한국헌법학회 2023년 5월 공동학술대회

과학기술의 발전에 따른 형사절차상 인권보호의 헌법적 과제

- 일시: 2023년 5월 19일(금) 15:00~17:30
- 장소: 헌법재판연구원 8층 대강의실
- 주최: 사단법인 한국헌법학회, 헌법재판소 헌법재판연구원

사단법인 한국헌법학회
Korean Constitutional Law Association

헌법재판소
헌법재판연구원

일 정

14:30~15:00 등록

15:00~15:20 개회식 ▸사회: 정인경 제도연구팀장

▸개회사: 권건보 한국헌법학회장

▸환영사: 이헌환 헌법재판연구원장

▸기념촬영 및 정리

15:20~16:40 제1부 ▸사회: 정광현 교수(한양대학교)

[제1주제] **온라인 수색과 헌법상 기본권의 보호**

▸발표: 소은영 책임연구관(헌법재판연구원)

▸토론: 김해원 교수(부산대학교)

차원일 헌법연구원(헌법재판소)

[제2주제] **과학기술의 발전에 따른 형사절차상 변화와 헌법적 쟁점**

▸발표: 윤지영 연구위원(한국형사·법무정책연구원)

▸토론: 이재홍 교수(이화여자대학교)

김현귀 교수(한국해양대학교)

16:40~16:50 휴식 및 정리

16:50~17:30 제2부 ▸사회: 손인혁 교수(연세대학교)

[제3주제] **모바일 전자증거 압수수색과 적법절차, 최근 쟁점과 법원 판례의 동향**

▸발표: 오현석 판사(대전지방법원)

▸토론: 성중탁 교수(경북대학교)

김종현 책임연구관(헌법재판연구원)

17:30 폐회식

▸폐회사: 권건보 한국헌법학회장

개회사

존경하는 한국헌법학회 회원 여러분, 그간 안녕하셨습니까.

오늘 우리 한국헌법학회가 2023년도 두 번째 학술대회를 헌법재판소 헌법재판연구원과 공동으로 개최하게 되어 매우 기쁩니다.

먼저 오늘 이 학술대회가 차질없이 진행될 수 있도록 아낌없는 노고와 지원을 해주신 헌법재판소 헌법재판연구원의 이헌환 원장님을 비롯한 관계자 여러분께 한국헌법학회를 대표하여 감사의 인사를 드립니다.

그리고 연구과 교육 활동 등으로 대단히 바쁘신 중에도 몸소 참석하셔서 이 자리를 빛내주신 고문님들과 선후배 동료 회원님들께도 진심으로 감사드립니다.

오늘 공동학술대회에서 다루게 될 대주제는 “과학기술의 발전에 따른 형사절차상 인권 보호의 헌법적 과제”입니다.

형사절차에 있어서 국가권력의 통제 수단 확보가 근대헌법의 출발점이었다고 해도 과언이 아닐 것입니다. 그런 만큼 인권의 역사에 있어서 형사절차상 인신 보호와 형사절차의 헌법화는 매우 중요한 과제였습니다. 그런데 우리나라는 독재권력의 유지를 위해 무고한 시민들을 불법적으로 연행하고 구금하거나 고문을 자행하는가 하면 민간인들까지 함부로 사찰하고 미행하는 등 형사절차에 있어서 숱한 인권 유린이 자행되던 시절이 있었습니다. 1987년의 시민혁명을 거치면서 현행 헌법에 따라 출범한 헌법재판소가 위헌적인 형사절차 관련 법령과 관행들에 대해 제동을 거는 기념비적인 결정들을 여러 차례 내놓은 바 있습니다. 그러한 헌법재판소의 적극적인 역할에 힘입어 최근 30여 년간 형사절차 관련 법제도들이 인권친화적으로 상당 부분 개선되어 온 것이 사실입니다.

