시해 봄으로써 국제적인 융합으로 발전할 수 있을 것으로 판단된다.

무엇보다, 새로운 증거 유형인 디지털 증거에 대하여 압수·수색 관련 규정이 아직도 미흡하고, 형사소송법상 압수·수색의 목적물도 정보저장매체로 규정하고 있어 개념이 확립되지 않은 상황이며, 적법절차 원칙을 보장하기 위한 각종 절차규정이 유체물을 전제로 한 것이어서 현실에 맞는 수사실무 운영에 한계가 있다. 또한 디지털 데이터의 다양성·대량성·증거분석의 복잡성 등으로 기존 방식 외에 새로운 방식이 필요하다. 따라서 영장에 구체적 집행방법을 기재하는 사전통제나 위법수집증거 배제법칙을 매개로 한 공판절차의 사후통제도 비실효적이고, 미흡한 대응이 될 수 있으므로 법원의 사전통제 및 사후통제에 더하여 당사자 참여권을 매개로 하는 중간단계의 통제를 강화할 필요가 있다.

특히 수사기관의 불가피한 기본권 침익적 행위는 적법절차의 원칙과 개인의 법률프라이버시(Privacy) 보호라는 헌법적 가치를 형량하여 필요한 만큼 최소한으로 이뤄져야할 것이다. 궁극적으로, 수사에 있어서는 실체적 진실의 발견만큼 중요한 것은 올바른 절차를 따르고 수사 단계 중에서 인권을 존중하는 것이다. 과학수사를 통해서 인권을 존중하면서도 실체적 진실을 밝혀내야 수사과정이 국민의 신뢰를 받기 위한 전제조건이 되는 것이다. 그러므로 과학 수사와 합리적 사고 및 전문지식으로 무장한 전문수사관들을 더욱 양성에 힘쓰고 전문인력의 수사를 강화해 인권존중의 수사관행을 확립하고 수사역량을 강화하도록 하여야 할 것이다.

<참고문헌>

1. 단행본

김대순, 국제법론(제20판), 삼영사, 2019.
신동운, 간추린 신형사소송법(14판), 법문사, 2022.
신호진, 형사소송법요론, 문형사, 2022.
이관희, 범죄수사입문, 박영사, 2021.
이관희・이상진, 디지털 증거법, 박영사, 2022,
이은모, 기본강의 형사소송법(제3판), 박영사, 2020.
이은모・김정환, 형사소송법(제7판), 박영사, 2019.
이주원, 형사소송법, 박영사, 2019.
이주호・김호, 판례로 본 디지털 증거법, 북랩, 2020.
이창현, 형사소송법(제6판), 정독, 2020.
정웅석・최창호, 형사소송법, 대명출판사, 2017.
정해상, 과학수사와 범죄, 일진사, 2020.
조성훈, 역외 전자정보 압수・수색 연구, 박영사, 2020.

2. 국내논문

강미영, “디지털 증거의 증거능력”, 외법논집 제43권 제3호, 2019.
권양섭, “경찰의 디지털 증거 수집 및 가이드라인 제정을 위한 실태조사 연구”, 원광법학 제33권 제2호, 2017.
_____, “디지털 증거의 증거능력에 관한 대법원 판례 분석 -위법수집증거와 증거능력을 중심으로-”, 디지털 포렌식 연구 제 13권 제1호, 2019.
김기범・이관희・장윤식・이상진, “정보영장 제도 도입방안 연구”, 경찰학연구 제11권 제3호, 2011.

김범식, “경찰현장수사에서 디지털 증거에 대한 압수·수색의 개선방안”, 외법논집 제38권 제4호, 2014.

김재운, “미국의 클라우드법(CLOUD Act)상 대테러정책 연구”, 한국테러학회보 제33호, 2018.

김성룡, 전자정보에 대한 이른바 “‘별건 압수·수색’-대법원 2015. 7. 16. 선고 2011모1839 전원합의체 결정의 평석을 겸하여-”, 형사법의 신동향 제49호, 2015.

김윤섭·박상용, “형사증거법상 디지털 증거의 증거능력 -증거능력의 선결요건 및 전문법칙의 예외요건을 중심으로-”, 형사정책연구 제26권 제2호, 2015.

김한균·김성은·이승현, “사이버범죄방지를 위한 국제공조방안 연구 -유럽사이버범죄방지협약을 중심으로-”, 대검찰청, 2009.

김현수, “적법한 압수·수색의 요건에 관한 고찰”, 인권과 정의 통권 제490호, 2020.

김형섭, 클라우드컴퓨팅에서의 개인정보 보호에 관한 법정책적 검토, 법과 정책연구, 제21권 제4호, 2021.

노명선, “전자적 증거의 수집과 증거능력에 관한 몇 가지 검토”, 형사법의 신동향 통권 제16호, 대검찰청, 2008.

