연구총서 23-A-08

www.kicj.re.kr

디지털 증거 압수수색절차 개선에 관한 연구

Issues in Search and Seizure of Digital Evidence and Possible Improvements

탁희성 · 이순옥 · 박중욱 · 손여옥

KICJ 한국형사·법무정책연구원
Korean Institute of Criminology and Justice

디지털 증거 압수수색절차 개선에 관한 연구

연구책임자

탁 희 성 한국형사·법무정책연구원 선임연구위원

공동연구자

이 순 옥 중앙대학교 법학전문대학원 교수

박 중 욱 원광대학교 경찰행정학과 강사

손 여 옥 국회도서관 전문경력관

연 구 지 원

이 다 미 한국형사·법무정책연구원 선임조사연구원

발간사

전세계에 걸쳐 IT 기술이 놀라운 속도로 변화 발전하고 있음에도 불구하고 우리 형사소송법은 여전히 유체물 중심의 압수수색 관점에서 벗어나지 못하고 있습니다. 하지만 정보통신기술의 급속한 발전과 코로나19로 인하여 비대면 디지털 전환이 가속화되면서 정보보호를 위한 데이터 암호기술이 더욱 강력해졌고, 클라우드 서비스의 확산으로 인한 데이터의 네트워크화는 기존의 법해석만으로는 해결하기 어려운 법적·기술적 난제들을 야기할 뿐 아니라 형사사법절차의 지향점이라 할 수 있는 실체적 진실의 발견을 가로막는 장애요소가 되고 있습니다.

물론 법적안정성을 추구하는 법률이 기술의 변화를 따라가는데 있어서는 한계가 있을 수밖에 없지만, 현재 우리의 디지털 증거 압수수색 관련 법제현황은 현실과 법률의 괴리를 심화시키는 주된 요인이 되고 있다고 할 것입니다.

이에 본 연구는 현행 형사소송법상 압수수색 규정과 디지털 증거의 부정합성의 문제를 검토해 봄으로써 현행 압수수색 규정의 한계와 개선방안을 제시해 보았습니다. 그리고 이와 아울러 디지털 환경에 부합하는 새로운 증거확보 방식의 도입과 관련한 쟁점들을 검토해 봄으로써 우리 입법에의 반영 가능성과 구체적인 입법안을 제시해 보고자 하였습니다. 이에 본 연구가 디지털 증거에 부합하는 압수수색 규정과 절차를 마련하는 데 조금이나마 기여할 수 있기를 바라는 바입니다.

끝으로 본 연구를 수행하는 데 있어서 공동연구자로 참여해 주신 이순옥 교수님, 박중욱 박사님, 손여옥 박사님께 감사의 말씀 드립니다. 그리고 보고서 정리 및 편집에 최선을 다해주신 이다미 선임조사연구원의 노고에도 감사를 드립니다.

2023년 12월

연구진을 대표하여

선임연구위원 **탁 희 성**

목 차

표 차례

국문요약

1. 정보통신기술의 급속한 발전과 코로나19로 인하여 비대면 디지털 전환이 가속화되면서 정보보호를 위한 데이터 암호기술이 더욱 강력해졌고, 클라우드 서비스의 확산으로 인한 데이터의 네트워크화는 기존의 법해석만으로는 해결하기 어려운 법적·기술적 난제들을 야기하고 있다. 이는 형사사법절차의 지향점이라 할 수 있는 실체적 진실의 발견을 가로막는 장애요소가 되고 있다. 따라서 수사절차상 디지털 증거를 확보해야 하는 경우 기존의 유체물에 기반한 압수개념에서 벗어나서 디지털 데이터의 특성에 부합하는 새로운 방식과 절차가 정립되어야 할 뿐 아니라 이를 뒷받침할 수 있는 입법적 지원이 이루어질 필요가 있다.

이에 본 연구는 첫째, 디지털 증거에 부합하는 압수수색 규정의 정비방향, 둘째, 디지털 환경하에서 수사절차상 실체적 진실의 발견과 프라이버시 보호라고 하는 두 가치의 균형을 토대로 한 입법의 방향성, 셋째, 디지털 데이터의 기술방식에 따른 존재양식을 고려한 새로운 증거확보 방식의 도입 가능성을 검토하는데 목적을 두고 있다.

따라서 본 연구내용은 다음과 같이 구성하고자 한다. i) 현행 「형사소송법」상 압수수색 규정과 디지털 증거의 부정합성의 문제를 검토해 보고자 한다, ii) 디지털 증거 압수수색과 관련된 쟁점별로 판례와 입법안의 변화와 경향성을 분석해 보고자 한다. iii) 디지털 증거 압수수색에 대응하는 주요 국가들의 입법 및 정책의 변화 등을 비교검토 해보고자 한다. iv) 디지털 증거 확보를 위한 새로운 강제수사 처분방식의 도입 필요성 및 입법 방향성 등을 검토해 보고자 한다.

2. 현행법상 압수수색 규정과 디지털 증거의 부정합성의 문제는 압수개념과의 부정합성, 압수수색 방식과의 부정합성, 입법체계와의 부정합성 문제로 논할 수 있다. 먼저 압수개념과의 부정합성의 문제는 현행 「형사소송법」상 압수대상을 물건, 즉 유체물로 한정하고 있는 데서 비롯된다. 하지만 이와 아울러 디지털 정보에 대한

압수는 피압수자의 정보에 대한 점유력을 배제하는 것이 아니기 때문에 근본적으로 디지털 정보 자체는 압수대상이 될 수 없다는 문제도 존재하고 있다. 다음으로 압수수색 방식과의 부정합성은 디지털 기술환경의 변화로 인해 기존의 수사방식으로는 디지털 데이터를 증거로 확보하는 데 있어서 현실적인 한계에 직면하고 있는 데서 비롯되는 것이라 할 수 있다. 따라서 디지털 증거를 확보하는 데 효율적인 새로운 수사방식의 도입에 대한 논의가 필요하다. 마지막으로 입법체계와의 부정합성은 현행「형사소송법」의 편장체계의 불합리성에서 비롯되는 문제라 할 수 있다. 즉 공판절차와 수사절차의 근본적인 차이를 무시한 채 공판절차 규정을 수사절차에 준용하도록 하는 현행 형사소송법체계는 실정법과 현실의 괴리를 야기할 뿐 아니라 기술의 발전에 따른 수사환경의 변화에 능동적으로 대응하지 못한다는 한계를 낳고 있다.

3. 형사절차상 디지털 증거의 중요성이 논의되기 시작했던 2000년 초반부터 현재까지 국회에 발의되었던 형사소송법 일부개정법률안 가운데 디지털 증거 압수수색과 관련하여 발의된 입법안은 17건에 불과하다. 국회에 발의된 입법안을 검토해 보면, 먼저 입법취지와 관련해서는 2015년 이전에는 개인정보보호와 자기정보통제권 보장을 위해 발의된 입법안이 대부분이었지만, 2015년 이후부터는 디지털 증거 압수수색 절차상 수사기관의 권한 남용에 대한 통제장치의 필요성에 입각한 입법안들이 발의되었고, 2021년 N번방 사건 이후로는 디지털 증거의 신속한 확보 및 보전을 위한 제도적 장치의 도입 필요성을 강조하는 입법안들이 발의되었다. 즉 디지털 기술의 발전으로 실체적 진실의 발견과 프라이버시가 충돌하는 상황에서 그 무게중심의 변화에 따라 입법안의 발의내용이 변화되어 옴을 알 수 있다. 이러한 변화는 입법안의 내용에서도 살펴볼 수 있는바, 초기에는 사생활과 개인정보보호를 위하여 압수수색 절차를 보다 세분화하여 통제하려는 관점에서 입법안이 발의되었지만, IT 기술이 고도화되어 감에 따라 기술의 발전속도를 따라가기 힘든 공권력만으로는 디지털 증거를 확보하는데 한계가 있다는 인식하에 디지털 증거를 보다 신속하고 효율적으로 확보하는 방식이 필요하다는 관점에서 입법안들이 발의되고 있음을 알 수 있다. 마지막으로 입법형식에 있어서는 2000년대 초반부터 2018년까지는 현행법과 같은 법원의 압수수색 규정을 개정하는 방향에서 입법안이 발의되었지만, 2019년 이후부터 발의된 디지털 증거

압수수색과 관련한 형사소송법 개정안들은 수사편에 규정된 제215조 이하의 수사기관의 압수수색 규정을 개정하는 방향으로 발의되고 있음을 볼 수 있다. 이러한 입법형식의 변화는 수사총량의 확대에 따른 절차적 통제의 필요성, 그리고 수사기관의 공권력에 대응할 수 있는 기술적 방어가 가능한 상황에서 디지털 증거의 확보에 부합하는 새로운 압수수색 방식의 도입 필요성 등에서 비롯되었다고 보여진다.

다른 한편으로 디지털 증거 압수수색과 관련한 판례의 변화를 검토해 보면, 먼저 디지털 증거 압수수색의 적법성과 관련하여 2020년 이전에는 참여권 보장이 주된 쟁점이었던 것에 비해, 2020년 이후부터는 임의제출물 압수가 주된 쟁점으로 나타나고 있음을 볼 수 있다. 그리고 디지털 증거 압수수색의 적법성 판단기준에 있어서는 초기에는 절차의 공정성 확보와 피압수자의 절차적 권리보장이라는 관점에서 이루어졌지만, 디지털 기술의 발전으로 방대한 양의 정보가 압수수색에 포함됨으로써 절차의 공정성보다는 프라이버시 보호의 측면에서의 적법절차 준수가 강하게 요구되고 있음을 알 수 있다.

4. 대륙법계 국가인 독일과 일본, 영미법계 국가인 영국과 미국의 경우 디지털 증거 압수수색과 관련한 입법적 쟁점의 변화 및 경향성을 검토해 보았다. 먼저 독일의 경우 우리와 달리 지난 20년간 법치국가원칙과 비례성 원칙에 기초하여 기술의 발전에 따라 가능해진 새로운 수사방법들을 지속적으로 법률에 수용하고 있을 뿐 아니라 기존의 수사방법에서 예상치 못했던 중대한 기본권 침해를 입법을 통해 적절히 상쇄하고자 시도하고 있음을 볼 수 있다. 일본의 경우 2011년 형사소송법 개정으로 전자적 기록의 압수와 관련하여 전자적 기록매체에 대한 대체집행(execution in lieu of seizure of record media concerning electronic record), 기록명령부 압수(seizure of record order copy), 원격접근(remote search and seizure) 등이 도입되었지만, 입법과정에서 논란이 되었던 역외압수(extraterritorial search and seizure), 전자적 기록의 압수범위의 확정 등과 관련해서는 여전히 다투어지고 있음을 볼 수 있다. 또한 전자적 기록의 압수와 관련하여 새로 도입된 제도인 기록명령부 압수에 있어서 수사기관의 명령에 불응한 경우 강제할 수단이 없다는 점에서 그 실효성 여부가 논란이 되고 있다.

다음으로 미국의 경우 수회에 걸친 법령개정을 통해 디지털 증거의 특성을 반영한 압수수색 절차를 명문으로 인정하고 있다. 즉 압수수색 대상에 정보를 명시하고 있으며, 전자영장제도를 도입하여 영장청구 및 발부절차의 신속성을 높였고, 관할권을 초월한 영장(Network Investigative Technique:NIT warrant)제도를 도입하여 관할권 밖에 있는 정보의 압수수색을 가능하게 했다. 또한 Cloud Act를 통하여 역외 압수수색을 허용하고 있다. 즉 미국의 경우 디지털 증거 압수수색 절차와 관련해서는 피의자의 사생활 보호를 위한 절차적 통제보다는 수사의 효율성을 고려한 규정들을 도입하고 있다고 볼 수 있다. 마지막으로 영국의 경우 2001년 CJPA(Criminal Justice and Police Act) 제정 당시 정보를 압수수색 대상으로 명문화하였을 뿐 아니라 PACE(Police and Criminal Evidence Act) 1984를 개정하면서 압수수색 대상을 '전자적 형식으로 저장된 것'이라고 하여 그 범위를 확대시켰다. 또한 IPA(Investigatory Powers Act) 2016에서 해외 통신사업자에 대한 데이터 제공 및 보전요청, 해외국가의 요청에 따른 감청도 가능하도록 규정하고 있다. CMA(Computer Misuse Act) 1990을 통해 온라인 수색을 법률로 규정하였고, RIPA(Regulation of Investigatory Powers) 2000에서 암호해제 요구통지를 할 수 있도록 했고, 통지 불이행 시 형사처벌이 가능하도록 규정하고 있음을 볼 수 있다. 즉 영국은 기존 법률규정이 급변하는 IT 기술을 따라가지 못함으로써 범죄수사가 어려워지고, 개인정보를 보호하지 못한다는 비판 속에서 지속적으로 법령의 제개정을 통해 그 문제점을 해결하고 있음을 볼 수 있다.

5. 현재 디지털 증거 압수수색과 관련하여 논의되고 있는 주된 쟁점은 현행 형사소송상 디지털 증거 압수수색의 적법성을 확보하기 위한 절차적 통제방안과 디지털 증거에 부합하는 새로운 압수수색 제도의 도입 여부라고 할 수 있다.

먼저 현행 「형사소송법」상 디지털 증거 압수수색의 적법성 확보를 위한 절차적 통제와 관련하여 논의되고 있는 주요 논제는 참여권 보장과 임의제출물 압수라고 할 수 있다. 디지털 증거 압수수색에 있어서 유무관 정보의 혼재로 인한 사생활 및 기본권 침해의 우려를 방지하기 위한 절차적 수단으로서 참여권이 갖는 의미가 중요함에도 불구하고, 현행법상 그에 부합하는 명확한 기준이 입법적으로 정비되지 못하고 있어서 그 해석과 관련하여 논란이 제기되고 있다고 볼 수 있다. 따라서 디지털

증거 압수수색에 있어서 참여권이 적법절차 실현을 위한 수단으로써 그 실효성을 확보하기 위해서는 참여권의 법적 지위를 명확히 해야 하고, 참여권자의 범위를 입법적으로 해결해야 하며, 참여권의 실질로서 무관정보 배제를 위한 압수목록 교부 규정의 개정과 무관정보 삭제 및 폐기 절차를 마련할 필요가 있다. 그리고 디지털 증거 임의제출 시 압수와 관련한 문제는 기존의 유체물에 대한 임의제출물 압수와 동일한 논리는 정보저장매체에 적용하는 경우 매체 전부에 대한 압수가 가능하다고 하는 불합리한 결과가 발생하는 데서 비롯된다. 특히 스마트폰과 같이 개인의 사생활과 관련된 정보가 다량으로 혼재되어 있는 매체를 임의제출하는 경우, 정보압수에 적용되는 기본원칙들이 적용되지 않는 한 피압수자의 프라이버시 및 기본권에 대한 심각한 침해를 야기할 수 있기 때문이다. 따라서 정보저장매체에 대한 임의제출 시에는 제출의사의 임의성 확인, 임의제출 범위의 제한 등이 수반되어야 할 뿐 아니라 압수의 강제성이 적법하다고 하기 위해서는 혐의사실과의 관련성 판단, 압수 범위의 선별 복제 및 출력, 참여권 보장 등이 이루어져야만 할 것이다.

다음으로 디지털 환경에 부합하는 새로운 증거확보 방안으로는 디지털 증거 보전명령제도, 전자영장제도, 원격지 압수수색제도, 온라인 수색제도 등을 검토해 보았다.

먼저 디지털 증거 보전명령제도는 전자통신서비스 또는 원격 컴퓨팅 서비스제공자로 하여금 일정기간 데이터를 보전하도록 함으로써 데이터가 손실되거나 변경될 가능성을 최소화하여 신속하게 중요한 디지털 증거를 확보하기 위한 제도이다. 데이터 보전명령은 데이터의 점유이전이 발생하지 않기 때문에 기본권 침해가 덜할 수 있지만, 데이터 이용의 제한, 업무의 제약 등이 발생하기 때문에 강제처분의 성격을 갖는다고 볼 수 있다. 따라서 데이터 보전명령제도를 입법화함에 있어서는 그 전제요건으로써 보충성과 필요성 및 관련성 등이 규정되어야 할 뿐 아니라 보전명령의 객체는 전자통신서비스 또는 원격 컴퓨팅 서비스제공자로 제한되어야 할 것이다. 또한 데이터 보전명령에 대해서는 일정기간 제한규정을 두어야 하고, 수사상 강제처분이라는 점에서 법원에 의한 사후 통제의 필요성이 있다고 할 것이다.

다음으로 전자영장제도는 이미 2020년 「형사사법절차에서의 전자문서 이용 등에 관한 법률」을 통해 도입되어 있지만, 아직 해당 법률이 시행되기 전이기 때문에 형사소송법상 영장 관련 규정에 대한 정비가 필요한 시점이라 할 수 있다. 즉 전자영장

제시를 위한 근거규정이 마련되어야 하고, 영장제시 원칙에 대한 예외규정을 개정할 필요가 있다고 할 것이다.

원격지 압수수색제도는 클라우드 서비스 또는 해외 이메일 서비스 등을 이용하는 사람에 대한 압수수색에 있어서 영장에 기재된 장소에 존재하는 정보저장매체에 접속하여 디지털 증거를 확보하기 위한 수단이라고 할 수 있다. 현재와 같은 디지털 환경 내에서 원격지 압수수색의 필요성에 대해서는 이론의 여지가 없지만, 영장에 기재된 디지털기기와 네트워크로 연결된 원격지 서버 등으로 수색의 장소적 범위가 확장되기 때문에 현행 압수수색 규정으로 포섭하는 데는 한계가 있다. 따라서 물리적 장소개념에 의존하는 현행 압수수색 규정과 분리하여 별도로 원격지 압수수색을 위한 근거규정을 마련할 필요가 있다. 그리고 압수수색 권한의 확장으로 제3자의 프라이버시 또는 타국의 관할권에 대한 침해를 유발할 수 있기 때문에 피처분자에게 주어진 일반적인 접근권한이 허용하는 한계 내로 제한하는 명시적 규정을 두어야 할 것이다.

마지막으로 온라인 압수수색제도는 타인의 정보기술시스템 이용을 감시하고, 저장된 내용을 읽고 기록하기 위한 목적으로 기술적 수단을 사용하여 타인의 정보기술시스템에 은밀하게 접근하는 것으로, 특정범죄에 대응하기 위한 국가에 의한 합법적 해킹이라 할 수 있다. 따라서 기존의 어떠한 강제수사보다도 기본권침해가 크기 때문에 온라인 수색은 원칙적으로 피의자에 한해서 허용되어야 하고, 대상범죄와 기간의 제한이 명확하게 규정되어야 할 뿐 아니라 이중적 통제장치 즉 법원에 의한 사전 규제와 국회에 의한 사후 규제가 필요하다고 보아야 할 것이다.

6. 디지털 증거 압수수색 절차 개선을 위한 입법의 방향성을 고려함에 있어서 IT 기술이 고도화될수록 정보통신기술과 네트워크를 이용한 범죄행위에 대한 소추가능성이 현실적으로 제약받을 수밖에 없는 한계에 직면하고 있다는 점에 대한 인식이 전제되어야 할 것이다. 이러한 전제하에서 정보의 압수수색의 적정성을 담보하기 위해서는 개인의 프라이버시와 기본권 보호에 있어서 실체적 진실의 발견과 균형을 이룰 수 있는 사법적 관점과 입법적 정비가 필요하다고 본다. 그리고 입법체계상 현행 「형사소송법」의 편장체계를 개선하여 수사절차와 공판절차에 관한 규정들을 분리하여 규정하고, 준용규정이 아닌 직접규정을 통해 수사절차를 규율하는 것이 오

히려 수사절차의 적정성과 사법통제의 가능성을 확보하는 데 보다 더 실효적이라 할 수 있을 것이다.

그리고 디지털 증거 압수수색 절차 개선과 관련하여 정책적으로 고려해야 할 문제로는 위법수집증거배제법칙의 강화와 무관정보 삭제 및 폐기 방안을 제시할 수 있다. 즉 디지털 증거 압수수색절차의 적법성을 일관되게 유지할 수 있는 명확한 법규정이 마련되어 있다는 것을 전제로, 그 절차적 규정을 위반한 경우에는 예외없이 위법수집증거배제법칙을 적용함으로써 디지털 증거 압수수색에 수반될 수 있는 프라이버시 및 기본권침해의 가능성을 최대한 억제하는 것이 바람직하다고 할 것이다. 즉 위법수집증거배제법칙의 엄격한 적용을 통해 증거의 사용을 배제하는 것이 어떠한 절차법적 규정보다도 강력하게 수사절차의 적법성을 담보할 수 있기 때문이다. 다음으로 무관정보의 삭제 및 폐기는 수사기관에서 압수한 디지털 증거의 이미징사본의 남용 내지 오용 가능성을 배제하고자 하는 취지에서 이루어지고 있지만, 압수 직후 이미징사본의 삭제 및 폐기는 오히려 형사절차의 공정성을 저해하는 요소가 될 수 있다는 점도 고려할 필요가 있다. 이러한 점에서 볼 때, 수사기관에서 확보한 이미징사본을 언제, 어떻게 삭제 또는 폐기할 것인가에 대한 절차적 논의가 있어야 할 것인바, 해당 사건에 대한 판결이 확정될 때까지 법원에 보관하도록 하는 방식도 하나의 대안이 될 수 있을 것이다.

서론

탁 희 성

제1장

서론

제1절 | 연구의 배경 및 연구방법

1. 연구의 배경

가. 연구 필요성

디지털 증거 압수수색과 관련하여 처음 논의가 시작되었던 30여 년 전 상황과 비교해 보면 그동안 디지털 기술은 놀라운 속도로 변화 발전하고 있음에도 불구하고, 여전히 우리의 「형사소송법」은 유체물 중심의 압수수색의 관점에서 디지털 증거를 포섭하고 있음을 볼 수 있다. 하지만 이미 수사기관의 압수수색에 있어서 무게중심은 유체물이 아닌 디지털 정보로 이동하였고, 압수수색의 방식 또한 비이전성을 본질로 하는 디지털 데이터의 특성상 물리적 점유이전에서 논리적 복제로 전환된 상황임에도 불구하고 여전히 매체중심적 사고에 기반한 압수개념을 디지털 정보에 그대로 적용함으로써 현실과 법률의 괴리가 심화되고 있다.

법적안정성을 추구하는 법률이 기술의 변화를 따라가는 데 있어서 뒤처질 수밖에 없지만, 현재 우리의 디지털 증거 압수수색 관련 소송법제 현황은 단지 입법의 지연 수준에 그치는 것이 아니라 입법의무의 방기 그 자체라고 할 것이다. 물론 디지털 증거 압수의 절차와 방법에 관해서는 한차례 법개정을 통해 디지털 정보의 압수방식을 규정하고 있기는 하지만, 이는 어디까지나 기존의 압수개념에 기반한 매체중심적 압수의 방식이기 때문에 매체독립적이면서 비이전성을 전제로 하는 디지털 데이터에 부합하는 수사절차와 방식으로는 한계를 드러낼 수밖에 없다.

이러한 입법의 태만으로 인해 디지털 증거 압수수색에 있어서는 법률과 해석의 공백들이 나타날 수밖에 없었고, 이러한 공백들을 결국 법원의 판단에 의지할 수밖에 없는 상황이 만들어졌다고 볼 수 있다. 그로 인해 현재 디지털 증거 압수수색에 있어서는 사법이 입법을 대신하는 불합리한 현상이 나타나고 있다고 볼 수 있다.

이와 같이 디지털 정보의 압수수색에 있어서 적법성을 담보하기 위해 요구되는 법률상 개념과 절차규정의 흠결로 인하여 영장청구, 원격지 압수수색, 참여권 보장, 임의제출뿐 아니라 압수물 목록작성에 있어서 조차 현실과 법규정의 심각한 괴리현상이 발생하고 있다. 이로 인해 엄격한 의미의 성문법률에 의해 규율되어야 할 형사절차인 압수수색이 법률이 아닌 판례의 해석에 의해 좌우됨으로써 법률명확성이 담보되지 못하고 있을 뿐 아니라, 압수수색을 하는 수사기관들 역시 판례가 제시하는 원칙과 기준을 수용하는 관점의 차이로 인해 사건의 유형에 따라 실무적 행위기준이 달라짐으로써 수사의 공정성에 문제가 발생할 여지가 크다고 할 수 있다.

더욱이 정보통신기술의 급속한 발전과 코로나19로 인하여 비대면 디지털 전환이 가속화되면서 정보보호를 위한 데이터 암호기술이 더욱 강력해졌고, 클라우드서비스의 확산으로 인한 데이터의 네트워크화는 기존의 법해석만으로는 해결하기 어려운 법적·기술적 난제들을 야기할 뿐 아니라 형사사법절차의 지향점이라 할 수 있는 실체적 진실의 발견을 가로막는 장애요소가 되고 있다. 따라서 수사절차상 디지털 증거를 확보해야 하는 경우 기존의 유체물에 기반한 압수개념에서 벗어나서 디지털 데이터의 특성에 부합하는 새로운 방식과 절차가 정립되어야 하고, 이를 뒷받침할 수 있는 입법적 지원이 이루어져야 현재와 같은 디지털 증거를 둘러싼 형사절차의 불명확성이 해소될 수 있다고 할 것이다.

나. 연구 목적

이에 본 연구는 크게 세 가지 방향에서 연구목적을 설정하고자 한다. 첫째는 디지털 증거에 부합하는 압수수색 규정을 어떠한 방향에서 정비하는 것이 바람직한가를 고민해 보고자 한다. 즉 현행「형사소송법」규정으로는 디지털 증거를 압수수색하는데 한계가 있기 때문에 법원의 판례에서 제시하고 있는 원칙과 기준들을 고려하여 각 수사기관별로 예규나 훈령의 형태로 디지털 증거의 압수수색절차를 보완하고 있는

것이 현실이다. 하지만 디지털 증거 압수수색과 관련한 대법원 판례들이 일관성을 갖고 있다고 보기도 어려울 뿐 아니라 학계로부터 비판을 받는 판례들도 있기 때문에 판례의 법해석을 통한 디지털 증거의 압수수색의 원칙과 기준을 신뢰하는 데도 한계가 있다고 할 것이다. 더욱이 디지털 정보에 대한 강제처분수사가 법률이 아닌 행정규칙으로 이루어지는 것은 강제처분 법정주의 원칙에도 부합하지 않는 측면이 있다. 따라서 수사절차상 디지털 증거를 확보함에 있어서 논의되어야 할 입법적 쟁점들을 검토해 보고자 한다. 이를 통해 디지털 수사로 인한 강제처분의 법률명확성을 담보하면서도 수사절차상 디지털 증거를 확보하는 과정에서 기술적 문제로 인해 야기될 수 있는 헌법적 권리의 침해문제와 어떻게 균형을 잡을 것인가를 고민해 보고자 한다.

둘째, 정보통신기술의 급속한 발전에 터 잡아 휴대와 이동의 편의성을 추구하는 이용자의 수요가 반영된 스마트폰 중심의 디지털 환경의 변화는 개인의 사회적 관계를 확장하고 강화시켰을 뿐 아니라 개인의 업무 및 금융활동, 취미 및 문화생활, 교육, 건강 및 의료 관련 서비스 등 모든 라이프 패턴을 가능하게 만들고 있다. 이와 같은 스마트기기 중심의 디지털 환경에 있어서는 다양한 개인정보의 수집, 처리, 활용, 공유 등을 통해 정보의 가치를 생산해 내고, 그러한 정보를 다양한 영역에서 활용할 수 있기 때문에, 개인의 프라이버시 및 정보보호의 필요성과 중요성에 대한 인식이 점차 높아져가고 있다. 따라서 개인의 프라이버시 및 개인정보 침해에 대한 우려로 인한 보안시스템의 강화 및 데이터의 암호화 등이 개인의 스마트기기에까지 적용되고 있고, 이러한 현상은 IT 기술이 발전할수록 점차 강화되어가는 추세에 있다고 할 수 있다.

이와 같이 기업의 정보시스템뿐만 아니라 개인들의 정보보안 요구에 상응하여 적용된 스마트기기의 보안시스템 강화와 데이터의 암호화로 인해 기존과 같은 강제수사처분만으로는 수사에 필요한 증거를 확보하는 것이 어렵거나 심지어는 불가능한 경우들이 이미 나타나고 있다. 즉 디지털 환경하에서 수사기관은 기존의 우월적 지위만으로는 범죄의 혐의를 입증하는 데 있어서 한계에 직면하고 있다고 볼 수 있다.

이러한 상황에서 수사절차상 디지털 증거를 확보함에 있어서는 프라이버시와 실체적 진실발견이 서로 충돌하는 지점이 발생할 수밖에 없다. 다만 아직까지는 수사기관의 우월적 지위로 인하여 실체적 진실의 발견을 위한 프라이버시와 개인정보 침해의

문제가 심각하다는 인식이 일반국민과 법원의 저변에 깔려있기 때문에 프라이버시와 개인정보 보호에 보다 더 중점을 두고 판단하는 경향이 있음을 볼 수 있다.

하지만 IT 기술이 고도화되고, 클라우드 인프라의 확산, 데이터 암호화 기법 및 알고리즘의 강화 등으로 데이터에 대한 접근 자체가 기존의 방식과 법률로는 한계에 부딪치는 경우에 있어서조차 개인의 프라이버시와 개인정보 보호에 중점을 두게 되면 실체적 진실의 발견을 통한 형사적 정의의 실현이 훼손되고 오히려 IT 기술의 양면성을 활용하여 법망을 회피하는 것이 가능하게 되는 사회가 될 수도 있을 것이다. 이와 같이 디지털 환경 내에서 행해지는 수사절차상 실체적 진실의 발견과 프라이버시 보호라고 하는 두 가지 가치에 있어서의 무게중심을 어디에 두고 입법의 방향성을 찾을 것인가를 고민해 보고자 한다.

셋째는 앞서 기술한 바와 같이 클라우드 기반의 디지털 환경과 IT 기술의 고도화로 인해 수사절차상 범죄혐의를 입증할 수 있는 증거로서 디지털 정보를 확보하는 데 현실적으로 상당한 어려움이 야기되고 있다. 이러한 상황에서 기존의 압수수색, 감청 등과 같은 강제수사처분만으로는 디지털 증거를 확보하는데 한계에 부딪치고 있는 것이다. 즉 기존의 증거확보방식은 공간과 물리적 장소 그리고 유체물을 전제로 한 것이기 때문에 네트워크를 통해 생성, 전송될 뿐 아니라 분산처리 및 가상화 기술을 통해 관리, 저장되는 디지털 데이터를 확보함에 있어서는 어려움이 있을 수밖에 없다. 더욱이 클라우드서비스 확산으로 데이터를 생성하는 주체와 저장 및 관리하는 주체가 분리되고, 인터넷을 통한 국경 간 데이터 이전이 자유로운 상황에서 국가 간 사법관할권의 문제는 여전히 존재하고 있기 때문에, 디지털 데이터의 본질과 속성, 그리고 기술방식에 따른 존재양식을 고려하여 새로운 증거확보 방식의 도입을 검토할 필요가 있다고 할 것이다. 따라서 OSP 나 ISP로 하여금 일정 기간 압수수색 대상이 되는 정보를 보전하도록 하는 보전명령제도, 정보주체 또는 정보보관자로 하여금 직접 디지털 증거를 제출하도록 하는 제출명령제도, 시공의 제한이 없는 디지털 정보를 추적하기 위한 온라인 수색, 클라우드 컴퓨팅 환경 내에서의 원격지 압수수색, 전자영장제도 등의 필요성과 기존 법체계와의 관계에서 도입 시 고려해야 할 쟁점, 도입가능성 및 방향 등을 다루어 보고자 한다.

2. 연구내용 및 방법

이에 본 연구내용으로는 첫째, 현행 「형사소송법」상 압수수색 규정과 디지털 증거의 부정합성 문제를 검토해 보고자 한다. 즉 기존 유체물 개념에 근간한 압수수색규정으로 디지털 증거를 포섭하고자 하는데서 비롯되는 문제점과 디지털 기술환경의 변화로 인한 현행 압수수색 방식의 한계 등을 검토하고자 한다. 또한 디지털 증거의 본질과 특성에 부합하지 않는 현행법상의 입법적 흠결을 판례의 해석을 통해 해결하고 있는 현재와 같은 상황에서 초래되는 법적 체계의 불안정성과 법적용의 불명확성으로 인한 절차의 공정성 문제를 논의해 보고자 한다.

둘째, 디지털 증거의 압수수색과 관련된 쟁점별로 판례와 입법안의 변화와 경향성을 분석해 보고자 한다. 즉 디지털 증거 압수수색과 관련하여 지난 20여 년간 발의되어 온 입법안과 대법원 판례의 쟁점과 경향성의 변화를 분석해 봄으로써, 강제수사처분으로서 디지털 증거를 확보함에 있어서 디지털 기술환경의 변화에 따른 법률적 쟁점의 해석방향을 검토함과 아울러 수사절차상 디지털 증거의 확보에 있어서 프라이버시 보호와 실체적 진실의 발견이라고 하는 두 가지 이념의 무게중심이 어떠한 방향으로 가고 있는지 살펴보고자 한다. 이를 토대로 수사절차상 디지털 증거를 확보하기 위해 개정되어야 할 「형사소송법」상 규정의 개정방향을 제시해 보고자 한다.

셋째, 영미법계와 대륙법계 주요 국가인 미국, 영국, 독일, 일본의 경우 디지털 증거 압수수색과 관련된 쟁점들이 무엇이며, 그것들이 어떠한 방향성을 갖고 변화되어 오고 있는지를 판례와 법규정 등을 통해 살펴보고자 한다. 그리고 이러한 디지털 증거 압수수색에 대응하는 주요 국가들의 입법 및 정책의 변화 경향성을 비교 검토해 봄으로써 향후 우리의 디지털 증거 관련 「형사소송법」 및 형사절차의 방향성을 제시하는 데 참고하고자 한다.

마지막으로 디지털 환경의 변화로 인하여 기존의 수사절차 규정과 방식으로는 디지털 증거를 확보하는데 한계에 부딪힐 수밖에 없는데, 이러한 디지털 기술과 환경적 변화에 대응하여 수사절차가 적법하고 공정하게 이루어지기 위해서 새로운 방식의 강제수사처분 도입이 논의될 필요가 있다고 할 것이다. 이에 본 연구에서는 디지털 증거를 확보하기 위한 새로운 강제수사처분방식으로서 보존명령제도, 제출명령제도,

온라인 수색 및 원격지 수색, 역외 압수수색 그리고 전자영장제도의 도입 필요성 및 가능성 등을 검토해 보고자 한다.

제2절 | 현행법상 압수수색 규정과 디지털 증거의 부정합성 문제

1. 압수개념과의 부정합성

현행 「형사소송법」상 압수의 대상은 물건, 즉 유체물로 규정하고 있기 때문에 디지털 정보 자체가 압수수색이 대상이 될 수 있는가에 대해서 논란의 여지가 있어 왔고, 그러한 논의는 입법적 해결이 이루어지지 않는 한 여전히 현재 진행형이라 할 수밖에 없다. 다만 이러한 논의를 일단락 지을 수 있었던 것은 2011년 「형사소송법」을 개정하면서 제106조 제3항에 디지털 증거 압수방법에 관한 규정이 신설되면서 자연스럽게 디지털 증거가 압수의 대상이 될 수 있다는 해석의 방향성을 제시했고, 이를 토대로 현재까지 디지털 증거를 압수해 오고 있기 때문이다.

하지만 디지털 정보가 압수의 대상이 될 수 있는가에 대한 논의에 앞서서 검토되어야 할 부분은 수사의 목적으로 디지털 정보를 수사기관이 취득하는 것을 압수라는 용어로 포섭하는 것이 현실적으로 가능한가 하는 것이다. 즉 압수는 물건의 점유를 취득하는 행위이기 때문에 점유의 이전을 전제로 하는 개념이라 할 수 있다. 하지만 디지털 정보는 출력 또는 복제의 방법으로 이루어지기 때문에 현실적으로 점유의 이전이 발생하지 않는다. 설령 정보저장매체 자체를 압수하는 경우라 할지라도 해당 범죄혐의와의 관련성으로 제한된 정보를 선별하여 복제한 후 다시 반환하는 것이 원칙이기 때문에 그 경우에도 디지털 정보의 점유이전은 생각하기 어려운 개념이라 할 수 있다. 다만 현행법상 디지털 정보를 강제처분에 의하여 수사기관이 확보하고 있는 현실을 포섭할 수 있는 법률상 개념이 존재하지 않기 때문에 압수의 개념을 임의로 확장하여 사용하고 있을 뿐이라고 할 수 있다.

즉 디지털 정보는 그 자체를 압수하는 것이 아니라 범죄혐의를 입증하는 데 있어서 증거로서의 가치가 있다고 인정되는 데이터를 출력, 복제 또는 이미징 방법을 통해

확보하여 법정에 제시하는 것일 뿐, 피압수자의 정보에 대한 점유력을 배제하는 것이 아니기 때문에 근본적으로 디지털 정보 자체는 압수의 대상이 될 수 없다고 할 것이다. 디지털 정보에 대한 압수가 이루어졌다고 해도 피압수자와 수사기관이 동일한 정보를 사실상 공동점유하고 있는 상태이고, 수사기관은 단지 해당 디지털 정보를 법원이 인식할 수 있는 상태로 전환하여 보존하고 있는 것이라는 점에서 볼 때 압수의 개념을 확장하여 해석한다고 하더라도 개념적으로 압수의 범주로 포섭하는 데는 한계가 있다고 할 것이다.

이와 같이 압수개념과 디지털 정보의 부정합성에서도 불구하고 현실적인 입법의 불비로 인해 압수의 개념으로 포섭하고자 한 데에서 디지털 증거에 대한 압수와 관련하여 제문제가 야기되는 것이라 할 수 있다. 즉 압수의 대상이 되기 어려운, 혹은 될 수 없는 디지털 정보를 압수의 목적물로 포섭함에 따라 기존 유체물의 압수에 적용되었던 모든 관련 규정들 역시 디지털 정보에 적용할 수밖에 없고, 그 역시 디지털 정보에 부합하기 어려운 규정이기 때문에 법률이 아닌 법해석으로 해결해야 하는 현실이 수사절차상 디지털 증거의 확보를 둘러싼 복잡한 논의들을 형성하는 가장 근본적인 요인이라 할 것이다. 즉 압수의 대상으로서 디지털 정보를 명시적으로 규정한다고 해서 수사절차상 디지털 증거를 둘러싼 복잡한 논의들이 모두 해소될 수 있는 차원의 문제는 아니라고 할 것이다.

2. 압수수색 방식과의 부정합성

디지털 기술환경은 D(Data: 빅데이터, 분산 클라우드), N(Network: IoT, 6G), A(AI: 기계학습, 양자 ML)라고 하는 핵심기술들의 융복합을 통해 산업과 사회구조를 지속적으로 변화시키고 있을 뿐 아니라, 메타버스 플랫폼을 기반으로 현실과 가상공간을 연결하여 사회경제 및 문화적 활동이 이루어지도록 하고 있다.[1] 즉 디지털 기술의 발전은 기술과 기술, 기술과 사람, 사람과 사람의 연결범위의 확대과정을 가속화시킴으로써 단순히 데이터의 생성, 저장뿐만 아니라 데이터를 가용할 수 있는 공간을

1) 한국지능정보사회진흥원(NIA), "디지털 전환 시대, NIA가 전망한 환경변화 13대 이슈", 『IT & Future Strategey』 보고서 제2호, 2022.5.12, 12-13면.

무한히 확장할 수 있는 환경을 만들어 내고 있다고 볼 수 있다. 또한 이러한 디지털 기술환경은 데이터의 활용가치를 극대화하기 위한 방향으로 나아가고 있기 때문에, 그에 비례하여 데이터보안에 대한 요구 역시 강화되고 있다.

이와 같이 데이터 가용공간의 무한한 확장과 데이터보안의 강화는 텔레그램과 같은 암호통신시스템을 이용하여 또는 순전히 범죄를 목적으로 한 암호통신망을 만들어서 범죄정보를 자유로이 유통시킬 수 있는 환경을 가능하게 만들고 있다. 그런데 여전히 현재 우리의 법제하에서 정보를 확보할 수 있는 수단은 물리적, 장소적 공간을 전제로 한 압수수색과 통신감청 밖에는 없는 상황에서, 초국경적 네트워크를 통해 분산저장되어 있을 뿐 아니라 데이터가 암호화되어 있는 경우에는 이를 증거로 확보하는 데 있어서는 현실적인 한계에 부딪힐 수밖에 없다. 이미 이러한 난제를 해결하기 위해 유럽연합국뿐 아니라 미국과 일본 등은 데이터 보전명령, 제출명령, 온라인 수색, 서비스제공자의 협조의무 등을 이미 부다페스트 협약에 기초하여 국내 이행입법을 마련한 바 있고, 제2 추가의정서의 채택[2]을 통해 인터넷서비스제공자를 상대로 한 직접 정보제공요청, 공조 요청국의 정보제공명령의 강제력 인정, 긴급상황 시 공조절차 등과 같은 규정을 도입함으로써 초국경적 디지털 증거를 효율적으로 확보할 수 있는 방안을 마련하고 있음을 볼 수 있다. 이는 디지털 증거를 확보함에 있어서는 이미 과거의 물리적 수사방식으로는 불가능할 뿐 아니라, 국가 간 신속한 협업 내지 협조 없이는 죄증을 확보하는 것이 불가능할 수도 있다는 위기의식이 전제되어 있는 것이라 할 수 있다.

우리나라도 부다페스트 협약에 가입의향서를 제출[3]하였으며, 2023년 2월 8일 유럽평의회 각료위원회에서 한국에 대한 가입초청이 결정되었고, 6월 26일부터 사이버범죄 협약위원회 총회에 참석하여 사무국과 협약 가입절차를 논하게 되었다.[4] 이를 토대로 국내 이행입법이 제정되는 경우에는 현재와 같은 디지털 증거 압수방식에 있어서의 부정합성은 향후 어느 정도 해결될 가능성이 있다고 할 것이다.

---

2) 부다페스트 협약 제2 추가의정서는 2022년 5월 채택되었지만, 아직 미발효인 상태에 있다.
3) 외교부 보도자료, "사이버범죄협약(일명 '부다페스트협약') 가입의향서 제출", 2022.10.11(https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=372854; 최종접속일 2023.6.25.).
4) 박선정 기자, "(단독) 유럽평의회, '디지털 범죄 국제 공조 협약' 한국 가입 만장일치 찬성", 『법률신문』 2023년 6월 26일자 기사(https://www.lawtimes.co.kr/news/188732; 최종접속일 2023.6.25.).

3. 입법체계와의 부정합성

현행 「형사소송법」상 압수수색규정은 공판상 압수수색에 관한 장에서 공판단계에서의 압수수색 및 검증에 관하여 규율하고 있고, 수사절차를 규정한 장에서는 공판상 압수수색 및 검증에 관한 규정을 포괄적으로 준용하는 방식을 취하고 있다. 즉 실무상 거의 존재하지 않는 법원의 압수수색과 관련해서는 압수수색의 적법성을 담보할 수 있는 절차적인 요건들을 총 30개의 조문에 걸쳐 상세히 규정하고 있으면서, 실제로 압수수색이 이루어지고 있는 수사절차상 압수수색에 관해서는 제215조부터 제218조의2까지 5개 조문으로 구성되어 있고, 적법성 요건으로서는 관련성 규정이 있을 뿐이며, 나머지 압수수색절차와 관련해서는 동법 제219조에 의해 공판상 압수수색에 관한 규정을 준용하고 있는 것이다.

이와 같이 수사기관의 압수수색에 있어서 법원의 직권에 의한 압수수색 규정을 준용하도록 함으로써 절차상 주체와 객체뿐 아니라 규정내용을 법원의 통제를 전제로 한 수사절차에 맞게 변경[5]해서 적용해야 하는 문제로 인하여, 명확한 법규정이 아닌 판례를 통한 법원의 해석에 맡겨지는 결과가 초래되고 있다. 뿐만 아니라 준용규정을 두고 있음에도 불구하고 제출명령규정은 수사절차에는 준용되지 않는다고 해석되는 등, 공개를 원칙으로 하는 재판절차와 밀행성을 기본으로 하는 수사절차의 차이를 고려하지 않은 채 포괄적으로 규정을 준용함으로써 입법체계와 수사절차가 서로 부합하지 않는 문제가 발생하고 있다.

다른 한편으로 수사를 '제2편 제1심'에 규정하고, 총칙에 규정한 법원의 압수수색을 수사절차에 준용하도록 규정하는 현재와 같은 법체계는 법원이 수사절차를 주도하는 것으로 오인하게 할 소지가 있다[6]고도 볼 수 있다. 하지만 이미 디지털 증거 압수수색에 있어서는 법원이 압수수색의 방법을 통제하고 있고, 최근 들어서는 압수수색 영장 사전심문제도를 도입하고 전자증거 압수수색 영장청구 시 검색어를 제한하고자 하는[7] 등 사실상 수사지휘라 할 수 있는 법체계를 갖추고자 하는 상황에서 반드시 오인

---

5) 이동희, "형사소송법의 편장체계 전면개정의 필요성과 개정시론 -일본 형사소송법에 대한 비교검토를 포함하여-", 『비교형사법연구』 제21권 제1호, 한국비교형사법학회, 2019.4, 5면.

6) 허준, "수사절차상 압수·수색 편제 및 절차 개선에 관한 연구", 박사학위논문, 아주대학교, 2020.8, 13면.

이라고만 하기도 어렵다고 할 것이다.

즉 현행법상 압수수색은 공개주의를 원칙으로 하는 공판절차와 밀행성을 기본으로 하는 수사절차가 서로 중첩되는 법체계로 인하여, 과거 시간과 공간이 제한된 형태의 범죄구조를 기본으로 하는 수사절차에서 시공의 제한없이 범죄의 무한 재확산이 가능한 디지털 환경에 부합하는 수사절차로의 전환 자체가 불가능한 상황에 처해 있다고 볼 수 있다. 현재와 같이 공판절차와 수사절차의 근본적인 차이를 무시한 채 절차적 규정을 준용하는 입법체계는 실정법과 현실의 괴리를 야기할 뿐 아니라, 기술의 발전에 따른 수사환경의 변화에 능동적으로 대응하지 못함으로써 오히려 사회적 부정의가 은폐될 수 있다는 우려를 야기할 수도 있을 것이다.

제3절 | 현행법상 디지털 증거 압수수색의 근본적 한계

1. 입법의무의 방기로 인한 입법의 흠결

현재 우리나라의 경우 성문법 국가임에도 불구하고 디지털 증거 압수수색에 있어서 만큼은 마치 불문법 국가인 것처럼 법원의 해석에 의해 수사절차가 좌지우지되는 경향을 보이고 있다. 이러한 기형적인 법적용 및 해석의 문제를 야기하는 가장 주된 요인은 바로 국회가 디지털 증거 압수수색과 관련하여 필요한 법률을 제정하지 않고 있는 데서 비롯된 것이라 할 수 있다.

우리사회에서 수사절차와 관련하여 디지털 증거에 대한 논의가 처음 시작된 것은 1990년대 초반이라 할 수 있는데 – 당시에는 컴퓨터 증거 또는 전자증거로 불렸다 – , 그로부터 30년을 훌쩍 넘어선 현재까지 수사절차의 기본법이라 할 수 있는 「형사소송법」에 제106조 제3항, 단 한 조항만 새로 신설되었을 뿐, 다른 어떤 규정이나 법률도 제정되지 못하였다. 하지만 그 기간동안 IT에 기반한 디지털 기술은 상상을 초월하는

---

7) 법원행정처, “형사소송규칙일부개정규칙안 입법예고”, 『법원행정처공고 제2023-37호』, 2023.2.3 (https://www.scourt.go.kr/portal/legislation/LegislationView.work?pageIndex=1&searchWord=%C7%FC%BB%E7%BC%D2%BC%DB%B1%D4%C4%A2&seqnum=434&gubun=1; 최종접속일 2023. 6.25.). 참조.

수준으로 급속하게 발전해 왔을 뿐 아니라 이미 초연결, 초지능을 토대로 한 디지털 환경이 구축되어 디지털 데이터의 생성량이 하루에 25억 기가바이트에 이르고 있으며, 2025년에는 연간 175제타바이트로 증가할 것으로 예측[8]하고 있다. 또한 150년 안에 비트 수가 지구의 원자 수를 초과함으로써 디지털 정보의 양이 지구 전체보다 더 많은 공간을 차지하게 될 것이라는 경고[9]가 나오고 있는 것이 현실이다.

더욱이 우리나라는 뛰어난 IT 기반 기술을 토대로 디지털 생산량 기준 글로벌 5대강국에 포함[10]될 만큼 방대한 데이터를 생산하고 있는 상황임에도 불구하고, 아날로그에 기반한 법제도를 고수함으로써 법과 현실의 괴리가 점점 더 커져가고 있고, 기술의 발전에 따른 데이터 생성, 관리 및 공유방식의 변화로 인한 디지털 수사환경을 법률로 포섭하지 못한 채 법해석에만 매달리는 현재의 상황에 이르렀다고 할 것이다.

이와 같이 입법의 공백을 판례의 해석으로 대신하게 되면서 디지털 증거의 압수수색과 관련한 사법현실에 있어서 법적용의 일관성은 현저히 뒤떨어지는 상황이라고 할 수 있다. 즉 법원이 디지털 증거의 압수수색과 관련하여 여러 가지 원칙과 기준을 제시하고는 있지만, 그러한 원칙과 기준은 피의자측에 강력한 변호인이 있는 경우에 한해서만 적용된다고 볼 수 있다. 즉 변호인이 없거나 변호인이 있어도 수사단계에서 적극적 대응을 하지 않는 변호사를 선임한 대다수의 형사피의자의 경우에 있어서는 디지털 증거 압수수색에 있어서 수사기관뿐만 아니라 법원도 그러한 원칙이나 기준을 따지지 않기 때문이다. 결국 판례에서 제시하는 디지털 증거 압수수색의 원칙이나 기준은 그것의 시시비비를 가릴 수 있는 능력을 가진 사람에 한하여 적용되는 것일 뿐, 누구에게나 적용되는 원칙이나 기준이 된다고 볼 수 없다는 것이다. 즉 판례에서 제시하는 원칙과 기준이 누군가에게는 권리가 되어 보호해 주지만 그것을 알지 못하는 혹은 알아도 그러한 권리를 누리는 것이 현실적으로 불가능한 누군가에게는 권리로서 기능하지 못한다는 것이다.

---

8) 문광주 기자, "디지털 재앙 "약 200년 후 디지털 정보의 양은 지구 전체보다 더 많은 공간 차지"", 『the SCIENCE plus』 2020년 8월 14일자 기사(http://m.thescienceplus.com/news/newsview.php?ncode=1065579012676159; 최종접속일 2023.6.16.).

9) 문광주 기자, 위의 기사.

10) 조주행, "[데이터로 본 한국인] 데이터 생산 세계 5위 강국이지만… 4차 산업혁명 기대보다 유출 걱정", 『한국일보』 2020년 1월 17일자 오피니언(https://m.hankookilbo.com/News/Read/2020011617473402 15; 최종접속일 2023.6.16.).

물론 디지털 증거 압수수색과 관련하여 수사절차상 필요한 입법안이 국회에 전혀 발의되지 않은 것은 아니었다. 하지만, 2000년부터 2010년까지 10년 동안 디지털 증거 압수수색과 관련해서는 단 2건의 「형사소송법」 개정안이 발의되었으며, 그 가운데 하나가 현재 「형사소송법」 제106조 제3항 신설규정과 거의 유사한 입법안이었지만 임기만료로 폐기되었고, 이후 2011년 6월 30일 사법제도개혁특별위원회안으로 발의되어 현재와 같은 규정이 제정되었다. 이후 2011년부터 다시 10년 동안 디지털 증거 압수수색과 관련하여 발의된 입법안은 7건(사개위안 제외)이었지만 그 가운데 2건은 임기만료로 폐기된 입법안의 내용을 다시 그대로 재발의한 것이었기 때문에 실제로는 5건의 입법안이 발의되었다고 할 수 있다. 발의되었던 5건의 입법안 역시 디지털 증거 압수수색에 필요한 규정의 체계적인 정비를 염두에 두었다기보다는 판례 내용을 반영하여 현행 압수수색 규정의 일부를 수정하는 데 그치고 있음을 볼 수 있다.

이와 같은 국회의 입법의무의 방기도 문제이지만 그와 더불어 법무부 역시 디지털 증거 압수수색과 관련해서는 단 한 건의 정부안도 발의하지 않았다는 사실에 비추어 볼 때, 그러한 입법의 공백을 법원의 법해석으로 채울 수밖에 없었던 현실적 한계를 수긍할 수밖에 없다고 할 것이다.

2. 디지털 기술 환경에 있어서 형사절차 지향점의 전환 – 실체적 진실 또는 프라이버시?

형사소송은 유무죄의 실체판단을 위한 것이기 때문에 그에 이르기 위한 절차적 이념은 실체적 진실의 발견에 있다고 할 수 있다. 하지만 형사절차에서 실체적 진실의 발견만을 추구하는 경우에는 피의자의 인권이 침해될 뿐 아니라 일반국민들의 기본권 조차도 보호받지 못하는 경우가 발생할 수 있다는 것은 이미 오랜 체험으로 지득한 사실이라 할 것이다. 따라서 우리 「헌법」은 제12조에 적법절차 규정을 둠으로써 국가의 형벌권보다 개인의 인권이 우위에 있음을 명시하고 있는바, 국가형벌권 실현의 목표로서 실체적 진실의 발견 역시 이러한 헌법적 요청, 즉 인간으로서의 존엄과 가치 그리고 기본권 존중에서 벗어나서는 안된다고 할 것이다. 즉 형사절차의 궁극적

지향점은 적법하고 공정한 절차에 의한 실체적 진실의 발견이며, 국가형벌권의 실현에 있어서도 기본적 인권을 보장하는 적법절차를 통해서만 이루어져야 한다는 방향에서 형사절차가 형성되어 왔다고 볼 수 있다.

이와 같이 형사절차를 규정하고 해석함에 있어서는 실체적 진실과 적정절차 두 이념의 긴장과 조화가 논의되어 왔었다. 그런데 디지털 증거가 형사절차에 등장하면서부터는 개인의 프라이버시가 형사절차의 적정성을 판단하는 핵심 이념으로 인식되기 시작했다. 즉 디지털 기술이 고도화되어 감에 따라 스마트폰을 매개로 개인의 일상생활뿐 아니라 업무, 의료, 금융 등과 같은 사회경제적 활동들이 가능해지면서 수사절차상 확보가 필요한 디지털 정보 이외의 개인의 사생활 정보가 혼재되어 있는 상황에 처해있기 때문이다. 더욱이 디지털 데이터는 본질적으로 불가시적, 불가독적일 뿐 아니라 클라우드서비스로 인해 그 자체가 분산저장되어 있기 때문에, 관련성이 추정되는 데이터에 대한 검색과정을 거쳐야 비로소 해당 데이터의 증거가치 존재 여부를 확인할 수 있어서 그와 같이 데이터를 선별하는 과정에서 개인의 프라이버시에 대한 침해가 발생할 가능성이 높아졌다고 할 수 있다. 다른 한편으로는 이와 같이 범죄혐의 관련 유관정보와 무관정보를 선별하는 과정에서 별건의 범죄에 대한 혐의가 발견되는 경우도 있어서 소위 '먼지털이식 수사'가 행해질 수 있다는 우려도 배제하기 어렵다고 할 수 있다.

이처럼 디지털 증거 압수수색 과정에서 수사기관에 의한 프라이버시 침해의 우려가 커진 데는 수사기관의 잘못된 수사관행도 하나의 원인이라고 할 수 있다. 즉 우리 수사기관들은 범죄의 증거확보를 위해 과도한 압수수색을 해왔을 뿐 아니라 행위보다는 행위자를 표적으로 삼아 디지털 데이터의 증거 관련성을 판단하는 과정에서 별건의 범죄혐의를 찾아서 기소하는 편법수사를 자주 해왔기 때문이다. 이와 같이 디지털 증거에 대한 과잉 압수수색은 프라이버시 침해를 수반할 수밖에 없어서, 프라이버시를 보호하기 위해 절차적 규정에 대한 엄격한 해석이 행해지고 있는 것이 현실이다. 즉 실체적 진실의 발견도 중요하지만, 개인의 프라이버시 보호도 그에 못지않게 중요하다고 보는 것이 현재 법원의 입장이라고 할 수 있다.

하지만 다른 한편으로 디지털 기술환경이 고도화될수록 범죄를 입증할 수 있는 증거의 은폐 가능성 역시 높아지고 있는 것이 현실이다. 스마트기기를 통해 모든

행위가 이루어지지만 정작 수사절차상 확보해야 하는 증거는 클라우드서비스를 통해 국경을 초월한 네트워크에 분산저장되어 있고, 스마트기기는 게이트 역할만을 하는 경우가 늘어나고 있다. 더욱이 스마트기기 자체의 암호시스템 그리고 저장된 데이터의 암호화가 용이하게 이루어지기 때문에 수사기관으로서는 기존의 압수수색 방식으로는 증거에 접근하는 것조차 불가능한 경우가 발생할 수 있다. 즉 데이터에 접근하고자 하는 수사기관의 위치와 데이터의 저장위치가 단절되어 있어서 압수수색 장소를 특정할 수도 없고, 데이터의 존재형태 또한 추정하기 어렵기 때문에 압수할 데이터를 특정하기도 곤란하며, 경우에 따라서는 압수수색 단계에서 피의자를 특정하는 것조차 어려운 경우도 있을 수 있다. 이러한 기술적 한계를 극복할 수 있는 입법적 대응이 없는 상태에서 디지털 환경에 부합하기 어려운 기존의 적법절차 프로세스를 엄격히 준수하도록 요구하는 경우, 디지털 기술을 이용하여 증거를 은폐하고 범죄를 은닉하더라도 수사기관의 적법절차 프로세스를 우회하거나 또는 수사기관의 대응에 있어서 적법성의 한계를 찾아서 법망에서 벗어날 수 있다는 무언의 가능성을 제공할 우려가 있다고 할 것이다.

물론 프라이버시권은 정보화사회 기술의 발달과 직접적 연관성을 갖는 헌법상 기본권으로, 특히 디지털 기술에 기반한 사회적 환경 내에서는 개인의 삶과 연관된 모든 정보가 정보주체의 의사와 무관하게 제3자의 네트워크에 집적될 뿐 아니라 집적된 정보의 경제적 가치에 따라 이용 또는 공개될 수 있는 환경이 가능해짐으로써 개인의 사생활과 정보를 보호해야 할 필요성이 강화되면서 프라이버시 기본권의 중요성이 두드러지게 되었다고 할 수 있다. 따라서 형사절차에 있어서도 이러한 프라이버시권 보호를 위해 엄격한 적법절차의 해석과 적용이 행해지고 있다고 볼 수 있고, 실체적 진실의 발견 역시 적법절차 내에서의 실체적 진실의 발견이어야 하기 때문에 실체적 진실이 적법절차에 의해 후퇴될 수 있다고도 볼 수 있다. 하지만 형사절차의 이념으로서 적법절차는 단순히 법정절차를 준수해야 하는 것이 아니라 공정한 법정절차를 준수해야 한다는 것을 의미한다[11]고 볼 수 있다. 그런데 디지털 기술환경에 부합하지 않는 법적 절차를 두고 있는 현재의 입법상황에서 해석을 통한 적법절차의 적용이 공정한 절차인가에 대해서는 좀더 고민할 필요가 있다고 할 것이다. 더욱이 디지털

11) 이재상·조균석, 『형사소송법』(제12판), 박영사, 2019, 27면.

성범죄 등과 같이 피해회복이 불가능할 뿐 아니라 피해의 무한 재확산이 가능한 경우에 있어서 프라이버시 보호를 위한 적법절차의 엄격한 적용으로 실체적 진실이 후퇴하는 것이 진정한 의미의 적정절차원칙인가, 그리고 피해자뿐만 아니라 사회 전체적으로도 그러한 적법절차가 공정한 절차인가에 대해서는 생각해 볼 필요가 있다고 할 것이다.

앞으로 더 고도화되어 갈 디지털 기술의 양상을 고려해 볼 때, 형사절차상 디지털 증거에 대응하기 위한 지향점이 실체적 진실과 프라이버시 보호 두 이념 사이 어디에 두어져야 할 것인가, 그리고 두 이념 간의 조화를 위한 선결조건으로서 디지털 기술에 부합하는 적법절차를 어떻게 마련할 것인가가 향후 해결해야 할 과제라 할 것이다.

디지털 증거 압수수색 현황 및 입법적·사법적 변화

탁 희 성

제2장

디지털 증거 압수수색 현황 및 입법적·사법적 변화

제1절 | 디지털 증거 압수수색 현황

현재 우리사회에서 디지털 증거 압수수색을 담당하는 수사기관별 디지털 증거 압수수색 및 분석 현황을 살펴보면 다음과 같다.

먼저 검찰의 경우 지난 10여 년간 디지털 증거 압수수색 및 분석 건수를 살펴보면, 압수수색 건수와 증거분석 건수가 약 2배가량 증가하고 있는 것으로 나타났다. 즉 2012년에 디지털 증거 압수수색 건수는 1,223건이었던 것이 2022년에는 2,692건으로 증가하였으며, 증거분석 건수는 2012년에 4,787건이었던 것이 2016년에 9,766건으로 증가하였다가 2022년에는 6,920건(법정증언 포함)으로 다소 감소하는 현상을 볼 수 있었다.

[표 2-1] 검찰에서 접수·처리한 디지털 증거 수집·분석 실적

(단위: 건)

구분	분석 건수										
	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
압수·수색	1,223	1,230	1,441	1,948	2,142	1,655	2,318	2,847	1,949	1,572	2,692
증거분석	4,787	5,368	6,708	8,179	9,766	9,880	8,819	8,940	6,606	4,712	6,920
기타	55	926	130	1,159	1,262	304	96	78	129	103	
합계	6,065	7,524	8,279	11,286	13,170	11,839	11,233	11,865	8,684	6,387	9,612

* 출처
- 2012, 2013년 : 대검찰청, 『2014 검찰연감』, 2014, 529면.
- 2014년 : 대검찰청, 『2015 검찰연감』, 2015, 576면.
- 2015년 : 대검찰청, 『2016 검찰연감』, 2016, 556면.
- 2016년 : 대검찰청, 『2017 검찰연감』, 2017, 602면.
- 2017년 : 대검찰청, 『2018 검찰연감』, 2018, 453면.
- 2018년 : 대검찰청, 『2019 검찰연감』, 2019, 420면.
- 2019년 : 대검찰청, 『2020 검찰연감』, 2020, 394면.
- 2020년 : 대검찰청, 『2021 검찰연감』, 2021, 420면.
- 2021년 : 대검찰청, 『2022 검찰연감』, 2022, 411면.
- 2022년 : 대검찰청, 사전정보공표대상 자료, "디지털 증거 압수수색, 증거분석 등 지원 현황" (https://www.spo.go.kr/site/spo/ex/announce/AnnounceInfo.do, 최종접속일 2023.6.13.).

2019년까지 지속적으로 증가해 왔던 디지털 증거 압수수색과 증거분석 건수가 2020년부터 감소하는 경향을 보이는 것은 2020년 1월 검경의 수사권 조정과 관련하여 「형사소송법」과 「검찰청법」 개정안이 국회를 통과하면서 검찰의 직접수사 범위가 현저히 축소된 데서 비롯된 현상이라 할 수 있을 것이다.

한편 디지털 증거 압수수색 및 분석 통계에 있어서 매체별 통계는 2012년부터 2015년까지만 확보할 수 있었는데, 그 이유는 2015년 이후로는 검찰에서 별도로 매체별 압수수색 및 분석 건수를 분류하고 있지 않은 데서 비롯된 것이라 할 수 있다. 분석매체 건수를 보면 2012년에 6,650건이었던 것이 2015년에는 2만 2,375건으로 3배 이상 급증하였으며, 압수수색 및 분석 매체 유형별 건수를 보면, PC의 경우 2012년에 316건이었던 것이 2015년에는 8,146건으로 증가하였으며, 스마트폰의 경우에도 2012년에 577건이었던 것이 2015년에는 7,023건으로 증가한 것으로 나타났다.[12] 한편 노트북, USB, 외장 HDD에 대한 압수수색 및 분석 건수는 해마다 약간씩 증가하는 정도에 그친반면, HDD는 감소하는 경향을 나타냈다.

다음으로 경찰의 디지털 증거 분석현황 통계를 살펴보면 2012년에 10,426건이었던 2021년에 75,420건으로 7배 이상 증가한 것으로 나타났다. 디지털 증거분석 매체유형별 건수를 보면, PC, 노트북 등 컴퓨터기기 분석 건수는 2012년에 3,830건에서 2021년 13,311건으로 약 3.5배 가량 증가하였으며, 스마트폰, 휴대폰 등 모바일기기에 대한 분석 건수는 2012년 5,870건에서 2021년 58,563건으로 10배 이상 증가한 것으로 나타났다.

12) 오이석 기자, "스마트폰·USB·컴퓨터는 안다 … 그들의 범죄", 『중앙SUNDAY』 제485호, 2016.6.26 (https://www.joongang.co.kr/article/20221173#home; 최종접속일 2023.6.13.).

[표 2-2] 디지털 증거분석 현황

(단위: 건)

구분	소계	컴퓨터기기 (PC, 노트북 등)	디지털기기 (CCTV, 네비)	모바일기기 (스마트폰, 휴대폰)	파일/기타 (해킹, 암호, DB 등)
2012	10,426	3,830	393	5,870	333
2013	11,200	3,138	483	7,332	247
2014	14,899	3,079	510	10,656	654
2015	24,295	3,357	712	19,526	700
2016	32,281	3,923	794	26,408	1,156
2017	36,060	4,198	867	30,238	757
2018	45,103	6,239	1,065	36,986	813
2019	56,440	7,295	1,412	46,551	1,182
2020	63,935	9,113	1,557	52,479	786
2021	75,420	13,311	2,353	58,563	1,193
전년대비 증가율	17.96%	46.07%	51.12%	11.60%	51.78%

* 출처: 경찰청, 『2021 경찰통계연보』 제65호, 2022.11, 373면.

법원이 지난 10여 년간 전체 압수수색영장 발부 건수의 변화를 보면, 2012년의 경우 107,479건에서 2021년 361,476건으로 약 3배가량 증가[13]한 데 비해, 디지털 증거 압수수색의 경우 검찰과 경찰을 포함해 보면 2012년 16,491건에서 2021년 81,807건으로 약 5배가량 증가한 것을 알 수 있다. 이외에 압수수색 권한을 갖고 있는 공수처, 국세청, 관세청 등의 디지털 증거 압수수색 건수[14]를 포함하면 실제로는 전체 압수수색에 있어서 디지털 증거 압수수색이 차지하는 비중은 훨씬 더 높다고 볼 수 있다. 특히 코로나19 이후 비대면 디지털 전환이 급속히 진행됨에 따라 압수수색 실무에 있어서 디지털 증거의 비중은 더욱 높아질 수밖에 없는 사회, 경제적 환경에 놓여 있다고 할 수 있다.

13) 법원행정처, 『사법연감』, 2012-2021년도 참조.

14) 세 기관의 경우 별도로 디지털 증거 압수수색 관련 통계를 공식적으로 발표하고 있지 않아서 정확한 건수의 파악이 현실적으로 어렵다. 하지만 국세청과 관세청의 경우 별도의 디지털포렌식 팀을 두고 있음을 감안해 볼 때, 디지털 증거의 비중은 훨씬 더 높다고 볼 수 있다.

제2절 | 디지털 증거 압수수색 관련 입법적 변화 및 동향 분석

1. 디지털 증거 압수수색 관련 입법안 발의 현황

형사절차상 디지털 증거의 중요성이 논의되기 시작되었던 2000년부터 현재까지 지난 23년 동안 국회에 발의되었던「형사소송법」일부개정법률안 451건 가운데 디지털 증거 압수수색과 관련해서는 17건의 입법안이 발의된 데 그쳤다. 그나마 2건은 임기만료로 폐기되었던 입법안을 다음 회기에 동일한 내용으로 재발의한 것이었기 때문에 실질적으로는 총 15건의 입법안이 발의되었다고 할 수 있다. 2009년 처음으로 무체물인 정보의 압수 방식에 대한 법적 근거를 마련하고자 발의되었던 입법안(의안번호 1804366)[15]을 시작으로 디지털 증거 압수수색과 관련한 개정안들이 발의되어 왔다. 하지만 IT 기술의 급속한 발전과 더불어 형사절차상 디지털 증거의 압수수색 필요성이 높아짐에 따라 현행법상 압수수색 규정에 대한 개정논의가 지속적으로 제기되어 왔던 데 비하면 정부와 국회의 입법노력은 현저히 낮았던 것으로 보여진다.

그동안 발의되었던 디지털 증거 압수수색 관련 입법안을 내용별로 분류하여 보면 다음과 같다.

2. 디지털 증거 압수수색 관련 입법안 유형

가. 압수 대상으로서 정보에 대한 법적 근거 마련

디지털 증거에 부합하는 압수수색절차를 마련함에 있어서는 무체물인 정보를 압수대상으로 포섭할 수 있는 규정을 마련하는 것이 무엇보다도 우선해야 할 일이라 할 것이다.

이와 같이 압수수색의 대상으로 정보를 포섭하고자 하는 개정안은 2015년에 처음 발의되었으며(의안번호 1913878), 이후 2016년(의안번호 2001352), 2021년(의안번호 2112092), 2022년(의안번호 2114302)에 정보를 압수목적물로 명시하는 개정안이 발의되었지만, 모두 임기만료로 폐기되었다.

---

15) 의안번호 1804366, 형사소송법 일부개정법률안(이주영의원 대표발의), 2009.4.1.

[표 2-3] 압수 대상으로서 정보에 대한 법적 근거 마련안

제안일자	의안번호	대상조문	개정(신설) 내용
2015-02-02	1913878	§106③ 개정	제1항의 증거물 또는 물건에는 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 "정보저장매체등"이라 한다)에 기억된 정보도 포함된다.
2016-08-02	2001352	§106③ 개정	제1항의 증거물 또는 물건에는 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 "정보저장매체등"이라 한다)에 기억된 정보도 포함된다.
2021-08-18	2112092	§106③ 개정	제1항의 증거물 또는 물건에는 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 "정보저장매체등"이라 한다)에 기억된 정보(이하 "전자정보"라 한다)도 포함된다.
2022-01-07	2114302	§106③ 개정	제1항의 증거물 또는 물건에는 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 "정보저장매체등"이라 한다)또는 정보저장매체 등에 기억된 정보도 포함된다.

나. 압수방식의 법적근거 마련

기존의 수사절차상 압수방식은 압수대상이 되는 유체물을 수사기관으로 그 점유를 이전하는 방식으로 이루어졌기 때문에, 디지털 증거의 경우에도 해당 데이터가 저장된 매체를 압수하는 방식을 취하게 되었다. 하지만 데이터가 저장된 컴퓨터나 서버 등 저장매체의 용량이 점차 커짐에 따라 혐의사실과 무관한 정보가 다량으로 혼합되어 있는 상태에서 매체 자체를 압수하는 경우, 개인의 사생활 침해는 물론이고 기업의 영업 자체가 불가능하게 되는 문제가 발생하게 되었다. 따라서 혐의사실과 관련성이 있는 정보에 한정하여 압수하기 위해 출력 또는 복제방식으로 정보를 확보함으로써 개인의 사생활과 기업의 영업활동에 대한 침해를 최소화하고자 입법안이 발의되었고, 이와 같이 "출력·복제 원칙, 매체압수 예외"라고 하는 디지털 증거 압수방식의 법적근거가 2011년 「형사소송법」 개정을 통해 마련되었다.

[표 2-4] 디지털 증거 압수방식에 대한 법적 근거 마련안

제안일자	의안번호	대상조문	개정(신설) 내용
2009-04-01	1804366	§106③ 신설	법원은 압수의 목적물이 정보가 기억된 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체인 경우에는 제1항의 압수를 갈음하여 그 정보를 출력하거나 복제하여야 한다. 다만, 그러한 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정하는 때에는 정보저장매체를 압수할 수 있다.
2011-06-30	1812487	§106③ 신설	법원은 압수의 목적물이 컴퓨터용디스크 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)인 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.

다. 디지털 증거 압수에 필요한 새로운 집행방법에 대한 법적 근거 마련

IT 기술이 발전함에 따라 기존과 같은 단순한 출력이나 복제 또는 매체 압수만으로는 현실적으로 디지털 증거를 확보하는 것이 점차 용이하지 않게 되었다. 즉 디지털 데이터의 특성상 삭제가 용이할 뿐 아니라 휘발성도 강하고, 이에 더하여 데이터를 저장, 이용 및 관리하는 ISP 또는 OSP의 정기적인 데이터 삭제 업무, 스마트기기를 이용한 원격 자동삭제기능 등으로 인해 데이터를 보전하는 것이 수사절차에 있어서 중요한 과제가 되었다. 이와 같이 디지털 증거 압수수색의 한계를 보완하기 위하여 긴급보전명령, 제출명령, 관리자의 협조의무, 원격지 압수수색 등의 방법을 신설하고자 하는 입법안들이 발의되었다.

[표 2-5] 디지털 증거 압수시 필요한 새로운 집행방법에 대한 법적 근거 마련안

제안일자	의안번호	대상조문	개정(신설) 내용
2009-05-13	1804839	§106② 후단 신설	법원은 제1항에 따른 압수의 목적이 컴퓨터용디스크 그 밖에 이와 비슷한 정보저장매체(이하 이조에서 "정보저장매체 등"이라고 한다)에 기억된 정보를 얻기 위한 것이고 그러한 목적을 달성하기 위하여 긴급히 필요하다고 인정하면 해당정보를 보관·관리하고 있는 자에게 관련정보의 보전을 명할 수 있다. 이 경우 보전기간은 필요한 최소한도의 범위 안에서만 하여야 한다.
		§106③ 신설	법원은 압수할 물건을 지정하거나 압수의 목적물인 정보의 저장매체 등에 기억된 정보의 범위를 지정하여, 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다.

제안일자	의안번호	대상조문	개정(신설) 내용
2015-02-02	1913878	§108의2 신설	① 법원은 정보를 압수할 필요가 있는 경우 「정보통신망 이용촉진 및 정보보호등에 관한 법률」제2조 제1항 제3호에 정한 정보통신서비스제공자에게 30일의 범위내에서 당해 정보가 삭제·변경되지 않도록 보존할 것을 서면으로 요청할 수 있다. 다만, 상당한 이유가 있다고 인정되는 경우 30일의 범위내에서 1회에 한해 연장할 수 있다.
		§115의2 신설	③ 압수수색 대상인 컴퓨터 등 정보처리장치와 정보통신망으로 연결되어 있는 정보저장매체 등에 집행대상 정보가 보관되어 있다고 인정할만한 상당한 이유가 있는 경우에는 그 정보를 당해 정보처리장치 또는 다른 저장매체로 이전 또는 복제하거나 이를 출력하는 방법으로 압수수색할 수 있다. 이 경우 당해 정보처리장치 관리자의 권한범위를 초과하여 집행할 수 없다.
		§120의2 신설	① 정보에 대한 압수수색 영장을 집행하는 자는 정보 또는 정보저장매체 등의 소유자·소지자·관리자에게 정보저장매체 등의 작동, 정보통신망으로 연결되어 있는 다른 정보저장매체등에의 접속 기타 필요한 협력을 요구할 수 있고, 협력요구를 받은 자는 부득이한 사유가 없는 한 협력하여야 한다. ② 정보에 대한 압수수색 영장을 집행하는 자는 당해 정보 또는 정보저장매체등의 소유자·소지자·관리자에게 저장된 정보의 범위를 정하여 출력, 복제, 제출하도록 명령할 수 있다.
2016-08-02	2001352	의안번호 1913878과 내용 동일	
2021-02-04	2107939	§216의2 신설	① 검사 또는 사법경찰관은 영상정보, 문자기록 등 정보저장매체에 저장된 전자정보를 확보하기 위한 것으로 증거인멸의 우려가 있거나 전자정보 확보를 위하여 긴급한 경우에는 해당 전자정보에 대한 압수수색검증의 긴급보전조치를 할 수 있다.
2021-08-18	2112092	§120의2 신설	① 전자정보에 대한 압수수색영장을 집행하는 자는 전자정보 또는 정보저장매체 등의 소유자·소지자·관리자(소유자·소지자·관리자가 피고인인 경우는 제외한다)에게 정보저장매체 등의 작동, 그 밖에 필요한 협력을 요구할 수 있다. ② 전자정보에 대한 압수수색영장을 집행하는 자는 전자정보 또는 정보저장매체 등의 소유자·소지자·관리자(소유자·소지자·관리자가 피고인인 경우는 제외한다)에게 전자정보의 범위를 정하여 출력, 복제, 제출을 명할 수 있다.
2022-08-24	2116983	§215의2 신설	① 검사 또는 사법경찰관은 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이조에서 “정보저장매체등”이라 한다)에 기억된 영상정보, 문자기록 등 전자정보를 얻기 위한 것으로 전자정보의 멸실우려 등 미리 압수수색검증영장을 발부받기 어려운 긴급한 사정이 있는 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조 제1항 제3호에서 정한 정보통신서비스제공자(이 이 조에서 “정보통신서비스제공자”라 한다)에게 해당 전자정보가 삭제 또는 변경되지 않도록 보전할 것(이하 이조에서는 “긴급보전조치”라 한다)을 요청할 수 있다. ② 제1항의 긴급보전조치를 요청받은 정보통신서비스제공자는 정당한 사유가 없는 한 해당 전자정보의 보전에 적극 협조하여야 한다.

라. 정보저장매체 정보탐색 관련 통제장치에 대한 법적 근거 마련

1) 매체 압수 시 정보탐색 통제

가) 스마트폰 압수 시 정보탐색에 대한 통제

디지털 기술이 모바일 중심으로 발전함에 따라 스마트폰이 모든 사회경제적 활동과 연계되어 데이터를 생성, 저장, 보관하는 핵심적인 매체가 되었다. 따라서 수사절차상 디지털 증거를 확보함에 있어서 스마트폰 압수가 필수적인 사항이 되었다. 하지만 스마트폰에는 개인의 사생활과 관련된 정보가 대량으로 저장되어 있기 때문에 스마트폰 자체를 압수하는 경우 사생활이 침해될 수 있다는 우려가 제기되고 있다. 이에 대하여 스마트폰 압수 시 저장된 정보의 압수수색에 있어서는 별도의 영장을 발부받도록 함으로써 수사기관에 의한 무분별한 정보탐색을 통제하고자 하는 입법안이 발의되었다.

[표 2-6] 스마트폰 압수 시 정보탐색에 대한 통제 관련 법적 근거 마련안

제안일자	의안번호	대상조문	개정(신설) 내용
2021-06-03	2110539	§215③ 신설	검사 또는 사법경찰관은 압수한 정보저장매체 등을 조사하여 전자정보를 탐색·복제·출력하기 위해서는 별도의 영장을 발부받아 집행하여야 한다.

나) 임의제출한 정보저장매체 압수 시 정보탐색에 대한 통제

현행법상 임의제출한 정보저장매체(스마트폰 포함)의 경우 영장없이 압수할 수 있도록 규정되어 있기 때문에, 수사의 편의상 임의제출 형식으로 정보저장매체를 압수하는 경우가 있다. 하지만 정보의 압수방식에 있어서는 원칙적으로 출력 및 복제가 우선이고, 매체압수는 예외에 해당함에도 불구하고, 임의제출의 형식으로 매체를 압수하는 경우에는 영장에 의한 통제가 없기 때문에 혐의사실과 무관한 정보를 탐색하는 등 과잉 압수수색이 발생할 여지가 클 뿐 아니라 그로 인해 프라이버시가 침해될 여지가 크다고 보아, 임의제출한 정보저장매체 압수 시 정보탐색과정에 대한 통제장치를 마련하고자 하는 입법안이 3건 발의되었다.

[표 2-7] 임의제출한 정보저장매체 압수 시 정보탐색에 대한 통제 관련 법적 근거 마련안

제안일자	의안번호	대상조문	개정(신설) 내용
2019-05-23	2020611	§218① 개정	검사, 사법경찰관은 피의자 기타인의 유류한 물건이나 소유자, 소지자 또는 보관자가 자발적이고 명시적인 동의에 의하여 제출한 물건을 영장없이 압수할 수 있다.
		§218②③④ 신설	② 제1항에 따라 물건을 압수하는 경우에 검사 또는 사법경찰관은 피의자·소유자·소지자 또는 보관자에게 그 제출을 거부할 수 있으며, 제출을 거부할시 어떠한 불이익도 받지 아니함을 미리 고지하여야 한다. ③ 제1항에 따른 압수의 목적물이 컴퓨터용 디스크·이동통신 단말장치, 그 밖에 이와 비슷한 정보저장매체(이하 이조에서는 "정보저장매체등"이라 한다)인 경우에는 검사 또는 사법경찰관은 탐색할 정보의 범위를 정하여 피의자·소유자·소지자 또는 보관자로부터 제출받아야 한다. ④제1항에 따라 정보저장매체 등을 압수한 경우에는 피의자·변호인 또는 피의자가 지정하는 사람을 그 정보를 탐색·저장 또는 복제하는 과정에 참여하게 하여야 한다.
2022-01-07	2114302	§108① 개정	소유자, 소지자 또는 보관자가 자발적이고 명시적인 동의에 의하여 제출한 물건을 영장없이 압수할 수 있다.
		§108②③④ 신설	② 제1항에 따라 물건을 압수하는 경우에 검사 또는 사법경찰관은 피의자·소유자·소지자 또는 보관자에게 그 제출을 거부할 수 있으며, 제출을 거부할시 어떠한 불이익도 받지 아니함을 미리 고지하여야 한다. ③ 제1항에 따른 압수의 목적물이 정보 또는 정보저장매체 등인 경우에는 탐색할 정보의 범위를 정하고 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 소유자·소지자 또는 보관자로부터 제출받아야 한다. ④제1항에 따라 정보저장매체 등을 압수한 경우에는 피고인·변호인 또는 피고인이 지정하는 사람을 그 정보를 탐색·저장 또는 복제하는 과정에 참여하게 하여야 한다.
2023-02-06	2119829	§218② 신설	제1항에 따라 물건을 압수하는 경우에 검사 또는 사법경찰관은 소유자, 소지자 또는 보관자에게 그 제출을 거부할 수 있고 압수의 목적물이 컴퓨터용 디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에는 저장된 정보의 범위를 정하여 출력하거나 복제하여 제출할 수 있음을 미리 고지하여야 한다.

다) 무관정보의 폐기

디지털 증거 압수방식으로서 범위를 정하여 이미징 복제를 하는 경우에도 혐의사실과 관련된 데이터만 선택적으로 복제할 수 있는 것이 아니기 때문에 혐의사실과 무관한 정보도 포함되어 복제되는 경우가 일반적이라 할 수 있다. 더욱이 정보저장매체 자체를 압수하고 임의제출된 매체를 압수하는 경우에는 훨씬 더 방대한 양의 무관정

보가 수사기관의 점유하에 있게 된다고 볼 수 있다. 이러한 무관정보가 수사기관에 지속적으로 집적되고 그에 대한 통제가 이루어지지 않는 경우, 수사기관에 의한 정보의 악용 및 남용 가능성을 배제하기 어려울 뿐 아니라 개인의 사생활의 비밀과 자유가 침해될 가능성이 높다고 할 수 있다. 이러한 위험성을 배제하기 위해서는 수사기관이 확보한 디지털 증거 가운데 범죄혐의와 무관한 정보를 삭제 또는 폐기하도록 할 필요가 있다는 전제하에서 입법안이 1건 발의되었다.

[표 2-8] 수사기관이 확보한 디지털 증거의 무관정보 폐기에 대한 법적 근거 마련안

제안일자	의안번호	대상조문	개정(신설) 내용
2021-04-23	2109697	§218의3 신설	① 검사는 제215조의 규정에 따라 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체에 기억된 정보를 압수한 후 압수된 전자정보가 각 호에 해당하는 경우에는 복원이 불가능한 기술적 방법으로 지체없이 폐기하여야 한다. 1. 수사 또는 재판과정에서 범죄사실과 관련성이 없는 것으로 확인된 경우 2. 압수의 원인이 된 사건에 대한 기소·불기소 등 종국처분에 따라 계속 보관할 필요성이 없다고 인정되는 경우 3. 판결이 확정되어 계속 보관할 필요성이 없다고 인정되는 경우

2) 압수수색 집행 과정에서의 참여권 보장

현행「형사소송법」제121조에 따라 압수수색영장 집행 시 검사, 피고인, 변호인이 참여할 수 있다. 이러한 참여권은 영장집행이 적법하게 이루어지도록 통제하기 위한 것이었지만, 디지털 증거 압수수색에 있어서는 그보다는 수사기관에 의한 무관정보 탐색을 차단하기 위한 절차적 보장장치로서 의미를 둔다고 볼 수 있다. 즉 디지털 증거의 압수수색 과정에 피압수자측의 참여권이 보장되지 않을 경우, 수사기관이 무관정보를 탐색, 복제하여 별건수사의 단서로 활용하는 문제가 발생할 수 있기 때문이다. 이와 같이 디지털 증거에 대한 압수수색절차를 통제하기 위한 수단의 하나로서 참여권을 보다 실효성 있고, 엄격하게 보장하고자 하는 입법안은 5건 발의되었다.

[표 2-9] 압수수색 집행 과정에서의 참여권 보장 대한 법적 근거 마련안

제안일자	의안번호	대상조문	개정(신설) 내용
2014-12-08	1912877	§122 개정	압수수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단, 전자에 규정한 자가 참여하지 아니한다는 의사를 명시한 때 또는 피고인이 증거를 인멸, 은닉, 위조 또는 변조하는 것이 가능하여 압수수색이 실효를 거두기 어려운 때에는 예외로 한다.
2015-02-02	1913878	§115조의3 신설	① 제115조의2 제2항에 따라 정보저장매체등을 압수함으로써 집행을 종료한 때에는 해당 사건과 관계가 있다고 인정할 수 있는 정보에 한정하여 이를 출력 또는 복제하여야 한다. ② 제1항의 경우 정보저장매체 등에 기억된 정보와 해당사건과의 관련성을 판단하기 위해 필요한 때에는 그 정보의 전부 또는 일부를 다른 저장매체로 복제하거나 열람할 수 있다. 이 경우 다른 저장매체로 복제된 정보 중에서 해당 사건과의 관련성이 없다고 인정되는 정보는 그 정보의 소유자, 소지자 또는 보관자에게 반환하거나 이를 폐기하여야 한다. ⑤ 피의자, 변호인 또는 제129조에 규정한 자는 제1항 및 제2항의 과정에 참여할 수 있다.
2016-08-02	2001352	상동	상동
2019-01-28	2018366	§121② 신설	제1항에도 불구하고 압수수색의 목적물이 「전자문서 및 전자거래기본법」제2조 제1호에 따른 전자문서인 경우에는 같은 법 제2조 제3호의 작성자 및 제4호의 수신자, 피고인(이하 이 조에서는 "작성자등"이라 한다)을 압수수색영장의 집행에 참여시켜야 한다. 다만, 다음 각호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. 1. 작성자등이 명시적으로 참여거부의사를 표현한 경우 2. 작성자등의 인적사항이 불명확하거나 소재불명 또는 그 밖에 이에 준하는 사유로 인하여 압수수색 집행에 참여시키기 어려운 경우
2021-08-18	2112092	§121② 신설	검사, 피고인 또는 변호인은 정보저장매체의 반출·복제·탐색, 전자정보의 복제·출력에 이르는 전자정보에 대한 압수영장의 집행에 참여할 수 있다.
2022-01-07	2114302	§115조의3 신설	① 제115조의2에 따라 정보 또는 정보저장매체등을 압수한 때에는 해당 사건과의 관련성을 인정할 수 있는 정보에 한정하여 이를 출력 또는 복제하여 압수하여야 한다. ② 제1항의 경우 정보저장매체 등에 기억된 정보와 해당사건과의 관련성을 판단하기 위해 필요한 때에는 그 정보의 전부 또는 일부를 다른 저장매체로 복제하거나 열람할 수 있다. 이 경우 다른 저장매체로 복제된 정보 중에서 해당 사건과의 관련성이 없다고 인정되는 정보는 그 정보의 소유자, 소지자 또는 보관자에게 반환하거나 이를 폐기하여야 한다. ⑤ 피의자, 변호인 또는 피고인이 지정한 자는 제1항 및 제2항의 과정에 참여할 수 있다.

3. 디지털 증거 압수수색 관련 입법안 분석

가. 입법취지의 변화

2009년 디지털 증거 압수수색과 관련하여「형사소송법」일부개정법률안이 첫 입안된 이후로 현재까지 발의된 입법안들의 제안이유를 살펴보면, 디지털 증거 압수수색에 대한 관점의 변화, 즉 사회적 환경의 변화에 따라 입법의 필요성에 대한 인식이 어떻게 바뀌고 있는지를 알아볼 수 있다.

먼저 2015년 이전에 발의된 디지털 증거 압수수색에 관한「형사소송법」개정법률안의 입법취지를 보면, 개인의 사생활 침해의 최소화와 개인정보보호 또는 자기정보통제권 보장을 위해 발의된 입법안들이 대부분이었다. 즉 우리 사회에 앱 기반의 스마트폰이 보급되고, 이를 이용한 SNS 등이 활발해지면서 기존의 매체 중심의 압수수색 방식으로는 개인의 사생활과 정보를 보호하는데 한계가 있다는 인식이 높아진 데서 비롯된 것이라 할 수 있을 것이다. 2011년 사법제도개혁특별위원회의「형사소송법」개정을 통해 "출력과 복제 원칙, 매체압수 예외"라고 하는 디지털 증거 압수수색 방식의 변화는 이러한 문제의식에서 비롯된 것이라 할 수 있다.

이와 같이「형사소송법」개정을 통한 디지털 증거 압수수색 방식의 명문화는 정보와 매체를 동일시했던 기존의 압수방식을 근본적으로 변화시킨 계기가 되었지만, 압수방식의 변화만으로는 IT 기술의 발전으로 인한 사회적 변화에 대응하는데 있어서 여전히 한계가 발생할 수밖에 없었다. 즉 압수의 대상을 정보 자체로 규정하지 않는 한 여전히 매체 중심적 압수방식에서 벗어날 수 없고, 특히 기술의 발전으로 매체의 저장용량이 기하급수적으로 증가했을 뿐 아니라, 이에 더 나아가 클라우드서비스 도입으로 저장용량 자체가 의미가 없다고 할 수 있는 상황에서 혐의사실과 관련있는 정보를 선택적으로 출력 또는 복제한다는 것은 결코 용이한 일은 아니라고 할 수 있다.

이로 인해 기술의 발전으로 변화하는 디지털 데이터의 존재양식에 부합하지 않는 압수수색 방식을 유지하는 과정에서 야기될 수밖에 없는 피의자 및 피압수자의 권리침해를 최소화하고 방어권을 보장하기 위한 절차적 보장수단의 필요성에 대한 인식이 높아졌다고 할 수 있다. 이러한 측면에서 2015년 이후부터는 수사기관 내 디지털 선별과정에 있어서의 참여권을 구체적으로 명문화하고자 하는 입법안들이 발의되었

으며, 이와 아울러 디지털 증거 압수 시 수사기관의 권한남용에 대한 통제장치의 필요성에 입각한 입법안들이 발의되었다.

하지만 다른 한편으로 디지털 증거 압수수색에 있어서 개인이 디지털 기술을 이용하여 수사기관의 공권력에 대응할 수 있는 상황이 가능해지면서, 2021년 이후로는 신속하고 효과적인 범죄해결 및 범죄예방, 범죄피해의 확산 방지를 위하여 디지털 증거의 신속한 확보 및 보전을 위한 제도적 장치 도입의 필요성을 강조하는 입법안들이 발의되기 시작하였다. 특히 N번방 사건과 같은 디지털 성범죄의 심각성에 대한 사회적 경각심이 높아지면서 중대한 범죄행위에 대해서는 피의자의 권리에 우선하여 국가의 형벌권을 확립하여 범죄자를 처벌하는 것이 중요하다는 인식이 입법에 반영된 것이라고 볼 수 있다. 그럼에도 불구하고 여전히 디지털 증거 압수수색과 관련한 수사실무에서 사생활 침해 및 별건압수 등이 문제가 되면서 사생활의 비밀과 자유의 침해를 제한하고자 하는 입법안들이 여전히 발의되고 있음을 볼 수 있다.

나. 입법 내용의 변화

디지털 증거 압수수색에 관하여 발의된 입법안들이 구체적으로 어떠한 내용을 규정하고자 했는가를 살펴보면, 가장 우선적으로 눈에 띄는 것은 압수대상으로서 정보저장매체 가운데 스마트폰에 대한 압수를 전제로 하여 발의된 입법안들이 증가하고 있다는 것이다. 특히 임의제출된 스마트폰 압수 시 사전고지 및 동의, 정보 탐색 및 복제과정에서의 참여권 보장, 정보탐색을 위한 별도의 영장 발부 등의 규정을 법률에 명시하고자 하는 입법안들이 그것이다. 심지어는 구체적으로 압수대상인 정보저장매체의 범위에 통신단말장치, 즉 스마트폰만을 별도로 명시하고자 하는 입법안[16]도 발의된 바 있다.

이와 같이 스마트폰 압수절차에 대한 통제규정을 명시하고자 하는 것은 서버나 컴퓨터와 같이 이동이 자유롭지 않은 정보저장매체의 경우 압수범위를 정하여 이미징 방식의 복제가 가능한 데 비해, 스마트폰의 경우에는 현장에서 포렌식을 할 수 있는 기술이 부족해서 현실적으로 예외적인 매체 압수에 해당할 뿐 아니라 부분 이미징 자체가 어렵기 때문에 사실상 전체 복제가 이루어지는 것이 일반적이라 할 수 있다.

16) 의안번호 1910402, 형사소송법 일부개정법률안(민현주 의원 대표발의), 2014.4.30.

그런데 스마트폰에는 개인의 사생활뿐 아니라 외부에 공개되어서는 안되는 업무내용까지 담겨져 있는 경우가 있기 때문에 사실상 전체 정보탐색과정에서 또 다른 혐의사실과 관련성 있는 정보가 발견될 가능성도 배제하기 어려울 뿐 아니라 타인에게 공개하고 싶지 않은 개인의 사생활이 수사기관에 노출될 수 있다는 우려도 배제할 수 없는 것이 현실이라 할 것이다. 이와 같이 스마트폰 압수수색 과정에서 혐의사실과 무관한 정보에 대한 수사기관의 접근을 통제함으로써 개인의 사생활과 정보를 보호하고자 하는 입법안들이 발의되고 있다고 볼 수 있다.

다른 한편으로 디지털 증거 압수수색의 한 방식으로서 ISP에 대해 일정한 의무를 부과하고자 하는 입법안들이 발의되고 있다. 이는 기술의 발전으로 데이터의 이용 및 저장이 정보저장매체보다는 매체에 연동된 클라우드 및 웹서버를 통해 이루어지고 있는 것이 일반적이기 때문에 매체 압수만으로는 필요한 정보를 확보하기 어려울 뿐 아니라, 대용량의 데이터 가운데 혐의사실과 관련성이 있는 정보만을 선별하여 압수하는 것이 용이하지 않은 현실을 반영한 것이라 할 수 있다. 따라서 현실적으로 데이터를 관리하는 인터넷 서비스제공자 또는 클라우드서비스제공자들이 직접 혐의사실과 관련된 정보를 선별하여 보전하도록 요구하거나 직접 수사기관에 제출하도록 하는 협력의무 내지 명령을 규정하는 것이 오히려 과도한 개인 및 기업의 정보유출을 최소화 할 수 있는 방안이라는 관점이 반영된 입법안들이 제기되고 있음을 볼 수 있다. 그리고 디지털 증거 압수수색에 있어서 데이터의 특성상 증거의 멸실에 대한 우려, 영장발부 절차로 인한 수사중단 및 피해확산 방지, 범죄혐의의 중대성 등으로 인한 신속한 증거확보의 필요성이라는 관점에서 긴급보전조치제도 또는 영장없는 압수수색제도를 도입하고자 하는 입법안도 발의된 바 있다. 이러한 긴급보전조치 또는 영장없는 압수수색은 영장에 의한 적법절차에 대한 예외에 해당하기 때문에 사후영장에 의한 적법성의 흠결에 대한 보완규정을 두고 있음을 볼 수 있다.

즉 디지털 증거 압수수색과 관련하여 발의되고 있는 입법안들은 디지털에 기반한 사회적 환경이 조성되고 있던 초기에는 사생활과 개인정보보호를 위하여 압수수색절차를 보다 세분화하여 통제하고자 하는 관점에서 법안을 발의하는 경우가 많았다고 볼 수 있다. 하지만 IT 기술이 고도화되고, 디지털 환경이 개인과 기업, 그리고 국가 전반에 걸쳐 갖추어짐에 따라 기술의 발전속도를 따라가기 힘든 공권력만으로는 디지털 증거를

확보하는데 한계가 있다는 인식하에서 디지털 증거를 보다 신속하고도 효율적으로 확보하는 방식이 필요하다는 방향에서 입법안들이 발의되고 있다고 보여진다.

다. 입법 형식의 변화

현행 「형사소송법」상 압수수색 규정은 법원의 압수수색을 총칙편에 규정하고, 수사기관의 압수수색은 법원의 압수수색을 준용하도록 규정하는 방식을 취하고 있다. 하지만 공개재판을 원칙으로 하는 공판절차에서의 압수수색과 실체적 진실을 찾기 위해 신속하되 적법하고 공정한 절차에서 행해져야 하는 수사기관의 압수수색은 주체와 내용, 형식에 있어서 차이가 있을 수밖에 없다. 더욱이 기존의 유체물 중심의 압수수색과는 전혀 차원이 다른 디지털 증거의 압수수색에 있어서도 여전히 법원의 압수수색을 준용하는 방식을 취함으로써 디지털 증거를 확보하는 데 필요한 절차적 수단을 마련하는 데 있어서 한계로 작용하고 있다고 볼 수 있다. 학계에서도 오래전부터 「형사소송법」의 편장체계를 개편하여 공판과 수사를 분리할 필요성이 있다는 문제제기를 해오고는 있지만 여전히 공판절차상 압수수색을 수사절차에 준용하고 있다.

하지만 디지털 증거 압수수색절차에 있어서 사생활 및 정보보호에 입각한 수사절차의 통제 필요성뿐만 아니라 디지털 증거에 부합하는 방식의 압수수색이 요구되고 있다. 이에 따라 디지털 증거 압수수색에 관한 입법안들도 2000년 초반부터 2018년까지는 현행법과 같은 법원의 압수수색 규정을 개정하는 방향에서 입법안이 발의되었음을 볼 수 있다. 하지만 2019년부터 발의된 디지털 증거 압수수색을 위한 「형사소송법」 개정안들은 수사편에 규정된 제215조 이하의 수사기관의 압수수색 규정에 대한 개정안임을 볼 수 있다. 이는 2019년 검경 수사권 조정안이 패스트트랙으로 지정되어 2020년 국회 본회의를 통과함으로써 검찰뿐 아니라 경찰의 독자적인 수사권한이 허용되었을 뿐 공수처의 신설에 따라 수사기관에 대한 통제의 필요성에 대한 인식이 좀 더 강화된 데 따른 것이 아닐까 한다. 혐의사실과 관련된 증거의 은닉과 멸실이 용이할 뿐 아니라 수사기관의 공권력에 대응할 수 있는 기술적 방어가 가능한 디지털 증거를 확보함에 있어서는 그에 부합하는 압수수색 방식을 마련해야 할 뿐만 아니라, 그러한 강제수사의 적정성을 담보할 수 있는 절차적 통제수단을 명확하게 규정할 수 있는

입법형식을 갖추는 것이 앞으로의 디지털 기술환경의 변화에 대응할 수 있는 시작점이 아닐까 한다.

제3절 | 디지털 증거 압수수색 관련 사법적 변화 및 동향 분석

1. 디지털 증거 압수수색 관련 판례 현황

2011년 디지털 증거 압수방식과 관련하여 「형사소송법」이 개정된 이후부터 2023년 현재까지 디지털 증거 압수수색에 관한 대법원 판례 38건을 검색하여 분석해 보았다. 디지털 증거 압수수색과 관련하여 대법원 판례에서 다루어진 쟁점들을 살펴보면, "출력복사 원칙과 매체압수 예외"의 준수 여부, 압수수색 전과정에 걸친 참여권의 적법성 판단, 전자정보 상세목록 교부 여부, 혐의사실과의 관련성 판단기준, 별건 혐의사실에 대한 영장없는 압수수색의 위법성 판단, 무관정보 탐색, 출력 및 복사의 적법성, 영장제시 원칙의 위반 여부, 원격지 압수수색의 적법성, 압수수색영장의 관련성 범위, 임의제출물 압수의 범위 및 관련성 판단기준, 제3자에 의한 임의제출물 압수 시 관련성 판단기준 및 참여권 보장, 무관정보의 폐기 여부 등의 문제가 다루어지고 있음을 알 수 있었다. 이를 쟁점별로 분류해 보면 압수수색 집행절차상 참여권 보장과 관련한 적법성 여부를 다룬 판례가 17건으로 가장 많았으며, 그다음이 전자정보 상세목록 미교부로 인한 적법절차 위반이 10건, 임의제출물 압수의 범위 및 관련성 판단기준과 관련한 판례가 8건, 영장제시 원칙 위반과 관련한 판례가 5건, 혐의사실과의 관련성 판단과 별건 혐의사실에 대한 영장없는 압수수색의 위법성 판단 관련 판례가 각각 4건, 출력복사 원칙과 매체압수 예외의 준수 여부와 원격지 압수수색의 적법성 관련 판례가 각각 3건, 무관정보 탐색, 출력 및 복사의 적법성과 압수수색영장의 관련성 범위, 제3자에 의한 임의제출물 압수 시 관련성 판단기준 및 참여권 보장 관련 판례가 각각 2건, 무관정보 폐기 여부 관련 판례가 1건으로 나타났다.[17] 각 쟁점별로

17) 전체 판례 합계가 38건을 초과하는 것은, 판례에 따라 여러 가지 쟁점들이 함께 다루어진 경우들이 많이 있어서 이를 쟁점별로 분류하여 재정리한 것에서 비롯되었다.

다루어진 논거에 대해서는 뒤에서 다시 정리하고자 한다.

이와 같이 디지털 증거 압수수색의 적법성 판단과 관련하여 여러 가지 쟁점들이 법적 판단의 대상이 되고 있지만, 그 가운데서도 대법원이 디지털 증거에 대한 압수수색 집행의 원칙과 예외를 일관되게 제시하고 있음을 볼 수 있다. 먼저 디지털 증거 압수수색 집행의 원칙으로 제시하고 있는 논거는 다음과 같다.

> "1. 영장발부의 사유로 된 혐의사실과 관련된 부분만 출력 또는 복사할 것.
> 2. 현장사정상 위 방식이 불가능하거나 현저히 곤란한 경우, 매체 자체를 직접 또는 이미징형태로 수사기관 사무실로 반출하여 압수수색할 수 있음.
> 3. 정보저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄혐의사실과 관련된 정보를 탐색하여 해당 정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 하나의 영장에 기한 압수수색 영장집행의 일환에 해당하므로, 그 경우 문서출력 또는 파일복제대상 역시 정보저장매체 소재지 압수수색과 마찬가지로 혐의사실과 관련된 부분으로 한정되어야 함.
> 4. 전자정보압수수색에 대한 예외의 사정으로 매체 또는 복제본을 수사기관의 사무실 등으로 옮겨 복제, 탐색, 출력하는 일련의 과정 역시 압수수색의 일환이므로, 형사소송법 제219조, 제121조에서 규정하는 피압수수색 당사자나 변호인에게 참여의 기회를 보장하고, 혐의사실과 무관한 전자정보의 임의적 복제를 막기 위한 적절한 조치를 취하는 등 영장주의 원칙과 적법절차를 준수할 것.
> 5. 수사기관 사무실 등으로 옮긴 정보저장매체에서 범죄혐의사실과 관련성에 대한 구분 없이 임의로 저장된 전자정보를 문서로 출력하거나 파일로 복제하는 행위는 원칙적으로 영장주의 원칙에 반하는 위법한 압수가 됨."[18]

대법원은 이와 같이 디지털 증거 압수수색 집행절차를 준수하는 것이 적법절차 원칙에 부합하는 것임을 명확히 하고 있지만, 다른 한편 그에 대한 예외가 인정될 수 있는 경우가 있다는 것도 설시하고 있다. 즉 "다만 수사기관의 절차위반행위가 적법절차의 실질적 내용을 침해하는 경우에 해당하지 아니하고, 오히려 그 증거를 배제하는 것이 헌법과 형사소송법이 형사소송에 관한 절차조항을 마련하여 적법절차

18) 대법원 2011.5.26.자 2009모1190 결정; 대법원 2014.2.27. 선고 2013도12155 판결; 대법원 2015.7.16.자 2011모1839 전원합의체 결정 외 다수.

원칙과 실체적 진실규명의 조화를 도모하고, 이를 통하여 형사사법 정의를 실현하려고 한 취지에 반하는 결과를 초래하는 것으로 평가되는 예외적인 경우라면, 법원은 그 증거를 유죄인정의 증거로 사용할 수 있다"[19]고 판시하고 있다.

즉 대법원은 디지털 증거 압수수색에 있어서 절차적 적법성 확보가 무엇보다 중요하지만, 절차의 위반으로 인한 침해의 정도 보다 실체적 진실규명을 통한 형사정의의 실현이라고 하는 공익이 우선하는 경우에는 적법절차 원칙에 대한 예외를 인정할 수 있음을 명확히 하고 있다고 볼 수 있다.

2. 판례에 나타난 디지털 증거 압수수색 관련 쟁점

가. 디지털 증거 압수수색절차상 참여권

1) 참여권의 법적 성질

압수수색절차상 참여권의 법적 근거는「형사소송법」제121조에 규정된 바와 같이 "검사, 피고인 또는 변호인은 압수수색영장의 집행에 참여할 수 있다"는 규정과 제123조에 규정된 공무소, 군사용 항공기 또는 선박, 차량의 책임자와 타인의 주거, 간수자 있는 가옥, 건조물, 항공기 또는 선박차량 등의 주거주, 간수자 또는 이에 준하는 사람에 대한 참여의무 규정이 그것이라 할 수 있다. 그리고「형사소송규칙」제60조에 다른 법원사무관 또는 사법경찰관리의 참여의무 규정이 있다. 이에 비추어 보면 압수수색절차에 있어서 피고인과 변호인의 참여권은 임의적 규정이며, 피의자와 변호인을 제외한 제3자에 대한 압수수색에 있어서는 주거주자, 간수자, 그에 준하는 자와 사법경찰관리의 참여권은 필요적 규정이라고 할 수 있다.

이러한 참여권의 법적 성질에 대해서 헌법재판소는 "압수수색의 사전통지나 집행당시의 참여권의 보장은 압수수색에 있어 국민의 기본권을 보장하고, 헌법상의 적법절차원칙의 실현을 위한 구체적인 방법의 하나일 뿐 헌법상 명문으로 규정된 권리는 아니"[20]라고 하며, 더 나아가 헌법재판소는 "압수수색에 관한 절차의 형성은 입법자의 입법형성권에 속하는 것으로서, …중략… 입법자가 규범체계 전체와의 조화와 압수수

19) 대법원 2014.2.27. 선고 2013도12155 판결.
20) 헌법재판소 2012.12.27. 2011헌바225 결정.

색에 의해 침해되는 기본권의 중요성과 그러한 절차에 의하여 수사의 목적이 제한되는 정도, 수사관행, 우리사회의 법현실 등 제반사정을 고려하여 정할 수 있는 입법재량이 있는 것"이라고 판시하고 있다.

즉 참여권 그 자체가 독자적인 적법절차로서의 지위를 갖는 것이라기보다는 개별 기본권과의 관계에서 비례의 원칙에 따라 평가할 수 있는 권리로서 이해되어야 할 것으로 보인다.

2) 참여권의 범위

대법원은 디지털 증거 압수수색절차상 어느 범위까지 참여권이 보장되어야 하는가에 대해서는 현장에서뿐만 아니라 "예외적으로 정보저장매체 또는 복제본을 수사기관의 사무실 등으로 옮겨 복제·탐색·출력하는 일련의 과정 역시 압수수색의 일환이므로 형사소송법 제219조, 제121조에서 규정하는 피압수수색 당사자나 변호인에게 참여의 기회를 보장해야 한다"고 명시하고 있다.[21]

즉 현장에서 혐의사실과 관련된 증거를 선별하여 그 범위 내에서만 출력 또는 복제한 경우가 아닌 한, 일단 수사기관 사무실로 옮겨서 혐의사실과의 관련성 판단을 위해 탐색이 요구되는 상황이라면 그 과정까지 압수수색 과정에 포함된다고 보기 때문에 탐색 후 출력까지 참여권이 보장되어야 한다고 보는 것이라 할 수 있다. 그리고 대법원은 이러한 참여권을 보장하지 않은 것이 적법절차 위반에 해당하지 않는다고 볼 수 있는 예외적인 사유로, 첫째, 피압수자측이 압수수색 과정에 참여하지 않겠다고 하는 의사를 명시적으로 표시한 경우, 둘째, 참여권 미보장의 절차위반행위가 압수수색 과정의 성질과 내용 등에 비추어 피압수자측에 절차참여를 보장한 취지가 실질적으로 침해되었다고 볼 수 없을 정도에 해당한다는 특별한 사정이 있을 것[22]을 명시하고 있다. 이 두 가지 예외사유에 해당하지 않는 한 압수수색 과정에서 참여권을 보장하지 않은 것은 적법절차 위반으로 압수수색절차 전체를 무효화시킬 수 있다고 보고 있는 것이다.

---

21) 대법원 2011.5.26.자 2009모1190 결정; 대법원 2014.2.27. 선고 2013도12155 판결; 대법원 2015.7.16.자 2011모1839 전원합의체 결정; 대법원 2017.9.21. 선고 2015도12400 판결 외 다수.

22) 대법원 2015.7.16.자 2011모1839 전원합의체 결정; 대법원 2017.9.21. 선고 2015도12400 판결; 대법원 2018.9.13. 선고 2018도8630 판결; 대법원 2019.7.11. 선고 2018도20504 판결.

다만 참여권 보장의 예외요건 가운데 첫 번째는 객관적 판단이 가능한 것인데 비해 두 번째 요건은 주관적 판단이 개입할 수밖에 없다는 점에서 case by case라 할 수 있다. 이와 같이 참여권 미보장으로 인한 절차 위법이 적법절차의 실질적 내용을 침해하지 않는다고 볼 수 있는 특별한 사정이 무엇인가에 대해서 법원은 두 가지 판례에서 그 예를 제시하고 있다. 먼저 "영장집행당시 피압수자가 압수수색절차에의 참여를 포기하거나 거부하겠다는 의사를 표명한 이후 절차가 개시되어 압수수색이 상당부분 진행이 된 상태에서 변호인이 선임된 경우, 이러한 상황에서 변호인에게 참여권을 별도로 고지해야 하는가에 대해서 판례나 수사기관의 내부지침이 없을 뿐 아니라 변호인이 그 과정에 참여를 요청하지도 않은 경우에는, 참여권 미보장으로 인한 절차의 위법이 적법절차의 실질적 내용을 침해하는 경우에 해당하지 않는다"[23] 고 보고 있다. 그리고 또 다른 판례에서는 "디지털 증거 압수수색절차에서 참여권을 보장하는 취지가 무관정보 탐색을 통한 피의자의 프라이버시 침해를 막기 위한 것이라는 점을 고려하여, 별도의 보호가치가 있는 무관정보의 혼재가능성이 없는 정보저장매체의 압수에 있어서는 참여기회를 보장하지 않은 것만으로 증거능력이 부정되지 않는다"[24]고 명시하고 있다.

3) 참여권자의 범위

현행 「형사소송법」상 압수수색절차에 참여할 수 있는 사람의 범위는 제121조의 검사, 피고인 또는 변호인, 제123조의 "공무소, 군사용 항공기 또는 선박·차량의 책임자, 타인의 주거, 간수자가 있는 가옥, 건조물, 항공기 또는 선박·차량의 주거주, 간수자 또는 이에 준하는 사람"이라고 명시되어 있다. 이에 대해 대법원은 "피압수수색당사자 또는 그 변호인"[25]을 참여권자로 명시함으로써 피압수자라는 개념을 사용하기 시작했으며, 이후의 판결에 있어서도 "피압수수색 당사자"라는 용어가 사용되고 있다. 다만, "형사소송법 제219조, 제121조에서 규정하는 피압수수색 당사자"[26]라고 설시하고 있음에 비추어 볼 때, 피고인인 피의자의 참여권 보장이라는 측면에서 피압수수색

23) 대법원 2020.11.26. 선고 2020도10729 판결.
24) 대법원 2021.11.25. 선고 2019도7342 판결.
25) 대법원 2011.5.26.자 2009모1190 결정.
26) 대법원 2015.7.16.자 2011모1839 전원합의체 결정.

당사자라는 개념을 제시한 것이 아닌가 한다. 하지만 디지털 증거 압수수색절차 참여권과 관련하여 모든 대법원 판례가 참여권자를 피압수수색 당사자로 표기하고 있는 것은 아니며, 여전히 "피의자나 변호인에게 참여의 기회를 보장해야 한다"[27]고 설시하고 있는 판례도 존재하고 있으며, 헌법재판소 역시 참여권자를 "피의자 및 변호인"[28]으로 명시하고 있다.

한편 대법원 판례가 압수수색절차에 있어서 참여권자를 피압수자로 해석하게 되면서, 제3자에 의한 임의제출물 압수 시 참여권자의 범위에 압수목적물의 실질적 소유·관리자인 피의자를 포섭하기 위해 "실질적 피압수자"[29]라는 개념이 제시되었다. 그리고 이와 같이 피의자가 실질적 피압수자에 해당하기 위해서는 "첫째, 압수수색과 시간적으로 근접한 시기까지 해당 매체를 현실적으로 지배관리할 것, 둘째, 그 정보저장매체내 정보 전반에 관한 전속적인 관리처분권을 보유행사할 것, 셋째, 자신의 의사에 따라 제3자에게 양도하거나 포기하지 아니할 것"이라는 요건을 제시하고 있다. 즉, 제3자에 의한 임의제출물 압수 시 단순히 피의자라고 해서 참여권이 인정되는 피압수자가 아니라 압수목적이 된 정보저장매체 내에 저장된 정보에 대한 실질적인 소유, 관리, 처분이 가능한 상태에 있어야 피압수자라고 평가할 수 있다고 보고 있는 것이다.[30] 따라서 단순히 압수된 정보저장매체 내 정보에 의해 식별되는 사람으로서 정보의 주체가 되는 자라고 해서 모두 참여권이 인정되는 것은 아니라는 점[31]을 명확히 설시하고 있다.

나. 임의제출물 압수의 적법성

1) 임의제출물 압수의 원칙

임의제출물 압수는 제출이 임의적으로 행해진다는 것일 뿐 압수의 효력은 영장에 의한 압수와 동일하다고 보아야 한다. 따라서 대법원은 디지털 증거를 임의제출하는 경우에 있어서도 "수사기관은 특정범죄 혐의와 관련하여 정보가 수록된 매체를 임의

27) 대법원 2018.2.8. 선고 2017도13263 판결.
28) 헌법재판소 2012.12.27. 2011헌바225 결정.
29) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.
30) 대법원 2022.1.27. 선고 2021도11170 판결.
31) 대법원 2022.1.27. 선고 2021도11170 판결.

제출받아 저장된 정보를 압수하는 경우, 그 동기가 된 범죄혐의사실과 관련된 전자정보의 출력물 등을 임의제출받아 압수하는 것이 원칙"[32]이라고 설시하고 있다. 즉 임의제출된 디지털 증거 압수에 있어서도 「형사소송법」 제106조 제3항의 "출력·복제 원칙, 매체압수 예외" 원칙을 준수해야 한다는 점을 명확히 하고 있다.

2) 임의제출물 압수의 범위

압수수색의 현장상황 또는 저장된 정보의 대량성으로 인한 탐색의 어려움 등의 예외적 사유로 인해 수사기관으로 매체 자체나 복제본을 임의제출 받아 압수하는 경우, 혐의사실과 무관한 정보가 혼재되어 있는 경우가 일반적이라 할 수 있다. 이와 같이 무관정보가 혼재된 매체 또는 복제본을 수사기관에 임의제출하는 경우 압수의 범위를 어떻게 판단할 것인가에 대해, 대법원은 원칙적으로 제출자의 의사를 기준으로 판단할 것을 요구하고 있으며, 따라서 수사기관으로 하여금 임의제출물 압수의 경우 제출자의 의사를 명확히 확인하도록 하고 있다.[33] 그리고 이러한 제출자의 의사는 엄격히 해석해야 하고, 확인되지 않은 제출자의 의사를 수사기관이 함부로 추단해서는 안된다고 판시하고 있다.[34]

하지만 임의제출 시 제출자의 의사가 명확히 확인되지 않는 경우가 존재하기 때문에 대법원은 제출자의 의사가 확인되는 경우와 그렇지 않은 경우로 나누어서 기준을 제시하고 있다. 먼저 임의로 제출한 자가 제출 및 압수의 대상이 되는 정보를 개별적으로 지정하거나 그 범위를 한정하는 경우, "수사기관은 제출자로부터 임의제출의 대상이 되는 정보의 범위를 확인하여 압수의 범위를 특정해야 한다"[35]고 판시함으로써 임의제출에 따른 영장없는 압수수색은 임의제출자의 의사에 종속되어야 한다는 점을 명확히 하고 있다. 그리고 제출자의 의사가 불명확하거나 확인되지 않아서 "제출자의 의사에 따른 정보의 압수대상과 범위가 명확하지 않거나 이를 알 수 없는 경우에는, 임의제출에 따른 압수의 동기가 된 혐의사실과 관련되고 이를 증명할 수 있는 최소한의 가치가 있는 정보에 한해 압수대상이 된다"[36]고 판시하고 있다.

---

32) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.
33) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.
34) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.
35) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.
36) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.

한편 제3자에 의해 임의제출된 정보저장매체를 압수하는 경우에 있어서는 앞서서 기술한 피의자 본인에 의한 임의제출보다도 더 엄격히 해석하도록 요구하고 있음을 볼 수 있다. 즉 "제3자가 피의자의 소유관리에 속하는 매체를 임의제출하는 경우, 임의제출에 따른 압수가 적법하더라도 임의제출의 동기가 된 범죄혐의사실과 구체적, 개별적 연관관계가 있는 전자정보에 한해 압수대상이 되는 것으로 더욱 제한적으로 해석해야 한다"[37]고 판시하고 있다. 이는 정보저장매체의 소유관리 주체인 피의자의 의사와 무관하게 압수됨으로 인해 해당 매체에 혼재된 무관정보로 인해 피의자의 사생활과 인격적 법익이 침해될 수 있다는 우려에서 비롯된 것이라 할 수 있다.

3) 임의제출물 압수 시 관련성 판단기준

앞서 기술한 바와 같이 수사기관이 임의로 제출된 정보저장매체를 압수하는 경우에 있어서도 압수의 범위는 범죄혐의사실과 관련된 정보로 제한되어야 한다. 이러한 관련성에 대하여 대법원은 다음과 같이 판단기준에 대하여 "그 관련성은 임의제출에 따른 압수의 동기가 된 혐의사실의 내용과 수사대상, 수사경위, 임의제출과정 등을 종합하여 구체적·개별적 연관관계가 있는 경우에만 인정되고, 혐의사실과 단순히 동종 또는 유사범행이라는 사유만으로 관련성이 있다고 할 것은 아니다"[38]라고 판시하고 있다. 그리고 범죄혐의사실과의 구체적·개별적 연관관계를 판단함에 있어서는 해당 정보저장매체의 기능과 속성상 "상습성이 의심되거나 피고인의 성적 기호 내지 경향성의 발현에 따른 일련의 범행일환으로 이루어진 것으로 의심되어 범행동기나 경위, 수단과 방법을 증명하기 위한 간접증거나 정황증거로 사용될 수 있는 경우에는 혐의사실과 구체적·개별적 연관관계를 인정할 수 있다"[39]고 판시하고 있다.

다. 별건 혐의사실에 대한 압수수색의 적법성

디지털 증거에 대한 압수수색 과정에 있어서는 정보저장매체의 대용량으로 인하여 범죄혐의사실과 관련된 정보 이외의 무관정보 또는 별도의 범죄혐의와 관련된 정보

---

37) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.
38) 대법원 2021.11.25. 선고 2016도82 판결; 대법원 2021.11.25. 선고 2019도7342 판결.
39) 대법원 2021.11.25. 선고 2019도7342 판결; 대법원 2021.11.25. 선고 2019도6730 판결; 대법원 2022.1.13. 선고 2016도9596 판결.

등이 혼재되어 있을 가능성이 매우 높다. 이러한 특성으로 인해 수사기관은 압수한 정보저장매체 또는 그 복제본에 대한 포괄적 수색을 통해 다양한 범죄혐의와 관련된 정보를 확보하고자 하는 경향이 있다. 하지만 이와 같은 수사기관의 포괄적 수색은 영장주의 원칙에 반할 뿐 아니라 해당 정보저장매체 소유자의 프라이버시 및 인격권에 대한 심각한 침해를 초래하기 때문에 위법수집증거배제 원칙에 따라 그 증거사용이 엄격히 제한되어야 한다.

그런데 정보저장매체의 특성상 대부분의 경우 수사기관에서 탐색과정을 통해서만 범죄혐의사실과 관련성 있는 정보를 추출할 수 있기 때문에, 탐색하는 과정에서 별건의 범죄혐의사실에 대한 정보를 발견하는 경우가 발생할 수 있다. 이와 같이 정보를 탐색하는 과정에서 별건의 혐의사실과 관련된 정보를 발견한 경우 이를 영장없이 압수할 수 있는가, 즉 별건 혐의사실에 대한 압수수색의 적법성을 어떻게 판단할 것인가에 대해서 대법원은 다음과 같은 기준을 제시하고 있다. 즉 "1. 전자정보에 대한 압수수색이 종료되기 전 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우일 것, 2. 더 이상 추가의 탐색을 중단하고 법원으로부터 별도의 범죄혐의에 대한 압수수색 영장을 발부받을 것, 3. 별건 혐의사실 피의자에 대해 참여권을 보장하고, 압수한 전자정보목록을 교부할 것"[40] 등이 그것이다. 따라서 "수사기관이 영장의 범위를 넘어서는 정보를 영장없이 압수수색하여 취득한 증거는 위법수집증거에 해당하고, 사후에 영장이 발부되었다거나 피고인이나 변호인이 이를 증거로 함에 동의했다고 그 위법성이 치유되는 것은 아니"[41]라고 판시함으로써 별건 혐의사실에 대한 압수수색의 적법성 판단에 있어서 사전영장 발부를 필수적 요건으로 제시하고 있음을 볼 수 있다.

라. 원격지 압수수색의 적법성

IT 기술의 발전으로 클라우드 컴퓨팅 서비스가 일반화되면서 기업뿐만 아니라 개인들도 자체적인 정보저장매체보다는 클라우드 컴퓨팅 서비스에서 제공하는 공간에

40) 대법원 2015.7.16.자 2011모1839 전원합의체 결정; 대법원 2018.4.26. 선고 2018도2624 판결; 대법원 2021.11.25. 선고 2016도82 판결.
41) 대법원 2021.11.25. 선고 2016도82 판결.

데이터를 저장하는 것을 당연하게 인식하게 되었다. 이로 인해 스마트폰과 같은 휴대용 정보저장매체는 물론 컴퓨터 등과 같은 정보처리장치들은 사실상 데이터에 접근할 수 있는 게이트의 역할을 하는 것이고, 실질적인 데이터는 클라우드 컴퓨팅 서비스업체에서 제공하는 가상공간 안에 저장되어 있는 것이 현실이라 할 수 있다. 따라서 수사의 목적상 범죄혐의 사실과 관련된 정보를 확보하기 위해서는 클라우드 컴퓨팅 서비스에 접속해야만 한다. 즉 이와 같이 정보통신망으로 연결된 제3자가 관리하는 원격지 서버에 저장되어 있는 정보에 대한 압수수색이 필요불가결한 상황에 직면했음에도 불구하고 입법적 보완이 이루어지지 않고 있기 때문에 현행 압수수색 규정에 대한 법원의 해석을 통해 이에 대응하고 있는 것이 현실이다.

이러한 원격지 압수수색에 대해 대법원은 "수색장소에 있는 정보처리장치를 이용하여 정보통신망으로 연결된 원격지의 저장매체에 접속하는 것이 형소법 제109조 제1항과 제114조 제1항의 규정 즉 영장에 수색할 장소를 특정하도록 한 취지에 위반하여 압수수색 영장에서 허용한 집행의 장소적 범위를 확대하는 것이라고 볼 수 없다"[42]고 판시함으로써 현행 「형사소송법」에 근거하여 원격지 압수수색을 할 수 있을 뿐 아니라 그 수단과 목적에 비추어 사회통념상 타당하다고 인정되는 대물적 강제처분으로 허용될 수 있음을 명확하게 설시하고 있다. 하지만 대법원은 원격지 압수수색이 적법하기 위해서는 다음과 같은 요건을 갖추어야 한다는 것도 함께 제시하고 있다. "1. 영장에 기재된 수색장소에 있는 컴퓨터 등 정보처리장치를 이용할 것, 2. 적법하게 취득한 피의자의 이메일 계정 아이디와 비밀번호를 입력하는 등 피의자가 접근하는 통상적인 방법에 따라 원격지 저장매체에 접속할 것, 3. 그곳에 저장되어 있는 피의자 관련 정보를 수색장소의 정보처리장치로 내려받거나 화면에 현출시킬 것,[43] 영장에 압수할 물건외에 별도로 원격지 서버에 저장된 정보를 특정할 것"[44] 등이 그것이다. 따라서 영장에 기재된 압수할 물건에 컴퓨터 등 정보처리장치에 저장된 정보만 기재되어 있음에도 불구하고 원격지 서버에 저장된 정보를 압수하는 것은 압수의 범위를 넘어선 것으로 적법절차 및 영장주의 원칙에 반하여 위법하다고 보고 있다.[45]

---

42) 대법원 2017.11.29. 선고 2017도9747 판결
43) 대법원 2017.11.29. 선고 2017도9747 판결; 대법원 2021.7.29. 선고 2020도14654 판결.
44) 대법원 2022.6.30.자 2020모735 결정; 대법원 2022.6.30. 선고 2022도1452 판결.
45) 대법원 2022.6.30.자 2020모735 결정; 대법원 2022.6.30. 선고 2022도1452 판결.

마. 영장제시 원칙

압수수색을 하는 경우「형사소송법」제118조에 의거하여 피처분자에게 반드시 영장을 제시해야 하도록 규정되어 있다. 이러한 명문규정이 있음에도 불구하고 여전히 압수수색절차의 적법성 판단에 있어서 여전히 영장제시 원칙의 준수 여부가 논의되고 있는 것은 영장제시 방식에 대한 법원과 수사기관 간의 판단의 차이에서 비롯되는 측면이 있다고 볼 수 있다. 특히 디지털 증거 압수수색절차에 있어서는 ISP나 OSP, 금융기관 등에 대한 압수수색 시 압수에 필요한 정보의 범위를 정해 해당 기관에 요청하게 되면, 해당 기관에서 직접 정보를 출력하거나 복제하여 수사기관에 디지털 방식으로 전달하는 것이 일반적이기 때문에, 수사기관들은 해당 기관에 영장을 팩스 또는 전자적 방식으로 송부하는 방식을 취하게 된다. 이 경우 피처분자에게 제시되는 영장은 원칙적으로 원본이 아니고 사본이기 때문에 법원은 영장원본제시 원칙에 반하는 위법한 절차로 판단[46]하는 경향이 있다. 즉 "수사기관이 금융기관 및 이메일 업체에 대한 압수수색영장을 집행하면서 모사전송 방식에 의하여 영장사본을 전송한 사실은 있으나, 영장원본을 제시하지 않았으므로 헌법과 형사소송법이 정한 절차를 위반하였다"[47]고 판시하고 있다. 하지만 이러한 모사전송 또는 전자적 송수신 방식에 의한 영장사본제시가 해당 기관의 자발적 협조의사에 따른 것이고, 최종 정보선별 후에 영장원본을 제시한 경우에는 영장의 적법한 집행방법에 해당한다[48]고 판시하고 있는 바, 영장사본제시가 피처분자의 요청 등과 같은 자발적 협조에서 비롯된 경우에는 사전영장제시 원칙에 반하지 않는다고 보고 있음을 알 수 있다.

또한 영장원본을 제시한 경우라 할지라도 "영장 첫 페이지와 혐의사실이 기재된 부분만 보여주고, 압수수색 및 검증할 물건, 장소, 사유, 압수대상 및 방법의 제한 등 필요적 기재사항 및 그와 일체를 이루는 부분을 확인하지 못하게 한 것은 적법한 압수수색 영장제시라 볼 수 없다. … 현장에서 압수수색을 당하는 사람이 여러 명일 경우에는 그 사람들 모두에게 영장을 제시하는 것이 원칙이다"[49]라고 판시하고 있는

---

46) 대법원 2017.9.7. 선고 2015도10648 판결; 대법원 2019.3.14. 선고 2018도2841 판결; 대법원 2022.5.31.자 2016모587 결정.
47) 대법원 2019.3.14. 선고 2018도2841 판결.
48) 대법원 2022.1.27. 선고 2021도11170 판결.
49) 대법원 2017.9.21. 선고 2015도12400 판결.

바, 영장제시를 통해 피처분자가 영장집행의 구체적인 내용을 충분히 인지할 수 있도록 함으로써 자신의 침해되는 권리에 대해 방어준비를 할 수 있도록 하는 것이 사전영장제시 원칙을 규정한 근본취지임을 명확히 하고 있다.

바. 무관정보 폐기

디지털 증거 압수수색절차에 있어서 혐의사실과 관련성 있는 정보에 한해서만 압수하도록 법에 규정되어 있기 때문에, 무관정보의 경우에는 피압수자에게 반환하거나 삭제 또는 폐기하는 것이 원칙이라고 할 수 있다. 이와 같이 압수수색 과정에서 수사기관에 의해 확보되어 있는 무관정보의 처리와 관련하여 법원은 다음과 같은 기준을 제시하고 있다. "수사기관이 혐의사실과 관련있는 정보를 선별하여 압수한 후에도 그와 관련이 없는 나머지 정보를 삭제, 폐기, 반환하지 아니한 채 그대로 보관하고 있다면 혐의사실과 관련이 없는 부분에 대해서는 압수의 대상이 되는 정보의 범위를 넘어서는 정보를 영장없이 압수수색하여 취득한 것이어서 위법하다. … 수사기관이 혐의사실과 관련있는 정보만을 선별하였으나, 기술적 문제로 정보 전체를 1개 파일 등으로 복제하여 저장할 수밖에 없다고 하더라도 압수목록이나 정보상세목록에 압수대상이 되는 정보 부분을 구체적으로 특정하고, 이와 같이 파일전체를 보관할 수밖에 없는 사정을 부기하는 등의 방법을 취할 수 있을 것으로 보인다"[50]고 판시하고 있다.

즉 대법원은 영장범위 내에 해당하는 정보를 탐색 및 선별하여 추출한 이후에는 무관정보를 피압수자에게 반환하거나, 삭제 폐기 등의 처분을 하는 것이 원칙이지만, 기술적인 문제, 특히 디지털 증거의 무결성 담보와 관련하여 문제가 발생하여 무관정보를 분리하여 반환하거나 삭제 또는 폐기하는 것이 불가능한 경우에는 압수한 매체 복제본 또는 파일 전체를 보관할 수밖에 없는 사정을 별도로 기재해야만 압수수색의 적법성이 인정된다고 보고 있는 것이다.

---

50) 대법원 2022.1.14.자 2021모1586 결정.

3. 디지털 증거 압수수색 관련 판례의 변화

가. 디지털 증거 압수수색 관련 쟁점의 변화

2011년 5월 26일에 선고된 2009모1190 결정에서 대법원이 디지털 증거 압수수색 영장집행의 적법성 요건으로 "1. 출력복사 원칙, 매체압수 예외, 2. 출력, 복사과정에서 참여권 보장, 3. 혐의사실과 관련성있는 부분에 한정된 출력 및 복사 원칙(무관정보 출력 및 복사 금지), 4. 압수대상 정보목록 작성 및 교부"를 제시한 이후, 이 요건들은 현재까지 디지털 증거 압수수색절차의 적법성을 판단하는 기준으로 자리 잡았다. 그에 따라 수사기관들도 디지털 증거 압수수색에 있어서는 대법원이 제시한 요건들을 최대한 준수하고자 하는 경향이 있기 때문에, 2014년 이후의 판례부터는 대법원이 제시한 각각의 요건들이 구체적인 상황에 따라 어떻게 그 적법성 여부가 판단되어지는가를 보여주고 있다. 즉 참여권과 관련해서는 권리보장 방식과 범위(인적범위와 시간적 범위)의 적법성 여부와 변호인의 참여권 보장 여부가 다루어졌고, 유관정보에 한정된 출력 및 복사 원칙과 관련해서는 혐의사실과의 관련성 범위 및 별건 혐의 관련 정보압수 방식의 적법성 여부, 압수대상 정보목록교부와 관련해서는 목록교부 방식의 적정성 여부 등과 관련해서 법원의 판단이 제시되었다. 한편 이와 같이 대법원 판례를 통해 꾸준히 디지털 증거 압수수색 영장집행의 적법성 요건이 명시적으로 제시되어 왔음에도 불구하고, 최근 들어 2022년과 2023년에 걸쳐 이러한 적법성 요건 위반으로 압수수색절차 자체가 위법한 것으로 판단되는 사례가 지속적으로 나타나고 있음을 볼 수 있다. 이는 디지털 증거 압수수색에 대한 수사기관들의 적법절차 인식의 결여에서 비롯된 것이라고 볼 수밖에는 없다고 할 것이다.

다음으로 디지털 기술의 발전으로 인한 클라우드서비스의 대중화로 디지털기기 자체는 데이터를 생성, 전송, 관리하는 역할을 하고 실질적인 데이터는 클라우드 서버에 저장되는 디지털 환경이 구축되면서, 수사기관의 압수수색 역시 디지털기기 자체보다는 클라우드 서버를 대상으로 할 수밖에 없는 상황에 처하게 되었다. 그로 인해 2017년 처음으로 원격지 압수수색의 적법성 요건에 관한 대법원의 판례[51]가 나오게 되었고, 이후 지속적으로 원격지 압수수색의 적법성 판단과 관련한 대법원 판례가

51) 대법원 2017.11.29. 선고 2017도9747 판결.

나왔으며, 최근 들어서는 특히 영장 내 수색장소 특정의 전제조건으로서 원격지 서버 내 저장정보의 특정이 적법한 압수수색의 필수적 요건[52]이라는 점을 제시한 바 있다.

한편 2020년 이후부터 디지털 증거 압수수색의 적법성 판단과 관련한 대법원 판례들에 있어서 가장 많이 보여지는 주된 쟁점은 임의제출물 압수의 적법성 판단 여부라고 볼 수 있다. 즉 스마트폰을 이용한 불법촬영행위가 빈번해지면서 현행범으로 체포되어 임의제출 형식으로 수사기관에 스마트폰을 제출하거나, 또는 피해자가 직접 피의자의 스마트폰을 수사기관에 제출하는 빈도도 높아지면서 나타나는 현상이라고 볼 수 있다. 이와 같이 임의제출된 스마트기기를 압수하는 경우 제출의 임의성 여부뿐 아니라 제출된 정보의 압수범위, 혐의사실과의 관련성 판단, 참여권 보장 방식 및 대상 등과 관련한 절차의 적법성 판단기준들이 판례에 제시되고 있음을 볼 수 있다. 특히 카메라 등 이용촬영행위로 인한 「성폭력범죄의 처벌 등에 관한 특례법」 위반행위 등과 같은 디지털성범죄에 해당하는 경우에 있어서 대법원은 "불법촬영으로 인한 성범죄 전자정보의 경우 피해자의 인격권을 현저히 침해하는 성격의 정보라는 점, 해당 영상이나 사진 등은 범죄행위로 생성된 몰수대상이라는 점, 그 특성상 불법촬영물의 유통가능성을 신속히 차단하여 피해자를 보호할 필요성이 있다는 점"[53]을 근거로 하여 압수매체 내 정보들에 대한 혐의사실과의 관련성 판단을 넓게 인정하고 있음을 볼 수 있다.

이와 같이 대법원은 판례를 통해 디지털 증거 압수수색절차의 적법성 요건과 판단기준들을 제시해 오고 있다. 다만 디지털 환경과 기술의 변화로 인해 직면하게 될 수밖에 없는 새로운 수사기법에 대한 적법성 판단에 있어서는 여전히 아날로그에 기반한 규정의 해석을 통해 접근할 수밖에 없기 때문에 향후 기술의 발전에 대응하는데 있어서는 한계는 있다고 보여진다. 즉 형사절차에 있어서는 「형법」과 달리 유추해석이 허용되지만 사법적 판단이 입법의 흠결을 이유로 새로운 규정을 창출하는 수준의 해석으로 나아가는 것은 바람직하다고 보기는 어려울 것이다.

---

52) 대법원 2022.6.30.자 2020모735 결정.
53) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.

나. 디지털 증거 압수수색의 적법성 판단기준의 변화

디지털 증거 압수수색절차의 적법성과 관련하여 대법원이 판단하는 논거의 변화를 살펴보면, 초기에는 절차의 공정성 확보와 피압수자인 피의자의 기본권 보호를 위한 절차적 권리의 보장이라는 관점에서 적법성 여부에 대한 판단이 이루어졌다고 보여진다. 따라서 수사의 목적을 달성하려는 공익과 압수수색과 관련한 피의자의 절차적 권리 사이의 균형을 고려하여, 적법절차 원칙과 실체적 진실규명의 조화를 도모하고자 했음을 알 수 있다. 이러한 관점에서 압수수색절차상 피압수자의 참여권에 대해서도 절차의 공정성과 피의자의 방어권이라는 점에서 보장되어야 할 권리이지만, 그 자체가 헌법적 권리가 아닌 적법절차 실현을 위한 입법적 수단의 하나라는 점을 명확히 설시하고 있음을 볼 수 있다.

그런데 디지털 환경의 변화와 기술의 발전으로 정보의 양이 기하급수적으로 증가하게 되면서 압수수색절차상 수사기관이 불가피하게 직면할 수밖에 없는 방대한 정보 가운데 결코 타인에게 공개되거나 침해되어서는 안 되는 개인의 인격권 및 사생활에 관한 정보가 포함될 수밖에 없게 되었다. 이에 대하여 법원은 개인의 정보를 보다 더 강하게 보호해야 할 필요성이 있다는 인식하에 "정보에 대한 압수수색은 인격권, 사생활의 비밀과 자유, 정보에 대한 자기결정권, 재산권 등을 침해할 우려가 크므로 포괄적으로 이루어져서는 안되고, 비례의 원칙에 따라 필요 최소한의 범위 내에서 이루어져야 한다"[54]고 판시함으로써, 개인정보 보호의 근거로서 인격권, 사생활 보호뿐만 아니라 정보자기결정권과 재산권까지 제시함으로써 정보에 대한 압수수색을 엄격한 기준에 따라 제한하고자 함을 알 수 있다. 이러한 기준에 따라 원격지 압수수색에 있어서도 영장 내 수색장소에 있는 정보저장매체 내 정보의 특정뿐 아니라 원격지 서버에 저장되어 있는 정보의 특정도 적법성 판단의 요건이 됨을 명시하고 있음을 볼 수 있다. 마찬가지로 임의제출물 압수에 있어서도 유관정보와 무관정보의 혼재가능성을 전제로 혐의사실을 증명할 수 있는 최소한의 가치가 있는 정보에 한하여 압수가 허용된다고 함으로써, 무관정보 탐색으로 인해 야기될 수 있는 피의자의 인격권 및 프라이버시 침해를 최대한 막고자 하는 의도를 찾아볼 수 있다.

---

54) 대법원 2017.11.14. 선고 2017도3449 판결.

즉 디지털 정보의 생성, 이용, 저장 및 관리가 개인에 의해 이루어졌던 환경하에서는 정보의 양이 어느 정도 제한적이었기 때문에 형사절차에 있어서도 절차의 공정성이라는 측면에서 적법절차의 준수가 요구되었다고 한다면, 그와 같은 정보의 생성, 이용, 저장 및 관리가 기업형 서비스를 통해 이루어지고 있는 현재의 상황하에서는 정보의 양에 있어서 거의 제한이 없을 뿐 아니라 정보의 유형도 기본적인 일상생활 외에 금융, 의료, 보안 등과 같이 타인에 의해 공개되거나 침해되어서는 안되는 정보들이 포함되어 있기 때문에 절차의 공정성보다는 오히려 프라이버시 보호라는 측면에서 적법절차의 준수가 훨씬 더 강하게 요구되고 있는 것이라고 보여진다.