그런데 오늘날 과학기술의 발전, 특히 지능정보기술의 비약적 발전으로 인하여, 형사절차에서 인권 보호 문제는 새로운 국면을 맞이하고 있습니다. 지능정보기술을 활용한 새로운 수사기법들이 등장함에 따라 신체의 자유를 넘어서 주거의 자유, 통신의 자유, 개인정보자기결정권 등 기본권 침해의 문제가 색다른 양상으로 대두되면서, 관련 헌법조항의 전향적 해석뿐만 아니라 적법절차원리에 대한 새로운 이해의 모색이 필요하게 되었습니다.

이에 이번 학술대회는 새로운 기술적 환경에서 형사절차상 야기될 수 있는 인권 침해의 양상과 그에 대한 헌법적 대응방안에 대해 함께 고민해보는 자리로 마련하게 되었습니다. 구체적으로 온라인 수색과 기본권의 보호, 과학기술의 발전에 따른 형사절차상 변화와 헌법적 쟁점, 모바일 전자증거 압수수색과 적법절차 등 세 가지 주제를 놓고 심도 있는 발표와 토론이 진행될 예정입니다.

오늘의 발표와 토론은 형사절차상 인권 보호의 문제에 깊이 있는 연구를 해오신 헌법학 전공자와 형사법학 전공자, 그리고 형사재판과 헌법재판의 실무에 정통하신 분들이 맡아주셨습니다. 이에 따라 오늘 학술대회는 헌법학과 형사법학 간 및 법학계와 법조실무 간의 의견 교류가 활발하게 이루어지는 공론의 장이 될 것으로 기대됩니다.

그간의 연구와 경험을 기초로 정성스럽게 발제문을 준비해주신 소은영 책임연구관님, 윤지영 연구위원님, 오현석 판사님께 깊이 감사드립니다. 그리고 훌륭한 토론문을 작성해주신 김해원 교수님, 차원일 헌법연구원님, 이재홍 교수님, 김현귀 교수님, 성중탁 교수님, 김종현 책임연구관님께도 감사드립니다. 또한 바쁘신 가운데도 오늘 사회를 맡아주신 정인경 제도연구팀장님, 정광현 교수님과 손인혁 교수님께도 감사의 인사를 드립니다.

아울러 오늘 공동학술대회 전반을 기획하고 준비하느라 수고해주신 강일신 학술이사님과 한동훈 책임연구관님을 비롯한 한국헌법학회 및 헌법재판연구원의 실무 담당자분들께 각별히 고마운 마음을 전하고 싶습니다.

오늘 학술대회는 과학기술의 발전에 따른 형사절차상 변화와 헌법적 과제들에 대해 함께 고민해보는 소중한 기회가 될 것입니다. 모쪼록 오늘의 이러한 논의가 헌법과 헌법재판제도의 발전방안을 모색하는 데 크게 이바지할 수 있기를 기대해 봅니다.

그러면 지금부터 한국헌법학회와 헌법재판연구원이 공동으로 주최하는 학술대회를 본격적으로 시작하겠습니다.

2023년 5월 19일

제29대 한국헌법학회 회장 **권 건 보**

환영사

초록이 나날이 짙어지는 5월 오늘, 한국헌법학회와 헌법재판연구원이 공동으로, 「과학기술의 발전에 따른 형사절차상 인권보호의 헌법적 과제」라는 주제로 학술대회를 개최하게 되어 무한한 영광으로 생각하면서, 오늘 이 자리에 참석해주신 한국헌법학회 권건보 회장님과 여러 회원님들께 열렬한 환영의 뜻을 전합니다.

오늘날 인류사회는 20세기 100년간 엄청난 속도로 발전한 과학기술로 말미암아 일찍이 경험하지 못했던 새로운 양상으로 바뀌고 있습니다. 과거에는 며칠씩 혹은 몇 달씩 걸리던 정보의 교환이 거의 동시간적으로 행해지고 있고, 그에 따라 공간적 제약도 거의 없어져 가는 시대가 되었습니다. 뿐만 아니라 정보저장의 수단도 거의 무한이라 할 수 있을 정도로 그 용량이 커지고 있습니다. 인류가 만들어온 온갖 역사적·문화적·과학적 성과물들도 오늘날에는 모든 인류가 공유하는 시대로 접어들고 있습니다. ChatGPT와 같은, 이른바 AI 기반의 정보검색프로그램은 인류의 미래가 오히려 과학기술에 종속되어 노예화할지 모른다는 두려움마저 갖게 하고 있습니다.

