Journal of The Korea Society of Computer and Information
Vol. 22 No. 2, pp. 133-139, February 2017
www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.02.133

A study on procedures of search and seize in digital data

Kim - Woon Gon*

Abstract

Today, the activities of individuals and corporations are dependent not only on digital technology but also on the future of society, which is referred to as the fourth industrial revolution.

Since the traces that arise from the crimes that occur in the digital society are also inevitably developed into a society that should be found in the digital, the judicial dependence of judging by the digital evidence is inevitably increased in the criminal procedure.

On the other hand, considering the fact that many users are using virtual shared computing resources of service providers considering the fact that they are being converted into a cloud computing environment system, searching for evidence in cloud computing resources is not related to crime. The possibility of infringing on the basic rights of the criminal procedure is increased, so that the ability of evidence of digital data which can be used in the criminal procedure is limited.

Therefore, considering these two aspects of digital evidence, this point should be fully taken into account in judging the evidence ability in the post-seizure warrant issuance and execution stage as well as the pre-emptive control. There is a view that dictionary control is useless, but it needs to be done with lenient control in order to materialize post-modern control through judging ability of evidence.

In other words, more efforts are needed than ever before, including legislation to ensure proper criminal procedures in line with the digital age.

▸ Keyword : Digital data, Evidential digital data, Admissibility of evidence, Hearsay rule, Evidence of illegal collection

I. Introduction

우리는 현재, 디지털 기술과 인터넷으로 대표되는 네트워크를 통해 기존의 시공간을 뛰어 넘는 새로운 공간 속에서, 무한한 정보의 유통이 이루어지고 있는 디지털 시대에 살고 있다. 또한 최근 시대적 화두로 떠오른 4차 산업혁명은 인공지능의 출현으로 사람의 두뇌를 대체하는 시대의 도래를 포함하기 때문에 경제적인 면에서나 사회적인 면에서 많은 변화를 초래하는 전환점이 될 것으로 전망된다.[1] 즉 자동화와 연결성의 극단이라 볼 수 있는 사회가 도래하기 때문에 그 사회 속에서 발생되는 범죄적 양상이나 발생된 범죄에 대응하는 형사절차도 많은 변화를 초래할 수밖에 없기 때문에 많은 기대와 우려를 낳고 있다.

자동화와 연결성의 극단적 사회는 디지털 기술이 우리의 모든 생활영역을 지배하고 있기 때문에 디지털 기기의 도움이 없으면 일상생활도 불편할 뿐만 아니라, 발생된 범죄의 수사에서도 디지털 기기 속에 숨겨진 범죄의 흔적을 찾아내지 않고서는 그 범죄를 해결하기 어려운 사회로 되어 가고 있다.[2]

즉 범죄행위자들은 디지털 기기에 남아있는 범죄의 흔적을 지우기 위하여 노력하고, 수사기관은 그 지워진 범죄흔적을 복원하여 잘 찾아낼 수 있느냐에 따라 범죄로부터 우리 사회를 안전하게 보호할 수 있느냐의 성공여부가 달려 있을 정도이다.

그럼에도 불구하고, 우리나라 형사소송법은 산업사회 방식의

• First Author: Woon-Gon Kim, Corresponding Author: Woon-Gon Kim
*Woon-Gon Kim(john1216@cst.ac.kr), Dept. of Maritime Police, Chosun College of Science & Technology.
• Received: 2017. 01. 20, Revised: 2017. 01. 27, Accepted: 2017. 02. 03.

형사소송절차를 근간으로 하고 있기 때문에 많은 충돌이 일어날 수밖에 없고, 그로 인하여 형사사법절차를 통한 범죄예방이나 범죄의 회복이 제대로 이루어지지 못하고 있다.

그 단적인 예가 다단계 사기범 조○○의 사건이라고 할 수 있다. 이 사건의 범죄자들은 디지털 데이터에 남아있는 범죄의 흔적을 지우고자 관리 서버를 30차례나 덮어쓰기로 증거를 훼손하였고, 수사기관은 이 디지털 증거를 7년 동안이나 찾지 못하면서 많은 피해자가 있는 사건이었음에도 수사가 답보된 분노를 샀던 사건이다.

그러다 2015년 검찰은 디지털수사과의 지원을 받아 2조8000억 원대로 알려진 사기 규모를 5조715억 원으로 밝혀내고, 공범들의 금융·통신기록을 분석해 710억 원의 은닉재산을 환수할 수 있었다.[3]

이처럼 최근 일어나고 있는 범죄를 해결하는 관점은 디지털 증거를 제대로 분석하여 증거능력을 인정받을 수 있는 증거를 찾아낼 수 있느냐에 달려있을 정도로 디지털 데이터와 관련된 압수수색과 그에 대한 증거능력의 중요성이 대두되고 있다.