주요 외국의 디지털 증거 압수수색 관련 쟁점의 변화 및 경향성 분석

박중욱 · 손여옥 · 이순옥

제3장

주요 외국의 디지털 증거 압수수색 관련 쟁점의 변화 및 경향성 분석

제1절 | 독일의 디지털 증거 압수수색 관련 규정 및 쟁점, 판례의 변화와 경향성

1. 서론

정보통신기술의 발전에 따라 형사절차에서 디지털 증거가 중요해지고 수사기관의 과도한 개인정보 수집이 문제되었던 것은 독일 또한 마찬가지이다. 오늘날의 정보기술환경에서 수사절차에서 발견되는 정보저장매체에는 대부분 범죄혐의와 관련된 정보(이하 "유관정보")와 그렇지 않은 정보(이하 "무관정보")가 혼재되어 있으며, 이는 정보가 개인의 단말기에 저장되어 있는 경우뿐만 아니라 기업·기관·단체나 통신서비스제공자(이하 "ISP/CP")의 서버에 저장되어 있는 경우에도 마찬가지이다. 하지만 디지털 정보의 특성상 대부분의 경우 유관정보와 무관정보는 압수수색의 집행 현장에서 즉시 구분되지 않는다. 이에 따라 수사기관은 실무에서 단말기나 서버 등의 정보저장매체에 저장된 정보를 일단 포괄적으로 열람 내지 수집하고자 하며, 이런 수사행위는 효과적인 형사소추라는 공익적 측면에서 불가피하게 요구된다. 반면 수사기관의 디지털 정보에 대한 포괄적인 접근 내지 확보는 거의 언제나 주거의 불가침(독일 기본법[Grundgesetz, 이하 "GG"] 제13조[55]), 편지·우편·통신의 비밀(GG 제10조[56]), 일반적

55) GG 제13조 [주거의 불가침(Unverletzlichkeit der Wohnung)] ① 주거는 침해될 수 없다. ② 수색은 법관에 의해서, 지체의 위험이 있는 경우에는 법률이 정한 다른 기관에 의해서 명령될 수 있으며, 법률에 규정된 방식으로만 집행된다.

56) GG 제10조 [편지·우편·통신의 비밀(Brief-, Post- und Fernmeldegeheimnis)] ① 편지의 비밀 및 우편·통신의 비밀은 침해될 수 없다. ② (제1항 비밀의) 제한은 법률에 근거해서만 명령될

인격권(GG 제1조 제1항과 결부된 GG 제2조 제1항[57]) 등의 기본권에 대한 중대한 침해를 야기하고, 나아가 불가침인 '사적 생활형성의 핵심영역(Kernbereich privater Lebensgestaltung)'[58]에 대한 침해로까지 이어질 수 있다. 따라서 수사기관에 의한 형사소추 목적의 정보수집은 법치국가 원칙 및 이것으로부터 도출되는 비례성 원칙에 따라 필요 최소한의 범위로 제한되어야 하고, 이를 위해 그 정보수집의 수권규범, 즉 처분요건과 절차법적 통제장치는 처분의 기본권 침해강도에 비례하도록 형성되어야 한다: "기본권 침해의 법률유보와 비례성 원칙".

이러한 전제 아래 독일에서는 디지털 증거의 확보를 위한 수권규범, 즉 수사상 증거확보의 기본적이고 전형적인 처분인 압수수색을 비롯한 통신감청 등의 비밀의 정보수집을 위한 법적 근거가 헌법적으로 정당화되기 위해서는 개별적으로뿐만 아니

수 있다. (제1항 비밀이) 연방이나 주의 존립이나 안전 또는 자유민주주의적 기본질서의 보호를 위해 제한되는 경우, 당사자에게 그 제한을 (사전이나 사후에) 통지하지 않을 것, 그리고 재판청구 대신에 의회가 구성한 기관 및 보조기관을 통해 그 제한에 대해 사후심사할 것을 법률로 정할 수 있다. [③ 내지 ⑦ 생략]

57) GG 제1조 [인간의 존엄, 인권, 기본권에의 구속(Menschenwürde, Menschenrechte, Rechtsverbindlichkeit der Grundrechte)] ① 인간의 존엄은 침해될 수 없다. 그 존중과 보호는 모든 국가권력의 의무이다.
GG 제2조 [인격적 자유권(Persönliche Freiheitsrechte)] ① 누구든지 타인의 권리를 침해하지 않으면서 헌법질서나 도덕률을 침해하지 않는 한 자신의 인격을 자유롭게 발현할 권리를 가진다.
※ '일반적인격권(Allgemeines Persönlichkeitsrecht)'은 독자적인 기본권이면서, 동시에 흠결 없는 기본권 보호를 위해 – 특별 자유권들에 대한 – 소위 '보충적 기본권'으로서 역할을 하는 넓은 의미의 일반적인 행동의 자유를 보장한다(*Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 7, 15, 21). 독일 연방대법원(Bundesgerichtshof, 이하 "BGH")과 독일 연방헌법재판소(Bundesverfassungsgericht, 이하 "BVerfG")는 독일연방공화국(Bundesrepublik Deutschland, 이하 "BRD") 초기부터 이미 여러 판결을 통해 위 보장으로부터 '독자적인 특별 자유권'을 도출하였고(*BVerfGE* 141, 186, 201 [Rn. 32]; *Di Fabio,* in: Maunz/Dürig, GG-K, Art. 2 Ab. 1 Rn. 127), 대외적이고 인격적인 자기표현의 이용에 대한 자기결정의 권리를 기본권적으로 보호하기 위해 GG 제1조 제1항과 결부된 GG 제2조 제1항에 근거하여 '일반적인격권'을 헌법상 보장되는 독립된 기본권으로 인정하였다(*BGHZ* 13, 334, 338; 27, 1, 7 f.; 27, 344, 351; 32, 373, 378 f.; 34, 238, 247; 72, 155, 170 [Tz. a)]; *Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 127 ff.). 한편 BVerfG는 이 일반적인격권에 근거하여 1983년의 인구조사 판결(*BVerfGE* 65, 1)에서는 '정보자기결정권(Recht auf informationelle Selbstbestimmung)'을, 2008년의 온라인 수색 판결(*BVerfGE* 120, 274)에서는 'IT-기본권(IT-Grundrecht)'을 독립된 기본권으로 창설하였다.

58) BVerfG는 BRD 초기의 판결부터 지금까지 지속적으로 GG의 각 기본권 규정과 결부된 제1조 제1항에 근거하여 시민에게는 '사적 생활형성의 불가침의 핵심영역', 즉 공권력의 전개에서 벗어나 절대적으로 보호되는 영역이 인정되고 절대적으로 보호되어야 한다는 점을 강조한다(*BVerfGE* 6, 32, 41; 27, 1, 6; 34, 238, 245; 80, 367, 373; 109, 279, 313; 113, 348, 390; 120, 274, 335; 124, 43, 69 m.w.N.). 따라서 사적 생활형성의 핵심영역 보호는 기본적으로 헌법적 차원의 인격권 보호의 한 내용이다. 다만 독일의 입법자는 2017년에 온라인 수색을 도입하는 법률 개정에서(아래 각주 5) StPO 제100조d를 신설함으로써 동 핵심영역 보호를 위한 처분의 집행 단계에 따른 절차법적 조치를 구체적으로 규정되었다.

라 법체계적으로 어떻게 형성되어야 하는지가 문제되었다. 이 논의는 크게 두 가지 쟁점으로 구성된다. 먼저 하나는 오늘날의 정보기술환경에서 압수수색 일반규정, 즉 독일 형사소송법(Strafprozessordnung, 이하 "StPO") 제94조 이하와 제102조 이하의 규정에 따른 – 단순 – 압수수색에서도 많은 경우 불가피하게 개인정보가 포괄적으로 수집되는데, 절차법적으로 기본권 보호를 위해 이를 통제하기 위한 방법은 무엇인가이다. 여기서는 StPO 창설시부터 존재하였던 StPO 제110조의 해석·적용, 특히 임시확보와 열람의 법적 성격 및 참여권의 인정 여부가 검토될 필요가 있다. 다른 하나의 쟁점은 수사기관의 증거확보를 위한 처분 중 '처분 당사자 모르게', 즉 '비밀로' 행해지는 압수수색 내지 정보수집은 헌법적으로 어떻게 정당화될 수 있는가이다. 이는 비밀의 압수수색 내지 정보수집을 위한 수권규범은 비례성 원칙과 법체계적 측면에서 통신감청 등 기존의 비밀의 강제처분을 위한 수권규범의 처분요건 및 절차법적 통제장치를 고려할 때 어떻게 형성되어야 하는가의 문제이기도 하다. 다만, 여기서는 비밀의 압수수색이나 정보수집이 ISP/CP의 서버에 저장된 정보를 대상으로 하는지, 아니면 스마트폰이나 PC 등의 개인 정보저장매체를 대상으로 하는지에 따라 구분된다. 전자와 관련하여 독일의 입법자는 압수수색 일반규정에 의해서는 공개의 처분만이 허용된다는 BGH와 BVerfG의 견해에 따라 수사기관이 피의자 아닌 자, 특히 ISP/CP의 서버에 저장된 정보를 압수수색하는 경우에 있어서 – 주로 피의자인 – 정보주체에 대한 통지를 유예하거나 배제하기 위한 요건을 2021. 6. 25.의 개정(이하 "2021년 개정")[59]을 통해 StPO 제95조a에 신설하였다. 후자는 소위 '온라인 수색(Online-Durchsuchung)'과 관련된 것으로서 BVerfG는 이미 2008. 2. 27.의 소위 '온라인 수색 판결'[60]에서 동 처분의 합헌성 및 헌법적 정당화 요건을 자세히 설시하였다. 하지만 이 판결에도 불구하고 독일에서는 온라인 수색이 수사목적을 위한 처분으로 도입되는 것이 타당한지에 대해 상당한 견해의 대립이 있었다. 결국 독일의 입법자는 2017. 8. 17.의 개정(이하 "2017년 개정")[61]을 통해 StPO 제100조b, d, e에 수사목적 온라인 수색의 수권규범을 신설하였다.

---

59) Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 25. Juni 2021, BGBl. I S. 2099.

60) *BVerfGE* 120, 274 = NJW 2008, 822.

61) Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017, BGBl. I S. 3202.

한편 독일은 유럽평의회(Council of Europe)의 회원국으로서 사이버범죄 협약(Convention on Cybercrime, 이하 "CCC")의 협약국이기도 하다.[62] 독일은 CCC의 비준을 위해 그 내용을 국내에 반영하기 위한 이행 입법을 행하였으며, 절차법과 관련된 내용은 2007. 12. 21.에 의결되어 2008. 1. 1.에 발효된 전기통신감청법(TKÜG)에 의한 개정(이하 "2007년 개정")[63]을 통해 국내법에 반영되었다.[64] 이 개정 당시에 독일에서 가장 크게 다투어진 부분은 혐의 없는 예방적인 교신데이터[65]의 수집·보관·이용을 위한 수권규범의 법적 형성이었지만((舊) 전기통신법[Telekommunikationsgesetz, 이하 "TKG"] 제113조a, b와 StPO 제100조g), 본 글의 주제와 관련된 것은 원격 압수수색을 위한 법적 근거의 창설이다(StPO 제110조 제3항). 나아가 유럽평의회는 최근인 2022. 5. 12.에 사이버범죄에서 국제형사사법공조가 좀 더 신속하게 이루어지도록 하는 CCC 제2 추가의정서(이하 "추가의정서")를 채택하였다.[66]

---

62) CCC는 2001. 11. 23.에 헝가리 부다페스트(Budapest)에서 의결되어(소위 '부다페스트 협약'), 2004. 12. 1.에 발효되었고, 독일은 동 협약을 2007. 11. 16에 비준하였으며, 2009. 3. 9.에 비준서를 기탁하였다. CCC의 창설은 사이버범죄가 전통적인 범죄와 달리 국경을 초월하여 행해지며 그 증거 또한 국경을 가리지 않고 존재한다는 점 때문에 동 범죄에 대한 형사적 대응을 위해서는 동일한 규정이 각 국가에 마련되어 있어야 하고 각 국가 간의 원활한 국제사법공조가 필수적이라는 점에 기인한다.

63) Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (TKÜG) vom 21. Dezember 2007, BGBl. Ⅰ S. 3198.

64) 독일의 CCC 비준 절차와 이행 입법과 관련된 자세한 내용은 박희영 외 2인, 『사이버범죄협약 이행입법 연구』, 연구용역보고서, 대검찰청, 2015.12, 157면 이하 참고.

65) 교신데이터(traffic data; Verkehrsdaten)는 우리 「통신비밀보호법」(이하 "통비법") 제2조 제11호의 '통신사실확인자료'에 상응하는 정보이다.

66) 유럽평의회(Council of Europe) 홈페이지, "Details of Treaty No.224"(https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224; 최종접속일 2023.9.15.). 이 추가의정서는 2001년에 만들어진 CCC의 형사사법공조 절차가 복잡하고 시간이 많이 소요되어 비효율적이라는 지적을 배경으로 기존 수사공조절차를 개선하기 위한 것이다. 그 자세한 내용은 박재성, "사이버범죄 국제조약의 동향 - 부다페스트 협약 제2 추가의정서 및 유엔 사이버범죄 조약을 중심으로 -", 『저스티스』 통권 제185호, 한국법학원, 2021.8, 246면 참고. 추가의정서는 효율적인 수사공조 및 그 남용방지와 인권보호를 규정하고 있는데, 전자와 관련한 주요 내용은 다음 3가지이다. 첫 번째로, 한 협약국의 관할관청(주로 수사기관)은 다른 협약국(정부)을 거치지 않고 그 고권 내에 있는 서비스제공자에게 직접 '도메인 네임 등록 신청자의 이름, (실물) 주소, 이메일 주소, 전화번호와 같은 정보' 및 저장된 '가입자정보'의 전달을 요청할 수 있다(제6조와 제7조). 두 번째로, 한 협약국의 관할관청(주로 법원)은 다른 협약국(정부)에게 그 고권 내에 있는 서비스제공자에게 저장된 가입자정보와 교신데이터를 제출하도록 하는 명령을 집행하도록 요청할 수 있다(제8조). 세 번째로, '인간의 생명이나 안전에 대한 상당하고 직접적인 위험이 존재하는 경우'('긴급상황'), 한 협약국의 관할관청은 형사사법공조의 절차를 거칠 필요 없이 CCC 제35조에 따른 상시적인 접속창구(point of contact)를 통해 다른 협약국에 있는 서비스제공자에게 가입자정보, 교신데이터, 내용데이터 등 저장된 컴퓨터데이터의 지체 없는 전달이 가능하도록 협조를

본 절에서는 먼저 StPO의 압수수색 일반규정의 전반적인 내용이 처분요건과 절차법적 통제장치를 중심으로 검토될 것이다(뒤의 2). 이때 디지털 정보 자체의 압수대상성에 대한 독일에서의 논의 및 증거확보를 위한 여러 유형의 수사처분에 대한 수권규범을 규정하는 StPO 제1편 제8장의 규범체계가 함께 검토될 것이다. 이어서 디지털 정보에 대한 압수수색에서 포괄적인 정보수집을 통제하기 위한 수단 내지 절차로서 – 규범적으로 – 그 활용이 요청되는 StPO 제110조가 자세히 검토될 것이다(뒤의 3). 여기서는 동 규정의 입법취지와 적용범위 이외에 수색 과정에서의 피압수자의 참여권 및 원격 압수수색에 관한 논의가 함께 다뤄질 것이다. 다음으로 서버나 단말기 등 정보저장매체에 저장된 정보의 '비밀의' 수집을 위한 허용요건이 앞에서 살펴본 StPO 제1편 제8장의 규범체계를 전제로 검토될 것이다(뒤의 4). 여기서는 BVerfG가 최근 자신의 판결·결정에서 반복해서 요구하는 정보 수집·처리·이용에서의 투명성 요청 및 이에 근거한 비밀의 강제처분의 허용요건들이 검토된 후, 이에 근거하여 신설된 StPO 제95조a 및 제100조b, d, e의 주요 내용이 검토될 것이다.

2. 독일 형사소송법(StPO)의 압수수색 관련 규정

가. 압수수색 일반규정의 개관

1) 압수: StPO 제94조 내지 제98조

StPO 제94조는 '증거물의 확보와 압수'라는 표제로 형사절차에서의 증거물 확보의 유형과 요건 및 압수에 대해 규정하고 있고, StPO 제95조는 '제출의무'라는 표제로 증거물의 제출강제에 대해 규정하고 있다(아래 가)).[67] StPO 제98조는 '압수절차'라는 표제 아래 압수의 절차법적 통제장치인 법관유보를 규정하고 있다(아래 나)).

요청할 수 있다(제9조). 마지막에 언급된 추가의정서 제9조의 내용은 원격 압수수색의 대상물이 해외 서버에 있는 경우인 역외 압수수색이 제한적인 요건 아래에서 허용될 수 있도록 하는 규정이다(후술).

67) 이어서 StPO 제96조는 '관청에 보관된 문서'의 수집 제한을, StPO 제97조는 증언거부권자 등의 증언거부권을 보장하기 위한 '압수금지물'을 규정하고 있다. 이 두 규정은 본 글의 쟁점과 직접적인 연관이 없으므로 별도로 다루지 않는다. 한편 2021년 개정을 통해 신설된 StPO 제95조a는 뒤의 3.에서 다룰 것이다.

가) 용어의 개념 및 압수의 실체적 요건

(1) 용어의 개념과 그 관계: 유치, 확보, 압수, 제출 요청과 강제

StPO 제94조 제1, 2항[68]과 제95조[69]에는 형사절차에서의 증거물 획득을 위한 공권력의 행사와 관련된 몇 가지 용어가 등장한다. 각 용어의 개념 및 그들 간의 관계에 대한 독일의 지배적인 견해에 따르면 상위개념은 '확보(Sicherstellung)'이며,[70] 이 개념 아래 '형식 없는 확보(formlose Sicherstellung)'로서 '관청의 유치(amtliche Verwahrung)'와 '기타 방법의 확보(Sicherstellung in anderer Weise)'가 있고(StPO 제94조 제1항),[71] '형식적인 확보(förmliche Sicherstellung)'로서 '압수(Beschlaganhem)'가 있다(StPO 제94조 제2항).[72] 형식 없는 확보는 피압수자의 자발적인 제출을 전제로 하는 것으로서 증거물 확보의 가장 간단한 형태이다.[73] 반면 형식적인 확보는 대상물이 자발적으로 제출되지 않는 경우에 행해질 수 있는 확보방법으로서 – 원칙적으로 – 법원의 명령을 통해(StPO 제98조) 또는 질서·강제수단을 통해(StPO 제95조) 실현된다.[74] 이때 StPO 제98조에 따른 법관유보와 결부된 압수는 전형적인 의미의 압수로서 협의의 압수라고도 한다.[75] 한편 수사기관이나 법원은 StPO 제95조 제1항에 따라 증거물 보관자에게 그 제출을 요청할 수 있는데,[76] 이 '제출요청(Herausgabeverlangen)'이 거부되는 때 수사기관이나 법원은 동조 제2항에 따라 StPO 제70조[77]에 따른 질서

---

68) StPO 제94조[증거(대상)물의 확보와 압수(Sicherstellung und Beschlagnahme von Gegenständen zu Beweiszwecken)] ① 대상물이 증거방법으로서 수사에 중요하다고 여겨지는 경우에는 유치되거나(in Verwahrung zu nehmen) 기타 방법으로 확보되어야 한다. ② 대상물을 보관하고 있는 개인이 그것을 자발적으로 제출하지 아니하는 때에는 압수가 행해질 수 있다. [③과 ④ 생략]

69) StPO 제95조 [제출의무(Herausgabepflicht)] ① 전조(제94조)에 언급된 종류의 대상물을 보관하는 자는 이를 (법원이나 수사기관의) 요청에 따라 제출·송부할(vorlegen und ausliefern) 의무가 있다. ② (제1항의 제출·송부를) 거절하는 경우에는 보관자에게 제70조에 규정된 질서 및 강제 수단이 부과될 수 있다. 증언거부권자에게는 제1문이 적용되지 않는다.

70) *Köhler*, M-G/Schmitt, § 94 Rn. 11; *Roxin/Schünemann*, § 34 Rn. 6; *Volk/Engländer*, § 10 Rn. 34; *Park*, Rn. 430.

71) *Volk/Engländer*, § 10 Rn. 34; *Park*, Rn. 432.

72) *Köhler*, M-G/Schmitt, Vor § 94 Rn. 3; *Volk/Engländer*, § 10 Rn. 34; *Park*, Rn. 433 u. 437 f.

73) *Köhler*, M-G/Schmitt, § 94 Rn. 12; *Roxin/Schünemann*, § 34 Rn. 7; *Park*, Rn. 432. 우리 법제상의 임의제출(형사소송법[이하 "형소법"] 제108조, 제218조)이 이러한 형식 없는 확보의 대표적인 예에 속한다.

74) *Köhler*, M-G/Schmitt, § 94 Rn. 13; *Park*, Rn. 433 ff.

75) *Roxin/Schünemann*, § 34 Rn. 8.

76) 이 제출요청에 따라 증거물이 자발적으로 제출되는 경우, 해당 증거물은 형식 없이 확보된 것이다(*Köhler*, M-G/Schmitt, § 95 Rn. 1).

77) StPO 제70조 [이유 없는 증언 또는 선서의 거부(Grundlose Zeugnis- oder Eidesverweigerung)]

과태료나 강제수단의 부과를 통해 증거물 보관자에게 그 제출을 강제할 수 있다. 다만 지배적인 견해에 따르면 이 '제출강제(Erzwingung der Herausgabe)'는 강제처분의 한 유형이기 때문에 수사기관은 법원의 명령에 의해서만 제출을 강제할 수 있다.[78] 그리고 제출강제는 StPO 제95조 제1항에 따른 제출의무가 없고 자기부죄거부의 특권이 있는 피의자에게는 행해질 수 없고, 피의자 아닌 자에게만 행해질 수 있다.[79] 이런 점에서 StPO 제95조 제2항의 제출강제는 증거물의 형식 없는 확보의 한 형태 또는 제3의 확보형식이 아니라 (형식적 확보인) 압수의 한 집행방법에 속한다.[80]

증거물의 확보 및 압수와 관련된 각 용어의 개념 및 그 구분은 위에서 기술된 바와 같지만, 형사절차에서 증거물 확보의 가장 전형적인 (강제)처분은 제94조 제2항과 제98조에 따른 압수이고, 그 집행방법은 자발성을 전제로 하지 않는다는 점에서 압수수색 일반규정은 기본적으로 압수를 전제로 한 절차통제에 관한 규정이다. 따라서 이하에서는 특별히 구분되어야 하는 경우가 아닌 한 증거물 확보는 '압수'를 의미한다.

(2) 압수의 실체적 요건: 압수대상성, 잠재적인 증거로서의 중요성, 최초혐의

압수는 '증명목적의 물건(Gegenständen zu Beweiszwecken)', 즉 증거물을 그 대상으로 하며, 이는 다른 말로 하면 '증거방법으로서의 물건(Gegenständen als Beweismittel)'을 의미한다(StPO 제94조 제1항).[81] 이 압수대상물로는 모든 종류의 물건이 고려된다. 따라서 시체, 혈액 등의 동산뿐만 아니라 건물과 토지 등의 부동산 이외에 디지털 정보가 저장되어 있는 정보저장매체와 컴퓨터출력물도 유체물로서 압수대상물에 포함된다.[82] 이때 디지털 정보 자체가 위 물건의 개념에 포함되어 압수의 대상이 될

---

① 법률상의 근거 없이 증언이나 선서를 거부하는 경우 증인에게 그 거부로 인하여 발생한 비용을 부과한다. 이와 동시에 그에게는 질서과태료(Ordnungsgeld)를 부과하며, 이 과태료의 징수가 불가능한 때에는 질서구금(Ordnungshaft)에 처한다. ② 또한 증언을 강제하기 위해 구금(Haft)이 명령될 수 있으나, 그 기간은 해당 심급에서의 절차의 종결시점을 초과하지 못하며 6개월을 초과할 수도 없다. ③ 이 처분권은 수사절차상의 법관 및 수명법관과 수탁판사에게도 있다. ④ 이러한 처분이 모두 사용되었다면, 동일한 행위를 대상으로 하는 (동일 또는 다른) 절차에서는 이 처분을 다시 행할 수 없다.

78) *Köhler*, M-G/Schmitt, § 95 Rn. 9; *Roxin/Schünemann*, § 34 Rn. 9; *Park*, Rn. 441.

79) *Köhler*, M-G/Schmitt, § 95 Rn. 5 u. 10 f.; *Volk/Engländer*, § 10 Rn. 34; *Park*, Rn. 442.

80) *Park*, Rn. 438 f. 제출강제는 협의의 압수에 비해 기본권을 덜 침해하는 경미한 집행방법 중 하나로서 비례성 원칙이 고려된 것이다(*Park*, Rn. 437).

81) *Köhler*, M-G/Schmitt, § 94 Rn. 3.

82) *Köhler*, M-G/Schmitt, § 94 Rn. 4.

수 있는지가 문제된다(아래 3) 참고).

StPO 제94조 제1항에 따르면 압수되어야 하는 물건, 즉 '압수대상물'은 "증거방법으로서 수사에 중요하다고 여겨지는 물건"이며, 특정한 범죄혐의에 근거하는 형사절차에서 사용되지 않을 것은 압수될 수 없다.[83] 증거방법이란 범죄나 범행의 정황을 직·간접적으로 증명하는 물건이고,[84] 법률효과나 양형의 판단에 영향을 줄 수 있는 증거물 및 증명력에 영향을 주는 증거물도 거기에 포함된다.[85] 따라서 '잠재적인 증거로서의 중요성(potenzielle Beweisbedeutung)'이 인정되는 대상물은 압수될 수 있으며, BVerfG와 BGH의 입장 및 문헌의 지배적인 견해에 따르면 이러한 '가능성(Möglichkeit)'으로 충분하다.[86] 가능성의 판단과 관련하여 대상물이 어떤 증명에 사용될 것인지까지 확정될 필요는 없지만, 최소한 그 대상물이 증거로서 중요할 수 있다는 어떤 구체적인 가능성은 존재해야 한다; 왜냐하면 무작위의 제한 없는 압수는 허용되지 않기 때문이다.[87] 압수된 대상물이 나중에 실제로 증거방법으로 사용되었는지는 중요하지 않다.[88]

이에 더해 압수명령의 실체적 요건으로서 범죄에 대한 '합리적인 사실상의 근거', 소위 '최초혐의(Anfangsverdacht)'가 요구된다(StPO 제152조 제2항[89]).[90] 최초혐의

---

83) *BVerfGE* 77, 1, 53 [Rn. 194](= NJW 1988, 890).

84) *Köhler*, M-G/Schmitt, § 94 Rn. 5.

85) *Park*, Rn. 455 f.

86) *BVerfG* NJW 1988, 890; *BGH* NStZ 1981, 94; *Köhler*, M-G/Schmitt, § 94 Rn. 6; *Volk/Engländer*, § 10 Rn. 32; *Park*, Rn. 456.

87) *Park*, Rn. 457. 독일 법제에서의 '잠재적인 증거로서의 중요성'은 우리 법제에서의 압수수색 '관련성'(형소법 제106조, 제109조, 제215조)에 상응하는 개념이라고 할 수 있고, 두 개념 모두 압수수색, 특히 압수의 범위를 제한하는 수단으로 활용되고 있다. 다만 – 우리와 달리 – 독일에서는 '잠재적인 증거로서의 중요성' 개념의 구체적인 내용이 무엇인지에 대한 연구가 거의 없다. 가장 큰 이유는 '관련성' 내지 '잠재적인 증거로서의 중요성'이 없는 정보의 수집행위에 대한 법적 통제장치로 위법수집증거배제법칙이 수용되어 있는지에서 차이가 있기 때문인 듯하다. 어쨌든 독일에서 동 중요성 개념은 압수수색에서 비례성 원칙이 반영된 것이라고 이해되며, 구체적인 사안에서 압수범위를 적절히 제한하는 역할을 한다.

88) *Park*, Rn. 457.

89) StPO 제152조 [기소관청, 기소법정주의(Anklagebehörde, Legalitätsgrundsatz)] ② 법률상 다르게 규정되어 있지 않는 한, 합리적인 사실상의 근거(단서)가 존재하는 경우, 검찰은 소추 가능한 모든 범죄행위에 대하여 조치를 취할 의무가 있다.

90) *BVerfGE* 113, 29, 53 [Rn. 108]; 115, 166, 197 [Rn. 117]; 124, 43, 66 [Rn. 79]; *Köhler*, M-G/Schmitt, § 94 Rn. 8 u. 18; *Volk/Engländer*, § 10 Rn. 32; *Park*, Rn. 459. 독일 문헌의 지배적인 견해와 BVerfG의 입장에 따르면 형사절차에서 범죄혐의(Tatverdacht)는 StPO에 차등적으로 구분되어 규정되어 있는데, 이는 범죄혐의의 강도와 수사처분에 의한 기본권 침해의 비중은 비례성 원칙에 따라 연동되어야 한다는 점에 근거한다(*Roxin/Schünemann*, § 39 Rn.

존부의 대한 판단권은 수사기관에게 있고 여기에는 일정한 재량이 존재한다.[91] 다만 구체적인 사실에 근거하지 않는 막연한 근거나 단순 추정으로는 최초혐의가 인정될 수 없다.[92] 이 혐의는 형사절차 개시의 필요·충분조건이다.[93] 따라서 최초혐의는 그것이 법규정에 명확히 표현되어 있는 경우(예를 들어, StPO 제98조a, 제110조a, 제163조f)뿐만 아니라, 그렇지 않은 경우(예를 들어, StPO 제94조와 제102조, 제99조)에도 요구된다. 최초혐의가 존재하는 경우에는 일반적으로 압수수색이 가능하고 허용되며, 이를 통해 수사가 개시될 수도 있다.[94]

나) 압수의 절차법적 통제장치

StPO 제98조[95] 제1항에 따르면 압수는 절차상 원칙적으로 법원의 사전심사에 의한 통제 아래 있지만, 지체의 위험이 있는 경우에는(bei Gafahr im Verzug) 수사기관인 검찰과 그의 수사관(사법경찰관)이 예외적으로 법원의 개입 없이 압수할 수 있다. 즉, 독일 법제상 압수는 원칙적으로 사전적 통제장치인 법관유보(Richtervorbehalt)와 결부되어 있지만, 예외적으로 이것이 배제될 수 있다. 한편 이러한 법관유보 원칙과 그 예외적 배제는 StPO 제105조 제1항[96]에 따른 수색에서도 마찬가지이다. 따라서

---

16). 이에 따라 현재 StPO에서 (범죄)혐의는 일반적으로 4단계로 구분된다: 최초혐의 내지 단순혐의(Einfacher Verdacht)-특정한 혐의(Bestimmter Verdacht)-충분한 혐의(Hinreichender Verdacht)-유력한 혐의(Dringender Verdacht). 최초혐의에 미치지 못하는 혐의가 존재하는 경우에는 내사(Vorermittlungen)가 가능하다(*Roxin/Schünemann*, § 39 Rn. 17). 이에 대한 추가적인 설명은 뒤의 3. 나. 2) 가) 참고. 한편 범죄혐의 정도의 차등화는 우리 형사법제에서도 어느 정도 행해지고 있으며, 최초혐의는 "범죄의 혐의가 있다고 사료되는 때"로(형소법 제196조, 197조), 체포와 구속을 위해 필요한 혐의는 '상당한 혐의'로(형소법 제70조와 제201조 및 제200조의2와 3: "죄를 범하였다고 의심할 만한 상당한 이유") 표현되어 있다.

91) *Schmitt*, M-G/Schmitt, § 152 Rn. 4.

92) *BVerfGE* 113, 29, 53 [Rn. 108]; 115, 166, 197 [Rn. 117]; 124, 43, 66 [Rn. 79]; *Schmitt*, M-G/Schmitt, § 152 Rn. 4.

93) *Diemer*, KK-StPO, § 152 Rn. 7; *Schmitt*, M-G/Schmitt, § 152 Rn. 4; *Roxin/Schünemann*, § 39 Rn. 15.

94) *Köhler*, M-G/Schmitt, § 94 Rn. 8 u. *Schmitt*, M-G/Schmitt, § 160 Rn. 5.

95) StPO 제98조 [압수절차(Verfahren bei der Beschlagnahme)] ① 압수는 법원에 의해서만, 지체의 위험이 있는 경우에는 검찰 및 그의 수사관(법원조직법[Gerichtsverfassungsgesetz, 이하 "GVG"] 제152조)에 의해서도 명령될 수 있다. 제97조 제5항 제2문에 따른 편집부, 출판사, 인쇄소, 방송국 공간에 대한 압수는 법원에 의해서만 명령될 수 있다. ② 법원의 명령 없이 대상물을 압수한 공무원은, 압수 시에 압수의 당사자나 그의 성인 가족이 출석하지 않은 경우 또는 당사자 및 그의 부재 시에는 그의 성인 가족이 압수에 대해서 명백한 이의를 제기한 경우, 3일 이내에 법원의 승인을 청구해야 한다. 당사자는 언제나 법원의 재판을 청구할 수 있다. (제2문의 경우) 법원관할은 제162조에 따라 정해진다. 당사자는 이러한 경우에도 압수가 행해진 관할구역의 구법원(Amtsgericht, 이하 "AG")에 청구서를 제출할 수 있다; 이 AG는 관할 AG로 (당사자의) 청구서를 이송한다. (압수) 당사자에게 그의 권리를 고지해야 한다. [③과 ④ 생략]

여기서는 압수와 수색의 법관유보를 함께 기술한다.

우선 압수수색은 기본권을 중대하게 침해하는 강제처분으로서 그 수권규범의 법적 형성에는 비례성 원칙이 엄격히 준수되어야 하며, 이때 원칙적으로 법관유보가 요구된다.[97] 법관유보는 처분 당사자의 권리보호를 위해 압수수색의 실체적 요건에 대한 사전심사를 보장하기 위한 절차법적 통제장치이며, 독립된 중립의 기관에 의한 강제처분의 예방적 통제를 지향한다.[98] 그것은 전체적으로 강제처분에 대한 적절한 한계설정을 통해 기본권 보호의 강화에 이바지하며,[99] 무엇보다 개별적인 사안에서 당사자의 이익이 적절하게 고려되도록 보장한다.[100] 이를 위해 법관은 압수수색의 헌법상·법률상 요건이 정확히 준수되었는지를 독자적인 책임으로 심사해야 한다.[101] 따라서 법관은 압수수색의 결정서를 충분한 이유제시와 함께[102] 스스로 작성해야 하며,[103] 적합한 표현을 통해 가능하고 합리적인 범위 내에서 명령과 그 집행이 평가·통제될 수 있도록 보장할 의무를 부담한다.[104] 법관유보를 통해 사후적 권리보호(대표적으로

---

96) StPO 제105조 [수색절차(Verfahren bei der Durchsuchung)] ① 수색은 법관에 의해서만, 지체의 위험이 있는 경우에는 검찰 및 그의 수사관(GVG 제152조)에 의해서도 명령될 수 있다. 제103조 제1항 제2문의 수색은 법관이 명령한다; (이때) 지체의 위험이 있는 경우에는 검찰도 명령할 수 있다. [②와 ③ 생략]

97) *BVerfGE* 20, 162 186 f.; 42, 212, 219 f.; 103, 142, 151 [Rn. 27]; 139, 245, 265 [Rn. 57]; NJW 2002, 1333 [Tz. a)]; 2009, 2516 [Rn. 21]; 2015, 1585, 1586 [Rn. 23 f.]. 비밀의 처분과 관련해서는 *BVerfGE* 125, 260, 338 [Rn. 249]; 141, 220, 275 f. [Rn. 118].

98) *BVerfGE* 103, 142, 151 [Rn. 28]; 125, 260, 337 [Rn. 248]; 139, 245, 265 [Rn. 57]; NJW 2009, 2516 [Rn. 21]; 2015, 1585, 1586 [Rn. 24]; *Park*, Rn. 69; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 16.

99) *BVerfGE* 103, 142, 152 [Rn. 29 a.E.]; 또한 *Park*, Rn. 69 u. 471; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 16.

100) *BVerfGE* 103, 142, 151 [Rn. 28]; 139, 245, 266 [Rn. 60]; NJW 2009, 2516 [Rn. 21]; NJW 2015, 1585, 1586 [Rn. 24].

101) *BVerfGE* 96, 44, 51 [Rn. 24]; 103, 142, 151 [Rn. 29 am Anfang]; 125, 260, 338 [Rn. 249]; NJW 2009, 2516, 2516 f. [Rn. 21]. 독일에서 영장전담판사(Ermittlungsrichter)의 심사권은 처분을 위한 법률상 요건(예를 들어, 최초혐의의 존재)이 존재하는지와 (헌법상의) 비례성 원칙이 유지되고 있는지의 법적 통제로 제한된다; 이것은 청구된 행위의 법률적 허용성, 즉 적법성과 관련된 것이다(StPO 제162조 제2항: 법원은 청구된 행위가 사건의 상황에 따라 법적으로 허용되는지 여부를 심사하여야 한다.)(*Park*, Rn. 70; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 14). 반면 처분 및 그 집행방법의 합목적성 심사는 법관이 아닌 수사절차의 지배자인 검사에게 유보되어 있다(*Schmitt*, M-G/Schmitt, § 162 Rn. 14 f.; *Park*, Rn. 70; *Schünemann*, ZStW 114 (2002), 1, 40; *Wohlers/Jäger*, a.a.O.). 수사의 전략 내지 구상은 검사의 권한에 속한다. 따라서 법관은 원칙적으로 검사에 의해 청구되지 않은 수사처분을 명령할 수 없고(*Schmitt*, M-G/Schmitt, § 162 Rn. 5), 청구된 처분을 그에게 더 좋다고 여겨지는 다른 처분으로 대체할 권한도 없다. 이 한도에서 영장전담판사는 검사의 청구에 구속된다.

102) *BVerfGE* 125, 260, 338 [Rn. 249].

103) *Schünemann*, ZStW 114 (2002), 1, 37.

준항고)의 불충분함이 가능한 한 포괄적으로 상쇄되어야 한다.[105]

한편 StPO 제98조 제1항 제1문과 제105조 제1항은 '지체의 위험이 있는 경우'에는 검찰과 그의 수사관이 법원의 사전심사 없이 압수수색을 명령할 수 있는 권한, 소위 '긴급권(Eilkompetenz)'을 허용한다. 이 권한은 헌법적 근거는 GG 제13조 제2항에서 찾을 수 있지만, BVerfG 결정에 따르면 증거방법 손실의 위험에 대처하여 효과적인 형사소추라는 공익을 달성하기 위한 수사기관의 구체적인 상황에 맞는 신속한 행위의 실현에도 그 근거가 있다.[106] 이런 점에서 위 긴급권은 비례성 원칙에 따라 기본권 보호와 효과적인 형사소추 사이에서 적절한 균형을 달성하기 위한 수단으로 이해된다.[107] 하지만 GG 제13조 제2항의 문언을 고려할 때, 어디까지나 법관유보가 원칙이고 수사기관의 긴급권은 '예외적으로'만 허용된다.[108] 이러한 긴급권의 예외성으로부터 몇 가지 요청이 도출된다. 우선 국가기관들은 원칙인 법관유보가 실무에서 실제로 유효하도록 노력할 헌법상 의무가 있다.[109] 따라서 수사기관은 일단 법관의 명령을 얻기 위해 노력할 의무를 부담한다.[110] 다음으로 지체의 위험이라는 개념은 좁게, 즉 엄격하게 해석되어야 하고,[111] 긴급권의 관할은 수사절차의 지배자인 검찰에게 우선적으로 부여되며, 그의 수사관의 긴급권은 후순위이고 보충적이다.[112] 끝으로 긴급권 이용은 제한 없는 법원의 사후 심사에 놓일 수 있어야 한다.[113]

---

104) *BVerfGE* 20, 162, 224; 42, 212, 220; 96, 44, 51; 103, 142, 151 [Rn. 29]; NJW 2009, 2516, 2517 [Rn. 22]; 2015, 1585, 1586 [Rn. 25]; *Roxin*, StV 1997, 654; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 16.

105) *Wohlers/Jäger*, SK-StPO, § 98 Rn. 6. 사후의 권리보호는 이미 발생한 기본권 침해를 일반적으로 제거하지 못하거나 제한적으로만 제거할 수 있다(*Park*, Rn. 471).

106) *BVerfGE* 139, 245, 268 [Rn. 68].

107) *BVerfGE* 103, 142, 154 [Rn. 36]; 139, 245, 268 [Rn. 68].

108) *BVerfGE* 103, 142, Tenor 1 und 155 [Rn. 37 f.]; 139, 245, 269 [Rn. 69 f.]; *Michalke*, StraFo 3/2014, 89, 90 f.

109) *BVerfGE* 103, 142, 156 [Rn. 41]; 139, 245, 267 [Rn. 62].

110) *BVerfGE* 139, 245, 270 [Rn. 70].

111) *BVerfGE* 103, 142, Tenor 1 und 153 [Rn. 33]; 139, 245, 269 [Rn. 69].

112) *BVerfG* NJW 2007, 1345, 1346 [Rn. 17]; NJW 2008, 3053, 3054 [Rn. 10]; *Greven*, KK-StPO, § 98 Rn. 11; *Köhler*, M-G/Schmitt, § 98 Rn. 6; *Park*, Rn. 95 u. 491.

113) *BVerfGE* 103, 142, Tenor 3 und 159 f. [Rn. 53]; 139, 245, 272 f. [Rn. 74-76]. 독일 법제상의 압수수색에서의 긴급권, 즉 법관유보의 배제는 우리 법제상의 – 임의제출을 제외한 – 영장주의 예외(형소법 제216조 내지 제217조)와 비교할 때 그 허용요건과 범위에서 많이 다르다. 물론 형소법상의 영장주의 예외가 모두 '긴급성'을 요건으로 한다는 점에서는 독일의 긴급권과 동일한 취지를 갖고 있다고 할 수 있으나, 그 내용상 체포·구속이라는 신체에 대한 강제처분의 상황을 전제로 한다는 점에서 독일의 긴급권에 비하여 그 적용범위가 훨씬 좁다. 또한 형소법상의 영장주

2) 수색: StPO 제102조 내지 제110조

우선 StPO 제102조는 '혐의자에 대한 수색'이라는 표제 아래 수색의 유형과 대상물 및 수색의 실체적 요건을 규정하고 있고, StPO 제103조는 '혐의자 아닌 자에 대한 수색'에서의 강화된 요건을 규정하고 있다(아래 가)). 이어서 StPO 제104조 내지 제110조는 수색의 절차법적 통제장치를 규정하고 있다(아래 나)).

가) 수색의 유형과 수색의 실체적 요건

(1) 수색의 유형

독일의 지배적인 견해에 따르면 주거수색의 개념에는 주거나 사무실 등의 공간에 존재하는 신체, 물건, 단서에 대한 찾기가 포함된다.[114] 그리고 StPO 제102조[115]에 따르면 수색은 그 목적에 따라 혐의자의 체포를 위한 수색, 소위 '체포수색(Ergreifungsdurchsuchung)'과 증거방법의 발견 내지 증거확보를 위한 수색, 소위 '수사수색(Ermittlungsdurchsuchung)'으로 구분된다.[116] 전자는 본 글의 쟁점과 직접적인 연관이 없으므로 별도로 다루지 않는다.

(2) 수색의 실체적 요건: 수색대상물, 증거방법 발견의 추정, 최초혐의

StPO 제102조에 따라 혐의자(Verdächtige)의 주거와 그 밖의 공간 및 그의 신체와 그에게 속하는 물건은 증거방법이 발견될 것이라고 추정되는 경우 수색될 수 있다. 이때 혐의자란 범죄수사상의 경험에 근거하여 범행에 대한 혐의, 즉 최초혐의를 받는 자이지만, 문언상 반드시 피의자여야 하는 것은 아니므로 수사절차의 개시 전에도 수색이 행해질 수 있다.[117] 증거방법이 발견될 것이라고 추정, 소위 '발견의 추정

의 예외에서는 성질상 사후영장이 불필요한 형소법 제216조 제1항 제1호의 경우 이외에는 언제나 사후영장이 요구된다. 요컨대, 독일의 긴급권은 압수수색에서 법관유보를 배제시키고 수사기관 스스로 강제처분을 명령할 수 있게 하는 매우 강력한 권한임에 비하여, 우리의 영장주의 예외는 본질적으로 '사전' 영장주의의 예외이고 그 범위 또한 매우 제한적이다.

114) *Park*, Rn. 30.

115) StPO 제102조 [혐의자에 대한 수색(Durchsuchung beim Verdächtigen)] 어떤 범죄의 정범이나 공범으로서 또는 데이터 불법취득죄, 범인은닉죄, 사법방해죄, 장물취득죄의 정범이나 공범으로서 혐의가 있는 자를 체포하기 위한 경우 및 수색으로 증거방법이 발견될 것이라고 추정되는 경우, 주거와 기타 공간 및 혐의자의 신체와 그에게 속하는 물건이 수색될 수 있다.

116) *Park*, Rn. 31 u. 50 f.

117) *Köhler*, M-G/Schmitt, § 102 Rn. 2 f.; *Volk/Engländer*, § 10 Rn. 54; *Park*, Rn. 36.

(Auffindungsvermutung)'은 범죄수사상의 경험에 따라 수색목적이 달성될 수 있다는 추정이 존재하는 경우에 인정된다.[118] 한편 StPO 제103조 제1항[119]에 따르면 '혐의자 아닌 자(andere Personen)', 즉 제3자도 수색될 수 있지만, 이때에는 위 발견의 추정이 – 수사상의 경험 이상의 – 구체적인 사실관계에 근거할 것이 요구된다는 점에서,[120] 그 수색의 요건은 혐의자에 대한 수색에서보다 더 엄격하다.[121] 이는 비례성 원칙에 따른 것이다.[122]

수색대상물은 StPO 제102조에 명문으로 언급되어 있듯이 주거와 그 밖의 공간 및 신체와 물건(Sachen)이다. 본 글의 주제와 관련하여 CD나 USB뿐만 아니라 PC나 스마트폰 등의 정보저장매체 등은 유체물로서 물건에 속하고 수색대상물이라는 점에 대해서는 이론이 없다. 한편 디지털 정보 자체가 수색대상물인지 여부는 – 압수대상성 논의와 달리 – 수색의 개념에 비추어 문제되지 않는다.

나) 수색의 절차법적 통제장치

StPO 제104조 내지 제110조에는 수색의 절차법적 통제장치가 규정되어 있다. 해당 규정 중에서 StPO 제105조 제1항은 법관유보에 관한 것으로 이미 앞에서 기술하였으므로 여기서는 언급되지 않을 것이다. 한편 독일에서 과도한 정보수집에 대한 중요한 절차법적 보장책으로 여겨지는 서류와 정보저장매체의 수색에 관한 특별규정인 제110조는 별도로 자세히 다룬다(뒤의 3). 여기서는 그 이외의 부분, 즉 수색증인과 피압수자의 입회, 처분의 집행 전·후의 조치 등 집행과정에 대한 법적 규제에 대해서만 기술한다.

(1) 수색의 집행방법 및 수색증인과 피압수자의 입회

우선 제104조[123]는 야간의 주거수색에 대해 규정하고 있다. 야간은 보통 밤의 휴식

---

118) *Park*, Rn. 43.

119) StPO 제103조 [혐의자 아닌 자에 대한 수색(Durchsuchung beim anderen Personen)] ① 혐의자 아닌 자에 대한 수색은 피의자의 체포를 위한 경우 또는 (범죄)단서의 추적이나 특정 대상물의 압수를 위한 경우에만, 추적 대상자 또는 (범죄)단서나 물건(Sache)이 수색될 공간에 존재한다고 추론될 수 있는 사실관계가 존재하는 경우에만 허용된다.

120) *BVerfG* NJW 2016, 1645, 1645 f. [Rn. 13 ff.].

121) *Volk/Engländer*, § 10 Rn. 55; *Park*, Rn. 43.

122) *Köhler*, M-G/Schmitt, § 103 Rn. 1a.

123) StPO 제104조 [야간수색(Durchsuchung von Räumen zur Nachtzeit)] ① 야간에 주거, 영업공간,

이나 특별한 사생활과 관련된다는 점에서 동 조항은 시민을 특별히 보호하기 위한 규정이다.[124] '야간'의 개념은 과거 여름과 겨울로 구분되어 있었으나,[125] 최근 2021년 개정을 통해 21시부터 6시까지의 기간으로 통일되었다. 이는 직접적으로는 BVerfG의 2019. 3. 12.의 결정[126]에 따른 것이지만, 19세기 농경사회 시절에 제정된 동 규정의 과거 내용이 오늘날에는 더 이상 맞지 않다는 점에 근거한다.[127] 한편 야간주거주색이 허용되는 경우로서 기존의 3가지 경우(StPO 제104조 제1항 제1, 2, 4호)에 더하여 2021년 개정을 통해 '특정한 사실관계에 비추어 수색 동안에 (피의자가) 증거방법으로서 고려되는 정보저장매체에 접근할 것이라는 혐의가 이유 있고, 야간수색 없이는 그 정보저장매체에 대한 분석이, 특히 암호화되지 않은 방식으로는 가망이 없거나 현저히 곤란한 경우'(동 제3호)가 추가되었다. 이 추가된 규정은 오늘날 발전된 암호화 기술로 인하여 수사기관이 범죄혐의와 관련된 정보가 저장된 정보저장매체를 확보하고도 거기에 저장되어 있는 정보에 접근하지 못하거나 그것을 분석하지 못하는 것에 대비하기 위한 것으로서, 주로 아동음란물이나 아동성착취물과 관련된 범죄의 수사를 위한 것이다.[128] 물론 새롭게 허용된 이런 경우에서의 야간수색은 StPO 제110조 제3항에 따라 외부저장매체로까지 확대될 수 있다.[129]

StPO 제105조 제2항[130]은 '수색증인(Durchsuchungszeugen)'에 대하여 규정하고

경계지워진 토지는 다음 각호의 경우에만 수색될 수 있다: 1. 현행범 추격의 경우, 2. 지체의 위험의 경우, 3. 특정한 사실관계에 비추어 수색 동안에 (피의자가) 증거방법으로서 고려되는 정보저장매체에 접근할 것이라는 혐의가 이유 있고, 야간의 수색 없이는 그 정보저장매체에 대한 분석이, 특히 암호화되지 않은 방식으로는 가망이 없거나 현저히 곤란한 경우, 4. 탈옥한 수형자의 재체포를 위해서. ② 제1항의 제한은 야간에 누구나 출입할 수 있는 공간 또는 경찰에게 범죄자의 숙소나 회합장소, 범죄를 통해 획득한 물건의 저장장소, 도박, 마약·무기거래, 매음을 위한 은신처로 알려진 공간에는 적용되지 않는다. ③ 야간이란 21시부터 6시까지의 기간이다.

124) BT-Drs. 19/27654, S. 72.

125) (2021.7.24.까지 유효했던) (舊) StPO 제104조 [야간수색(Durchsuchung von Räumen zur Nachtzeit)] ③ 야간이란 4월 1일부터 9월 30일 사이에는 밤 9시부터 아침 4시 사이의 시간이고, 10월 1일부터 3월 31일 사이에는 밤 9시부터 아침 6시 사이의 시간이다.

126) *BVerfG* Beschluss vom 12. März 2019 – 2 BvR 675/14 (= NJW 2019, 1428).

127) BT-Drs. 19/27654, S. 73; *Park*, Rn. 184.

128) BT-Drs. 19/30517, S. 18. 한편 동 입법자료에 따르면, 신설된 제3호의 야간수색은 해석상 기존 규정인 제1호나 제2호에 의해서도 허용될 수 있으나, 이는 언제나 명확한 것이 아니고 법관마다 그 포섭에 대한 판단이 달라질 수 있다는 점에서 제3호가 신설된 것이다(a.a.O.).

129) BT-Drs. 19/30517, S. 18.

130) StPO 제105조 [수색절차(Verfahren bei der Durchsuchung)] ② 법관이나 검사의 참관 없이 주거, 업무공간, 경계 지워진 사유지의 수색이 행해지는 경우, 가능하다면(wenn möglich) 수색이 이루어지는 관할구역의 지방자치단체 공무원이나 동 단체의 구성원(주민) 2인이 소환되어야

있다. 이것은 수색의 규정에 따른 집행 및 그 증명 가능성을 보장하기 위한 것이다.[131] 증인의 입회는 해당 규정의 문언('가능하다면')에 따라 가능해야 하지만, 그에 따른 시간의 손실로 수색의 결과가 위험해지는 경우에는 불가능할 것이다.[132] 유력한 견해에 따르면 이 입회 가능성에 대한 판단은 수색을 집행하는 공무원이 의무재량에 따라 판단하지만,[133] 그 상황은 StPO 제105조 제1항 의미의 '지체의 위험의 존재'와 유사하다.[134] 따라서 동 문언은 불특정하지만 심사될 수 있는 법적 개념이고, 객관적으로 판단될 수 있어야 한다.[135] 수색증인의 입회는 수색 공무원의 위법한 침해로부터 당사자를 보호하지만, 반대로 수색의 유형과 방식에 관한 당사자의 부당한 비난으로부터 수색 공무원을 보호한다.[136]

이어서 StPO 제106조 제1항[137]은 수색될 공간이나 대상물의 점유자 및 그의 대리인의 입회에 대해 규정한다. 동 규정 제1문의 '점유자(Inhaber)'는 재산관계가 아니라 사실상의 상황, 즉 공간 사용권이나 지배관계에 따른다.[138] StPO 제102조에 따른 피의자에 대한 수색에서는 그가 일반적으로 점유자일 것이다. 체포·구금된 피의자는 이 입회권을 갖지 못하지만,[139] 그는 제2문에 근거하여 변호사 등에게 자기의 대리인

(zuziehen) 한다. 경찰공무원이나 검찰의 수사관은 지방자치단체의 구성원(주민)으로서 소환될 수 없다.

131) *BGH* NJW 1963, 1461; *Park*, Rn. 172.

132) *BGH* NStZ 1986, 84, 85; *Köhler*, M-G/Schmitt, § 105 Rn. 11; *Park*, Rn. 174; *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 56.

133) *Bruns*, KK-StPO, § 105 Rn. 14; *Köhler*, M-G/Schmitt, § 105 Rn. 11; *Park*, Rn. 175; *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 57.

134) *Park*, Rn. 175; *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 57.

135) *Park*, Rn. 175; *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 57.

136) *BGH* NJW 1963, 1461; *Bruns*, KK-StPO, § 105 Rn. 14; *Köhler*, M-G/Schmitt, § 105 Rn. 12; *Park*, Rn. 177; *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 53. 따라서 수색 당사자나 공무원은 StPO 제105조 제2항의 준수를 각각 포기할 수 있고, 수색증인 입회의 최종적 배제를 위해서는 그들이 일치하여 그것을 포기해야 한다(*Roxin*/*Schünemann*, § 35 Rn. 10). 그 결과 이목을 피하고자 수색증인의 입회를 배제하려는 당사자의 요청의 경우, 그 판단은 수색 공무원의 재량에 따른다(*Bruns*, a.a.O.; *Park*, a.a.O.).

137) StPO 제106조 [수색대상 점유자의 소환(Zuziehung des Inhabers eines Durchsuchungsobjekts)] ① 수색될 공간이나 대상물의 점유자는 수색에 입회할 수 있다. 점유자가 부재중인 경우에는 가능하다면(wenn möglich) 그의 대리인 또는 성년의 친족, 동거인, 이웃이 소환되어야 한다.

138) *Park*, Rn. 167; *Wohlers*/*Jäger*, SK-StPO, § 106 Rn. 4. 수인이 공동 점유자인 경우, 각자 출석할 권리가 있다(*Park*, a.a.O.; *Wohlers*/*Jäger*, a.a.O. Rn. 5).

139) *Köhler*, M-G/Schmitt, § 106 Rn. 2; *Wohlers*/*Jäger*, SK-StPO, § 106 Rn. 9. 기결수와 미결수는 자신 감방의 점유자가 아니기 때문에 그들은 그 감방의 수색에서 출석권이 없고, 그의 변호인도 출석할 권리가 없다(*OLG Stuttgart* NStZ 1984, 574).

으로서 입회할 것을 위임할 수 있다.[140] 즉, 수색될 공간 등의 점유자가 직접 수색에 입회할 수 없는 경우에 제2문에 규정된 그의 대리인 등이 열거된 순서에 따라 수색에 입회할 수 있고, '가능하다면' 입회되어야 한다.[141] 여기의 입회 가능성의 개념 또한 – StPO 제105조 제2항에서와 같이 – 객관적으로 심사될 수 있는 법적 개념이다. 지배적인 견해에 따르면 수색 공무원은 점유자나 그의 대리인이 나타날 때까지 기다릴 의무가 없지만,[142] 수색목적이 위험해질 수 있는 경우가 아니라면 대리인 등, 특히 피의자의 변호인에게 입회할 기회를 주어야 한다; 예를 들어, 증거인멸의 위험이 없고 변호인의 즉각적인 출석이 예고된 경우.[143] 이 대리인 등의 입회는 피압수자인 점유자의 이익을 대변하기 위한 것이기 때문에 점유자가 자신의 출석권을 포기한 경우, 그의 입회 가능성도 탈락한다.[144]

반면, StPO 제103조에 따른 피의자 아닌 자에 대한 수색에서는 혐의가 없는 모든 자, 예를 들어, 피의자의 부모, 형제, 친구, 동료 및 회사 등 기업이나 단체 또는 ISP/CP가 점유자일 수 있다. 이 경우 피의자는 StPO 제106조 제1항 제1문 의미의 점유자가 아니므로 출석권이 없고, 따라서 그의 변호인도 마찬가지다.[145] 물론 이때 피의자와 그의 변호인은 수색될 공간의 점유자가 자신의 주거권을 통해 출석을 허용하는 경우 사실상 수색에 입회할 수 있다.[146]

---

140) *Köhler*, M-G/Schmitt, § 106 Rn. 2. 지배적인 견해에 따르면 변호인은 수색에서 원칙적으로 독자적인 출석권을 갖지 못하지만(*Köhler*, M-G/Schmitt, § 106 Rn. 3; *Park*, Rn. 196 f.; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 10), 일반적으로 피의자의 권리에 근거하여 수색되는 공간에 접근할 수 있다(*Park*, Rn. 196; *Wohlers/Jäger*, a.a.O.).

141) *Bruns*, KK-StPO, § 106 Rn. 2; *Köhler*, M-G/Schmitt, § 106 Rn. 4; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 13. 이 대리인도 수색증인으로서의 성격을 갖고 있다고 할 수 있지만(*Bruns*, KK-StPO, § 106 Rn. 2), 이들의 입회는 그 기능의 차이 때문에 StPO 제105조 제2항에 따른 수색증인의 입회에 의해 대체될 수 없다(*Wohlers/Jäger*, SK-StPO, § 106 Rn. 13).

142) *Park*, Rn. 160 u. 198; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 10.

143) *Park*, Rn. 198. 실무에서 이 기회의 부여는 보통 범죄의 종류에 좌우된다(a.a.O.).

144) *Park*, Rn. 168; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 13.

145) *Bruns*, KK-StPO, § 106 Rn. 3; *Köhler*, M-G/Schmitt, § 106 Rn. 3; *Park*, Rn. 169; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 11. 다만, 여기서 회사나 ISP/CP에 대한 수색 당사자인 경우, 그 경영자, 지배인, 임원진과 같이 회사 등의 주도적인 지위에 있는 자들은 제2문 의미의 대리인이 아니라 제1문 의미의 점유자이다(*Wohlers/Jäger*, a.a.O. Rn. 4).

146) *Park*, Rn. 169 u. 196 f.; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 11; *Peters*, NZWiSt 2017, 465, 472 am Anfang.

(2) 압수수색 집행 전·후의 조치

StPO 제106조 제2항[147]은 제103조 제1항에 따른 수색에서 해당 수색이 제103조 제2항이나 제104조 제2항의 요건 아래에서 행해지는 경우가 아니라면, 동조 제1항의 점유자나 그의 대리인으로 입회한 자에게 '수색의 목적'이 그 '개시 전'에 고지되어야 한다고 규정한다. 이어서 StPO 제107조 제1문[148]은 수색 당사자에게 '수색의 이유'가 그 '종료 후'에 요청에 따라 서면으로 통지되어야 한다고 규정한다. 하지만 지배적인 견해에 따르면 위 두 규정의 문언은 당사자와 법원에 의한 기본권 침해의 평가·통제 가능성의 측면에서 BVerfG가 설정한 기준을 충족하지 못하기 때문에 헌법합치적으로 해석되어야 한다고 한다.[149]

따라서 StPO 제106조 제2항 제1문은 – 문언상 명백한 – 제103조 제1항에 따른 수색에서뿐만 아니라, 그 고지가 수색목적을 위험하게 만드는 경우가 아니라면, 제102조에 따른 수색의 경우에도 적용된다.[150] 또한 StPO 제107조 제1문은 예외적인 경우, 즉 수사목적의 위험을 이유로 수색 당사자에게 수색의 개시 전에 그 목적만이 통지되고 그 이유가 완전히 또는 부분적으로 통지되지 않은 경우에만 적용된다는 의미로 해석되어야 한다.[151] 즉 StPO 제34조,[152] 제35조[153] 제2항, 제36조[154] 제2항

147) StPO 제106조 [수색대상 점유자의 소환(Zuziehung des Inhabers eines Durchsuchungsobjekts)] ② 제103조 제1항의 경우에는 점유자 또는 점유자의 부재중에 소환된 자에게 수색의 목적에 대해 수색을 개시하기 전에 고지하여야 한다. 본 규정은 제104조 제2항에 열거된 공간의 점유자에게는 적용되지 않는다.

148) StPO 제107조 [수색증명서, 압수목록(Durchsuchungsbescheinigung, Beschlagnahmeverzeichnis)] 수색 당사자의 요청이 있는 경우에는 수색 종료 후 수색의 사유(제102조, 제103조)가 서면으로 통지되어야 하며, 제102조의 경우에는 (서면으로) 범죄행위도 통지되어야 한다. [제2문 생략]

149) *Park*, Rn. 164 u. 170; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 25.

150) *Bruns*, KK-StPO, § 106 Rn. 4; *Köhler*, M-G/Schmitt, § 106 Rn. 5; *Park*, Rn. 164 u. 170; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 25.

151) *Bruns*, KK-StPO, § 107 Rn. 3: 법률문언("종료 후[nach deren Beendigung]")에도 불구하고 당사자는 가능하다면 수색의 개시 전에 이미, 최소한 구두로 수색의 이유에 대해 통지받아야 한다.

152) StPO 제34조 [불복될 수 있고 기각하는 재판의 이유제시(Begründung anfechtbarer und ablehnender Entscheidungen)] 상소로써 불복될 수 있거나 청구를 기각하는 재판에는 그 이유가 제시되어야 한다.

153) StPO 제35조 [고지(Bekanntmachung)] ① 당사자가 출석한 상태에서 내려진 재판은 그 출석자에게 선고를 통해(durch Verkündung) 고지된다. 요청이 있는 경우 출석자에게 사본이 제공될 수 있다. ② (제1항의 출석 재판 이외의) 다른 재판은 송달을 통해(durch Zustellung) 고지된다. 재판의 고지를 통해 기간이 진행되는 경우가 아닌 한 고지의 형식은 문제되지 않는다.

154) StPO 제36조 [송달과 집행(Zustellung und Vollstreckung)] ① 재판의 송달은 재판장이 명령한다. 법원사무국은 그 송달이 이루어지도록 조치한다. ② 집행을 요하는 재판은 이를 위해 필요한 조치를 지휘하는 검사에게 전달되어야 한다. 단, 공판정의 질서와 관련된 재판은 그러하지 아니하다.

제1문에 따라 법관의 수색결정서는 원칙적으로 검찰을 거쳐 - 최소한 수색의 개시 직전에라도[155] - 이유를 갖춘 완전한 정본 또는 최소한 그 사본의 교부를 통해[156] 출석한 수색 당사자에게 제시되거나 고지되어야 하지만, 예외적으로 이를 통해 수색 목적이 위험해질 수 있는 경우에는 이유의 고지가 유보될 수 있다.[157] 이런 예외적인 경우가 아니라면 당사자에게 수색명령만, 즉 이유를 포함하지 않은 법관의 결정문만을 교부하는 것은 위헌의 소지가 있다. 나아가 수색의 자세한 이유는 가능한 한 그 위험이 제거되자마자 고지되어야 하기 때문에 위 통지는 수색 종료 후 가능하다면 현장에서 즉시 행해져야 한다.[158] 이를 통해 불필요한 (준)항고가 회피될 수 있을 뿐만 아니라,[159] 처분 및 그 집행의 적법성이 사후에 효과적으로 평가·통제될 수 있다.[160]

수색이 종료된 후에는 StPO 제109조[161]에 따라 압수대상물은 정확히 목록화되어야 하며, 이 목록은 StPO 제107조 제2문[162]에 따라 압수 당사자의 요청이 있는 경우 그에게 교부되어야 하고, 혐의 있는 것이 발견되지 않은 경우에는 그에 관한 증명서, 소위 '발견없음 증명서(Negativattest oder-bescheinigung)'가 교부되어야 한다.[163] 위 규정들에는 압수목록이나 발견없음 증명서가 언제 작성·제공되어야 하는지가 포함되어 있지 않지만, - StPO 제107조 제1문에 따른 수색 결정서의 통지와 같이 - 가능하

155) *Park*, Rn. 164.

156) *Wohlers/Jäger*, SK-StPO, § 106 Rn. 26; *Park*, Rn. 211 u. 164: 법관의 수색결정서는 수색할 때 당사자에게 교부되어야 하며, 이것은 복사본이나 팩스의 형식으로도 가능하다.

157) *BGH* NStZ 2003, 273, 274 [Tz. 4]; *Wohlers/Jäger*, SK-StPO, § 107 Rn. 6; *Bruns*, KK-StPO, § 107 Rn. 3; *Park*, Rn. 211; a.A. *Köhler*, M-G/Schmitt, § 107 Rn. 2: 제1문 의미의 수색 증명서에는 수사목적이 위험해질 수 있는지에 상관없이 수색목적의 추상적인 기재(예를 들어, 체포나 증거방법 발견을 위해)로 충분하다.

158) *Park*, Rn. 212; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 26 u. § 107 Rn. 5 f.

159) *BGH* NStZ 2003, 273, 274 [Tz. 4]; *Park*, Rn. 211; *Wohlers/Jäger*, SK-StPO, § 107 Rn. 6.

160) 따라서 예를 들어, 수색 당사자나 그의 대리인 등이 불출석하거나 그들이 수색에 대해 전혀 알지 못했기 때문에 당사자가 이 통지를 요청할 수 없는 경우, 효과적인 권리보호의 기회를 보장하기 위해 그에게 필요한 서면의 통지가 직권으로 행해져야 한다(*Park*, Rn. 215; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 25 u. § 107 Rn. 3)

161) StPO 제109조 [압수된 대상물의 표시(Kennzeichnung beschlagnahmter Gegenstände)] 유치·압수된 대상물은 정확히 목록화되어야 하며, 착오방지를 위해 관인이나 기타 방법으로 식별될 수 있어야 한다.

162) StPO 제107조 [수색증명서, 압수목록(Durchsuchungsbescheinigung, Beschlagnahmeverzeichnis)] [제1문 생략] 또한 그(수색 당사자)의 요청이 있는 경우에는 유치·압수된 대상물의 목록을 교부하여야 하며, 혐의 있는 물건이 발견되지 않은 경우에는 이에 관한 증명서를 교부하여야 한다.

163) 실무에서는 일련번호, 대상물에 대한 간략한 설명 등이 수기로 채워지는 양식화된 목록(서식)이 이용된다; 하지만 이들이 연방차원에서 통일적으로 정해져 있지는 않다(*Kemper*, wistra 3/2008, 96 [Fn. 9]).

다면 현장에서 바로 작성·교부되어야 한다.[164] 하지만 이것이 불가능한 경우, 특히 방대한 서류나 디지털 정보가 확보되는 경우에는[165] 그 작성·교부가 StPO 제110조에 따른 임시확보와 열람 후에 즉시 행해져야 한다.[166]

압수목록의 작성에 있어서 가장 중요한 것은 대상물을 적절한 방식으로 식별할 수 있게 하는 것, 즉 대상물의 명확한 식별 가능성 내지 구별 가능성이다.[167] 디지털 정보의 압수와 관련하여 정보저장매체 자체 또는 거기에 저장된 정보 전체나 대부분이 압수된 경우에는 확보된 정보가 집합명칭을 통해 표시되는 것으로 충분하다.[168] 또한 해당 목록으로부터 정보나 파일의 본질적인 구조뿐만 아니라, 그들이 당사자에게서 직접 확보되었는지, 아니면 StPO 제110조 제3항에 따라 공간적으로 떨어진 저장매체에서 확보되었는지, 그리고 데이터베이스 전체가 확보되었는지, 아니면 개별 파일만이 확보되었는지도 인식될 수 있어야 한다.[169]

(3) 수색절차의 위반과 그 법적 효과

독일 문헌의 지배적인 견해와 BGH의 2007년 결정에 따르면, StPO 제105조 제2항, 제106조, 제107조 제1문은 법관이나 수사기관이 그 준수를 임의로 배제할 수 있는 질서규정이 아니라 수색 당사자의 기본권 보호에 이바지하는 중요한 절차를 규정한 강행규정이며, 수색의 적법성은 동 규정들의 준수에 좌우된다.[170] 그 논리적인 결과로

---

164) *OLG Stuttgart* StV 1993, 235; *Bruns*, KK-StPO, § 107 Rn. 4; *Wohlers/Jäger*, SK-StPO, § 107 Rn. 8.

165) *Kemper*, wistra 3/2008, 96. 97 f.

166) *BGH* NStZ 2003, 670; *Bruns*, KK-StPO, § 107 Rn. 4 f.

167) *Bruns*, KK-StPO, § 107 Rn. 4; *Kemper*, wistra 3/2008, 96, 96 f.; *Köhler*, M-G/Schmitt, § 107 Rn. 3; *Park*, Rn. 213; *Wohlers/Jäger*, SK-StPO, § 107 Rn. 7 u. § 109 Rn. 2.

168) *Kemper*, wistra 3/2008, 96, 99.

169) *Kemper*, wistra 3/2008, 96, 99.

170) *BGHSt* 51, 211, 213 ff. [Rn. 6-8]; *Bruns*, KK-StPO, § 105 Rn. 14; *Köhler*, M-G/Schmitt, § 105 Rn. 10, § 106 Rn. 1 u. § 107 Rn. 1; *Park*, Rn. 171 u. 176; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 58 u. § 106 Rn. 27; *Zimmermann*, JA 5/2014, 321, 323; a.A. *Hofmann*, NStZ 2005, 121, 124. 법관에게는 비밀리에 집행될 수색을 StPO 제102조에 근거하여 명령하는 것이 금지되고, 수사기관에게는 동조에 따른 법관의 명령을 의도적으로 비밀리에 집행하는 것이 금지된다(*BGHSt* a.a.O. [Rn. 9]; *Hamm*, NJW 2007, 930, 932). 이 BGH 결정에 의해 수색에서의 StPO 제106조 제1항 제1문에 따른 출석권의 침해가 수색 자체의 적법성에는 아무 영향도 미치지 않을 것이라고 판결한 그의 과거의 판결(NStZ 1983, 375, 376)은 더 이상 유지될 수 없다. 반면, 지배적인 견해에 따르면 StPO 제109조는 순수한 질서규정이기 때문에, 그 위반은 압수의 법적 효력에 영향을 주지 않을 뿐만 아니라, 당연히 증거사용금지도 발생시키지 않는다(*Bruns*, KK-StPO, § 109 Rn. 1; *Kemper*, wistra 3/2008, 96, 97; *Köhler*, M-G/Schmitt, § 109 Rn. 2; *Wohlers/Jäger*, SK-StPO, § 109 Rn. 4).

해당 규정에 대한 위반의 경우 당사자에게는 독일 형법(Strafgesetzbuch, 이하 "StGB") 제32조에 따른 정당방위가 가능하다.[171] 반면, BGH는 위 2007년 결정에서 위 StPO 규정들의 불준수가 – 수사행위를 위법하게 만드는 것을 넘어 – 획득된 정보의 사용금지의 결과를 가져오는지에 대해 심사하지 않았다.[172] 이와 관련하여 동 법원은 '최소한 중대하거나, 인식 있거나, 자의적인 절차위반의 경우에(zumindest bei schwerwiegenden, bewussten oder willkürlichen Verfahrensverstößen)'(만) 하자 있는 압수·수색의 결과로서 증거사용금지가 요청된다는 BVerfG의 결정[173]을 참고로 인용하였을 뿐이다.[174] 독일 문헌의 지배적인 견해 또한 이와 다르지 않다.[175] 따라서 현재 독일에서 해당 규정들의 효력은 이 한도로 제한된다.[176]

나. 디지털 정보 자체의 압수대상성

정보기술시스템 등 정보저장매체가 유체물로서 압수수색의 대상물이라는 점에는 독일에서도 이론이 없다. 따라서 디스켓, CD, DVD, USB 등의 외부 저장매체 및 PC, 스마트폰 등의 개인 정보처리장치, 그리고 ISP/CP나 기업의 서버[177]도 StPO 제94조 제1항의 '대상물'과 제102조의 '물건'에 속하고, 디지털 정보의 출력물도 유체물로서

---

171) *Köhler*, M-G/Schmitt, § 105 Rn. 11; *Park*, Rn. 176; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 58.

172) *Park*, Rn. 171.

173) *BVerfGE* 113, 29, 61 [Rn. 135].

174) *BGHSt* 51, 211, 214 [Rn. 8].

175) *Amelung*, NJW 1991, 2533, 2538 [Tz. 4]; *Bruns*, KK-StPO, § 105 Rn. 21, § 106 Rn. 6 u. § 107 Rn. 5; *Köhler*, M-G/Schmitt, § 105 Rn. 11 u. 18 f.; *Park*, Rn. 415-419; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 80, § 106 Rn. 28 u. § 107 Rn. 10; *Roxin/Schünemann*, § 35 Rn. 9; a.A. *Krekeler*, NStZ 1993, 263, 268: "(규정들의) 침해는 위법하게 획득된 증거방법의 사용불가능성을 야기해야 한다."
※ 독일 법제에는 위법수집증거법칙이 수용되어 있지 않다. 다만 이와 비교될 수 있는 '증거사용금지(Beweisverwertungsverbot)'가 이론상 인정되고, 법률상 부분적으로 수용되어 있으나(예를 들어, StPO 제100조d 제2항과 제5항, 제136조a 제3항), 학계의 지배적인 견해 및 BVerfG의 지속적인 판례에 따르면 증거사용금지는 독일 법제에서 예외적인 것이다. 즉 실체적 진실주의에 기초한 독일 소송모델에서 증거사용금지는 자명한 것이 아니며(*Roxin/Schünemann*, § 24 Rn. 13), 하자 있는 압수수색의 결과로서의 '최소한 중대하거나, 인식 있거나, 자의적인 절차위반의 경우'에만 요청된다(*BVerfGE* 113, 29, 61 [Rn. 135]; NJW 2011, 2417, 2419 [Rn. 45]; *Köhler*, M-G/Schmitt, § 105 Rn. 19; *Roxin/Schünemann*, § 24 Rn. 51).

176) *Park*, Rn. 171.

177) 서버는 일반적으로 인터넷을 통해 e-mail, SNS, cloud-computing 등의 서비스를 제공하기 위한 컴퓨터를 지칭하며, 대용량의 정보저장매체 또는 고성능의 정보처리장치라 할 수 있다.

압수능력이 있다는 점은 명백하다.[178] 이외에 수사기관에 의해 확보된 정보를 읽고 볼 수 있게 하는 기술적 보조수단, 즉 정보를 현출하는 특수한 소프트웨어나 컴퓨터 프로그램도 필요한 경우 함께 확보·이용될 수 있다.[179] 하지만 규범명확성의 측면에서 StPO의 문언상 디지털 정보 자체가 압수대상성을 갖는지는 명확하지 않다.

우선 한 견해에 따르면 유체물인 정보저장매체만이 StPO 제94조에 따라 압수될 수 있고, 거기에 저장된 디지털 정보는 유체물이 아니므로[180] 또는 형체화되어 있지 않기 때문에[181] 그 자체로 압수될 수 없다.[182] 다만, 이 견해에 따르더라도 정보만이 형사소추기관의 저장매체로 복제되거나 옮겨지는 것은 정보저장매체 자체의 압수보다 덜 침해적이기 때문에 비례성 원칙에 따라 가능하고 허용된다.[183] 즉, 이 견해에 따르면 디지털 정보의 '복제'나 '옮김'은 형사절차법의 측면에서 개념적으로 StPO 제94조에 의해 포섭되지 않는 완전히 다른 유형의 처분이지만,[184] 2008년 개정[185]으로 신설된 StPO 제110조 제3항(뒤의 3. 가. 참고)은 이런 작업방식을 명확히 허용한다고 여긴다.[186] 반면, 디지털 정보 자체의 압수대상성을 긍정하는 입장은 동 규정의 입법이 디지털 정보가 StPO 제94조 의미의 대상물로서 압수될 수 있다는 점의 근거가 된다고 주장한다.[187] 물론 기존의 압수 개념에 따르면, 디지털 정보의 복제 후에도

---

178) *Köhler*, M-G/Schmitt, § 94 Rn. 4.

179) *Greven*, KK-StPO, § 94 Rn. 4; *Kemper*, NStZ 2005, 538, 540 [Fn. 30]; *Köhler*, M-G/Schmitt, § 94 Rn. 4; *Park*, Rn. 800 u. 812.

180) *Klesczewski*, ZStW 123 (2011), 737, 747: 유체물만; *Roxin/Schünemann*, § 34 Rn. 4; *Wohlers/Greco*, SK-StPO, § 94 Rn. 26. BGH는 과거 'Mailbox에 저장된 정보'의 압수수색을 위한 법적 근거를 판단함에 있어서, 해당 처분은 유형의 대상물의 확보가 아니기 때문에 또는 주거나 기타 공간 내로의 유형의 침입이 아니기 때문에 압수수색 일반규정의 직접적인 적용이 배제된다고 설시했었다(NJW 1997, 1934, 1935).

181) *Kemper*, NStZ 2005, 538, 540 u. 541: "정보저장장치에 형체화된 정보가 확보·압수될 수 있다는 것을 입법자가 정말로 근거로 삼으려면, 그는 이것을 법률에 명백히 표현할 수 있고, 그래야 한다, 특히 이러한 기본적인 법질서의 문제와 관련되는 경우."

182) *Kemper*, NStZ 2005, 538, 540 f.; *Klesczewski*, ZStW 123 (2011), 737, 747; *Roxin/Schünemann*, § 34 Rn. 4; *Wicker*, MMR 2013, 765, 766; *Wohlers/Greco*, SK-StPO, § 94 Rn. 26.

183) *Greven*, KK-StPO, § 94 Rn. 4 u. 13; *Kemper*, NStZ 2005, 538, 540; *Roxin/Schünemann*, § 34 Rn. 4; *Wohlers/Greco*, SK-StPO, § 94 Rn. 26.

184) *Klesczewski*, ZStW 123 (2011), 737, 747.

185) Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlini 2006/24/EG (TKÜG) vom 21. Dezember 2007, BGBl. I S. 3198.

186) 반면 다른 한 견해는 압수·수색을 위한 '복제물' 생성의 허용성은 입법자의 개입을 통해서 해결되어야 한다고 주장한다(*Kemper*, NStZ 2005, 538, 541 f.).

187) *Hofmann*, NStZ 2005, 121, 123; *Park*, Rn. 799.

피의자가 해당 정보에 접근할 가능성이 배제되지 않기 때문에, 정보의 복제나 옮김이 압수의 개념에 포섭되는지가 의문일 수 있다. 하지만 이 반대견해는 StPO 제94조에 따른 압수는 본질적으로 처분권 박탈이 아닌 범죄의 조사와 규명을 위한 증거확보를 목적으로 하고,[188] 동 규정은 증거방법으로서 조사에 중요할 수 있는 모든 물건에 적용된다는 점에서,[189] 무형의 디지털 정보도 압수의 대상에 속한다고 한다.[190]

한편 독일의 입법자는 1992년 개정[191]에서 디지털 정보의 자동화된 비교분석을 허용하는 StPO 제98조a-c를 창설하였으며, 2004. 8. 24.의 제1차 사법현대화법을 통한 개정(이하 "2004년 개정")[192]의 입법자료에 따르면, "StPO 제110조 제1항은 ……, '서류'의 개념에는 모든 유형의 문서가 포함되는데, 전자문서도 포함된다."[193] 독일의 입법자는 또한 2021년 개정에서 StPO 제110조 제3항과 제4항을 통해 '정보의 (임시)확보'가 허용됨을 명백히 하였다. 이외에 BVerfG 또한 컴퓨터 하드디스크에 저장된 모든 정보의 복사본에 대한 압수결정을 대상으로 한 헌법소원 심사에서 다음과 같이 설시하였다: "(StPO 제94조) 문언의 의미는 무체물도 '대상물'로 이해하는 것을 허용한다. 무체물이 제94조에 포섭된다고 하더라도 …… 그 문언의 한계를 넘은 것은 아니다."[194]

다. StPO에서 증거확보를 위한 법적 근거의 법체계적 구성

형사소추 목적의 증거확보를 위한 법적 근거의 구성과 관련하여 StPO는 비례성 원칙에 근거하여 처분의 집행 유형과 방식 및 그 침해강도에 따라 단계적인 규범체계를 형성하고 있다. 이 체계는 크게 3단계로 구분할 수 있다: StPO 제161조 제1항, 제163조

---

188) *Sieber*, 69. DJT 2012, C 114: "StPO의 정보기술의 새로운 도전에의 적응의 과정에서 유형의 가시적인 대상물을 위해 발전된 압수의 '박탈개념'은 무형물의 증거사용과 몰수를 위한 별도의 개념을 통해 보충되어야 한다."

189) *BVerfGE* 113, 29, 51 [Rn. 102]; 124, 43, 61 [Rn. 63].

190) *Bär*, EDV-Beweissicherung, Rn. 407; *Graulich*, wistra 8/2009, 299; *Meininghaus*, Der Zugriff auf E-Mails, 203 f.; *Köhler*, M-G/Schmitt, § 94 Rn. 4 u. 16a; *Park*, Rn. 799; *Singelnstein*, NStZ 2012, 593, 596 f. u. 602; *Zimmermann*, JA 5/2014, 321, 322.

191) Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) vom 15. Juli 1992, BGBl. I S. 1302.

192) Erstes Gesetz zur Modernisierung der Justiz (1. Justizmodernisierungsgesetz, JuMoG) vom 24. August 2004, BGBl. I S. 2198.

193) BT-Drs. 15/1508, S. 24.

194) *BVerfGE* 113, 29, 50 [Rn. 100].

제1항의 '수사 일반조항(Generalklauseln der Ermittlung)'[195], StPO 제94조 이하, 제102조 이하의 '압수수색 일반규정(allgemeine Vorschriften der Beschlagnahme und Durchsuchung), 마지막으로 비밀의 수사처분을 위한 StPO 제99조 이하의 '독자적인 수권규범(selbstständige Ermächtigungnormen)'[196]. 위 일반조항과 일반규정에는 – 그 '일반'이라는 명칭이 이미 보여주듯이 – 처분의 집행 유형과 방식에 대한 제한이 없거나 부분적으로만 존재한다. 반면에 StPO 제99조 이하의 처분들은 전체적으로 압수수색 일반규정에 비하여 가중된 처분요건 및 절차법적 통제장치와 결부되어 있다. 이들은 그 집행의 유형과 방식, 특히 '비밀성'에 따른 가중된 기본권 침해강도 때문에 새로운 독자적인 성질을 가지므로 개별적인 정당화가 요구된다.[197] 이러한 단계적인 규범체계로부터 수사 일반조항, 압수·수색 일반규정, 각 독자적인 수권규범들은 상호 특별·보충 관계에 있다는 점이 도출된다.[198]

수사 일반조항인 StPO 제161조 제1항과 제163조 제1항은 수사기관의 임무 내지 의무 및 권한만을 규정하지만,[199] 동 일반조항으로부터 "수사절차의 자유로운 형성의 원칙(Grundsatz der freien Gestaltung des Ermittlungsverfahrens)"이 도출되고,[200] 이에 근거하여 수사기관은 모든 유형의 – 공개의 또는 비밀의 – 수사를 행할 수 있다. 하지만 이것은 StPO의 특별한 수권규범에 포섭되지 않는, 즉 기본권을 침해하지 않거나 단지 경미하게 침해하는 수사행위만을 정당화한다("보충적 법적 근거").[201] 형사절

195) StPO 제161조 [검찰의 일반적 수사권한(Allgemeine Ermittlungsbefugnis der Staatsanwaltschaft)] ① 검찰은 제160조 제1항 내지 제3항에 규정된 목적을 위하여, 다른 법률규정이 특별히 규제하지 않는 한, 모든 관청으로부터 정보(제공)를 요청할 권한이 있으며, 모든 유형의 수사를 직접 행하거나 경찰청과 경찰공무원을 통해 행할 수 있다. 경찰청과 경찰공무원은 검찰의 요청이나 지시에 따를 의무가 있으며, 이 경우 그는 모든 관청으로부터 정보(제공)를 요청할 권한이 있다.
StPO 제163조 [수사절차에서의 경찰의 임무(Aufgaben der Polizei im Ermittlungsverfahren)] ① 경찰청과 경찰공무원은 사건의 증거인멸을 방지하기 위해 범죄를 조사하고, 즉시 발해질 수 있는 모든 명령을 내려야 한다. 이를 위해 경찰청과 경찰공무원은, 다른 법률이 그 권한을 특별히 규제하지 않는 한, 모든 관청에게 정보(제공)를 요청할 권한이 있으며, 지체의 위험이 있는 경우에도 정보(제공)를 요청할 수 있고, 모든 유형의 수사를 행할 수 있다.

196) StPO 제1편 제8장의 압수수색 및 정보수집과 관련된 수권규범 중에서 StPO 제98조a-c과 제111조는 신원확인을 위한 처분인 '자동화된 비교분석(Rasterfahndung)'과 검문소 설치의 수권규범으로서 증거확보를 위한 처분과 관련이 없고, StPO 제111조a 이하는 압수 집행의 방법 등에 관한 것이다.

197) *BGHSt* 51, 211, 215 [Rn. 10]. 이에 대해서는 뒤의 4. 나. 1) 참고.

198) 유사한 취지의 기술로는 *BVerfGE* 124, 43, 58 f. [Rn. 58].

199) *Volk/Engländer*, § 10 Rn. 1.

200) *Schmitt*, M-G/Schmitt, § 161 Rn. 7 u. § 163 Rn. 64; *Roxin/Schünemann*, § 39 Rn. 23; *Volk/Engländer*, § 10 Rn. 1.

차에서 강제(Zwang)는 법률유보 원칙에 따라 형사절차법이 그것을 허용하는 경우에만 가능하기 때문에,[202] 위 일반조항은 강제처분의 법적 근거가 될 수 없다.[203] 반면 StPO 제99조 이하의 독자적인 수권규범들은 처분의 집행 유형과 방식을 구체적으로 규정함으로써 각 규정에 의해 허용되는 처분을 엄격히 제한하며, 처분요건과 절차법적 통제장치가 각 처분의 침해강도에 따라 비례적으로 각각 다르게 규정되어 있다. 결국 StPO의 압수수색 일반규정은 강제처분인 압수수색을 규제하므로 그 적용에 있어서 수사 일반조항에 우선하지만,[204] 증대된 침해강도를 갖는 처분이나 특별한 방법의 정보수집을 정당화하기 위한 법적 근거인 StPO 제99조 이하의 수권규범보다는 후순위이다. 이런 점에서 해당 일반규정은 수사 일반조항에 근거해서는 정당화될 수 없을 정도로 기본권을 침해하지만, StPO 제99조 이하에 따른 처분의 침해보다는 경미하거나 그 집행 유형과 방식이 동 규정에 의해 포섭될 수 없는 처분들을 정당화한다.

한편 이러한 단계적인 규범체계는 추상적·개념적인 것으로서 구체적인 경우, 특히 기존 규정에 근거하지만 (과학)기술적 환경의 변화에 따라 예상치 못한 강력한 기본권 침해를 야기하는 처분 또는 기존 규정에 포섭될 수 없는 새로운 유형의 처분에서 그 수권규범이 무엇인지가 종종 명확하지 않다. 이와 관련하여 독일에서는 특히 '비밀의' 정보수집이 압수수색 일반규정에 의해서도 허용되는지, 아니면 기존의 통신감청 규정에 근거할 수 있는지, 이것도 아니면 새로운 수권규범이 필요한지가 문제되었다. 이에 대해서는 별도로 자세히 다룬다(뒤의 4).

---

201) *BGHSt* 51, 211, 218 [Rn. 21]; 55, 138, 143 [Rn. 18]; *Schmitt*, M-G/Schmitt, § 161 Rn. 1; *Kudlich*, GA 2011, 193, 198; *Soiné*, NStZ 2014, 248, 251 [Tz. Ⅳ]; *Wohlers*, SK-StPO, § 161 Rn. 4. 위 일반조항은 개인정보의 일반적인 수집 및 민간기관에 대한 정보조회, 즉 금융회사에의 정보조회를 위한 법적 근거를 형성하며(*BVerfG* NJW 2009, 1405, 1407 [Rn. 26], *Singelnstein*, NStZ 2012, 593, 603), StPO 제95조 제1항에 근거한 제출요청도 이러한 수사행위에 속한다(*LG Koblenz* wistra 9/2002, 359).

202) *Schmitt*, M-G/Schmitt, Einl. Rn. 45 u. § 163 Rn. 32.

203) 이런 점에서 StPO의 수사 일반조항은 우리 법제상 검찰과 경찰의 수사권 규정인 형소법 제196조 제1항과 제197조 제1항 및 임의수사의 법적 근거인 형소법 제199조 제1항 제1문에 상응하는 규정이라 할 수 있다.

204) *Singelnstein*, NStZ 2012, 593, 603.

3. 디지털 정보의 수색 방법

가. StPO 제110조[205]

StPO 제110조 [서류와 정보저장매체의 열람]

① 수색 당사자의 서류를 열람할 권한은 검찰 및 검찰의 명령을 받은 그의 수사관(GVG 제152조)에게 있다.

② 그 밖의 경우 (검찰 및 그의 수사관이 아닌 다른) 공무원은 서류의 점유자가 열람을 허용한 경우에만 발견된 서류를 열람할 수 있다. 그렇지 않은 경우 해당 공무원은 열람이 필요하다고 생각되는 서류를 점유자 입회하에 관인을 찍어 봉인된 봉투로 검찰에게 교부해야 한다.

③ 수색 당사자의 정보저장매체에 대한 열람 또한 제1항과 제2항의 기준에 따라 허용된다. 이 열람은 해당 저장매체와 공간적으로 떨어져 있지만 그것으로부터 접근될 수 있는 저장매체에까지도 확대될 수 있다; 단, 그렇지 않으면 찾고 있는 데이터의 상실이 우려되는 경우이어야 한다. 수사에 중요할 수 있는 데이터는 확보될 수 있다.

④ 서류가 열람을 위해 반출되거나 정보가 임시로 확보된 경우, 제95조a와 제98조 제2항이 준용된다.

1) 이력 및 의미와 목적

StPO가 창설되던 때(1879. 10. 1.)부터 존재하는 StPO 제110조는 지금까지 총 6차례 개정되었는데, 중요한 개정 사항은 다음 3가지이다. 첫째로, 서류의 열람권자가 처음에는 법관만이었으나, 1968년의 개정을 통해 검찰이 추가되었고,[206] 2004년 개정에서 검찰의 수사관인 사법경찰도 추가되었다. 이러한 열람권자의 지속적인 확대는 실무상 열람되어야 하는 서류의 양이 증가했기 때문이다. 둘째로, StPO 창설시부터 제3항에는 서류 점유자의 참여권이 규정되어 있었는데, 동 조항은 2004년 개정으로 삭제되었다. 하지만 독일에서 해당 참여권의 인정 여부는 여전히 논란이 되고 있다. 이에 대해서는 별도로 자세히 다룬다(아래 나.). 셋째로, 2007년 개정을 통해 – 2004년 개정으로

---

205) 아래의 내용은 박중욱, "수사기관 내에서의 범죄혐의 관련 정보 탐색 등 행위의 법적 성격 – 독일 형사소송법 제110조에 관한 논의를 참고하여 –", 『비교형사법연구』 제24권 제4호, 한국비교형사법학회, 2023.1, 347, 358-368면의 내용을 요약한 것이다.

206) Einführungsgesetz zum Gesetz über Ordnungswidrigkeiten (EGOWiG) vom 24. Mai 1968, BGBl. Ⅰ S. 503.

삭제되었다가 – 다시 신설된 제3항에 원격 압수수색이 신설되었다(아래 다.).[207] 이 조항의 내용은 2021년 개정을 통해 현재와 같이 제3항과 제4항으로 나누어졌다.

StPO 제110조의 입법목적은 서류와 정보저장매체에 대한 압수수색의 집행에서 개인의 인격보호와 정보보호인데, 제1항과 제2항의 '열람권 제한' 및 제3항과 제4항의 '임시확보'는 그것을 위한 것이다. 독일 문헌에 따르면 실무상 열람권 제한을 통한 정보보호는 거의 구현되지 않고 있다.[208] 이런 이유로 현재 StPO 제110조는 수사기관의 과도한 개인정보 침해를 제한하기 위한 수단인 열람 및 그것을 위한 임시확보의 법적 근거로서만 의미를 가진다.[209]

StPO 제110조에 따른 열람은 서류 등이 최종적으로 압수 또는 환부되어야 하는지를 심사하는 수단이다.[210] 이런 점에서 동 규정은 수사절차에서의 기본권 보호를 위한 규정이다.[211] 서류 등의 내용이 무관정보인 경우 또는 절대적으로 보호되는 핵심영역에 속하는 정보로서 헌법상 증거사용금지가 고려되거나 StPO 제97조의 압수금지물에 속하는 것이 명백한 경우에는 그것에 대한 열람은 가능한 한 억제되어야 한다는 점에서, StPO 제110조의 열람은 기본권 침해강도의 완화를 목적으로 한다.[212]

2) 구성요건의 개념과 적용범위

독일의 지배적인 견해에 따르면 StPO 제110조 제1항의 '서류(Papiere)'는 – 2021년 개정 전부터 – 광의로 해석되었다.[213] 따라서 내용상 의미가 있는 모든 기록물이 해당 서류의 개념에 포함되며, 정보매체의 종류는 상관없기 때문에 종이뿐만 아니라 다른 물질이나 체계가 이용되는 매체도 본 규정의 서류로서 간주될 수 있다.[214] 즉,

---

207) (2008. 1. 1.부터 2021. 6. 30.까지 유효했던) ③ 수색 당사자의 정보저장매체에 대한 열람은 그것으로부터 공간적으로 떨어져 있지만 접근될 수 있는 저장매체에도 확대될 수 있다; 단, 그렇지 않으면 찾고 있는 정보의 상실이 우려되는 경우이어야 한다. 수사에 중요할 수 있는 정보는 확보될 수 있다; 제98조 제2항이 준용된다.

208) *Park*, Rn. 262.

209) *Wohlers/Jäger*, SK-StPO, § 110 Rn. 6; *Doege*, NStZ 2022, 466.

210) *Köhler*, M-G/Schmitt, § 110 Rn. 2; *Cordes/Reichling*, NStZ 2022, 712, 713. 서류에서 어느 것이 찾고 있는 증거방법인지, 아니면 압수금지의 정보인지는 열람 이후에야 비로소 명확해질 수 있다(*OLG Koblenz* NStZ 2007, 285, 286 [Rn. 5]).

211) *Bär*, CR 1999, 292, 294; *Park*, Rn. 228: 특별규정.

212) *BVerfGE* 113, 29, 58 [Rn. 126]; 124, 43, 72 [Rn. 96]. [박중욱, 각주 205의 논문, 360-361면(재인용)]

213) *BGH-Ermi-Ri* CR 1999, 292, 293; *Köhler*, M-G/Schmitt, § 110 Rn. 1; *Park*, Rn. 232.

214) *BGH* NStZ 2003, 670, 671 [Rn. 6]; *Bruns*, KK-StPO, § 110 Rn. 2; *Dauster*, StraFo 6/1999,

녹음·영상 저장장치와 같은 아날로그 미디어뿐만 아니라 모든 유형의 디지털 정보저장장치(예를 들어 PC, 태블릿 PC, 스마트폰, ISP/CP의 서버 등) 및 거기에 저장되어 있는 e-mail을 포함한 모든 유형의 디지털 정보도 StPO 제110조의 적용영역에 속한다.[215] 나아가 정보의 현출에 필요한 소프트웨어와 하드웨어도 서류의 개념에 포함된다. 이러한 해석은 2021년 개정 통해 StPO 제110조 제3항 제1문에 "정보저장매체" 문언이 추가되었으므로 여전히 유효할 뿐만 아니라 입법적으로 더 명확해졌다고 할 수 있다.[216]

StPO 제110조의 '열람(Durchsicht)'이란 그 내용을 들여다보는 것, 즉 그 내용의 지득이다.[217] 지배적인 견해와 BVerfG는 동 규정의 입법취지를 고려하여 열람의 성격을 수색으로 여긴다.[218] 따라서 이 열람은 압수범위에 관한 최종적 결정 전에 행해지며,[219] 서류 등이 열람 중인 경우에는 수색이 아직 진행 중인 것이다.[220] 따라서 서류의 점유자 등은 StPO 제106조 제1항에 따라 열람에 출석할 수 있다(아래 나.). 압수 후에는 StPO 제109조의 목록이 StPO 제107조 제2항에 따라 서류의 점유자에게 교부되어야 한다.[221] 디지털 정보의 수집방법과 관련하여 개인정보가 온라인으로 연결된 외부 저장매체에 저장되어 있는 경우, 수사기관은 수색과정에서 발견된 정보기술시스템을 경유하는 방법으로 열람을 확대할 수 있다(아래 다.). 한편 수색의 과정에서 우연히 발견된 증거방법(Zufallsfunde)은 StPO 제108조[222]에 따라 임시로 압수될 수 있

186; *Köhler*, M-G/Schmitt, § 110 Rn. 1; *Park*, Rn. 232 f.; *Peters*, NZWiSt 2017, 465, 467; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 8. [박중욱, 각주 205의 논문, 361면의 각주 49(재인용)]

215) *BVerfGE* 113, 29, 50 f. [Rn. 100 f.] und NJW 2002, 1410: 노트북에 저장되어 있는 정보; *BVerfGE* 124, 43, 68 f. [Rn. 87 f.] und NJW 2014, 3085, 3088 [Rn. 44]: 서버에 저장되어 있는 e-mail. [박중욱, 각주 205의 논문, 361면의 각주 49(재인용)]

216) 박중욱, 각주 205의 논문, 361면의 각주 49.

217) *Graulich*, wistra 8/2009, 299, 300; *Park*, § 2 Rn. 234; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 12 und 20.

218) *BVerfGE* 124, 43, 75 f. [Rn. 107]; NJW 2003, 2669, 2670; *BGH* StV 1988, 90; NStZ 2003, 670, 671 [Rn. 2]; *OLG Jena* NJW 2001, 1290, 1293; *Brodowski/Eisenmenger*, ZD 3/2014, 119, 120; *Bruns*, KK-StPO, § 105 Rn. 20; *Köhler*, M-G/Schmitt, § 110 Rn. 2; *Michalke*, StraFo 3/2014, 89, 91; *Szesny*, WiJ 2012, 228, 230 [Tz. 1)]; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 2.

219) *BVerfGE* 113, 29, 56 [Rn. 118]; 124, 43, 68 f. [Rn. 88] und 75 [Rn. 106]; NJW 2003, 2669, 2670; *Szesny*, WiJ 2012, 228, 230 [Tz. 1)]); *Cordes/Reichling*, NStZ 2022, 712, 713.

220) *BGH* NStZ 2003, 670, 671 [Rn. 2].

221) 이때 서류가 임시로 확보되었고 그것이 어느 관청으로 옮겨지는지에 대한 안내도 포함되어야 한다(*Graulich*, wistra 8/2009, 299, 302 [Tz. 4.5]).

222) StPO 제108조 [압수 대상물 아닌 물건의 압수(Beschlagnahme anderer Gegenstände)] ① 수색할

다.[223] 끝으로 StPO 제110조의 열람은 압수명령이 내려지면 종료하는데,[224] 열람 종료 후 최종적으로 압수된 서류나 정보를 확인하는 것은 더 이상 StPO 제110조 의미의 열람이 아니라 압수된 증거방법의 활용일 뿐이다.[225]

StPO 제110조 의미의 열람에서는 정보의 분류·분리의 가능성이 개별적인 상황에 따라 다양하게 고려되어야 한다.[226] 이때 관련성에 따른 정보의 분류는 예를 들어 주제·시간·인물별로 또는 적절한 검색어나 특별한 검색프로그램을 갖춘 검색기능의 이용을 통해서도 행해질 수 있다.[227] 이와 관련하여 독일 실무에서는 일반적으로 거의 언제나 2가지 리스트가 작성된다고 한다: "찾고 있는 구체화된 증거방법 리스트"(무엇을 찾는가)와 "검색어/색인어 리스트"(어떻게 찾을 것인가).[228] 전자는 압수되어야 하는 대상물과 관련된 것인 반면, 후자는 그러한 정보를 찾아내기 위한 수단, 즉 수색을 위한 도구이다. 검색어는 압수될 정보를 탐색하는 기능을 갖는다.[229] 수사기관은 압수수색 영장을 청구할 때 그때까지 밝혀진 사실관계에 근거하여 작성된 리스트를 첨부하여 영장을 청구해야 하고, 법관은 해당 리스트 목록의 적절성을 심사한 후 영장을 발부해야 하는데, 그는 리스트의 검색어를 부분적으로 – 경우에 따라서는 검사와의 협의를 통해 – 삭제·변경할 수도 있다.[230]

3) 임시확보

2021년 개정과 상관 없이 독일의 통설과 판례에 따르면 수사기관이 압수수색 현장에서 발견된 정보저장매체나 그 복제본을 StPO 제110조의 열람을 위해 자신의 사무실

때 해당 수사와 관련이 없으나 다른 범죄의 범행을 암시하는 물건이 발견된 경우, 그 물건은 임시로 압수될 수 있다. 이에 대해 검찰에게 통지되어야 한다. 제103조 제1항 제2문에 따른 수색의 경우에는 제1문이 적용되지 않는다. [②와 ③ 생략]

223) *Graulich*, wistra 8/2009, 299, 301; *Mildeberger/Riveiro*, StraFo 2004, 43, 44 [Tz. b)].

224) *Dauster*, StraFo 6/1999, 186. 188 f.

225) *OLG Bremen* wistra 1999, 74, 76; *Ciolek-Krepold*, Rn. 145; *Glock*, NStZ 2019, 248, 249 am Anfang; *Mildeberger/Riveiro*, StraFo 2004, 43, 44 [Tz. 1] und 46; *Park*, Rn. 229, 246 u. 261; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 27. [박중욱, 각주 205의 논문, 362-363면(재인용)]

226) *BVerfGE* 113, 29, 55 [Rn. 114-116]; 124, 43, 67 f. [Rn. 84-86]; *Köhler*, M-G/Schmitt, § 94 Rn. 19a. [박중욱, 각주 205의 논문, 363면(재인용)]

227) *BVerfGE* 113, 29, 55 f. [Rn. 116]; 124, 43, 68 [Rn. 86]. [박중욱, 각주 205의 논문, 363면(재인용)]

228) *Hiéramente*, wistra 11/2016, 432, 435. [박중욱, 각주 205의 논문, 363면(재인용)]

229) *Hiéramente*, wistra 11/2016, 432, 435 [Tz. (1)]. [박중욱, 각주 205의 논문, 363면(재인용)]

230) 박중욱, 각주 205의 논문, 363면.

로 반출하는 것은 "임시확보(Vorläufige Sicherstellung)"이고,[231] 이는 수색인 열람을 위한 (사전)조치이므로 압수가 아니라 '관청에서의 수색의 지속'을 의미한다.[232] 요컨대 개정 전 StPO 제110조 제3항에는 열람을 위해 서류나 정보저장매체가 '반출'되거나 '임시로 확보'될 수 있다는 문언이 명확하게 존재하지 않았으나, 지배적인 견해는 StPO 제110조, 더 근본적으로는 헌법상의 비례성 원칙에 근거하여 실무에서 그러한 집행 방법이 허용 또는 요청된다고 하였다.[233]

임시확보를 통해 반출된 서류는 권한 있는 자에 의해 지체 없이 열람되어야 하고, 이를 통해 적절한 기간 내에 압수가 청구되거나 환부·삭제되어야 한다.[234] 이때 관청에서의 열람의 기간은 본질적으로 검토되어야 하는 자료의 양과 내용의 어려움에 좌우되지만, StPO 제110조의 열람은 압수물의 활용이 아니라 확보된 서류 등이 압수되어야 하는지의 심사를 위한 것이므로 비례성 원칙에 따라 그것에 필요한 기간만이 허용된다.[235]

StPO 제110조에 따른 서류나 정보저장매체의 임시확보와 열람은 압수가 아니라 수색이지만, 피압수자나 피의자의 측면에서 그것은 수색에 근거한 고통보다는 압수와 유사한 고통을 야기한다.[236] 이런 이유로 임시확보가 그 분량 때문에 아직 종료되지 않고 있는 경우, 특히 영장에 명시된 기간을 초과하여 계속되는 경우, 검사는 StPO 제98조 제2항 제1문을 준용하여, 압수가 아닌 "열람을 위한 임시확보"를 위한 승인을 법원에 청구해야 하고, 수색 당사자는 StPO 제98조 제2항 제2문을 준용하여 임시확보

---

231) *BVerfG* NJW 2002, 1410, 1411; *BGH* NStZ 2003, 670; *BGH-Ermi-Ri* CR 1999, 292, 293; *Bruns*, KK-StPO, § 110 Rn. 4; *Köhler*, M-G/Schmitt, § 110 Rn. 2a; *Park*, Rn. 812; *Szesny*, WiJ 2012, 228, 229 u. 230 [Tz. 1)]; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 16.

232) *Hiéramente*, wistra 11/2016, 432, 438; *Kemper*, wistra 8/2010, 295, 297; *Köhler*, M-G/Schmitt, § 110 Rn. 10; *Park*, Rn. 249. [박중욱, 각주 205의 논문, 364면(재인용)]

233) *BVerfGE* 113, 29, 55 ff.; 124, 43, 67 ff.; NJW 2014, 3085, 3088 [Rn. 44 f.]; *BGH* 2010, 1297, 1298 [Rn. 19]; *OLG Jena* NJW 2001, 1290, 1293 f.; *BGH-Ermi-Ri* CR 1999, 292, 293; *LG Hildesheim* StraFo 3/2007 114, 115; *Bruns*, KK-StPO, § 110 Rn. 9; *Glock*, NStZ 2019, 248, 248 f.; *Hiéramente*, wistra 11/2016, 432, 439; *Köhler*, M-G/Schmitt, § 110 Rn. 2a u. 10; *Park*, Rn. 249; *Peters*, NZWiSt 2017, 465, 466; *Szesny*, WiJ 2012, 228, 229 f.; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 16. [박중욱, 각주 005의 논문, 364면(재인용)]

234) *LG Mühlhausen* StV 2003, 433, 434 [Rn. 35]; *LG Hildesheim* StraFo 3/2007, 114, 115; *Szesny*, WiJ 2012, 228, 232. [박중욱, 각주 205의 논문, 365면(재인용)]

235) 박중욱, 각주 205의 논문, 365면(재인용).

236) *BVerfG* NJW 2003, 2669, 2670; *BGH-Ermi-Ri* CR 1999, 292, 293; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 2. [박중욱, 각주 2058의 논문, 366면(재인용)]

와 열람의 정당성 및 비례성 원칙의 준수에 대한 심사를 법원에 청구할 수 있다.[237] 이러한 임시확보에 대한 적법성 통제는 2021년 개정을 통해 명확해졌다(StPO 제110조 제4항).[238]

4) 활용의 요청과 실무에서의 경시

앞에서 검토하였듯이 독일의 지배적인 견해와 최고법원의 지속적인 판례에 따르면 StPO 제110조의 입법취지는 서류와 정보저장매체에 대한 압수수색에서 유관정보만을 압수하고 무관정보는 환부 내지 삭제해야 한다는 것이고, 독일의 입법자는 2021년 개정을 통해 이러한 점을 명백히 하였다. 하지만 이러한 요청이 실무에서 종종 준수되지 않는다고 한다.[239] 한 견해는 압수명령과 수색명령이 하나의 서면, 소위 "결합-결정서(Kombi-Beschluss)"로 결부되어 발부되는 실무를 그 원인으로 지적하지만, 다른 한 견해는 이 결합-결정서에는 구분된 두 명령이 하나로 합쳐져 있을 뿐이라는 점에서 위헌의 우려가 있지는 않다고 한다.[240] 다만, 판례와 지배적인 견해에 따르면 동 결정서의 압수명령은 압수되어야 할 대상의 정확한 구체화가 이루어지지 않고 단지 종류에 따른 표현만이 행해진 경우라면 무효이고, 수색에 대한 지침으로서만 의미를 가질 뿐이라고 한다.[241] 따라서 이런 경우 압수 당사자는 동 결정서에 따른 압수에 대해 StPO 제98조 제2항 제2문에 따라 법관의 판단을 청구할 수 있다고 한다.[242]

---

237) *BVerfG* NJW 2002, 1410, 1411; NJW 2003, 2669, 2671; *BGH* StV 1988, 90; NStZ 2003, 670, 671; *BGH-Ermi-Ri* CR 1999, 292, 293 f.; *Bruns*, KK-StPO, § 110 Rn. 9; *Graulich*, wistra 8/2009, 299, 301 [Tz. 4.4]; *Köhler*, M-G/Schmitt, § 110 Rn. 10; *Mildeberger/Riveiro*, StraFo 2004, 43, 45; *Park*, Rn. 258; *Szesny*, WiJ 2012, 228, 235. [박중욱, 각주 205의 논문, 364면(재인용)]

238) 박중욱, 각주 205의 논문, 366면.

239) *Dauster*, StraFo 6/1999, 188, 188 f.

240) *Park*, Rn. 488. [박중욱, 각주 205의 논문, 368면(재인용)]

241) *BVerfG* NJW 1992, 551, 552; NStZ 2002, 212, 213 [Rn. 6]; *OLG Koblenz* NStZ 2007, 285, 286 [Rn. 6]; *LG Bielefeld* wistra 3/2008, 117, 119; *Graulich*, wistra 8/2009, 299, 300; *Köhler*, M-G/Schmitt, § 98 Rn. 9 u. 19; *Park*, Rn. 481. [박중욱, 각주 205의 논문, 368면(재인용)]

242) *BVerfG* NJW 1992, 551, 552; *BGH-Ermi-Ri* CR 1999, 292; *OLG Koblenz* NStZ 2007, 285, 286 [Rn. 6 f.]; *LG Essen* wistra 2/2010 78, 80; *Park*, Rn. 482; *Köhler*, M-G/Schmitt, § 98 Rn. 19; *Wohlers/Greco*, SK-StPO, § 98 Rn. 19. [박중욱, 각주 205의 논문, 368면(재인용)]

나. 열람에의 참여권 인정 여부[243]

1) 논의의 배경과 독일 연방헌법재판소의 입장 및 최근 Kiel 지방법원의 결정

독일에서도 디지털 정보의 과도한 압수가 문제되면서, 처분 당사자의 수색 과정에의 참여권 여부가 문제되었다. 이미 언급하였듯이 2004년 개정으로 참여권의 법적 근거 중 하나였던 (舊) StPO 제110조 제3항[244]이 '자세한 이유제시 없이 그리고 대체 규정도 없이' 삭제되었다.[245] 이에 대해 BVerfG는 2005년 결정에서 위 삭제에도 불구하고 개별적인 경우 비례성 준수를 위해 '피압수자'에게 참여권/출석권(Teilnahmerecht/Anwesenheitsrecht)이 제공될 수 있다고 설시하였고,[246] 2009년 결정에서 참여권 보장은 효과적인 형사소추와 정보침해의 강도를 고려하여 판단되어야 한다고 전제한 후,[247] 피압수자가 피의자 아닌 제3자라는 점만으로 임시확보된 정보에 대한 참여권이 헌법상 도출되지는 않는다고 설시하였다.[248]

위 BVerfG의 결정 이후 하급심에서 피압수자와 그의 변호인에게 열람 과정에의 참여권이 인정되는지가 여러 차례 심사되었지만, 그 (명확한) 법적 근거의 부재 및 비례성 원칙에 따라 – 예외적인 경우에만 – 인정될 수 있다는 BVerfG의 입장을 이유로 기각되었다.[249] 하지만 2021년 6월에 Kiel 지방법원(Landesgericht Kiel, 이하 "LG

---

243) 아래의 내용은 박중욱, "전자정보의 압수수색과 피의자의 참여권 – 대법원 입장의 비판적 수용 및 독일 논의의 참고 –", 『형사정책연구』 제34권 제1호, 한국형사·법무정책연구원, 2023.3, 29, 41-47면의 내용을 요약한 것이다. 다만 해당 논문에서도 밝히고 있듯이 독일에서의 견해 대립은 '피압수자'의 출석권/참여권에 대한 것이다. 현행 StPO에는 형소법 제121조와 같은 피의자의 참여권에 관한 규정이 없고, 피의자는 StPO 제106조 제1항 의미의 점유자가 아니기 때문에, 독일에서 피의자와 그의 변호인은, 특히 3자간 구조의 압수수색 사안에서 독자적인 참여권을 갖지 못한다.

244) (1879. 10. 1.부터 2004. 8. 31.까지 유효했던) ③ 서류의 점유자나 그의 대리인에게는 (관인 옆에) 자신의 인장을 같이 찍는 것이 허용된다; 그 이후 봉인해제와 서류열람이 명령되는 경우, 가능하다면 서류의 점유자나 그의 대리인에게는 참여가 요청되어야 한다.

245) *BVerfGE* 113, 29, 58 [Rn. 127]; 124, 43, 72 [Rn. 96]; *Hiéramente*, wistra 11/2016, 432, 438; *Park*, § 2 Rn. 253; *Szesny*, WiJ 2012, 228, 232 [Tz. 2)]. 위 규정의 문언이 피압수자의 참여권을 인정한 것이지는 명확하지 않으나, 독일의 지배적인 견해는 수사기관의 요청 의무에 근거하여 피의자의 참여권이 규정된 것으로 본다.

246) *BVerfG*, Beschluss vom 12. April 2005 - 2 BvR 1027/02 (= *BVerfGE* 113, 29, 58 f. [Rn. 126 f.]). 이 결정은 수사기관이 영장에 의해 피의자의 사무실을 수색하여 거기에 있는 서류 및 PC 등에 저장된 전자정보를 확보한 사안에 대한 것이다. [박중욱, 각주 243의 논문, 42면(재인용)]

247) *BVerfG*, Beschluss vom 16. Juni 2009 - 2 BvR 902/06 (= *BVerfGE* 124, 43, 72 [Rn. 96 a.E.]). 이 결정은 ISP/CP가 영장에 근거하여 메일서버에 저장된 피의자의 약 2,500개의 e-mail 복제본을 수사기관에 전달한 사안에 대한 것이다. [박중욱, 각주 243의 논문, 42면(재인용)]

248) *BVerfGE* 124, 43, 77 [Rn. 112]. [박중욱, 각주 243의 논문, 42면(재인용)]

Kiel")은 – 실무상 처음으로 – 참여권을 인정하는 결정을 내렸다.[250] 동 결정에 따르면 피의자 아닌 자인 피압수자에게서 (수사)절차와 관련성이 없는 것으로 추정되는 디지털 정보가 포괄적으로 확보된 상황에서 피압수자에게는 정보의 열람에 출석할 상당한 이익이 있고, 이는 절차촉진과 소송경제보다 후순위가 아니기 때문에 출석으로 인한 절차지연이 명확하지 않는 한 시간적 제한은 감수되어야 한다.[251]

2) 견해의 대립

위 BVerfG의 설시에 대해서는 여러 해석이 있지만 동 재판소가 참여권을 인정했다고 보기는 어렵다고 하는는 것이 일반적이다.[252] 왜냐하면 독일 법제에서 비례성 원칙은 기본권 침해의 정당성 및 한계를 심사하는 헌법상 기본원칙 중 하나이기도 하지만, 동시에 개별적인 사안에서 구체적 타당성을 기하기 위한 원칙이기도 하기 때문이다.[253] 이런 이유로 2004년의 (舊) StPO 제100조 제3항의 삭제와 위 BVerfG의 결정에도 불구하고 문헌에서는 수색인 열람의 과정에의 참여권 보장 여부가 지속적으로 문제되고 있다.

우선 참여권을 인정하는 견해는 입법자의 개정이유서에 그 삭제 이유가 특별히 언급되어 있지 않다는 점을 이유로[254] 해당 삭제를 단순한 '편집상의 실수

249) *LG Braunschweig*, Beschluss vom 12. April 2006 – 6 Qs 88/06, 6 Qs 97/06 (= BeckRS 2011, 9575); *LG Bonn*, Beschluss vom 23. August 2011 – 27 Qs 17/11 (= BeckRS 2013, 13669); *OLG Koblenz*, Beschluss vom 30. März 2021 – 5 Ws 16/21 (= NZWiSt 2021, 386).

250) *LG Kiel*, Beschluss vom 18. Juni 2021 – 3 Qs 14/21 (= NZWiSt 2021, 408). 이 결정은 실무에서 참여권을 인정한 첫 번째 사례라고 한다(*Buchholz*, NZWiSt 2021, 369, 370 f.; *Doege*, NStZ 2022, 466, 468). 그 사실관계에 따르면, 수사기관은 피의자에 대한 Kiel구법원(Amtsgericht Kiel, 이하 "AG Kiel")의 수색영장에 근거하여 그의 사무실, 즉 피의자 아닌 자인 협회(Verein)의 공간과 서버에 있는 정보를 임시로 확보하였고, 이 확보된 정보를 열람할 때 수사기관은 처음에 협회 변호인의 출석을 허용하였으나 2번의 출석 후 소송경제를 이유로 더 이상의 출석을 불허하였다. 이 불허 결정에 대해 해당 변호인은 AG Kiel에 (준)항고를 제기하였고, 동 법원은 출석을 허용하라는 결정을 내렸다. 이에 이번에는 검찰이 해당 AG Kiel의 결정에 대해 항고를 제기하였으나, LG Kiel은 이를 기각하였다.

251) *LG Kiel* NZWiSt 2021, 408. 이 결정의 심사대상은 피의자 아닌 피압수자(협회)의 변호인에게 StPO 제110조에 따른 열람에 대한 출석권이 인정되는지 여부이지만, 동 출석권은 피압수자의 출석권을 전제로 한다는 점에서 법이론적 쟁점은 본질적으로 동일하다.

252) *Hiéramente*, wistra 11/2016, 432, 438: "BVerfG는 …… 당사자에게 열람에의 출석이 허용되어야 하는지 여부에 대해 충분히 검토하지 않았다."

253) 박중욱, 각주 243의 논문, 44면.

254) BT-Drs. 15/3482, S. 21. 이런 이유로 동 삭제에 대해서는 입법자의 의도가 추론조차 되지 않는다거나(*Hiéramente*, wistra 11/2016, 432, 438), 최소한 StPO 제106조와의 체계적 연관성이 언급됐어야 했다(*Buchholz*, NZWiSt 2021, 369, 372)는 비판이 제기된다. [박중욱, 각주 243

(Redaktionsversehen)'라 여기고,[255] 헌법적 차원에서는 비례성 원칙으로부터, 형사절차법 차원에서는 StPO 제110조의 열람이 공개의 수사처분인 수색에 속한다는 체계적인 관점으로부터[256] 참여권이 여전히 도출된다고 여긴다.[257] 특히 후자와 관련하여 이 견해에 따르면 해당 열람이 공개적 성격을 갖는 수색에 속한다는 점, 참여권을 인정하지 않으면 동 열람은 사실상 통신감청 등과 같은 비밀의 수사처분이 된다는 점, StPO 제106조 제1항이 수색에의 참여권을 규정하고 있다는 점을 주요 근거로 제시한다.[258] 나아가 이 견해는 참여권 보장을 통해 StPO 제108조[259]에 반하는 위법한 수사행위인 '별건정보(Zufallsfunde)의 의도적 찾기'의 위험을 최소화할 수 있다고 한다.[260] 결국 참여권을 인정하는 견해는 2004년의 삭제가 – 의도치 않은 또는 중대한 – '규제흠결(Regelungslücke)'을 야기했고,[261] 출석권은 다시 입법화되어야 한다고 주장한다.[262]

반면, 참여권을 부정하는 견해의 핵심 근거는 2004년 개정에서의 그 삭제 자체에 있다.[263] 즉 참여권은 현재 법률상 존재하지 않으며, 입법자료에 삭제의 이유가 제시되지 않았다고 하여 그 삭제를 단순히 '편집상의 실수'라고 치부할 수는 없다는 것이다.[264] 그리고 StPO 제106조에 따른 출석권은 수색 현장에서 수색물을 현실로 보관하

의 논문, 44면(재인용)]

255) 이를 처음 언급한 것은 *Knauer/Wolf*, NJW 2004, 2932, 2937; 이에 동조하는 *Peters*, NZWiSt 2017, 465, 471 [Tz. 2]; *Buchholz*, NZWiSt 2021, 369, 371 f. 한편 그것이 실수인지는 확실하지 않다는 견해로는 *Wohlers/Jäger*, SK-StPO, § 110 Rn. 25. [박중욱, 각주 243의 논문, 44면(재인용)]

256) 이에 대해서는 뒤의 4. 가. 참고.

257) 박중욱, 각주 243의 논문, 44면.

258) *Knauer/Wolf*, NJW 2004, 2932, 2937 f.: "따라서 삭제에도 불구하고 기존의 법상태는 그대로이다"; *Szesny*, WiJ 2012, 228, 232 [Tz. 2)]; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 25; *Hiéramente*, wistra 11/2016, 432, 438 f.; *Peters*, NZWiSt 2017, 465, 470. [박중욱, 각주 243의 논문, 45면(재인용)]

259) StPO 제108조 [압수물 아닌 물건의 압수(Beschlagnahme anderer Gegenstände)] ① 수색의 기회에 해당 수사와 관련이 없으나 다른 범죄의 범행을 암시하는 물건이 발견된 경우, 이것은 임시로 압수될 수 있다. 이는 검찰에게 통지되어야 한다. [②과 ③ 생략]

260) *Szesny*, WiJ 2012, 228, 232 [Tz. 2)]; *Hiéramente*, wistra 11/2016, 432, 439; *Buchholz*, NZWiSt 2021, 369. [박중욱, 각주 243의 논문, 46면(재인용)]

261) *Peters*, NZWiSt 2017, 465, 470 a.E.; *Buchholz*, NZWiSt 2021, 369, 372. [박중욱, 각주 243의 논문, 46면(재인용)]

262) *Peters*, NZWiSt 2017, 465, 472. [박중욱, 각주 243의 논문, 46면(재인용)]

263) *Köhler*, M-G/Schmitt, § 110 Rn. 5; *Wenzl*, NStZ 2021, 395, 399; *Doege*, NStZ 2022, 466, 468. [박중욱, 각주 243의 논문, 46면(재인용)]

264) *Doege*, NStZ 2022, 466, 468. 특히 입법자가 최근 StPO 제110조에 대한 개정에서 참여권과 관련한 수정을 행하지 않았다는 점을 고려하면 더욱 그렇다(*LG Bonn* BeckRS 2013, 13669;

고 있는 점유자에게 인정되는 것이므로 반출된 후 수사기관 내에서 행해지는 열람에는 동 규정이 직접이든 유추로든 적용되지 않는다고 한다.[265]

다. 외부 저장매체로의 열람의 확대

오늘날 보편적으로 이용되는 정보통신서비스인 전자우편 서비스(e-mail service), SNS(social networking service), 클라우드 컴퓨팅(cloud-computing) 등은 기술적으로 IMAP(Internet messge access protocol)에 기반하기 때문에 ISP/CP의 서버에 저장된 정보는 정보주체인 서비스이용자가 그것을 의도적으로 삭제하지 않는 한 해당 서버에 계속 남아 있고, 이 정보는 범죄수사에 있어 중요한 증거가 된다. 따라서 수사기관이 서버에 저장된 정보를 정보주체가 삭제·훼손·은폐하기 전에 획득하려고 하는 것은 당연한 시도라 할 것이다. 수사기관이 압수수색 집행과정에서 발견된 PC나 스마트폰 등의 정보기술시스템을 이용하여 현장에서 곧바로 피압수자가 이용하는 정보통신서비스의 서버에 접근하여 거기에 저장된 정보를 열람·수집하는, 소위 '원격 압수수색'은 효과적인 집행방법이다. CCC 제19조[266] 제2항에 따르면 협약국은 동 원격 압수수색을 국내법으로 입법할 의무를 부담한다. 독일은 해당 내용을 2007년 개정을 통해 StPO 제110조 제3항 제1문(현재, 제2문)에 반영하였다.

Doege, a.a.O.). [박중욱, 각주 243의 논문, 46면(재인용)]

265) *LG Bonn* BeckRS 2013, 13669; *Doege*, NStZ 2022, 466, 468 f. [박중욱, 각주 243의 논문, 46-47면(재인용)]

266) CCC 제19조 [저장된 컴퓨터데이터의 수색과 압수(Search and seizure of stored computer data)] ① 각 협약국은 자국의 영토 내에서 다음 각호를 수색하거나 이에 준하는 방법으로 거기에 접속할 권한을 자국의 관할관청에게 부여하기 위한 입법적 조치 및 그 밖의 조치를 취한다: a. 컴퓨터시스템이나 그 일부 및 거기에 저장된 컴퓨터데이터, b. 컴퓨터데이터가 저장될 수 있는 컴퓨터데이터 저장매체. ② (관할)관청이 제1항 a호에 따라 특정한 컴퓨터시스템이나 그 일부를 수색하거나 이에 준하는 방법으로 거기에 접속하여, 찾고 있는 데이터가 해당 협약국의 영토 내의 다른 컴퓨터시스템이나 그 일부에 저장되어 있으며, 해당 데이터가 첫 번째 (컴퓨터)시스템으로부터 적법하게 접속되거나 이용될 수 있다고 추정할 만한 이유가 있는 경우에, 각 협약국은 그 (관할)관청이 수색 또는 이에 준하는 접속을 다른 시스템으로 신속하게 확대할 수 있도록 하기 위한 입법적 조치 및 그 밖의 조치를 취한다. ③ 각 협약국은 제1항이나 제2항에 따라 접속한 컴퓨터데이터를 압수하거나 이에 준하는 방법으로 확보할 권한을 자국의 관할관청에게 부여하기 위해 필요한 입법적 조치 및 그 밖의 조치를 취한다. 이러한 조치는 다음의 권한을 포함한다: a. 컴퓨터시스템이나 그 일부 또는 컴퓨터데이터 저장매체를 압수하거나 이에 준하는 방법으로 확보할 권한, b. 컴퓨터데이터의 복사본을 만들어 유치할 권한, c. 저장된 해당 컴퓨터데이터의 무결성을 유지할 권한, d. 접속된 컴퓨터시스템의 컴퓨터데이터에 접속하지 못하게 하거나 삭제할 권한. [④와 ⑤ 생략]

StPO 제110조 제3항 제2문의 '정보저장매체'는 현재의 정보기술환경과 동 규정의 입법취지를 고려할 때 광의로 이해되어야 한다.[267] 그리고 문언에 따르면, 원격 압수수색은 '외부의 저장장소가 수색된 정보저장매체로부터 접근될' 수 있어야 하고(전단), 이러한 열람의 확대가 없다면 '증거로서 중요한 정보의 손실이 우려'되어야 한다(후단).[268] 한편 동 규정 제4항에 따르면 ISP/CP와 같은 외부 저장매체의 점유자에게는 StPO 제98조 제2항이 준용된다.[269] 따라서 해당 점유자는 해당 조항 제2문에 따라 자신의 권리를 보호하기 위해 법원에 재판(항고)을 청구할 수 있으며, 제5문에 따라 이에 대해 고지받아야 한다.[270] 이런 점에서 StPO 제110조 제3항에 따른 처분은 ISP/CP와 같은 제3자에게도 공개수색의 성격을 잃지 않는다.[271]

한편 StPO 제110조 제3항 제2문이 외부 저장매체, 특히 ISP/CP의 서버가 외국에 존재하는 경우에도 적용되는지가 문제된다. 이는 소위 '역외 압수수색'의 허용성 문제로서, 수권 없는 외국에서의 고권처분은 원칙적으로 해당 국가의 국제법상의 주권을 침해한다.[272] 하지만 CCC 제32조를 고려할 때, 이런 역외 접근이 공중이 접근할 수 있는 정보를 대상으로 하는 경우에는 협약국에 대해서는 동 규정 a호에 따라, 비협약국에 대해서는 국제관습법에 따라 정당화될 수 있다.[273] 반면 해당 접근이 공중이 접근할 수 없는 정보를 대상으로 하는 경우라면, 동 규정 b호에 따라 – 최소한 협약국에 대해서 – 권한 있는 자의 적법하고 자발적인 동의가 필요하다.[274] 그렇지 않다면 동 접근은 원칙적으로 허용되지 않으며 공식적인 국제사법공조의 요청이 필요하다(CCC 제31조 제1항).[275] 이에 따라 일부 문헌에 따르면 역외 압수수색을 위해서는

---

267) BT-Drs. 16/5846, S. 27: 컴퓨터시스템; auch *Schlegel*, HRRS 2008, 23, 27; a.A. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 122: 목적론적 해석상 § 110 Abs. 3의 적용영역은 유일한 od. 적어도 그 일반적인 목적이 개인의 정보저장을 대체 bzw. 보충하는 서비스로 제한되어야 한다.

268) *Köhler*, M-G/Schmitt, § 110 Rn. 6; *Park*, Rn. 817; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 9.

269) BT-Drs. 16/6979, S. 45; *Park*, Rn. 820; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 9.

270) *Köhler*, M-G/Schmitt, § 110 Rn. 11; *Park*, Rn. 820.

271) *Köhler*, M-G/Schmitt, § 110 Rn. 8; *Obenhaus*, NJW 2010, 651, 653 [Tz. 2].

272) *Kasiske*, StraFo 6/2010, 228, 234; *Sieber*, 69. DJT 2012, C 143 f.

273) *Bruns*, KK-StPO, § 110 Rn. 8a; *Köhler*, M-G/Schmitt, § 110 Rn. 7a; 특히 *Sieber*, 69. DJT 2012, C 144 f.: 오늘날 인터넷의 당연한 세계적인 이용, 호출되는 정보의 저장장소에 대한 이용자 인식의 부재, 세계적인 사이버공간에서의 공중이 접근할 수 있는 정보호출의 경미한 침해강도를 고려할 때.

274) *Brodowski/Eisenmenger*, ZD 3/2014, 119, 123.

275) *Bruns*, KK-StPO, § 110 Rn. 8a; *Gaede*, StV 2009, 96. 101 f.; *Köhler*, M-G/Schmitt, § 110 Rn. 7a; *Obenhaus*, NJW 2010, 651, 654.

원칙적으로 서버가 존재하는 국가들에 대한 사법공조 요청이 필요하고, 이런 절차에 따르지 않은 접근은 외국의 주권과 사법공조협정을 침해하는 국제법 위반이며, 이는 결국 일반적으로 증거사용금지로 이어질 수 있다고 한다.[276] 반면 이에 반대하는 견해에 따르면 클라우드 컴퓨팅이 보편화되어 있는 오늘날 형사소추관청의 측면에서 공식적인 사법공조요청이 어느 나라를 대상으로 해야 하는지가 명확하지 않을 뿐만 아니라,[277] 이것은 실무상 극복될 수 없는 어려움이다.[278] 이런 점을 고려할 때 수색되어야 하는 정보가 외국의 그 어딘가에 존재할 단순한 가능성이 수사관청에게 사법공조의무를 야기하지는 않으며,[279] 이 가능성의 비고려가 외국 주권의 자의적인 경시를 의미하지도 않는다.[280] 따라서 역외 압수수색은 일반적으로 StPO 제110조 제3항에 의해 포섭될 수 있는 국내에서의 적법한 수사행위이고, 타국의 주권을 침해하지 않으며, 그 결과로 획득된 정보의 증거사용금지로 이어지지도 않는다.[281] 다만, 정보의 확보·이용이 주권이 침해된 국가의 명백한 반대에 반하여 행해진 경우,[282] 또는 수사관청이 국제법으로 보장된 개인의 권리를 알면서 무시한 경우에는[283] 증거사용금지가 고려될 수 있을 것이다. 한편 2022년에 채택된 CCC 제2 추가의정서의 제9조에 따르면, '긴급상황', 즉 인간의 생명이나 안전에 대한 상당하고 직접적인 위험이 존재하는 경우, 한 협약국의 관할관청은 형사사법공조의 절차를 거칠 필요 없이 CCC

---

276) *Bär*, EDV-Beweissicherung, Rn. 375; *Park*, Rn. 801; *Sieber*, 69. DJT 2012, C 148: CCC 제25조의 위반; *Zimmermann*, JA 5/2014, 321, 322 f.

277) *Köhler*, M-G/Schmitt, § 110 Rn. 7b; *Wicker*, MMR 2013, 765, 768 [Tz. Ⅳ].

278) *Wohlers/Jäger*, SK-StPO, § 102 Rn. 15a; *Kudlich*, GA 2011, 193, 208: 순수한 실무상의 어려움.

279) *Köhler*, M-G/Schmitt, § 110 Rn. 7b; vgl. T-CY Guidance Note # 3, Transborder access to data (Art. 32) vom 3. Dez. 2014, S. 6 [Tz. 3.2](https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a, 최종접속일 2023.9.15.); auch T-CY Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data vom 6. Dez. 2012, What are the options?, S. 29 [Rn. 138](https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8, 최종접속일 2023.9.15.).

280) *Wohlers/Jäger*, SK-StPO, § 102 Rn. 15a und § 110 Rn. 30a.; *Wicker*, MMR 2013, 765, 768 f.: "따라서 기준이 되는 것은 수사관의 실제의 행위가 국내에서 행해진다는 것이다. …… 즉, 어떤 접근이 클라우드-이용자에게서 가능하다면 정보의 위치는 중요하지 않다."

281) *Brodowski/Eisenmenger*, ZD 3/2014, 119, 123; *Köhler*, M-G/Schmitt, § 110 Rn. 7c; *Wicker*, MMR 2013, 765, 768 f.; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 30a.

282) *BGHSt* 34, 334, 344; *Bruns*, KK-StPO, § 110 Rn. 8a; *Köhler*, M-G/Schmitt, § 110 Rn. 7c; *Sieber*, 69. DJT 2012, C 148; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 30a.

283) *Bruns*, KK-StPO, § 110 Rn. 8a; *Köhler*, M-G/Schmitt, § 110 Rn. 7c; *Sieber*, 69. DJT 2012, C 148; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 30a.

제35조에 따른 상시적인 접속창구를 통해 다른 협약국에 있는 서비스제공자에게 내용 데이터의 지체 없는 전달이 가능하도록 협조를 요청할 수 있다. 동 규정의 해석상 역외 압수수색의 대상이 되는 정보가 어느 특정 국가에 위치한 서버에 저장되어 있다는 것이 명확한 경우에는 제한적인 요건 아래에서 위 제9조가 활용될 수 있을 것이다. 다만, 오늘날 거대 다국적 IT 회사의 서버는 보통 여러 나라에 분산되어 있고, 수사기관은 압수수색의 현장에서 찾고 있는 정보가 어느 나라에 있는 서버에 저장되어 있는지를 보통 즉각 확인할 수 없다는 한계가 있다.

4. 전송과정 종료 후 정보저장매체에 저장된 정보의 '비밀의' 수집

가. 논의의 배경

이미 앞의 3. 다.에서 언급하였듯이 IMAP에 기반하는 오늘날의 정보기술환경에서 ISP/CP의 서버에는 압수되어야 하는 정보가 존재하며, 수사기관이 그 서버에 접근하려고 하는 것은 당연하다. 하지만 종래 – 정확히 말하면, 2021년 개정을 통해 StPO 제95조a가 신설되기 전까지 – 독일의 통설과 판례에 따르면 압수수색 일반규정에 근거하는 압수수색은 '언제나' 공개로 행해져야 했다.[284] 즉, 동 일반규정에 따른 압수수색은 예외적으로도 비밀로 명령되거나 집행될 수 없었고, 그 집행 사실이 – 주로 피의자인 – 정보주체에게 '예외 없이' 사전에 통지되어야 했으며(아래 다. 1) 참고), 이를 통해 원칙적으로 그에게 처분의 집행에 입회할 기회가 주어져야 했다(앞의 2. 가. 2) 나) 참고). 하지만 이러한 요청은 증거인멸·훼손의 위험을 발생시킴으로써 수사목적을 위험하게 만드며, 특히 테러 등 안보범죄와 아동음란물 배포, 마약거래, 위조통화유통 등의 조직범죄에서는 StPO 제110조 제3항에 따른 원격 압수수색이 불가능하거나 효과가 없도록 하는 문제를 야기하였다. 다른 한편 유럽 및 독일에서는 2000년대 중반부터 잇따른 테러나 조직범죄에 대처하기 위해 정보기관과 수사기관을 중심으로 전형적인 압수수색이나 기존의 통신감청으로는 해결되지 않는 암호화된 정보전송에 대응하기 위한 수단으로서 온라인 수색이 도입될 필요가 있다는 주장이 지속적으로

284) BT-Drs. 19/27654, 61면: "압수는 StPO에서 공개의 수사처분으로서 형성되어 있다."

제기되었다. 이러한 수사 현실의 어려움 내지 한계 때문에 수사기관을 중심으로 압수수색 일반규정에 따른 처분의 공개성에 의문을 제기하면서 동 규정에 따른 압수수색 또한 비밀로 집행될 수 있다는 주장이 제기되었다.[285] 하지만 BGH와 BVerfG는 이런 주장을 기각하며, 특히 당시 StPO에는 처분의 비밀성을 배제할 법적 근거가 없음을 이유로 기존 압수수색 일반규정에 따른 처분의 집행은 언제나 공개로 행해져야 한다는 기존의 입장을 유지하였다.

우선 BGH는 2007년 결정에서 압수수색 일반규정의 문언 및 StPO 제1편 제8장에 규정되어 있는 수권규범들의 법체계를 고려할 때 동 규정에 의해서는 비밀의 압수수색이 허용될 수 없다고 설시하였다.[286] 즉, BGH의 견해에 따르면 StPO 제106조 제1항과 제107조의 문언에 따라 압수수색은 공개로 집행되어야 하고, 동 규정들은 강행규정으로서 수사기관과 법원은 그에 따른 법적 보호를 임의로 배제할 수 없다(앞의 2. 가. 2) 나) (3) 참고). 또한 StPO 제100조a 이하에 따른 통신감청 등 비밀의 수사처분을 위한 수권규범들이 처분의 비밀성 때문에 증대된 침해강도를 상쇄하기 위해 비례성 원칙에 따라 압수수색 일반규정에서보다 강화된 처분요건 및 절차법적 통제장치와 결부되어 있다는 점을 고려할 때, 해당 일반규정에 근거하여 비밀의 압수수색이 허용되는 것은 법체계적으로 타당하지 않다.

한편 압수수색 일반규정에 따른 처분의 공개성 요청과 관련하여 BVerfG는 압수수색되는 정보가 처분 당사자의 지배영역인 사적인 단말기에 저장되어 있는 경우와 타인의 지배영역인 ISP/CP의 서버에 저장되어 있는 경우를 다르게 취급한다. 먼저 2006. 3. 2.의 결정(2 BvR 2099/04)에서 BVerfG는 수사기관이 처분 당사자가 알게, 즉 '공개로' 그의 PC나 핸드폰 등에 접근하여 행한 압수수색의 합헌성을 심사하면서 해당 처분은 그 집행이 공개로 행해졌기 때문에 압수수색 일반규정에 따라 명령될 수 있다고 설시하였다.[287] 이어서 BVerfG는 2009. 6. 16.의 판결(2 BvR 902/06)에서

---

285) 예를 들어, 독일 연방검찰청의 고등검사(Oberstaatsanwalt)였던 *Hofmann*은 – 최소한 – 테러 등 안보범죄의 영역에서 유용한 수사방법인 온라인 수색이 압수수색 일반규정에 근거하여 명령·집행될 수 있어야 한다고 주장하였다(*Hofmann*, NStZ 2005, 121, 123).

286) *BGHSt* 51, 211, 212-216 [Rn. 5-13] (= NJW 2007, 930). BGH는 이 결정에서 앞서 언급된 *Hofmann* 검사의 견해를 비판하였다.

287) *BVerfGE* 115, 166, 194 ff. [Rn. 104-112]. 이 결정의 핵심 쟁점은 '압수수색 일반규정'이 유관·무관정보가 혼재하는 정보저장장치에 대한 압수수색을 정당화할 수 있을 정도로 규범이 명확하고 엄격하게 형성되어 있는가였다.