인류역사에서 석기에서 청동기로, 청동기에서 철기로, 그리고 화약과 비행기 등의 전쟁무기의 발달로 한 집단의 다른 집단에 대한 지배-종속 관계를 만들었듯이, 오늘날에는 과학기술의 선점이 곧 한 집단의 다른 집단에 대한 지배-종속 관계를 구축할 수도 있습니다. 이러한 양상은 국가 사이의 경계를 넘어 전지구적인 차원에서 전개되고 있습니다.

아울러, 새로운 과학기술의 발달은 기존의 법체계와 그 집행기능을 송두리째 흔들어 놓고 있습니다. 특히 국가기능으로서의 형사사법기능의 집행에서 제기되는 문제들은 오랜 시간 동안 형성되어온 형사사법체계와 그 집행과정에서 적지 않은 문제들을 야기하고 있습니다.

권건보 회장께서 적절히 지적하신 바와 같이, 지능정보기술의 급격한 발달은 범죄의 양태 뿐만 아니라 그에 대응하는 수사기법에도 크게 영향을 미치고 있습니다. 인권침해의 가능성이 더 커지는 데에 대응하여 헌법적인 차원에서 새로운 해석론과 정책론을 모색하는 것은 시대적 요구라 할 것입니다. 오늘의 세부주제인 「온라인 수색과 기본권보호」, 「과학기술의 발전에 따른 형사절차상 변화와 헌법적 쟁점」, 「모

바일 전자증거 압수수색과 적법절차 – 최근 쟁점과 법원 판례의 동향」 등은 이러한 새로운 해석론과 정책론의 모색에 길잡이가 되는 선구적 논문으로 되리라 확신합니다. 각각의 주제를 발제해 주시는 헌법재판연구원의 소은영 박사님, 한국형사·법무정책연구원의 윤지영 연구위원님, 대전지법의 오현석 판사님께 깊이 감사드립니다. 아울러 토론을 맡아주실, 부산대 김해원 교수님, 헌법재판소의 차원일 연구원님, 이화여대의 이재홍 교수님, 한국해양대의 김현귀 교수님, 경북대의 성중탁 교수님, 헌법재판연구원의 김종현 연구관님께도 감사의 말씀을 드립니다. 사회를 맡아주시는 정인경 팀장님, 정광현 교수님, 손인혁 교수님께 감사의 말씀을 전하는 것은 당연히 빠뜨려서는 안되겠지요.

푸르름이 더해가는 5월은 답답한 대회장을 벗어나 산뜻한 공기와 자연에 마음껏 취하도록 유혹하는 계절입니다. 달콤한 봄날의 유혹을 물리치고 오늘의 주제에 관하여 열띤 발표와 토론이 이루어져서, 헌법학과 형사법학 그리고 실무계에 많은 기여가 있기를 다시 한 번 기원하면서, 오늘의 학술대회에 대한 환영의 말씀에 갈음하고자 합니다.

감사합니다.

2023년 5월 19일

헌법재판연구원 원장 **이 헌 환**

목 차

【제1주제】

온라인 수색과 헌법상 기본권의 보호*

소 은 영**

Ⅰ. 머리말

우리 일상은 이제 디지털 네트워크과 불가분의 관계에 있다. IT 기술과 우리 생활이 밀접하게 연결됨에 따라, 사이버공간을 활용하거나 사이버공간을 무대로 이용하는 범죄의 유형이 새로이 발생되고 증가하면서 범죄수사에서도 컴퓨터나 스마트폰 안에 있는 정보를 확보하고 수집하는 일이 매우 중요해졌다. 디지털정보의 압수·수색에 관해서는 2011년 형사소송법 개정 당시 제106조 제3항을 신설하였고,[1] 2017. 11. 29. 대법원은 원격 압수·수색 및 역외 압수·수색으로 취득한 디지털정보의 증거

---

* 이 글은 소은영, 온라인 수색에 관한 헌법적 검토, 헌법이론과 실무 2022-A-9, 헌법재판소 헌법재판연구원, 2023의 내용을 토대로 작성한 것임을 밝힙니다. 또한, 이 글의 내용은 발제자 개인의 견해이며 소속 기관의 공식 견해와는 무관합니다.