더군다나 사회 구성원의 모든 사람이 디지털화 된 기기를 함께 사용하는 사회로 발전되어 감에 따라, 범죄수사에 활용되는 디지털 자료 속에는 수사의 목적이 된 범죄행위와는 전혀 관련이 없는 사람들의 디지털 자료도 혼합되어 있는 상태로 존재하재 하게 되면서 수사자료를 수집하는 과정에서 범죄와 관련없는 일반인의 디지털 자료가 노출될 위험이 상존하고 있다.

이와 같은 상황을 고려해보면 범죄자를 검거하고 처벌함으로써 형사사법정의를 확립하여야 하면서도 또 한편으로는 범죄와 관련 없는 개인의 디지털 데이터를 보호해야 할 필요성이 디지털 데이터와 관련된 형사사법절차에서 중요한 과제이다.

여기에서는 디지털 데이터의 증거능력과 관련된 대법원 판례의 태도와 2016. 5. 19. 국회 본회의를 통과해 개정된 형사소송법상의 관련 규정들을 검토해 보고자 한다.

II. Aadmissibility of evidence of Digital Data

전통적인 방식의 범죄수사는 범죄행위자가 범죄행위 과정에서 나타나는 흔적을 찾아내는 것이 수사의 기본이다. 따라서 아날로그 시대에는 아날로그 형태로 나타난 흔적을 찾아내느냐가 수사의 목적을 달성하는데 중요한 관건이 되었듯이, 사회의 구성이 모두 디지털화 되어가고 있는 현대 사회에서는 디지털화된 흔적을 찾아내는 것이 수사의 목적을 달성하는데 관건이 될 수밖에 없기 때문에 현대 사회에서 수사는 디지털 증거를 제대로 찾아내고 분석할 수 있느냐에 달려 있다.

따라서 여기에서는 디지털 증거가 갖는 특징을 살펴보고, 그 특징에 따라서 증거능력을 인정받기 위해서는 어떻게 해야 하는지를 대법원 판례를 통해 검토하고자 한다.

1. Characteristics of digital evidence

디지털 증거는 일반 물리적 증거에 비해 매체의 독립성, 비가시성과 비가독성, 취약성(복사·변조·삭제의 용이성), 대량성, 네트워크 관련성, 초국경성 등의 특징을 가지고 있다.[4] 이런 특성과 더불어 암호화된 파일들을 가시가 가능하도록 복호화해야 하고, 파일명이나 확장자명을 변경하거나 삭제한 파일들을 복구해야 할 필요성 등이 있기 때문에 일반 증거에 비해 범죄와 관련된 내용만을 선별적으로 찾아내기가 어려운 점이 상존하고 있다.

1.1 Modulation potential of digital evidence

디지털 기기는 중복되는 업무를 쉽게 처리할 수 있는 수단으로 사용하기 위하여 탄생된 배경을 가지고 있기 때문에, 디지털화 된 정보는 그 정보를 쉽게 수정하거나 삭제할 수 있다. 따라서 변경과 조작이 용이하다. 이러한 점들은 업무처리에서는 장점이 될 수 있지만 증거적인 측면에서 보면 일반 물리적 증거에 비해 증거를 쉽게 조작하거나 인멸할 수 있고, 그 흔적을 쉽게 찾을 수 없다는 단점이 있다.

즉 “1”이라는 정보가 담긴 디지털 증거를 조작할 목적으로 “0”으로 바꿨을 때 추후 해당 증거가 조작이 이루어졌는지, 조작이 이루어졌다면 언제·어디에서·누구에 의해 조작이 되었는지를 판별할 수 없는 취약성이 존재하게 된다.[5]

또한 디지털 데이터는 물리적 증거에 비해 자료의 일부분만 삭제하거나 변경하는 것이 쉽기 때문에, 증거수집·보존·분석과정에서 사용하는 각종 소프트웨어나 장비의 사용과정에서 인위적인 조작이나, 시스템의 작동과정에서 시스템내의 많은 파일들에 변화가 일어나는 경우도 있을 수 있다.[6] 따라서 수사관은 특정인이 사용하였었던 데스크톱 컴퓨터가 디지털 증거로 사용하기 위하여 압수·분석하면서, 별도의 조치 없이 그 컴퓨터를 부팅시키고, 로그인하면 시스템 작동과 관련된 파일들이 프로그래밍화 된 시스템에 따라 자동생성되거나 변경되어 디지털 증거로서 가치는 재평가될 수밖에 없다.

