이학석사 학위논문

계정 접속을 통한 역외 압수수색의 허용성과 무결성 입증 방안에 대한 연구

- 검증기관 도입의 필요성

2018년 2월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학 전공

이 신 애

계정 접속을 통한 역외 압수수색의 허용성과 무결성 입증 방안에 대한 연구

- 검증기관 도입의 필요성

지도교수 이 상 원

이 논문을 이학석사 학위논문으로 제출함
2017년 12월

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식학 전공
이 신 애

이신애의 석사 학위논문을 인준함
2018년 1월

위 원 장 _____ (인)

부위원장 _____ (인)

위 원 _____ (인)

요약(국문초록)

인터넷 기술의 비약적인 발전으로 인하여 현대 사회의 삶의 방식도 변화하고 있다. 아날로그 시대의 막이 내리고 디지털 시대로 발돋움하면서 모든 곳에서 디지털 기기가 사용되고 있고, SNS 시대는 우리로 하여금 일상의 디지털화를 이루어가게 하고 있다. 이러한 변화는 형사법의 변화도 요구하고 있다. 법이 현실의 변화 속도를 쫓아가지 못하게 되면서 다양화된 범죄의 증거 수집이 어려워졌다. 해외 서비스 제공자가 제공하는 서버 이용자가 확대됨에 따라 해외 서버에 저장된 디지털 증거의 확보가 필요하나, 이를 위하여 형사사법공조절차에 따를 경우 시간과 절차상의 제약이 있어 디지털 증거가 훼손될 우려가 매우 크다. 따라서 해외 서버에 저장된 디지털 증거의 확보를 위해서는 형사사법공조절차가 아닌 다른 압수수색의 방법을 검토하여야 하는바, 수사기관이 당사자의 계정 정보를 알게 되었을 경우 서버에 직접 접속하여 압수수색하는 방법이 거론되고 있고 수사실무에서도 사용되고 있다.

계정 접속을 통한 역외 압수수색에 대하여는 그 허용성과 관련하여 타국의 관할권 침해 문제, 압수수색 절차상의 문제, 계정의 취득과 관련된 개인정보 침해 문제 등이 제기되고 있는바, 국내·외 사례 등을 참고하여 현행법상으로도 허용될 수 있는지를 검토하였다.

또한 만약 계정 접속을 통한 역외 압수수색의 허용성을 인정한다면, 그로 인해 취득한 증거의 문제점과 관련하여 무결성을 중심으로 살펴보았다. 해외에서 운영하는 서버의 경우 서버의 원본을 압수할 수도 없고 이미징도 어려우며, 형사사법공조절차를 통하지 아니하고는 서비스 제공자의 협조를 얻기 어렵기에 원본과 사본의 동일성, 무결성이 문제될 것이기 때문이다. 따라서 이렇게 취득한 증거의 무결성을 입증하기 위하여 제3검증기관의 도입을 제안하였다.

제안된 제3검증기관은 공인된 포렌식 전문가들이 실시간 검증을 통해 증거의 무결성을 보장하고 수사기관의 권한 남용을 통제함으로써 증거의 신뢰성을 확보할 수 있도록 할 것이다. 또한 그 외에도 디지털 증거에 대한 독립된 검증기관으로서 객관적이고 중립적인 운영을 통해 헌법과 법률이 정하는 바에 따라 국민의 기본권 보호의 목적도 달성할 수 있을 것이다.

주요어 : 디지털 증거, 계정 정보 취득, 역외 압수수색, 관할권, 무결성, 검증기관 신설
학 번 : 2016-26055

목 차

제 1 장 서 론

제 1 절 문제 제기

바야흐로 네트워크를 통해 전 세계가 연결된 하나의 새로운 세상이 펼쳐지고 있다. 종이로 된 서면, 눈에 보이는 증거에서 벗어나 사용자의 모든 정보가 전자적 형태로 저장, 현출되는 시대이다.

이렇듯 우리의 일상 속으로 파고 든 '디지털화'는 '디지털 증거'를 남긴다. 디지털 기기를 통하여 우리의 흔적이 기록, 저장되고, 아날로그 시대에서 발견하기 어려웠던 증거도 이제는 어디엔가 남아있을 가능성을 엿볼 수 있게 된다.

디지털 증거는 아날로그 증거와 다른 여러 특성을 지닌다. 디지털 증거는 광범위할 뿐만 아니라 대용량이고, 국경을 초월하며, 언제 어디에서나 저장, 삭제가 가능하다. 이러한 여러 특성으로 인해 디지털 기기를 이용한 범죄 행위도 늘어나고 있고, 반면에 범죄 행위를 입증하기 위한 증거 확보의 필요성도 매우 높아지고 있다.

종래 형사소송법 제106조에서 압수의 대상에 관하여 '증거물 또는 몰수할 것으로 사료하는 물건'을 압수할 수 있다고 규정하였으나, 위와 같은 시대적 흐름에 따라 2011. 7. 18. 개정된 형사소송법에서 제106조 제3항을 신설하여 '압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다.'라고 규정하는 등 전자 증거도 압수의 대상이 됨을 명시하였다.

이에 수사기관에서는 컴퓨터 등 정보저장매체에 대한 압수수색을

진행할 경우, 정보저장매체 내에 저장된 정보의 내용을 CD에 저장하거나 종이에 인쇄하는 방법 등으로 출력하여 증거로 제출하게 된다.

그런데 최근에는 개인용 PC나 휴대폰에 정보를 저장하고 이용하는 것을 넘어, 국제적 사업자가 제공하는 인터넷 서버 공간에 정보를 저장하고 이용하는 시대가 되면서 단순히 사용자가 소지하고 있는 PC나 휴대폰을 압수수색하는 것만으로는 더 이상 압수의 목적을 달성하기 어려워진 것이 사실이다. 이제는 압수수색의 목적물인 증거를 만들고 삭제하는 사용자와, 증거를 보관하고 있는 사업자가 구별되어 있으며, 사용자와 사업자는 국적을 초월하기도 한다. 따라서 압수수색의 방법에 대해서도 기존의 규정만으로는 현실적으로 집행이 불가능한 경우가 발생한다.

오늘날 전 세계 대부분의 사람들이 매일, 매시간 PC나 휴대폰을 통하여 인터넷에 접속하고, 중요 정보를 PC 내 저장 공간, 혹은 외부 저장 공간(USB 등)에 저장하는 외에, 인터넷 메일, 클라우드, 또는 SNS에 남기기도 한다. 특히 구글, 페이스북 등 인터넷 서비스 제공자가 국외에 있는 다국적 기업이 늘어나고, 국적을 초월하여 이러한 서비스를 이용하는 사람들이 늘어나면서 기존의 국내법상으로 해결되지 않는 법적 쟁점도 함께 늘어나고 있다. 인터넷 상에서 발생되는 사이버 범죄의 경우 나날이 진화하고 있고, 국내법의 적용을 피하기 위해 외국 기업이 제공하는 인터넷 서비스를 이용하는 경우가 점차 증가되고 있다.

그러나 국내법은 이러한 시대적 흐름에 따라가지 못하고 있는 것이 현실이다. 비트코인을 이용한 범죄, 구글에서 제공하는 클라우드 서비스를 이용한 범죄, 랜섬웨어, 파밍 등 여러 형태의 사이버 범죄가 우리 생활 속에 깊숙이 들어와 있다. 예를 들어 중국에서 국내인

들을 대상으로 한 파밍 범죄 등의 경우 아이피 추적만으로는 중국 소재 아이피라는 것만 확인이 가능할 뿐, 바로 검거하는 것은 현실적으로 어렵다. 또한 해외 이메일을 이용하는 경우 이메일 내용을 제공받기 위해서는 해외 이메일 서버 제공자에 영장을 집행해야 하나, 관할권 문제 등 여러 복잡한 문제가 생기며, 형사사법공조절차를 거쳐 확보하는 방법이 있으나 위 절차는 실제 장시간이 소요되어 영장 집행이 무익화 될 수 있다. 또한 형사사법공조조약을 체결하지 않은 국가에는 실제 영장 집행의 방법이 없다는 문제점도 있다.

따라서 위와 같은 현실적 한계점을 극복하기 위하여 해외 소재 서버에 대한 압수수색의 새로운 방법은 없는 것인지, 또한 그러한 방법에 의한 압수수색의 결과로 도출된 목적물의 무결성은 어떻게 입증해야 하는지 문제가 된다.

제 2 절 연구의 목적 및 방법

형사소송법 제106조 제3항에서는 '압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체'인 경우를 상정하고 있다.

유체물의 압수와 디지털 증거의 압수를 비교하여 보자면, 유체물의 압수는 유체물에(예컨대, 글씨가 써진 일기장) 정보의 내용이 담겨져 있고, 그러한 내용이 유체물에 의하여 바로 눈에 보이며, 그 유체물을 압수함으로써 압수의 목적을 달성하게 된다. 그런데, 디지털 증거의 압수는 정보가 USB 등 작은 저장매체에 담겨져 있는 경우 그 유체물을 압수함으로써 압수의 목적을 달성하게 되기는 하나,

USB만으로 바로 정보가 눈에 보이는 것이 아니며 어떠한 정보가 담겨져 있는지 확인하는 절차가 필요하게 된다. 또한, USB가 아닌 서버에 저장된 디지털 증거의 압수는 유체물인 서버 컴퓨터를 압수한다는 것은 현실적으로 불가능하며 서버 내에 있는 정보를 수색하여 종이나 다른 저장매체 등에 현출시킬 수밖에 없게 된다. 결국, 현재 압수수색의 방법을 규정한 위 제106조 제3항으로는 디지털 증거의 압수를 수용하지 못하게 된다. 이에 사실상 디지털 증거의 압수수색은 '정보'를 궁극적 대상으로 하기 때문에, 형사소송법 제106조의 압수수색 대상에 '정보'를 포함시켜야 한다는 의견도 있다. 디지털 정보를 증거로 확보하기 위해 현실적으로 정보를 유체물인 디스켓 등에 저장하거나 그 출력물을 압수하는 방법에 의할 수 밖에 없으나 이는 압수하기 위한 수단에 불과하고 대상물은 여전히 디지털 정보 그 자체이기 때문이다.[1)]

여하튼 위와 같은 쟁점은 논외로 하더라도, 디지털 증거에 대한 압수수색 방법을 규정한 위 제106조 제3항이 유체물의 압수수색과는 다른 '불완전한' 규정이라는 것이다. 기존의 유체물 압수수색의 경우 직접 압수수색 장소에 수사기관이 가서 유체물을 수색한 후 압수해 오면 되었으나, 디지털 증거의 압수수색은 개인용 PC나 휴대폰에 저장되어 있는 것을 제외하고 웹이나 서버 상에 저장되어 있는 정보의 경우 수사기관이 직접 '웹이나 서버 소재지' 또는 '인터넷 서비스 제공자의 소재지'에 가는 것이 현실적으로 곤란할 뿐만 아니라, 수사기관이 직접 웹이나 서버 내에 있는 정보를 수색할 수도 없을뿐더러, 그 정보를 압수하는 것도 '저장 매체'를 압수할 수 없기 때문에 별도의 방법으로(출력 등) 해야 하는 등 유

1) 원혜욱, 과학적 수사방법에 의한 증거수집 - 전자증서의 압수·수색을 중심으로 - , 비교형사법연구 제5권 제2호, 2003, 174

체물의 압수수색과는 전혀 다른 모습임에도 불구하고, 그 압수수색의 방법에 대해 입법적으로 규정이 완비되지 못하였다.

이러한 규정의 미비는 전자정보의 압수수색에 대한 방법에 대하여 해석의 여지를 남긴다. 일례로 형사소송법 제120조 제1항에서는 '압수·수색영장의 집행에 있어서는 건정을 열거나 개봉 기타 필요한 처분을 할 수 있다' 고 규정하고 있는바, 전자정보의 압수수색에 있어서 정보가 암호화 되어 있는 경우 이를 복호화할 수 있는 근거로 위 규정을 적용하여 사용자에게 아이디와 패스워드를 제출하게 할 수 있다는 의견도 있다.[2)]

마찬가지로 전자정보의 압수수색에 대한 방법 중의 하나로 외국에 소재하고 있는 서버 등에 접속하여 정보를 취득하는 방법으로서 역외 압수수색이라는 쟁점은 여러 방면으로 다양하게 논의가 진행중이나, 현재까지 법률로 규정된 바가 없고 국제적으로도 일관된 내용은 없는 것으로 보인다. 최근 서울고등법원에서도 같은 쟁점에 관하여 엇갈린 결론의 판결을 시사할 정도로 그 허용성도 확립되지 않은 상태이다.

이 논문에서는 위와 같이 해외 서버에 있는 게시물 등 정보에 대한 압수수색의 방법으로써 계정 접속을 통한 압수수색이 허용되는지, 그러한 압수수색의 결과물의 무결성을 입증할 수 있는 방안은 무엇인지 연구하고자 한다.

이에 디지털증거의 특성 및 증거능력 인정요건은 무엇인지와 관련하여 무결성을 위주로 논한 후, 디지털 증거의 증거능력을 검증할 제3검증기관을 도입하여 계정 접속을 통한 역외 압수수색 시 망 연동을 통해 실시간 검증하는 방안을 논의하고자 한다.

---

2) 이숙연, 형사소송에서의 디지털증거의 취급과 증거능력, 고려대학교 박사학위논문, 2011, 33-34

제 2 장 역외 압수수색의 필요성과 허용성

제 1 절 디지털 증거 압수수색의 특성

Ⅰ. 디지털 증거의 특성

디지털 증거란 컴퓨터 또는 기타 디지털 저장 매체에 저장되거나 네트워크를 통해 전송 중인 자료로서 법정에서 신뢰할 수 있는, 증거가치가 있는 정보를 말한다.[3] 이러한 디지털 증거는 디지털 저장 매체에 저장되어 있으나 매체와는 독립된 정보라는 형태를 가지고 있어 네트워크를 통해 전송도 가능하고, 매체와 별개로 삭제도 가능하며, 같은 내용을 복사하여 다른 매체에 저장할 수도 있다(매체독립성, 원본과 사본의 구별 곤란성). 또한 디지털 저장 매체의 존재만으로는 그 내부의 정보를 볼 수 없고 정보를 확인하기 위해서는 어떠한 변환절차가 필요하며, 이를 가독할 수 있도록 하는데 전문적인 컴퓨터 기술이나 프로그램이 사용된다(비가시성・비가독성, 전문성). 디지털 증거는 클릭 등 하나의 명령만으로 순식간에 변경, 삭제가 용이하기 때문에 디지털 증거의 분석에서도 변경, 삭제되지 않도록 유의하여야 하고, 수사기관의 입장에서는 사용자가 증거를 임의로 조작, 삭제하기 전에 증거의 확보를 필요로 하므로 압수수색의 신속성도 필요로 한다(취약성). 또한 기존의 유체물과는 달리 저장기술의

3) 이상진, 디지털 포렌식 개론, 이룬, 2011, 65

비약적 발전으로 인해 방대한 분량의 정보를 하나의 저장매체에 모두 저장할 수 있어, 매체 내 저장 정보 중 압수수색의 목적물을 찾기란 쉽지도 아니하다(저장 정보의 대량성).[4] 마지막으로 현대는 인터넷 시대이기 때문에 개인용 PC나 모바일에 저장된 정보보다는 네트워크를 통하여 웹 또는 서버 상에 정보를 저장하는 경우가 상당수이므로 그러한 서버가 해외에 소재하는 경우의 압수수색 장소가 문제될 수 있으며, 반면 웹이나 서버는 네트워크를 통하여 언제, 어디서나 연결되어 있기 때문에 권한만 있다면 정보의 변형도 쉽게 발생할 수 있다(네트워크 관련성).

Ⅱ. 디지털 증거의 증거능력

디지털 증거는 위와 같은 특성을 가지고 있으므로, 이를 증거로 사용하기 위해서는 몇 가지 요건을 갖추어야 한다. 대법원 판례에서는 디지털 증거의 증거능력과 관련하여 다음과 같이 판시하고 있다.

“압수물인 디지털 저장매체로부터 출력한 문건을 증거로 사용하기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력한 문건의 동일성이 인정되어야 하고, 이를 위해서는 디지털 저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았음이 담보되어야 한다. 특히 디지털 저장매체 원본을 대신하여 저장매체에 저장된 자료를 ‘하드카피’ 또는 ‘이미징’한 매체로부터 출력한 문건의 경우에는 디지털 저장매체 원본과 ‘하드카피’ 또는 ‘이미징’한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입

4) 이윤제, 디지털 증거의 압수·수색과 증거능력, 형사법의 신동향 통권 제23호, 2009, 176-177

력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다. 그리고 압수된 디지털 저장매체로부터 출력한 문건을 진술증거로 사용하는 경우, 그 기재 내용의 진실성에 관하여는 전문법칙이 적용되므로 형사소송법 제313조 제1항에 따라 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다.” [5]

결국 디지털 증거는 (원본과 출력물의) 동일성(또는 원본성), 진정성, 무결성, 신뢰성, 전문증거로서의 증거능력 등이 인정되어야 증거로 사용될 수 있다. 또한 이 모든 것들의 전제로서 수집절차가 적법해야 한다.[6] 이 중 전문증거 전반에 적용되는 전문법칙을 제외하고 실제 디지털 증거의 증거능력에서 문제가 되는 것은 진정성과 무결성이 대부분이다. 원본성의 문제는 출력물을 원본과 동일하게 볼 수 있는지에 관한 문제이나 형사소송규칙 제134조의7에서 ‘컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체에 기억된 문자정보를 증거자료로 하는 경우에는 읽을 수 있도록 출력하여 인증한 등본을 낼 수 있다.’라고 규정하고 있어 특별한 독자적 의미를 가지지 못하며,[7] 신뢰성의 문제는 디지털 증거의 수집, 분석에 사용되는 장비나 프로그램, 이를 수행하는 전문가에 대한 신뢰여부에 관한 문제이며, 얼마나 전문성을 갖추고 있는지, 검증된 도구를 통해 동일한 조건에서 제3자에 의해서도 같은 결과가 도출될 수 있는지가 문제되나, 현재 디지털 포렌식 도구나 포렌식 수사관의 전문성에 대하여는 크게 다툼의 대상이 경우는 많지 않은 것으로 보인다.

---

5) 대법원 2007. 12. 13. 선고 2007도7257 판결
6) 형사소송법 제308조의2
7) 이윤제, 앞의 논문, 204-205

1. 진정성

디지털 증거의 진정성이란 수사기관이 증거를 수집, 저장하는 과정에서 오류가 없었으며, 제출된 증거가 특정인에 의해 특정시간에 생성한 그 자료와 같다는 것을 의미한다. 미국 연방증거규칙 제901조(a)는 '증거로 채택하기 위해서는 그 증거를 신청한자가 제출된 증거의 위조가능성이 없는 진정하고 원본과 동일한 것이라고 주장하고 이를 입증해야 한다.' 라고 규정하여 진정성의 내용에 대해 정의하고 있다.[8)]

위 판례의 취지에 비추어 보면, 진정성을 인정받기 위해서는 결국 동일성, 무결성, 신뢰성이 충족되어야 하는 것으로 보인다.

2. 무결성

디지털 증거의 무결성이란 디지털 증거가 원본으로부터 수집되어 보관, 분석되는 과정에서 수정, 변경, 훼손이 없도록 유지되어야 한다는 것이다. 위 판례에서는 '디지털 저장매체 원본이 압수 시부터 문건 출력시까지 변경되지 않았음이 담보되어야 한다.' 라고 판시하고 있다.

디지털 포렌식 수사실무에서는 디지털 증거의 무결성을 보장하기 위하여, 증거 수집 시(특히 이미징 작업 시) 해쉬 함수를 이용하여 해쉬 값을 도출하고 디지털 저장매체 원본의 해쉬 값과 법정에 제출된 해쉬 값을 비교 검증하여 동일하다면 무결성을 입증할 수 있다.