서버에 저장된 e-mail에 대한 접근이 정보주체인 피의자 알게, 즉 '공개로' 행해진 경우, 그 처분은 압수수색 일반규정에 의해 정당화될 수 있지만,[288] 그것이 정보주체가 모르게, 즉 '비밀로' 행해지는 경우에는 그렇지 않다는 취지로 설시하였다.[289] 다만, BVerfG는 이 판결에서 수사기관이 서버에 저장된 피의자의 정보를 비밀로 접근하는 경우를 정당화하기 위한 요건이 구체적으로 무엇인지에 대해서는 기술하지 않았다. 요컨대 – 2021년 개정 전까지 – BVerfG의 입장에 따르면 압수수색 일반규정에 근거하여 처분 당사자의 사적인 단말기뿐만 아니라 제3자인 ISP/CP의 서버에 저장된 정보도 압수수색될 수 있지만, 이때 '예외 없이' 처분 당사자 알게, 즉 공개로 집행되어야 한다는 것이다.

이러한 이해를 전제로 독일에서는 두 가지 쟁점이 논의되었다: 개인의 정보저장매체에 비밀로 접근하는 수사처분, 소위 '온라인 수색(Online-Durchsuchung)'이 허용되기 위한 요건 및 ISP/CP의 서버에 저장된 피의자의 정보를 수사기관이 그 피의자 모르게 수집하기 위한 요건. 이하에서는 먼저 (수사상) 처분의 비밀성이란 무엇을 의미하고, 비밀의 강제처분이 허용되기 위한 요건은 무엇인지를 최근 BVerfG의 판결과 결정을 중심으로 검토한 후(아래 나.), 제3자 보관 정보에 대한 압수에서 정보주체인 피의자에 대한 통지가 유예되기 위한 요건(StPO 제95조a, 아래 다. 참고) 및 온라인 수색의 허용요건(StPO 제100조b, d, e, 아래 라. 참고)을 검토할 것이다.

---

288) 이때 BVerfG는 현재의 정보통신 환경에서 ISP/CP의 서버에 저장된 정보에 대한 접근은 모든 수사에서 일반적으로 요구된다고 전제한 후, 그런 압수수색이 공개로 행해지는 경우에는 범죄수사라는 공익을 고려할 때 중대한 범죄와 증대된 혐의를 통한 제한이 요구되지 않는다고 설시하였다(*BVerfGE* 124, 43, 63-65 [Rn. 71-74]).

289) *BVerfGE* 124, 43, 62 ff. [Rn. 69-77]. 사실관계에 따르면, 서버에 저장되어 있었던 피의자의 e-mail 교신 상대방(제3자)의 약 2,500개의 e-mail이 그가 알고 있는 상태에서 압수수색 일반규정에 근거한 명령에 따라 정보저장장치에 복제되어 수사관청에게 전달되었다. 이 판결의 쟁점은, 통신감청 규정이 아닌, '압수수색 일반규정'이 ISP/CP의 서버에 저장된 정보에 대한 접근을 정당화하는가였다.

나. 비밀의 강제처분과 그 허용요건[290]

1) 수사처분의 비밀성과 비밀의 강제처분

수사처분의 비밀성 그 자체는 공정한 절차의 원칙에 기초하는 기망금지에 반하지 않으며,[291] 그것이 처분의 불허용성을 발생시키지는 않는다.[292] 오히려 많은 경우 비밀성은 효과적인 형사소추를 위해 필수적인 조건이다.[293] 이미 과거부터 조직범죄 등 중대한 범죄에 대처하기 위해 비밀수사의 필요성과 정당성은 인정되어 왔다.[294] 수사관청은 수사절차의 자유로운 형성의 원칙에 따라 일반적으로 범죄의 사실규명에 기여하는 모든 허용되는 처분을 취할 수 있고,[295] 사용할 수 있는 수사전략과 수사기술에 대해 폭넓은 재량을 가진다.[296]

하지만 법치국가에서 기본권 침해처분의 비밀성은 예외적인 것이며, 특별한 정당화가 필요하다.[297] 무엇보다 이것은 비밀의 수사처분이 기본권을 중대하게 침해하는 경우, 즉 '비밀의 강제처분'에서 그렇다. 시민이 수사처분의 집행을 그에 앞서 아는 경우, 그는 수사의 진행에 영향을 끼칠 수 있는 기회를 통해 자신의 이익을 대변할 수 있다.[298] 공개의 정보수집에서 당사자는 – 변호사의 조력을 받으면서 – 법적 하자 있는 처분의 집행에 대처하고, 압수의 지침을 포함한 영장에 기재된 한계의 준수를 감시하며, 그 집행방법의 제한에 대한 위반에 대응할 수 있다.[299] 반면에 비밀의 처분

---

290) 아래의 내용은 박중욱, "수사절차에서의 "비밀의 강제처분"의 합헌성 요건 – 기술적 비밀의 수사처분에 대한 독일 연방헌법재판소 판결의 분석을 중심으로– ", 『형사법의 신동향』 통권 제63호, 대검찰청, 2019.6, 43, 57-69면의 내용을 요약·보완한 것이다.

291) *BVerfGE* 109, 279, 324 [Rn. 156].

292) *BVerfG* NJW 2009, 1405, 1407 [Rn. 28]; *BGHSt* 39, 335, 346; 42, 139, 150; *Schmitt*, M-G/Schmitt, § 161 Rn. 7.

293) *BVerfGE* 109, 279, 325 [Rn. 156]; NJW 2009, 1405, 1407 [Rn. 28].

294) *BVerfG* NJW 1985, 1767: 효율적인 형사사법을 위한 경찰 밀정의 정당성; *BGH* NJW 1980, 1761: "마약범죄와 같이 특히 위험하고 사실규명이 어려운 범죄의 퇴치를 위하여 이러한 비밀수사는 포기될 수 없다."

295) *BVerfG* NJW 2009, 1405, 1407 [Rn. 26]; *Schmitt*, M-G/Schmitt, § 161 Rn. 7.

296) *Schmitt*, M-G/Schmitt, § 163 Rn. 64.

297) *BVerfGE* 118, 168, 197 [Rn. 134]; 120, 274, 325 [Rn. 238]; *Kasiske*, StraFo 6/2010, 228, 231; *Zerbes/El-Ghazi*, NStZ 2015, 425, 432 [Tz. c)]. 다만, 지속적으로 발전하는 기술적 가능성을 고려할 때, 이러한 공개·비밀 처분의 원칙-예외-관계에는 부분적으로 의문이 제기되기도 하지만, 다른 한편으로는 그것에 의해 형사절차가 정보기관의 임무수행과 같이 운용될 수 있다는 우려도 존재한다(*Singelnstein*, NStZ 2012, 593).

298) *BVerfGE* 118, 168, 197 f. [Rn. 134]; 120, 274, 325 [Rn. 238].

299) *BVerfGE* 115, 166, 194 f. [Rn. 106]; 또한 *BGHSt* 51, 211, 215 [Rn. 10]: "그 공개집행은

에서는 그렇지 못하고, 여기서 당사자는 빨라야 침해가 종료된 후 그것에 대해 통지받거나 다른 방식으로 알게 되었을 때야 비로소 침해에 대해 법적 조치를 취할 수 있다. 따라서 이러한 유형의 침해는 법적 방어가능성을 배제하기에 처분 당사자의 권리에 대한 높은 위험을 내포하며,[300] 기본권 침해의 비중을 증대시킨다.[301] 이런 점에서 '비밀의 강제처분'은 새로운 독자적인 성격을 가지며,[302] 그 정당화를 위해서는 비례성 원칙에 따라 강화된 처분요건 및 절차법적 통제장치와 결부되어야 한다. BVerfG는 통신감청, 온라인 수색, 주거감청(Akustische Wohnraumüberwachung), (혐의 없이 수집·보관된) 교신데이터 이용과 같이 기본권을 '특히 강력히 침해'하는 비밀의 수사처분 및 그 수권규범의 합헌성 심사에서 각 처분이 그 비밀성 때문에 처음부터 불허되는 것은 아니지만 그것을 정당화하는 각 수권근거는 비례성 원칙에 따라 그 강력한 침해강도를 상쇄할 수 있는 엄격한 처분요건 및 절차법적 통제장치와 결부되어야 한다고 설시하였다.[303]

2) 비밀의 강제처분의 허용요건: 가중된 처분요건과 절차법적 통제장치

BVerfG의 결정에 따르면, 우선 비밀의 강제처분의 처분요건과 관련해서는 '범죄의 중대성'과 '범죄혐의의 강도'가 고려된다.[304] 이때 정보침해와 관련된 처분에서는 획득될 정보의 잠재적인 증거로서의 중요성과 이 정보를 통해 발견될 혐의의 정도도 고려되어야 한다.[305] 이외에 보충성(Subsidiarität)[306]도 처분요건에 속하는데, 이것은

당사자에게 상황에 따라 찾고 있는 대상물의 환부를 통해 처분을 방지할 기회 내지 처분의 기간과 강도를 제한할 기회 또는 처분의 법적 요건에 흠결이 있는 경우에는 – 경우에 따라서는 변호사 조력을 받으면서 – 집행 중인 처분에 대처할 기회나 최소한 수색의 유형과 방식을 통제할 기회, 특히 수색결정(서)에 설정된 한계의 준수를 감시할 기회를 제공한다. 비밀수색은 당사자에게서 이러한 기회를 박탈한다."

300) *BVerfGE* 113, 348, 384 [Rn. 142]; 또한 107, 299, 321: "당사자의 권리에 대한 특별한 위험."

301) BVerfGE 107, 299, 321 [Tz. (d)]; 113, 348, 383 [Rn. 141]; 115, 166, 194 f. [Rn. 106]; 118, 168, 198 [Rn. 134]; 120, 274, 325 [Rn. 238]; 124, 43, 62 [Rn. 68] m.w.N; *BGHSt* 51, 211, 215; *Zimmermann*, JA 5/2014, 321, 323: "비밀처분은 바로 그 비밀성 때문에 공개적으로 행해진 대응물에 비하여 상당한 침해강도를 갖는다."

302) *Roxin/Schünemann*, § 36 Rn. 2; *BGHSt* 51, 211, 215 [Rn. 10].

303) *BVerfGE* 109, 279, 310 ff. (주거감청); 120, 274, 315 ff. (온라인 수색); 125, 260, 325 ff. (교신데이터 이용); 129, 208, 240 ff., 250 ff. (통신감청) 등. 각 비밀의 수사처분의 허용성 및 적용범위는 법정책의 문제이므로, 그것은 입법을 통해서 정해져야 한다(*Vogel*, ZIS 2012, 480, 482).

304) *BVerfGE* 113, 29, 53 [Rn. 108]; 115, 166, 197 [Rn. 117]; 124, 43, 66 [Rn. 79]; *Köhler*, M-G/Schmitt, § 94 Rn. 18 und § 102 Rn. 15a.

305) *BVerfGE* 115, 166, 197 f. [Rn. 117 f.]; 124, 43, 66 [Rn. 79]. 따라서 구체적인 경우 수사될

비례성 원칙에서 도출되는 최후수단성(ulitma ratio)을 의미한다. 즉 비밀의 강제처분은 원칙적으로 동급의 공개의 처분보다 후순위로 사용되어야 한다. 다른 한편, 절차법적 통제장치는 수사기관의 과도한 정보침해나 수집된 정보의 무권한·불법적 이용에 대처함으로써 처분의 침해강도를 상쇄하기에 충분해야 한다. 기술적 비밀의 수사방법들의 처분요건과 절차법적 통제장치(StPO 제99조 이하)는 기본적으로 단순 압수·수색의 그것(StPO 제94조 이하, 제102조 이하)보다 엄격하게 형성되어 있다.[307]

가) 가중된 처분요건

비밀의 강제처분은 중대한 법익의 보호를 위해서만 허용된다.[308] 따라서 각 처분의 정당화는 규명되어야 하는 범죄의 의미와 중대성에 좌우되며, 이것은 각 수권규범의 적용범위에 영향을 준다.[309] 현재 비밀의 강제처분에 관한 StPO의 수권규범에는 범죄의 비중이 3가지 단계로 구분되어 있다:[310] "특별히 중대한 범죄행위(besonders schwere Straftaten)",[311] "중대한 범죄행위(schwere Straftaten)",[312] "중요한 의미의 범죄행위(Straftaten)."[313] 앞의 두 개념의 의미 내지 범위는 개별 규정에 구체적으로 목록화되어 있지만(소위 '범죄목록(Straftatenkatalog)'; 예를 들어, StPO 제100조a 제

범죄의 경미함, 압수될 정보의 경미한 증거로서의 중요성, 발견될 혐의의 막연함은 데이터베이스의 강제적 확보와 모순될 수 있다(115, 166, 198 [Rn. 119]; 124, 43, 67 [Rn. 79]).

306) StPO 제99조 이하의 수권규범 중 통신감청 등 대부분의 수권규범(StPO 제100조a 제1항, 제100조b 제1항, 제100조c 제1항, 제100조f 제1, 2항, 제100조g 제1, 2항, 제100조h 제1, 2항, 제110조a 제1항, 제163조f 제1항)에는 보충성이 다음과 같은 문언으로 반영되어 있다: "(어떤 처분이 사실관계의 조사나 범죄자/피의자의 거주지 수사가) 다른 방법으로는 성과를 기대하기 [매우] 어렵거나, 가망이 없거나, [현저히, 지나치게] 곤란한 경우." 다만, 정보수집의 유형과 성격 또는 처분의 침해강도에 따라 일부 수권규범(StPO 제99조, 제100조i, 제100조j 제1항 제1문)에는 보충성 요건이 배제되어 있다.

307) *Roxin/Schünemann*, § 29 Rn. 5: StPO에서 강제적 수사처분의 수권근거는 비례성 원칙에 따라 도식적으로 연동되어 규정되어 있으며, 이때 3개의 "유보조건", 즉 "(범죄)비난의 비중", "범죄혐의의 강도", "명령기관의 관할"이 고려된다.

308) *BVerfGE* 141, 220, 270 [Rn. 106 ff.].

309) *BVerfGE* 100, 313, 375 f. [Rn. 219]; 107, 299, 321 [Tz. (2)].

310) *BVerfGE* 109, 279, 344 ff. [Rn. 228 ff.]; 141, 220, 270 [Rn. 107]. 도그마틱적으로 이 개념들은 비례성 원칙 및 그 하부요소인 과잉금지에 속한다(vgl. *Rieß*, GA 2004, 623, 631 am Anfang: 중요한 의미의 범죄행위).

311) 이 개념은 주거감청을 허용하기 위한 1998. 3. 26.의 GG 제13조 제3항의 개정(BGBl. I S. 610) 및 이로부터 나온 (舊) StPO 제100조c 제1항 제3호(BGBl. I S. 845)의 신설을 통해 StPO에 도입되었다.

312) 이 개념은 (舊) StPO 제100조a, b의 도입 시에 처음으로 StPO에 규정되었고, 이 규정들은 형사소추 목적의 통신감청을 위해 1968. 11. 1.에 발효된 법률(G 10)을 통해(BGBl. I S. 949) 창설되었다.

313) 이 법적 개념은 1992년의 OrgKG에 의해 StPO에 도입되었다(앞의 각주 191).

2항, 제100조b 제2항, 제100조g 제2항 제2문), 마지막 범죄 개념은 그렇지 않다.[314] 이러한 가중된 의미를 가지는 범죄의 범위는 일단 입법자가 재량적으로 판단하지만, 규범통제를 행하는 BVerfG에 의해서 그 최소한이 요구될 수 있다.[315]

다른 한편 범죄혐의의 강도 또한 비례성 원칙에 근거하여 처분의 침해강도에 따라 StPO에 차등화되어 있다.[316] – 이미 언급하였듯이 – 일반적인 형사사건에서는 합리적인 사실상의 근거가 존재하는 경우, 최초혐의가 인정되어 (단순) 압수·수색이 가능하고, 이를 통해 수사가 개시될 수 있다(앞의 2. 가. 1) 가) (2) 참고). 반면, 비밀의 수사처분을 위한 수권규범(예를 들어, StPO 제100조a 제1항, 제100조b 제1항, 제100조c 제1항, 제100조f 제1항, 제100조g 제1, 2항, 제100조i 제1항, 제163조d 제1항)에서는 '특정한 사실관계(bestimmte Tatsachen)'에 근거한 혐의, 소위 "가중된 범죄혐의(qualifizierter Tatverdacht)"가 요구된다.[317] 이를 위해서는 구체화 된 혐의상황, 즉 구체적이고 어느 정도 짙어진 상황이 사실적 기초로서 존재할 것이 요구된다.[318] 이 혐의는 최초혐의보다 더 높은 정도의 혐의이지만, 공소제기(StPO 제170조)와 공판개시(StPO 제203조)를 위한 '충분한 혐의(hinreichender Tatverdacht)', 또는 미결구금(StPO 제112조)과 가구금(StPO 제127조)을 위한 '유력한 혐의(dringender Tatverdacht)'의 정도에 도달될 필요는 없다.[319] 왜냐하면, StPO 제100조a 이하의 처분들이 기본권을 강력히 침해할지라도, 그 목적은 형사소추를 위해 절차상 중요한 정보를 수집하는 것이고, 그 강도는 신체의 자유에 대한 침해보다 경미하기 때문이다.

---

314) '중요한 의미의 범죄행위'라는 개념에 대해 그 불명확성과 불특정성 때문에 부분적으로 위헌의 우려가 제기되지만(*Rieß*, GA 2004, 623, 624), 입법자는 1992년의 OrgKG를 통해 해당 개념을 도입한 이래로 그것을 지속적으로 사용하고 있다. BVerfG 또한 이 개념의 사용이 헌법상 문제되지 않는다고 한다. BVerfG의 결정 및 지배적인 견해에 따르면 '중요한 의미의 범죄행위'란, 그 범죄행위가 최소한 중급 범죄의 영역에 속할 수 있어야 하고, 법적 평화를 민감하게 교란해야 하며, 법적 안정성에 대한 시민의 감정을 현저히 침해하기에 적합해야 한다(*BVerfGE* 103, 21, 34 [Rn. 52]; 107, 299, 322; 109, 279, 344 [Rn. 228]; 112, 304, 305 f. [Rn. 48]; 124, 43, 64 [Rn. 73]; *LG Mannheim* StV 2001, 266; *Schmitt*, M-G/Schmitt, § 81g Rn. 7a).

315) *BVerfGE* 125, 260, 328 f. [Rn. 227-229].

316) *Roxin/Schünemann*, § 39 Rn. 16.

317) *BVerfGE* 141, 220, 325 [Rn. 280].

318) *BVerfGE* 100, 313, 395; 109, 279, 350 f. [Rn. 247]; 129, 268 [Rn. 273].

319) *BVerfGE* 109, 279, 350 [Rn. 247]; 129, 208, 268 [Rn. 273]; *Diemer*, KK-StPO, § 152 Rn. 7; *Schmitt*, M-G/Schmitt, § 152 Rn. 4; *Wolter*, SK-StPO, § 100c Rn. 41.

나) 가중된 절차법적 통제장치

BVerfG는 통신감청, 온라인 수색, 주거감청, (협의 없이 수집·보관된) 교신데이터 이용 등과 같이 기본권을 중대하게 침해하는 비밀의 수사처분의 헌법적 정당성과 관련된 최근의 판결들에서 동 처분들의 절차법적 통제장치가 (협의의) 비례성 원칙 및 '재판청구권(GG 제19조 제4항)과 결부된 각 개별 기본권'에 근거하여 투명성 요청, 효과적인 권리보호, 감독적 통제, 무관정보의 삭제·기록 의무 등이 보장되도록 형성될 것을 요구한다.[320] 특히 BVerfG는 투명성 요청(Transparenzanforderungen)에 근거하여 위와 같은 처분들에서 원칙적으로 그 집행 사실이 처분 당사자에게 사후에 통지되고 이에 기초하여 개별적인 권리보호의 기회가 주어질 것을 요구한다. BVerfG 판결의 설시에 따르면 정보 수집·처리의 투명성은 국가의 비밀처분에 대해 신뢰와 법적 안정성이 발생할 수 있도록, 그리고 정보의 취급이 민주주의 담론과 결부되도록 기여해야 한다.[321] 투명성에 근거하여 가능하다면 처분 당사자에게는 법원을 통한 주관적인 권리보호가 가능해야 하고 국가에 의한 (비밀)감시의 막연한 위협이 대처될 수 있어야 한다.[322] 한편 주관적인 권리보호의 보장, 즉 처분 당사자에 대한 통지와 (준)항고가 처분의 비밀성이나 그 집행의 유형과 방식 때문에 덜 확보될수록 기관 내의 감독적 통제에 더 큰 비중이 놓인다.[323] 아래에서는 비밀의 강제처분에 대한 가장 중요한 절차통제라 할 수 있는 사전 통제장치인 법관유보 및 사후 통제장치인 당사자에 대한 통지와 이를 통한 효과적인 권리보호(준항고나 증거사용금지 등)에 대해서만 검토한다.

기본권을 중대하게 침해하는 처분, 특히 온라인 수색, 주거감청, 통신감청, 교신데이터 이용 등과 같은 비밀의 강제처분에 대해서는 비례성 원칙에 따라 원칙적으로 헌법상 독립된 기관에 의한 사전적·예방적 통제인 법관유보가 요청된다.[324] 다만,

---

320) 이에 대한 최초의 자세한 설시는 *BVerfGE* 125, 260, 334 ff. [Rn. 239 ff.]; 이후 129, 208, 250 f. [Rn. 226 f.]; 133, 277, 365 ff. [Rn. 204 ff.]; 141, 220, 282 ff. [134 ff.].

321) *BVerfGE* 133, 277, 366 [Rn. 206]; 141, 220, 282 [Rn. 135].

322) *BVerfGE* 125, 260, 335 [Rn. 242]; 141, 220, 282 [Rn. 135]; 또한 133, 277, 366 f. [Rn. 207] u. 369 [Rn. 214].

323) *BVerfGE* 133, 277, 367 [Rn. 207]; 141, 220, 282 [Rn. 135].

324) *BVerfGE* 120, 274, 332 [Rn. 259]; 125, 260, 347 [Rn. 248]; 141, 220, 275 [Rn. 117]. 침해강도가 강한 감시·수사처분. 주거감청의 처분에 대해서는 이미 Art. 13 Abs. 2-4에 법관유보가 규정되어 있다.

법관유보는 처분의 법률적 허용성, 즉 적법성 심사로 제한되기 때문에, 너무 불특정하게 규제되거나 너무 낮게 설정된 처분요건(대표적으로 압수수색 일반규정)의 흠결을 상쇄하기에는 적합하지 않다. 따라서 입법자는 강력한 침해강도를 갖는 비밀의 수사처분에서 법관유보를 규범명확한 형식으로 '법원명령의 내용과 이유제시에 대한 엄격한 요청'과 결부시켜야 한다.[325] 이를 위해 (처분)명령의 청구에 대한 효과적인 통제를 가능하게 하는 충분히 실증적인 이유제시, 즉 청구기관의 측면에서의 완전한 정보가 법원에 제출되어야 한다.[326] 다음으로 법원의 명령서는 내용이 충분하도록 이유가 제시되어야 한다. 이때 수집되거나 전달되어야 하는 정보는 수사관청과 협력의무자인 ISP/CP가 독자적인 사안심사를 행할 필요가 없을 정도로 충분히 구분되고 명확한 방식으로 표시되어야 한다.[327]

한편 비밀의 강제처분에서 효과적인 권리보호는 당사자의 처분에 대한 인식을 통해서만 보장될 수 있다. 당사자에게 자신과 관련된 정보 수집·이용에 대한 – 최소한 사후의 – 인식이 제공되지 않는다면, 당사자는 해당 처분의 불법성 및 수집된 정보의 삭제·수정·배상에 대한 권리를 주장할 수 없다.[328] 이런 점에서 정보침해 당사자에게 통지 규정은 일반적으로 기본권적 정보보호의 기초적인 도구에 속하고,[329] 이를 통해 당사자는 통지받은 후 재판청구권(GG 제19조 제4항)에 근거하여 합리적인 방식으로 법원의 적법성 통제를 받을 수 있다.[330] 따라서 비밀의 강제처분에 대한 수권규범의 법적 형성에서 입법자는 사후의 통지(비밀성) 및 법원의 적법성 통제를 위한 규정을 창설해야 한다.[331] 이때 사전통지의 제한을 통해 생기는 권리보호의 흠결을 고려할 때, 그 제한은 독립된 중립의 기관인 법원의 통제 아래 있어야 한다.[332] 요컨대 투명성

---

325) *BVerfGE* 125, 260, 338 [Rn. 249]; 141, 220, 275 [Rn. 118].

326) *BVerfGE* 125, 260, 338 [Rn. 249]; 141, 220, 275 [Rn. 118]. 그래야만 비로소 독립된 기관인 법원은 독자적인 책임으로 청구된 처분들이 법적 요건과 침해한계를 준수하고 있는지 여부에 대해 판단할 수 있다(*BVerfGE* 125, 260, 338 [Rn. 249]). 이를 위한 필수적인 물적·인적 요건들을 창설하는 것은 주 사법행정청과 관할법원 의장의 의무이다(*BVerfGE* 141, 220, 275 f. [Rn. 118]).

327) *BVerfGE* 125, 260, 338 [Rn. 249].

328) *BVerfGE* 125, 260, 335 [Rn. 242]; 129, 208, 250 [Rn. 226]; 133, 277, 366 [Rn. 206].

329) *BVerfGE* 129, 208, 250 [Rn. 226]. 이러한 당사자에 대한 정보제공(통지)은 정보의 실제적 관련성에 대한 부지로부터 발생하는 위협을 감소시키고, 불안한 억측에 대처하며, 당사자에게 해당 처분을 공개적인 논의할 수 있는 기회를 제공한다(*BVerfGE* 125, 260, 335 [Rn. 242]).

330) *BVerfGE* 141, 220, 283 f. [Rn. 138].

331) *BVerfGE* 125, 260, 335 [Rn. 244] u. 339 [Rn. 251].

332) *BVerfGE* 100, 313, 361 [Rn. 171].

요청에 따라 개인정보의 수집·이용을 위한 형사절차상 강제처분은 공개성 원칙(Grundsatz der Offenheit)의 지배를 받고, 이에 따라 처분 당사자는 그의 정보가 이용됨에 앞서 원칙적으로 통지받아야 하지만,[333] 정보의 비밀 이용, 즉 정보의 당사자 모르게 그의 정보를 이용하는 것이 개별적으로 필요하다면 허용될 수 있으나, 법관에 의해 명령된 경우에만 가능하다: 비밀의 수사처분에서 사전통지 배제를 위한 법관유보.[334] 나아가 이때 최소한 사후통지가 규정되어야 하는데, 이 사후통지 또한 제3자의 법익과 이익형량에 따라 예외적으로 배제될 수 있으나, 이것은 무조건 필요한 경우로 제한되어야 한다.[335] BVerfG는 StPO 제1편 제8장에 규정된 비밀의 강제처분들에 대한 사후통지를 규제하고 있는 StPO 제101조 제5항과 제6항[336]이 위에 기술된 기준에 부합한다고 결정하였다.[337]

---

333) 다만, - 형사소추를 위해서가 아니라 - 위험방지와 정보기관의 임무수행을 위해서는 공개성 원칙의 배제가 원칙적으로 수인될 수 있다; 그렇지 않으면 여기서는 일반적으로 조사의 목적이 무위로 된다(*BVerfGE* 125, 260, 336 [Rn. 243]). 나아가 이 원칙은 안보범죄의 영역에서의 수사준비를 위한 초기정보수집의 경우에도 적용되지 않는다(*BVerfGE* 141, 220, 283 [Rn. 137]).

334) *BVerfGE* 125, 260, 336 [Rn. 243 a.E.].

335) *BVerfGE* 109, 279, 364; 125, 260, 336 [Rn. 244]

336) StPO 제101조 [비밀처분에서의 절차규정(Verfahrensregelungen bei verdeckten Maßnahmen)] ① 다른 규정이 없는 한, 아래의 규정들은 제98조a, 제99조, 제100조a 내지 f, 제100조h, 제100조i, 제110조a, 제163조d 내지 g의 처분에 적용된다. [② 내지 ④ 생략] ⑤ 통지는 수사목적, 인간의 생명, 신체의 완전성, 개인적 자유, 중요한 자산에 대한 위험 없이 가능한 경우에 즉시 행해진다; 제110조a에서의 통지는 비밀수사관의 계속적 투입 가능성에 위해가 되지 않는 경우에도 즉시 행해진다. 제1문에 따른 통지가 유예되는 경우, 그 이유가 문서로 작성되어야 한다. ⑥ 제5항에 따라 유예된 통지가 처분의 종료 후 12개월 이내에 행해지지 않은 경우, 이 통지의 추가 유예를 위해서는 법원의 동의가 필요하다. 추가 유예의 기간은 법원이 정한다. 통지의 요건이 거의 확실하게 장래에도 성립되지 않을 경우, 통지의 최종적 배제에 법원은 동의할 수 있다. [⑦과 ⑧ 생략]

337) *BVerfGE* 129, 208, 251 ff. [Rn. 228 ff.]. 다만, StPO 제100조g에 따른 교신데이터 이용에서의 사후의 통지와 적법성 통제에 대해서는 StPO 제101조a 제6항 제2문이 규정하고 있다: StPO 제101조 제4항 제3문과 제5항 제1문에 따른 통지의 중단과 유보를 위해 언제나 관할 법원의 명령이 필요하다(*BVerfGE* 125, 260, 354 [Rn. 282]).

다. 서버에 저장된 정보에의 비밀의 접근[338][339]

1) StPO에 따른 집행절차: 2021년 개정 전의 법적 상황

StPO에 따르면 압수수색은 원칙적으로 법관에 의해, 예외적으로 수사기관에 의해 명령될 수 있으며(제98조 제1항, 제105조 제1항), 원칙적인 모습인 법원의 명령은 절차참가자에 대한 사전청문의 절차를 거친 후(제33조[340] 제3항), 출석한 당사자에게는 선고를 통해, 불출석한 당사자에게는 송달을 통해 '고지/통지'되어야 한다(제35조 제1, 2항[341]).[342] 이때 사전청문은 StPO 제33조 제4항의 '명령의 목적이 위험해질 경우'에 근거하여 예외적으로 배제될 수 있는데, 문헌의 지배적인 견해에 따르면 '급습처분의 필요성'이 존재하는 경우가 그 경우이며, 구속에서의 도망의 우려 또는 압수수색에서의 압수물의 은닉·폐기·삭제의 우려가 있는 경우가 그 예에 속한다.[343] 문헌에 따르면 실무상 압수수색 명령의 발부와 집행에서 이 사전청문은 StPO 제33조 제4항에 따라 거의 예외 없이 배제된다고 한다.[344] 이에 반해, 법관의 명령에 근거한 강제처분의 당사자[345]에 대한 재판의 고지/통지를 규정하는 제35조에는 청문절차의 배제를

---

338) 아래의 내용은 박중욱, "제3자 보관 정보의 압수수색과 정보주체에 대한 통지 - 강제처분의 공개성/비밀성에 대한 독일 논의를 참고하여 -",『원광법학』 제38권 제3호, 원광대학교 법학연구소, 2022.9, 51, 62-70면의 내용을 부분적으로 발췌·요약한 것이다.

339) ISP/CP나 기업의 서버에 저장되어 있는 정보가 수사상 필요한 경우, 실무상 수사기관은 ISP/CP나 기업에게 영장의 집행에 대한 협조를 요청하면 충분하고, 그들 모르게 그들의 서버에 접속할 필요는 없다. 즉 수사기관이 ISP/CP 등의 서버에 비밀로 접근하는 것은 – 이론적으로는 생각될 수 있을지라도 – StPO 제100조a 제4항과 TKG 제170조(= (舊) TKG 2004 제110조)를 고려할 때 일반적으로 고려되지 않는다(*Brodowski*, JR 2009, 402, 403 [Tz. b) (ii)] und 411 [Tz. 2. b)]; 또한 *Singelnstein*, NStZ 2012, 593, 596 a.E.: "ISP에게 …… 처분은 예외 없이 공개로 행해져야 한다. 따라서 …… 클라우드에 있는 정보에의 비밀 접근은 StPO에 의해 충족되지 않는다."). 다른 한편 ISP/CP는 기본적으로 증인으로서 자신이 알고 있는 사실관계를 진술할 의무가 있고(StPO 제48조 제1항 제2문, 제161조a 제1항 제1문), 증거 대상물의 보관자로서 그것을 제출·인도할 의무가 있다(StPO 제95조 제1항). 요컨대 수사기관이 ISP/CP로부터 정보를 수집하는 것은 ISP/CP의 입장에서 언제나 공개수사이다.

340) StPO 제33조 [(절차)참가자의 청문] ① 공판중인 법원의 재판은 (절차)참가자에 대한 의견청취 후에 내려진다. ② 법원의 공판 외의 재판은 검찰의 서면이나 구두의 의견진술 후에 내려진다. ③ 제2항의 재판에서 (검찰 이외의) 다른 (절차)참가자(ein anderer Beteiligter)의 의견이 청취되어야 하며, 이 의견청취는 그 다른 (절차)참가자가 의견을 진술하지 않은 사실관계나 증거조사결과가 그에게 불리하게 이용되기 전에 행해져야 한다. ④ 미결구금, 압수 또는 그 밖의 처분에 대한 명령에서, 사전청문으로 그 명령의 목적이 위험해질 경우 제3항은 적용되지 아니한다. 제3항은 참가자의 청문을 특별히 규율하는 규정에 영향을 주지 않는다.

341) 앞의 각주 153 참고.

342) 박중욱, 각주 338의 논문, 65-66면.

343) *Maul*, KK-StPO, § 33 Rn. 12; *Schmitt*, M-G/Schmitt, § 33 Rn. 15 f.

344) *Park*, Rn. 72 u. 473. [박중욱, 각주 338의 논문, 66면(재인용)]

허용하는 제33조 제4항과 같은 그 유예나 배제를 허용하는 규정이 없다.[346] 또한 통설과 BGH의 판결에 따르면, 압수수색 일반규정에 따른 공개의 압수수색에 대해서는 StPO 제99조 이하에 따른 비밀의 수사처분을 위한 통지의 유예와 배제를 규정한 StPO 제101조 제5항과 제6항이 (유추)적용되지 않는다.[347]

요컨대 – 2021년 개정 전까지 – 기존의 일반규정에 따른 공개의 압수수색에서는 '급습 처분의 필요성'을 이유로 사전청문은 배제될 수 있을지라도, 그에 대한 통지는 최소한 처분 집행의 개시 직전에 처분 당사자에게 행해져야 했고,[348] 이런 통지가 유예되거나 배제될 수 있는 법적 근거가 존재하지 않았다. 따라서 서버에 저장된 정보가 압수수색을 위해 ISP/CP로부터 수사기관에 전달되는 경우, 수사기관은 – 주로 피의자인 – 정보주체에게 그 사실에 대해 늦어도 정보를 전달받기 직전에는 통지해야 했다.[349] 만약에 이런 통지가 StPO 제101조의 (유추)적용을 통해 또는 수사기관의 임의적인 판단으로 사전에 행해지지 않거나 집행의 종료 후에도 계속적으로 유예되거나 최종적으로 배제된다면, 해당 침해는 더 이상 공개로 집행된 것이 아니라 비밀로 집행된 것이고,[350] 이런 통지의 유예나 배제는 법적 근거 없이 행해진 위법한 것이다.[351]

---

345) StPO 제33조 의미의 '절차참가자(Beteiligte)' 및 StPO 제35조 의미의 '재판 당사자(die von Entscheidungen betroffenen Person)'란 법원의 재판에 의해 자신의 권리나 법적 지위가 직·간접적으로 침해당한 모든 절차참여자와 제3자를 의미하고(*Maul*, KK-StPO, § 35 Rn. 3; *Schmitt*, M-G/Schmitt, § 35 Rn. 2; BT-Drs. 19/27654, 61면), StPO 제98조 이하 규정에 따른 '압수 당사자(die von der Beschlagnahme betroffenen Personen)'란 압수를 통해 (대상물의) 보관을 침해당하거나 소유·점유권을 침해당한 모든 자연인·법인을 의미한다(*Greven*, KK-StPO, § 98 Rn. 18; *Köhler*, M-G/Schmitt, § 35 Rn. 2; BT-Drs. 19/27654, 61면). 압수 당사자가 반드시 피의자인 것은 아니지만(*Greven*, KK-StPO, § 98 Rn. 18), 서버에 저장된 정보의 압수에서 (주로 피의자인) 정보주체는 해당 압수에 의해 기본권(정보자기결정권)이 침해당하므로 재판 당사자이자 처분 당사자에 속한다(BT-Drs. 19/27654, 61면).

346) 박중욱, 각주 338의 논문, 66면.

347) *BGH* NJW 2010, 1297, 1298 [Rn. 19]; NStZ 2015, 704, 705; *Greven*, KK-StPO, § 98 Rn. 21; *Kasiske*, StraFo 6/2010, 228, 232면; *Köhler*, M-G/Schmitt, § 98 Rn. 10; *Singelnstein*, NStZ 2012, 593, 596면. 더 나아가 BGH는 StPO 제94조 이하, 제102조 이하에 따른 압수수색에서 통지의 유예를 허용하여 처분이 비밀로 집행되는 것을 허용할지 여부는 입법자의 임무라고 설시하였다(BGH NStZ a.a.O.). [박중욱, 각주 338의 논문, 66면(재인용)]

348) *Greven*, KK-StPO, § 98 Rn. 21; *Köhler*, M-G/Schmitt, § 98 Rn. 10 u. § 105 Rn. 4; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 30. [박중욱, 각주 338의 논문, 66면(재인용)]

349) *BVerfGE* 124, 43, 71 f.; *BGH* NJW 2010, 1297. 1298 [Rn. 19]; *Köhler*, M-G/Schmitt, § 98 Rn. 10; *Wohlers/Greco*, SK-StPO, § 98 Rn. 23; abw. *Sieber*, 69. DJT 2012, C 111: 집행 직후에 예외 없이 고지되어야 한다; a.A. *Brunst*, CR 2009, 584, 592 [Tz. a)]. *Brunst* 박사는 실무에서 이러한 사전통지는 오히려 예외이며, 처분의 공개성은 형사소추관청이 당사자에게 해당 처분을 사후에 통지하는 것으로 달성된다고 주장한다.

350) 이에 관련하여 BVerfG는 이미 2009년 판결(2 BvR 902/06)에서 적절히 설시하였다: "ISP/CP의

2) 피압수자인 피의자에 대한 통지의 유예: StPO 제95조a

지금까지 검토한 바에 따르면, – 2021년 개정 전까지 – 압수수색 일반규정에 따른 압수수색은 공개로, 즉 처분 당사자 알게 집행되어야 했고(위의 가. 참고), 법원의 압수수색 명령에 따른 압수의 대상물이 혐의 없는 제3자가 보관하는 피의자의 물건이나 정보인 경우에는 StPO 제35조 제2항에 따라 처분의 집행 사실이 – 최소한 규범적으로는 – '예외 없이' 처분 당사자, 특히 정보주체인 피의자에게 통지되어야 했다(위의 1) 참고). 하지만 이것은 ISP/CP의 서버에 저장되어 있는 정보의 압수수색에서 증거인멸·훼손의 위험을 야기한다는 점에서 효과적인 형사소추의 이익을 중대하게 침해한다.[352] 이에 따라 혐의 없는 제3자가 보관하는 피의자의 물건이나 정보를 압수하는 경우에 피의자에 대한 통지를 유예할 수 있는 법적 근거가 필요했다. 한편 이러한 유예는 결국 압수수색이 정보주체인 피의자 모르게, 즉 비밀로 집행되도록 하며, 이에 따라 동 처분은 비밀의 강제처분이 되고, BVerfG의 입장에 따르면 그러한 처분이 정당화되기 위해서는 가중된 처분요건과 절차법적 통제장치가 필요하다(위의 나. 2) 참고).[353] 이때 처분요건과 절차법적 통제장치가 어느 수준으로 형성되어야 하는지가 문제되는데, 전송과정 종료 후 ISP/CP의 서버에 저장되어 있는 정보의 수집은 전송 중인 정보를 수집하는 통신감청에 상응할 수 있다는 점에서 위 통지유예의 허용요건은 통신감청의 처분요건(StPO 제100조a)에 상응하게 형성될 필요가 있다.[354]

서버에 들어온 e-mail이 우편함에서 확보되는 경우 …… (정보주체의 권리보호를 위해), 원칙적으로 형사소추관청에 의해 그에게 미리 통지될 것이 요구될 수 있다. …… 이런 요구는 StPO 제35조와 제98조 제2항 제6문에 의해 고려되고 있다. (하지만) …… 압수수색 명령은 제35조에 따라 언제나 처분의 집행 전에 당사자에게 고지되어야 한다"(*BVerfGE* 124, 43, 71 f. [Rn. 94-95]). 앞의 인용문에서 '제6문'은 '제5문'의 오기이다.

351) 다만, 독일에서는 이러한 위법성이 일반적으로 획득된 정보의 사용금지를 야기하지는 않을 것이다(앞의 2. 가. 2) 나) (3) 참고).

352) BT-Drs. 19/27654, 61면 이하: 원칙적인 공개성이 수사를 완전히 무력화시키는 것은 허용될 수 없다. [박중욱, 각주 338의 논문, 66면(재인용)]

353) BT-Drs. 19/27654, 62면.

354) BVerfG는 2 BvR 902/06 판결에서 서버에 저장된 정보의 압수수색이 일반규정에 근거하여 비밀로 행해지는 경우를 정당화하기 위한 요건을 명시적으로 언급하지는 않았지만, 그러한 처분이 공개로 행해지는 경우에는 침해강도가 증대되지 않는다는 점을 통신감청과의 대비를 통해 이유제시하였다(*BVerfGE* 124, 43, 62 f. [Rn. 69]). 결국 동 재판소는 ISP/CP의 서버에 저장된 정보에 대한 비밀의 압수수색을 위한 통제장치로서 통신감청의 그것에 상응하는 통제장치가 요구된다는 점을 간접적으로 드러냈고, 독일의 입법자는 StPO 제95조a를 신설할 때 이것을 고려하였다.

이에 따라 독일의 입법자는 2021년 개정을 통해 압수대상물을 피의자 아닌 자가 보관하는 경우에서 압수대상물의 점유자나 소유자이자 압수 당사자인 피의자에 대한 통지의 유예를 허용하는 법적 근거인 StPO 제95조a를 신설하였다:

StPO 제95조a [피의자에 대한 통지의 유예; 공개금지]

① 피의자 아닌 자가 보관하는 대상물의 압수에 대한 법원의 명령이나 승인의 경우 압수 당사자인 피의자에 대한 통지는 다음의 경우에서 그것이 수사목적을 위험하게 만드는 경우에 한하여 유예될 수 있다:

1. 피의자가 정범이나 공범으로서 개별적인 경우에도 중요한 의미의 범죄행위, 특히 제100조a 제2항에 열거된 범죄를 범하였다는 혐의, 가벌적 미수에서 이러한 범죄의 실행에 착수했다는 혐의 또는 다른 범죄행위를 통해서 위 범죄를 예비하였다는 혐의가 특정한 사실관계에 비추어 이유 있고,
2. 사실관계의 조사나 피의자의 거주지 수사가 다른 방법으로는 가망이 없거나 현저히 곤란한 경우.

② 제1항에 따른 피의자에 대한 통지의 유예는 법원에 의해서만 명령될 수 있다. 해당 유예는 6개월 이하로 기한이 정해져야 한다. 유예의 요건이 계속 존재하는 경우 각 3개월 이내의 기간으로 법원에 의한 유예의 연장이 허용된다.

③ 혐의자 아닌 자가 보관하는 대상물이 법원의 명령에 의하지 않고 압수된 후 3일 이내에 압수에 대한 법원의 승인 및 제1항에 따른 피의자에 대한 통지의 유예가 청구된 경우, 제98조 제2항 제5문에 따른 압수 관련 피의자에 대한 고지는 배제될 수 있다. 제98조 제2항에 따른 절차에서는 법원에 의한 피의자에 대한 사전청문(제33조 제3항)이 필요하지 않다.

④ 제1항에 따라 유예된 피의자에 대한 통지는 그것이 수사목적의 위험 없이 가능해지자마자 행해진다. 통지의 경우 피의자에게는 제5항에 따른 사후적 권리보호의 가능성과 그 법정기한이 안내되어야 한다.

⑤ 제1항에 따른 유예의 종료 후에도 피의자는 제4항에 따른 자신에 대한 통지 후 2주 이내에 해당 압수, 그 집행의 유형과 방식, 통지의 유예에 대한 적법성 심사를 처분의 명령을 관할하는 법원에 청구할 수 있다. 이러한 법원의 재판에 대해서는 즉시항고가 허용된다. 공소가 제기되어 있고 피고인이 통지를 받은 경우에는 해당 사건을 처리하는 법원이 절차를 종료하는 재판에서 해당 청구에 대해 결정한다.

⑥ 제1항에 따른 통지의 유예가 명령되는 경우, 이와 동시에 (피의자 아닌 자인 압수처분의)

대상자는 유예기간 동안 피의자와 제3자에게 압수 및 그에 선행하는 제103조와 110조에 따른 수색이나 제95조에 따른 제출명령을 공개할 수 없다는 점이 모든 사정에 대한 고려와 당사자들의 이익형량에 따라 개별적으로 명령될 수 있다. (법원의 명령에 의하지 않은 압수에서) 제3항에 따라 고지가 배제되고 압수에 대한 법원의 승인과 피의자에 대한 통지의 유예가 청구된 경우, 제2항은 지체의 위험의 경우 검사와 그의 수사관(법원조직법 제152조)도 제1문에 따른 명령을 내릴 수 있다는 조건으로 준용된다. 검사나 그의 수사관이 이러한 명령을 내리는 경우 3일 이내에 법원의 승인이 청구되어야 한다.

⑦ 제6항에 따른 공개금지에 대한 위반의 경우 제95조 제2항이 준용된다.

제1항은 통지유예의 요건을, 제2항은 통지유예 명령의 관할을, 제3항은 법원에 의하지 않은 압수명령에서의 통지유예를, 제4항과 제5항은 유예기간 종료 후의 통지와 사후적 권리보호 절차를, 제6항과 제7항은 압수물 보관점유자인 제3자의 비밀유지 의무와 그 강제를 위한 수단을 규정한다.[355]

우선 제1항에 따르면 압수수색 일반규정에 근거한 '제3자 보관의 대상물'에 대한 압수수색에서 StPO 제35조 제2항에 따른 '피의자인 정보주체'에 대한 통지가 일정한 요건 아래에서 유예될 수 있다. 문언에 따라 통지유예는 전자정보를 포함한 모든 대상물의 압수에 적용되며, 정보주체가 피의자인 경우에만 허용된다.[356] 통지유예는 중대한 범죄에 대한 증대한 혐의가 존재하고 수사목적이 위험해질 경우에 한하여[357] 보충적으로만 명령될 수 있는데, 이런 요건은 대체적으로 통신감청의 수권규범인 StPO 제100조a 제1항과 제2항의 내용에 상응한다.[358] 이어서 제2항에 따르면 통지유예의 명령 관할은 법원에게만 있고, 법원은 반드시 기간을 정하여 유예를 명령해야 한다. 여기서 – 통신감청의 관할에 관한 StPO 제100조e 제1항과 달리 – 수사기관의 긴급권이 인정되지 않는 것은 통지가 유예되면 압수수색은 더 이상 공개의 처분이 아니라 예외적인 비밀의 처분이 된다는 점이 고려된 것이다.[359] 제4항과 제5항에

355) 박중욱, 각주 338의 논문, 69면.

356) BT-Drs. 19/27654, 63면. [박중욱, 각주 338의 논문, 69면(재인용)]

357) 보통 문헌에서는 비밀의 집행을 통해 증거로서 중요한 정보가 획득될 수 있는 경우, 공개의 집행을 의미하는 통지는 '수사목적을 위험하게' 만든다고 해석된다(*Köhler*, M-G/Schmitt, § 101 Rn. 19; BT-Drs. 19/27654, 63면). [박중욱, 각주 338의 논문, 69면(재인용)]

358) BT-Drs. 19/27654, 63면 이하. [박중욱, 각주 338의 논문, 69면(재인용)]

359) BT-Drs. 19/27654, 65면. 물론 수사기관은 압수수색 영장을 청구할 때 통지유예의 명령도 함께 청구할 수 있다(a.a.O.). [박중욱, 각주 338의 논문, 69면(재인용)]

따르면 수사목적의 위험이 없어지거나 유예기간이 도과된 후 통지는 즉시 행해져야 하고, 피의자인 정보주체는 준항고를 통해 원처분인 압수명령과 그 집행의 유형과 방식, 그리고 통지유예 명령의 적법성에 대해 다툴 수 있다.[360] 제6항과 제7항은 통지유예의 실효성을 확보하기 위한 제3자에 대한 공개금지 명령과 그 준수의 관철을 위한 (간접)강제의 법적 근거이다.[361]

라. 수사목적의 온라인 수색

1) 입법 배경

온라인 수색이란 기술적 수단으로 처분 당사자가 이용하는 정보기술시스템에 비밀리에 침입하여, 거기에 저장된 정보를 수집하거나 그 이용을 감시하는 수사행위를 의미한다. 이 처분은 기술적 측면에서 본다면 수사기관이 처분 대상자에 의해 사용되는 단말기인 스마트폰, PC, 태블릿 PC 등에 국가의 악성 소프트웨어인 스파이프로그램, 소위 '국가 트로이 목마(Staatstrojaner)'를 비밀리에 투입·설치하여 해당 단말기에 침입하는 방식으로 행해진다.[362] 수사기관의 수사상 처분으로서의 온라인 수색은 개념상 개인의 정보저장매체에 대한 단순 공개의 압수수색이 단지 처분 당사자 모르게, 즉 비밀로 행해지는 것이라 생각될 수도 있지만, 해당 처분에 의한 기본권 침해의 정도를 고려할 때 온라인 수색은 단순 압수수색과는 전혀 다른 유형의 처분이다. 즉, 오늘날의 정보기술환경에서 스마트폰 등 개인의 복합적인 정보기술시스템이 가지는 중요성과 각 시스템 간의 연결 가능성 및 비밀리에 집행되는 온라인 수색을 통해 수집될 수 있는 개인정보의 광범위함과 다양성 등을 고려할 때, 온라인 수색의 기본권 침해강도는 기존의 압수수색보다 훨씬 강력하다. 이런 점에서 이 수사방법의 이용은 매우 제한된 범위에서 보충적으로만 허용되며, 독립된 외부 기관의 강력한 통제가 요구된다.

독일에서 정보기관과 수사기관을 중심으로 테러나 조직범죄 등 국가안보범죄의 영역에서 암호화된 정보전송에 대처하기 위한 수단으로서 온라인 수색의 필요성이

---

360) 박중욱, 각주 338의 논문, 69면(재인용).
361) 박중욱, 각주 338의 논문, 66면(재인용).
362) *Beukelmann*, NJW-Spezial 2017, 440; *Blechschmitt*, MMR 2018, 361, 364. 이런 점에서 온라인 수색은 '국가의 해킹'이라 할 것이다(BT-Drs. 16/5846, S. 64 am Anfang).

주장되었고, 이것을 – 수사목적이 아닌 – 정보기관의 임무수행을 위한 처분으로서 처음 합법화한 곳은 노르트라인-베스트팔렌(Nordrhein-Westfalen: NRW)주(州)였다. 동 주는 2006. 12. 20.에 해당 주의 헌법호보법(Gesetz über den Verfassungsschutz in NRW: 2006 VSG NRW)을 개정함으로써 주의 국내정보기관인 헌법보호청(Landesbehörde für Verfassungsschutz: LfV)[363]의 임무수행을 위한 집행방법의 하나로서 온라인 수색을 도입하였다: 2006 VSG NRW 제5조 제2항 제11호 후단. 하지만 이 규정에 대해서는 BVerfG에 바로 규범통제를 위한 위헌법률심판이 제기되었고, 동 재판소는 2008. 2. 27.에 그 합헌성 및 허용요건에 대한 판결, 소위 '온라인 수색 판결'을 내렸다.[364]

온라인 수색 판결에서 BVerfG는 과학기술의 발전과 생활환경의 변화 과정에서 새로운 유형의 인격에 대한 위험에 대처하고 그 기본권적 보호의 흠결을 보충하기 위해 일반적인격권에 기초한 기존 보호를 초과하는 새로운 보호가 필요하다고 판단하였고,[365] 이를 위해 일반적인격권의 새로운 구체화로서 '정보기술시스템의 비밀성과 무결성의 보장에 관한 기본권(Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)', 소위 'IT-기본권(IT-Grundrecht)'[366]을 새로이 창설하였다.[367] 동 판결에 따르면 개인정보를 생성·처리·저장할 수

---

363) 독일의 정보기관은 연방과 주의 기관으로 구분된다. 연방기관으로는 국외정보의 수집을 담당하는 연방정보부(Der Bundesnachrichtendienst: BND), 군(軍) 관련 정보의 수집을 담당하는 (연방)군정보부(Der Militärische Abschirmdienst; MAD), 국내정보의 수집을 담당하는 연방헌법보호청(Das Bundesamt für Verfassungsschutz: BfV)이 있고 주의 기관으로는 각 주 내의 정보수집을 담당하는 16개 헌법보호청이 있다. 이에 대한 자세한 내용에 대해서는 박희영·홍선기, "독일 정보기관의 공법 체계 및 경찰과의 분리원칙", 『법학논집』 제26권 제3호, 이화여자대학교 법학연구소, 2022.3, 235면 참고.

364) *BVerfGE* 120, 274 = NJW 2008, 822.

365) 박중욱, "수사목적 온라인 수색의 허용요건 – 독일의 논의를 참고한 입법론적 검토 –", 『형사정책연구』 제34권 제3호, 한국형사법무정책연구원, 2023.9, 95, 96면[각주 4](재인용).

366) *Gurlit*, NJW 2010, 1035, 1036; *Dalby*, CR 2013, 361, 367; *Roggan*, StV 2017, 821, 823; *Derin/Golla*, NJW 2019, 1111, 1114; 박희영, "예방 및 수사목적의 온라인 비밀 수색의 허용과 한계", 『원광법학』 제28권 제3호, 원광대학교 법학연구소, 2012.9, 153, 160면). 한편 동 기본권은 '컴퓨터-기본권(Computer-Grundrecht)'이라고 불리기도 한다(*Kudlich*, GA 2011, 193, 198; *Singelnstein/Derin*, NJW 2017, 2646, 2648; *Zimmermann*, JA 5/2014, 321, 323).

367) *BVerfGE* 120, 274, 313-315 [Rn. 201-206]. 이 판결에서 BVerfG는 컴퓨터-기본권 창설의 배경 다음과 같이 설명한다. 현대 정보사회에서 인격발현을 위해서는 네트워크(인터넷)로 연결된 정보기술시스템의 이용이 필수적이고 중요한 요소이지만(a.a.O. 303-305 [Rn. 171-176]), 해당 시스템에 대한 기술적 접근 가능성은 인격에 대한 새로운 위험을 야기하였고, 이 위험에 효과적으로 대처하는 것은 개인, 최소한 평균적 이용자에게는 과도한 요구이고 실질적으로 불가능하다

있는 모든 정보기술시스템이 컴퓨터-기본권에 의한 특별히 보호되어야 하는 것은 아니다.[368] 하지만 정보기술시스템에의 접근을 통해 해당 시스템의 이용 그 자체가 감시되거나 그 저장매체가 수색되는 경우[369] 또는 수량과 다양성에서 한 개인의 생활형성의 본질적인 부분을 들여다보거나 중요한 내용을 가진 인격상을 얻는 것을 가능하게 할 정도의 개인정보가 획득되는 경우에는[370] 동 기본권에 의해 보호되어야 한다.

한편 이 기본권은 무제한적이지 않으며 예방적 목적이나 형사소추를 위해 제한될 수 있다. 이와 관련하여 BVerfG는 무엇보다 전체적 이익형량에 따라 정보기술시스템에 대한 비밀접근이라는 높은 강도의 기본권 침해[371]를 정당화하기 위한 강화된 처분요건과 절차법적 통제장치를 요구하였다.[372] 동 재판소는 우선 강화된 처분요건으로 '매우 중요한 법익'에 대한 '구체적인 위험'과 이 위험에 대한 '사실상의 근거'가 존재할 것을 요구하였고,[373] 강화된 절차법적 통제장치로는 엄격한 법관유보 이외에[374] 절대적으로 보호되는 사적 생활형성의 핵심영역에 대한 침해를 피하기 위한 충분한 법적 안전장치를 요구하였다.[375] 이때 BVerfG는 온라인 수색의 집행에서 사적 생활형성의 핵심영역에 속하는 정보를 보호하기 위해 2단계의 심사, '수집 전이나 수집 중의 단계'와 '수집 후의 분석 단계'에서 각각 획득될 또는 획득된 정보의 핵심영역 관련성이 심사될 것 및 관련성이 인정되는 정보는 즉시 삭제될 것을 요구하였다(소위 "2단계 보호구상"). 여기서 BVerfG는 실무상 첫 번째 단계보다 두 번째 단계에서의 보호가 실질적으로 중요하다고 하면서 수집된 정보의 열람 과정에서 당사자의 이익이 충분히 고려될 수 있는 절차가 법적으로 형성될 것을 요구하였는데,[376] 그 절차는 구체적으로

(a.a.O. 305-306 [Rn. 177-180]). 따라서 정보기술시스템에 대한 기본권적 보호 필요성이 발생하지만, 통신의 비밀, 주거의 불가침, 일반적인격권, 정보자기결정권 등 기존의 기본권으로는 그 보호를 충분히 달성할 수 없기 때문에 새로운 기본권이 요구된다(a.a.O. 306-313 [Rn. 181-200]).

368) *BVerfGE* 120, 274, 313 [Rn. 202].

369) *BVerfGE* 120, 274, 308 [Rn. 186].

370) *BVerfGE* 120, 274, 314 [Rn. 203].

371) *BVerfGE* 120, 274, 322 ff. [Rn. 229 ff.]. BVerfG의 설시에 따르면 복합적인 정보기술시스템에서의 정보수집은 인격탐구에 대한 상당한 가능성을 열어주며(a.a.O. 322 [Rn. 231]), 무엇보다 동 시스템 이용의 장기간 감시와 정보의 실시간 수집을 가능하게 한다는 점에서 기본권 침해의 비중이 특별히 중대하다고 한다(a.a.O. 323 [Rn. 234]).

372) *BVerfGE* 120, 274, 326 ff. [Rn. 242 ff.].

373) *BVerfGE* 120, 274, 327-331 [Rn. 246-256].

374) *BVerfGE* 120, 274, 331-333 [Rn. 257-261].

375) *BVerfGE* 120, 274, 335-339 [Rn. 270-285].

법관유보를 의미한다. 이는 온라인 수색 판결에 명확히 드러나 있지 않지만, 동 판결이 참조한 BVerfG의 2004.3.3. 판결, 소위 '주거감청 판결'[377]에 명시적으로 드러나 있다. BVerfG는 이 판결에서 2단계 보호구상의 두 번째 단계에서의 열람된 정보의 핵심영역 관련성에 대한 판단을 형사소추관청 이외에 독립된 기관, 즉 법원도 내릴 수 있어야 한다고 설시하면서, 법원이 (수사절차 종료 후인) 공판준비절차가 돼서야 비로소 핵심영역 관련성 판단을 내릴 수 있도록 하는 것은, 관련성 판단이 실질적으로 사용가능성에 대한 판단이라는 점을 고려할 때, 핵심영역 보호와 모순되며, 수사과정에서 그 관련성이 명확하지 않다면 수사기관은 법원에 그에 대한 판단을 구할 의무가 있고, 입법자는 이런 내용을 법률에 명확히 규정해야 한다고 설시하였다.[378]

2) 수권규범: StPO 제100조b, d, e, 제101조, 제101조b[379]

이후 독일의 입법자는 2017년 개정을 통해 BVerfG가 제시한 기준을 고려하여 형사소추 목적의 온라인 수색을 StPO에 도입하였다. 이때 그 처분요건과 절차법적 통제장치는 이미 StPO에 도입되어 있던 비밀의 강제처분 중 가장 강력한 기본권 침해강도를 갖는다고 평가되었던 주거감청과 동일한 수준으로 형성되었고,[380] 이에 따라 주거감청에 대한 기존의 규제들((舊) StPO 제100조c 제4-7항)이 2017년 개정을 통해 온라인 수색에까지 확대되었다(StPO 제100조b, d, e, 제101조, 제101조b).

우선 처분요건과 관련하여 처분의 대상 범죄는 '특별히 중대한 범죄'로 제한되어 있고(StPO 제100조b 제1항 제1호), 그 구체적인 목록은 제2항에 열거되어 있다: 소위 '범죄목록(Straftatenkatalog)'. 이 목록에 열거된 범죄로는 내란·외환 등, 범죄단체·테

---

376) *BVerfGE* 120, 274, 339 [Rn. 283].
377) *BVerfGE* 109, 279 = NJW 2004, 999.
378) *BVerfGE* 109, 279, 333 f. [Rn. 190-194].
379) 각 규정의 전체 내용은 독일법연구회(譯), 『독일 형사소송법』, 사법발전재단, 2018 참고.
380) 이는 두 처분의 침해강도가 동일하다는 입법적 고려에 근거한다(BT-Drs. 18/12785, S. 54; *BVerfGE* 141, 220, 303 [Rn. 210 a.E.]). BVerfG는 2008.12.25.에 개정되고 2009.1.1.에 발효된 국제테러 위험방지 법률(das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008, BGBl. I S. 3083)을 통해 신설된 연방범죄수사청법(Bundeskriminalamtgesetz: BKAG) 제3절a에 대한 헌법소원을 심사한 2016. 4. 24.의 판결(*BVerfGE* 141, 220 = NJW 2016, 1781)에서 주거감청과 정보기술시스템에 대한 비밀의 접근을 침해강도의 측면에서뿐만 아니라(a.a.O. 273-275 [Rn. 114-116]), 요구되는 침해요건과 절차법적 통제장치의 측면에서도 전반적으로 동일하게 취급하였다(a.a.O. 275 ff. [Rn. 117 ff.]).

러단체 조직, 화폐·유가증권 위조, 아동 음란물 배포·취득·소지, 자금세탁, 증뢰·수뢰, 탈세, 난민법 및 외국인체류법 위반행위, 마약 유통·거래·수입, 전쟁무기통제법·국제형법(집단학살 등)·무기법 위반행위 등이 있다.[381] 다음으로 절차법적 통제장치와 관련하여 온라인 수색은 법원의 강력한 통제 아래 있다. 우선 사적 생활형성의 핵심영역 보호를 위한 규정인 StPO 제100조d에는 2단계 보호구상을 포함하여 BVerfG가 요구한 내용이 전부 반영되어 있다. 이어서 StPO 제100조e에 따르면 법원은 온라인 수색의 처분절차에 다층적으로 개입하는데, 이와 관련하여 무엇보다 수사기관은 그 집행의 종료 시에 처분의 결과뿐만 아니라 (집행)과정도 법원에 보고해야 한다(동조 제5항 제2, 3문).[382] 이외에 처분에 대한 사후 통지 및 법원의 적법성 통제에 대해서는 StPO 제101조가 적용된다. 사후 통지와 관련하여 가장 중요한 부분은 동 통지의 예외적인 유예와 배제의 사유 및 그 판단권자인데, StPO 제101조 제4항 내지 제6항에 따르면 최초의 통지 유예는 수사기관의 판단에 의해 가능하지만 그 계속적 유예 및 최종적 배제를 위해서는 법원의 승인이 필요하다.[383]

3) 입법에 대한 비판과 운용 현황

2017년 수사를 위한 온라인 수색의 도입은 문헌에서 많이 비판되고 있다.[384] 우선 그 법적 근거가 입법과정에서 '뒷문을 통하듯이'[385] 또는 '큰 고민 없이'[386] StPO에 삽입되었다고 지적된다.[387] 이외에 수권규범에 동 처분의 기술적 수단에 대한 제한이 없고, 법문언에 단지 "기술수준에 따라(nach dem Stand der Technik)"라는 조건만 있다는 비판도 제기된다.[388] 하지만 가장 큰 비판은 온라인 수색이 – 위험방지나

---

381) 박중욱, "수사목적 온라인 수색의 허용요건 – 독일의 논의를 참고한 입법론적 검토 -", 120-121면(재인용).

382) 박중욱, 위의 논문, 121면(재인용).

383) 박중욱, 위의 논문, 122면(재인용).

384) *Beukelmann*, NJW-Spezial 2017, 440; *Roggan*, StV 2017, 821; *Singelnstein/Derin*, NJW 2017, 2646; *Freiling/Safferling/Rückert*, JR 2018, 9; *Blechschmitt*, MMR 2018, 361; *Soiné*, NStZ 2018, 497 m.w.N.

385) *Beukelmann*, NJW-Spezial 2017, 440 am Anfang.

386) *Blechschmitt*, MMR 2018, 361, 366.

387) 법률초안의 내용은 이미 입법과정에서 많은 전문가들에 의해 신랄하게 비판되었음에도 불구하고, 해당 초안은 충분한 토론 없이 연방하원의 위원회안으로 수용되었다(*Beukelmann*, NJW-Spezial 2017, 440; *Singelnstein/Derin*, NJW 2017, 2646).

388) *Köhler*, M-G/Schmitt, § 100a Rn. 14i. 물론 이는 "기술적으로 열려있게" 구상된 것이지만,

정보기관 임무수행의 방법을 넘어 – 형사소추를 위한 수사방법으로서 과연 필요한 것인지 및 신설된 규정의 처분요건과 절차법적 통제장치로 정당화될 수 있는지에 대한 의문의 제기이다.[389] 전자와 관련해서는 수사목적의 온라인 수색의 도입은 범죄예방과 형사소추 사이의 한계를 희미하게 만든다는 비판이 있다.[390] 반면 후자와 관련해서는 온라인 수색을 통해 획득될 수 있는 정보의 범위가 통신감청뿐만 아니라 주거감청보다도 훨씬 더 깊고 넓다는 점이 지적된다.[391] 즉, 동 처분에 의해 정보기술 시스템에 이미 저장된 모든 정보와 새로 도착한 통신내용 및 당사자의 전체 이용행위가 감시될 수 있고, 더 나아가 'Live-접근', 즉 '어깨 위에서의 비밀 감시(heimliche Blick über die Schulter)'도 가능하며, Keylogging을 수단으로 획득되는 ID와 PW와 같은 접속코드도 수집될 수 있다는 것이다.[392] 이런 점에서 온라인 수색은 추가의 정보 수집·처리 없이 단독으로 사적 영역을 특별히 깊게 침투하는 침해를 가능하게 한다.[393] 요컨대 온라인 수색은 기술적으로 헌법상 금지된 무제한의 감청을 가능하게 하지만,[394] 그 금지의 보장이 현재 기술적 측면에서 명확하지 않다는 것이다. 따라서 온라인 수색의 (잠재적인) 침해강도는 StPO 제100조c에 따른 주거감청의 그것보다 훨씬 더 강력하고, 오히려 '반복적으로 행해질 수 있는 비밀의 주거수색'과 유사하다.[395] Roggan 교수는 두 처분의 침해강도를 유사하게 취급한 2016년의 BKAG 판결에서의 BVerfG의 관점과 2017년 개정의 입법이유를 비판한다.[396]

한편 독일 연방법무부(Das Bundesministerium der Justiz: BMJ)의 최근 공고에 따르면, StPO에 따른 수사목적의 온라인 수색은 2020년에 총 10개의 수사절차에서 총

정보안전의 흠결을 메우기 위한 구체적인 기술적인 안전조치도 마찬가지로 미해결인 채로 남아 있다는 것이다(a.a.O. Rn. 14k).

389) *Roggan*, StV 2017, 821, 827.

390) *Beukelmann*, NJW-Spezial 2017, 440; *Roggan*, StV 2017, 821, 827.

391) *Roggan*, StV 2017, 821, 826; *Blechschmitt*, MMR 2018, 361, 365.

392) *Roggan*, StV 2017, 821, 825.

393) *Roggan*, StV 2017, 821, 826. BVerfG 또한 온라인 수색 판결에서 동 처분은 당사자 인격에 대한 포괄적인 추론을 가능하게 할 명백한 위험을 가진다고 설시하였다(*BVerfGE* 120, 274, 323 [Rn. 232]).

394) *Blechschmitt*, MMR 2018, 361, 365; *Roggan*, StV 2017, 821, 826.

395) *Roggan*, StV 2017, 821, 826 a.E. 현재 일반적인 견해에 따르면 StPO의 개별적인 비밀의 수사처분들 중에서 온라인 수색의 침해강도가 가장 강력하다고 평가된다(*Singelnstein/Derin*, NJW 2017, 2646, 2647; *Soiné*, NStZ 2018, 497).

396) *Roggan*, StV 2017, 821, 826 f.

23회(최초명령 12회, 연장명령 11회) 내려졌으나, 실제로는 8회만이 집행되었다. 명령이 내려진 대상 범죄와 횟수는 테러단체나 범죄단체 조직죄(StPO 제100조b 제2항 제1호 b목) 3회, 아동음란물 배포·취득·소지죄(동호 e목) 1회, 범죄단체구성 절도죄(동호 h목) 1회, 중강도죄와 강도치사죄(동호 i목) 1회, 강도적 공갈죄과 특히 중대한 공갈죄(동호 j목) 8회, 마약유통·거래·수입 등 죄(동 제4호 b목) 9회이다. 2019년에는 동 처분이 총 21개의 수사절차에서 총 33회(최초명령 22회, 연장명령 11회) 내려졌으나, 실제로는 12회만이 집행되었다. 명령이 내려진 대상 범죄와 횟수는 내란·외환 등의 죄(StPO 제100조b 제2항 제1호 a목) 1회, 테러단체나 범죄단체 조직죄(동호 b목) 2회, 성적자기결정에 대한 죄(동호 d목) 1회, 개인의 자유에 대한 죄(동호 g목) 4회, 중강도죄와 강도치사죄(동호 i목) 2회, 강도적 공갈죄와 특히 중대한 공갈죄(동호 j목) 13회, 자금세탁과 부정수익은닉죄(동호 l목) 1회, 마약유통·거래·수입 등 죄(동 제4호 b목) 12회, 전쟁무기통제법 위반죄(동 제5호 a목) 1회이다.[397]

5. 소결 및 우리에게의 시사점

정보통신기술의 발전으로 유체물만을 상정하였던 기존의 압수수색 규정과 그 해석·적용이 실재적인 측면뿐만 아니라 규범적인 측면에서도 도전을 받았던 것은 독일에서도 마찬가지였다. 다만 독일은 우리와 달리 지난 20여 년 동안 법치국가 원칙과 비례성 원칙에 기초하여 기술의 발전에 따라 가능해진 새로운 수사방법을 지속적으로 법률에 수용하고 있으며, 기존 수사방법에서 예상치 못했던 중대한 기본권 침해를 입법을 통해 적절히 상쇄하려고 시도하고 있다. 이러한 독일의 개정방향은 근본적으로 BVerfG의 일련의 판결에 따른 것인데, 이와 관련하여 동 재판소가 특히 중요하게 여기는 것은 압수수색을 통한 과도한 정보수집의 제한과 수사처분의 비밀성에 대한 가중된 통제이다. 전자와 관련하여 BVerfG는 StPO 제110조에 따른 열람과 이를 위한 임시확보를 중요한 절차적 수단으로 여기며, 후자와 관련해서는 가중된 처분요건과 절차법적

397) 독일 연방법무청(Bundesamt für Justiz) 홈페이지, "Statistiken der Rechtspflege"(https://www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken_node.html#AnkerDokument44152; 최종접속일 2023.9.15.). 다만, 2019년의 통계 자료에는 전체 명령 건수와 범죄별 명령 건수의 합에서 4회의 오차가 있다.

통제장치에 큰 비중을 둔다. 이때 가중된 처분요건과 관련해서는 범죄의 중대성과 범죄혐의의 강도 및 보충성이 고려되고, 가중된 절차법적 통제장치와 관련해서는 단순 압수수색에서의 그것보다 엄격한 법관유보 및 사후 통지의 절차가 고려된다.

반면 우리나라는 디지털 증거의 압수수색과 관련하여 지금까지 2차례의 개정만이 있었고, 그 내용 또한 제한적이다. 우선 2011. 7. 18.의 개정을 통해 전자정보의 압수범위와 압수방법이 명시되었고, 최근인 2022. 2. 3의 개정을 통해 피처분자와 피고인(피의자)이 다른 경우 영장의 제시와 사본교부가 생략될 수 있도록 변경되었다. 그 이외에 디지털 증거의 압수수색과 관련된 개정은 없다. 오히려 현재 디지털 증거의 압수수색에 대한 통제는 입법적으로 보다는 대법원의 (전원합의체) 판결/결정에 따라 규제되고 있다. 특히 대법원은 압수수색 과정에서 발견된 디지털 증거의 수사기관으로의 반출 및 열람을 수색의 한 과정으로 봄으로써 StPO 제110조가 있는 독일과 동일한 법리를 전개하고 있다. 나아가 대법원은 수사기관으로 반출된 정보의 열람 과정에 피압수자와 정보주체의 출석권을 위법수집증거배제법칙과 결부하여 인정함으로써, 이 부분과 관련해서는 피의자 내지 피압수자의 방어권을 독일보다 더 강력하게 보장하고 있다. 하지만 우리의 입법자와 대법원, 나아가 헌법재판소 또한 – 독일과 달리 – 기본권을 중대하게 침해하는 비밀의 수사처분, 즉 '비밀의 강제처분'에 대한 강력한 입법적 통제를 별도로 요구하지 않는다. 이는 헌법재판소의 2012. 12. 27.의 결정(2011헌바225)과 통비법 제9조의2와 제9조의3의 내용을 보면 알 수 있다.

자유-법치주의 국가에서 형사절차상의 기본권 침해와 그 한계설정은 언제나 논의의 중심에 놓여 있다. 국가는 현실의 변화에 따른 새로운 위험에 대처해야 하지만, 여기에는 반드시 법치국가적 한계가 있기 때문이다. 국가의 안전보장과 질서유지의 임무 및 이와 충돌되는 기본권 보호의 의무는 법치국가에서 모두 포기될 수 없는 것이다. 기본권을 중대하게 침해할 수 있는 수사처분은 법률유보 원칙, 규범명확성 원칙, 비례성 원칙에 따라 법률에 더 엄격하게 규정될 필요가 있다. 특히 개별 처분의 기본권 침해의 유형과 방식 및 강도에 따라 각 처분의 명령요건과 절차적 통제장치가 법률로 구체적으로 규정될 필요가 있다. 이런 처분에 대한 통제가 전반적으로 행정기관이나 법원에 위임되는 것은 법치국가적 측면에서 타당하지 않다.

제2절 | 일본의 디지털 증거 압수수색 관련 법률과 판례 검토

1. 일본의 디지털 증거 압수수색의 개념과 현황

가. 사이버범죄의 개념

현재 일본에서 '사이버범죄'는 인터넷 등 고도정밀통신네트워크를 사용한 범죄를 통칭하는 의미로 사용하지만,[398] 형법에 명문상 규정된 개념은 아니다. 따라서 범죄의 개념 정의나 분류방법은 학자에 따라 다소 차이가 있다.[399] 한편, 인터넷의 보급이 발달하기 이전에는 '컴퓨터 시스템에 대한 범죄 또는 이를 악용한 범죄'를 '컴퓨터범죄'라고 정의했다.[400] 이 중 "컴퓨터가 행위 수단 내지 목적인 반사회적 침해행위를 말하며, 컴퓨터 및 컴퓨터 네트워크를 수단으로 기존의 전통적 범죄행위를 실행하는 것을 제외한 것"을 협의의 범죄로 정의하는 견해도 있다.[401] 이후 정보통신기술의 발전과 더불어 컴퓨터 및 전기통신기술을 악용한 범죄를 '하이테크 범죄'라고 칭하기 시작했다.[402] 즉, 컴퓨터를 이용한 범죄와 함께, 컴퓨터 네트워크상에서 발생하는 범죄 및 컴퓨터 네트워크를 사용한 기존의 범죄 모두를 아우르는 개념으로 '하이테크 범죄'를 사용한 것이다.[403] 이후, 유럽평의회에서 사이버범죄협약의 초안을 작성하는 과정에서 '사이버범죄'라는 개념이 등장하여 '컴퓨터시스템을 공격하는 범죄 및 컴퓨터 시스템을 이용하여 이루어지는 범죄'를 지칭하는 용어로 정착했다. 한편, 정보통신기술의 고도화에 대응하는 관점에서 범죄행위를 바라볼 경우 '하이테크 범죄'라는 용어가 더욱 적합하며 국경이나 물리적 존재를 뛰어넘는 네트워크 사회에서 시민생활이나 경제생활의 안전을 보호하는 관점에서 이를 규제하고자 할 때는 '사이버범죄'라

398) 安冨 潔, "情報化社会における刑事立法の役割：コンピュータ犯罪からサイバー犯罪へ",『慶應法学』42巻, 2019, p.382.
399) 岡田 好史, "サイバー刑法の概念と展望",『専修大学法学論集』118号, 2013, p.66.
400) 安冨 潔, 위의 논문, p.382.
401) 岡田 好史, 위의 논문, p.69.
402) '하이테크 범죄'라는 용어는 선진 8개국(G8) 국가들이 채택한 '하이테크 범죄 방지를 위한 10가지 기본원칙 및 10가지 행동지침에 등장한다(安冨 潔, 위의 논문, p.382).
403) 指宿 信, "サイバースペースにおける証拠収集とデジタル証拠の確保：2011年改正法案を考える",『法律時報』83巻7号, 2011, p.84.

는 용어가 적합하다는 견해도 있다.[404] 한편 일본 경찰청에서 발간하는 경찰백서에는 사이버범죄를 "부정 액세스 행위 금지 등과 관련된 법률 위반, 컴퓨터·전자적기록대상 범죄 그 밖에 범죄 실행에 불가피한 수단으로 고도정보통신네트워크를 이용한 범죄"로 정의한다.[405]

나. 전자적기록(디지털데이터)과 디지털 증거

전자적기록(電磁的記錄)은 "전자적(電子的) 방식, 자기적(磁氣的) 방식, 그 밖에 타인이 지각으로 인식할 수 없는 방식으로 작성된 기록으로 전자계산기에 의한 정보처리용으로 제공되는 것"을 말한다(형법 제7조의2). 한편 일본 판례는 전자적기록이라는 용어와 함께 데이터라는 용어를 사용하기도 한다.[406]

그리고 기계적으로 작성된 디지털 데이터를 분석하여 얻은 객관적·과학적 증거를 '디지털 증거'라 한다.[407] 다만 디지털 증거 역시 사이버범죄와 마찬가지로 법률상 규정된 개념은 아니다.[408] 컴퓨터나 스마트폰 등을 일상적으로 사용하는 과정에서 개인의 활동은 각종 디지털 디바이스(전자적기록매체)에 끊임없이 기록으로 남게 된다. 이렇게 남은 흔적은 범죄의 수사에 유용하게 활용할 수 있다. 전자메일의 송·수신 이력, 접근 로그, 스마트폰에 기록된 영상 및 사진 등을 분석하면 범죄의 유무죄는 물론 범죄의 수행방법까지 구체적으로 밝혀낼 수 있기 때문이다. 따라서 형사절차에서 디지털 증거의 중요성은 계속하여 증가할 것이다. 디지털 증거는 디지털 데이터를 분석한 것이므로 일반 증거와 다른 특성을 지닌다. 아래에서는 디지털 정보의 특징 중 특히 중요한 내용을 살펴보기로 한다. 먼저 디지털 데이터는 '유체물'이 아닌 '정보' 그 자체이다. 아날로그 방식의 경우 복사본의 신호가 원본의 신호보다 감소하게 되어

---

404) 指宿 信, "サイバー犯罪条約およびその国内法化について", 『刑法雑誌』 45巻1号, 2005, p.118.
405) 警察庁, 『令和5年 警察白書』, 2023, p.104(각주 6).
406) "전자적기록을 보관한 기록매체가 사이버범죄에 관한 조약 체결국에 소재하고…(밑줄은 저자)"(最二小決 令和3年2月1日 刑集第75巻2号123頁), "본건 검증 경과 및 내용을 기재한 검증조서 및 본건 검증 결과 취득한 데이터를 정리한 수사보고서는…(밑줄은 저자)"(東京高裁 平成28年12月7日 高集第69巻2号5頁).
407) 小坂谷 聡·上原 哲太郎, "刑事手続におけるデジタル証拠の改ざん防止措置について", 『分散協調とモバイルシンポジウム』, ルチメディア, 2017, p.680.
408) 디지털 정보에 대한 특성과 증거에 대한 사회적 합의는 시대에 따라 변화될 수 있으므로 디지털 증거에 대한 정의도 변화해야 한다고 밝힌 견해로 탁희성·이상진, 『디지털 증거분석도구에 의한 증거수집절차 및 증거능력확보방안』, 연구총서 06-21, 한국형사정책연구원, 2006.12, 34면 참고.

이론적으로 원본과 복사본의 구분이 가능하지만, 디지털 신호의 경우 신호형태를 복사하는 것이 아닌 신호의 유무만을 검출하여 기록하는 것이므로 정보 값이 같다면 어느 매체에 저장되어 있든 매체와 독립하여 동일한 가치를 지닐 수 있다.[409] 이는 디지털 증거의 진정성의 문제와도 직결될 수 있지만 (법적 근거가 명확하다면) 압수수색과 관련하여서는 침해의 최소성을 위한 집행방법을 취할 수 있음을 의미하기도 한다. 또한 디지털 데이터는 수정·삭제·변경·조작 등이 용이하다. 이를 반대로 이용하면 디지털 데이터를 간단히 이동시켜 변조 및 삭제할 수 있다는 것을 뜻하기도 한다.[410] 디지털 데이터의 이동에는 물리적 거리 제한이 없다.[411] 이로 인해 압수수색의 범위를 특정하기 곤란한 경우가 발생한다. 일반 유체물의 압수·수색은 장소적 개념을 전제로 범위를 설정하는데, 국외 혹은 저장매체 자체가 어느 곳에 존재하는지 조차 파악하기 곤란한 경우도 종종 발생하기 때문이다.

디지털 데이터의 특징 중 중요한 다른 하나는 방대한 정보량이다. 전자기록매체의 물리적 크기와 상관없이 방대한 분량의 디지털 정보를 저장할 수 있으며, 네트워크에 접속하여 클라우드 서버 등을 활용할 경우 더욱 방대한 양의 전자적정보를 저장할 수 있다. 이러한 정보에는 범죄와 관련성이 없는 수많은 정보들이 혼재한다. 따라서 사생활과 영업의 비밀 등을 침해하지 않도록 압수·수색의 범위와 방법을 제한할 필요가 있다. 이 외에도 디지털 정보는 사람의 지각으로 바로 인식할 수 없기 때문에(비가독성) 압수수색의 현장에서 이를 즉시 확인하고 관련성을 확인하기가 쉽지 않다는 점 역시 압수수색과 관련하여 문제가 된다.[412]

---

409) 손지영·김주석, 『디지털 증거의 증거능력 판단에 관한 연구』, 연구총서 2015-08, 사법정책연구원, 2015.6, 26면.

410) 高村 紳, "捜査におけるデジタル情報収集に対する法的規制", 『中央学院大学法学論叢』 36巻1号, 2022, p.95.

411) 高村 紳, 위의 논문, p.95.

412) 디지털 증거 자체로도 검토하여야 할 수많은 문제들이 있다. 다만, 이번 보고서는 디지털 증거의 압수수색 '절차'에 관한 내용이 주제인 만큼 이번 보고서에는 디지털 증거의 개략만을 언급하기로 한다.

2. 일본의 디지털 증거 압수수색 관련 법 규정

가. 디지털 증거 압수수색에 관한 법률의 개정과정 및 최근 논의

1) 유럽 사이버범죄 방지협약 체결 이전

1990년대 중반 정보통신기술의 발전으로 인터넷 보급이 활발해지면서 국경을 넘는 자유로운 정보교환이 가능해졌다. 과거 컴퓨터를 사용한 범죄는 전문 지식을 갖춘 일부 사람들만 할 수 있는 것으로 여겨졌다. 하지만 손쉽게 정보를 검색하거나 교환할 수 있게 되면서 특별한 전문지식이 없더라도 컴퓨터 네트워크를 이용하거나 컴퓨터 네트워크를 향한 범죄를 할 수 있게 된 것이다.[413] 이처럼 인터넷상의 범죄가 일반화되고 보편화되면서 피해 범위와 규모도 급격히 증가하기 시작했다.[414] 인터넷을 활용한 범죄는 컴퓨터 네트워크라는 눈에 보이지 않고 지리적 제한조차 없는 공간 속에서 이루어지기 때문에 기존의 형사절차로는 해결하기 어려운 문제가 나타났다. 인터넷상의 범죄는 거의 대부분의 증거가 전자화되어 정보로 존재한다. 따라서 유체물이 아닌 디지털 정보를 형사소송법상 압수수색 할 수 있는 것인지는 매우 중요한 쟁점이 될 수밖에 없었다. 당시 일본 형사소송법은 압수수색의 대상을 유체물로 한정하고 있었으며 디지털 정보의 압수수색에 관한 별도의 규정을 두고 있지 않았다. 때문에 해당 정보를 압수수색하기 위해서는 임의 협조 등을 통하는 것이 가장 현실적인 방법이었다. 만약 디지털 정보가 반드시 필요한 상황임에도 임의 협조를 구하지 못한 경우 영장을 통한 강제처분을 할 수 있는가에 대해서는 견해가 대립했다.[415] 기존 일본 학설은 (전자적)정보를 포함한 무체물의 압수에 대한 가능성 및 필요성에 대해 소극적인 입장이었다. 민사소송법과 달리 형사소송법은 무형의 권리를 압수할 실익이 비교적 적으며, 압수의 정의가 '특정 목적물을 소유자나 점유자로부터 법원이나 수사기관으로 이전시키는 처분'이라는 점을 고려해 볼 때 (전자적)정보와 같은 무형물을 특정하고 관리하기 어렵다는 것 등이 그 이유였다.[416] 이러한 주장에 대해서는 현대사

413) 指宿 信, "インターネットを使った犯罪と刑事手続", 『法律時報』 69巻7号, 1997, p.10.
414) 指宿 信, "インターネットを使った犯罪と刑事手続", p.10.
415) 당시 일본의 논의 상황에 관해서는 탁희성, "전자증거의 압수·수색에 관한 일고찰", 『형사정책연구』 제15권 제1호, 한국형사정책연구원, 2004.3, 42면 이하를 참고.
416) 劉 芳伶, "「情報の差押」という制度の在り方について (論説) ", 『法律時報』 82巻2号, 2010, p.91.

회의 실정을 고려해 볼 때 형사소송법 내에서도 정보를 독립해서 압수할 실익이 분명히 있으며, 과학기술을 사용한다면 정보를 특정하거나 관리하는 것이 가능하다는 반론이 있었다. 이처럼 사이버범죄의 압수수색에 관한 형사소송법상 규정이 존재하지 않아 실무에서 임의협조 등을 통한 우회적 방법을 사용하고 있는 상황에 대해 '수사의 필요성이 있음에도 해당 규정을 마련하지 않아 수사기관이 기존의 규정을 임의적으로 해석하거나 혹은 협조에 의지하는 태도는 결국 강제처분 법정주의의 본질을 흐리는 것'이라고 비판하기도 했다.[417]

2) 유럽 사이버범죄방지협약 체결 ~ 2011년 형사소송법 개정

가) 유럽 사이버범죄방지협약과 내용

유럽 사이버범죄방지협약(일명 '부다페스트 조약'. 이하에서는 '사이버범죄협약'이라 한다)은 초국가적이고 다양해지는 사이버범죄에 대한 대응을 위해 2001년 유럽평의회 각료 위원회에서 채택된 세계 최초의 국제 협약이다. 현재 G7 국가를 포함한 68개국이 동 협약의 체약국이다. 사이버공간의 특성상 범죄자들은 쉽게 사법관할을 넘나들며 범죄를 저지를 수 있으므로 현실 공간의 사법관할만으로는 실질적 대응을 기대하기 어렵다.[418] 따라서 보다 효과적인 대응을 위해서는 서로 다른 국가 사이에 공통된 법규로 수사를 집행할 필요가 있다. 이를 위해 동 협약은 초안 작성 단계부터 미국, 캐나다, 일본 등 비유럽국가의 전문가도 함께 참여하였다.[419] 작성된 초안은 유럽평의회 범죄문제검토위원회(CDCP)의 세부 수정을 거쳐 2001년 11월 8일 유럽평의회 각료회의에서 채택한 후 2001년 11월 23일 부다페스트에서 개최된 '정보네트워크 범죄에 관한 국제회의'에서 40여 개국이 동 협약에 서명하였다. 사이버범죄협약의 핵심 내용은 크게 세 가지로 정리할 수 있다.[420] 첫째, 사이버범죄에 관하여 국가별로

---

417) 劉 芳伶, 앞의 논문, p.96.

418) 라광현·윤해성, "유럽평의회 사이버범죄방지협약 성과에 대한 실증적 검토", 『범죄수사학연구』 제5권 제1호, 경찰대학 범죄수사연구원, 2019.6, 53면.

419) クリスティアン シュワルツネッガー, 夏井 高大·笠原 毅彦(訳), "サイバー犯罪条約(2001年11月23日)によるコンピュータ犯罪法及びインターネット犯罪法の国際調和ハツキング、違法をデータ入手及び違法な通信傍受を例に", 『判例タイムズ』 1108号, 2003, p.76.

420) 사이버범죄협약에 관한 원문 및 일본어판은 외무성 홈페이지, "サイバー犯罪に関する条約"(https://www.sangiin.https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html; 최종접속일 2023.9.17.)을 참고.

서로 다른 실체법의 국제 조화를 추구한다. 사이버 범죄규정의 조화를 위해 컴퓨터 시스템에 대한 위법한 접근 등 일정 행위를 범죄화하는 것이다. 대상 범죄는 ① 위법접근, 데이터 훼손·변조 디도스 공격 등 시스템 방해 및 바이러스, 해커 툴의 제조, 배포, ② 데이터 위조 및 이를 이용한 사기, ③ 아동포르노, 저작권침해 등 데이터 내용에 관한 범죄, ④ 그리고 이러한 범죄의 미수, 방조, 교사 등이다.[421] 둘째, 컴퓨터 범죄 및 정보네트워크 범죄영역의 수사와 소추를 위해 형사소송법상 절차를 통일하여 전자적 형식으로 기록된 데이터를 용이하고 시의적절하게 확보하고자 한다. 사이버범죄의 수사 및 형사절차에 관한 규정은 ① 데이터의 신속한 보전(제16조), ② 통신기록의 신속한 보전과 부분개시(제17조), ③ 데이터 및 가입자 정보 제출명령(제18조), ④ 데이터 수색 및 압수(제19조), ⑤ 통신기록 리얼타임 수집(제20조), ⑥ 통신내용(자국의 국내법상 중대범죄에 한정)을 제3자가 수신하는 행위(傍受) 등이다. 이러한 형사절차상 권한 및 적용에 대해 유럽인권조약, 유엔 자유권규약이 규정하는 권리를 확보하고 비례원칙을 포함하여 국내법의 조건 및 보장조치를 따르도록 한다.[422] 셋째, 사이버 범죄의 수사를 위하여 범죄인 인도 및 증거제공 등 국제협력을 규정하고 있는데 이는 광의의 국제형사사법공조에 해당한다. 국제협력에 관한 규정은 일반원칙(제23조), 범죄인 인도(제24조), 법 집행에 관한 상호원조의 일반원칙(제25조), 자발적 정보제공(제26조), 상호원조요청(제27조), 상호원조요청의 제한(제28조), 데이터의 신속보전요청(제29조), 보전된 기록의 신속한 개시(제30조), 데이터 접근에 관한 상호요청(제31조), 역외접근 등에 관한 허용(제32조), 통신기록의 리얼타임 수집에 관한 상호원조(제33조), 통신내용 리얼타임 수집에 관한 상호원조(제34조), 주7일 24시간(24/7) 대응체제 확립(제35조), 그 밖에 조약 서명과 관련한 각종 규정(제36조~제48조)이다.

나) 정보처리 고도화에 대처하기 위한 형법 등 일부를 개정하는 법률안

2001년 11월 일본은 비유럽국가인 미국, 캐나다, 호주, 뉴질랜드와 함께 사이버범죄협약서에 공동 서명하였다. 2003년 3월 법무성은 협약내용의 국내법화를 위한 목적으로 법제심의회에 '하이테크 범죄 대처를 위한 형사법 정비에 관한 자문(자문 63호)'

421) 寺林 裕介, "サイバー犯罪条約第２追加議定書の概要: 国境を越えるサイバー犯罪捜査のための国際協力", 『立法と調査』, 2023, p.15.
422) 寺林 裕介, 위의 논문, p.15.

을 발신했고[423] 2003년 9월 동 심의회는 '하이테크 범죄 대처를 위한 형사법 정비에 관한 요강(골자)'을 답신했다.[424]

답신의 주요 내용은 (1) 부정지령전자적기록등 작성 등의 죄 신설(형법 제168조의2 신설), (2) 음란물을 데이터화한 경우 이를 처벌하는 규정의 도입(형법 제175조) 개정, (3) 전자적기록에 관한 기록매체의 압수 집행방법, (4) 기록명령부 압수, (5) 전자계산기에 전기통신회선으로 접속한 기록매체에서 복사, (6) 전자적기록에 관한 기록매체의 압수영장을 집행 받는 자에게 협력 요청, (7) 보전요청 등(90일), (8) 부정하게 만들어진 전자적기록 등의 몰수로 이루어진 것이었다. 2005년, 답신을 기초로 협약의 국내법화와 관련한 법안을 묶은 개정안인 '범죄의 국제화와 조직화 및 정보처리의 고도화에 대처하기 위한 형법 등의 일부를 개정하는 법률안'[425]이 제159회 국회에 상정되었다. 사이버범죄에 관한 형사절차를 개정하는 최초의 개정안이었다. 개정안 중 형사소송법상의 내용을 정리하면 다음과 같다. (1) 수사기관이 직접 데이터를 압수, (2) 보관자에게 데이터를 압수해 둘 것을 명령, (3) 대상 컴퓨터 시스템 이외의 시스템에 대한 압수수색, (4) 관리자에 협력요청, (5) ISP에 대한 통신이력 보전요청, (6) 음란 영상이나 바이러스 등 위법 데이터의 몰수이다.[426][427]

개정안은 발의된 이후 약 5년 동안 계속 심의가 이루어졌으나 심의미료(審議未了)로 성립하지 못하였고 정권 교체 이후에는 법안의 상정조차 이루어지지 않았다.[428] 개정안이 오랜 시간 성립하지 못한 배경에는 개정안에 담긴 '국제적 조직범죄 방지를 위한 공모죄 도입'이 있었다.[429][430] 2011년 4월 의견의 대립이 격렬한 조직범죄의

---

423) 자문의 구체적 내용과 설명에 대해서는 指宿 信, "変わる捜査の対象:モノからデータへ—サイバー刑事法制の諮問を契機として—", 『法律時報』 75巻7号, 2003, p.1-3 참고.

424) 법무성 홈페이지, "答申(ハイテク犯罪に対処するための刑事法の整備に関する要綱(骨子))", 2003. 9.10(https://www.moj.go.jp/shingi1/shingi_030910-5-1.html; 최종접속일 2023.9.17.).

425) 참의원 홈페이지, "犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案"(https://www.sangiin.go.jp/japanese/joho1/kousei/gian/160/meisai/m16003159046.htm; 최종접속일 2023.9.17.)

426) 법무성, "サイバー関係の法整備の概要"(https://www.moj.go.jp/content/001267492.pdf; 최종접속일 2023.9.17.)

427) 당시 개정안에 대해서 "절차규정은 개정안의 조문만으로는 구체적인 내용이 불분명한 경우가 많으므로 수사방법을 규정하고 공정성과 적정성을 담보하기 위하여 '전자적 범죄 수사규범'등과 같은 가이드라인을 만드는 것이 바람직하다"고 평가한 견해로는 指宿 信, "サイバー犯罪条約およびその国内法化について", 『刑法雑誌』 45巻1号, 2005, p.129를 참고.

428) 指宿 信, "サイバースペースにおける証拠収集とデジタル証拠の確保 : 2011年改正法案を考える", p.84.

429) 高村 紳, 앞의 논문, p.96.

공모죄에 관한 규정을 덜어내고 사이버범죄협약과 관련된 법 정비 및 강제집행방해죄의 벌칙 정비 등만을 남긴 '정보처리 고도화에 대처하기 위한 형법 등 일부를 개정하는 법률안'[431]이 제177회 국회에 제출되었다. 동 법률안은 2011년 6월 17일 가결·성립되었고, 같은 달 24일 공포되었다. 동 개정으로 형사소송법과 관련하여 다음 6개의 항목이 개정 및 신설되었다. (1) 전자적기록매체의 압수 집행방법과 기록명령부압수제도의 신설(제99조 제2항 외), (2) 원격접근제도의 도입(제99조의2 외), (3) 집행을 명령받은 자에게 전자계산기 등의 조작이나 그 밖에 필요한 협력을 구하는 '협력요청'(제111조의2), (4) 통신사업자에게 수사대상자의 통신기록이 사라지지 않도록 60일간 동결할 것을 요청하는 보전요청(제197조 제3항), (5) 비밀유지요청(제197조 제5항), (6) 부정하게 작성된 전자적기록 등의 몰수 규정 신설(제498조의2)이 그것이다.[432]

2011년 개정안 중에서는 2005년의 개정안 내용의 일부를 수정 보완한 규정도 있었다. 개정 법안 중 형사소송법과 관련된 수정사항을 발췌 정리하면 〈표 3-1〉과 같다.

2005년 제출법안에서는 ISP에 대한 보전요청의 보전기간을 최대 90일까지로 규정하고 있었다. 미연방법 제18편 제2703조(f)에 규정된 '정부기관에 의한 90일간의 보존(preserve) 요청' 및 사이버범죄협약 제16조의 90일 규정과도 동일한 기간이었다.[433]

하지만 2011년 개정안에서는 사업자의 부담 등을 이유로 기존의 90일이었던 보전기간을 60일로 단축했다. 당시 경제계에서는 의견서를 통해 "한 번의 보전요청으로 대응 할 수 있는 용량에는 한계가 있음을 고려해야 한다"고 하며 대형 ISP의 업무부담과 시스템 부하에 관한 불안을 우려하였다.[434] 이에 대해 "대용량 기억장치가 빠르게 개발되고 있는 지금 상황에서 ISP의 부담이란 결국 조달비용을 말하는 것일 뿐 고도의 기술적 부담은 아니다. 이는 각 유저에게 스토리지 요금을 부과하면 해결할 수 있는

---

430) 사이버범죄협약에 서명한 2001년 이후 좀처럼 개정작업이 이루어지지 않자 일본 내에서도 이전부터 공모죄에 관한 부분을 제외하고 컴퓨터 바이러스 작성죄 등을 먼저 제정하자는 주장이 나타났다. 다만 이러한 주장이 받아들여지지 않은 것에 대해 '당시에는 사이버범죄가 지금 보다 자주 등장하는 개념이 아니었으며, 관료들이 사이버범죄의 중대성과 심각성에 대하여 공감하지 못했다'고 분석하는 견해도 있다(須川 賢洋, "「情報処理の高度化等に対処するための刑法等の一部改正」に関する一考察", 『情報処理学会研究報告』, 2012, p.2).

431) 법무성, 情報処理の高度化等に対処するための刑法等の一部を改正する法律安(https://www.moj.go.jp/content/001267495.pdf; 최종접속일 2023.9.17.).

432) 각 조문에 대한 상세한 설명은 指宿 信, "サイバースペースにおける証拠収集とデジタル証拠の確保 : 2011年改正法案を考える", p.86. 이하를 참고.

433) 指宿 信, "サイバースペースにおける証拠収集とデジタル証拠の確保 : 2011年改正法案を考える", p.90.

434) 指宿 信, "サイバースペースにおける証拠収集とデジタル証拠の確保 : 2011年改正法案を考える", p.91.

문제"라고 하며 ISP의 부담을 고려하여 보전기간을 단축한 2011년의 개정안을 비판하는 견해도 있다.[435]

[표 3-1] 2011년 제출 개정법률안 중 형사소송법 관련 수정사항

구분	2005년 제출법안	주요 의견	2011년 제출법안
원격 접근 (제218조 제2항)	압수 할 물건이 전자계산기인 때에는 해당 전자계산기에 전기통신회선으로 접속하고 있는 기록매체로, 해당 전자계산기에서 처리하여야 할 전자적기록을 보관하기 위해 사용되는 것으로 인정할 만한 상황에 있는 것으로 부터 전자적기록을 해당 전자계산기 등에 복사한 후 해당 전자계산기 등을 압수할 수 있다.	복사 대상이 되는 기록매체의 범위가 지나치게 확장될 우려가 있다. 예컨대 압수대상물인 전자계산기 사용자가 단순히 열람할 수만 있는 전자기록을 보관한 기록매체도 압수대상에 포함될 수 있다.	대상 기록매체를 "해당 전자계산기에서 작성 또는 변경한 전자기록 또는 해당 전자계산기에서 변경 혹은 삭제 및 제거 할 수 있게 되어 있는 전자적 기록을 보관하기 위해 사용 하는 것으로 인정할 만한 상황에 있는 것"으로 함 ※ 단지 열람만 할 수 있는 전자기록에 관한 기록매체를 포함시키지 않음.
보전 요청	전자통신을 하기 위한 설비를 타인의 통신을 위해 제공하는 사업을 하는 자(ISP)등에게 업무상 기록하고 있는 통신이력 전자적 기록 중 필요한 것을 특정하여 90일을 넘지 않는 기간을 정하여 이를 삭제하지 않도록 요구할 수 있다.	필요한 요건을 규정하지 않았음. 수사기관에 의한 남용의 우려	•보전요청의 주체를 '검찰관, 검찰사무관 또는 사법경찰관'으로 한정(사법순사를 제외) •'압수 또는 기록명령부압수를 하기 위해 필요한 때'라는 요건을 추가
		보전기간 상한이 90일인 것은 프로바이더에게 과도한 부담임	•보전요청 기간은 '원칙상 30일 이내로 하고 특별히 필요한 때에는 30일 이내로 연장할 수 있도록 함'(최장 60일 이내)
		구두요청을 허용하면 수사기관이 이를 남용할 우려가 있음	•보전요청은 '서면'으로

* 출처 : 법무성, "情報処理の高度化等に対処するための刑法等の一部を改正する法律案における修正点について"의 내용 중 일부 발췌(https://www.moj.go.jp/content/001267491.pdf; 최종접속일 2023.9.17.).

3) 전자데이터 증거수집에 관한 최근의 논의: 전자적기록명령 도입에 관한 검토

정보통신기술의 지속적인 발달과 함께 이제는 종이(서면)가 담당하고 있던 많은 역할이 전자데이터로 옮겨졌다. 한편 행정절차와 민사재판은 IT 기술 활용을 위한 법제도 정비가 꾸준히 검토되었다. 또한 코로나19를 거치며 일본 사회도 전 분야에서 비대면화, 비서면화가 확대되기 시작했다. 2020년 7월 17일 각의 결정한 '세계 최선단

435) 須川 賢洋, 앞의 논문, p.5.

디지털 국가 창조선언·관민 데이터활용추진기본계획', '성장전략 팔로업'에서도 "형사절차에 디지털화를 실시하는 것은 수사절차에 관여하는 국민의 부담 경감으로 이어질 수 있으며 감염증이나 감염 확대 시에도 원만하고 신속한 공판절차를 가능하게 한다는 관점에서 유용하다고 생각되며, 디지털화를 초기에 실현하는 것은 관계자 권리이익을 보호하는 데 기여한다. 따라서 형사절차에서 가능한 분야를 효율화, 비대면화, 원격화 하는 것을 목표로 2020년도 중에 사법부의 자율적 판단을 존중하면서 정부에서 영장청구와 발부를 시작으로 하는 서류의 온라인 교부, 형사 서류의 데이터화, 온라인을 활용한 공판 등 수사와 공판의 디지털화 방책의 검토를 시작한다"고 하였다. 이에 일본 법무성 법제심의회 형사법부회는 '형사절차에서 정보통신기술 활용에 관한 검토회(이하, '검토회'라고 한다)'를 설치하고 형사절차에서 정보통신기술 활용방책에 관한 법적 문제를 검토하기 시작했다.[436] 2021년 3월 첫 번째 회의를 시작으로 2022년 3월까지 11차례의 회의를 거쳐 최종보고서를 발표하였는데 검토된 사항 중에는 '전자데이터의 증거수집'에 관한 내용이 포함되어 있었다.[437]

전자데이터의 증거수집에 관한 주된 검토사항은 법원이 필요하다고 인정하는 때 전자데이터를 보관하는 자에게 필요한 전자데이터를 온라인으로 제공할 것을 명할 수 있도록 할 수 있는가(전자적기록제공명령)와, 수사기관이 범죄수사를 위해 필요하다고 인정하는 때에 재판관이 발부한 영장으로 전자데이터를 보관하는 자에게 필요한 전자데이터를 온라인으로 제공할 수 있도록 할 수 있는가에 관한 것이다.[438] 현행 일본 형사소송법은 전자적기록 보관자의 협력을 구할 수 있는 강제처분으로써 '기록명령부압수'를 규정하고 있다(제99조의2, 제218조). 기록명령부압수 규정은 보관자에게 명령하여 필요한 전자적기록을 기록매체에 기록하게 하여 해당 기록매체를 압수하는 것이기 때문에 '수사기관이 해당 기록매체가 있는 장소로 가서 점유를 취득'하는 형태로 압수한다.[439] 검토회 보고서에는 기존의 이러한 압수 방식에서 '해당사업자가

436) 동 검토회의 회의기록은 법무성 홈페이지에서 확인할 수 있다. 법무성 홈페이지, "刑事手続における情報通信技術の活用に関する検討会"(https://www.moj.go.jp/keiji1/keiji07_00011.html; 최종접속일 2023.9.17.).

437) 관련 형사소송법 조문(제99조, 제106조~제109조, 제197조, 제218조).

438) 刑事手続における情報通信技術の活用に関する検討会, 『「刑事手続における情報通信技術の活用に関する検討会」取りまとめ報告書』, 2022.3, p.13.

439) 刑事手続における情報通信技術の活用に関する検討会, 앞의 보고서, p.13.

보관하는 전자적기록을 수사기관이 관리하는 전자계산기에 온라인으로 송신'하는 방법을 통한 압수를 검토한다. 이러한 압수방식을 통해 수사기관은 이동의 부담을 줄일 수 있고, 전자기록 보관자의 입장에서는 수사기관이 직접 압수를 집행하러 올 경우에 대한 대응과 전해줄 기록매체를 준비하는 부담을 덜 수 있다고 한다.[440] '기록명령부압수'를 근간으로 삼으면서도 압수의 대상물이 '기록매체'가 아니라는 점에서 '전자적기록제공명령'이라는 용어를 사용한다. '전자적기록명령'은 '기록명령부압수'에서 '압수'라는 수사관의 직접강제가 사라진 것이다. 하지만, '제공명령'이 내려진 것이므로 피처분자에게 제공에 관한 의무는 여전히 존재한다. 다만, 수사관의 압수라는 직접강제가 사라지면 결국 현실적으로 사업자의 협조에 의존할 수밖에 없어 실효성 확보에 관한 문제가 발생할 수 있다. 검토보고서에서도 이러한 문제를 지적하며 '영장에 근거한 처분으로써의 실효성을 확보하기 위한 방책으로 규제를 통한 간접강제의 마련' 등을 검토할 필요가 있다고 한다.[441]

4) 협력 및 전자적 증거 개시 강화에 관한 사이버범죄방지협약 제2 추가의정서

2000년대 초반에 마련된 사이버범죄협약은 체약국에 압수수색에 관한 절차 정비를 요구하는 것이었다. 다만, 협약이 마련된 시기만 해도 대다수 형사사건의 증거는 여전히 수사를 진행하는 국가 내부에 존재하였기에 형사사법공조의 필요성은 크게 부각되지 않았다.[442] 협약체결 당시와 비교하여 인터넷의 이용량이 증가하면서 사이버 공간에서 이루어지는 범죄는 악질화되고 수법도 복잡해졌다. 이러한 문제의식하에 2017년부터 유럽평의회는 국경을 넘는 사이버범죄에 대응하기 위해 협약 체결국 사이에 보다 원활하고 신속하게 디지털 증거 수집이 가능하게 함을 목적으로 사이버범죄협약의 추가 의정서 작성 교섭을 시작하였다. 2021년 11월 17일 유럽평의회 각료위원회에서 '협력 및 전자적 증거 개시 강화에 관한 사이버범죄방지협약 제2 추가의정서(Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, 이하 "추가의정서"라고 한다)'[443]가 채택되었

---

440) 刑事手続における情報通信技術の活用に関する検討会, 위의 보고서, p.13.
441) 刑事手続における情報通信技術の活用に関する検討会, 위의 보고서, p.14.
442) 박재성, 앞의 논문, 252면.
443) 의정서의 영문 전문은 외무성 홈페이지(https://www.mofa.go.jp/mofaj/files/100342970.pdf; 최종접속일 2023.9.17.)에서 확인할 수 있음.

다. 추가의정서는 범죄의 증거가 되는 전자적기록이 여러 국가의 서버에 존재하거나 알 수 없는 관할지에 존재하는 경우가 점점 증가하는 상황을 바탕으로 이러한 전자적증거를 효율적으로 수집하기 위해 각 국가 간 협력을 강화함과 동시에 국가와 민간부문(ISP 등)의 직접적 협력절차에 관한 내용을 규정한다.[444] 일본은 2022년 5월 12일 개최된 서명식에서 21개국 대표와 함께 추가의정서에 서명하였다.[445]

추가의정서안은 크게 4장으로 구성되어있으며 총 25개 조항으로 이루어져 있다. 제1장에는 정의규정 등 일반규정을 담고 있으며 제2장은 수사공조와 관련된 규정, 제3장은 개인정보보호에 관한 규정, 제4장은 그 외의 가입절차 등에 관한 규정을 각각 담고 있다.[446] 이 중 전자적증거의 압수와 관련된 내용으로는 (1) 다른 협약국의 인터넷 서비스제공자나 단체를 상대로 직접 협력을 요청할 수 있는 절차정비(제2장 제2절), (2) 저장된 컴퓨터데이터를 개시하기 위해 가입국가 간 국제협력을 강화하는 내용의 규정(제2장 제3절) 등이 있다.[447]

가) 도메인 등록정보 개시

추가의정서 제6조는 다른 체약국의 영역에 소재하는 도메인 등록서비스를 제공하는 단체(등록사업자)에게 도메인 명의 등록자를 특정하거나 연락할 수 있는 정보를 직접 요청할 수 있는 권한과 절차를 규정하고 있다. 도메인을 악용하는 사이버범죄 등을 수사하기 위해서는 도메인 등록정보가 필요하다. 지금까지는 Whois에 등록된 도메인을 활용하였으나, 유럽 일반 개인정보 보호법(GDPR)을 비롯해 각국의 개인정보 취급방침이 엄격해지면서 도메인 등록정보가 비공개되는 경우가 늘어났다.[448] 다른 나라의 수사기관으로부터 도메인 등록정보의 개시를 요청받은 경우 도메인 등록사업자는 자신의 국내법에서 정하는 합리적 조건에 따르면 되는 것으로(제6조 제2항) 반드시 이를 제공하여야 하는 것은 아니다.

---

444) 寺林 裕介, 앞의 논문, p.17.
445) 외무성 보도자료, "「協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書」への署名", 2022年5月12日(https://www.mofa.go.jp/mofaj/press/release/press3_000814.html; 최종접속일 2023.9.17.).
446) 해당 추가의정서에 관한 자세한 내용은 박재성, 앞의 논문, 250면 이하를 참고.
447) 이에 관한 자세한 내용은 中村 真利子, "サイバー犯罪条約の第二追議定書によるサイバー犯罪捜査の変化",『성균관법학』제35권 제1호, 성균관대학교 법학연구원, 2023.3, 523-529면 참고.
448) 寺林 裕介, 앞의 논문, p.17.

일본의 경우 외국에 있는 제3자에게 개인의 데이터정보를 제공하는 경우 「개인정보의 보호에 관한 법률」 제28조 제1항에 따라 사전에 본인의 동의를 받아야 한다.[449] 따라서 외국에 있는 제3자에게 개인의 데이터 정보를 제공할 경우에는 사전에 본인의 동의를 받아야 한다. 다만, 법령에 근거하는 경우 사전에 본인의 동의를 받는 것에 대한 예외를 인정하는데(제27조 제1항 제1호)[450] 이때 법령은 외국의 법령을 의미하는 것은 아니다.

나) ISP가 보유하고 있는 정보 개시

사이버범죄의 수사과정에서 다른 나라의 ISP가 보유하고 있는 전자적기록의 압수수색이 필요한 경우는 일반적으로 발생하고 있으며, 증거를 취득하기 위해 필요한 절차이기도 하다. 추가의정서 제7조는 다른 체약국에 있는 ISP가 보유하고 관리하는 가입자 정보를 취득하기 위해 각 체약국 수사담당기관이 ISP에게 직접 정보 개시를 명할 수 있는 권한과 절차를 규정한다. 또한 자국의 ISP가 이러한 가입자 정보를 다른 나라의 수사기관에 개시할 수 있도록 필요한 입법조치 및 그 밖의 조치를 취할 것을 함께 규정한다. 그러면서도 추가의정서 제19조는 ISP가 보유한 정보 개시 규정을 유보할 수 있음을 밝히고 있다. 앞서 살펴본 바와 같이 일본은 외국에 있는 제3자에게 개인정보 데이터를 제공할 경우 사전에 본인의 동의를 받도록 하고 있으며(「개인정보의 보호에 관한 법률」 제28조 제1항), 전기통신사업자가 취급 중인 통신의 비밀을 침해해서는 안된다고 규정하고 있으므로(「전기통신사업법」 제4조 제1항) 현행법과의 정합성을 고려할 때 추가의정서 제7조는 유보할 것으로 보여진다.[451]

---

449) 제28조(외국에 있는 제3자에게 제공의 제한) ① 개인정보취급사업자는 외국(본국 역외에 있는 국가 또는 지역을 말함. 이하 본 조 및 제31조 제1항 제2호에서도 같음)(개인의 권리이익 보호에 관하여 일본과 동등한 수준의 개인정보보호제도를 가진 외국으로 개인정보보호위원회 규정에서 정하는 경우는 제외함. 이하 동조 및 동호에서도 같음)에 있는 제3자(개인데이터 취급에 관하여 이 절의 규정에 의한 개인정보 취급사업자가 취하여야 할 조치(제3항에서 '해당 조치'라 한다)를 지속적으로 마련하기 위해 필요한 것으로 개인정보보호위원회 규정으로 정하는 기준에 적합한 체제를 정비하고 있는 자를 제외함. 이하 동항 및 다음 항, 그리고 동호에서도 같음)에게 개인데이터를 제공하는 경우 전조 제1항 각호에 열거한 경우를 제외하고, 사전에 외국에 있는 제3자에게 제공을 허락한다는 본인의 동의를 얻어야 한다. 이 경우 동 조의 규정을 적용하지 않는다. ②~③ 〈생략〉

450) 제27조(제3자 제공제한) 개인정보 취급사업자는 다음의 경우를 제외하고, 사전에 본인의 동의를 구하지 않고 개인데이터를 제3자에게 제공해서는 아니된다.
1. 법령에 근거하는 경우 〈이하 생략〉

451) 寺林 裕介, 앞의 논문, p.19.

다) 데이터의 신속한 개시를 위한 국제협력 강화

추가의정서 제8조는 가입자 정보 및 통신기록의 신속한 제출을 위한 다른 체약국의 명령집행을 규정한다. 구체적으로는 다른 체약국에 대한 요청의 일부로 요청을 받은 체약국 영역 내 ISP가 보유 또는 관리하는 가입자 정보 및 통신기록을 제출할 수 있도록 강제할 권한을 당사국에게 부여할 수 있도록 필요한 입법조치를 취하도록 한다(제8조 제1항). 이처럼 대체집행의 형식을 보이기 때문에 추가의정서 제7조의 정보 개시를 거부한 ISP에게도 정보 개시를 기대할 수 있다고 보기도 한다.[452]

또한 추가의정서에는 자연인의 생명 또는 안전에 중대하고 긴박한 위험이 있는 상태를 '긴급상태'로 규정하고(제3조 제2항c) 긴급사태에 대한 상호원조를 규정한다(제9조). 다른 체약국의 ISP로부터 데이터를 신속하게 제공받을 수 있도록 자국의 연락부국이 다른 체약국의 연락부국에 즉시 원조를 요청할 수 있도록 필요한 입법과 조치를 마련하도록 한다. 요청할 수 있는 정보는 '컴퓨터데이터'로 되어 있어 단순한 가입정보 이외의 폭 넓은 전자적정보를 요청할 수 있다고 볼 수 있다.[453] 또한 체약국 간 상호원조에 관하여는 특히 신속한 상호원조를 요청할 수 있다고 규정한다(제10조).

5) 소결

일본 형사소송법은 '증거물 또는 몰수할 물건으로 사료되는 것'을 압수할 수 있다고 규정하고 있어 유체물만을 그 대상으로 삼고 있었다. 채권, 전기, 에너지 등의 무체물이 압수의 대상이 될 수 없는 것과 마찬가지로 디지털 데이터 역시 검색하거나 컴퓨터 장치나 기억장치에서 특정 데이터를 취득하는 강제처분을 할 수 없다는 것이 일반적인 생각이었다. 따라서 디지털 증거가 필요한 경우 전자적기록이 보존된 유체물(플로피디스크, CD-R 등) 자체를 압수하는 방법을 채용해 왔다. 실무에서는 당사자의 협조를 얻어 이를 해결하는 방법을 취하기도 했지만 이는 근본적 해결책이 될 수 없었다. 전자적기록을 보존하는 기록매체의 발전으로 압수대상 전자적기록이 사건과 무관한 제3자의 전자적기록과 혼재되는 경우가 늘어났고, 기록매체의 종류도 다양해지면서 기존의 압수수색 규정으로 대응하기 곤란한 상황에 이르게 되었다.

---

452) 中村 真利子, 앞의 논문, 527면.
453) 中村 真利子, 위의 논문, 528면.

컴퓨터 시스템을 공격하는 범죄 및 컴퓨터 시스템을 이용하여 이루어지는 사이버범죄에 대한 실효성 있는 대응에 관한 논의는 세계적으로 중요한 주제였고 2001년 11월 8일 사이버범죄에 대처하기 위한 법적 구속력이 있는 국제문서가 유럽평의회 각료위원회 회의에서 정식 채택되었다(사이버범죄협약). 일본은 2003년 3월 24일 미국, 캐나다, 호주, 뉴질랜드 등과 함께 사이버범죄협약에 공동 서명하였다. 2004년 4월 동 협약 체결에 관한 국회의 승인을 얻었으며, 협약 체결을 위한 국내법의 정비작업이 시작되었다. 2005년 '범죄의 국제화와 조직화 및 정보처리의 고도화에 대처하기 위한 형법 등의 일부를 개정하는 법률안'이 국회에 제출되었으나 의견 대립이 격렬했던 '조직범죄의 공모죄' 등이 개정 법률안에 포함되어 있었다는 이유 등으로 법률안 성립에 난항을 겪고 있었다. 2011년 논란의 대상이었던 조직범죄의 공모죄에 관한 내용을 덜어내고 종전의 개정안에 부정지령전자적기록에 관한 죄를 추가, 원격접속에 관한 규정, 보전요청을 수정한 내용을 담은 '정보처리 고도화에 대처하기 위한 형법 등 일부를 개정하는 법률안'을 제출하였고, 같은 해 5월 동 개정안이 성립하였다. 하지만 새로 도입된 여러 규정들에서도 압수의 대상은 '유체물'인 기록매체이다. 압수수색과 같은 강제처분은 본래 구체적 물건을 대상으로 삼는다. 그리고 2011년 형사소송법 개정은 기존의 압수수색 규정을 확장한 형태이기 때문에 결국 유체물에 대한 압수수색을 전제로 할 수밖에 없다.[454] 하지만 전자적기록의 수집 자체에 집중하면 반드시 기록매체를 압수하지 않아도 가능하다.[455] 2022년 법무성 법제심의회 형사법부회 '형사절차에 정보통신기술 활용에 관한 검토회'의 최종보고서에 담겨진 '전자적기록제공명령'이 '기록매체의 압수 없는 전자기록의 수집'의 한 유형으로 볼 수 있을 것이다. 향후 동 제도가 어떻게 정착되고 시행될 것인지 꾸준히 지켜보아야 할 것이다.

2022년 5월 일본은 국경을 초월한 사이버범죄의 규제를 한층 강화하는 내용을 담은 사이버죄방지조약 제2 추가의정서에 서명했다. 동 의정서는 사이버범죄 수사 또는 형사소송법뿐만 아니라 일반 범죄에 관한 데이터(전자적 형태)의 증거 수집에도 적용된다(제2조1a). 추가의정서 체약국가는 조약과 마찬가지로 국내법 정비의무가 부과되므로(제13조) 향후 해당 의정서에 따른 일본 국내법 정비에 주목할 필요가 있다.[456]

---

454) 高村 紳, 앞의 논문, p.97.
455) 高村 紳, 위의 논문, p.97.
456) 中村 真利子, 앞의 논문, 523면.

이처럼 일본은 디지털 증거에도 일반 압수수색 규정을 적용하다가 2011년 형사소송법 개정을 통해 관련 규정을 정비하고 이를 활용하고 있다. 이에 대하여 지금까지 디지털 증거의 수사에 관한 법적 규제는 '디지털 증거 취득 및 수집'을 위주로 정비되어 온 것이라 평가하면서 취득 후의 이용과 취급에 관한 법적 규제가 미흡하다는 지적이 있다.[457] 정보기술의 발달로 수사기관이 많은 전자적정보를 수집하기가 쉬워졌고, 빅데이터의 이용과 분석으로 파악할 수 있는 개인정보의 범위가 늘어나면서 정보가 지니는 가치가 높아졌다는 점을 고려해 보았을 때 수사기관이 취득한 정보에 대한 적절한 규제가 필요하다는 것이다.[458]

나. 현행 형사소송법상 디지털 증거의 압수수색에 관한 규정

1) 전자적기록매체에 대한 대체집행(제110조의2 및 제222조 제1항에 의한 준용)

기존 일본 형사소송법에서 압수수색의 대상은 유체물에 한하는 것이었다. 따라서 컴퓨터, 스마트폰, 외장하드와 같은 유체물은 기존의 압수수색 방법에 따라 이를 압수수색 할 수 있었다. 하지만 무형물인 전자기록(데이터)은 일반 압수수색 규정으로 압수수색하는 것이 곤란하기 때문에 이를 압수수색하기 위해서는 전자기록이 보존된 기록매체 자체를 압수하는 방법이나 검증을 활용할 수밖에 없었다. 실무에서는 검증보다는 전자적기록매체를 압수하는 방법이 보다 일반적으로 활용되었다.[459] 하지만 압수하려는 전자적기록이 제3자가 소유하고 보관하는 전자적기록매체에 저장되어 있는 경우이거나 혹은 압수 대상 전자적기록이 다른 계약자들의 데이터와 섞여 혼재하는 경우, 수사기관이 전자적기록매체를 압수하는 행위가 프라이버시 침해 및 ISP의 업무방해가 될 수 있다. 실제로 피의자가 이용한 ISP를 수색하는 과정에서 ISP가 소유한 고객데이터를 대량(428명)으로 압수한 사건에 대하여 압수의 필요성이 인정되지 않는다는 이유로 데이터의 압수처분을 취소하는 1998년 판례도 있다.[460] 방대한 전자적기록 중 일부의 전자적기록만 취득하면 증거수집의 목적을 달성할 수 있는 경우

457) 高村 紳, 위의 논문, p.98.
458) 高村 紳, 위의 논문, p.99.
459) 千葉 陽一, "インターネットのプロバイダが管理するホームページへの被疑者の一定期間のアクセスログを差押対象とする捜索差押許可状及びプロバイダの任意提出を前提にした差押許可状の発付の可否と留意点", 『別冊判例タイムズ』 35号, 2012, p.157.
460) 平城10年2月27日 東京地決1637号152頁.

과거에는 형사소송법 제111조의 '필요한 처분'으로 압수한 후 인쇄나 복사를 하고 기록매체를 신속히 돌려주는 방법 등을 사용했다. 다만, 이러한 방법을 통한 영장 집행은 적법성의 면에서 안정적이지 못하다는 지적이 있었다.[461]

2011년 형사소송법 개정으로 '전자적기록매체를 압수대상으로 하는 때에는 전자적 기록을 다른 매체에 복사, 인쇄 또는 이전한 후 해당 매체를 압수'할 수 있는 규정이 신설되었다(제110조의2). 이때 전자적기록매체를 복사, 인쇄 또는 이전하는 작업은 압수를 하는 수사기관이 할 수도(제110조의2 제1호), 압수를 받는 피처분자(제110조의2 제2호)가 할 수도 있다. 다만 전자기록에 관한 압수라 하더라도 기록매체 자체에 증거가치가 있는 경우(데이터의 삭제 흔적을 분석하여야 하는 경우 등)가 존재하므로 전자기록에 관한 압수에 전자적기록매체에 대한 대체집행이 원칙적으로 적용되어야 하는 것은 아니다.[462] 형사소송법 제110조의2의 대체집행은 영장을 집행하는 과정에서 현장 수사관의 판단에 따라 실시한다. 따라서 통상의 압수수색영장에 따르면 충분하기 때문에 정보를 인쇄한 종이 등 '다른 기록매체'를 다시 압수대상물로 압수영장에 기재하지 않아도 된다.[463] 전자적기록을 다른 매체에 옮기는 방법(복사, 인쇄, 이전) 역시 수사관의 재량에 따른다. 또한 형사소송법 제222조 제1항 규정이 준용되므로 체포현장에서 이루어지는 영장 없는 압수수색처분(제220조 제1항)에도 전자적기록매체에 대한 대체집행을 할 수 있다.

2) 기록명령부압수(제99조의2, 제218조 제1항)

기록명령부압수는 수사기관이 전자적기록매체에서 전자적기록을 다른 매체에 옮긴 후 이를 압수하는(제110조의2) 경우와 달리, 수사기관이 전자적기록을 보관하는 사람 혹은 이용 권한을 가진 자에게 특정한 전자적기록을 수사기관이 지시한 기록매체에 옮기도록 '명령'하여 이를 취득(압수)하는 것이다. 이 제도는 2011년 형사소송법 개정을 통해 도입되었다.[464] 기록명령부압수제도는 사이버범죄협약 제18조 '제출명

461) 柴田 和也, "情報機器に関する令状実務について(覚書)", 『判例タイムズ』 1459号6月号, 2019, p.12.
462) 千葉 陽一, 앞의 논문, p.157.
463) 南部 晋太郎, "電磁的記録媒体に対する捜索差押" 『別冊判例タイムズ』 35号, 2012, p.149.
464) 이 제도의 도입 전에는 수사기관이 필요한 정보를 종이에 인쇄 또는 CD 등에 기록하게 하여 압수하는 방법에 대하여 '영장 발부 시점에 존재하지 않았던 물건(종이나 CD 등)을 대상으로 할 수 있는가'에 관한 논의가 있었다(南部 晋太郎, 앞의 논문, p.149).

령'을 국내법화 한 규정으로 보여지나, 전자적기록의 특성을 고려한 강제규정의 신설 필요성은 이미 오래전부터 논의되어 온 것이기도 했다.[465] 기록명령부압수를 활용하면 수사기관이 압수한 기록매체에는 피의사실과 관련된 전자적기록만 저장되어 있어, 피의사실과 무관한 제3자의 프라이버시를 침해할 위험을 회피할 수 있고, ISP의 업무 방해에 관한 위험도 피할 수 있다.[466]

기록명령부압수는 통상 압수수색영장이 아닌 기록명령부압수영장으로 한다. 해당 영장에는 기록매체, 기록매체가 보관된 장소 등을 기재할 필요가 없으므로 기록매체를 보관한 장소가 많거나 불명확한 경우에도 활용할 수 있다.[467] 기록명령부압수영장에 기재할 사안은 '기록하게 하거나 인쇄하게 할 전자적기록' 및 '기록하게 하거나 인쇄하게 할 사람'이다(제219조 제1항). 이때 방대한 규모의 전자적기록 중 무엇을 기록하게 할 것인가를 특정할 필요가 있는데, 구체적 기재방법은 개별 사안에 따라 달라질 수 있다.[468] 기록명령부압수는 기록과 인쇄를 명령할 수 있으므로 전자적기록의 이전이[469] 필요한 경우라면 다른 규정 적용을 검토해야 한다.[470] 기록명령부압수는 명령을 통해 전자적기록을 제출받는 것이기 때문에 관리자의 협조를 확보하는 것이 무엇보다 중요하다. 따라서 형사소송법에 전자적기록을 보관하는 사람 혹은 이용 권한을 가진 자가 수사기관의 기록명령에 불응할 경우 이를 처벌할 수 있는 별도의 규정이 없어 간접강제로 실효성을 확보하기 어렵다는 지적도 있다.[471] 하지만, 기록명령부압수를 사용하지 않더라도 수사기관은 전자적기록매체를 압수할 수 있으며, 전자적기록을 보관하는 자는 수사기관의 이러한 직접적 압수과정에서 발생할 수 있는 피해 등을 고려해 결국 대부분 수사기관의 명령에 응한다는 현실을 들어 2차적 강제처분을 예정한 간접강제적 성격을 가졌다고 설명하기도 한다.[472]

---

465) 指宿 信, "サイバースペースにおける証拠収集とデジタル証拠の確保：2011年改正法案を考える", p.86.
466) 樺 清隆, "インターネットのプロバイダのメールサーバ内の電子メールに対する捜索差押許可状を発付することの可否", 『別冊判例タイムズ』 35号, 2012, P.154.
467) 川瀬 孝史, "磁的記録に対する捜索差押え上の諸問題：令状実務とその周辺の諸問題", 『警察学論集』 74巻9号, 2021, p.89.
468) 南部 晋太郎, 위의 논문, p.149.
469) '이전'이란 전자데이터를 별도의 기록매체에 복사한 후 원래의 기록매체로부터 삭제하는 것을 의미한다.
470) 우지이에 히토시, "일본의 전자적 증거 압수에 관한 2011년 개정법 소개", 『형사법의 신동향』 통권 제49호, 대검찰청, 2015.12, 418면.
471) 指宿 信, "サイバースペースにおける証拠収集とデジタル証拠の確保：2011年改正法案を考える", p.87.

3) 원격접근(제99조 제2항, 제218조 제2항 준용)

우리가 일상적으로 사용하는 컴퓨터는 네트워크에 접속한 채로 이용하는 경우가 대부분이다. 개인용 컴퓨터 내에서만 정보를 처리하고 저장하던 과거와 달리 이제는 네트워크를 통해 물리적으로 떨어진 장소에도 빠르게 전자적기록을 저장할 수 있다. 따라서 단순히 개인용 컴퓨터 등을 압수하는 것만으로는 필요한 전자적기록을 확보할 수 없는 상황이 발생했다. 네트워크가 연결되어 있는 전자적기록매체(전자적기록의 보존처)를 압수하기 위해서는 기존의 유체물을 대상으로 하는 형사소송방식으로는 사이버공간에서의 범죄의 유력한 증거인 전자적기록을 압수하기 곤란하다는 지적과 함께[473] 2011년 형사소송법 개정을 통해 원격접근방식을 도입했다. 원격접근은 압수물이 컴퓨터나 휴대전화기, 핸드폰, 태블릿 등 '전자계산기'인 경우, 해당 컴퓨터와 네트워크로 연결된 스토리지(기록매체)가 해당 컴퓨터에서 '작성'하거나 '변경'한 전자적기록 또는 변경이나 '삭제'할 권한이 있는 전자적기록을 보관하는 데 사용하는 것으로 인정되면[474] 해당 기록매체로부터 전자적기록을 그 컴퓨터나 다른 기록매체에 복사한 후 컴퓨터와 함께 또는 기록매체를 압수하는 것을 말한다.[475] 따라서 단지 열람만을 할 수 있는 전자적기록은 원격접근의 대상이 되는 전자적기록이 아니다.[476] 압수 대상 외의 컴퓨터와 (서버) 압수대상 컴퓨터가 장소적으로 떨어져 있기에 원격접근(リモートアクセス)이라고 부른다. 원격접근에 의하면 압수하려는 전자적기록이 컴퓨터 본체에 저장된 것이 아니라 회사 공유 서버 등에 저장되어 있는 경우에도 압수할 수 있다. 한편, 해당 컴퓨터(전자계산기)뿐만 아니라 다른 기록매체에 복사할 수 있게 한 이유는 해당 컴퓨터의 저장용량이 복사하기에 부족한 경우나 해당 컴퓨터 자체를

---

472) 指宿 信, "サイバースペースにおける証拠収集とデジタル証拠の確保：2011年改正法案を考える", p.87. 한편 실무에서는 전자적기록매체를 관리하는 자와 피의자 사이에 특별한 관계성이 존재하지 않는 경우에 주로 활용한다.

473) 柴田 和也, 앞의 논문, p.13.

474) 압수 대상 외의 컴퓨터는 ① 압수대상 컴퓨터와 '접속성'을 가져야 하며, ② 압수대상 컴퓨터에서 전자적기록을 작성, 변경, 삭제하였다는 '관련성'이 있어야 하고, ③ 이러한 데이터를 보관하고 있다는 '사용 개연성'이 인정되어야 한다(指宿 信, "サイバースペースにおける証拠収集とデジタル証拠の確保：2011年改正法案を考える", p.88). 한편, 대상이 되는 전자데이터의 경우 전자계산기를 조작하여 '작성', '변경', '삭제'할 수 있는 경우로 한정하고 있으므로 열람만 하는 경우라면 포함되지 않는다(柴田 和也, 위의 논문, p.13).

475) 川瀬 孝史, 앞의 논문, p.90.

476) 柴田 和也, 위의 논문, p.13.

조사할 필요가 있는 경우(해당 컴퓨터에 전자적기록의 삭제 흔적이 남아있어 이를 조사할 필요가 있는 경우) 등을 고려한 것이다.[477] 원격접근은 기본적으로 일반적인 압수수색영장에 의한다. 영장에는 압수해야 할 물건으로 전자계산기를 특정하여 기재하여야 하고 "압수하여야 할 전자계산기에 전자통신회선으로 접속된 기록매체로 전자적기록을 복사해야 할 범위"를 기재하여야 한다(형사소송법 제107조 제2항 및 제219조 제2항). 이로써 복사 대상이 되는 전자적기록매체를 특정할 수 있으며, 피의사실과 전자적기록이 기록된 것인지 그 '개연성'을 판단할 수 있다.[478] 또 '복사해야 할 범위'는 구체적 사안에 따라 다르게 기재할 수 있는데, 실무상 압수할 전자계산기 사용자가 이용하는 ID로 접속할 수 있는 기록영역 등으로 기재하는 경우가 많고, 이러한 실무의 운용방식에 관하여 보다 구체적으로 이를 기재하여야 한다는 지적이 있다.[479]

원격접근을 통한 복사처분은 전자계산기를 압수대상으로 하는 경우 집행방법으로 부가적으로 인정되는 처분이다.[480] 따라서 이미 압수한 전자적계산기의 경우 이를 다시 압수할 수 없다. 실무현장에서 수사기관이 컴퓨터를 켜고, 네트워크에 접속하여 기록매체에 접근하려고 할 때 필요한 로그인 ID 등을 밝혀내지 못하여 복사처분을 하지 못한 경우, 해당 컴퓨터를 먼저 압수한 후 다시 다른 곳에서 원격접근을 시도하는 것은 허용되지 않는다.[481]

4) 소결

과거 일본 형사소송법은 압수수색의 대상을 유체물로 한정하고 있었기에, 수사에 필요한 전자적증거를 확보하기 위해서는 전자적기록이 저장된 전자적기록매체 자체를 압수할 수밖에 없었다. 인터넷을 사용한 범죄가 급증하면서 기존 유체물을 대상으로 하는 형사소송법 규정만으로는 부족하다는 지적이 꾸준히 제기되었다. 2011년 형사소송법 개정으로 사이버범죄와 관련된 법 제도가 신설되고 정비되었다. 그중 전자적기록의 압수와 관련된 제도로 (1) 전자적기록매체에 대한 대체집행, (2) 기록명령

---

477) 江口 和伸, "ネットワーク接続コンピュータを対象とする捜索 , 差押え", 『別冊判例タイムズ』 35号, 2012, p.160.
478) 松田 克之·宮崎 桃子, "情報通信機器の発達を背景とした令状 : 捜査に対する司法審査の在り方等に関する研究", 『判例タイムズ』 1488号11月号, 2021, p.57.
479) 松田 克之·宮崎 桃子, 위의 논문, p.57.
480) 柴田 和也, 앞의 논문, p.13.
481) 松田 克之·宮崎 桃子, 위의 논문, p.58.

부압수, (3) 원격접근을 살펴보았다. 이러한 압수의 방법은 전자적기록 특유의 성질을 반영하여 증거를 취득할 수 있도록 하면서도 전자기록의 특성으로 인해 강제처분과정에서 발생할 수 있는 과도한 침해를 최소화하려는 노력이 함께 반영된 것으로 보여진다. 예를 들어 전자적기록이 기록된 유체물 그 자체를 빠짐없이 압수할 경우, 기록매체 내에 혼재된 피의사실과 관련 없는 여러 정보들을 함께 압수함으로써 발생할 수 있는 프라이버시 침해의 문제 및 기록매체를 압수하여 발생할 수 있는 업무방해 등에 관한 문제는 (1) 전자적기록매체의 전자기록을 복사, 인쇄, 이전시킨 후 이를 저장한 기록매체를 압수하거나, (2) 전자기록의 보관자 등에게 특정한 전자적기록을 수사기관이 지시한 기록매체에 옮기도록 '명령'하여 이를 압수하는 방법을 통해 일부 해결할 수 있다.[482] 하지만, 입법 과정에서 미처 다루지 못했던 부분들은 여전히 다툼의 대상이 되고 있고(역외압수 등), 비가시성과 비가독성을 특성으로 하는 전자적기록의 압수범위의 확정 역시 꾸준히 논쟁이 되고 있다. 한편, 관련 규정에 대한 실효성 확보에 관한 문제도 종종 언급되는 바, 기록명령부압수에서 전자적기록을 보관하는 사람 혹은 이용 권한을 가진 자가 수사기관의 명령에 불응할 경우 이를 강제할 수단이 없다는 점이나 원격접근에서 로그인 ID를 알지 못할 경우 이를 강제로 취득할 방법이 없어 원격접근을 할 수 없는 경우에 관한 문제 등이 그 예이다.[483]

3. 디지털 증거 압수영장에서 압수대상물 특정에 관한 문제

일본 헌법 제35조 제1항은 "누구라도 주거, 서류 및 소지품에 대하여 침입, 수색 및 압수를 당하지 않을 권리는 제33조의 경우를 제외하고 정당한 이유에 근거하여 발생한다. 수색하는 장소 및 압수하는 물건을 명시한 영장 없이는 이 권리는 침해할 수 없다"고 규정한다. 이 규정은 전통적으로 '주거는 사생활의 중심'이라는 사상을 바탕으로 '주거 등의 불가침'을 규정한 것으로 여겨졌으나, 규정의 취지에 비추어 재산적 이익의 보호 이외에도 사생활이나 자유의 비밀까지도 포함하여 보호하고 있다고 해석한다.[484] 한편, 학설에서는 이러한 헌법상 주거불가침에 관한 권리를 형사절차

482) 高村 紳, 앞의 논문, p.96.
483) 松田 克之·宮崎 桃子, 앞의 논문, p.58; 高村 紳, 위의 논문, p.97.
484) 海野 敦史, "監視型情報収集と憲法35条１項との関係:「私的領域に侵入されることのない権利」を保障する意義", 『情報通信政策研究』 第2巻第1号, 2018, p.34.