또한 특정 데이터를 일정한 프로그램을 사용하여 데이터의 생성 없이 이진수 형식으로 된 자료의 일부를 간단하게 수정하는 것이 가능하다.[7]

이처럼 디지털 증거는 취급자의 고의적인 변경이나 훼손 없이도 외부적·내부적 환경의 변화만으로도 변경 또는 훼손될 수 있고, 일반적인 물리적 증거는 그 존재 자체만으로 증거가치가 부여되기 때문에 대부분 최초 수집된 증거 상태 그대로 법정에 제출되는데 반하여 디지털 증거는 그 존재 자체만으로 증거가 되기보다는 그 내용을 분석하여 나온 결과에 따라 해당 범죄사실에 대한 증명가치를 부여받을 수 있기 때문에 법정에 제출되기 전에 반드시 조사·분석과정을 거치지 않을 수 없다.[8]

디지털 증거의 이와 같은 특성 때문에 최초에 수집된 증거가 저장된 매체에서 법정에 제출되기까지 변경이나 훼손이 없었다는 무결성을 확보하는 절차와 기술이 필요하다.

1.2. Invisible evidence

디지털 증거는 존재여부와 그 증거의 내용을 사람의 5관을 통해서 확인할 수 없기 때문에 디지털 자료를 증거로 사용하기 위해서는 전문가가 개입하여 디코딩하거나 압축해제 등의 절차를 거쳐야 하기 때문에 이러한 절차과정에서 전문성이나 신뢰성이 확보될 필요가 있다.[9]

1.3. Bulking of scale

WD, SSD 등 저장매체의 기술발달과, 다중이 공동으로 이용할 수 있는 서버기술의 발전으로 인하여 여러 사람이 사용하는 방대한 분량의 디지털 데이터가 혼재되어 저장할 수 있게 되었다. 이에 따라 하나의 저장 매체에는 범죄 행위자와 관련된 정보 외에도 전혀 관련이 없는 제3자의 정보도 함께 저장되어 있게 된다. 특히 여러 사람이 함께 사용할 수 있도록 되어 있는 서버와 같은 저장매체에서는 이러한 문제가 더 클 수밖에 없다.[10]

이러한 특성 때문에 압수·수색의 범위와 방법 등을 제한하지 않는다면, 그 저장매체를 공동으로 사용하는 사람들에게 불편과 재산적 피해를 줄 수 있는 문제점이 있다.

1.4. Network relevance

디지털 기술이 발전하면 할수록 디지털 기기간의 관계는 독립적으로 움직이기보다는 네트워크로 연결되어 움직이는 경우가 많아지고 있다. 이러한 디지털 기술의 발전에 따라 네트워크는 현대인에게 일상적 생활로 변모할 정도이다. 네트워크와 연계된 생활 속에서 발생된 범죄행위라면 웹하드, 파일공유 네트워크, 클라우드 서비스 등 네트워크로 공유된 네트워크 속에서 디지털 증거를 수집해야 한다.

따라서 네트워크와 관련된 디지털 증거를 수집할 때에는 네트워크가 갖는 기술적 특성과 더불어 헌법상 보장되고 있는 개인의 자유와 권리도 함께 고려해야 할 필요가 있다.[11]

1.5. Super border

클라우드 컴퓨팅의 환경 속에서 데이터 압수수색에서는 저장 장소가 어디에 있는지를 찾는 것도 어렵지만, 설령 찾아낸다 하더라도 글로벌 기업 같은 경우에는 디지털 정보를 보관하고 있는 서버가 외국에 있는 경우에는 우리나라 법원에서 발행한 압수수색의 영장이 효력을 발휘할 수 있는지의 문제가 발생할 수 있다.

2. Aadmissibility of evidence of Digital Data

일반적 증거는 유체물인 증거, 사람이 법정에서 한 진술증거를 증거를 전제로 하였기 때문에, 전술한 바와 같은 디지털 증거의 특성을 고려할 때, 일반적 증거와 똑같은 증거능력을 인정하기 어렵다.