---

8) 전명길, 디지털증거의 수집과 증거능력, 법학연구 제41권, 2011, 330

제 2 절 역외 압수수색의 정의

Ⅰ. 개념

역외 압수수색에 대하여 명확히 정의된 바는 아직까지 없는 것으로 보이나, 일반적으로 수사기관이 수사상 필요성에 의해 역외에 존재하는 컴퓨터 데이터 및 관련 디지털 증거에 대해 집행하는 압수수색 방법을 말한다.[9] 그 외에도 네트워크를 통한 해외 서버의 원격 압수수색으로, 수사과정에서 해외 서비스에 대한 계정과 비밀번호를 알게 되었을 때, 수사기관 사무실 등에서 해외 서버에 접속하여 관련증거를 확보하겠다는 내용을 기재한 영장을 발부받아 집행하는 압수수색 방법이라고 보는 견해도 있다.[10] 그러나 뒤에서 살펴볼 바와 같이 위와 같은 압수수색의 방법은 역외 압수수색 유형 중 일부로 해석되고, 역외 압수수색의 의미는 포괄적으로 해외에 존재하는 서버 내 전자정보에 대하여 어떠한 방법으로 압수수색할 것인지에 관한 문제라고 정의할 수 있다.

Ⅱ. 유형

역외 압수수색에 대하여 유럽평의회 사이버범죄방지협약에서는 역외 압수수색을 다섯 가지로 유형화하고 있는바, 첫째, 원격지 압

9) 정소연, 디지털 증거의 역외 압수수색에 대한 법적 고찰, 디지털포렌식연구 제11권 제1호, 2017, 62

10) 정대용 외, 디지털 증거의 역외 압수수색에 관한 쟁점과 입법론 - 계정 접속을 통한 해외서버의 원격 압수수색을 중심으로 -, 법조, 2016, 136

수수색, 둘째, 합법적으로 획득한 계정정보를 이용한 압수수색, 셋째, 전문 소프트웨어 또는 기술적 수단을 이용하는 압수수색, 넷째, 동의를 얻어 접근하는 압수수색, 다섯째, 인터넷서비스제공자로부터 정보를 제공받는 압수수색이 그것이다.[11] 위와 같은 구분은 결국 계정 정보를 어떻게 취득하여 압수수색을 진행하는지에 따른 것으로 보인다.

위와 같이 사이버범죄방지협약에서 구분된 분류를 포함하여 역외 압수수색은 다음과 같은 기준에 따라 유형을 나눌 수 있다.

1. 서비스 제공자와 서버의 소재지에 따른 구분

서비스 제공자와 서버의 소재지에 따라서 역외 압수수색은 다음과 같이 구분된다. 첫째, 서비스 제공자와 서버의 소재지가 모두 해외에 있는 경우, 둘째, 서비스 제공자는 해외에, 서버의 소재지는 국내에 있는 경우, 셋째, 서비스 제공자는 국내에, 서버의 소재지는 해외에 있는 경우, 넷째, 서비스 제공자와 서버의 소재지는 해외에 있으나 서비스 제공자가 국내에 지점을 두고 있는 경우 등이다. 이중 서비스 제공자가 국내에 있는 경우에는, 뒤에서 살펴볼 것이지만 서버의 소재지가 해외에 있다고 하더라도 이를 관리하는 국내 서비스 제공자에 우리나라 영장의 집행이 가능하여, 국내 서비스 제공자로부터 협조를 얻어 증거를 확보할 수 있다.

2. 계정 정보 취득 방법에 따른 구분

수사기관에서 해외 서버 내 정보에 대한 원격 압수수색을 진행할

11) Report of the Transborder Group, Transborder access and jurisdiction: What are the options?, T-CY(Cybercrime Convention Committee), 2016, 19-23

경우, 계정 정보 취득 여부와 방법과 관련하여 다음과 같은 구분이 가능하다. 첫째, 계정 정보를 당사자로부터 직접 동의를 얻어 취득하는 방법, 둘째, 디지털 포렌식을 통해 계정 정보를 알게 된 경우, 셋째, 수사기관이 직접 해킹 프로그램 등을 통해 계정 정보를 취득하는 경우, 넷째, 영장을 통해 계정 정보를 인터넷 서비스 제공자로부터 취득하는 방법이 그것이다.

3. 압수수색 집행 방법에 따른 구분

형사소송법 제215조 내지 제218조의 규정에 따르면 압수수색은 영장에 의하여 하거나, 임의제출물을 영장 없이 압수하거나, 체포 구속 시 체포현장에서 영장에 의하지 아니하고 압수수색하거나, 긴급체포 시 소유, 소지, 보관하는 물건을 긴급 압수수색하는 등의 방법이 있다.

역외 압수수색의 경우에도 사용자의 동의를 얻어 계정 내 정보를 취득하는 방법과 영장에 의하여 압수수색하는 방법을 생각해 볼 수 있으며, 긴급성의 요건을 갖추는 경우 영장 없이 압수수색하는 방법도 상정할 수 있다. 영장에 의하여 압수수색을 하는 경우, 형사사법공조절차를 통해 영장 집행을 할 수 있다. 다만, 마이크로소프트, 트위터, 페이스북, 구글 등의 경우 가입정보, 접속 로그(IP, 시각 등) 등은 압수영장 또는 통신사실확인자료 제공요청 허가서를 보내주면 정보를 제공하고 있는 것이 수사실무이다.[12)13)]

---

12) 마이크로소프트사의 경우, 영장을 한국마이크로소프트에 팩스 송부하여 대상 정보를 요청하는 방법을 사용하고 있고, 구글은 구글 본사로 이메일 송부, 트위터는 트위터 본사로 팩스 송부하여 대상 정보를 요청하는 방법을 사용하고 있다. 페이스북의 경우 페이스북이 제공하고 있는 사이트인 https://www.facebook.com/records에 접속하여 메일로 '온라인 요청 시스템'에 접속할 수 있는 링크를 회신 받은 후 위 시스템에서 요청 정보를 입

4. 논의하고자 하는 역외 압수수색의 방법

살펴본 바와 같은 다양한 역외 압수수색의 방법 중 현실적으로 사용자의 동의를 얻어 압수수색하는 방법[14]은 논외로 하고, 또한 서비스 제공자가 국내에 있는 경우는 일반적인 역외 압수수색과는 약간 상이하므로,[15] 서비스 제공자가 해외에 있는 경우(그 중 서버가 해외에 있는 경우를 중점적으로[16]) 수사기관이 수사과정 중 적법하게 취득한 계정정보를 이용하여 수사기관 컴퓨터를 압수수색 장소로 특정한 영장을 발부받아 계정에 접속하는 방법의 압수수색을 논하고자 한다. 뒤에서 살펴볼 것처럼 수사기관이 사용자 계정 정보까지 영장으로 취득하고자 하는 것은 통신의 자유 등을 침해할 소지가 있고 그러한 영장이 발부된다는 것을 기대하기도 어려우므로 수사기관이 압수한 물건을 포렌식하는 과정이나 수사과정 중 적법하게 계정정보를 취득한 경우에 한정하고자 한다.

력하고, 영장 원본과 영문번역본을 스캔하여 첨부하는 방법으로 대상 정보를 요청하고 있다.

13) 즉, 서버 내 이용자가 작출한 정보가 아닌, 가입정보나 접속로그 등 컨텐츠와 관련 없는 정보에 대해서는 역외 압수수색의 논의에서 제외된다.

14) 이러한 압수수색은 강제처분이 아닌 임의처분으로 행하여지는 것이다. 전강진, 일본의 하이테크범죄의 현상과 과제, 해외연수검사연구논문집 제18집(2), 법무연수원, 2003, 235 각주63

15) 앞서 검토한 것처럼 서비스 제공자가 국내에 있는 경우에는 직접 서비스 제공자에 영장을 제시하고 협조를 구할 수 있고 형사사법공조절차의 문제도 발생되지 않는 것으로 보인다.

16) 뒤에서 살펴볼 바와 같이 서버가 국내에 있다고 하더라도 해외 서비스 제공자가 여러 서버를 분산하여 운영하고 있는 경우 어느 서버에 어떤 정보가 저장되어 있는지 알 수 없는 경우도 있기에 실제 집행 장소로 기재할 서버를 특정하기 어려울 것이다.

제 3 절 계정 접속을 통한 역외 압수수색의 필요성

Ⅰ. 국경을 초월한 증거의 소재

디지털 증거는 앞에서 살펴본 바와 같이 취약성과 네트워크 관련성이라는 특징을 가지고 있어, 국경을 초월하여 언제 어디서든 생성, 변경, 삭제가 가능하다. 따라서 디지털 증거가 유형물이 아니고, 위와 같은 디지털 증거의 특성으로 인하여 기존의 유형물에서 요구하는 압수, 수색의 기준을 그대로 적용할 수는 없다.[17] 특히, 클라우드 서비스나 구글, 트위터, 페이스북 등 실시간으로 데이터를 전송, 저장하는 인터넷 매체들이 등장하면서 범죄의 수단으로 사용될 가능성과 그 종류는 다양해진 반면에, 수사실무는 이러한 세태를 쫓아가지 못하고 있는 것이 현실이다.

이와 같이 국경의 벽을 넘어 디지털 증거가 실시간으로 저장되거나 관리되면서 디지털 증거를 확보하기 위해 네트워크를 통한 수사의 필요성도 점차 증가되고 있다. 클라우드 서비스에 저장된 여러 자료를 확보하거나, 구글 등 해외 이메일 서버에 저장된 내용을 확보하거나, 트위터 등 SNS에 저장한 게시글 내용을 확보할 필요성이 그것이다.

Ⅱ. 시·공간을 초월한 증거훼손의 우려

기존 디지털 증거는 자신이 관리하고 있는 PC나 휴대폰 내부 저

17) 이윤제, 앞의 논문, 173

장소 또는 USB 등 외부 저장매체에 정보가 저장되어 있으므로, 압수수색 진행 시 위와 같은 물리적 매체를 압수수색의 대상으로 삼을 수 있었다. 그러나 위에서 본 바와 같은 네트워크 환경의 변화로 정보가 물리적 압수가 불가능한 서버, 특히 해외에 있는 서버에 저장되어 있어 기존 압수수색 규정에 따라 영장을 발부받더라도 사법관할권 등의 한계로 직접 서버를 물리적으로 압수할 수 없다.

따라서 형사사법공조절차에 따라 서버 소재지인 해당 국가에 협조를 요청할 수밖에 없는데, 해당 국가가 협조를 하지 않을 가능성이 항상 존재할 뿐만 아니라 적극적으로 협조를 요구하기가 어렵고, 협조를 하더라도 시간이 오래 걸린다는 애로점이 있다.

반면에, 사용자는 디지털 증거를 언제, 어디서든 자유롭게 해외 서버에 저장, 변경, 삭제할 수 있는 권한을 가지고 있다. 사용자의 권한만 있으면 집이든, 회사이든, 또는 그곳이 어디든지 관계없이 서버에 접속할 수 있고, 그 서버가 국내에 있는지 해외에 있는지도 상관없다. 그렇기에 수사기관이 영장을 발부받아 형사사법공조절차를 거쳐 해당 인터넷 서비스 제공자로부터 협조를 구하는 동안 사용자는 직접 네트워크에 접속하여 저장된 증거를 얼마든지 변경하거나 삭제할 수 있는 증거훼손의 가능성이 항상 존재하는 것이다.

결국 기존의 유형물에 대한 압수수색과 관련하여서는 형사사법공조절차를 통해 진행하더라도 디지털 증거보다는 훨씬 증거훼손의 염려가 적은 반면, 디지털 증거의 특성으로 말미암아 이에 대한 압수수색과 관련하여서는 형사사법공조절차를 이용할 실익이 크지 않다. 이에 디지털 증거에 대한 새로운 압수수색 방법이 필요하게 되었으며, 디지털 증거의 취약성, 네트워크 관련성을 고려해 보면 수사기관이 계정에 접속을 하여 증거가 훼손되기 전 확보를 할 수 있도록 하는 압수수색 방법이 필요하다.

제 4 절 계정 접속을 통한 역외 압수수색의 허용성

Ⅰ. 서설

위와 같이 디지털 증거의 특성을 고려하여 볼 때, 기존 압수수색 방법과는 다른 방법의 모색이 필요한 것은 사실로 보인다. 앞서 살펴본 것처럼 역외 압수수색의 유형에는 여러 가지가 있으나, 형사사법공조를 통한 압수수색 방식을 제외한 방법 중 가장 현실적인 방법은 계정 접속을 통하여 해외 서버를 역외 압수수색하는 것이라고 판단된다.

그런데 수사기관이 계정 정보를 가지고 해외 서버에 접속하여 압수수색하는 방법은 현행법상 규정되거나 제도화되지 아니한 압수수색이기에, 그 허용성에 관하여 여러 쟁점이 도출될 수 있다. 전제적으로 문제되는 것은 수사기관이 역외 압수수색을 진행하기 위하여 취득하는 계정 정보에 관한 문제이다. 위에서 살펴보았듯이 계정 정보의 취득은 '적법하게' 아니면 '적법한 절차를 거치지 아니하고' 취득하게 되는데, 이러한 계정 정보의 취득이 개인정보침해로서 문제되지 않는지 쟁점이 된다.

또한, 계정 접속을 통한 역외 압수수색은 해외 서버에 저장된 정보를 대상으로 하는 것이므로 압수수색 집행에 있어서 국가관할권이 있는지 여부가 쟁점이 된다. 해외 서버에 대한 압수수색은 국내의 영장으로 다른 나라의 관할권 내에 있는 정보를 수색하는 것이므로 일반적으로는 형사사법공조를 통해 해결하거나 별도의 조약 등을 통해 목적을 달성하여야 하는 것이 원칙이다. 그러나 네트워크

환경의 급속한 변화와 현실적인 압수수색의 어려움 등으로 형사사법공조가 쉽게 이루어지기는 어려운 실정이다.

그 외에도 기존의 압수수색과는 다른 방법으로 진행하는 압수수색이기에, 소유자, 보관자 등을 상대로 직접 영장을 제시하고 압수수색하는 것이 아니라 서버제공자인 정보보관자의 참여 없이 진행되는 것이기에 압수수색 규정 위배 또는 영장주의 위배 여부도 문제될 수 있다.

Ⅱ. 허용성 여부

1. 학설의 대립

가. 긍정설

계정 접속을 통한 역외 압수수색을 긍정하는 입장으로, 계정 내 정보에 대한 처분권은 계정의 소유자에게 귀속되고, 수사기관이 계정정보를 이용하여 피압수자가 통상적으로 접속하는 방식과 동일하게 접속한다면, 타국에 소재하는 서버를 수사기관이 침탈하는 것이 아니라 피압수자인 계정 소유자의 접근권한을 이용하여 접근하는 것이기에, 피압수자의 접근권한을 일부 제한하는 강제처분에 해당한다고 볼 수 있어 허용할 수 있다는 견해가 있다.[18]

또한 해외에서는 각국의 수사기관이 영장을 집행하기 위해 해외 컴퓨터에 접속하는 상황이 발생할 수 있고, 정보에 관한 관할권은 물리적 저장위치에만 의존할 것이 아니라 시스템의 소유자가 다른

18) 정대용 외, 앞의 논문, 158

곳에서 접속할 수 있도록 설정한 이상 법집행 목적에서 관할권이 존재하는 것으로 보아야 한다는 견해[19], 역외 사이버범죄에 대항하기 위한 수단으로 영토주권에 의해 금지되지도, 전례가 없는 것도 아니므로 일방적인 역외집행을 타국의 주권에 대한 불법침입으로 볼 것이 아니라, 새로운 관습법의 정착과정으로 보아야 한다는 견해[20]도 있다.[21]

나. 부정설

계정 접속을 통한 역외 압수수색을 부정하는 견해는, 주로 영장의 장소적 범위를 벗어나 위법하다거나, 타국의 관할권을 침해하므로 위법하다는 주장이 다수로 보인다. 다른 컴퓨터에 대한 접속권한은 개인에 귀속되는 권한이지 컴퓨터라는 물건에 주어진 것이 아니기 때문에 접속권한이 컴퓨터 관리권의 일부로 볼 수 없고, 영장의 장소적 범위를 벗어난 다른 장소에 있는 컴퓨터에 대하여 영장의 효력이 미친다고 볼 수 없어 허용되지 않는다는 것이다.[22] 또한 해외 서버에 대한 압수수색은 허용 필요성은 있으나 입법적으로 해결해야 한다는 견해도 있다.[23]

---

19) Sussmann, Michael A, “The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium”, Duke Joumal of Comparative & International Law 9.2, 1999, 472

20) Goldsmith, Jack L, “The Internet and the Legitimacy of Remote Cross-Border Searches”, University of Chicago Legal Forum, 2001, 13

21) 정대용 외, 앞의 논문, 155

22) 전승수, 형사절차상 디지털 증거의 압수수색 및 증거능력에 관한 연구, 박사학위논문, 서울대학교, 2011, 198; 전강진, 앞의 논문, 234

23) 오병철, 클라우드 컴퓨팅에서의 사법관할권, IT와 법연구 제7집, 2013, 110; 정교일, 디지털증거의 압수와 공판정에서의 제출방안, 형사법의 신동향 통권 제25호, 2010, 146

2. 판례

계정 접속을 통한 역외 압수수색에 관하여, 최근 서울고등법원에서 엇갈린 해석을 내놓았다. 그 해석의 결과와 논거는 아래와 같다.

가. 외국계 이메일 계정에 대한 압수수색 절차를 적법하다고 본 판례(서울고등법원 2017노146)

국정원 수사관들이 피고인들의 메모 등에 기재된 아이디와 비밀번호를 이용하여 외국계 이메일 계정에 접속하는 방법으로 압수수색을 진행한 사안에 대하여, ① 국정원 수사관이 피고인들의 이메일 계정에 접속한 것은 수사의 필요상 법원의 영장에 의하여 영장에 기재된 상당한 방법에 따라 채증활동을 한 것이므로, 이는 정당한 접근권한을 가지고 해당 이메일 계정에 접속한 것에 해당하는 점, ② 형사소송법 제120조 제1항에서 '압수·수색영장의 집행에 있어서는 건정을 열거나 개봉 기타 필요한 처분을 할 수 있다'고 규정하고 있고, 이는 검증영장을 집행하는 경우에 준용되는바, 수사관이 적법하게 알아낸 피고인들의 이메일 아이디와 비밀번호를 입력하는 것도 이러한 '기타 필요한 처분'에 해당한다고 봄이 상당한 점, ③ 개인정보 보호법은 개인정보처리자가 정보주체의 동의를 얻지 않고 개인정보를 제3자에게 제공하는 등의 행위를 금지하고 있을 뿐, 법원의 영장에 의한 개인정보 취득까지 모두 금지하는 법률이라고 할 수 없으므로, 이러한 수사방식이 개인정보 보호법을 위반한 것으로 볼 수 없는 점, ④ 외국계 이메일이라 하더라도 전 세계 어디서나 접속할 수 있으므로, 이메일 서버관리자의 의사는 정당한 권한을 가지고 아이디와 패스워드를 아는 자라면 어디서든지 접속할 수 있도록 하려는 것으로 추정되고, 따라서 법원의 영장에 기하여

위 이메일에 접근할 정당한 권한을 가진 국정원 수사관이 대한민국에서 이메일에 접근했다고 하더라도 어떠한 위법이 있거나 국제적인 관할권의 문제가 생긴다고 볼 수 없는 점, ⑤ 국정원 수사관은 외국계 이메일 서버에 접속하여 범죄혐의와 관련된 파일을 추출하여 저장하는 방법으로 압수한 것일 뿐, 외국에 위치한 서버 그 자체에 대해 압수·수색을 한 것이 아니므로, 외국계 이메일의 압수·수색에 외국의 간수자가 참여할 필요는 없고, 국정원 수사관의 이러한 행위가 국제법상 관할의 원인이 되는 특별한 문제를 야기하는 것도 아니므로 사법공조를 거쳐야 한다고 볼 수 없는 점, ⑥ 컴퓨터를 조작하여 외국계 이메일에 아이디와 비밀번호를 입력하고 마우스를 클릭하는 행위는 압수수색검증 절차에 참여한 외부 디지털 포렌식 전문가가 담당하였는바, 위 전문가는 이메일을 다운로드받아 컴퓨터에 저장한 후 그 해시값과 USB에 복사한 이후의 해시값을 비교하여 동일함을 확인하였으므로, 이메일 파일을 USB에 저장하는 과정에서 어떠한 조작이 있을 수 없었던 것으로 보이는 점, ⑦ 한국인터넷진흥원에서 외국계 이메일 계정에 대한 압수·수색·검증 절차가 진행되기 전 피고인들에게 이를 통지하고 참여여부를 물은 이상, 그 통지가 당일에 이루어졌다는 것만으로 피고인들의 참여권이 형해화되었다고 보기 어려운 점, ⑧ 외국계 이메일에 대한 압수수색검증은 그 아이디와 비밀번호를 변경하거나 메일을 삭제하는 방법 등으로 손쉽게 증거인멸을 할 수 있어 긴급을 요하므로, 피고인들에게 당일 압수수색검증 사실을 통지하였다고 하여 위법하다고 볼 수 없는 점 등을 근거로 들어 압수수색이 적법하다고 판시하였다.