** 헌법재판소 헌법재판연구원 책임연구관

1) 형사소송법 제106조(압수) ①~② (생략)
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.

능력을 인정한 바 있다.[2] 한편, 사이버공간에서의 범죄 중에서 특히 다크웹(dark web)[3]에서 발생하는 테러, 마약이나 불법 무기 거래, 인신매매, 탈세와 불법자금세탁, 아동 성착취물 거래 등은 이제 국경을 넘어 전 세계적으로 문제되고 있는 상황이다. 우리나라에서도 잘 알려진 '웰컴 투 비디오' 사건을 시작으로 다크웹을 이용한 마약 유통, 불법마권거래 범죄가 적발되고 있다.

다크웹을 이용한 범죄는 매우 중대하고 사회적으로 악영향이 큰 유형이 많지만, 폐쇄적 네트워크를 통하여 은밀하게 발생하기 때문에 증거의 확보가 용이하지 않고 확보된 정보를 증거로 활용하는 면에서도 전통적인 형사절차에서 경험하지 못했던 문제들이 발생하고 있다. 이러한 상황에 대응하기 위한 수사기법으로 거론되는 것 중에, 처분대상자가 알지 못하는 사이에 대상자의 컴퓨터 등에 온라인 수색용 프로그램 등을 설치하여 정보를 수집하는 방식인 '온라인 수색'은 아직 우리 법체계에 도입되지 않았다. 이에 위와 같은 다크웹을 이용한 중범죄를 발견하고 대응하기 위하여 증거확보의 방법으로 온라인 수색 의 활용을 고려할 필요가 있다는 주장이 제기되고 있다.[4] 그런데 온라인 수색은 국가기관에 의하여 개인의 기본권이 침해될 소지가 매우 크기 때문에, 어떤 점에서 온라인 수색을 도입할 필요가 있는지 살펴보고, 만일 도입한다면 헌법상 기본권이 과도하게 제한되지 않도록 제도를 설계할 필요가 있다.

---

2) 대법원 2017.11.29. 선고 2017도9747 판결.

3) 다크웹(dark web)은 "일반 인터넷 검색 엔진에서 검색되지 않고, 특정 환경의 인터넷 브라우저에서만 접속되는 웹사이트"를 말한다(한국정보통신기술협회 정보통신용어사전 참조 (http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=101021-4 검색일: 2022. 11. 9.) 다크웹은 특히 익명성을 강화한 것으로서, 여러 국가의 네트워크를 경유하는 등의 방식을 사용하여 IP 추적을 피하고, 사용자로 하여금 접근을 위한 조건을 부가하여 접근성을 제한한다. 다크웹은 익명성과 추적의 어려움이라는 특성 때문에 범죄에 악용되는 사례가 증가하고 있다. 다크웹에서 이루어지는 범죄에서는 가상계좌를 이용하여 다양한 암호화폐로 거래가 이루어지는 경우가 많다.

4) 전현욱·윤지영, 디지털 증거 확보를 위한 수사상 온라인 수색제도 도입 방안에 대한 연구, 한국형사정책연구원, 대검찰청연구용역보고서, 한국형사정책연구원, 2012, 2쪽. 2021. 11. 국가인권위원회 위탁연구보고서에서는 디지털 성착취 범죄에 대처하기 위한 방법으로 "범죄자들이 디지털 기술을 사용해 외부와 차단해 놓은 범죄 정보에 수사기관이 접근하려면 그에 상응하는 '해킹' 기술이 요구된다"며 온라인 수색 도입의 필요성이 언급되었고(이화여자대학교 산학협력단(최희경·강정은·김구슬·김진·김희진·박숙란·조진경), 아동·청소년 성착취 피해예방과 인권적 구제방안 실태조사-디지털 성착취 피해를 중심으로, 국가인권위원회, 2021, 245, 323쪽), 2022. 4. 20. 경찰청은 '온라인 수색 활동의 적법성 검토와 도입 방안'에 관한 연구용역을 공개 입찰한 바 있다.