디지털 증거가 갖는 특성 등을 고려할 때, 일반적 증거와 같이 수집 절차의 적법성이 확보되어야 할 뿐만 아니라 무결성, 진정성, 신뢰성, 원본성 등의 문제가 해결되어야 한다.[12]

즉 디지털 증거는 일반적 증거에서 요구하는 수집절차의 적법성과 더불어 디지털 증거의 특성을 고려한 무결성, 진정성, 신뢰성, 원본성이 확보 되어야만 증거능력을 인정받을 수 있다.[13]

2.1. Identity and authenticity

디지털 증거는 물리적 증거와는 달리 변형시키기가 쉽다는 취약성을 가지고 있기 때문에 디지털 증거가 최초 저장된 곳에서 형사법정에서 제출되기까지 변경이나 훼손이 없었다는 점을 입증할 필요가 있다. 디지털 증거를 수집·분석·보관·처리하고, 법정에 제출되는 과정에서 원본 데이터의 무결성이 그대로 유지되었다는 절차적 보증이 필요하다. 대법원판결에서도 압수물인 디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력된 문건의 동일성이 인정되어야 할 것인데, 그 동일성을 인정하기 위해서는 디지털 저장매체 원본이 압수된 이후 문건 출력에 이르기까지 변경되지 않았음이 담보되어야 하고, 특히 디지털 저장매체 원본에 변화가 일어나는 것을 방지하기 위해 디지털 저장매체 원본을 대신하여 디지털 저장매체에 저장된 자료를 '하드카피'·'이미징'한 매체로부터 문건이 출력된 경우에는 디지털 저장매체 원본과 '하드카피'·'이미징'한 매체 사이에 자료의 동일성도 인정되어야 한다. 나아가 법원 감정을 통해 디지털 저장매체 원본 혹은 '하드카피'·'이미징'한 매체에 저장된 내용과 출력된 문건의 동일성을 확인하는 과정에서 이용된 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다고 판시하였다.[14]

여기에서 논란이 될 수 있는 문제는 압수수색영장 집행의 종료시점을 어느 시점으로 볼 것이냐의 문제와도 관련된다. 즉 수사기관이 압수·수색영장의 집행 현장에서 저장매체를 봉인한 후 수사기관의 점유하에 둔 시점에서 압수·수색 영장의 집행은 종료된다고 보는 견해[15]와 디지털 증거의 압수·수색의 목적물은 저장매체가 아니라 저장매체 속에 저장되어 있는 디지털 데이터이므로 압수하고자 하는 디지털 데이터를 복사 또는 출력한 시점으로 보아야 한다는 판례의 태도[16]가 나뉘고 있다.

이에 대하여 대법원은 디지털 정보로 되어 있는 증거물의 압수절차는 저장매체 자체 또는 복사정보를 저장한 매체를 수사기관이 취득하는 것만으로 압수절차가 끝나는 것이 아니라 그 저장매체를 수사기관의 사무실로 가져 왔을 때에는 저장매체 속에 들어있는 압수하여야 할 디지털 정보를 확정하는 때에 비로소 압수가 완료된다고 보고 있다. 이와 같은 대법원의 해석은 미국에서 논의되는 2단계 수색이론(two-stage search)을 참고한 것으로 보인다. 디지털 정보의 압수절차에서 완료시점을 대법원과 같이 해석한다면, 압수절차에서 피의자나 피압수자의 참여도 저장매체의 압수현장에서 압수하는 단계뿐만 아니라 수사기관의 사무실에서 그 저장매체에 있는 파일들을 검색하는 단계에도 계속 참여시켜야 한다는 문제가 대두된다. 이 문제에

대하여 독일은 2004년 형사소송법을 개정하면서 선별절차도 수색에 포함시켰지만, 수색관정에 압수물의 소유자를 참여하게 하는 조문(독일형사소송법 제106조 제1항)은 선별적 열람절차에는 적용하지 않도록 하는 입법적 해결을 하였다.

2.2. Relevance to the case

압수수색 요건으로 '사건과의 관련성'을 엄격하게 해석하면서 원본 저장매체 자체의 압수보다는 디지털 데이터를 선별하여 압수해 와야 하는 경우가 많아졌다.

기존 아날로그 증거의 경우 유체물적 성격이 강하기 때문에 그 현장에서 증거의 점유를 확보하는 방법으로 압수가 가능하였다. 그러나 디지털 데이터의 경우 무체물로써 네트워크를 통해 예상치 못한 곳에 저장되어 있는 경우가 많고, 이 경우 기존 아날로그와 같은 압수수색 방법을 고집할 경우 압수수색의 실효성이 현저히 저하되는 문제가 발생할 수 있다.

대법원은 압수수색을 할 때 원본 매체가 아니라 사건과 관련이 있는 정보만을 선별해 압수해야 한다며 압수수색의 요건으로 사건과 관련성을 엄격하게 해석하고 있다.

또한 압수한 자료에서 피의사실과 관련이 없는 또 다른 범죄를 발견했을 때, 그 혐의에 맞는 영장을 받아 적법하게 압수수색해야만 증거능력을 인정할 수 있다고 본다.