나. 외국계 이메일 계정에 대한 압수수색을 위법하다고 본 판례(서울고등법원 2017노23)

국정원 수사관들이 피고인의 usb에 들어 있던 파일을 복호화하여 알게 된 이메일 주소와 암호를 이용하여 외국계 이메일 계정에 접속하는 방법으로 압수수색을 진행한 사안에 대하여, ① 형사소송법에서 정하고 있는 압수수색은 압수할 물건을 상대로 이루어지는 대물적 강제처분인바, 외국에 위치한 서버에서 해당 디지털 정보 자체를 보관하고 있는 이메일서비스제공자에 대한 강제처분이 아닌 그 밖의 방법에 의하여 해당 이메일 계정에 접근하여 자료를 확보하는 것은 형사소송법이 상정하고 있는 압수수색방법이 아닌 점, ② 실제로는 해외 이메일서비스제공자가 외국 소재 서버에서 보관중인 전기통신 등을 압수수색의 대상으로 하면서도 압수수색 영장상의 압수수색 장소는 국내의 임의의 장소로 기재하고, 실제로 그 장소에서 압수수색을 집행하게 되는바, 이는 압수수색은 해당 대상물을 소지하고 있는 소유자, 소지자 또는 보관자를 상대로, 전기통신의 경우에는 해당 전기통신을 소지 또는 보관하고 있는 기관 등을 상대로 해당 물건이나 전기통신에 대하여 이루어질 것을 정하고 있는 형사소송법 제106조, 제107조 규정과 저촉되는 점, ③ 처분을 받는 자에게 해당 압수수색영장을 반드시 제시하도록 정하고 있는 형사소송법 제118조, 압수수색이 피고인 또는 피의자의 주거지 외에서 이루어질 경우 해당 주거주 또는 간수자 등을 참여하도록 정하고 있는 형사소송법 제123조 규정을 실질적으로 회피하게 되는 점, ④ 이러한 압수수색 방식은 압수수색 처분을 받게 되는 이메일서비스제공자의 참여를 배제한 채 이루어지게 됨으로써, 수집된 증거의 원본성과 무결성을 실질적으로 담보할 수 없게 되는 점, ⑤ 건정을 열거나 개봉하여 압수수색하는 장소 내지 대상물이 해외에 존재하여 대한민국의 사법관할권이 미치지 아니하는 해외 이메일서비스제공자의 해외 서버 및 그 해외 서버에 소재하는 저장매체 속 디지털 정보에

대하여까지 압수수색검증영장의 효력이 미친다고 보기는 어려운 점 등을 근거로 압수수색이 위법하다고 판시하였다.

3. 해외 사례

가. 사례

미국에서 계정 접속을 통한 역외 압수수색을 허용한 대표적인 사례로 United State v. Gorshkov Case가 있다. 이는 러시아에서 미국의 은행에 대한 해킹을 통해 금융정보를 빼낸 사건이 발생하자 미국 FBI가 러시아 해커를 채용이라는 미끼로 유인하고, 위와 같이 미국의 은행 사이트를 해킹하도록 테스트하여 러시아 해커가 러시아에 있는 서버에 접속해 해킹 툴을 다운받도록 한 뒤 접속한 계정 정보를 확보하여 러시아 서버에 접속하고 해킹 툴 등 데이터를 다운받아 증거로 활용한 사안이었다.

이 사안에서 변호인은 위와 같은 압수수색이 수정헌법 4조 또는 러시아법을 위반하였다고 주장하였으나, 미국 법원은 ' 수정헌법 4조는 미국인이 아닌 자에 대한 역외 수색에는 적용되지 않고, 수정헌법 4조가 적용되더라도 긴급한 사유로서 영장 예외 사유에 해당한다(즉시 복제하지 않으면 증거가 파괴되거나 사용하지 못하게 할 위험성이 있다는 합리적 이유가 있다), 또한 러시아법도 위반하지 않았으며, 그렇다고 하더라도 미국 재판 절차에서 증거를 금할 근거가 되지 않는다.'라고 판단하여 압수수색을 정당하다고 판시하였다.[24)]

---

24) Jihyun Park, "International trend against cybercrime and controversy over the F.B.I.'s practice of "Extra-territorial Seizure of Digital

일본의 경우 개정 형사소송법에서 제99조 제2항 및 제218조를 추가하여 ‘압수할 것이 전자계산기인 때에는 당해 전자계산기에 전기통신회선으로 접속하고 있는 기록 매체로서, 당해 전자계산기로 작성 또는 변경을 한 전자적 기록이나 당해 전자계산기로 변경 또는 삭제할 수 있는 전자적 기록을 저장하는데 사용되고 있다고 인정할 만한 상황에 있는 때에는 그 전자적 기록을 당해 전자계산기나 다른 기록 매체에 복사한 후, 당해 전자계산기나 다른 기록 매체를 압수할 수 있다’라고 해외 서버에 저장되어 있는 정보에 대한 압수수색도 가능하도록 규정한 사실이 있다.[25]

나. 유럽평의회 사이버범죄방지 협약

부다페스트 협약이라고도 불리는 사이버범죄방지협약(Convention on Cybercrime)은 1997년 각국의 사이버 범죄 전문가로 구성된 전문가 회의를 통해 사이버 범죄에 관한 최초의 국제협약을 제정하기 위해 시작하여 2001년 11월 23일 유럽평의회[26] 각료회의의 승인을

Evidence“, 국제법학회논총 제49권 제3호, 2004; 이 사건에서는 피의자의 인터넷 계정에 접속하여 피의자의 파일을 다운로드한 행위에 대하여 이것은 피고인 또는 다른 누군가의 데이터에 대한 재산상 이익을 침해한 것이 아니라는 이유로 압수에 해당하지 않는다고 결론 내렸다. 조기영, 디지털 세계에서의 압수수색, 법학연구 통권 제49집, 2016. 8. 254

25) 김범식, 경찰현장수사에서 디지털증거에 대한 압수수색의 개선방안, 외법논집 제38권 제4호, 2014, 179; 이원상, 클라우드 컴퓨팅 환경에서의 디지털 증거 확보를 위한 소고, 형사법의 신동향 통권 제38호, 2013, 197; 강철하 외, 디지털 포렌식에서 디지털증거의 특성과 법적 쟁점, 조선대학교 법학논총 제19권 제3호, 2012, 45

26) 유럽의 경제 및 사회적 발전 촉진을 위해 유럽 각국 정부간 협력을 도모하고 있는 기구(COE: Council of Europe), 보안뉴스 2015. 7. 21.자 기사 <사이버범죄 국제 공조 위한 부다페스트 협약, 우린 왜 아직?>

받아 탄생하였다.[27] 이 협약은 현재까지 유럽평의회 가입국 46개국, 미가입국 14개국이 가입한 상태이다.[28]

사이버범죄방지협약은 서문과 4장 및 48개 조문으로 구성되어 있는바, 제1장은 정의규정, 제2장은 범죄행위에 대한 처벌 및 그 절차에 관한 규정, 제3장은 국제공조에 관한 규정, 제4장은 협약의 가입, 발효 등 표준 규정을 두고 있다.

위 협약 제2장 중 19조에서는 '조사자가 만약 특정한 컴퓨터 시스템이나 그 시스템의 일부에 접근·수색할 권한이 있다고 확신하고 있고 또한 조사자가 그 시스템을 통하여 압수 대상 데이터가 저장된 다른 컴퓨터 또는 그 시스템의 일부에 접근할 수 있다면 조사자는 처음 시스템에 대한 접근 및 수색의 권한을 확장하여 다른 시스템까지 적용할 수 있다' 는 취지로 규정하고 있어,[29] 결국 허용성을 부정하는 입장의 주된 논거인 수색장소와 대상물이 보관된 장소가 달라 영장의 장소적 범위를 벗어난다는 부분을 입법적으로 해결하고 있다.

위 협약 제3장에서는 국제공조에 관한 특별규정으로 저장된 컴퓨터데이터의 신속한 보존, 보존 전송데이터의 신속한 공개, 저장된 컴퓨터데이터에 대한 초국경적 접속, 전송데이터의 실시간 수집에 관한 공조, 컨텐츠데이터의 방해에 관한 공조, 1주일 24시간 네트워

---

27) 이영준, 유럽의회의 사이버범죄방지를 위한 국제협약 소고, 형사정책연구, 2001, 7-8; 박영우, 사이버범죄방지협약의 국내법적 수용문제, 정보보호학회지, 2003, 70

28) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

29) 독고지은, 디지털증거 압수·수색에 대한 개정 형사소송법의 규제와 집행에 관한 연구 - 영장 집행 시 제기되는 쟁점을 중심으로 -, 법조, 2013, 31-32

크 조항을 두고 있다.[30] 그 중 협약 제32조에서 규정하고 있는 저장된 컴퓨터데이터에 대한 초국경적 접속의 내용은, ' 동의에 의한 또는 공개되어 있는 저장된 컴퓨터 데이터에 대한 초국경적 접속 당사국은 다른 당사국의 승인을 얻지 않은 상태에서, a. 데이터의 지리적 위치에 관계없이, 공개되어 있는 저장된 컴퓨터 데이터에 접속할 수 있고, b. 만약 당사국이 데이터를 공개할 법적 권한이 있는 자의 적법하고 자발적 동의를 얻었다면, 자국 영토내의 컴퓨터 시스템을 통해 다른 당사국에 위치한 저장된 컴퓨터 데이터에 접속하거나 이를 수령할 수 있다 '는 것이다.[31]

그런데 위 조문에서는 ' 동의에 의한 또는 공개된 컴퓨터 데이터에 대한 ' 역외 접속만을 규정하고 있고, 동의를 얻지 아니한, 강제처분에 대하여는 규정하고 있지 않기 때문에 완전히 계정 접속을 통한 역외 압수수색을 인정하고 있다고는 볼 수 없다. 다만, 위와 같은 규정은 결국 역외 압수수색 허용의 전제가 되는 사법관할권 문제에 대하여, 종래의 사법관할권을 초월한 수사가 가능하다는 의미로 해석될 여지가 있고, 컴퓨터 데이터에 대한 처분 등 권한이 사용자에게 있어, 사용자의 동의가 있다면 서버 제공자의 동의 여부 등과는 관계없이 압수수색이 가능하다는 취지로 선해할 여지도 있다.[32]

---

30) 이영준 외, 사이버범죄방지조약에 관한 연구, 형사정책연구원 연구총서, 2001. 12. 14-15

31) 사이버범죄협약 제32조, 전현욱 외, 사이버범죄의 수사 효율성 강화를 위한 법제 개선 방안 연구, 경제·인문사회연구회 미래사회 협동연구총서 15-17-01, 109-110

32) 결국 위 협약 제19조에서 자국내의 원격지 압수수색을 인정하고, 제32조에서 국경을 초월한 원격지 압수수색을 인정하고 있다고 해석된다. 법무연수원, 검찰실무 Ⅰ, 409

4. 쟁점의 검토

가. 문제 제기

(1) 관련 쟁점

계정 접속을 통한 역외 압수수색을 진행하기 위해서는 전제적으로 피압수자, 즉 사용자의 계정 정보를 알아야 한다. 또는 계정 정보를 알지 않더라도 계정에 접근할 방법이 있어야 한다. 결국 수사기관이 사용자의 계정 정보를 동의에 의하여 알게 되거나, 수사 중 알게 되거나, 영장에 의하여 강제수사의 일환으로 취득하거나, 또는 해킹 등의 방법으로 계정 정보를 취득하거나 계정에 접속하여야 한다. 그런데, 사용자의 계정 정보는 개인 정보에 해당하는 중요한 정보이므로, 이러한 개인 정보를 취득함에 있어서 어떠한 문제점은 없는지, 문제가 있다면 어떠한 방법까지 허용할 수 있는지 여부가 문제된다.

또한, 계정 접속을 통한 역외 압수수색은 계정을 제공하는(정보저장서버를 제공하는) 서비스 제공자가 존재하기 마련인데, 만약 압수수색을 진행하는 경우 서비스 제공자와 서버의 위치가 동일한 국가에 존재하지 아니한다면 압수수색 절차를 어떻게 진행해야 하는지, 서비스 제공자와 서버의 소재지에 따라 역외 압수수색의 허용성이 달라지는지 여부 등도 문제가 될 수 있을 것이다.

(2) 허용성 문제

계정 접속을 통한 역외 압수수색의 허용성을 논하기 위해서는 크

게 두 가지의 쟁점이 발생한다. 첫 번째는 국가 관할권, 즉 주권의 침해 문제이다. 일반적으로 해외 서버의 압수수색은 타국의 관할권을 침해하기 때문에 조약체결의 대상으로 보아야 한다는 견해도 있다.[33] 해외에 있는 기업에 대하여 압수수색을 진행하는 경우, 집행관할권이 다르므로 우리나라의 영장으로 곧바로 해외에서 집행할 수 없고 국제 사법 공조 절차에 의하여야 함이 원칙이다. 압수수색 외에 체포, 구속 등의 경우에도 마찬가지이다. 그렇다면 해외에 직접 나가서 영장을 집행하여 압수수색하는 것과 달리, 국내의 컴퓨터 등으로 '권한 있는 자'의 계정 정보를 입력하여 해외 계정에 접속하는 방법으로 진행되는 역외 압수수색에서도 관할권 침해의 문제가 발생하는지 쟁점이 될 수 있다.

둘째로, 종전의 압수수색 절차와 달리 해외 서버에 대한 계정 접속의 방법으로 압수수색이 진행되므로, 기존 형사소송법상 영장 제시, 사전통지, 참여권 규정 등을 준수할 수 있는지, 압수수색 규정을 회피하거나 위배하게 되는 것은 아닌지도 문제가 될 수 있다.

(3) 역외 압수수색으로 취득한 증거의 문제

만약 역외 압수수색이 허용된다면, 그로 인해 취득한 증거, 즉 계정 내 정보의 내용을 화면 또는 인쇄물로 출력한 결과물의 증거능력을 인정함에는 아무런 문제가 없을까. 서버의 특성상 다른 디지털 증거와 같이 원본을 압수하거나 원본 전체에 대한 이미징 작업이 곤란하기 때문에 기존의 무결성 입증 방법으로는 압수수색 결과물에 대한 원본성 및 무결성 입증이 어렵다고 사료된다. 그렇다면 계정 접속을 통한 역외 압수수색으로 취득한 증거의 무결성 입증은

33) 오기두, 사이버수사 및 디지털 증거수집 실태조사 결과발표 및 토론회의 토론문, 국가인권위원회, 2012; 이숙연, 앞의 논문, 36

어떠한 방법으로 가능할지 살펴볼 필요가 있다.

나. 계정 접속을 통한 역외 압수수색의 특성 이해

(1) 정보에 대한 압수수색

압수수색은 대물적 강제처분에 해당한다. 따라서 압수수색의 대상은 증거물 또는 몰수할 것으로 사료하는 물건[34]으로서 결국 '물건'이 된다. 사실 디지털 증거와 유체물인 증거는 그 특성만 다를 뿐 증거의 내용이나 수집에 관하여 큰 차이가 난다고 볼 수는 없다. 어떤 피의자가 증뢰의 증거로서 수뢰자와 증뢰액 등에 관하여 기존에는 수첩에 기재한 후 비밀 창고에 보관하여 자물쇠로 잠근 후 보관하는 방법으로 증거를 은닉하였다면, 이제는 피의자가 해외 클라우드 서비스를 이용하여 암호화된 계정에 접속한 후 그러한 메모를 저장시키는 방법으로 발전하였을 뿐이다. 수사기관은 그 증거를 찾기 위해 유체물의 경우 피의자의 주거지 내에 있는 비밀창고의 문을 열고 들어가(필요한 처분) 전부 수색한 후 수첩을 압수하게 되고, 디지털 증거의 경우 피의자가 사용하는 클라우드 서비스의 계정에 접속하여(필요한 처분) 정보를 수색한 후 필요한 증거인 메모를 출력하는 방법으로 압수하게 되는 것이다. 다만, 디지털 증거는 유체물과 비교하여 대량의 정보를 한 곳에 저장할 수 있고, 그에 따라 무관 정보가 대량 노출될 위험이 있는 것이다.

그런데 디지털 증거의 압수수색의 경우 유체물과 다르게 그 정보의 내용을 보기 위해서는 출력이라는 새로운 행위가 있어야 하기에, 압수수색의 대상이 '정보'인지, 수색의 결과로 얻어 낸 '출력

34) 형사소송법 제106조

물’ 인지에 대하여 논란이 있다. 전자적 기록, 즉 정보에 대하여 압수수색의 대상이 될 수 있는지 여부에 관하여는 긍정설과 부정설의 학설상 대립은 있으나, 개정 형사소송법 제106조 제3항에서 ‘압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다’고 규정하여, 결국 압수수색의 대상은 컴퓨터용디스크 등의 정보저장매체, 곧 유체물이라는 것을 암시하고 있다.

그러나 여전히, 종국적으로 증거의 실질이 되는 것은 정보저장매체가 아닌 그 안에 저장된 ‘정보’라는 모순에 빠진다. 압수수색이라는 것은 우리가 만질 수 있어 취득할 수 있는 어떠한 유체물이 있어야 가능한 행위임은 틀림없으나, 그 결과로 취득한 ‘물체’가 증거의 내용이 되는 것은 아니기 때문이다. 디지털 증거라는 특성이 그렇다. 어찌되었든 재판정에 증거로 제출하기 위해서는 ‘정보’의 상태를 제출할 수는 없으므로, 그 내용이 보일 수 있도록 문서 또는 화면으로 출력하여야 한다. 정보저장매체(원본)를 압수하더라도 매체 내에 저장된 정보를 보기 위하여 어떠한 프로그램이 존재하여야 하고, 이로써 문서 또는 화면으로 출력하여야 하는 것이다. 따라서 기존의 디지털 증거는 원칙적 선별압수, 예외적 매체압수의 방법에 따라서 압수수색의 현장에 존재하는 컴퓨터 등 장치에서 정보를 선별, 출력하거나 그것이 어려우면 매체를 압수하여 수사기관 내에서 선별, 출력하였다.

그런데, 인터넷 기술의 발전과 글로벌 네트워킹 환경의 변화로 단순히 컴퓨터 또는 개인용 외부 저장매체에 정보를 저장하고 관리

하는 시대에서, 대용량 정보를 저장할 수 있는 서버를 제공하는 서비스 제공자가 나타나고 이를 이용하는 이용자들이 국경을 초월하여 증가하면서 기존의 압수수색 방법을 이용하기 곤란해졌다. 압수수색 현장에 출동하여 원본 매체의 내용을 검색하여 선별 압수하거나, 원본 매체를 압수하는 2가지 방법 모두 불가능하다 할 것이다. 서버가 위치한 곳에 직접 현장 압수수색을 할 수 없고, 현장에 출동하더라도 서비스 제공자의 협조 없이는 대규모의 서버 내에서 피압수자의 정보를 찾기란 곤란하며, 원본 매체인 서버를 압수할 수도 없기 때문이다. 결국 이와 같은 환경에서는 서비스 제공자의 협조가 없이는 압수수색이 이루어질 수 없다. '대물적 강제처분'인 압수수색은, 이제는 실질적으로는 서비스 제공자에 대한 협조의무를 강제할 수밖에 없는 상황에 이르렀다.[35]

반면에 계정 접속을 통한 압수수색의 방법은 사실상 서비스 제공자의 협조가 필요치 아니하다. 대규모의 서버 내에서 피압수자의 정보를 검색하기 위해 서비스 제공자의 협조를 얻을 일이 없고, 그렇다고 하여 원본의 압수가 필요하지도 아니하다. 서비스 제공자의 입장에서는 정당한 권한자의 접근이기 때문이다.