법상 영장주의와 결부시키는 경우도 있다. 이러한 이유는 '제33조의 경우를 제외하고', '영장이 없이는'이라는 수색 등이 결국 수색 등의 정당화 사유를 염두한 것이라고 해석할 수 있다는 것에 근거한다.[485] 압수대상물을 영장에 기재하도록 하는 이유는 수사권의 한계를 정함과 동시에 압수를 당하는 사람이 압수대상물을 예측하고 수사기관의 권한남용에 대한 이의를 제기할 수 있도록 하기 위함이라고 설명한다.[486] 전자적 기록매체의 경우 문서 등을 압수할 때와 같이 '압수할 필요가 있는 물건'을 특정하여 기재하여야 한다. 하지만 피의자나 제3자가 수사기관에 비협조적이라면 실제로 영장을 집행하려는 현장의 전자적기록매체의 수량 및 유형을 특정하기 어려운 문제가 발생한다. 이러한 경우에는 압수영장에 문서 등 다른 목적물과 동일하게 일정부분 '추상적이고 포괄적인 기재'를 허용할 수 있다.[487] 다만 '하드디스크, USB 메모리'처럼 기록매체의 종류만을 기록하는 것이 아니라 영장을 집행할 수사기관과 피처분자가 각각 대상물의 해당성을 판단할 수 있을 정도로(예를 들어 고객리스트와 거래처 관계가 기록된 하드디스크 등) 한정할 필요가 있다.[488] 원격접근의 경우에는 이에 덧붙여 압수 영장에 '압수하려는 전자계산기의 전기통신회선으로 접속하려는 기록매체로 전자적기록을 복사하여야 할 범위'를 기재하여야 한다(형사소송법 제107조 제2항 및 제219조 제2항). 즉, 원격접근을 하려는 컴퓨터 등을 기재하고 수집하려는 범위(예컨대 피의자의 ID 등으로 접속 가능한 기록영역)를 기재하면 된다.[489] 기록매체가 있는 물리적 장소나 구체적 IP주소까지 특정할 필요는 없다. 만약 회사 업무와 관련된 범죄를 저지른 피의자가 회사 컴퓨터로 범죄의 준비 및 실행한 것으로 여겨지는 경우 '피의자가 사용한 컴퓨터에 접속하고 있는 기록매체로 피의자가 사용하는 ID로 접속할 수 있고 피의자가 소속된 부서의 직원들이 작성한 컴퓨터 파일을 보관하는 데 사용하는 것'으로 기재하면 압수 대상이 특정된 것으로 볼 수 있다.[490] 한편, 기록명령부압수의 경우 프로바이더가 관리하는 전자적기록이 압수의 대상이 되므로 영장에

485) 海野 敦史, "憲法35条1項に基づく権利の保障と令状主義の要請との関係",『情報通信学会誌』38巻 3号, 2020, p.40.
486) 宮木 康博, "電磁的記録媒体の差押え（最決平成 10·5·1）",『法学教室』2019年11月号, 2019, p.16.
487) 南部 晋太郎, 앞의 논문, p.148.
488) 川瀬 孝史, 앞의 논문, p.94.
489) 川瀬 孝史, 위의 논문, p.95-96.
490) 江口 和伸, 앞의 논문, p.160.

전자적기록매체의 종류를 특정하지 않아도 된다(기록명령부 압수영장 사용). 서버가 존재하는 주소 역시 기재 대상이 아니다. 다만, 기록하게 해야 할 혹은 인쇄하게 해야 할 전자적기록이 무엇인지는 명시해야 한다.[491]

한편, 범행 전후기간의 접근로그(access log)를 압수할 수 있는가에 관한 문제도 발생할 수 있다. 압수는 수사의 초기단계에서 이루어지기 때문에 압수 단계에서는 필요한 접속로그의 기간을 특정하기 어렵다. 다만 범행계획 등을 파악하기 위해서는 범행 전후 기간의 접근로그도 압수할 필요가 있다고 한다.[492]

4. 디지털 증거 압수수색 집행과정에서의 문제

가. 디지털 증거의 압수대상물 해당성 판단을 위한 내용확인

전자적기록매체를 압수하려는 경우 해당 전자적기록매체가 압수대상물인지 여부를 판단하기 위해서는 기록매체의 성질, 보관자, 보관장소 및 보관상태 등의 외부적 상황을 먼저 살펴볼 수 있다. 즉, 기록매체에 라벨링이 되어 있는 경우에는 보다 쉽게 해당성을 판단할 수 있을 것이다. 하지만 대부분의 경우 기록매체의 외부를 살펴보는 것만으로는 그 내용을 특정하기 어렵다. 이때에는 직접 전자적기록매체의 내용을 살펴봐야 하는 경우가 발생한다. 즉 현장에서 발견한 노트북컴퓨터가 '본건에 관한 정보가 기재된 하드디스크, USB 메모리 그 밖의 기록매체'인 것인지를 확인하기 위해서는 노트북컴퓨터를 켜고 모니터 등을 통해 전자적기록 내용을 확인하는 방법 등을 들 수 있다. 이 과정에서 로그인 등이 필요한 경우 피처분자에게 협력을 요청할 수 있지만(형사소송법 제222조 제1항, 제111조의2) 이를 거부하더라도 별도로 처벌할 수 있는 규정은 없다.[493] 피처분자의 협력을 구하지 못한 경우 압수 등에 '필요한 처분'으로 수사기관이 직접 노트북컴퓨터를 찾아보거나, 보조자를 입회시킨 후 전문가에게 노트북컴퓨터의 조작을 하도록 하는 방법도 고려할 수 있다.[494]

---

491) 川瀨 孝史, 앞의 논문, p.95.
492) 千葉 陽一, 앞의 논문, p.157.
493) 川瀨 孝史, 앞의 논문, p.96.
494) 川瀨 孝史, 위의 논문, p.97.

나. 검증

일반적으로 실무에서는 압수수색영장과 동시에 검증영장을 신청하기도 한다. 압수수색영장으로 컴퓨터와 하드디스크 등 전자적기록기록매체를 압수한 경우 전자데이터를 해석하기 위해 수사기관은 형사소송법 제111조 소정의 '필요한 처분'으로 피의자를 입회인으로 하여 컴퓨터를 조작할 수 있도록 협조를 구하거나 이러한 상황을 사진으로 촬영할 수 있다.[495] 따라서 피의사실 범행이 주거 내 컴퓨터에 한정된 경우라면 압수수색 영장만으로도 압수목적을 달성할 수 있다.[496] 하지만 인터넷을 사용하여 반복적으로 범죄를 해 온 경우(인터넷을 통해 일정기간 마약을 판매한 경우 등) 피의자에게 그 범행 과정을 재연시키고 이를 기록하여 증거로 삼으려는 경우 검증영장을 발부받을 수 있는가가 문제된다.

5. 디지털 증거 압수수색에 관한 판례의 경향

가. 압수수색 과정에서 디지털 증거의 '개연성(관련성)'에 관한 판례

압수수색이 대상이 되는 전자적기록매체에는 영장에 기재된 사실과 관련 있는 정보와 그렇지 않은 정보가 혼재하여 저장되어 있으며, 저장된 정보의 양 역시 방대하기 때문에 수사기관이 압수수색영장의 집행 현장에서 범죄혐의와 관련한 내용을 전부 선별하고 개별적으로 압수하는 것은 사실상 기대하기 어렵다. 이로 인하여 실무에서는 수사기관이 전자적기록매체를 포괄적으로 압수하는 경우가 종종 활용되었다. 하지만 포괄적 압수는 프라이버시 침해 및 일본 헌법 제35조 위반의 우려가 있다. 먼저 전자적기록의 포괄적 압수에 관한 리딩케이스인 오움진리교 사안(이하, '1998년 최고재판소 결정'이라 한다)을 먼저 살펴보면 다음과 같다. 당시 경찰은 오움진리교가 전자적기록매체에 저장된 정보를 순식간에 삭제할 수 있는 프로그램을 가지고 있다는 정보를 사전에 입수한 상황이었다. 경찰은 압수수색영장을 집행하는 현장에서 기록된 정보 내용을 일일이 확인하지 않고 전자적기록매체(컴퓨터 1대, 플로피디스크 108장)를 압

495) 柴田 和也, 앞의 논문, p.14.
496) 柴田 和也, 위의 논문, p.15.

수하였다. 이러한 경찰의 포괄적 압수에 대하여 일본 최고재판소는 "영장으로 압수하려는 컴퓨터, 플로피디스크 등 중에 피의사실에 관한 정보가 기록되어 있을 개연성이 인정되는 경우 그 정보가 실제로 기록되어 있는지를 그 장소에서 확인하는 것이 기록된 정보를 훼손시킬 위험이 있는 때에는 내용을 확인하지 않고 컴퓨터, 플로피디스크 등을 압수할 수 있다"고 하여 해당 압수가 적법하다는 결정을 내렸다.[497] 즉, 이 결정에서 포괄적 압수를 허용하기위해 고려한 사항은 ① 플로피디스크(전자적기록매체)에 피의사실과 '관련된' 정보'가 존재할 '개연성'이 인정되어야 하며, ② 해당 정보를 영장집행 현장에서 확인하였을 경우 정보가 훼손될 우려가 있는가로 정리할 수 있다.[498] 수사기관이 압수한 플로피디스크가 증거물로써 의미를 가질 수 있는 개연성(내지 가능성)이 있다는 점과 해당 사안에 대해 이미 오움진리교의 신자들이 전자적정보를 순식간에 삭제(혹은 변경)할 수 있는 프로그램을 보유하고 있었기에 현장에서 전자적기록의 확인이 불가능했다는 것이 함께 고려된 것(요건 ②)으로 볼 수 있다.

한편, 전자적증거의 압수에 관하여 많은 쟁점이 다루어진 2021년 최고재판소결정[499] 중에도 포괄적 압수에 관한 내용이 검토되었다. 수사기관이 원격접근으로 전자적기록의 복사를 허가받은 압수수색영장을 집행하면서 개개의 전자적기록의 내용을 확인하지 않은 채 포괄적으로 압수한 것에 대해 최고재판소는 "압수수색영장에 따른 원격접근 복사처분의 대상이 되는 전자적기록에 피의사실과 관련한 정보가 기록되어 있다는 개연성이 인정되는 경우 압수 현장에서 전자적기록 내용확인의 곤란성과 확인작업 과정에서 정보 훼손이 발생할 우려가 있다는 사정이 있는 경우 각 전자적기록의 개별 내용을 확인하지 않고 복사 처분 할 수 있다"고 결정하였다.

1998년 최고재판소결정과 2021년 최고재판소결정은 모두 수사기관의 포괄적 압수가 적법하다고 인정한 결정이다. 2021년 최고재판소결정은 1998년 최고재판소결정이 판시한 ① 전자적기록매체에 피의사실과 관련된 정보가 존재할 개연성의 논리구조는 대체로 유사하게 구성하고 있지만, ② 해당 정보를 영장집행 현장에서 확인하였을 경우 정보가 훼손될 우려에 관해서는 다소 차이가 있다. 물론 2021년 최고재판소

497) 最二小決 平成10年5月1日 刑集第52巻4号275頁.
498) 이를 '제한적 긍정설'로 설명하기도 한다(정대희·이상미, "디지털증거 압수수색절차에서의 '관련성' 문제", 『형사정책연구』 제26권 제2호, 한국형사정책연구원, 2015.여름, 120면).
499) 最二小決 令和3年2月1日 刑集第75巻2号123頁.

결정에서도 '압수 현장에서 전자적기록 내용확인의 곤란성과 확인작업 과정에서 정보 훼손이 발생할 우려가 있다는 사정이 있는 경우(밑줄은 저자)'라는 표현이 등장하지만 2021년 최고재판소결정의 사실관계를 살펴보면 피처분자가 이를 삭제나 변경하는 등의 훼손의 위험성이 현실적으로 존재한다고 보기 어렵기 때문이다.[500]

이는 2021년 최고재판소결정의 원심판결에서도 확인할 수 있다.[501] 오사카고등재판소는 "원격접근으로 복사할 수 있는 전자적기록은 피의사실과 관련성이 인정되어 압수대상물로 여겨지는 해당 전자계산기로 작성 혹은 변경한 전자적기록 또는 변경, 삭제할 수 있다고 여겨지는 전자기록으로이므로 통상 피의사실과 관련성이 있다고 사료되는 것으로 보여지는 이상 압수 현장에서 이러한 전자기록에 대해 하나하나 확인할 것을 요구하는 것은 수사의 신속성에 반하며 수사기관에게 현실적인지 않은 과중한 부담을 지워주는 결과가 되므로 개별 전자적기록에 관하여 개별 관련성 유무를 판단해야 한다고 할 것은 아니다"라고 하면서 "보존된 정보의 양이 대량이어서 복사 전에 피의사실과의 관련성을 개별적으로 확인하는 것 자체에 상당한 시간이 필요할 뿐만 아니라 본건의 증거구조상 수사관들이 현장에서 바로 해당 정보수집의 필요 여부를 판단하기가 곤란하며, 확인작업을 하는 사이에 정보가 훼손, 변조, 개조할 우려는(밑줄은 저자) 해당 사무소에 소재하는 서버 등의 기록매체 내용을 확인하는 경우와 비교하더라도 명백히 크다고 할 수 있다"고 하여 해당 압수가 적법하다 하였다.[502] 그리고 "소론[503]이 인용한 최고재판소결정은 영장으로 압수하려는 컴퓨터, 플로피디스크 등에 피의사실에 관한 정보가 기록되어 있는 개연성을 인정할 수 있는 경우, 그러한 정보가 실제로 기록되어 있는지를 현장에서 확인하다가는 기록된 정보를 훼손시킬 위험이 있는 사정하에서는 내용을 확인하지 않고 위의 컴퓨터, 플로피디스크 등을 압수가 허용된다고 하고 있으나 이러한 최고재판소결정은 반드시 내용을 확인하지 않고 전자적기록매체를 압수하는 것이 허용되는 경우를 소론이 주장하는

500) 中島 宏, "電磁的記録媒体の差押え等の適法性[大阪高裁平30.9.11判決]", 『法学セミナー』 通巻768号, 2019, p.130.

501) 해당 재판에서 변호인은 1998년 최고재판소결정이 (1) 정보가 기록되어 있다는 개연성 및 (2) 확인 전에 정보훼손의 위험성이 존재하는 경우에 한하여 관련성을 확인하기 전에 전자적기록매체를 압수할 수 있는 것이라고 주장했다.

502) 大阪高等裁判所 平成30年9月11日 平成29(う)635.

503) 변호인의 주장을 말한다(각주 501 참고).

조건이 존재하는 경우에 한정하는 취지라고 해석할 수 없다"고 하여 1998년 최고재판 소결정은 당시 사실관계를 전제로 한 예시로 봐야 한다고 하였다.

나. 원격접근

네트워크 통신의 발달로 국외에 있는 전자적기록매체에도 전자기록을 손쉽게 보관할 수 있게 되었다. 이용자는 보다 간단히 전자적정보를 이전하고 은폐할 수 있게 되었다. 따라서 수사기관은 전자기록이 저장된 전자적저장매체 지정이 더욱 곤란해졌다. 나아가 단순히 전자적저장매체를 압수하는 것만으로는 수사목적 달성이 어려운 경우도 발생했다. 전자적기록의 특성을 반영한 증거수집 절차의 정비와 사이버범죄협약의 국내법 정비 등을 목적으로 2011년 일본 형사소송법 개정과정에서 도입된 원격접근은 '압수대상물이 전자계산기일 경우 해당 전자계산기와 네트워크로 연결된 다른 기록매체에 기록된 전자적기록을 해당 전자계산기 또는 다른 기록매체에 복사하여 이를 압수하는 처분'을 말한다(형사소송법 제99조 제2항, 제218조 제2항). 제도의 도입과정에서 클라우드 서비스처럼 전자적 기계가 외부에 항상 접속하고 있는 지금의 사용 환경을 고려할 때 해외 서버를 압수하는 행위가 쉽게 발생할 수 있어 이에 대한 한계설정이 필요하다는 지적이 있었다.[504] 이에 대해 당시 입법담당자는 "일반적으로 전자기록을 복사해야 하는 전자기록매체가 다른 나라의 영역 내에 있다고 판명한 경우 (사이버조약) 제32조로 접근 등을 할 수 있는 경우에 해당하지 않으면 해당 국가의 주권 관련 문제가 생길 가능성이 있으므로 이러한 처분을 자제하고 해당 다른 국가에 동의를 얻거나 수사공조를 요청하는 것이 바람직하다"는 취지의 설명을 하였다.[505] 이처럼 국외에 있는 서버에 존재하는 전자적정보를 취득하기 위한 형사절차적 방법은 원격접근에서 가장 중요한 과제이기도 하다. 아래에서는 원격접근에 관한 주요 판례와 실무상의 문제를 함께 검토하도록 한다.

---

504) 指宿 信, "押収済みパソコンを用いて検証許可状に基づき海外メールサーバにアクセスした捜査に重大な違法があるとして証拠を排除した事例", 『新·判例解説』 20号, 2017, p.226.

505) 杉山 徳明·吉田 雅之, "「情報処理の高度化等に対処するための刑法等の一部を改正する法律」について(下)", 『法曹時報』 64巻5号, 2012, p.1095.

1) 원격접근을 목적으로 하는 재압수, 검증영장에 의한 원격접근의 가부(可否)

가) 원격접근을 목적으로 하는 재압수

원격접근으로 복사를 실행하려는 경우 현재 네트워크에 접속이 되어 있는 상태의 컴퓨터(전자적기록매체)를 압수하기 전에 이를 실시하여야 한다. 하지만 압수수색 현장에서 컴퓨터에 비밀번호 등이 설정되어 있어 로그인하지 못한 경우, 혹은 접속하려는 ID를 입수하지 못한 경우에는 현장에서 원격접근을 실시할 수 없다. 현장에서 압수수색의 목적을 달성하지 못한 경우, 해당 컴퓨터를 먼저 압수하여 원격접근을 시도하는 것은 불가능하다. 원격접근은 해당 압수 컴퓨터가 네트워크에 접속되어 있는 상태에서 시행하여야 함은 물론 컴퓨터를 압수하기 전에 이를 실시하여야 하기 때문이다.[506] 그렇다면 컴퓨터를 압수한 후, 추후에 이루어지는 원격접근에 대하여 복사를 처분하는 영장을 별도로 발부받아 시행하는 것(재압수)은 가능할지가 논의되었다.[507] 재압수 자체는 필요성이 인정되는 한 허용될 수 있기 때문이다.[508] 원격접근을 위한 재압수에 대해서는 원격접근은 어디까지나 부수처분이라는 점을 들어 원격접근만을 목적으로 한 재압수는 필요성을 결여한 처분으로 허용될 수 없다고 한다.[509] 왜냐하면 이미 확보한 전자적기록매체를 원격접근을 위해 다시 압수할 경우 압수목적은 전적으로 원격접근일 것이기 때문이다. 한편, 디지털 정보의 압수수색의 필요성과 현실성을 고려하여 이미 압수한 컴퓨터에 재압수청구도 허용해야 한다는 견해도 있다.[510]

나) 검증영장에 의한 원격접근

수사기관이 원격접근을 할 수 있는 영장을 발부받아 이를 집행하는 현장에서 컴퓨터를 압수하였으나 컴퓨터 로그인에 필요한 비밀번호를 알 수 없어 원격접근을 사용한 복사처분을 실시하지 못하였다. 이후 압수한 컴퓨터를 조사하던 중 범행과 관련된 흔적 및 메일 접속 이력을 발견하고 다시 해당 컴퓨터로 원격접근을 시행하고자 했다. 이를 위해 압수한 컴퓨터에 다시 원격접근 압수영장을 신청하는 방안을 검토해 보았

506) 柴田 和也, 앞의 논문, p.13.
507) 松田 克之·宮崎 桃子, 앞의 논문, p.59.
508) 松田 克之·宮崎 桃子, 위의 논문, p.59.
509) 柴田 和也, 위의 논문, p.13.
510) 小向 太郎, "クラウド上のデータを対象とする犯罪捜査に関する法的課題", 『情報処理学会研究報告』, 2018, p.2.

으나 압수된 물건에 다시 압수영장을 청구하는 것은 인용되지 않을 우려가 있다고 판단한 후, 컴퓨터를 조작한 결과를 검증하는 검증영장을 청구하기로 결론내렸다. 압수한 컴퓨터를 사용해 메일서버에 원격접근하는 것을 '검증에 필요한 처분'으로 볼 수 있을 것이라는 고려가 반영된 결과였다. 수사기관은 압수한 컴퓨터를 '검증하여야 할 물건'으로 하여 검증영장을 발부받은 후 해당 컴퓨터 내용을 복제한 컴퓨터로 인터넷에 접속한 후 압수한 컴퓨터의 이력이 남아있는 메일의 서버에 원격접근하여 메일 송수신이력과 내용을 다운로드한 후 저장하였다. 이처럼 수사기관이 검증영장을 발부받아 원격접근을 하는 것이 적정한 것인가에 대하여 1심 재판소인 요코하마지방재판소는 "본건 검증은 '검증하여야 할 물건'으로 본건 컴퓨터가 기재된 것 뿐인 검증영장에 기초하여 검증에 필요한 처분으로 원격접근을 한 것인바, 수사기관이 검증영장에 근거하여 컴퓨터 상태를 검증할 권한을 가진다 하더라도 해당 컴퓨터로 인터넷에 접속하여 메일 서버에 원격접근하는 것이 당연히 인정되지 않음은 형사소송법 규정의 취지(원격접근으로 복사처분을 하는 것은 전자계산기를 압수하는 것에 해당하고 해당 전자계산기가 접속한 서버 내에 기록된 해당 전자계산기가 작성·변경·삭제 가능한 데이터를 해당 전자계산기 등에 복사한 후 동 전자계산기를 압수하는 처분으로 어디까지나 전자계산기의 압수에 수반하는 처분으로 실시하는 것이 인정된 것이므로 해당 복사처분은 전자계산기의 압수에 선행하여 실시되어야 하고 압수가 종료된 후에 실시할 수 있음은 상정하지 않는다)에서 보더라도 분명하다"[511]라고 판시하였다. 2심재판소인 도쿄고등재판소 역시 "본건 검증은 본건 컴퓨터 내용을 복제한 컴퓨터로 인터넷에 접속하여 메일 서버에 원격접근한 후 메일 등을 열람·저장한것인 바 본건 검증영장에 근거하여 할 수 없는 강제처분을 한 것으로"[512]라고 하여 원심의 판결을 지지하였다. 이러한 판결에 대해 접속된 서버의 수사가 압수 당시에만 한정되는 것은 타당하지 않다고 하면서 압수한 컴퓨터에 다시 압수영장을 발부할 수 있도록 해야 한다는 견해도 있다.[513]

---

511) 横浜地裁 平成28年3月17日 判時2367巻115頁.
512) 東京高裁 平成28年12月7日 高集第69巻2号5頁.
513) 小向 太郎, 앞의 논문, p.2.

2) 수사기관이 영장 없이 임의협조 하에 전자정보를 열람하고 사진을 촬영한 경우

피고인이 전 교제상대의 아들에게 사 준 태블릿 단말기의 초기설정을 피고인의 스마트폰과 동기화시켜 두어 태블릿과 스마트폰으로 검색이력을 상호 열람할 수 있음을 인지한 수사기관이 전 교제상대에게 임의협조를 구해 며칠 동안 전자적계산기(태블릿)를 빌린 후 해당 태블릿 단말기를 사용하여 인터넷에 접속해 피고인 계정의 검색이력을 망라적으로 열람하고 사진촬영을 한 것이 적법한지가 다투어진 사안에서, 도쿄고등재판소는 전 교제상대가 피고인의 검색이력을 열람한 것은 피고인이 수인가능한 행위로 허용된다고 하면서 "본건 열람수사는 합리적으로 여겨지는(推知) 피고인의 의사에 반하여 사적영역의 상당히 깊은 부분에 광범위하게 침입한 것이므로 개인의 의사를 제압하여 헌법이 보장하는 중요한 법적이익인 프라이버시권을 침해하는 것으로 형사소송법상 특별한 근거규정이 없는 한 허용될 수 없는 강제처분이라 할 것이다. 그리고 본건 열람수사는 전자계산기인 피고인의 스마트폰 또는 본건 태블릿과 전기통신회선으로 접속된 기록매체인 구글사의 서버 중 피고인의 스마트폰 또는 본건 태블릿으로 작성한 전자적기록을 보관하기 위해 사용되는 본건 검색이력 기억영역에 기록되어 있는 전자적기록을 가독성 있는 문자로 변환하여 이를 사진촬영한 것이므로 형사소송법 제218조 제2항이 규정하는 원격접근과 같은 효과를 지닌다. 이처럼 본건 열람수사 중 피고인의 스마트폰 검색이력에 관한 부분은 피고인 승낙도, 원격접근 영장도 받지 않은 채 시행된 것으로 위법하다"고 판시하였다.[514]

3) 국외의 서버에 원격접근을 이용한 수색(역외 압수수색)

수사과정에서 압수수색의 대상이 되는 전자적기록이 다른 나라 서버에 존재하는 경우는 매우 빈번히 발생한다. 외국에 있는 증거를 수집하는 방법은 크게 자국의 수사기관이 외국의 증거를 직접 수집하는 방법과 자국의 수사기관이 외국의 수사기관 등에 증거수집의 위탁을 통해 수집하는 방법을 택할 수 있다.[515] 하지만 수사활동과 같은 집행관할권에 기초한 강제처분은 원칙적으로 각 국가의 영역 내에만 인정되기 때문에(임의수사도 포함)[516] 실무상 국제공조에 의한 방법으로 증거수집을 하도록

514) 東京高裁 平成31年1月15日 高等裁判所刑事裁判速報集令和元年95頁.
515) 早乙女 宜宏, "リモートアクセスによる差押えに伴う問題点の一考察", 『日本大学法科大学院法務研究』第16号, 2019, p.72.

하고 있다. 따라서 국외 서버에 있는 전자적기록을 취득하려는 경우에도 원칙상 국제수사공조 등에 의하는 것이 바람직하다. 하지만, 국제수사공조의 경우 요청 및 대응이 각 국가의 국내법에 따라 실시되기 때문에 복잡한 절차를 거쳐야 하며 많은 시일이 소요된다.[517] 이 과정에서 증거가 되는 전자적기록을 이전시켜 은폐해 버리거나 의도적으로 변조, 삭제해 버릴 수 있으며, 전자적기록을 이전시켜버린 경우 이전된 전자적기록이 존재하는 국가를 특정하기도 쉽지 않은 문제가 발생한다.[518] 한편 클라우드 서비스의 경우 수사기관은 물론 이용자와 서비스제공자조차 전자적정보가 어느 곳에 기록되었는지 특정하기 어려운 경우도 있을 수 있다. 서버의 소재지조차 판명되지 않은 경우, 동의 및 수사공조를 구해야 하는 상대방을 알 수 없으므로 수사기관이 직접 원격접근을 할 수밖에 없다.[519] 원격접근을 이용하여 다른 나라의 서버에 접속한 경우 이러한 행위가 상대방의 주권을 침해할 가능성이 있는 것인지, 반드시 국제수사공조에 의하여야 하는 것인지 등이 문제될 수 있는바 아래에서는 이와 관련한 판례를 살펴보도록 한다.

가) 역외 압수수색에 관한 판례의 경향과 흐름

수사(임의수사를 포함)나 재판은 주권행사로 원칙상 자국 내에서만 가능하다.[520] 국내 정보통신망에 접속된 컴퓨터로 다른 국가에 있는 서버에 접근하여 기록된 전자적정보를 열람하고 복사하는 경우에도 해당 국가의 승인이 필요하다.[521] 역외 압수수색을 다룬 의미 있는 판례로는 2016년 도쿄고등재판소판결과 2021년 최고재판소결정을 들 수 있다. 2016년 도쿄고등재판소판결은 수사기관이 검증영장을 발부받아 메일서버에 원격접근하여 전자적증거를 수집한 사안이다. 당시 수사기관은 피의자가 이용하는 메일서버가 해외법인 소유임을 파악하고 있었으므로 메일서버가 국외에 존재할 가능성이 높다고 인식했지만 별도로 이에 대한 고려 없이 국외에 존재하는 메일서버에 원격접근하였다. 국외서버에 원격접근하고 복사하는 행위가 적법한 것인지에 대하여

516) 寺林 裕介, 앞의 논문, p.14.
517) 수사에 필요한 전자적기록을 국제수사공조를 통해 취득하기까지 실제로 소요되는 시간은 대략 6개월에서 24개월이 걸린다(小向 太郎, 앞의 논문, p.4).
518) 寺林 裕介, 위의 논문, p.15; 早乙女 宜宏, 위의 논문, p.73.
519) 松田 克之·宮崎 桃子, 앞의 논문, p.61-62.
520) 草野 耕一 외 3인, "最高裁第二小法廷令3.2.1決定", 『判例タイムズ』 1494号5月号, 2022, p.49.
521) 松田 克之·宮崎 桃子, 위의 논문, p.61.

도쿄고등법원은 “본건 메일서버는 미국법인의 것으로 해당 메일서버가 다른 나라에 존재하는 경우 다른 나라의 주권에 대한 침해가 문제 될 수 있다. 이러한 점에 관하여 국제적으로 통일된 견해가 존재하지 않고 수사기관으로써는 국제수사공조를 요청하는 방법에 의함이 바람직하다”고 판시하였다.[522] 해당 판결의 원심판결인 요코하마지방재판소는 “서버 컴퓨터가 타국에 존재하는 경우에 그 서버에 접근하는 것은, 컴퓨터 네트워크가 타국으로부터 접근하는 것을 당연히 전제로 하는 시스템이라 하더라도 해당 국가의 주권에 대한 침해가 문제 될 수 있다. 이에 대해 국제적으로 통일된 견해는 아직 형성되었다고 할 수 없지만(사이버범죄협약 제32조도 해당 원격접근이 동의에 기초한 경우 또는 해당 데이터를 공공이 이용할 수 있는 때라는 한정된 경우 이외에 어떠한 경우에 원격접근에 의한 복사처분을 허용하는지에 대해 명시하고 있지 않다. 또한 본 건은 앞의 경우에도 해당하지 않는다) 수사기관은 수사활동에서 이러한 문제가 발생하지 않도록 서버 컴퓨터가 국외에 존재한다고 인정되는 경우에는 기본적으로 원격접근에 의한 복사처분을 자제하고 국제수사공조를 요청하는 방법이 바람직하다. 본건에서도 서버 컴퓨터가 국외에 존재할 가능성이 높았으며 수사기관도 이를 인식하고 있었으므로 이러한 처분(원격접근: 필자 주)을 하는 것은 기본적으로 피해야 한다고 할 수 있지만, 수사기관은 본건 검증으로부터 상당한 기간이 경과한 후인 본건 공판 중에 일미(日米)형사공조조약에 근거한 공조요청을 하였음이 인정된다. 수사기관은 수사목적 달성을 우선시하여 관련한 법적 문제에 관한 적절한 배려를 결하였다 할 것이다”[523]라고 판시하여 국제수사공조 없는 원격접근이 적절하지 못하다고 하였다.

또한 2019년 도쿄고등재판소판결은 역외 압수수색을 정면으로 다루고 있는 사안은 아니지만, 미국 구글사의 서버에 원격접근하는 것은 다른 나라의 주권을 침해할 수 있어 위법하다는 주장에 대하여 견해를 밝히고 있다는 점에서 의미가 있다. 해당 사안에서 도쿄고등재판소는 “일반적으로 서버가 외국에 있을 가능성이 있는 경우 원격접근의 가부(可否)에 관하여 사이버범죄조약상 규정이 없고 국제적 합의를 구하지 못하였다고 보인다. 원격접근을 하기 위해서는 국제수사공조를 요청하는 것이 바람직하지만 국제수사공조 요청 없이 원격접근을 하여 외교상의 문제가 발생할 수

522) 東京高裁 平成28年12月7日 高集第69巻2号5頁.
523) 横浜地裁 平成28年3月17日 平成24年(わ)第2075号.

있는 것은 차치하고, 일본 형사소송법 해석상 수사의 위법성 판단에 직접적인 영향을 미친다고 할 수 없다"고 판시하였다.[524]

한편, 2021년 최고재판소결정에서 원격접속의 적법성이 논의된 사실관계를 간략히 정리하면 다음과 같다. 수사기관은 원격접근영장을 발부받아 이를 행사하는 과정에서 원격접근을 하고자 하는 메일서버가 국외에 존재할 수도 있다는 점을 인지하였다. 수사기관은 원격접근을 시도하기에 앞서 메일서버가 국외에 존재하는 경우 상대국의 주권을 침해할 우려가 있으므로 메일서버가 국외에 있는 것으로 판명되면 원격접근 복사를 포기하고 컴퓨터사용자등(이하 "甲등" 이라 한다) 승낙을 얻어 이를 실시하기로 사전에 협의하였다. 수사기관은 甲등의 승낙을 얻어 甲등이 사용하는 컴퓨터로 원격접근을 실시하고 메일 등 전자적기록을 복사한 해당 컴퓨터를 피의자가 임의제출하는 형식으로 확보하였다(절차①). 이와 같은 전자적기록 복사행위에 상당한 시간이 소요될 것으로 예견되면서 피의자 등은 자신의 영업에 피해가 가지 않도록 자신의 사무실 이외의 장소에서 수사기관의 컴퓨터로 메일서버에 원격접근하여 복사할 수 있도록 계정을 만들어 주겠다는 제안을 하였다. 경찰은 피의자 등이 작성한 협의서에 근거하여 사무실 이외의 장소에서 원격접근을 하고 전자기록을 복사한 행위(절차②)에 대해 수사기관이 국외에 존재할 개연성이 높은 메일서버에 원격접근하여 복사한 행위가 적법한지가 중요한 쟁점으로 다루어진 사안이었다. 최고재판소는 절차①과 절차②의 대상인 전자적기록매체가 일본 국외에 있을 개연성을 부정할 수 없다고 하면서 "형사소송법 제99조 제2항 및 제218조 제2항의 문구, 이들 규정이 사이버범죄 협약 체결을 위한 절차법 정비의 일환으로 제정되었다는 입법경위 및 동 조약 제32조 규정내용 등에 비추어 볼 때 형사소송법이 앞의 각 규정에 근거한 일본 국내에 있는 기록매체를 대상으로 하는 원격접근 등만을 상정하였다고 해석할 수 없고 전자적기록을 보관한 기록매체가 동 협약의 체약국에 소재하고 동 기록을 공개할 정당한 권한을 가진 자의 합법적이고 임의적인 동의가 있는 경우라면 국제수사공조에 의하지 않고 기록매체에 대한 원격접근 및 기록의 복사를 허용할 수 있다고 해석하여야 한다"고 판시했다. 이는 사이버범죄협약 제32조에 해당하는 경우라면 국제수사공조 요청 없이 원격접근을 허용한다고 해석한 것으로 볼 수 있다.[525]

---

524) 東京高裁 平成31年1月15日 高等裁判所刑事裁判速報集令和元年95頁.

나) 사이버범죄협약 제32조

사이버범죄협약 제32조는 ① 공적으로 이용가능한 장치가 된 컴퓨터데이터인 경우(제32조a), ② 컴퓨터시스템을 사용하여 데이터를 개시할 정당한 권한을 가진 자의 합법적이고 임의적인 동의가 있는 경우(제32조b)에는 다른 체약국의 동의가 없더라도 데이터에 접근할 수 있다고만 규정하고 있다. 따라서 협약에 규정된 경우를 제외한 경우, 즉 데이터가 있는 체약국의 동의 없이 '수사목적'으로 원격접근 등을 하는 것이 국제법상 위법한 집행관할권을 행사하는 것인가에 관하여는 국가별로 견해의 차이가 있다.[526] 일본은 '범죄수사를 위하여' 국외 서버에 원격접근할 때 필요한 조건이나 명확한 기준을 밝히고 있지 않다.

다. 소결

전자적기록의 압수수색을 다룬 주요 판례의 쟁점과 내용을 정리하면 다음과 같다.

[표 3-2] 전자적기록의 압수수색에 관한 주요 판례 정리

구분	1998년[527] 최고재판소결정	2016년[528] 도쿄고등재판소판결	2019년[529] 도쿄고등재판소판결	2021년[530] 최고재판소결정
쟁점 사항	•포괄적 압수수색	•검증영장에 의한 원격접근 •역외 원격접근	•역외 원격접근 •영장 없이 태블릿을 빌려 전자적기록을 열람하고 사진촬영한 행위	•포괄적 압수수색 •역외 원격접근
주요 내용	•포괄적 압수수색 : 허용 [허용요건] ① 피의사실과 관련된 정보가 기록되어있을 개연성 ② 현장에서 관련성을 확인하면 정보가 훼손될 위험이 있는 경우	•검증영장에 의한 원격접근 : 허용할 수 없음 •역외 원격접근: 수사공조를 요청해야 하므로 수사공조에 의하지 않은 일방적 원격접근은 허용할 수 없음 ※ 원심 : 요코하마지방재판소	•영장 없이 태블릿을 빌려 열람하고 사진 촬영을 한 행위 : 강제행위에 해당 → 영장 없이 한 해당행위는 위법 •역외 원격접근 : 국제수사공조'를 하지 않았다고 반드시 증거능력이 부정되는 것은 아니다(반드시 참고해야 할 필요는 없다).	•포괄적 압수수색 : 허용 [허용요건] ① 피의사실과 관련된 정보가 기록되어있을 개연성 ② 현장에서 관련성을 확인할 때 정보가 훼손될 우려가 '반드시' 존재해야 하는 것은 아님(수사 현실고려) •역외 원격접근

525) 横山 裕一, "国外へのリモートアクセスによる電磁的記録の複写の処分", 『日本大学法科大学院法務研究 』19号, 2022, p.101.
526) 寺林 裕介, 앞의 논문, p.16.

구분	1998년[527] 최고재판소결정	2016년[528] 도쿄고등재판소판결	2019년[529] 도쿄고등재판소판결	2021년[530] 최고재판소결정
				(임의협조에 의한 것) : 허용 ※ 해당 서버가 사이버 범죄협약 체결국에 있었음 ※ 원심 : 오사카 고등법원

* 해당 판례의 쟁점 사항 중 전자적 증거의 압수수색에 관한 사항만을 발췌 정리한 것임. 해당 조문 역시 형사소송법상의 조문만을 정리하였음.

1) 포괄적 압수: 관련성, 개연성, 위험성

1998년 최고재판소결정과 2021년 최고재판소결정 모두 전자적기록매체의 포괄적 압수를 적법하다고 인정하였다. 먼저 1998년 최고재판소결정은 전자적기록매체에 '관련정보가 기록되어 있을 개연성'이 높은 경우와 '기록된 정보를 훼손시킬 위험성'이 있을 경우에는 내용을 확인하지 않고 포괄적 압수를 할 수 있다고 하였다. 이때 위험성은 당시 수사기관이 확보하고 있던 오움진리교 신자들이 기록된 정보를 순식간에 제거할 수 있는 소프트웨어를 개발하였다는 사전정보 등에서 찾을 수 있을 것이다. 한편 당시 형사소송법의 규정상 전자적정보를 압수하기 위해서는 컴퓨터 1대와 플로피 디스크 108장 등 전자적기록매체 자체를 압수하는 방법을 사용할 수밖에 없었다. 전자적기록매체 자체를 압수하는 것은 피의사실과 관련 없는 제3자의 프라이버시를 침해할 우려가 있다.[531] 이러한 침해를 줄이기 위한 방안으로 2011년 형사소송법 개정을 통해 전자적기록매체에 대한 대체집행(제110조의2)이 도입되었다.

한편, 2021년 최고재판소결정에서는 '전자적기록이 피의사실과 관련된 정보일 개연성'과 '해당 정보를 영장집행 현장에서 확인하였을 경우 정보가 훼손될 우려'를 들고 있지만 1998년 최고재판소결정과 같은 현실적 위험성이 존재하였다고 보기 어렵다는 점은 앞서 살펴본 바와 같다. 두 판례가 공통으로 들고 있는 '개연성'은 피의사실

527) 最二小決 平成10年5月1日 刑集第52巻4号275頁.
528) 東京高裁 平成28年12月7日 高集第69巻2号5頁.
529) 東京高裁 平成31年1月15日 高等裁判所刑事裁判速報集令和元年95頁.
530) 最二小決 令和3年2月1日 刑集第75巻2号123頁.
531) 해당 판례에 대해 사건과 무관계한 정보를 대량으로 수집할 우려가 있어 지지할 수 없다고 밝힌 견해로는 高村 紳, 앞의 논문, p.100.

과 '관련성'이 있을 것을 지칭한다. 일본의 실무현장에서 '관련성'은 외부적 사정(피의사실 내용, 증거물의 종류 등)에서 보아 이를 추인할 수 있는 정도면 인정하고 있다.[532] 특히 원격접근의 경우 대상이 되는 것은 "해당 전자계산기로 작성 혹은 변경한 전자적 기록 또는 해당 전자계산기로 변경 혹은 삭제나 제거를 할 수 있다고 보여지는 전자적 기록"에 한하기 때문에, 이러한 전자적기록은 통상 피의사실과 관련된 것으로 볼 수 있다고 한다.[533] 하지만 관련성 내지 개연성을 이렇게 폭넓게 해석하는 판례의 태도에 대해 이는 결국 수사기관의 압수에 관한 재량을 사실상 확장시키는 것이며 종국적으로 영장주의의 본질에 반할 수 있다는 지적이 있다.[534] 관련성은 압수대상물의 피의사실을 해명하는 데 기여하는 것이므로 압수수색 현장에서 관련성을 개별적으로 확인하여야 한다고 하기도 한다.[535] 다만, 판례는 구체적 개별상황을 고려하여 내용의 확인 없는 압수가 허용된 것이라고 본 것으로 모든 전자적기록의 압수에서 개별내용을 확인할 필요가 없다는 의미가 아니라는 것은 주의하여야 한다.[536]

2021년 최고재판소결정 원판결인 오사카고등재판소는 제110조의2를 택하지 않은 것이 위법한 것인가에 대해 "수사의 목적에 비추어 이러한 방법[537]이 항상 유용하고 적절하다고 할 수 없으며 법문상에서도 이러한 처분은 기록매체 자체의 압수에 대한 대체 처분으로 자리매김하고 있어 이를 선택할지 여부는 압수하는 자의 재량에 의한다"고 하며 "수사관들이 압수 현장에서 즉시 기록매체의 내용을 파악하고 보존된 전자적기록 중 수집이 필요한 범위나 기록매체 자체의 압수 대신 복사 등의 대체적 방법을 선택하는 것이 적합한지 판단하기에 용이하지 않았다고 보여지며 전자적기록이라는 대상의 특질상, 복사 등의 작업 과정에서 정보의 훼손, 개조, 변조 등이 발생할 가능성도 있다. 이러한 사정을 감안해 보면 수사관이 복사 등의 대체적 방법을 선택하지 않고 기록매체 자체를 압수한 것이 재량을 넘어선 것으로 위법하다 할 수 없다"고 판시하였다. 이러한 2021년 최고재판소 결정에 대해 개조와 변조가 용이한 전자적기

532) 川瀬 孝史, 앞의 논문, p.98. 한편 전자적기록매체 전부를 피의사실과 관련하는 증거물로 보는 것은 '관련성의 범위가 너무 느슨해지는 것'이라고 지적하는 견해도 있다(指宿 信, "海外サーバからの電磁的記録の差押え等の適法性が争われた事例", 『新·判例解説 Watch』 No.117, 2018, p.188).
533) 松田 克之·宮崎 桃子, 앞의 논문, p.57.
534) 宮木 康博, 앞의 논문, p.18.
535) 宮木 康博, 위의 논문, p.18.
536) 草野 耕一 외 3인, 앞의 논문, p.51.
537) 전자적기록매체에 대한 대체집행을 말한다.

록의 특성상 압수수색 시점 당시 상태를 보존해야 할 필요성이 있음을 들어 이를 지지하면서도 피처분자가 감수할 불이익을 고려하여 압수 후 전자적 정보를 분석하고 확인한 후 필요하지 않다고 판단되는 전자적 정보를 환부하는 조치 등을 검토할 필요가 있다는 견해도 있다.[538]

2) 역외 압수수색에 관한 논의

사이버범죄의 경우 국경을 초월한 법 집행의 필요성이 증가하고 있다. 수사기관이 국제적 규모로 이루어지는 불법행위 수사과정에서 해외에 보존된 전자기록의 확보는 매우 중요한 의미를 갖기 때문이다. 하지만 국경을 넘어 이루어지는 수사활동은 다른 나라 주권을 침해할 우려가 있으므로 상대국의 국제적 협력이 필요하다. 역외 압수수색은 전자적정보의 압수수색에서 매우 중요한 위치를 차지한다.

원격접근하려는 대상 서버가 국외에 존재할 가능성이 있는 경우에 대하여 일본 고등재판소는 각기 다른 판결을 내렸다. 먼저 2016년 도쿄고등재판소는 외국에 있는 서버에 저장된 전자적정보를 수집하기 위해서 수사기관은 원격접근을 이용한 복사를 자제하고 국제수사공조요청을 하여야 한다고 판시하였다.

한편, 2021년 최고재판소결정의 원심인 2018년 오사카고등재판소[539] "일본의 수사기관이 국제수사공조 등을 통해 상대국의 동의를 얻지 않고 해외 원격접근 처분을 한 경우에는 강제수사와 임의수사를 불문하고 대상 기록매체가 소재하는 상대국의 주권을 침해한다는 국제법상 위법을 발생시킬 여지가 있다(생략)"고 하면서, "본건 … 원격접근 등은 실질적으로 사법심사를 거쳐 본건 압수수색영장에 기초하여 실시된 것이라고 평가할 수 있으므로 피고인들에게 이러한 위법성을 주장할 당사자적격이 있는지 의문이다", "[사이버범죄]조약 제32조b의 취지에 대해 수사기관은 피처분자의 적법하고 임의 동의가 있는 경우 상대국과 수사공조를 하지 않더라도 적법한 해외 원격접근을 실시할 수 있다고 볼 여지가 충분히 있다", "원격접근 등은 실질적으로 일본형사소송법에 따라 발부된 본 건 각 영장에 기초하여 실시된 강제수사의 일환으

538) 川瀬 孝史, 앞의 논문, p.102. 한편, 관련되지 않은 정보의 취득을 최소화 하기 위한 방법으로 기록명령부압수(제99조의 2 및 제218조 제1항) 등을 활용하는 방법을 택하는 것이 적절하였을 것이라고 하며 판례를 비판하는 견해로는 中島 宏, 앞의 논문, p.130 참고.

539) 大阪高等裁判所 平成30年9月11日　平成29(う)635 : 2021년 최고재판소결정의 원판결(필자 주).

로 실시된 것이기 때문에 비록 서버 소재국의 주권침해 및 해외 서버 관리자의 권리침해가 있더라도 이로 인하여 수사기관의 원격접근 등의 위법은 증거능력을 잃을 만큼 중대한 것이라고 볼 수 없다"고 판시하였다. 또한 원격접근을 정면으로 다룬 것으로 보기는 어렵지만 2019년 도쿄고등재판소 판결에서도 "원격접근을 하기 위해서는 국제수사공조를 요청하는 것이 바람직하지만 국제수사공조 요청 없이 원격접근을 하여 외교상의 문제가 발생할 수 있는 것은 차치하고, 일본 형사소송법 해석상 수사의 위법성 판단에 직접적인 영향을 미친다고 할 수 없다"고 판시하였다. 각각의 판례는 모두 국외에 존재하는 서버에 원격접근하는 것에 대하여 해당 국가의 주권침해 가능성을 인정한다는 점에서 공통한다. 다만, 일본의 수사기관의 행위가 국제법상 위법한 것임이 명확하다 하더라도 형사소송법상 위법한 것인지에 대해서는 판단을 달리하고 있는 것이다.[540]

제3절 | 미국의 디지털 증거 압수수색 관련 규정 및 판례의 변화

1. 디지털 증거 압수·수색 관련 규정의 변화 과정

가. 개요

구글(Google), 마이크로소프트(Microdoft) 등 거대 IT 기업을 가지고 있는 미국 역시 기술의 변화를 곧바로 법률에 반영할 수 없었기에 디지털 증거의 압수·수색과 관련하여 많은 견해 대립이 있었고, 미국 각 법원은 상반된 결론에 이르기도 했다. 미국은 이러한 법과 현실의 괴리를 판례 변경 또는 법령의 제·개정을 통해서 해결하여 왔는바, 디지털 증거의 압수·수색에 관한 규정의 개정 과정 및 경향성을 검토하기 위해서는 압수·수색 절차를 규정하고 있는 헌법, 디지털 증거와 관련된 법령의 제·개정 과정을 살펴볼 필요가 있다.[541] 미국의 디지털 증거 압수·수색에 관한 주요 규정을

540) 松田 克之·宮崎 桃子, 앞의 논문, p.63.
541) 지면 관계상 이 글에서는 논의의 범위를 미국 내의 각 주의 법령이 아닌 미연방 법령으로 한정한다.

연방 법령을 중심으로 살펴보면, 아래와 같다.

첫째, 압수·수색에 관한 일반규정으로는 미국 연방 수정헌법(약칭, "수정헌법") 제4조, 연방 형사소송규칙(Federal Rule of Criminal Procedure: 약칭 "Rule") 제41조가 있고, 위 규정은 전통적인 유체물의 압수·수색뿐만 아니라 디지털 증거의 압수·수색에도 적용된다.

둘째, 디지털 증거 수집에 관한 특별규정으로 1986년 제정된 전기통신사생활법(Electronic Communications Privacy Act, 이하, "ECPA")을 들 수 있다. ECPA는 유선, 구두 및 전자통신이 이루어지고 전송되는 동안의 정보뿐만 아니라 컴퓨터에 저장된 정보까지 그 대상으로 하여 규율하고 있다. ECPA의 Title I에는 수사 목적 감청과 관련된 감청법(The Wiretap Act),[542][543] Title II에는 인터넷의 발달로 정보통신의 중요한 부분을 차지하게 된 인터넷 서비스와 관련된 저장통신법(Stored Communications Act, 이하, "SCA"),[544] Title III에서는 전화의 송수신 번호 등[545]의 수집과 관련된 Pen/Trap법(Pen Register/Trap and Trace)[546]이 규정되어 있다.

일반적으로 수사기관이 피의자 등이 소유한 노트북, 휴대폰 등 특정 저장매체에 저장된 디지털 증거를 수집할 때는 Rule 41.이 적용되고, 인터넷 서버 등 인터넷 서비스제공자(Internet Service Provider, 이하 "ISP") 또는 통신서비스제공자(Communication Service Provider; 이하 "CSP") 등 제3자가 보관하고 있는 디지털 증거를 수집하는 경우 ECPA/SCA 등의 법률이 적용된다.

---

542) 18 U.S.C. §2510-2523.

543) 안보 목적의 감청에 관하여는 감청법이 아닌 해외정보감시법(Foreign Intelligence Surveillance Act 1978)에서 규정하고 있고(50 U.S.C. §1801-1811), 해외정보 수집 목적 가입자 통화내역 기록장치 및 발신지 추적장치와 관련한 것은 50 U.S.C. §1842, 1843에 규정되어 있다. 이 연구보고서는 수사기관의 디지털 증거 수집에 관한 것인바, 해외정보, 안보 목적 감청 등에 관한 것은 논외로 한다.

544) 18 U.S.C. §2701-2712.

545) USA Patriot Act 2001에서 전화번호 기록장치와 관련된 법률에 인터넷 통신을 포함시킴에 따라, 특정 이메일 계정에 송수신되는 이메일 계정, 컴퓨터 IP 주소 등의 수집방법도 Pen/Trap법에 포함되었다. USA Patriot Act 2001은 원래 테러방지를 위하여 4년간만 효력을 유지하는 형태의 한시적인 법으로 제정된 것이었으나, 이후까지 몇 번의 개정을 거쳐서 계속하여 효력을 유지해 온 것으로, 테러단체와의 연관성이 의심되면 법원의 영장 없이 감청이 가능하고(§206), 사전영장 없이 압수·수색(§213)이 가능하도록 하였다(이진구·김일환, "통신비밀의 보호범위와 한계에 관한 비교법적 연구 -미국의 통신비밀보호법제를 중심으로-", 『미국헌법연구』 제27권 제1호, 미국헌법학회, 2016.4, 232면.).

546) 18 U.S.C. §3121-3127.

나. 미국 수정헌법 제4조

[미국 연방 수정헌법 제4조[547]]

불합리한 수색과 압수에 대하여 신체, 주거, 서류, 물건의 안전을 확보할 국민의 권리는 침해되어서는 안 된다. 선서나 확약에 의하여 상당하다고 인정되는 이유가 있어 특별히 수색할 장소와 압수할 물건, 체포·구속할 사람을 특정한 경우를 제외하고는 영장이 발부되어서는 안 된다.

수정헌법 제4조는 국가가 개인의 주거, 신체, 물건 등을 압수·수색하기 위해서는 법관이 발부한 영장을 필요로 할 뿐만 아니라, 그 영장에 기재된 물건 등이 특정되어야 한다고 규정한 것으로, '영장주의'와 '포괄영장 금지' 원칙을 선언하고 있는 것으로 평가되고 있다.[548][549]

수정헌법 제4조는 유체물을 대상으로 한 전통적인 압수·수색은 염두에 두고 제정된 것이지만 연방대법원은 디지털 증거의 압수·수색에도 위 조항을 적용하여 위법성 여부를 판단하고 있다.

IT 기술의 발전에 따라 디지털 증거에 대한 압수·수색은 전통적인 압수·수색과는 다른 형태의 사생활 침해를 야기하였고, 이에 따라 물리적 침입을 수반하지 않는 감청 등이 미국 연방 수정헌법 제4조의 영장주의가 적용되는 영역인가에 다툼이 있었으나, 미국 연방대법원은 디지털 증거의 압수·수색에 관하여 연방 수정헌법 제4조의 해석을 변경하여 영장주의를 확대 적용해 오고 있다.[550] 디지털 증거의 압수·수색과 관련한 연방 수정헌법 제4조의 해석론 변화에 대하여는 아래에서 구체적으로 살펴보기로 한다.

---

547) The Fourth Amendment. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized(밑줄은 강조를 위하여 필자가 그은 것임, 이하 동일함).

548) 박병민·서용성, 『디지털 증거 압수·수색 개선방안에 관한 연구 -법률 개정에 관한 논의를 중심으로-』, 연구총서 2021-05, 사법정책연구원, 2021.3, 26면.

549) 수정헌법 제4조는 영장의 발부요건을 규정한 것으로, 반드시 모든 압수·수색에 있어서 영장을 발부받아야 한다는 것을 의미한다고 보기는 어렵다는 견해도 있으나, 미국의 형사실무 및 대법원 모두 압수·수색에 있어서 영장주의를 원칙으로 한다고 해석하고 있기 때문에 견해 대립의 실익은 크지 않다(백승주, "미국의 압수·수색영장 일부기각 및 압수방법 제한에 관한 실무연구 -디지털 증거를 중심으로-", 『법조』 통권 제682호, 법조협회, 2013.6, 203면).

550) 박병민·서용성, 위의 연구보고서, 26면.

다. 연방 형사소송규칙 제41조

미국 연방 형사소송규칙(Federal Rule of Criminal Procedure: 이하 "Rule") 제41조는 'Search and Seizure'라는 제목 아래 '영장'에 의한 압수·수색절차에 대하여 상세하게 규정하고 있다.

1) 압수·수색 대상에 "정보(information)" 명시, 압수방법으로 "복사(copy)" 인정

Rule41(a)(2)에서 압수·수색의 대상으로서의 '물건(property)'에 "문서(documents), 장부(books), 서류(papers) 및 그 밖의 유체물(any other tangible objects) 또는 정보(information)를 포함한다"[551]고 규정하여 디지털 정보를 압수·수색의 대상으로 명시하고 있다. 2009년 개정을 통해서 Rule 41(e)(2)(B)에서 전자적으로 저장된 정보를 대상으로 하는 영장의 경우, 정보저장매체 자체의 압수 또는 "복사(copying of electronically stored information)"를 통한 압수를 규정하여 디지털 정보가 압수·수색의 대상임을 명확히 하였고, 디지털 정보의 복사 및 분석이 압수·수색 현장이 아닌 다른 장소에서 이루어질 수 있음을 명시하였다.

2) 전화 또는 기타 신뢰할만한 전자적 방식에 의한 영장청구

수사기관이 압수·수색 영장을 청구하는 경우 법관의 앞에서 영장청구 이유 등에 대하여 진술하는 것이 원칙이다. 수사기관이 법관을 대면하여 영장을 청구하는 경우 ① 수사기관이 영장의 내용을 뒷받침하는 선서진술서(Affidavit)를 제출하면, 법관이 진술인을 출두하도록 하여 직접 심문하거나, ② 서면진술서 전부 또는 일부를 생략하고, 청구 이유 등을 진술인에게 선서하고 증언(Sworn Testimony)하도록 하거나, ③ 법원 속기사 또는 적절한 기록장치를 이용하여 증언을 녹취(Recording Testimony)하도록 하는 방식으로 진행된다.[552]

1977년 개정을 통해서 비대면 영장청구 방식으로 Rule 41(d)(3)에서 전화 또는 기타 신뢰할만한 전자적 방식(Telephonic or Other Reliable Electronic Means)을 이용한

---

551) Rule 41(a)(2)(A) "Property" includes documents, books, papers, any other tangible objects, and information.

552) Rule 41(d)(2).

영장청구가 허용되었다.[553] 전화를 통한 수색영장 청구는 위 규칙 개정 전에도 판례를 통하여 합법적인 것으로 인정되어 왔던 것인데,[554] 이를 명문화한 것이다. 위 규정은 수사기관이 법관이 부재중인 경우 법관과 의사소통이 어렵다는 이유로 영장을 발부받은 것을 회피하는 경향이 있었기 때문에 법관의 의사소통을 편리하게 하여 미리 영장을 발부받도록 하기 위하여 도입한 것으로,[555] 실제로 전화 영장 제도가 도입된 이후 영장에 의한 압수·수색이 크게 증가하였다.[556] 더 나아가 1993년 개정에서는 기록된 정보를 효율적이고 정확하게 전송하는 데 있어 팩시밀리의 정확성, 대중성 등을 고려하여 선서진술서를 팩스를 이용하여 전송하는 것도 허용하였다.[557] 위와 같은 개정은 서면에 의한 영장청구라는 형식에 얽매이기보다 전화, 팩스 등을 이용한 영장청구를 명시적으로 인정하는 등 절차의 간소화를 통해 영장 취득을 회피하는 수사기관을 견제하고, 신속하게 영장을 발부하여 증거가 은닉 또는 파괴될 위험성을 저하시켰다는데 의미가 있다.

3) 모바일 추적장치(mobile tracking device) 부착 영장

원칙적으로 치안판사(magistrate judge)는 관할구역 내에서만 압수·수색영장을 발부할 권한이 있고, 치안판사가 영장을 발부할 수 없는 합리적인 사정이 있는 경우 관할구역 내 기록을 보존하는 주 법원 판사(judge of a state court)가 압수·수색영장을 발부한다.[558] 압수물이 관할 밖에 있는 경우에도 영장 발부 당시에 관할구역에 있었던

---

553) Rule 41(d)(3).

554) 캘리포니아 항소법원은 Becker 경관이 비밀정보원으로부터 Peck이 불법적으로 마리화나를 판매하고 있다는 정보를 받아 Peck의 주거지를 압수·수색하기 전에 판사에게 전화 수색영장(Becker 경관이 판사에게 전화로 수색 장소, 이유 등을 설명하고 판사는 그 내용을 녹음하여 녹음테이프 원본, 필사본, 수색영장 원본 및 Becker가 서명한 원본의 사본이 제출됨)을 발부받아 마리화나 등을 압수하였다. 이때, Peck은 서면진술서 없이 전화영장이 발부된 것은 위헌이라는 주장을 하였으나, 법원에서 전화영장은 위헌이 아니라고 판시하였다(People v. Peck, 38 Cal.App.3d 993, 113 Cal.Rptr. 806 (1974)).

555) Committee Notes on Federal Rule of Criminal Procedure(이하, "Rules") - 1977 Amendment.

556) 1970년 캘리포니아주에서 전화수색영장을 허용하는 법 개정이 있은 후 전화 수색영장의 65%가 1시간 이내에 발부되었고, 발행된 영장의 수가 5배 증가하였다고 한다(Miller, "Telephonic Search Warrants: The San Diego Experience", 9 The Prosecutor 385, 386 (1974)(https://www.ojp.gov/ncjrs/virtual-library/abstracts/telephonic-search-warrants-san-diego-experience; 최종접속일 2023.9.14.)).

557) Notes of Advisory Committee on Rules—1993 Amendment of Rule 41.

558) Rule 41(b)(1).

경우에는 해당 지역 치안판사가 집행 관련한 영장을 발부할 수 있다.[559][560]

2006년 개정에서는 압수·수색영장을 발부할 수 있는 치안판사는 관할구역 내에서 18 U.S.C. §3117(b)[561]가 규정하는 모바일 추적장치(mobile tracking device)[562]를 설치할 수 있는 영장을 발부할 권한을 가지고 있고, 해당 영장으로 그 지방 안이나 밖 또는 그 지방의 안팎에 있는 사람 또는 물건의 이동을 추적하는 장비를 사용하는 것을 허가할 수 있다는 규정이 도입되었다.[563]

위 규정은 United States v. Karo(1984) 판결[564]에서 수사기관이 영장 없이 비퍼(beeper) 형태의 전자추적 장치를 이용하여 피의자의 집의 위치를 파악하고 집을 모니터링하면서 마약의 위치를 파악한 것이 수정헌법 제4조에 위반한 것이라는 판시를 하였으나, 당시까지 Rule 41.에는 추적장치를 영장을 발부할 수 있는 절차적 지침이 없었기에 추적장치 부착 영장의 근거를 마련한 것이다.[565]

4) 전자영장제도

미국은 2006년 개정을 통해 Rule 41(e)에 치안판사가 '신뢰할 수 있는 전자수단'을 사용하여 압수·수색영장을 발부할 수 있도록 하여, '전자 압수·수색영장'을 도입하였다. 2011년 규칙 개정을 통해, 압수·수색영장 외에 체포영장, 소환장(summons)도 전자적 방법에 따른 발부가 가능하게 되면서 Rule 4.1.에서 통합하여 규정하게 되었다.[566]

---

559) Rule 41(b)(2).

560) 다만, 테러행위와 관련된 활동이 이루어지는 지역 관할 내의 판사는 관할과 무관하게 그 지역 안이나 밖에 있는 사람 또는 물건에 대하여 압수·수색영장을 발부할 수 있다(Rule 41(b)(3)).

561) 18 U.S.C. §3117. Mobile tracking devices
(b) Definition.-As used in this section, the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or object. 이때 추적장치는 사람이나 물체의 움직임을 추적할 수 있는 전자 또는 기계장치를 의미하는 것으로 모바일 추적장치(Mobile tracking devices)를 의미한다.

562) Rule 41(a)(2)(E).

563) Rule 41.(b)(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both;

564) 연방대법원은 수사기관이 피의자(Karo)가 구입할 것으로 예상되는 마약제조에 사용되는 화학약품 통에 미리 전자추적 장치를 설치하고 Karo가 그 화학약품 통을 구입하자 위치추적 장치를 통하여 그의 주거지 등을 파악한 다음 주거지 내에 있는 마약의 존재를 파악한 것은 몰래 개인의 주거지에 침입한 것과 같으므로 수정헌법 제4조 위반이라고 판시하였다(United States v. Karo, 468 U.S. 705 (1984)).

565) Committee Notes on Rules—2006 Amendment of Rule 41.

전자영장이 발부되기 위해서는 ① 선서 하에 증언이 이루어져야 하고(Taking Testimony Under Oath),[567] ② 증언과 증거물에 대하여 기록이 만들어져야 하며(Creating a Record of the Testimony and Exhibits),[568] ③ 영장 원본 초안(배포본 포함)과 복제된 원본이 준비되어야 하고(Preparing a Proposed Duplicate Original of a Warrant),[569] 영장청구인은 부본 초안을 작성하여 법관 앞에서 그대로 읽거나 다른 방법으로 전달하여야 한다.[570] ④ 영장청구인이 부본 초안의 내용을 읽는 경우 법관은 그 내용으로 영장 원본을 작성하여야 한다. 이때 영장청구인이 신뢰할만한 전자적 수단으로 내용을 송부하는 경우 판사가 수령한 송신문을 원본으로 본다.[571] ⑤ 법관은 필요한 경우 영장을 수정할 수 있는데, 영장을 수정(Modification)한 경우 수정된 영장을 영장청구인에게 전자적 수단으로 전달하고, 그 원본을 소송기록에 보관하고, 영장청구인에게 부본 초안을 변경하도록 한다.[572] ⑥ 법관은 영장을 발부할 때 영장 원본에 서명을 하고, 발부 일자 및 시간을 기재하여 영장청구인에게 전자적 수단으로 이를 전달하거나, 영장청구인에게 부본에 법관의 이름을 기재하고 발부 날짜와 시간을 기입하도록 한다.[573] 이때, 수사기관이 전자영장을 전송을 받은 경우 그 내용 자체가 원본이 되는 것이다.[574] 이러한 전자적 방법에 의한 영장 발부가 비합리적이라는 증거항변은 원칙적으로 허용되지 않는다.[575]

---

566) Rule 4.1은 전화 기타 전자적 수단에 의한 영장 및 소환장 신청 및 발부절차를 하나로 통합하기로 하기 위하여 2011년 4월 26일에 개정되어 같은 해 12월 1일부터 시행되었다. 위 규정에 따라 영장청구권자는 압수·수색영장뿐만 아니라 체포영장까지도 전자 기타 신뢰할 만한 전자적 수단으로 영장을 청구할 수 있게 되었다. 즉, 이러한 전자적 방식에 의한 영장 등의 확대는 현대기술의 발전으로 영장청구권자의 법관에 대한 접근이 쉬워졌기 때문에 사전영장 없이 강제처분을 할 필요성이 줄어들었다는 인식에 기초한 것이다(Committee Notes on Rules-2011 Amendment).

567) Rule 4.1(b)(1).

568) Rule 4.1(b)(2).

569) 영장의 복제원본(duplicate original)이라 함은 서명을 포함한 영장 원본의 요소를 모두 포함한 것으로 사실상 원본과 구별이 되지 않는다. 이에 대하여 '중복원본'이라고 번역하기도 한다(손지영·김주석, 『압수수색 절차의 개선방안에 관한 연구』, 연구총서 2016-07, 사법정책연구원, 2016.3, 96면).

570) Rule 4.1(b)(3).

571) Rule 4.1(b)(4).

572) Rule 4.1(b)(5).

573) Rule 4.1(b)(6).

574) Rule 4.1(b)(4).

575) Rule 4.1(c).

5) 영장 집행기간 제한의 특칙

위치추적 장치(Tracking-Device) 부착영장[576]을 제외하고, 압수·수색영장은 압수·수색 대상 등이 특정(specific)되어야 하고, 영장을 반환받은 법관을 지정하여야 한다.[577] 압수·수색영장은 원칙적으로 발부한 때로부터 14일 이내에 집행되어야 하고, 영장 집행 후 지정된 법관에게 영장을 반환하여야 한다.[578]

2009년 개정을 통하여, Rule 41(e)(2)(B)에 전자정보 압수·수색영장의 집행절차에 대하여는 따로 특칙을 마련하였다. 저장매체 또는 정보에 대한 압수·수색 영장은 영장에 달리 특정되어 있지 않다면 저장매체 또는 정보의 사후분석 권한을 포함하도록 하여, 저장매체 자체의 압수를 원칙적인 것으로 인정하면서 저장매체에 저장된 정보의 압수 또는 "복사(copy)"도 가능하도록 명시하였다. 또한, 14일의 영장 집행기간의 제한은 저장매체 또는 정보의 압수 또는 복사에 적용되는 것으로, 현장 외에서 복제 및 사후분석(off-site copying or review)에는 적용되지 않는다고 명시하였다.[579] 따라서 영장을 발부한 날로부터 14일이 경과한 경우에도 계속하여 현장 외에서 저장매체 또는 정보의 사후분석은 허용된다. 저장매체는 대량의 정보를 저장하고 있고, 암호화되어 있을 수도 있어 현장에서 이를 수색하고 분석을 완료한다는 것은 비효율적일 뿐만 아니라 사실상 불가능함을 반영한 규정이라고 할 수 있다.[580]

위 규정은 압수·수색현장에서 정보저장매체 자체를 압수하거나 이를 복제하고, 그 후 압수·수색현장 외(off-site)에서 정보 분석을 통해서 영장에서 특정한 정보를 압수할 수 있도록 2단계에 걸친 절차(two-step process)로 구분한 것이라고 할 수 있다.

위 규정 이전에도 일반적으로 현장에서 발견된 저장매체를 일괄적으로 압수한 다음, 압수·수색 현장이 아닌 다른 장소에서 저장매체 내의 내용을 분석하였고, 법원 역시 압수·수색현장이 아닌 별도의 디지털 증거분석실에서 이를 분석하는 것을 승인

---

576) 위치추적 장치 부착 영장에 대하여는 Rule 41(e)(2)(C)에서 별도로 규정하고 있다. 그 내용은 추적할 사람이나 물건을 특정하고 영장을 반환받은 법관을 지정하며, 원칙적으로 영장이 발부된 날로부터 45일을 초과할 수 없다. 다만, 법관은 정당한 사유가 있는 경우 45일을 초과하지 않는 합당한 기간 동안 1회 연장을 승인할 수 있는데, 이때 10일 이내의 지정된 시간 내에 보증서에 의해 설치를 완료하여야 한다.

577) Rule 41(e)(2)(A).

578) Rule 41(e)(2)(A).

579) Rule 41(e)(2)(B).

580) 박병민·서용성, 앞의 연구보고서, 58면

해 왔다.[581] 그러나 이러한 절차에 대하여는 United States v. Hill 판결(2006)[582]을 비롯하여 많은 비판이 있었기 때문에 현재 미국 법무부는 영장을 신청할 때 선서진술서(affidavit)에 현장 외에서 증거분석이 필요한 이유를 따로 기재하도록 권고하고 있다.[583][584]

6) 영장의 집행 및 집행 후 절차

영장을 집행한 수사관은 영장을 집행한 일자, 시간을 정확히 기재하여야 하고,[585] 다른 수사관과 피압수자의 참여하에 압수물 목록(inventory of any property seized)을 작성한 후 확인을 받아야 한다. 참여 수사관과 피압수자 둘 중 한 명이라도 참여하지 않은 경우 수사관은 적어도 다른 신뢰할 수 있는 사람의 참여하에 압수물 목록을 작성하고 이를 확인받아야 한다.[586] 위 규정을 피압수자의 참여권을 인정하는 근거규정이라고 보는 견해도 있으나, 압수된 저장매체의 이미징 및 정보에 대한 분석은 별도의 장소에서 이루어지고 이때에는 피압수자의 참여권을 인정하고 있지 않은 점 등에 비추어 위 규정만으로 미국이 명문으로 피압수자의 참여권을 인정하고 있다고 보기는 어렵다.[587]

---

581) 조성훈, 『역외 전자정보 압수·수색 연구』, 박영사, 2020, 78면,

582) United States v. Hill, 459 F.3d 966, 976(9th Cir. 2006).

583) 미국 법무부는 Hill 판결에 대하여 모든 컴퓨터 압수·수색의 경우 저장매체의 이미징과 삭제 등 포렌식 작업이 필요하기 때문에 이러한 내용을 선서진술서에 기재하지 않았다고 하여 수정헌법 4조에 위반이라는 것에 대하여는 의심스럽다(doubtful)고 하는바, 위 판결에 찬성하는 입장은 아닌 것으로 보인다(U.S. Depart of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"(Third edition)(이하, "미국 연방 법무부 매뉴얼"이라고 함), 2009, 78면).

584) 다만, Rule 41(e)(2)(B)의 개정으로 저장매체 압수·수색영장에는 특별한 사정이 없는 한 사후분석 권한도 포함된다고 규정하고 있어 수사기관에게 현장 외 분석이 필요한 이유를 소명하도록 한 United States v. Hill 판결의 취지는 반감되었다(박병민·서용성, 위의 연구보고서, 87면).

585) Rule 41(f)(A).

586) Rule 41(f)(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. (이하 생략)

587) 원칙적으로 저장매체 자체를 현장에서 압수하고 그 압수물목록에도 압수한 정보가 아니라 압수한 저장매체를 기재하도록 하고 있다는 점, 특별한 사정이 없는 한 분석은 압수·수색현장이 아닌 별도의 장소에서 하는 것이 인정되는 점, 압수·수색 현장 외 이미징 또는 분석 시에 피압수자 참여권을 인정하는 규정이 없는 점에 비추어 분석과정에서의 피압수자의 참여권을 명문으로 인정하고 있다고 보기 어렵다(김범식, "영·미의 디지털 증거 압수·수색에 관한 소고", 『형사법의 신동향』 통권 제45호, 대검찰청, 2014.12, 180면).

한편, 2009년 규칙 개정에서는 정보저장매체 또는 디지털 증거의 압수 또는 복사의 경우 압수물목록에는 압수 또는 복사되는 "정보저장매체 그 자체"를 기재하는 것으로 충분하고, 수사관은 압수 또는 복제된 디지털 정보의 복사본을 보유할 수 있도록 하였다.[588] 즉, 압수·수색 대상을 정보(information)라고 보는 경우, 압수된 정보 내용 자체를 압수물 목록에 기재하게 할 수도 있으나, 현장에서 압수한 디지털 정보를 기록하게 하는 경우 정보의 대량성 등에 비추어 실용적이지 않다는 점을 고려한 규정이라고 할 수 있다.[589] 이것은 압수된 정보를 압수목록에 나열하도록 요구하는 우리 대법원 판례와는 달리 실용성, 현실성을 강조한 것이라고 볼 수 있다.[590]

7) 원격지 압수·수색 영장 도입

2016년 개정을 통하여 Rule 41(b)(6)에 특정한 상황에서 전자정보저장매체의 압수·수색영장에 대하여 "원격지 압수·수색영장"을 도입하였다.[591] 범죄와 관련된 활동이 발생한 관할지역 내에서 영장 발부권한을 가진 법관은 '(A) 저장매체 또는 정보의 위치가 기술적 수단에 의하여 숨겨져 있는 경우, (B) 미국 연방법 제18편 제1030조(a)(5)를 위반하여 봇넷의 생성 및 제어 등 인터넷에 악성 프로그램을 의도적으로 유포하는 유형의 범죄[592]를 수사하는 경우 관할 밖에 있는 정보저장매체에 원격으로 접근(remote access)하여 수색하거나 전자정보를 복사 또는 압수할 수 있는 영장을 발부' 할 수 있도록 하고 있다. 위와 같이 원격지에서 접속할 수 있는 권한이 부여된 디지털 영장을 "NIT(Network Investigatory Techniques) 영장"이라고 한다.[593]

아동포르노 사이트와 같이 범죄를 목적으로 하는 사이트의 경우 수사기관의 추적을 피하기 위하여 주로 다크 웹(Dark Web)[594]을 이용하고 있다. Rule 41(b)(6) 규정이

---

588) Rule 41(f)(1)(B).

589) Committee Notes on Rules-2009 Amendment of Rule 41.

590) 디지털 증거의 압수의 경우 압수물 목록에 개별적인 디지털 정보 파일을 전부 기재하는 것이 아니라, 압수·수색의 대상이 된 "정보저장매체"만을 기재할 수 있도록 하여 압수물 목록의 기재는 우리보다 특정의 정도를 완화하였다.

591) Rule 41.(b)(6).

592) 18 U.S.C. §1030(a)(5).

593) MJEB, 『A Guide for Ninth Circuit Magistrate Judges When Reviewing Government Applications to Obtain Electronic Information』(3rd Edition), 2017, 26면.

594) '다크 웹(Dark web)'이란, 인터넷을 사용하지만, 이에 접속하기 위해서 기존의 웹 브라우저로는 접근할 수 없고, 특정한 프로그램을 사용해야 하는 웹을 의미하는 것으로, 일반적인 방법으로 접속자나 서버를 확인할 수 없기 때문에 사이버상에서 범죄에 활용된다. 인터넷상에서 수사기관

도입되기 이전에 수사기관이 다크 웹 운영자의 IP 주소를 알아내기 위해 감시 소프트웨어를 사용하여 웹사이트에 접근하는 것이 치안판사 등이 원칙적으로 관할 내의 범죄에 대해서만 영장을 발부할 수 있도록 한 Rule 41(b)를 위반한 것인지 여부가 지속적으로 문제되었는데, 2016년에 이를 입법적으로 해결한 것이다.[595]

한편, 2016년 개정에서는 Rule 41(f)(1)(C) 후단에서 전자정보저장매체를 검색하여 저장된 정보를 압수 또는 복제하기 위하여 원격지에서 접속할 수 있는 영장을 집행하는 경우에도, 수사관은 피압수자 또는 복제 또는 압수된 정보의 소유자(who possessed the information that was seized or copied)에게 영장 사본(a copy of the warrant)과 영수증(receipt)을 송달하기 위한 합리적인 노력을 하여야 하고, 이때 송달의 방법은 전자적 수단을 포함하여 피압수자에게 합리적으로 도달 가능한 모든 수단을 이용할 수 있다고 규정하였다.[596] 원격지 압수·수색영장은 수사기관이 직접 피압수자와 물리적으로 대면하여 영장을 집행하는 것이 아니기 때문에 영장 사본 및 영수증 교부가 일반적인 물건의 압수와 다른 방식일 수밖에 없음을 인정한 것이다. 영장과 압수목록 사본(a copy of the inventory)을 법관에게 반환할 때에도 신뢰할만한 전자적 수단을 이용할 수 있다.[597]

라. 전기통신사생활법(Electronic Communications Private Act 1986)

1) 개요

전기통신사생활법(Electronic Communications Privacy Act of 1986, 이하 "ECPA"라고 함)[598] 제정당시는 인터넷 또는 모바일 장치가 보편화되기 이전으로 정보통신과 관련된 과학기술의 발전이 법률에 반영되지 않았기 때문에 ECPA는 제정 이후 지금까지 여러 차례 개정되었다.[599]

의 트래픽 분석, 속성 정보 분석 등을 차단하여 범죄자의 신원 또는 위치를 파악할 수 없도록 하기 위하여 사용된다(네이버 지식백과, "다크 웹"(https://terms.naver.com/entry.naver?docId=3581037&cid=59088&categoryId=59096; 최종접속일 2023.9.14.)).

595) 박병민·서용성, 앞의 연구보고서, 56면

596) Rule 41(f)(1)(C).

597) Rule 41(f)(1)(D).

598) ECPA는 1986년 연방 감청 및 전자 감청(electronic eavesdropping) 조항을 확대 및 개정하기 위하여 제정된 것으로, 도청법 개정안을 포함하여, SCA, PEN/REGISTER법이 포함되었다.

599) ECPA는 1986년 제정 이후 1994년, 2001년, 2006년 및 2008년, 2018년에 주요 개정이 있었다(Electr

ECPA는 ① 전자통신을 가로챌 수 없도록 하는 '감청법(Wiretap Act, Title I)', ② 통신서비스제공자가 저장한 파일과 가입자의 이름, 청구 정보 및 IP, 주소와 같은 가입자 정보에 관한 '저장통신법(Stored Communications Act, Title II, 이하 "SCA")',[600] ③ 특정 전화기에서 발신 전화를 건 번호를 기록하는 장치 및 특정 전화기로 걸려오는 전화번호를 기록하는 장치 등에 관한 'Pen/Trap법(Pen Register/Trap and Trace Devices, Title III)' 3가지 파트로 구성되어 있다.

ECPA는 주로 전화, 정보통신서비스 이용자에 대한 정보를 수집하는 방법에 대하여 규정하고 있는 것으로, 피압수자가 정보주체가 아닌 ISP/CSP로 제3자 보관 디지털 증거 수집방법에 관한 것이다. 한편, 미국 정부가 해외에 저장된 정보를 SCA에 따라 수집할 수 있는지 여부가 문제되자 2018년 '합법적 해외 데이터 활용의 명확화 법률(Clarifying Lawful Overseas Use of Data Act: 이하, "CLOUD ACT")'[601]에서 역외 압수·수색 규정을 마련하였다.

2) 내용

가) 내용(contents)을 제외한 가입자 정보

ECPA/SCA는 정보의 종류에 따라서 수사기관의 정보 수집방법을 달리 정하고 있다. 구체적으로 살펴보면, 가입자의 성명, 주소, 전화기록(착발신 시간 및 통화시간), 제공된 서비스의 유형과 기간, 지급수단(신용카드 또는 은행계좌 번호 포함) 등을 포함하는 '기본 가입자 정보(Basic Subscriber Records)'[602]의 경우 수사기관이 서비스제공자에게 제출요청(subpoena)을 통해서 정보를 제공받을 수 있다.[603] 이때, 수사기관은 정보

---

onic Privacy Information Center(전자개인정보보호센터, 이하 "EPIC") 홈페이지, "Electronic Communications Privacy Act (ECPA)"(https://epic.org/ecpa/; 최종접속일 2023.9.14.) 참조).

600) 저장통신법(SCA)은 "전송 중인 아닌" 저장된 미사용 통신에 대한 접근(acess)에 대하여 규정하고 있다. 즉, 전자 통신 서비스가 제공되는 시설에 의도적으로 접속하여 해당 시스템 서버에 있는 유선 또는 전자 통신에 대하여 무단으로 접근, 변경하는 것을 불법으로 규정하고 있다. 다만, SCA는 법집행기관이 미사용 저장통신에 대하여 압수할 수 있는 예외 등을 규정하고 있다(EPIC, 홈페이지, "Electronic Communications Privacy Act (ECPA)"(https://epic.org/ecpa/; 최종접속일 2023.9.14.)).

601) 조성훈, 앞의 책, 33면.

602) 이것은 우리나라 전기통신사업법 제83조 제3항에 규정된 '통신자료'와 그 내용이 유사하다(18 U.S.C. §2703(c)(2)).

603) 물론 기본 가입자 정보를 법원의 명령(court order) 또는 영장(warrant)을 이용하여 수집할 수도 있다.

를 제공받은 후에도 정보주체에게 그 사실을 통지할 의무는 없다.[604]

거래기록, 로그기록, 가입자와 교신한 이메일 주소 등을 의미하는 '기타 가입자 정보(Other Subscriber Information)'[605]의 경우, 수사기관은 '법원의 명령(court order)' 이상의 근거가 있어야 정보를 수집할 수 있다. '기타 가입자 정보'에 관한 법원의 명령을 받기 위해서는 해당 정보가 진행 중인 범죄 수사와 관련이 되고, 중요하다고 믿을만한 합리적 근거가 있음을 구체적이고 명확하게 제시하여야 한다.[606]

나) 내용(contents) 정보

정보통신의 내용과 관련하여서는 180일을 기준으로 그 수집절차가 달라진다.

먼저, 수사기관이 180일 미만 저장된 정보를 수집하는 경우에는 '상당한 이유(Probable Cause)'를 요건으로 하는 영장을 발부받아야 하고,[607] 이때 수사기관은 가입자에게 영장 발부 사실을 통지할 필요가 없다.[608] 그리고 법원은 서비스제공자에게 특정 이메일의 전체 내용을 제출할 것을 요구하지만, 영장의 집행에 있어서 수사기관에게 영장에 기재된 특정 정보만 수색하도록 그 범위를 제한한다.[609]

반면, 180일 이상 저장된 정보의 경우 대배심의 제출명령(grand jury subpoena)이나 법원의 명령(court order)을 이용할 수 있다.[610] 수사기관은 이 경우 가입자에게 원칙적으로 법원 명령의 존재 등을 사전통지하여야 하지만, 그 통지는 법원의 결정을 받아 90일 동안 유예가 가능하고, 그 기간을 갱신할 수 있다.[611] ① 개인의 생명, 신체의 안전에 대한 우려가 있는 경우, ② 도주 및 증거인멸·변조, 잠재적 증인에 대한 위협 등의 우려가 있는 경우, ③ 수사를 위태롭게 하거나, 재판을 부당하게 지연시킬 염려가 있는 경우에는 통지를 유예할 수 있다.[612]

---

604) 18 U.S.C. §2703(c)(3).
605) 이것은 우리나라 「통신비밀보호법」 제2조 제11호에 규정된 '통신사실확인자료'와 그 내용이 유사하다.
606) 18 U.S.C. §2703(d) 전단.
607) 18 U.S.C. §2703(a) 전단.
608) 18 U.S.C. §2703(b)(1)(A).
609) MJEB, 『A Guide for Ninth Circuit Magistrate Judges When Reviewing Government Applications to Obtain Electronic Information』(3rd Edition), 2017, 11면.
610) 18 U.S.C. §2703(a), §2705.
611) 18 U.S.C. §2705(a) .
612) 18 U.S.C. §2705(a)(1),(2).

연방대법원은 현재까지 SCA의 적용을 받는 이메일 등 저장된 전자통신이 수정헌법 제4조의 사생활보호에 대한 합리적인 기대를 가지는 대상인지 여부에 관하여 명확히 판단하지 않고 있다.[613] 다만, 2010년 제6 연방항소법원이 United States. v. Warshak 판결(2010)[614]에서 사용자는 이메일에 대하여 사생활에 대한 합리적인 기대를 가지고 있으므로, 수사기관이 그 보관기간을 고려하지 않은 채 이메일의 내용을 영장에 의하지 않고 수집한 것이 수정헌법 제4조 위반이라고 판시한 이후부터, 연방 검사는 180일 이상 보관된 이메일의 내용을 압수·수색할 때에도 대배심의 제출명령 또는 법원의 명령보다는 엄격한 요건인 '상당한 근거(probable cause)'를 요구하지만, 수사기관이 가입자에게 사전통지를 할 필요가 없는 Rule 41.에 규정된 압수·수색영장(warrant)을 선호한다고 한다.[615] 이 경우 수사기관은 대부분 서비스제공자가 가입자에게 그 내역을 통지하는 것을 배제하는 명령을 함께 청구한다.[616]

수사기관이 수집하고자 하는 정보의 형태에 따라 영장의 필요여부 및 근거법령이 아래와 같이 달라진다.

[표 3-3] 디지털 정보 유형·저장기간별 정보 수집방법 및 근거법령

통신 유형	수사기관 접근방법	관련 법령
전송 중인 이메일 (email in transit)	영장(Warrant)	18 U.S.C. §2516
개인 컴퓨터에 저장된 이메일 (email in storage on home computer)	영장(Warrant)	수정 헌법 제4조
원격 저장소에 저장된 오픈된 이메일 (email in remote storage, opened)	소환장(Subpoena)	18 U.S.C. §2703
원격 저장소에 180일 미만 저장된 오픈되지 않은 이메일 (email in remote storage, unopened, stored for 180 days or less)	영장(Warrant)	18 U.S.C. §2703
원격 저장소에 180일 이상 저장된 오픈되지 않은 이메일 (email in remote storage, unopened, stored for more than 180 days)	소환장(Subpoena)	18 U.S.C. §2703

* 출처 : EPIC 홈페이지, "Electronic Communications Privacy Act (ECPA)"(https://epic.org/ecpa/; 최종접속일 2023.9.14.).

613) EPIC 홈페이지, "Electronic Communications Privacy Act (ECPA)"(https://epic.org/ecpa/; 최종접속일 2023.9.14.).

614) U.S. v. Warshak, 631 F.3d. 266 (6th Cir. 2010).

615) MJEB, 『A Guide for Ninth Circuit Magistrate Judges When Reviewing Government Applications to Obtain Electronic Information』(3rd Edition), 2017, 3면.

616) 대부분의 정보통신서비스제공자는 계약상 가입자에게 영장 집행 사실을 통지할 의무가 있는데, 수사기관이 제출명령(subpoena), 법원명령(court order) 또는 영장(warrant)에 의해 정보를 수집하면서 ① 생명, 신체의 안전을 해할 우려, ② 도주 및 증거인멸 우려(잠재적 증인 위협 포함), ③ 재판 지연 염려 등이 있다고 소명한 경우 법원은 상당한 기간 동안 정보통신서비스제공자에게 영장 집행 사실을 통지하지 않도록 명할 수 있다(18 U.S.C. §2705(b)).

다) 증거 보전요청(Requirement To Preserve Evidence)

ECPA에는 "유선 또는 전기통신서비스제공자, 원격 컴퓨팅서비스제공자(이하, "서비스제공자 등")는 수사기관이 요청하면 법원의 명령 등이 발부될 때까지 90일 동안 증거를 보전하기 위한 조치를 취하여야 하고, 수사기관의 추가적인 요청이 있는 경우 위 보전기간은 90일간 연장할 수 있다"[617]고 하여 증거의 보전요청(Requirement To Preserve Evidence)에 관하여 규정하고 있다. 서비스제공자가 위와 같은 보전명령에 불응한 경우 손해배상청구 등 민사적 제재도 가능하다.[618]

이때 증거보전의 대상은 이미 이루어진 정보통신에 한정되고, 장래의 것은 그 대상이 아니다.[619] 주로 ① 특정한 계정, 그 계정과 연관된 계정에 의해 저장된 일체의 통신이나, 파일의 내용, 이메일 주소 및 IP 주소의 발신지 및 송신지(목적지) 같은 통신이나 파일과 연관된 정보 일체, ② 특정 계정 및 그 관련된 계정의 모든 기록 및 기타 정보가 보전요청의 대상이 된다.[620]

특히, 2018년 시행된 클라우드법(CLOUD Act)[621]에 따라, 서비스제공자는 통신, 기록 등 정보의 저장 위치에 관계 없이(국내 또는 국외 불문) 보유(possession), 보존(custody), 관리(control)하고 있는 통신정보를 '보전(preserve)', 복제(backup) 또는 제공(disclose)하도록 하는 의무규정을 두고 있는바,[622] 역외에 저장된 정보까지 보전 및 압수할 법률적 근거가 마련되어 있다.

이때, 수사기관은 다른 법률에 따라 가입자 등에게 통지의무가 없고, 증거 파괴 우려 등의 사유가 있는 경우[623] 보전명령을 받은 서비스제공자에게 적당한 기간을 정하여 증거보전명령을 발령받은 사실을 가입자 등에게 통지하지 못하도록 강제함으로써 비밀을 유지하게 할 수 있다.[624] 이러한 비밀유지명령을 위반한 경우 민사적

---

617) 18 U.S.C. §2703(f).
618) 18 U.S.C. §2707(e).
619) 장래의 통신 등에 대한 자료는 전자감시법률(the electronic surveillance statutes)에 근거하여야 한다.
620) 송규영, "해외 디지털 증거의 확보 -관할권의 확정 및 디지털 증거 보존제도의 필요성을 중심으로-", 『저스티스』 통권 제173호, 한국법학원, 2019.8, 210면.
621) 송규영, 위의 논문 193면.
622) 18 U.S.C. §2713.
623) 개인의 생명 또는 신체의 안전을 위협하는 행위, 도주, 잠재적 증인에 대한 협박, 조사를 심각하게 위태롭게 하거나 재판을 부당하게 지연시킬 수 있는 경우 통지를 하지 않도록 할 수 있다(18 U.S.C. §2705 (2)).

제재가 가능하다.[625] 통신서비스제공자 등이 보관한 정보의 경우, 해당 사업자의 내부적 규정에 따라 언제든지 삭제될 수 있기 때문에 압수·수색영장 청구 이전에 위와 같은 보전요청을 통하여 증거를 확보할 수 있는 단계를 마련한 것이다. 이것은 EU 사이버범죄협약에 따른 입법이기도 하다.

마. Pen/Trap법

Pen/Trap법은 전화번호 기록장치(Pen Register/Trap and Trace)를 통한 전화번호를 수집하는 것을 내용으로 한다. 수사기관이 특정 전화에서 송수신된 전화번호를 수집하려면 대상 전화에 '전화번호 기록장치'인 Pen Register와 Trap and Trace를 설치해야 한다. 이때, 'Pen Register'는 특정 전화(예를 들면 A)에서 발신한(outgoing) 모든 전화번호를 기록하는 장치이고,[626] Trap and Trace는 특정 전화(A)에서 수신한(incoming) 모든 전화번호를 수집하는 장치이다.[627]

미국 애국법(The USA Patriot Act of 2001)에 따라 전화번호 기록장치 관련 법률에 인터넷 통신을 포함시키게 되면서 수사기관은 Pen/Trap법에 근거하여 특정 이메일 계정에 송수신되는 컴퓨터의 인터넷 주소, 이메일 계정 등을 수집할 수 있게 되었다.[628] 다만, 이메일의 제목은 내용이 포함되어 있어 위 법에 따라서 수집할 수 없다.[629]

바. 감청법(The Wiretap Act)

1) 개요

감청은 실시간으로 이루어지는 통신의 내용을 감시하는 것으로, 법원의 명령 등 법률이 정한 사유가 없는 경우 누구도 구두 대화, 유무선 통신에 개입하거나 그 내용을 취득 또는 이용할 수 없다.[630]

---

624) 18 U.S.C. §2705(2).
625) 18 U.S.C. §2705(2).
626) 18 U.S.C. §3127(3)
627) 18 U.S.C. §2705(4)
628) 18 U.S.C. §2705(3),(4).
629) EPIC 홈페이지, "Electronic Communications Privacy Act (ECPA)"(https://epic.org/ecpa/; 최종접속일 2023.9.14.).
630) 18 U.S.C. §2511.

예외적으로 ① 18 U.S.C. §2518에서 정한 법원의 명령이 있는 경우, ② 당사자가 적법하게 동의한(lawful consent) 경우, ③ 통신서비스제공자가 자신의 권리 또는 재산을 보호하기 위한 경우, ④ 컴퓨터의 불법적 침입을 막기 위한 경우, ⑤ 서비스제공자가 우연히 얻게 된 범죄 증거인 경우, ⑥ 일반 공중이 접근할 수 있는 경우 등과 같이 법률이 허용한 경우에만 감청이 허용된다.[631]

2) 감청허가의 요건

수사기관은 ① 18 U.S.C. §2516(1)에 열거된 중범죄,[632] 전자통신에 관한 연방 중범죄를 저지르고 있거나 저지르려 한다고 믿을만한 상당한 이유가 있고, ② 범행과 관련한 특정 통신의 내용 등을 수사기관이 확보할 수 있으며, ③ 정상적인 수사절차로는 수사목적을 달성할 수 없거나 없을 것이라는 합리적인 이유(보충성)가 있고, 해당 통신이 개입되는 장소, 시설이 범행 또는 범인과 관련이 되었다는 상당한 이유가 있음을 소명하여 법원으로부터 감청허가명령을 받을 수 있다.[633][634]

3) 긴급감청 및 감청 녹음물의 반환

누군가의 즉각적인 살인 또는 중상해의 위험, 국가 안보이익을 위협하는 음모활동, 조직범죄의 특징적인 음모활동 등 긴급성이 인정되는 경우 법무부 장관 등은 법원의 명령이 없이도 감청할 수 있다.[635] 다만, 48시간 이내에 사후 허가를 청구하여야 하고, 사후 허가를 받지 못한 경우 즉시 중단해야 하고, 감청 허가 명령이 없는 경우에는 감청 목적의 통신을 획득하였거나 사후 허가를 거부당한 때 즉시 중단하여야 한다.[636]

---

631) 18 U.S.C. §2511(2),(3).

632) 이때, 중범죄란 살인, 납치, 도박, 강도, 뇌물 수수, 강탈, 마약 거래, 마리화나 또는 기타 위험한 약물 또는 기타 생명에 위험한 범죄 등을 의미한다.

633) 18 U.S.C. §2511(3).

634) 감청 허가 명령은 '감청 대상자, 감청 권한이 부여된 통신 시설의 특성 및 위치(장소), 감청 대상 통신 유형에 대한 설명 및 범죄 관련성, 감청기관 및 승인권자, 감청 기간 및 지속 여부' 등이 포함되어 있어야 한다(18 U.S.C. §2511(4)).

635) 18 U.S.C. §2511(7)(a).

636) 18 U.S.C. §2511(7)(b).

사. 클라우드법(CLOUD ACT)

미국 정부가 정보통신서비스제공자가 해외에 저장한 정보를 SCA에 따라 요구할 수 있는지 여부가 문제된 Microsoft 사건[637]에서, 제2연방 항소법원이 수사기관이 영장을 발부받아 정보통신서비스제공업체로부터 180일 이내에 보관된 정보의 내용을 압수할 수 있음을 규정한 18 U.S.C. §2703 규정이 미국 영토 밖인 아일랜드 더블린에 저장된 정보의 공개를 허용한 규정이 아니라고 판시한 바 있다. 연방정부가 위와 같은 위 판결에 대하여 전원합의체 재심리를 요청하였으나 제2 연방항소법원이 이를 거부하였다.[638][639]

미국 정부는 위 연방항소법원 판결 이후 2018. 3. 23. 수사기관이 정보통신서비스업체가 소유, 소지 또는 관리하는 정보에 대하여 저장장소를 불문하고 제공요청을 할 수 있도록 하는 내용으로 '저장통신법(SCA)'을 개정하는 '합법적 해외 데이터 활용의 명확화 법률(CLOUD ACT)'[640]을 제정하여 역외 압수·수색의 허용문제를 입법적으로 해결하였다. 위 법률에 따라 신설된 18 U.S.C. §2713은 "전기통신서비스제공자 또는 원격컴퓨팅서비스제공자는 해당 통신 또는 정보가 미국 내에서 저장되어 있는지 여부와 관계없이, 그가 소유, 소지 또는 관리하는 통신의 내용과 가입자 관련 정보를 보존, 백업 또는 공개할 법적 의무를 준수하여야 한다"[641]고 규정하여, 디지털 증거의 역외 압수·수색을 입법을 통해 허용하였다.

---

637) 미국 정부가 요청한 정보는 마이크로소프트사의 아일랜드 데이터 저장소에 있었기 때문에 마이크로소프트사는 해당 전자통신에 대한 압수·수색이 데이터 저장소인 아일랜드의 관할권에서 발생하기 때문에 SCA의 부적절한 역외 적용이라고 주장하였고, 제2 연방항소법원도 같은 취지로 판단하였다(In the Matter of a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016)).

638) 2017 WL 362765 (2d Cir. Jan. 24, 2017).

639) 연방정부는 연방대법원에 상고하였고 상고 심리 중에 아래와 같이 SCA에 대한 개정이 이루어져서 연방대법원은 소송의 이익이 없다는 이유로 위 사건을 파기환송하였다(U.S. v. Microsoft Corp., 138 S. Ct. 1186 (2018)).

640) 조성훈, 앞의 책, 33면.

641) 18 U.S.C. §2713.

2. 디지털 증거 압수·수색과 관련된 주요 판례의 변화 과정

가. 개요

최근 급격하게 발전한 기술은 수사기관이 범죄수사 분야에서 도청, 모바일 위치 추적장치 부착 등 새로운 유형의 증거수집을 가능하게 하였고, 이로 인해 수사과정에서 국가에 의한 사생활 침해는 더욱 심해졌고, 수사기관이 사용하는 새로운 증거수집 방법이 수정헌법 제4조의 영장주의가 적용되는 압수·수색에 해당하는지 여부가 문제되었다.

종래 미국 연방대법원은 헌법의 보호대상이 된 특정 장소에 '물리적으로 침입(physical intrusion)하거나 재산(property)에 대한 침범(trespass)이 있는 경우'에 수정헌법 제4조에 따라 영장이 필요한 압수·수색에 해당한다고 보았다. 이러한 법리에 따라 연방대법원은 Olmstead v. United States(1928) 판결에서, 피의자의 주거지에 침범하지 않고 외부선을 통해서 한 전화 도청은 재산에 대한 침범이 없으므로 수정헌법 제4조의 규율대상이 아니라고 하였다.[642] 그러나 위 판결로부터 약 40년이 경과한 이후 연방대법원은 Katz v. United States(1967)[643] 판결에서, 수정헌법 제4조는 '장소(place)를 보호하려는 것이 아니라 사람(people)을 보호하려는 것'[644]이라고 하면서 영장 없이 공중전화 외부에 설치한 도청장치를 이용하여 Katz의 전화를 녹음한 것은 '사생활에 대한 합리적인 기대(Reasonable Expectation of Privacy)'를 침해한 것으로, 수정헌법 제4조에 위반된다며 판례를 변경하였다.[645]

그 이후 연방대법원은 수사기관이 영장 없이 피의자의 주거지 부근에 '열 영상장치(thermal imaging device)'를 설치하여 얻은 정보를 근거로 압수·수색영장을 발부받은

642) Olmstead v. United States, 277 U.S. 438 (1928).
643) Katz v. United States, 389 U.S. 347 (1967).
644) Katz v. United States, 389 U.S. 351 (1967).
645) 위 판결에서 별개의견을 제시한 Harlan 대법관은 '사생활의 비밀에 대한 합리적인 기대에 대한 심사기준'을 최초로 제시하였는데, 이것은 오늘날까지 압수·수색 관련 영장주의 적용에 있어서 핵심적인 기준이 되고 있다. Harlan 대법관은 Warden v. Hayden 판결(1967)에서 미국 수정헌법이 보호하고자 하는 영역에 프라이버시를 포함시킨 이후 프라이버시 보호에 대한 합리적 기대의 기준에 ① 개인의 주관적 프라이버시 보호 기대와 ② 사회가 합리적인 것으로 인식할 수 준비가 있는지에 대한 기대를 함께 포함시켜 이중기준이론을 적용하였다(남정아, "미국 연방헌법 수정증보 제4조의 압수 및 수색의 범위에 관한 고찰 -연방법원 판례의 동향을 중심으로-", 『서울법학』 제27권 제3호, 서울시립대학교 법학연구소, 2019.11, 5면).

Kyllo v. United States(2001) 판결의 다수의견[646]에서, 수사기관이 피고인의 집에 들어간 것은 아니지만(즉, 물리적 침입은 아니지만), 주거지에 대해 사생활에 대한 합리적인 기대를 침해한 것이어서 수정헌법 제4조의 '수색'에 해당함을 인정하였다.[647] 즉, 사생활에 대한 합리적인 기대(Reasonable Expectation of Privacy) 이론을 수정헌법 제4조 위반 여부를 판단하는 기준으로 공식적으로 받아들이게 된 것이다.

위와 같은 판례는 연방대법원이 새로운 기술의 발전으로 인한 사생활 침해 가능성에 대하여 수정헌법 제4조의 영장주의를 적용한 것으로, 재산에 대한 물리적 침해뿐만 아니라 새로운 기술과 환경에 따른 비재산적 권리에 대한 침해까지[648] 수정헌법 제4조의 적용범위를 확대한 것이라고 볼 수 있다. 이제는 수사기관이 컴퓨터 등 저장매체에 저장된 정보에 접근할 때 정보주체는 개인정보 보호에 대한 합리적인 기대를 갖는다고 보는 것이 일반적이다.[649]

나. 영장주의 적용 여부가 문제되는 경우: '휴대폰 위치정보' 수집이 수정헌법 제4조 '수색'에 해당하는지 여부

1) 제3자 법리(Third Patry Doctrine) 적용

1976년 연방대법원은 United States v. Miller 판결[650]에서, 은행 등 제3자가 피의자를 위해 보관하는 정보는 피의자가 제3자에게 자발적으로 제공한 것이고, 그 정보가 제3자로부터 정부에 이전될 수 있다는 위험을 감수한 것이어서 사생활에 대한 합리적인 기대가 인정되지 않으므로, 수사기관은 영장 없이 이러한 정보를 수집할 수 있다는 "제3자 법리(Third Party Doctrine)"를 선언한 이래 계속하여 수사기관이 영장없이 제3자 보관 정보를 수집하더라도 수정헌법 제4조 위반이 아니라고 하였다.

위와 같은 제3자 법리에 따라 1979년 연방대법원은 경찰이 영장 없이 통신회사에

646) Kyllo v. United States, 533 U.S. 27 (2001).
647) 박병민·서용성, 앞의 연구보고서, 34면.
648) 김슬기, "미국에서의 정보저장매체의 압수·수색에 관한 연구", 『법학연구』 제25권 제4호, 연세대학교 법학연구소, 2015.12, 146면.
649) H. Marshall Jarrett Director, EOUSA, Michael W. Bailie Director, OLE, "searching and seizing computers and obtaining electronic evidence in criminal investigation", Office of Legal Education Executive Office for United States Attorneys, 2009, 3면.
650) United States v. Miller, 425 U.S. 435 (1976).

피의자가 사용하는 전화번호에 대하여 Pen Register를 설치하도록 하여 통화내역 자료를 받은 Smith v. Maryland 판결[651]에서 사생활에 대한 합리적인 기대를 부정하고, 수정헌법 제4조가 적용되지 않는다고 보았다.

2) 제3자 법리(Third Patry Doctrine)의 예외 인정

2018년 연방대법원은 Carpenter v. United States 판결[652]에서 수사기관이 수색영장 없이 SCA에 따른 법원의 명령(court order)[653]을 통해 통신서비스제공자로부터 휴대폰 위치자료(Cell-Site Location Information, "CSLI")를 제출받은 것은 영장 없는 수색에 해당하여 수정헌법 제4조 위반에 해당한다고 판시하였다.

위 사건에서 수사기관은 체포된 무장강도단 4명 중 1명으로부터 제출받은 휴대폰의 통화내역을 분석하여 범행 시간 무렵 통화한 16개의 통화내역을 찾은 다음 법원의 명령에 따라 통신회사로부터 이와 연결된 휴대폰의 가입자 정보, 통화내역, 휴대폰 위치정보 자료 등을 받아 Carpenter가 범행 당시 공범들과 인근에 있었음을 확인할 수 있는 증거자료[654]를 확보하였다. 이때 문제된 것은 휴대폰 위치자료인데, 제1심인 연방 미시간 동부법원 및 제6 연방항소법원[655]은 "휴대폰 위치자료는 통신내용과는 달리 통신을 용이하게 하는 메타 데이타에 해당하는 것으로 수정헌법 제4조의 보호대상이 아니고, 수사기관이 Carpenter로부터 정보를 수집한 것이 아니라 제3자인 통신회사의 영업정보[656]를 수집한 것이므로 제3자 법리에 따라 수정헌법 제4조의 수색에 해당하지 않는다"[657]라고 판시하였다.

---

651) Smith v. Maryland 442 U.S. 735 (1979).

652) Carpenter v. United States, 138 S. Ct. 2206 (2018).

653) 18 U.S.C. §2703(d). 수정헌법 제4조는 압수·수색에 있어 범죄혐의의 상당성(probable cause)을 요구하나, SCA §2703(d)에 근거한 법원의 명령(Court Order)은 진행 중인 범죄수사와 관련되어 있다고 믿을만한 합리적인 근거(reasonable ground)만 있으면 되기 때문에 영장보다 낮은 정도의 범죄혐의만 있으면 된다.

654) FBI는 127일 동안 Carpenter의 움직임을 분석할 수 있는 12,898개의 위치 포인트를 얻었고, 검찰은 강도사건이 발생할 당시 Carpenter의 전화기가 강도 사건 장소 중 4곳 근처에 있었다는 것을 입증하여 Carpenter는 1심에서 징역 116년을 선고받았고, 최종적으로 파기환송심에서 위 형이 확정되었다(Cornell Law School, Legal Information Institute, "CARPENTER v. UNITED STATES"(https://www.law.cornell.edu/supremecourt/text/16-402; 최종접속일 2023.9.14.)).

655) United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016).

656) 무선 통신업체는 네트워크의 약점을 찾고 다른 통신업체가 셀 사이트를 통해 데이터를 라우팅할 때 "로밍" 요금을 부과하는 등 자체 비즈니스 목적으로 CSLI를 수집하고 저장하고 있기 때문에 이것은 영업정보라고 할 수 있다.

그러나 연방대법원의 다수의견은 "현대사회의 대다수 시민들이 휴대폰을 사용하고 있고, 그 특성상 사용자의 의사와 무관하게 사용자의 위치정보가 자동으로, 그리고 시간 순서대로 빠짐없이 수집되는 것으로 '사생활에 대한 합리적인 기대'가 인정되기 때문에, Smith 사건에서 전화통신과 관련하여 적용되었던 제3자 법리는 오늘날 휴대폰 위치자료에는 적용될 수 없다"[658]고 보았다. 수사기관이 영장 없이 휴대폰 '발신기지국 위치추적' 자료를 포함한 과거 기록에 접근하는 것은 수정헌법 제4조 위반이라고 본 것이다.[659] 다만, 다수의견은 위 판결의 적용범위를 좁게 제한하여, 위 판결의 법리가 은행 등이 보관하는 기록에 대해 적용되었던 제3자 법리에 영향을 주는 것은 아니고, 위 판결이 긴급상황이나 국가 안전보장을 위해 영장 없이 휴대폰 위치정보를 수집하는 것을 막을 수도 없다고 하였다.[660][661]

Carpenter v. United States 판결 이후 제3자 보관 디지털 증거의 압수수색에 있어서 위 판결의 법리를 원용하여 법집행기관의 영장 없는 디지털 증거수집이 수정헌법 제4조 위반이라는 주장을 하는 경우가 많아졌다. 예를 들면, United States v. Gratkowski 판결[662]에서, 법집행기관은 가상화폐 거래소인 코인베이스(Coinbase)에 소환장(subpoena)을 보내어 아동포르노 웹사이트로 비트코인을 보낸 코인베이스 계정기록을 제출할 것을 명령하였고, 코인베이스가 소환장에 응하여 Gratkowski가 위

657) United States v. Carpenter, 819 F.3d 887 (6th Cir. 2016).

658) Jones 사건에서 수집된 GPS 정보보다 CSLI는 더 상세하고 대부분의 무선통신업체들이 5년 보존 정책에 따라 5년간 위치정보를 비롯한 각종 정보를 저장하기 때문에 정부는 더욱 완벽한 감시가 가능하고 더 큰 사생활 침해의 문제가 발생할 수 있다(Carpenter v. United States, 138 S. Ct. 2206(2018)).

659) 다만, 위 사건의 파기환송심은 위법수집증거배제법칙의 예외이론인 'Good Faith' 이론에 따라 수사기관이 관련 법률의 위헌성 여부에 대하여 선의이었기 때문에 SCA에 근거하여 수집된 휴대폰 위치정보의 증거능력을 배제하지 않았고, Carpenter에게 징역 116년을 선고하였다.

660) Carpenter v. United States, 138 S. Ct. 2220(2018).

661) Carpenter 사건에서 4인의 재판관은 다수의견에 대하여 반대하였다. 먼저, Kennedy 대법관은 새로운 기술에 대하여 법원이 수정헌법 제4조에 대한 기존 선례를 깨는 것은 바람직하지 않다고 하면서 다수의견의 논리는 수사기관이 행사는 합법적이고 필요한 집행 권한에 부당한 제한을 가하는 것이라고 하면서 영장 없이 휴대폰 위치정보를 수집하는 것이 수정헌법 제4조 위반이 아니라고 하였고, Thomas 대법관은 수정헌법 제4조를 엄격하게 해석하여 국가의 압수·수색으로 인한 시민의 재산권 침해만이 문제되는데, Carpenter의 휴대폰 위치정보는 그의 사유재산이 아니므로 수정헌법 제4조 위반이 아니라고 하였다. Alito 대법관은 다수의견의 논리는 수정헌법 제4조의 근본적인 두 축을 무너뜨리는 것으로 적법하고 가치있는 수사기관의 행동을 위협한다고 하였다. 한편, Gorsuch 대법관은 수정헌법 제4조 위반이라는 다수의견의 결론에는 동의하지만 휴대폰 위치정보는 휴대폰 소유자의 사적 재산이기 때문에 영장 없이 압수·수색할 수 없다는 종래의 침해이론을 주장하였다(박병민·서용성, 앞의 연구보고서, 49-50면).

662) United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020).

사이트에 비트코인을 보내 물건을 구매한 고객이라는 자료를 송부하였다. 법집행기관은 이를 근거로 Gratkowski의 집을 수색하고, 그곳에 저장된 범죄 증거를 압수하였다. 이때 Gratkowski는 퍼블릭 블록체인에서 사생활에 대한 합리적인 기대가 있으므로 영장 없이 코인베이스 계정기록을 수집한 것은 영장 없는 수색에 해당하여 수정헌법 제4조 위반이라고 주장하였다. 그러나 제5회 순회법원은 "코인베이스의 비트코인 블록체인거래에 대한 정보는 개인의 삶에 대한 친밀한 창을 제공하는 것이 아니라 고객의 가상화폐 거래에 관한 정보만 제공하는 것으로 Carpenter의 CSLI보다는 Miller의 은행기록에 가깝다"[663]고 하면서 Carpenter 판결 이론을 확대하는 것을 거부하였다. 비트코인 사용자들은 익명으로 거래하지만, 공개된 블록체인을 통하여 거래하기 때문에 블록체인 사용자들은 누구나 모든 비트코인 주소와 거래량을 볼 수 있고 코인베이스와 같은 중개기관을 이용함으로써 프라이버시를 희생하는 선택을 한 것으로 이때는 제3자 법리가 그대로 적용된다고 본 것이다.[664]

위와 같이 연방대법원이 Carpenter v. United States 판결의 적용범위를 제한적으로 인정하였기 때문인지 주 법원 등에서는 휴대폰의 과거 위치정보 외에 실시간 위치정보의 경우에도 위 판결의 법리가 적용된다고 인정하면서도[665] 영장 없이 3시간 이내에 5회 미만으로 살인 용의자의 휴대폰 실시간 위치정보(real-time CSLI)를 취득한 사안에 대해서도 사생활에 대한 합리적 기대를 부정하여 수정헌법 제4조 위반이 아니라고 판시[666]하는 등 영장 없는 위치추적자료에 대하여 Carpenter 판결과 달리 적법하다고 판단한 다수의 판례가 선고되었다.[667]

---

663) United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020).

664) Orin S. Kerr, 『Computer Crime Law』(Fifth edition), WEST ACADEMIC PUBLISHING, 2022, 469면.

665) Carpenter 판결은 휴대폰의 실시간 위치정보가 아니라 과거 위치정보자료에 대하여 사생활에 대한 합리적인 기대를 인정한 것으로, 아직까지 휴대폰 실시간 위치정보에 대하여 수정헌법 제4조가 적용되어야 하는지 여부에 대한 연방대법원 판결은 존재하지 않고 하급심 법원의 의견은 대립한다(전치홍, "실시간 휴대폰 위치정보 추적 수사의 적법성에 대한 미국 판결의 최신 동향 -Carpenter v. United States 판결 이후의 미국 하급심 판결 동향을 중심으로-", 『법학논총』 제41권 제4호, 전남대학교 법학연구소, 2021.11, 164면).

666) 살인사건에서 경찰은 영장을 발부받지 않고 SCA에 근거하여 Sims의 실시간 휴대폰 위치정보를 취득하여 위치를 파악하고 검거하였다. 이에 대하여 Sims는 영장 없이 위치정보를 취득한 것은 수정헌법 제4조 위반이라고 주장하였으나, 텍사스주 1심 및 형사 항소법원 모두 수정헌법 제4조 위반이 아니라고 판시하였다. 항소법원은 Carpenter 판결이 7일 미만의 위치정보를 취득하는 경우에는 사생활에 대한 합리적인 기대를 침해하는지 여부에 대하여 언급하지 않았다고 하면서 침해 여부는 사건별로 개별적으로 판단해야 한다고 하였다(Sims v. State, 569 S.W.3d 634 (Tex. Crim. App. 2019)).

다. 영장주의의 예외 법리의 적용 여부

1) 개요

미국 연방 법률은 영장주의의 예외에 대하여 명문규정으로 정하고 있지 않다. 다만, 판례에 의하여 영장주의의 예외가 인정되어 오고 있는데, 이러한 영장주의의 예외는 과거 유체물에 대한 압수·수색을 전제로 하는 것이어서 디지털 증거의 압수·수색에도 그대로 적용되어야 하는가에 대하여 미국 내에서도 많은 논란이 있다.[668]

미국 연방 법무부의 '범죄수사에 있어 디지털 증거의 획득 및 압수·수색 매뉴얼(Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 2009; 이하 "미국 연방 법무부 매뉴얼")'은 제1장 무영장 컴퓨터 압수·수색(Searching and Seizing Computers Without a Warrant), 제2장 영장에 의한 컴퓨터의 압수·수색(Searching and Seizing Computers With a Warrant)을 구분하여 규정하고 있는바,[669] 디지털 증거의 압수·수색에 있어서도 영장주의의 예외가 허용되고 있음은 분명하다.

2) 체포에 수반되는 압수·수색(Search Incident to a Lawful Arrest)

가) 일반론

체포에 수반되는 압수·수색의 예외는 주로 수사기관이 피의자를 체포할 때 또는 피의자 또는 피의자의 즉시 통제가 가능한 영역에서 영장 없는 압수·수색을 허용하는 법리이다.[670] 위 이론은 1969년 연방대법원이 Chimel v. California 판결[671]에서 "체

667) 경찰이 영장 없이 피의자 Kinslow의 소포 안에 GPS 장치를 넣고 피의자가 그의 차 안에 위 소포를 넣어 경찰이 6시간 동안 피의자의 차량을 추적한 사건에서, 인디애나 항소법원은 위와 같은 행위는 수색에 해당하지 않으므로 수정헌법 제4조 위반이 아니라고 판시하였다(Kinslow v. State, 129 NE3d 810 (Ind. Ct. App. 2019)).

668) 박병민·서용성, 앞의 연구보고서, 67면.

669) U.S. Depart of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"(Third Edition), 2009.

670) 박병민·서용성, 위의 연구보고서, 35면.

671) 경찰은 Chimel을 그의 집에서 체포영장에 따라 체포한 후 그에게 집 수색에 대한 동의를 요청하였으나 Chimel은 이를 거부하였다. 그러나 경찰은 적법한 체포를 근거로 계속하여 영장 없이 여러 방을 수색하였고, Chimel의 아내에게 여러 개의 서랍을 열어 물건을 꺼내게 한 후 동전 등을 압수하였다. 법원은 위 사건에서 경찰의 압수수색의 범위가 Chimel이 무기 또는 증거를 획득할 수 있는 즉각적인 통제범위를 넘어선 것으로 합리적인 수색의 범위를 벗어나 위법하다고 판단하였다(Chimel v. California, 395 U.S. 752 (1969)).

포가 이루어질 때 체포된 사람이 체포에 저항하거나 도망하기 위하여 사용할 수 있는 무기를 제거하기 위해 그를 수색하는 것이 합리적이다. 또한, 경찰이 피체포자에 대한 증거의 은닉이나 파괴를 방지하기 위해 피체포자에 대한 증거를 압수·수색하는 것도 합리적이다. 체포된 사람이 무기나 증거물을 얻기 위해 접근할 수 있는 구역에도 유사한 법칙이 적용되어야 한다. (중략) 체포된 사람의 '즉각적인 통제(immediate control) 범위 내에 있는' 구역을 수색하는 것은 충분한 정당성이 있다"고 판시하면서 정립되었다.

더 나아가, 1973년 연방대법원은 United States v. Robinson 판결[672]에서 적법한 체포에 수반된 압수·수색에는 추가적인 정당화 요소가 필요하지 않다고 판시하면서, 압수·수색의 요건을 더욱 완화하였다.[673] 적법한 체포라면 경찰관에 대한 위해 위험성 및 도주 또는 증거인멸 염려와 같은 추가적인 정당화 근거가 없는 경우에도 피체포자에 대하여 영장 없는 완전한 수색(a full search)이 가능하다고 본 것이다.

나) 스마트폰에 저장된 정보의 특별한 취급: 체포에 수반된 압수·수색의 불허

2014년 연방대법원은 Riley v. California 판결[674]에서 위 Robinson 사건에서 선언한 압수·수색 예외의 법리를 스마트폰 내에 저장된 디지털 증거의 압수·수색에 적용하면, 체포사유와 관련성이 없는 범죄에 대한 수사로 이어질 가능성이 높다는 등의 이유를 들어[675] 체포에 수반하는 압수·수색의 예외 법리가 피의자의 스마트폰에 저장된 디지털 증거에는 적용될 수 없다고 선언하였다.[676] 즉, 위 판결에 따르면, 경찰이

---

672) United States v. Robinson, 414 U.S. 218, 235 (1973).

673) 위 사안은 경찰이 무면허운전 중인 피의자(Robinson)를 체포한 후 몸을 수색하면서 그가 소지한 담배상자 안에 헤로인이 들어있는 것을 발견하고 영장없이 압수한 것인데, 연방대법원은 이러한 압수·수색이 수정헌법 제4조에 위반되지 않는다고 보았다(박병민·서용성, 앞의 연구보고서, 36면).

674) 위 사건은 경찰이 등록 유효기간이 지난 자동차를 타고 가는 피의자(Riley)를 검문하면서 그의 차량에서 불법 총기류를 발견하여 불법 무기 소지 혐의로 체포한 후, 피의자가 소지한 스마트폰을 수색하다가 스마트폰 안에 저장된 사진 등을 통해 그가 갱단(Lincoln Park)의 구성원으로 총기 불법사용 등의 범죄를 저질렀다는 것을 확인하고 피의자를 갱단의 총격 사건 등으로 기소하였던 사건이다. 위 판결은 디지털 증거와 관련하여 영장주의의 예외를 확대해서는 안 된다는 주장을 뒷받침하는 대표적인 판례라고 할 수 있다(Riley v. California, 573 U.S. 373 (2014)).

675) 최우구, "영장에 의하지 아니하는 강제처분의 특수문제로써 스마트폰에 저장된 정보에 대한 수색 -Riley v. California 판결 평석-", 『안암법학』 제47권, 안암법학회, 2015.3, 365면.

676) 주요 판시내용은 "Robinson 판결의 법리는 물리적인 물건(physical object)의 맥락에서는 적정한 균형을 제공하지만, 휴대폰의 디지털 콘텐츠와 관련해서는 힘을 쓰지 못한다. (중략) 휴대폰은 그야말로 사람들의 손안에 막대한 양의 개인정보를 놓아두게 한다. 휴대폰 내 정보의 수색은 Robinson 사건에서 고려된 간단한 물리적 수색과는 전혀 유사하지 않다. 그러므로 우리는

적법한 체포과정에서 영장 없이 스마트폰 자체를 압수할 수 있지만, 그 내용을 수색하기 위해서는 법관으로부터 영장을 발부받아야 하는 것이다.

3) Plain View Doctrine

가) 일반론

Plain View Doctrine[677]이란, 수사기관이 어떤 장소에 적법하게 들어가거나(entry), 적법하게 체포(arrest) 또는 수색(search)하는 경우, 육안으로 직접 다른 범죄의 증거임을 즉시 인식할 수 있는 상황이라면 영장 없이 그 물건을 압수할 수 있다는 원칙이다.[678] Plain View Doctrine은 긴급성을 요건으로 하지 않고 수사기관의 주관적 의도(subjective intent) 역시 고려하지 않는다.[679] 그러나 유죄의 증거가 발견될 때까지 영장 없이 일반적인 수색까지 할 수 있음을 의미하는 것은 아니다.[680] Plain View Doctrine은 아래와 같은 요건에서 적용된다.[681]

첫째, 수사기관이 적법하게 대상물을 관찰할 수 있는 장소에 들어갔어야 하는 것으로(prior valid intrusion) 수사기관이 대상물을 명백하게 발견할 수 있는 장소에 접근할 때까지 위법이 없어야 한다.

둘째, 대상물이 범죄행위의 증거물이라는 것이 명백해야(immediately apparent) 한다.[682] 예를 들면, 대상물이 법에서 소지를 금지하는 마약 등과 같은 금제품이거나

Robinson 판결을 휴대폰 내 디지털 정보의 수색에까지 확대하는 것을 거부하고, 그 대안으로 경찰은 일반적으로 그러한 압수·수색을 하기 전에 영장을 확보해야만 한다"는 것이다(Riley v. California, 134 S. Ct. 2473, 2484 (2014)).

677) 'Plain View Doctrine'이란, 국내에서 '명백한 육안 발견의 예외'라고 번역되기도 한다.

678) 미국 연방 법무부 매뉴얼, 34면.

679) 조성훈, 앞의 책, 80면.

680) 'Plain View Doctrine' 이후 연방대법원은 Minnesota v. Dickenson, 508 U.S. 366 (1993) 사건에서 Plain Touch 원칙의 도입 가능성을, 제5 연방항소법원은 United States v. Jackson, 588 F.2d 1046 (5th Cir, 1979) 사건에서 Plain Hearing 원칙을, 제10 연방항소법원은 United States v. Vasquez-Castillo, 258 F.3d 1207 (10th Cir. 2001) 사건에서 Plain Smell 원칙을 인정하여 영장주의의 예외를 시각뿐만 아니라 촉각(Plain Touch), 청각(Plain Hearing), 후각(Plain Smell)까지 분야까지 확대 적용하고 있다. 다만, 이 글에서는 디지털 증거와 관련된 'Plain View Doctrine'에 대하여만 살펴보는 것으로 그 논의의 범위를 한정한다(박병민·서용성, 앞의 연구보고서, 70-71면).

681) 박병민·서용성, 위의 연구보고서, 70면.

682) Of course, the extension of the original justification is legitimate only where it is immediately apparent to the police that they have evidence before them; the "plain view" doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges(Coolidge v. New Hampshire, 403 US 443(1971)).

범죄의 증거 또는 수단이라고 믿을만한 상당한 이유(probable cause)가 있어야 한다.

셋째, 수사기관이 대상물에 대한 적법한 접근 권한(lawful right of access)을 가질 것, 즉 원래 허용된 수색의 통상적인 범위 내에서 대상물을 발견한 경우여야 한다.[683] 위 원칙은 수사기관에게 대상물이 들어있는 장치를 열 권한이 없음에도 이를 열어서 대상물을 관찰하는 것까지 허용하는 것은 아니다.[684]

나) 디지털 증거의 압수·수색에 있어서 Plain View Doctrine 적용 여부

디지털 증거의 압수·수색에 있어서도 Plain View Doctrine을 그대로 적용할 수 있을 것인가에 대하여는 미국에서도 견해의 대립이 있다.[685] 현재까지 연방대법원은 이에 대하여 명시적으로 이에 대하여 판단한 바 없고, 하급심 법원의 견해는 일치되지 않는다.

미국의 디지털 증거 압수·수색은 관련 증거의 '선별적 사본 압수'를 원칙으로 하는 우리 법제와 달리, 저장매체 원본 압수 또는 저장매체 전체 이미징을 원칙으로 하고, 사후에 다른 장소에서 저장매체의 복사본을 분석하는 방식을 취하고 있다.[686] 따라서 저장매체 전체를 이미징한 사본에서 압수·수색의 대상 정보를 탐색하여 압수할 때, Plain View Doctrine을 전면적으로 적용한다면, 영장에 기재된 범죄와 무관한 정보에 대해서도 무제한적으로 압수·수색을 할 수 있게 되어 수정헌법 제4조의 '특정성' 요건에 반하는 결과가 된다.

연방항소법원 판결 중에는 디지털 증거의 특수성을 인정하여 Plain View Doctrine을 제한한 것이 다수 있다. 그 대표적인 예로 제10 연방항소법원의 United States v. Carey 판결(1999)[687]을 들 수 있다. 위 사건에서, 수사기관은 마약사건에 관한 압수·수색영장을 발부받아 피의자의 컴퓨터 안에 저장된 파일을 수색하는 과정에서,

---

683) 박병민·서용성, 앞의 연구보고서, 70면.

684) 미국 연방 법무부 매뉴얼, 35면.

685) 예를 들면, Orin S. Kerr 교수는 디지털 저장매체의 복제본 분석과정에서 Plain View Doctrine은 배제되어야 한다고 하면서 "수사기관이 독립된 증거원에 따라 동일한 증거를 발견할 수 있었음을 입증한다거나(independent source and inevitable discovery rule), 긴급상황의 예외(exigent circumstances exception)가 적용될 수 있음을 입증하는 경우 증거능력이 인정될 수 있다"고 하였다(Orin S. Kerr, "Searches and Seizures in a Digital World", 119 Harvard Law Review 531 (2005) 582-584(박병민·서용성, 위의 연구보고서, 72면, 각주 186 재인용)).

686) 백승주, 앞의 논문, 204면.

687) United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).

① 아동포르노 파일을 발견하자 마약 거래 관련 분석을 중지하고, 추가 수색을 진행하여 ② 약 200개 이상의 아동포르노 파일을 추가로 발견하여 압수하였다. 법원은 디지털 증거의 특수성을 언급하면서[688] 수사기관이 우연히 열어본 ①의 파일 외에 ②라는 다른 파일을 압수한 것은 위법한 수색에 의한 것이므로 위법수집증거에 해당하여 증거능력을 인정할 수 없다고 하였다.

한편, 제4 연방항소법원은 United States v. Williams 판결(2010)[689]에서는 정반대의 결론에 이르기도 했다. 위 법원은 수사기관이 컴퓨터를 압수·수색할 수 있는 적법한 영장을 발부받았다면, 그 안에 있는 개별 파일들은 마치 '하나의 캐비넷에 들어있는 수많은 개별 문서들과 같은 것(search of a file cabinet containing a large number of documents)'이므로 수사기관이 아동포르노 파일을 발견하였음에도 기존 혐의와 관련된 증거분석을 중지하지 않은 상태에서 추가로 아동포르노 파일을 발견한 것이라면 Plain View Doctrine이 적용되어 증거능력이 인정된다고 판시하였다.[690]

4) 긴급한 상황의 예외(Exigent Circumstances Exception)

가) 일반론

수사기관은 긴급한 상황의 경우, 즉 "공공의 안전, 증거보전을 위해 급박한 필요가 있는 경우 영장 없이 압수·수색"을 할 수 있고, 이것을 '긴급한 상황의 예외'라고 한다.[691] 미국 연방 법무부 매뉴얼에 따르면, ① 증거인멸의 위험, ② 경찰관 등 제3자에 대한 물리적인 위해의 우려가 있는 경우, ③ 피의자에게 도주의 위험이 있는 경우에는 긴급성이 인정되어 영장 없이 압수·수색을 할 수 있다.[692] 그리고 수사기관의 합법적인 노력을 부당하게 좌절시키는 결과를 가져올 우려가 있는 경우에도 영장 없는 압수·수색을 허용한다.

---

688) "첫 번째 파일을 열어보기 전까지는 그 내용을 알 수 없기에 Plain View 상황에 이르렀다고 보기 어렵다고 보았다. 다만, 디지털 증거의 경우 포괄적 일반 압수·수색을 막기 위한 '특별한 접근'이 필요하다"고 하였다(United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)).

689) United States v. Williams, 592 F.3d 511 (4th Cir. 2010).

690) 박병민·서용성, 앞의 연구보고서, 73면.

691) Mincey v. Arizona, 437 U.S. 385 (1978).

692) The exigent circumstances exception to the warrant requirement generally applies when one of the following circumstances is present: (1) evidence is in imminent danger of destruction; (2) a threat puts either the police or the public in danger; (3) the police are in "hot pursuit" of a suspect; or (4) the suspect is likely to fee before the officer can secure a search warrant(미국 연방 법무부 매뉴얼, 27면).

연방대법원은 긴급한 상황의 예외가 어떠한 것인지에 대하여 명확한 기준을 제시한 바가 없다.[693] 다만, 하급심 법원에서 압수하려는 물건이 증거를 포함하고 있거나 금제품이라는 점에 대한 상당한 이유를 소명할 것을 요구[694]하는 등 긴급한 상황의 예외를 폭넓게 인정하고 있다. 구체적으로 그 판단기준을 보면, ① 긴급성의 정도, ② 사전영장 발부 가능성, ③ 증거가 제거 또는 파괴되는지 여부, ④ 현장에서의 위험 가능성, ⑤ 증거의 확보 또는 보존, 공공의 안전을 보장할 수 있는 대체적 수단의 이용가능성 등을 종합적으로 고려하여 판단한다.[695] 이때, 증거인멸의 염려는 현실적으로 증거가 파괴될 것을 요건으로 하는 것이 아니라 인멸의 '위험성'만 있으면 된다.[696]

나) 디지털 증거압수·수색에서의 '긴급한 상황의 예외' 인정 여부

현재까지 디지털 증거의 압수·수색 과정에서 긴급상황의 예외가 적용되어서는 안 된다는 주장을 찾아보기 어렵고, 오히려 디지털 증거 압수·수색에서 Plain View Doctrine을 폐기하여야 한다는 논거로 긴급상황의 예외이론을 적용해야 한다는 주장이 있다.[697]

증거인멸의 위험은 컴퓨터 수색에서 가장 흔히 발생하고, 컴퓨터데이터는 본질적으로 취약한 성질을 가지기 때문에 적절하게 보전되기 전에 긴급한 상황이 발생할 수 있다.[698] 예를 들어, 피고인이 컴퓨터를 파괴하는 것을 수사기관이 본 경우 긴급한 상황의 예외로 영장 없이 이를 압수할 수 있다.[699] 다만, 긴급한 상황에서 저장매체인 컴퓨터를 압수하는 것과 그 안에 있는 디지털 정보에 대한 압수·수색은 별개로 보아, 컴퓨터 안에 저장된 자료에 대하여는 영장을 발부받아야 한다고 한 판결도 있다.[700] 미국 법무부 역시 긴급한 상황에서 컴퓨터 등 저장매체의 압수는 정당할 수 있지만, 컴퓨터 등에 대한 수색은 별개의 문제로 보면서, 저장된 데이터에 즉시 접근해야

693) Orin S. Kerr, 『Computer Crime Law』(Fifth edition), WEST ACADEMIC PUBLISHING, 2022, 497면.
694) U.S. v. Cisneros-Gutierrez, 598 F.3d 997, 1004 (8th Cir. 2010).
695) Orin S. Kerr, 『Computer Crime Law』(Fifth edition), WEST ACADEMIC PUBLISHING, 2022, 497면.
696) 김연희, "온라인 수색 도입을 위한 문제점과 방안에 관한 소고", 『법학연구』 제64호, 전북대학교 법학연구소, 2020.12, 54면.
697) United States v. Reed, 935 F.2d 641, 642 (4th Cir. 1991); United States v. Plavcak, 411 F.3d 655, 664-65 (6th Cir. 2005), 미국 연방 법무부 매뉴얼, 28면.
698) 미국 연방 법무부 매뉴얼, 28면.
699) United States v. David, 756 F.Supp. 1385 (D.Nev. 1991), 미국 연방 법무부 매뉴얼, 28면.
700) United States v. David, 756 F.Supp. 1385 (D.Nev. 1991).

하는 경우가 아니라면 영장을 발부받고 디지털 포렌식을 통해 증거를 분석할 것을 권고하고 있다.[701]

5) 동의(Consent)

가) 일반론

미국 연방 법령은 임의제출물 압수 또는 동의에 의한 수색을 명문으로 규정하고 있지는 않다. 다만, 연방대법원은 ① 동의할 수 있는 권한이 있는 사람이 ② 자발적으로 수색에 동의(consent)한 경우 영장주의의 예외로서 증거능력을 인정하여 왔다.[702]

이때 동의를 거부할 수 있는 권리를 인식한 경우에만 동의의 자발성이 인정될 수 있는지 여부가 문제된다. Schneckloth v. Bustamonte(1973) 판결[703]에서, 연방대법원의 다수의견은 '동의를 거부할 권리'에 대한 인식 여부는 동의의 유효성 판단에 필수적인 요건이 아니라, 하나의 요소일 뿐 수색에 동의한 사람이 동의거부권이 있음을 알았다는 것을 국가가 증명할 필요가 없으며, 동의의 유효성 여부는 다른 여러 가지 사정을 종합하여 판단하여야 한다고 판시한 바 있다.[704][705]

한편, 피압수자의 '동의의 범위'가 문제되는데, 연방대법원은 '보통의 합리적인 사람'을 기준으로 구체적인 사실관계에 따라 달리 판단하여야 한다고 한다.[706] 수사기관이 피의자에게 특정한 범죄 또는 물건, 장소로 수색의 범위를 제한하여 동의를 받았다면, 적법한 수색의 범위는 동의를 받은 그 범위에 한정된다.[707] 즉, 합의된 수색은

---

701) H. Marshall Jarrett Director, EOUSA, Michael W. Bailie Director, OLE, 앞의 자료, 2009, 30면.

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

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

704) Schneckloth v. Bustamonte, 412 U.S. 218 (1973)(JUSTIA 홈페이지, "Schneckloth v. Bustamonte, 412 U.S. 218 (1973)"(https://supreme.justia.com/cases/federal/us/412/218/; 최종접속일 2023. 9.14.) 참조).

705) 이때, 3명의 대법관은 반대의견으로 '동의거부권'의 존재를 모르는 사람이 그 권리를 포기할 수 있다는 다수의견의 논리는 비상식적이라고 하면서, 동의거부권의 인식 여부는 유효한 동의를 위한 필수적인 요소라고 판시하였다(Schneckloth v. Bustamonte, 412 U.S. 218 (1973)(JUSTIA 홈페이지, "Schneckloth v. Bustamonte, 412 U.S. 218 (1973)"(https://supreme.justia.com/cases/federal/us/412/218/; 최종접속일 2023.9.14.) 참조).

706) Florida v. Jimeno, 500 U.S. 248, 251 (1991); United States v. Donlin, 982 F.2d 31, 33 (1st Cir. 1992).

707) Turner의 이웃집에 사는 Megan Thomas 폭행 사건의 신고를 받고 출동한 경찰관이 Turner의 집 창턱에서 핏자국을 발견하고, Turner의 집 건물, 차량, 개인 재산을 수색하는데 동의를 얻어 수색을 하던 중 Turner의 컴퓨터에서 아동포르노그래피를 발견하여 압수한 사건에서, 제1 연방항소법원은 Turner의 동의는 이웃집 폭행 사건과 관련된 증거만 수집하는 것에만 효력을 미치기

동의의 범위를 초과할 수 없다.[708]

피의자가 아닌 제3자가 수색에 동의한 경우 영장 없이 수색한 것이 정당한지가 문제 된다. 이에 대해 연방대법원은 United States v. Matlock(1974) 판결[709]에서, '수색 장소에 공동권한을 가진 제3자로부터 자발적인 동의를 받아 수색한 경우 수정헌법 제4조에 위반되지 않는다'고 판시하였다. 이때, 공동권한이란, '제3자가 수색 장소에 대하여 피고인과 함께 접근권 또는 통제권을 가지고 있는 경우를 의미하는 것으로, 공동 거주자(A)는 누구든지 자신의 권리로 수색을 허용할 수 있고 다른 공동 거주자(B)는 공동 거주자(A)가 공동 구역을 수색하는 것을 허용할 위험을 감수하여야 한다'는 취지로 판시하였다. 한편, 연방대법원은 Georgia v. Randolph(2006) 판결[710]에서, 피의자가 물리적으로 현장에 존재하고, 수색에 반대하였다면 제3자인 아내의 주거 수색 동의는 효력이 없다고 판시한 바 있다.[711]

나) 디지털 증거의 압수·수색에 있어 동의

(1) 동의의 범위

디지털 증거의 압수·수색에 있어서도 일반적인 유체물에서의 압수·수색에 대한 동의와 마찬가지로 수사기관이 범죄 관련성 및 저장매체를 범위를 특정하여 동의를 받은 경우 그 범위에 한정하여서만 영장 없는 수색이 허용된다. 이에 대하여 디지털 증거의 압수·수색에 있어서 저장매체에 대한 수색에 동의한 경우 그 동의의 범위는 전체 디지털 증거가 아니라 동의를 받을 당시 수색의 원인이 된 범죄사실과 관련된 부분에 한정하여 수색하는 것에 동의한 것으로 판단한다. 수사기관이 특정 범죄에 대하여 피의자의

때문에 위와 같은 아동 포르노그래피의 압수는 수정헌법 제4조 위반이라고 하였다(U.S. v. Turner, 169 F.3d 84 (1st Cir. 1999)).

708) "consensual search may not exceed the scope of the consent given"(United States v. Rudolph, 970 F.2d 467, 468 (8th Cir. 1992)).

709) U.S. v. Matlock, 415 U.S. 164 (1974).

710) Georgia v. Randolph, 547 U.S. 103 (2006).

711) 위 Matlock 사건은 은행 강도 혐의를 받는 피의자 Matlock이 체포된 상태에서, 공동 거주자인 Mrs. Graff가 주거에 대한 수색에 동의하였고, 공동으로 거주하는 침실에서 현금 4,995달러를 압수한 것이나, Randolph 사건은 피의자 Scott Randolph가 주거에 대한 수색을 명시적으로 거부하는 상태에서 그의 아내인 Janet Randolph가 수색에 동의하여 코카인 투약이 의심되는 빨대를 발견하였던 사건으로, Randolph 사건은 피의자의 현존(presence)하는 상태에서 명시적으로 수색에 반대(objection)하였다는 점에서 차이가 있다.

동의(①)를 받은 다음 컴퓨터 수색 중에 우연히 다른 범죄의 디지털 증거, 즉 동의의 범위를 넘어서는 증거를 발견한 경우 이것을 동의(①)에 근거하여 압수·수색할 수는 없지만, 피의자로부터 추가 수색에 대한 동의(②)를 받았다면 수정헌법 제4조에 위반되지 않는다.[712] 다만, 별건 증거에 대하여 추가 수색에 관한 동의를 따로 받지 않고 영장 없이 수색하였다면, 수정헌법 제4조 위반에 해당한다고 할 수 있다.

피의자가 컴퓨터 수색에 동의한 경우 압수·수색 장소에 있던 전원이 연결되지 않았지만 컴퓨터에 연결되어 있던 외장 하드디스크도 동의의 범위에 포함되는지 문제가 된 United States v. Beckmann(2015) 판결[713]에서, 제8 연방항소법원은 "컴퓨터는 컴퓨터의 작동에 관여하는 구성부분들의 집합(component part involved in the computer's operation)"이고, Beckmann은 경찰이 외장 하드 드라이브를 전기 콘센트에 꽂고 검색을 했을 때에도 수색에 반대하지 않은 점을 들어 외장 하드디스크도 동의의 범위에 포함된다고 판시한 바 있다. 위 제8 연방항소법원은 자발적으로 저장매체의 수색에 동의한 경우 일반 유체물의 수색 동의와 유사하게 연결된 다른 저장매체의 압수·수색까지 동의의 범위에 포함시키고 있다.