2.3. Hearsay Rule and Printed document

대법원은 압수된 디지털 저장매체로부터 출력된 문건이 진술증거로 사용되는 경우에는 그 기재 내용의 진실성에 관하여 전문법칙이 적용되므로, 형사소송법 제313조 제1항에 의하여 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다고 판단하였다.[17]

수사기관이 디지털 저장매체에서 출력하여 증거로 제출한 문건은 그 작성자가 법정에서 그 성립의 진정함을 인정하였을 때 증거능력이 인정된다. 그렇지 않고 그 작성자가 성립의 진정함을 부정하는 경우에는 증거로 사용할 수 없다.

이러한 대법원의 태도는 범행사실 자백 내용이 담긴 SNS·이메일·컴퓨터 문서 일기장에 대해 피고인이 법정에서 부인하면 피고인이 작성했음이 과학적으로 입증돼도 증거로 쓸 수 없는 문제점을 안고 있었다.

또한 관련 증거를 인정하는 피고인은 처벌 받는 반면, 거짓말하는 피고인은 기존 '종이 증거법'에 따라 이를 증거로 쓸 수 없는 모순이 있었다.

III. Judgment of the Supreme Court related to digital data

디지털 데이터의 증거능력과 관련된 판례는 1999년의 99도2317판결(소위 영남위원회 사건), 2007년의 2007도7257 판결(소위 일심회 사건), 2011년의 2009모1190 판결(소위 전교조 이메일 사건)을 들 수 있다.

1. Supreme Court 99Do2137

이 사건에서는 피의자들을 긴급체포하는 과정에서 피의자들이 소지하고 있던 컴퓨터 디스켓을 현장에서 압수하면서 디스켓들을 한꺼번에 모아놓고 사진촬영한고, 압수목록을 작성하였으며, 압수목록에는 피압수자의 서명, 무인을 받았다.

이 압수물의 증거능력과 관련하여 대법원은 "피고인들은 위 컴퓨터 디스켓의 압수방법이 위법하다는 것이나, 컴퓨터 디스켓을 압수함에 있어 위조, 변조 등의 위험을 피하기 위하여 피고인들이 주장하는 바와 같은 방법을 취하는 것이 바람직하다 하더라도 이는 단지 압수방법의 적정 여부에 관한 것일 뿐 그와 같은 조치를 취하지 않은 것이 반드시 위법한 것이라고는 할 수 없다"고 판시하였다.

이 사례를 통하여 디지털 저장매체와 최종 출력 문건 사이의 동일성 확보가 필요하다는 점에 대해 실무계의 인식이 높아진 것만큼은 부인할 수 없다.

2. Supreme Court 2007Do7257

이 사건에서 수사관들은 피의자들을 긴급체포하면서 이들이 소지, 소유하고 있던 디지털 저장매체를 압수하였다. 여러 형태의 디지털 저장매체 가운데 USB와 같은 것은 바로 압수하면서 봉함되었고, 이후 압수된 저장매체로부터 바로 최종 문건이 출력되었다. 컴퓨터 하드디스크 등과 같이 보다 대용량의 복잡한 저장매체의 경우 수사관들은 그 저장매체를 압수하면서 그 일부분을 '하드카피' 또는 '이미징'이라는 기법을 통하여 별도의 저장매체에 복제하였다. 복제 과정은 피의자들이 입회한 가운데 이루어졌고, 이러한 전 과정은 비디오테이프로 녹화되었다. 그런데 이 과정에서 원 저장매체의 해쉬(Hash)값과 복사한 저장매체의 해쉬값이 동일하다는 점을 확인하는 절차가 누락되었다. 이에 따라 디지털 저장매체의 내용과 최종 출력 문건의 동일성 여부가 문제되었다.

이와 관련하여 대법원은 원본 디지털 저장매체의 내용과 최종 문건 사이의 동일성 판단에 대해 다음의 기준을 제시하였다.

① 압수물인 디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력된 문건의 동일성이 인정되어야 한다.

② 양자의 동일성을 인정하기 위해서는 디지털 저장매체 원본이 압수된 이후 문건 출력에 이르기까지 변경되지 않았음이 담보되어야 한다.

③ 특히 디지털 저장매체 원본에 변화가 일어나는 것을 방지하기 위해 디지털 저장매체 원본을 대신하여 디지털 저장매체에 저장된 자료를 '하드카피'·'이미징'한 매체로부터 문건이 출력된 경우에는 디지털 저장매체 원본과 '하드카피'·'이미징'한 매체 사이에 자료의 동일성도 인정되어야 한다.