이와 같은 문제의식에 따라 이 글에서는 먼저 온라인 수색의 개념과 특징을 살펴보고, 이미 온라인 수색에 관한 입법을 마련한 해외 국가들의 사례를 검토한 후, 만일 온라인 수색을 법제화한다면 헌법상의 어떤 기본권이 제한되며 기본권의 제한 정도를 최소화하기 위하여 짚어보아야 할 내용은 무엇인지 검토하고자 한다.[5]

Ⅱ. 온라인 수색의 개념 및 허용 여부

1. 온라인 수색의 개념 및 방법

(1) 온라인 수색의 개념

선행 연구에 따르면, 온라인 수색은 대체로 “국가가 정보통신망에 연결되어 있는 타인의 정보기술시스템(IT 시스템)에 비밀리에 접근”[6]하여 “그 안에 있는 데이터를 수집하거나 해당 시스템의 이용행위를 감시하는 국가기관의 행위”[7]를 의미한다. 그리고 이를 다시 ‘온라인 검열’과 ‘온라인 감시’로 구분하여, 전자는 타인의 IT 시스템에 비밀리에 접근하여 저장된 데이터를 복제·열람하는 것을 의미하고, 후자는 일정 기간 동안 작동 중인 대상자의 IT 시스템의 이용 상황을 비밀리에 감시하는 것을 의미한다고 설명하기도 한다.[8] 혹은 국가가 타인의 컴퓨터시스템에 비밀리에 접

---

5) 온라인 수색을 도입하고 있는 국가들 중에서는 범죄를 포착하거나 수사하기 위한 목적으로 이용하는 경우뿐만 아니라 국가안보를 위한 정보수집의 목적으로 사용하기도 한다. 이는 수사기관이 아닌 정보기관에서 실시하는 것으로 파악되며 범죄 관련 온라인 수색과 구별하지 않고 함께 규율하기도 하고 별도의 규율을 마련하는 경우도 있다.(김창섭·이상진, 안보위협 최신 암호통신에 관한 대응방안 연구, 국가안보와 전략 제21권 제3호, 국가안보전략연구원, 2021, 59-65쪽 참조)

6) 박희영a, 예방 및 수사목적의 온라인 비밀 수색의 허용과 한계, 원광법학 제28권 제3호, 원광대학교 법학연구소, 2012, 154쪽; 신상미, 온라인수색의 법률적 문제점과 허용가능성, 경찰학연구 제20권 제3호, 경찰대학 경찰학연구편집위원회, 2020, 176쪽, 각주 8.

7) 박희영b, 보안취약점 이용 온라인수색과 국가의 기본권 보호의무, 비교형사법연구 제24권 제2호, 한국비교형사법학회, 2022, 151쪽. 다른 연구에서도 이와 거의 같은 의미로 온라인 수색을 파악하고 있다. 윤지영·류부곤·이병욱·전현욱·김진묵·김민규·이원상. 제4차 산업혁명 시대의 형사사법적 대응 및 발전방안(Ⅱ): 사물인터넷(IoT)과 블록체인, 한국형사정책연구원, 2019, 274쪽; 박희영a, 위의 글, 154쪽; 박웅신·이경렬, 다크넷 범죄현상과 형사법적 대응방안, 형사법의 신동향 통권 58호, 대검찰청, 2018, 237쪽; 신상미, 위의 글, 176쪽.

8) 박희영a, 위의 글, 154쪽 참조.