(2) 제3자의 동의

수사기관이 제3자의 동의를 받아 피의자의 컴퓨터를 압수하는 경우, 제3자가 컴퓨터에 대한 공동권한이 있어야 그 동의가 유효하다는 입장을 취하면서도, 연방 항소법원은 그 컴퓨터에 대한 공동권한이 있는지 여부에 대하여는 엄격하게 해석하고 있다. 제4 연방항소법원은 피의자 아내의 동의를 얻어 피의자의 컴퓨터를 압수·수색하면서 암호가 설정되어 있는 파일까지 수색하였는데, 이 경우, 피의자의 아내는 암호가 걸린 파일에 대한 수색에 동의할 권한까지 있다고 보기는 어렵다고 보았다.[714] 즉, 컴퓨터의 공동사용자 A, B는 일반적으로 컴퓨터에 저장된 파일에 대한 검색에 동의할 수 있지만, A가 자신의 파일을 비밀번호로 보호하고 있고, 다른 공동사용자 B와 비밀번호를 공유하지 않았다면 B는 비밀번호로 잠겨진 A의 파일에 대한 검색에 유효한 동의를 할 수 없다고 보는 것이다.[715]

---

712) U.S. v. Whaley, 415 Fed.Appx. 129 (11th Cir. 2011).
713) U.S. v. Beckmann, 786 F.3d. 679-680 (8th Cir. 2015).
714) U.S. v. Buckner, 473 F.3d 551 (4th Cir. 2007).

(3) 동의의 철회

수사기관이 피의자 등으로부터 컴퓨터에 대한 수색에 대하여 동의를 받아 이를 이미징한 후 그 복사본을 분석하던 중에 동의를 철회한 경우[716]는 물론, 저장매체를 이미징한 후 이를 분석하기 전에 피의자가 동의를 철회한 경우[717]에도 수사기관이 적법하게 이미징한 매체를 수색할 수 있다고 본다. 즉, 수사기관이 피의자 등으로부터 저장매체에 관한 수색에 대하여 동의를 받아 이미징한 후에는 동의를 철회하여도 소급적으로 저장매체 수색에 대한 동의를 무효화하지는 못한다고 본다. 종이 문서를 복사한 것과 하드 드라이브를 복사한 것을 구별할 이유가 없으며,[718] 자신의 컴퓨터를 이미징한 후 컴퓨터 검색에 대한 동의를 취소한 피고인은 하드 드라이브 이미징사본에 대하여는 사생활에 대한 합리적인 기대가 없다고 본 것이다.[719][720]

라. 위법수집증거배제법칙 예외법리로서 '선의의 예외' 법리 적용 여부

1) 위법수집증거배제법칙 예외로서의 '선의의 예외 법리(Good Faith Exception Rule)' 일반론

연방대법원은 1914년 영장 없이 주거지 내에서 압수·수색하여 취득한 증거물에 대하여 수정헌법 제4조에 위반한 것으로 증거로 사용할 수 없다고 판시한 Weeks v. United States 판결[721] 이후 오늘날까지 계속하여 원칙적으로 수정헌법 제4조를 위반하여 수집한 증거의 증거능력을 부정하고 있다.

그러나 수정헌법 제4조에 위반하여 수집된 증거에 대하여 예외적으로 '선의의 예외(Good Faith Exception)' 법리를 적용하여 증거능력을 인정한 사례도 다수 있다. 선의

---

715) Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001).
716) U.S. v. Megahed, 2009 WL 722481 (M.D. Fla. 2009).
717) U.S. v. Sharp, 2015 WL 4641537 (N.D.Ga.2015).
718) H. Marshall Jarrett Director, EOUSA, Michael W. Bailie Director, OLE, 앞의 자료, 2009, 16면.
719) United States v. Megahed, 2009 WL 722481, at 3 (M.D. Fla. Mar. 18, 2009).
720) 위 판결에 대하여는 동의가 철회될 때까지 이미지에 대한 검색이 시작되지 않은 경우 동의 철회는 원본과 복사본 모두에 대한 검색 권한의 철회를 의미하는 것으로 봐야 한다는 비판도 있다(Orin S. Kerr, "Computer searches and the problem of withdrawn consent", 『The washington Post』, 2015년 8월 11일자(https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/08/11/computer-searches-and-the-problem-of-withdrawn-consent/; 최종접속일 2023. 9.14.).
721) Weeks v. U.S., 232 U.S. 383 (1914).

의 예외 법리는 연방대법원이 1984년 United States v. Leon 판결[722]에서 범죄혐의에 대한 '상당한 이유' 없이 발부된 압수·수색영장은 수정헌법 제4조에 위반된 것이지만, 수사기관이 객관적으로 보아 위 영장을 신뢰하였다는 것에 합리성이 인정된다면 그 영장을 집행하여 수집한 증거의 증거능력이 부정되지 않는다고 선언한 것으로, 위 판결 이후 다양한 판결에서 채택되고 있는 법리이다. 선의의 예외 법리는 수사기관이 위헌적 법률에 따라 압수·수색을 한 경우에도 적용된다.[723]

2) 디지털 증거의 압수·수색에 있어 선의의 예외 법리 적용 여부

연방대법원의 Carpenter 판결[724] 이후 파기환송심[725]에서, 제6 연방항소법원은 영장 없는 휴대폰 위치 정보의 수집은 수정헌법 제4조 위반으로 위법하지만, 연방대법원의 판결 이전에는 위헌성이 명백하지 않았으므로 '선의의 예외 법리'에 근거하여 위치정보의 증거능력을 인정한 바 있다. 디지털 증거의 압수·수색에 있어서도 '선의의 예외 법리'가 적용된다.

마. 디지털 증거 관련 특수 쟁점

1) 법원에 의한 압수·수색영장의 집행방법에 대한 사전규제 가능 여부

디지털 증거의 특성상 저장매체 안에는 무관정보가 혼재되어 있을 가능성이 높기 때문에, 무관정보를 압수하지 않도록 하기 위하여 법원이 압수·수색영장을 발부함에 있어서 수사기관에게 증거분석계획(search protocol)을 제출하도록 하고, 법원이 승인하기 전까지는 증거분석을 할 수 없다는 등의 조건을 부가하여 영장을 발부하는 것이 가능한지 여부, 즉 법원에 의한 영장 집행방법에 대한 사전규제가 가능한지 여부가 실무상 논란이 된 바 있다.[726] 증거분석계획 및 승인을 조건으로 영장을 발부하는 것이 미국 다수 법원의 태도는 아니다.[727] 그러나 2008년부터 2010년까지 제9

722) U.S. v. Leon, 468 U.S. 897 (1984).
723) 연방대법원은 수사기관이 위헌적 법률에 따라 압수·수색을 한 경우에도 그 법이 명백히 위헌이라고 할 수 없다면 수사기관이 그 법의 위헌성에 대해 의문을 품었다고 하기 어려우므로, 그 이전에 수집된 증거가 배제될 수는 없다고 판시한 바 있다(Illinois v. Krull, 480 U.S. 340 (1987) 판결).
724) Carpenter v. United States, 138 S. Ct. 2206 (2018).
725) U.S. v. Carpenter, No.14-1572 (6th Cir. 2019).
726) 박병민·서용성, 앞의 연구보고서, 88면.

연방항소법원에서 3차례에 걸쳐서 이루어진 United States v. Comprehensive Drug Testing 판결(이하 "CDTⅠ, CDTⅡ, CDTⅢ 판결")[728]은 디지털 증거의 압수·수색영장의 집행방법을 법원이 구체적으로 제시한 판결로 자주 인용되기도 하고, 우리나라에도 자주 소개되고 있는바, 이에 대하여 살펴볼 필요가 있다.

가) 사실관계

수사기관은 사설 검사기관이 보유하고 있는 메이저리그 프로야구 선수들에 대한 스테로이드 검사결과 파일에 대한 압수·수색영장을 발부받았는데, 그 영장에는 '금지약물을 복용하였다고 의심할만한 상당한 이유가 있는 10명의 선수에 대한 정보를 대상으로 하되, 수사기관이 아닌 디지털포렌식 전문가가 위 정보를 선별할 수 있도록 하여야 한다'는 조건이 부가되어 있었다. 이에 따라 디지털포렌식 요원이 'Tracy'라는 폴더를 복사하였는데, 위 폴더에는 ① 수사대상자인 10명의 선수 이외에 ② 다른 프로야구선수들과 ③ 일반인들에 대한 검사결과도 포함되어 있었다. 제9 연방항소법원에서 10명의 선수 외에 ②, ③의 증거가 대배심(Grand Jury) 절차에서 사용될 수 있는지 여부가 쟁점이 되었다.

나) CDT Ⅰ 판결

2008년 제9 연방항소법원 3인 재판부는 ㉠ 수사기관이 현장에서 자료를 검토하여 필요한 부분만 분리하는 것은 현실적으로 어렵다는 점을 충분히 설명하였던 점, ㉡ 영장을 신청하면서 여러 자료가 혼재된 대상물을 압수하는데 필요한 절차를 제시하였다는 점, ㉢ 영장에 부가된 조건을 준수하여 압수·수색하였던 점, ㉣ 저장매체 자체가 아니라 특정한 폴더만 복사하여 압수범위를 최소화하기 위하여 노력하였다는 점을 들어, 'Tracy' 폴더를 복사한 것이 수정헌법 제4조 위반이 아니라고 판결하였다.[729]

다) CDT Ⅱ 판결

2009년 제9 연방항소법원 전원재판부는 최초 수사대상자였던 ① 10명의 선수에 대한 증거만이 대배심 절차에서 증거로 사용할 수 있다고 판시하였다.[730] 위 전원재판

727) 조성훈, 앞의 책, 83면.
728) United States v. Comprehensive Drug Testing, 621 F.3d 1162, 1180 (9th Cir.).
729) United States v. Comprehensive Drug Testing, 513 F.3d 1085 (9th Cir. 2008).

부는 연방치안판사가 디지털 증거 관련 영장을 심사할 때 '㉠ 수사기관에게 향후 재판과정에서 Plain View에 의한 영장주의 예외를 포기할 것을 영장발부절차에서 요구하여야 하고, ㉡ 수사기관은 법원에 증거분석계획(Search Protocol)을 제출하고, 승인된 계획에 따라서만 증거분석을 수행하여야 하며, ㉢ 수사담당자와 디지털포렌식 요원이 분리되어야 한다는 조건을 부가하여야 하고, ㉣ 필요한 증거를 분리한 후에 다른 부분은 파기하거나 피압수자에게 하드웨어 등과 함께 반환하여야 한다'는 영장 심사 가이드라인을 제시하였다.

라) CDT Ⅲ 판결

연방 법무부는 법원이 영장 집행방법에 대하여 엄격하게 규제하는 위 가이드라인에 대하여 강력하게 반대의견을 피력하였고, 2010년 제9 연방항소법원은 'CDT Ⅱ'의 판결을 일부 수정하여 엄격한 규제를 다소 완화하였다.[731] 그 결과 위 가이드라인은 제9 연방항소법원 산하의 연방치안판사가 준수하여야 할 지침이 아니라 참고할 기준으로서의 의미만 가지게 되었다.[732]

마) 소결

Rule 41.에 의하면 법관은 상당한 이유가 인정되면, 영장을 '발부하여야 한다(must issue)'고 규정되어 있을 뿐, 법관이 조건부로 영장을 발부할 수 있는 권한이 규정된 법령은 존재하지 않는다. 연방대법원 역시 2006년 United States v. Grubbs 판결[733]에서 압수·수색 대상을 특정하는 것 이외에 영장 집행 방식에 대한 상세한 기재가 포함될 이유가 없다고 판시한 바 있다. 현재까지도 미국 법무부는 디지털 증거분석과정에 대하여 사전 조건을 부가하는 것은 연방대법원의 선례와도 맞지 않는다고 하면서 위와 같은 CDT Ⅱ 판결에 부정적인 태도를 보이고 있다.[734]

---

730) 3인 재판부의 판결에 대하여 CDT 측이 '전원재판부(en banc)'에 의한 재심리를 요청하여 전원재판부에서 2번째 판결을 하게 되었다(United States v. Comprehensive Drug Testing, 579 F.3d 989(9th Cir. 2009); 조성훈, 앞의 책, 84-85면).

731) 연방 법무부는 2009년 전원재판부 판결에 대하여 전체 전원재판부(super en banc)에서 재심리하여 달라고 요청하였으나, 제9 연방항소법원은 전체 전원재판부에서 심리하지는 않고 위와 같이 수정판결을 하였다(United States v. Comprehensive Drug Testing, 621 F.3d 1162(9th Cir. 2010); 조성훈, 위의 책, 86면).

732) 조성훈, 위의 책, 86면.

733) United States v. Grubbs, 547 U.S. 90 (2006).

2) 암호해제 요구

가) 개요

오늘날 프라이버시에 대한 인식이 높아짐에 따라 휴대폰, 노트북 등 개인용 전자기기에 패스워드, 또는 지문, 홍채 인식 등 생체 정보를 이용하여서만 접근이 가능하도록 타인의 접근을 차단하는 경우가 많다. 또한, 이메일 등이 저장된 인터넷 서버의 경우도 아이디 및 패스워드 등 접근권한정보를 아는 경우에만 접속이 가능하다. 따라서 오늘날 수사기관이 디지털 증거를 압수·수색함에 있어서는 선제적으로 아이디, 패스워드 등 접근권한정보를 획득하는 것이 필수적이다.

미국에서도 피의자에게 패스워드 등 접근권한정보의 제출을 요구하거나, 직접 접근권한 정보를 입력하게 할 수 있는지 여부, 휴대폰 잠금해제를 위해 지문 채취를 강제할 수 있는지 여부, 제3자인 휴대폰 제조사에게 잠금해제를 위해 협력을 강제할 수 있는지 여부가 문제되고 있으나, 현재까지 연방대법원의 명시적인 판단은 없는 상황이다. 우선, 이와 관련하여 미국 수정헌법 제5조에 관한 이론에 대한 이해가 필요한바, 아래 항에서 간략히 살펴보기로 한다,

나) 미연방 수정헌법 제5조와의 관계

수사단계에서 Rule 17.에 규정된 제출명령(subpoena)을 송달받은 사람은 자기가 보관 또는 소지하고 있는 것으로 현재 계속 중인 절차의 쟁점과 관련성이 있는 문서, 물건을 제출하여야 한다.[735] 만일 이에 불응하면 법원에 법정모욕죄(contempt)로 기소될 수 있기 때문에[736] 사실상 제출을 강요당하는 것이라고 볼 수 있다. 따라서 수사기관이 피의자에게 패스워드 등 접근권한 정보 등을 제출명령을 통하여 요구하는 경우, 수정헌법 제5조에 규정된 "어떤 사람도 형사사건에서 그 자신에게 증인이 되도록 강요

---

734) 미연방 법무부는 판사가 CDT 판결과 같이 디지털 증거를 조사하는 방법을 제한하여 영장을 발부하는 경우, 그러한 방법이 증거를 확보하는 정부의 능력을 심각하게 방해할 가능성, 증거가 컴퓨터에 은닉될 가능성, 현장 수색의 필요성에 대한 설명 등을 통해 위와 같은 영장 집행방식의 제한에 반대하여야 한다는 입장이다(미국 연방 법무부 매뉴얼, 80면).

735) 조성훈, 앞의 책, 158면.

736) Rule 17(g) Contempt. The court (other than a magistrate judge) may hold in contempt a witness who, without adequate excuse, disobeys a subpoena issued by a federal court in that district. A magistrate judge may hold in contempt a witness who, without adequate excuse, disobeys a subpoena issued by that magistrate judge as provided in 28 U.S.C. §636(e).

받지 않는다"[737]는 자기부죄거부특권(right against compelled self-incriminating testimony)을 침해하는 것인지 여부가 문제된다.[738]

다) 피압수자에 대한 암호해제 요구 가능 여부

수사기관이 피압수자를 상대로 암호해제를 요구할 수 있는 방법은 ① 패스워드를 '진술'해달라고 요구하는 방식, ② 피압수자에게 패스워드를 '직접 입력'하도록 요구하거나 암호가 해제된 '정보의 제공'을 요구하는 방식, ③ 스마트폰의 잠금해제를 위해서 지문 또는 홍채 인식 등 '생체정보의 제공'을 요구하는 방식이 있다.[739]

① 수사기관이 피압수자에게 패스워드를 진술해달라고 요구하는 것이 수정헌법 제5조 위반인지 여부에 대하여 미국 하급심 법원의 태도는 일관되지 않는다. "패스워드는 피의자 내면의 정보(contents of individual's mind)에 해당하고, 그것이 피의자에게 범죄혐의를 인정하는데 사용될 수 있으므로, 피의자에게 패스워드 누설을 요구하는 것은 수정헌법 제5조 위반이다"[740]라고 판시하는 등 자기부죄거부특권 침해를 인정한 판결이 다수이지만,[741] 패스워드 제공 강제가 수정헌법 제5조 위반이 아니라고 한 판결[742]도 있다.

② 피의자에게 패스워드 등 접근권한정보를 "직접 입력"하도록 하거나, 암호를 해제한 "정보의 제공"을 강제할 수 있는지 여부에 관하여 현재까지 연방대법원의 판단은 없고, 하급심 법원의 견해는 일치하지 않는다.[743] 이것은 피의자에게 접근권한과 관련

---

737) Amendment 5 - Trial and Punishment, Compensation for Takings
"(전략) no person … shall be compelled in any criminal case to be a witness against himself… (후략)".

738) 이때, 거부할 수 있는 것은 형사상 자기에게 "형사상" 불리한 "진술(testimony)"이다.

739) 박병민·서용성, 앞의 연구보고서, 102면.

740) 아동포르노를 다운로드 받은 혐의로 기소된 피고인에 대하여 수사기관은 피고인의 하드 드라이브에 있는 암호화된 파일의 내용을 확보하기 위해 기소 후 대배심 소환장을 통해 패스워드를 공개하도록 명령하였으나 법원은 이에 대하여 수정헌법 제5조에 위반되어 허용할 수 없다고 보았다(United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010)).

741) Laurent Sacharoff, Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 203 (2018)(조성훈, 위의 책, 162면 재인용).

742) Commonwealth v. Davis, 176 A.3d 869(pa. Super. Ct. 2017).

743) 연방 제3 순회항소법원은 아동음란물 사건에서, 수사기관이 유효한 영장에 따라 압수한 아이폰의 암호화된 아이폰, 컴퓨터, 외장하드를 완전히 암호화되지 않은 상태로 제출할 것을 명령하였으나, 피고인이 이에 응하지 않자 법정모욕죄로 기소한 사건에서, 수사기관이 기기의 암호화된 영역에 파일이 존재하고, 피고인이 접근권한을 가지고 있다는 점을 입증하는 증거를 제출하였으므로 이를 강제하는 것은 수정헌법 제5조 위반이 아니라고 판시하였다. 즉 법정모독죄가 유죄로

하여 일정한 행위를 하도록 하는 것으로, 외관상 진술이 아니므로 수정헌법 제5조 위반이 아닌 것처럼 보인다. 그러나 연방대법원은 '진술 또는 의사표현의 성격을 가지는 행위'를 강요하는 것 역시 수정헌법 제5조 위반이라고 보고 있는바,[744] 위와 같이 피의자에게 일정한 행위를 요구하는 것이 진술로 평가될 수 있는 경우 수정헌법 제5조의 보호대상에 해당한다.

제출명령에 따라 접근권한정보를 제공하면, ① 증거가 존재한다는 사실, ② 제출명령을 받은 사람이 그 증거를 보관하고 있다는 사실, ③ 제공된 증거가 제출명령에서 요구하는 그 증거라는 사실이 인정되는 경우 그 '제공행위'는 '진술'로 평가되어[745] 수정헌법 제5조 위반에 해당할 수 있다. 다만, 수사기관이 위와 같은 사실을 알고 있는 경우는 '정부가 이미 알고 있는 결론(Foregone Conclusion)'[746][747]에 불과하므로 위와 같은 제공행위는 진술로 평가되지는 않는다.

2014년 매사추세츠주 대법원은 Commonwealth v. Gelfgatt(2014) 판결[748]에서, 피의자에게 컴퓨터의 패스워드를 입력하도록 하는 것은 진술을 강요하는 것으로 볼 수 있지만, 그 행위에 내포된 진술내용(피의자가 소유하고 관리하는 컴퓨터라는 사실, 패스워드가 존재하고 피의자가 이를 알고 있다는 사실)은 이미 수사기관에게 알려진 것이기 때문에 수정헌법 제5조 위반이 아니라고 하였다. 그러나 2020년 인디애나주 대법원은 Seo v. State 판결(2020)[749]에서, "피의자에게 아이폰 잠금해제를 강요하는

인정되었다. 위 사건은 피고인에 대하여 암호화되지 않은 데이터 제출을 강제하기 위하여 writs 영장을 적용한 최초 사례이자, 자기부죄특권에 대한 피고인의 주장을 극복하기 위해 foregone conclusion을 적용한 최초 사례이다(United States v. Apple MacPro Computer, No. 15-3537 (3d Cir. 3/20/17); 송영진, "디바이스 복호화 명령과 자기부죄거부특권: 미국 법원의 실행과 영국의 입법례를 중심으로", 『형사정책연구』 제31권 제1호, 한국형사법무정책연구원, 2020.3, 170면).

744) Schmerber v. California, 384 U.S. 757 (1966).

745) United States v. Hubbell, 530 U.S. 27 (2000).

746) Foregone Conclusion Doctrine이란, 연방대법원이 수정헌법 제5조의 해석과 관련하여, 피의자에게 문서제출요청을 하는 경우 수사기관이 피의자가 문서를 소지하고 있다는 사실을 이미 알고 있었다면(수사기관이 이를 입증해야 함), 문서제출을 강제하는 과정에서 피의자에게 강요하는 암묵적인 진술은 이미 알려진 결론(foregone conclusion)이기 때문에 수정헌법 제5조 위반 문제가 발생하지 않는다는 이론이다(Fisher v. United States, 425 U.S. 391 (1976); United States v. Hubbell, 530 U.S. 27 (2000)).

747) Foregone Conclusion을 "필연적인 결론"으로 해석하기도 한다(송영진, 앞의 논문, 170면).

748) Commonwealth v. Gelfgatt, 11 N.E.3d 605, 615 (Mass. 2014).

749) 수사관이 영장에 따라 압수한 피의자의 스마트폰이 비밀번호로 잠겨있자 피의자에게 잠금을 해제하라는 명령을 하는 영장(warrant)을 발부받았으나, 피의자가 잠금해제를 거부하였고 제1심 법원은 피의자에게 모욕죄를 선고한 사건이었으나, 항소심 및 인디아나 대법원 모두 서씨의

것은 수사기관이 아직 알지 못하는 정보를 제공할 수 있는 것으로 수정헌법 제5조에 위반한다"고 판시한 바 있다.[750] 판례에 의하면, 수사기관이 접근권한 정보 자체를 입력하게 하거나 암호를 해제한 정보를 제공하도록 요구할 때, 정부가 이미 알고 있는 결론의 범위를 어떻게 해석하는지에 따라 접근권한 정보를 입력하게 하는 등의 행위를 강제할 수 있는지 여부가 달라진다.[751]

③ 스마트폰 잠금해제를 위하여 지문 등 생체정보의 취득(biometric access)을 강제할 수 있는지 여부와 관련하여, 2017년 미네소타주 항소법원이 State v. Diamond (2017) 판결[752]에서, 지문 제공은 수정헌법 제5조가 보호하는 '진술'에 해당한다고 볼 수 없다고 판결한 것을 비롯하여 대부분의 법원은 지문 등 생체 인식 및 접근을 강제하는 것은 진술(testimony)이 아니기 때문에 수정헌법 제5조 위반은 아니라고 보고 있다.[753] 그러나 일리노이 북부 연방지방법원이 2017년 In Re Application for a Search Warrant(2017) 판결[754]에서, 스마트폰을 열기 위한 지문 채취 허가는 수정헌법 제5조 위반이라고 판단한 것을 비롯하여 일부 법원은 수정헌법 제5조 위반에 해당한다고 보았다.

라) 제3자에 대한 휴대폰 암호해제 등의 협력 요구

미국에서도 최근 수사기관이 적법하게 휴대폰을 압수수색할 권한을 취득하였음에

사례에서 아이폰 잠금해제명령은 수정헌법 제5조를 위반하는 것이라고 하여 서씨에 대한 법정모독죄에 대하여 무죄 취지의 판결을 하였다(Seo v. State, 109 N.E.3d 418 (Ind. App. 2018); Seo v. State, Indiana Supreme Court, 148 N.E.3d 952 (2020)).

750) 제11 연방항소법원에서도 같은 취지로 잠금해제 명령이 수정헌법 제5조 위반이라고 판시한 바 있다(In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012)).

751) 조성훈, 앞의 책, 178면.

752) 위 법원은 수정헌법 제5조 위반이라는 피고인의 주장에 대하여, 지문을 제공하는 것은 정신작용과 무관하기 때문에 수정헌법 제5조가 보호하고자 하는 '진술'이라고 보기 어렵다는 점을 근거로 제시하였다(State v. Diamond, 890 N.W.2d 143 (Minn. Ct. App. 2017)).

753) Orin S. Kerr, 『Computer Crime Law』(Fifth edition), WEST ACADEMIC PUBLISHING, 2022, 645면.

754) 위 법원은 수정헌법 제5조 위반에 대하여 "피의자는 스마트폰을 열기 위해 손가락을 사용함으로써 스마트폰 내에 있는 정보를 제공한다. 한 번의 손가락 접촉으로, 피의자는 과거 스마트폰에 접촉한 적이 있다는 사실, 피의자가 현재 스마트폰 및 그 내용 정보와 관련이 있고 이를 관리하고 있다는 사실을 '진술'하게 된다"는 것을 그 근거로 내세웠다(In Re Application for a Search Warrant, No. 17M081, 2017 WL 758218 (N.D. Ill. Feb. 16, 2017); MJEB, 『A Guide for Ninth Circuit Magistrate Judges When Reviewing Government Applications to Obtain Electronic Information』(3rd Edition), 2017, 40면.

도 비밀번호 등으로 잠겨져 있는 경우, 그 제조사 등에게 휴대폰 잠금장치를 해제할 것을 요구할 수 있는지 여부가 문제되고 있다.

FBI 등 수사기관은 필요한 경우 제3자에게 수사기관의 활동에 조력할 것을 명령하는 'All Writs' 영장을 발부받아 협조를 요구할 수 있는데,[755] 최근 위 영장의 효력으로 애플(Apple) 등 휴대폰 제조사에게 잠금 해제를 요구하도록 할 수 있는지 여부가 문제되었다. FBI는 압수한 아이폰이 애플(Apple)의 암호화 기술로 잠겨져 있어서 그 안에 저장된 데이터에 접근할 수 없게 되자, 애플(Apple)에게 휴대폰의 잠금장치를 우회하는 프로그램을 만들도록 강제하는 All Writs 영장을 청구하였는데, 2016년 캘리포니아 중부 연방지방법원은 이를 허용하였으나[756] 비슷한 시기에 뉴욕 동부 연방지방법원은 이를 허용할 수 없다[757]고 하였다.

뉴욕 동부 연방지방법원은 All Writs의 경우 '법의 원칙에 부합'할 것이 요구되는데, '법 집행기관을 위한 정보통신 조력법(Communications Assistance for Law Enforcement Act, "CALEA")' 47 U.S.C. §1002(b)(3)[758]에서는 "통신사업자는 자신이 암호화를 제공하고 통신을 해독하는 데 필요한 정보를 보유하고 있지 않는 한, 가입자 또는 고객이 암호화한 모든 통신을 해독하거나 정부의 해독 능력을 보장할 책임이

---

755) 28 U.S.C. §1651(a)에는 "대법원, 그리고 모든 연방법원은 법 집행을 돕는 데 적절하고 필요하며, 또 그것이 법의 원칙에 부합하는 경우에 'All Writs'라는 영장을 발부할 수 있다"라고 규정되어 있는데, 1789년에 입법된 위 규정은 'All Writs Act'라고 부른다.

756) 2015년 12월 캘리포니아주 San Bernadino 지역에서 14명을 학살한 총기 난사 사건과 관련하여 FBI는 애플(Apple)에게 총격범이 사용한 아이폰의 주요 보안기능(10회 잘못된 비밀번호를 입력하면 아이폰 내부에 저장된 데이터가 자동 삭제되는 등의 기능)을 비활성화할 수 있는 프로그램을 제공할 것을 요청하였으나 애플(Apple)이 이를 거절하자 캘리포니아 중부 지방법원(치안판사 Sheri Pym)은 'All Writs'를 발부하여 위 요청에 협조할 것을 명령하였다(In re Search of an Apple Iphone Seized During Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016); Filippo Raso, "Federal Court Orders Apple to Unlock iPhone. Apple Refuses", 『Harvard Journal of Law & Technology』, 2016년 3월 29일자(https://jolt.law.harvard.edu/digest/federal-court-orders-apple-to-unlock-iphone-apple-refuses; 최종접속일 2023.9.14.)).

757) 마약 판매혐의의 남성의 아이폰 암호해제를 위하여 FBI가 'All Writs' 영장을 신청하였으나, 뉴욕 동부지방법원(치안판사 James Orenstein)은 위와 같은 사유로 불허하였다(In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 2016 WL 783565, at *5, 15-MC-1902 (JO) (E.D.N.Y. Feb. 29, 2016); Kateconger, "Have we seen the last of the All Writs Act in the encryption fight?", 『Tech Crunch』, 2016년 4월 26일자(https://techcrunch.com/2016/04/25/have-we-seen-the-last-of-the-all-writs-act-in-the-encryption-fight/?ncid=rss; 최종접속일 2023.9.14.)).

758) 47 U.S.C. §1002(b)(3).

없다"고 규정하고 있는바, 휴대폰 제조사 등에게 잠금장치 해제와 같은 의무를 부과하는 것은 법의 원칙에 부합하지 않는다고 보았다. 위 두 사건 모두 애플(Apple)이 All Writs 영장에 강력히 항의하였고 결국 FBI가 다른 방법으로 아이폰의 암호를 해제한 후 관련 소송을 취하하여[759][760] 연방대법원에 의한 판단은 내려지지 않았다. 위와 같은 소송의 경과를 보면, 앞으로 미국 수사기관이 All Writs 영장을 이용하여 휴대폰 제조사 등에게 잠금 해제를 요구하는 것은 쉽지 않아 보인다.

3. 디지털 증거의 압수·수색에 관한 법령 및 판례 변화의 경향

가. 디지털 증거 압수·수색 관련 법령 변화의 경향

1) 디지털 증거의 특성을 반영한 법령

미국은 수회에 걸친 법령 개정을 통해 대량성, 혼재성, 비가독성 등의 디지털 증거의 특성을 반영한 압수·수색절차를 아래와 같이 명문으로 인정하고 있다.

첫째, 일찍부터 압수·수색의 대상에 정보(information)를 명시하여,[761] 정보 자체가 압수·수색의 대상이 됨을 인정하였다.

둘째, 디지털 증거에 관한 압수·수색영장의 집행 및 집행 후 절차에 있어 디지털 증거의 특성, 영장 실무를 반영하여 절차를 간소화하였다. 2009년 정보저장매체 또는 정보의 압수·수색에서 '복사(copy)'를 압수의 한 방법으로 명문화하고,[762] 영장에 특별한 기재가 없는 한 저장매체의 압수는 복사 후 사후분석에까지 미치지만, 14일의 영장 집행기한은 현장 외 복제 및 사후분석에는 적용되지 않는다[763]고 규정하여,

---

759) 애플(Apple)은 캘리포니아 중부 지방법원의 All Writs 영장에 대하여 수정헌법 제1조 및 제5조에 위반된다며 항소하였다. 그러나 그 이후 FBI가 제3자를 통하여 아이폰 암호를 해제한 후 법원에 해당 소송을 취하하여 이에 대한 상급 법원의 판단은 이루어지지 않았다(THE EDITORIAL BOARD, "After Apple vs. FBI, more reasons to be wary in privacy fight", 『Los Angeles Daily News』, 2016년 4월 29일자(https://www.dailynews.com/2016/04/29/after-apple-vs-fbi-more-reasons-to-be-wary-in-privacy-fight/; 최종접속일 2023.9.14.)).

760) FBI는 뉴욕 동부지방법원의 위 판결에 항소하였으나 다른 경로로 비밀번호를 제공받아 항소를 취하하였다(VentureBeat, "U.S. to continue appeal of iPhone data case in New York", 2016년 4월 9일자(https://venturebeat.com/business/u-s-to-continue-appeal-of-iphone-data-case-in-new-york/; 최종접속일 2023.9.14.)).

761) Rule 41(a)(2)(A).

762) Rule 41(e)(2)(B).

저장매체 압수와 사후 복제 및 분석이라는 2단계 집행절차를 명시하였다. 또한, 영장 집행 후 피압수자에게 교부되는 압수물 목록의 기재에 있어서도 압수한 정보 전부를 구체적으로 나열하는 것이 아니라 '정보저장매체 그 자체'를 기재하는 것으로 충분하다[764]고 규정하였다. 저장매체에 저장된 정보의 대량성, 암호화 등으로 인해 현장에서 복사 및 분석이 어려운 점을 인정하고 명문으로 이를 규정한 것이다. 엄격하게 압수·수색 현장에서 관련 증거를 선별하여 압수하여야 하고, 압수물 목록에 있어서도 압수한 정보를 특정하는 것을 원칙으로 하고 있는 우리 형사법제 및 판례와 다른 태도라고 볼 수 있다.

셋째, 미국은 긴급성을 이유로 영장없이 압수·수색하는 것을 막기 위하여 오래전부터 전화 또는 전자수단을 이용한 영장 청구 및 발부를 허용하여 왔고 영장사본 및 영수증까지 전자적 방식에 의해 송부하도록 하고 있다.[765] 최근 미국에서는 전자영장의 효율성 및 신속성이 인정되어 '전자영장(electronic warrant, e-Warrant)' 제도를 도입하는 주(state)가 증가하고 있다.[766] 즉, 영장주의를 관철하기 위해 영장 청구 및 발부절차를 용이하게 하여 신속성을 높인 것이다.

넷째, 2016년에는 원격지 압수·수색영장 등 관할권을 초월한 영장('NIT' 영장)을 도입하여 관할권 밖에 있는 ISP 등이 보관하고 있는 정보를 압수·수색할 수 있도록 하였다.[767] 미국은 우리나라와 달리 각 주(state)마다 다른 법률을 가진 연방국가이기 때문에 미국에서 관할권 위반의 문제는 우리의 관할권과 다른 의미라고 볼 수 있다. 그럼에도 불구하고 다크 웹을 통한 마약류 범죄, 아동포르노 관련 범죄에서 감시 소프트웨어를 사용하여 피의자의 웹사이트에 접근한 후 IP 주소를 알아내는 것이 관할권 위반이라는 주장이 제기되자, 연방형사소송규칙에 명문으로 디지털 증거의 압수·수색에 있어서 각 주의 관할권까지 초월할 수 있는 NIT 영장의 근거규정을 마련하였다.

다섯째, 2018년 Cloud Act를 통하여 통신서비스제공자가 미국 외 다른 나라에 저장한 정보도 압수·수색할 수 있도록 하였다.[768] 디지털 증거의 압수·수색에 있어서 역외

763) Rule 41(e)(2)(B).
764) Rule 41(f)(1)(B).
765) Rule 4.1.
766) 이상원, 『전자영장제도의 도입방안에 관한 연구』, 연구용역보고서, 법무부, 2012, 80면.
767) Rule 41(b)(6).

압수·수색을 허용한 것이다. 제2 연방항소법원이 마이크로소프트 사건에서 아일랜드에 저장된 정보에 대하여 제출을 요청한 것은 SCA의 부적절한 역외 적용이라고 판결[769]하였음에도 불구하고 위 판결과 반대되는 내용을 입법화하였다.

여섯째, 미국은 수사기관이 통신서비스제공자 등 제3자가 보관한 정보를 수집하는데 있어 180일 미만의 저장된 정보에 대하여는 영장주의를 적용하는 등 엄격한 절차를 규정하고 있고,[770] 통신서비스제공자 등에게 증거보전요청[771] 및 비밀유지명령을 하여[772] 제3자가 보관하는 정보가 영장 발부 시까지 보존되고, 증거가 피의자 등에 의하여 삭제되지 않도록 하는 안전장치를 마련하고 있다. 또한, 미국의 수사기관은 ISP/CSP 등이 보관하는 정보 중 이메일 내용 등과 같은 것 이외에 기타 정보는 압수·수색영장이 아닌 대배심의 소환장을 통한 제출명령[773]을 통하여 수집할 수 있도록 비교적 완화된 규정을 두고 있다.

2) 디지털 증거 압수·수색 관련 법령에 대한 평가

위에서 살펴본 바에 의하면, 미국 연방법령은 우리나라의 「형사소송법」 등보다 비교적 이른 시기부터 디지털 증거의 특수성을 반영한 절차규정을 마련하였다는 점을 알 수 있다. 뿐만 아니라 디지털 증거 압수·수색절차와 관련해서는 피의자의 사생활보호 등의 명목으로 절차를 지나치게 엄격하게 규정하기보다는 수사의 효율성 측면을 우선 고려한 규정이라고 볼 수 있다.[774]

미국에서도 디지털 증거의 압수·수색에 있어서 개인정보 보호 또는 사생활 보호를 강화하여야 한다는 입장과 국가의 안전보장 등을 이유로 수사기관의 디지털 증거 수집을 어렵게 해서는 안 된다는 입장이 극렬하게 대립하고 있다.

---

768) 18 U.S. Code § 2713.

769) In the Matter of a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016).

770) 통신의 내용에 대하여는 제3자 이론에 따라 사생활에 대한 합리적 기대가 인정되지 않는 것으로 보았던 판례의 전통적 입장을 변경하여 상당한 이유를 요건으로 하는 영장을 발부받도록 하였다(18 U.S.C §2703(a) 전단).

771) 18 U.S.C. §2703(f), §2713.

772) 18 U.S.C. §2705(2).

773) 18 U.S.C. §2703(d) 전단.

774) 김민이, "디지털 증거 압수·수색관련 미국, 영국, 프랑스 입법례", 『최신입법정보』 통권 제127호, 국회도서관, 2021.4, 2면.

특히, 상원이 국가 안전보장을 위한다는 명목으로 반대하여 사생활 보호에 관한 규정들이 입법화되지 못하고 있는 것에 대하여는 많은 비판이 있다. 예를 들면, 1986년 ECPA가 제정될 당시에는 Gmail과 같은 웹 기반 이메일이 존재하지 않아서 180일 이상 보관된 이메일의 경우 사용자에 의해 버려진 재산과 같이 취급하여 수사기관이 이를 수집하는 경우에도 영장을 필요로 하지 않는다고 보았다. 하지만, 이러한 원칙은 기간에 상관없이 거의 무제한의 이메일을 보관할 수 있는 클라우드 시스템을 이용하고 있는 현재의 환경에서는 적절하지 않으므로 180일 이상 저장된 이메일 역시 영장에 따라 수집하여야 한다는 비판이 있었고, 실제로 위와 같은 Email Privacy Act of 2016 (이하, "EPA")이 하원에서 통과되었으나, 상원에서의 통과가 수차례 좌절되었다.[775]

더 나아가, ECPA 등 디지털 증거의 수집과 관련한 미국 연방 법령에 대해서는 급격하게 발전하는 통신기술의 변화를 법에 그대로 반영하지 못하고 있다는 비판도 있다. 예를 들면, 전송 중인 통신을 수집하는 것은 Wiretap Act의 적용대상이고, 저장된 통신을 수집하는 것은 SCA의 적용대상으로 수사기관이 이를 수집할 때 요건이 다르다. 그러나 단일 이메일을 구성하는 패킷이 분리되어 여러 서버와 라우터를 통해 전송된 다음 사용자가 접속할 수 있도록 재결합되어 원격지 서버에 저장되는 경우, 이메일을 '전송 중'인 것으로 보아 Wiretap Act의 적용을 받는 것으로 보아야 할지, 원격서버에 '저장된 것'으로 보아 SCA의 적용을 받는 것으로 보아야 할지 각 단계마다 적용법률이 명확하지 않다는 문제점이 있다.[776]

3) 기타 쟁점

우리나라에서는 디지털 증거의 압수·수색절차에서 피의자 등의 참여권을 보장하여야 한다고 명시적으로 규정하고 있으나, 미국은 경찰 등 수사기관이 압수·수색 이전에 미리 피압수자 또는 피의자(또는 그 변호인)에게 참여권을 통지해야 한다거나 참여의

---

775) EPIC 홈페이지, "Electronic Communications Privacy Act (ECPA)"(https://epic.org/ecpa/; 최종접속일 2023.9.14.).

776) 이러한 점에 근거하여 180일 이상 저장된 통신의 경우에도 수색영장을 발부받도록 하고, 영장의 집행 전에 이메일 사용자에게 사전통지를 해야 한다는 이메일 개인정보보호법(Email Privacy Act of 2016)이 하원에서 통과되었지만, 114차~116차 회기(2015~2021) 모두 위 조항의 내용은 결국 상원에서 통과되지 못했다(GIBSON DUNN 홈페이지, "U.S. Cybersecurity and Data Privacy Outlook and Review – 2019", 2019년 1월 28일자(https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2019/; 최종접속일 2023.9.14.)).

기회를 보장하여야 한다는 명시적 규정을 두고 있지 않다.

다만, Rule 41(f)(1)(B)에서는 압수물 목록을 작성할 때 다른 경찰관과 피압수자(the person from whom, or from whose premises, the property was taken)의 참여(Presence)하에 할 것을 규정한 것[777]을 근거로 미국 역시 피압수자가 압수·수색 절차에 참여하는 것을 전제로 하고 있다고 보는 견해[778]가 있다. 그러나 미국에서 피압수자 또는 피의자의 참여권을 명시적으로 인정하지 않고 있다는 것이 다수의 견해이다.[779] 더 나아가, 저장매체를 압수한 후 저장매체에서 범죄와 관련된 정보를 선별하는 과정, 즉 사후분석과정에서 피압수자 측의 참여가 보장되어야 한다는 판례나 학계의 논의도 찾기는 어렵다.[780] 이메일 등 제3자 보관 정보의 경우 통신서비스제공자가 계약에 의하여 압수·수색영장 등의 집행 전에 고객에게 통지하도록 되어 있는 경우가 있으나, 수사기관이 압수·수색영장을 청구하면서 통지배제명령을 함께 신청하는 것이 일반적이기 때문에 통신서비스제공자의 통지의무를 근거로 정보주체인 피의자의 참여권을 보장하였다고 보기는 어렵다.

한편, 아동포르노 웹사이트, 다크 웹을 이용한 마약거래 사건 수사를 위해서 자주 이용되는 '온라인 수색'[781]이 각 주 연방법원의 관할권을 위배하여 문제가 된 바 있다. 온라인 수색은 해킹 등의 방법을 이용하여 대상자의 컴퓨터 등에 접속하여 감시프로

---

777) Rule 41.(f)(1)(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so **in the presence** of another officer and **the person from whom, or from whose premises, the property was taken**. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

778) 박병민·서용성, 앞의 연구보고서, 252면.

779) 김기준, "수사단계의 압수·수색 절차 규정에 관한 몇 가지 고찰", 『형사법의 신동향』 제18호, 대검찰청, 2009.2, 5면.

780) 박병민·서용성, 위의 연구보고서, 252면.

781) 온라인 수색(Online Search)이란, 통상적으로 "국가기관이 해킹 프로그램 설치 등을 통하여 비밀리에 상대방의 컴퓨터 등 정보기술시스템(컴퓨터, 스마트폰 등의 통신기기를 포함)에 침입하여 범죄 관련 정보 등을 탐색, 복사하는 새로운 형태의 디지털 증거 압수·수색 방법"이다.김학경, "미국의 온라인 수색 제도에 관한 연구: 연방형사소송규칙 제41장 개정내용 중심으로", 『시큐리티연구』 제72호, 한국경호경비학회, 2022.9, 65면; 이원상, "온라인 수색에 대한 고찰: 독일의 새로운 논의를 중심으로", 『형사법연구』 제20권 제4호, 한국형사법학회, 2008.12, 335-336면; 김연희, 앞의 논문, 287-288면.

그램(surveillance software)을 설치한 후 관련 자료를 수색하고 압수하는 것이기 때문에 사생활의 비밀 등 기본권 침해 가능성이 매우 높고, 각 서버의 저장위치를 영장 발부 단계에서는 알 수 없기 때문에 필연적으로 역외 관할권의 허용 여부 문제가 발생한다. 이러한 문제점이 있음에도 불구하고, 미국은 그동안 실무상 '네트워크 수사기법' 또는 '온라인 수색'을 개별적이고 특화된 법적 근거 없이 일반적인 압수·수색영장 규정[782]에 근거하여 인정하여 왔다.[783] 그러나 아동포르노 웹사이트에 대한 Playpen 판결[784] 이후 2016년 Rule 41(b)(6) 개정을 통해 온라인 수색을 제도적으로 인정하게 되었다. Playpen 사건에서 온라인 수색영장의 '역외 관할권' 등이 문제되자, 법 개정을 통하여, 관할을 초월하여 원격(remote access) 압수·수색이 가능한 NIT (Network Investigatory Techniques) 영장을 입법화한 것이다. 또한, 2016년 개정을 통해 Rule 41(f)(1)(c)에 영장을 집행한 후 영장사본 및 압수물 목록을 이메일 등 합리적인 범위 내에서 전자적 수단을 이용하여 교부할 수 있도록 하여 영장 집행 이후의 절차도 간소화하였다.

---

782) 온라인 수색이라는 법률용어는 공식적으로 존재하지 않고, 온라인으로 수색을 허용하는 영장을 실무적으로 'NIT(Network Investigative Technique) 영장'으로 지칭하고 있었다.

783) Rule 41. 개정 전까지는 온라인 수색영장이라는 별도의 영장에 대한 규정이 없었고, Rule 41(e)(1)(B)의 전자정보 압수·수색영장 형태로 발부·집행되어 왔다(조성훈, 앞의 책, 207면; 김학경, "미국의 온라인 수색 제도에 관한 연구: 연방형사소송규칙 제41장 개정내용 중심으로", 6면).

784) Playpen 사건은 'Playpen'이라는 다크 웹에서 아동청소년 성착취물을 광고·판매하자 미연방수사국(FBI)이 외국 경찰기관의 첩보를 바탕으로 수사를 개시한 사건으로, 위 사이트는 'Tor' 소프트웨어를 이용하기 때문에 접속경로가 암호화되어 이용자들의 IP를 특정하기가 불가능하였다. FBI는 'Playpen' 메인서버를 버지니아주에 있는 시설로 옮긴 다음 신분위장수사를 통해 위 사이트를 운영하면서 악성코드를 설치하여 전자정보를 압수·수색할 수 있는 영장을 발부받아 위 사이트에 접속한 이용자들의 컴퓨터에 악성코드를 설치하고 이를 통하여 IP 주소 등을 파악하였으나, 위 사람들이 대부분 압수·수색영장이 발부된 버지니아 동부지역이 아닌 관할 연방구역 밖(Out-of-District)에 거주하고 있었다. 따라서 이용자들이 각자의 관할지역에서 재판을 받게 되면서 각 연방지방법원에서는 각기 다른 판결을 하게 되었는데, 대부분의 연방지방법원 및 항소법원은 관할 연방 역외에 있는 물건에 대한 온라인 수색영장은 개정 전 Rule 41(b)를 위반한 것으로 압수·수색의 불법성을 인정하였다. 다만, '선의의 예외'(Good Faith Exception) 이론을 적용하여 증거능력은 인정하였다(김학경, "미국의 온라인 수색 제도에 관한 연구: 연방형사소송규칙 제41장 개정내용 중심으로", 16-17면; United States v. Matish, 193 F. Supp. 3d 585 (E.D. Va. 2016)).

나. 디지털 증거 압수·수색 관련 판례의 경향

1) 새로운 증거수집방법에 대한 수정헌법 제4조 적용의 확대

수사기관에 의한 디지털 증거 수집과 관련하여서는 수정헌법 제4조의 적용과 관련하여 전통적인 침입이론보다는 '사생활에 대한 합리적인 기대' 이론을 적용하여 수정헌법 제4조가 적용되는 수색인지 여부를 판단하고 있다. 즉, 물리적인 침입이 없는 경우에도 디지털 증거의 수집으로 인해 사생활에 대한 합리적인 기대가 침해되었다면, 영장 없는 통화 감청에 대하여 수정헌법 제4조 위반이라고 하는 등 수정헌법 제4조의 적용범위를 확대하였다.

2) 스마트폰 압수·수색절차에 대한 특별한 취급

2014년 연방대법원은 Riley v. California 판결[785]에서는 그동안 판례법상 인정되어 오던 체포에 수반하는 압수·수색을 스마트폰과 같은 디지털 증거에는 적용할 수 없다고 하면서 영장주의 예외 법리의 적용을 제한하였다.

그러나 2018년 사우스캐롤라이나주 대법원은 피의자가 절도 범행 후 피해자의 집에 두고 간 휴대폰을 경찰이 피해자로부터 제출받아 영장 없이 압수·수색한 State v. Brown 판결(2018)[786]에서, 피의자가 휴대폰을 범행현장에 두고 간 다음 통신사에 통신서비스를 해지하고 6일 동안 전화기를 되찾으려는 노력을 하지 않았다면[787] 휴대폰에 있는 사생활에 대한 기대를 포기한 것으로 봐야 하기 때문에 영장 없는 수색은 적법하다고 판단하였다. 즉, 피의자의 휴대폰이 비밀번호에 의해 잠겨져 있었다고 해도 일반적인 물건과 같이[788] 소유권 등 권리를 포기를 인정한 것으로 스마트폰에 대한 특별한 취급을 하였다고 보기 어렵다.[789]

---

785) Riley v. California, 134 S. Ct. 2473, 2484 (2014).

786) State v. Brown, 815 S.E.2d 761 (S.C. 2018).

787) Brown은 자신의 휴대폰을 찾기 위해 전화를 걸지 않았을 뿐만 아니라 문자메시지도 보내지 않았다.

788) 경찰이 영장 없이 피의자의 전(前) 주거지를 수색하여 증거물인 총을 압수한 사건에서, 제4연방항소법원은 피의자가 전 주거지를 떠나면서 집 소유주(임대인)에게 그곳에 있는 자신의 재산을 여자친구에게 전부 주겠다는 편지를 쓰면서 자신을 전 세입자(former renter)로 표현한 경우, 전 주거지에 대한 사생활에 대한 합리적인 기대를 포기하는 것으로 보았다. 즉, 사생활에 대한 보호를 자발적으로 포기한 경우 수정헌법 제4조의 보호를 받지 못한다고 본 것이다(U.S. v. Stevenson, 396 F.3d 538 (4th Cir. 2005)).

2018년 연방대법원은 Carpenter v. United States 판결[790]에서 통신서비스제공자 등 제3자가 보관하는 정보에 대하여는 사생활에 대한 합리적인 기대가 인정되지 않는다고 보았던 제3자 법리(Third Party Doctrine)를 스마트폰 위치추적 자료에 한하여 적용할 수 없다고 판시한 바 있다.

그러나, 2020년 매사추세츠 대법원은 마약사범을 검거하기 위하여 경찰이 영장 없이 다리에 설치된 자동차 번호판 판독기(ALPR)을 이용해 약 2개월 반 동안 피의자의 움직임을 추적한 Commonwealth v. McCarthy 판결(2020)[791]은 Carpenter v. United States 판결에서 휴대폰 위치추적 자료(CSLI)에 대한 판단과는 달리 '모자이크 이론'에 따라 법집행기관이 2개 다리 끝에 설치한 4개의 카메라로 수집한 ALPR만으로는 사생활의 합리적인 기대를 침해하는 것은 아니라고 판단하였다. 즉, 2개의 다리 끝에 설치된 4개의 카메라를 이용한 위치정보만 수집한 것으로 사생활의 침해에 이를 정도가 아니므로 수정헌법 제4조 위반은 아니라고 본 것이다. 따라서 수사기관에 의한 휴대폰 위치정보의 수집이 무조건 영장이 필요한 '수색'이 된다고 보기 어렵고, 다른 정보를 종합하여, 개인의 삶을 친밀한 창을 통해서 볼 수 있을 정도(provide an intimate window into a person's life)가 되는 경우 수정헌법 제4조의 수색에 해당한다고 볼 수 있다.[792]

3) 새로운 쟁점에 대해 일관되지 않은 하급심 법원의 견해

디지털 증거의 수집에 있어서 영장주의 예외이론 중 하나인 Plain View Doctrine, 긴급상황의 예외이론을 적용할 것인지에 대하여는 연방대법원의 명시적인 판단이 없는 상태에서 하급심 법원은 각각 달리 판단하고 있다.

법원이 영장 발부단계에서 영장의 집행방법을 제한하여 사전적 규제를 할 수 있는지에 관하여서도 연방대법원의 판례는 존재하지 않는다. 다만, CDT Ⅱ 판결에서 제시한 디지털 증거 압수·수색에 있어 Plain View Doctrine의 포기, 수사관과 증거분석관

789) 그러나 대법원장 BETTY는 반대의견을 피력하면서 Riley v. California 판결은 특별한 사정이 없는 한 법집행기관이 휴대폰 데이터를 검색하기 위해서는 반드시 검색영장을 발부받아야 한다는 원칙을 만들어 낸 것으로 위 사건의 수색은 수정헌법 제4조 위반이라고 판시하였다(State v. Brown, State v. Brown, 815 S.E.2d 766 (S.C. 2018)).

790) Carpenter v. United States, 138 S. Ct. 2206 (2018).

791) Commonwealth v. McCarthy, 484 Mass. 493, 142 N.E.3d 1090 (Mass. 2020).

792) Orin S. Kerr, 『Computer Crime Law』(Fifth edition), WEST ACADEMIC PUBLISHING, 2022, 472면.

의 분리, 무관증거 삭제 등을 지지하는 하급심 판례가 등장하고 있다.

피의자에 대하여 스마트폰 등 저장매체의 암호를 해제할 것을 요구하는 것이 수정헌법 제5조의 자기부죄거부특권을 침해하는지에 관해서도 아직 연방대법원의 명시적인 판단이 없다. 다만, 하급심 법원의 경우 암호해제 요구가 수정헌법 제5조의 적용이 문제되는 영역이나 피의자가 해당 저장매체를 소유 및 관리하고 있고, 패스워드 등을 알고 있으며, 범죄와 관련한 정보가 해당 저장매체에 저장되어 있다는 것을 수사기관이 이미 알고 있는지 여부, 이를 입증하였는지 여부에 따라 'Foregone Conclusion'에 해당하는지가 결정되고 이에 해당하는 경우 수정헌법 제5조 위반은 아니라는 것이 다수 법원의 입장인 것으로 보인다. 한편, 통신서비스제공자 등 제3자에 대하여 암호해제를 요구할 수 있는지 여부에 대하여 연방대법원의 명시적인 판례는 없고, 하급심 법원의 태도 역시 일관되지 않는다.

제4절 | 영국의 디지털 증거 압수수색 관련 규정 및 판례의 변화

1. 디지털 증거 압수·수색 관련 규정의 변화 과정

가. 개요

영국은 대표적인 불문헌법 국가[793]로 개인의 자유권을 보장하기 위한 Common Law 원칙과 구체적인 성문법의 제정을 통해 형사절차에서의 개인의 권리에 대한 침해를 통제해 왔다.[794]

그러나 영국에서도 압수·수색에 관한 기존의 법률규정이 정보의 대량성, 혼재성, 네트워크 관련성 등을 전제로 하는 급격한 IT 기술의 발전을 따라가지 못하고 있어서 범죄 수사를 어렵게 할 뿐만 아니라 수사과정에서 개인정보를 충분히 보호하지 못하

793) 영국은 미국, 프랑스와 달리 헌법이 법전의 형태, 즉 성문헌법의 형태로는 존재하지 않고 불문헌법으로 존재한다고 보는 것이 일반적이다(이병규, "영국헌법의 본질과 특색", 『동아법학』 통권 제48호, 동아대학교 법학연구소, 2010.8, 63면).

794) 정희도, "영국 수사기관의 전자우편 취득절차 및 한계", 국외훈련검사연구논문집 제26집, 법무연수원, 2011, 126면.

고 있다는 비판이 지속적으로 제기되어 왔다.[795] 이에 대하여 영국 의회 및 정부는 아래에서 보는 바와 같이 압수·수색과 관련된 법령의 제·개정을 통하여 그 문제점을 해결하려고 하고 있다.

한편, 영국 법원은 구체적 사안에서 디지털 증거 압수·수색의 위법성을 판단함에 있어서, 압수·수색 절차 규정 외에도 유럽연합 인권협약(European Convention on Human Rights : 이하, "HCHR")[796]을 그대로 반영한 인권법(The Human Rights Act 1998)[797] 제8조 '사생활과 가족에 대한 권리'를 부당하게 침해하는 것인지 여부를 중요한 기준으로 삼고 있다.

이하에서는 디지털 증거의 압수·수색절차와 관련된 영국 법령의 변화에 대하여, ① 압수·수색에 관한 일반적인 규정인 "경찰 및 형사증거법 1984(Police and Criminal Evidence Act 1984 : 이하, "PACE")", ② 수사기관의 압수·수색 권한을 강화한 "형사사법 및 경찰법 2001(Criminal Justice and Police Act 2001 : 이하, "CJPA")", ③ 감청,

---

795) 영국 법률개혁위원회(Law Commission Reforming the Law)는 1965년 법률위원회법(Law Commissions Act 1965)에 따라 설립된 법정 독립기관으로, 영국의 법률 중 개정이 필요한 부분에 대하여 검토하여 의회에 보고서를 제출하고 영국의회가 이를 수용할지 여부를 검토한다. 위 위원회는 2020년 수색영장에 대한 입법 개선을 위해 보고서를 작성한 바 있다. 위 보고서에 의하면, 영국에는 개별 법률에 약 176개의 수색영장 조항이 있으나 위 규정들은 전자자료와 디지털 증거 수사의 고유한 특성을 제대로 반영하지 못하고 있다고 한다(Law Commission Reforming the Law, "Search warrants", 2020.10.7, 14.2(324면); 14.37(331면); Law Commission Reforming the Law, "Search warrants reform to help law enforcement investigate crime", 2020.10.7(https://www.lawcom.gov.uk/search-warrants-reform-to-help-law-enforcement-investigate-crime/; 최종접속일 2023.9.14.)).

796) 인권협약의 정식명칭은 '인권과 기본적 자유의 보호를 위한 협약(Convention for the Protection of Human Rights and Fundamental Freedoms)'으로, 미국, 독일, 우리나라의 헌법에 규정된 인권, 자유권 등에 대한 보호규정이 포함되어 있다.

797) 2000. 10. 2.부터 시행된 인권법(The Human Rights Act 1998)은 영국에 거주하는 모든 사람들에게 적용되고 경찰을 포함한 공공당국이 침해할 수 없는 권리와 자유에 대하여 규정하고 있다. 인권법(HRA 1998) 제2조 생명권, 제3조 고문이나 비인도적이고 굴욕적인 대우로부터의 자유, 제4조 노예제도 및 강제노동으로부터의 자유, 제5조 자유와 안전에 대한 권리, 제6조 공정한 재판을 받을 권리, 제7조는 형사법정주의(법 없이는 처벌없다), 제8조 사생활과 가족에 대한 권리 등이 형사절차와 관련하여 중요한 의미를 가지고 있다. 영국은 2020. 1. 31. 유럽연합(EU)에서 탈퇴한 후(After Brexit) 유럽연합의 회원국 지위를 상실하였지만, 아직도 인권법은 형사절차의 적법 여부를 결정하는 중요한 판단기준이 되고 있다. 영국 정부는 인권법이 HCHR과 완전히 동일하여 유럽법이 영국법보다 우월하다는 인식을 주기 때문에 인권법을 '영국 권리장전(Bill of Rights)'으로 대체할 것을 제안한 바 있으나 통과되지는 못했다(The British Institute of Human Rights 홈페이지, "What's in the Human Rights Act?"(https://www.bihr.org.uk/get-informed/legislation/whats-in-the-human-rights-act; 최종접속일 2023.9.14.); StudySmarter 홈페이지, "Human Rights Act 1998"(https://www.studysmarter.co.uk/explanations/politics/uk-government/human-rights-act-1998/; 최종접속일 2023.9.14.)).

통신데이터 수집에 관한 "수사권한법 2016(Investigatory Powers Act 2016 : 이하, "IPA")", ④ 암호화된 정보의 해독과 관련한 "수사권한규제법 2000(Regulation of Investigatory Powers Act 2000 : 이하, "RIPA")", ⑤ 전자기기에서 증거를 추출하는 방법 및 절차 등에 관하여 규정한 "경찰, 범죄, 양형 및 법원법 2022(Police, Crime, Sentencing and Courts Act 2022, 이하 "PCSCA")"[798] 및 관련 하위규정, ⑥ 경찰 등 수사기관이 지켜야 할 지침인 '법무부장관의 증거개시에 관한 가이드라인(Attorney General's Guidelines on Disclosure : Supplementary Guidelines on Digitally Stored Material, 2022; 이하, "AG Guidelines")'[799] 순서로 살펴보기로 한다.[800]

나. 경찰 및 형사증거법(PACE 1984)

1) 개요

PACE 1984 Part Ⅱ는 압수·수색 일반규정이라고 할 수 있는데,[801] 수색영장(제8조 내지 제16조), 영장없는 수색(제17조, 제18조), 압수 등(제19조 내지 제22조), 부칙(제23조)으로 구성되어 있다.

2) 영장에 의한 압수·수색

가) 영장의 청구 및 발부

영국 수사기관은 전자정보를 압수하고자 할 때 주로 정보 자체가 컴퓨터, 휴대폰

798) 이 글에서는 PCSCA 중에서 PART 2. CHAPTER 3(Extraction of information from electronic devices, 제37조 내지 제44조) 및 SCHEDULE 3(Extraction of information from electronic devices: authorised persons)으로 그 논의의 범위를 한정한다.

799) 위 법무부장관의 가이드라인은 법적 효력은 없으나 이를 위반한 경우 증거능력이 부정될 수 있다(박지영, 『정보저장매체에 관한 압수·수색제도의 문제점과 개선방안』, NARS 현안보고서 제278호, 국회입법조사처, 2015.12, 23면; Attorney General's Office, "Attorney General's Guidelines on Disclosure -For investigators, prosecutors and defense practitioners-", 2022).

800) 영국의 각 법령에서는 디지털 증거, 디지털 정보라는 표현보다는 '전자데이터(electronic data)'라는 표현을 주로 쓰고, 저장매체라는 표현보다는 '전자기기(electronic device)'라는 표현을 주로 사용하고 있다. 따라서 영국의 디지털 증거 압수·수색에 관한 이 글에서 법령을 소개하는 부분에서는 법문에 충실하게 전자데이터, 전자기기라는 표현을 사용하기로 한다.

801) 영국의 경우 특이하게 수색을 위해 건물의 부지에 들어갈 수 있는 권한(Power of Entry), 즉 '진입권'을 따로 인정하고 있다. 영장에 의한 압수·수색의 일반규정인 Part 2의 제목이 "진입, 수색 및 압수영장(Powers of Entry, Search and Seizure Search warrants)"이다(정희도, 앞의 논문, 130면).

등 전자기기(electronic device)에 대한 압수·수색영장을 청구한다.[802] 이때 영장에는 ① 신청 근거, ② 영장이 발부되는 법령, ③ 수회 출입을 위한 영장인지 여부,[803] ④ 가능한 한 수색 대상인 물품이나 사람을 식별할 수 있도록 하는 정보 등에 대하여 기술하여야 한다.[804]

특히, 영장에는 가능한 한 수색 대상 물품이나 사람을 식별할 수 있도록 특정해야 하는데,[805] 이것은 소유자 등이 압수 또는 수색의 한계를 알 수 있게 하여 압수의 적법성에 이의를 제기할 수 있도록 하기 위한 목적도 있다.[806][807] 다만, 판례는 휴대폰과 같은 전자기기에 저장된 특정한 정보를 압수하는 것이 궁극적 목적인 경우에도 영장의 압수대상에 해당 정보가 아닌 휴대폰 자체를 적시한 것이 PACE 제15조(6)(b)를 위반한 것은 아니라고 판시한 바 있다.[808]

영장을 청구한 경찰은 치안판사(the justice of the peace) 또는 청문판사(judge hearing the application)의 질문에 대하여 선서를 하고 답변을 하여야 한다.[809] 치안판사는 ① 기소대상 범죄가 발생하였고, ② 압수·수색 장소에 범죄 수사에 가치가 있는 물건이 존재하며, ③ 그 물건이 범죄와 관련성이 있고, ④ 해당 물건이 법적 특권(legal privilege)[810]을 가지고 있거나 배제되는 자료(excluded material)[811] 또는 특별절차

---

802) 치안판사협회를 상대로 조사한 바에 의하면 영장 중 81%가 전자기기에 대한 것이라고 한다. 위와 같이 실질적으로 압수·수색하고자 하는 것은 전자데이터이면서도 전자기기에 대한 압수·수색 영장을 청구하는 것은 전자기기와 전자데이터를 서로 연결된 단일한 품목으로 개념화하는 '단일품목이론(the "single item theory")'에 바탕을 두고 있다(Law Commission Reforming the Law, "Search warrants", 2020.10.7, 14.1-14.3, 331-332면).

803) 수색영장은 복수의 출입을 허용하지 않는 한, 원칙적으로 1회 출입만 허용된다. 다만, 복수의 출입을 허용할 경우 그 근거와 무제한 출입을 위한 것인지, 출입 횟수의 상한선을 정하고자 하는 것인지 여부를 영장에 특정하여야 한다(PACE s.15(4)(5)).

804) PACE s.15(2)(a).

805) PACE s.16(6)(b).

806) Lee&Ors v. Solihull Magistrates Court & Anor [2013] EWHC3779(Admin).

807) 뇌물수수 및 자금세탁 사건 수색영장청구서에 압수물건을 '금융서류(financial documentation)'라고만 특정한 것은 금융거래의 성격, 기간 등을 전혀 알 수 없는 무제한의 영장이어서 수색이 불법하다고 판단한 바 있다(R (Brook) v Preston Crown Court [2018] EWHC 2024 (Admin), 42).

808) R (A) v Central Criminal Court and another [2017] EWHC 70 (Admin) at [81], [2017] 1 WLR 3567 at [43]; Cabot Global Ltd & Ors v Barkingside Magistrates's Court&Ors, [2015] EWHC 1458(Admin) at [51], [2015] 2 Cr AppR 26.

809) PACE s.15(4).

810) 법적 면책사항에 관한 자료는 주로 변호사 등 법률가와 의뢰인, 의뢰인과 대리인 사이에 법적 조언을 하는 과정에서 발생한 의사소통의 내용을 의미한다(PACE s.10).

811) 배제되는 자료는 주로 비밀로 관리되어 오던 특별한 자료를 의미한다. 업무상 비밀 등 사적 기록(personal records), 의료 목적 등으로 보관 중인 인간의 세포조직 또는 조직액(human tissue

자료(special procedure material)[812]가 아닌 경우 영장을 발부할 수 있다.[813] 경찰은 허용된 압수·수색의 목적을 달성하기 위하여 필요한 모든 물건을 압수할 수 있다.[814]

나) 영장의 집행: 참여권, 영장 제시, 압수물 기록 교부 등

진입 및 수색영장은 모든 경찰에 의하여 집행될 수 있다.[815] PACE 제16조는 영장의 집행에 관하여 규정하면서 점유자, 관리인 등 다양한 사람의 참여에 대하여 규정하고 있으나, 압수·수색현장에서 피압수자 등이 참여하는 것을 의무사항으로 하고 있지 않다.[816] PACE 제16조 제2항에서는 경찰이 출입 및 수색영장을 집행할 때, 다른 사람이 참여하는 것을 허가할 수 있다고 규정하고 있는데, 이때 참여인(persons to accompany any constable)은 경찰관의 감독 아래에서만 참여할 수 있고, '영장의 집행', '영장과 관련된 물건의 압수' 등에 있어서 경찰과 같은 권한을 갖는다.[817] 참여인의 자격에 관하여는 따로 규정된 바가 없으나 피압수자의 권리보호 차원에서 일반인의 참여로 해석된다.[818]

압수·수색영장은 발부일로부터 3개월 안에 집행되어야 한다.[819] 영장에 따라 출입 및 수색하고자 할 때, 해당 장소의 점유자(the occupier of such premises)가 있는 경우 경찰관 신분을 밝혀야 하고, 만일 경찰관 제복을 입지 않은 경우 경찰관이라는 증빙서류를 제출하여야 하며, 영장을 제시하고 영장 사본을 교부하여야 한다.[820] 압수·수색 당시 점유자가 없으나 해당 장소를 관리하는 것으로 보이는 다른 사람(some other person who appears to the constable to be in charge of the premises is present)이 있는 경우 그 관리자에게 영장을 제시하고, 영장 사본을 교부하여야 한

---

or tissue fluid), 언론자료(journalistic material)의 세 가지 범주로 구성된다(PACE s.11).

812) 특별절차 자료는 주로 배제물품이 아닌 언론자료와, 법적 면책사항에 관한 자료가 아닌 것으로서 업무과정에서 취득한 것으로서 압수·수색 절차 이전에 보관자의 의사 또는 행동, 법률적 의무 등에 의하여 비밀리에 보관되는 자료 등을 의미한다(PACE s.12).

813) PACE s.8(1).

814) PACE s.8(2).

815) PACE s.16(1).

816) 김현숙, 『영국의 PACE 법 연구』, 책임연구보고서 2011-19, 치안정책연구소, 2011.12, 30-40면.

817) PACE s.16(2)(2B).

818) 김무석, "디지털 포렌식 절차상 참여권 보장 방안에 대한 연구", 석사학위논문, 고려대학교, 2019.2, 24-25면; 이규봉, "디지털 증거 압수·수색 과정에서 피압수자 등의 참여 범위", 석사학위논문, 고려대학교, 2021.2, 58면.

819) PACE s.16(3) Entry and search under a warrant must be within three months rom the date of its issue.

820) PACE s.16(5).

다.[821] 압수·수색 장소의 점유자 또는 관리자가 없는 경우 경찰은 영장 사본을 눈에 잘 띄는 장소에 두어야 한다.[822]

PACE 제19조에 의하면, 경찰은 압수가 제한되는 언론, 출판물 등(professional privilege)을 제외하고 합리적인 근거(reasonable grounds)가 있는 경우 영장에 기재되어 있지 않은 것이라도[823] ① 범죄의 결과로 취득한 것, ② 은닉(concealed), 분실(lost), 손상(damaged), 변경(altered), 파괴(destroyed)를 방지하기 위하여 압수가 필요한 물건은 해당 부지[824]에 있는 어떤 것이든 압수할 수 있다.[825] 또한, 경찰은 그가 조사하고 있는 범죄 또는 기타 범죄와 관련된 증거이고, 증거가 은닉, 분실, 변경 또는 파괴되는 것을 방지하기 위해 압수할 필요가 있다고 믿을만한 합리적인 근거가 있는 경우 영장에 기재되지 않았더라도 해당 부지에 있는 모든 물건을 압수할 수 있다.[826]

다) 압수물 목록 교부, 압수물에 대한 접근 및 복사의 허용, 영장 반환 등

경찰은 압수 후에도 영수증을 교부할 의무가 없다.[827] 다만, 압수 후 압수·수색된 장소의 점유자라고 주장하는 자와 압수 직전에 그 물건을 점유 또는 관리하였다고 주장하는 자가 요청하는 경우 그에게 합리적인 시간 내에 압수물 목록(a record of what he seized)을 교부하여야 한다.[828] 다만, 전자기기를 압수한 경우 전자기기 안에 저장된 내용을 품목별로 분류한 상세목록을 제공할 의무는 없다.[829]

경찰이 범죄 수사를 위하여 압수한 물건을 보관 중인 경우, 압수 직전에 압수품을 점유 또는 관리한 자 또는 그 대리인이 수사담당자에게 요청하면 경찰 감독하에 그 물품에 접근할 것을 허용하여야 한다.[830] 압수물의 촬영이나 복사를 요청한 경우

---

821) PACE s.16(6)(b).
822) PACE s.16(7).
823) Law Commission Reforming the Law, 앞의 보고서, 14.51, 334면.
824) 부지(premise)는 일반적인 장소, 자동차, 선박, 비행기, 호버크라프트, 해양 설비, 모든 재생에너지 설치, 텐트 또는 이동식 구조물을 포함한다(PACE s.23.).
825) PACE s.19(2).
826) PACE s.19(3).
827) Richard Stone, 『THE LAW OF ENTRY, SEARCH, AND SEIZURE』, OXFORD UNIVERSITY PRESS, 2013, 107면.
828) PACE s.21(1)(2).
829) Business Energy Solutions Ltd v Crown Court at Preston [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [116].
830) PACE s.21(3).

경찰의 감독 아래 이를 허용하거나 직접 촬영 또는 복사를 해줄 수 있다.[831] 다만, 경찰은 수사 또는 압수와 관련된 범죄 외의 다른 범죄의 수사, 이와 관련된 소송에 방해가 될 수 있다고 판단한 경우 압수물에 대한 접근, 촬영 또는 복사를 불허할 수 있다.[832] 영장은 집행한 후 법원의 담당공무원 등에게 반환하여야 하고,[833] 반환된 영장은 12개월 동안 보관되어야 한다.[834]

라) 압수물 보관[835]

경찰은 PACE 제19조, 제20조에 따라 압수한 자료를 필요한 기간 동안 보관할 수 있는 일반적 권한이 있다.[836] (a) 범죄수사를 목적으로 압수된 것은 재판에서 증거로 사용하기 위해 또는 디지털 포렌식 검사(forensic examination), 관련 범죄 수사를 위해 필요한 경우,[837] (b) 범죄를 통해 얻은 것이라고 믿을만한 합리적인 근거가 있는 경우 합법적인 소유자를 파악하기 위해 수사기관에서 보관할 수 있다.[838] 다만, 범죄수사 목적으로 압수한 물건은 사진 또는 사본으로 그 목적을 달성할 수 있는 경우라면 계속 보관할 수 없다.[839]

3) 영장 없는 진입, 수색 및 압수

가) 체포를 위한 진입 및 수색

경찰은 찾고자 하는 사람이 해당 부지에 있다고 믿을만한 상당한 이유가 있으면 ① 체포영장의 집행, ② 기소 가능한 범죄를 범한 자의 체포를 위해, ③ 특정한 범죄를 범한 사람을 체포하기 위해[840] 어떤 부지(premises)에든 영장 없이 들어가 수색할 수 있다.[841]

---

831) PACE s.21(4).
832) PACE s.21(8).
833) PACE s.16(10).
834) PACE s.16(11).
835) 경찰 등 법집행기관이 압수물의 보관 또는 보유하는 것과 관련하여 PACE 제22조, CJPA 제53조 등 여러 법률에 중복된 규정이 산재해 있고, 수색영장이 집행된 후 압수된 경우에도 이러한 여러 규정이 중복하여 적용되기도 한다(Law Commission Reforming the Law, 앞의 보고서, 14.73, 342면).
836) PACE s.22(1).
837) PACE s.22(2)(a).
838) PACE s.22(2)(b).
839) PACE s.22(4), (2)(a).
840) PACE s.17(1)(c)-(cab).

나) 체포 시의 진입, 수색 및 압수

PACE 제32조에 의하면, 용의자를 '경찰서 이외의 장소'에서 체포한 경우 그가 행한 범행이 기소 가능한 범죄라면 체포 시의 건물 부지 또는 체포된 사람이 체포 직전에 떠난 장소에 들어가 범죄 관련 증거를 수색할 권한이 있고,[842] 범죄의 증거이거나 범죄를 저지른 결과로 얻은 것이라고 합리적으로 믿을만한 근거가 있는 경우 이를 압수하여 보유할 수 있다.[843][844] 이때, 경찰은 범죄와 관련한 어떤 목적으로 사용하고 있었다고 믿을만한 합리적인 근거가 있는 모든 차량을 수색할 수 있다.[845]

PACE 제32조는 PACE 제18조와 달리 경찰에게 체포된 사람이 해당 장소 등을 소유하거나 관리 또는 통제하고 있었는지 여부와 관계없이 그 부지를 수색할 수 있는 권한을 부여한다.[846] 위 규정은 체포 시로부터 어느 정도의 시점까지가 근접한 시점인지 규정하고 있지는 않지만, 경찰이 체포 후 몇 시간 후 구내로 돌아와서 수색하는 것까지 허용하는 것은 아니다.[847] 이 경우 PACE 제18조에 의한 수색이 가능할 수는 있다.

한편, 체포된 사람이 자기 또는 타인에게 위험을 초래할 수 있다고 믿을만한 합리적인 근거가 있는 경우에는 체포된 사람을 수색할 수 있고,[848] 자기 또는 타인의 신체에 상해를 입히는 데 사용될 수 있는 모든 것을 압수하고 보유할 수 있다.[849]

다) 체포 후의 진입, 수색 및 압수

PACE 제18조에 의하면, 경찰은 '기소 가능한 범죄'로 체포된 사람이 점유하거나

---

841) 그 외에도 불법하게 도망 중인 자를 추적하거나 체포하기 위한 경우, 생명이나 신체를 구하거나 재산에 대한 심각한 피해를 방지하기 위해서도 진입하여 수색할 수 있다(PACE s.17(1)(cb),(d),(e)).

842) PACE s.32(2)(b).

843) PACE s.32(9)(a).

844) 그 외에도 체포된 사람이 합법적인 구금상태에서 탈출하는 데 도움이 될 수 있는 경우에도 체포된 사람을 수색할 수 있고, 그러한 물건이라고 믿을만한 합리적인 근거가 있는 경우 압수하여 보유할 수 있다(PACE s.32(2)(a), 32(9)(a)).

845) David Ormerod CBE, KC(Hon), David Perry QC, 『Blackstone's criminal practice』, Blackstone Press, 2023, 1555면.

846) David Ormerod CBE, 앞의 책, 1555면.

847) PACE s.32와 관련하여, 체포 후 2시간 10분 후에 수색한 것은 위법하다고 판시한 바 있다(R(Hewiston) v Chief Constable of Dorset Police [2003] EWHC 3296(Admin)(David Ormerod CBE, KC(Hon), 앞의 책, 1556면 재인용)).

848) PACE s.32(8),(1).

849) PACE s.32(9),(1).

관리한 건물의 부지 안에 법적 특권(legal previlege)이 있는 항목이 아닌, 체포된 범죄와 관련되거나 체포된 범죄와 연결되거나 유사한 다른 범죄의 증거가 있다고 믿을만한 '합리적인 이유'가 있는 경우에는 그 건물의 부지에 들어가 수색할 수 있고,[850] 수색할 수 있는 것을 압수하고 보유할 수 있다.[851] 이때, 수색은 증거를 발견할 목적으로 합리적으로 요구되는 범위까지만 허용된다.[852]

PACE 제32조가 체포 시점에서의 건물의 부지 진입수색권을 규정한 것이라면, PACE 제18조는 기소 가능한 범죄로 체포된 피체포자가 점유하거나 사용한 건물의 부지라면 어디든 진입하여 수색할 수 있다[853]는 점에서 제18조가 더 광범위한 수색권을 인정하고 있는 것이라고 할 수 있다. 다만, 체포된 범죄와 관련성이나 연결성, 또는 유사한 범죄의 증거가 있다고 믿을만한 '합리적인 이유'를 요건으로 하여 그 범위를 제한하고 있다. 즉, 피체포자가 체포된 범죄와의 관련성이 있거나 그 범죄와 연결되거나 유사한 범죄의 증거가 있다고 믿을만한 합리적인 사유가 있어야 한다. 따라서 절도 범죄로 체포된 피의자의 집에서 마약을 수색한 것은 위 조항에 의한 적법한 수색이라고 할 수 없다.[854] 피체포자가 관리하거나 점유하였다는 이유만으로 영장 없이 모든 장소에 진입하여 수색하는 것을 허용하게 되면 개인의 자유권에 대한 지나친 침해가 되기 때문에 범죄와의 관련성이라는 제한을 둔 것이다.[855]

라) 기타 압수

PACE 제19조는 경찰이 영장 또는 법령, 피수색자의 동의에 의한 것이든 일단 적법하게 진입한 상태에서 발견한 일정한 물건에 대하여 별도의 영장을 발부받지 않고 압수할 수 있는 권한을 인정하고 있다. 앞서 살펴본 바와 같이 범죄 실행의 결과로 획득하였다고 믿을만한 상당한 이유가 있거나 수사 중인 범죄 또는 다른 범죄와 관련된 증거가 발견되고, 그 증거의 은닉, 분실, 손상, 변경, 파괴를 방지하기 위하여 압수가 필요한 물건이면 이를 영장 없이 압수할 수 있다.[856] 다만, 법적 특권의 대상이

850) PACE s.18(1).
851) PACE s.18(2).
852) PACE s.18(3).
853) 정희도, 앞의 논문, 138면,
854) Jeffrey v. Black[1978] Q. B. 490.
855) 정희도, 앞의 논문, 139면.
856) PACE s.19(2),(3).

되는 것은 압수할 수 없다.[857]

위와 같은 권한은 다른 권한에 추가되는 것으로[858] PACE 제32조 체포 시의 진입 및 수색, 제18조 체포 후의 진입 및 수색에 근거하여 영장 없이 구내에 적법하게 들어간 상태에서, 경찰은 범죄 관련 증거를 수집하기 위하여 별도의 영장 없이도 그가 가지고 있는 휴대폰 등 전자기기를 검색하여 문자메시지, 사진, 통화기록 등 저장된 내용을 수색할 수 있고 변경, 파괴 등의 위험이 있으면 휴대폰 등을 압수할 수 있다.

4) 전자정보 압수·수색과 관련한 특별규정

가) 가시성, 가독성 있는 자료 제공 요구

PACE 제19조 제4항[859] 은 전자정보의 압수 전 단계에 관한 규정으로, "① 경찰이 수사하고 있는 범죄 또는 기타 범죄와 관련된 증거이거나 범죄를 저지른 결과 취득한 것으로, ② 은닉, 분실, 조작 또는 파괴되는 것을 방지하기 위해 필요한 경우라고 합리적으로 믿을만한 근거가 있는 경우 ⓐ '전자적으로 저장(*stored in any electronic form*)'되고, 부지에서 접근할 수 있는 모든 정보를 ⓑ 가져갈 수 있고 보고 읽을 수 있는 형태로 제공하거나, ⓒ '보고 읽을 수 있는 형태로 쉽게 생성될 수 있는 것(*from which it can readily be produced in a visible and legible form*)'으로 제공하도록 요구할 수 있다"고 규정하고 있다.

나) 압수 권한의 확대

PACE 제20조[860]에서는 전산화된 정보에 대한 압수 권한을 명문으로 인정하여,

---

857) PACE s.19(6).

858) PACE s.19(5).

859) PACE s.19(4) The constable may require any information which is [F1 *stored in any electronic form*] and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible [F2 or *from which it can readily be produced in a visible and legible form*] if he has reasonable grounds for believing—
(a) that—
(i) it is evidence in relation to an offence which he is investigating or any other offence; or
(ii) it has been obtained in consequence of the commission of an offence; and
(b) that it is necessary to do so in order to prevent it being concealed, lost, tampered with or destroyed. (밑줄은 필자에 의한 것으로 CJPA 2001이 제정된 이후 추가된 부분이다.)

860) PACE s.20. Extension of powers of seizure to computerised information.

"이 법에 규정되는 모든 압수 권한에는 해당 부지에서 접근 가능한 컴퓨터에 '전자적 형식으로 저장된(stored in any electronic form)' 모든 정보를 가져갈 수 있고 보고 읽을 수 있는 형태로 제공하거나, ⓒ '보고 읽을 수 있는 형태로 쉽게 생성될 수 있는 형태로(from which it can readily be produced in a visible and legible form)' 제공할 것을 요구할 수 있는 권한이 포함된다"고 규정하여 기존의 압수 권한을 확대하였다.[861] 위 조항은 법원의 영장 또는 명령이 아닌 수사기관의 명령으로, 피압수자에게 필요한 디지털 정보의 제출을 요구하고, 필요한 경우에 제3의 장소로 이동한 후 분석을 통해 가시성 및 가독성이 있는 상태로 만들 것을 요구할 수 있는 권한을 부여하고 있다.[862] 물론, 수사기관은 이러한 명령을 하는 대신 전자기기 또는 이에 저장된 정보에 대한 영장을 별도로 발부받아 압수할 수도 있다. 위 규정은 PACE 제8조, 제18조, 별표 13의 1(schedule 1 para 13)에 의한 압수 권한에 한정하지 않고 다른 법령에 의한 압수 권한에도 적용되는 것으로[863] 수사기관의 전자정보에 대한 압수 권한을 전반적으로 확대한 것으로 볼 수 있다.

다만, 저장매체를 그대로 이미징한 경우에는 원본을 압수할 필요가 없고,[864] 현장에서 전체 이미징이 어려운 경우 다른 곳에서 검색하기 위하여서 저장매체 자체를 수색 현장에서 제거하여 다른 장소로 이동하여야 한다. 정보저장매체 원본이 압수된 경우 합리적으로 실행이 가능한 경우 해당 자료의 소유자를 위하여 자료를 복사하거나 이미지 복사할 준비가 되어 있어야 한다.[865]

---

(1) Every power of seizure which is conferred by an enactment to which this section applies on a constable who has entered premises in the exercise of a power conferred by an enactment shall be construed as including a power to require any information [F1 *stored in any electronic form*] contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible [F2 or *from which it can readily be produced in a visible and legible form*]. (밑줄은 필자에 의한 것으로 CJPA 2001이 제정된 이후 추가된 부분이다.)

861) PACE s.20은 PACE 이전에 제정된 법률, PACE s.8(Power of justice of the peace to authorise entry and search of premises) 및 s.18(Entry and search after arrest), 별표 1의 제13항, PACE 이후에 제정된 법률에 적용된다(PACE s.20(2)).

862) 수사기관의 제출명령이 인정되는 것이다(박병민·서용성, 앞의 연구보고서, 324면).

863) PACE s.20(2).

864) AG Guidelines, Annex A-Digital Material para. 16. (2022).

865) The Home Office, "Police And Criminal Evidence Act 1984 Codes of Practice Code B", 2013, para 7.17.

다) 법률 개정의 의미

1984년 PACE 제정 당시 제19조, 제20조는 '컴퓨터 안에 보관된 자료(in a computer)'를 '가져갈 수 있고 보고 읽을 수 있는 형태(in a form in which it can be taken away and in which it is visible and legible)'로 제공하는 것만을 압수방법으로 규정하였다. 위 규정은 컴퓨터와 같은 저장매체 또는 독립형 네트워크에 저장된 디지털 정보를 종이에 인쇄하여 제출받는 것을 전제로 만들어진 것이다.[866] 위 규정의 문언적 해석에 따르면, 정보가 프린트된 서류는 눈으로 볼 수 있고, 읽을 수 있기 때문에 위 조건을 만족시키지만, 정보를 복사한 저장매체는 이에 해당하지 않아서 정보를 저장매체에 복사하여 줄 것을 요구할 수는 없었다.[867]

그러나 2001년 CJPA에 의하여 PACE 제19조 제4항, 제20조 제1항이 개정되면서 ⓐ '전자적으로 저장되어 있고(stored in any electronic form)', 접근 가능한 어떤 형태의 전자정보에 대하여서 ⓒ '보고 읽을 수 있는 형태로 쉽게 생성되도록(from which it can readily be produced in a visible and legible form)'이라는 문구가 추가되었다. 따라서 경찰은 컴퓨터 등 특정 저장매체에 저장된 정보에 한정하지 않고 어떠한 방식으로 어디든 전자적으로 저장되기만 하면 제출을 요구할 수 있게 되어[868] 인터넷 서버 등 네트워크에 저장된 정보에 대하여도 제출요구를 할 수 있게 된 것이다. 또한, 정보를 제공받을 수 있는 방법도 프린트된 인쇄물에 한정하지 않고 보고 읽기 쉬운 형태(in visible and legible form)인 하드카피의 형태로 요구할 수 있게 되었다.[869][870]

다만, 위 제19조 제4항과 제20조는 해당 정보 등의 생산을 요구할 수 있다는 규정일 뿐 이것에는 압수 권한을 규정한 것은 아니어서 정보를 생산한 이후에 PACE 제19조 제3항과 같은 별도의 압수 권한 규정이 있어야 정보에 대한 압수가 이루어질 수 있다.[871] 한편, PACE 제19조, 제20조에는 위와 같이 저장된 정보를 복사하여 제공하는 사람이 해당 장소의 점유자인지, 컴퓨터의 소유자인지, 자료에 접근할 수 있는 권한을

---

866) Richard Stone, 앞의 책, 26면.
867) 정희도, 앞의 논문, 129면.
868) 즉, 컴퓨터, 메모리카드 등이 아닌 인터넷 서버, 클라우드 등에 전자적으로 저장된 경우를 포함한다.
869) Richard Stone, 앞의 책, 27면.
870) CJPA s.63(1)에서 압수 권한에 사본을 가져가는 것을 포함시키면서 PACE s.20(1)과 함께 디지털 증거의 압수·수색의 방법으로 복사본의 취득이 인정되었다고 할 수 있다.
871) Richard Stone, 앞의 책, 107면.

가진 사람인지 명확히 규정되어 있지 않다. 따라서 개별적인 상황에 따라 관련 법령에서 정한 조건에 따라 제출자가 달라진다고 할 수 있는데, 경찰은 일반적으로 정보를 제공할 수 있는 능력이 있는 사람이면 누구에게나 제출요구를 할 수 있는 것으로 해석된다.[872]

5) 동의에 의한 수색

PACE Code B(이하, "Code B")는 PACE를 실행하는 경찰의 직무규칙으로 수색, 압수 및 보유에 대하여 규정하고 있고, Code B. para 5에서 동의에 의한 수색을 허용할 수 있는 요건을 규정하고 있다.

경찰은 해당 장소에 출입을 허용할 수 있는 책임자의 동의를 얻어 수색을 제안하는 경우, 가능하다면 권한 및 권리통지서를 서면으로 제공하여야 한다.[873] 또한, 수색 동의를 얻기 전에 경찰은 수색의 목적 및 범위를 명시하고 압수·수색의 대상을 명확히 하여야 하며, 그 사람에게 수색에 동의할 의무가 없고 수색이 시작되기 전 또는 도중에라도 언제든지 동의를 철회할 수 있으며 압수된 모든 것이 증거로 제시될 수 있음을 분명히 알려야 하고, 대상자에게 범죄 혐의가 없는 경우 그러한 사실 역시 수색의 목적을 설명할 때 말해주어야 한다.[874] 만일, 수색이 완료되기 전에 동의를 철회한 경우 수색을 계속할 수 없고, 협박에 의하여 동의를 얻은 경우 해당 장소에 들어가 수색할 수 없다.[875] 동의를 구하는 것이 당사자에게 과도한 불편을 초래하는 경우 이를 생략할 수 있다.[876] 대상자의 동의를 얻어 수색하는 과정에서 범죄의 증거라고 믿을만한 합리적인 근거가 있거나 범죄를 저지른 결과 획득한 물건으로 은닉, 분실, 변경, 손상, 파괴를 방지하기 위하여 필요한 경우 영장 없이 압수할 수 있다.[877]

정보저장매체 역시 소유자의 동의를 받아 압수할 수 있는데, 이때 증인이나 고소인(witness/complainant)으로부터 디지털 자료를 제출받을 때 개인 및 사생활에 대한 최소한의 침해 수단을 사용하여야 한다.[878] 압수 또는 생성 명령 등이 불가능한 경우

872) Richard Stone, 앞의 책, 107면.
873) PACE Code B. para 5.1.
874) PACE Code B. para 5.2.
875) PACE Code B. para 5.3.
876) PACE Code B. para 5.4.
877) PACE Code B. para 7.1.

수사기관은 저장매체 또는 데이터 소유자의 동의를 받아 디지털 자료를 획득하기도 하는데, 저장매체에는 대량의 정보가 혼재되어 제출되기 때문에 특정 데이터 보호 문제가 발생한다.[879] 이에 대하여 영국 정보국장 역시 휴대폰을 동의를 받아 압수·수색하는 각 지역 경찰마다 데이터 보호법(Data Protection Act 2018)[880]에 대한 일관되지 않은 이해와 적용으로 동의의 요건, 범위 등에 있어 명확하지 못한 등 많은 문제점이 있다고 비판한 바 있다.[881] 동의에 의한 디지털 저장매체 압수·수색에 관하여는 최근에 제정된 경찰, 범죄, 양형 및 법원법 2022(Police, Crime, Sentencing and Courts Act 2022, 이하 "PCSCA")에서 구체적으로 살펴보기로 한다.

다. 형사사법 및 경찰법(CJPA 2001)

1) 개요

형사사법 및 경찰법(Criminal Justice and Police Act 2001 : 이하, "CJPA")은 범죄와 알코올로 인한 무질서에 보다 효과적으로 대처하기 위하여 경찰에 막강한 권한을 부여한 법으로 압수·수색 권한에 대해서도 추가적인 권한을 부여하고 있다.[882] 다만, 이 글에서는 디지털 정보와 관련된 압수·수색 권한의 확대에 관해서만 살펴보기로 한다.

2) 압수대상에 정보(information) 명시, 압수방법에 '복사(copy)' 포함

CJPA Part 2에서는 압수 권한(Power of Seizure)에 관하여 규정하고 있는데, 위 법 제66조 제1항은 "모든 형태로 기록된 정보도 문서에 포함한다"[883]고 규정하고 있어서 압수·수색의 대상에 '정보'가 포함된다는 것을 명문화하였다. 한편, 제63조 제1항에서 압수 권한에 "복사하여 가져가는 것을 포함"[884]하면서 사본과 원본의 동일

878) AG Guidelines, Annex A-Digital Material para. 12. (2022).
879) Law Commission Reforming the Law, 앞의 보고서, 14.72, 342면.
880) DPA s.35(2)(1).
881) Information Commissioner's Office, "Investigation report: Mobile phone data extraction by police forces in England and Wales", 2020.6, 53면(https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/; 최종접속일 2023.9.14.).
882) Criminal Justice and Police Act 2001 Explanatory Notes(https://www.legislation.gov.uk/ukpga/2001/16/notes/division/2; 최종접속일 2023.9.14.).
883) CJPA s.66(1).
884) CJPA s.63(1)(a).

성을 인정하고,[885] 제50조 제2항에는 전자적 형태로 보존된 자료를 하드카피하는 것도 압수 권한에 포함하여, 디지털 증거의 압수방법으로서 복사 또는 복사하여 하드카피에 저장하는 방식을 압수의 한 형태로 규정하였다.

3) 압수 권한의 확대

CJPA 제50조에서는 경찰이 압수·수색 장소에서 대량의 압수대상물을 발견하여 그 자리에서 바로 관련성 등을 판단하는 것이 시간적으로나 장소적으로 불가능한 경우, 압수대상에 해당하는지 여부를 판단하기 위하여 일단 대상물을 수색 장소 밖으로 가지고 나올 수 있는 권한을 부여하고 있다.[886] 다만, 병원, 기업 등과 같은 영업장소에서 이와 같이 원본을 압수하여 가지고 나오는 경우 그 소유자에게 심각한 피해를 줄 수 있기 때문에 이러한 권한은 최소의 범위 내에서 행사하여야 한다.[887]

위 규정이 디지털 증거에 적용된다는 명시적인 표현은 없지만, 주로 디지털 증거의 압수·수색에서 많이 문제된다. 디지털 증거의 경우 범죄사실과 관련된 정보(이하, "유관정보")와 그렇지 않은 정보(이하, "무관정보")가 혼재되어 저장매체에 저장되고, 저장매체를 열기 전에는 어떤 정보가 들어 있는지 알 수 없기 때문에 현장에서 유관정보만을 압수하기가 쉽지 않다. 영국 수사기관은 저장매체에 대한 수색영장을 집행할 때, 현장에서 저장매체 전체를 이미징하기보다는 저장매체 원본을 압수한 후 압수·수색 현장 외부에서 디지털 포렌식을 통해 이미징, 탐색 및 분석 조사를 하고 있다.[888]

CJPA 제50조 제1항은 경찰이 합법적으로 부지(Premises)에 들어온 것을 전제로, 그가 수색할 권한이 있다고 믿을 수 있는 합리적인 근거가 있는 물건과 관련되어 있다. 경찰이 적법하게 수색하는 과정에서 해당 물건이 압수대상에 해당하는 것인지 여부를 모든 상황에 비추어 합리적으로 결정하기 어려운 경우 일단 위 규정에 따라 압수할 수 있다.[889]

---

885) CJPA s.63(1)(b).

886) 이것은 대량의 정보 또는 물건을 압수하는 경우 압수·수색 장소 또는 사람으로부터 정보저장매체 또는 물건을 압수한 다음 다른 장소에서 이를 조사 또는 분석할 수 있도록 권한을 부여한 것이다. 즉 디지털 증거 압수·수색의 측면에서 보면, 압수와 조사분석을 다른 장소에서 할 수 있도록 2단계 절차를 인정한 것으로 볼 수 있다.

887) PACE Code 7.7.

888) 영국의 경우, 압수된 전자기기를 경찰이 아닌 상업용 디지털 포렌식 서비스 제공업체에 아웃소싱 방식으로 제공하여 포렌식을 하기도 한다(Law Commission Reforming the Law, 앞의 보고서, 350면).

한편, CJPA 제50조 제2항은 적법한 수색의 과정에서, 수색자가 적법하게 압수할 수는 있지만 다른 압수할 수 없는 것이 포함되어 있고, 그것을 분리하는 것이 모든 상황 비추어 합리적으로 실행 가능하지 않다면 전체를 압수하는 것을 허용한다. CJPA 제50조 제1항은 법적 특권(Legal Privilege)이 있는 자료의 경우 그 압수 권한이 확장되지 않으나, 제2항의 경우 법적 특권이 있는 자료에도 그 압수 권한이 확장되기 때문에 법적 특권이 인정될 수 있는 자료가 혼재되어 있고 분리 불가능한 경우 그 자료까지 포함하여 압수할 수 있다.[890] 따라서 CJPA 제50조 제2항의 압수범위가 제1항보다는 광범위하다고 할 수 있다.[891]

CJPA 제50조 제1항의 압수 권한 내의 물건인지 결정하기가 합리적으로 어려운 경우 또는 같은 조 제2항을 분리하는 것이 가능한지 합리적으로 여부를 판단함에 있어 ① 해당 장소에서 결정하는 데 걸리는 시간 및 분리에 필요한 시간, ② 이를 수행하는 데 필요한 사람의 수, ③ 이것이 재산상 피해를 수반하는지 여부, ④ 분리 등에 사용할 필요가 있는 기구 또는 장비, ⑤ 분리가능성이 있거나 해당 장소에서 합리적으로 실행 가능한 유일한 수단인 경우 분리하여 압수한 물건의 일부 또는 전부를 사용할 수 없게 되는지 여부 등이 고려되어야 한다.[892]

CJPA 제50조 제2항은 특히, 디지털 증거의 특성을 고려한 조항이라고 할 수 있다. 예를 들어, 압수대상 문서가 컴퓨터 하드 드라이브에 전자적으로 저장된 경우로 해당 문서가 삭제되었지만 복구 가능한 경우 수색하는 경찰이 현장에서 해당 문서만 분리하는 것이 합리적으로 가능하지 않기 때문에 CJPA 제50조 제2항에 따라 적법하게 저장매체인 컴퓨터 자체를 압수할 수 있다.[893] 어떠한 사람에 대한 합법적인 수색을 수행하는 경우에도 그 사람이 압수할 물건에 해당하는지 여부를 판단함에 있어서도 위와 같다.[894]

정리해 보자면, CJPA 제50조는 대량의 혼재된 정보가 압수·수색의 대상인 경우 경찰에 무관정보까지 압수·수색 현장 밖으로 가지고 나올 수 있도록 추가적인 압수

889) CJPA s.50(1).
890) CJPA s.50(4).
891) Richard Stone, 앞의 책, 128면.
892) CJPA s.50(3).
893) Richard Stone, 앞의 책, 127-128면.
894) CJPA s.51.

권한(Additional powers of seizure)을 부여한 것이라고 할 수 있다.[895] 다만, 불가분하게 연결된 자료(inextricably linked material)는 자료의 출처를 밝히거나 무결성을 제공하는 것 이외에 다른 목적으로 조사, 이미지, 복사 또는 사용할 수 없다.[896][897]

4) 압수 후 통지

CJPA 제50조, 제51조에 따라 압수한 경우 수사관은 압수·수색 장소의 점유자 또는 관리자에게 서면에 의하여 압수한 물건, 권한의 근거, 압수의 효과, 압수된 물건과 관련하여 사법 당국에 통지받을 사람의 이름, 주소를 명시하고, 압수물 반환 신청 방법, 초기 조사[898] 참여방법, 초기 조사 참여권자의 이름, 주소를 명시한 '서면'으로 통지를 하여야 한다.[899] 압수·수색 대상이 사람인 경우에도 마찬가지이다.[900] 해당 장소에 점유자가 없는 경우 해당 장소를 책임지고 있는 다른 사람에게 통지하고, 아무도 없는 경우 위와 같은 내용을 담은 통지서(Notice)를 눈에 잘 띄는 장소에 부착하여야 한다.[901] CJPA 제52조에 근거한 압수 후 통지는 점유자 등의 요청에 따른 PACE 제21조 제1항 압수물 목록 제공의무에 추가된 것이라고 해석된다. 이때 통지의무는 압수된 물건을 품목별로 분류하여 종합 목록을 제공할 의무까지 포함하는 것은 아니다.[902] 즉, 컴퓨터를 압수한 후 압수통지를 할 때, 압수한 물건을 특정함에 있어 컴퓨터, 휴대폰 메모리 등 전자기기 안에 저장된 내용을 나열하여 세부 목록을 작성할 필요는 없다.[903] 한편, 판례는 수사기관이 압수 후 CJPA 제52조의 통지를

---

895) Richard Stone, 앞의 책, 127면.

896) PACE Code B, Notes for guidance 7H Paragraph 7.14 (ii) applies if inextricably linked material is seized under the Criminal Justice and Police Act 2001, sections 50 or 51. Inextricably linked material is material it is not reasonably practicable to separate from other linked material without prejudicing the use of that other material in any investigation or proceedings. For example, it may not be possible to separate items of data held on computer disk without damaging their evidential integrity. Inextricably linked material must not be examined, imaged, copied or used for any purpose other than for proving the source and/or integrity of the linked material; 박지영, 앞의 연구보고서, 24면.

897) AG Guidelines Annex A-Digital Material para. 23. (2022).

898) CJPA s.53(2).

899) CJPA s.52(1),(2).

900) CJPA s.53(4).

901) CJPA s.53(3).

902) Law Commission Reforming the Law, 앞의 보고서, 14.75, 344면

903) 위 판례에서 법원은 휴대폰, 컴퓨터를 압수한 후 그 안에 저장된 정보의 내용을 분류하여 압수할 물건에 대한 특정한 통지서를 요구하는 것은 실행 불가능한 것을 요구하는 것이라고 하는 경찰의

하지 않았다고 하더라도 위 통지가 합법적인 압수의 전제조건이 아니므로, 제50조에 근거한 압수가 반드시 위법하게 하는 것은 아니라고 하면서 이것은 압수에 대한 이의신청에 관한 CJPA 제59조 또는 불공정한 증거의 배제에 관한 PACE 제78조에서 고려될 문제라고 판시한 바 있다.[904]

5) 압수물 보관, 참여권, 데이터의 합법적 처리

CJPA 제50조, 제51조에 따라 압수된 물건은 다른 자료와 별도로 안전하게 보관하여야 하고,[905] CJPA 제53조에 따라 어떤 자료가 계속 보유할 수 있는 자료인지 결정하기 위한 조사 과정에 피압수자 또는 이해관계인이 참여할 수 있는 기회를 제공하여야 하며, 이때 경찰은 이해관계인 등의 참석 요청을 수용하기 위해 합당한 조치를 취하여야 한다.[906] CJPA 제53조는 압수된 물건에 대한 최초의 조사단계에서 하는 작업에 관한 것으로, 합리적으로 가능한 한 빨리 진행되어야 하고, 위와 같은 조치는 CJPA 제50조 및 제51조에 따라 압수한 경우에만 적용된다.[907] 수사기관은 하드카피에 대해 수색, 분석절차의 모든 과정을 기록할 필요는 없고, 저장된 수백 건의 수색이나 분석에 대하여도 기록을 만들 필요는 없다. 다만, 해당 자료의 탐색, 분석과정에서 합리적인 수색, 분석이 진행되었음을 보여주기 위해 참여의 기회를 보장하여야 한다.[908]

수사기관이 보관할 수 있는 자료는 (a) 사건의 증거 또는 잠재적으로 증거가 될 수 있는 자료, (b) 증거자료가 보관되어 있는 경우 그 증거자료와 합리적으로 분리하는 것이 불가능하게 불가분적으로 연결된 비관련 자료,[909] (c) 수사와 관련되어 있고, 아직은 미사용(미제출) 자료이지만 제출이 계획되어 있는 자료,[910] (d) 그 자체로는

주장에 동의하였다(Business Energy Solutions Ltd v Crown Court at Preston [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [116]).

904) R (Dulai) v Chelmsford Magistrates' Court [2012] EWHC 1055 (Admin), [2013] 1 WLR 220 at [59, 60].

905) 증거 또는 관련 자료(a)가 관련성이 없는 자료(b)와 불가분하게 연결되어 있거나 조사 또는 절차에서 다른 자료의 사용을 침해하지 않고 연결된 다른 자료와 분리하는 것이 합리적으로 불가능한 경우에는 해당 자료(b)도 보관할 수 있다(AG Guidelines, Annex A-Digital Material para. 22. (2022)).

906) PACE Code 7.7 내지 7.8.

907) Law Commission Reforming the Law, 앞의 보고서, 14.78, 345면.

908) AG Guidelines, Annex A-Digital Material para. 49. (2022).

909) PACE Code B para. 7.

910) CPIA s.23(1), CPIA Code para 5.1, 5.2에 의하면, 수사관의 기록 및 압수물 보관의무에 대하여 정하고 있다. 수사관은 범죄수사에서 획득한 수사 관련 자료의 원본 또는 사본을 보관할 의무가

관련자료가 아닐 수 있지만, 아직 미사용 관련 자료와 불가분하게 연결된 자료[911]가 있다.[912] (a)와 같이 전자자료를 증거 목적으로 보관하는 경우 그 출처 및 연속성을 입증할 목적으로 전자자료 전체 또는 이미징한 사본을 보관할 필요가 있고, 이 경우 영장의 범위를 벗어난 것처럼 보이는 전자데이터도 1996년 형사절차 및 수사법(Criminal Procedure and Investigations Act 1996 ; 이하, "CPIA")에 따라 보관할 필요가 있다.[913] 즉, 증거의 무결성 등을 입증하기 위해 전자자료 전체를 보관하여야 할 필요가 있는 경우에는 이를 허용한다.

위 보관 가능한 자료 외에는 CJPA 제53조 내지 제55조에 따라 제출자에게 반환되어야 한다.[914] 이때, 자료의 반환(return)은 원래 영장의 범위에 포함되지 않는 자료를 삭제할 의무가 포함될 수 있고, 복사된 전자자료의 반환의무에는 복사본의 삭제가 포함될 수도 있다.[915] 다만, 반드시 복사된 자료를 삭제하여야 하는 것은 아니고 합리적 분리의 실행가능성에 따라 삭제 여부가 달라진다. 이때 합리적 분리의 실행가능성은 물리적 또는 기술적인 가능성을 의미하는 것이 아니고, 실질적이고 실용적인 관점에서의 실행가능성을 의미한다. 즉, 물리적 또는 기술적으로 분리가능한 경우에도 반드시 해당 자료를 삭제하여야 하는 것은 아니다.[916]

다만, 법적 특권이 인정되는 자료의 경우 합법적으로 압수된 후 해당 자료를 합리적으로 분리하기 불가능한 경우에만 보관할 할 수 있고, 분리가 가능한 경우 압수된 자료의 전체 조사 없이도 압수한 후 가능한 한 빨리 반환하여야 한다.[917] 이것은

있다. 특히 수색영장 집행 후 압수된 자료의 경우 관련 자료 또는 관련 자료의 사본을 보관할 의무가 있다.

911) PACE Code B para. 7.

912) AG Guidelines, Annex A-Digital Material para. 24. (2022).

913) AG Guidelines, Annex A-Digital Material para. 24(a). (2022).

914) AG Guidelines, Annex A-Digital Material para. 25. (2022).

915) 수사기관이 피고인의 사기 혐의에 대하여 여러 개의 수색영장을 발부받아 컴퓨터 장치를 압수하여 압수된 장비는 총 53테라바이트이고, 컴퓨터에 저장된 문서는 2억 개 이상이며 오디오 녹음은 약 77만개에 이른 사건에서, 피고인이 압수물반환 신청을 하자 형사법원이 이를 거부하였다. 이에 대하여 피고인이 행정소송으로 압수한 컴퓨터 장치에서 수사기관이 복사한 데이터가 CJPA 2001의 53(2), (3)에 따라 반환될 수 있는 재산이라며 반환청구를 한 사안이다(Business Energy Solutions Ltd v Crown Court at Preston [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [83]).

916) Business Energy Solutions Ltd v Crown Court at Preston [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [89].

917) CJPA s.55.

언론의 취재원 비밀유지권과 관련된 자료 등 특별한 취급이 인정되는 자료의 경우도 마찬가지이다.[918] CJPA 제53조 내지 제56조의 규정에 따른 압수물의 보관은 다른 법률의 관련 규정에 의하여 해당 물건에 대한 보유가 허용되는 것을 전제로 한다.[919] 따라서 다른 법률에 의해 수사기관의 보유를 허용하지 않는 자료를 CJPA에 근거하여 보관할 수는 없다.

수색영장 집행 후 압수한 전자데이터에 개인정보가 포함된 경우 2018년 데이터 보호법이 적용됨에 따라[920] 데이터 관리자인 법집행기관은 데이터 보호법상 규정을 준수하여야 하고, 이를 준수하였다는 것에 대하여 입증책임이 있다.[921]

라. 수사권한법(IPA 2016)

1) 개요

통신 감청 등에 대하여는 수사권한규제법(Regulation of Investigatory Powers Act 2000 : 이하, "RIPA")에서 규정하고 있었으나 2016년 11월 29일 수사권한법(Investigatory Powers Act 2016 : 이하, "IPA")이 제정되면서 감청, 통신데이터 수집에 관한 부분은 RIPA에서 삭제되고, IPA에서 통합하여 규율하게 되었다.[922] IPA Part 2.에서는 감청(Lawful interception of communications), Part 3.에서는 통신데이터 취득(Authorisations for obtaining communications data), Part 4.에서는 통신데이터에 대한 보전(Retention of communications data)제도를, IPA Part 5.에서 장비 간섭(Equipment interference)[923]에 관하여 규정하고 있다.[924]

---

918) AG Guidelines, Annex A-Digital Material para. 33. (2022).

919) CJPA s.57(3).

920) Data Protection Act 2018 s.30(1), 3(2)(4).

921) Data Protection Act 2018 s.34(3).

922) 통신감청에 관한 RIPA Chapter I of Part 1은 통신감청(interception)에 관한 것으로 IPA 제정 이후 IPA Part 2 and Chapter I of Part 6에서, RIPA Part 2는 통신서비스제공자로부터 통신데이터(통신내용 불포함)를 취득할 수 있는 권한(Acquisition and disclosure of communications data)에 대하여 규정하고 있었는데, IPA Part 3에서 규율하게 되었다(Investigatory Powers Act 2016, EXPLANATORY NOTES, 2016, 11면).

923) Part 5. 장비 간섭(Equipment interference) 부분에는 특정 대상에 관한 온라인 수색(Online Search)이 규정되어 있다.

924) IPA 2016은 통신의 내용 및 통신데이터를 확보하기 위한 법집행기관, 보안 및 정보기관의 수사권한의 사용, 이에 대한 감독에 대하여 각 법률에 흩어져 있는 규정들을 통합한 법률이다. 감청영장에 대하여 국무장관의 승인(Secretary of State authorisation)을 받은 후 판사가 위 영장을 승인

2020년 IPA는 ① 대부분의 통신데이터 요청에 대하여 독립적인 행정적 또는 사법적 승인을 받도록 하였고, ② 통화내역 및 위치정보와 같은 통신데이터를 획득 또는 보존 요청할 수 있는 범죄를 종전보다 제한하여 중대범죄만을 대상으로 하도록 개정되었다.[925] 이러한 개정은 데이터 보전 및 수사권한법(Data Retention and Investigatory Powers Act 2014 : 이하, "DRIPA")[926]에 규정되어 있던 영국의 데이터 보전 체제에 대하여 "범죄 퇴치를 목적으로 모든 전자 통신 수단(전자 통신의 대량 감시)과 관련된 모든 가입자 및 등록 사용자의 모든 트래픽 및 위치 데이터를 일반적이고 무차별적으로 보유하도록 하는 법률은 유럽연합 기본권 헌장의 개인정보보호 권리 및 데이터 보호 권리를 침해한다"는 유럽사법재판소(Court of Justice of the European Union : CJEU)의 판결[927]이 계기가 된 것이다. 위 판결 이후 영국은 2018년 데이터 보존 및 획득 규정(THE DATA RETENTION AND ACQUISITION REGULATIONS 2018)을 제정하였고,[928] 이에 따라 IPA를 개정하게 된 것이다.[929]

할 때까지 효력을 발효할 수 없도록 이중의 잠금장치('double-lock')를 한 것, 수사권한위원회(Investigatory Powers Commissioner)를 통하여 사후감독이 이루어지도록 한 것은 권한에 통제를 강화한 부분이다. 그 외에 디지털 시대에 적합하게 법집행기관이 인터넷 통신기록(internet connection records)을 보관할 수 있도록 한 부분은 법집행기관의 권한을 강화한 부분이라고 할 수 있다(GOV.UK 사이트, "Investigatory Powers Act"(https://www.gov.uk/government/collections/investigatory-powers-bill; 최종접속일 2023.9.14.)).

925) 공중보건, 정부부서에 지급해야 할 세금, 관세 등 징수, 금융서비스 및 시장 규제, 금융 안정성과 관련된 기능을 유지하기 위한 목적으로 통신데이터 수집 및 보존요청을 할 수 없게 위 3가지 목적은 삭제되었다(EXPLANATORY MEMORANDUM TO THE DATA RETENTION AND ACQUISITION REGULATIONS 2018(No. 1123)).

926) 데이비드 데이비스(David Davis)와 토마스 왓슨(Thomas Watson)은 각각 보수당과 노동당 의원으로 2014년 데이터 보존 및 조사 권한법(Data Retention and Investigatory Powers Act 2014, "DRIPA")에 따라 설정된 데이터 보존 권한에 대한 사법심사를 신청했다. DRIPA는 2015년 신청 당시 시행되었지만 2016년에 수사권법("IPA")으로 대체되었기 때문에 IPA가 개정된 것이다(Columbia University, Freedom of Expression 홈페이지, "Secretary of the State for the Home Department v. Watson"(https://globalfreedomofexpression.columbia.edu/cases/secretary-state-home-department-v-watson/; 최종접속일 2023.9.14.)).

927) 유럽사법재판소 판결(Tele2/Watson Case)에 따라 영국 항소법원(The U.K. Court of Appeal)이 위 DRIPA가 EU법에 위반되었다는 판결을 하였다(EUR-Lex 홈페이지, 판결문 전문(영문)(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203; 최종접속일 2023.9.14.); Columbia University, Freedom of Expression 홈페이지, "Secretary of the State for the Home Department v. Watson"(https://globalfreedomofexpression.columbia.edu/cases/secretary-state-home-department-v-watson; 최종접속일 2023.9.14.); 유럽사법재판소, 판결문 전문(원문)(https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1088733; 최종접속일 2023.9.14.)).

928) 위 데이터 보존 및 획득 규정은 영국의 EU 탈퇴와는 무관하게 효력을 유지한다고 밝히고 있다(EXPLANATORY MEMORANDUM TO THE DATA RETENTION AND ACQUISITION REGULATIONS 2018(2018 No. 1123) 7.5. 및 8.1.).

2) 감청

누구든지 적법한 권한 없이 공용 우편서비스 또는 공용 또는 사적 전파통신 시스템을 이용한 전송 중인 통신을 검열 또는 감청하여서는 안 된다.[930] 다만, 통신의 당사자 또는 일방 당사자의 동의(Consent)에 의한 경우,[931] 수사기관 또는 정보기관의 장이 특정 목적을 위하여 국무장관(the Secretary of State)에게 영장을 청구하여 발부받은 경우에는 적법하게 감청할 수 있다.[932]

IPA는 통신시스템에 '저장된 통신'의 경우에도 ① Part 5. 표적 장비 감청 영장(targeted equipment interference warrant) 또는 Chapter 3 of Part 6 대량 장비 간섭 영장(bulk equipment interference warrant),[933] ② 정보를 얻거나 문서 또는 기타 물건을 점유할 목적으로 행사되는 법적 권한 행사,[934] ③ 법원의 명령(court order)[935]에 따라 감청이 가능하도록 규정하고 있다. ②는 PACE 1984 등 관련 법률[936]에 의하여 법집행기관이 수색영장에 따라 전자기기를 수색하거나, 전자데이터의 생성을 요구명령하는 경우를 포함한다.[937] 통신시스템에 저장된 통신에 접속하는 것은 수신자가 이를 접속하였는지 여부나 전송 전 또는 후와 관계없이(whether before or after its transmission)[938] 감청으로 간주된다.[939] 따라서 법 집행기관은 범죄 증거 수집을 위한 조사 중에 IPA 제6조(c)의 권한을 사용하여 웹 기반 서버에 저장된 이메일

---

929) 유럽사법재판소는 통신사업자가 데이터를 보존하는 것은 심각한 범죄(serious crime)에 한정되어야 하고, 반드시 필요한 경우에 국한되어야 한다는 등의 지침을 제시하여 이에 따라 IPA 규정(종전 RIPA 포함)이 개정된 것이다(Investigatory Powers Act, EXPLANATORY NOTES, 2016, 2면).

930) IPA s.3(1).

931) IPA s.44.

932) IPA s.19.

933) IPA s.6(c)(i).

934) IPA s.6(c)(ii).

935) IPA s.6(c)(iii).

936) powers of search, seizure or production under the Police and Criminal Evidence Act 1984; powers to search or obtain content under the Proceeds of Crime Act 2002; powers to search under the Firearms Act 1968, Protection of Children Act 1978, Theft Act 1968 and the Misuse of Drugs Act 1971; powers to examine imported goods under the Customs and Excise Management Act 1979 to examine imported goods; powers to search or examine under Schedule 7 of the Terrorism Act 2000, etc.

937) The Home Office, "Interception of Communications Code of Practice", 2018.3, para 12.14.

938) IPA s.4(4)(b).

939) Association of Chief Police Officers(ACPO), 『Good Practice Guide for Digital Evidence』, 2012, 22면.

또는 저장된 음성 메일에 접근하여 이를 획득할 수 있다.[940] 다만, 각 범죄별로 적용되는 근거법령은 다르다. 전송 중인 자료에 대한 감청으로 얻은 증거자료는 법정에서 증거로 사용할 수 없고 법적 절차 등에서 공개, 제시 등이 금지되지만,[941] 수색영장으로 이어지는 조사에 도움이 될 수는 있다.

3) 통신데이터 획득 및 데이터 보전[942]

가) 통신데이터 획득

IPA Part 3은 통신데이터의 획득에 관하여 규정하고 있다. 이때 통신데이터는 발신자, 수신자, 위치정보 등을 의미하는 것으로 통신의 내용은 이에 포함되지 않는다.[943]

IPA Part 3은 영국 외에서의 행위나 외국인에게도 적용된다는 역외 적용규정을 두고 있다.[944] 따라서 해외 통신 및 우편사업자에게도 적용되고, 해외에 있는 사람에게도 전자적 방법 또는 다른 수단에 의해서 통지가 된다.[945]

나) 통신데이터의 보전

특정한 법정 목적을 명시하여 12개월을 초과하지 않는 범위 내에서 통신사업자가 통신데이터를 보전하도록 통지할 수 있다. 이러한 통지에는 지정된 데이터를 보관하는 것 외에도 보관한 데이터의 처리, 보안과 관련된 요구사항 등을 부과할 수 있다. 통신데이터가 통신의 발신자, 수신자를 식별하는데 사용되거나 식별하는데 도움이 될 수 있는 경우 전화번호, 이메일주소, IP 등을 보전할 수 있다. 웹사이트, 인스턴트 메시징 애플리케이션과 같은 특정 장치가 연결되는 인터넷 서비스 기록과 같은 인터넷 연결기록도 보관할 수 있는데, 이것으로 특정인이 해당 인터넷 사이트에 접속하였

940) The Home Office, "Interception of Communications Code of Practice", 2018.3, para 12.15, 12.16.

941) IPA s.56(1).

942) 영국은 유럽 사이버범죄 방지 협약(Convention on Cybercrime) 가입국으로 위 협약의 내용을 국내법으로 제정하여야 할 의무가 있다. IPA의 데이터 보전에 관한 규정은 사이버범죄 방지 협약 제16조를 국내법으로 도입한 것이다.

943) IPA s.261(5).

944) IPA s.85(1).

945) 다만, 해외 통신서비스제공자 등에게 데이터를 요청하는 경우 해당 국가의 법률에 따른 요구사항 및 제한사항, 해당국의 법률을 위반하지 않는 방식으로 의무준수가 합리적으로 실행가능한지 여부를 고려하여 결정한다(IPA s.85(4)).

는지는 알 수 있지만, 어떤 일을 하였는지 식별할 수는 없다.

국무장관이 통신데이터 보전통지 허가를 신청한 경우 사법위원은 보전의 요건, 필요성, 비례성 등에 대하여 법원이 사법심사에 적용하는 것과 동일한 원칙을 적용하여 심사를 하여야 한고, 통지에 대한 승인을 거부하는 경우 서면으로 그 이유를 명시하여야 한다.

IPA 제97조에서는 영국 외부에 기반을 두고 있지만, 영국 내에 있는 고객에게 서비스를 제공하는 해외 통신 및 우편사업자에게도 적용된다는 역외 적용 규정을 두고 있다. 따라서 해외 통신사업자 등은 보전통지를 받은 경우 통신데이터를 보전해야 하며, 보완요구사항을 준수할 의무가 있다.

4) 온라인 수색(장비간섭)

영국에서 온라인 수색은 장비간섭(Equipment interference)이라고 불리고 모든 장비에 대한 물리적 및 원격 간섭을 허용한다.[946] 온라인 수색영장(Targeted Equipment Interference Warrant : TEIW)[947]은 IPA Part 5. 제99조 내지 제135조에 규정되어 있다. 영국에서 온라인 수색은 IPA에 의하여 처음 도입된 제도가 아니고, 경찰법(Police Act 1997)에도 규정되어 있었던 것으로, IT 기술의 발전 및 테러범죄에 대응하기 위하여 과거의 제도를 개선하여 수사기관에게 강력한 권한을 부여하되, 그 규정을 명확히 한 것이다.[948] 현재, 영국에서 온라인 수색영장은 아동성착취범죄나 테러범죄에 대응하기 위하여 활발히 활용되고 있다.[949]

영국의 온라인 수색영장의 대상은 통신(Communications), 장비데이터(Equipment Data), 그리고 기타 정보(Any other information)이다. 이때, 통신은 '저장된 통신(stored

946) 장비간섭에는 원격으로 전자장치에 접속하여 전자정보를 추출하고 개인의 로그인 자격증명을 이용하여 전자데이터에 접속하여 전자정보를 다운로드 하는 등의 광범위한 IT 기술이 포함된다. 이것은 원칙적으로 컴퓨터 오용법(Computer Misuse Act 1990)에 따라 범죄에 해당할 수 있으나, IPA에 따라 허가를 받은 경우 허용된다(Law Commission Reforming the Law, 앞의 보고서, 14.64, 340면).

947) 수사권한법 Part 6에는 정보기관의 불특정 다수의 개인 또는 장치를 대상으로 하는 '대량 온라인 수색영장(Bulk Warrant)'에 대하여도 규정하고 있으나, 이 글에서는 수사기관이 온라인 수색을 하는 경우를 논의하기 위한 것이므로 대량 온라인 수색영장에 대하여는 따로 논의하지 않는다.

948) UK Government, INVESTIGATORY POWERS BILL: EQUIPMENT INTERFERENCE; 김학경, "영국 수사권한법에 규정된 온라인 수색 법제에 관한 소고", 『형사법의 신동향』 제74호, 대검찰청, 2022.3, 77면.

949) 김학경, "영국 수사권한법에 규정된 온라인 수색 법제에 관한 소고", 92면.

communication)'을 의미한다.[950] 장비 간섭 영장은 이메일과 같이 인터넷 등 통신시스템에 저장된 통신을 획득할 수 있는 합법적인 권한도 부여하는 것으로, 사용자가 이메일을 확인하였는지 여부와는 상관없이 법집행기관이 이를 획득할 수 있다.

경찰 등 수사기관의 온라인 수색영장은 지역경찰청장(Chief Constable) 등과 같은 수사기관의 수장이 발부권자이다. 위 영장은 사법위원(Judicial Commissioner)의 승인이 있어야 유효하며,[951] 영장의 유효기간은 원칙적으로 6개월이다.[952] 다만, 사법위원장이 승인하지 않는 경우 발부권자는 수사권한위원(Investigatory Powers Commissioner)에게 재심의 요청이 가능하다.[953] 지역경찰청장 등 영장발부권자는 긴급한 사정이 있는 경우에는 사법위원의 승인 없이도 '긴급온라인 수색영장'을 발부할 수 있는데, 이러한 영장은 근무일을 기준으로 12일 동안만 유효하다.[954] 사법위원이 긴급온라인 수색영장에 대하여 동의를 하지 않는 경우 영장의 효력은 즉시 중지되고, 이때에는 수사권한위원에게 재심의를 신청할 수 없다.[955]

온라인 수색영장은 ① 중대범죄의 예방 및 수사,[956] ② 사람의 생명·신체·정신적 건강에 대한 보호나 위해방지의 목적이 있는 경우[957]에만 발부될 수 있다. 온라인 수색영장은 의회의원, 변호사의 비밀유지특권 대상 항목, 기밀보도자료 및 언론에 관한 것인 경우 사법위원장의 동의뿐만 아니라 영국 수상(the Prime Minister)의 동의를 받도록 하는 등 추가적인 통제규정을 두고 있다.[958]

대상이 특정된 온라인 수색영장은 원칙적으로 영국 밖에서는 발생하는 사안에 대하여 발부될 수 없는 국내용 영장이다.[959] 다만, 온라인 수색영장은 ① 범죄 수사 대상자가 영국 국민이거나, ② 영국의 민사 또는 형사소송의 객체가 될 가능성이 있는 경우, 또는 영국 국민에게 영향을 미치거나 영국 법정에서 증거로 사용될 가능성이 있는 경우 역외 적용도 허용된다.[960]

---

950) IPA s.99(8).
951) IPA s.108(1).
952) IPA s.117.
953) IPA s.108(5).
954) IPA s.109.
955) IPA s.109조(4).
956) IPA s.106(1)(a).
957) IPA s.106(3)(a).
958) IPA s.111-113.
959) 김학경, "영국 수사권한법에 규정된 온라인 수색 법제에 관한 소고", 91면.

마. 수사권한규제법(RIPA 2000)[961]

1) 개요

수사권한규제법(Regulation of Investigatory Powers Act 2000 : "RIPA")은 인터넷을 이용한 범죄와 아동성착취 범죄 등에 대하여 사회적인 우려가 높던 시기인 2000년에 큰 반대 없이 통과되어 제정되었다.[962] 제정 당시 RIPA는 수사기관, 정보기관을 포함한 국가기관의 정보감시활동, 통신감청, 통신데이터 취득과 제출, 비밀감시, 위장정보원, 암호화 전자데이터의 복호화 또는 접근수단의 확보에 대한 법적 근거를 확보하고, 이와 관련한 수사권한의 내용과 사법적 통제절차를 규정하고 있었다.

그러나 2016년 IPA 제정으로 감청 등 상당 부분이 RIPA에서 삭제되고 IPA에서 규정되게 됨에 따라 RIPA에서 디지털 증거 압수·수색과 관련된 것은 Part Ⅲ '암호화된 전자데이터의 수사(Investigation of electronic data protected by encryption)' 중[963] 제49조 내지 제51조 암호해제 요구권한(Power of require disclosure), 제53조 내지 제54조 암호해제 요구 불이행 및 비밀누설에 대한 형사처벌(Offences) 규정이다. 또한, '암호화된 전자정보의 수사에 관한 규칙(Code of practice for investigation of protected electronic information)'[964]에서 수사기관이 암호화된 정보를 해독할 수 있도록 패스워드 등 접근권한 정보의 제공을 명령할 수 있도록 규정하고 있는바, 위 규칙도 함께 살펴보기로 한다.

---

960) The Home Office, "Equipment Interference Code of Practice", 2018.3, para 3.29, 17면.

961) 수사권한규제법(RIPA)은 김한균, "피의자 휴대전화 비밀번호의 제출 강제 -영국 입법례 참고한 디지털 증거 압수·수색시 협력의무 부과 법안 추진 비판-", 『형사소송 이론과 실무』 제13권 제2호, 한국형사소송법학회, 2021.6, 150-151면; Regulation of Investigatory Powers Act 2000, Introductory text.

962) 김한균, 앞의 논문, 152면, 각주 176.

963) 암호해제와 관련된 조항은 2001년 제정 이후 바로 시행된 것이 아니라 2007년 10월에서야 시행되었는데, 그 이유는 제정당시에는 암호화 기법이 널리 사용되지 않아서 위 조항을 실행할 필요성이 크지 않았기 때문이라고 한다(김한균, 앞의 논문, 154면, 각주 176).

964) 암호화된 전자정보의 수사에 관한 규칙은 암호해제 요구 통지에 따른 권한과 의무에 대하여 2016년 수사권한법(IPA) 제정 이후 IPA 제227조에 따라 임명된 수사권한감독위원의 검토를 받도록 하는 등의 개정이 있었다(Home Office, Investigation of Protected Electronic Information Revised Code of Practice).

2) 암호해제요구

RIPA 제49조에 의하면, 경찰(the Police), 국가범죄수사청(the National Crime Agency) 등 수사기관[965]은 적법하게 수집된 디지털 증거[966]가 암호화되어 있는 경우, 법원 등[967]에 암호해제 통지(notice) 허가를 신청할 수 있다.

수사기관은 국가기술지원센터(The National Technical Assistance Center : "NTAC")에 서면으로 조언을 받아 암호해제 통지(Notices requiring disclosure)를 위한 허가를 받아야 하는데, 이때 NTAC의 서면 조언은 적법요건으로, 국무장관이 동의하지 않는 한 NTAC가 아닌 다른 공공기관에서 조언을 받을 수도 없다.[968] 수사기관이 암호해제 통지 허가를 신청한 경우 법관이 암호해제 통지 허가권한을 가진다.[969]

암호해제요구는 (a) 당해 암호화된 정보의 암호해제수단(Key)을 소지하고 있고, (b) 암호화된 정보에 대하여 암호해제요구가 (i) RIPA 제49조 제3항의 법정사유에 해당하거나, (ii) 공권력의 법적 권한 내지 의무의 정당한 수행 또는 효과적 행사를 위하여 필요하거나 (c) 암호해제요구가 그 목적에 비례하거나 (d) 암호해제요구 통지 없이는 해독 가능한 형태로 암호화된 정보를 취득하기 위한 동의를 받을 현실적인 가능성이 없다고 믿을만한 상당한 이유가 있는 경우, 법원 등의 허가를 받아 암호해제 수단(key)을 소지하고 있다고 인정되는 자에게 암호해제요구를 통지할 수 있다.[970]

암호해제요구 사유로는 (a) 국가안보의 필요, (b) 범죄방지 및 적발의 목적, (c) 국가경제적 복리의 필요성을 들 수 있는데,[971] 수사기관의 경우 대부분 (b) 범죄방지 및 적발 목적으로 암호화된 정보에 대하여 암호해제를 요구한다.

---

965) 암호해제를 요구할 수 있는 기관은 경찰, 국가범죄수사청 등 수사기관에 한정되지 않고, 정부부처(office under the Crown), 국세관세청(Her Majesty's Revenue and Customs) 등도 RIPA 제49조에 따라 암호해제요구 통지 허가를 신청할 수 있다. 다만, 이 글은 수사기관의 압수·수색에 관한 것인바, 수사기관의 권한을 위주로 살펴보기로 한다(Regulation of Investigatory Powers Act 2000 부칙(Schedule) 제2편 제2조 제3항).

966) 이때 수사기관이 수집한 디지털 증거는 적법한 압수·수색, 감청 등의 결과로 취득하였거나 취득할 가능성이 있는 것까지 포함한다(RIPA s.49(1)).

967) 잉글랜드와 웨일즈의 경우 치안법원 지방판사가 허가권자이다(Regulation of Investigatory Powers Act 2000 부칙(Schedule) 제2편 제1조 제1항).

968) Investigation of Protected Electronic Information Revised Code of Practice(2018. 8.) para. 3.10.

969) Investigation of Protected Electronic Information", Revised Code of Practice(2018. 8.) para. 9.5.

970) RIPA s.49(2).

971) RIPA s.49(3).

3) 암호해제요구 통지 및 암호해제요구 통지 불이행죄 등

RIPA 제50조 제1항에 의하면, 암호해제요구 통지를 받은 자는 (a) 자신이 가지고 있는 암호해제 수단으로 당해 정보를 해독 가능한 형태[972]로 만들어야 하고, (b) 통지된 대로 해독 가능한 형태의 정보를 공개(제출)하여야 한다.[973]

수사기관은 암호해제요구 통지의 상대방에게 ① 암호화된 정보를 해독 가능하게 하거나, 암호화된 정보에 접근할 수 있거나 암호화된 정보를 읽을 수 있는 수단을 공개,[974] 또는 ② 암호해제요구에 대해 비밀을 유지할 것을 요구할 수 있다.[975] 다만, 위와 같은 권한은 다른 방법으로는 해당 정보를 취득할 수 없는 경우[976] 등 엄격한 요건 아래 필요 최소한의 범위 내에서 인정되는 것으로,[977] 명령 이후 7일 이내에 서면 또는 수사권한감독위원회(the Investigatory Powers Commissioner)에 전자적 수단으로 통지하도록 하고 있다.[978] 이때, 암호해제 통지의 상대방(the person given notice)[979]은 자신이 관리하는 데이터를 보호하기 위해 제품이나 서비스를 사용하는 개인(예를 들면, 휴대폰 소유자), 저장매체 등을 생산 또는 공급하는 기업, 특정 인터넷 사이트를 관리하는 인터넷서비스제공자 등 그 대상을 제한하지 않는다.[980]

암호해제요구 통지를 고의로 이행하지 않은 경우 처벌한다.[981] 이때 위 통지가 있기 전에 암호 키(Key)를 소유하고 있었다는 것이 합리적인 의심을 넘어 입증된

---

972) RIPA s.50(1)에는 '이해할 수 있는 형태(intelligible form)'로 표현되어 있으나, 이 글에서는 암호를 해제하여 해독할 수 있는 형태로 번역한다.

973) 암호해제란, 암호화 또는 기타 과정을 통해 보호되는 정보를 보호되기 전의 상태로 복원하는 것을 의미한다(Investigation of Protected Electronic Information, Revised Code of Practice(2018.8.) para. 3.16).

974) 암호해제할 수 있는 수단(Key)을 공개하는 것은 키를 공개하지 않는 경우 암호해제를 요구하는 목적이 전체 또는 부분적으로 무효화될 수 있는 특별한 상황이고, 키의 공개가 비례성의 원칙에 의해서도 부당하지 않은 경우이어야 한다는 특별한 추가 조건이 더 부가되고 있다(Investigation of Protected Electronic Information, Revised Code of Practice(2018.8.) para. 6.3~6.5).

975) RIPA s.50.

976) RIPA s.51(4).

977) 암호화된 정보에 대하여 암호해제를 요구하는 것은 사생활보호 및 개인정보보호권을 침해하는 것으로 볼 수 있는바, 유럽인권협약 제8조, 인권법(Human Right 1998)에 따라 비례성의 원칙을 지켜야 한다(Investigation of Protected Electronic Information, Revised Code of Practice(2018.8.) para.3.37).

978) RIPA s.51(7).

979) 암호해제요구의 상대방은 RIPA 제49조에 따라 암호해제요구를 받은 사람으로 암호화된 정보, 당해 정보에 대한 접근수단 및 해독 가능한 형태로의 암호해제 수단을 소지한 자이다(김한균, 앞의 논문, 158면, 각주 176).

980) Investigation of Protected Electronic Information, Revised Code of Practice(2018. 8.) para. 4.2.

981) RIPA s.53(1).

경우, 통지 후 키를 공개하도록 정해진 기간 내에 키(Key)를 소유하고 있지 않았다는 것을 입증하지 못하면 계속 소유하고 있는 것으로 간주되고,[982] 통지를 받았을 당시 또는 공개를 요구받은 이후 자신이 해당 시점 이전에 키(Key)를 가지고 있었는지 여부에 대하여 의심을 제기하지 않은 경우에도 키(Key)를 계속 소유하고 있는 것으로 간주된다.[983] 암호해제가 이루어졌지만, 암호해제된 정보가 명백히 일부이거나 불완전하거나 암호화된 정보 이외의 정보인 것으로 암호해제통지를 준수하지 않았다는 것이 합리적인 의심 없이 입증되는 경우에도 처벌된다.

정식기소 사건에서 국가 안전 또는 아동의 성착취와 관련된 범죄에 대해 암호해제 요구를 이행하지 않은 경우 5년 이하의 징역 또는 벌금형, 그 밖의 사안인 경우 2년 이하의 징역형에 처할 수 있다.[984] 약식재판에서 유죄선고를 받은 자(summary conviction)는 6월 이하의 징역형과 법정 상한 이하의 벌금형에 처한다.[985]

한편, RIPA 제49조에 따른 통지 사실, 통지 내용, 통지에 따른 의무 이행사실에 대한 비밀을 누설한 경우(Tipping-Off)에도 위와 같이 처벌한다.[986]

바. 경찰, 범죄, 양형 및 법원법(PCSCA 2022)[987]

1) 개요

경찰, 범죄, 양형 및 법원법 2022(Police, Crime, Sentencing and Courts Act 2022

982) RIPA s.53(2); Investigation of Protected Electronic Information, Revised Code of Practice (2018. 8.) para. 10.3.

983) Investigation of Protected Electronic Information, Revised Code of Practice(2018. 8.) para. 10.4.

984) 이때, 징역형과 벌금형은 병과할 수 있다(RIPA s.53(5),(5A),(6)).

985) RIPA s.53(2)(b).

986) RIPA s.54(1),(4).

987) 2022. 4. 28. 시행된 위 법률은 아동에 대한 계획적 살인의 경우 법정형을 종신형(가석방없는 종신형)까지 상향하는 등 일부 범죄에 대한 형량 상향, 시위와 집회를 제한할 수 있는 경찰권 강화, 전자기기에서 증거를 추출하는 방법 등 증거확보 방법을 명확화하는 등 형법 및 형사소송법적 요소가 두루 포함되어 있다. 위 법률은 대체로 법집행기관 등 범죄 예방, 수사 등을 위해 국가기관의 권한을 강화하는 것을 내용으로 한 것으로 표현의 자유, 언론의 자유, 항의권(저항권)에 대한 침해라는 비판이 다수 있었고, 이로 인해 법 통과 저지를 위한 시위가 발생하기도 했다(WIKIPEDIA, "Police, Crime, Sentencing and Courts Act 2022"(https://en.wikipedia.org/wiki/Police,_Crime,_Sentencing_and_Courts_Act_2022; 최종접속일 2023.9.12.); itvNEWS, "Thousands march through Bristol for 'Kill the Bill' protest", 2022년 3월 1일자(https://www.itv.com/news/westcountry/2021-03-21/hundreds-gather-in-bristol-for-kill-the-bill-protest; 최종접속일 2023.9.12.); LIBERTY, "THE POLICING BILL – WHAT HAPPENED, AND WHAT NOW?", 2022년 4월 29일자(https://www.libertyhumanrights.org.uk/issue/the-policing-bill-what-happened-and-what-now/; 최종접속일 2023.9.12.)).

: 이하, "PCSCA")은 범죄 예방, 적발, 수사 및 기소 등을 위해 처벌을 강화하고, 경찰 및 기타 정부기관의 권한을 새롭게 규정하는 등 형사사법제도 전반에 걸쳐서 변경을 가져온 법률[988]이다. 이 글에서는 PCSCA Part 2 제3장 중 전자기기로부터 정보추출(Extraction of information from electronic devices)에 대하여 규정하고 있는 제37조 내지 제44조, 별표 3 정보를 추출할 수 있는 권한이 있는 사람(Extraction of information from electronic devices: authorised persons)에 관하여 살펴본다.