④ 디지털 저장매체 원본 혹은 '하드카피'·'이미징'한 매체에 저장된 내용과 출력된 문건의 동일성을 확인하는 법원의 감정 과정에서는 이용된 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다.

대법원은 이와 같은 판단기준을 근거로 삼아, 출력된 문건은 압수된 디지털 저장매체 원본에 저장되었던 내용과 동일한 것으로 인정할 수 있어 증거로 사용할 수 있는 판단을 내렸다.

3. Supreme Court 2009Do1190

이 사건에서는 디지털 저장매체에 수록되어 있는 8,000여개의 이메일에 대한 일괄적 압수·수색의 적법성이 문제되었다. 이에 대해 대법원은 사생활 보호를 위하여 디지털 저장매체에 수록되어 있는 방대한 양의 정보 가운데 피의사실과 관련성이 있는 것만을 압수할 수 있다는 원칙을 제시하였다. 이에 따라 2011년 7월의 형사소송법 제106조와 제215조의 개정하여 반영하였다.

4. Intermediate conclusion

디지털 증거에 관한 위법수집 증거 배제법칙의 적용문제를 검토하여 보면, 디지털 증거의 증거능력 판단은 일반적 증거의 증거능력 판단에서처럼 형식적인 법규의 위배 여부만을 판단하는 것이 아니라 디지털 증거가 가지고 있는 특성들, 예컨대, 범죄와 관련이 없는 정보의 주체들을 보호할 필요성, 일반 국민들에게 헌법상 보장되어 있는 기본권 보장을 고려해야 할 필요성이 범죄의 실체적 진실을 파악하는 것보다 더 높다고 할 수 있는 점들을 고려하여야 하기 때문에 이에 대한 조화를 고려할 필요가 있다.

독일은 이러한 점으로 고려하여 국가의 형사소추이익과 침해되는 당사자의 기본권 사이의 이익을 교량하여 판단한다.[18] 즉 기본권의 침해가 어느 정도이고, 수색 대상이 되는 디지털 데이터가 그 형사사건에서 얼마나 중요한 증거인가를 비교하여 판단한다는 것이다. 독일은 기본권의 불가침 핵심영역을 인정하고, 이를 침해하는 방법으로 수집된 증거는 증거능력을 절대적으로 부정하고 있다.

우리 대법원도 2007. 11. 15. 전원합의체 판결을 통하여 위법수집증거배제법칙을 수용하여 기존의 대법원 견해를 변경하면서 독일과 같이 비교형량을 채택하였고,[19] 그 후 디지털 증거에 관한 판결[20]에서도 이와 같은 비교형량이 유지되고 있다.

4.1. Principle of legitimacy

가장 기본적인 원칙으로 입수한 증거자료는 적법절차를 거쳐 얻어져야 한다는 원칙이다. 이는 위법절차를 통해 수집된 증거의 증거능력을 부정하는 위법수집증거배제법칙에 따르는 것이다. 예를 들어 불법 해킹을 통하여 수집한 파일은 증거능력이 없다. 이른바 '독수의 과실' 이론은 위법하게 수집된 증거에서 얻은 2차적 증거도 증거능력이 없다는 것이며, 불법 해킹을 통하여 얻어진 패스워드를 통하여 파일을 해독했을 경우에도 복호화된 파일은 증거능력이 없다고 보아야 한다.

4.2. Principle of reproduction

디지털 데이터를 처리할 때, 같은 조건이라면 수행결과는 항상 같게 나와야 한다. 이는 동일한 대상 시스템을 다양한 증거분석 도구로 수행하더라도 같은 결과가 도출되어야 한다.

4.3. Continuity of procedure

디지털 포렌식은 보통 '증거물 획득→이송→보관→분석→법정 제출' 등으로 이어지는 각 단계에서 담당자 및 책임자를 명확히 해야 한다. 즉 증거로 확보된 하드디스크가 이송과정에서 물리적인 손상이 발생하였다면 이송 담당자는 이를 확인하고 그 내용을 인수인계하여 이후 과정에서 복구 및 보고서 작성 등 적절한 조치를 취할 수 있게 하여야 한다. 즉 디지털 증거 원본을 확보한 이후에 진행된 과정을 모두 상세하게 기록하고, 입회자를 참여시켜 신뢰성을 확보해야 한다.