독고지은, “디지털 증거 압수·수색에 대한 개정 형사소송법의 규제와 집행에 관한 연구”, 고려대학교 박사학위논문, 2013.

박경신, “E-메일 압수·수색의 제문제와 관련 법률개정안들에 대한 평가”, 법학연구 13권 2호, 2010.

박민우, “디지털 증거 압수·수색에서의 적법절차”, 고려대학교 박사학위논문, 2016.

박병민, “디지털 증거 압수·수색의 절차적 규제 개선방안 -참여권강화, 영장사본교부제도 도입 등-”, 2021 공동학술대회 디지털 증거 압수·수색 개선방안, 2021.

박병민·서용성, “디지털 증거 압수·수색 개선방안에 관한 연구 -법률개정에 관한 논의를 중심으로-”, 사법정책연구원 보고서, 2021.

박봉진・김상균, “디지털 증거 압수・수색에 관한 연구”, 법과 정책 제19집 제1호, 2013.

박석훈, “제3자 보관 디지털 증거에 대한 원격지 압수・수색 체계에 관한 연구”, 고려대학교 박사학위논문, 2016.

_____, “전자증거의 압수・수색 및 임의제출 과정에서의 데이터 범위 한정가능성”, 법조 제64권 제6호, 2015.

박혁수, “개정 형사소송법상 디지털 증거의 증거능력 -관련성, 신뢰성, 진정성, 원본성을 중심으로-”, 해외연수검사 연구논문집 제25집, 2010.

박희영, “독일의 사이버범죄방지조약의 비준에 관한 법률(下)”, 법제, 2009.

박희영・최호진・최성진, “사이버범죄협약 이행입법 연구”, 대검찰청연구용역보고서, 2015.

방경휘, “독립적 긴급 압수・수색 제도의 필요성에 관한 재고찰”, 숭실대학교 법학논총 제50권, 2021.

서주연, “클라우드 컴퓨팅 환경에서의 디지털 증거 확보에 관한 논의”, 전북법학 제64집 2020.

손지영・김주석, “디지털 증거의 증거능력 판단에 관한 연구”, 대법원 사법정책연구원 연구보고서, 2015.

_____・_____, “압수・수색 절차의 개선방안에 관한 연구”, 사법정책연구원, 2016.

손 진, “해외 서버 압수・수색에 대한 연구 -미국의 예-”, 대검찰청 형사법아카데미 자료집, 2017.

손창현, “사이버테러에 대한 대응방안으로서의 디지털 증거 압수・수색”, 비교형사법연구 21권 3호, 2019.

_____, “사이버테러 대응방안으로서의 디지털 증거 압수・수색에 대한 비교법적 고찰 -원격 압수・수색 및 제3자 보관 정보에 대한 압수・수색을 중심으로 한 정책 제언-”, 한국공안행정학회보, 제28권 제3호, 2019.

송영진, “미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점”, 형사정책연구 제29권 제2호, 2018.

신도욱, “원격 압수·수색의 적법성 -해외에 존재한 서버에 저장된 이메일 압수·수색을 중심으로-”, 법조 제67권 제3호, 2018.

신상미, “온라인수색의 법률적 문제점과 허용가능성”, 경찰학연구 제20권 제3호, 2020.

신용우, “유럽 사이버범죄 방지 협약 체결 현황과 우리나라의 입법·정책적 대응 방향 “, 국제관계 동향과 분석 제77호, 2020.

오경식·김창우, “안보형사법상 증거재판주의와 자유심증주의의 이론과 실제”, 형사법의 신동향 제70권, 2021.

윤신규, “수사 단계에서 확보한 법과학 증거의 요건과 질적 수준”, 한국과학수사학회지 제16권 제1호, 2022.

이경렬, “디지털정보 관련 증거의 압수·수색 규정의 도입방안 연구”, 홍익법학 제13권 제3호, 2012.

이경렬·하건우, “유럽평의회 사이버범죄조약 가입·비준을 위한 국내 이행법률의 마련과 준비 비교”, 비교형사법연구 제19권 제4호, 2018.

이기리, “ ‘유동적 위법’ 개념을 통한 영장, 임의제출에 의한 디지털 증거의 압수·수색과 증거능력의 이해”, 사법발전재단 제1권 제54호, 2020.

이기수·민수현, “한국과 중국의 사이버범죄 형사사법공조 강화를 위한 법 개정 검토 -유럽 사이버 범죄협약을 기준으로-”,비교형사법연구 제19권 제4호, 2018.

이동현, “디지털 증거의 수집 관련 국제 공조 방안 -형사사법공조 절차의 문제점과 이를 해결하기 위해 미국 실무상 논의되는 방안을 중심으로-”, 법과학의 신동향 통권 제1호, 2020.