(2) 수색과 압수의 구별

압수수색은 통상적으로 함께 이루어지고, 영장도 단일영장으로

35) 서울고등법원 2017노23 판결문에서는 송수신이 완료된 이메일 압수수색에 관하여, 전기통신에 대한 압수수색은 비록 대상이 유형물이 아니어서 실제 압수수색을 하기 위해서는 해당 자료를 보관하고 있는 기관 등의 협조가 필수적이라는 특징이 있기는 하나, 이를 달리 볼 것은 아니므로 기존 압수수색 규정이 그대로 적용된다는 취지로 판시하였으나, 판결문 내용과 같이 정보(전기통신)는 유형물이 아니므로 이에 대한 압수수색이 기존 유형물에 대한 압수수색과 같을 수는 없다.

발부되고 있는 것이 현실이나, 압수와 수색은 다르다. 압수란 물건의 점유를 취득하는 강제처분을 말하고, 수색은 압수할 물건 또는 체포할 사람을 발견할 목적으로 주거, 물건, 사람의 신체 또는 기타 장소에 대하여 행하는 강제처분을 말한다.[36] 결국 수색은 압수를 위한 선제적 행위를 말한다고 볼 수 있다. 따라서 압수의 대상이 곧 수색의 대상과 일치한다고는 볼 수 없다.

주로 디지털 증거에 대한 압수수색에서, 압수와 수색의 구별이 잘 드러난다고 사료된다. 정보저장매체 내에 있는 정보 중 증거로 사용될 일부 정보는 압수의 대상이 되지만, 나머지는 압수의 필요성이 없다. 그렇지만 그 일부 정보의 범위를 정하기 위하여 정보저장매체 내에 있는 모든 정보가 수색의 대상이 된다. 수색 행위는 '출력'의 행위를 필요로 하지 않으며, '출력'은 압수를 하기 위하여, 즉 유체물로 전환하기 위하여 필요한 행위이다. 따라서 증거로 사용할 일부 정보를 찾기 위해 정보저장매체 내 정보를 수색한 후, 증거로 사용할 정보의 내용에 대해서만 출력을 하여 그 출력물을 압수물로 사용하게 되는 것이다.

계정 접속을 통한 역외 압수수색에서도 마찬가지로, 수색을 위하여 계정에 접속한 후 계정 내에 있는 정보들을 대상으로 수색하고, 그 중 증거로 사용할 정보의 내용을 화면 또는 인쇄물로 출력하여 그 출력물을 압수물로 사용하게 된다고 할 수 있다.

(3) 선별 압수 가능

계정 접속을 통한 역외 압수수색의 경우, 위에서 검토한 바와 같이 원본의 압수가 불가능하고, 원본에 대한 이미징도 불가능하다. 결국 위와 같은 압수수색의 방식은 원본 내 저장된 정보에 대한 선

36) 이재상, 신형사소송법 제2판, 박영사, 2009, 300

별 압수만이 가능하다. 수사기관은 계정 내 정보를 수색하여 관련성과 필요성이 인정되는 정보의 범위를 정하여 선별하여 출력하고 이를 증거로 사용할 수 있다. 즉, 선별 압수의 원칙에 충실할 수 있으며, 서버를 이용하는 다른 이용자들이나 서버 관리자, 피고인 등 모두에게 있어서 그 침해의 정도가 약한 수사방법이라고 사료된다.[37]

다. 서비스 제공자와 서버 소재지에 따른 역외 압수수색 가능성 여부

(1) 문제 제기

역외 압수수색은 서비스 제공자와 서버 소재지에 따라, 서비스 제공자와 서버 소재지 모두 해외에 있는 경우, 서비스 제공자만 해외에 있는 경우, 서버 소재지만 해외에 있는 경우로 나눌 수 있을 것이다. 그런데 이 장에서 논의하고자 하는 계정 접속을 통한 역외 압수수색은 압수수색에 있어서 국내에서 영장을 집행할 수 없는 경우를 전제하고 있다. 만약 국내에서 영장 집행이 가능하다면 (디지털 증거의 특성상 증거인멸의 우려로 계정 접속을 통한 압수수색의 필요성은 있을지 몰라도) 형사사법공조절차도 필요하지 아니하고, 계정 접속을 통해 역외 압수수색을 할 근거가 부족하다고 볼 것이다.

한편 해외에 서비스 제공자나 서버 소재지가 있는 경우, 형사사

37) 안경옥, 형사재판절차에서 테크놀로지의 활용과 형사소송법적 문제점, 21세기 형사사법개혁의 방향과 대국민 법률서비스 개선방안 Ⅳ, 한국형사정책연구원, 2004, 169

법공조절차를 통해 영장을 집행하거나 협조를 구할 때 과연 서비스 제공자의 소재지를 관할하는 국가와 서버 소재지를 관할하는 국가 중 어느 국가에 공조를 요청할 것인가의 문제도 발생한다. 이는 결국 압수수색의 대상이 '물건' 그 자체에 관한 것인지, 관리자인 '사람'에 대한 것인지의 문제로도 연결될 수 있다.

(2) 검토

위에서 살펴보았듯이 압수수색은 원칙적으로 대물적 강제처분이므로, 압수수색의 대상은 물건이다. 그러나 글로벌한 대규모 네트워킹 환경에서 서비스 제공자는 서버를 두며 사용자의 정보를 관리하고 있고, 다만 서버 내에 저장된 정보에 대한 작성, 수정, 삭제, 접근에 대한 권리는 모두 권한을 가진 사용자가 가지고 있다.

원칙적인 입장에서 압수수색의 대상은 '물건'이므로, '물건'인 서버의(또는 서버에 저장된 정보의) 소재지가 압수수색의 장소가 된다고 볼 것이다. 이에 따르면 서버가 소재한 국가에 대하여 압수수색 영장을 집행하여야 한다.

그런데 현실적으로는 서비스 제공자가 소재한 국가에 대하여 공조 요청을 함이 타당하다고 사료된다. 왜냐하면 앞서 검토한 바와 같이 서버만 있을 뿐 서비스 제공자의 협조가 없다면 실질적으로 서버 내 전자정보의 압수가 불가능하다고 할 것이고, 또한 서비스 제공자가 한 국가만이 아닌 여러 국가에 서버를 두고 있는 경우도 있기에,[38] 당해 데이터가 어느 서버에 저장되어 있는지 알 수 없기 때문이다. 실제로 구글, 아마존, 페이스북 등 국제적인 서비스의 경우 전 세계에 데이터 센터를 두고 서버를 가상화·분산화하여 운영하고 있어 압수할 전자 정보가 어느 국가의 관할에 존재하는지 확인

38) 전현욱 외, 앞의 논문, 114

하기도 어렵다.[39]

서비스 제공자 소재지를 기준으로 압수수색의 관할을 따져본다면, 서비스 제공자 소재지가 우리나라에 있는 경우에는, 서버가 해외에 있다고 하더라도 우리나라의 영장을 서비스 제공자에게 제시하고 데이터를 압수수색할 수 있기에 계정 접속을 통한 역외 압수수색에 대한 필요성이 낮다.[40]

따라서 계정 접속을 통한 역외 압수수색은 서비스 제공자가 해외에 있는 경우를 상정하고, 또한 서비스 제공자가 여러 서버를 두고 있는 경우라도 서비스 제공자의 소재지 관할권의 적용을 받는다고 할 것이다.[41]

한편, 서비스 제공자가 해외에 있으나 국내에 지사를 두고 있는 경우는 어떠할까. 국내 영장의 집행이 국내에 소재한 지사에서 가능하다면 역외 압수수색의 필요성은 낮아진다. 살피건대 만약 국내 소재 지사에서 데이터를 관리하는 권한이 있어 영장집행에 협조가 가능하다면 형사사법공조나 역외 압수수색의 허용 가능성은 거의 없다고 판단된다. 그러나 대부분의 데이터는 본사에서 관리되는 것이 사실이며, 실제로 페이스북과 구글은 한국 지사가 있지만, 모든 데이터는 미국 본사에서 관리하고 있어 자료제공에 있어 아무런 역할을 하지 못하고 있다.[42] 그렇다면 국내에 지사가 있는지 여부와 관계없이 역외 압수수색은 서비스 제공자가(그 본사가) 해외에 있는

---

39) 정대용 외, 앞의 논문, 149

40) 다만 긴급성이 있어 원격 압수수색이 필요한 경우도 있을 수 있지만, 그 문제는 별론으로 한다.

41) 해외 서비스 제공자가 국내에 서버를 두고 있는 경우라고 하더라도 앞서 본 바와 같이 서버만 있다고 하여 디지털 포렌식 전문가들이 그 서버에서 원하는 정보를 취득하기란 어렵고, 반드시 서비스 제공자의 협조가 요구되므로 결론은 다르지 않다고 할 것이다.

42) 전현욱 외, 앞의 논문, 170

경우에만 허용된다고 봄이 상당하다.

라. 계정 접속을 위한 계정정보 취득 문제

(1) 서설

사용자의 계정 정보는 개인정보로서 비밀의 영역에 해당한다. 헌법 제17조는 '모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.'고 사생활의 비밀과 자유, 즉 프라이버시권을 규정하고 있다. 이로부터 도출된[43] 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리를 말하는바,[44] 당해 개인을 식별할 수 있는 개인정보를 당사자의 동의 없이 유통하거나 공개하는 경우 이러한 권리가 침해될 수 있다.

유체물을 대상으로 하는 압수수색은 유체물의 특성에 따라 그 존재 범위와 정보의 내용에 어느 정도의 한계가 있었으나, 과학기술의 발달에 따라 대용량의 정보를 저장할 수 있는 매체가 생기면서 네트워크 공간에 개인이 비밀로 보호하고자 하는 정보가 대량으로 저장될 수 있어, 과학수사기법에 따른 수사가 개인의 프라이버시를 침해할 가능성이 더 커졌다. 따라서 임의 수사의 원칙에 따라 당사자

---

43) 개인정보자기결정권이 헌법 제10조에서 도출된다는 견해(김철수), 헌법 제17조에서 도출된다는 견해(권영성)도 있으나, 대법원(96다42789) 및 헌법재판소(2003헌마282 등) 판례는 헌법 제10조와 제17조에서 그 근거를 찾고 있다.

44) 헌법재판소 2005. 5. 25. 99헌마513, 2004헌마190 결정 참조; 사용자의 아이디와 암호 등 계정 정보는 그 정보주체를 타인으로부터 식별가능하게 하는 개인정보에 해당된다고 보인다.

의 동의에 따른 수사가 가능한 경우라면 강제수사가 곤란하고, 예외적으로 필요한 경우에 한하여 영장을 발부받아 강제수사를 함이 타당하다.

계정 접속을 통한 역외 압수수색을 하기 위해서는 필연적으로 사용자의 계정 정보를 알아야만 한다. 계정 정보를 취득하는 과정은 크게 동의에 의한 방법과 동의에 의하지 않은 방법이 존재하고, 동의에 의한 방법은 임의 수사에 해당되므로 개인 정보 침해의 여지가 적어진다.

그러나 여전히, 동의에 의하지 않은 계정 정보의 취득은 문제의 소지가 될 수 있다. 동의에 의하지 않은 계정 정보의 취득은 다시 수사 과정 중 별도의 절차를 거치지 아니하고 적법하게 계정 정보를 취득하게 된 경우(수사를 통해 얻은 정보로 유추하거나, 포렌식 과정에서 계정 정보를 알아낸 경우), 영장을 통해 강제수사의 일환으로 계정 정보를 취득하는 경우, 해킹 등 기술적 조치를 통해 계정 정보를 취득하거나 계정에 접근하는 경우로 나누어 볼 수 있다. 가장 문제가 되는 것은 해킹 등 기술적 조치를 이용하거나 강제적인 방법으로(영장 등에 의해) 계정 정보를 알아내는 것이다.

그렇다면 과연 당사자의 동의 없이 계정 정보를 취득하는 행위가 헌법상 개인정보자기결정권을 침해할 소지가 있지는 않은지, 어떠한 방법으로 계정에 접속하는 것까지 허용할 수 있는지 문제가 된다.

(2) 수사상 필요한 처분과 개인정보자기결정권

이에 대하여는 수사기관이 압수수색 장소에 존재하는 컴퓨터로 해당 웹사이트에 접속하여 디지털 증거를 다운로드한 후 이를 출력 또는 복사하거나 화면을 촬영하는 방법으로 압수한다는 취지를 영

장청구서에 기재하여 압수수색영장을 발부받는 경우에는 수사기관이 피압수자에게 해당 웹사이트에 접속할 수 있는 아이디와 패스워드 등의 제공을 요구할 수 있고, 이는 형사소송법 제120조에 정한 '압수수색영장의 집행에 필요한 처분'의 범위에 속할 수 있다는 견해가 있다.[45] 이에 반하여 건정을 열거나 개봉하는 것은 집행기관의 행위일 뿐이므로 '필요한 처분'에 피처분자의 협력을 명령하는 내용을 포함시키는 것은 무리한 해석이라는 견해도 있다.[46]

살피건대, 계정 접속을 통한 역외 압수수색을 하기 위하여 사용자의 동의 없이 개인정보인 계정 정보를 취득하는 행위는 개인정보 자기결정권을 제한하는 것에 해당한다. 따라서 이러한 제한이 정당화되기 위해서는 범죄수사 등의 합목적성과 비례의 원칙에 따라 판단해 보아야 한다.

계정 접속을 통한 역외 압수수색은 네트워크를 통한 전 세계의 연결이 시·공간을 초월하여 클릭 한 번으로 가능하게 된 현재의 수사상황에서 해외에 소재한 증거를 수집하여 형사사법의 실체적 진실에 부합하도록 하기 위한 수사의 방법으로서 그 목적의 정당성이 인정되고, 증거 훼손이 매우 손쉽게 이루어질 수 있다는 점에서 긴급성이 있어 이러한 역외 압수수색이 그와 같은 목적을 달성하기 위한 효과적이고 적절한 방법의 하나가 될 수 있으며, 형사소송법 제120조 제1항에서 '압수·수색영장의 집행에 있어서는 건정을 열거나 개봉 기타 필요한 처분을 할 수 있다.'라고 규정하고 있어 사용자의 계정 정보를 입력하여 네트워크에 접속하는 것이 위 규정에

45) 이숙연, 앞의 논문, 33-34; 특히 예방적 온라인수색을 인정하고자 하는 입장에서는 수사상 필요성을 이유로 영장이나 기술적 조치를 통해 정보를 취득할 수 있다고 볼 것이다.
46) 이윤제, 디지털 증거 압수수색영장의 집행에 있어서의 협력의무, 형사법연구 제24권 제2호, 2012, 313

서 말하는 기타 필요한 처분에 해당된다고 사료된다. 따라서 실체적 진실 발견이라는 수사의 목적을 달성하기 위해 증거가 저장되어 있다고 추정되는 서버의 계정 정보를 취득하는 행위는 그 목적의 정당성과 수단의 적합성이 인정된다.

그러나 수사기관이 수사 활동을 통해 정당하게(위법하지 않은 방법으로) 수집한 증거로부터 계정 정보를 지득하였다면, 피의자의 개인 정보를 취득하기 위해 어떠한 침해적인 방법을 사용하지 않았고 그러한 방법을 따로 사용할 가능성도 없는 점, 해외 서버 내 정보를 취득하기 위해서는 사실상 계정 정보를 입력하여 접근하는 방법이 효율적이고, 실현 가능한 수단이 되며, 서버 내 다른 이용자들의 정보 침해나 서버 관리자에 대한 재산권 보호 등의 측면에서도 가장 침해의 정도가 최소화되는 것으로 보이는 점에 비추어 과잉금지의 원칙에 위배된다고 볼 수 없겠으나, 한편, 수사기관이 역외 압수수색을 하기 위하여 사용자의 계정 정보를 취득해야 한다는 점을 이유로 계정 정보 취득을 위한 영장을 발부받거나, 해킹 등 기술적인 조치를 이용하여 사용자의 계정 정보를 취득하는 경우에는 역외 압수수색으로 인한 사생활 비밀 등 기본권 제한에 더하여 개인정보를 보호하고자 하는 헌법이나 법률의 취지에 반하여 개인정보 취득을 위한 또 다른 수단을 사용하게 되어 기본권 침해 정도가 커지게 되는 점, 임의수사의 원칙에 따라 사용자의 동의를 얻어 계정 정보를 취득할 가능성도 있는 점, 발부받은 영장을 서비스 제공자에게 집행하여 계정 정보를 취득하고자 한다면 서비스 제공자의 재산권 등 보호에 제한을 가하게 되는 점, 또한 해킹 등의 기술적 조치는 수사기관이 법률상 규정되어 있는 정당한 방법이 아닌 오히려 ‘권한 없는 자’의 접근으로서 불법한 방법을 사용하게 되는 점 등을 고려해 볼 때 피해의 최소성이나 법익 균형성이라는 틀에 비추어 기

본권 침해적인 수사 방법이라고 생각된다.

결국 수사기관이 계정 접속을 통한 역외 압수수색이라는 방법을 사용하고자 하는 경우라도, 이는 사용자의 동의를 얻어 계정 정보를 취득하거나, 예외적으로 수사기관에서 수사 중 적법하게 지득한 계정 정보를 이용하여 접근하는 방법만이 가능하다고 하여야 할 것이다.

마. 관할권(주권) 검토

(1) 문제 제기

계정 접속을 통하여 해외에 있는 서버에 접근하고 서버에서 정보를 취득하는 경우, 대한민국의 사법관할권이 미치지 않는 것이 아닌지 문제가 된다. 국가 간 경계가 되는 영토를 기준으로 관할권을 정하는 경우, 해외 기업에 대한 압수수색은 관할권을 벗어나는 것이므로 형사사법공조절차를 거치지 아니하고는 집행이 곤란하다고 할 것이다. 그러나 현재와 같이 국경을 초월한 네트워크 환경을 고려하여 본다면, 사법관할권의 범위를 기존과 같이 영토만을 기준으로 삼아야 하는지에 대해서는 의문이 있다.

더 나아가 과연 계정 접속의 방법으로 해외 서버에 저장된 정보를 취득하는 압수수색이 타국의 관할권을 실질적으로 침해하는 것인지에 대하여도 검토할 필요가 있다.

(2) 기존 국가관할권의 정의와 시대의 변화

기존의 국가관할권은 국제법상의 주권 및 국가 영토의 개념과 관

련되어 그 행사의 범위를 중심으로 발전되어 왔다.[47] 이른바 원칙적 속지주의에 따라 해당 국가 내에서 발생한 사건에 대한 관할권은 해당 국가에서 갖는 것이다. 사법적 처리와 관련하여 사법관할권의 행사는 타국의 영토주권을 침해할 수는 없으나, 범죄 행위로 인하여 피해를 입은 국가가 적절한 조치를 취하지 못하여 형사사법의 정의를 구현하지 못하고 자국민의 피해를 계속하여 방치해 둘 수도 없는 문제가 생기기에 사법관할권의 보장도 필요하다.[48]

기본적으로 각 국가의 사법행위는 그 국가의 주권에 관한 문제이므로 대부분의 국가가 외국 수사기관이나 법집행기관이 자국 내에서 범죄수사 행위를 하거나 사법행위를 수행하는 것을 용인하지 않고 있으며 국제적 형사사법 조약 등을 통하여 제한된 범위 내에서만 허용되고 있다.[49]

그러나, 클라우드 컴퓨팅 환경에서는 전통적인 방식을 통해 관할권을 결정하기 어렵다. 클라우드 컴퓨팅 환경의 특성상 사용자의 국적지와 사용자의 정보를 저장한 매체가 존재하는 물리적 위치가 동일하지 않은 경우가 발생하기 때문이다. 관할권의 충돌이 일어난 경우 정보의 주체가 속한 국가와 정보를 저장한 매체가 존재하는 국가 중 어느 나라가 지배권을 가져야 하는지에 대한 논란도 있다.[50] 앞서 본 바와 같이 서비스 제공자와 서버의 소재지가 각기 다른 국가에 있기도 하고, 여러 국가에 분산되어 있거나 심지어 어느 국가

---

47) 원재천, 자국법의 역외적용과 한국의 대응방안에 관한 연구, 법무부, 2011, 2

48) 정소연, 앞의 논문, 67

49) 한봉조, 사이버범죄수사에 대한 국제적 협력문제, 형사정책연구, 2000, 34

50) 정현지 외, 클라우드 컴퓨팅 환경에서의 디지털 포렌식 동향 및 전망, 정보보호학회지 제22권 제7호, 2012, 10; 이창범 외, 클라우드 컴퓨팅 활성화를 위한 법제도 개선 방안 연구, 한국인터넷진흥원, 2010, 386-390

에 서버가 존재하는지 여부를 알 수 없는 경우도 있다.