2) 동의에 의한 전자기기 제출, 승인된 자에 의한 정보추출

위 법률에서 전자기기는 정보가 전자적으로 저장될 수 있는 모든 장치를 의미하며, 해당 장치의 구성요소를 포함한다.[989] 전자기기의 사용자가 전자기기에서 정보를 추출하는 것을 승인받은 자(이하, "경찰 등"[990])에게 ① 기기를 자발적으로 제출하고, ② 해당 장치에서 정보를 추출하는 것에 동의한 경우[991] 범죄를 예방, 탐지, 조사 또는 기소하기 위한 목적으로[992] 정보를 추출할 수 있다. 이때 경찰 등은 전자기기의 정보가 현재 진행중인 사건과 합리적인 관련성이 있거나 그 경찰 등이 추적할 예정으로[993] 해당 정보가 범죄 수사 등 목적을 달성하기 위해 필요하고 비례의 원칙에도 반하지 않아야 한다.[994] 만일, 그 과정에서 해당 목적 이외의 정보를 취득할 위험이 있는 경우 원칙적으로는 정보를 추출할 수 없지만, 다른 방법에 의하여 정보를 얻을 수 없거나 다른 수단이 합리적으로 가능하지 않은 경우 정보를 추출할 수 있다.[995]

---

988) UK Parliament 홈페이지, "Have your say on the Police, Crime, Sentencing and Courts Bill", 2021년 5월 6일자(https://www.parliament.uk/business/news/2021/may/have-your-say-on-the-police-crime-sentencing-and-courts-bill/; 최종접속일 2023.9.14.).

989) 휴대폰, 태블릿, 노트북, 컴퓨터 등의 장치와 이동식 저장 장치 USB 또는 기타 저장 장치 등의 구성 요소가 포함될 수 있으며, 스마트 시계나 음성 활성화 스피커와 같은 '스마트' 장치도 포함될 수 있다(The Home Office, "Extraction of information from electronic devices: code of practice(accessible)", 2023.3.16, para. 9).

990) 별표 3에는 정보를 추출할 수 있는 권한이 있는 사람(Extraction of information from electronic devices: authorised persons)에 대하여 규정되어 있는데, 이때 잉글랜드와 웨일즈 경찰 순경, 경찰서장이 임명한 직원 등은 제37조 내지 제41조의 모든 목적과 관련하여 정보추출의 권한을 부여받을 수 있다.

991) PCSCA s.37(1).

992) 그 외에도 실종자를 찾는데 도움을 주거나, 아동이나 위험에 처한 성인을 방치, 신체적, 정신적 피해로부터 보호하기 위하여도 전자기기에서 정보를 추출할 수 있다(PCSCA s.37(2)).

993) PCSCA s.37(5)(a).

994) PCSCA s.37(5)(c).

995) PCSCA s.37(6).

추출의 방법에는 모든 형태의 복제가 포함된다.[996]

전자기기의 이용자가 18세 미만의 아동이나, 무능력자[997]인 성인의 경우 위와 같이 자발적 제출 또는 추출에 대한 동의를 할 수 없고,[998] 아동의 부모 또는 보호자 등,[999] 무능력자인 성인의 부모 또는 후견인 등[1000]이 자발적으로 전자기기를 제공하고 정보의 추출에 동의한 경우에는 정보추출이 가능하다.

경찰 등은 전자기기를 제공하거나 장치에서 정보추출에 동의하도록 과도한 압력을 가해서는 안 되고,[1001] 제출자에게 찾고 있는 정보, 정보를 찾는 이유, 정보추출 후 처리방법, 전자기기 제출 및 정보제공 거부권, 동의를 거부하더라도 정보를 구하는 목적을 위한 조사 등이 종료하지 않음을 명시한 서면으로 통지하고,[1002] 통지서에 제출자의 확인을 받고, 그 사본을 제공하여야 한다.[1003] 이때, 경찰 등은 제출자의 확인이 구두로 전달된 경우 경찰 등은 해당 확인 기록의 사본(하드카피 또는 전자적 방식)을 제공하여야 한다.[1004]

이때 기기 제출에 대한 동의를 철회하는 경우 기기를 반환하여야 하나, 이미 정보추출이 이루어진 후 동의를 철회하였다면 삭제나 반환이 불가능할 수 있다.[1005] 또한, 추출에 대한 동의를 철회하는 경우 정보의 추출이 아직 수행되지 않은 경우에 기기에서 정보를 가져오지 않는다는 것만을 의미한다. 일단 정보추출이 시작되면, 수사기관은 변호인에게 정보를 공개할 의무가 있기 때문에 수사기관이 획득한 정보의 삭제 또는 반환이 불가능할 수 있는 것이다.

---

996) 정보추출에는 모든 형태의 복제도 포함되므로 물리적 복사 및 모든 형태의 전자 또는 디지털 복제(예: 스크린샷) 등도 포함된다(PCSCA s.37(14); The Home Office, "Extraction of information from electronic devices: code of practice(accessible)", 2023.3.16, para. 10).

997) 2005년 정신능력법(Mental Capacity Act 2005) 상의 무능력자(People who lack capacity) 등을 의미한다.

998) PCSCA s.38(1).

999) PCSCA s.38(2),(3).

1000) PCSCA s.38(7),(8).

1001) 이때, 과도한 압력이란, 대상자에게 해당 기기를 자발적으로 사용하고 추출에 동의하는 것에 대한 선택권이 없는 것처럼 느끼게 만드는 것을 의미한다. 추출에 동의하지 않는 경우 조사가 조기에 중단될 것이라고 느끼게 하거나 합리적인 조사라인을 따르지 않을 것이라고 느끼게 하는 경우를 의미한다(PCSCA 39(2); The Home Office, "Extraction of information from electronic devices: code of practice(accessible)", 2023.3.16, para. 146).

1002) PCSCA s.39(3).

1003) PCSCA s.39(6).

1004) PCSCA s.39(7).

1005) PCSCA s.39(2); The Home Office, "Extraction of information from electronic devices: code of practice(accessible)", 2023.3.16, para. 159.

3) 사망자, 실종자, 아동 또는 무능력자인 성인이 전자기기의 사용자인 경우

사용자가 전자기기를 자발적으로 제공하지 않거나, 정보추출에 동의하지 않았지만 경찰 등이 전자기기의 정보를 추출할 수 있는 예외적인 경우가 있는데 아래 A, B, C 조건 중 어느 하나라도 해당하면 된다.[1006] 전자기기의 사용자가 사망한 경우 사망 직전까지 그 기기를 사용한 경우(A),[1007] 전자기기의 사용자가 아동 또는 무능력자인 성인이고, 경찰 등이 사용자의 생명이 위험에 처해 있거나 심각한 해를 끼칠 위험이 있다고 합리적으로 믿는 경우(B),[1008] 전자기기의 사용자가 실종되었고 실종 직전까지 기기를 사용하였고 실종자의 생명이 위험에 처했거나 심각한 해를 끼칠 위험이 있는 경우(C)[1009]에도 전자기기에서 정보를 추출할 수 있다.

4) 실행지침

위 실행지침(Extraction of information from electronic devices: code of practice)은 PCSCA Part 2. 제3장의 다른 조항, 수색영장(a search warrant), 명령(production order), 법적 통지(statutory notice)에 의한 정보추출, 전자기기가 아닌 클라우드 등에 저장된 정보의 추출에는 적용되지 않는다.[1010] PCSCA 제37조 및 제41조의 정보추출 권한은 유럽인권협약('ECHR')의 준수를 보장하는 '인권법 1998(The Human Rights Act 1998)', '평등법 2010(The Equality Act 2010)', '데이터 보호법 2018(Data Protection Act 2018)', '영국 일반 데이터 보호규정(UK General Data Protection Regulation)'을 준수하여야 한다.

범죄 용의자의 전자기기에서 정보를 추출하는 경우 대부분 증거의 손실 또는 파괴를 방지하고, 증거개시 규정 등을 지키기 위해 PACE 등에 따라 전자기기를 압수할 가능성이 높기 때문에 위 지침을 활용할 가능성은 크지 않다.[1011] 다만, 공유 노트북 또는 태블릿 장치와 같이 전자기기의 사용자가 여러 명인 경우 동의에 의한 기기

1006) PCSCA s.40(1).
1007) PCSCA s.40(1),(2),(5).
1008) PCSCA s.40(1),(3),(5).
1009) PCSCA s.40(1),(4),(5).
1010) The Home Office, "Extraction of information from electronic devices: code of practice (accessible)", 2023.3.16, para. 22.
1011) *id para.* 50.

제출 또는 정보추출이 활용되는데, 이때 경찰은 해당 전자기기를 자발적으로 제출하고 정보추출에 동의하는 사람이 그 장치를 일반적으로 사용하는 사람인지 확인하여야 한다.[1012] 그러나 이 경우 일반적인 사용자가 반드시 그 기기의 소유자이어야 하는 것은 아니다.[1013]

추출되었으나 관련성이 없는 것으로 간주되는 정보는 수사기관이 이를 보유할 권한이 없다면 삭제되어야 하고,[1014] 검토 결과 과잉 정보 또는 기타 정보를 획득하였고, 획득한 정보를 보유할 법적인 권한이 없다면 관련성이 없는 것으로 간주된다.[1015]

사. 범죄법(해외생성명령)[Crime(Overseas Production Orders) Act 2019]

영국은 유럽 사이버범죄 방지협약의 가입국으로 Crime(Overseas Production Orders) Act 2019에서 해외에 저장된 전자데이터[1016]에 대하여 저장 위치에 상관없이 생산하거나(produce the electronic data), 접근할 수 있도록(give access to the electronic data) 해외 생성 명령(Overseas Production Orders, 이하, "OPO")을 법원(Crown Court)에 신청할 수 있도록 허용하고 있는데, 이것은 IPA 제52조 등의 이행을 위한 것이다.[1017] 이러한 신청을 할 수 있는 신청권자(Appropriate officers)는 '경찰관, 국세청 또는 관세청 직원 등'으로 지정되어 있다.[1018]

해외 생성 명령의 상대방은 범죄의 수사 또는 기소와 관련하여 상호 지원 제공과 관련된 지정된 국제협력협정의 당사자이거나 참여하는 영국 이외의 국가에서 활동하거나 기반을 둔 자이다.[1019] 현재 영국은 미국과 데이터 상호 지원 약정을 체결하여, 위 규정에 따라 미국법에 규정된 전자데이터와 관련하여 생성 명령을 할 수 있다.[1020]

1012) *id para.* 51.
1013) *id para.* 52.
1014) *id para.* 138.
1015) *id para.* 139.
1016) 전자데이터는 전자적으로 저장된 데이터를 의미한다(OPO 3(3)).
1017) David Ormerod CBE, 앞의 책, 1568면(D1.206).
1018) 그 외에도 SFO(Serious Fraud Office) 구성원, 공인된 금융조사관(an accredited financial investigator), 대테러 금융수사관(a counter-terrorism financial investigator), 국무장관이 지정한 규정에 명시된 사람'이 권한자이다(OPO s.2(1)(a)).
1019) OPO s.1(2)(a),(5).
1020) Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020 (SI 2020 No 38).

법관은 기소 가능한 범죄가 저질러졌고, 범죄와 관련된 절차가 시작되었거나 범죄 수사 중이라고 믿을만한 합리적인 근거가 있는 경우 또는 테러범죄 수사 목적인 경우에 해외 생성 명령을 발령한다. 법적 특권(legal privilege) 또는 비밀인 개인의 기록(confidential personal record)과 같은 예외적 전자데이터는 요구할 수 없다.[1021] 따라서 해외 생성 명령은 개인의 비밀기록[1022]이나 합법적인 직업상 특권에 의하여 보호되는 자료에 대해서는 요구할 수 없다.[1023]

해외 생성 명령이 있으면, 그 상대방은 명시되어 있거나 설명되어 있는 전자데이터를 가져갈 수 있고 보고 읽을 수 있거나, 쉽게 보고 읽을 수 있는 형태로 제공될 수 있도록 생성하도록 해야 한다.[1024] 접근권한 부여를 명령하는 경우, 전자데이터를 보고 읽을 수 있는 형태로 접근권한을 부여하고, 특정인에 의하여 요구되는 경우, 또는 특정인의 설명에 따라 전자데이터를 생성해야 하는 경우 가져갈 수 있고, 보고 읽을 수 있거나, 쉽게 보고 읽을 수 있는 형태로 제공할 수 있도록 접근권한을 부여야 하여야 한다.[1025]

2. 디지털 증거 압수·수색 관련 주요 판례

가. 개요

수사기관이 부적절하거나 부당한 방법으로 증거를 취득한 경우 common law에 의한 증거배제도 가능하지만, 더 광범위하게 증거배제를 인정하는 것은 PACE 제78조이다.[1026] PACE 제78조 제1항은 “어떤 소송절차이든 증거가 획득된 상황을 포함한 모든 사정을 고려하여 검사가 제안한 증거가 절차의 공정성에 위반하여 취득된 경우 법원에 제출될 수 없고, 법원은 이를 증거로 인정해서는 안 된다”고 규정하고 있는바,

---

1021) OPO s.3(3).
1022) 개인의 신체적, 정신적 건강, 영적 상담이나 도움 등을 의미하고(OPO 3(7)) 개인 기밀 기록이란, 개인에게 어떠한 의무를 발생시키는 상황에서 만들어져서 공개제한 또는 비밀유지의무가 있는 기록을 의미한다(OPO s.3(8)).
1023) David Ormerod CBE, 앞의 책, 1569면(D1.207).
1024) OSO s.6(1).
1025) OSO s.6(2).
1026) David Ormerod CBE, 앞의 책, 2910면.

PACE 제78조는 불법하거나, 부당하게 얻은 증거뿐만 아니라 불공정하게 얻은 증거까지 배제할 수 있는 가능성을 열어두어 관습법에 의한 증거배제 권한을 확장하였다.[1027] 이에 대하여 판례는 "어떤 경우에도 관습법(common law)에 의하여 증거를 적절하게 배제할 수 있다면, PACE 제78에 따라 당연히 배제될 수 있다(in any case where the evidence could properly be excluded at common law or pursuant to the PACE 1984, s. 78.)[1028]"고 판시한 바 있다. 다만, 판례는 PACE 또는 PACE Code 등을 위반하여 취득한 증거에 대하여 반드시 증거배제를 하여야 하는 것은 아니고, 사건의 특성을 반영하여 증거배제 여부가 결정되어야 한다고 하면서[1029] 경찰의 부적절한 행위가 절차의 공정성에 영향을 미친다면 증거배제를 하여야 하나, 단순히 증거를 취득한 방법에 대한 승인을 거부하기 위하여 증거배제결정을 해서는 안 된다고 판시한 바 있다.[1030]

더 나아가, 증거를 획득한 과정이 유럽인권협약 제8조를 위반하였다고 해도 그러한 증거를 재판에 사용하는 것이 협약 제6조 공정한 재판을 받을 권리를 침해하지 않는 경우 해당 증거능력을 인정한 판례,[1031] RIPA 2000 규정을 위반하여 공동피고인간의 대화를 비밀리에 녹음한 대화의 증거능력을 인정한 판례,[1032] RIPA 2000 및 PACE 제30조(1A) 규정을 위반하였더라도 범죄의 심각성(강도, 허위 감금 및 총기 소지) 및 피해자 보호의 필요성을 고려할 때, 법 위반의 정도가 경미한 것이라고 보아 위법한 비밀녹음의 증거능력을 인정한 판례[1033] 등 위법하게 수집한 증거의 증거능력을 인정한 것이 다수 있다.

영국에서 디지털 증거의 압수·수색 절차가 위법하였는지 여부, 해당 증거의 증거능력 유무에 대하여 PACE 제8조, 제9조 등 압수·수색에 관한 각 규정뿐만 아니라 여러 법령에 산재되어 있는 절차 규정, 데이터 보호법(Data Protection Act 2018), 유럽인권협약(ECHR)[1034] 및 인권법(Human Right 1998) 등을 종합하여 판단한다. 특히, 디지

1027) David Ormerod CBE, 앞의 책, 2911면.
1028) Matto v Wolverhampton Crown Court [1987] RTR 337, O'corner(1986) 85 CrApp R298.
1029) Khan(Sultan)[1995[QB 27; Keenan[1990] 2QB 54 per Hodgson J p.69면(David Ormerod CBE, 앞의 책, 2912면 재인용).
1030) David Ormerod CBE, 앞의 책, 2912면.
1031) Khan v UK(2001) 31 EHRR 45(1016).
1032) Bond [2020] EWCA Crim 1596(David Ormerod CBE, KC(Hon), 앞의 책, 2919면 재인용).
1033) Plunkett [2013] EWCA Crim 261, [2013] 1 WLR 3121.

털 증거의 압수·수색은 인권법 제8조 사생활 존중에 대한 권리와 관련이 깊다. 법집행기관의 압수·수색으로 인한 위 권리에 대한 침해가 정당화되려면 ① 법을 준수할 것, ② 합법적인 목적을 추구할 것, ③ 민주사회에서 반드시 필요한 것일 것[1035]이라는 3가지 요건을 갖추어야 한다.[1036]

다만, 앞서 살펴본 바와 같이 위법한 절차에 의하여 증거를 획득하였다고 해서 무조건 증거가 배제되지 않고, 절차의 공정성을 심하게 해한 경우에 증거가 배제된다. 이때 절차의 공정성에 영향을 미쳤는지 여부는 절차 "전체"가 공정하였는지 여부를 기준으로 하기 때문에[1037] 영국의 경우 디지털 증거의 압수·수색에 관한 판례가 어떠한 경향성을 띄고 있다기 보다는 개별 사건마다 증거배제 여부를 판단하고 있는 것으로 보인다. 따라서 이하에서는 디지털 증거의 압수·수색과 관련하여 최근 영국 법원이 선고한 판례를 중심으로 그 경향성을 살펴보기로 한다.

나. 대용량 전자기기의 압수·수색과 관련한 압수대상의 특정성 등에 대한 판단

영국에서 수색영장은 전형적으로 '물건(material)', '물품(articles)', '문서(documents)'를 압수·수색의 대상으로 한다. 전자기기(electronic devices)는 수색영장에 기재된 법률용어인 물건, 물품, 문서에 포함되지 않는다는 주장이 수차례 제기되었지만, 판례는 전자기기가 위와 같은 용어에 포함될 수 있다고 판시하였다.[1038] 즉, 수색영장의 대상인 '물건(material)' 등은 광범위한 의미를 가지는 것이기 때문에 실제로는 컴퓨터, 하드디스크 등에 저장된 전자데이터를 압수·수색하려는 것임에도 영장에 컴퓨터, 하드디스크 등 전자기기만 기재한 경우에도 특정성에 관한 PACE 제15조(6)(b)를 위반한 것은 아니라고 본 것이다. 또한, 전자기기에 영장 청구 범죄사실과 관련이 없는

1034) 2020. 1. 31. EU를 탈퇴하기 전까지 그 회원국으로, 유럽연합의 인권협약(ECHR)을 국내법으로 편입하여 인권법(The Human Rights Act 1998)을 제정하였고, EU를 탈퇴한 이후에도 계속하여 위 인권협약 및 인권법은 형사절차의 위법성을 판단하는 중요한 기준이 되고 있다.

1035) Beghal v DPP [2015] UKSC 49, [2016] AC 88 at [119].

1036) 이것은 주로 합법성 및 비례성의 원칙으로 해석된다(Law Commission Reforming the Law, 앞의 보고서, 14.48, 347면).

1037) David Ormerod CBE, 앞의 책, 2919면.

1038) G v Commissioner of Police for the Metropolis [2011] EWHC 3331 (Admin) at [5]; Kent Pharmaceuticals Ltd v Serious Fraud Office [2002] EWHC 3023 (QB) at [27]; and Hargreaves v Brecknock and Radnorshire Magistrates' Court[2015] EWHC 1803 (Admin), (2015) 179 JP 399 at [37](Law Commission Reforming the Law, 앞의 보고서, 15.6, 361면 재인용).

등 부적절한 자료가 다소 포함되어 있다고 해도 이러한 전자기기를 압수·수색의 대상으로 기재한 영장 청구를 적법하다고 보고 있다.[1039]

또한, 전자기기를 압수한 후에 PACE 제20조 제2항에 따라 압수물 목록을 교부하여야 하나, 판례는 전자기기 안에 저장된 내용을 품목별로 분류한 상세목록을 제공할 의무는 없다고 판시하고 있다.[1040]

CJPA 제53조에 따라 압수물에 대한 초기 검토를 수행한 후 압수대상에 포함되지 않는 전자데이터의 반환의무가 있다. 이에 대하여 판례는 청구인이 CJPA 제59조에 따라 수사기관이 영장에 따라 압수한 약 53TB 상당의 컴퓨터 등 전자기기 등에 대하여 물리적 반환을 청구한 사안에서, '① 수사기관이 자체 장비를 이용하여 압수한 전자기기로부터 복사한 사본은 CJPA 제59조의 반환대상에 해당하고, ② 수사기관이 압수한 복사본의 반환의 한 방법에 '삭제' 포함될 수 있으며,[1041] ③ CJPA 제53조 제5항에서 합리적으로 실행가능한 경우 반환을 하도록 하고 있는데, 이때 합리적 실행가능성은 물리적 또는 기술적 가능성을 의미하는 것이 아니라 그것을 뛰어넘는 실질적인 가능성을 의미한다'고 보았다.[1042] 즉, 합리적 분리의 실행이 가능한 경우에 이러한 반환의무(삭제의무)가 있는 것이나, 물리적 또는 기술적으로 삭제가 가능하다고 해도 시간, 비용, 투입인원 등을 종합적으로 고려하였을 때, 현실적으로 분리하는 것에 어려움이 있는 경우 삭제의무가 인정되지 않는다.[1043]

다. 디지털 저장매체에 대한 합리적인 조사방식에 대한 지침 선언

영국 항소법원은 R v Bater-James[1044] and Sultan Mohammed[1045] EWCA Crim

---

1039) R(Faisaltex Ltd) v Preston Crown Court [2008] EWHC 2832(Admin), [2009]1 WLR 1687; Cabot Global Ltd v Barking side Magistrates' Court [2015] EWHC 1458 (Admin), [2015] 2 Cr App R 26(355)(David Ormerod CBE, 앞의 책, 1552-1553면 재인용).

1040) Business Energy Solutions Ltd v Crown Court at Preston [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [116].

1041) 그러나 CJPA 제59조의 반환청구에 대하여 법원이 반드시 복사한 데이터의 반환 또는 파기를 명령하여야 하는 것은 아니라고 판시하였다(*id at* [88]).

1042) *id at* [98].

1043) Business Energy Solutions Ltd v Crown Court at Preston [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [89].

1044) 피고인 Carl Bater James는 응급구조요원을 구타한 혐의, 고소인에 대한 성폭행 등 여러 가지 범죄로 기소되어 1심에서 총 9년 2개월을 선고받았다. 피고인이 성폭행 부분에 대하여 부인하

790 사건에서, 범죄수사 과정에서 고소인 또는 증인(complaint or witness : 이하, "고소인 등") 소유의 전자기기의 압수, 검사, 복사, 공개 및 삭제 등과 관련된 발생하는 여러 가지 문제에 대한 지침을 선언하였다.[1046] 위 판결에서는 고소인 등의 휴대폰에는 그들의 사생활과 관련된 정보가 다수 포함되어 있기 때문에 사생활 침해에 대한 고려 없이 관행적으로 고소인 등의 휴대폰을 압수하는 것은 지양해야 한다는 원칙을 밝히고 있다. 다만, 자료의 비공개는 피고인의 공정한 재판을 받을 권리를 침해할 수 있으므로 이를 위해 고려해야 할 것을 지침의 형태로 판시하였다. 디지털 정보에 대한 지침은 위 판결 이후에도 꾸준히 영국의 각종 문헌과 정부 발표 자료에서 부각되면서 중요한 지침으로 활용되고 있는바,[1047] 아래에서 자세히 살펴보기로 한다.

첫째, 수사관이 고소인의 디지털 통신을 검토하는 것은 언제 필요하고, 수사관이 접근할 수 있는 디지털 통신은 언제 공개해야 하는가? 고소인의 휴대폰이나 기타 전자장치에 접속하거나 소유하지 않고도 필요한 정보에 쉽게 접근할 수 있는 방법이 있는지 먼저 고려를 해야 하고, 공개는 피고인의 사건에 도움이 될 수 있다고 합리적으로 판단한 경우에만 이루어져야 한다.[1048]

여 경찰이 고소인이 피고인으로부터 폭행을 당한 시점 이후에 피고인과 소통하는데 사용하였고 재판 당시에도 사용하고 있는 휴대폰에 대하여 제출을 요구하였으나 고소인은 제출을 거부하였고, 휴대폰에 저장된 콘텐츠의 다운로드 역시 거부하였다. 그 후 고소인은 재판과정에서 판사의 제출명령에 응하여 휴대폰을 제출하였으나 2019. 6. 13.경(피고인에 대한 기소사건이 끝날 무렵)까지의 통화기록 등 일부 기록이 삭제된 상태에서 제출하였다. 이에 대하여 피고인은 고소인이 증거를 파기하는 등 재판과정을 조작하여 공정한 재판을 받을 권리를 침해하였다고 주장하였다. 그러나 항소법원은 위와 같은 고소인의 행동이 그녀의 신뢰성을 훼손했는지 여부를 고려할 필요가 있는데, 고소인이 제출한 자료는 법정 증거와 다른 점이 없다는 사실을 고려했다는 점 등에 비추어 재판에 결과적 불공정이 없었다고 판단하였다(R v Bater-James [2020] EWCA Crim 790(BAILIE 홈페이지, 판결 전문(https://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html; 최종접속일 2023.9.14.).

1045) 피고인 Sultan Mohammed는 1심 법원에서 술에 취한 고소인에 대한 강간혐의로 유죄 판결을 받았다. 피고인이 합의에 의한 성관계였다며 강간을 부인하는 사건에서, 경찰은 고소인의 휴대폰에 저장된 내용을 다운로드하여 복사한 다음 키워드 검색을 통해 휴대폰에 대한 분석을 하였고, 피고인의 변호인에게 키워드와 키워드 검색결과를 공개하였다. 이에 대하여 피고인 측은 압수된 '40,000' 상당의 통신 전체를 경찰이 조사하여야 한다고 주장하면서 검색어를 사용한 수사가 부적법하고, 모든 항목을 개별적으로 공개하여야 한다고 주장했으나 법원은 이를 받아들이지 않았다.

1046) R v Bater-James and Sultan Mohammed [2020] EWCA Crim 790.

1047) 항소법원이 선언한 위 지침은 CPS 지침 '합리적인 조사방식 및 통신 증거에 대한 지침(Disclosure - A guide to "reasonable lines of enquiry" and communications evidence)'에 반영되었다(Crown Prosecution Service, "Disclosure Manual: Chapter 30 - Digital Material", 2022년 7월 14일자(https://www.cps.gov.uk/legal-guidance/disclosure-manual-chapter-30-digital-material; 최종접속일 2023.9.14.)).

둘째, 고소인의 디지털 통신에 대하여 공개가 필요한 정당한 사유가 있는 경우, 증인의 전자 통신에 대한 검토는 어떻게 수행되어야 하나? 고소인의 휴대폰 등에 저장된 정보가 필요한 경우에도 반드시 고소인으로부터 휴대폰 등을 제출받아야 하는 것은 아니다. "먼저, ① 필요한 검토의 성격, 세부사항, 검토해야 할 특정 영역, 이것이 고소인의 휴대폰이나 기타 장치를 사용하지 않고 이루어질 수 있는지 여부를 고려하여야 한다. ② 고소인의 핸드폰을 검색하여야 하는 경우, 제한된 영역(예를 들어 식별된 메시지, 이메일 문자열 또는 소셜 미디어의 특정 게시물)을 보는 것만으로 충분한지 검토하는 것이 중요하다. 어떤 경우에는 장치를 소유하거나 복사하지 않고 단순히 관련 자료를 보고 스크린샷을 찍거나 기타 기록을 작성함으로써 이를 달성할 수 있다. ③ 좀 더 광범위한 조사가 필요한 경우에는 고소인에게 불편을 최소화하면서 기기의 콘텐츠를 다운로드 받아야 하며, 가능하다면 불필요한 지체없이 기기를 반납해야 한다. 자료가 방대할 경우 피고인의 참여 하에 검색어를 사용하여 적절하게 초점을 맞춘 조사를 고려해야 한다. 모든 검색에 데이터 매개변수를 적용하는 것이 가능할 수 있다. 마지막으로, ④ 관련 없는 개인정보가 노출되는 것을 방지하기 위해 공개된 자료에 대해 적절한 편집이 이루어져야 한다"[1049]고 판시하였다.

셋째, 검토 범위와 사건과 관련된 자료 공개 상황에 관해 고소인에게 어떤 확신을 주어야 하나? "① 검찰은 수사관이 장치를 보관할 기간을 포함하여 공개와 관련하여 내려진 모든 결정(복사를 통해 "추출"할 계획; 그리고 그 이후에 무엇이 "검토"되어 잠재적으로 공개될 것인지)에 대해 정보를 제공할 것이다. ② 어떤 경우에도 휴대폰이나 기타 장치 내의 모든 콘텐츠는 검찰의 공개 의무를 이행하기 위한 다른 적절한 방법이 없는 경우에만 복사되거나 검사된다. ③ 자료는 공개에 대한 엄격한 테스트를 충족하는 경우에만 피고인에게 제공되며 개인정보 또는 기타 관련 없는 정보(예를 들어, 사진, 주소 또는 전체 전화번호)가 불필요하게 공개되지 않도록 적절하게 수정된 형식으로 제공된다"[1050]는 확신을 주어야 한다.

넷째, 고소인이 관련 가능성이 있는 장치에 대한 접근 허용을 거부하거나 관련 자료를 삭제한 경우 어떤 결과가 발생하나? 이에 대하여 법원은 "접근 거부 이유를

1048) R v Bater-James [2020] EWCA Crim 790 at [77].
1049) R v Bater-James [2020] EWCA Crim 790 at [88].
1050) R v Bater-James [2020] EWCA Crim 790 at [89-92].

주의 깊게 살펴보고 조사관이 장치를 사용할 수 있게 되면 따라야 할 절차에 대해 증인에게 설명과 확신을 주는 것이 중요하다. 소송절차를 중단해야 한다고 제안되는 경우, 법원은 재판절차의 적절성을 고려해야 하며, 이것이 특히 증인에 대한 반대 심문을 통해 피고인에게 공정성을 보장할 수 있는지 여부를 고려해야 한다. 법원은 이용할 수 없게 된 자료의 내용과 의미를 추측해서는 안 되고, 법원은 특정한 증거가 누락된 것의 영향과 재판 과정이 증거 부재를 충분히 보상할 수 있는지 여부를 평가해야 한다. 증인이 자료를 삭제하는 경우 각 사건은 자체 사실에 따라 평가되어야 하지만 우리는 반대 심문과 신중하게 만들어진 사법 지침의 잠재적인 유용성을 강조하여, 절차가 중단되지 않고 재판이 진행되는 경우, 적절한 심문을 통해 조사된 증인의 비협조적인 입장은 배심원이 증거 수용 여부를 결정할 때 고려해야 할 중요한 요소가 될 것이다"[1051]라고 판시한 바 있다.

위 판결은 급격한 기술 발전으로 인해 디지털 증거의 압수·수색 과정에서 발생하는 여러 가지 어려움을 경험한 실무영역에 대하여 명확성을 제공한 판결로 평가되고 있고,[1052] 이후 영국 검찰은 2022. 7. 15. 개정한 Legal Guidance(Sexual offences)에도 위 지침을 반영하고 있다.[1053]

3. 디지털 증거에 압수·수색에 관한 법령 및 판례 변화의 경향

가. 디지털 증거 압수·수색 관련 법령 변화의 경향

1) 디지털 증거의 특성을 반영한 압수·수색절차 규정

영국이 디지털 증거를 압수·수색의 대상으로 보아 이를 법규정에 본격적으로 반영한 것은 2001년 CJPA 제정시부터라고 할 수 있다.[1054] CJPA는 정보(information)를

1051) R v Bater-James [2020] EWCA Crim 790 at [99].

1052) Julian Jones, Park Square Barristers, "Obligations in relation to electronic records and devices: fresh guidance from the Court of Appeal (Criminal Division)", 『Park Square Barristers』 2020년 6월 26일자(https://www.parksquarebarristers.co.uk/news/obligations-relation-electronic-records-devices-fresh-guidance-court-appeal-criminal-division/; 최종접속일 2023.9.14.)).

1053) Crown Prosecution Service, "Legal Guidelines, Rape and Sexual Offences - Chapter 3: Case Building", 2021년 5월 21일자(https://www.cps.gov.uk/legal-guidance/rape-and-sexual-offences-chapter-3-case-building; 최종접속일 2023.9.14.).

압수·수색의 대상인 문서(document)에 포함시켜 정보를 압수·수색의 대상으로 명문화하고,[1055] 압수의 방법으로 복사하여 가져가는 것을 인정하였으며,[1056] 사본과 원본의 동일성을 인정하고,[1057] 하드카피 형식으로 전자자료를 압수하는 것을 압수의 방법으로[1058] 명시하였다. 또한, 압수·수색의 일반규정인 PACE 1984를 개정하면서 전자정보를 압수·수색의 대상을 컴퓨터에 저장된 자료에 한정하지 않고, '전자적 형식으로 저장된 것'이라고 하여 그 범위를 확대하고, 가시성 및 가독성 있게 생성하여 제출하는 것에서 더 나아가 가시성 및 가독성 있는 자료로 쉽게 생성할 수 있는 형태로 제공하는 것까지 압수의 방법에 포함시켜[1059] 디지털 증거의 압수·수색 실무를 법률에 그대로 반영하였다.

더 나아가, 압수영장의 집행 등과 관련해서도 디지털 증거의 대량성, 혼재성 등을 고려하여 압수·수색 현장에서 디지털 저장매체를 제거하여 다른 곳에서 이미징 등 포렌식 절차를 거칠 수 있도록 하였고, 이때 무관정보가 혼재된 저장매체 자체를 압수하는 것까지 허용하였다.[1060] 다만, 법적 특권이 인정되는 자료 등 무관정보의 압수를 막기 위하여 압수 후 최초 조사 전에 서면으로 해당 장소의 점유자 또는 관리자에게 통지를 하여[1061] 압수·수색 절차에 대한 이의신청을 할 수 있게 하고,[1062] 최초 증거 선별 과정에 참여할 수 있도록 하는 보호장치도 마련하였다. 아울러 최초 증거 선별과정에서 무관증거에 해당하고 합리적으로 분리 가능한 증거의 경우 빠른 시일 내에 제출자에게 반환하도록 하는 규정도 두었다.[1063] 특히, CJPA의 위 규정들은 디지털 정보가 압수의 대상이라는 점을 인정하면서도 합리적 실행가능성을 따져서 현장에서 정보만을 추출하여 압수하기보다는 저장매체 자체에 대한 압수를 폭넓게 허용하고 있다는 특징이 있다.

1054) 물론 2001년 이전에 전자기기를 압수하여 그 안에 저장된 정보를 압수하는 것에 대하여 PACE에 포함된 압수·수색 대상이 아니라고 주장하는 피고인들의 주장을 판례가 모두 받아들이지 않았다.
1055) CJPA s.66(1).
1056) CJPA s.63(1)(a).
1057) CJPA s.63(1)(b).
1058) CJPA s.50(2).
1059) PACE s.19(4), 20.
1060) CJPA s.50, 51.
1061) CJPA s.52.
1062) CJPA s.59.
1063) CJPA s.53-55.

다만, 저장매체에 압수대상물에 법적 특권이 인정되는 자료 등 배제자료가 포함된 경우 가능한 한 빨리 반환하도록 하는 등 특별한 취급을 하고 있고,[1064] 수사기관이 압수한 개인정보의 처리에 대하여는 2018년 데이터보호법에 따른 엄격한 제한을 통하여 개인정보 및 사생활 침해를 최소화하고 있다. 종합해보면, 영국의 법제는 압수·수색 현장에서 무관정보가 포함된 저장매체 자체를 압수하는 것은 비교적 넓게 허용하고 있으나, 압수물의 보관 및 반환, 사후분석 등에 있어서 무관증거의 보관 등을 엄격하게 통제하고 있다고 할 수 있다.

또한, 영국은 IPA 2016에서 자국 범죄의 수사 및 기소를 위하여 해외 통신사업자에 대하여 통신데이터의 제공 및 보전을 요청할 수 있고, 해외국가의 요청에 따라 감청까지도 가능하도록 하고 있다.[1065] 다만, 이것은 국내 입법으로 실행 가능한 것이 아니라 국가간의 상호협약이 뒷받침 되어야 실질적으로 이행이 가능한데, 현재는 미국과만 위 협정이 체결되어 있다. 영국은 오래전 사이버범죄협약에 가입하였을 뿐만 아니라 위 IPA 규정을 실질적으로 이행하기 위하여 Crime(Overseas Production Orders) Act 2019를 제정하여 해외 통신사업자를 상대로 정보생성을 요구하거나 접근권한을 요구할 수 있도록 하는[1066] 등 해외에 저장된 정보의 압수·수색에도 적극적으로 대응하고 있다.

2) 광범위한 영장 없는 압수·수색 권한의 인정

영국의 경우 체포 시 또는 체포 후 진입 및 수색에 이어진 압수를 하는 경우 사후에 영장을 별도로 발부받을 것을 요구하지 않고,[1067] 수사기관이 적법하게 구내에 진입한 상태라면, 수사 중인 범죄뿐만 아니라 다른 범죄 관련 증거 등으로 은닉, 멸실, 변경, 파괴 등의 위험이 있는 경우 이를 방지하기 위해서 광범위한 압수 권한을 인정하고 있다.[1068] 이러한 원칙은 디지털 정보의 저장매체의 경우에도 그대로 인정된다.

3) 강력한 압수·수색 권한의 인정: 온라인 수색 및 암호해제 요구

영국의 경우 오래전부터 장치 간섭을 통한 '온라인 수색'을 인정해 왔다. 주로 테러

1064) CJPA s.55.
1065) IPA s.52, 85, 97.
1066) OSO s.1(4)(5), 6.
1067) PACE s.32(9), 18(2).
1068) PACE s.19(2),(3).

범죄에 대응하기 위하여 이용되었던 온라인 수색은 오늘날 아동성착취범죄 수사에 자주 이용되고 있다. 온라인 수색은 원칙적으로 암호해킹 등을 통하여 다른 사람의 인터넷 통신에 침입하는 것으로, 컴퓨터 오용법(Computer Misuse Act 1990)에 따라 범죄가 될 수 있음에도 예외적으로 중대범죄 수사를 위하여 적법한 수사방법으로 법률에 규정한 것이다.[1069]

RIPA 2000에서는 수사기관은 일정한 경우 법원의 허가를 받아 암호화된 전자데이터에 대하여 암호해제 요구통지를 할 수 있도록 하고, 통지를 받은 자가 비밀정보 등 접근권한 정보를 제공하지 않는 등 통지를 불이행한 경우 최고 형사처벌까지 하는 강력한 규정을 두고 있다.[1070] 암호해제의 상대방이 해당 정보의 주체에 한정되지 않고 인터넷 서비스제공자 등 제3자를 포함한다.

4) 통신 및 통신데이터 수집권한에 대한 규제 강화 및 현실 반영

IPA 2016의 제정 및 개정 과정을 통해서 살펴본 바와 같이, 영국은 통신 및 통신데이터의 수집, 보전 권한에 있어서 여러 법률에 복잡하게 규정되어 있던 내용을 위 법률에 통합하면서 각 규정을 명확하게 하고, 법집행기관 등 정부의 권한 행사에 제한장치를 마련하였다.

예를 들면, 통신감청 등의 경우 원칙적으로 사법위원장의 승인을 받도록 하고, 수사권한위원회의 사후감독을 받게 하는 등 권한에 대한 일정한 통제장치를 마련하였고, 온라인 수색의 대상자가 의회의원이거나, 변호사의 비밀유지특권 대상 항목 등인 경우 영국 수상의 동의를 받도록 하는 등 이중의 통제장치를 마련하여 권한행사를 엄격히 제한하였다. 뿐만 아니라 유럽사법재판소의 판결 등에 영향을 받아 통화내역, 위치정보와 같은 통신데이터의 획득 및 보존요청을 할 수 있는 범죄를 중대범죄로 제한하는 등 개인정보 및 사생활보호를 위한 노력도 함께 하고 있다.

5) 동의에 의한 저장매체 압수·수색의 확대 및 절차의 명확화

영국은 2022년에 제정된 PCSCA에는 전자기기로부터 정보추출하는 절차, 방법 등에 대하여 규정하고 있다. 위 법률에는 동의에 의하여 전자기기, 즉 저장매체가 제출된

1069) Law Commission Reforming the Law, 앞의 보고서, 14.64, 340면.
1070) RIPA s.53(1).

경우 영장이 없이도 범죄 관련 증거뿐만 아니라 범죄 예방, 탐지, 조사 등의 목적으로 증거를 추출할 수 있도록 하여 경찰 등의 권한을 확장하고 있다. 위 법률에 대하여 많은 비판이 있는 것은 사실이지만, 동의에 따라 저장매체를 제출한 경우 수색의 범위, 제출자에게 제공되어야 할 정보의 서면 통지 등에 대하여 명확히 규정하였을 뿐만 아니라 실질적으로 동의를 할 능력이 되지 않는 아동 또는 무능력자의 저장매체 등에 대하여도 증거를 추출하는 절차를 명확히 하였다는 점에 의의가 있다.

나. 디지털 증거 압수·수색 관련 판례 변화의 경향

1) 압수·수색 대상의 특정성, 참여권 등

판례는 영장의 적법성 또는 집행의 적법성과 관련하여, 영국 법원은 법적 특권이 인정되는 자료 등 압수·수색에서 배제되는 자료가 포함된 전자기기(예를 들어, '휴대폰', '노트북')를 압수·수색 대상으로 하여 영장에 의한 압수한 경우, 영장의 특정성, 식별가능성에 문제가 없다고 보고 있다. 또한, 영장의 집행과정에서, 법적 특권이 인정되는 자료 등을 분리하는 것이 합리적으로 실행가능한가 여부를 따져서 가능하지 않다면 일단 CJPA 제50조는 휴대폰 압수는 적법한 것으로 본다.

CJPA 제50조(4)에 따라 전자기기에서 압수대상을 선별하고자 하는 최초 조사에 전자기기의 소유자, 점유자 등에게 참여의 기회를 부여하는 것은 중요한 절차로 보아서 통지의무를 인정하고 있다. 다만, 위와 같은 통지를 하지 않았다고 해도 곧바로 CJPA 제50조의 압수 권한을 무효화하지는 않는다고 판시하여,[1071] 다른 여러 가지 사정을 함께 고려하고 있는 것으로 보인다.

2) 고소인(또는 증인) 휴대폰에 대한 합리적 조사방식

피고인과 고소인이 주장이 일치하지 않는 성폭행 등 사건에서, 유럽인권협약 제6조 공정한 재판을 받을 권리를 강조하면, 피고인과 고소인의 대화 내역을 확인하기 위해서 고소인 등의 휴대폰을 압수하여 분석하는 것이 관행처럼 이루어져 왔다.

그러나 영국 법원은 휴대폰에는 많은 사생활 정보가 포함되기 때문에 고소인 등의

1071) R(Energy Fianancing Ltd) v Bow Street Court(DC)[2005]EWHC 1626 at [92].

휴대폰 자체를 제출받아 그 안에 저장된 내용을 압수하는 것에 신중할 것을 요구하고 있다. 비례성의 원칙에 따라 고소인의 휴대폰 등을 제출받지 않고 최대한 다른 방법으로 증거자료를 확보하려는 노력을 우선적으로 할 것을 요구하고 있다. 디지털 증거의 압수·수색과 관련하여 피의자(또는 피고인)의 권리에 중점을 두고 절차의 위법성을 판단하는 우리 법원과는 달리, 범죄사실의 입증을 위하여 고소인 등의 디지털 저장매체를 압수할 필요가 있는 경우에도, 고소인 등의 개인정보보호권 등에 대한 침해를 최소화한 방법으로 압수·수색절차를 진행하였는지 여부 역시 절차의 위법성을 판단함에 있어 중요한 요소로 보고 있는 것이다.

디지털 증거 압수수색 관련 쟁점 분석

탁 희 성

제4장

디지털 증거 압수수색 관련 쟁점 분석

제1절 | 디지털 증거 압수수색의 절차적 통제

1. 압수수색 과정에서의 참여권

가. 현행법상 참여권 규정의 법리와 문제점

현행법상 참여권의 법률상 근거는 법원에 의한 압수수색 규정인「형사소송법」제121조와 제123조, 그리고 이를 수사기관의 압수수색에 준용하는 제219조에 있다. 이러한 압수수색 시 참여권은 "공개주의를 원칙으로 하는 법원의 절차에서 사건관계인들이 참여함으로써 절차의 적정을 도모하고, 절차과정을 봄으로써 검사와 피고인이 각각 소송준비를 할 수 있도록 하는 취지"[1072]에서 마련된 것이었다. 즉 절차의 공정성과 피고인의 방어권 확보 차원에서 규정된 참여권은 적법절차 원칙을 실현하기 위한 하나의 수단으로서 규정되었다고 볼 수 있다. 그런데 거의 사회 전 분야에 있어서 디지털 환경이 구축되어 감에 따라 수사절차에 있어서도 디지털 증거 압수수색이 필수적인 상황이 되면서 적법절차를 확보함에 있어 참여권의 중요성이 부각되었다고 볼 수 있다.

압수수색절차에 있어서 참여권이 부각된 데는 디지털 증거 자체의 취약성에서 비롯된 측면이 있다고 볼 수 있다. 즉 디지털 증거는 크게 두 가지 측면에서 취약하다고 볼 수 있다. 즉 첫 번째는 데이터의 휘발성과 위변조의 용이성이며, 두 번째는 불가시

1072) 백형구·박일환·김희옥(편집대표),『주석 형사소송법(I)』(제4판), 한국사법행정학회, 2009, 530면(이완규, "디지털 증거 압수절차상 피압수자 참여방식과 관련성 범위 밖의 별건 증거 압수방법",『형사법의 신동향』통권 제48호, 대검찰청, 2015.9, 107면 재인용).

적이고 불가독적인 데이터가 대량으로 축적됨으로 인해 혐의사실과 무관한 정보들이 혼재되어 있다는 것이다. 전자의 취약성은 수사기관의 실체적 진실의 발견을 저해할 우려가 있는 반면, 후자의 취약성은 피압수자의 기본권을 침해할 우려가 크다는 점이다. 이와 같이 압수수색절차에서 디지털 증거가 갖는 취약성을 보완하기 위한 절차적 수단의 하나로 참여권이 강조되고 있다고 볼 수 있다. 또한 참여권의 법적 성질에 대한 논의도 이러한 디지털 증거의 두 가지 측면의 취약성 가운데 어느 부분에 더 초점을 두는가에 따라 견해가 달라지는 측면이 있다.

참여권의 법적 성질에 관한 학계의 논의를 살펴보면, 무관정보 배제설, 무결성 보장설, 강제처분 신뢰확보설 등으로 견해가 나누어지고 있음을 볼 수 있다. 먼저 무관정보 배제설은 참여권을 수사기관의 무분별한 정보압수를 막기 위한 사전적 통제장치로서 이해하고 있다.[1073] 즉 피압수자의 참여권이 보장되지 않을 경우 수사기관 내부적으로 무관정보에 대한 임의적인 탐색·복제·출력이 행해져도 이를 확인할 방법이 없기 때문에, 참여권을 통해 영장허용범위를 넘어 무관정보에 대한 임의적 탐색·복제·출력 여부를 감시할 수 있도록 함으로써 범죄혐의와 관련성이 있다고 인정할 수 있는 것에 한정하여 압수를 허용하는 「형사소송법」 제219조, 제215조, 제106조 제1항의 규범력을 실효적으로 확보하고자 하는 절차적 보장규정이 바로 「형사소송법」 제219조, 제121조가 규정하고 있는 참여권이라는 것이다.[1074] 다음으로 무결성 보장설은 디지털 증거의 본질적 특성에서 비롯되는 훼손 및 변경의 용이성이라고 하는 측면에 초점을 둔 견해로, 압수수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손, 오남용 및 임의적 복제나 복사를 막기 위한 적절한 조치로서 참여권이 보장되어야 한다고 보는 것이다.[1075] 즉 디지털 증거의 무결성에 대한 논란을 사전에 차단하고자 하는 데 참여권의 목적이 있다고 보는 견해라 할 수 있다.[1076] 마지막으로 강제처분 신뢰확보설은 피압수자가 압수수색절차에 참관 내지 그러한 기회를 보장받는 경우 재판과정에서 새로운

1073) 조광훈, "전자정보의 압수수색절차에서 참여권의 범위와 한계 -대법원 2015.7.16.자 2011모1839 전원합의체 결정을 중심으로-", 『법조』 제64권 제12호, 법조협회, 2015.12, 310면.
1074) 대법원 2015.7.16.자 2011모1839 전원합의체 결정에서 대법관 김창석, 박상옥의 반대의견 (다)(1) 인용.
1075) 대법원 2011.5.26.자 2009모1190 결정.
1076) 박혁수, "디지털 정보압수수색의 실무상 쟁점", 『형사법의 신동향』 통권 제44호, 대검찰청, 2014.9, 99면.

법익침해나 재판의 공정성에 대한 시비는 원천적으로 차단되고 전자정보의 무결성에 대한 신뢰를 확보할 수 있다고 보는 것이다.[1077] 즉 참여권 보장의 취지가 전자정보의 압수수색 과정에서 수사기관에 의한 무분별한 침해로부터 피압수당사자의 프라이버시 등 법익을 보호하고, 이로써 형사절차의 공정성을 확보하고자 하는 데 있다는 것이다.[1078]

이와 같이 참여권의 법적 성질에 대한 여러 견해들 가운데 우리 대법원의 입장은 앞선 판례분석에서 본 바와 같이 무관정보 배제설에 입각하여 참여권을 보장하고 있다고 볼 수 있다. 즉 정보저장매체의 용량이 기하급수적으로 증가하면서 그 안에 대량으로 존재하는 디지털 정보 안에서 혐의사실과 관련되어 있는 정보만을 선별하여 압수하는 것이 용이하지 않은 상황에 처하게 되자, 피압수자의 참여를 통해 수사기관이 영장의 범위를 벗어나서 정보를 탐색 내지 압수하는 것을 사전에 통제하고자 하는 데 참여권이 갖는 의미가 있다고 보는 것이라 할 수 있다. 다만 참여권 그 자체는 「헌법」상 적법절차 원칙을 실현하기 위한 구체적인 방법의 하나일 뿐, 「헌법」상 권리는 아니라고 보는 것이 헌법재판소의 관점[1079]인데 비하여, 대법원은 신체의 자유와 정보에 대한 자기결정권을 동등한 차원의 것으로 이해할 뿐 아니라, 「헌법」에 보장된 진술거부권과 같은 의미를 디지털 시대 전자정보에 대한 압수수색에 관철할 필요가 있다[1080]고 보고 있다. 이러한 대법원의 관점은 적법절차 원칙을 실현하기 위한 입법정책적 수단의 하나로 법률에 규정한 참여권을 「헌법」에 규정된 적법절차 원칙과 동격으로 이해하고자 한다는 점에서 지나친 해석의 비약이라 할 것이다. 만약 실체적 진실이 명확함에도 불구하고 형사절차상 참여권을 기본권화하여 위반 시 절차 전체를 무효화 하게 된다면, 피고인의 인권을 위해 피해자뿐 아니라 일반국민들로 하여금 형사적 부정의 상황을 감내 내지 수용하라는 의미로 읽힐 수밖에 없을 것이다. 이는 형사사법의 존재 자체에 대한 회의를 야기하는 것으로, 또 다른 의미에서 사법불신을 초래한다고도 볼 수 있을 것이다.

1077) 박성민, "전자정보의 압수수색에 있어 정보검색의 성격과 피압수자 참여권 보장의 의미", 『형사정책』 제28권 제2호, 한국형사정책학회, 2016.9, 213면.
1078) 이진국, "전자정보압수·수색에서 피압수·수색 당사자의 참여권에 관한 일고", 『동아법학』 제11권 제4호, 아주대학교 법학연구소, 2018.2, 332면.
1079) 헌법재판소 2012.12.27. 2011헌바225 결정.
1080) 대법원 2015.7.16.자 2011모1839 전원합의체 결정에서 대법관 이인복, 이상훈, 김소영의 보충의견.

IT 기반 기술의 급격한 발전으로 사실상 디지털화된 사회에 살고 있는 현상황에서 디지털 정보의 중요성과 보호의 필요성은 이론의 여지가 없지만, 개인과 사회, 때로는 국가적 피해를 야기하는 범죄적 상황에 직면했을 때 이에 대응할 수 있는 입법적 수단도 결여된 상태에서 아날로그적 수사에 적용되는 적법절차를 그대로 디지털 수사에 적용하는 경우, 그동안 형사절차의 또 다른 핵심원리인 실체적 진실의 발견과의 조화를 도모해 왔던 형사사법의 균형을 유지하는 데 있어서 한계에 부딪힐 수밖에 없다고 할 것이다.

나. 참여권의 범위와 한계

현행법상 압수수색절차에 있어서 참여권의 범위와 관련해서는 어떠한 규정도 없기 때문에 온전히 법원의 해석에 의존하고 있다. 참여권의 범위와 관련해서는 압수수색 집행절차의 범위와 참여권자의 범위라고 하는 두 가지 측면에서 살펴볼 수 있다.

1) 압수수색 집행절차상 참여권의 범위

디지털 증거 압수수색절차에 있어서 어느 단계까지 참여가 가능한가라는 참여권의 범위는 압수의 종료시점을 언제로 볼 것인가 하는 문제와 직결되어 있다고 볼 수 있다.

이와 관련해서 먼저 현장에서 저장매체를 압수하는 순간 영장집행은 객관적으로 종료되고, 그 이후에 수사기관에서 행해지는 선별, 이미징, 복제, 분석 등의 행위는 압수물을 확인하는 임의수사의 영역이라고 보는 견해[1081]와 정보저장매체를 수사기관으로 반출하거나 이미징복제본을 만드는 단계는 압수절차가 완료된 것이 아니며, 복제본을 이용하여 정보를 탐색하면서 당해 사건과 관련성 있는 정보를 찾는 과정은 수색에 해당하고, 따라서 관련성 있는 정보를 탐색하여 압수대상이 되는 정보를 선별한 후 그 선별된 정보를 압수함으로써 압수절차가 종료된다고 보는 견해,[1082] 독일 형사소송법의 가압수 개념을 전제로 현장에서의 반출행위는 가압수단계이고, 수사기관 내에서의 이미징, 선별 탐색, 추출 및 출력까지를 압수단계로 보는 견해[1083] 등이 있다.

1081) 이완규, "디지털 증거 압수수색과 관련성 개념의 해석", 『법조』 제686호, 법조협회, 2013.11, 149-150면 참조.

1082) 오기두, "형사절차상 컴퓨터 관련 증거의 수집 및 이용에 관한 연구", 박사학위논문, 서울대학교, 1997.2, 76-81면 참조.

이와 관련하여 압수수색 집행절차상 참여권의 범위에 대해서 대법원은 2011년 결정문에서 "저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수수색 영장 집행의 일환에 포함된다"[1084]고 판시함으로써, 참여권이 보장되어야 하는 범위를 압수수색 집행현장에서 수사기관 내 사무실로 확장시켰다고 볼 수 있다. 즉 디지털 증거의 경우 현장선별이 가능한 일부 경우를 제외하고는 수사기관의 디지털포렌식 절차를 거쳐야 비로소 혐의사실과의 관련성을 토대로 내용상 식별이 가능한 상태가 되기 때문에, 사실상 디지털 증거가 수사기관에 의해 확보되는 단계는 선별작업 이후라고 할 수 있다. 따라서 대법원은 수사기관 내 사무실에서의 선별과정까지를 압수수색영장의 집행과정이라고 보는 것이라 할 수 있다. 이는 정보저장매체 자체의 용량 증가뿐 아니라 클라우드서비스를 통한 데이터 이용 및 저장에 있어서 시공간의 확대로 인해 다양한 정보의 혼재가능성이 높아질 수밖에 없는 현실에서 비롯된 것이라 할 수 있다. 즉, 수사기관 역시 혐의사실과의 관련성을 토대로 압수대상 정보를 사전에 또는 현장에서 특정한다는 것이 기술적으로도 시간적으로도 매우 어렵기 때문에, 사실상 다양한 정보가 혼재된 채 수사기관으로 이전되는 데서 비롯되는 기본권 침해 가능성을 배제하고자 수사기관 내 선별작업까지를 압수집행절차로 볼 수밖에 없는 것이라 할 수 있다. 이와 같이 육안으로 식별이 불가능한 디지털 증거에 한해서는 압수종료시기를 수사기관 내 선별작업시까지로 확장할 수밖에 없는 불가피성이 있다고 할 수 있다.

하지만 혐의사실과 관련성 있는 디지털 증거선별을 위한 수사기관 내 디지털포렌식 과정에 피압수자를 참여시키는 것이 참여권의 본질, 즉 절차의 공정성과 무관정보 배제에 실효적인가에 대해서는 논의의 여지가 있다. 즉, 혼재되어 있는 정보 전체에 대한 탐색을 전제하지 않고서는 유관정보를 선별한다는 것이 불가능한 상황에서 선별과정에 참여한다고 해서 무관정보의 탐색이 차단되는 것은 아니기 때문이다. 더욱이 삭제된 데이터를 복원하거나 특정 프로그램의 프로세스를 거쳐야 비로소 데이터를

1083) 박경규, "ICT 환경에서 압수·수색의 '피의사건과의 관련성' 요건이 가지는 의미, 현행법의 문제점 및 개선방안"(발표문), 『ICT 환경에서 형사실체·절차법의 주요쟁점』 2019년 하계 공동 학술세미나, 경북대학교 법학연구원 형사법센터·IT와 법 연구소·대검찰청 공동주최, 2019.8.27, 50면 이하.

1084) 대법원 2011.5.26.자 2009모1190 결정.

산출해 낼 수 있는 포렌식절차의 경우, 수사관이 아닌 포렌식전문가의 작업을 거치게 되는데 포렌식업무 담당자의 경우 IT 기술 전문가이기 때문에 담당수사관이 요청한 정보만을 선별할 뿐 스스로 무관정보 여부를 판단하지 않는 것이 일반적이라 할 수 있다. 또한 이와 같이 기술적이고 기계적인 포렌식업무의 경우 관련분야의 전문가가 아니고서는 무관정보의 탐색 및 추출 여부를 확인한다는 것이 어렵다고 할 수 있다. 결국 디지털포렌식에 특화된 전문변호사가 참여하는 경우에 한해서 무관정보에 대한 탐색 및 추출의 배제가 가능하다고 할 수 있으며, 그러한 전문변호사의 조력을 받을 수 없는 대부분의 피의자에게 있어서 참여권은 형식적 절차 가운데 하나에 불과하다고 볼 수 있다.

2) 참여권자의 범위

다음으로 참여권의 범위와 관련해서는 참여권자를 어느 범위까지 인정할 것인가에 대해서 대법원과 학계 간에 논란이 지속되고 있음을 볼 수 있다.

현행 「형사소송법」상 압수수색에 있어서 참여권자에 대한 규정은 제121조에 의한 당사자로서 검사, 피고인 또는 변호인의 참여권과 제123조의 피압수자의 참여권이 있으며, 제121조에 의한 참여권은 '참여할 수 있다'고 하는 임의적 규정인 반면, 제123조의 참여권은 '참여하게 하여야 한다'는 강제적 규정으로 되어 있다. 그리고 이 두 조항은 동법 제219조에 의해 수사기관의 압수수색에도 준용되기 때문에 피의자에 대해서도 참여권이 보장된다. 이와 같이 법률상 규정에 참여권자가 명시되어 있음에도 불구하고 실무와 판례에 있어서 참여권자의 범위와 관련하여 논란이 제기될 수밖에 없는 데는 다음과 같은 문제가 있기 때문이라 할 수 있다. 먼저 현행법 규정에 따르면 '피의자 = 피압수자'인 경우에는 피의자의 참여권은 강제적 규정에 해당하지만, '피의자 ≠ 피압수자'인 경우에는 피의자의 참여권은 임의적 규정에 해당에 해당한다고 볼 수 있다. 그런데 후자의 경우 피압수자가 보관 중이거나 점유 중인 실질적 압수대상인 정보의 소유자(주체)가 피의자인 경우에는 원칙적으로 '피의자 ≠ 피압수자'인 경우에 해당하기 때문에 피의자의 참여권은 수사기관의 재량적 판단이 개입될 여지가 있음에도 불구하고, 실질적 압수대상이 피의자 소유의 정보이기 때문에 피의자에게 실질적 피압수자의 지위를 부여하게 되면 '피의자 = 피압수자(실질적 피압수

자)'가 되어 참여권 보장이 강제되는 결과가 된다.

이는 디지털 증거 압수수색에 있어서는 형식적 압수대상인 정보저장매체의 점유 및 보관자와 실질적 압수대상인 정보의 소유자가 서로 다른 경우가 있을 뿐 아니라, 피의자와 실질적 압수대상인 정보의 소유자가 서로 다른 경우가 있는 데서 비롯되는 문제라고 할 수 있다. 더욱이 앞서 기술한 바와 같이 압수종료 시기를 현장압수에서 수사기관의 사무실에서의 탐색 및 선별절차까지 확장함으로 인해 현장에서 상황에 따라 참여가 배제 내지 제외된 경우라 하더라도 현장 외 수사기관 사무실에서의 탐색 및 선별과정에 있어서는 참여를 배제하거나 제외할 이유가 거의 없다고 볼 수 있기 때문에, 사실상 참여권의 문제는 대부분 현장 외 수사기관 사무실 내 압수수색의 참여권의 문제라 할 수 있는 것이다.

이와 같이 디지털 증거 압수수색절차에 있어서 참여권자와 관련하여 대법원은 '피압수수색 당사자(피압수자)'라는 용어를 사용하여 수사기관 사무실 내 복제, 탐색, 출력하는 전체과정에 참여의 기회를 보장해야 한다고 판시하였다.[1085] 하지만 현행법상 참여권 관련 규정인 「형사소송법」 제121조와 제123조, 그리고 제219조에 있어서는 피압수자라는 개념규정이 없기 때문에 판례에서 설시한 피압수자가 구체적으로 누구를 의미하는가에 대해서는 명확하지 않다고 할 수 있다. 다만 2015년 대법원 전원합의체 결정에 있어서 피압수자는 법 제121조에서 규정하는 피압수자라고 설시함으로써 '피압수자 = 피고인/피의자'라고 이해할 수 있다. 그러나 이후 정보의 저장 및 점유 또는 관리주체가 제3자인 경우가 일반화되면서 '피압수자 ≠ 피고인/피의자'가 되고, 따라서 피의자에 대한 참여권은 임의적 규정으로 해석될 수밖에 없는 상황에 처하게 되었다. 이에 대법원은 형식적인 압수수색의 당사자는 제3자이지만 제3자가 점유 또는 보관, 관리하는 정보의 실질적 소유자(주체)가 피의자인 경우에는 '실질적 피압수자'[1086]로 볼 수 있다고 판시하였고, 이에 의하는 경우 '피의자 = 피압수자(실질적 피압수자)'가 되기 때문에 피의자의 참여권은 배제할 수 없는 강제규정으로 해석할 수 있게 되는 것이다. 즉, 피의자에 대해 법 제121조의 임의적 규정이 적용됨으로 인해 참여권이 배제될 수 있는 상황에서, '실질적 피압수자'라는 개념을 가져와서

1085) 대법원 2011.5.26.자 2009모1190 결정; 대법원 2015.7.16.자 2011모1839 전원합의체 결정.
1086) 대법원 2021.11.25. 선고 2019도7342 판결; 대법원 2022.1.27. 선고 2021도11170 판결.

'피의자 = 피압수자'가 성립되도록 함으로써 법 제123조의 강제적 규정을 적용하여 압수대상인 실질적 정보의 주체인 피의자에 대해서는 절차상 참여권을 배제할 수 없도록 하고자 한 것이라고 이해되어 진다. 또한 참여권자를 실질적 피압수자인 피의자[1087]라고 적시함으로써 피의자에 한해 실질적 피압수자의 지위를 허용하고 있음을 알 수 있다.

다만 대법원은 이와 같이 실질적 피압수자로서 피의자의 참여권을 보장하고자 하는데 있어서도 "압수수색 당시 매체 내 전자정보 전반에 관한 전속적인 관리처분권을 보유, 행사하여야 하고, 압수수색 당시 외형적, 객관적으로 인식가능한 상태를 기준으로 판단"해야 한다고 하면서 정보주체에 해당한다고 해서 실질적 피압수자가 되는 것은 아니라고[1088]판시함으로써, 실질적 피압수자의 허용범위에 있어서 일정한 제한요건을 두고 있음을 볼 수 있다. 즉 압수대상이 되는 정보의 주체에 대해 피압수자의 지위를 허용하는 경우 참여권자의 범주가 무한히 확대될 우려가 있을 뿐 아니라, 설령 피의자가 정보의 소지보관자이거나 실질적으로 그에 의해 작성된 정보라 할지라도 참여권의 취지인 무관정보의 배제라는 측면에서 참여권을 보장할 가치가 없는 경우이거나, 압수수색 당시 해당 정보에 대한 현실적인 점유권을 포기, 상실, 방기한 경우에는 피압수자로서의 지위는 제한된다고 보고 있는 것이다.

그리고 이에 따라 형식적 피압수자가 아닌 피의자가 실질적 피압수자에도 해당하지 않는 경우에는 법 제121조의 임의규정에 의해 참여권이 제한될 수 있고, 따라서 참여권을 제한한다고 해서 위법은 아니라고 볼 수 있는 것이지, 피의자가 참여권자가 아니라고 해석[1089]할 것은 아니라고 보여진다.

다. 실무상 참여권 운용의 한계

앞서 살펴본 바와 같이 대법원이 디지털 증거 압수수색절차에 있어서 만큼은 '실질적 피압수자'라는 개념을 사용하면서까지 피의자의 참여권 보장의 필요성을 강조할

1087) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.
1088) 대법원 2022.1.27. 선고 2021도11170 판결.
1089) 구길모, "디지털 증거 압수수색과 참여권 보장", 『형사법연구』 제34권 제4호, 한국형사법학회, 2022.12, 226-227면; 박중욱, "전자정보의 압수수색과 피의자의 참여권 -대법원 입장의 비판적 수용 및 독일 논의의 참고-", 39면.

만큼, 디지털 증거 압수수색절차상 유무관 정보가 혼재된 상황에서 무관정보를 배제함으로써 피의자의 프라이버시 침해를 최소화하는 데 있어서 참여권이 갖는 의미는 적지 않다고 볼 수 있다. 하지만 참여권의 범위가 실제 압수대상인 정보를 선별·추출하게 되는 수사기관 내 디지털포렌식 과정으로 확대되면서 수사기관의 측면에서도, 피의자의 측면에서도 참여권 보장에 있어서 어려움이 야기되는 측면이 있음을 알 수 있다.

먼저 피의자의 측면에서 참여권을 행사하는 데 어려움을 겪는 경우를 살펴보면 다음과 같다. 피의자가 구치소에 수감되어 있는 경우 수사기관에서 참여를 요청해도 구치소에서 출감조치 협조가 잘 안되는 경우가 있어서 별도의 임의대리인을 지정해서 참여해야만 하는 경우가 발생한다고 한다.[1090] 이 경우 변호인이 있는 피의자의 경우에는 변호인 참여로 대체할 수 있지만, 변호인 이외의 임의대리인을 지정해서 참여하는 경우 임의대리인을 통한 무관정보의 배제가 가능할 것인가의 문제, 피의자가 본인 이외의 제3자(가족을 포함한)에게조차 공개하기 곤란한 내용의 정보인 경우에는 사실상 임의대리인을 지정하는 것조차 불가능한 문제로 인해 참여권이 보장되는데 한계가 있다고 볼 수 있다. 이외에도 피의자가 병원에 장기간 입원에 있거나 외국에 거주하는 경우, 국내라 하더라도 원격지 거주자 등의 경우에는 수사기관 내에서 이루어지는 디지털 증거 탐색, 선별 및 추출작업에 참여한다는 것이 현실적으로 용이하지 않을 뿐 아니라, 그로 인한 수사절차의 지연 내지 중단은 피해자뿐 아니라 경우에 따라서는 일반 국민들로 하여금 범죄로 인한 불안을 감내하도록 강요하는 결과를 초래할 수도 있다고 할 것이다.

다음으로 디지털포렌식 과정에의 참여는 단순 영상이나 텍스트의 선별이 아니고서는 어느 정도 포렌식에 대한 지식을 가지고 있어야 실질적 참여가 가능하다고 볼 수 있다. 이 경우 포렌식 전문변호사의 조력을 받을 수 있는 피의자의 경우에는 실질적인 참여권 보장을 받을 수 있지만, 전문변호사의 조력은 고사하고 일반 변호사의 조력도 받기 어려운 피의자의 경우에는 형식적으로 참여할 수밖에 없다고 할 것이다. 또한 피의자가 생계유지 활동을 멈출 수 없는 경우에는 장기간에 걸쳐 이루어지는 포렌식 과정에 참여하는 것이 현실적으로 불가능하다는 문제도 생각해 볼 수 있다. 수사실무상 피의자측이 포렌식 과정에까지 참여하는 비율이 10% 내외에 불과하다는

1090) 외부전문가(디지털포렌식 담당 경찰관) 자문회의(2023.8.29.) 내용 중 발췌.

담당자들의 얘기에 비추어 보아도 현실적으로 참여권을 행사할 수 있는 피의자들은 일부에 불과함을 알 수 있다. 더욱이 판례상 참여권자를 실질적 피압수자 – 법률상 정의되지 않은 – 를 포함하는 개념으로 해석함으로써 수사담당자에 따라 이를 해석하는 기준에 있어서 차별이 있을 수 있고, 그로 인해 사건의 경중 혹은 피의자의 사회적 지위에 따라 참여의 범위가 달리 적용될 가능성도 배제하기 어렵다고 할 것이다. 이러한 상황에서 적법절차 판단 시 참여권 여부가 유무죄 여부를 좌우하게 된다면 이는 또 다른 의미의 유전무죄 무전유죄의 결과를 초래할 수 있다는 우려를 배제하기 어렵다고 할 것이다.

한편 수사기관 측면에서 참여권 운영의 어려움 가운데 대표적인 것은 피의자측에 의한 참여권 악용이라고 할 수 있다. 즉, 피의자측에서 참여일자를 계속 연기하여 수사진행을 방해하는 경우가 가장 대표적인 경우라 할 수 있다. 그 외에 장기간에 걸쳐 포렌식작업이 이루어지는 경우 포렌식 담당자들은 업무시간 내에 작업이 이루어져야 함에도 피의자측이 그중 몇 시간만 참여하고 다른 날 참여하겠다고 하면 중간에 분석작업을 중단해야 하기 때문에 분석작업이 제대로 이루어지지 못하는 문제가 발생할 수 있다. 그리고 포렌식업무에 사용되는 분석툴과 관련해서 툴을 제공하는 업체와의 계약상 제품의 작동과정을 공개하는 것은 물론이고 제품의 외형, 심지어는 제품이름의 공개도 금지하는 경우가 있는데, 이 툴을 사용하여 분석하는 과정에 피의자측의 참여를 허용하게 되면 수사기관으로서는 계약위반 상황이 발생하기 때문에 참여를 허용하기 어려운 문제도 발생한다는 점도 지적된 바 있다.[1091] 다른 한편으로 수사기관의 사정에 따라 차이가 있기는 하지만, 수사기관 내 업무환경상 별도의 참여실이 없어서 담당 수사관의 옆자리에서 정보선별작업에 참여하는 경우 사실상 동일 공간 내 다른 수사관이나 다른 피의자의 시선으로부터 자유롭지 못하기 때문에 참여과정이 오히려 피의자의 프라이버시 침해를 유발할 우려를 배제하기는 어렵다고 할 수 있다. 마찬가지로 디지털포렌식이 진행되는 업무공간에 있어서도 별도로 마련된 참여실에서 분석관과 피의자측 참여인만 있는 상황에서 진행되지 않는 한, 수사관 사무실 내 참여와 동일한 문제가 발생할 여지가 있다고 할 수 있다.

1091) 외부전문가(디지털포렌식 담당 경찰관) 자문회의(2023.8.29.) 내용 중 발췌.

라. 디지털 증거 압수수색에 있어서 참여권의 개선방향

디지털 증거 압수수색에 있어서 유무관 정보의 혼재로 인한 사생활 및 기본권 침해의 우려를 방지하기 위한 절차적 수단으로서 참여권이 갖는 의미는 명확하다고 할 수 있다. 그럼에도 불구하고 현행법상 참여의 범위, 참여권의 주체, 참여권 보장을 위한 사전통지의 명확성 및 그 예외사유 등과 관련하여 디지털 증거의 압수수색에 부합하는 명확한 기준이 입법적으로 정비되지 못한 탓에 그 해석과 관련하여 논란을 야기하고 있다고 볼 수 있다. 그리고 디지털 증거 압수수색 시 적법절차를 확보함에 있어서 참여권이 갖는 의미를 지나치게 강조함으로써 마치 '참여권 = 적법절차'를 동일시하여, 참여권을 헌법적 권리로 이해하고자 하는 지나친 논리의 비약도 수사절차상 참여권이 실효적으로 작동하는데 오히려 역효과를 초래할 수도 있다고 볼 수 있다. 즉 참여권이 디지털 증거 압수수색 시 무관정보 배제를 위한 유일한 수단도 아니고, 실무상 모든 피의자에게 적합한 실효적인 수단이라고 보기도 어려운 상황에서, 참여권이 실체적 진실을 포기하고서라도 지켜야 할 정도의 가치가 있는 것인가 또는 그것이 형사적 정의를 실현하는 길인가에 대해서는 형사소송 이념의 재정립이라는 관점에서 신중한 논의가 필요하다고 할 것이다.

다만 참여권이 적법절차 실현을 위한 수단으로서 실효성을 담보하기 위해서는 그 방향성을 명확히 할 필요가 있다고 생각한다.

1) 참여권의 법적 지위의 명확화

압수수색절차에 있어서 참여권의 법적 지위와 관련해서는 이미 헌법재판소가 명확하게 "참여권의 보장은 국민의 기본권을 보장하고 헌법상 적법절차원칙의 실현을 위한 구체적인 방법의 하나일 뿐 헌법상 명문으로 규정된 권리는 아니다. …중략… 그 예외와 예외의 범위를 정하는 것은 입법자가 규범체계 전체와의 조화와 압수수색에 의해 침해되는 기본권의 중요성과 그러한 절차에 의해 수사목적이 제한되는 정도, 수사관행, 우리사회의 법현실 증 제반사정을 고려하여 정할 수 있는 입법재량이 있는 것"[1092]이라고 설시하고 있다. 즉 참여권은 적법절차 원칙을 실현하기 위한 입법적 수단 가운데

1092) 헌법재판소 2012.12.27. 2011헌바225 결정.

하나이기 때문에 그 자체를 적법절차 원칙으로 인식하는 것은 바람직하지 않다고 할 것이다. 따라서 수사의 공정성과 피의자의 방어권 보장이라는 측면에서 그 실효성을 담보할 수 있는 입법적 방안을 모색하는 것이 보다 더 적절하다고 할 것이다.

2) 참여권자에 대한 입법적 해결

현행 「형사소송법」상 참여권자에 관한 규정은 기존의 유체물에 대한 압수를 전제로 마련된 것일 뿐 아니라 법원에 의한 압수수색의 관점에서 규정된 것이기 때문에, 수사기관에 의한 무체정보, 즉 디지털 증거에 대한 압수수색에 있어서는 부적합한 측면이 나타날 수밖에 없다. 이러한 입법과 현실의 부적합성을 메우기 위해 법원이 궁여지책으로 내놓은 것이 '실질적 피압수자'라고 하는 개념이라고 할 수 있다. 즉 디지털 증거 압수수색에 있어서 압수대상과 피의자가 불일치하는 경우가 많을 뿐 아니라, 압수대상과 관련하여 피의자와 제3자 간의 이해관계의 충돌 내지는 프라이버시 침해 등의 문제가 야기될 수도 있기 때문에 어느 범위까지 참여권자로서 허용할 것인가가 용이하지 않은 문제가 될 수밖에 없다.

또한 현행법상 피의자에 대한 임의적 참여 규정, 피압수자에 대한 강제적 참여 규정이라고 하는 기본적인 틀을 디지털 증거에 대해서도 유지할 것인가에 대해서도 입법적 논의가 필요한 문제라고 할 수 있다. 즉 실질적 피압수자라는 개념을 통해 압수대상 정보의 주체인 피의자를 피압수자로 보아 강제적 참여를 허용하고 있는 실무에 비추어 볼 때, 피의자에 대해서도 피압수자와 마찬가지로 강제적 참여 규정을 두되, 디지털 증거의 취약성으로 인해 야기될 수 있는 증거의 훼손 및 멸실 등의 우려(원격 삭제, 안티포렌식 툴을 사용한 조작 및 삭제 등) 등과 같이 수사절차상 참여권을 배제할 수 있는 제한사유를 명확히 규정하는 것이 피의자에게는 방어권을 보장하면서도 수사의 목적이 훼손되지 않는 방안이 될 수 있을 것이다.

3) 참여권의 실질 확보

앞서 기술한 바와 같이 디지털 증거 압수수색절차에 있어서는 참여를 허용한다고 해서 모든 참여권자가 수사기관의 무관정보 탐색을 막거나 유관정보의 선별을 정확히 파악하는 것이 가능하다고 보기는 어렵다. 즉 참여행위 그 자체보다는 참여시 선별된

압수목록을 정확히 피의자 또는 피압수자에게 전달하는 것이 오히려 무관정보의 배제 여부를 확인하는데 보다 실효적이라 할 수 있을 것이다. 다만 이와 같이 압수목록을 통해 피의자 또는 피압수자측이 혐의사실과의 관련성 여부를 판단하기 위해서는 목록 기재의 구체성이 전제되어야 함은 당연하다고 할 것이다. 특히 디지털 증거의 경우 단순한 파일명만으로는 정보의 내용을 파악하는 것이 용이하지 않기 때문에, 좀 더 상세하게 파일 명세를 적시하는 것이 필요하다고 할 것이다. 이와 관련하여 판례도 "압수물 목록은 피압수자 등이 압수처분에 대한 준항고를 하는 등 권리행사절차를 밟는 가장 기초적인 자료가 되므로 …중략… 압수된 정보의 상세목록에는 정보의 파일 명세가 특정되어 있어야 하고"[1093]라고 설시하고 있다. 즉 압수대상이 되는 정보의 상세목록을 교부하는 것이 참여의 형식보다 오히려 참여권의 실질 – 무관정보 배제 및 방어권 확보 – 을 확보하는 데 있어서 훨씬 더 실효적이라 할 수 있는 것이다. 다만 이와 같이 압수정보의 상세목록을 교부함에 있어서 입법적으로 보다 명확히 하기 위해서는 압수의 목적물이 정보저장매체 또는 복제본, 이미징사본, 출력물이 아닌 디지털 정보 그 자체가 되어야 할 것이다. 즉 현행법상 압수의 목적물에 정보가 포함되지 않음에도 불구하고 정보가 압수의 대상이 된다고 하는 암묵적인 합의 하에 판례와 실무가 이루어지고 있는 것이 현실이지만, 수사기관에 대해 압수정보의 상세목록 교부라고 하는 의무를 부여하기 위해서는 그에 부합하는 입법적 개선이 우선되어야 할 것이다.

다른 한편으로 참여권의 실질을 확보할 수 있는 방안으로 검토해 볼 수 있는 것이 무관정보의 삭제 및 폐기라고 할 수 있다. 즉 수사기관이 정보저장매체를 압수하는 경우이든 아니면 이미징사본, 혹은 하드카피사본을 압수하는 경우에는, 혐의사실과의 관련성을 토대로 유관정보를 선별, 추출한 후에도 무관정보가 여전히 수사기관에 남아있게 된다. 이 경우 수사기관이 무관정보 탐색을 통해 별건 혐의의 단서를 포착하여 재수사를 하거나 2차 압수를 하는 경우도 있고, 이미 수사기관 내에 보관하고 있는 이미징사본에 대한 압수수색영장을 발부받는 경우도 발생할 수 있다. 이와 같이 정보저장매체 혹은 이미징사본 등을 압수하는 경우에는 영장에 기재된 혐의사실의 범위를 벗어난 정보를 수사기관이 활용할 가능성 때문에 사실상 압수의 효과가 매체 전체에

1093) 대법원 2018.2.8. 선고 2017도13263 판결.

미치는 불합리한 결과를 초래할 수 있는 것이다. 따라서 압수영장의 범위를 벗어난 무관정보가 혼재된 매체 혹은 이미징사본 등의 압수 시에는 유관정보의 선별 및 추출 후 매체의 반환 또는 이미징사본 등의 삭제 혹은 폐기가 이루어져야만 무관정보의 불법적 이용을 막을 수 있다고 할 수 있다.

그런데 이러한 무관정보의 삭제 및 폐기와 함께 고려되어야 하는 문제는 디지털 증거의 무결성 확보를 위한 디지털포렌식의 기본원칙 가운데 가장 중요한 무결성의 원칙과 재현의 원칙을 어떻게 유지할 것인가 하는 것이다. 즉 디지털포렌식에 있어서 정보저장매체 자체를 분석하는 것이 아니라 매체 자체에 대한 이미징사본을 작성한 후 매체는 반환하고 사본으로 분석하게 되는데, 이 경우 매체와 이미징사본의 동일성 검증을 위해 해시값을 확보하는 것이 원칙이고, 이 해시값을 통해 법정에서 동일성의 검증 및 chain of custody를 입증하게 된다. 그런데 무관정보 사용을 막기 위해 유관정보 선별 후 이미징사본을 삭제 내지 폐기하게 되면 해시값은 아무 의미가 없게 되고, 매체 원본과의 동일성 검증 자체가 불가능하게 된다. 또한 정보저장매체의 경우 피의자 또는 피압수자에게 환부되는 순간 이미 해시값이 달라지기 때문에 압수정보의 동일성과 무결성에 대한 사후 검증은 사실상 불가능하게 되는 것이다. 그럼에도 불구하고 법원은 판례를 통해 무관정보의 삭제 내지 폐기를 요구하고 있기 때문에, 수사실무상 동일성과 무결성 검증을 기술적 검증 아닌 기록상 검증으로 대체할 수밖에 없다. 이와 같이 압수정보의 무결성과 동일성 확인에 있어서 기록상 검증을 통한 방식은 디지털 증거에 있어서는 상당한 위험, 즉 증거의 오염 가능성을 내포할 수도 있다.

디지털 증거 압수수색에 있어서 수사기관의 과잉 압수로 인한 기본권 침해를 막기 위해서 무관정보의 삭제 및 폐기의 필요성이 불가피하다면, 디지털 증거의 무결성과 동일성 확보를 위한 기술적 검증이 가능한 방식으로 이루어질 필요가 있다고 할 것이다. 즉 압수 당시 해시값 확인을 통해 동일성이 검증된 이미징사본의 경우 유관정보의 선별 및 추출 후에는 수사기관이 아닌 중립적인 제3의 기관 또는 법원이 이를 일정 기간 – 사건별 기록보관 기간 동안 – 보관하도록 하는 방식을 검토해 볼 수 있을 것이다. 이 경우 수사기관이 분석을 위해 사용한 이미징사본의 복사본은 유관정보 선별, 추출 후 즉시 삭제 및 폐기하는 방식이 병행하여 이루어져야 무관정보 배제라는 본래의 취지가 실현될 수 있다고 할 것이다.

2. 디지털 증거 임의제출 시 압수와 관련한 쟁점

가. 임의제출물 압수의 법리 검토

임의제출물 압수는「형사소송법」제108조에 규정된 것으로, "소유자, 소지자 또는 보관자가 임의로 제출한 물건 또는 유류한 물건은 영장없이 압수할 수 있다"고 하는 영장주의 예외에 관한 규정이라 할 수 있다. 즉 점유의 취득과정에 강제력이 수반되지 않기 때문에 영장을 요하지는 않지만, 일단 수사기관으로 점유가 이전되면 임의제출자가 제출물을 다시 가져갈 수 없다는 점유의 강제성으로 인해 압수와 동일한 효과를 갖고 있기 때문에 강제처분으로 이해되고 있다.[1094] 이와 같이 임의제출물 압수규정은 제출의 임의성과 압수의 강제성이라고 하는 이질적인 두 가지 법률효를 하나의 조문으로 규정하고 있어서, 임의성에 중점을 두고 제도를 이해하는 입장과 강제성에 중점을 두고 제도를 이해하는 입장 간에 견해차가 존재하고 있다. 더욱이 임의제출물 압수의 경우 사후영장을 요하지 않기 때문에, 수사기관의 입장에서는 비교적 용이하게 증거를 확보할 수 있는 수단이 됨으로써 수사권 남용 가능성이 항상 내포되어 있다고 볼 수 있다. 즉 수사기관의 우월적 지위로 인해 임의제출의 명목으로 실질적인 강제압수를 행할 수 있기 때문이다. 따라서 영장없는 압수의 강제성을 정당화하기 위해서는 제출의 임의성에 대한 입증이 필수적이고, 이러한 임의성에 대한 입증은 검사가 합리적 의심을 배제할 수 있을 정도로 증명해야 한다고 대법원은 판시하고 있다.[1095]

이와 같이 기존의 임의제출물 압수에 있어서는 제출의 임의성에 대한 입증만으로도 압수의 적법성이 확보될 수 있었지만, 디지털 증거에 대한 임의제출물 압수에 있어서는 임의성에 대한 입증과 더불어 디지털 증거에 적용되는 압수의 법리가 그대로 적용되어야 한다는 것이 판례의 입장이라 할 수 있다. 이는 기존의 유체물에 대한 임의제출 시 압수와 같은 논리를 정보저장매체에 대한 임의제출 시 그대로 적용하게 되면 정보저장매체 전부에 대한 압수가 가능하다고 볼 수 있는 불합리한 결과가 발생하기 때문이다. 즉 영장에 의한 압수의 경우에 있어서도 정보저장매체에 저장된 정보 가운데 혐의사실과 관련성 있는 정보에 한해서 압수가 가능함에도 불구하고, 영장없는 압수

1094) 이재상·조균석, 앞의 책, 329면.
1095) 대법원 2016.3.10. 선고 2013도11233 판결.

의 경우인 임의제출 시에 혐의사실과의 관련성 여부와 상관없이 정보저장매체 전부에 대한 압수가 가능하다고 보게 되면, 관련성 판단, 참여권 보장 및 압수목록 교부 등과 같이 정보압수에서 요구되는 적법절차적 통제수단이 배제되는 문제가 발생할 수밖에 없는 것이다. 특히 스마트폰과 같이 개인의 사생활과 관련된 다량의 정보가 혼재되어 있는 매체를 임의제출하는 경우에 있어서는, 관련성에 기한 압수범위의 제한이 수반되지 않는 한, 피압수자의 프라이버시는 물론 다수의 기본권에 대한 심각한 침해를 야기할 수 있다는 우려를 배제하기 어렵다고 할 것이다.

따라서 디지털 증거에 대한 임의제출 시 압수와 관련해서는 제출의 임의성에 대한 입증과 함께 정보압수의 기본원칙에 따른 압수절차의 적법성 판단이 이루어져야, 비로소 임의성과 강제성이라고 하는 양면적 성격의 임의제출물 압수의 정당성이 확보된다고 보아야 할 것이다.

나. 제출의 임의성 입증

1) 제출의사의 임의성

임의제출물 압수의 적법성 판단에 있어서 가장 기본적이면서도 중요한 요소는 제출의사의 임의성이다. 여기서 임의성이란 단순한 자발적 의사에 그치는 것이 아니라, 제출자가 자신의 행위의 의미와 그 행위로 인한 발생효과,[1096] 즉 임의제출 시 발생하는 법적 효과를 알고 있음에도 불구하고 자발적으로 대상물건을 수사기관에 제출하는 것[1097]을 의미한다고 보아야 한다. 따라서 제출의 임의성을 입증하기 위해서는 제출자가 임의제출의 법적 효과인 제출물의 압수가 발생한다는 사실을 알고 있어야 한다고 보아야 한다. 따라서 자발적 제출이었지만 일단 수사기관으로 점유가 이전되면 임의로 반환받지 못하는 강제성이 발생한다는 사실을 제출 당시 인지하지 못했다면 임의성이 있다고 보기는 어렵다고 할 것이다.[1098]

1096) 김인회, "2016년 형사소송법 중요 판례", 『인권과 정의』 제464호, 대한변호사협회, 2017.1, 252면.
1097) 박상욱, "임의제출물에 대한 압수와 임의성 판단", 『법률신문』 2023년 8월 4일자 로펌 뉴스레터(율촌)(https://www.lawtimes.co.kr/LawFirm-NewsLetter/189979; 최종접속일 2023.9.20.).
1098) 동일한 취지로는 권창국, "임의제출에 의한 수사기관의 전자정보 압수와 관련한 제 문제의 검토 -대상판례: 대법원 2021.11.18. 선고 2016도348 전원합의체 판결 및 대법원 2022.1.27. 선고 2021도11170 판결-", 『사법』 통권 제62호, 사법발전재단, 2022.12, 253면 참조.

이와 같이 제출자가 제출의 법적 효과인 압수 여부를 인지하기 위해서는 제출 시 압수효가 발생한다는 사실 뿐만 아니라 제출을 거부할 수도 있다는 점을 수사기관으로부터 고지받아야 한다. 이러한 고지에도 불구하고 제출자가 자발적으로 수사기관에 대상 물건의 점유이전을 용인하였다면 임의제출의사를 명확히 표명한 것이라 볼 수 있고, 이를 통해 제출의 임의성에 대한 입증이 이루어진다고 할 것이다.

다만 현행법상으로는 임의제출물 압수 시 압수사실에 대한 사전고지의무가 수사기관에 부여되어 있지 않지만, 현재 수사기관 훈령인 「디지털 증거의 수집, 분석 및 관리 규정」(대검예규 제1285호) 제25조의 경우에는 '임의제출의 취지와 범위 확인', 경찰청 훈령인 「디지털 증거의 처리 등에 관한 규칙」(경찰청 훈령 제1086호) 제22조에 의한 '임의제출 의사의 확인'과 '제출된 정보가 증거로 사용될 수 있음을 설명하고 제출받아야 함'이라고 규정하고 있음을 볼 때, 수사기관의 입장에서도 제출의 임의성 확보의 필요성에 대한 인식이 존재하고 있음을 알 수 있다. 하지만 임의제출물 압수 자체가 임의수사가 아닌 강제수사라는 점에 대해서 이론의 여지가 없는 상황에서, 기본권 침해를 전제로 하는 강제수사의 적법성 확보의 전제조건인 임의성 입증요건을 법률이 아닌 행정규칙임의제출에 의한 수사기관의 전자정보압수와 관련한 제문제의 검토로 규정하는 것은 바람직하다고 보기는 어려울 것이다. 또한 임의제출물 압수를 통해 영장주의 원칙을 우회하는 불합리한 결과를 초래하지 않기 위해서는 합리적 의심의 여지가 없을 정도로 임의성에 대한 입증이 이루어져야 할 것이다.[1099]

한편 제출의사의 임의성 입증과 관련하여 가장 문제가 될 수 있는 상황으로는 현행범체포에 수반되는 임의제출물 압수를 들 수 있다. 즉 현행범체포 시 수사기관은 증거확보 수단으로 사후영장 또는 임의제출 가운데 하나를 취사선택할 수 있는데, 전자는 압수 후 영장처리업무가 수반되는 반면, 후자는 영장없이 압수가 가능하기 때문에 수사기관으로서는 임의제출방식을 선호할 수밖에 없다. 그런데 체포과정에 있는 피의자가 자신의 죄책을 증명하는 물건을 자발적으로 제출하는 것이 현실적으로 가능한가, 체포현장에서 심리적으로 위축되어 있는 피의자가 우월적 지위에 있는 수사기관의 증거물 제출요구를 거절할 수 있다고 보는 것이 일반적인 상식에 부합하는가에 대해서는 의문의 여지가 있다고 할 수 있다. 이에 대해 대법원은 "현행범체포현장

1099) 대법원 2016.3.10. 선고 2013도11233 판결.

이나 범죄장소에서도 소지자 등이 임의로 제출하는 물건은 영장없이 압수할 수 있고, 이 경우에는 검사나 사법경찰관이 사후에 영장을 받을 필요가 없다"[1100]고 함으로써 현행범체포 시 제출의 임의성이 인정될 수 있음을 전제하는 입장을 취하고 있다. 현행범체포 시 제출의 임의성 판단은 구체적 상황에 따라 종합적으로 판단해야 하겠지만, 수사기관의 우월적 지위에서 거부권의 고지 없이 또는 압수효의 발생사실에 대한 설명 없이 일방적 제출요구에 따라 임의제출이 이루어진 경우에는 실질적 의미의 임의성이라 하기는 어렵다고 본다. 이러한 경우에는 압수 후 사후영장에 의하는 것이 영장주의 원칙에 부합하는 것이라 할 것이다.

2) 제출자에 의한 임의제출 범위의 제한

디지털 증거에 대한 임의제출 시 논의가 되고 있는 쟁점 가운데 하나가 제출자가 제출의 범위를 제한할 수 있는가 하는 문제이다. 즉 임의제출에 의한 압수를 정당화할 수 있는 근거가 제출자의 자발적 제출의사에 있는 이상, 제출자가 범위를 한정하여 제출하는 것까지 임의성의 범위에 포함되는가 하는 것이다. 이에 대하여 법률상으로는 아무런 규정이 없지만 판례의 입장을 살펴보면, "혐의사실과 관련된 정보와 무관정보가 혼재되어 있는 매체나 복제본을 수사기관에 임의제출하는 경우 제출자는 제출 및 압수의 대상이 되는 정보를 개별적으로 지정하거나 그 범위를 한정할 수 있다. …중략… 매체를 임의제출하는 사람이 거기에 담긴 정보를 지정하거나 제출범위를 한정하는 취지로 한 의사표시는 엄격하게 해석해야 하고, 확인되지 않은 제출자의 의사를 수사기관이 함부로 추단하는 것은 허용될 수 없다"[1101]고 판시함으로써, 제출의사의 임의성에는 제출 여부에 관한 결정뿐 아니라 제출 범위에 대한 선택까지 포함된 것으로 해석하고 있음을 알 수 있다.

만약 제출 시 임의제출의 범위를 한정해서 제출했음에도 불구하고 그와 무관하게 임의제출물 전부에 대한 압수를 진행하는 경우, 제출범위를 벗어나서 압수한 정보에 대해서는 임의성에 대한 입증이 없다고 볼 수 있고, 따라서 영장주의에 위배되는 위법한 압수라 할 것이다. 앞서 기술한 바와 같이 대검찰청예규에 있어서도 위와

1100) 대법원 2016.2.18. 선고 2015도13726 판결; 대법원 2019.11.14. 선고 2019도13290 판결.
1101) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.

같은 판례의 태도를 반영하여 임의제출물 압수 시 압수의 범위를 확인하도록 규정하고 있음을 볼 수 있다.

즉 유체물에 대한 임의제출 시 압수의 법리를 정보저장매체에 그대로 적용하는 경우, 해당 매체에 혐의사실과 무관하게 혼재되어 있는 프라이버시, 기타 기본권 관련 정보들에 대해서까지 수사기관으로 하여금 탐색하도록 허용하는 결과를 초래할 수 있다는 점을 고려하여 볼 때 정보저장매체에 대한 임의제출에 대해서는 그 임의성 입증을 보다 엄격하게 해석하는 것이 타당하다고 본다.

3) 임의제출의 주체 – 제3자에 의한 임의제출과 관련한 문제

현행법상 임의제출물 압수 규정에 따르면 제출의 주체는 소유자, 소지자, 보관자로 한정되어 있다. 따라서 피의자가 아닌 제3자도 그 물건을 소유, 소지, 보관하고 있는 경우에는 수사기관에 임의로 제출할 수 있도록 되어 있다. 이 경우 제출자가 적법한 권리자일 필요는 없다는 것이 학계의 대체적인 견해이다.[1102] 따라서 적법한 권리자가 아니라 할지라도 물건을 소지, 보관하고 있는 사람은 소유자의 제출의사와 무관하게 임의제출할 수 있지만, 제출대상이 되는 물건을 소지 또는 보관하지 않은 자가 임의제출하는 것은 위법하다고 본다.

이 경우 문제가 되는 것은 피해자가 피의자 소유의 증거물을 절취하여 수사기관에 임의제출하는 경우, 불법촬영을 목격한 현장에서 제3자가 피의자로부터 스마트폰을 빼앗은 후 수사기관에 임의제출하는 경우 등과 같이 불법적 수단으로 확보한 증거에 대해 피해자 또는 제3자가 임의제출의 주체가 될 수 있는가 하는 것이다. 즉 사인이 위법하게 수집한 증거를 임의제출의 형식을 빌어 증거로 사용하는 것이 타당한가에 대해서 이의를 제기할 수 있기 때문이다.[1103]

앞서 살펴본 바와 같이 소지나 보관에 있어서 적법한 권원 여부를 문제삼지 않는다고 보는 다수의 견해에 비추어 보면, 불법적 수단에 의한 소지라 하더라도 소지자에 해당하기 때문에 임의제출이 가능하다고 볼 수 있고, 따라서 합법적인 증거로 압수할

1102) 이재상·조균석, 앞의 책, 329면; 신동운, 『신형사소송법』(제5판), 법문사, 2014, 435면; 한상훈, "임의제출물의 영치와 위법수집증거 배제법칙 -대법원 2016.3.10. 선고 2013도11233 판결-", 『법조』 제65권 제8호, 법조협회, 2016.10, 609면.

1103) 최병각, "휴대폰의 압수와 저장정보의 탐색", 『비교형사법연구』 제22권 제3호, 한국비교형사법학회, 2020.10, 178-179면 참조.

수 있다고 보아야 할 것이다. 하지만 피의자의 입장에서는 자신의 범죄사실과 별개로 타인의 불법적 행위로 인한 피해상황에 놓여 있음에도 불구하고, 범죄사실과의 관련성으로 인해 기본권 침해를 수인하게 될 수밖에 없게 된다고 볼 수 있다. 이 경우 만약 피의자의 인권을 고려하여 합법적인 소지 또는 보관자에 의한 임의제출만 영장없는 압수대상으로 하는 경우, 피해자가 자신의 범죄피해를 입증하기 위해 또는 제3자가 내부고발이나 공익적 목적을 위해 피의자 소유의 물건이나 기타 증거를 확보하는 것이 원천적으로 차단되는 문제가 발생할 수 있기 때문에 오히려 형사적 정의에 반하는 결과를 초래한다고도 볼 수 있다. 이와 관련하여 대법원은 제3자에 의해 수집된 증거를 대상으로 영장없는 압수수색을 할 수 있다고 보고 있으며, 다만 이 경우 압수의 범위와 관련하여 "혐의사실과 관련성을 증명할 수 있는 최소한의 가치가 있는 정보"[1104]로 엄격히 제한하여 해석함으로써 피의자의 기본권 침해에 대한 우려를 최소화하고 있음을 볼 수 있다.

다. 압수의 강제성

디지털 증거의 경우 임의제출 시 압수에 있어서는 제출의 임의성이 입증되었다고 해서 압수의 적법성이 바로 인정되는 것은 아니며, 비록 영장에 의한 것이 아니라 하더라도 정보압수의 기본원칙들 – 혐의사실과의 관련성, 압수의 범위, 참여권 보장, 압수목록 교부, 별건 혐의 발견 시 조치 – 이 그대로 준수되어야만 압수의 적법성이 인정될 수 있다. 즉 제출 자체는 임의적이지만 수사기관에 점유가 이전되는 순간 개인의 기본권을 침해하는 강제처분인 압수효가 발생하기 때문에 강제수사로서의 규제가 필요하다. 특히 정보저장매체의 경우 사생활의 비밀과 자유, 정보에 대한 자기결정권 등 인격적 법익에 관한 것이 모두 저장되어 있기 때문에, 강제수사로서의 규제가 수반되지 않게 되면 피의자의 기본권에 대한 심각한 침해가 발생할 수밖에 없다고 할 수 있다.

1104) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결; 대법원 2021.11.25. 선고 2016도82 판결.

1) 혐의사실과의 관련성 판단기준

임의제출물 압수 시 관련성 판단기준과 관련하여 대법원은 "그 관련성은 임의제출에 따른 압수의 동기가 된 혐의사실의 내용과 수사대상, 수사경위, 임의제출과정 등을 종합하여 구체적·개별적 연관관계가 있는 경우에만 인정되고, 혐의사실과 단순히 동종 또는 유사범행이라는 사유만으로는 관련성이 있다고 할 것은 아니다"라고 판시하고 있다.[1105] 관련성과 관련하여 특히 불법촬영의 경우에 있어서는 "범죄의 속성상 해당 범행의 상습성이 의심되거나 피고인의 성적 기호 내지 경향성의 발현에 따른 일련의 범행의 일환으로 의심되는 경우에는 간접증거나 정황증거로서 범행과의 구체적 개별적 연관관계를 인정할 수 있다"[1106]고 판시함으로써 관련성의 판단기준으로 객관적 범행사실과 함께 주관적인 행위자 특성도 고려할 수 있음을 보여주고 있다.

한편 피의자가 아닌 피해자 등 제3자가 피의자 소유의 매체를 임의제출하는 경우에 있어서는 관련성 판단기준을 피의자에 의한 임의제출 시 보다 엄격하게 해석하도록 요구하고 있는 것이 대법원의 입장이다. 즉 "피의자가 소유관리하는 매체를 피의자가 아닌 피해자 등 제3자가 임의제출하는 경우에는 …중략… 임의제출의 동기가 된 범죄혐의사실과 구체적·개별적 연관관계가 있는 전자정보에 한해 압수대상이 되는 것으로 더욱 제한적으로 해석해야 한다. … 피의자가 소유관리하는 매체에는 …중략… 인격적 법익에 관한 모든 것이 저장되어 있어서 제한없이 압수수색이 허용될 경우 피의자의 인격적 법익이 현저히 침해될 우려가 있기 때문이다"[1107]라고 판시하고 있다.

2) 압수의 범위

임의제출물 압수의 경우 원칙적으로 제출의 임의성이 담보되기 위해서는 제출의사의 임의성뿐만 아니라 제출내용의 임의성까지 보장되어야 한다. 따라서 제출자가 임의제출의 범위를 지정하거나 제한한 경우에는 압수의 범위는 제출자의 의사에 따라 제한되어야 한다. 이는 판례가 일관되게 판시하고 있는 임의제출 시 원칙적인 압수의 범위이기 때문에, 수사기관 역시 예규를 통해 임의제출자의 제출범위를 명확히 특정하도록 규정하고 있음을 볼 수 있다.

1105) 대법원 2021.11.25. 선고 2016도82 판결; 대법원 2021.11.25. 선고 2019도7342 판결.
1106) 대법원 2021.11.25. 선고 2019도7342 판결; 대법원 2021.11.25. 선고 2019도6730 판결.
1107) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.

이 경우 제출자가 임의제출의 범위를 특정하지 않고 제출한 경우 압수의 범위를 어떻게 해석할 것인가가 문제될 수 있다. 즉 임의제출자가 피해자나 제3자인 경우 제출대상 정보에 대한 이해관계가 없기 때문에 압수의 범위를 구체적으로 특정하여 제출할 필요성을 느끼지 못하는 경우가 있다. 그리고 피의자의 경우에도 현행범체포와 같은 상황에서 당황하게 되면 설령 수사기관에 의한 고지가 있더라도 제대로 대응하지 못하고 제출하는 경우가 있을 수 있다. 이와 같이 압수범위와 관련하여 임의제출자의 의사가 불명확한 경우에 있어서 대법원은 "임의제출자의 의사에 따른 정보의 압수대상과 범위가 명확하지 않거나 이를 알 수 없는 경우, 임의제출에 따른 동기가 혐의사실과 관련되고 이를 증명할 수 있는 최소한의 가치가 있는 정보에 한해 압수대상이 된다"[1108]고 판시하고 있다. 따라서 임의제출된 매체에서 압수대상이 되는 정보의 범위를 초과하여 탐색, 복제, 출력하는 경우에는 위법한 압수수색에 해당하기 때문에 위법수집증거배제법칙에 따라 증거로 사용할 수 없도록 하고 있다.

3) 참여권 보장

제출자가 임의제출함으로써 수사기관으로 대상 매체가 점유이전되는 순간부터 압수가 진행되는 것은 사실이지만, 영장에 의하지 아니한 압수이기 때문에 「형사소송법」 제121조에 규정된 영장집행 시 요구되는 참여권이 임의제출물 압수 시에도 적용되는가에 대해서는 논의의 여지가 있을 수 있다. 즉 임의제출물 압수는 영장없는 압수이고, 따라서 영장집행과는 무관하기 때문에, 법문상으로만 보면 영장집행 시 참여권 규정의 적용이 배제되는 것으로 볼 수 있는 것이다.[1109] 하지만 영장집행 시 참여권이 영장 자체의 적법성이 아닌 압수의 공정성과 적법성을 담보하기 위한 것이라고 본다면, 영장 없는 압수라 하더라도 압수 자체의 적법성을 담보할 수 있는 절차적 통제의 필요성은 분명히 존재한다고 보아야 할 것이다.

특히 정보저장매체에 대한 임의제출 시에는 영장에 의한 정보압수와 같이 "현장선별원칙, 예외적 매체압수"가 행해지기보다는, 일단 수사기관으로 정보저장매체 자체의 점유이전이 행해진 이후에 관련 정보의 선별이 이루어지는 것이기 때문에, 영장

1108) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결.
1109) 박용철, "정보저장매체 임의제출 압수의 의의", 『외법논집』 제46권 제1호, 한국외국어대학교 법학연구소, 2022.2, 273면.

에 의한 압수수색 현장과 같이 피압수자 참여로 인한 증거인멸 또는 훼손, 은닉의 우려가 거의 없다고 볼 수 있고, 따라서 관련 정보의 선별압수 과정에 피압수자의 참여권 보장을 제한할 이유가 없다고 할 것이다. 더욱이 정보저장매체 전체가 수사기관의 점유하에 있기 때문에 관련 정보를 탐색하는 과정에서 별건 혐의를 발견하거나 또는 피압수자의 인격권을 심각하게 침해할 우려가 있는 정보를 탐색할 가능성을 배제하기 어렵다고 할 수 있다. 이와 같이 임의제출의 원인이 된 관련 정보의 범위를 넘어서는 정보의 탐색, 선별에 대한 우려를 배제하기 위한 수단으로써 피압수자의 참여권을 보장하는 것이 압수의 적법성을 담보하는 데 필요하다고 본다.

임의제출물 압수 시 참여권 보장과 관련하여 특히 문제되는 부분은 피해자 또는 제3자에 의하여 피의자 소유 및 관리에 속하는 정보저장매체가 임의제출된 경우, 피의자에 대해서 참여권을 보장할 것인가라고 할 수 있다. 이에 대하여 대법원은 "제3자가 피의자의 소유관리에 속하는 매체를 영장에 의하지 않고 임의제출한 경우 실질적 피압수자인 피의자가 수사기관으로 하여금 그 정보 전부를 무제한 탐색하는 데 동의한 것으로 보기 어려울 뿐 아니라, 피의자 스스로 임의제출한 경우 피의자의 참여권이 보장되어야 하는 것과 견주어 보더라도 특별한 사정이 없는 한 형소법 제219조, 제121조에 따라 피의자에게 참여권을 보장하고 압수한 정보목록을 교부하는 등 피의자의 절차적 권리를 보장하기 위한 적절한 조치가 이루어져야 한다"[1110]고 판시함으로써 실질적 피압수자라는 개념을 들어 제3자에 의한 임의제출물 압수 시 피의자의 참여권을 보장하고 있다. 제3자에 의한 임의제출물 압수에 대한 대법원의 태도를 보면, 제출자는 정보저장매체의 점유상태를 수사기관으로 이전시킨 것에 불과할 뿐 아니라 해당 매체에 저장된 정보의 압수로 인하여 기본권이 침해되는 주체도 아니고, 압수절차에 있어서 참여권을 보장받아야 할 실질적 이해관계를 갖고 있는 것도 아니기 때문에 제출자를 피압수자로 볼 수 없다고 판단하고 있는 것이라 보여진다. 그에 비해 임의제출로 인해 실질적인 압수의 객체가 된 해당 매체의 소유관리자는 압수절차에서 자신의 정보가 무분별하게 탐색되는 것을 막아야 하는 이해관계를 갖고 있기 때문에 실질적 피압수자로서 참여권을 보장받아야 한다고 보고 있는 것이라 할 것이다.

1110) 대법원 2021.11.18. 선고 2016도348 전원합의체 판결; 대법원 2021.11.25. 선고 2019도7342 판결.

다만 이러한 경우 임의제출한 제3자가 내부고발자이거나 피해자인 경우, 수사기관은 정보저장매체를 임의제출 받은 후에 비로소 해당 사건에 대한 범죄사실을 인지하게 되는 것이 일반적이라 할 수 있다. 이 경우 제출된 매체에 대한 탐색과 그에 기반한 수사가 이루어지지 않고서는 해당 혐의사실에 대한 피의자를 특정하거나 전체 범죄사실에 대한 정확한 파악이 이루어지는 것이 불가능하다고 볼 수 있다. 이와 같이 피의자가 특정되지 않거나 설령 특정되었다고 하더라도 아직 혐의사실에 대한 정확한 파악이 이루어지지 않은 상태에서 임의제출된 정보저장매체에 대한 탐색과정에 실질적 피압수자인 피의자를 참여하게 하는 경우, 피의자로 하여금 혐의사실과 관련된 증거를 인멸하거나 훼손할 수 있는 사실상의 기회를 제공하는 결과를 초래할 수 있다는 우려를 배제하기는 어렵다고 할 것이다. 따라서 제3자에 의한 임의제출물 압수에 있어서 실질적 피압수자인 피의자의 참여권에 대해서는 일정한 예외를 인정할 필요성이 있다고 할 것이다.

라. 디지털 증거에 부합하는 임의제출물 압수규정의 개선방향

현행법상 임의제출물 압수규정은 유체물을 전제로 한 것이기 때문에 압수대상이 특정될 수 있고, 관련성 역시 대부분 외형적 판단이 가능하기 때문에 압수범위에 대한 특별한 고려가 필요하지 않았다고 볼 수 있다. 하지만 앞서 기술한 바와 같이 정보저장매체에 대한 임의제출 시 압수에 있어서는 해당 매체에 대한 탐색이 이루어지기 전에는 수사기관으로서도 임의제출의 동기가 된 혐의사실과의 관련성 또는 피의자를 인지하는 것 자체가 현실적으로 불가능하다는 문제가 있다. 또한 정보저장매체의 기능과 특성으로 인해 해당 매체 소유자의 프라이버시나 기본권을 침해할 수 있는 내용의 정보가 포함되어 있는 것이 일반적이기 때문에, 유관정보와 무관정보가 혼재된 상태로 정보탐색을 하는 과정에서 기본권 침해에 대한 우려를 배제하기 어렵다고 볼 수 있다. 즉 현행법상 임의제출물 압수규정은 영장에 의하지 않고도 혐의사실과의 관련성 판단을 배제한 채 매체에 저장된 모든 정보를 탐색할 뿐 아니라 압수할 수도 있는 가능성을 제공하는 규정이라고도 볼 수 있다. 정보압수에 수반될 수밖에 없는 기본권 침해의 가능성을 통제할 수 있는 입법적 대응이 마련되지 못한 상태에서 임의제출물 압수 규정은 영장에 의한 통제를 회피하는 동시에 수사의 편의를 우선할 수

있는 우회수단이 될 수밖에 없다. 즉 수사절차상 디지털 증거의 확보가 필수적인 상황임에도 이에 대한 입법적 개선이 이루어지지 못한 상태에서 임의제출물 압수규정은 디지털 수사의 적법성을 담보하는데 저해요인이라 할 수 있을 것이다.

이와 같이 정보저장매체에 대한 임의제출 시 압수로 인해 야기되는 정보의 과잉압수 및 기본권 침해에 대한 우려를 배제하기 위해, 법원은 제출의 임의성과 압수의 강제성을 분리하여 임의성의 입증과 정보압수의 기본원칙의 적용을 통한 절차적 통제를 강조하게 되었다. 뿐만 아니라 임의성 입증에 있어서 제출의사의 임의성뿐 아니라 제출정보 범위의 임의성까지 요구하게 되었고, 정보압수의 강제성 통제를 위한 절차적 수단으로서 압수 전과정에 있어서 참여권 보장 및 참여권자의 확장적 해석 – 실질적 피압수자 개념 도입 – 을 통해 정보주체의 기본권 침해 가능성을 최대한 억제하고자 하고 있음을 볼 수 있다. 즉 정보저장매체에 대한 임의제출 시 압수에 대한 입법의 흠결을 보완하기 위해서는 사법적 통제가 필수적이 될 수밖에 없다고 할 것이다.

하지만 임의제출물 압수 규정에 대한 법원의 통제수단이 반영된 입법적 개선이 이루어져야 수사절차상 정보압수에 있어서의 일관된 적법성이 온전히 담보될 수 있다는 점에 대해서는 이의의 여지가 없다고 할 것이다. 따라서 정보저장매체에 대한 임의제출 시 압수에 있어서 지켜져야 할 입법적 원칙을 정리해 보면 다음과 같다.

첫째, 제출의 임의성 담보를 위해서는 제출대상이 압수된다는 것과 제출을 거부할 수 있다는 사실을 사전에 고지해야 한다.

둘째, 정보저장매체를 임의로 제출받는 경우 제출자가 제출하고자 하는 정보의 범위를 제한할 수 있다는 사실을 고지해야 한다.

셋째, 제출자가 제출 시 정보의 범위를 제한하는 경우에는 그 범위 내에서만 압수가 이루어져야 한다. 만약 제출자가 정보의 범위를 사전에 제한하지 못했거나 전부를 임의제출한 경우에도 압수의 전제가 되는 혐의사실과 관련된 범위에 한해서만 압수할 수 있다.

넷째, 제출의 임의성과 별개로 압수의 강제성이 수반되는 이상, 디지털 정보 압수수색의 기본원칙, 즉 i) 혐의사실과 관련된 부분에 한해서 출력 또는 복사, 예외적으로 전체 이미징 또는 복제 후 선별 출력, ii) 압수 전과정에 있어서 참여권 보장, iii) 압수완료 후 임의제출된 정보저장매체의 반환, iv) 압수목록 교부 등을 준수해야 한다.

다섯째, 임의제출된 정보저장매체에서 별건 혐의와 관련된 정보 발견 시, 해당 정보는 임의제출대상이 아니므로 별도로 압수수색영장을 발부받아야 한다.

여섯째, 제3자에 의한 임의제출물 압수 시 실질적 피압수자인 피의자에 대한 사전고지 및 참여권 보장의 필요성과 함께 예외규정의 필요성도 명백히 존재하므로 예외사유도 마련해야 한다.

제2절 | 디지털 환경에 부합하는 새로운 증거확보방안 – 법률적 문제점과 도입가능성

1. 디지털 증거(데이터) 보전명령제도

가. 필요성 및 해외 입법동향

디지털 환경하에서 수사의 성패는 관련 데이터를 얼마나 신속하게 확보하는가에 달려있다고 볼 수 있다. 디지털 기술의 발전으로 인한 네트워크 연결성의 확장으로 시공간의 제약없이 데이터를 삭제 또는 파기할 수 있을 뿐 아니라, 데이터를 보관·관리하는 ISP나 OSP 뿐만 아니라 일반 기업들도 개인정보보호 차원에서 업무정책상 정보보관 기간을 설정해서 정기적으로 데이터를 삭제하기 때문에, 통상적인 압수수색 영장 발부절차가 진행되는 경우에 있어서는 고의적으로 또는 통상적인 업무과정에서 데이터가 변경 또는 삭제될 수 있는 가능성을 배제할 수 없다. 이와 같이 데이터가 손실되거나 변경될 가능성을 최소화함으로써 신속하게 중요한 디지털 증거를 확보하고자 논의되는 것이 데이터 보전명령제도라고 할 수 있다.

현행 「형사소송법」은 제184조와 제185조에 증거보전청구절차를 규정하고 있지만, 이 규정은 디지털 증거와 같이 실시간으로 변화가 가능할 뿐 아니라 시공의 제한없이 원격으로 삭제 및 변경이 용이한 무형의 데이터를 상정한 것이 아니기 때문에 그 절차상 한계가 있다. 즉 해당 규정은 영장청구와 유사하게 법원에 서면으로 그 사유를 소명하도록 규정하고 있기 때문에 디지털 증거를 확보하기 위한 실효적인 조치로서는

한계가 있다고 볼 수 있다. 더욱이 동 규정은 압수, 수색, 검증 등의 방법을 통해 증거를 확보한 후 보전하는 것을 전제로 하기 때문에 영장집행절차가 선행되어야 한다는 점에서 신속히 디지털 데이터의 프리징을 통해 변경, 훼손, 삭제 등의 가능성을 배제해야 하는 상황하에서는 적합하다고 보기 어렵다. 이러한 입법적 한계를 고려하여 제18대 국회에서는「형사소송법」제106조 압수규정에 데이터 보전명령제도를 신설하는 입법안[1111]이 발의된 바 있었으며, 제19대와 제20대 국회에서도「형사소송법」제108조의2에 정보보존요청제도를 신설하는 입법안[1112]이 발의된 바 있었지만, 모두 임기만료로 폐기됨으로써 법률개정이 이루어지지는 않았다.

미국의 경우 이미 1986년에 전자통신프라이버시법(18 U.S.C. §2703)을 통해 "유선 또는 전자통신서비스 또는 원격 컴퓨팅서비스제공자는 정부기관의 요청이 있는 경우, 법원의 명령 또는 기타 다른 절차가 있을 때까지 기록과 다른 증거를 보전하는 데 필요한 조치를 취해야 하며, 보전기간은 90일이며, 정부기관에 의한 재요청이 있는 경우에는 추가로 90일의 기간을 연장할 수 있다"[1113]고 규정하고 있다. 이는 서비스제공자들이 통상 30일 또는 60일 간격으로 관련 기록들을 삭제하는 정책에 대응하기 위해 마련된 것이라 할 수 있다. 이러한 보전명령의 수범자는 유선통신서비스제공자, 전기통신서비스제공자, 원격정보처리서비스제공자이며, 보전대상은 '기록 및 기타 증거'로 규정되어 있지만 실무상 보전대상으로는 특정 계정 및 그와 연계된 계정에 의해 저장된 통신 또는 파일 내용, 이메일 주소 또는 IP 주소 등 해당 통신 또는 파일과 관련된 정보 등이 열거되어 있다.[1114]

1111) "제106조(압수) ② 법원은 제1항에 따른 압수의 목적이 컴퓨터용디스크 그 밖에 이와 비슷한 정보저장매체(이하 이조에서 "정보저장매체 등"이라고 한다)에 기억된 정보를 얻기 위한 것이고 그러한 목적을 달성하기 위하여 긴급히 필요하다고 인정하면 해당정보를 보관관리하고 있는 자에게 관련정보의 보전을 명할 수 있다. 이 경우 보전기간은 최도한도의 범위안에서만 하여야 한다" (의안번호 1804839, 형사소송법 일부개정법률안(이종걸 의원 대표발의), 2009.5.13.).

1112) "제108조의2(정보의 보존요청 등) ① 법원은 정보를 압수할 필요가 있는 경우「정보통신망 이용촉진 및 정보보호등에 관한 법률」제2조 제1항 제3호에 정한 정보통신서비스제공자에게 30일의 범위내에서 당해 정보가 삭제변경되지 않도록 보존할 것을 서면으로 요청할 수 있다. 다만, 상당한 이유가 있다고 인정되는 경우 30일의 범위내에서 1회에 한해 연장할 수 있다. ② 제1항의 경우 당해 정보를 압수할 필요가 없다고 인정되는 때에는 지체없이 보존요청을 취소하여야 한다" (의안번호 1913878, 형사소송법 일부개정법률안(김도읍 의원 대표발의), 2015.2.2.; 의안번호 2001352, 형사소송법 일부개정법률안(김도읍 의원 대표발의), 2016.8.2.).

1113) 18 U.S.C. §2703(f)(1)(2).

1114) U.S. Dept. of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal investigations", "Appendix C. Sample Language for Preservation Request under

한편 디지털 증거의 휘발성 및 훼손의 용이성에 대응하여 디지털 증거를 확보하고자 하는 노력의 일환으로 마련된 사이버범죄 방지협약(Convention on Cybercrime)에 있어서도 보전명령제도가 도입되었고, 동협약에 가입된 국가들 역시 이행입법을 통해 보전명령제도를 도입하고 있음을 볼 수 있다.[1115]

먼저 사이버범죄 방지협약의 경우 제16조 저장된 컴퓨터데이터의 신속한 보전, 제17조 트래픽데이터의 신속한 보전 및 부분 공개 규정을 두고 있다.

제16조 저장된 컴퓨터데이터의 신속한 보전[1116]

1. 각 당사국은 컴퓨터데이터가 특히 손실 또는 변경에 취약하다고 믿을만한 근거가 있는 경우, 자국의 권한있는 기관으로 하여금 컴퓨터 시스템에 저장된 트래픽 데이터를 포함한 특정 컴퓨터데이터의 신속한 보존을 명령하거나 이와 유사한 방법으로 확보하는데 필요한 입법적 조치 및 그 밖의 조치를 취하여야 한다.
2. 당사국이 개인이 소유하거나 관리하는 특정한 저장된 컴퓨터데이터를 보전하도록 명령함으로써 위 제1항을 시행하는 경우, 당사국은 필요한 기간동안 최대 90일까지 컴퓨터데이터의 무결성을 보존하고 유지하여 이를 권한있는 기관에 전달할 수 있도록 필요한 입법 및 기타 조치를 취해야 한다. 가입국은 그 명령이 이후 갱신될 수 있도록 규정할 수 있다.
3. 각 당사국은 컴퓨터데이터를 보전하거나 보관하는 사람에게 국내법에 의해 규정된 기간동안 이러한 절차의 수행을 비밀로 유지하도록 의무화하는데 필요한 입법 및 기타 조치를 취해야 한다.
4. 이 조항에서 말하는 권한과 절차는 제14조 및 제15조에 따른다.

제17조 트래픽데이터의 신속한 보전과 일부 공개[1117]

1. 각 당사국은 제16조에 따라 보전해야 할 트래픽 데이터와 관련하여 다음과 같이 필요한 입법 및 기타 조치를 취해야 한다.
   a. 하나 이상의 서비스제공자가 해당 통신전송에 관여했는지 여부와 상관없이 트래픽데이터의 신속한 보전이 가능하도록 보장하고,
   b. 당사국이 서비스제공자와 통신이 전송된 경로를 식별할 수 있도록 충분한 양의 트래픽데이터를 당사국의 관할 기관이나 이 기관으로부터 지정받은 자에게 신속하게 제출하도록 하는데 필요한 입법 및 기타 조치를 취해야 한다.

---

18 U.S.C. §2703(f)"(www.justice.gov/file/442111/download; 최종접속일 2023.10.10.).

1115) 동 협약에 가입한 당사국은 61개국이며, 협약에 서명했거나 가입에 초대된 국가는 21개국이다(유럽평의회(Council of Europe) 홈페이지, "The Budapest Convention (ETS No. 185) and its Protocols"(https://www.coe.int/en/web/cybercrime/the-budapest-convention; 최종접속일 2023.10.10.)).

1116) Convention on Cybercrime(European Treaty Series-No. 185)(https://rm.coe.int/168008156 1; 최종접속일 2023.10.10.).

1117) Convention on Cybercrime(European Treaty Series-No. 185)(https://rm.coe.int/168008156 1; 최종접속일 2023.10.10.).

다음으로 사이버범죄 방지협약 가입국인 독일의 경우를 보면, 통신감청법 제113a조, 제113b조에 의해 통신서비스제공자에게 통신정보를 6개월간 의무적으로 저장하도록 의무를 부과하는 규정을 두었지만, 해당 규정이 위헌결정을 받음으로써 법을 개정하여 정보의 종류에 따라 10주와 4주로 보존기간을 달리하여 규정하고, 정보내용은 보존대상에 포함하지 않고 있다.[1118] 그리고 형사소송법상 데이터 보전명령에 관한 규정을 별도로 두고 있지 않지만, 일반규정인 동법 제94조[1119]의 증거대상의 보전 규정과 통신데이터에 대한 동법 제100g조를 보전명령과 유사한 조치로 해석하고 있다.[1120]

2001년 동 협약에 가입한 일본은 형사소송법 제197조 제3항부터 제5항까지를 신설하여 통신이력 전자적 기록에 대한 보전요청제도를 신설하였다.

제197조(수사에 필요한 조사)

③ 검찰관, 검찰사무관 또는 사법경찰원은 압수 또는 기록명령부 압수를 하기 위하여 필요한 때에는 전기통신을 하기 위한 설비를 타인의 통신용으로 제공하는 사업을 영위하는 자 또는 자기 업무를 위하여 불특정 또는 다수의 통신을 매개할 수 있는 전기통신을 하기 위한 설비를 설치하고 있는 자에 대하여, 그 업무상 기록하고 있는 전기통신의 송신원, 송신처, 통신일시 그 밖의 통신이력의 전자적 기록 중 필요한 것을 특정하여 30일을 초과하지 아니하는 기간을 정하여 이를 소거하지 아니하도록 서면으로 요구할 수 있다. 이 경우 해당 전자적 기록에 대하여 압수 또는 기록명령부 압수를 할 필요가 없다고 인정된 때에는 해당 요구를 취소하여야 한다.

④ 전항의 규정에 따라 소거하지 아니하도록 요구하는 기간에 대하여는 특히 필요한 때에는 30일을 초과하지 아니하는 범위내에서 연장할 수 있다. 다만, 소거하지 아니하도록 요구하는 기간은 총 60일을 초과할 수 없다.

⑤ 제2항 및 제3항의 규정에 의한 요구를 하는 경우 필요한 때에는 함부로 이에 관한 사항을 누설하지 아니하도록 요구할 수 있다.

한편 동 협약에도 불구하고 EU 집행위원회는 2018년 "형사관련 전자증거에 대한 유럽의 제출명령 및 보전명령에 관한 규정안"을 제안하였다. 이러한 제안의 이유와 목표에 대해서는 다음과 같이 설명하고 있다.

> "디지털 기술에 기반한 소셜미디어, 웹메일, 애플리케이션 등은 전세계 수억 명의 사용자를 서로 연결함으로써 사회경제적 이점을 제공함과 더불어 심각한 범죄를 야기하거나 조장하는

1118) 박병민·서용성, 앞의 연구보고서, 128면.

1119) 독일 형사소송법 제94조(증거대상의 보전) ① 증거방법으로서 심리에 중요할 수 있는 대상은 유치하거나 또는 다른 방법으로 보전해야 한다.

1120) 이용, "디지털 증거 수집에 있어서의 협력의무", 박사학위논문, 서울대학교, 2016.2, 187면.

> 도구로 오용될 가능성도 내포하게 되었다. 따라서 디지털 기반 기술 서비스와 앱은 범죄의 증거를 찾을 수 있는 유일한 장소가 될 수 있기 때문에 자국이나 회원국뿐 아니라 제3국의 서비스제공자가 저장한 데이터에 대한 접근이 요구되며, 이는 디지털 시대에 맞는 국가 간 협력 메커니즘 하에서 현대적인 형태의 범죄에 대응할 수 있는 도구의 제공을 제안하게 되었다. 이 제안은 당국, 서비스제공자 및 피해자들의 법적 확실성을 향상시키고, 법집행 요구에 대한 높은 기준을 유지함으로써 기본권, 투명성, 책임을 보장하는 것을 목표로 한다. 또한 다른 관할권에 설립된 서비스제공자가 저장 및/또는 보유하고 있는 전자증거를 확보하고 획득하는 절차를 신속하게 진행하고자 하는 것이다."[1121]

동 규정안은 데이터의 제거, 삭제 또는 변경을 방지하기 위한 목적으로 보전명령을 규정하고 있고, 수사기관으로 하여금 정보를 열람하게 하거나 데이터 이전을 허용하는 처분이 아니라 보관자가 직접 임시보전조치를 취하도록 하는 것이기 때문에 보전대상이 되는 정보의 유형에 제한을 두고 있지는 않다.[1122]

이와 같이 데이터 보전명령제도는 사이버범죄에 신속하게 대응하기 위한 수단으로서 상당수의 국가들이 도입하여 시행하고 있음을 알 수 있다. 특히 보전명령은 제출명령과 달리 데이터의 점유가 수사기관으로 이전되는 것이 아니라 데이터의 소유자나 소지자, 관리자 본인의 통제하에 있는 것이기 때문에 기존의 강제수사절차에 비하여 기본권에 대한 침해의 우려가 적다고 볼 수 있어서 그 도입에 있어서 법적 쟁점이 크지 않다고 보여진다. 또한 디지털 기술 기반 서비스업체 또는 일반 기업 등을 상대로 직접적인 압수수색을 하는 것보다는 보전명령을 통해 데이터를 확보하는 것이 해당 기업의 통상적인 업무에 대한 침해를 최소화할 수 있는 것일 뿐 아니라 데이터의 무결성을 신속하게 확보할 수 있다고 할 것이다.[1123]

앞서 살펴보았던 주요 국가들의 규정을 살펴보면, 수사절차상 데이터의 삭제, 변경

1121) European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters", Strasbourg, 2018.4.17(https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF; 최종접속일 2023.10.10.).

1122) 노소형, "제3자 보관 디지털증거에 대한 긴급증거보전 제도 신설방안 연구", 박사학위논문, 성균관대학교, 2020.8, 155면.

1123) 물론 이러한 경우 해당 기업이 범죄혐의사실과 무관하고 단순히 관련 데이터를 저장·보관·공유하는 업무를 수행한다는 사실이 전제되어야 데이터의 무결성을 신뢰할 수 있다고 할 것이다.

등을 막기 위한 수단의 필요성에 입각해서 보전명령제도를 도입하되 제출명령 또는 압수절차의 전제로서 허용하고 있음을 볼 수 있다. 또한 데이터 보전 자체는 데이터를 저장·관리·공유하는 디지털 기술 기반 서비스업체 또는 개인에게 부담을 부과하는 처분이기 때문에 일정한 보전기간을 두고 있으며, 보전 대상 데이터에 있어서는 가입자 데이터나 접속데이터와 같이 통신기록 확인자료로 제한하거나 콘텐츠 데이터까지 그 대상으로 하는 제한하는 경우가 있음을 알 수 있다.

나. 법적 성격 및 쟁점

데이터 보전명령제도는 수사절차상 법원의 허가 또는 영장집행절차를 진행하는 과정에서 데이터가 변경, 삭제, 폐기 등이 행해질 우려가 있는 경우, 또는 피의자를 특정하기 어려운 상황에서는 데이터에 대한 접근권한이 누구에게 있는가를 확인하기 어렵기 때문에 수사가 노출되는 경우 원격으로 데이터가 삭제될 우려를 배제하기 위해서도 그 필요성이 인정된다고 볼 수 있다.

하지만 데이터 보전명령이 압수 또는 제출명령 등과 같이 강제처분에 선행하여 이루어지고, 데이터의 점유이전이 발생하지 않기 때문에 기본권 침해가 덜하다고 볼 수 있지만, 보전명령으로 인해 해당 데이터의 이용이 제한될 뿐 아니라 해당 데이터의 보전으로 인한 업무의 제약 및 경제적 부담 등과 같은 영업권 침해의 문제가 발생할 수 있다는 점에서 보면 강제처분의 성격을 갖는다고 보아야 할 것이다. 따라서 형사절차의 기본원칙인 적법절차 원칙을 준수해야 할 뿐만 아니라 보충성의 원칙과 비례의 원칙에 따라 이루어질 수 있도록 데이터의 변경, 삭제의 우려 등과 같이 긴급하게 필요한 경우에 한해서 행해져야 하고, 그 대상과 범위가 필요 최소한도로 제한되어야 할 것이고, 일정한 형태의 사법통제도 수반될 필요가 있다고 할 것이다.

이와 함께 보전명령의 대상을 통신사실 확인자료로 제한할 것인지 아니면 데이터 콘텐츠까지 포함할 것인가 여부, 보전명령의 수범자를 디지털 기술 기반 서비스제공자로 제한할 것인지 아니면 개인에 대해서까지 확대할 것인가, 사법통제를 어느 수준에서 할 것인가, 보전명령의 실효성을 어떠한 방식으로 담보할 것인가 등에 대해서는 법리적 검토와 함께 입법정책적 판단이 요구되는 부분이라 할 것이다.

다. 입법적 고려사항

1) 데이터 보전명령의 전제 요건

데이터 보전명령은 데이터 이전을 전제로 하지는 않지만, 해당 데이터의 자유로운 이용과 공유 등을 차단할 뿐 아니라 이를 관리하는 기업의 업무 일부를 정지시키는 것이기 때문에 기본권의 침해가 없다고는 볼 수 없다. 또한 형사절차의 일환으로 수범자로 하여금 일정 데이터를 프리징하도록 의무를 부담시키는 것이기 때문에 강제처분으로서의 성격도 배제하기 어렵다고 할 것이다. 따라서 형사절차적 수단으로서 데이터 보전명령을 도입하고자 하는 경우 적법절차적 통제방안이 고려되어야만 한다. 즉 기본권의 제약을 전제로 하는 강제처분에 해당하는 한, 필요 최소한으로 제한할 수 있는 법적 규제장치가 필요하고, 강제수사법정주의에 의하여 「형사소송법」상 그 요건과 절차 등이 규정되어 있어야만 하는 것이기 때문이다. 또한 형사절차상 강제처분은 기본권에 대한 제약을 수반하기 때문에 「헌법」의 기본권과 그 제한원리를 전제로 해서만 정당화될 수 있고, 따라서 「형사소송법」 역시 제199조에 강제처분은 법률에 특별한 규정이 있는 경우에 그리고 필요 최소한도의 범위 안에서 해야 한다고 규정되어 있는 것이다.

이와 같이 데이터 보전명령이 기본권 제한을 수반하는 한 법치국가적 통제의 기본원리인 비례성 원칙에 따라 그 목적의 적합성, 필요성, 최소침해의 원칙 등이 준수되어야 한다. 먼저 데이터 보전명령은 범죄사실과 관련성이 있는 데이터의 훼손, 변경, 삭제 등의 우려로 인한 증거인멸의 방지가 그 목적이라 할 수 있다. 디지털 기술이 고도화될수록 데이터의 저장, 이용, 관리가 원격화되고 있기 때문에 시공과 무관하게 원격 삭제가 용이한 상황에서 수사대상이 되는 데이터가 압수수색영장을 집행할 때까지 온전히 존재할 것을 기대하기는 어려운 것이 현실이다. 더욱이 「개인정보보호법」 제21조에 의하여 개인정보처리자는 불필요한 개인정보를 지체없이 파기하도록 규정하고 있고, 기업들 역시 개인정보보호 정책에 따라 정보 보유기간을 최대한 단축하고 있기 때문에 압수 전에 데이터가 삭제되는 것을 차단할 방법이 현재로서는 없다. 또한 체포를 전제하지 않는 긴급 압수수색 규정도 없기 때문에 데이터 보전명령제도는 압수에 앞서서 데이터가 변경되거나 훼손 및 삭제될 개연성이 있는 경우 증거인멸을 방지할 수 있는

실효적인 수단이 될 수 있다는 점에서 목적 적합성이 있다고 할 것이다.

다음으로 데이터 보전명령은 기존의 증거확보 수단, 즉 임의제출, 압수수색 및 검증, 증거보전 등에 의해서는 데이터의 삭제 및 변경으로 인하여 증거확보가 어렵다고 하는 보충성과 필요성이 인정되어야 할 것이다. 즉 신속하게 데이터를 보존하지 않으면 범죄사실의 입증에 있어서 증거가치가 있는 데이터를 확보하기 곤란하다는 필요성이 인정되는 경우에 한해서 허용되어야 하는 것이다.

마지막으로 데이터 보전명령은 범죄혐의사실과 일정한 관련성이 있는 데이터에 한해서 허용되어야 할 것이다. 압수수색에 비해서 기본권 침해의 정도가 낮다고는 하지만 강제처분으로서 성격을 갖고 있는 이상 범죄혐의사실과의 관련성에 대한 입증이 요구된다고 보아야 할 것이다. 만약 관련성 요건이 배제되는 경우 디지털 증거의 특성상 사생활 침해의 우려가 클 수밖에 없고, 수사의 효율성을 우선적으로 추구하는 수사기관의 속성상 보전명령의 남용에 대한 우려 역시 배제하기 어렵다고 할 것이다.

2) 보전명령의 주체와 객체

데이터 보전명령을 수사상 강제처분의 일환으로 보게 되면 명령의 주체는 수사기관이라고 볼 수 있다. 하지만 이에 대하여 사법통제의 필요성과 수사상 압수수색이 법원의 압수수색 규정을 준용하고 있는 현행법의 체계에 비추어 볼 때 법원이 보전명령의 주체가 되어야 한다고도 볼 수 있다. 다만 법원이 보전명령의 주체가 되는 경우 압수수색절차와 마찬가지로 수사상 보전명령이 필요한 경우 영장과 같은 법원의 사전 허가를 전제로 할 수밖에 없고, 현재와 같이 서면기록에 의하게 되면 기관 간 공간적 이동으로 인한 시간의 소요가 필수적이기 때문에 신속하게 데이터를 프리징 상태로 보전해야 하는 수사상 필요와 부합하기 어려운 문제가 야기될 수 있을 것이다.

데이터의 변경 및 삭제의 우려 또는 데이터 보관기간의 만료로 인한 삭제의 우려 등을 최대한 신속하게 배제하고, 증거인멸을 방지하고자 하는 데이터 보전명령의 취지와 그 필요성을 고려할 때, 데이터 보전명령의 주체는 수사기관으로 하는 것이 보다 합리적이라 보여진다. 앞서 살펴본 데이터 보전명령제도를 운영하고 있는 주요 국가들에 있어서도 보전명령의 주체는 수사기관으로 하고 있음을 참고할 필요가 있다고 할 것이다. 다만 수사기관이 직접 데이터 보전명령을 할 수 있도록 하되 이에

대한 일정한 사법통제가 필요하다는 점은 분명하다고 본다. 이에 대해서는 사법심사와 관련한 부분에서 기술하고자 한다.

다음으로 데이터 보전명령의 객체를 어느 범위로 할 것인가와 관련해서 볼 때, 이미 동 제도를 운영하고 있는 국가들에 있어서는 보전명령 수신자를 전자통신서비스 또는 원격 컴퓨팅 서비스제공자, 즉 디지털 기술 기반 서비스제공자[1124]로 하거나 법인은 물론 데이터를 소지 및 통제하고 있는 자연인까지 포함하되 피의자는 제외[1125]하는 방식을 취하고 있음을 볼 수 있다. 피의자를 제외한 제3의 개인이 소지, 보관하고 있는 데이터에 대한 보전의 필요성이 있는 경우가 있을 수 있지만, 이와 같이 개인에 대해서까지 보전명령을 허용하게 되면 기본권 침해의 대상이 과도하게 확대될 뿐 아니라 제도의 취지를 벗어나서 남용될 가능성을 배제하기 어렵다고 볼 수 있다. 특히 피의자의 경우에는 방어권과 충돌할 우려가 있기 때문에 설령 개인을 수범자로 하더라도 피의자는 수범자에서 배제해야 할 것이다. 생각건대 데이터 보전명령의 객체는 디지털 기술 기반 서비스제공자로 제한하는 것이 제도의 목적과 취지에 보다 부합한다고 할 것이다.

3) 보전명령의 대상

데이터 보전명령의 대상과 관련해서는 첫째, 실질적으로 보전되어야 하는 데이터의 유형을 어느 범위까지로 할 것인가의 문제이며, 둘째는 보전명령이 적용되는 범죄의 유형을 어느 범위로 할 것인가의 문제라고 할 수 있다.

먼저 보전명령의 대상이 되는 데이터의 유형과 관련해서 볼 때, 사이버범죄협약의 경우 저장된 컴퓨터데이터로 명시할 뿐 데이터의 종류를 구분하고 있지는 않으며, 미국의 경우에는 모든 기록 또는 기타 증거로 규정하고 있으며, 캐나다의 경우에도 컴퓨터데이터로 명시할 뿐 데이터의 종류에 관한 제한을 두고 있지 않아서 저장된 통신내용도 포함된다고 본다.[1126] 독일 역시 보전대상을 특별하게 제한하고 있지 않지만 일본의 경우에는 송신원, 송신지, 통신일시 및 기타 통신이력의 전자적 기록으로 보전대상을 제한하고 있음을 볼 수 있다. 즉 데이터 보전명령제도를 운영하고 있는

1124) 미국, 일본, 노르웨이.
1125) 캐나다, 독일, 네덜란드, EU.
1126) 노소형, 앞의 박사학위논문, 91면.