Ⅳ. Hearsay Rules of Digital Data and Legislation

1. Hearsay Rules and Judgment of the Supreme Court

1999년의 99도2317(영남위원회 사건) 대법원 판례에서는 "컴퓨터 디스켓에 들어 있는 문건이 증거로 사용되는 경우 위 컴퓨터 디스켓은 그 기재의 매체가 다를 뿐 실질에 있어서는 피고인 또는 피고인 아닌 자의 진술을 기재한 서류와 크게 다를 바 없다"면서 전문법칙의 예외를 규정한 형사소송법 제313조 제1항에 따라 "그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다"고 하였다.

이처럼 대법원은 직접심리주의에 따라 가능한 한 원진술자의 직접 진술을 증거로 사용하려는 태도를 취하고 있다.

즉 범행사실을 자백한 내용이 담긴 E-mail·컴퓨터에 저장된 일기장은 그 피고인이 법정에서 "내가 안 썼다"고 하면 피고인이 작성했음이 과학적으로 입증되거나 심지어 자백을 SNS에 게시해도 법정에서 "내가 작성 안 했다"고 하면 범인이 게시한 것이 과학적으로 입증돼도 증거능력이 부정돼 법정 증거로 사용할 수 없는 문제점이 발생하였다. 참고로 미국의 연방증거법은 필적감정이나 그 밖의 정황증거에 의한 진정성립의 입증을 허용하고 있다.

2. Legislation

최근 전기통신기술의 비약적인 발전에 따라 컴퓨터 등 각종 정보저장매체를 이용한 정보저장이 일상화되었고, 범죄행위에 사용된 증거들도 종이문서가 아닌 전자적 정보의 형태로 디지털화되어 있는 현실을 고려하여, '진술서' 및 그에 준하는 '디지털 증거'의 진정성립은 '과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법'으로도 인정할 수 있도록 하되, 피고인 아닌 자가 작성한 경우 반대신문권이 보장됨을 명확히 규정하였다.

2016. 5. 19. 국회를 통과한 형사소송법의 개정된 내용을 보면, 제313조 제1항은 본문 내용 중 "그 서명 또는 날인이 있는 것"을 "그 서명 또는 날인이 있는 것(피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 문자·사진·영상 등의 정보로서 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체에 저장된 것을 포함한다. 이하 이 조에서 같다)"로 개정하였다.

제313조 제2항은 "제1항 본문에도 불구하고 진술서의 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하는 경우에는 과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있다. 다만, 피고인 아닌 자가 작성한 진술서는 피고인 또는 변호인이 공판준비 또는 공판기일에 그 기재 내용에 관하여 작성자를 신문할 수 있었을 것을 요한다."로 개정하였다.

제313조에는 제3항에 "감정의 경과와 결과를 기재한 서류도 제1항 및 제2항과 같다."라는 규정을 신설하였다.

제314조의 본문 내용 중 "조서 및 그 밖의 서류"를 "조서 및 그 밖의 서류(피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 문자·사진·영상 등의 정보로서 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체에 저장된 것을 포함한다)"로 개정하였다.

이와 같이 형사소송법을 개정함으로써 디지털 증거가 최초로 형사소송법에 명기되었으며, 디지털 증거는 '과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법'으로 증명된 경우에 한해 증거로 인정된다고 함으로써 대법원의 직접심리주의에 따라 가능한 한 원진술자의 직접 진술을 증거로 사용하려는 태도를 취함에 따라 나타났던 디지털 데이터 수사상의 문제를 해결하였다. 또한 단순히 이메일 계정이 특정인의 것이라는 점만이 아니라, 접속 IP·위치정보·사용내역·암호설정 등의 다양한 정보를 입체적으로 분석한 결과가 뒷받침되어야만 증거능력이 인정되도록 하였다.

한편 제3자가 작성한 디지털 증거는 피고인이 작성자로 지목된 사람을 법정에서 직접 증인신문 할 수 있도록 함으로써, 피고인의 절차적 방어권이 보장되도록 하였다.

Ⅴ. Conclusion

오늘날 개인이나 기업의 활동은 많은 부분이 디지털 기술에 의존하여 생활할 뿐만 아니라 4차 산업혁명이라고 일컬어지는 앞으로의 사회는 발달된 디지털 기술과 인간이 함께 생활해야 할 정도로 디지털 기술에 대한 의존도가 높아지고 있다.

이러한 디지털 사회 속에서 발생되는 범죄 속에서 발생되는 흔적 또한 디지털 속에서 찾아내야 하는 사회로 진전될 수밖에 없기 때문에 형사절차에서도 디지털 증거에 따른 판단 의존도가 높아질 수밖에 없다.