네트워킹 사회에서 압수수색 대상 기재사항에 공간을 특정하도록 요구하는 것은 장소를 특정하는 물리적 위치 개념에서 범죄와의 관련성 및 논리적 공간을 특정하는 개념으로 변화해야 할 것이다.[51] 네트워킹 사회에서는 물리적으로 국경을 넘어 진입하는 것이 아닌 가상세계에서 물리적 공간을 초월하여 언제, 어디서나 데이터에 접근이 가능하므로 기존의 물리적 공간에 따른 관할권이 그대로 적용된다고 보기도 어렵다. 원격지에서 범행을 실행하지만 그 피해는 당해 국가가 아닌 다른 국가의 국민에게 입히게 되는 경우도 계속 증가하게 될 것이다. 그 가운데서 각 국가의 영토주권과 집행관할권 등의 충돌이 발생하게 된다. 기존의 속지주의, 예외적 속인주의 원칙에 따르더라도 이러한 행위는 자국에서 사법처리 될 수밖에 없으나, 피해국가의 입장에서는 국민을 보호하기 위해 보호책과 예방책, 그리고 차후 사건이 일어날 경우에 대한 대비책을 강구해야 할 것이다. 기존의 영토를 기준으로 한 국가관할권 개념만으로는 해결하기 어려운 것이다.

실질적으로는 국가 간 상호 조약 등에 의하여 관할권의 정의나 예외적으로 집행이 가능한 경우 등 디지털 증거와 네트워크 시대의 변화에 대응할 수 있는 방안을 마련하여야 할 것이나, 입법적 조치가 이루어지기 이전에도 미국의 사례와 같이 관할권 적용에 대한 유연적인 해석이 필요하다고 사료된다.

(3) 계정 접속을 통한 역외 압수수색의 관할권 침해 여부

51) 정교일, 앞의 논문, 145

해외 서버(또는 클라우드)에 계정 접속을 통하여 압수수색을 진행하는 경우 다른 국가의 관할권을 침해하는지 여부가 문제되는데, 이에 대하여 물리적으로 상대국가에 진입하여 집행하는 것이 아니라 원격으로 접속하여 집행하는 것으로, 상대국가의 주권침해의 정도를 가장 경미하게 하면서도 실질적인 목적을 달성하는 것이라는 견해가 있다.[52] 또한 수사기관이 타국에 소재하는 서버를 침탈하는 것이 아니라 피압수자인 계정 소유자의 접근권한을 이용하여 수사기관이 접근하는 것으로 해석한다면 사법관할권 침해의 논란을 피할 수 있고,[53] 피압수자의 접근권한을 일부 제한하는 강제처분으로 해석하여 위와 같은 압수수색을 허용할 수 있다는 견해도 있다.[54]

이에 반하여 전통적인 견해는 실제 수색의 대상이 해외 서버에 저장되어 있음에도 수색의 장소를 국내로 적시하는 것은 압수수색은 소유자, 소지자, 보관자, 체신관서 또는 그 밖의 관련 기관을 상대로 압수하도록 규정하는 형사소송법에 위배된 것으로서, 피압수자의 참여를 배제하게 되고 사법관할권의 범위를 넘어서는 것이라고 한다. 이를 긍정하게 되면 수색의 대상인 정보가 영장에 기재된 수색장소에 존재하지 아니함에도 압수수색을 허가하는 결과가 되므로 압수수색영장에서 수색장소 특정의 의미가 몰각된다[55]고 보는 것이다.

살피건대, 수색의 대상인 정보는 해외 서버에 소재하고 있고, 실제 수색을 진행하는 집행 장소는 국내이기에, 영장에서 수색 장소를 특정하여 실제 수색을 하면서 그 대상이 확장됨으로써 재산권 침해

52) 오병철, 앞의 논문, 111
53) 전현욱 외, 앞의 논문, 115
54) 이관희, 디지털 정보의 취급에 관한 형사절차 개선방안, 고려대학교 석사학위 논문, 2012, 103-104
55) 법무연수원, 검찰실무Ⅰ, 2013, 408

등 기본권이 침해될 우려를 방지하고자 하는 의미가 무색해질 수 있다는 우려도 이해된다. 실질적 집행이 가능한 국내와는 달리 해외의 경우 수색 대상이 존재하는 장소에서 집행이 불가능하고 국내 수사기관 등 컴퓨터가 집행 장소가 되기에, 피압수자가 참여를 통해 과잉압수에 따른 재산권 침해 여부를 지켜볼 수 없는 것도 사실이다.

그러나 계정 접속을 통한 역외 압수수색을 진행할 경우 뒤에서 살펴볼 것처럼 영장에 압수수색할 장소를 '수사기관 내 지정된 컴퓨터'로 기재하면서(또는 판례에서와 같이 한국 인터넷 진흥원 내 컴퓨터로 기재), 더하여 실제로 수색 대상이 되는 해외 서버 내 정보 중 피의자 계정 내의 정보를 수색한다는 취지, 즉 '압수수색 장소에 존재하는 컴퓨터로 해당 웹사이트(서버)에 접속하여 디지털 증거를 다운로드한 후 이를 출력 또는 복사하거나 화면을 촬영하는 방법으로 압수한다'는 것을 영장에 기재하게 되므로, 직접 수색 대상 서버가 존재하는 장소에서 집행하지 못하더라도 원격 접속을 통해 해당 계정 내 정보만을 압수수색한다는 것이 명확하기에 수색장소가 예상치 못한 곳으로 무리하게 확장될 염려는 거의 없다고 보인다.[56] 또한 물론 해외에 존재하는 서버에 저장된 정보를 얻기 위해 네트워크에 접근하는 것은 맞으나, 결국 이는 직접적으로 타국의 영토에

56) 현재 은행 등에 대해 계좌압수수색 영장을 팩스송신을 통해 집행하는 과정에서도, 사실 영장의 집행장소는 수사기관 내이며, 이를 전달받은 은행의 협조를 통해 대상 정보를 팩스로 다시 송부 받아 압수하게 되므로, 수사기관이 압수를 하는 것은 수사기관 내에서 이루어진다. 물론 압수수색 대상 정보를 수사기관이 아닌 피압수자가 선별하여 송부하게 된다는 점은 다르다.; 다만, 만약 계정 내 정보에서 링크 페이지 등을 통하여 다른 페이지로 넘어가 수색을 하는 것은 영장의 범위를 벗어나는 것이므로 허용될 수 없고, 새로운 영장을 발부받아야 한다고 판단된다.

들어가 압수수색을 진행하는 것이 아니고, 집행 장소가 국내이기에 집행관할권 침해의 소지는 크지 않다. 또한 엄밀히 분석한다면 접근된 네트워크를 통하여 서버에 저장된 전자 정보가 국내에 위치한 수사기관의 컴퓨터에 전송되고, 이미 전송되어 컴퓨터 내 RAM에 임시적으로 저장된 정보를 모니터 또는 프린터 등 출력기기에 의하여 출력되는 것이다. 즉, 압수의 행위 자체도 사실상 국내에서 발생한다.[57]

이에 더하여 압수수색의 과정에서 서버 관리자인 서비스 제공자는 아무런 역할을 하지 않는다. 오히려 서비스 제공자의 입장에서는 권한자의 접속이기에 압수수색을 한다는 사실도 알지 못한다. 협조를 요구하지도 아니하고, 실제로 서버 본체를 압수수색 당하지도 아니한다. 결국 실제적인 피압수자는 서버 이용자인 피의자라고 할 수 있으며, 피의자가 서버 내 저장된 정보의 소유자이며[58] 처분권한자로서 그의 권한을 (법원의 영장에 의하여 정당하게) 일부 이용하는 방법의 압수수색이기에[59] 서비스 제공자와는 압수수색 진행과 실질적으로 연관되지 아니한다.[60]

---

57) 물론 압수를 하기 위하여 해외 서버에 존재하는 정보에 접근하고 이를 수색하는 행위 자체가 일괄적으로 압수수색의 과정이므로 외국의 사법관할권이 아예 배제된다고 보기는 어려울 것이다.

58) 페이스북에서는 '모든 콘텐츠와 정보의 소유권은 회원님에게 있으며,'라고 약관에 기재하고 있다. https://www.facebook.com/legal/terms 참조

59) 이관희, 앞의 논문에서는 역외 압수수색이 피압수자의 접근권한을 일부 제한하는 강제처분이라고 주장하나, 실제로 피압수자의 계정 접속, 정보처분 등 권한에 아무런 제한이 발생하지 아니하므로(동시 접속도 사실상 가능하므로), 접근권한을 일부 제한하는 강제처분이 아닌 피압수자의 접근권한을 일부 이용하는, 즉 피압수자에게 수인의무를 부과하는 의미의 강제처분으로 볼 것이다.

60) 압수수색에서 피압수자의 협조를 요구하는 경우와 달리, 피압수자의 협조나 참여가 이루어지지 않기에 실제 정보를 압수당한 이용자(피의자)가

따라서 계정 접속을 통한 역외 압수수색의 방법은 타국의, 서비스 제공자가 속한 국가의 관할권을 반드시 침해하는 것이라고 보기 어렵다. 다만 국가 간 이익 충돌을 근본적으로 방지하기 위하여 사이버범죄협약에 가입하는 방법이나 새로운 조약을 체결하는 등 사법공조를 통해 역외 압수수색이 가능하도록 입법적인 조치를 취함이 바람직하다.

바. 영장주의 및 압수수색 규정 위배 여부 검토

(1) 영장 제시 문제(형사소송법 제118조)

형사소송법 제118조는 '압수수색영장은 처분을 받는 자에게 반드시 제시하여야 한다.'고 영장 제시 의무 규정을 두고 있다. 형사소송법이 영장 집행시 피압수자에게 영장을 제시하도록 규정한 것은 법관이 발부한 영장 없이 압수수색을 하는 것을 방지하여 영장주의 원칙을 절차적으로 보장하고, 영장에 기재된 물건, 장소, 신체에 대해서만 압수수색을 하도록 하여 개인의 사생활과 재산권의 침해를 최소화하는 한편, 준항고 등 피압수자의 불복신청의 기회를 실질적으로 보장하기 위한 것이다.[61]

수사실무에서는 피압수자가 해외에 소재하는 등 그 집행방식이 일반적인 경우와 달라 위와 같은 압수수색 절차 규정을 제대로 준수하지 못하는 경우가 많았다.[62] 다만 위에서 살펴본 서울고등법원 판결(2017노23, 2017노146)의 사례에서는, 피압수자인 해외 서버

피압수자인 서버 관리자에 대해 어떠한 재산권 침해 등에 대해 이의제기를 할 여지도 거의 없다고 보인다.

61) 대법원 2017. 9. 21. 선고 2015도12400 판결

62) 전현욱 외, 앞의 논문, 115-116

의 서비스 제공자가 아닌, 피고인에게 영장을 제시한 것으로 보인다.[63]

먼저 영장 제시와 관련하여 살펴보면, 일반적인 압수수색에서는 피압수자인 서비스 관리자에게 영장을 제시하고 서비스 관리자의 협조를 얻어 서버 내 정보를 취득하는 방식으로 압수를 진행하게 된다. 그러나 역외 압수수색의 경우 일반적인 압수수색과는 달리 피압수자인 서비스 관리자의 협조가 필요하지 아니하고,[64] 실제로 압수수색 사실을 서비스 관리자가 알지 못하며, 어떠한 피해를 입지도 아니하고 참여의 필요성도 없다. 또한 피압수자가 해외에 소재하므로 영장 원본을 직접 제시하는 것도 현실적으로 곤란하다. 그렇다고 하여 실질적으로는 피처분자가 피고인(또는 피의자)이므로 위 서울고등법원 판결 사례에서와 같이 피고인에게 압수수색영장을 제시하는 것은 서버 내 정보를 취득하는 압수수색에서의 피압수자가 서비스 관리자임에 비추어 반드시 타당하다고 볼 수만은 없으며, 실제로는 피고인이 현존하는 장소에서 압수수색을 바로 실행하지 아니하는 한 역외 압수수색의 긴급성에 비추어 계정 이용자인 피의자에게 영장 제시를 하기도 어렵다.

대법원 판례[65]에 비추어 보면, 형사소송법 제118조의 영장제시 규정은 영장제시가 현실적으로 가능한 상황을 전제로 한 규정으로 보아야 하고, 영장제시가 현실적으로 불가능한 경우에는 영장을 제

63) 위 사례에서만 한정되고, 실무상으로는 영장 제시가 쉽지는 않을 것으로 보인다.
64) 형사소송법 제106조 제2항은 '법원은 압수할 물건을 지정하여 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다'고 피의자 아닌 제3자에 대한 압수에 대해 규정하고 있는바, 문언적 해석에 따라 제3자에 대하여는 압수 시 제출(협조)을 명할 수 있도록 하고 있으나 계정 접속을 통한 역외 압수수색 시에는 이러한 협조가 요구되지 아니하여 차이가 있다.
65) 대법원 2015. 1. 22. 선고 2014도10978 전원합의체 판결

시하지 아니한 채 압수수색을 하더라도 위법하다고 볼 수 없다. 해외 서버에 대한 역외 압수수색은 압수수색 현장 자체가 국내에 있으므로 피압수자의 현장 부재는 이미 전제된 사실이다. 따라서 현행 압수수색 제도 내에서 해석한다면, 계정 접속을 통한 역외 압수수색은 피압수자가 현장에 없어 영장제시가 현실적으로 불가능한 상황이기에 영장을 제시하지 아니하더라도 허용된다고 보아야 한다.[66] 다만, 궁극적으로는 일반 압수수색과는 그 특성이 여러모로 다른 역외 압수수색에 관한 절차 규정을 새롭게 도입하여 그 특성에 맞게 규율하여야 한다고 본다.

(2) 압수수색 시 사전 통지, 당사자 및 책임자 참여 문제(형사소송법 제121조, 제122조, 제123조)

형사소송법 제121조는 '검사, 피고인 또는 변호인은 압수수색영장의 집행에 참여할 수 있다.'고 규정하고 있고, 동법 제122조는 '압수수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단, 전조에 규정한자가 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 예외로 한다.'고 규정하고 있으며, 동법 제123조 제1항은 '공무소, 군사용의 항공기 또는 선차 내에서 압수수색영장을 집행함에는 그 책임자에게 참여할 것을 통지하여야 한다.', 동조 제2항에서는 '타인의

66) 다만 최근 대법원 판례(대법원 2017. 9. 7. 선고 2015도10648 판결)에서는 압수수색영장 원본을 서비스 제공자에게 제시하지 않은 경우 위법하다고 판시한 사실이 있어, 영장 원본 제시 의무에 대한 논란이 있으나, 이는 국내 인터넷 서비스 제공자에 대한 판시이고, 해외 서비스 제공자에 대하여는 실질적으로 원본 제시가 불가능하므로 다른 해석이 필요할 것으로 보인다.

주거, 간수자 있는 가옥, 건조물, 항공기 또는 선차 내에서 압수수색 영장을 집행함에는 주거주, 간수자 또는 이에 준하는 자를 참여하게 하여야 한다.', 동조 제3항에서는 '전항의 자를 참여하게 하지 못할 때에는 인거인 또는 지방공공단체의 직원을 참여하게 하여야 한다.'고 규정하는 등 사전 통지의무, 당사자의 참여권, 책임자 등 참여의무 규정을 두고 있다.

압수수색 절차에서 사건관계인이나 피압수자가 참여하는 것은 영장 집행절차의 적정성과 압수물의 무결성을 확보하고, 무관정보를 임의로 복제 또는 출력하는지 감시, 통제하며, 피고인이 압수된 내용을 확인함으로써 방어권을 보장하기 위한 취지이다.[67] 앞의 서울고등법원 판결 사례에 비추어 보면, 수사기관은 당일 피고인에게 압수수색 사실을 통지하고 참여권을 통지한 것으로 보이고, 인거인인 한국인터넷진흥원의 직원의 참여 하에 압수수색을 진행하는 것으로 보인다. 이에 대하여 압수수색 직전에 참여의 통보가 이루어지므로 피고인 또는 피의자의 참여권을 실질적으로 보장하지 못한다는 의견이 있다.[68]

살피건대, 참여권을 보장하고 있는 취지가 참여권의 보장으로 실제 목적을 달성할 수 있는지, 즉 사건관계인이나 피압수자가 참여한다고 하여 절차의 적정성, 무결성을 확보할 수 있고, 무관정보의 탐색을 막을 수 있으며, 피고인의 방어권 보장에 도움이 되는지 여부에 관하여 논의가 있으나, 법률상 보장된 참여권이 위와 같은 목적을 달성할 수 있는지 여부, 즉 비효율적이라는 이유만으로 인정여부를 달리할 수 없다.[69] 다만 참여권은 제도의 보장만으로 목적의 달

67) 백형구 등, 주석 형사소송법 Ⅰ, 한국사법행정학회, 2009, 530-533; 이완규, 디지털 증거 압수 절차상 피압수자 참여 방식과 관련성 범위 밖의 별건 증거 압수 방법, 형사법의 신동향 통권 제48호, 2015, 106
68) 앞의 서울고등법원 2017노23 판결문 참조

성이 가능하므로, 실제 사건관계인이 참여하지 않더라도 위법하다고 볼 수 없고, 그것이 압수수색 직전에 이루어진다고 하더라도 위법하다고 보기 어렵다.

계정 접속을 통한 역외 압수수색을 진행할 경우, 해외 서버에 있는 정보의 훼손 우려가 있기에 긴급성이 있고, 따라서 압수수색 참여의 통보가 압수수색 직전에 이루어질 수밖에 없다. 조문에서도 '급속을 요하는 때' 에는 통지의 예외를 두고 있다. 이와 같은 경우 피고인의 방어권 보장 및 무관정보 탐색에 대한 통제는 압수목록의 교부로 그 목적 달성이 가능하다고 본다.[70]

그러나 궁극적으로는 게정 접속을 통한 역외 압수수색에서 참여권의 보장은 오히려 계정 이용자인 피고인이 당해 압수수색 절차에 참여하는 경우 계정 내 정보에 대한 변경, 삭제 우려를 불식시키므로, 적극적으로 참여를 권장하여야 한다고 본다. 다만 참여의 통지 이후 실제 압수수색 절차에 참여하기까지 데이터의 변경, 삭제가 이루어진다면 압수의 목적을 달성하기 어려우므로, 입법적으로는 협력의무의 하나로 증거 보존의무를 신설함이 타당하다. 그러한 환경에서는 수사기관이 사건관계인의 참여를 활성화하는 계기가 될 수 있다.

한편, 책임자의 참여 규정과 관련하여, 역외 압수수색은 실제로는 수사기관 내, 또는 앞서 본 서울고등법원 사례와 같이 한국인터넷진흥원 등에서 이루어지는 바, 형사소송법 제123조 제1항 또는 제2항에서 규정하는 '공무소, 그 외의 주거, 가옥, 건조물' 등에서 압수수색

---

69) 이정민, 디지털증거의 압수수색과 절차적 진실, 형사법연구 제28권 제3호, 2016, 157

70) 실질적으로 피고인이 압수수색 현장에 참여하더라도 무관정보의 탐색 행위에 대해 통제가 쉽게 이루어질 수 없고, 무관정보에 대해서는 법정에서 위법수집증거로서 배제를 주장하는 것으로 통제가 가능하다.