상당수의 국가들은 보전대상이 되는 데이터의 종류에 대해 제한을 두고 있지 않음을 알 수 있다. 이는 수사기관이 해당 데이터를 열람하거나 수색하는 처분이 아니고, 단지 데이터 보관자가 임시적으로 보전하는 조치를 취한다는 점에서 데이터 종류에 따른 제한이 필요하지 않다고 보고 있는 것이라 할 것이다.[1127]

실체적 진실의 발견이라는 측면에서 보면 데이터 보전명령의 대상이 되는 데이터의 종류에 제한을 두지 않는 것이 바람직하다고 볼 수 있다. 특히 콘텐츠 데이터의 경우에는 실질적인 정보의 내용이 포함되어 있기 때문에 실체적 진실을 파악하는 데 보다 실효적이라 볼 수 있기 때문이다. 뿐만 아니라 데이터 보전명령 대상을 데이터 내용까지 포함한다고 해서 수사기관이 해당 내용을 열람하거나 탐색할 수 있는 것이 아니고, 차후에 영장을 통해 압수의 범위가 정해지는 것이기 때문에 사생활에 대한 침해가 야기된다고 보기는 어렵다고 할 수 있다. 다만 보전명령으로 인해 데이터가 프리징되기 때문에 통신의 자유가 침해될 우려를 배제하기는 어려우며, 특히 보전대상이 되는 데이터의 종류와 범위에 제한을 두지 않는 경우 과잉금지원칙에 반할 가능성도 있다고 볼 수 있다. 또한 보전명령의 대상에서 데이터 내용을 제외하게 되면, 현행 「통신비밀보호법」 제2조 제11호에 규정된 통신사실확인자료와 별 차이가 없기 때문에 새로운 제도를 도입할 실익이 크지 않다[1128]는 비판도 존재한다.

데이터 보전명령으로 인해 데이터가 수사기관으로 점유가 이전되는 것은 아니지만, 모든 범죄에 대해서 데이터 보전명령의 대상이 되는 데이터에 제한을 두지 않는 것에 대해서는 개인정보보호에 대한 우리 국민들의 민감성, 그리고 정보화 사회에 있어서 무엇보다도 중요하게 인식되는 정보에 대한 자기결정권의 침해 여부 등을 고려하지 않을 수 없다고 본다. 따라서 보전명령의 대상이 되는 데이터의 유형은 보전명령이 적용되는 범죄의 유형과 연계하여 고려해 볼 필요가 있다고 할 것이다. 즉 입법정책적으로 보전명령이 요구되는 일정한 유형의 중대범죄에 한해서는 데이터 기록뿐 아니라 데이터 내용까지 보전명령의 대상이 된다고 보는 반면, 그 이외의 범죄에 대해서는 일본과 같이 가입자 데이터, 접속데이터, 메타데이터 등으로 보전명령의 대상을 제한하는 것이 보다 국민의 법감정에 부합하는 것이 아닐까 한다. 다만 앞서 기술한 바와

1127) 노소형, 위의 박사학위논문, 155면.
1128) 박병민·서용성, 앞의 연구보고서, 314면.

같이 「통신비밀보호법」상 긴급통신제한조치와의 차별성이 없다는 비판과 관련해서 보면, 데이터의 변경 및 삭제 등의 우려로 인한 증거인멸의 방지라고 하는 목적에 있어서 차이가 있을 뿐 아니라 통신제한조치의 경우 장래의 통신을 그 대상으로 하는 반면, 데이터 보전명령은 저장된 데이터를 그 대상으로 하고 장래의 데이터에 대해서는 적용되지 않는다는 점에서 명확한 차이가 있다고 보아야 할 것이다.

4) 데이터 보전명령의 기간 제한

데이터 보전명령은 수사절차상 압수수색 또는 검증이 예상되는 데이터의 변경 또는 삭제를 막기 위한 임시적 보전조치라고 할 수 있기 때문에 그 기간에 대한 제한이 있어야 한다. 즉 기간에 대한 제한 없이 수사절차상 데이터를 보전할 수 있다고 한다면 데이터 소유자의 통신의 자유 및 정보의 자기결정권에 대한 심각한 침해를 야기할 뿐 아니라, 보전명령 수범자인 디지털 기술 기반 서비스업체의 영업권에 대한 중대한 피해를 야기할 수 있다는 점에서 볼 때, 기간의 제한 없는 보전명령은 목적에 부합하지 않는 과도한 수단으로서 비례의 원칙에 반하는 것이라 할 것이다.

따라서 보전명령제도를 두고 있는 국가들에 있어서도 데이터 보전기간을 두고 있는 바, 사이버범죄협약의 경우 최대 90일, 미국의 경우에는 90일(1회에 한해서 연장 가능, 총 180일), 캐나다의 경우에는 21일(외국법에 저촉되는 경우 90일), 일본의 경우에는 30일(30일 범위 내에서 연장 가능, 최대 60일), 네덜란드의 경우에는 90일(1회에 한해서 연장 가능, 총 180일), 노르웨이의 경우에는 최대 90일, EU의 경우에는 60일로 규정하고 있다.[1129] 이에 비추어 볼 때, 데이터 보전명령제도를 도입함에 있어서도 일정한 기간 제한을 두어야 할 것이고, 압수수색 및 검증과 같은 강제수사의 전제로서 행해지는 점을 감안해 볼 때, 30일 이내로 그 기간을 제한하는 것이 합리적이지 않을까 한다.

5) 사법적 통제

데이터 보전명령에 대한 사법적 통제의 필요성은 보전명령의무를 수반하는 강제처분으로 규정할 것인가 아니면 단순한 협조요청으로 규정할 것인가에 대해서 달리 판단될 수 있을 것이다. 하지만 데이터 보전명령의 필요성과 취지에 비추어 볼 때,

---

1129) 노소형, 앞의 박사학위논문, 62-177면 참조.

일정한 협조의무를 수반하는 보전명령으로 규정되어야 그 실효성을 담보할 수 있다고 본다. 따라서 보전명령의 수범자에 대한 강제처분의 형식으로 이루어지는 한 일정한 형태의 사법적 통제의 필요성은 불가피하다고 보아야 할 것이다.

다만 보전명령은 데이터의 삭제, 변경 등 긴급한 우려로 인해 증거를 보전해야 할 필요성이 있는 경우에 한해서 허용되고, 수사기관에 의해 해당 정보가 열람되거나 수색되는 것이 아니므로 직접적인 기본권 침해가 발생한다고 보기는 어려우며, 보존명령 대상 정보에 대한 압수수색 또는 제출명령이 이루어지는 경우에는 사법심사가 이루어질 수밖에 없다는 점에서 보면, 보전명령에 대한 사법통제는 영장집행절차와 같은 엄격한 사전통제 방식에 의하기보다는 법원에 대한 사후보고 형식으로 이루어지는 것이 합리적이라 할 것이다. 수사기관에 의한 강제처분에 대해서는 사법통제가 수반되는 것이 일반적이지만, 데이터 보전명령과 같이 신속성이 무엇보다 우선할 수밖에 없는 강제처분에 있어서 법원에 의한 사전통제장치는 신속성과 양립하기 어려운 속성을 갖고 있다는 점을 고려할 필요가 있다.[1130]

보전명령제도를 두고 있는 국가들의 예를 보더라도, 미국, 독일, 일본, 네덜란드, 노르웨이의 경우에는 사법심사를 거치지 않으며, 캐나다의 경우 수사기관에 의한 보전요청에 대해서는 사법심사가 없지만 치안공무원의 신청에 의해 법원이 발하는 보전명령에 대해서는 사법심사가 규정되어 있음을 볼 수 있다.[1131]

6) 데이터 보전명령의 실효성 담보

다음으로 데이터 보전명령에 대한 실효성을 어떻게 입법적으로 담보할 것인가에 대해서도 검토되어야 할 부분이라 할 것이다. 먼저 보전명령의 유형을 명령과 같은 강제적인 처분형식을 취할 것인가 아니면 요청과 같은 자발적 처분형식을 취할 것인가에 따라서 달리 검토되어야 할 것이다. 먼저 보전명령에 대하여 강제성을 결합시키는 경우 그 위반에 대한 제재를 부과하는 방식을 취하게 되는데, 민사적 제재를 부과하는 방식, 약식벌금을 부과하는 방식, 자유형을 부과하는 방식 – 이 경우는 법원이 보전명령을 부과하는 경우에 한한다 – 등이 존재하고 있음을 볼 수 있다. 한편 보전요

1130) 노소형, 앞의 박사학위논문, 193면.
1131) 노소형, 위의 박사학위논문, 62-177면 참조.

청방식을 취하는 경우에는 수범자에 대한 협조의무가 함께 규정되어 있지만, 그에 대한 제재규정은 존재하지 않는 경우가 대부분이라 할 수 있다. 즉 보전명령의 수범자인 디지털 기술 기반 서비스 기업들의 경우 범죄와 무관함에도 불구하고 국가의 필요에 의해 일정한 의무를 부담시킬 뿐 아니라 경우에 따라서는 그들의 영업권에 대한 침해를 수반하는 것이기 때문에 형사적 제재를 부과하는 것은 현실적으로 불가능하다고 볼 수 있다. 따라서 보전명령의 실효성 담보를 위해서는 미국과 같은 민사적 제재 또는 행정적 제재를 부과하는 방식을 검토해야 할 것으로 생각된다. 다른 한편으로 미국의 경우 보전명령의 수범대상인 서비스업체에 대해서 보전명령으로 인해 발생하는 손해에 대한 비용을 상환하는 방식[1132]을 규정하고 있으며, 일부 주에서는 보전명령 수범자인 서비스업체에 대한 면책규정을 둠으로써 보전명령으로 인해 발생할 수 있는 모든 민형사상 책임을 지지 않도록 규정하고 있다.[1133] 이와 같이 데이터 보전명령으로 인한 수범자의 손실을 국가가 보상하고, 그로 인한 민형사상 책임을 면책시키는 방식도 보전명령의 현실적인 가능성을 담보할 수 있는 하나의 방법이라 할 수 있을 것이다.

이와 함께 데이터 보전명령의 실효성을 담보하기 위해 요구되는 것이 비밀유지의무라고 할 수 있다. 즉 보전명령 자체가 원격에 의한 데이터 삭제 및 변경 등과 같은 증거인멸에 대응하기 위한 수단이라는 점을 감안해 볼 때, 해당 데이터의 소유자나 피의자 등에게 수사와 관련하여 보전조치가 취해진다는 사실이 사전에 알려지는 경우 데이터의 변경이나 삭제 등의 위험을 피하기 어렵다고 할 수 있다. 따라서 보전명령제도를 두고 있는 대부분의 국가들에 있어서는 보전명령과 함께 비밀유지의무를 함께 규정하고 있음을 볼 수 있다. 즉 보전명령의 수범자로 하여금 증거보전과 관련한 내용을 데이터의 소유자 또는 피의자에게 알리지 못하도록 의무를 부여하여 신속하게 데이터를 프리징함으로써 증거인멸 가능성을 배제할 수 있기 때문이다. 따라서 「통신비밀보호법」에 따른 통지 등이 필요한 경우라 할지라도 데이터 보전명령을 통해 관련 증거가 명확하게 확보된 이후에 가능하다고 보아야 할 것이다.

1132) 18 U.S.C. §2706(a)-(c).
1133) Fl Title 47 Criminal Procedure and Corrections §934.23(8).

2. 전자영장제도

가. 필요성

현행 사법체계 가운데 민사, 특허, 가사, 행정 등 대부분의 분야에서 전자소송이 도입되어 운영되고 있다. 행정소송의 경우 99.9%, 민사소송은 77.2%가 전자소송으로 진행될 정도로 정착되어 있다.[1134] 이에 반해 형사소송절차는 여전히 일부 전자약식 사건을 제외한 대부분의 사건들에 있어서는 여전히 서면에 의존하고 있는 현실이다.

하지만 형사절차에 있어서 서면으로 작성되는 기록 자체도 수기가 아닌 디지털기기로 작성된 전자적 기록임에도 불구하고 이를 다시 종이로 출력하여 제출하는 방식을 취함으로써, 사건의 송치 및 이송, 영장신청 및 청구, 상급심 송부 등 물리적으로 기관 간 또는 지역 간 이동과 시간이 요구되고, 이는 신속한 업무처리를 저해하는 요인이 될 수밖에 없다. 더욱이 이미 2010년에 「형사사법절차 전자화 촉진법」에 의해 각 형사사법업무 처리기관인 법무부, 검찰, 경찰, 법원은 각 기관의 형사사법정보시스템(KICS)을 구축했음에도 불구하고 시스템 통합범위에 대한 이견으로 인해 기관별로 각각 시스템을 구축하여 각 기관이 정보를 별도로 관리하고, KICS는 정보의 흐름만을 관리하는 역할에 그치고 있다. 이와 같이 형사사법 전분야에 걸친 디지털 인프라를 이미 갖추고 있음에도 불구하고 시스템 통합의 미비로 인하여 여전히 형사절차는 아날로그 방식에 의존하고 있는 것이 현실이다.

이와 같이 형사사법절차 전자화가 답보상태에 있는 관계로 형사절차의 시작이라 할 수 있는 영장발부 역시 서면기록에 의존함으로 인해, 특히 디지털 증거와 같이 신속한 증거확보가 요구되는 상황에 대응하기 어려운 문제 등이 발생하고 있다. 즉 디지털 증거의 경우 정보를 탐색하는 과정에서 새로운 범죄혐의 등이 발견된 경우, 현재 대법원의 판단기준에 따르면, 새로운 증거의 발견 시 수색을 멈추고 다시 영장을 발부하도록 요구하고 있는바, 새로운 영장이 발부되는 기간 동안 기존 영장에 따른 수색이 중단될 뿐 아니라 경우에 따라서는 디지털 증거가 원격으로 삭제될 가능성도 배제하기 어렵다고 할 것이다. 뿐만 아니라 현행과 같은 서면에 의한 영장집행절차에

1134) 김승일, "전자서명 기반 전자영장을 활용한 압수·수색영장의 원격 집행 방안에 대한 연구 -금융계좌추적용 압수·수색영장 집행을 중심으로-", 석사학위논문, 서울대학교, 2022.2, 85면.

의하는 경우 디지털 증거와 같이 증거확보에 있어서 지체의 위험이 있는 경우 긴급상황으로 판단하여 영장주의 예외를 적용함으로써 오히려 수사기관으로 하여금 영장을 회피하고자 하는 동기를 강화시키는 역효과를 낳는다고도 볼 수 있다. 실제로 현행범 체포 시 임의제출물 압수를 통해 정보저장매체를 확보하는 경우가 빈번한데, 이는 수사실무상 48시간 내에 수사서류를 작성하는 것도 빠듯하여 사후 압수영장까지 청구할 시간적 여유가 없다고 하는 실무상의 어려움이 있다고 얘기되고 있다.

따라서 전자영장에 의하여 신속한 영장집행이 가능하게 된다면, 영장집행절차의 신속성이 확보됨은 물론이고, 수사기관이 긴급성을 근거로 한 사전영장주의 예외를 인정할 여지가 줄어들게 되고, 결과적으로 사전영장에 기한 강제수사가 보편화됨으로써 오히려 영장주의를 두텁게 보호하는 효과를 기대할 수 있다고 할 것이다.[1135] 또한 수사기관이 현장에서 확보하는 증거들이 디지털 방식으로 존재하는 경우 실시간으로 영장담당판사에게 전달함으로써 보다 정확하게 영장발부 여부를 판단할 수 있도록 할 수 있다.[1136]

전자영장제도를 이미 시행하고 있는 미국의 경우를 보면, 2011년 연방형사소송규칙의 개정으로 Rule 4.1에 '전화 또는 기타 신뢰할 수 있는 전자적 수단을 통한 영장, 소환장, 고발장'이라는 표제하에 "(6) 영장이나 소환장을 발부하려는 판사는 원본문서에 서명하고, 영장이나 소환장에 발행날짜와 시간을 기재하고, 신뢰할 수 있는 전자적 수단으로 영장이나 소환장을 신청자에게 전송하거나 신청자에게 원본의 복본에 판사의 이름에 서명하고 날짜와 시간을 기재하도록 지시하여야 한다"[1137]고 규정하고 있으며, 이에 따라 Rule 41의 압수수색 규정에 있어서도 "Rule4.1에 따라 치안판사는 전화 또는 믿을만한 전자적 수단에 의해 전달된 정보에 기초하여 영장을 발부할 수 있다"[1138]고 규정하고 있다. 이러한 연방형사소송규칙을 반영하여 현재 미국 내 최소 45개 주에서 법률, 규칙, 명령의 형식으로 전자영장발부를 허용하고 있다.[1139] 하지만 미국의 경우에는 전자영장과 일반영장을 병행하는 방식을 취하고 있기 때문에 완전한

1135) 김시원, "전자영장에 관한 연구 -집행절차를 중심으로-", 『사법』 통권 제54호, 사법발전재단, 2020.12, 371면.
1136) 이상원, 앞의 연구용역보고서, 95면.
1137) Federal Rules of Criminal Procedure Rules 4.1(6).
1138) Federal Rules of Criminal Procedure Rules 41(d)(3).
1139) 김시원, 앞의 논문, 361면.

의미의 전자영장제도가 도입되었다고 보기는 어렵지만, 미네소타, 유타, 델라웨어, 애리조나, 텍사스, 켄터키, 하와이, 아이오와의 경우에는 전자영장제도가 도입되어 시행되고 있다.[1140] 미국 외에도 싱가포르,[1141] 필리핀[1142] 등에서 전자영장제도를 시행하고 있는 것으로 알려져 있다.

나. 도입 현황

법무부는 2020년 8월 형사사법절차 전자화를 위해 "형사사법절차에서의 전자문서 이용 등에 관한 법률" 제정안을 입법예고하였으며, 2021년 1월 26일 국무회의를 통과하였고, 동년 9월 28일 국회 본회의를 통과하여 2021년 10월 19일 법률로 제정되었다. 하지만 형사절차에서 전자문서의 작성·유통을 지원하고, 최신 IT 기술을 적용하는 차세대 KICS 구축사업이 진행 중에 있는 관계로 시행은 2024년 10월 20일로 되어 있다. 동법률의 주요내용을 보면, 전자문서에 기존 종이문서와 동일한 효력을 부여하고 있으며(동법 제5조), 종이문서에 서명날인 하는 것을 대신하여 전자문서 등에 전자서명하도록 규정하고, 전자서명에, 서명, 서명날인, 기명날인과 동일한 효력을 부여하고 있다(동법 제8조). 그리고 형사사법기관에 대해서 전자문서 작성을 의무화하고(동법 제10조), 형사사법기관 간에 전자문서 등을 전자적으로 전송하는 방법으로 전자문서를 유통하도록 하고 있으며(동법 제13조), 전자적 방법으로 사건기록을 열람 및 출력하는 것이 가능하며(동법 제16조), 영장은 전자문서 등의 형태로 제시, 전송함을 원칙으로 하며(동법 제17조), 전자문서 등은 모니터, 스크린 등을 이용해 열람하는 등으로 증거조사가 가능하도록 규정하고 있다(동법 제18조).

동법률에 의하여 영장발부, 압수수색영장, 영장에 의한 체포, 구속, 압수·수색·검증에 따른 집행 시 전자문서 등의 형태로 제시 및 전송이 가능해짐으로써 영장집행의 전과정, 즉 신청, 청구, 발부, 집행 등 모든 단계가 전자적 방식으로 처리되는 전자영장제도가 가능해졌다고 볼 수 있다. 다만 앞서 기술한 바와 같이 현재 형사사법정보는

1140) 김시원, 위의 논문, 362-370면 참조.

1141) 정성민, 『형사 전자소송의 바람직한 발전방향』, 연구총서 2020-05, 사법정책연구원, 2020.4, 223면.

1142) CNN Philippines Staff, "Enhanced e-warrant system launched for faster issuance of arrest warrants", CNN NEWS, 2020.9.8(https://www.cnnphilippines.com/news/2020/9/8/pnp-supreme-court-enhanced-ewarrant-system.html; 최종접속일 2023.10.19.).

형사사법정보시스템에서 공유되거나 유통되고 있지 않지만, 각 형사사법기관 간 정보의 이동과 흐름을 제어하는 시스템을 구성하는 경우, 형사사법정보의 전자적 전송과 이동을 관리하는 역할을 수행할 수 있다고 할 것이다.[1143]

한편 법원은 "형사사법 절차에서의 전자문서 이용 등에 관한 규칙" 제정안을 마련하여 현재 내부적인 의견조회 절차를 거치고 있는 것으로 보고되고 있다.[1144] 동 제정안에는 "전자문서로 발부된 영장은 모바일 기기 등을 통한 전자적 제시 방식으로 집행하되, 당해 영장 등이 전자적 형태로 송신 또는 수신될 수 있는 정보를 대상으로 하는 경우에는 전자문서로 된 영장 등을 전송하는 방식으로도 집행할 수 있도록 하는 규정"이 마련되어 있다.[1145] 이 외에도 "전자문서를 제출하는 자는 해당 문서에 개인정보 보호조치 또는 기록열람 제한이 필요한 내용이 포함되어 있는 경우, 이에 관한 의견을 제출할 수 있도록 하는 규정"도 마련되어 있다.[1146]

이와 같이 이미 전자영장제도를 시행할 수 있는 입법적 뒷받침은 마련되어 있기 때문에 이를 실무적으로 구현할 수 있는 기술적 뒷받침과 기관 간 시스템 통합이 이루어지게 되면 형사절차상 전자영장이 활용될 수 있을 것이다.

다. 법적 쟁점

1) 영장의 원본성 문제

현행「형사소송법」제118조는 "압수수색 영장은 처분을 받는 자에게 반드시 제시하여야 하고, 처분을 받는 자가 피고인인 경우에는 그 사본을 교부하여야 한다"고 규정함으로써 영장제시 원칙을 선언하고 있다. 동 규정의 제정 당시에는 사본을 염두에 둘 여지가 전혀 없었기 때문에 영장은 당연히 원본을 전제한 것이었다. 하지만 팩스, 복사기, 인터넷 등을 이용한 기계적 또는 전자적 전송이 가능해지면서 영장의 사본제시가 문제가 되자 영장제시 원칙은 영장원본제시 원칙으로 이해되기 시작하였다. 특

1143) 김승일, 앞의 석사학위논문, 112면.
1144) 박수연 기자, "(단독) 휴대폰으로 영장 제시하는 시대 오나… 대법원, 전자영장 시대 준비", 『법률신문』 2023년 6월 28일자 기사(https://www.lawtimes.co.kr/news/188714; 최종접속일 2023. 10.11.).
1145) 박수연 기자, 위의 기사.
1146) 박수연 기자, 위의 기사.

히 정보통신기술의 발달로 금융기관이나 ISP나 OSP 등을 통한 데이터나 이메일 압수수색의 경우 영장사본제시가 관행적으로 이루어지게 되었다.

하지만 대법원은 영장원본제시 원칙을 선언하면서 이러한 영장사본제시의 관행에 제동을 걸었다. 즉 "수사기관은 압수수색영장을 집행할 당시 팩스로 영장사본을 송신한 사실은 있으나 영장원본을 제시하지 않았고, … 위와 같은 방법으로 압수된 각 이메일은 헌법과 형사소송법 제118조가 정한 절차를 위반하여 수집한 위법수집증거로 원칙적으로 유죄의 증거로 삼을 수 없고, 이러한 절차위반은 헌법과 형사소송법이 보장하는 적법절차원칙의 실질적 내용을 침해하는 경우에 해당하고"[1147]라고 판시하였다. 영장제시 원칙은 「헌법」적 요청일 뿐 아니라 영장집행 절차를 규율하는 「형사소송규칙」에 의해서도 원본을 송부하도록 규정하고 있다는 점에 비추어 볼 때, 대법원의 영장원본제시 원칙의 선언은 당연하다고 볼 수 있다.[1148] 그럼에도 불구하고 디지털 증거 압수수색과 관련해서는 ISP나 OSP를 통한 제3자 압수가 보편화되었고, 수사기관의 직접 압수보다는 영장에 제시된 데이터를 회사가 직접 선별해서 수사기관에 송부하는 방식을 취하기 때문에, 수사기관에서 해당 회사에 직접 영장을 들고 찾아가기보다는 팩스나 이메일을 통해 영장사본을 송부하는 방식이 회사의 입장에서도 업무에 도움이 되었다고 볼 수 있다. 하지만 대법원이 영장원본제시 원칙을 고수함에 따라 팩스나 이메일을 통한 영장사본송부 방식에 제동이 걸리게 된 것이다. 이와 같이 대법원이 영장원본제시 원칙을 준수하도록 요구하는 것은 영장의 이중집행의 위험성을 고려한 것이라고 볼 수 있다.

이와 같이 기존의 서면영장에 대해서도 원본성에 대한 우려가 제기되었는바, 전자영장의 경우에는 기술적으로 원본과 사본의 구분이 무의미할 뿐 아니라 무한복제가 가능한 상황에서 영장의 원본성을 어떻게 판단할 것인가가 문제될 수 있다. 전자영장의 원본성과 관련하여서는 여전히 단일 원본을 유지해야 한다는 견해와 복수 원본을 인정해야 한다는 견해로 나뉘고 있다. 즉 단일원본설은 영장의 이중집행을 막기 위해서는 전자영장의 경우에도 원본은 하나만 존재해야 한다는 견해이다. 단일원본설에 있어서도 법원시스템에 제출된 전자영장만 원본이라고 보는 견해와 검찰시스템에

1147) 대법원 2017.9.7. 선고 2015도10648 판결.
1148) 김시원, 앞의 논문, 373면.

존재하는 전자영장이 원본이라고 보는 견해로 나뉜다.[1149] 한편 복수원본설은 수사기관의 시스템에서 작성된 전자영장이 법원시스템으로 전송되고, 다시 법원의 전자서명을 거친 전자영장이 법원시스템에서 수사기관시스템으로 전송되기 때문에 기술적 동일성이 확보된다면 모두 원본이라고 볼 수 있다는 것이다.[1150]

영장원본제시 원칙의 취지라고 할 수 있는 영장의 이중집행의 위험성을 고려해 볼 때 전자영장의 경우에도 단일원본설이 타당해 보이지만, 전자영장의 단일성 유지를 위해서는 영장이 저장된 매체 하나만 유지해야 하고, 그 매체로부터 하나의 전자기기에서만 전자영장을 현출해야 한다는 것이 된다.[1151] 이는 형식만 전자영장일 뿐 사실상 서면영장과 차이가 없는 것으로, 전자영장제도의 근본적인 취지에 반하는 것이라 할 수 있다.

전자영장 집행절차를 생각해 볼 때 법원시스템을 통해 영장담당판사가 전자서명을 한 영장이 형사사법통합시스템을 통해 검찰과 경찰시스템에 전송 및 저장되고, 다시 영장집행 담당자의 전자기기 화면에 전송되어 피압수자가 해당 전자영장파일을 열람하는 방식으로 이루어진다고 볼 수 있다. 즉 신뢰성이 확보된 동일한 시스템을 통해 작성되고, 전송되고, 저장되고, 열람되는 이상 해당 영장파일이 어느 단계에 있더라도 동일하다고 볼 수 있으므로 단계별 원본성 여부를 의심할 여지는 없다고 보아야 할 것이다. 따라서 법관의 전자서명이 포함된 전자적으로 전송된 영장의 제시는 영장제시 원칙에 부합하는 적법한 절차라고 보아야 할 것이다.[1152]

다만, 법원시스템에 저장된 영장파일과 수사기관 시스템에 저장된 영장파일의 내용이 서로 다른 경우 어느 단계에서 변경이 발생했는가와 관련된 문제는 원본성의 문제가 아니라 진정성의 문제로 검토되어야 할 것이다.[1153]

1149) 이상원, 앞의 연구용역보고서, 100-101면.
1150) 이상원, 위의 연구용역보고서, 101면.
1151) 정성민, 앞의 연구보고서, 328면.
1152) 미네소타주는 2016년 형사소송규칙 Rule. 37.02를 개정하여 전자영장의 효력에 관한 규정을 두면서, 주석(comment)에 "영장요청방법, 문서전송방법, 서명적용방법이 다양해지면서 많은 상황에서 전통적으로 원본영장으로 간주되었던 영장은 더 이상 존재하지 않는다. 영장을 취득한 방법에 관계없이 승인된 절차중 하나에 따라 영장을 요청하고 서명했다면 그 영장은 유효하고 집행이 가능하다"고 설명하고 있음을 볼 수 있다(MINNESOTA COURT RULES, "CRIMINAL PROCEDURE"(https://www.revisor.mn.gov/court_rules/cr/id/37/#37.01; 최종접속일 2023. 10.18.)).
1153) 이상원, 앞의 연구용역보고서, 102면.

2) 영장의 중복집행의 제한과 피의자에 대한 사본교부

압수수색영장은 수사기관이 영장을 제시하고 집행에 착수하여 압수수색을 실시하고 그 집행을 종료했다면 영장의 유효기간 내라고 할지라도 동일 장소, 동일 목적물에 대해 재압수수색을 할 수 없다는 것이 영장의 중복집행의 제한이다. 서면영장에 의하는 경우 집행의 종료에 대한 판단을 피압수자가 할 수 없기 때문에 사실상 수사기관의 판단 여하에 따라 영장 유효기간 내라면 재압수도 가능하다고 볼 수 있다. 이러한 문제는 전자영장의 경우에도 동일하게 발생할 수 있는바, 전자영장의 경우 수사기관이 일단 영장집행을 종료한 경우 전자영장시스템에 완료 기록을 입력하게 함으로써 영장의 유효기간 내라고 하더라도 전자영장이 유효성을 상실할 수 있도록 통제하는 방식을 고려해 볼 수 있다고 할 것이다.

그리고「형사소송법」제118조에 의하여 피압수자가 피고인인 경우에는 그 사본을 교부해야 한다고 규정하고 있다. 전자영장의 경우 앞서 기술한 바와 같이 원본과 사본의 구분이 무의미하기 때문에 사본교부를 어떻게 해석할 것인가가 문제될 수 있다. 생각건대 전자영장의 경우 형사사법통합시스템 내에서만 존재할 때 그 신뢰성과 무결성을 담보할 수 있다고 보아야 하기 때문에 이를 피압수자인 피고인에게 전자적 형태로 전달하는 방식은 적절하지 않다고 할 것이다. 대신에 전자영장을 정확성과 신뢰성을 담보할 수 있는 전자적 장치를 통해 출력할 수 있다면 그 내용과 형태가 전자문서와 동일하기 때문에 출력물을 교부하는 것으로 사본교부를 대신할 수 있다고 볼 수 있을 것이다.

3) 전자영장제시의 방식

전자영장을 제시하는 방식으로는 대면 제시방식과 비대면 제시방식이 가능한데, 대면 제시방식의 경우 압수수색 현장에서 스마트폰 또는 태블릿 등의 전자기기로 전송된 영장파일을 피압수자에게 직접 제시하는 것으로 기존의 서면영장 제시방식과 큰 차이가 없다고 할 수 있다. 한편 비대면 제시방식의 경우 OSP나 ISP 등과 같은 디지털 기술 기반 서비스 사업자나 금융기관, 병원, 기타 공공기관 등과 같이 제3자에 대하여 압수수색영장을 집행하는 경우에 적합한 방식이라 할 수 있다. 그동안「형사소송법」상 영장원본제시 원칙으로 인해 팩스나 이메일을 통한 비대면 영장제시 자체가

적법절차 위반으로 간주되어 왔지만, 전자영장이 도입됨으로써 비대면 영장제시방식도 적법절차로서 허용가능하게 되었다. 다만 기존의 팩스나 이메일 송부 방식은 서면영장을 기계적으로 복사하여 디지털화한 것이기 때문에 조작이나 변경이 용이하지 않은 반면, 전자영장은 수사기관에 의한 작성부터 판사의 전자서명을 거쳐 발부되기까지 정보통신시스템을 통해 전송되어 전자기기 화면으로 출력되는 이상 전자영장의 무결성 담보를 위하여 보안문제에 대한 우려를 배제하기는 어렵다고 할 것이다. 또한 피압수자의 입장에서 수사기관에 의해 전자적으로 제시된 영장의 진정성 또는 무결성을 확인하고자 하는 필요성도 고려해 볼 수 있다. 따라서 형사사법포털시스템에 영장조회가 가능한 항목을 만들어 피압수자로 하여금 시스템에 접속하여 자신에게 발부된 영장을 직접 확인할 수 있도록 하는 비대면 영장제시방식을 생각해볼 필요가 있다고 할 것이다.[1154]

라. 입법적 고려사항

1) 전자영장제시 근거규정 마련

「형사사법절차에서의 전자문서 이용 등에 관한 법률」 제17조에 의하여 압수수색영장을 전자적으로 제시하거나 전송하는 방식으로 영장집행을 할 수 있는 근거가 마련되었다. 하지만 「형사소송법」 제118조에 전자영장의 제시에 관한 근거규정을 마련할 필요가 있다고 할 것이다. 즉 서면영장과 전자영장을 병행하는 방식을 취하는 경우에는 현행법과 같이 제1항을 그대로 두고 제2항에 영장의 전자적 제시에 관한 근거규정을 두어야 할 것이지만, 만약 전자영장으로만 운영하게 된다면 원칙적으로 영장을 전자적으로 제시하도록 하는 규정을 두어야 할 것이다.

2) 영장제시 원칙의 예외규정의 개정

「형사소송법」 제118조는 단서규정으로 "처분을 받는 자가 현장에 없는 등 영장의 제시나 그 사본의 교부가 현실적으로 불가능한 경우 또는 처분을 받는 자가 영장의 제시나 사본의 교부를 거부한 때에는 예외로 한다"고 규정하고 있다. 하지만 영장을

1154) 이순옥, "인터넷서비스제공자가 보관한 정보에 대한 압수·수색 절차", 『법학논문집』 제43집 제3호, 중앙대학교 법학연구원, 2019.12, 182면 참조.

전자적으로 제시하는 방식에 의하는 경우 비대면 제시방식이 가능하기 때문에, 피처분자로 하여금 전자영장을 확인할 수 있는 방식 – 예를 들어 형사사법포털시스템에 접속하는 방식 등 – 을 사전에 고지 내지 통지한다면 피처분자는 영장집행 전에 본인이 원하는 시간과 장소에서 언제든지 영장을 확인할 수 있다고 할 것이다. 즉 영장을 전자적으로 제시하는 경우에는 영장의 제시가 물리적 또는 현실적으로 불가능한 경우를 상정하는 것이 어렵다고 볼 수 있으므로 현행법과 같은 단서규정은 전자영장에 부합하는 방식으로 개정될 필요가 있다고 할 것이다.

3. 원격지 압수수색

가. 필요성 및 논의 현황

정보통신기술의 발달과 초국경적 네트워크 기반이 구축됨으로 인해 클라우드 컴퓨팅 서비스가 보편화되면서 이용자의 컴퓨터나 스마트폰과 같은 디지털기기 자체에 데이터를 저장하지 않고, 원격지에 있는 서버나 저장장치에 데이터를 저장하는 방식이 일상화 되어가고 있다. 즉 디지털 데이터는 네트워크를 통해 생성, 이용, 저장, 관리되기 때문에 데이터를 생성, 입력, 처리하는 장치와 정보가 저장, 관리되는 장치가 장소적으로 분리될 수 있어서, 사실상 디지털기기는 단지 데이터에 접근하기 위한 수단 내지 통로로서의 기능을 갖는다고도 볼 수 있다. 따라서 압수수색영장에 특정되어 있는 피의자가 소유 또는 소지한 디지털기기를 확보해도 그 기기 내에는 압수수색할 수 있는 데이터가 존재하지 않기 때문에, 물리적 장소를 대상으로 하는 기존의 압수수색으로는 이러한 상황에 대응하기 어렵다고 할 수 있다. 뿐만 아니라 정보기술 시스템에 있어서는 물리적 장소의 분리와 무관하게 다른 장소에 위치한 시스템에의 접속이 논리적으로는 최초 현장에 있는 시스템에의 접속과 분리되지 않는다[1155]는 점을 고려하면, 디지털 데이터 자체에 대해서 물리적 장소의 개념을 적용하는 것은 현실과의 괴리를 심화시킬 뿐이라 할 수 있다.

이와 같이 클라우드서비스 또는 해외 이메일 서비스 등을 이용하는 사람에 대한

1155) 정대용, “사이버공간에서의 증거 수집과 기본권 보장에 관한 연구”, 박사학위논문, 고려대학교, 2018.2, 101면.

압수수색에 있어서 영장에 기재된 장소에 존재하는 정보저장매체에 접속하여 디지털 증거를 확보하기 위한 수단으로써 이용되는 것이 원격지 압수수색이라 할 수 있다.

현재 수사실무상으로 최초 압수수색 현장에서 컴퓨터 또는 스마트폰을 통해 원격지에 소재한 저장매체에 접속한 후 디지털 증거를 수색 및 압수하거나, 수사과정에서 취득한 해외서비스 계정정보를 이용하여 수사기관의 사무실 등에서 직접 해외 서버에 접속한 후 혐의사실과 관련된 데이터를 압수하는 방식 등을 통해 원격지 압수수색을 행하고 있는 것이 현실이다.[1156] 또한 원격지 압수수색과 관련하여 대법원도 현행 「형사소송법」상 압수수색 규정으로 허용될 수 있는 압수수색 방식으로 인정하고 있음을 볼 수 있다. 뿐만 아니라 국제적으로도 원격지 압수수색을 입법화함으로써 적법한 수사방식으로 인정하는 것이 일반적인 추세라고 할 수 있다. 즉 유럽사이버범죄협약 제19조 제2항[1157]에 원격지 압수수색 규정을 두고 있으며, 협약당사국인 프랑스도 형사소송법 제57조의1[1158]에, 독일도 형사소송법 제110조 제3항[1159]에, 그리고 일본도 형사소송법 제218조 제2항[1160]에 원격지 압수수색 규정을 두고 있다.

1156) 정대용, 위의 박사학위논문, 95면.

1157) Convention on Cybercrime(European Treaty Series-No. 185), Title 4. Art. 19, 2. "각 당사국은 제1항 a에 따라 특정 컴퓨터 시스템 또는 그 일부에 대한 수색 또는 유사한 접근을 그 당사국이 진행할 경우, 그리고 찾고자 하는 데이터가 해당 영역내의 다른 컴퓨터 시스템 또는 그 일부에 저장되어 있으며, 해당 데이터가 최초 시스템에서 합법적으로 접근이 가능하거나 사용이 가능한 경우, 당사국은 신속하게 다른 시스템으로의 수색 또는 유사한 접근을 확장할 수 있도록 필요한 입법 및 기타 조치를 채택해야 한다"(https://rm.coe.int/1680081561; 최종접속일 2023.10.25.).

1158) Code de Procedure penale §57-1 "사법경찰관 또는 그들의 책임하에 있는 사법경찰대리인은 본 조항에 규정된 조건에 따라 수색을 하는 동안 수색이 진행되는 장소에 설치된 컴퓨터 시스템을 통해 현재 수사와 관련된 데이터에 접근할 수 있다. 해당 데이터는 최초 시스템에서 접근할 수 있거나 최초시스템에서 사용할 수 있는 경우 해당 시스템이나 다른 컴퓨터 시스템에 저장된다. 최초 시스템에서 접근 가능하거나 최초 시스템에서 사용가능한 이러한 데이터가 국토 외부에 위치한 다른 컴퓨터시스템에 저장되어 있다는 것이 이전에 입증된 경우, 국제법이 제공하는 접근 조건에 따라 사법경찰관이 확보할 수 있다"(https://www.lexbase.fr/texte-de-loi/27093707-art-57-1-code-de-procedure-penale; 최종접속일 2023.10.25.).

1159) StPO §110(3) "수색대상자에게서 발견한 전자저장매체에 대한 열람은 그 전자저장매체와 공간적으로 분리되어 있는 다른 저장매체까지로 확장할 수 있지만, 이는 그 전자저장매체를 통하여 그 다른 저장매체에 접근할 수 있고, 이러한 접근을 하지 않으면 찾고자 하는 데이터를 상실할 우려가 있는 경우에 한한다"(https://www.gesetze-im-internet.de/stpo/__110.html; 최종접속일 2023.10.25.).

1160) 일본 형사소송법 제218조 제2항 "압수물이 컴퓨터인 경우, 해당 컴퓨터에 전기통신회선으로 접속하고 있는 기록매체로서, 해당 컴퓨터에서 작성 또는 변경을 한 전자적 기록 또는 해당 컴퓨터에서 변경 또는 삭제할 수 있도록 되어 있는 전자적 기록을 보관하기 위해 사용되고 있다고 인정하기에 충분한 상황에 있는 경우, 그 전자적 기록을 해당 컴퓨터 또는 다른 기록매체에 복사한 후, 해당 컴퓨터 또는 해당 다른 기록매체를 압수할 수 있다".

이와 같이 디지털 증거 수사에 있어서 원격지 압수수색의 필요성에 대해서는 이론의 여지가 거의 없지만, 영장에 기재된 디지털기기와 네트워크로 연결된 원격지 서버 등으로 수색의 장소적 범위를 실질적으로 확장하는 결과를 가져오기 때문에 현행법상 압수수색 규정으로 포섭가능한 수단인가에 대해서는 견해가 나뉘고 있다. 즉 현행 「형사소송법」 제114조 및 제219조는 압수수색영장에 '수색할 장소'를 기재하도록 규정하고 있고, 법원은 이와 관련하여 압수수색할 장소는 특정되어야 하고, 영장에 기재되어 있는 장소와 동일성이 인정되지 않는 장소에 대한 압수수색은 허용하지 않고 있기 때문이다.[1161] 이러한 압수수색 장소의 동일성 기준만으로 네트워크를 통해 원격지 서버 등에 대한 압수수색의 적법성이 확보된다고 볼 수 있는가에 대해서는 이견이 있을 수밖에 없다고 할 것이다. 더욱이 대법원은 2009.3.12. 선고 2008도763 판결에서 영장에 특정되는 압수대상에 대한 엄격한 해석의 필요성과 피압수자에게 불리한 확장 또는 유추해석의 금지를 강조한 바 있기 때문에, 압수수색의 범위를 장소적 특정이 가능한 디지털기기에서 장소적 개념이 무의미한 네트워크로 확장하는 원격지 압수수색이 허용될 수 있는가에 대해서 해석에 의존하고 있는 현재의 사법상황은 근본적인 문제를 안고 있다고 할 수 있다.

이와 관련하여서는 적극설(긍정설), 소극적(부정설), 제한적 적극설(절충설) 등으로 견해가 나누어지고 있음을 볼 수 있다. 먼저 적극설의 경우 현행 압수수색 규정으로 원격지 압수수색이 가능하다고 보는 견해로, 원격지 압수수색을 하더라도 현실적으로 해당 데이터를 다운로드하거나 출력하는 장소는 수색장소이기 때문에 영장의 집행범위를 넘지 않으며, 피압수자에게 해당 웹사이트 접속 계정정보를 요구하는 것은 「형사소송법」 제120조의 "압수수색 영장 집행에 필요한 처분"의 범위에 포함될 수 있다는 점 등을 그 근거로 들고 있다.[1162] 한편 소극설은 현행 압수수색 규정으로는 원격지 압수수색이 불가능하다는 견해로, 영장의 장소적 범위를 벗어난 장소에 있는 컴퓨터에 대해 영장의 효력이 미친다고 볼 수 없다고 보고 있다.[1163] 다만 소극설은 현행법상 압수수색 규정의 해석만으로는 원격지 압수수색이 불가능하기 때문에 원격지 압수수

1161) 광주고등법원 2008.1.15. 선고 2007노370 판결.
1162) 이숙연, "형사소송에서의 디지털증거의 취급과 증거능력", 박사학위논문, 고려대학교, 2011.2, 34면.
1163) 전승수, "형사절차상 디지털 증거의 압수수색 및 증거능력에 관한 연구", 박사학위논문, 서울대학교, 2011.2, 178-179면.

색에 관한 규정을 입법화할 필요가 있다고 주장한다.[1164]

마지막으로 제한적 적극설은 원격지 압수수색은 일정한 조건 하에서는 현행 압수수색 규정으로 가능하다고 보는 것으로, 비록 영장기재 장소가 피처분자의 컴퓨터가 존재하는 장소로만 되어 있을지라도 해당 데이터가 그로부터 합법적으로 접속가능한 시스템 안에 존재하는 한 영장기재의 특정성을 위반한 것은 아니라고 보는 것이다.[1165] 이 견해는 현재 대법원이 원격지 압수수색의 적법성을 판단하는 논거와 거의 유사하다고 볼 수 있다.

나. 실무상 원격지 압수수색의 운영현황

정보화 사회가 고도화되어 갈수록 정보는 디지털 형태로 분산, 가상화되어 가고 있기 때문에, 수사목적상 압수수색의 범위를 기존의 장소적 개념에 고정시키게 되면 현실적으로 디지털 증거의 확보는 거의 불가능하다고 볼 수밖에 없다. 더욱이 영장집행 범위 내 디지털기기가 존재하는 물리적 장소를 차단해도 네트워크상에 존재하는 디지털 증거는 시간적 공간적 제한없이 원격으로 변경, 삭제 등이 가능하다는 점을 고려하면, 현행의 압수수색영장만으로는 디지털 증거를 확보하는데 한계가 있을 수밖에 없다. 이와 같이 디지털 증거 확보의 필요성이 높아질수록 디지털 증거에 대한 접근가능성은 점점 더 어려워지는 상황에서 압수수색영장 집행의 필요성과 적정성 확보를 위해 제한적 요건 하에서 원격지 압수수색의 적법성을 인정하고 있음을 볼 수 있다.

먼저 수사기관들은 원격지 압수수색을 위해 "압수수색 장소에 존재하는 컴퓨터로 해당 웹사이트에 접속하여 디지털 정보를 다운로드한 후, 이를 출력, 복사하거나 화면을 촬영하는 방식으로 압수한다"는 취지를 영장청구서에 기재하는 방식으로 적법성을 확보하고자 노력하고 있다.[1166]

한편 대법원은 2015.7.16.자 2011모1839 전원합의체 결정에서 처음으로 원격지 압수수색의 가능성을 인정하는 의견을 제시한 바 있다. 즉 다수의견에 대한 대법관

1164) 손동권, "새로이 입법화된 디지털 증거의 압수,수색제도에 관한 연구 -특히 추가적 보완입법의 문제-", 『형사정책』 제23권 제2호, 한국형사정책학회, 2011.12, 340-341면.

1165) 탁희성, 앞의 논문, 32면.

1166) 법원행정처, 『압수수색 영장 실무』(개정 2판), 2016, 76면(박병민·서용성, 앞의 연구보고서, 307면, 각주 818에서 재인용).

이인복, 이상훈, 김소영의 보충의견 가운데서 "원격지 서버에 저장되어 있는 정보라도 영장에 기재된 수색장소에 해당 서버 또는 웹사이트에 접속하여 범죄와 관련된 이메일 등 전자정보를 복제하거나 출력하는 방법으로 하는 압수수색도 가능하다"고 판시한바 있다. 하지만 이 판례는 원격지 압수수색의 적법성 판단을 위한 것이 아니라 전자정보 압수절차상 참여권의 범위 및 별건 압수수색의 위법성 등에 관한 결정이었기 때문에 원격지 압수수색에 대하여 그 이상의 논거나 요건은 제시된 바 없다. 하지만 이후 대법원은 2017.11.29. 선고 2017도9747 판결에서 원격지 압수수색의 적법성에 대한 판단기준을 구체적으로 제시하였다. 즉 "1. 영장에 따라 영장기재 수색장소에 있는 컴퓨터 등 정보처리장치를 이용할 것, 2. 적법하게 취득한 피의자의 아이디와 비밀번호를 입력할 것, 3. 피의자가 접근하는 통상적인 방법에 따라 그 원격지 저장매체에 접속할 것, 4. 원격지 저장매체에 저장되어 있는 피의자 관련 전자정보를 수색장소의 정보처리장치로 내려받거나 그 화면에 현출시킬 것"[1167]이 그것이다. 이러한 기준에 부합하는 원격지 압수수색의 경우 "수색장소에 있는 정보처리장치를 이용하여 정보통신망으로 연결된 원격지의 저장매체에 접속하는 것은 압수수색 영장에서 허용한 집행의 장소적 범위를 확대한 것이라고 볼 수 없다"[1168]고 판시함으로써, 현행 압수수색 규정에 포섭될 수 있는 수단임을 명확히 하고 있다. 또한 원격지 압수수색이 영장집행의 적정성, 필요 최소한도의 범위, 수단과 목적의 타당성에 부합하는 경우에는 대물적 강제처분으로서 허용될 뿐 아니라 원격지 저장매체의 소재가 국외라 하더라도 동일한 판단기준이 적용될 수 있다고 보고 있다.[1169] 즉 원격지 저장매체 소재가 외국이라 하더라도 외국에 소재한 서버 자체에 대한 압수수색을 하는 것이 아니라 권리자와 동일한 적법한 권한을 갖고 해당 서버에 접속하는 것이기 때문에 서버관리자 등의 협조나 참여가 필요없고, 따라서 국제법상 관할권 문제를 야기하는 것도 아니므로 사법공조도 필요하지 않다고 보는 것이다.[1170]

이후 대법원은 2021.7.29. 선고 2020도14654 판결에서 원격지 압수수색에 대하여 동일한 판단기준을 제시하였다. 하지만 대법원 2022.6.30.자 2020모735 결정과 대법

1167) 대법원 2017.11.29. 선고 2017도9747 판결.
1168) 대법원 2017.11.29. 선고 2017도9747 판결.
1169) 대법원 2017.11.29. 선고 2017도9747 판결.
1170) 천성덕·강구민, "실무적 관점에서 본 원격지 서버에 대한 압수·수색 절차 제언", 『형사소송이론과 실무』 제11권 제1호, 한국형사소송법학회, 2019.6, 65-66면.

원 2022.6.30. 선고 2022도1452 판결에서는 원격지 압수수색에 의한 기본권 침해와 일반 압수수색으로 인한 기본권 침해의 정도가 다르다는 관점에서, 앞서 제시된 원격지 압수수색의 적법성 판단기준 외에 "영장에 적힌 압수할 물건에 별도로 원격지 서버 저장 정보가 특정되어 있어야만 한다"[1171]고 함으로써 원격지 압수수색의 적법성 요건을 보다 강화하고 있음을 볼 수 있다.

다. 법적 쟁점

1) 관할권 문제

원격지 압수수색은 영장에 기하여 피압수자의 계정정보를 확보하여 피압수자와 동일한 권한 하에서 원격지에 소재하는 서버 등 저장매체에 접근한다는 점에서 보면, 원격지, 특히 국외에 소재하는 서버업체나 그 관리자에 대해서 어떠한 침해나 업무방해 등의 문제도 야기하지 않기 때문에 관할권 문제의 대상이 아니라고 할 수 있다. 하지만 디지털 정보가 실질적으로는 국외에 소재하는 서버 등에 저장되어 관리되고 있는 중이라고 한다면 수사기관에 의한 서버에 대한 접근행위 자체가 국가관할권 위반이라는 비판도 제기될 여지는 충분히 있다고 볼 수 있다. 특히 국가관할권 가운데 기본적으로 영토제약성을 갖는 집행관할권을 타국의 영토로 확장하는 것은 그 타국의 주권을 직접적으로 침해하는 행위가 되기 때문에, 타국의 동의없이 타국의 영토에서 권력적 기능, 즉 체포, 수사, 압수, 처벌 등을 수행할 수 없는 것이 원칙이라 할 것이다.[1172] 따라서 비록 피압수자와 동일한 권한을 갖고 국외에 소재하는 서버에 접근한 것이라 하더라도 수사의 목적으로 수사기관이 직접 국외 서버에 접근했다는 점에서 보면 집행관할권 위반으로 볼 수 있다.

이에 관련하여 앞서 기술했던 대법원 판결은, 압수수색 대상이 되는 디지털기기가 국외 소재 서버와 네트워크로 연결되어 있고, 영장에 의해 적법하게 취득한 계정과 비밀번호를 통해 국외 소재 서버에 대한 접근권한을 확보한 경우에는 관할권 문제가 발생하지 않는다고 보고 있다. 이와 같이 접근하는 경우 원격지 압수수색의 허용범위

1171) 대법원 2022.6.30.자 2020모735 결정; 대법원 2022.6.30. 선고 2022도1452 판결.
1172) 신상미, "원격지에 저장된 디지털 정보의 압수·수색에 관한 법적 연구", 석사학위논문, 경찰대학교, 2021.2, 44면.

가 남용될 가능성을 배제하기 어려운 측면이 있을 뿐 아니라, 국외 소재 서버로부터 확보하는 디지털 정보의 유형 – 해당 국가 또는 주요 기업의 기밀정보 등 – 에 따라 관할권 문제가 야기될 수 있는 소지도 배제하기 어렵다고 볼 수 있다. 그리고 자국에 소재하는 서버에 대한 압수수색을 관할권 침해로 인식하는 다른 국가가 잠재적으로 존재할 가능성을 배제하기 어려운 이상, 원격지 압수수색은 해당 국가와의 관계에서 관할권 침해 문제를 야기할 가능성이 있다고 할 것이다.[1173] 하지만 디지털 데이터는 적법하고 유효한 권한을 가진 사람이라면 시간과 공간의 제약 없이 항상 접근이 가능할 뿐 아니라 자유로운 데이터 이동을 전제로 하는 인터넷상에 국경이 존재한다고 보기 어렵다는 점을 고려한다면 – 물론 자국의 데이터 보호를 위한 데이터 지역화 조치가 존재하기는 하지만 – , 데이터에 대한 관할권 성립은 물리적 경계인 영토주의적 접근방식보다는 논리적 경계인 데이터에 대한 접근권한으로 이해하는 인식의 전환이 필요하지 않을까 한다.

현재 대부분의 국가들이 네트워크상의 범죄수사의 필요성을 절실히 인식하고 있고, 경우에 따라서는 국가 간 공조를 통해 여러 국가에 걸쳐서 행해지고 있는 사이버상의 범죄문제해결에 협력하는 추세에 있기 때문에, 피압수자의 적법한 권한을 통한 비침해적 접속방식으로 서버에 저장된 디지털 정보를 다운로드하는 방식의 수사에 대해서는 자국 내 법률규정을 통해 그 적법성을 확보해 나가는 경향이 있음을 볼 수 있다. 일본의 경우도 사이버범죄방지협약 체결을 위한 절차법적 정비의 일환으로 원격지 압수수색 규정이 도입되었는 바, “전자적 기록을 보관한 기록매체가 협약 체약국에 소재하고, 동 기록을 공개할 정당한 권한을 가진 자의 합법적이고 임의적인 동의가 있는 경우라면 국제수사공조에 의하지 않고 기록매체에 대한 원격 접근 및 기록의 복사를 허용할 수 있다고 해석해야 한다”[1174]고 보고 있다.

우리나라도 사이버범죄협약에 정식으로 가입할 수 있는 초청서를 받았기 때문에 국내이행입법 정비가 완료되면 원격지 압수수색으로 인한 관할권 문제는 크지 않을 것으로 보여진다.

다만 대법원이 최근 원격지 압수수색 판결에서 제시한 바와 같이 기본권 침해의

1173) 방경휘, “수사상 역외 압수·수색에 관한 연구 -일본 최고재판소 레이와 3년 2월 1일 결정을 계기로-”, 『법학논총』 제35권 제1호, 국민대학교 법학연구소, 2022.6, 162면.

1174) 横山 裕一, 앞의 논문, p.101.

정도가 일반 압수수색의 경우와 차이가 있다고 본다면, 원격지 압수수색에 대해서는 일반 압수수색보다는 엄격한 입법적 제한을 두는 방안을 고려할 필요가 있다고 할 것이다. 앞서 기술했던 프랑스의 경우에는 원격지 압수수색 규정에 '국제법이 제공하는 접근조건에 따라 확보할 수 있다'는 제한을 두고 있으며, 독일의 경우도 '접근하지 않으면 찾고자 하는 증거가 상실될 우려가 있는 경우'로 제한하고 있음을 볼 때, 현재와 같이 실무상 필요에 우선하여 현행 압수수색 규정으로 유추해석을 통해 원격지 압수수색을 포섭하기보다는 별도로 원격지 압수수색 규정을 마련할 필요가 있다고 할 것이다.

2) 원격지 압수수색의 허용범위

현재와 같이 원격지 압수수색에 관한 명시적인 규정이 없는 상황에서, 기존의 압수수색 규정으로 접근하게 되면, 압수수색영장에 기재된 디지털기기를 통해 합법적으로 접근가능한 모든 원격지 서버에 저장되어 있는 디지털 정보 전체에 대한 수색으로 변질될 수 있다는 우려를 배제하기 어렵다고 할 수 있다.[1175] 즉 원격지 서버에 저장된 정보의 사건과의 관련성 여부를 확인하기 위해서는 영장기재대상 디지털기기를 통해 접근할 수 있는 모든 정보저장매체 전체로 수색의 범위가 광범위하게 확장될 수 있고, 이는 결국 수사권의 남용을 허용할 수 있는 기제로 작용할 수 있는 것이다. 특히 스마트폰과 같은 경우 이용자의 접근권한이 부여된 수많은 웹사이트와 애플리케이션이 연동되어 있어서 수사기관의 입장에서도 포괄적 압수수색에 대한 유혹을 받지 않을 수 없다고 할 수 있다.

따라서 원격지 압수수색의 경우 혐의사실과 관련성 있는 디지털 정보가 저장되어 있다고 예상되는 원격지 소재 정보저장매체를 어느 정도 특정하도록 하는 것이 바람직할 것이다. 원격지 압수수색영장이 포괄영장으로 변질되지 않도록 하기 위해서는 대법원이 제시하고 있는 적법성 요건과 원격지 서버의 특정, 보충성 원칙 등이 입법화되어야 할 것이다.

1175) 정대용, 앞의 박사학위논문, 119면.

라. 입법적 고려사항

1) 법적 근거 마련

현재 수사기관에 의해 행해지고 있는 원격지 압수수색은 법원이 제시하고 있는 허용요건에 기반하여 그 적법성을 확보하는 방식을 취하고 있다. 하지만 앞서 기술한 바와 같이 기존의 압수수색 규정으로 원격지 압수수색을 포섭하는 데는 한계가 있다. 즉 수사기관이 영장에 기재된 수색장소에 있는 디지털기기의 고장 – 우연이든 또는 고의든 간에 –, 또는 정전 등과 같은 외부적 영향 등으로 현장에서 원격지 서버에 접근할 수 없는 경우, 적법하게 취득한 접근권한으로 수색장소가 아닌 수사기관 내 디지털기기를 통해 원격지 서버에 접속해서 거기에 저장된 데이터를 다운로드 받는 경우에는 영장에 기재된 수색장소의 범위를 벗어난 경우라 할 수 있고, 이는 기존의 영장주의 원칙을 벗어난 위법한 압수수색이 된다. 그리고 앞서 기술한 바와 같이 수색 대상 디지털기기와 정보통신망으로 연결된 원격지 서버에 대한 구체적인 특정이 없는 경우, 해당 디지털기기로부터 접속가능한 모든 원격지 서버에 대한 접근이 가능하다는 점에서 포괄영장의 우려도 배제하기 어렵다고 볼 수 있다.

따라서 현재와 같이 물리적 장소의 개념에 의존하고 있는 압수수색 규정과 분리하여 별도로 원격지 압수수색에 대한 근거규정을 마련할 필요가 있다고 본다. 이와 같이 법적 근거를 통해 압수수색 권한의 확장의 적법성을 확보하되, 이러한 압수수색 권한의 확장으로 인해 제3자의 프라이버시 또는 다른 국가의 관할권에 대한 침해를 유발할 수 있다는 점을 고려하여, 피처분자에게 주어진 일반적인 접근권한이 허용하는 한계 내로 제한하는 명시적 규정을 두어야 할 것이다.[1176]

2) 원격지 정보저장매체에 대한 접근권한의 범위

원격지 압수수색의 적법성 요건의 하나로 대법원은 적법하게 획득한 접근권한과 그에 의한 통상적인 접근방법을 제시하고 있다.[1177] 즉 피처분자에게 주어진 일반적인 접근권한이 허용하는 범위 내에서만 원격지 서버 등에 대한 압수수색이 가능하다

1176) 탁희성, "전자증거에 관한 연구 -압수·수색과 증거능력을 중심으로-", 박사학위논문, 이화여자대학교, 2004.2, 150면.

1177) 대법원 2017.11.29. 선고 2017도9747 판결.

고 함으로써 수사기관에 의한 계정접속 방법에 대해 일정한 제한을 두고 있는 것이다.

이 경우 통상적인 접근방법에 대한 판단기준은 정보통신시스템 관리자 입장에서 서비스 이용자가 통상적으로 접속하는 방법과 동일하게 서버에 접속하는 것으로 인식하는가라고 볼 수 있다. 따라서 피처분자 또는 제3자가 계정정보를 제공한 경우, 압수수색 과정에서 확보한 자료에 기재된 계정정보를 이용하는 경우, 자동 로그인 기능이 설정되어 있는 경우에는 피처분자의 통상적인 접근방법과 동일한 접근방식으로서 허용될 수 있다.[1178] 하지만 이와 달리 수사기관이 매크로프로그램을 이용하여 계속적 접속을 시도하거나 시스템 보안상 취약점을 이용하여 침입하는 경우 등은 피처분자의 통상적인 접근방법이라고 볼 수 없을 뿐 아니라 원격 정보통신시스템에 대한 침해적 접근방식이라 할 것이므로 원격지 압수수색에 대한 수사기관의 접근방법으로써 허용되어서는 안된다고 할 것이다.[1179] 이러한 접근방식은 원격지 정보통신시스템에 대한 침해를 유발할 뿐 아니라 업무상 부담을 야기할 수도 있기 때문에 통상적인 접근권한이 허용하는 한계를 벗어난 위법한 수단이라 할 것이다.

따라서 원격지 압수수색을 입법화하는 경우 접근 수단 및 권한 확보절차의 적법성 그리고 수단의 적정성 요건을 마련할 필요가 있다고 할 것이다.

3) 원격지 압수수색의 제한 요건

원격지 압수수색은 일반 압수수색에 비하여 기본권 침해의 정도가 더 크다고 볼 수 있다. 즉 원격지 압수수색은 그 대상이 되는 디지털기기로부터 접속가능한 범위 내의 정보저장매체 내의 정보로까지 그 범위가 확장되기 때문에 그로부터 확보할 수 있는 정보의 범위 또한 확대될 수밖에 없고, 그만큼 프라이버시 등과 같은 기본권 침해 가능성이 커지기 때문이다. 따라서 원격지 압수수색에 있어서는 일반 압수수색의 요건인 범죄혐의사실과의 관련성 외에 관련 정보가 보관되어 있다고 인정할 만한 상당성, 독일의 경우와 같은 정보 상실의 우려, 원격지 압수 대상 정보의 범위 등과 같은 요건들을 규정함으로써 원격지 압수수색에 대한 수사기관의 권한을 일반 압수수색에 비하여 좀 더 제한할 필요가 있다고 할 것이다.

1178) 김기범·이관희·장윤식·이상진, "정보영장제도 도입방안 연구", 『경찰학연구』 제11권 제3호, 경찰대학, 2011.9, 108면(이상국, "원격지에 저장된 디지털 정보 접근방안 -원격 압수·수색을 중심으로-", 석사학위논문, 서울대학교, 2020.2, 50면에서 재인용).

1179) 김기범·이관희·장윤식·이상진, 앞의 논문, 108면(이상국, 위의 석사학위논문, 50면에서 재인용).

4. 온라인 수색제도

가. 필요성과 도입 현황

온라인 수색이란 "타인의 정보기술시스템 이용을 감시하고, 저장된 내용을 읽고 기록하기 위한 목적으로 기술적 수단을 사용하여 타인의 정보기술시스템에 은밀하게 접근하는 행위"[1180]를 말한다. 즉 온라인 수색은 특정범죄에 대응한 범죄예방 및 범죄진압을 위해 도입된 국가에 의한 합법적 해킹이라고 할 수 있다.[1181] 따라서 온라인 수색은 기술적 보안시스템을 기반으로 폐쇄적인 네트워크로 운영되는 비밀영역에 대한 수사방법이기 때문에 수사 자체도 해킹이라는 기술적 수단과 비밀성이 그 전제가 되고, 이는 기존의 강제수사보다 훨씬 더 강한 기본권 침해를 수반할 수밖에 없다.

이러한 온라인 수색을 합법적인 수사방법으로 활용하게 된 데는 텔레그램과 같은 암호통신시스템, 그리고 소위 인터넷 암시장을 형성하고 있는 온라인 플랫폼인 다크넷을 이용한 테러나 조직범죄, 마약범죄, 아동 음란물 유통 및 성착취물 형태의 디지털 성범죄, 자금세탁 등에 대한 수사에 있어서는 기존의 수사방법으로는 한계에 직면할 수밖에 없을 뿐 아니라 실체적 진실에 접근하고자 시도하는 것조차 용이하지 않기 때문이라 할 수 있다. 특히 암호화 기술이 고도화될수록 익명성과 폐쇄성에 기반한 온라인 플랫폼에의 접근 자체가 기존의 수사방법으로는 불가능에 가깝기 때문에, 국가의 안전뿐만 아니라 개인의 생명, 신체, 자유를 심각하게 침해하는 범죄행위가 웹상에서 이루어지고 있음에도 불구하고 기존 법률의 테두리 내에서는 이러한 범죄에 대응하기 위해 국가가 사용할 수 있는 수단은 제한적일 수밖에 없다. 이는 기존 법률에 규정된 범죄대응 수단들은 암호화 기술로 무장된 온라인 플랫폼상의 범죄를 상정하지 못한 데서 비롯된 당연한 결과라고 할 수 있다.

이와 같이 갈수록 고도화되어 가는 정보통신기술의 악용으로 야기되는 법익침해상황에 대처하기 위해서 그러한 기술적 상황에 부합하는 수사방법이 요구될 수밖에 없고, 온라인 수색도 그러한 수사방법 가운데 하나라고 할 수 있다.

1180) BTS-Drs.18/12875; KK-StPO/Bruns, 8.Aufl.2019, StPO §100b Rn.3(박병민·서용성, 앞의 연구보고서, 134면에서 재인용).

1181) 박희영, "국가의 합법적인 해킹행위로서 온라인 수색에 관한 독일 법제 동향", 『최신외국법제정보』 2019년 제1호, 한국법제연구원, 2019.4, 55면.

실제로 미국의 경우 2017년 무기, 마약, 위조문서, 위조지폐, 살인 청부 등의 거래처로 사용되었던 '실크로드'라는 다크웹을 잠입수사 방식을 통해 폐쇄[1182]했으며, 2020년 프랑스와 네덜란드 합동수사팀은 마약, 무기, 청부살인 등이 행해졌던 'EncroChat'을 온라인 수색을 통해 해체한 바 있었다.[1183] 이 외에도 독일과 미국의 공조로 2022년 마약, 해킹자료, 위조문서, 비트코인 믹싱을 통한 돈세탁 거래와 각종 불법물품판매 등 사이버범죄의 온상이었던 '히드라'를 적발하여 폐쇄하였으며, 유로폴도 'The Giftbox Exchange'라는 아동포르노 사이트를 수색하기 위해 온라인 수색방식을 사용한 바 있다.

온라인 수색제도를 최초로 법제화한 국가는 프랑스로 2011년 형사소송법에 도입하였으며, 현재는 독일, 영국, 오스트리아, 네덜란드, 스페인, 스위스, 미국, 호주 등에서 온라인 수색제도가 도입되어 있다.[1184] 이 가운데 주요 국가들의 온라인 수색 관련 규정을 살펴보면 다음과 같다. 먼저 프랑스의 경우 형사소송법 제706-102-1조 데이터 정보의 수집(De la captation des données informatiques)이라는 표제하에 "컴퓨터데이터가 컴퓨터 시스템에 저장되어 있거나, 이용자의 자동 데이터 처리시스템의 모니터에 나타나 있거나 이용자에 의해서 입력되고 있거나 주변장치에 의해서 송수신되고 있는 경우에는 관련자의 동의 없이 어디서나 컴퓨터데이터에 접근하여, 이를 기록, 저장, 전송하는 것을 목적으로 하는 기술적 장치를 설치할 수 있다"고 규정하고 있다.[1185] 이 온라인 수색 규정은 조직범죄에 대해서만 규정하도록 되어 있다.

다음으로 영국은 '2016년 수사권한법(Investigatory Powers Act 2016)'을 제정하여 수사기관 및 정보기관으로 하여금 인터넷 및 통신에 있어서 대규모 통신감시를 허용하고 있다.[1186] 수사권한법 Part 5에 규정된 "Equipment interference"에서 온라인 수색영장이라 할 수 있는 '대상특정 장비침입 영장(Targeted Equipment Interference

---

1182) 이원상, "다크넷 수사를 위한 수사제도에 대한 소고", 『형사법의 신동향』 통권 69호, 대검찰청, 2020.12, 355면.

1183) 박희영, "유럽에서 온라인 수색과 암호통신망 EncroChat 사건", 『형사법의 신동향』 통권 제78호, 대검찰청, 2023.3, 37-61면 참조.

1184) 박희영, "유럽에서 온라인 수색과 암호통신망 EncroChat 사건", 40-41면.

1185) 박희영, "유럽에서 온라인 수색과 암호통신망 EncroChat 사건", 43면; Code de procédure pénale(https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/; 최종접속일 2023.10.18.).

1186) 박희영, "유럽에서 온라인 수색과 암호통신망 EncroChat 사건", 50면.

Warrant)'에 관한 규정을 두고 있다. 즉 대상특정 장비침입영장이란 "통신, 장비데이터 기타 정보를 수집할 목적으로 장비에 침입할 수 있도록 관계자에게 권한을 부여하거나 요구하는 영장"[1187]이라고 규정하고 있으며, "통신 기타 정보의 획득이란 사람의 통신 또는 기타 활동을 감시, 관찰, 청취하고, 그렇게 감시하거나 관찰된 또는 청취된 모든 것을 기록하는 것을 포함한다"[1188]고 규정하고 있다. 그리고 영장의 대상은 "개인 또는 다수의 개인 및 단체가 소유, 사용, 점유하고 있는 장비나 특정위치에 있거나 특정활동을 목적으로 사용되는 장비"[1189]로 규정하고 있으며, "중대한 범죄를 예방하거나 탐지할 목적으로 필요하다고 판단되는 경우"[1190] 영장을 발부할 수 있도록 규정하고 있다. 또한 Part 5에 의해 영장발부 결정을 승인할 때 사법위원회는 "해당 영장이 관련 근거에 따라 필요한지 여부, 해당 영장에 의하여 승인되는 행위가 그 행위로 인하여 달성하고자 하는 목적에 비례하는지 여부"[1191]를 검토하도록 되어 있다.

독일의 경우 형사소송법 제100b조에 온라인 수색이 규정되어 있는데, "1. 일정 사실에 근거해 볼 때 제2항에서 정한 특히 중대한 범죄를 정범 또는 공범으로 실행했다는 혐의가 인정되는 경우 또는 그 범죄의 미수를 처벌하는 때에는 범죄의 실행에 착수했다는 혐의가 인정되는 경우, 2. 범행이 개별사안에서도 특별히 중대하다고 인정되는 경우, 3. 사실관계의 규명이나 피의자 소재 파악이 다른 방법으로는 매우 어렵거나 불가능할 것으로 예상되는 경우, 당사자가 알지 못하더라도 기술적 수단을 이용해 당사자가 사용하는 정보기술시스템에 침입하여 그로부터 정보를 획득할 수 있다"[1192]고 되어 있다. 이러한 온라인 수색은 피의자에 대해서만 할 수 있지만 예외적으로 "1. 피의자가 다른 사람의 정보통신기술시스템을 사용한 경우, 2. 피의자의 정보기술시스템에 침입하는 것만으로는 사실관계를 규명하거나 공동피의자의 소재를 파악할 수 없는 경우에는 불가피하게 피의자 아닌 사람의 정보기술시스템에 침입하는 것이 허용된다"고 규정하고 있다.[1193] 이와 같이 온라인 수색제도를 법률로 규정하고 있는

1187) Investigatory Powers Act 2016, Part5, §99(2).
1188) Investigatory Powers Act 2016, Part5, §99(4). 구체적으로 장비침입기능이 무엇인가에 대해서는 The Home Office, "Equipment Interference Code of Practice", 2018.3, p.10에 설명되어 있다.
1189) Investigatory Powers Act 2016, Part5, §101(1).
1190) Investigatory Powers Act 2016, Part5, §106(1)(a).
1191) Investigatory Powers Act 2016, Part5, §108(1).
1192) StPO §100b(1).
1193) StPO §100b(3).

국가들에 있어서 공통적으로 규정하고 있는 요건이 있음을 볼 수 있다. 즉 대상범죄가 조직범죄와 같은 중대범죄로 제한되어 있다는 것이고, 둘째, 타인의 정보기술시스템에 당사자의 동의 없이 데이터를 감시, 기록, 저장, 전송할 수 있는 기술적 수단을 설치할 수 있다는 것이고, 셋째, 그 행위와 그 행위로 달성하고자 하는 목적이 비례하는지 또는 다른 방법으로는 사실관계 규명 등이 불가능한 경우인지, 즉 비례성과 보충성의 원칙에 부합하는지를 요구하고 있음을 볼 수 있다.

나. 법적 쟁점

1) 기본권 침해에 대한 실질적 허용 요건과 절차적 통제

독일에서 온라인 수색제도는 2번의 위헌판결을 거친 후 형사소송법 규정으로 도입되었는데, 2번의 위헌판결에 있어서 핵심적인 논거는 '개인의 기본권의 침해' 여부라고 할 수 있다. 즉 2006년 노르트라인 베스트팔렌(Nordrhein-Westfalen) 헌법보호법 제5조는 주헌법보호청의 직무를 수행하기 위한 권한을 새로 도입하면서 동조 제2항 제11호에 온라인 수색을 규정하였다.[1194] 동조 제2항 제11호 규정을 보면 "(2) 헌법보호청은 정보기관의 수단으로서 정보획득을 위하여 동법 제7조상의 전제하에 다음과 같은 수단들을 사용할 수 있다. … 11. 특히 통신장치에 비밀리에 참여하거나 통신장치를 수색하는 것과 같은 비밀관찰과 그 밖의 인터넷 수사 및 기술적 수단의 투입으로 정보기술시스템에 비밀리에 접근하는 것, 그러한 조치가 서신, 우편 및 통신비밀을 침해하거나 종류와 중요성에서 이와 동일한 경우 이 조치는 서신, 우편 및 통신비밀의 제한에 관한 법률상의 조건하에서만 허용된다"고 되어 있다.[1195] 이 규정은 해당 주의 시민들의 반대에 부딪혀 헌법소원을 통해 그 위헌성을 다투었지만, 독일 연방헌법재판소는 동 조항이 기본권 제1조 제1항과 연결된 제2조 제1항, 제10조 제1항, 제19조 제1항 제2문과 합치되지 않아서 무효라고 선언하였다.[1196] 즉 2008년 독일 연방헌법재판소는 이 판례에서 온라인 수색 규정이 규범 명확성, 비례성 원칙의 요구를 보장하

1194) 박희영, "독일에 있어서 경찰의 온라인 수색에 관한 판례 및 법제 동향", 『최신외국법제정보』 2011년 제2호, 한국법제연구원, 2011.4, 89면.
1195) 박희영, "독일에 있어서 경찰의 온라인 수색에 관한 판례 및 법제 동향", 89면.
1196) 허황, "최근 개정된 독일 형사소송법 제100조b의 온라인 수색과 제100조a의 소스통신감청에 관한 연구", 『형사법의 신동향』 통권 제58호, 대검찰청, 2018.3, 109면.

지 않았으며, 사적 생활 형성의 핵심영역을 보호하기 위한 충분한 장치를 규정하고 있지 않기 때문에 무효이며, 독일 헌법 기본권 제1조 제1항과 연결된 제2조 제1항의 일반적 인격권으로부터 도출된 '정보기술시스템의 신뢰성과 무결성의 보장'이라고 하는 IT 기본권을 침해하는 것으로 판단했다.[1197] 하지만 인터넷 수사를 위한 정보기술시스템에 대한 비밀접근은 기본적으로 적절한 수사처분이라고 보고 있으며, 다만 그러한 침입수단의 비밀성은 예외에 속하는 것이고 특별한 정당성을 요구하며, 기본권 침해로 간주되지 않는 경우에는 이러한 조치를 취할 수 있다고 함으로써 온라인 수색 자체는 허용될 수 있다는 것을 인정했다는 점에서 의미가 있다.[1198]

온라인 수색에 대한 연방헌법재판소의 판결 내용을 반영[1199]하여 2008년 연방수사청법에 온라인 수색과 관련하여 '정보기술시스템에 대한 비밀침입' 규정을 마련하였다. 이에 대하여 2016년 연방헌법재판소는 연방수사청법상 국제테러의 위험을 방지하기 위한 비밀감시처분들 – 온라인 수색을 포함한 – 에 관한 수권규정은 기본적으로 헌법상 기본권과 일치하지만, 사생활의 핵심영역의 보호에 관한 규정은 헌법에 합치하지 않는다고 판결했다.[1200] 즉 동법 제20k조 제7항에 규정하고 있는 온라인 수색 시 사생활의 핵심영역 보호에 관한 규정은 수집된 데이터를 선별하는 기관의 독립성이 충분히 보장되어 있지 않으며, 데이터 선별의 이행과 결정에 대한 책임은 독립된 제3자에게 있어야 함에도 동 규정은 이러한 요건들을 충족하지 못하고 있다고 보았다.[1201]

이와 같이 독일의 연방헌법재판소는 수사절차상 온라인 수색의 필요성은 인정하면서도 그로 인해 침해되는 개인의 기본권을 보호할 수 있는 법적·기술적 장치가 필수적이라는 점을 분명히 하고 있음을 볼 수 있다.

즉 인터넷상 암호통신기술에 기반하여 폐쇄적으로 이루어지고 있는 테러, 마약, 무기 밀매, 돈세탁, 아동 음란물 및 성착취물 유통 등의 범죄를 차단하기 위해서는

1197) 박희영, "정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권(下)", 『법제』, 법제처, 2008.11, 60면.

1198) 박희영, "정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권(下)", 63면; 허황, 위의 논문, 111면.

1199) 첫째, 아주 중요한 법익에 대한 구체적 위험이 발생한 실체적 근거가 존재할 것, 둘째, 독립적이고 중립적인 법관의 판단에 근거한 처분일 것, 셋째, 법률로서 개인의 기본권을 보호할 것 등이 주요 내용이라 할 수 있다(정이현, "온라인 수색의 법제화 방안 연구", 석사학위논문, 성균관대학교, 2021.2, 52면).

1200) 박희영, "국가의 합법적인 해킹행위로서 온라인 수색에 관한 독일 법제 동향", 57면.

1201) 허황, 위의 논문, 114면.

그러한 폐쇄적인 네트워크 속으로 사람이 직접 들어가거나(잠입수사) 또는 그러한 네트워크에 기술적 침입수단(온라인 수색)을 투입할 수밖에 없는 현실적인 필요성은 명백히 존재한다고 볼 수 있다. 하지만 비밀리에 정보통신시스템에 기술적 침입수단을 투입하여 그 이용을 감시하고, 저장된 정보를 확보하는 것은 자유로운 지식과 정보의 공유를 지향하는 웹의 본질을 훼손하는 것일 뿐 아니라, 그 이용자들의 정보에 대한 자기결정권뿐 아니라 정보통신망을 통해 형성되는 사생활에 대한 중대한 침해를 초래할 수밖에 없다. 정보화 사회에 있어서는 개인들의 경우 자신의 인격 내지 정체성의 발현 및 사회적 관계를 형성하는 수단으로 정보기술시스템을 이용하게 되며, 기업들의 경우에는 기업운영에 필요한 재무회계뿐만 아니라 특허 기술, 인적 네트워크 등 핵심적인 기업정보의 저장, 이용, 전송 등을 정보기술시스템에 의존하게 될 수밖에 없다. 따라서 이러한 시스템에 비밀리에 접근하는 것이 가능해진다면 방대한 양의 정보가 수집될 수 있고, 그로 인해 개인의 인격과 사생활에 대한 심각한 침해 또는 기업의 생존을 좌우할 수 있는 피해를 야기할 수 있다고 할 것이다. 이와 같이 정보통신시스템에 대한 기술적 침입을 전제로 하는 온라인 수색을 허용하게 되면 기존의 헌법상 기본권으로도 보호하기 어려운 중대한 권리침해가 발생할 수밖에 없다는 우려가 제기될 수 있다. 독일의 연방헌법재판소가 온라인 수색과 관련하여 IT 기본권이라고 하는 새로운 기본권을 기존의 인격권에서 분리하여 별도의 법적 보호장치의 필요성을 강조한 것도 이러한 이유에서 비롯된 것이라 할 것이다.

국가에 의한 온라인 수색이 범죄의 예방 및 진압수단으로써 정당화되기 위해서는 그로 인한 기본권의 제한을 국민들이 수인할 수 있는 수준의 법적 뒷받침이 존재해야만 한다. 즉 온라인 수색이 요구되는 목적과 수단에 비례해야 할 뿐 아니라 다른 수단에 의해서는 사실관계에 대한 수사 또는 피의자에 대한 조사가 불가능하다는 보충성의 원칙도 명확히 규정되어야 할 것이다. 그리고 무엇보다도 온라인 수색에 관한 규정은 명확성의 원칙에 충실하게 규정함으로써 수사기관뿐만 아니라 법원에 대해서도 유추 내지 확장해석의 여지를 두지 않도록 해야 할 것이다. 이와 같이 법률상 허가 요건을 명확히 함으로써 온라인 수색이 수사절차상 필요 최소한의 범위를 벗어나지 않도록 해야 한다.

또한 온라인 수색에 대해서는 이중적 통제장치를 둠으로써 수사기관에 의한 남용

가능성을 원천적으로 차단할 필요가 있다고 할 것이다. 즉 법원에 의하여 사전에 영장을 발부받도록 하는 사전통제와 온라인 수색이 종료된 후 분기별 또는 반기별로 국회에 온라인 수색이 행해진 사건의 유형과 집행 방식 등 구체적 사실에 대하여 보고하도록 하는 사후통제가 그것이라 할 것이다.

2) 기술적 침입수단의 관리

온라인 수색은 국가에 의한 합법적인 해킹이라는 점에서 볼 때, 거기에 사용된 기술적 침입수단으로서 해킹 프로그램에 대한 관리가 필요하다고 할 것이다. 즉 법원에서 거기에 사용되는 프로그램의 기능에 대해서 제대로 알지 못하는 상태에서 온라인 수색에 대한 사전영장을 발부하게 되는 경우, 수사기관이 해당 프로그램을 어떻게 오남용할지에 대해서는 통제가 불가능하게 될 수도 있다. 따라서 수사기관이 사용하는 해킹프로그램에 대한 일정한 관리가 필요하다고 생각한다.

통신감청의 경우 「통신비밀보호법」에 감청설비에 대해서 인가기관과 인가 절차, 신고 등의 규정을 두고 있는 것과 마찬가지로 수사기관이 사용, 관리하는 해킹프로그램에 대해서는 기술명세서를 포함하여 일정한 등록 절차를 거치도록 하고, 해당 프로그램에 대한 접근권한의 수준을 설정하여 둠으로써 무권한자에 의한 사용을 통제하는 것도 생각해 볼 수 있다고 할 것이다. 그리고 해당 프로그램을 사용한 경우에는 사용자, 대상사건, 사용기간, 수집된 정보의 유형 등을 기록하도록 하고, 이 기록을 분기별 또는 반기별로 국회에 보고하도록 함으로써 수사기관에 의한 오남용 가능성을 배제할 필요가 있다고 할 것이다.

3) 기존 영장제도의 한계

기존의 압수수색영장을 집행함에 있어서는 집행할 장소를 특정하도록 규정하고 있다. 이는 유체물에 대한 압수수색을 전제로 마련된 규정이기 때문에 디지털 증거 압수수색, 특히 온라인 수색에 있어서는 정보통신시스템에 기술적 수단을 침입하는 방식이기 때문에 해당 정보통신시스템을 운영하는 서버의 장소를 특정해야 하는 문제가 생길 수 있다. 하지만 서버의 장소를 특정하기 어려운 경우가 있을 수 있다는 점을 감안하면 온라인 수색 대상이 되는 정보통신시스템을 특정하는 것으로 대신할

필요성을 고려해 보아야 할 것이다.

다음으로 현행법상 영장집행 시 사전영장제시 및 피처분자에 대한 사전통지, 참여권 보장 등이 규정되어 있는데, 온라인 수색의 경우 비밀성을 기본전제로 하기 때문에 사전통지 또는 압수수색 과정에서 참여권 보장 등과 같은 피처분자의 권리에 대하여 일정한 제한이 부과될 필요가 있다고 본다. 다만 필요한 경우 온라인 수색이 종료된 이후 피처분자에 대해 사후 통지를 하거나 온라인 수색을 통해 확보된 디지털 증거에 대한 선별과정에 피처분자의 참여권을 보장하는 것은 가능하다고 할 것이다. 이와 같이 기존의 영장집행과 관련한 규정들은 온라인 수색에 부합하지 못하는 측면이 있기 때문에 온라인 수색에 부합하는 영장집행절차를 입법화할 필요가 있다고 본다.

4) 관할권 문제

온라인 수색에 있어서 국외에 소재하는 정보통신기술시스템에 대한 기술적 침입수단을 사용하는 경우에는 국가관할권 문제가 제기될 수밖에 없다. 특히 법원 또는 행정기관이 체포, 강제조사 등의 물리적 강제조치에 따라 국내법을 집행하는 권한을 의미[1202]하는 집행관할권의 경우 영토적 제약성을 지니고 있어서 다른 국가의 동의 없이 타국의 영역에서 권한을 행사할 수 없음이 원칙이기 때문에, 수사의 목적으로 국외 소재의 정보통신기술시스템에 비밀리에 침입하는 것은 집행관할권을 타국으로까지 확장하는 것이 되기 때문에 국제법 위반이 제기될 수밖에 없다. 앞서 기술한 원격지 수색의 경우에는 이용자의 통상적인 접근방법이라고 하는 비침해적 수단으로 국외에 소재하는 원격지 서버에 접근하기 때문에 관할권 문제의 소지가 적은 반면, 온라인 수색은 명백히 국외 소재 정보통신시스템에 대한 침해와 위험을 야기하는 침해적 수단이기 때문에 관할권 문제가 해결되지 않고서는 국외 소재 정보통신시스템에 대해서는 적용할 수 없다고 할 것이다.

현재 온라인 수색을 입법화하여 활용하고 있는 국가들에 있어서도 다크넷 수사와 같이 여러 국가에 걸쳐 범죄행위가 행해지고 있는 경우에는 여러 국가의 수사기관들의 공조를 통해 온라인 수색을 실시하고 있음을 볼 수 있다. 즉 온라인 수색이라고 하는

1202) 석광현, "클라우드 컴퓨팅의 규제 및 관할권과 준거법", 『Law&Technology』 제7권 제5호, 서울대학교 기술과법센터, 2011.9, 24면(조성훈, "역외 디지털증거 수집과 국제형사 규범의 발전", 『법학논총』 제43권 제3호, 단국대학교 법학연구소, 2019.9, 122면에서 재인용).

기술적 침입수단이 필요한 중대범죄 – 마약, 테러, 아동포르노 등 – 의 경우 한 국가에 국한되기보다는 인터넷과 네트워크 기술을 이용하여 여러 국가에 걸쳐 동시에 행해지고 있기 때문에 국가 간 국제형사사법공조의 필요성이 매우 높다.

현재로서는 국제형사사법공조를 통해서만 국외 소재 정보통신시스템에 대한 온라인 수색이 가능하다고 볼 수 있기 때문에, 해당 국가의 동의와 협조가 우선되지 않고서는 국외 온라인 수색은 불가능하다고 보아야 할 것이다.

다. 입법 시 고려사항

1) 온라인 수색에 대한 실질적 요건 마련

앞서 기술한 바와 같이 수사절차상 온라인 수색은 비례성 원칙, 보충성 원칙, 명확성 원칙을 준수해야만 그로 인한 기본권 침해에 대한 정당성이 부여된다고 볼 수 있다. 즉 비례성 원칙에 따라 온라인 수색은 국가안보, 사람의 신체·생명·자유에 대한 심각한 피해를 야기하는 중대한 범죄의 발생에 대한 구체적인 위험이 존재한다는 사실적 근거가 존재하는 경우에만 허용된다고 보아야 할 것이다. 여기서 사실적 근거를 요구하는 것은 추측이나 일반적 경험칙만으로는 온라인 수색이 정당화될 수 없다는 것을 의미한다고 볼 수 있다.[1203] 이 경우 독일의 온라인 수색 규정과 같이 '실행에 착수했다는 혐의의 근거가 되는 사실이 있는 경우'라고 문구를 명시함으로써 범죄의 구체적 실행에 대한 대응수단이라는 점을 명확히 하는 것이 온라인 수색의 취지를 반영하는 것이라 할 수 있다.

또한 독일 형사소송법상 온라인 수색 규정과 같이 사실관계의 조사나 피의자의 소재에 대한 수사가 다른 방법으로는 현저히 어려움을 겪거나 불가능할 것으로 예상되는 경우[1204]에 한해서, 그리고 필요 최소한의 범위 내에서 이루어져야 한다는 보충성의 원칙도 법률에 명시해야 한다. 그리고 명확성의 원칙에 따라 온라인 수색의 대상이 되는 중대범죄를 구체적으로 열거해야 하는바, 「통신비밀보호법」 제5조 제1항에 규정된 범죄를 고려해 볼 수 있지만, 온라인 수색에 내재한 기본권 침해의 정도와

1203) 박희영, "예방 및 수사목적의 온라인 비밀수색의 허용과 한계", 『원광법학』 제28권 제3호, 원광대학교 법학연구소, 2012.9, 178면.

1204) StPO §100b(1) 3..

필요 최소한의 침해를 고려해 볼 때 통신제한조치의 허가요건으로써 열거된 범죄유형보다는 훨씬 더 제한적으로 열거해야 할 것이다.

2) 온라인 수색에 대한 절차적 통제방안

온라인 수색에 대한 절차적 통제와 관련하여 독일연방헌법재판소는 "온라인 수색은 정보기술시스템에 대한 비밀접근의 한 수단으로서 수사기관이 사생활의 핵심영역에 해당하는 개인데이터를 수집할 위험이 있다. 하지만 그 비밀성으로 인해 피처분자는 자신의 사생활의 핵심영역이 침해되는지 여부를 확인할 수도 없기 때문에, 특별한 절차적 예방조치를 통해 핵심영역 침해의 위험으로부터 보호받아야 한다"[1205]고 판시함으로써 절차법적 통제의 필요성을 강조하고 있음을 볼 수 있다. 즉 정보통신시스템에 대한 국가에 의한 비밀감시조치의 필요성이 인정될 수밖에 없다고 할지라도 기존의 다른 수사절차상의 감시조치와 비교할 수 없을 정도의 침해를 유발할 가능성이 내재되어 있는 한, 법률상 보다 엄격한 절차적 통제장치를 통해 그러한 위험성을 억제해야 한다고 보는 것이라 할 수 있다. 따라서 온라인 수색의 입법적 전제로서 갖추어야 할 절차적 통제방안을 검토할 필요가 있다고 본다.

가) 온라인 수색의 주체와 객체

온라인 수색은 비밀성에 기반한 강제수사처분이기 때문에 사법적 통제의 대상이 되며, 따라서 법관의 영장에 의한 사전심사 대상이 된다고 보아야 할 것이다. 즉 수사기관에 의한 강제처분 권한의 남용을 억제하고, 침해의 우려가 있는 시민의 기본권을 보장하기 위해서는 법관유보가 필요하기 때문이다. 따라서 온라인 수색에 대한 처분권한은 법관에게 있다고 보아야 한다. 다만 온라인 수색에 있어서 긴급성을 이유로 법관유보의 예외를 인정할 것인가가 문제될 수 있는데, 온라인 수색에 수반되는 기본권제한의 정도와 그 침해의 수준을 고려한다면 사전영장주의의 예외를 인정하지 않는 것이 바람직하지 않을까 한다. 다만 영장주의에 수반되는 영장제시 원칙과 사전통지에 관한 규정은 비밀수사처분으로서 온라인 수색과 부합하지 않은 측면이 있기 때문에, 사전영장제시 및 통지에 관한 규정에 대해서는 예외를 인정하는 것이 필요하다고 본다.

1205) BVerfGE 120,274. Rn.272, 275(https://www.servat.unibe.ch/dfr/bv120274.html; 최종접속일 2023.10.21.).

한편 온라인 수색의 객체, 즉 피처분자는 원칙적으로 피의자로 제한해야 할 것이다. 즉 온라인 수색을 통한 기본권 침해의 정당성은 피의자의 범죄사실에 한해서만 허용되는 것이고, 그렇게 함으로써 기본권 침해를 필요 최소한으로 억제할 수 있다고 할 것이기 때문이다. 다만 피의자가 제3자의 정보통신시스템을 이용하는 경우에는 제3자의 정보통신시스템에 대한 온라인 수색이 허용될 필요가 있다고 할 것이다. 독일의 경우 다른 사람의 정보기술시스템에 대한 접근은 피의자가 다른 사람의 정보기술시스템을 이용하고 있고, 피의자의 정보기술시스템에 대한 침입만으로는 공동피의자의 소재지나 사실관계의 조사를 위해서 충분하지 않은 경우에 가능[1206]하도록 규정하고 있음을 볼 수 있다. 이 경우 제3자에 대해서는 영장주의 원칙의 제반규정들이 그대로 적용될 수는 있지만 비밀유지의무를 부과함으로써 온라인 수색의 비밀성을 유지해야 할 것으로 생각된다.

나) 대상범죄와 기간의 제한

앞서 기술한 바와 같이 온라인 수색이 행해질 수 있는 대상범죄는 국가안보 또는 개인의 신체, 생명, 자유를 심각하게 침해하는 범죄로 제한되어야 하며, 그 대상범죄는 법률상 명시적으로 열거되어 있어야 한다. 이는 온라인 수색이라고 하는 침해적 수단과 그로 인해 보호되는 법익의 중요성이 비례해야 할 뿐 아니라 그와 같이 중대한 범죄를 수사하고 소추하고자 하는 목적에 적합한 수단이어야 한다는 비례성의 원칙에서 요구되는 절차적 요건이라 할 수 있다.

따라서 온라인 수색의 대상범죄를 어느 범위로 할 것인가에 대해서 고려할 때 「통신비밀보호법」상 통신제한조치 대상범죄를 생각해 볼 수 있지만, 온라인 수색은 기본권 제한의 정도가 전기통신감청보다 훨씬 높다는 위험성을 고려할 때 통신제한조치 대상범죄보다는 훨씬 더 그 범위가 제한적으로 적용되어야 할 것으로 생각된다. 즉 「통신비밀보호법」상 통신제한조치 대상범죄 가운데서도 특히 내란죄, 간첩죄, 범죄단체조직죄, 살인죄, 돈세탁 등과 같은 종래의 중대범죄와 함께 아동·청소년 대상 성범죄, 아동 음란물 및 성착취물 유포, 마약류 유통 등과 같이 정보통신시스템을 범죄의 수단으로 악용하여 심각하게 개인의 신체, 자유 등을 침해하는 범죄에 대해서는 온라

1206) StPO §100b(3).

인 수색이 허용될 수 있다고 할 것이다. 하지만 구체적으로 어떤 범죄유형에 대해 온라인 수색이 허용될 수 있는가에 대해서는 그 피해의 중대성에 대한 입법정책적 논의를 거쳐 결정되어야 할 것이다.

다음으로 온라인 수색의 경우에는 정보통신시스템에 대한 기술적 침입을 허용하는 것이기 때문에 그 기간이 제한적이어야 한다. 즉 온라인 수색은 필요 최소한도의 범위 내에서 이루어져야 하기 때문에 기술적 침입이 이루어지는 기간 역시 필요 최소한도로 제한되어야 할 것이다. 온라인 수색의 기간과 관련해서 영국은 6개월(연장 가능), 프랑스의 경우 1개월(1회 연장), 독일은 1개월(최대 6개월까지 연장)로 규정하고 있음을 볼 수 있다. 그리고 우리의 경우 통신제한조치에 대해서 2개월(1회 연장)로 규정하고 있음을 고려할 때 통신제한조치의 기간 보다 넘어서서 허용되는 것은 불합리하다고 보여지는 바, 최대 2개월을 초과해서는 안된다고 할 것이다. 그리고 불가피하게 연장이 필요한 경우에는 다시 법원에 의한 통제를 전제로 하여 연장할 수 있다고 보아야 할 것이다.

다) 사생활 보호

온라인 수색에 있어서 사생활 보호와 관련한 규정의 필요성은 정보통신시스템에 있어서 자유로운 정보의 생성, 저장, 이용 등에 대한 개인의 신뢰가 온라인 수색으로 인해 침해될 가능성이 매우 크다는 데 있다고 할 수 있다. 즉 정보화 사회에 있어서 개인들은 자신의 인격 발현을 대부분 정보기술시스템의 이용에 의존하고 있기 때문에, 그러한 시스템에 의해 생성, 저장, 처리되는 데이터가 비밀로 유지된다는 기밀성[1207]에 대한 합리적 기대를 가지고 있다고 볼 수 있는 것이다. 따라서 정보기술시스템에 대한 비밀접근을 통한 데이터 수집은 개인들이 신뢰하는 자신의 데이터에 대한 기밀성뿐 아니라 그 데이터에 내포되어 있는 사생활 불가침의 핵심영역을 침해할 수 있는 가능성을 내포하게 되는 것이다. 이와 같이 범죄예방 또는 형사소추의 목적으로 정당화될 수 있는 온라인 수색이라 하더라도 범죄사실과 무관한 또는 그 개연성이 현저히 낮은 개인의 사생활에 대한 데이터에 대해서는 그 수집 및 이용을 제한하는 것이 헌법상 기본권제한의 법리 즉 권리의 본질적 내용을 침해할 수 없다는 「헌법」

1207) 김재희·박희영, 『온라인 수색활동의 적법성 검토 및 도입방안 연구』, 연구용역보고서, 경찰청, 2022.12, 138-139면.

제37조에 부합하는 것이라 할 수 있다. 이와 관련하여 독일의 연방헌법재판소도 "사생활의 핵심영역에 영향을 미칠 수 있는 감시조치에 대한 법적 승인은 핵심영역과 관련된 데이터가 최대한 수집되지 않도록 보장해야 하고, … 핵심영역과 관련하여 발견 및 수집된 데이터는 즉시 삭제해야 하며, 해당 데이터의 사용은 제외되어야 한다"[1208] 고 판시하고 있음을 볼 수 있다.

따라서 온라인 수색을 헌법합치적 수단으로 구성하기 위해서는, 사생활의 핵심영역과 관련된 데이터를 수집대상에서 제외할 수 있는 기술적 수단을 활용해야 하며, 그럼에도 불구하고 데이터 수집과정에서 핵심영역에 속하는 데이터가 수집된 경우에는 즉시 삭제하도록 하는 입법적 조치가 취해져야 할 것이다. 이에 더하여 수집과정에서 핵심영역에 해당하는 데이터 여부를 확인하기 어려운 경우에는 수집 후 분석과정에서 핵심영역 데이터를 분리, 삭제하도록 규정하고, 이후 형사절차에서 증거로써 사용되는 것을 금지하도록 해야 할 것이다. 이와 관련하여 독일 형사소송법 제100d조 제3항의 규정을 보면 "온라인 수색으로 확보한 사생활의 핵심영역에 관한 정보는 지체없이 삭제하거나 검사로 하여금 수색을 명한 법원에 제출해 법원의 그 사용가능성과 삭제 여부를 결정할 수 있게 해야 한다"고 되어 있음을 볼 수 있다. 즉 온라인 수색에 수반되는 기본권 침해의 정도에 비추어 볼 때 사생활 보호를 위해서는 엄격한 이중적 보호장치를 두어야 한다는 것을 보여주는 것이라 할 수 있다.

라) 이중 통제 – 사법통제와 국회통제

온라인 수색은 수사상 강제처분이기 때문에 사법통제의 대상이 된다는 점은 명확하다. 따라서 사전에 법원에 영장을 청구하여 목적의 정당성, 수단의 적합성 및 필요성, 기간의 적정성 등에 대한 심사를 거쳐 발부된 영장에 의해서만 가능하다고 해야 할 것이다. 온라인 수색은 「통신비밀보호법」상 통신제한조치보다 기본권 침해의 정도가 크다고 할 수 있으므로, 독일과 같이 영장전담판사 단독으로 영장을 발부하기보다는 3명의 법관이 관여하는 합의부를 통해서 발부[1209]하도록 하는 것이 그 판단의 공정성과 합리성을 도모하는데 더 바람직하다고 할 것이다.

이와 같이 온라인 수색에 대해서는 영장주의 원칙에 의한 사법통제와 아울러 국회

1208) BVerfGE 120,274, Rn.277.
1209) StPO §100e(2).

에 의한 사후통제가 병행되어야 할 것으로 생각된다. 온라인 수색에 비하여 기본권 제한이 덜하다고 생각되는 「통신비밀보호법」상 통신제한조치의 경우를 보더라도 동법 제15조에 국회의 통제라는 규정을 두고, 국회 상임위원회와 국정감사 및 조사위원회로 하여금 통신제한조치에 관하여 보고를 요구할 수 있도록 규정하고 있다.[1210] 온라인 수색의 경우에 있어서는 이보다 좀 더 엄격한 요건에 입각한 사후 국회통제가 필요하다고 볼 수 있다. 즉 온라인 수색이 행해지는 경우, 해당 수사기관은 온라인 수색에 사용된 기술침입 시스템에 관한 정보, 온라인 수색 대상이 되는 정보통신 시스템에 관한 정보, 온라인 수색의 대상이 된 데이터의 유형과 범위, 기간 등 관련 정보를 분기별, 반기별 또는 연례보고서의 형태로 국회에 보고하도록 해야 할 것이다. 통신제한조치에 대한 국회통제가 특정사안 또는 국정감사나 조사 등 필요한 경우에 한 해 일회성으로 실시할 수 있는 통제라고 한다면, 온라인 수색에 대한 국회통제는 정기적인 의무이행을 담보할 수 있는 통제라고 할 것이다.

법원의 영장에 의한 사전통제가 온라인 수색의 정당성을 담보하기 위한 요건이라고 한다면, 국회에 의한 사후통제는 온라인 수색의 남용 가능성과 인권침해 등을 억제하기 위한 요건이라 할 것이다. 즉, 정보통신기술의 발달로 인해 범죄사실에의 접근을 불가능하게 하는 기술적 장애를 극복할 수 있는 수단으로서 온라인 수색을 허용함으로써 수사기관으로 하여금 국가와 공공의 안전, 국민들의 신체, 생명, 자유를 담보하기 위한 형사소추의 의무를 다할 수 있는 수단을 제공하되, 그로 인해 야기될 수 있는 국민들의 기본권 침해에 대한 우려와 국가에 의한 감시라고 하는 오남용의 가능성 등을 통제하기 위해서는 법원에 의한 사전통제와 국회에 의한 사후통제라는 이중적 통제장치를 두는 것이 실체적 진실의 발견이라고 하는 형사소송의 이념을 실현할 수 있는 규범적 장치로서 온라인 수색이 자리매김할 수 있는 방안이라 할 것이다.

1210) 「통신비밀보호법」 제15조 제1항.

디지털 증거 압수수색절차 개선을 위한 입법정책적 제언

탁 희 성

제5장

디지털 증거 압수수색절차 개선을 위한 입법정책적 제언

제1절 | 디지털 증거 압수수색에 관한 입법의 방향성

1. 실체적 진실발견과 프라이버시 보호의 균형

IT 기술에 기반한 기업들은 고객의 데이터를 기반으로 산업을 운영하게 되었고, 개인들은 IT 기반 서비스 기업들이 제공하는 네트워크를 이용하여 일상생활을 영위하면서 자신의 사적인 정보를 가상의 공간 안에서 생성, 저장, 관리하게 됨으로써 사회 전반에 걸쳐서 데이터는 정보화 사회의 필수재가 되었다. 이러한 정보화 사회에 있어서 국가 공권력의 강화는 기업뿐 아니라 개인들의 정보의 자유에 대한 큰 위협이 될 수 있다고 할 것이다. 따라서 IT 기업들은 강력한 개인정보보호 정책과 강화된 보안기술을 적용하게 되었으며, 개인들도 자신의 사적인 정보보호를 위해 디지털 기술 기반 서비스를 선택하는 주요 기준으로 정보보안기술의 적용 여부를 고려하게 되었다.[1211]

하지만 이와 같이 강화된 데이터 보안기술은 국가안보, 개인의 생명, 신체, 자유에 대한 중대하고도 긴급한 침해가 발생한 경우 또는 국민의 안전과 법률상 보호되는 법익에 대한 침해가 발생한 경우 수사에 장애를 유발하거나 경우에 따라서는 수사 자체를 불가능하게 만듦으로써 오히려 국민의 기본권과 공익이 침해되는 결과가 초래

1211) 우리나라의 경우에도 카카오톡에 대한 수사기관의 모니터링에 대한 우려, 카톡 먹통사태 등이 발생하면서 사생활 침해를 우려한 개인들이 대거 텔레그램 메신저로 전환하는 현상이 나타났다. 텔레그램의 모든 메시지는 강력한 암호화로 인해 보낸 사람과 받은 사람만 볼 수 있고, 기간 지정 시 메시지가 자동삭제될 뿐 아니라 서버에 기록이 남지 않는다.

하고 있다. 즉 정보화 사회에 있어서 디지털 기술은 양날의 검이라 할 수 있는 것이다.

이러한 문제는 비단 어느 한 국가만의 문제가 아니며 전 세계적으로 디지털 네트워크를 이용하여 행해지고 있는 각종 범죄문제를 해결하기 위한 방안을 고안하고 있다고 볼 수 있다. 그 대표적인 것이 유럽 사이버범죄 방지협약으로, 68개국이 협약당사국이며 23개국이 협약에 가입했거나 가입하도록 초대를 받았다.[1212]

국가는 범죄로부터 국민을 보호해야 할 의무와 국민의 기본권을 보호해야 할 의무를 모두 부담해야만 한다. 하지만 범죄로부터 국민을 보호하기 위한 형사소추의 의무를 다하기 위해서는 필요불가결하게 강제수사방식을 취할 수밖에 없는데, 이러한 강제수사는 국민의 기본권 침해를 전제로 하기 때문에 국가의 기본권 보호의무와 충돌할 수밖에 없다. 이와 같이 범죄문제로 인해 상충되는 국가의 두 의무 간의 균형을 잡아주는 것이 적법절차의 원칙 또는 적정절차의 원칙이라 할 것이다. 즉 형사소추의 효율성과 기본권 침해의 정도는 서로 반비례하기 때문에 적법절차 원칙에 의해 그 균형점을 찾도록 하는 것이 헌법적 형사소송의 기본원리라 할 것이다. 이러한 기본원리에 입각하여 그동안 「형사소송법」은 국가에 의한 강제수사로부터 국민의 기본권을 보호하기 위한 절차적 규정들을 지속적으로 마련해 왔다. 그런데 인터넷과 정보통신기술의 발전으로 인해 디지털 데이터가 범죄수사에 있어서 필수적으로 확보해야 하는 대상이 되면서 기존의 적법절차 규정들에 의해 유지되어 온 형사소추의 효율성과 기본권 침해 사이의 균형에 균열이 생기기 시작했다. 즉 수사대상이 되는 디지털 데이터의 존재양식 – 불가시성, 불가독성, 매체독립성 등 – 으로 인해 범죄 유관정보와 무관정보가 혼재되어 있고, 무관정보 가운데는 침해되어서는 안 되는 개인의 사적인 정보들이 포함되면서 강제수사로 인한 기본권 침해의 범위가 과거와 비교할 수 없을 정도로 확대되는 문제가 나타났다. 더욱이 정보통신기술이 발달할수록 개인들의 일상생활 대부분이 디지털화 되어가고 있기 때문에 점점 더 많은 사생활 관련 정보들이 디지털기기를 통해 접근가능한 상황에 놓이게 되었다. 이에 더하여 초연결 모바일 네트워크의 가속화로 네트워크 연결성이 급속히 확장되면서 시간과 장소, 사물의 제

1212) 이 협약은 인터넷 네트워크를 통해 이루어지고 있는 범죄 – 저작권침해, 인터넷 사기, 아동포르노, 네트워크 보안침해 등 – 에 대한 최초의 국제조약으로, 이러한 사이버범죄에 대응함에 있어서 필요한 일련의 수사절차와 정부기관의 권한 등에 관한 규정을 포함하고 있다(유럽평의회(Council of Europe) 홈페이지, "The Budapest Convention (ETS No. 185) and its Protocols" (https://www.coe.int/en/web/cybercrime/the-budapest-convention; 최종접속일 2023.10.10.)).

한 없이 정보의 무한한 확장과 유통이 가능해졌기 때문에, 수사의 목적으로 디지털 정보에 접근하고자 하는 유인이 훨씬 더 강해졌다고 볼 수 있다.

이와 같이 범죄와 관련한 실체적 진실에 접근함에 있어서 디지털 정보는 수사의 필수요소가 될 수밖에 없음에도 불구하고, 그 본질적 특성으로 인해 혐의사실과의 관련성 범위 내로 정보를 사전에 특정하는 것이 현실적으로 어려울 뿐 아니라 일반적으로 유관정보와 무관정보가 혼재되어 있기 때문에 의도치 않게 압수수색의 범위가 확대됨으로써 사적인 무관정보가 수사기관에 노출되는 현상이 발생하고 있다. 그로 인해 별건 혐의가 발견되어 제2의 압수수색영장이 발부되거나 전혀 다른 범죄의 단서가 되는 정보가 발견되는 등, 영장의 범위를 넘어서는 정보에 대한 압수수색의 문제가 발생했다. 즉 디지털 정보의 압수수색에 있어서는 불가피하게 압수수색의 불명확성이 수반될 수밖에 없고, 그로 인한 기본권 침해 역시 명확하게 제한하기 어려운 문제가 야기되었다. 더욱이 현재 디지털 정보 압수수색에 있어서 기본권 침해를 제한하기 위한 입법적 대응방안이 흠결되어 있는 입법 공백 상태이기 때문에 피압수자의 프라이버시와 기본권 보호를 위해 대법원은 기존의 유체물에 적용되어 왔던 적법절차 규정과 원칙들을 유추해서 적용하고 있다. 특히 디지털 정보의 압수수색 과정에서 사적인 정보의 노출과 그로 인한 기본권의 침해는 그 범위와 수준에 있어서 예측불가능하기 때문에, 대법원은 디지털 정보 압수수색에 있어서 적법절차 관련 규정과 원칙들을 이전의 유체물의 경우보다 더 엄격하게 적용하고자 하는 입장을 취하고 있을 뿐 아니라 점점 더 수사기관의 디지털 정보 압수수색 권한을 제한하는 방향으로 나아가고 있음을 볼 수 있다. 즉 참여권의 범위를 압수수색 현장에서 수사기관 내 디지털포렌식 과정으로까지 확대했을 뿐 아니라, 참여권의 주체 역시 실질적 피압수자라는 개념을 도입하여 피의자의 참여권 보장을 두텁게 하고 있다. 또한 적법절차적 수단 가운데 하나인 참여권을 「헌법」상 진술거부권과 동등한 권리로서 수용[1213]하고자 하고 있음을 볼 수 있다. 이외에도 디지털 정보에 대한 임의제출물 압수 시 임의성의 요건을 강화했을 뿐 아니라 영장에 의한 정보압수 절차와 동일한 절차적 요건을 준수하도록 요구하고 있다. 혐의사실과의 관련성 판단에 있어서도 동종의 유사한 범행이라 할지라도 혐의사실과 장소적, 시간적 근접성이 인정되는 구체적 개별적 연관관계

1213) 대법원 2015.7.16.자 2011모1839 전원합의체 결정에서 대법관 이인복, 이상훈, 김소영의 보충의견.

가 있는 경우에 한해서만 관련성을 인정하고 있다. 이와 같이 디지털 정보의 압수수색과 관련한 입법적 공백상황에서 초래될 수 있는 개인의 프라이버시와 기본권 침해의 가능성을 사법적 통제를 통해 제한하고자 함은 필요하고도 당연한 것이라 할 것이다.

이와 같이 대법원은 디지털 정보의 압수수색에 있어서 프라이버시와 기본권 보호에 관한 절차적 통제에 중점을 둠과 아울러 실체적 진실의 발견은 기본권 보호를 위한 적법절차를 위해 포기될 수도 있다는 입장을 제시한 바 있다.[1214] 즉 디지털 정보의 압수수색에 있어서는 실체적 진실의 발견과 적법절차 원칙의 조화와 균형보다는 적법절차 원칙이 우선하는 가치가 될 수 있다고 보고 있는 것이다. 물론 정보화 사회에 있어서 디지털 정보가 갖는 가치와 중요성에 비추어 볼 때, 수사기관에 의한 디지털 정보의 압수로 인해 침해될 수 있는 법익의 침해가능성이 결코 적지 않을 수 있다는 점은 분명하다고 할 수 있다. 하지만 여기서 고려되어야 할 중요한 문제가 있다. 즉 디지털 기술의 고도화는 개인으로 하여금 자신의 정보를 보호할 수 있는 강력한 수단으로 암호화 기술을 활용할 수 있도록 하고 있다는 것이다. 뿐만 아니라 스마트기기를 생산하는 업체들도 보다 강화된 보안기능을 지속적으로 업데이트하고 있으며, 익명성과 암호통신기술이 적용된 텔레그램이나 다크웹 등은 추적이 어려울 뿐 아니라 블록체인 기술을 활용한 가상화폐가 더해지면서 용이하게 범죄를 은폐할 수 있는 네트워크 환경이 구축되어 있다고 볼 수 있다.

이는 과거와 같은 수사기관의 압수수색 방식으로는 디지털 범죄의 실체에 접근하는 것이 현실적으로 매우 어렵다는 것을 의미하는 것으로, 수사기관이 피압수자로부터 정보저장매체 또는 디지털 정보 자체를 확보한다고 하더라도 암호화되어 있거나 삭제 또는 은닉되어 있는 경우 피압수자는 수사기관의 압수수색에 대응할 수 있는 방어수단을 확보하고 있는 것이라 할 수 있다. 즉 현행범체포 시 수반되는 디지털기기 압수를 제외하고는 일반적인 압수수색영장 발부 시 집행 전에 해당 기기를 초기화하거나 용이하게 구할 수 있는 안티포렌식 프로그램을 이용해서 저장된 정보를 삭제하는 방식, 특별한 암호 알고리즘을 이용하여 데이터를 암호화하는 등으로 데이터를 은닉하는 방식, 사법권한이 미치지 않는 해외 서버에 데이터를 저장하고 다크웹 등을 이용하는 방식 등으로 개인의 정보에 대한 수사기관의 접근 자체를 무력화시키는

1214) 대법원 2015.7.16.자 2011모1839 전원합의체 결정에서 대법관 이인복, 이상훈, 김소영의 보충의견.

것이 가능해졌기 때문에, 디지털 정보 압수수색에 있어서는 피압수자의 기술적 방어를 통해 정보를 보호할 수 있다. 뿐만 아니라 유체물의 압수수색의 경우 「형사소송법」 제120조에 규정된 필요한 처분을 통해 개봉이나 시건장치를 열어서 관련 증거를 확보할 수 있었지만, 디지털 정보의 경우 압수수색에 필요한 처분이라 할 수 있는 계정정보를 제공하도록 하는 것은 「헌법」상의 진술거부권과 자기부죄거부특권에 반하는 것이 되어 그 자체가 위법행위가 된다는 문제가 있기 때문에 법률상 방어를 통해서도 자신의 정보를 보호할 수 있는 것이다.

이 경우 수사기관 스스로 암호화되어 있거나 삭제 또는 은닉된 정보에 접근할 수 있는 기술적 수단을 확보해야 하는데, 현실적으로 수사기관이 디지털기기 생산업체 또는 정보통신기술 기반 서비스 업체에서 제공하는 암호 내지 보안기술 보다 더 우월한 기술을 갖는 것은 불가능하다고 볼 수 있다. 더욱이 디지털기기 생산업체의 경우 기술보안이 기업의 생명이라 할 수 있고, 마찬가지로 디지털기술 기반 서비스업체도 정보보안이 기업의 생명이기 때문에 수사기관에 관련 기술의 제공이나 협조를 기대하기는 어려우며, 특히 해외에 소재하는 기업의 경우에는 사실상 불가능하다고 볼 수 있다. 유럽의 사이버범죄방지협약도 이와 같이 디지털 범죄와 관련한 수사에의 어려움을 극복하기 위해 보전명령, 제출명령, 원격지 압수수색, 데이터 감청 등과 같은 수사방식을 도입했으며, 이후 제2 추가의정서를 통해 도메인 등록정보에 대한 요청, 타국 인터넷 서비스제공자에 대한 가입자 정보제공요청, 공조요청 국가의 가입자 정보와 트래픽 데이터 제출명령에 대한 타국에서의 강제력 부여, 긴급상황에서의 공조절차 등을 마련할 것을 합의하고 있음을 볼 수 있다.[1215] 이와 달리 현재 우리의 경우 디지털 정보의 확보와 관련한 수사절차상의 한계를 극복할 수 있는 입법적 대응이 전혀 마련되어 있지 않다는 점을 고려해야만 한다.

이와 같이 디지털 정보의 소유자인 피의자 또는 ISP나 OSP, 디지털기기 생산업체의 협력 없이는 암호화된 정보에 접근하는 것 자체가 어려운 환경으로 인해 혐의사실과 관련한 실체적 진실을 발견하거나 접근하는 것이 현실적으로 어려운 상황에 있다고 볼 수 있다. 그럼에도 불구하고 디지털 정보의 압수수색에 있어서 개인의 프라이버시

1215) "협력 및 전자적 증거 개시 강화에 관한 사이버범죄방지협약 제2 추가의정서"(Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence) 원문(https://rm.coe.int/1680a49dab; 최종접속일 2023.10.28.).

와 기본권 침해 가능성만을 강조하게 되면 범죄혐의에 대한 실체적 진실에 접근하고자 하는 수사방식에 대한 통제를 우선하게 될 수밖에 없다고 할 것이다.

하지만 적법절차의 범위 내에서 실체적 진실의 발견이 가치가 있다고 하기 위해서는 그 전제로서 디지털 범죄에 대응할 수 있는 적법절차가 마련되어야 한다고 할 것이다. 이미 물리적 장소와 유체물에 기반한 환경에서 초연결 모바일 네트워크로 구축된 정보화 환경으로 바뀌었음에도 불구하고 기존의 적법절차 규정만으로 범죄에 대응하고자 하는 것은 불합리할 뿐 아니라 오히려 범죄의 안전지대를 확보해 주는 결과를 초래할 수 있다는 우려를 배제하기 어렵다고 할 것이기 때문이다. 디지털 정보에 대한 압수수색으로 초래되는 개인의 프라이버시와 기본권에 대한 침해 못지않게 초연결 모바일 네트워크를 이용한 범죄로 야기되는 타인의 자유와 권리, 더 나아가 신체와 생명에 이르는 피해가 과거 물리적 환경 내에서의 피해와는 비교되지 않을 정도로 크다는 것도 충분히 고려될 필요가 있다고 할 것이다.

이와 같이 IT 기술이 고도화될수록 정보통신기술과 네트워크를 이용한 범죄행위에 대한 형사소추의 가능성이 현실적으로 제약을 받을 수밖에 없다는 한계에 직면하고 있다는 점을 고려해 볼 때, 디지털 정보의 압수수색의 적정성을 담보함에 있어서는 개인의 프라이버시와 기본권 보호에 있어서 실체적 진실의 발견과 균형을 이룰 수 있는 사법적 관점과 입법적 정비가 필요하다고 할 것이다.

2. 공판절차와 수사절차 규정의 분리

현행 「형사소송법」의 체계를 살펴보면, 형사절차가 진행되는 순서대로 규정된 것이 아니라 제1편 총칙에 형사절차 전반에 걸쳐 수사와 공판에 공통된 규정들이 마련되어 있으며, 제2편 제1심의 제1장에 수사에 관한 규정들이 있다. 즉 제1심에 수사절차 관련규정이 포함됨으로 인해 수사절차가 공판절차의 예비절차로 보여지는 측면이 있다.[1216] 이러한 입법방식은 소추와 재판이 분리되지 않고, 강제처분에 대한 권한을 법원 내지 예심판사가 갖고 있던 과거의 소송구조하에서 가능했던 것[1217]이라 할

1216) 이승현 외 5인, 『형사소송법 편장체계 개편방안 연구 -수사절차를 중심으로-』, 연구총서 19-BB-03, 한국형사정책연구원, 2019.12, 75면.

1217) 형사소송법 개정특별위원회, 『형사소송법 개정연구』, 연구총서 10-14, 한국형사정책연구원, 2010.12, 43면.

수 있다. 따라서 현재와 같이 공판절차의 주체와 수사절차의 주체가 분리되어 있는 형사사법체계와는 맞지 않는 입법체계임에도 불구하고, 수사절차에 대한 사법통제의 중요성을 강조하는 법원은 여전히 수사절차는 법원의 권한 내에 있어야 하는 것으로 인식함에 따라 과거의 소송구조의 정당성을 여전히 주장하고 있다. 이러한 법원의 인식은 최근 들어 압수수색영장 사전심문제도의 도입, 전자증거 압수수색영장 청구 시 검색어 제한 등과 같이 사실상 수사지휘라고 할 수 있는 법체계를 도입하고자 하는 시도 등에서도 나타나고 있음을 볼 수 있다.

이와 같이 현행 「형사소송법」은 수사절차에 관한 편장체계를 공판절차에 귀속시켜 놓았을 뿐 아니라, 수사절차에 관한 규정들 역시 수사절차가 아닌 공판절차에 규정하고, 이를 다시 수사절차에 준용하는 방식을 취함으로써 공판과 수사가 동일한 절차를 거치는 것으로 보여지는 측면[1218]이 있을 뿐 아니라 법원이 수사의 주체로 인식되어지기도 한다. 또한 수사절차에 관한 규정의 주체가 법원으로 규정되어 있기 때문에 실제 수사를 담당하는 수사기관에게 해당 규정을 준용하도록 하기 위해서는 절차상 주체와 객체를 변환해서 재해석해야 함으로 인해, 명확한 법규정에 의한 사법통제가 아니라 법원의 해석에 의한 사법통제 방식으로 이루어지고 있다고 볼 수 있다.

즉 현행 「형사소송법」은 수사절차에 관한 광범위한 준용규정으로 인해 조문내용이 명확히 인지되지 못할 뿐 아니라, 준용규정이 있음에도 불구하고 특정 조문[1219]의 경우에는 수사절차에 적용되지 않는다고 해석하는 등 포괄적 준용규정으로 인한 입법체계와 수사절차의 부조화 문제가 발생하고 있는 것이다. 특히 강제수사절차와 관련한 포괄적 준용규정의 경우 명확성의 원칙에 부합한다고 보기 어려울 뿐 아니라, 공개주의를 원칙으로 하는 공판절차와 밀행성을 기본으로 하는 수사절차의 근본적인 차이를 무시한 것으로 실정법과 법현실 간의 괴리를 오히려 심화시키고 있다고 볼 수 있다. 그 예로 과거 시간과 공간이 제한된 형태의 범죄구조를 기본으로 하는 수사절차에서 시공의 제한없이 범죄의 무한 재확산이 가능한 디지털 환경에 부합하는 수사절차로의 전환이 이루어져야 함에도 불구하고, 법원을 주체로 하는 수사규정을 고수함으로써 디지털 정보와 관련한 범죄수사에 실효적으로 대응하지 못하는 문제들이 야기되고 있다고 볼 수 있다.

1218) 이승현 외 5인, 위의 연구보고서, 75면.
1219) 「형사소송법」 제106조 제2항.

이 외에도 수사절차에 관한 규정의 대부분이 공판절차에 규정되어 있기 때문에 현실적으로 수사기관에 적용되어야 할 수사절차들에 관한 새로운 규정들이 있어도 현행법상 공판절차에 관한 규정으로 포섭하는 것은 불가능하다. 따라서 수사절차에 적용되어야 하는 적법절차 관련 규정들이 「형사소송법」이 아닌 하위법령이나 수사기관 내부 예규로 규정되는 경우가 대부분이라 할 수 있다. 따라서 하위법령에 규정된 수사절차로 인하여 기본권 침해의 우려가 있는 경우라 할지라도 적법절차적 통제에 한계가 있을 수밖에 없다고 할 것이다. 더욱이 과학기술의 발달에 따른 새로운 수사기법의 필요성에 직면하게 되는 경우, 수사상 필요에 입각하여 수사기관의 내부 규정 등을 통해 활용되는 경우 그 적법성 여부는 물론이고 그로 인한 기본권 침해 여부를 판단하기 어렵게 되고, 이는 국민들의 자유와 권리를 침해하는 결과를 초래할 수 있다는 점에서 결코 바람직하지 않다고 할 것이다. 이와 같이 형사절차 법률주의와 강제처분 법정주의가 적용되어야 하는 수사절차에 있어서 법률로 규율되어야 할 수사방법들이 「형사소송법」의 체계상의 한계로 인해 규정되지 못한다는 것은 형사절차의 이념인 적법절차의 원칙이 「형사소송법」을 통해 제대로 구현될 수 없다는 것을 의미한다고도 볼 수 있다.

이와 같이 형식적 체계에서뿐 아니라 내용적 체계에 있어서도 그 한계를 나타내고 있는 현행 「형사소송법」의 문제를 제대로 인식하고, 그 체계와 구성을 형사절차의 흐름에 맞게 재정비해야 할 필요가 있다고 할 것이다. 따라서 형사절차의 기본적인 흐름, 즉 '수사 - 기소 - 공판 - 상소 - 형집행'의 순서로 조문을 배열하는 것이 합리적일 뿐 아니라 일반 국민들이 형사절차의 체계를 이해하는 데도 도움이 될 수 있다고 할 것이다.[1220] 그리고 이를 통해 수사절차와 공판절차에 관한 규정들을 분리하여 규정하고, 준용규정이 아닌 직접규정을 통해 수사절차를 규율하는 것이 오히려 수사절차의 적정성과 사법통제의 가능성을 확보하는 데 보다 더 실효적이라 할 수 있을 것이다.

1220) 형사소송법 개정특별위원회, 앞의 연구보고서, 27면.

제2절 | 디지털 증거 압수수색을 위한 입법적 개선방안

1. 디지털 증거에 부합하는 현행 압수 규정 개선

가. 압수대상으로서 정보의 적법성 확보와 압수개념의 재정립

현행 「형사소송법」상 디지털 증거 압수에 관한 규정은 제106조와 제215조로 다음과 같다.

> **제106조 (압수)** ① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다.
> ③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)인 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.
>
> **제215조** (압수, 수색, 검증) ① 검사는 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 지방법원판사에게 청구하여 발부받은 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.
> ② 사법경찰관이 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 검사에게 신청하여 검사의 청구로 지방법원판사가 발부한 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.

디지털 증거 압수에 관한 논의에 있어서 가장 기본적인 전제가 되는 것이 디지털 정보에 대한 압수 여부라고 할 수 있다. 형사절차상 디지털 정보에 대한 압수의 필요성이 제기되었던 2000년대 초부터 가장 먼저 문제가 제기되었던 것이 압수의 대상으로서 디지털 정보의 포섭 가능성 여부였다. 현행 「형사소송법」상 압수규정은 유체물을 전제로 규정된 것이었기 때문에 정보저장매체가 아닌 정보 그 자체에 대한 압수규정으로서는 부적합하다고 볼 수 있다.

이와 관련하여 대법원 2011.5.26.자 2009모1190 결정에서 정보저장매체가 아닌 디지털 정보 자체가 압수대상임을 전제로 하는 선별압수 원칙을 제시[1221]하였고, 이후 2011년 7월 18일 「형사소송법」 제106조 제3항을 신설하여 '선별압수 원칙, 매체압

수 예외'를 규정하게 되었다. 하지만 동 규정은 디지털 정보에 대한 압수의 절차와 방법에 대한 규정일 뿐 압수대상으로서 디지털 정보 그 자체가 포섭됨을 명시적으로 규정한 것은 아니었기 때문에 압수대상으로서 디지털 정보의 적법성 여부의 문제는 여전히 현재 진행형이라 할 수 있다. 동 규정이 제정되었던 당시 디지털 정보 자체에 대한 압수문제 관련 논의가 크지 않았던 이유는 당시의 디지털 기술 수준에 있어서는 매체와 분리된 정보를 상정할 필요가 없었던데 있었다고 할 수 있다. 즉 당시에는 디지털 정보의 특성상 매체종속성을 전제로 한다고 볼 수 있었기 때문에 매체 압수와 정보압수를 분리하여 논할 실익이 적었다고 볼 수 있다.

하지만 디지털 기술에 기반한 IT 산업이 고도화되고, 데이터 자체가 정보화 사회의 필수재(必須財)가 되면서 디지털 정보의 본질적 속성이 매체독립성이라는 점을 인식하지 않을 수 없게 되었다. 이와 같이 무체성에 기반한 디지털 정보 자체를 압수수색의 대상으로 해야 함에도 불구하고 현행법은 유체물에 기반한 규정을 둠으로 인해 현실과 법 사이의 괴리현상이 생길 수밖에 없는 것이다. 대법원이 판례를 통해 압수영장 집행의 완료시기를 수사기관 내 디지털포렌식 과정으로까지 확대한 것도 최종적으로 혐의사실과의 관련성을 토대로 분석과정을 거쳐 정보를 확보하는 단계에서 압수절차가 완료되는 것으로 보았기 때문이고, 이는 압수의 대상이 매체가 아닌 정보라는 전제하에서만 가능한 해석이라 할 수 있다. 즉 정보가 압수의 대상이라는 것을 법이 아닌 판례의 해석을 통해서 명확히 하고 있는 것이다. 또한 압수물 목록 교부에 있어서도 압수한 전자정보의 상세한 목록을 기재하도록 하는 것 역시 압수의 대상이 정보라는 사실을 판례를 통해 제시하고 있는 것을 볼 수 있다. 이는 압수수색의 대상으로 정보가 명시적으로 규정되지 못하고 있는 입법적 흠결상황을 판례가 대신하고 있는 것이라 할 수 있다.

초연결 모바일 네트워크 기술의 발달로 정보이용방식이 변화하고 있고, 매체 자체는 정보에 접근하기 위한 하나의 문(gate)에 불과할 뿐, 매체 내에 정보가 존재하지 않는 경우가 일반적 형태가 되어가고 있기 때문에[1222], 법률상 압수의 대상은 정보 그 자체로 규정하는 것이 법현실에 부합한다고 할 것이다.

1221) 박병민·서용성, 앞의 연구보고서, 223면.

1222) 최용성·강동욱, "현행 디지털 증거제도 입법화 방안 연구", 『치안정책연구』 제34권 제3호, 경찰대학 치안정책연구소, 2020.9, 79면.

다음으로 수사절차상 범죄혐의에 대한 입증수단으로서 디지털 정보를 확보하는 것을 압수라는 기존의 개념으로 포섭할 수 있는가에 대해서도 논의할 필요가 있다고 할 것이다. 압수란 점유의 취득을 전제로 하는 개념, 즉 제로섬으로서 의미를 갖는 것인데 비해 디지털 정보는 비이전성을 그 특성으로 하기 때문에 점유의 취득이라고 하는 개념과는 본질적으로 맞지 않는다. 즉 디지털 정보에 대해서는 수사상 강제처분으로서 이를 확보할 수는 있지만 그것이 기존의 압수와 같은 점유취득의 방법이 아니더라도 압수목적으로 디지털 정보의 확보가 가능하다는 점을 인식할 필요가 있다. 따라서 디지털 정보를 강제수사의 방식으로 확보함에 있어서는 압수와는 다른 개념으로 접근해야 하고, 이를 법률상 어떻게 수용할 것인가에 대해서도 논의할 필요가 있다고 본다.

현행「형사소송법」제106조 제1항의 압수대상에 정보를 포섭시킴으로써 증거방법으로서 정보의 법적 지위를 명문화하는 것도 필요하지만, 그와 함께 유체물에 기반을 둔 압수와 별개로 무형의 정보인 디지털 증거에 대한 수사상 강제처분 방식에 적합한 개념을 도입하는 것도 압수와 디지털 증거 간의 개념적 이질성에서 비롯되는 해석상의 논란을 해소하는 하나의 방안이 될 수 있다고 본다.

이와 같이 압수수색의 대상으로서 디지털 정보에 대한 법적 근거를 마련할 필요성이 있다는 점에 대해서는 그동안 지속적으로 논의되어 왔고, 입법안도 꾸준히 발의되어 왔었다.

먼저 국회에 발의되었던 입법안들을 정리하여 보면 다음과 같다.

제안일자	의안번호	대상조문	개정(신설) 내용
2015-02-02	1913878	§106 ③ 개정	제1항의 증거물 또는 물건에는 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 "정보저장매체등"이라 한다)에 기억된 정보도 포함된다.
2016-08-02	2001352	§106 ③ 개정	제1항의 증거물 또는 물건에는 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 "정보저장매체등"이라 한다)에 기억된 정보도 포함된다.
2021-08-18	2112092	§106 ③ 개정	제1항의 증거물 또는 물건에는 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 "정보저장매체등"이라 한다)에 기억된 정보(이하 "전자정보"라 한다)도 포함된다.
2022-01-07	2114302	§106 ③ 개정	제1항의 증거물 또는 물건에는 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 "정보저장매체등"이라 한다) 또는 정보저장매체 등에 기억된 정보도 포함된다.

다음으로는, 관련 논문과 보고서 등에서 제시되었던 입법안들을 정리하여 보면 아래와 같다.

연도	저자 및 논문	대상조문	개정(신설) 내용
2020	차종진, "디지털증거법제의 발전동향과 입법과제"[1223]	§106① 개정	① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건 또는 전자정보를 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다.
2020	정성남, "경찰 수사현장에서 디지털 증거의 압수·수색에 관한 연구"[1224]	§106① 개정	① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건 및 디지털 정보를 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다.
2020	최용성·강동욱, "현행 디지털 증거제도 입법화 방안 연구"[1225]	§106① 개정	법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물이나 몰수할 것으로 사료되는 물건 또는 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)에 기억된(=digital) 정보를 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다.

이와 같이 국회에 발의된 입법안과 논문 등에서 제시된 입법안 모두 현행법 제106조 개정을 통해 디지털 정보를 압수의 목적물로 포섭하고자 하고 있음을 볼 수 있다. 즉, 동 규정 제1항에 압수의 대상으로서 전자정보를 명시하게 되면 제3항의 정보의 압수방법에 관한 규정과도 보다 논리적으로 연결된다고 볼 수 있다. 즉 관련성 있는 정보의 압수가 원칙이지만, 매체를 압수해야 하는 경우에는 정보의 범위를 정하여 압수하도록 제한함으로써 매체압수로 인한 정보에 대한 포괄압수의 위험성을 배제할 수 있다고 할 것이다.

「형사소송법」 편장체계의 개선 없이 현행법 규정 내에서 정보압수를 명문화하고자 하는 경우에는 제106조의 압수규정을 개정하는 것이 최선이라 할 것이다. 하지만 앞서 기술한 바와 같이 「형사소송법」의 편장체계에 있어서 수사절차와 공판절차를

1223) 차종진, 『디지털증거법제의 발전동향과 입법과제』, 책임연구보고서 2020-09, 치안정책연구소, 2021.5, 104면.
1224) 정성남, "경찰 수사현장에서 디지털 증거의 압수·수색에 관한 연구 -스마트 폰을 중심으로-", 박사학위논문, 인천대학교, 2020.2, 206면, 각주 558.
1225) 최용성·강동욱, 앞의 논문 97면.

분리함으로써 체계의 합리성을 도모하고자 한다면 제106조의 개정과 함께 제215조의 개정도 동시에 이루어져야 할 것으로 생각한다.

따라서 본 보고서에서는 다음과 같은 개정안을 제시해 보고자 한다.

제106조 (압수) ① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 생각되는 물건 또는 전자정보를 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다.

제215조 (압수, 수색, 검증) ① 검사 또는 사법경찰관은 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할만한 정황이 있고 해당사건과 관계가 있다고 인정할 수 있는 것에 한하여 피의자의 물건 또는 전자정보를 지방법원 판사가 발부한 영장에 의하여 압수할 수 있다.
② 검사 또는 사법경찰관은 압수의 목적물이 컴퓨터용 디스크, 기타 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 정보저장매체 등을 압수할 수 있다.

나. 디지털 증거 압수수색에 있어서 참여권 규정의 개정

현행 「형사소송법」상 압수수색 영장집행 시 참여에 관한 규정은 제121조와 제123조로, 다음과 같다.

제121조 (영장집행과 당사자의 참여) 검사, 피고인 또는 변호인은 압수·수색영장의 집행에 참여할 수 있다.

제123조 (영장의 집행과 책임자의 참여) ① 공무소, 군사용 항공기 또는 선박·차량 안에서 압수·수색영장을 집행하려면 그 책임자에게 참여할 것을 통지하여야 한다.
② 제1항에 규정한 장소 외에 타인의 주거, 간수자 있는 가옥, 건조물(建造物), 항공기 또는 선박·차량 안에서 압수·수색영장을 집행할 때에는 주거주(住居主), 간수자 또는 이에 준하는 사람을 참여하게 하여야 한다.
③ 제2항의 사람을 참여하게 하지 못할 때에는 이웃 사람 또는 지방공공단체의 직원을 참여하게 하여야 한다.

참여권 조항은 종래 압수수색의 적법성 통제와 관련하여 논의된 적이 거의 없었던 규정이라 할 수 있다. 그런데 2015년 대법원이 전원합의체 결정으로 디지털 증거 압수수색에 대한 절차적 통제수단으로서 참여권을 보장하지 않으면 압수수색절차

전체가 위법하다고 판시함으로써 막강한 규범력을 부여하였다.[1226]

이와 같이 참여권 규정이 디지털 증거 압수수색에 있어서 특히 문제가 되는 것은 형식적 압수대상인 정보저장매체의 점유 및 보관자와 실질적 압수대상인 정보의 소유자가 서로 다른 경우가 있을 뿐 아니라 피의자와 실질적 압수대상인 정보의 소유자가 서로 다른 경우가 있는 데서 비롯되는 문제라 할 수 있다.

정보의 압수 시 법원이 압수영장의 별지를 통해 정보압수의 범위를 제한한다고 하더라도 압수대상이 되는 정보를 구체적으로 특정하는 것은 현실적으로 불가능하기 때문에 어느 정도 포괄압수에 대한 우려를 배제하기 어렵다고 할 수 있다. 따라서 대법원은 정보에 대한 포괄압수 내지 과잉압수에 대한 우려를 배제하기 위한 통제수단으로서 참여권의 중요성을 강조하고 있다고 볼 수 있다. 이에 더하여 대법원은 참여권의 범위를 압수수색의 현장을 벗어나 수사기관 내 사무실에서의 관련증거 선별과정 절차로 확장시킴으로써, 다양한 정보가 혼재된 채 수사기관으로 이전되는 데서 비롯되는 기본권 침해 가능성을 배제함과 아울러 압수의 적정성을 확보하고자 하고 있음을 알 수 있다.

다만 대법원이 참여권을 디지털 증거 압수수색절차의 적법성을 담보하기 위한 필수적 요건으로 보고 있다는 점을 피의자측에서 악용하여 수사진행을 방해하는 경우도 발생하고 있음을 볼 때, 디지털 증거 압수수색절차의 적법성을 담보할 수 있는 참여권 규정에 대한 입법적 개선이 필요하다고 할 것이다.

먼저 압수수색 집행과정에서 참여권 보장과 관련하여 국회에 발의된 입법안은 다음과 같다.

제안일자	의안번호	대상조문	개정(신설) 내용
2014-12-08	1912877	§122 개정	압수수색 영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단, 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 때 또는 피고인이 증거를 인멸, 은닉, 위조 또는 변조하는 것이 가능하여 압수수색이 실효를 거두기 어려운 때에는 예외로 한다.
2015-02-02	1913878	§115조의3 신설	① 제115조의2 제2항에 따라 정보저장매체등을 압수함으로써 집행을 종료한 때에는 해당 사건과 관계가 있다고 인정할 수 있는 정보에 한정하여 이를 출력 또는 복제하여야

1226) 박병민·서용성, 앞의 연구보고서, 251면.

제안일자	의안번호	대상조문	개정(신설) 내용
			한다. ② 제1항의 경우 정보저장매체 등에 기억된 정보와 해당사건과의 관련성을 판단하기 위해 필요한 때에는 그 정보의 전부 또는 일부를 다른 저장매체로 복제하거나 열람할 수 있다. 이 경우 다른 저장매체로 복제된 정보 중에서 해당 사건과의 관련성이 없다고 인정되는 정보는 그 정보의 소유자, 소지자 또는 보관자에게 반환하거나 이를 폐기하여야 한다. ⑤ 피의자, 변호인 또는 제129조에 규정한 자는 제1항 및 제2항의 과정에 참여할 수 있다.
2016-08-02	2001352	상동	상동
2019-01-28	2018366	§121② 신설	제1항에도 불구하고 압수수색의 목적물이 「전자문서 및 전자거래기본법」제2조 제1호에 따른 전자문서인 경우에는 같은 법 제2조 제3호의 작성자 및 제4호의 수신자, 피고인(이하 이 조에서는 "작성자등"이라 한다)을 압수수색영장의 집행에 참여시켜야 한다. 다만, 다음 각호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. 1. 작성자등이 명시적으로 참여거부의사를 표현한 경우 2. 작성자등의 인적사항이 불명확하거나 소재불명 또는 그 밖에 이에 준하는 사유로 인하여 압수수색 집행에 참여시키기 어려운 경우
2021-08-18	2112092	§121② 신설	검사, 피고인 또는 변호인은 정보저장매체의 반출·복제·탐색, 전자정보의 복제·출력에 이르는 전자정보에 대한 압수영장의 집행에 참여할 수 있다.
2022-01-07	2114302	§115조의3 신설	① 제115조의2에 따라 정보 또는 정보저장매체등을 압수한때에는 해당 사건과의 관련성을 인정할 수 있는 정보에 한정하여 이를 출력 또는 복제하여 압수하여야 한다. ② 제1항의 경우 정보저장매체 등에 기억된 정보와 해당사건과의 관련성을 판단하기 위해 필요한 때에는 그 정보의 전부 또는 일부를 다른 저장매체로 복제하거나 열람할 수 있다. 이 경우 다른 저장매체로 복제된 정보 중에서 해당 사건과의 관련성이 없다고 인정되는 정보는 그 정보의 소유자, 소지자 또는 보관자에게 반환하거나 이를 폐기하여야 한다. ⑤ 피의자, 변호인 또는 피고인이 지정한 자는 제1항 및 제2항의 과정에 참여할 수 있다.