그런 반면에 클라우드 컴퓨팅 환경체계로 전환되고 있는 점들을 고려한다면 서비스 제공자의 가상의 공유 컴퓨팅 자원을 다수의 이용자들이 사용하는 특성 때문에, 클라우드 컴퓨팅 자원에서 증거자료를 찾는 행위는 범죄와 관련이 없는 제3자의 기본권을 심대하게 침해할 수 있는 개연성이 높아지기 때문에 형사절차에서 사용될 수 있는 디지털 데이터의 증거능력을 제한할 수밖에 없는 점 또한 상존하고 있다.

따라서 이러한 디지털 증거의 이러한 양면성을 고려하여 압수·수색영장 발부 및 집행 단계에서의 사전적 통제와 함께 사후의 증거능력 판단에 있어서도 이러한 점을 충분히 고려하여야 할 것이다. 사전적 통제가 무용하다는 견해도 있으나 증거능력 판단을 통한 사후적 통제를 실질화하기 위해 사전적 통제가 내실 있게 이루어질 필요가 있다.

즉 디지털 시대에 맞게 형사절차의 적정화를 기하기 위한 입법 등 다양한 노력이 어느 때보다 더 필요하다.

REFERENCES

[1] Pil-Seong, Jang, 2016 Davos Forum: What is our strategy for the forthcoming Fourth Industrial Revolution?), 「Science & Technology Policy」, Vol.26, No.2, Science & Technology Policy Institute, 2016. 2, p.12.

[2] Jae-Bong, Kim, Admissibility of Digital Evidence and Identification, 「Hanyang Journal Of Law」, Institute for Legal Studies Hanyang university , Vol.31, No.1, 2014. 3, p.171.

[3] Donga Ilbo, "Digital evidence growth … alpago to be opened during the era of the investigation", 2016. 5. 30, A12.

[4] Jang, Sang-Gwi, "A Study on Evidence of Digital Evidence", Law Working Council, 2009. 5, p.227.

[5] Tak Hee-Sung·Lee Sang-Jin, "A Study on the digital evidence collection procedure in digital forensic and the

admissibility of digital evidence", Korean criminological review a library, Vo12006 No-1, Korean institute of criminology, 2006, p.36.
[6] Kun-Won Yang, "A Study on Collection and Admissibility of Digital Evidence in Criminal Procedure", Doctoral Dissertation, KyungHee University, 2006, p.22.
[7] Jeong Gyo-Il, "Confiscation of digital evidence and submissions in court", 「Prosecution Service」, Vol.25, Supreme Prosecutor's Office, 2010. 4, p.114.
[8] Tak Hee-Sung·Lee Sang-Jin, Paper[5], p.139.
[9] Kun-Won Yang, "A Study on the Characteristics of Digital Evidence and Legal Issues", 「KyungHee Law Journal」 Vol.41 No.1, The Institute of Legal Studies KyungHee University, 2006, p.181.
[10] Kyong-Ok Ahn, Use of technology in criminal procedure and legal problems of criminal proceedings", Korean institute of criminology, 2004, p.156
[11] Jong-keun Park, "Digital evidence seizure and search and legal system", 「Prosecution Service」, Supreme Prosecutor's Office, Vol.18, 2009, p.35.
[12] Young-Ki Kim, "Generation of Digital Evidence", 「Korean journal of criminal case studies」, Vol.19, 2011. 6, p.516.
[13] Jang, Sang-Gwi, Paper[4], p.227; Son Ji-Young·Kim, Joo-Seok, 「Research on Determining the Admissibility of Digital Evidence」, Judicial Policy Research Institute, 2015. 8, p.30.
[14] Supreme Court 2007. 12. 13, 2007Do7257.
[15] Seung-Soo Chun, "Confiscation of digital evidence. Execution of search warrant - Supreme Court 2011. 5. 26. 2009Mo1190 case review for decision-, 「Lawyers association journal」, Vol.670, Lawyers association, 2012. 7, p.254.
[16] Supreme Court 2011. 5. 26. 2009Mo1190.
[17] Supreme Court 1999. 9. 3. 99Do2317.
[18] BVerfG 2 BvR 1027/02, 2 BvR 902/06.
[19] Supreme Court 2007. 11. 15. 2007Do3061.
[20] Supreme Court 2012. 7. 26. 2011Do12407; Supreme Court 2015. 1. 22. 2014Do10978.

Authors

Woon Gon Kim received the B.S., M.S. and Ph.D. degrees in Law from Chosun University, Korea, in 1993, 1995 and 1998, respectively. He is a graduate of Chosun University graduate school and majored in criminal law.

He is currently teaching criminal law at the Maritime Police Department of Chosun College of Science and Technology. He is interested in digital evidence of criminal procedures, and computer crime.