을 진행하는 것으로 보아 그 책임자를 참여하게 할 수 있다고 판단된다. 이러한 경우 압수수색절차의 공정성을 담보하는 등의 방안으로 동조 제3항에서 규정하는 '인거인 또는 지방공공단체의 직원'을 참여시키는 것이 상당하다고 사료된다.[71]

(3) 압수목록 교부 등(형사소송법 제129조)

형사소송법 제129조에 따르면 '압수한 경우에는 목록을 작성하여 소유자, 소지자, 보관자 기타 이에 준할 자에게 교부하여야 한다.'고 하여 압수목록의 교부의무를 규정하고 있다.

일각에서는 현실적으로 압수직후 현장에서 압수목록을 교부하는 것이 불가능하고, 다만 추후 계정 이용자인 정보주체에게 통신비밀보호법의 절차에 따라 통지하는 것은 가능하다는 의견을 제시하고 있다.[72] 압수목록의 교부는 피압수자에게 하여야 하나, 피압수자인 서버 제공자가 해외에 있고, 압수수색 사실도 알지 못하기 때문이다.

형사소송법 제129조에서 압수목록을 교부하도록 한 것은, 압수물의 존부·형상변경 등을 둘러싸고 벌어질 수 있는 여러 논란을 사전에 차단하고, 피압수자들의 압수물에 대한 환부·가환부청구권 등 각종 권리행사를 보장하려는데 있다.[73] 즉, 압수물의 내역을 알 수 있도록 하여 형상변경에 대한 다툼을 막고, 피압수자들에게 권리가 있는 경우 이를 보장하기 위한 것으로 보인다.

살피건대, 계정 접속을 통한 역외 압수수색의 경우, 서버의 원본

---

71) 정대용 외, 앞의 논문, 163
72) 전현욱 외, 앞의 논문, 115; 정대용 외, 앞의 논문, 163; 정소연, 앞의 논문, 67
73) 서울고등법원 2013. 8. 30. 선고 2012노803 판결 참조

을 압수하거나 그에 대한 이미징 작업을 하는 것이 아니라 저장된 정보의 내용만을 복제하는 방법으로 압수가 진행되기 때문에, 피압수자인 서버 제공자에게 환부청구권 등은 인정될 여지가 없는 것으로 보인다. 또한 조문을 살펴보면, 압수목록의 교부는 '소유자'에게 하는 것이 허용되고, 압수의 대상인 계정 내 정보의 소유자는 계정 이용자인 피고인으로 해석되므로,[74] 피고인에게 압수목록을 교부하는 경우 형상변경에 따른 다툼을 막을 수 있고, 그에 따라 피압수자에게 압수목록을 교부하는 것보다 피고인의 방어권 보장에도 오히려 도움이 된다고 생각된다. 계정 접속을 통한 역외 압수수색은 원본의 압수가 불가능하여, 오히려 계정 내 정보에 대한 선별 압수가 가능하고, 현장에서 범죄사실과 관련성 있는 증거를 바로 출력한 출력물을 압수할 수 있다. 그렇다면, 출력하여 압수한 압수물의 목록을 피고인에게 교부하는 것이 가능하다.[75]

따라서 압수목록의 교부는 정보의 소유자인 피고인에게 하는 것으로 가능하고, 다만 피압수자의 재산권 등 보호차원에서 통신비밀보호법의 절차에 따라 정보 이용자의 권한에 의해 접속하여 압수수색을 하였다는 통지를 하는 것은 가능하다고 보인다.

(4) 영장주의와 압수수색 비례의 원칙

강제수사는 국민의 기본권 보호와 상충관계에 있다. 증거 수집을 통한 실체적 진실의 규명은 그 절차에 있어서 국민의 사생활의 비

---

74) 앞의 각주50 참조

75) 압수목록은 압수경위 및 압수물의 내역을 알 수 있도록 정확하게 기재되어야 하고, 압수 즉시 또는 압수 후 신속하게 교부되어야 한다. 부산고등법원 2013. 6. 5. 선고 2012노667 판결; 피고인이 압수수색에 참여하지 않은 경우라도, 일반 압수수색의 경우와 같이 피고인에게 압수목록의 교부는 가능하다.

밀과 자유, 통신의 비밀과 자유, 개인정보자기결정권 등과 충돌할 수밖에 없다. 국가는 개인의 자유를 침해하지 아니할 의무와 동시에 개인의 기본권을 보호할 의무도 진다.

디지털 증거에 대한 압수수색에서도 일반적·탐색적 압수수색은 금지되나 수사의 현실과 디지털 증거의 특성상 정보저장매체에 저장되어 있는 해당 파일을 확인하기 위해서는 어쩔 수 없이 광범위한 압수수색을 필요로 하기도 한다.[76] 전자정보의 대량성 때문에 혐의사실과 '관련된 정보' 뿐만 아니라 혐의사실과 '관련이 없는 정보'가 혼재하는 경우, 압수수색과정에서 영장이 발부된 범죄사실과 관련한 증거뿐만 아니라 관련이 없는 증거까지 대량으로 수집될 가능성이 농후하다.[77] 이러한 전자정보의 압수수색으로 인하여 개인은 사생활의 비밀과 자유, 개인정보자기결정권, 통신의 자유 등이, 기업은 영업비밀, 재산권 등이 침해될 우려가 크다.[78] 따라서 개인의 자유와 공동체의 이익 사이의 긴장관계를 어떻게 조화시킬 것인지, 양 법익 사이의 균형점을 찾아내는 제도와 절차를 마련하는 것이 오늘날 헌법의 과제라 하겠다.[79]

특히 계정 접속을 통한 역외 압수수색은 법률상 규정된 압수수색의 절차와는 다소 다른 절차로 진행되고, 서버 이용자의 계정에 직접 접속함으로서 대량의 정보가 과잉 압수될 가능성이 있으며, 검증기관이 신설되어 압수수색 절차에 참여하는 경우 서버 이용자의 개

---

76) United States v. Williams, 592 F. 3d 511, 521(4th Cir. 2010)
77) 김병수, 전자정보에 관한 압수수색의 문제점과 개선방안, 비교형사법연구 제18권 제3호, 2016, 33
78) 대법원, 압수·수색 절차의 개선방안에 관한 연구, 사법정책연구원 연구총서, 2016, 39-40
79) 한수웅, 헌법학, 법문사, 449; 이숙연, 전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여 - 대법원 2011모1190 결정에 대한 평석을 중심으로 한 연구, 헌법학연구 제18권 제1호, 2012, 10

인정보가 노출될 가능성이 더 커지기에, 위와 같은 기본권 침해의 소지가 있다고 보인다.

해외 서버에 원격으로 계정 접속하여 압수수색하는 역외 압수수색은 이미 살펴본 것처럼 일반적인 유체물의 압수수색과 그 절차 등 기준을 동일하게 판단하기 어렵다. 그렇지만 역외 압수수색이라는 방법이 기존의 까다로운 형사사법공조절차를 대체한 압수수색 방법이고 그 긴급성을 인정하여 허용하여야 하는 것이기에 유연적인 해석만으로 압수수색을 인정하게 된다면, 실질적으로 피고인의 개인정보보호와 통신의 비밀, 사생활의 비밀 등을 침해하게 될 소지가 있다. 디지털 증거의 압수수색은 저장정보의 대량성 때문에 많은 개인정보 및 사건과 관련 없는 증거를 포함하고 있기에[80] 과잉 압수수색의 논란에서 벗어나기 어렵기 때문이다.

따라서 역외 압수수색이 완벽하게 보장되기 위해서는 비례의 원칙에 따라 다음과 같은 엄격한 절차가 준수되어야 한다고 본다. 첫째로, 역외 압수수색은 오로지 '영장'에 의하여 이루어져야 하고, 압수수색 영장을 발부하기 위하여 법원은 몇 가지 조건을 붙이거나, 엄격한 비례의 원칙에 따라 범죄의 형태나 경중, 압수물의 증거가치 및 중요성, 범죄와의 관련성, 증거인멸의 우려, 긴급성, 피압수자가 받게 될 불이익 등 제반사정을 고려하여 영장 심사 시 세밀히 검토하여야 한다.[81] 이러한 엄격한 영장 심사로 인해 수사기관의 강제수사로 인한 피고인의 기본권 침해를 제한할 수 있다. 둘째로 역외 압수수색에 적용하여야 하는 새로운 절차 규정을 도입하여야 한다. 현재의 압수수색 규정은 역외 압수수색에는 그대로 적용하기에는 무리가 있으며, 별도의 규정이 필요하다고 사료된다. 대표적으로는

80) 이정민, 앞의 논문, 151
81) 이정민, 앞의 논문, 160

압수수색 후 계정 이용자인 피고인에게 계정 정보를 변경하도록(즉, 암호를 변경하도록) 통지해주도록 규정함이 상당하다. 수사기관이 계정 정보를 알고 있고 피고인이 암호를 변경하지 않는 경우 계정에 다시 접속할 우려가 있고, 임의로 수사기관이 암호를 변경할 수도 없기 때문이다. 또한 당사자가 압수수색에 참여하지 못하는 경우 수사기관의 권한 남용과 통제를 위해 객관적인 제3자가 참여할 수 있는 절차를 모색하여야 하는바, 이는 뒤에서 살펴 볼 무결성 입증 방안으로 제시되는 제3검증기관의 도입으로 그 목적을 달성할 수 있다.

사. 증거의 원본성 및 무결성

(1) 역외 압수수색 증거 무결성 입증의 미비

수사기관은 압수수색 단계에서부터 증거의 원본과 사본의 해쉬값을 산출하여 디지털증거에 대한 무결성을 증명하는 방법을 사용하고 있으나 그래도 여전히 디지털증거의 무결성에 대한 논란은 해결되지 않고 있다.[82] 우리 형사소송법상 디지털 증거의 압수수색은 '정보저장매체'를 압수하거나 '정보의 범위를 정하여 출력하거나 복제한' 서류를 압수하는 방법을 채택하고 있는데,[83] 결국 압수의 대상 자체는 정보의 내용임에도 이는 무체물이기에 증거로 사용하려면 유체물로의 변환이 있어야 한다는 의미로 해석된다.

---

82) 성혜정 외, 소송절차에서 독립된 디지털증거 검증기관의 필요성에 대한 연구, 한국정보기술학회 하계학술대회 논문집, 2014, 224

83) 원칙은 '정보의 범위를 정하여 출력하거나 복제하여 제출'해야 하고, 예외적으로 이것이 불가능하거나 현저히 곤란한 경우 '정보저장매체등'을 압수할 수 있다(원칙적 선별압수, 예외적 매체압수).

그렇지만 정보가 저장된 원본, 즉 원본 저장매체를 압수하지 아니하고, 원칙적인 내용과 같이 기억된 정보의 범위를 정하여 출력하거나 복제하는 경우에는 저장된 원본 정보가 변경될 가능성이 있으므로 출력물과의 동일성을 인정받아야 한다. 결국 디지털 증거의 특성으로 인해 증거의 원본성과 무결성이 문제되는 것이다. 이로 인해 앞서 말했듯 수사기관은 증거의 원본과 사본의 해쉬값을 비교하는 방법으로 그 원본성과 무결성을 입증해 오고 있다.

그런데, 계정 접속을 통해 역외 압수수색을 하는 경우 원본 저장매체를 압수할 수 없고, 기억된 정보의 범위를 정하여 출력하거나 복제할 수밖에 없다. 원본 서버에 저장된 정보를 전체적으로 이미징하여 해쉬값을 산출하기도 어렵다. 따라서 출력된 정보가 실제 해외 서버에 저장된 그 정보가 맞는지 여부를 판단할 기준이 없으며, 새롭게 그 무결성을 입증할 방법이 강구될 필요가 있다.

(2) 새로운 입증방법의 필요성

결국 기존의 해쉬값 산출 등의 방법만으로는 서울고등법원 판례(2017노23)에서 적시한 바와 같이 수집된 증거의 원본성과 무결성을 실질적으로 담보할 수 없게 되는 문제가 발생될 수 있다.

따라서 원본에 대한 압수나 이미징, 해쉬값 산출이 가능하지 않은 상황에서는 원본에 저장된 정보와 출력하여 법정에 제출한 정보가 동일하다는 것을 입증할 다른 기술적 수단이 필요하다. 증거 수집 과정에 대한 기록과 계정 접속을 통해 접근한 서버의 진위성 확인 등 적절한 인증이 필요하다고 사료되고, 뒤에서 살펴볼 것처럼 그러한 무결성의 입증은 종전과는 달리 중립적인 제3의 기관에서 담당하여야 함이 바람직하다고 사료된다.

Ⅲ. 결론

네트워킹 환경의 변화는 법의 세계에도 변화를 주고 있다. 수사기관은 실체적 진실의 발견을 위하여 여러 곳에 분산된 증거를 수집하고자 활동하는데, 디지털 시대 이전에는 주로 피고인이 증거를 보관하고 있는 장소를 찾고자 하였다면, 디지털 시대에는 피고인이 어느 저장매체에 정보를 저장하였는지를 찾고자 한다. 바야흐로 네트워크를 통한 글로벌 시대에서는 그 저장매체가 국내가 아닌 해외에 있는 경우도 다반사이다. 그러나 수사 인력과 활동 범위에 한계가 있기 때문에 증거를 수집하기 위해 해외에 직접 나가거나 형사사법공조절차를 통해 원하는 증거를 취득하기가 어려운 상황이다.

특히 해외 서버에 저장된 정보에 대하여 국경을 초월하여 언제, 어디서든 작성과 변경, 삭제가 가능하다는 점에 비추어 적절한 시점에 증거를 수집하지 아니하면 증거가 훼손될 우려가 크므로, 수사기관이 적법하게 피의자의 계정 정보를 알게 된 경우 피의자의 계정 접속 권한을 이용하여 해외 서버에 접근하고 계정 내 정보를 수색, 필요한 증거를 압수할 수 있는 수사 방법이 필요하다. 이에 대하여는 여러 학설의 대립이 있으며, 판례에서조차 그 의견의 대립이 나타나고 있는바, 시대 변화의 흐름에 비추어 기존의 형식을 탈피한 새로운 압수수색 방법을 인정해야 한다고 본다. 다만, 새로운 압수수색 방법에 대하여는 입법적으로 규율된 것이 없기에, 그러한 제도가 완벽하게 정착하기 위해서는 압수수색 절차 규정 등 입법적 해결이 필요하고, 역외 압수수색이 합목적적인 수사를 통해 실체적 진실 발견이라는 가치와 수사로 인해 피의자의 기본권을 침해하지 않도록 하는 절차적 적정성이라는 가치가 조화될 수 있도록 조금 강화된 영장 심사가 필요하다고 사료된다.

그런데, 이러한 방법으로 취득된 증거는 원본 증거 또는 원본 증거의 해쉬값을 재판정에 제출할 수 없다는 특이성으로 인하여 기존의 해쉬값 비교 방법만으로는 그 무결성 입증에 한계가 생긴다. 따라서 무결성을 입증하기 위해 원본, 즉 서버가 진정한 서버라는 점과 출력물이 원본 서버로부터 다운로드 받아 출력한 증거이고, 그 과정에서 조작이나 변경이 없었다는 것을 검증해 줄 중립적인 기관이 필요하게 되었다.

제 3 장 역외 압수수색의 무결성 입증을 위한 제안

제 1 절 서 설

계정 접속을 통한 역외 압수수색은 관할권, 영장주의, 압수수색 규정 위배 여부가 문제될 수 있으나, 앞서 살펴본 바와 같이 디지털 증거의 특성과 인터넷 시대 환경의 변화, 관할권 개념의 변동 추세에 비추어 허용성을 인정하여야 한다고 본다.

그런데, 수사기관이 계정 접속을 통해 해외 서버에 접근한 후 정보를 출력의 방법으로 압수하는 경우, 그와 같이 출력된 증거의 원본성과 무결성이 담보되려면 접근한 해외 서버가 진실한 서버라야 하고, 그 서버에 저장된 정보와 출력된 정보가 조작 없이 동일하여

야 할 것이다.

현재의 수사실무는 그 무결성을 담보하기 위하여 계정 접속을 통해 해외 서버에 접근한 후 현출된 화면을 캡쳐, 저장하거나 첨부된 파일이 있는 경우 파일을 저장한 다음, 디지털 포렌식 프로그램(Encase7 등)을 이용하여 각 파일에 대한 해쉬값을 생성한 후 전체 파일을 USB 등에 저장하는 방법을 사용하고 있는 것으로 보인다.[84] 즉, 해외 서버에 저장된 정보를 화면에 출력하여 이를 캡쳐한 후 그 이미지 파일에 대한 해쉬값을 생성하는 것이다.

그런데 위와 같이 화면에 출력된 정보를 캡쳐한 이미지 파일은 해외 서버에 저장된 정보와 동일한 것이 맞는지, 정보를 출력하는 과정에서 조작은 없었는지에 대한 무결성을 보장하기는 어려운 방법이라고 생각된다. 해쉬값을 생성하는 것도 해외 서버에 저장된 정보 원본에 대한 해쉬값을 생성할 수 없고, 캡쳐한 이미지 파일에 대하여 해쉬값을 생성하는 것이기에, 정보를 캡쳐하여 파일로 저장한 후 법정에 현출되기까지의 무결성은 담보할 수 있으나 최초 저장된 정보 원본과 캡쳐본의 무결성까지는 담보하기 어려운 것이다.

또한 이에 더하여 수사기관이 자신이 수집한 증거에 대한 무결성을 자체적으로 입증한다는 것이 모순이라는 견해도 있다. 디지털증거가 삭제 및 변경이 용이하다는 특징에 의해 수사기관의 분석에 대해 투명하지 못하다는 지적을 받을 수 있고, 따라서 수사기관 이외의 제3의 기관이 필요하다는 것이다.[85]

---

84) 서울고등법원 2017노23 판결문 참조

85) 이규안, 디지털 증거 인증기관의 필요성에 대한 연구, 한국전자통신학회 2011 추계종합학술대회지 제5권 제2호, 한국전자통신학회, 2011, 85-88; 김준한 외, 신뢰 가능한 디지털 증거의 무결성 보장 절차에 대한 연구, 보안공학연구논문지 제10권 제5호, 2013, 530-531; 서울신문 2012. 12. 19.자 기사 <디지털 증거 조작 쉬워... 국과수 같은 '인증기관' 필요>

따라서 수사기관이 수사기관의 컴퓨터를 이용하여 계정 접속을 통해 해외 서버에 접근하는 방식으로 저장된 정보를 취득하고자 하는 경우, 수사기관이 접속한 해외 서버가 진실한 서버가 맞는지, 그 사용자의 계정 내에 정보가 저장되어 있었던 것이 맞는지, 서버에 저장되어 있던 정보를 그대로 화면에 출력하여 캡쳐한 것이 맞는지, 그 과정에서 수사기관의 조작이나 변경이 없었는지를 검증할 수 있는 제도가 필요하다고 할 것이다. 그 방법의 하나로 본 논문에서는 수사기관과 별개의 제3검증기관을 신설하여, 그 검증기관이 수사기관의 위와 같은 압수수색 진행 과정을 원격으로 검증하고, 압수수색 전 과정을 녹화, 저장하여 무결성을 보장하는 방법을 제안하고자 한다.

제 2 절 무결성 입증을 위한 제3검증기관 도입 제안

Ⅰ. 제3검증기관 도입의 의의

다양한 디지털 기기의 사용 환경을 이해하기 위해서는 일반적으로 시스템과 네트워크 환경, 파일들 간의 복잡한 상호관계 및 작용 등에 대한 이해가 선행되어야 하며, 이는 컴퓨터와 하드디스크 뿐 아니라 정보통신분야의 여러 전문 기술에 대한 이해가 선행되어야 한다.[86] 디지털 증거가 점차 증거로서의 비중이 높아지면서, 수사기관과 법원 모두 디지털 증거에 대한 이해를 요구하고 있지만, 전문적인 분야에 대한 깊은 지식까지 모두 요구할 수는 없는 것이 현실

86) 성혜정 외, 앞의 논문, 225

이다.