이수용·임규철, “역외 압수·수색의 절차적 위법성에 대한 비판적 소고”, 비교법연구 제18권 2호, 2018.

이순옥, “디지털 증거의 역외 압수·수색 -대법원 2017. 11. 29. 선고 2017도9747 판결을 중심으로-”, 중앙법학 제20집 제1호, 2018.

_____, “디지털 증거의 압수·수색절차에 관한 판례 연구”, 중앙법학 제19집 제2호, 2017.

이 용, “디지털 증거의 보전명령제도에 관한 고찰”, 법조 제64권 제12호(통권 제711호), 2015.

_____, “디지털 증거 수집에 있어서의 협력의무”, 서울대학교 법학연구소 법학연구총서 60, 2016.

이원상, “수사절차에서 통신자료 활용에 따른 쟁점 고찰”, 형사소송 이론과 실무 제7권 제1호, 2015.

_____, “디지털 증거의 증거능력, -관련성과 전문증거에 대한 최근 판례 견해를 기반으로-”, 국민대학교 법학연구소 주최 학술회의 발표논문, 2016.

이윤제, “디지털 증거 압수·수색영장의 집행에 있어서 협력의무”, 형사법연구 제24권 제2호, 한국형사법학회, 2012.

이인곤, “형사절차상 디지털 증거 압수·수색에 대한 문제점과 개선방안”, 한국경찰연구 제15권 제4호, 2016.

이인곤·강철하, “클라우드 컴퓨팅 환경에서 전자정보 압수·수색의 문제점과 개선방향”, 형사법의 신동향 제54호, 2017.

이재윤·강민구, “ 디지털 증거 역외 압수·수색 쟁점 고찰”, 한국산업보안연구 제9권 제2호, 2019.

이정민, “외국계 이메일 계정에 대한 압수·수색의 정당성 -[대상판결1] 서울고등법원 제12부 2017. 6. 13. 선고 2017노23, [대상판결2] 서울고등법원 제8형사부 2017. 7. 5. 선고 2017노146-”, 비교형사법연구 제19권 제3호, 2017.

장상귀, “디지털 증거의 증거능력에 관한 연구”, 법학교수·검찰 실무연구회 발표자료집(Ⅰ), 대검찰청, 2009.

장석준, “임의제출된 정보저장매체에 저장된 전자정보의 증거능력”, 사법발전재단 제1권 제59호, 2022.

장응혁, “디지털 증거의 압수·수색에 있어서 전문가 참여의 법적 성격 검토”, 디지털포렌식연구 제15권 제1호, 2021.

전명길, “디지털 증거의 압수·수색에 있어서 참여권에 관한 연구”, 인문사회21, 제8권 제2호, 2017.

전승수, “디지털 증거 압수절차의 적정성 문제 -피압수자 참여 범위 및 영장 무관

정보의 압수를 중심으로-”, 형사판례연구 제24권, 2016.

전현욱・윤지영, “디지털 증거 확보를 위한 수사상 온라인 수색제도 도입 방안에 대한 연구”, 한국형사정책연구원 연구보고서, 2012.

전현욱・이자영, “사이버범죄협약과 형사절차상 적법절차원칙 -저장된 데이터의 보존 및 일부 공개를 중심으로-”, 형사정책연구 제25권 제2호, 2014.

정대용・김기범・권헌영・이상진, “디지털 증거의 역외 압수・수색에 관한 쟁점과 입법론 -계정접속을 통한 해외서버의 원격 압수・수색을 중심으로-”,법조 제65권 제9호, 2016.

정대용・김기범・이상진, “수색 대상 컴퓨터를 이용한 원격 압수・수색의 쟁점과 입법론”,법조 제65권 제3호, 2016.

정병곤, “디지털 증거의 수집과 증거능력에 관한 연구”, 조선대학교 박사학위논문, 2012.

정성남, “경찰 수사현장에서 디지털 증거의 압수・수색에 관한 연구 -스마트 폰을 중심으로-”, 인천대학교 박사학위논문, 2020.

정소연, “디지털 증거의 역외 압수・수색에 대한 법적 고찰”, 디지털포렌식연구 제11권 제1호, 2017.

정영수, “역외 전자정보 수집의 범위와 한계 -국가관할권의 확정과 위법수집증거 배제 법칙의 적용을 중심으로-”, 제11회 한국형사학대회 학술대회 토론문, 2022.

정웅석, “개정법상 진술서 등의 증거능력에 관한 고찰”, 저스티스 통권 제158권 제3호, 2017.

정찬욱, “형사절차상 범죄협의에 관한 연구”, 전남대학교 박사학위논문, 2022.

조미지・송영진, “형사절차상 디지털 증거 압수・수색 법제에 관한 비교법적 고찰 -러시아 형사소송법과의 비교를 중심으로-”, 입법과 정책, 제13권 제3호, 2021.