압수수색절차에 있어서 참여권 보장과 관련하여 국회에 발의되었던 입법안을 보면, 현행 규정인 제121조에 제2항을 신설하여 대법원이 제시한 전자정보의 탐색, 복제, 출력과정까지 참여를 인정하는 방식, 그리고 제115조의3을 신설하여 제106조 제3항에 규정된 전자정보에 대한 압수방법을 동조로 이전함과 아울러 그러한 압수과정, 즉 출력 또는 복제, 열람 과정에의 참여를 인정하는 방식이 있다. 이 외에도 제121조

제2항을 신설하여 압수의 목적물이 전자문서인 경우에는 전자문서의 수신자와 피의자에 대하여 참여권을 의무적으로 보장하는 안이 발의된 바 있다.

다음으로, 논문과 보고서 등에서 참여권과 관련하에 제안된 입법안의 내용은 아래와 같다.

연도	저자 및 논문	대상조문	개정(신설) 내용
2022	황성민, "디지털증거 압수·수색 관련 최근 판례 동향 -스마트폰에 대한 긴급 압수·수색에 있어서의 제문제 등-"[1227]	§122 개정	압수·수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단, 전조에 규정한 자가 참여하지 아니한다는 의사를 명시하거나 참여 일정을 고의로 지연시키는 등의 특별한 사정이 있는 경우 또는 급속을 요하는 때에는 예외로 한다.
2021	박병민, "디지털 증거 압수수색의 절차적 규제 개선방안 -참여권 강화, 영장 사본 교부제도 도입 등-"[1228]	§121 개정	검사, 피고인, 변호인 또는 제129조에 규정된 자는 압수·수색영장의 집행에 참여하여 의견을 진술할 수 있다.
		§122 단서 개정	① 압수·수색영장을 집행함에는 미리 집행의 일시 와 장소를 전조에 규정한 자에게 통지하여야 한다. 다만 다음 각 호의 경우에는 예외로 한다. 1. 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 때 2. 통지가 불가능하거나 현저히 곤란한 때 3. 증거 인멸의 우려가 있는 때 ② 제1항 단서의 사유가 해소된 때에는 전조의 규정 한 자에게 즉시 통지하여야 한다.
2021	박병민·서용성, "디지털 증거 압수수색 개선방안에 관한 연구 -법률 개정에 관한 논의를 중심으로-"[1229]	§121 개정	검사, 피고인, 변호인 또는 제129조에 규정된 자는 압수·수색영장의 집행에 참여하여 의견을 진술할 수 있다.
		§122 단서 개정	① 압수·수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 다만 다음 각 호의 경우에는 예외로 한다. 1. 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 때 2. 통지가 불가능하거나 현저히 곤란한 때 3. 증거 인멸의 우려가 있는 때 ② 제1항 단서의 사유가 해소된 때에는 전조의 규정한 자에게 즉시 통지하여야 한다.

1227) 황성민, "디지털증거 압수·수색 관련 최근 판례 동향 -스마트폰에 대한 긴급 압수·수색에 있어서의 제문제 등-"(발표문), 『디지털증거 압수수색 관련 최근 동향』, 2022년 한국형사소송법학회 추계 학술대회, 2022.9.16, 134면.

1228) 박병민, "디지털 증거 압수수색의 절차적 규제 개선방안 -참여권 강화, 영장 사본 교부제도 도입 등-"(발표문), 『디지털증거 압수수색 개선방안』, 2021 공동학술대회(사법정책연구원·대한변호사협회·한국형사법학회·대법원 형사법연구회 공동주최), 2021.3.26, 11면.

1229) 박병민·서용성, 앞의 연구보고서, 261면.

논문 등에서 참여권과 관련하여 제안된 입법안들의 경우 현행법에 규정된 참여권 통지 예외사유인 '급속을 요하는 때'가 수사기관의 재량적 판단을 가능하게 함으로써 참여권자의 참여기회를 배제하는데 남용될 수 있다는 전제하에, 고의지연, 증거인멸의 우려, 통지불능 등과 같이 보다 구체화 된 예외사유를 규정하고 있음을 볼 수 있다. 즉 참여권에 대한 사전통지가 참여권 보장의 전제조건이 되기 때문에 통지예외사유를 보다 명확하게 규정하는 것이 중요하다고 할 수 있다. 다만 제안된 입법안 가운데 고의지연의 사유는 사전통지 단계에서는 고의지연 의도 등을 파악하는 것이 현실적으로 불가능하기 때문에 오히려 참여권 배제사유에 해당한다고 보는 것이 더 적합하다고 볼 수 있을 것이다.

그리고 참여권자의 범위에 「형사소송법」 제129조에 규정된 자들을 포함함으로써 소유자, 소지자, 보관자, 기타 이에 준할 자까지 참여권이 보장되도록 하고 있으며, 참여의 기회에 의견을 진술할 수 있도록 하는 규정을 두어 압수수색절차의 적법성 여부에 대한 항고사유를 보다 구체적으로 적시할 수 있도록 하고 있음을 볼 수 있다.

디지털 증거 압수수색에 있어서 참여권과 관련하여 입법적 개선이 요구되는 부분은 대법원이 제시하고 있는 바와 같이 압수수색 현장 외에서의 전자정보의 복제, 탐색, 출력과정에 있어서 참여기회의 보장과 피압수자는 아니지만 압수대상 정보의 실질적 주체인 피의자에 대한 참여권 보장이라고 할 수 있다. 대법원이 '실질적 피압수자'라는 개념까지 사용하여 압수대상 정보주체인 피의자의 참여권 보장을 강조하고 있는 데는, 정보의 생성/이용과 정보의 보관/관리가 분리되는 디지털 기술 기반 서비스로 인해 영장에 의해 허용된 범위 내의 정보압수에 대한 피압수자의 보호이익의 주체가 불명확해졌기 때문이라 할 수 있다. 즉 현행법 규정에 의하게 되면 피압수자가 아닌 피의자의 경우에는 수사기관의 재량에 의해 참여권이 배제될 수 있기 때문에, 압수대상 정보의 실질적 주체임에도 불구하고 참여기회의 배제로 인해 영장의 범위 내에서 수인해야 할 범위를 넘어서서 기본권이 침해될 수 있을 뿐 아니라 집행절차의 공정성을 담보하지 못할 우려가 있다고 본 것이다. 다만 대법원이 참여권을 통해 보호하고자 하는 것은 형사절차의 공정성에 대한 실질적 이해관계를 갖는다고 볼 수 있는 정보의 주체이자 피의자인 것이지, 압수대상이 되는 모든 정보의 주체에 대해 피압수자의 지위를 허용하고자 하는 것은 아니라는 것을 명확히 할 필요가 있다. 현실적으로

압수수색의 대상이 되는 모든 정보의 주체에 대해 피압수자의 지위를 허용하는 경우 참여권자의 범위가 무한히 확대됨으로 인해 사실상 수사가 불가능해지는 결과를 초래할 수도 있기 때문이다. 이에 의하면 국회에 발의된 입법안과 논문 등에서 제시된 참여권자의 범위에 「형사소송법」 제129조에 규정된 소유자, 소지자, 보관자, 기타 이에 준할 자까지 포함시키는 것은 수사절차의 적정성을 담보하는 데 있어서 합리적인 범위라고 보기는 어렵다고 할 것이다.

또한 「형사소송법」 편장체계의 문제의 하나로 영장집행의 주체는 수사기관임에도 불구하고 법원에 의한 압수수색과 같은 장에 포함되는 것은 바람직하지 않다고 본다. 따라서 압수수색 영장의 집행에 관한 규정들은 수사편에 편입되는 것이 체계상 더 적합하다고 보여진다.

이러한 관점에서 본 보고서에서는 참여권과 관련하여 다음과 같은 개정안을 제시해 보고자 한다.

제215조의n (영장집행과 참여) ① 검사 또는 사법경찰관은 피의자 또는 변호인을 압수수색 영장의 집행에 참여하게 하여야 한다.

② 검사 또는 사법경찰관은 정보에 대한 압수수색 영장을 집행하는 경우 정보의 복제, 탐색, 선별, 출력과정 전체에 걸쳐 전항에 규정된 자를 참여하게 하여야 한다.

제215조의n (영장집행과 참여자에의 통지) ① 검사 또는 사법경찰관은 압수수색 영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단 다음의 경우에는 예외로 한다.

1. 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 경우
2. 전조에 규정한 자의 소재불명 기타의 사유로 인해 압수수색 집행에 참여가 어려운 경우
3. 증거의 은닉, 인멸, 위변조 등의 우려가 있는 경우
4. 개인정보보호의 필요성이 있는 경우

② 전항에 규정된 예외사유가 영장집행이 종료되기 전에 해소된 경우에는 전조에 규정된 자에게 즉시 통지해야 한다.

③ 전조에 규정한 자가 참여의 통지를 받은 후 고의로 지연하여 영장집행을 방해하는 경우에는 참여를 배제할 수 있다.

다. 임의제출물 압수규정의 개정

현행 「형사소송법」상 임의제출물 압수에 관한 규정은 제108조와 제218조로 다음과 같다.

> **제108조 (임의제출물 등의 압수)** 소유자, 소지자 또는 보관자가 임의로 제출한 물건 또는 유류한 물건은 영장없이 압수할 수 있다.
>
> **제218조 (영장에 의하지 아니한 압수)** 검사, 사법경찰관은 피의자 기타인이 유류한 물건이나 소유자, 소지자 또는 보관자가 임의로 제출한 물건을 영장없이 압수할 수 있다.

임의제출물 압수는 취득의 강제성은 없지만 점유의 강제성으로 인해 압수와 사실상 동일한 효과를 갖기 때문에 강제처분으로 이해되는 것이 일반적이다. 하지만 강제처분임에도 사후영장을 요하지 않기 때문에 수사기관의 입장에서는 비교적 용이하게 증거를 확보할 수 있는 수단으로, 수사권 남용의 가능성이 항상 내포되어 있다고 볼 수 있다. 따라서 제출의 임의성에 대한 입증은 검사가 합리적 의심을 배제할 수 있을 정도로 증명하도록 요구하고 있다.[1230]

이와 같이 기존의 임의제출물 압수에 있어서는 제출의 임의성에 대한 입증만으로 압수의 적법성이 확보될 수 있었지만, 디지털 증거에 대한 임의제출 시 압수에 대해서는 기존의 법리를 그대로 적용하여 제출의 임의성 입증만으로 압수의 적법성이 인정된다고 보게 되면 정보저장매체 전부에 대한 압수가 가능하다고 볼 수 있는 불합리한 결과가 발생할 수 있다. 즉 현행법상 임의제출물 압수규정은 영장에 의하지 않고도 혐의사실과의 관련성 판단을 배제한 채 정보저장매체에 저장된 모든 정보를 탐색, 압수할 수 있는 가능성을 제공하는 규정이라고 할 수 있는 것이다.

이와 같이 정보저장매체에 대한 임의제출 시 압수로 인해 야기될 수 있는 정보의 과잉압수와 기본권 침해를 막기 위해서는 제출의 임의성과 압수의 강제성을 분리하여, 제출의 적법성은 임의성 입증을 통해, 그리고 압수의 적법성은 정보압수의 기본원칙 – 즉, 혐의사실과의 관련성, 선별압수 원칙과 매체압수 예외, 참여권 보장, 압수목록 교부, 별건 혐의 발견 시 조치 – 을 통해 확보해야만 수사절차상 정보압수에 있어서

1230) 대법원 2016.3.10. 선고 2013도11233 판결.

의 일관된 적법성이 온전히 담보될 수 있다고 할 것이다.

정보압수에 수반될 수밖에 없는 기본권 침해의 가능성을 통제할 수 있는 적법절차적 규정이 마련되지 못한 상태에서 현재와 같은 임의제출물 압수규정은 영장에 의한 통제를 회피하는 동시에 수사의 편의를 우선시할 수 있는 우회수단이 될 수밖에 없다고 할 것이다. 따라서 정보저장매체에 대한 임의제출 시 압수에 대한 적법절차적 통제를 위해서는 입법적 개선이 필수적이라 할 것이다.

따라서 정보저장매체에 대한 임의제출 시 압수와 관련하여서 국회에서도 여러번 입법안이 발의된 바 있다. 이를 표로 정리하여 보면 다음과 같다.

제안일자	의안번호	대상조문	개정(신설) 내용
2019-05-23	2020611	§218① 개정	검사, 사법경찰관은 피의자 기타인의 유류한 물건이나 소유자, 소지자 또는 보관자가 자발적이고 명시적인 동의에 의하여 제출한 물건을 영장없이 압수할 수 있다.
		§218②③④ 신설	② 제1항에 따라 물건을 압수하는 경우에 검사 또는 사법경찰관은 피의자·소유자·소지자 또는 보관자에게 그 제출을 거부할 수 있으며, 제출을 거부할시 어떠한 불이익도 받지 아니함을 미리 고지하여야 한다. ③ 제1항에 따른 압수의 목적물이 컴퓨터용 디스크·이동통신 단말장치, 그 밖에 이와 비슷한 정보저장매체(이하 이조에서는 "정보저장매체등"이라 한다)인 경우에는 검사 또는 사법경찰관은 탐색할 정보의 범위를 정하여 피의자·소유자·소지자 또는 보관자로부터 제출받아야 한다. ④제1항에 따라 정보저장매체 등을 압수한 경우에는 피의자·변호인 또는 피의자가 지정하는 사람을 그 정보를 탐색·저장 또는 복제하는 과정에 참여하게 하여야 한다.
2022-01-07	2114302	§108① 개정	소유자, 소지자 또는 보관자가 자발적이고 명시적인 동의에 의하여 제출한 물건을 영장없이 압수할 수 있다.
		§108②③④ 신설	② 제1항에 따라 물건을 압수하는 경우에 검사 또는 사법경찰관은 피의자·소유자·소지자 또는 보관자에게 그 제출을 거부할 수 있으며, 제출을 거부할시 어떠한 불이익도 받지 아니함을 미리 고지하여야 한다. ③ 제1항에 따른 압수의 목적물이 정보 또는 정보저장매체 등인 경우에는 탐색할 정보의 범위를 정하고 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 소유자·소지자 또는 보관자로부터 제출받아야 한다. ④제1항에 따라 정보저장매체 등을 압수한 경우에는 피고인·변호인 또는 피고인이 지정하는 사람을 그 정보를 탐색·저장 또는 복제하는 과정에 참여하게 하여야 한다.
2023-02-06	2119829	§218② 신설	제1항에 따라 물건을 압수하는 경우에 검사 또는 사법경찰관은 소유자, 소지자 또는 보관자에게 그 제출을 거부할 수 있고 압수의 목적물이 컴퓨터용 디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에는 저장된 정보의 범위를 정하여 출력하거나 복제하여 제출할 수 있음을 미리 고지하여야 한다.

임의제출물 압수규정과 관련하여 발의된 입법안의 형식을 보면「형사소송법」제108조를 개정하는 방식과 제218조를 개정하는 방식으로 되어 있다. 하지만 동법 제108조는 제219조에 의해 수사기관의 압수수색에 준용되지 않기 때문에, 제108조만을 개정하는 경우에는 수사기관에 의한 임의제출물 압수규정은 현행과 동일한 형태로 남게 되고, 정보저장매체에 대한 임의제출 시 압수의 문제가 그대로 남게 된다. 그에 비해 동법 제218조의 규정을 개정하게 되면 수사기관에 의한 임의제출물 압수에 관한 적법절차적 통제가 가능해진다고 볼 수 있고, 동법 제108조는 원칙적으로 법원에 의한 임의제출물 압수라고 볼 수 있고, 따라서 별도의 사법적 통제를 요하지 않기 때문에 현행과 동일한 형태로 두어도 무방하다고 볼 수 있을 것이다. 다음으로 임의제출물 압수규정에 관한 입법안의 내용을 보면, 임의성 입증요건으로 자발적이고 명시적인 동의, 거부권 고지를 규정하고 있으며, 압수의 적법성 요건으로 관련성, 선별압수원칙, 참여권 등의 내용을 규정하고 있음을 볼 수 있다.

한편 논문과 보고서 등에서 임의제출물 압수와 관련하여 제시한 입법안을 보면 다음과 같다.

연도	저자 및 논문	대상조문	개정(신설) 내용
2022	김환권, "디지털 증거의 임의제출과 관련된 법적 쟁점"[1231]	§108 개정	① 소유자, 소지자 또는 보관자가 임의로 제출한 물건 또는 유류한 물건은 영장없이 압수할 수 있다. 다만 피고인이 소유·관리하는 제106조 제3항의 정보저장매체 등을 피고인 아닌 제3자가 임의제출하는 경우에는 임의제출의 동기가 된 범죄혐의사실과 구체적·개별적 연관관계가 있는 전자정보에 한하여 압수의 대상이 된다. ② 제1항에 의한 정보저장매체 등에 대한 압수 및 탐색 가능 범위는 원칙적으로 해당 사건에 한정되나, 피해자가 있는 경우 동일 피해자에 대한 증거는 압수할 수 있다.
		§218 개정	① 검사, 사법경찰관은 피의자 기타인의 유류한 물건이나 소유자, 소지자 또는 보관자가 임의로 제출한 물건을 영장없이 압수할 수 있다. 다만 피의자가 소유·관리하는 제106조 제3항의 정보저장매체 등을 피의자 아닌 제3자가 임의제출하는 경우에는 임의제출의 동기가 된 범죄혐의사실과 구체적·개별적 연관관계가 있는 전자정보에 한하여 압수의 대상이 된다. ② 제1항에 의한 정보저장매체 등에 대한 압수 및 탐색 가능 범위는 원칙적으로 해당 사건에 한정되나, 피해자가 있는 경우 동일 피해자에 대한 증거는 압수

연도	저자 및 논문	대상조문	개정(신설) 내용
			할 수 있다. ③ 임의제출물을 영장 없이 압수하기 전에 다음 각 호의 사항을 알려주어야 한다. 1. 해당 물건을 제출하지 아니할 수 있다는 것 2. 해당 물건을 제출하는 경우에는 임의로 다시 가져갈 수 없으며, 법정에서 유죄의 증거로 사용될 수 있다는 것 ④ 검사, 사법경찰관은 임의제출을 받는 경우 제출자에게 그 임의제출과 관련된 혐의에 대한 범죄사실을 서면으로 고지하여야 한다. 다만 제출자가 위와 같은 고지를 원하지 아니하는 경우에는 그렇지 아니하다.
		§218의3 신설	제218조의3(임의제출물 탐색 중단·폐기·회수권) ① 임의제출자와 임의로 제출된 물건(전자정보를 포함한다. 이하 동조에서 '임의제출물'이라 한다)의 소유자는 임의제출물(임의제출물의 복제물이 있는 경우 그 복제물을 포함한다. 이하 동조에서 같다)에 대하여 그 탐색 중단이나 폐기나 회수를 임의제출물을 관리하는 수사기관에게 요청할 수 있다. 다만 공소제기가 이루어진 경우 그 임의제출물이 증거로 제출되었거나 제출될 예정이라면, 그 요청을 할 수 없다. ② 제1항 본문의 요청이 있는 경우 수사기관은 해당 임의제출물에 대하여 요청시부터 72시간 이내에 탐색을 중단하거나 폐기하거나 반환하여야 하고, 임의제출물을 계속 압수할 필요가 있는 경우에는 위 72시간 이내에 압수수색영장을 청구하여야 한다. 이 경우 법원은 영장 청구서가 법원에 접수된 때로부터 48시간 이내에 영장의 발부 여부를 결정하여야 하고, 영장의 발부 여부가 결정될 때까지 수사기관은 임의제출물에 대한 처분을 유보할 수 있다. 영장이 기각된 경우 수사기관은 지체 없이 제1항 본문의 요청을 이행하여야 한다.
2021	박병민·서용성, "디지털 증거 압수수색 개선방안에 관한 연구 -법률 개정에 관한 논의를 중심으로-"[1232]	§218 개정	① 검사, 사법경찰관은 피의자 기타인의 유류한 물건이나 소유자, 소지자 또는 보관자가 임의로 제출한 물건 또는 정보를 영장없이 압수할 수 있다. ② 검사, 사법경찰관은 제1항에 따라 임의제출받는 경우에 미리 다음 각호의 사항을 서면으로 알려주어야 한다. 1. 범죄사실의 개요 2. 물건 또는 정보를 제출하지 않을 수 있다는 것 3. 물건 또는 정보를 제출하지 않아도 불이익을 받지 않는다는 것 4. 임의로 제출한 물건 또는 정보는 법정에서 유죄의 증거로 사용될 수 있다는 것 5. 임의로 정보를 제출한 때에는 그 정보가 저장된 정보저장매체등의 분석 과정에 참여할 수 있다는 것

논문과 보고서 등에서 제시된 임의제출물 압수규정 개정안의 중심은 「형사소송법」 제218조의 개정에 있다고 볼 수 있다. 즉 수사기관에 의한 임의제출물 압수에 대한 입법적 통제장치로서 사전고지방식을 제시하고 있으며, 그 내용으로는 혐의사실과의 연관성, 제출거부권 및 거부로 인한 불이익 금지, 정보 제출범위의 제한 및 참여권 보장 등이 제시되어 있다. 다만 임의제출물 탐색 중단 및 폐기, 회수권 등의 신설안은 제출의 임의성을 토대로 한 영장에 의하지 않은 압수라는 동 규정의 취지와 부합하기는 어렵다고 보여진다.

따라서 정보저장매체에 대한 임의제출 시 압수와 관련하여 적법절차적 통제를 가능하도록 하기 위해서는 현행 「형사소송법」 제218조의 규정을 개정하여, 임의성의 적법성과 압수의 적법성을 동시에 담보할 수 있는 요건들을 명문화하는 것이 바람직하다고 할 것이다. 다만 임의제출 시 압수과정에 참여권을 인정하기 위한 법적 근거로 「형사소송법」 제121조가 적합한가에 대해서는 재고할 필요가 있다. 즉 동법 제121조의 참여권 규정은 압수수색영장 집행에의 참여를 전제로 규정된 것이기 때문에 영장에 의하지 아니하는 압수인 임의제출물 압수에 대한 참여권의 근거라고 하기는 어렵다고 볼 수 있다. 만약 동법 제121조가 영장의 유무와 상관없이 압수수색절차에의 참여를 허용하고자 하는 취지라고 한다면, 제121조부터 제123조까지 규정을 영장집행 그 자체보다는 압수수색절차에의 참여에 관한 내용으로 개정할 필요가 있다고 할 것이다.

따라서 본 보고서에는 임의제출물 압수에 관한 입법안과 함께 참여권과 관련한 규정의 개정안을 「형사소송법」 편제상 수사편에 두는 것을 전제로 입법안을 제시하고자 한다.

1231) 김환권, "디지털 증거의 임의제출과 관련된 법적 쟁점"(발표문), 『디지털증거 압수수색 관련 최근 동향』, 2022년 한국형사소송법학회 추계 학술대회, 2022.9.16, 31면.

1232) 박병민·서용성, 앞의 연구보고서, 287-288면.

제220조 (영장에 의하지 아니한 압수) ① 검사, 사법경찰관은 피의자, 기타 소유자, 소지자 또는 보관자가 자발적이고 명시적 동의에 의하여 제출한 물건 또는 정보를 영장없이 압수할 수 있다.
② 검사, 사법경찰관은 제1항에 따라 물건 또는 정보를 임의제출받는 경우 사전에 다음의 사항을 고지하여야 한다.
1. 물건 또는 정보의 제출을 거부할 수 있다는 것
2. 제출한 물건 또는 정보는 압수되며, 법정에서 유죄의 증거로 사용될 수 있다는 것
3. 정보제출시 제출하고자 하는 정보의 범위를 제한할 수 있다는 것
4. 정보제출시 정보의 복제, 탐색, 선별, 출력 과정에 참여할 수 있다는 것
③ 제출된 정보에서 별건 혐의와 관련된 사실을 발견한 경우에는 전 2개항의 규정을 적용하지 아니하며, 제215조의 규정에 따른다.

제215조의n (압수수색절차에의 참여) ① 검사 또는 사법경찰관은 피의자 또는 변호인을 압수수색절차에 참여하게 하여야 한다.
② 검사 또는 사법경찰관은 정보에 대한 압수수색절차를 진행하는 경우 정보의 복제, 탐색, 선별, 출력과정 전체에 걸쳐 전항에 규정된 자를 참여하게 하여야 한다.

제215조의n (참여자에의 통지) ① 검사 또는 사법경찰관은 압수수색절차를 진행함에는 미리 그 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단 다음의 경우에는 예외로 한다.
1. 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 경우
2. 전조에 규정한 자의 소재불명 기타의 사유로 인해 압수수색 집행에 참여가 어려운 경우
3. 증거의 은닉, 인멸, 위변조 등의 우려가 있는 경우
4. 개인정보보호의 필요성이 있는 경우
② 전항에 규정된 예외사유가 압수가 종료되기 전에 해소된 경우에는 전조에 규정된 자에게 즉시 통지해야 한다.
③ 전조에 규정한 자가 참여의 통지를 받은 후 고의로 지연하여 압수를 방해하는 경우에는 참여를 배제할 수 있다.

2. 디지털 증거에 부합하는 새로운 압수수색 제도 도입을 위한 입법안

가. 디지털 증거(데이터) 보전명령

현행 「형사소송법」은 제184조와 제185조에 증거보전 청구절차를 규정하고 있다. 하지만 이 규정은 영장청구와 유사하게 법원에 서면으로 그 사유를 소명하도록 규정하고 있기 때문에 변경 또는 삭제 가능성을 배제하기 위해 신속하게 디지털 증거를 확보하기 위한 실효적인 조치로서는 한계가 있다. 즉 동 규정은 압수, 수색, 검증

등의 방법을 통해 증거를 확보한 후 보전하는 것을 전제로 하기 때문에 영장집행절차가 선행되어야 한다는 점에서 신속히 디지털 정보를 프리징함으로써 변경, 훼손, 삭제 등의 가능성을 배제해야 하는 디지털 수사상황 하에서는 적합하다고 보기 어렵다.

디지털 증거 보전명령은 보전 대상인 데이터의 점유가 수사기관으로 이전되는 것이 아니라 데이터의 소유자나 소지자, 관리자 본인의 통제하에 있는 것이기 때문에, 기존의 강제수사절차에 비해서는 기본권 침해의 우려가 크지 않을 뿐 아니라 명령의 객체가 되는 디지털 기술 기반 서비스업체나 일반기업의 통상적인 업무에 대한 침해를 최소화할 수 있고, 데이터의 무결성도 신속하게 확보할 수 있다는 이점이 있다. 하지만 보전명령으로 인해 해당 데이터의 이용이 제한될 뿐 아니라 데이터 보전으로 인한 업무의 제약 및 경제적 부담과 같은 영업권 침해의 문제가 발생할 수 있다는 점에서 보면 강제처분의 성격을 갖는다고 보아야 할 것이다.

따라서 데이터 보전명령이 기본권 제한을 수반하는 한 법치국가적 통제의 기본인 비례성 원칙에 따라 그 목적의 적합성, 필요성, 최소침해의 원칙 등이 준수되어야 할 뿐 아니라 기존의 증거확보 수단으로는 데이터의 삭제 및 변경 등으로 인한 증거확보가 어렵다고 하는 보충성 원칙의 준수, 그리고 무엇보다도 범죄혐의사실과의 관련성 등이 인정되는 경우에 한해 허용될 수 있다고 할 것이다.

이와 같이 데이터 보전명령을 수사상 강제처분으로 보게 되면, 명령의 주체는 수사기관이 되어야 하며, 명령의 객체는 이 제도를 운영하고 있는 다른 나라들의 예에 비추어 볼 때 디지털 기술 기반 서비스제공자로 제한하는 것이 동 제도의 목적과 취지에 보다 부합한다고 볼 수 있다. 그리고 보전명령의 대상과 관련해서 동 제도를 운영하는 상당수의 국가들은 보전대상이 되는 데이터 종류에 제한을 두고 있지 않지만, 모든 범죄에 대해 보전명령의 대상이 되는 데이터에 제한을 두지 않는 것은 정보에 대한 자기결정권 침해 등과 관련하여 문제의 소지가 있다고 볼 수 있다. 따라서 보전명령이 요구되는 일정한 유형의 중대범죄에 한해서는 데이터 기록은 물론 데이터 내용까지 보전명령의 대상이 된다고 보는 반면, 그 외의 범죄에 대해서는 데이터 기록으로 그 대상을 제한하는 것이 바람직하다고 할 것이다. 또한 데이터 보전명령은 수사절차상 압수수색 또는 검증이 예상되는 데이터의 변경 또는 삭제를 막기 위한 임시적 보전조치라고 할 수 있기 때문에 그 기간에 있어서 일정한 제한을 두어야 한다. 그리고

마지막으로 데이터 보전명령을 수사절차상 강제처분으로 보는 이상 사법적 통제는 반드시 필요하지만, 사전통제방식은 데이터 보전명령의 취지와 맞지 않기 때문에 사후통제방식으로 이루어지는 것이 합리적이라 할 것이다.

데이터 보전명령제도의 신설과 관련하여 국회에 발의된 입법안은 다음과 같다.

제안일자	의안번호	대상조문	개정(신설) 내용
2009-05-13	1804839	§106②후단 신설	법원은 제1항에 따른 압수의 목적이 컴퓨터용디스크 그 밖에 이와 비슷한 정보저장매체(이하 이조에서 "정보저장매체 등"이라고 한다)에 기억된 정보를 얻기 위한 것이고 그러한 목적을 달성하기 위하여 긴급히 필요하다고 인정하면 해당정보를 보관·관리하고 있는 자에게 관련정보의 보전을 명할 수 있다. 이 경우 보전기간은 필요한 최소한도의 범위안에서만 하여야 한다.
2015-02-02	1913878	§108의2 신설	① 법원은 정보를 압수할 필요가 있는 경우 「정보통신망 이용촉진 및 정보보호등에 관한 법률」제2조 제1항 제3호에 정한 정보통신서비스제공자에게 30일의 범위내에서 당해 정보가 삭제·변경되지 않도록 보존할 것을 서면으로 요청할 수 있다. 다만, 상당한 이유가 있다고 인정되는 경우 30일의 범위내에서 1회에 한해 연장할 수 있다.
2016-08-02	2001352	의안번호 1913878과 내용 동일	
2021-02-04	2107939	§216의2 신설	① 검사 또는 사법경찰관은 영상정보, 문자기록 등 정보저장매체에 저장된 전자정보를 확보하기 위한 것으로 증거인멸의 우려가 있거나 전자정보 확보를 위하여 긴급한 경우에는 해당 전자정보에 대한 압수수색검증의 긴급보전조치를 할 수 있다.
2022-08-24	2116983	§215의2 신설	① 검사 또는 사법경찰관은 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이조에서 "정보저장매체등"이라 한다)에 기억된 영상정보, 문자기록 등 전자정보를 얻기 위한 것으로 전자정보의 멸실우려 등 미리 압수수색검증영장을 발부받기 어려운 긴급한 사정이 있는 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조 제1항 제3호에서 정한 정보통신서비스제공자(이 이 조에서 "정보통신서비스제공자"라 한다)에게 해당 전자정보가 삭제 또는 변경되지 않도록 보전할 것(이하 이조에서는 "긴급보전조치"라 한다)을 요청할 수 있다. ② 제1항의 긴급보전조치를 요청받은 정보통신서비스제공자는 정당한 사유가 없는 한 해당 전자정보의 보전에 적극 협조하여야 한다.

데이터 보전명령과 관련하여 국회에 발의된 입법안의 경우 대부분은 증거인멸의 우려와 같은 긴급한 필요성을 그 요건으로 하고 있음을 볼 수 있다. 다만 명령의 주체와 관련해서는 2020년 이전에 발의된 입법안은 법원을 주체로 하고 있으며, 2020년 이후로 발의된 입법안은 수사기관을 주체로 하고 있다는 점에서 차이가 있다. 그리고 명령의 객체는 「정보통신망법」 제2조 제1항 제3호에 규정된 정보통신서비스 제공자 또는 정보를 보관·관리하고 있는 자로 규정하고 있다. 다만 정보를 보관·관리하는 자로 하는 경우 피의자도 포함될 수 있는데, 그 경우 피의자의 방어권과 충돌할 우려가 있기 때문에 피의자는 수범자에서 배제하는 것이 타당하다고 할 것이다. 한편 데이터 보전명령의 대상이 되는 데이터 유형과 관련해서는 어떠한 입법안에서도 언급된 바가 없으며, 데이터 보전기간의 경우 1개의 입법안에서만 30일(30일 범위 내 1회 연장 가능)의 제한을 두고 있음을 볼 수 있다. 또한 데이터 보전명령에 대한 사법통제 방식에 대해서도 구체적인 규정을 두고 있지 않음을 알 수 있다.

다음으로, 논문이나 보고서에서 디지털 증거 보전명령과 관련하여 제시된 입법안은 아래와 같다.

연도	저자 및 논문	대상조문	개정(신설) 내용
2021	박병민·서용성, “디지털 증거 압수수색 개선방안에 관한 연구 –법률 개정에 관한 논의를 중심으로–”[1233]	§218조의4 신설	제218조의4(정보의 보존요청 등) ①검사 또는 사법경찰관은 정보를 압수하기 위하여 긴급한 필요가 있는 경우 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조 제1항 제3호에 정한 정보통신서비스제공자(이하 “정보통신서비스제공자”라고 한다)에게 그 업무상 보관하고 있는 정보(정보의 내용은 제외한다)중 필요한 것을 특정하여 7일의 범위내에서 해당 정보가 삭제·변경되지 않도록 보존할 것을 요청할 수 있다. 다만, 상당한 이유가 있다고 인정되는 경우 7일의 범위 내에서 1회에 한해 연장할 수 있으나, 보존기간은 총 14일을 초과할 수 없다. ② 제1항의 정보의 보존을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 보존할 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한하. 이하 같다) 또는 지원의 허가를 받아야 한다. 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 정보의 보존요청을 한 후 지체없이 그 허가를 받아 정보통신서비스제공자에게 송부하여야 한다.

연도	저자 및 논문	대상조문	개정(신설) 내용
			③ 제1항의 경우 당해 정보를 압수할 필요가 없다고 인정되는 때에는 지체없이 보존요청을 취소하여야 한다.
2020	차종진, “디지털증거법제의 발전동향과 입법과제”[1234]	§199③,④ 신설	③ 검사 또는 사법경찰관은 피고사건과 관계가 있다고 인정할 수 있는 정보에 한정하여 「정보통신망 이용촉진 및 정보보호등에 관한 법률」 제2조제1항제3호에 정한 정보통신서비스제공자에게 30일의 범위 내에서 당해 정보가 삭제·변경되지 않도록 보전할 것을 서면으로 요청할 수 있다. 다만, 상당한 이유가 있다고 인정되는 경우 30일의 범위 내에서 1회에 한해 연장할 수 있다 ④ 제3항에 따라 보전을 요청받은 자는 이에 관한 사항을 누설하여서는 아니된다.
2020	노소형, “제3자 보관 디지털증거에 대한 긴급증거보전 제도 신설방안 연구”[1235]	§184조의2 신설	제184조의2(긴급증거보전 요청과 협조) ① 판사, 검사, 사법경찰관, 특별사법경찰관 또는 군사법경찰관은 미리 증거를 임시로 보전하지 아니하면 그 증거를 사용하기 곤란한 사정이 있고 긴급을 요하는 때에 범죄와 관계가 있다고 인정할 수 있는 것에 한정하여 제106조제1항부터 제3항까지 및 제107조제1항의 대상을 30일 이내의 기간을 정하여 소지자, 보관자 또는 관리자에게 긴급한 임시보전(이하 “긴급증거보전”이라고 한다)을 요청할 수 있다. ② 제1항의 요청을 받은 자(이하 “수신자”라고 한다)는 특별한 사정이 없는 한 지체 없이 긴급증거보전하기 위한 모든 필요한 조치를 하여야 하며, 조치가 완료되면 그 사실을 긴급증거보전 요청자(이하 “요청자”라고 한다)에게 통지하여야 한다. ③ 제1항의 요청은 서면에 의하여야 한다. 다만, 긴급증거보전의 방법 등에 관한 사항은 미리 구두로 협의할 수 있다. ④ 제1항의 보전 기간에 연장이 필요한 때에는 30일 이내의 기간을 정하여 별도의 서면으로 요청할 수 있다. 단, 보전 기간은 총 90일을 초과할 수 없다. ⑤ 요청자는 필요한 때에 요청 사실과 요청에 관한 사항을 외부에 공개하거나 누설하지 않도록 요청할 수 있다. ⑥ 요청자는 긴급증거보전을 요청한 후 보전 기간 이내에 압수·수색, 제출명령 등의 처분을 하지 않아 보전 기간이 만료되거나 증거의 필요성이 없어지면 지체 없이 해당 주체에게 긴급증거보전한 사실을 서면으로 통지하여야 한다. ⑦ 수신자는 요청자가 소속된 기관의 장에게 그 업무수행에 관한 비용의 지급을 청구할 수 있다. ⑧ 전항에 따른 비용의 산정 및 그 지급방법 등은 수신자와 요청자가 소속된 기관의 장이 협의하여 정한다.

논문이나 보고서 등에서 제시된 데이터 보전명령과 관련한 입법안은 국회에서 발의된 입법안에 비하여 데이터 보전명령의 적법성을 확보하는 데 있어서 필요한 절차적 요건들을 보다 구체적으로 열거하고 있음을 알 수 있다. 즉 데이터 보전명령의 요건으로서 긴급성과 관련성을 제시하고 있을 뿐 아니라 보전명령의 기간도 제한하고 있으며, 사법통제 절차도 규정하고 있음을 볼 수 있다. 그리고 데이터 보전명령의 주체와 객체에 대해서는 각각 수사기관과 정보통신서비스 사업자를 규정하고 있으며, 보전명령의 대상이 되는 데이터 유형과 관련해서는 한 개의 입법안에서만 데이터 내용을 보전명령의 대상에서 제외하도록 하는 규정을 두고 있을 뿐, 나머지 입법안에서는 데이터의 유형과 관련해서는 규정된 내용이 없다.

이에 본 보고서에서는 디지털 증거(데이터) 보전명령제도가 수사절차상 강제처분 수단으로서 적법성을 갖출 수 있는 입법안을 다음과 같이 제시해 보고자 한다.

제219조 (정보의 긴급보전요청) ① 검사 또는 사법경찰관은 피의사실과 관계가 있다고 인정할 수 있는 정보의 삭제 또는 변경에 대한 긴급한 우려가 있는 경우, 「정보통신망 이용촉진 및 정보보호등에 관한 법률」 제2조제1항제3호에 정한 정보통신서비스제공자에게 당해 정보가 삭제 또는 변경되지 않도록 보전요청을 할 수 있다.

② 제1항의 보전요청대상이 되는 범죄가 「통신비밀보호법」 제5조에 해당하는 경우에는 정보의 기록과 정보의 내용에 대해서도 보전요청을 할 수 있으며, 그 외의 범죄에 해당하는 경우에는 정보의 기록에 대해서만 보전요청을 할 수 있다.

③ 제1항의 보전요청대상이 되는 범죄가 「통신비밀보호법」 제5조에 해당하는 경우에는 보전요청기간을 30일로 하며, 1회에 한해 연장할 수 있다. 그 외의 범죄에 해당하는 경우에는 보전요청기간을 15일로 하며, 1회에 한해 연장할 수 있다.

④ 검사 또는 사법경찰관은 제1항에 의하여 긴급보전요청을 한 경우, 즉시 지방법원판사에게 보전요청사유, 보전요청 대상범죄, 보전대상 정보와 혐의사실과 관련성, 보전요청 대상 정보의 범위와 내용 등을 전자문서로 제시하거나 전송하여야 한다.

⑤ 제1항에 의하여 긴급보전요청을 받은 자는 이에 관한 사항을 공개해서는 안된다.

⑥ 제1항에 의하여 긴급보전요청을 받은 자는 특별한 사정이 없는 한 보전요청에 협조해야 하며, 그로 인한 모든 민형사상 책임을 지지 아니한다.

1233) 박병민·서용성, 앞의 연구보고서, 318면.
1234) 차종진, 앞의 연구보고서, 105면.
1235) 노소형, 앞의 박사학위논문, 209-211면.

나. 전자영장

법무부는 2021년 형사사법절차 전자화를 위해「형사사법절차에서의 전자문서 이용 등에 관한 법률」을 제정하였으며, 법원도 "형사사법 절차에서의 전자문서 이용 등에 관한 규칙" 제정안을 마련하여 현재 내부 의견조회절차를 거치고 있음을 앞에서 언급한 바 있다. 동 법률에 의하여 영장발부, 압수수색영장, 영장에 의한 체포, 구속, 압수수색검증에 따른 집행 시 전자문서 등의 형태로 제시 및 전송이 가능해짐으로써 영장집행의 전과정, 즉 신청, 청구, 발부, 집행 등 모든 단계가 전자적 방식으로 처리되는 전자영장제도가 가능해졌다. 이와 같이 전자영장제도를 시행할 수 있는 입법적 뒷받침은 마련되어 있다고 볼 수 있다.

하지만「형사소송법」제118조에 의하면 압수수색의 피처분자에게 원본을 제시해야 하고, 피의자에게는 그 사본을 교부하도록 되어 있다. 이에 의하면 전자영장에 의하는 경우에는 법관의 전자서명이 포함되어 전자적으로 전송된 영장은 그것이 제시되는 디지털기기의 유형과 상관없이 원본이라고 보아야 할 것이다. 그리고 사본교부의 문제는 전자영장의 경우 원본과 사본의 구분이 무의미하므로 전자적 형태로 피의자에게 전달할 수도 있겠지만, 전자영장의 무결성과 신뢰성의 담보를 위해서는 전자적 형태로 전달하는 것보다는 출력물을 교부하는 것으로 사본교부를 대신하는 것이 더 타당하다고 볼 수 있다. 만약 전자적 형태의 사본을 교부하는 경우에는 수신자에 의한 조작이 불가능한 방식으로 전송되어야 할 것이다.

전자영장제도 도입과 관련하여 국회에 발의된「형사소송법」개정안은 단 한 건도 없었으며, 다만 논문에서 전자영장제도 도입을 위하여「형사소송법」개정안을 제시한 입법안은 1건으로, 그 내용은 다음과 같다.

연도	저자 및 논문	대상조문	개정(신설) 내용
2018	김기범, "압수·수색 영장의 전자적 제시에 관한 입법적 연구"[1236]	§118② 신설	② 압수수색 영장은 처분을 받는 자가 동의하는 경우 전자적 방법으로 제시할 수 있다. 이때 신분을 표시하는 증표를 전자적 방법 등을 활용하여 제시하여야 한다.

1236) 김기범, "압수·수색영장의 전자적 제시에 관한 입법적 연구",『경찰학연구』제18권 제2호, 경찰대학, 2018.6, 165면.

본 논문에서 제시된 입법안은 피처분자의 동의를 전제로 한 전자영장제시라고 할 수 있다. 하지만 이미 법률에 의하여 압수수색검증영장의 제시를 전자문서의 제시 또는 전송하는 방식으로 할 수 있도록 규정하고 있다는 점을 고려하면, 피처분자의 동의를 전제로 할 것은 아니라고 본다.

본 보고서에서는 디지털 증거 압수수색에 있어서 시간적 공간적 효율성을 담보할 수 있는 방안 가운데 하나인 전자영장에 대한 법적 근거를 마련하기 위한 「형사소송법」 개정안을 다음과 같이 제시해 보고자 한다. 다만 「형사소송법」 편장체계상 압수수색영장의 제시도 수사기관이 그 주체가 되는 규정이라고 할 것이므로, 동법 제215조의 수사기관에 의한 압수수색검증에 관한 규정 다음으로 위치하는 것이 바람직하다고 보여진다.

제216조 (영장의 제시) ① 검사 또는 사법경찰관은 압수·수색·검증 영장을 그 처분을 받는 자에게 반드시 제시해야 한다.
② 제1항에 의한 영장의 제시는 「형사사법절차에서의 전자문서 이용 등에 관한 법률」 제17조에 따라 전자문서를 제시하거나 전송하는 방법으로 제시할 수 있다.
③ 제1항에 의하여 처분을 받는 자가 피의자인 경우에는 사본 또는 전자문서의 출력물로 교부할 수 있다.
④ 제1항에 의하여 처분을 받는 자가 현장에 없는 등 영장의 제시나 사본 등의 교부가 현실적으로 불가능한 경우에는 형사사법포털시스템에 등록된 전자영장를 확인할 수 있는 방식을 고지해야 한다.
⑤ 제1항에 의하여 처분을 받는 자가 영장의 제시나 사본 등의 교부를 거부한 때에는 예외로 한다.

다. 디지털 증거 원격지 압수수색

원격지 압수수색은 이용자가 자신의 디지털기기 자체에 데이터를 저장하지 않고, 원격지에 있는 서버나 저장장치 등에 데이터를 저장하는 방식이 일상화되어 가면서 그 필요성이 부각되는 수사방식이라고 할 수 있다. IT 기술이 고도화될수록 데이터의 생성·이용과 저장·관리가 분리됨으로써 물리적 장소를 대상으로 하는 기존의 압수수색으로는 대응하기 어렵다는 현실적 한계를 극복하기 위한 수단이라 할 수 있다. 즉 클라우드서비스 또는 해외 이메일 서비스 등을 이용하는 사람에 대한 압수수색에

있어서 영장에 기재된 장소에 존재하는 정보저장매체에 접속하여 디지털 증거를 확보하기 위한 수단으로 이용되는 것이 원격지 압수수색이다. 원격지 압수수색과 관련하여 대법원도 현행 「형사소송법」상 압수수색 규정으로 허용될 수 있는 압수수색 방식으로 인정하고 있으며, 국제적으로도 원격지 압수수색은 적법한 수사방식으로 인정하고 있는 것이 일반적인 추세라고 할 수 있다.

원격지 압수수색의 필요성에 대해서는 이론의 여지가 없지만, 영장에 기재된 디지털기기와 네트워크로 연결된 원격지 서버 등으로 수색의 장소적 범위를 실질적으로 확장하는 결과를 가져오기 때문에 현행법상 압수수색규정으로 포섭이 가능한가에 대해서는 이론(異論)이 있다. 이에 대해 대법원은 판례를 통해 "1. 영장에 따라 영장 기재 수색장소에 있는 컴퓨터 등 정보처리장치를 이용할 것, 2. 적법하게 취득한 피의자의 아이디와 비밀번호를 입력할 것, 3. 피의자가 접근하는 통상적인 방법에 따라 그 원격지 저장매체에 접속할 것, 4. 원격지 저장매체에 저장되어 있는 피의자 관련 전자정보를 수색장소의 정보처리장치로 내려받거나 그 화면에 현출시킬 것"[1237]이라고 하는 원격지 압수수색의 적법성 판단기준을 제시하고 있다.

하지만 대법원이 제시하고 있는 원격지 압수수색의 적법성 판단기준에 의하더라도 기본권 침해의 정도에 있어서 일반 압수수색에 비하여 크다고 할 수 있기 때문에 보다 물리적 장소개념에 의존하고 있는 일반 압수수색 규정보다 엄격한 입법적 제한을 두는 방안을 고려할 필요가 있다. 이러한 법적 근거를 통해 압수수색 권한의 확장에 대한 적법성을 확보하되, 압수수색 권한의 확장으로 인한 프라이버시 또는 다른 국가의 관할권에 대한 침해를 유발할 가능성을 고려하여, 피처분자에게 주어진 통상적인 접근권한이 허용하는 한계 내로 제한하는 명시적 규정을 두어야 할 것이다.[1238] 이와 함께 원격지 압수수색으로 인해 수사기관에 의해 확보가능한 정보의 범위 또한 확대될 수밖에 없고, 이는 프라이버시 및 기본권 침해에의 우려를 높인다고 할 수 있다. 따라서 원격지 압수수색을 허용하기 위한 법률상 요건을 좀 더 구체적으로 제한할 필요가 있다고 할 것이다. 즉 혐의사실과의 관련성 외에 원격지 서버에 관련 정보가 저장되어 있다고 인정할 만한 상당성, 정보의 삭제 및 변경의 우려 등과 같은 요건들을

1237) 대법원 2017.11.29. 선고 2017도9747 판결.
1238) 탁희성, 앞의 박사학위논문, 150면.

규정함으로써 원격지 압수수색이 보다 엄격하게 행해질 수 있도록 하는 입법적 방안이 제안되어야 할 것으로 생각된다.

원격지 압수수색과 관련하여 국회에서 발의된 입법안은 다음과 같다.

제안일자	의안번호	대상조문	개정(신설) 내용
2015-02-02	1913878	§115조의2③ 신설	③ 압수수색 대상인 컴퓨터 등 정보처리장치와 정보통신망으로 연결되어 정보저장매체 등에 집행대상 정보가 보관되어 있다고 인정할만한 상당한 이유가 있는 경우에는, 그 정보를 당해 정보처리장치 또는 다른 저장매체로 이전 또는 복제하거나 이를 출력하는 방법으로 압수수색할 수 있다. 이 경우 당해 정보처리장치 관리자의 권한범위를 초과하여 집행할 수 없다.
2016-08-02	2001352	§115조의2③ 신설	상동

국회에 발의된 원격지 압수수색 관련 입법안은 상당성 요건과 함께 정보처리장치 관리자의 권한범위 내라는 제한적 요건을 두고 있음을 볼 수 있다. 하지만 대법원이 제시했던 원격지 압수수색의 적법성 요건인 '적법하게 취득한 권한'에 대한 규정은 두고 있지 않음을 볼 수 있다.

다음으로, 논문이나 보고서 등에서 제시된 원격지 압수수색에 관한 입법안은 아래와 같다.

연도	저자 및 논문	대상조문	개정(신설) 내용
2021	박병민·서용성, "디지털 증거 압수수색 개선방안에 관한 연구 -법률 개정에 관한 논의를 중심으로-"[1239]	§115조의2 (정보의 압수집행)④ 신설	④ 압수수색 대상인 컴퓨터 등 정보처리장치와 정보통신망으로 연결되어 있는 정보저장매체 등에 집행대상 정보가 보관되어 있다고 인정할만한 상당한 이유가 있는 경우에는, 그 정보를 당해 정보처리장치 또는 다른 저장매체로 이전 또는 복제하거나 이를 출력하는 방식으로 압수할 수 있다.
		§114(영장의 방식)③ 신설	③ 제115조의2 제4항에 의하여 압수수색하는 경우에는 압수수색 영장에 제1항에 기재된 사항 외에 압수수색대상인 컴퓨터 등 정보처리장치와 정보통신만으로 연결되어 있는 정보저장매체에 보관된 정보의 범위를 기재하여야 한다.
2020	차종진, "디지털증거법제의 발전 동향과 입법과제"[1240]	§106④ 신설	④ 압수·수색 대상인 전자정보가 저장된 정보저장매체등과 정보통신망으로 연결되어 있는 정보저장매체등에 집행 대상 전자정보가 보관되어 있

연도	저자 및 논문	대상조문	개정(신설) 내용
			다고 인정할 만한 상당한 이유가 있는 경우에는, 그 전자정보를 당해 정보저장매체등 또는 다른 저장매체로 이전 또는 복제하거나 이를 출력하는 방법으로 압수·수색할 수 있다.
2020	이재윤 "클라우드 환경에서 역외 압수·수색에 관한 연구"[1241]	§215③ 신설	③ 검사 또는 사법경찰관은 압수할 전자정보가 다른 컴퓨터에 기억되어 있다고 인정되고 컴퓨터 시스템을 통해 그 전자정보에 접근할 수 있는 경우에 법원으로부터 그 전자정보를 확보하기 위한 정당한 권한을 얻은 경우에 한하여 다른 정보저장매체에 대한 수색을 할 수 있다. 이 경우 제106조제3항에 따라 그 컴퓨터 등 또는 다른 정보저장매체에 복제하여 압수할 수 있다
2020	최용성·강동욱, "현행 디지털 증거제도 입법화 방안 연구"[1242]	§106④ 신설	④ 법원은 압수·수색 대상인 컴퓨터 등 정보처리장치와 정보통신망으로 연결(=link)되어 있는 정보저장매체등에 집행 대상 정보가 대한민국영역 내에 보관되어 있다고 인정할 만한 상당한 이유가 있는 경우에는, 그 정보를 당해 정보처리장치 또는 다른 정보저장매체로 이전 또는 복제하거나 이를 출력하는 방법으로 압수·수색할 수 있다. 이 경우 당해 정보처리장치 관리자의 적법한 범위를 초과하여 집행할 수 없다.

이와 같이 논문이나 보고서에서 제시하고 있는 원격지 압수수색 입법안은 기존의 압수수색 규정 가운데 하나의 조항을 신설하는 방식을 취하고 있음을 볼 수 있다. 즉 별도로 원격지 압수수색에 관한 규정을 두기보다는 기존의 압수수색 방식에 더하여, '정보통신망으로 연결된 매체 내 정보의 압수'를 추가함으로써 대법원과 같은 관점, 즉 기존의 압수수색 규정으로 포섭하고자 하고 있음을 알 수 있다. 다만 원격지 압수수색의 요건으로서 '원격지 매체에 정보가 저장되어 있다고 인정할 만한 상당한 이유'라고 하는 상당성 요건을 둠으로써 그 범위를 제한하고 있다. 그 외에 이재윤 논문에서 제시하고 있는 입법안의 경우에서만 '법원으로부터 그 전자정보를 확보하기 위한 정당한 권한'이라고 하는 규정을 둠으로써 대법원이 제시한 '적법하게 취득한 권한'을 요건으로 하고 있음을 볼 수 있다. 또한 최용성·강동욱 논문에서는 원격지

1239) 박병민·서용성, 앞의 연구보고서, 308면.
1240) 차종진, 앞의 연구보고서, 105면.
1241) 이재윤, "클라우드 환경에서 역외 압수·수색에 관한 연구", 박사학위논문, 성균관대학교, 2020.8, 179면.
1242) 최용성·강동욱, 앞의 논문, 98면.

압수수색의 범위를 '대한민국 영역 내'라고 명시함으로써 관할권 문제가 발생하지 않도록 하고 있다. 하지만 상당수의 정보통신서비스제공자의 서버가 해외에 소재하고 있는 점을 감안해 볼 때, 동 입법안에 의하면 원격지 압수수색의 범위가 지나치게 제한되는 문제가 있다고 할 것이다. 그리고 원격지 압수수색의 방식에 있어서는 모든 입법안들이 압수수색 대상이 된 '정보처리장치 또는 다른 저장매체로 복제 또는 출력'을 제시하고 있다.

이와 같이 기존의 압수수색 규정에 원격지 압수수색방식을 포섭하고자 하는 경우 오히려 원격지 압수수색의 적법성 요건을 제대로 갖추기 어려운 한계가 있다고 보여진다. 따라서 기존의 압수수색 규정과 별도의 원격지 압수수색 규정을 두고 적법절차적 요건을 명시하는 것이 동 제도의 취지와 실효적 통제를 가능하게 하는 것이라 할 것이다.

따라서 본 보고서에서는 원격지 압수수색에 관한 입법안과 관련하여 혐의사실과의 관련성 및 원격지 매체 내 정보가 존재할 수 있다는 상당성 요건, 수사기관에 의한 계정접속 권한과 수단의 적법성, 관할권 문제 등을 고려하여 다음과 같은 입법안을 제시해 보고자 한다.

제217조 (원격지 압수수색) ① 검사 또는 사법경찰관은 피의사실과 관계가 있다고 인정할 수 있는 전자정보가 압수수색 대상인 컴퓨터 등 정보처리장치와 정보통신망으로 연결되어 있는 정보저장매체 등에 보관되어 있다고 인정할만한 상당한 이유가 있는 경우에는, 지방법원판사에게 그 사유 등을 소명하여 발부받은 영장에 의하여 압수 수색할 수 있다.

② 제1항에 의하여 정보통신망으로 연결된 정보저장매체 등으로부터 해당 사건과 관계가 있다고 인정할 수 있는 전자정보의 압수는 해당 정보처리장치 또는 다른 저장매체로 이전, 복제하거나 출력하는 방법으로 할 수 있다.

③ 제1항에 의하여 정보통신망으로 연결된 정보저장매체 등에 보관된 전자정보에의 접근권한은 적법한 절차에 의해 획득해야 하며, 해당 정보처리장치 관리자의 접근권한의 범위를 초과해서는 안 된다.

④ 압수수색 대상인 전자정보가 정보통신망으로 연결된 국외에 소재하는 정보저장매체에 있는 경우, 국가간 협약 또는 국제법상 요건에 따라야 한다.

라. 디지털 증거 온라인 압수수색

온라인 수색은 "타인의 정보기술시스템 이용을 감시하고, 저장된 내용을 읽고 기록하기 위한 목적으로 기술적 수단을 사용하여 타인의 정보기술시스템에 은밀하게 접근하는 행위"[1243]로서, 특정범죄에 대응한 범죄예방 및 범죄 진압을 위해 도입된 국가에 의한 합법적 해킹이라고 할 수 있다.[1244] 즉 수사방법 자체가 해킹이라는 기술적 수단과 비밀성을 전제로 하기 때문에 디지털 증거를 확보하기 위한 강제수사 가운데 가장 강력한 방법이고, 따라서 그로 인한 기본권 침해 역시 매우 크다고 할 수밖에 없다.

그럼에도 불구하고 이와 같이 강력한 강제수사방법이 필요한 것은 기존의 수사방법으로는 암호화 기술로 무장된 온라인 플랫폼상의 중대범죄 – 테러나 조직범죄, 마약범죄, 아동음란물 및 성착취물 유통, 자금세탁 등 – 로 인해 야기되는 국가의 안전, 개인의 생명, 신체, 자유에 대한 심각한 침해에 대응하지 못하는 현실적 한계에 부딪혀 있기 때문이라 할 수 있다. 실제로 미국, 프랑스, 독일 등의 경우 마약, 무기, 청부살인, 위조지폐 등의 거래처로 사용되었던 다크웹에 대한 수사에 있어서는 국가 간 협조를 통해 온라인 수색방법을 사용하고 있음은 앞서 기술한 바와 같다. 그리고 온라인 수색제도를 법제화하고 있는 국가들 – 프랑스, 영국, 독일 등 – 이 공통적으로 법제화하고 있는 요건으로는 첫째, 대상범죄가 조직범죄와 같은 중대범죄로 제한되어 있다는 것, 둘째, 타인의 정보통신기술시스템에 당사자의 동의 없이 데이터를 감시, 기록, 저장, 전송할 수 있는 기술적 수단을 설치할 수 있다는 것, 셋째, 그 행위와 그 행위로 인해 달성하고자 하는 목적이 비례하는지, 다른 방법으로는 사실관계 규명이 불가능한지 등의 비례성과 보충성 원칙을 두고 있다는 점이다.

이와 같이 온라인 수색제도는 정보통신시스템에 대한 국가의 비밀감시조치라는 점에서 필요 최소한도의 범위 내에서만 허용되어야 그 남용 가능성을 배제할 수 있다고 할 것이다. 따라서 이를 입법화함에 있어서는 비례성 원칙, 보충성 원칙, 명확성 원칙을 준수할 수 있는 요건을 규정해야 할 뿐 아니라 엄격한 형태의 절차법적 통제장치를 둠으로써 온라인 수색으로 인한 기본권 침해의 위험성을 최대한 억제해야만 한다.

따라서 온라인 수색은 비밀성에 기반한 강제수사처분이기 때문에 법관의 영장에

1243) BTS-Drs.18/12875; KK-StPO/Bruns, 8.Aufl.2019, StPO §100b Rn.3(박병민·서용성, 앞의 연구보고서, 134면에서 재인용).

1244) 박희영, "국가의 합법적인 해킹행위로서 온라인 수색에 관한 독일 법제 동향", 55면.

의한 사전심사 대상이 된다고 보아야 하고, 긴급성을 이유로 한 법관유보의 예외는 인정하지 않는 것이 타당하다고 본다. 다만, 비밀수사처분으로서의 취지를 구현하기 위해서는 사전영장 제시 및 통지에 관한 규정은 예외를 인정하는 것이 타당하다고 본다. 그리고 온라인 수색의 피처분자는 피의자로 제한되어야 하지만, 피의자가 제3자의 정보통신시스템을 이용하는 경우에는 제3자에 대해서도 온라인 수색이 허용될 필요성이 있다고 할 것이다. 이 경우 제3자에 대해서는 비밀유지의무를 부과함으로써 온라인 수색의 비밀성이 유지되도록 해야 할 것이다.

온라인 수색의 대상과 관련해서는 중대범죄로 제한되어야 함은 당연하지만, 어느 범위까지 중대범죄로 볼 것인가는 입법정책적 논의를 거쳐서 결정되어야 할 문제라 할 수 있다. 다만 생각건대 「통신비밀보호법」상 통신제한조치 대상 범죄 가운데 특히 내란죄, 간첩죄, 범죄단체조직죄, 살인죄, 돈세탁 등과 같은 종래의 중대범죄와 함께 아동·청소년 대상 성범죄, 아동 음란물 및 성착취물 유포, 마약류 유통 등과 같이 정보통신시스템을 범죄의 수단으로 악용하여 심각하게 개인의 신체, 자유 등을 침해하는 범죄로 제한하는 것이 바람직하다 할 것이다. 또한 온라인 수색은 정보통신기술시스템에 대한 기술적 침입을 허용하는 것이기 때문에 그 기간이 제한적이어야 하는데, 현행법상 통신제한조치보다 기본권 침해의 우려가 크다는 점을 고려하면 통신제한조치 기간보다 넘어서서 허용되는 것은 불합리하다고 볼 것이다.

그리고 무엇보다도 온라인 수색은 개인의 사생활에 대한 침해의 우려가 크다는 점에서 볼 때, 온라인 수색으로 확보된 전자정보가 혐의사실과 무관한 사생활에 관한 것일 때에는 지체없이 삭제하도록 하되, 혐의사실과 관련성이 있는 사생활 정보인 경우에는 법원으로 하여금 그 사용가능성 여부를 결정하도록 한 독일의 입법례를 참고할 필요가 있다고 본다. 마지막으로 온라인 수색에 대한 절차법적 통제는 영장주의 원칙에 의한 사법통제와 아울러 국회에 의한 사후통제가 병행되어야 한다고 본다. 통신제한조치의 경우에도 국회 상임위원회와 국정감사 및 조사위원회로 하여금 통신제한조치에 관해 보고를 요구할 수 있도록 규정하고 있는 것과 마찬가지로, 온라인 수색에 대해서도 기술침입시스템에 대한 정보, 수색 대상이 된 정보통신시스템에 대한 정보, 온라인 수색 대상이 된 데이터의 유형과 범위, 기간 등을 분기별, 반기별 또는 연례보고서 형태로 국회에 보고하도록 할 필요가 있다고 본다.

온라인 수색과 관련해서는 현재까지 국회에 발의된 「형사소송법」 개정 입법안이 단 한 건도 없으며, 논문의 경우에는 "온라인 수색의 법제화 방안 연구"라고 하는 석사논문에서 간단한 입법안을 제시한 것이 전부이다. 다만 이 논문에서는 국가안보 목적 온라인 수색에 대해서는 「통신비밀보호법」과 「테러방지법」에 규정을 신설하는 안을 제시하고 있음을 볼 수 있다.

연도	저자 및 논문	대상조문	개정(신설) 내용
2020	정이현, "온라인 수색의 법제화 방안 연구"[1245]	§120③ 신설	③ 디지털 정보를 대상으로 수색영장을 집행하는 경우, 디지털 기기에 비공개 정보수색도구를 설치하는 등 필요한 처분을 할 수 있다.

이처럼 온라인 수색에 대한 입법안이 제시되기 어려운 데는 온라인 수색의 본질적 특성이 정보화 사회의 기본권이라 할 수 있는 정보자기결정권 또는 IT 기본권에 대한 심각한 침해 가능성을 수반하기 때문이라 할 수 있다. 즉 스마트폰과 인터넷을 통한 사이버공간으로 사회·경제·문화·예술 등 개인의 모든 일상생활 영역이 확장되었기 때문에, 이러한 모든 정보가 생성, 이용, 저장, 관리되는 정보통신시스템에 기술적으로 침입하여 비밀리에 감시한다는 것은 '빅브라더'의 위험을 상기시키기 때문이다.

하지만 고도화된 IT 기술에 기반한 폐쇄적인 비닉성(祕匿性) 온라인 플랫폼을 이용하여 국가의 안전뿐 아니라 개인의 생명, 신체, 자유에 대한 심각한 범죄가 이루어지고 있음에도 불구하고, 이에 대응할 수 있는 기술적 수단이 개인의 기본권을 침해하는 수단이라는 이유로 거부하게 되면, 현실적으로 범죄의 실체적 진실에 접근하는 것 자체가 불가능하게 되어 범죄를 방임하는 결과를 초래할 수 있다는 점에 대한 진지한 검토가 필요하다고 본다. 앞서 살펴본 것처럼, 이미 온라인 수색제도를 활용하고 있는 국가들과 같이 테러범죄나 마약, 청부살인, 아동포르노 유포 등과 같은 중대한 범죄가 우리나라에서는 아직 심각한 수준이 아니기 때문에 그와 같이 중대한 온라인 수색제도를 도입할 필요성이 없다고 하는 것은 지나치게 안일한 인식이라 하지 않을 수 없다. 우리 사회 역시 N번방 사건에서 보았듯이 텔레그램을 이용하여 아동·청소년 성착취물이 제작 및 유포되고 있었으며, 그 사건 이후로도 여전히 동종의 유사한 범죄행위들이 텔레그램 내에서 이루어지고 있다고 보는 것이 경찰의 시각이다. 또한

1245) 정이현, 앞의 석사학위논문, 103면.

마약거래 역시 텔레그램이나 다크웹 등을 통해 거래되고 있는 것이 현실이다.[1246] 이와 같이 기존의 법률과 수사방식을 통해서는 접근할 수 없는 영역에서 이루어지고 있는 범죄에 대응하기 위한 현실적인 수단이 필요하다는 사실은 자명하다고 볼 수 있다.

그럼에도 온라인 수색제도의 도입에 대한 의혹의 눈길을 지우기 어려운 것도 사실이라 할 수 있다. 즉 이제까지 우리 수사기관들의 불법적 수사관행과 공권력 남용의 행태가 사라지지 않고 있는 현실에서 사실상 가장 강력한 수단이라 할 수 있는 온라인 수색을 허용하기에는 불안이 앞서기 때문이다. 따라서 온라인 수색제도의 도입에 있어서는 법률을 통한 입법적 통제, 법원을 통한 사법적 통제, 그리고 국회에 의한 사후통제를 거치도록 함으로써 그 남용가능성을 최대한 배제해야만 할 것이다.

이러한 관점에서 본 보고서에서는 온라인 수색과 관련하여 다음과 같은 입법안을 제시해 보고자 한다.

제218조 (온라인 압수수색) ① 검사 또는 사법경찰관은 다음의 경우 지방법원 합의부로부터 영장을 발부받아 피의자가 이용하는 정보통신시스템에 기술적 수단을 이용하여 개입함으로써 정보를 압수수색할 수 있다.

1. 다음 각목의 범죄를 범했거나 실행에 착수했다는 혐의를 뒷받침할 수 있는 사실이 있는 경우
   가. 형법 제92조 내지 제98조의 죄, 제114조, 제119조, 제198조, 제207조, 제287조 내지 제291조
   나. 국가보안법 제3조 제1항 및 제2항에 해당하는 죄, 제4조 제1항 제1호와 제2호에 해당하는 죄
   다. 마약류관리에 관한 법률에 규정된 범죄 중 제58조 제1항에 해당하는 죄
   라. 아동청소년 성보호법 제11조 제1항, 제2항 및 제3항에 해당하는 죄
   마. 아동청소년에 대한 성폭력범죄의 처벌 등에 관한 특례법 제14조 제2항 및 제3항의 죄
2. 다른 방법으로는 혐의사실을 입증하는 것이 매우 곤란하거나 불가능한 경우② 제1항에 의하여 정보통신시스템에 기술적 수단을 이용하여 개입함으로써 정보를 확보하는 경우 영장의 범위를 벗어난(또는 혐의사실과 관련성이 없는) 정보는 즉시 삭제해야 한다.

③ 제1항에 의하여 정보통신시스템에 기술적 수단을 이용하여 개입함으로써 정보를 확보하는 경우 그 기간은 1개월을 초과할 수 없다. 다만 불가피한 사유로 연장이 필요한 경우 법원의 심사를 거쳐 1회에 한해 연장할 수 있다.

1246) 장승주 기자, "변화하는 마약거래 특성 감안해 형사절차 개선해야", 『아주경제』 2023년 3월 12일자 기사(https://www.ajunews.com/view/20230312090826557; 최종접속일 2023.11.11.).

④ 제1항에 의하여 기술적 수단이 개입되는 정보통신시스템 관리자에 대해서는 압수수색이 완료된 후 그 사실을 통지해야 한다. 이 경우 해당 정보통신시스템 관리자는 그 사실을 비밀로 해야 한다.
⑤ 검사 또는 사법경찰관은 제1항에 따른 기술적 수단을 사용하는 경우 그에 관한 구체적인 사항을 기록하여 연례보고서로 국회 정보통신위원회에 보고해야 한다. 다만, 혐의사실과 관련된 범죄수사가 진행 중이고 공개되어서는 안되는 경우에는 차년도 연례보고서로 대신할 수 있다.
1. 사용한 기술적 수단의 명칭과 사용 기간
2. 관련 범죄혐의사실
3. 압수수색한 정보의 유형
⑥ 제1항에 의하여 기술적 수단이 개입되는 정보통신시스템에 대해서는 본 조항으로 인하여 제기되는 모든 민형사상 책임으로부터 면제된다.
⑦ 제1항에 의하여 기술적 수단이 개입되는 정보통신시스템이 국외에 위치하는 경우 국가간 협약 또는 국제법상 요건에 따라야 한다.

제3절 | 디지털 증거 압수수색절차 개선을 위한 정책적 제언

1. 위법수집증거배제법칙 적용의 강화

제1절과 제2절에서는 디지털 증거 압수수색절차를 위한 입법적 제언을 제시하여 보았다. 형사절차에서 디지털 증거가 문제되기 시작한 지가 이미 20여 년을 넘어섰음에도 불구하고 여전히 12년 전에 규정된「형사소송법」제106조 제3항, 단 하나의 법조항에 의존하고 있기 때문에 디지털 증거 압수수색절차에 관한 입법적 정비는 무엇보다도 시급한 입법과제라 할 수 있다.

그러나 무엇보다도 고려되어야 할 부분은, 이와 같이 디지털 증거 압수수색과 관련한 입법규정의 미비가 적법절차의 문제와 직결될 수밖에 없다는 점이다. 즉 디지털 증거 압수수색절차에 관한 구체적인 법률규정이 없기 때문에 적법절차 준수 여부를 어떠한 기준으로 판단할 것인가 하는 것이다. 현재로서는 '선별압수 원칙, 매체압수 예외'를 제외한 나머지 디지털 증거 압수수색과 관련한 절차적 문제는 모두 대법원의 해석을 기준으로 적법절차 여부가 논하여지고 있다. 즉 디지털 증거 압수수색절차의

적법성과 관련하여 대법원은 참여권, 별건 혐의사실에 대한 압수수색, 영장제시 원칙, 임의제출 시 압수범위 등과 관련하여 세분화 된 판단기준을 제시하고 있다.

하지만 디지털 증거 압수수색절차 위반으로 압수한 증거의 증거능력을 배제함에 있어서 법률이 아닌 판례에 의존함으로 인해, 새로운 판례가 나올 때마다 압수수색 실무 담당자들은 판례내용을 숙지해야 하는데, 이를 제대로 숙지하지 못함으로 인해 압수한 증거를 유죄의 증거로 사용하지 못하는 경우가 발생하고 있다. 경우에 따라서는 사회적 이목이 집중되거나 법원이 관심을 갖는 사건에 있어서는 디지털 증거 압수수색과 관련한 판례의 기준을 제대로 준수하지만, 그렇지 못한 사건에 있어서는 그 기준을 제대로 준수하지 않는 경우도 있다. 법원 역시 디지털 증거 압수수색절차와 관련하여 제시된 판례의 기준을 제대로 알지 못하는 피고인이 절차의 적법성을 문제 삼지 않는 한, 모든 사건에 있어서 디지털 증거 압수수색절차의 적법성 여부를 판단하지는 않기 때문에 결국 적법절차 원칙의 적용이 불공정해지는 문제가 야기될 수 있다.

따라서 디지털 증거 압수수색절차의 적법성을 일관되게 규율할 수 있는 법규정이 마련되어야 적법절차 준수 여부에 대한 명확하고도 공정한 판단이 이루어질수 있을 뿐 아니라 위법수집증거배제법칙의 적용도 보다 강화할 수 있다고 할 것이다. 디지털 증거 압수수색에 있어서는 개인의 프라이버시와 관련된 정보가 노출될 우려가 크기 때문에, 절차적 규정의 적용이 엄격하게 이루어질 필요가 있다는 점에 대해서는 이론의 여지가 없다고 할 것이다. 하지만 절차적 규정이 명확하지 않은 현재의 상황하에서는 위법수집증거배제법칙의 적용 여부가 법관의 적법성 판단기준에 의해 좌우될 수도 있다고 할 것이다.

디지털 증거 압수수색절차의 적법성을 일관되게 유지할 수 있는 명확한 법규정을 마련하고, 그 절차적 규정을 위반한 경우에는 예외없이 위법수집증거배제법칙을 적용함으로써 디지털 증거 압수수색에 수반될 수 있는 프라이버시 및 기본권 침해의 가능성을 최대한 억제하는 것이 바람직하다고 할 것이다. 즉 위법수집증거배제법칙의 엄격한 적용을 통해 증거의 사용을 배제하는 것이 어떠한 절차법적 규정보다도 강력하게 수사절차의 적법성을 담보할 수 있다고 할 것이고, 따라서 디지털 증거 압수수색과 관련하여 프라이버시와 기본권 보장을 위해서는 위법수집증거배제법칙의 강화는 필요불가결한 조건이라 할 것이다.

이와 같이 디지털 증거 압수수색에 있어서 절차적 규정을 위반한 경우에는 예외없이 압수한 전자정보를 유죄의 증거로 사용하지 못하게 한다면 수사기관으로서도 절차적 규정의 준수를 위해 노력하지 않을 수 없다고 할 것이다. 대법원이 판례를 통해 디지털 증거 압수수색과 관련하여 적법절차적 판단기준을 오랫동안 제시해 왔음에도 불구하고, 여전히 수사기관들이 '선별압수 원칙, 매체압수 예외', '영장제시 원칙', '참여권 보장', '압수목록 교부' 등과 같은 디지털 증거 압수수색의 기본조차도 준수하지 않는 경우[1247]들이 있음을 볼 때, 절차법적 규정의 마련과 함께 위법수집증거배제법칙의 적용을 강화함으로써 압수수색 실무 담당자들의 적법절차 준수에 대한 인식을 변화시킬 필요가 있다고 할 것이다.

2. 압수종료 후 무관정보 삭제 및 폐기 방안 재고

디지털 증거 압수 시 선별압수가 원칙이기 때문에 압수수색 현장에서 혐의사실과 관련된 부분만을 선별, 복제, 출력하는 것이 일반적이지만, 현장 선별에 시간이 오래 걸리거나 증거의 은닉, 삭제 등으로 포렌식 과정이 필요한 경우에는 정보저장매체를 복제하거나 이미징한 후 수사기관 내에서 선별작업을 거치게 된다. 이 경우 디지털 증거의 무결성 확보를 위해 압수수색 대상 정보저장매체의 해시값과 이미징한 매체의 해시값 비교를 통해 증거의 무결성과 동일성을 확보하는 방식을 취하게 된다. 하지만 수사기관 내 포렌식 과정에서 선별작업을 통해 혐의사실과 관련된 정보만을 선별, 복제, 출력한 경우, 이미징한 사본 내에는 무관정보가 존재할 수 있는데 이러한 이미징 사본을 그대로 수사기관에 보관하게 되면 경우에 따라 이미징사본 내에서의 영장없는 추가적인 압수수색 또는 별건 혐의에 대한 수사 단서를 확보하는 데 이용될 가능성을 배제하기 어려운 문제가 있다. 또한 임의제출물 압수 시 제출자가 제출하고자 하는 전자정보의 범위를 정하지 않고 정보저장매체 전체를 제출한 경우에도 동일한 문제가 야기될 수 있다. 이는 수사기관으로 하여금 영장주의 원칙을 우회하는 수단을 제공할 수 있다는 점에서 바람직하지 않다고 볼 수 있다. 이와 같이 수사기관 내 선별 후

1247) 대법원 2022.7.14.자 2019모2584 결정; 대법원 2022.7.28. 선고 2022도2960 판결; 대법원 2023.6.1. 선고 2018도19782 판결 등.

남게 되는 전자정보의 문제점과 관련하여 대법원은 "수사기관이 혐의사실과 관련있는 정보를 선별하여 압수한 후에도 그와 관련이 없는 나머지 정보를 삭제, 폐기, 반환하지 아니한 채 그대로 보관하고 있다면 혐의사실과 관련이 없는 부분에 대하여는 압수대상이 되는 정보의 범위를 넘어서는 정보를 영장없이 압수수색하여 취득한 것이어서 위법하고"[1248]라고 판시하고 있다. 이러한 대법원 판례에 따라 현재 수사기관들도 선별된 유관정보를 제외한 나머지 부분은 삭제하거나 폐기하는 방식을 취하고 있다.

하지만 이와 같이 사건이 종료되기 전에 해시값을 통해 무결성과 동일성을 입증할 수 있는 이미징사본을 삭제 또는 폐기하는 것은 디지털포렌식의 기본원칙이라 할 수 있는 재현의 원칙을 포기하는 것이라 할 수 있다. 즉 해당 증거가 법정에서 문제되었을 때 디지털포렌식을 통해 재검증하거나 재현할 수 있어야 함에도 불구하고 이미 압수종료 단계에서 삭제되기 때문에 현실적으로 불가능하다고 할 수 있다. 또한 원본 저장매체에서 삭제된 파일을 복원하는 경우 온전한 형태의 데이터가 아니기 때문에 바로 해시값이 추출될 수 있는 것이 아니고, 분석과정을 통해 조합된 파일을 복원했을 때 비로소 해시값이 추출되는바, 복원된 파일이 이미징사본에서 삭제되었던 데이터를 복원한 것이 맞는가를 입증하기 위해서는 이미징사본이 있어야 하지만, 무관정보 삭제를 이유로 이미징사본을 폐기하게 되면 해시값만으로는 이를 입증하는 것이 불가능하게 될 수 있다.

더욱이 원본 정보저장매체는 피의자에게 즉시 반환되기 때문에 이미 반환되는 시점에서 원본 정보저장매체의 해시값은 의미가 없게 될 뿐 아니라, 피의자에 의해 원본 정보저장매체의 변경, 삭제 등이 이루어지기 때문에 압수 당시의 원본매체와 동일성을 유지할 수 있는 것은 이미징한 사본뿐이라고 할 수 있다.

이는 피의자의 입장에서도 압수된 방대한 양의 정보 가운데 수사기관이 선별한 정보가 원본 정보저장매체에서 이미징한 사본으로부터 추출한 것이 맞는가에 대하여 다투고자 할 때 이미징사본이 없기 때문에 수사기관에 의한 조작이 있어도 확인할 방법이 없게 된다. 현실적으로 피의자에게 압수한 전자정보의 상세목록이 교부된다고 하더라도 방대한 양의 정보목록을 일일이 확인하는 것이 가능하지 않기 때문에, 비록 피의자가 압수수색 과정에 참여하고 압수목록을 확인했다고 하더라도 압수된 디지털

1248) 대법원 2022.1.14.자 2021모1586 결정.

증거의 원본성과 동일성 여부를 확인할 수 있는 이미징사본은 최소한 사건이 종료되는 시점까지는 남겨둘 필요성이 있다고 할 것이다.

따라서 수사기관에서 압수한 디지털 증거의 이미징사본의 남용 내지 오용 가능성을 배제하고자 하는 취지에서 행해지고 있는 압수 직후 이미징사본의 삭제 및 폐기는 오히려 형사절차의 공정성을 저해하는 요소가 될 수 있다는 점도 고려할 필요가 있다고 할 것이다. 이러한 점에서 볼 때, 수사기관에서 확보한 이미징사본을 언제, 어떻게 삭제 또는 폐기할 것인가에 대한 절차적 논의가 있어야 할 것으로 생각된다. 만약 수사기관에 의한 이미징사본의 오남용에 대한 우려를 배제하고자 하는 것이라면 해당 사건에 대한 판결이 확정될 때까지 법원에 보관하도록 하는 방식도 하나의 대안이 될 수 있을 것이다. 그리고 판결이 확정된 후 이미징사본을 삭제 또는 폐기하게 된다면 무관정보의 오남용에 대한 우려는 배제할 수 있다고 할 것이다.

참고문헌

1. 국내 문헌

(1) 단행본

독일법연구회(譯), 『독일 형사소송법』, 사법발전재단, 2018.

신동운, 『신형사소송법』(제5판), 법문사, 2014.

이재상·조균석, 『형사소송법』(제12판), 박영사, 2019.

조성훈, 『역외 전자정보 압수·수색 연구』, 박영사, 2020.

(2) 학술지논문

구길모, "디지털 증거 압수수색과 참여권 보장", 『형사법연구』 제34권 제4호, 한국형사법학회, 2022.12.

권창국, "임의제출에 의한 수사기관의 전자정보 압수와 관련한 제 문제의 검토 -대상판례: 대법원 2021.11.18. 선고 2016도348 전원합의체 판결 및 대법원 2022.1.27. 선고 2021도11170 판결-", 『사법』 통권 제62호, 사법발전재단, 2022.12.

김기범, "압수·수색영장의 전자적 제시에 관한 입법적 연구", 『경찰학연구』 제18권 제2호, 경찰대학, 2018.6.

김기준, "수사단계의 압수·수색 절차 규정에 관한 몇 가지 고찰", 『형사법의 신동향』 제18호, 대검찰청, 2009.2.

김민이, "디지털증거 압수·수색관련 미국, 영국, 프랑스 입법례", 『최신입법정보』 통권 제127호, 국회도서관, 2021.4.

김범식, "영·미의 디지털 증거 압수·수색에 관한 소고", 『형사법의 신동향』 통권 제45호, 대검찰청, 2014.12.

김슬기, "미국에서의 정보저장매체의 압수·수색에 관한 연구", 『법학연구』 제25권 제4호, 연세대학교 법학연구소, 2015.12.

김시원, “전자영장에 관한 연구 -집행절차를 중심으로-”, 『사법』 통권 제54호, 사법발전재단, 2020.12.

김연희, “온라인 수색 도입을 위한 문제점과 방안에 관한 소고”, 『법학연구』 제64호, 전북대학교 법학연구소, 2020.12.

김인회, “2016년 형사소송법 중요 판례”, 『인권과 정의』 제464호, 대한변호사협회, 2017.1.

김학경, “영국 수사권한법에 규정된 온라인수색 법제에 관한 소고”, 『형사법의 신동향』 제74호, 대검찰청, 2022.3.

김학경, “미국의 온라인수색 제도에 관한 연구: 연방형사소송규칙 제41장 개정내용 중심으로”, 『시큐리티연구』 제72호, 한국경호경비학회, 2022.9.

김한균, “피의자 휴대전화 비밀번호의 제출 강제 -영국 입법례 참고한 디지털 증거 압수·수색시 협력의무 부과 법안 추진 비판-”, 『형사소송 이론과 실무』 제13권 제2호, 한국형사소송법학회, 2021.6.

남정아, “미국 연방헌법 수정증보 제4조의 압수 및 수색의 범위에 관한 고찰 -연방법원 판례의 동향을 중심으로-”, 『서울법학』 제27권 제3호, 서울시립대학교 법학연구소, 2019.11.

라광현·윤해성, “유럽평의회 사이버범죄방지협약 성과에 대한 실증적 검토”, 『범죄수사학연구』 제5권 제1호, 경찰대학 범죄수사연구원, 2019.6.

박성민, “전자정보의 압수수색에 있어 정보검색의 성격과 피압수자 참여권 보장의 의미”, 『형사정책』 제28권 제2호, 한국형사정책학회, 2016.9.

박용철, “정보저장매체 임의제출 압수의 의의”, 『외법논집』 제46권 제1호, 한국외국어대학교 법학연구소, 2022.2.

박재성, “사이버범죄 국제조약의 동향 - 부다페스트 협약 제2 추가의정서 및 유엔 사이버범죄 조약을 중심으로 -”, 『저스티스』 통권 제185호, 한국법학원, 2021.8.

박중욱, “수사절차에서의 “비밀의 강제처분”의 합헌성 요건 – 기술적 비밀의 수사처분에 대한 독일 연방헌법재판소 판결의 분석을 중심으로 –”, 『형사법의 신동향』 통권 제63호, 대검찰청, 2019.6.

박중욱, “수사기관 내에서의 범죄혐의 관련 정보 탐색 등 행위의 법적 성격 – 독일 형사소송법 제110조에 관한 논의를 참고하여 –”, 『비교형사법연구』 제24권 제4호, 한국비교형사법학회, 2023.1.

박중욱, “전자정보의 압수수색과 피의자의 참여권 -대법원 입장의 비판적 수용 및 독일 논의의 참고-”, 『형사정책연구』 제34권 제1호, 한국형사법무정책연구원, 2023.3.
박중욱, “제3자 보관 정보의 압수수색과 정보주체에 대한 통지 - 강제처분의 공개성/비밀성에 대한 독일 논의를 참고하여 -”, 『원광법학』 제38권 제3호, 원광대학교 법학연구소, 2022.9.
박중욱, “수사목적 온라인 수색의 허용요건 – 독일의 논의를 참고한 입법론적 검토 –”, 『형사정책연구』 제34권 제3호, 한국형사법무정책연구원, 2023.9.
박혁수, “디지털 정보 압수수색의 실무상 쟁점”, 『형사법의 신동향』 통권 제44호, 대검찰청, 2014.9.
박희영, “정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권(下)”, 『법제』, 법제처, 2008.11.
박희영, “독일에 있어서 경찰의 온라인 수색에 관한 판례 및 법제 동향”, 『최신외국법제정보』 2011년 제2호, 한국법제연구원, 2011.4.
박희영, “예방 및 수사목적의 온라인 비밀 수색의 허용과 한계”, 『원광법학』 제28권 제3호, 원광대학교 법학연구소, 2012.9.
박희영, “국가의 합법적인 해킹행위로서 온라인 수색에 관한 독일 법제 동향”, 『최신외국법제정보』 2019년 제1호, 한국법제연구원, 2019.4.
박희영, “유럽에서 온라인 수색과 암호통신망 EncroChat 사건”, 『형사법의 신동향』 통권 제78호, 대검찰청, 2023.3.
박희영·홍선기, “독일 정보기관의 공법 체계 및 경찰과의 분리원칙”, 『법학논집』 제26권 제3호, 이화여자대학교 법학연구소, 2022.3.
방경휘, “수사상 역외 압수·수색에 관한 연구 -일본 최고재판소 레이와 3년 2월 1일 결정을 계기로-”, 『법학논총』 제35권 제1호, 국민대학교 법학연구소, 2022.6.
백승주, “미국의 압수·수색영장 일부기각 및 압수방법 제한에 관한 실무연구 -디지털증거를 중심으로-”, 『법조』 통권 제682호, 법조협회, 2013.6.
손동권, “새로이 입법화된 디지털 증거의 압수,수색제도에 관한 연구 -특히 추가적 보완입법의 문제-”, 『형사정책』 제23권 제2호, 한국형사정책학회, 2011.12.
송규영, “해외 디지털증거의 확보 -관할권의 확정 및 디지털증거 보존제도의 필요성을 중심으로-”, 『저스티스』 통권 제173호, 한국법학원, 2019.8.
송영진, “디바이스 복호화 명령과 자기부죄거부특권: 미국 법원의 실행과 영국의 입법

례를 중심으로-", 『형사정책연구』 제31권 제1호, 한국형사법무정책연구원, 2020.3.

우지이에 히토시, "일본의 전자적 증거 압수에 관한 2011년 개정법 소개", 『형사법의 신동향』 통권 제49호, 대검찰청, 2015.12.

이동희, "형사소송법의 편장체계 전면개정의 필요성과 개정시론 -일본 형사소송법에 대한 비교검토를 포함하여-", 『비교형사법연구』 제21권 제1호, 한국비교형사법학회, 2019.4.

이병규, "영국헌법의 본질과 특색", 『동아법학』 통권 제48호, 동아대학교 법학연구소, 2010.8.

이순옥, "인터넷서비스제공자가 보관한 정보에 대한 압수·수색 절차", 『법학논문집』 제43집 제3호, 중앙대학교 법학연구원, 2019.12.

이완규, "디지털 증거 압수수색과 관련성 개념의 해석", 『법조』 제686호, 법조협회, 2013.11.

이완규, "디지털 증거 압수절차상 피압수자 참여방식과 관련성 범위 밖의 별건 증거 압수방법", 『형사법의 신동향』 통권 제48호, 대검찰청, 2015.9.

이원상, "온라인 수색에 대한 고찰: 독일의 새로운 논의를 중심으로", 『형사법연구』 제20권 제4호, 한국형사법학회, 2008.12.

이원상, "다크넷 수사를 위한 수사제도에 대한 소고", 『형사법의 신동향』 통권 69호, 대검찰청, 2020.12.

이진구·김일환, "통신비밀의 보호범위와 한계에 관한 비교법적 연구 -미국의 통신비밀 보호법제를 중심으로-", 『미국헌법연구』 제27권 제1호, 미국헌법학회, 2016.4.

이진국, "전자정보 압수·수색에서 피압수·수색 당사자의 참여권에 관한 일고", 『동아법학』 제11권 제4호, 아주대학교 법학연구소, 2018.2.

전치홍, "실시간 휴대전화 위치정보 추적 수사의 적법성에 대한 미국 판결의 최신 동향 -Carpenter v. United States 판결 이후의 미국 하급심 판결 동향을 중심으로-", 『법학논총』 제41권 제4호, 전남대학교 법학연구소, 2021.11.

정대희·이상미, "디지털증거 압수수색절차에서의 '관련성' 문제", 『형사정책연구』 제26권 제2호, 한국형사정책연구원, 2015.여름.

정희도, "영국 수사기관의 전자우편 취득절차 및 한계", 국외훈련검사연구논문집 제26집, 법무연수원, 2011.

조광훈, “전자정보의 압수수색절차에서 참여권의 범위와 한계 -대법원 2015.7.16.자 2011모1839 전원합의체 결정을 중심으로-”, 『법조』 제64권 제12호, 법조협회, 2015.12.

조성훈, “역외 디지털증거 수집과 국제형사 규범의 발전”, 『법학논총』 제43권 제3호, 단국대학교 법학연구소, 2019.9.

천성덕·강구민, “실무적 관점에서 본 원격지 서버에 대한 압수·수색 절차 제언”, 『형사소송 이론과 실무』 제11권 제1호, 한국형사소송법학회, 2019.6.

최병각, “휴대폰의 압수와 저장정보의 탐색”, 『비교형사법연구』 제22권 제3호, 한국비교형사법학회, 2020.10.

최용성·강동욱, “현행 디지털 증거제도의 입법화 방안 연구”, 『치안정책연구』 제34권 제3호, 경찰대학 치안정책연구소, 2020.9.

최우구, “영장에 의하지 아니하는 강제처분의 특수문제로써 스마트폰에 저장된 정보에 대한 수색 -Riley v. California 판결 평석-”, 『안암법학』 제47권, 안암법학회, 2015.3.

탁희성, “전자증거의 압수·수색에 관한 일고찰”, 『형사정책연구』 제15권 제1호, 한국형사정책연구원, 2004.3.

한상훈, “임의제출물의 영치와 위법수집증거 배제법칙 -대법원 2016.3.10. 선고 2013도11233 판결-”, 『법조』 제65권 제8호, 법조협회, 2016.10.

허황, “최근 개정된 독일 형사소송법 제100조b의 온라인 수색과 제100조a의 소스통신감청에 관한 연구”, 『형사법의 신동향』 통권 제58호, 대검찰청, 2018.3.

中村 真利子, “サイバー犯罪条約の第二追議定書によるサイバー犯罪捜査の変化”, 『성균관법학』 제35권 제1호, 성균관대학교 법학연구원, 2023.3.

(3) 학위논문

김무석, “디지털 포렌식 절차상 참여권 보장 방안에 대한 연구”, 석사학위논문, 고려대학교, 2019.2.

김승일, “전자서명 기반 전자영장을 활용한 압수·수색영장의 원격 집행 방안에 대한 연구 -금융계좌추적용 압수·수색영장 집행을 중심으로-”, 석사학위논문, 서울대학교, 2022.2.

노소형, “제3자 보관 디지털증거에 대한 긴급증거보전 제도 신설방안 연구”, 박사학위논문, 성균관대학교, 2020.8.

신상미, “원격지에 저장된 디지털 정보의 압수·수색에 관한 법적 연구”, 석사학위논문, 경찰대학교, 2021.2.

오기두, “형사절차상 컴퓨터 관련 증거의 수집 및 이용에 관한 연구”, 박사학위논문, 서울대학교, 1997.2.

이규봉, “디지털 증거 압수·수색 과정에서 피압수자 등의 참여 범위”, 석사학위논문, 고려대학교, 2021.2.

이상국, “원격지에 저장된 디지털 정보 접근방안 -원격 압수·수색을 중심으로-”, 석사학위논문, 서울대학교, 2020.2.

이숙연, “형사소송에서의 디지털증거의 취급과 증거능력”, 박사학위논문, 고려대학교, 2011.2.

이용, “디지털 증거 수집에 있어서의 협력의무”, 박사학위논문, 서울대학교, 2016.2.

이재윤, “클라우드 환경에서 역외 압수·수색에 관한 연구”, 박사학위논문, 성균관대학교, 2020.8.

전승수, “형사절차상 디지털 증거의 압수수색 및 증거능력에 관한 연구”, 박사학위논문, 서울대학교, 2011.2.

정대용, “사이버공간에서의 증거 수집과 기본권 보장에 관한 연구”, 박사학위논문, 고려대학교, 2018.2.

정성남, “경찰 수사현장에서 디지털 증거의 압수·수색에 관한 연구 -스마트 폰을 중심으로-”, 박사학위논문, 인천대학교, 2020.2.

정이현, “온라인 수색의 법제화 방안 연구”, 석사학위논문, 성균관대학교, 2021.2.

탁희성, “전자증거에 관한 연구 -압수·수색과 증거능력을 중심으로-”, 박사학위논문, 이화여자대학교, 2004.2.

허준, “수사절차상 압수·수색 편제 및 절차 개선에 관한 연구”, 박사학위논문, 아주대학교, 2020.8.

(4) 연구보고서 및 정부기관 발간자료

경찰청, 『2021 경찰통계연보』 제65호, 2022.11.

김재희·박희영, 『온라인 수색활동의 적법성 검토 및 도입방안 연구』, 연구용역보고서, 경찰청, 2022.12.

김현숙, 『영국의 PACE 법 연구』, 책임연구보고서 2011-19, 치안정책연구소, 2011.12.

대검찰청, 『검찰연감』, 2014~2022.

박병민·서용성, 『디지털 증거 압수·수색 개선방안에 관한 연구 -법률 개정에 관한 논의를 중심으로-』, 연구총서 2021-05, 사법정책연구원, 2021.3.

박지영, 『정보저장매체에 관한 압수·수색제도의 문제점과 개선방안』, NARS 현안보고서 제278호, 국회입법조사처, 2015.12.

박희영·최호진·최성진, 『사이버범죄협약 이행입법 연구』, 연구용역보고서, 대검찰청, 2015.12.

법원행정처, 『사법연감』, 2012~2021.

손지영·김주석, 『디지털 증거의 증거능력 판단에 관한 연구』, 연구총서 2015-08, 사법정책연구원, 2015.6.

손지영·김주석, 『압수수색 절차의 개선방안에 관한 연구』, 연구총서 2016-07, 사법정책연구원, 2016.3.

이상원, 『전자영장제도의 도입방안에 관한 연구』, 연구용역보고서, 법무부, 2012.

이승현·박경규·김성룡·이석배·조기영·하태인, 『형사소송법 편장체계 개편방안 연구 – 수사절차를 중심으로–』, 연구총서 19-BB-03, 한국형사정책연구원, 2019.12.

정성민, 『형사 전자소송의 바람직한 발전방향』, 연구총서 2020-05, 사법정책연구원, 2020.4.

차종진, 『디지털증거법제의 발전동향과 입법과제』, 책임연구보고서 2020-09, 치안정책연구소, 2021.5.

탁희성·이상진, 『디지털 증거분석도구에 의한 증거수집절차 및 증거능력확보방안』, 연구총서 06-21, 한국형사정책연구원, 2006.12.

한국지능정보사회진흥원(NIA), "디지털 전환 시대, NIA가 전망한 환경변화 13대 이슈", 『IT & Future Strategey』 보고서 제2호, 2022.5.12.

형사소송법 개정특별위원회, 『형사소송법 개정연구』, 연구총서 10-14, 한국형사정책연구원, 2010.12.

(5) 발표문·토론문

김환권, “디지털 증거의 임의제출과 관련된 법적 쟁점”(발표문), 『디지털증거 압수수색 관련 최근 동향』, 2022년 한국형사소송법학회 추계 학술대회, 2022.9.16.

박경규, “ICT 환경에서 압수·수색의 ‘피의사건과의 관련성’ 요건이 가지는 의미, 현행법의 문제점 및 개선방안”(발표문), 『ICT 환경에서 형사실체·절차법의 주요쟁점』 2019년 하계 공동 학술세미나, 경북대학교 법학연구원 형사법센터·IT와 법 연구소·대검찰청 공동주최, 2019.8.27.

박병민, “디지털 증거 압수수색의 절차적 규제 개선방안 –참여권 강화, 영장 사본 교부 제도 도입 등–”(발표문), 『디지털증거 압수수색 개선방안』, 2021 공동학술대회(사법정책연구원·대한변호사협회·한국형사법학회·대법원 형사법연구회 공동주최), 2021.3.26.

황성민, “디지털증거 압수·수색 관련 최근 판례 동향 –스마트폰에 대한 긴급 압수·수색에 있어서의 제문제 등–”(발표문), 『디지털증거 압수수색 관련 최근 동향』, 2022년 한국형사소송법학회 추계 학술대회, 2022.9.16.

(6) 기사

문광주 기자, “디지털 재앙 “약 200년 후 디지털 정보의 양은 지구 전체보다 더 많은 공간 차지””, 『the SCIENCE plus』 2020년 8월 14일자 기사(http://m.thescienceplus.com/news/newsview.php?ncode=1065579012676159; 최종접속일 2023.6.16.).

박상욱, “임의제출물에 대한 압수와 임의성 판단”, 『법률신문』 2023년 8월 4일자 로펌 뉴스레터(율촌)(https://www.lawtimes.co.kr/LawFirm-NewsLetter/189979; 최종접속일 2023.9.20.).

박선정 기자, “(단독) 유럽평의회, ‘디지털 범죄 국제 공조 협약’ 한국 가입 만장일치 찬성”, 『법률신문』 2023년 6월 26일자 기사(https://www.lawtimes.co.kr/news/188732; 최종접속일 2023.6.25.).

박수연 기자, “(단독) 휴대폰으로 영장 제시하는 시대 오나… 대법원, 전자영장 시대 준비”, 『법률신문』 2023년 6월 28일자 기사(https://www.lawtimes.co.kr/news/188714; 최종접속일 2023.10.11.).

오이석 기자, “스마트폰·USB·컴퓨터는 안다 … 그들의 범죄”, 『중앙SUNDAY』 제485호, 2016.6.26(https://www.joongang.co.kr/article/20221173#home; 최종접속일 2023.6.13.).

장승주 기자, “변화하는 마약거래 특성 감안해 형사절차 개선해야”, 『아주경제』 2023년 3월 12일자 기사(https://www.ajunews.com/view/20230312090826557; 최종접속일 2023.11.11.).

조주행, “[데이터로 본 한국인] 데이터 생산 세계 5위 강국이지만… 4차 산업혁명 기대보다 유출 걱정”, 『한국일보』 2020년 1월 17일자 오피니언(https://m.hankookilbo.com/News/Read/202001161747340215; 최종접속일 2023.6.16.).

(7) 기타

네이버 지식백과, “다크 웹”(https://terms.naver.com/entry.naver?docId=3581037&cid=59088&categoryId=59096; 최종접속일 2023.9.14.).

대검찰청, 사전정보공표대상 자료, “디지털 증거 압수수색, 증거분석 등 지원 현황”(https://www.spo.go.kr/site/spo/ex/announce/AnnounceInfo.do, 최종접속일 2023.6.13.).

법원행정처, “형사소송규칙일부개정규칙안 입법예고”, 『법원행정처공고 제2023-37호』, 2023.2.3(https://www.scourt.go.kr/portal/legislation/LegislationView.work?pageIndex=1&searchWord=%C7%FC%BB%E7%BC%D2%BC%DB%B1%D4%C4%A2&seqnum=434&gubun=1; 최종접속일 2023.6.25.).

외교부 보도자료, “사이버범죄협약(일명 ‘부다페스트협약’) 가입의향서 제출”, 2022.10.11(https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=372854; 최종접속일 2023.6.25.).

2. 독일 문헌

(1) 학술지논문

Amelung, Knut, Grundfragen der Verwertungsverbote bei beweissichernden Haussuchungen im Strafverfahren, NJW 1991.

Bär, Wolfgang, BGH-Ermittlungsrichter: Sicherstellung von Datenträgern mit Anmerkung, CR 1999.

Beukelmann, Stephan, Online-Durchsuchung und Quellen-TKÜ, NJW-Spezial 2017.

Blechschmitt, Lisa, Strafverfolgung im digitalen Zeitalter – Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren, MMR 2018.

Brodowski, Dominik/*Eisenmenger*, Florian, Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden - Sachliche und zeitliche Reichweiter der "kleinen Online-Durchsuchung" nach § 110 Abs. 3 StPO, ZD 3/2014.

Brunst, Phillip W., BVerfG: Sicherstellung und Beschlagnahme von Mails auf dem Mailserver mit Anmerkung, CR 9/2009.

Buchholz, Momme, Das Anwesenheitsrecht bei der Durchsicht von Datenbeständen nach § 110 Abs. 1 StPO, NZWiSt 2021.

Cordes, Malte/*Reichling*, Tilman, Grenzen der Durchsicht von Papieren und elektronischen Speichermedien gemäß § 110 StPO und Rechtsfolgen von Verstößen, NStZ 2022.

Dalby, Jakob, Das neue Auskunftsverfahren nach § 113 TKG – Zeitdruck macht Gesetze – Eine Beurteilung der Änderung des manuellen Auskunftsverfahrens und der Neuschaffung des § 100j StPO, CR 6/2013.

Dauster, Manfred, Betroffenheit in der Vertraulichkeitssphäre, polizeiliche "venia legendi" aufgrund richterlicher Beschlagnahmeanordnung und die Restriktionen des § 110 StPO, StraFo Juni 1999.

Derin, Benjamin/*Golla*, Sebastian J., Der Staat als Manipulant und Saboteur der IT-Sicherheit?-Die Zulässigkeit von Begleitmaßnahmen zu "Online-Durchsuchung" und Quellen-TKÜ. NJW 2019.

Doege, Felix, Das Anwesenheitsrecht des Betroffenen und seines Rechtsbeistands bei der Durchsicht gem. § 110 StPO, NStZ 2022.

Freiling, Felix/*Safferling*, Christoph/*Rückert*, Christian, Quellen-TKÜ und Online-

Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018.

Gaede, Karsten, Der grundrechtliche Schutz gespeicherter EMails beim Provider und ihre weltweite strafprozessuale Überwachung, StV 2009.

Glock, Stefan, Unterlagen, deren richterliche Beschlagnahme noch nicht angeordnet oder bestätigt wurde, dürfen seitens der Ermittlungsbehörden nicht verwendet werden, NStZ 2019.

Graulich, Volker, Die Sicherstellung von während einer Durchsuchung aufgefunden Gegenständen - Beispiel Steuerstrafverfahren, wistra 8/2009.

Gurlit, Elke, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010.

Hamm, Rainer, Unzulässigkeit einer "verdeckten Online- Durchsuchung" – BGH, Beschluss vom 31.1.2007 - StB 18/06 mit Anmerkung, NJW 2007.

Hiéramente, Mayeul, Durchsuchung und "Durchsicht" der Unternehmens-IT – Betrachtungen zu §§ 103, 110 StPO, wistra 11/2016.

Hofmann, Manfred, Die Online-Durchsuchung - staatliches "Hacken" oder zulässige Ermittlungsmaßnahme?, NStZ 2005.

Kasiske, Peter, Neues zur Beschlagnahme von E-Mails beim Provider, StraFo 6/2010.

Kemper, Martin, Die "Mitnahme zur Durchsicht" – Ein vom Gesetz nicht vorgesehenes Instrument zur Sicherstellung von Beweismitteln?, wistra 8/2010.

Kemper, Martin, Das Beschlagnahmeverzeichnis nach § 109 StPO in Wirtschafts- und Steuerstrafverfahren, wistra 3/2008.

Kemper, Martin, Die Beschlagnahmefähigkeit von Daten und E-Mails, NStZ 2005.

Klesczewski, Diethelm, Straftataufklärung im Internet, ZStW 123 (2011).

Knauer, Christoph/*Wolf*, Christian, Zivilprozessuale und strafprozessuale Änderungen durch das Erste JuMoG - Teil 2: Änderungen der StPO, NJW 2004.

Krekeler, Wilhelm, Beweisverwertungsverbot bei fehlerhaften Durchsuchungen, NStZ 1993.

Kudlich, Hans, Strafverfolgung im Internet - Bestandsaufnahme und aktuelle Probleme -, GA 2011.

Michalke, Reinhart, Durchsuchung und Beschlagnahme – Verfassungsrecht im Alltag, StraFo 3/2014.

Mildeberger, Tobias/*Riveiro*, Karen, A., Zur Durchsicht von Papieren gem. § 110 StPO, StraFo Februar 2004.

Obenhaus, Nils, Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, NJW 2010.

Peters, Kristina, Anwesenheitsrechte bei der Durchsicht gemäß § 110 StPO: Bekämpfung der Risiken und Nebenwirkungen einer übermächtigen Ermittlungsmaßnahme, NZWiSt 2017.

Rieß, Peter, Die »Straftat von erheblicher Bedeutung« als Eingriffsvoraussetzung – Versuch einer Inhaltsbestimmung, GA 2004.

Roggan, Fredrik, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit, StV 2017.

Schlegel, Stephan, "Beschlagnahme" von E-Mail-Verkehr beim Provider – Zugleich Besprechung zu BVerfG 2 BvR 902/06 vom 29.06.2006, HRRS 2/2007.

Schünemann, Bernd, Wohin treibt der deutsche Strafprozess?, ZStW 114 (2002).

Singelnstein, Tobias, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen, NStZ 2012.

Singelnstein, Tobias/*Derin*, Benjamin, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens-Was aus der StPO-Reform geworden ist, NJW 2017.

Soiné, Michael, Personale verdeckte Ermittlungen in sozialen Netzwerken zur Strafverfolgung, NStZ 2014.

Soiné, Michael, Die strafprozessuale Online-Durchsuchung, NStZ 2018.

Szesny, André-M., Durchsicht von Daten gem. § 110 StPO, WiJ 2012.

Vogel, Joachim, Informationstechnologische Herausforderungen an das Strafprozessrecht, ZIS 2012.

Wenzl, Christopher, Die Datenlieferungsvereinbarung, NStZ 2021.

Wicker, Magda, Durchsuchung in der Cloud Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013.

Zerbes, Ingeborg/*El-Ghazi*, Mohamad, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, NStZ 2015.

Zimmermann, Till, Der strafprozessuale Zugriff auf E-Mails, JA 5/2014.

(2) 단행본

Bär, Wolfgang, Handbuch zur EDV-Beweissicherung im Strafverfahren, Richard Boorberg, 2007. (인용: *Bär*, EDV-Beweissicherung, Rn. …)

Ciolek-Krepold, Katja, Durchsuchung und Beschlagnahme in Wirtschaftsstrafsachen, NJW-Schriftenreihe Band 68, C.H. Beck, München 2000. (인용: *Ciolek-Krepold*, Rn. …)

Hannich, Rolf (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, 8. Auflage, C.H. Beck, München 2018. (인용: *작성자*, KK-StPO, § … Rn. …)

Maunz/Dürig (Hrsg.), GG-Kommentar, 77. EL Juli 2016 / 85. EL November 2018. (인용: *작성자*, in: Maunz/Dürig, GG-K, Art. … Rn. …)

Meininghaus, Florian, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, Kovač, Hamburg 2007. (인용: *Meininghaus*, Der Zugriff auf E-Mails, S. …)

Meyer-Goßner/Schmitt, Strafprozessordnung mit GVG, Nebengesetze und ergänzende Bestimmungen, 62. Auflage, C.H. Beck, München 2019. (인용: *작성자*, M-G/Schmitt, § … Rn. …)

Park, Tido, Durchsuchung und Beschlagnahme, 3. Auflage, C.H. Beck, München 2015. (인용: *Park*, Rn. …)

Roxin, Claus/*Schünemann*, Bernd, Strafverfahrensrecht, 29. Auflage, C.H. Beck, München 2017. (인용: *Roxin/Schünemann*, § … Rn. …)

Sieber, Ulich, Straftaten und Strafverfolgung im Intenet, Gutachten C zum 69. DJT, C.H. Beck, München 2012. (인용: *Sieber*, 69. DJT 2012, C …)

Volk, Klaus/*Engländer*, Armin, Grundkurs StPO, 8. Auflage, C.H. Beck, München 2013. (인용: *Volk/Engländer*, § … Rn. …)

Wolter, Jürgen (Hrsg.), SK-StPO, 5. Auflage, Carl Heymanns, Köln 2016. (인용: *작성자*, SK-StPO, § … Rn. …)

(3) 기타

Convention on Cybercrime(European Treaty Series-No. 185)(https://rm.coe.int/1680081561; 최종접속일 2023.10.10.).

T-CY Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data vom 6. Dez. 2012, What are the options?, S. 29 [Rn. 138](https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8, 최종접속일 2023.9.15.).

T-CY Guidance Note # 3, Transborder access to data (Art. 32) vom 3. Dez. 2014, S. 6 [Tz. 3.2](https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a, 최종접속일 2023.9.15.).

독일 연방법무청(Bundesamt für Justiz) 홈페이지, "Statistiken der Rechtspflege" (https://www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken_node.html#AnkerDokument44152; 최종접속일 2023.7.31.).

유럽평의회(Council of Europe) 홈페이지, "Details of Treaty No.224"(https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224; 최종접속일 2023.9.15.).

유럽평의회(Council of Europe) 홈페이지, "The Budapest Convention (ETS No. 185) and its Protocols"(https://www.coe.int/en/web/cybercrime/the-budapest-convention; 최종접속일 2023.10.10.).

3. 일본 문헌

(1) 학술지논문

千葉 陽一, "インターネットのプロバイダが管理するホームページへの被疑者の一定期間のアクセスログを差押対象とする捜索差押許可状及びプロバイダの任意提出を前提にした差押許可状の発付の可否と留意点", 『別冊判例タイムズ』 35号, 2012.

クリスティアン シュワルツネッガー, 夏井 高大·笠原 毅彦(訳), "サイバー犯罪条約(2001年11月23日)によるコンピュータ犯罪法及びインターネット犯罪法の国際調和

ハツキング、違法をデ－タ入手及び違法な通信傍受を例に”,『判例タイムズ』1108号, 2003.

江口 和伸, “ネットワーク接続コンピュータを対象とする捜索, 差押え”,『別冊判例タイムズ』35号, 2012.

海野 敦史, “監視型情報収集と憲法35条１項との関係:「私的領域に侵入されることのない権利」を保障する意義”,『情報通信政策研究』第2巻第1号, 2018.

海野 敦史, “憲法35条1項に基づく権利の保障と令状主義の要請との関係”,『情報通信学会誌』38巻 3号, 2020.

指宿 信, “インターネットを使った犯罪と刑事手続”,『法律時報』69巻7号, 1997.

指宿 信, “変わる捜査の対象:モノからデータへ―サイバー刑事法制の諮問を契機として―”,『法律時報』75巻7号, 2003.

指宿 信, “サイバー犯罪条約およびその国内法化について”,『刑法雑誌』45巻1号, 2005.

指宿 信, “サイバースペースにおける証拠収集とデジタル証拠の確保：2011年改正法案を考える”,『法律時報』83巻7号, 2011.

指宿 信, “押収済みパソコンを用いて検証許可状に基づき海外メールサーバにアクセスした捜査に重大な違法があるとして証拠を排除した事例”,『新･判例解説』20号, 2017.

指宿 信, “海外サーバからの電磁的記録の差押え等の適法性が争われた事例”,『新･判例解説 Watch』No.117, 2018.

槫 清隆, “インターネットのプロバイダのメールサーバ内の電子メールに対する捜索差押許可状を発付することの可否”, 『別冊判例タイムズ』35号, 2012.

川瀬 孝史, “磁的記録に対する捜索差押え上の諸問題 : 令状実務とその周辺の諸問題”,『警察学論集』74巻9号, 2021.

小向 太郎, “クラウド上のデータを対象とする犯罪捜査に関する法的課題”,『情報処理学会研究報告』, 2018.

小坂谷 聡･上原 哲太郎, “刑事手続におけるデジタル証拠の改ざん防止措置について”, ルチメディア , 分散協調とモバイルシンポジウム, 2017.

草野 耕一･菅野 博之･三浦 守･岡村 和美, “最高裁第二小法廷令3.2.1決定”,『判例タイムズ』1494号5月号, 2022.

劉 芳伶, “「情報の差押」という制度の在り方について(論説)”,『法律時報』82巻2号, 2010.

松田 克之·宮崎 桃子, “情報通信機器の発達を背景とした令状 : 捜査に対する司法審査の在り方等に関する研究”, 『判例タイムズ』 1488号11月号, 2021.

宮木 康博, “電磁的記録媒体の差押え(最決平成 10·5·1)”, 『法学教室』 2019年11月号, 2019.

中島 宏, “電磁的記録媒体の差押え等の適法性[大阪高裁平30.9.11判決]”, 『法学セミナー』 通巻 768号, 2019.

南部 晋太郎, “電磁的記録媒体に対する捜索差押”, 『別冊判例タイムズ』 35号, 2012.

早乙女 宜宏, “リモートアクセスによる差押えに伴う問題点の一考察”, 『日本大学法科大学院法務研究』 第16号, 2019.

岡田 好史, “サイバー刑法の概念と展望”, 『専修大学法学論集』 118号, 2013.

柴田 和也, “情報機器に関する令状実務について(覚書)”, 『判例タイムズ』 1459号6月号, 2019.

須川 賢洋, “「情報処理の高度化等に対処するための刑法等の一部改正」に関する一考察”, 『情報処理学会研究報告』, 2012.

杉山 徳明·吉田 雅之, “「情報処理の高度化等に対処するための刑法等の一部を改正する法律」について(下)”, 『法曹時報』 64巻5号, 2012.

高村 紳, “捜査におけるデジタル情報収集に対する法的規制”, 『中央学院大学法学論叢』 36巻1号, 2022.

寺林 裕介, “サイバー犯罪条約第２追加議定書の概要: 国境を越えるサイバー犯罪捜査のための国際協力”, 『立法と調査』, 2023.

安冨 潔, “情報化社会における刑事立法の役割 : コンピュータ犯罪からサイバー犯罪へ”, 『慶應法学』 42巻, 2019.

横山 裕一, “国外へのリモートアクセスによる電磁的記録の複写の処分”, 『日本大学法科大学院法務研究 』 19号, 2022.

(2) 보고서 및 백서

警察庁, 『令和5年 警察白書』, 2023.

刑事手続における情報通信技術の活用に関する検討会, 『「刑事手続における情報通信技術の活用に関する検討会」取りまとめ報告書』, 2022.3.

(3) 기타

법무성 홈페이지, “答申(ハイテク犯罪に対処するための刑事法の整備に関する要綱(骨子))”, 2003.9.10(https://www.moj.go.jp/shingi1/shingi_030910-5-1.html; 최종접속일 2023.9.17.).

법무성 홈페이지, “刑事手続における情報通信技術の活用に関する検討会”(https://www.moj.go.jp/keiji1/keiji07_00011.html; 최종접속일 2023.9.17.).

법무성, “サイバー関係の法整備の概要”(https://www.moj.go.jp/content/001267492.pdf; 최종접속일 2023.9.17.).

법무성, “情報処理の高度化等に対処するための刑法等の一部を改正する法律案における修正点について”(https://www.moj.go.jp/content/001267491.pdf; 최종접속일 2023.9.17.).

법무성, 情報処理の高度化等に対処するための刑法等の一部を改正する法律安(https://www.moj.go.jp/content/001267495.pdf; 최종접속일 2023.9.17.).

외무성 보도자료, “「協力及び電子的証拠の開示の強化に関するサイバー犯罪に関する条約の第二追加議定書」への署名”, 2022年5月12日(https://www.mofa.go.jp/mofaj/press/release/press3_000814.html; 최종접속일 2023.9.17.).

외무성 홈페이지, 사이버범죄 방지협약 제2 추가의정서(영문 전문)(https://www.mofa.go.jp/mofaj/files/100342970.pdf; 최종접속일 2023.9.17.).

외무성 홈페이지, “サイバー犯罪に関する条約”(원문 및 일본어판)(https://www.sangiin.https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html; 최종접속일 2023.9.17.)을 참고.

참의원 홈페이지, “犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案”(https://www.sangiin.go.jp/japanese/joho1/kousei/gian/160/meisai/m16003159046.htm; 최종접속일 2023.9.17.).

4. 영미 문헌

(1) 논문 및 단행본

Association of Chief Police Officers(ACPO), 『Good Practice Guide for Digital Evidence』, 2012.

Attorney General's Office, "Attorney General's Guidelines on Disclosure -For investigators, prosecutors and defense practitioners-", 2022.

David Ormerod CBE, KC(Hon), David Perry QC, 『Blackstone's criminal practice』, Blackstone Press, 2023.

H. Marshall Jarrett Director, EOUSA, Michael W. Bailie Director, OLE, "searching and seizing computers and obtaining electronic evidence in criminal investigation", Office of Legal Education Executive Office for United States Attorneys, 2009.

Investigatory Powers Act 2016, EXPLANATORY NOTES, 2016.

Law Commission Reforming the Law, "Search warrants", 2020.10.7.

MJEB, 『A Guide for Ninth Circuit Magistrate Judges When Reviewing Government Applications to Obtain Electronic Information』(3rd Edition), 2017.

Orin S. Kerr 『Computer Crime Law』(Fifth edition), WEST ACADEMIC PUBLISHING, 2022.

Richard Stone, 『THE LAW OF ENTRY, SEARCH, AND SEIZURE』, OXFORD UNIVERSITY PRESS, 2013.

The Home Office, "Equipment Interference Code of Practice", 2018.3,

The Home Office, "Extraction of information from electronic devices: code of practice(accessible)", 2023.3.16.

The Home Office, "Interception of Communications Code of Practice", 2018.3,

The Home Office, "Police And Criminal Evidence Act 1984 Codes of Practice Code B", 2013.

U.S. Depart of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"(Third Edition), 2009.

(2) 기타

BAILIE 홈페이지, 판결 전문(https://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html; 최종접속일 2023.9.14.

Bureau of Justice Assistance 홈페이지, "Electronic Communications Privacy Act of 1986(ECPA)"(https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#general-provisions; 최종접속일 2023.9.14.).

CNN Philippines Staff, "Enhanced e-warrant system launched for faster issuance of arrest warrants", CNN NEWS, 2020.9.8(https://www.cnnphilippines.com/news/2020/9/8/pnp-supreme-court-enhanced-ewarrant-system.html; 최종접속일 2023.10.19.).

Columbia University, Freedom of Expression 홈페이지, "Secretary of the State for the Home Department v. Watson"(https://globalfreedomofexpression.columbia.edu/cases/secretary-state-home-department-v-watson/; 최종접속일 2023.9.14.).

Cornell Law School, Legal Information Institute, "CARPENTER v. UNITED STATES"(https://www.law.cornell.edu/supremecourt/text/16-402; 최종접속일 2023.9.14.).

Criminal Justice and Police Act 2001 Explanatory Notes(https://www.legislation.gov.uk/ukpga/2001/16/notes/division/2; 최종접속일 2023.9.14.).

Crown Prosecution Service, "Disclosure Manual: Chapter 30 - Digital Material", 2022년 7월 14일자(https://www.cps.gov.uk/legal-guidance/disclosure-manual-chapter-30-digital-material; 최종접속일 2023.9.14.).

Crown Prosecution Service, "Legal Guidelines, Rape and Sexual Offences - Chapter 3: Case Building", 2021년 5월 21일자(https://www.cps.gov.uk/legal-guidance/rape-and-sexual-offences-chapter-3-case-building; 최종접속일 2023.9.14.).

Electronic Privacy Information Center 홈페이지, "Electronic Communications Privacy Act (ECPA)"(https://epic.org/ecpa/; 최종접속일 2023.9.14.).

EUR-Lex 홈페이지, 판결문 전문(영문)(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203; 최종접속일 2023.9.14.).

European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT

AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters", Strasbourg, 2018.4.17(https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF; 최종접속일 2023.10.10.).

Filippo Raso, "Federal Court Orders Apple to Unlock iPhone. Apple Refuses", 『Harvard Journal of Law & Technology』, 2016년 3월 29일자(https://jolt.law.harvard.edu/digest/federal-court-orders-apple-to-unlock-iphone-apple-refuses; 최종접속일 2023.9.14.).

GIBSON DUNN 홈페이지, "U.S. Cybersecurity and Data Privacy Outlook and Review – 2019", 2019년 1월 28일자(https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2019/; 최종접속일 2023.9.14.).

GOV.UK 사이트, "Investigatory Powers Act"(https://www.gov.uk/government/collections/investigatory-powers-bill; 최종접속일 2023.9.14.).

Information Commissioner's Office, "Investigation report: Mobile phone data extraction by police forces in England and Wales", 2020.6, 53면(https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/; 최종접속일 2023.9.14.).

itvNEWS, "Thousands march through Bristol for 'Kill the Bill' protest", 2022년 3월 1일자(https://www.itv.com/news/westcountry/2021-03-21/hundreds-gather-in-bristol-for-kill-the-bill-protest; 최종접속일 2023.9.12.).

Julian Jones, Park Square Barristers, "Obligations in relation to electronic records and devices: fresh guidance from the Court of Appeal (Criminal Division)", 『Park Square Barristers』 2020년 6월 26일자(https://www.parksquarebarristers.co.uk/news/obligations-relation-electronic-records-devices-fresh-guidance-court-appeal-criminal-division/; 최종접속일 2023.9.14.)).

JUSTIA 홈페이지, "Schneckloth v. Bustamonte, 412 U.S. 218 (1973)"(https://supreme.justia.com/cases/federal/us/412/218/; 최종접속일 2023.9.14.).

Kateconger, "Have we seen the last of the All Writs Act in the encryption fight?", 『Tech Crunch』, 2016년 4월 26일자(https://techcrunch.com/2016/04/25/have-we-seen-the-last-of-the-all-writs-act-in-the-encryption-fight/?ncid=rss; 최종접속일 2023.9.14.).

Law Commission Reforming the Law, “Implementation Table”(https://www.lawcom.gov.uk/our-work/implementation/table/; 최종접속일 2023.9.14.).

Law Commission Reforming the Law, “Search warrants reform to help law enforcement investigate crime”, 2020.10.7(https://www.lawcom.gov.uk/search-warrants-reform-to-help-law-enforcement-investigate-crime/; 최종접속일 2023.9.14.).

LIBERTY, “THE POLICING BILL – WHAT HAPPENED, AND WHAT NOW?”, 2022년 4월 29일자(https://www.libertyhumanrights.org.uk/issue/the-policing-bill-what-happened-and-what-now/; 최종접속일 2023.9.12.).

Miller, “Telephonic Search Warrants: The San Diego Experience”, 9 The Prosecutor 385, 386 (1974)(https://www.ojp.gov/ncjrs/virtual-library/abstracts/telephonic-search-warrants-san-diego-experience; 최종접속일 2023.9.14.).

MINNESOTA COURT RULES, “CRIMINAL PROCEDURE”(https://www.revisor.mn.gov/court_rules/cr/id/37/#37.01; 최종접속일 2023.10.18.).

Orin S. Kerr, “Computer searches and the problem of withdrawn consent”, 『The washington Post』, 2015년 8월 11일자(https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/08/11/computer-searches-and-the-problem-of-withdrawn-consent/; 최종접속일 2023.9.14.).

StudySmarter 홈페이지, “Human Rights Act 1998”(https://www.studysmarter.co.uk/explanations/politics/uk-government/human-rights-act-1998/; 최종접속일 2023.9.14.).

The British Institute of Human Rights 홈페이지, “What's in the Human Rights Act?”(https://www.bihr.org.uk/get-informed/legislation/whats-in-the-human-rights-act; 최종접속일 2023.9.14.).

THE EDITORIAL BOARD, “After Apple vs. FBI, more reasons to be wary in privacy fight”, 『Los Angeles Daily News』, 2016년 4월 29일자(https://www.dailynews.com/2016/04/29/after-apple-vs-fbi-more-reasons-to-be-wary-in-privacy-fight/; 최종접속일 2023.9.14.).

U.S. Dept. of Justice, “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal investigations”, “Appendix C. Sample Language for Preservation Request under 18 U.S.C. §2703(f)”(www.justice.gov/file/442111/download; 최종접속일 2023.10.10.).

UK Parliament 홈페이지, “Have your say on the Police, Crime, Sentencing and Courts Bill”, 2021년 5월 6일자(https://www.parliament.uk/business/news/2021/may/have-your-say-on-the-police-crime-sentencing-and-courts-bill/; 최종접속일 2023.9.14.).

VentureBeat, “U.S. to continue appeal of iPhone data case in New York”, 2016년 4월 9일자(https://venturebeat.com/business/u-s-to-continue-appeal-of-iphone-data-case-in-new-york/; 최종접속일 2023.9.14.).

WIKIPEDIA, “Police, Crime, Sentencing and Courts Act 2022”(https://en.wikipedia.org/wiki/Police,_Crime,_Sentencing_and_Courts_Act_2022; 최종접속일 2023.9.12.).

미국 국회 홈페이지(https://www.congress.gov/amendment/116th-congress/senate-amendment/1583; 최종접속일 2023.9.14.).

유럽사법재판소, 판결문 전문(원문)(https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1088733; 최종접속일 2023.9.14.).

“협력 및 전자적 증거 개시 강화에 관한 사이버범죄방지협약 제2 추가의정서”(Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence) 원문(https://rm.coe.int/1680a49dab; 최종접속일 2023.10.28.).

Abstract

Issues in Search and Seizure of Digital Evidence and Possible Improvements

Tak, Heesung · Lee, Soon-Ok · Park, Joongwook · Son, Yeo-Ok

1. The rapid development of information and communication technology (ICT) and the spread of non-face-to-face digital transformation spurred by COVID-19, data encryption technology for information protection has become more powerful, and the networking of data due to the spread of cloud services is creating legal and technical challenges that are difficult to solve through traditional legal interpretation alone, creating obstacles to the discovery of substantive truth, which is the goal of the criminal justice process. Therefore, in obtaining digital evidence in the investigation process, we need to move away from the traditional concept of seizure focused on physical objects, and establish new methods and procedures that are compatible with the characteristics of digital data, as well as secure legislative support to support them.

Against this backdrop, this study seeks to explore: i) the direction of improvement on the seizure and search provisions aligned with digital evidence; ii) the direction of legislation guided by the balance between the discovery of substantive truth and the protection of privacy in the investigative process in the digital environment; and iii) the possibility of introducing a new evidence acquisition method that considers how digital data exists as determined by their technological methods.

As such, this study progresses as follows: i) review the current seizure and search regulations in the Criminal Procedure Act and the issue of incompatibility with

digital evidence; ii) analyze changes and trends in the relevant case law and legislations, highlighting major issues related to the seizure and search of digital evidence; iii) compare legislations and policy changes in major countries aimed at addressing the seizure and search nf digital evidence; and iv) examine the necessity of new methods for compulsive investigation to secure digital evidence.

2. The incompatibility between the current law and digital evidence can be discussed from several perspectives: incompatibility with the concept of seizure; incompatibility with the method of seizure; and incompatibility with the legislative structure. First, the incompatibility with the concept of seizure stems from the fact that the current Criminal Procedure Act limits the scope of seizure to tangible objects. However, we also need to consider that digital information itself cannot be seized because the seizure of digital information cannot exclude the affected person from possessing the information. Next, the incompatibility with the method of seizure arises from the fact that the existing investigative methods have come to face practical limitations in securing digital data evidence due to changes in the digital technology environment. Therefore, we need to discuss the introduction of new investigative methods to ensure efficient securing of digital evidence. Finally, the incompatibility with the legislative structure has its roots in the unreasonableness of how the titles and chapters of the current Criminal Procedure Act are organized. The Act, as it is currently organized, ignores the fundamental difference between trial process and the investigative process by applying the rules for the former mutatis mutandis to the latter. This not only creates a gap between the actual law and the reality, but also restricts the ability to proactively respond to changes in the investigation environment boosted by technological advancements.

3. From the early 2000s, when the importance of digital evidence in criminal proceedings began to be discussed, to the present, only 17 bills have been

introduced in the National Assembly to amend the digital evidence provisions in the Criminal Procedure Act. As for the purpose of the bills, before 2015, most of them were aimed at ensuring the protection of personal information and the right to control one's own information. In and after 2015, bills were introduced to address the need to control the abuse of authority by investigative agencies in the digital evidence seizure process. After the so-called Nth Room case, in which the perpetrator blackmail victims into making sexually exploitative videos and spread them online, legislative bills were submitted that emphasized the need for an institutional mechanism for rapid securing and preservation of digital evidence. This legislative history suggests that the purposes of the legislative bills have changed in accordance with how the center of gravity shifts in the situation where the discovery of substantive truth conflicts with the protection of privacy as digital technologies develop. These changes can be also found in the content of the bills. Earlier bills were drafted with a focus on controlling the seizure and search process by introducing more granular provisions on investigative methods, so as to protect privacy and personal information. However, as IT technology become more advanced, many of the recent bills were proposed with a focus on securing digital evidence more faster and more efficiently, guided by the recognition that there are limitations in securing digital evidence through public authorities that are not equipped to keep up with the speed of technological advancement. Finally, in terms of the structure of the law, several bills were introduced between the early 2000s and 2018, for amending provisions on the seizure and search process in courts. To the contrary, since 2019, amendments to the Criminal Procedure Act related to the seizure of digital evidence have been proposed for amending the provisions on seizure and search at investigative agencies under Article 215 and the following articles of the Investigation Division. These changes in the structure seems to stem from the need for procedural control to address the expansion of the total amount of investigations and the need to introduce a new seizure and search method to secure digital evidence in situations where technical defenses

are available to counter the power of the investigative agencies.

On the other hand, a review of changes in the case law related to the seizure and search of digital evidence shows that, first of all, the right to participate in the seizure and search process was the main issue before 2020, whereas the seizure of voluntary submissions was primarily discussed in and after 2020. In addition, the criteria for determining the legality of seizure and search against digital evidence were initially discussed from the perspective of ensuring the fairness of the process and protecting the procedural rights of the defendants. However, with advancements in digital technology, the focus has shifted from procedural fairness to the due process for privacy protection, as advancements in digital technology greatly expanded the amount of information subject to seizure and search.

4. This study also examines the evolution and trends in legislative issues related to the seizure and search of digital evidence in two sets of countries: Germany and Japan, which follows the civil law system; and the United Kingdom and the United State, which are common law countries. Germany, unlike the United States, has not only continued to incorporate new investigative methods made possible by technological advances into its laws over the past two decades based on the rule of law and the principle of proportionality, but has also attempted to offset serious violations of fundamental rights unforeseen by existing investigative methods through legislations. In Japan, the 2011 amendment to its Code of Criminal Procedure introduced new provisions on the seizure of electronic records including the execution in lieu of seizure of record media concerning electronic records, the seizure of record order copy, and the remote search and seizure. There were other provisions included in the bill for the amendment that did not make it into the final amendment due to their controversial nature, such as those on the extraterritorial search and seizure and the determination of the scope of seizure of electronic records. In addition, the amendment introduced a new system for the seizure of electronic record orders. However, the effectiveness of the system

is currently being questioned as it lacks the means to enforce the order of the investigative agencies in case of non-compliance.

The United States has explicitly built a seizure process aligned with the characteristic of digital evidence through several amendments, by specifying the information to be seized, introducing an electronic warrant system to speed up the process of requesting and issuing warrants, and introducing a trans-jurisdictional Network Investigative Technique warrant (NIT warrant) system to enable the seizure of information outside its jurisdiction. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) also allows for offshore seizures. In other words, when it comes to the procedures for the seizure of digital evidence, the United States adopted regulations that consider the efficiency of investigations rather than procedural controls to protect the privacy of suspects. Finally, in the United Kingdom, the 2001 Criminal Justice and Police Act (CJPA) not only specified information as an object of seizure, but also amended the 1984 Police and Criminal Evidence Act (PACE) to increase the scope of seizure to include "anything stored in electronic forms." In addition, the 2016 Investigatory Powers Act (IPA) allows the government to request provision and preservation of data by foreign telecommunication service providers, and intercept data at the request of a foreign country. The 1990 Computer Misuse Act (CMA) provides for online search, and the 2000 Regulation of Investigatory Powers (RIPA) allows the government to force a suspect to decrypt data, and subject a non-compliant suspect to criminal punishment. These legislations indicate how the United Kingdom has continuously addressed the difficulty in criminal investigations and the protection of personal data caused by the inability of the existing law to keep up with the rapid changes in ICT, by introducing and amending various laws and regulations.

5. The main issues currently discussed regarding the seizure and search of digital evidence include procedural controls to ensure the legality of the seizure of digital evidence in criminal proceedings and the possibility of introducing a new seizure

and search system that is compatible with digital evidence.

To elaborate, the main issues discussed regarding the procedural controls to ensure the legality of seizure and search under the current Criminal Procedure Act include the right to participate and the seizure of voluntary submissions. Despite the importance of the right to participate in preventing violations of privacy and fundamental rights caused by the mixture of internal and external information in the seizure of digital evidence, the current legislations fail to stipulate clear standards for the right, causing controversies regarding its interpretation. Therefore, in order to ensure the effectiveness of the right to participate as a means to realize due process in the seizure and search of digital evidence, the relevant legislations need to clarify the legal status of the right, define the scope of the people with the right to participate, change the provisions for issuing seizure lists to exclude irrelevant information, which constitutes the essence of the right of participation, and establish procedures for the deleting and disposing of irrelevant information. As for the seizure and search of voluntary submissions, the issue arises mainly because, if we apply the rationale for the seizure of voluntarily submitted tangible objects to information storage media, it leads to the unreasonable conclusion that the entire media can be seized. In particular, the seizure of media containing a large amount of information related to personal privacy, such as smartphones, may cause serious violations of the privacy and fundamental rights of the person subject to the seizure unless the process complies with the basic principles that apply to the seizure of information. Therefore, voluntary submission of information storage media not only requires a process to verify the voluntariness of submission and limitation of the scope of submission, but also determination of relevance to the alleged facts, selective reproduction and display of the scope of seizure, and the protection of the right to participate in the seizure, which are aimed at ensuring the lawfulness of the process.

This study also examines the order to preserve digital evidence, the electronic warrant system, the remote location search system, and the online search system

as new methods of securing evidence in the digital environment.

First, the order to preserve digital evidence is aimed at securing important digital evidence promptly, minimizing the possibility of data loss or alteration by requiring telecommunications service or remote computing service providers to preserve data for a certain period of time. The preservation order is less likely to infringe on fundamental rights because it does not involve the transfer of data. However, it can be understood as a compulsory measure because it restricts data use and the performance of certain tasks. Therefore, a legislation of the data preservation order should provide requirements for the order including the exhaustion of other procedures, necessity, and relevance. The targets of the preservation order should be limited to telecommunications service or remote computing service providers. In addition, a certain time limit should be set for the data preservation order, and the order needs to be controlled by the courts as it constitutes an compulsory investigative measure.

As for the electronic warrant system, the relevant provisions have been already legislated within the 2020 Act on the Use of Electronic Documents in Criminal Justice Procedures. As the Act has not entered into effect, it is high time that Korea improved on the warrant provisions in its Criminal Procedure Act. Specifically, the Act needs to lay the legal groundwork for the electronic warrant system, as well as a revision to the rules providing for exceptions to the principle of presentation of warrants.

The remote search system is a means of obtaining digital evidence by accessing information storage media located at a location specified in the warrant, which can be used in a seizure and search against a person who uses cloud services or overseas email services. While the need for remote search in the current digital environment cannot be questioned, it would be difficult to fully accommodate remote seizure and search into the current statutory provisions because the geographical scope of the search would have to be expanded to include digital devices listed in the warrant and remote servers connected to the network.

Therefore, a legal basis for remote seizure and search needs to be put in place under new statutory provisions separate from the current provisions that rely on the physical concept of space. In addition, as the expansion of the seizure and search authority may result in the infringement on the privacy of third parties or the jurisdiction of other countries, explicit provisions should be introduced to limit the scope of the authority to the extent permitted by the general access rights granted to the person against whom the seizure and search is conducted.

Lastly, online search involves covert accessing another person's ICT system using technical means for the purpose of monitoring the use of the system, and reading in and recording the content stored in the system. It can be described as 'lawful hacking' by the state to respond to specific crimes. By its nature, online search infringes on fundamental rights more than any existing compulsory investigation methods. Therefore, it should be allowed only against criminal suspects, the target crimes and time limits must be explicitly defined, and a dual control mechanism should be introduced that consists of preventive regulation by the courts and follow-up regulation by the National Assembly.

6. When we consider the direction of legislation to improve on the process of searching and seizing digital evidence, the discussion should be predicated on the recognition that as IT technology becomes more sophisticated, the possibility of prosecuting criminal activities using ICT and networks is bound to be restricted in practice. Ensuring appropriate seizure and search of information under this premise requires a judicial perspective and legislative reform that balance the protection of privacy and fundamental rights with the discovery of the substantive truth. In addition, the title and chapter structure of the current Criminal Procedure Act needs to be revised to separate the provisions on investigative procedures from those on the trial procedures, and regulate the investigation process through provisions specifically enacted for the purpose, rather than borrowing the provisions on the trial process. These would be more effective in ensuring

appropriateness and judicial control of the investigative procedures.

Lastly, policy considerations for improving the seizure and search process for digital evidence include strengthening the exclusion of illegally obtained evidence and deleting and destroying irrelevant information. As long as explicit provisions are in place to consistently maintain the lawfulness of the digital evidence seizure process, it would be desirable to apply the exclusion of illegally obtained evidence without exception in cases where procedural rules are violated, so as to minimize the possibility of privacy and fundamental rights being violated in the process of searching for and seizing digital evidence. Strict exclusion of illegally obtained evidence may provide a more powerful means of guaranteeing the legitimacy of investigation than any procedural rules. As for the second consideration, the deletion and destruction of irrelevant information is conducted as a means to eliminate the possibility of abuse or misuse of "imaging" copies of digital evidence seized by investigative agencies. However, it should be also considered that the deletion and destruction of imaging copies immediately after seizure may undermine the fairness of criminal proceedings. As such, there needs to be a procedural discussion on when and how to delete or destroy imaging copies obtained by investigative agencies. A possible alternative would be requiring the court to store the evidence until the final and conclusive judgment.

연구총서 23-A-08

디지털 증거 압수수색절차 개선에 관한 연구

발　　행 | 2023년 12월
발 행 처 | 한국형사·법무정책연구원
발 행 인 | 하 태 훈
등　　록 | 1990. 3. 20. 제21-143호
주　　소 | 서울특별시 서초구 태봉로 114
전　　화 | (02)575-5282
홈페이지 | www.kicj.re.kr
정　　가 | 10,000원
인　　쇄 | 크리커뮤니케이션 (02)2273-1775
I S B N | 979-11-986058-4-9　93360

• 사전 승인없이 보고서 내용의 무단 전제 및 복제를 금함.

디지털 증거 압수수색절차 개선에 관한 연구

Issues in Search and Seizure of Digital Evidence and Possible Improvements

KICJ 한국형사·법무정책연구원
Korean Institute of Criminology and Justice

93360
9 791198 605849
ISBN 979-11-986058-4-9