현재까지 법원에서는 디지털 증거에 대하여 대부분 수사기관의 디지털 전문 포렌식 수사관의 역량과 분석 장비의 신뢰성에 그 증거능력 인정여부의 척도로 가장 중요시하고 있는 실정이다. 포렌식 수사관의 증거 분석내용과 의견에 거의 전적으로 의존하고 있다고 보아도 과언이 아니다.[87] 그러나 수사기관이 '입증 책임'을 지고 있는 기관이라고 하더라도 그러한 입증 방법이 과연 신뢰성, 정확성 등을 충족하고 있는 것인지에 대해서는 법원에서 판단하여야 하는 바, 법원에서 디지털 증거에 대한 전문적 지식을 모두 갖추고 있기는 현실적으로 어려움이 있기에, 그러한 판단의 근거가 될 수 있도록 중립적이고 전문적인 검증기관이 필요하다.

이에 수사기관과 별도로 공정성을 담보할만한 제3검증기관을 도입하여, 수사기관의 압수수색 절차의 하자를 방지하면서 동시에 권한의 남용을 통제하고, 원본과 출력물의 무결성을 담보하며, 객관적인 신뢰성과 전문성을 확보하여 수사의 결과물을 검증할 수 있도록 함이 바람직하다.

Ⅱ. 제3검증기관 도입의 정당성

1. 제3검증기관의 역할

소위 '일심회' 사건으로 불리는 대법원 판결의 항소심 당시 피고측은 검찰에서 진행한 포렌식 수사로써 독립적으로 디지털 원본 매

87) 오길영, 디지털 검증의 현재와 그 부당성: 소위 '왕재산' 사건을 대상으로, 민주법학 제48호, 2012, 159-195

체의 무결성을 절차적, 기술적으로 보장하고 있다고 볼 수 없어 그 신뢰성을 배척해야 한다고 주장한 사실이 있다.[88] 물론 위 사건에서, 그리고 그 후로도 현재까지 수사기관 내 포렌식 전문가의 분석 내용의 신뢰성은 아직 인정되고 있으나, 더 이상 수사기관 포렌식 전문가의 분석만으로 그 신뢰성을 인정하기는 어려울 것으로 보이고, 수사기관이 아닌 독립적 기관에 대한 주장의 목소리가 커질 것으로 보인다. 현재까지는 디지털 증거에 관하여 수사기관 포렌식 전문가의 분석과 입증으로 충분하다 하였으나, 수사관은 포렌식 전문가일 뿐만 아니라 수사기관의 직원이라는 지위에 비추어 증거 수집 과정과 수집된 내용, 그리고 그에 관한 분석에 있어서 얼마든지 편향된 시각으로 바라볼 수 있기 때문에, 포렌식 전문가로서의 신뢰성을 보장할 수 없다.

따라서 객관적인 신뢰성을 확보하고, 수사기관의 권한남용을 통제하며, 피고인의 방어권 보장을 위해서도 제3자적인 검증기관이 필요하다. 제3검증기관은 현재 과학수사와 관련한 전문기관인 국립과학수사연구원과 같이 객관성, 중립성, 전문성을 띤 신뢰도 있는 기관이 되어야 한다.

제3검증기관이 도입되는 경우 제3검증기관에서는 디지털증거가 압수수색 절차를 통해 수집된 직후부터 위·변조 되지 않았다는 무결성을 보증하는 제3자로서의 감시자 역할, 공판정에서의 해쉬 값 검증절차를 대신하여 무결성을 확인하는 역할, 디지털증거에 대한 수사기관이나 피고 측의 분석 또는 감정의 결과를 검증하여 객관적 증거로서의 사실여부를 확인하고 서면의 형태로 법원에 결과를 송

88) 서울중앙지방법원 2007. 4. 16. 선고 2006고합1365 판결, 서울고등법원 2007. 8. 16. 선고 2007노929 판결, 대법원 2007. 12. 13. 선고 2007도7257 판결 참조

부하는 역할, 검증이 완료된 후 소송의 상대방에 실질 증거로 활용될 증거분석 내용에 대한 검증결과가 기록된 검증조서를 열람·등사할 수 있도록 제공하는 전자증거개시 중재자로서의 역할 등을 담당하도록 함이 상당하다.[89]

2. 검증기관 도입과 국민의 기본권 보장

계정 접속을 통한 역외 압수수색은 수사의 필요성에 대한 강한 요구에서 비롯된 제도임은 분명하다. 앞서 살펴본 바와 같이 압수수색의 비례의 원칙에 충실하게 운영된다면 역외 압수수색이 비단 위헌적인 공권력의 행사라고 볼 수만은 없을 것이다. 하지만 계정 접속을 통한 역외 압수수색은 피압수자인 서버 제공자의 협조를 받아 관련된 자료만을 받아볼 수 있는 것은 아니어서 서버 이용자인 피의자의 무관정보까지 탐색이 가능하다는 점에서 과잉 압수수색의 논란이 있을 수 있고, 이는 사생활의 비밀과 자유, 통신의 비밀과 자유 등 헌법상의 기본권 침해로 이어질 수 있다. 물론 위법한 수사로 취득한 증거에 대하여 법정에서 위법증거배제법칙에 의하여 증거로 사용하지 못하게 하는 가장 강력한 통제방법이 있으나, 이는 사후적 통제에 불과하여 수사단계에서 권한 남용으로 인한 기본권 침해를 방지할 수단이 필요한 것도 사실이다.

이러한 의미에서 제3검증기관의 도입은 수사기관의 권한 남용으로부터 국민의 기본권을 보장하기 위함이라는 목적의 정당성이 인정된다. 제3검증기관은 수사기관, 사법기관과는 독립된 기관으로서 수사기관의 압수수색 절차에 참여함으로써 적절한 통제가 이루어질 수 있도록 하는 제도적 보장 방법이 된다. 물론 당사자의 참여권이 과잉 압수수색에 대한 더 수월한 통제 방안이 될 수 있으나, 압수수

89) 성혜정 외, 앞의 논문, 226

색 과정의 전문성과 변조가 용이하다는 증거의 특성으로 인해 사실상 당사자의 절차 참여가 어렵거나 참여의 실질적 의미가 무색해질 수 있는 역외 압수수색에서 제3자적 입장에 있는 전문가인 검증기관이 참여하고, 이러한 검증 내용을 당사자가 확인할 수 있다면 압수수색으로 인한 기본권 침해 방지뿐만 아니라 사건관계인의 실질적 방어권 보장이 이루어질 수 있을 것이다.

3. 적법절차 준수, 무결성 확보를 위한 중립적 수단

계정 접속을 통한 역외 압수수색에서 수사기관이 스스로 압수수색의 전 과정을 녹화하는 방법으로 무결성을 입증할 수도 있다. 검증기관이라는 새로운 기관의 도입으로 인해 오히려 개인정보의 유출 문제가 새로 발생할 가능성도 제기될 수 있지 않을까.

그러나 앞서 언급하였듯 수사기관이 입증책임을 지고 있다고 하더라도 증거에 대한 최종적인 판단은 법원에서 하므로, 수사기관이 스스로 무결성을 입증하기 위해 압수수색 과정을 녹화하였다고 하더라도 이는 입증방법에 불과하고, 법원에서 이와 같은 방법의 무결성 입증이 정당한지 검증하는 과정이 필요하다. 하지만 법관은 디지털 포렌식에 있어서 전문가적인 지식을 모두 갖추고 있지는 못하므로, 실제로는 전문가의 검증이 선행되어야 하나, 현재까지는 수사기관 내 포렌식 전문가의 증언이나 보고서만을 신뢰하고 있는 상황이다.

그런데 디지털 증거의 변조용이성 등 특성으로 인해 사건 당사자의 경우 수사기관의 분석에 대해 투명하지 못하다는 문제를 제기할 수 있다.[90] 따라서 수사기관 내 포렌식 전문가보다는 좀 더 객관적

90) 김준한 외, 앞의 논문, 530

이고 중립적인 입장에서 무결성 입증을 담보해줄 기관이 필요하다. 수사기관의 입장에서도 수사과정에서 적법절차의 원칙이 준수되었고, 수집한 디지털 증거의 무결성이 보존되어 증거능력이 있음을 법정에서 입증함에 있어서 검증기관이 수사절차에 참여함으로써 보다 수월해질 수 있다.

당사자의 입장에서는 수사기관 이외의 검증기관이 수사 절차에 참여함으로써 개인정보의 유출 가능성이 증대되었다고 볼 수도 있으나, 반면 수사기관의 권한 남용에 대한 통제가 가능하고 공정한 전문가의 검증을 받을 수 있으며, 적법절차나 형식적 요건 미비로 인한 법정에서의 무익한 다툼을 방지할 수 있어 절차적 정당성을 통해 헌법과 형사소송법이 추구하는 신속한 재판의 원칙[91]과 적법절차의 원칙을 실현할 수 있다는 측면에서 유리한 제도임은 분명하다. 특히 기존에는 당사자가 디지털 증거의 검증을 요청하더라도 실질적으로 수사기관이 자체적인 검증을 거치는 것에 불과하였기 때문에, 제3검증기관의 도입으로 새로운 시각에서의 증거에 대한 분석 및 검증이 가능할 것으로 보인다. 다만, 위와 같은 개인정보 유출 우려에 대해서는 아래에서 살펴볼 바와 같이 검증기관의 윤리성과 비밀준수의무, 접근 차단에 대한 기술적 조치 등 제도적으로 예방책을 마련해야 할 것이다.

4. 검증기관의 신뢰성 보장 문제 - 검증의 정당성

디지털 범죄에 대한 수사역량은 디지털 증거에 대한 효율적인 압수수색과 분석절차를 얼마나 정확하고 신속하고 타당성 있게 진행하여 신뢰성을 유지하고 확보하느냐에 있다. 전문 포렌식 수사관이

91) 성혜정 외, 앞의 논문, 226

라고 하더라도 수집·분석하는 과정이나 이를 분석하는 도구가 100% 정확하다고 단정할 수는 없다.

포렌식 수사관이 전문성을 띄고 있다고 하더라도 제3자가 아니라 수사기관으로서 증거를 수집, 분석하고 있으므로 이에 대한 공신력에는 한계가 있을 수 있다. 과학적 증거에 관하여 수사기관인 대검찰청 내 과학수사 전문가들이 증거 분석의 전문성을 가지고 있으나, 수사기관과 별도의 기관으로서 국립과학수사연구원이 전문적인 인력을 양성하여 과학수사의 신뢰성을 보장하고 있는 것처럼, 디지털 증거에 관하여도 높은 전문성을 가진 포렌식 전문가가 제3검증기관에서 증거분석에 대한 공신력을 높여준다면 결국에는 디지털 증거의 무결성을 보장할 수 있을 것이다.

제3검증기관의 도입은 국립과학수사연구원의 사례가 가장 좋은 본보기가 될 것이다.[92] 그 조직은 사법기관과 민간연구소, 학계 등과 의견 조율이 가능하고, 운영면에서 경제적인 이해득실에 얽매이지 않도록 하며, 해당 이해관계자와의 접촉을 철저히 봉쇄하여 중립성과 신뢰성을 갖춘 정부기관으로 하도록 하고,[93] 내부 구성원은 공인된 포렌식 전문가들로 구성하여야 할 것이다. 이에 따라 그러한 전문적인 인력을 양성하기 위하여 사설 자격과는 다른 국가공인 자격제도를 도입하는 등 국민이 신뢰할 인증제도와 기준을 갖추는 것이 필요하다.[94] 또한 포렌식에 사용하는 도구와 기술적인 방법 모두 그 정확성, 신뢰성, 투명성이 공인된 것으로 하여야 한다. 바로

92) 김준한 외, 앞의 논문, 536
93) 곽병선, 디지털 포렌식 수사의 문제점과 개선방안, 법학연구 제42권, 2011, 180; 조상수 외, 디지털 증거의 무결성 보장 절차에 대한 개선, 정보과학회논문지: 정보통신 제39권 제2호, 2012, 189
94) 윤신자 외, 전자정보의 압수·수색 절차 개선방안 연구, 경찰학연구 제13권 제4호 통권 제36호, 2013, 243-244

이 기관에서 디지털 증거의 진정성을 인정받도록 디지털 포렌식 절차의 표준을 마련하도록 하여 일관성 있게 검증하도록 하여야 한다.[95]

제 3 절 계정 접속을 통한 역외 압수수색 시 무결성 입증의 구체적 방안

Ⅰ. 제3검증기관 검증의 내용

본 연구에서 제안하는 계정 접속을 통한 역외 압수수색 절차에서 무결성 입증에 대한 방안은 역외 압수수색을 진행하는 수사기관의 컴퓨터 네트워크와 검증기관의 네트워크 망을 연결하여, 수사기관의 해외 서버 접근, 그에 따른 정보 수집 절차 전반을 검증기관에서 검증하고 인증할 수 있도록 하는 것이다. 검증기관의 전문가가 역외 압수수색 과정에 직접 참여하는 방법도 생각해 볼 수 있으나, 검증기관의 규모적 한계로 시간적, 공간적인 여유가 부족하여 쉽지 않을 수 있고,[96] 기관 간 상호 망 연동이 된다면 전문가가 굳이 현장에 참여하지 않더라도 검증기관에서 수사기관의 압수수색 과정을 감시하고 분석할 수 있다.

수사기관의 계정 접속을 통한 역외 압수수색은 다음과 같은 절차에 따라 이루어진다. 첫째, 인터넷이 연결된 네트워크상에 접근하고자 하는 서버의 주소를 입력한다. 둘째, 서버 내 계정에 접속하기

95) 곽병선, 앞의 논문, 185-187
96) 김준한 외, 앞의 논문, 531-532

위하여 이용자의 계정 정보를 입력한다. 셋째, 계정 내에 저장된 정보를 열람하여 혐의와 관련성이 있는 정보를 탐색한다. 넷째, 정보 탐색 후 관련성 있는 정보를 화면에 출력하여 캡쳐하거나, 이를 문서의 형태로 다운로드 받아 다른 저장매체에 저장하거나 인쇄물로 출력한다. 다섯째, 다운로드 받아 저장된 문서와 다른 저장매체 저장한 자료들에 대하여 디지털 포렌식 프로그램을 이용하여 해쉬값을 생성한다. 이 과정에서 생성되는 해쉬값은 서버 내 저장된 정보의 원본이 아닌 이를 수사기관의 컴퓨터에 다운로드 받아 저장한 정보에 대한 해쉬값이기 때문에, 서버 내 저장된 정보의 원본이 출력물과 동일하다는 무결성 보장 방법이 필요하다. 따라서 검증기관을 통하여 서버 내 저장된 정보의 원본이 변경, 조작되지 아니하고 그대로 출력되었음을 보장할 수 있도록 검증하는 역할을 한다.

이렇게 제3검증기관이 역외 압수수색 절차에 대해 검증하기 위해서는, 첫째로 수사기관이 위와 같은 방법으로 역외 압수수색함을 기재하여 영장을 발부받고, 둘째로 수사기관이 역외 압수수색을 진행하기 전 수사기관의 네트워크 망과 검증기관의 네트워크 망을 연결할 수 있도록 망 연동이 가능한 채널에 접속하고, 영장의 내용 등 관련 정보를 입력해야 한다. 셋째로 검증기관에서 망 연동이 승인되면 제3검증기관은 절차에 따라 압수수색을 하고, 압수할 정보를 출력하기 전 검증기관의 인증 시스템에 따라 인증 표시를 하며, 검증기관이 녹화한 내용을 암호화한 후 그 암호키 조각을 받아 이를 다시 해쉬함수 등으로 암호화하여 보관해야 한다. 마지막으로 압수수색이 종료되면 수사기관에서는 압수수색이 종료되었음을 검증기관에 알리고 망 연동을 해제함이 필요하다.

Ⅱ. 검증의 절차

1. 제3검증기관과 수사기관의 망 연동

역외 압수수색을 위해서는 수사기관의 컴퓨터 네트워크와 검증기관의 네트워크를 원격으로 연결하여야 하는데, 이는 팀뷰어(Teamviewer)[97], 리모트콜[98]과 같은 원격제어 프로그램을 사용할 수 있다.

수사기관에서는 역외 압수수색을 위한 PC를 지정하여 원격제어 프로그램을 설치하고, 제3검증기관에서 수사기관의 검증 요청을 받으면 원격제어 시스템을 가동하여 원격 지원 대상 PC를 선택하여 네트워크 망을 연동한다. 이 과정에서 수사기관에서 제3검증기관에 검증 요청 시 검증 대상 압수수색 관련 정보를 입력하게 하여 요청사항을 확인할 수 있도록 한다.

수사기관과 검증기관의 PC가 연동되면 검증기관에서는 그때부터 원격으로 제어가 가능한바, 아래에서 검토할 바와 같이 실시간 검증을 위한 프로그램과 녹화를 위한 프로그램을 설치하여 검증을 시작할 수 있게 된다. 검증기관과의 망 연동이 해제되지 아니하고 지속되는 경우 정보의 유출 등 문제가 발생하므로 자동 연결되지 아니하도록 원격지원 프로그램 접속 시 PC 정보 입력, 압수수색 절차 종료시 접속 종료 등 절차를 준수하여야 한다.

---

97) 컴퓨터 간 원격 제어, 데스크톱 공유, 파일 전송을 위한 컴퓨터 소프트웨어 패키지이다. 위키백과 참조

98) 원거리의 PC화면을 로컬 PC에서 원격 제어하는 솔루션으로서, 사내 업무 지원이나 고객 센터에서 PC지원 용도로 활발히 사용된다. 위키백과 참조

2. 제3검증기관의 실시간 검증 및 녹화, 저장

가. 서버 IP 검증

압수수색의 첫 단계에서 수사기관은 대상 서버에 접속한 후 계정 정보를 입력하게 되는바, 접속한 서버의 IP 주소가 올바른지, DNS 서버에서 잘못된 IP를 제공하지는 않았는지 검증이 필요하다. 소위 '파밍(Pharming)'[99]공격에 따라 DNS 또는 프락시 서버의 주소가 변조되어 실제 사이트가 아닌 다른 사이트로 접속되는 등 목적한 서버의 진정성을 확보하기 위해서이다. 서버로부터 다운로드 받은 파일과 수사기관이 이를 복제하여 저장, 법원에 제출한 파일의 무결성은 해쉬값 산출을 통해 가능하지만, 실제로 진정한 서버로부터 다운로드 받은 파일이 맞는지, 즉 서버의 진정성과 그로부터 취득한 증거의 원본성(동일성) 입증은 해쉬값으로는 불가능하기 때문이다. 따라서 압수수색 시 접속하여 계정을 입력한 사이트(서버)가 실제 사이트가 맞는지 검증하는 분석 프로그램이 필요하다.

IP 검증과 관련된 기술적 프로그램으로는 보안용 툴바를 웹 브라우저에 추가하여 해당 사이트가 조작되었는지에 대한 진위여부를 확인하는 기법,[100] 접속하고 있는 사이트가 피싱 사이트인지 여부를 제3의 기관(TTP: Trust Third Party)을 통해 인증 받는 방식인 URL 스푸핑 기법,[101] 네트워크 정보 센터가 관리하고 있는 통신망

---

99) 해커가 사이트 주소를 관할하는 도메인서버를 직접 공격해 인터넷 프로토콜(IP) 주소 자체를 변경해 'www'로 시작하는 주소를 정확히 입력해도 가짜 사이트가 뜨게 해 개인정보를 빼가는 수법, 한경 경제용어사전 참조

100) 주용완 외, 피싱과 파밍에 대한 보안 대책 연구, 한국통신학회 종합학술 발표회 논문집(하계), 2005, 1791

101) 강지윤 외, 피싱/파밍 사례 및 대응방안 분석, 한국컴퓨터종합학술대

에 관한 정보 제공 서비스로 전 세계 각 기관들이 할당 받은 IP정보 및 등록한 호스트네임 정보를 관리하는 WHOIS를 이용하여 IP주소나 호스트네임의 정보를 확인하는 검증 기법[102] 등을 제시할 수 있다. 따라서 이와 같은 프로그램을 이용하여 해당 서버나 사이트 접속 전 IP 검증을 마친 후 접속하도록 하면 서버의 진정성을 입증할 수 있다.