조광훈, “디지털 증거의 압수・수색의 문제점과 개선방안”, 서울법학 제21권 제3호, 2014.

_____, “정보저장매체 등을 외부로 반출한 이후의 절차에서 피압수자의 참여권을

둘러싼 실무상 쟁점과 해석론”, 영남법학 41권 0호, 2015.

조성훈, “디지털 미란다 원칙 : 전자정보에 대한 압수·수색과 당사자의 참여권”, 사법 36호, 2016.

“역외 디지털 증거의 수집과 국제형사규범의 발전”, 단국대학교 법학논총, 제43권 제3호, 2019.

_____, “역외 전자정보 수집과 국가관할권 행사의 합리성 이론 -미연방 ‘클라우드 법’의 제도적·법이론적 기원에 대한 분석을 중심으로-”, 형사정책연구 제32권 제1호(통권 제125호), 2021.

_____, “역외 전자정보 수집의 범위와 한계 -국가관할권의 확정과 위법수집증거배제 법칙의 적용을 중심으로-”, 제11회 한국형사학대회 학술대회 발표문, 2022.

최윤정, “전자정보 압수·수색에 적용되는 영장주의 원칙과 그 예외에 관한 법적 검토”, 저스티스 통권 제153호, 2016.

최재민·신대민·이상진·임종인, “물리적 복구방법을 활용한 디지털 포렌식 기술”, 한국방송공학회, 2007.

한성훈, “디지털 증거의 압수·수색의 합리화 방안에 관한 연구”, 홍익법학 제16권 제3호, 2015.

한정미, “미래산업 분야 법제이슈에 관한 연구(Ⅳ) -클라우드컴퓨팅 환경의 이용자 보호에 관한 법제연구-”, 한국법제연구원, 2016.

3. 외국문헌

加藤康榮, “無令状捜索差押えの許容範囲--「緊急捜索差押え」の可否を巡って” 日本法学 第76巻 第4号, 日本大学法学研究所, 2011年.

後藤昭＝白取祐司『新・コンメンタール刑事訴訟法』[第3版](日本評論社 、 2018年.

우지이에 히토시, “일본의 전자적 증거 압수에 관한 2011년 개정법 소개”, 형사법의 신동향 통권 제49호, 2015. 12.

히라라기토키오 저·조균석 역, 일본 형사소송법, 박영사, 2012.

Ahmed Ghappour, “Searching Places Unknown : Law Enforcement Jurisdiction on the Dark Web”, 69 Stanford Law Review 1075(2017)

Devin M. Adams, “COMMENT : The 2016 Amendments to Criminal Rule 41 : National Search Warrant to Seize Cyberspace, “Particularly” Speaking”, Richmond Law Review Symposium Book volume 51.

UNODC · CTED · IAP,『Practical Guide for Requesting Electronice Evidence Across Borders』(e-book).

United States v. Microsoft Corp. 584 US 2018.

In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, No. 13 Mag. 2814, 2014 WL 1661004(S.D.N.Y. Apr. 25, 2014).

Microsoft v. United States, No. 14-2985 (2d Cir. 2016); In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., Case No. 14-2985 (2d Circuit July 14, 2016).

CLOUD Act, H.R. 1625, 115th Cong. div. V, § 103(b) 2018. (18 U.S.C. §2703(h)).

T-CY, (Draft) elements of an Additonal Protocol to the Budapest Convention on Cybercrime regarding tranboder access to data(2013), -proposal prepared by the Ad-hoc Subgroup on tranboder access.

Law Commission, “Search Warrants”, Consultation Paper No235, 2018.

4. 기타 참고자료

김경환, [판례해설] “해외 서버에 저장된 e-메일에 대한 압수·수색”, 법률신문 2017. 9. 12.

디지털 증거의 수집·분석 및 관리 규정<대검예규 제1151호, 2021. 1. 1. 시행>

대검찰청, 형사소송법 개정과 개인정보 보호법의 시행에 따른 디지털 증거 압수·수색의 신뢰성 확보 방안에 관한 연구, 2012.

박병민 판사(사법정책연구원) 발표문, 2021 공동학술대회 “디지털 증거 압수·수색

개선방안”, 2021.

박병민・서용성, “디지털 증거 압수・수색 개선방안에 관한 연구 -법률개정에 관한 논의를 중심으로-”, 사법정책연구원 보고서, 2021.

이태한, [판례해설] “카카오톡 서버에 대한 압수・수색 취소”, 법률신문 2016. 3. 14.

입법조사처, “정보저장매체에 관한 압수・수색제도의 문제점과 개선방안”, 2015.

한국형사정책연구원(전현욱・이상미), “형사절차상 디지털 증거의 압수・수색 및 증거능력”, 형사정책연구원 대검찰청 법무・법제(형사법제 등) 전문검사 커뮤니티, 2014. 12. 19.