나. 디지털 녹화 프로그램을 이용한 압수수색 전 과정 녹화, 저장

제3검증기관은 증거 수집의 전 과정을 녹화 프로그램을 이용하여 기록하고, 수집 과정에 불법적인 행위나 수사관이 무결성을 훼손하는 행위를 하지 않는지 기록하고 저장하여야 한다.[103] 수사기관의 컴퓨터와 원격으로 연동이 되었다면, 검증기관에서는 신뢰성 있는 녹화 프로그램을 작동시켜 수사기관의 압수수색 과정을 기록하고, 서버에서 다운로드 된 파일이 그대로 출력되는지, 해쉬값 산출에 어떠한 조작이나 실수가 있지 않은지 확인할 수 있다.

서버 검증을 마치고 압수수색의 진행 내용과 해쉬값 생성, 압수물 출력에 이르는 전 과정을 디지털 녹화 프로그램을 이용하여 녹화하였다면, 시간정보 등의 변경이나 훼손을 방지하기 위해 디지털 타임 스탬프(e-Timestamp)[104] 등으로 인증하거나 전자서명, 워터마킹 등으로 검증기관에서 검증하였음을 인증하는 것도 필요하다.

회 논문집, 2013, 739

102) 강지윤 외, 인터넷 주소 등록기관을 활용한 피싱 URL 분석 연구, 정보보호학회지 제23권 제6호, 2013, 16

103) 정교일, 앞의 논문, 184

104) e-Timestamp를 이용한 인증과 관련해서는 정교일, 앞의 논문, 185-186 참조

녹화된 내용은 무결성 입증을 위한 원본으로 사용되는바, 이를 검증기관에서 저장하고 암호화함이 요구되고, 법원에서 요청하는 경우 위 녹화 내용을 통해 무결성 입증이 가능하다.

Ⅲ. 수사기관 및 검증기관 관리자의 접근

1. 수사기관 및 검증기관 접근 차단 필요성

만약 수사기관이나 검증기관에서 위와 같이 압수수색 과정이 녹화된 저장물에 다시 접근할 가능성이 있는 경우 변경, 훼손이 가능하여 그 녹화물의 신뢰성을 보장할 수 없고, 압수수색 과정 중 나타난 해쉬값과 그 산출 과정 등 암호 기술이 노출되는 문제가 발생한다. 따라서 압수수색 과정을 검증, 녹화하여 인증을 마친 저장물에 대하여 수사기관이나 검증기관에서 일방적으로 접근, 열람할 수 없도록 하는 방법이 필요하다. 특히 위와 같은 저장물은 검증기관에 저장되어 있을 것이므로 검증기관의 공정성 확보를 위해서도 검증기관 내부 관리자가 이를 함부로 열람하지 못하도록 해야 한다.

2. 비밀 분산 기법에 의한 암호화

가. 비밀 분산 기법

Shamir의 Secret Sharing 기법은 비밀키를 여러 개의 비밀 조각으로 분할하여 다수에게 공유시킴으로써 비밀키를 보다 안전하게 관리하는 방법이다.[105] 복원이 필요한 경우 각자의 키를 모아 복호

105) 김기백, 권한에 따라 비밀 키 조합이 가능한 임계 비밀분산법, 한양대학교 석사학위논문, 2008, 6

화할 수 있다. 이러한 기법은 특정 한 사람이 비밀키를 가지고 있는 경우 쉽게 복호화할 수 있다는 위험을 방지하고자 하는 것이다.

각각의 분할된 비밀키 조각을 shadow라고 하고, n개의 shadow가 있을 때 k개의 shadow만을 모으면 비밀 정보가 복구 가능하도록 구성될 수 있는데, 이를 (k, n) threshold 방식이라고 한다.[106]

비밀 분산 기법은 다음과 같이 이루어진다. 임의의 비밀 정보 S를 분할하여 n명에게 분배하고, 이들이 모여 분할된 키를 복원할 수 있는 것인바, n-1개의 임의의 정수 S_1 , … S_{n-1} 개를 무작위로 뽑아서 n-1명에게 나누어 주고, 나머지 1명에게는 $S-\sum_{k=1}^{n-1} S_k$ 값을 주면 된다.[107][108]

비밀 분산 기법의 경우 비밀 정보를 분할한 n명이 모여야 키 복구가 가능한데, Shamir의 임계 암호기술은 그 n명 중 k명이 모이더라도 키 복구가 가능한 기술이다. 이를 구체적으로 살펴보면 다음과 같다.[109]

큰 소수 p를 정하고 $f(x)=a_{k-1}x^{k-1}+...+a_1x+S(\mathrm{mod}p)$ 인 다항식을 만든다. 여기서 $a_{1\ ...}a_{k-1}$은 [0, p-1]에서 랜덤하게 선택한다. 그리고 참여자 P_i에게 $S_i=f(i)\mathrm{mod}p, 1\le i\le n$ 값을 전송한다.

---

106) 채승철 외, 증명가능한 비밀 분산 방식을 이용한 키 복구 시스템에 관한 연구, 1998년 한국멀티미디어학회 춘계학술발표논문집, 1988, 170

107) 강석한, 전자정보 압수수색에서의 참여권 보장을 위한 기술적 조치 연구 - 임계 암호기술을 이용하여, 서울대학교 석사학위논문, 2016, 38

108) Shamir의 비밀 분산 기법은 임계 암호 방식(비밀 분산 기법으로 분산된 암호키 중 일부만 모이면 복원이 가능한 방식으로 비밀 분산 기법보다 유연하게 대응할 수 있도록 한 방법)으로 발전되었으나, 본 논문에서는 임계 암호 방식이 굳이 필요하지는 않은 것으로 보인다. 김기백, 앞의 논문, 7-8, 강석한, 앞의 논문, 38-40 참조

109) 이하는 채승철 외, 앞의 논문, 170

k개 이상의 비밀 조각이 모이면 Lagrange의 보간법에 의해 $f(x)$의 지수 $a_j(1 \le j \le k-1)$를 계산할 수 있는데, 비밀정보는 다음에 의해 계산된다.

$f(0) = S$

k차의 다항식 $f(x)$의 지수를 모를 때, 점$(x_i, y_i)(1 \le i \le k)$이 주어지면 $f(x) = \sum_{i=1}^{k} y_i \prod_{1 \le j \le k, j \ne 1} \frac{x - x_i}{x_i - x_j}$ 공식에 의해 $f(0) = S$이기 때문에 분산된 비밀은 다음과 같이 표현된다.

$$S = \sum_{i=1}^{k} C_i Y_i \ \ (C_j = \prod_{1 \le j \le k, j \ne 1} \frac{x_j}{x_j - x_i})$$

나. 암호화를 통한 접근차단

이러한 암호 기술을 이용하여, 역외 압수수색 과정의 녹화물을 암호화한 후,[110] 암호 키를 위와 같은 비밀 분산 기법에 따라 두 조각으로 나누어 수사기관, 검증기관이 각각 가지고 있으며 필요한 경우 법정에서 수사기관과 검증기관의 키 조각을 받아 암호 키를 복구하도록 할 수 있다.[111] 다만 수사기관과 검증기관의 키 조각을 쉽게 취득할 수 있는 경우 암호 키 복구가 가능하므로, 키 조각을 쉽게 취득할 수 없도록 검증기관과 수사기관에서 각각의 키 조각에 대한 별도의 암호화 조치도 필요할 것으로 보인다.

---

110) 암호화의 방법은 공개키 기반의 인증서를 이용하여 인증하는 방법을 예로 들 수 있다.

111) 이러한 제안은 강석한, 앞의 논문, 50-53을 참조하였다. 수사기관, 검증기관, 법원의 3조각으로 나누어 그 중 2조각 이상 모이는 경우 키 복구가 가능하도록 하는 방법도 있을 것이다.

Ⅳ. 입법 시 고려사항

검증기관의 위와 같은 검증은 서버의 진정성, 서버 내 정보와 그로부터 다운로드한 파일, 이를 출력한 출력물의 무결성을 보장하려는데 그 목적이 있으나, 기존의 수사방식과 같이 서버에서 다운로드한 원본파일과 이를 다른 저장매체에 저장하는 방법으로 출력한 파일의 각 해쉬값을 생성하여 비교하는 방법의 무결성 입증 절차도 동시에 이루어져야 한다. 출력물이 서버에서 다운로드 받은 원본파일과 일치한다는 점은 기존과 같은 해쉬함수를 이용한 입증이 가능하기 때문이다. 결국 이중의 무결성 입증을 필요로 한다.

검증기관의 검증내용은 법정에서 증거로 사용되는 것이 아니고 무결성 입증을 위한 자료에 불과하므로, 검증기관에서 보관하였다가 법원에서 요청할 경우 제출하게 되며, 사건이 종국적으로 종결하게 되는 경우 보관된 자료를 삭제하여야 한다. 검증기관에서 이미 종결된 자료를 보관하고 있는 경우 기본권 침해 소지가 높으므로 보관자료 삭제에 대하여 절차적 규정을 마련하여야 한다.

또한 검증기관은 앞에서 본 것처럼 무결성 입증 이외에 디지털 증거 분석 등 여러 검증의 역할을 담당하여야 하므로 검증기관 전문가들은 그 과정에서 나타난 증거들이 수사 단계에서 외부로 노출되지 않도록 비밀 준수 의무를 부과하여야 한다. 디지털 증거의 경우 개인정보의 유출 우려가 기존 유형물보다 더 크고, 수사기관만으로 한정되어 있던 개인정보의 취득이 검증기관에까지 노출된 것이므로 더 까다로운 절차와 엄격한 정보 통제 관리가 필요하다. 이에 검증기관의 조직원들은 어느 상황에서도 중립성을 지키고, 부적절한 접근을 차단하는 등 고도의 윤리성을 갖출 수 있도록 함이 상당하

다고 사료된다.[112]

제 4 장 결 론

기술한 바와 같이 디지털 환경의 변화는 현재의 수사 환경에 변화를 요구하고 있다. 그러나 법은 시대의 흐름을 완벽히 쫓아가지는 못하고 있으며 무력화되는 경우도 상당하다. 국경을 초월한 범죄가 점차 증가하고 있고, 인터넷이라는 거대한 네트워크 망은 국경을 허물었다고 보아도 과언이 아니다. 초국경적 기업의 등장으로 클라우드 서비스, SNS가 우리 생활의 전부가 되기 시작하였다. 수많은 정보가 서비스 제공자가 운영하는 서버, 어디에 존재하는지도 알 수 없는 서버에 저장되고 관리되며 일초에도 셀 수 없을 정도의 변경을 이루고 있다.

그런데 단순히 해외에서 운영되는 서버라는 이유로 증거 수집을 하지 못하게 되면, 이러한 서버는 범죄에 이용될 우려가 매우 높아진다. 형사사법공조절차는 인터넷 시대의 흐름에 비추어 너무나도 복잡한 절차와 상당한 시간을 요구하고 있다. 이에 따라 적절한 증거 수집이 이루어지지 못하는 경우, 결국 실체 진실의 발견이라는 형사사법의 목적을 달성하기 어렵고, 새로운 압수수색 방식을 허용하지 않은 국가가 그 피해를 고스란히 지게 된다.

결국 해외 서비스 제공자가 운영하고 있는 서버를 일반 국민들이

112) 조상수 외, 앞의 논문, 189

통용하며 중요 증거들을 디지털 증거의 형태로 은닉하고 있는 현시점에서, 수사기관이 적법하게 계정 정보를 입수한 경우에는 계정 접속을 통한 역외 압수수색을 허용함이 바람직하다. 이러한 방법은 선별 압수가 가능하고 개인 정보에 대한 침해를 최소화한다는 점에서도 당사자나 피압수자 모두 수용 가능한 방법으로 보아야 할 것이다.

다만 이러한 압수수색 방식은 서버를 압수수색하거나 이에 대한 해쉬값 산출이 곤란하다는 점에 비추어 무결성 입증에 한계가 있을 수 있다. 따라서 수사기관이 아닌 별개의 독립된 검증기관을 설치하여 역외 압수수색 과정을 검증하는 방법으로 무결성 입증을 하도록 하는 방법을 살펴보았다.

그 방법으로 수사기관은 계정 접속을 통한 역외 압수수색을 진행할 경우 제3검증기관과 네트워크 망을 연동시켜 압수수색 단계의 전 과정을 녹화, 실시간으로 서버를 검증함으로써 서버 내 저장된 원본과 저장된 값의 동일성과 무결성을 확인하고, 검증, 녹화된 결과가 변경, 조작되지 않도록 암호화하여 비밀 분산 방식에 따라 암호키 조각을 수사기관과 검증기관이 공유하는 방법을 제안하였다.

제3검증기관은 계정 접속을 통한 역외 압수수색 시 무결성을 입증함으로써 위와 같은 수사방법의 허용성을 한층 강화할 뿐만 아니라, 디지털 증거 전반에 대한 신뢰성을 확보하고, 당사자의 방어권 보장 및 디지털 증거 수집 절차 등 증거능력에 관한 법정에서의 소모적인 분쟁을 감소시키는 데 실효적인 역할을 할 것으로 기대한다.

참 고 자 료

[국내 문헌]

강석한, 전자정보 압수수색에서의 참여권 보장을 위한 기술적 조치 연구 - 임계 암호기술을 이용하여, 서울대학교 석사학위논문, 2016

강지윤 외, 인터넷 주소 등록기관을 활용한 피싱 URL 분석 연구, 정보보호학회지 제23권 제6호, 2013

강지윤 외, 피싱/파밍 사례 및 대응방안 분석, 한국컴퓨터종합학술대회 논문집, 2013

강철하 외, 디지털 포렌식에서 디지털증거의 특성과 법적 쟁점, 조선대학교 법학논총 제19권 제3호, 2012

곽병선, 디지털 포렌식 수사의 문제점과 개선방안, 법학연구 제42권, 2011

김기백, 권한에 따라 비밀 키 조합이 가능한 임계 비밀분산법, 한양대학교 석사학위논문, 2008

김범식, 경찰현장수사에서 디지털증거에 대한 압수수색의 개선방안, 외법논집 제38권 제4호, 2014

김병수, 전자정보에 관한 압수수색의 문제점과 개선방안, 비교형사법연구 제18권 제3호

김준한 외, 신뢰 가능한 디지털 증거의 무결성 보장 절차에 대한 연구, 보안공학연구논문지 제10권 제5호, 2013

대법원, 압수·수색 절차의 개선방안에 관한 연구, 사법정책연구원 연구총서,

2016

독고지은, 디지털증거 압수·수색에 대한 개정 형사소송법의 규제와 집행에 관한 연구 - 영장 집행 시 제기되는 쟁점을 중심으로 - , 법조, 2013

박영우, 사이버범죄방지협약의 국내법적 수용문제, 정보보호학회지, 2003

백형구 등, 주석 형사소송법 Ⅰ, 한국사법행정학회, 2009

법무연수원, 검찰실무 Ⅰ, 2013

성혜정 외, 소송절차에서 독립된 디지털증거 검증기관의 필요성에 대한 연구, 한국정보기술학회 하계학술대회 논문집, 2014

안경옥, 형사재판절차에서 테크놀로지의 활용과 형사소송법적 문제점, 21세기 형사사법개혁의 방향과 대국민 법률서비스 개선방안 Ⅳ, 한국형사정책연구원, 2004

오기두, 사이버수사 및 디지털 증거수집 실태조사 결과발표 및 토론회의 토론문, 국가인권위원회, 2012

오길영, 디지털 검증의 현재와 그 부당성: 소위 '왕재산' 사건을 대상으로, 민주법학 제48호, 2012

오병철, 클라우드 컴퓨팅에서의 사법관할권, IT와 법연구 제7집, 2013

원재천, 자국법의 역외적용과 한국의 대응방안에 관한 연구, 법무부, 2011

원혜욱, 과학적 수사방법에 의한 증거수집 - 전자증서의 압수·수색을 중심으로 - , 비교형사법연구 제5권 제2호, 2003

윤신자 외, 전자정보의 압수·수색 절차 개선방안 연구, 경찰학연구 제13권 제4호 통권 제36호, 2013

이관희, 디지털 정보의 취급에 관한 형사절차 개선방안, 고려대학교 석사학위 논문, 2012

이규안, 디지털 증거 인증기관의 필요성에 대한 연구, 한국전자통신학회 2011 추계종합학술대회지 제5권 제2호, 한국전자통신학회, 2011

이상진, 디지털 포렌식 개론, 이룬, 2011

이숙연, 형사소송에서의 디지털증거의 취급과 증거능력, 고려대학교 박사학위논문, 2011

이숙연, 전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여 - 대법원 2011모1190 결정에 대한 평석을 중심으로 한 연구, 헌법학연구 제18권 제1호, 2012

이영준, 유럽의회의 사이버범죄방지를 위한 국제협약 소고, 형사정책연구, 2001

이영준 외, 사이버범죄방지조약에 관한 연구, 형사정책연구원 연구총서, 2001. 12.

이완규, 디지털 증거 압수 절차상 피압수자 참여 방식과 관련성 범위 밖의 별건 증거 압수 방법, 형사법의 신동향 통권 제48호, 2015

이원상, 클라우드 컴퓨팅 환경에서의 디지털 증거 확보를 위한 소고, 형사법의 신동향 통권 제38호, 2013

이윤제, 디지털 증거의 압수·수색과 증거능력, 형사법의 신동향 통권 제23호, 2009

이윤제, 디지털 증거 압수수색영장의 집행에 있어서의 협력의무, 형사법연구 제24권 제2호, 2012

이재상, 신형사소송법 제2판, 박영사, 2009

이정민, 디지털증거의 압수수색과 절차적 진실, 형사법연구 제28권 제3호, 2016

이창범 외, 클라우드 컴퓨팅 활성화를 위한 법제도 개선 방안 연구, 한국인터넷진흥원, 2010

전강진, 일본의 하이테크범죄의 현상과 과제, 해외연수검사연구논문집 제18집(2), 법무연수원, 2003

전명길, 디지털증거의 수집과 증거능력, 법학연구 제41권, 2011

전승수, 형사절차상 디지털 증거의 압수수색 및 증거능력에 관한 연구, 박사학위논문, 서울대학교, 2011

전현욱 외, 사이버범죄의 수사 효율성 강화를 위한 법제 개선 방안 연구, 경제·인문사회연구회 미래사회 협동연구총서 15-17-01

정교일, 디지털증거의 압수와 공판정에서의 제출방안, 형사법의 신동향 통권 제25호, 2010

정대용 외, 디지털 증거의 역외 압수수색에 관한 쟁점과 입법론 - 계정 접속을 통한 해외서버의 원격 압수수색을 중심으로 -, 법조, 2016

정소연, 디지털 증거의 역외 압수수색에 대한 법적 고찰, 디지털포렌식연구 제11권 제1호, 2017

정현지 외, 클라우드 컴퓨팅 환경에서의 디지털 포렌식 동향 및 전망, 정보보호학회지 제22권 제7호, 2012

조기영, 디지털 세계에서의 압수수색, 법학연구 통권 제49집, 2016. 8

조상수 외, 디지털 증거의 무결성 보장 절차에 대한 개선, 정보과학회논문

지: 정보통신 제39권 제2호, 2012

주용완 외, 피싱과 파밍에 대한 보안 대책 연구, 한국통신학회 종합 학술발표회 논문집(하계), 2005

채승철 외, 증명가능한 비밀 분산 방식을 이용한 키 복구 시스템에 관한 연구, 1998년 한국멀티미디어학회 춘계학술발표논문집, 1998

한봉조, 사이버범죄수사에 대한 국제적 협력문제, 형사정책연구, 2000

한수웅, 헌법학, 법문사

Jihyun Park, “International trend against cybercrime and controversy over the F.B.I.‘s practice of ”Extra-territorial Seizure of Digital Evidence“, 국제법학회논총 제49권 제3호

[해외 문헌]

Goldsmith, Jack L, “The Internet and the Legitimacy of Remote Cross-Border Searches”, University of Chicago Legal Forum, 2001

Report of the Transborder Group, Transborder access and jurisdiction: What are the options?, T-CY(Cybercrime Convention Committee), 2016

Sussmann, Michael A, “The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium”, Duke Joumal of Comparative & International Law 9.2, 1999

[인터넷 자료 등]

보안뉴스 2015. 7. 21.자 기사 <사이버범죄 국제 공조 위한 부다페스트 협약, 우린 왜 아직?>

서울신문 2012. 12. 19.자 기사 <디지털 증거 조작 쉬워... 국과수 같은 '인증기관' 필요>

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

https://www.facebook.com/legal/terms