근하는 행위를 통틀어 온라인 접근(Online-Zugriff)이라고 한 후, 저장된 데이터를 복제하기 위하여 다른 컴퓨터시스템에 일시적으로 접근하는 온라인 수색(Online-Durchsuchung)과 컴퓨터시스템에서 이루어지는 활동을 다소 지속적으로 모니터링하는 온라인 감시(Online-Überwachung)가 이에 포함된다고도 한다.[9)]

한편, "수사기관이 잠재적 범죄자로 여기고 있는 개인의 컴퓨터에 해킹프로그램을 설치하여 그 컴퓨터를 통하여 교환되는 모든 통신내역이나 그 컴퓨터에 저장된 데이터를 감시하고 획득하는 것"[10)]을 '정보통신망 모니터링'이라고 정의하면서, 전자감시(electronic surveillance)[11)]를 포함하는 좀 더 넓은 범위의 감시수단을 의미하는 용어인 모니터링에는 실시간 전자통신내역을 감시하는 '감청'과 이미 통신업체 소유의 컴퓨터 서버에 저장되어 있는 통신 내역을 탐색하는 '온라인 수색'의 방식이 이에 포함된다고 보는 견해도 있다.[12)]

온라인 수색에 관한 선행 연구의 개념 표지에는 ①국가기관이 ②정보통신망과 연결되어 있는 IT 시스템에서 이루어지는 대상자의 행위 내지 활동을 ③대상자가 알지 못하는 사이에 기술적 수단을 사용하여 ④그 내용을 열람·수집하는 것이 포함되어 있다. '수색'이란 "압수할 물건이나 체포할 피의자·피고인을 발견할 목적으로 사람의 신체, 물건 또는 주거 기타의 장소를 '뒤져 찾는' 강제처분"[13)]을 의미하며, 온라인 수색 역시 타인의 IT 시스템에서 범죄사실 등을 '찾는' 것임은 분명하다. 다만, 타인의 IT 시스템에 있는 내용을 일회적으로 저장하는 것을 의미하는지 혹은 일정 기간 타인의 IT 시스템을 모니터링하는 것까지 포함하는지 여부에 관하여 선행 연구의 정의가 반드시 일치하지는 않는 것으로 보인다. 일정 기간 동안 대상자가 IT

---

9) 박희영c, 독일에 있어 경찰에 의한 '예방적' 온라인 수색의 위헌여부, 경찰학연구 제20호, 경찰대학, 2009, 185쪽; Ulrich Sieber, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen, Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg, 2007. 10, p. 1.

10) 오기두, 정보통신망 모니터링에 의한 범죄통제의 적합성, 형사정책연구 제27권 제4호, 한국형사정책연구원, 2016, 8쪽.

11) '전자적 감시'는 주로 미국의 판례와 관련 논의에서 등장하는 용어이다. 전자적 감시와 관련하여 미국 연방수정헌법 제4조에 관한 미국의 판례 및 입법례를 다룬 문헌으로, 윤지영, 미국의 통신감청 관련 법규 및 논의 동향, KIC 형사정책연구소식(2016 봄), 2016, 34쪽 이하 참조.

12) 오기두, 위의 글, 8쪽.

13) 이주원, 형사소송법, 박영사, 2022, 165-166쪽.

시스템을 사용하는 것을 모니터링한 후에 시스템 안의 내용을 저장하는 것도 가능하므로 일회적 접근에 의한 정보 수집과 일정 기간 동안의 감시를 명확히 구분하는 것이 쉽지 않고, IT 시스템을 열람하는 동안 실시간으로 이루어지는 대화내용을 모니터링하는 경우 감청과의 경계도 분명하지 않은 측면이 있다. 생각건대 IT 시스템 내에서의 활동을 모니터링하는 경우(이른바 전술한 '온라인 감시')라도 기술상 그 내용을 실시간으로 시스템 안에 저장하거나, 수사와 관련된 사항을 선별하여 저장하는 것이 가능하므로, 정보의 수집이 수반되는 한 온라인 수색의 개념 안에 포함될 수 있다고 본다. 이와 같은 점을 고려하여, 이하에서는 온라인 수색을 "국가가 정보통신망에 연결되어 있는 대상자의 IT 시스템에 대상자 모르게 접근하여 그 안에 있는 정보를 수집하는 행위"로 정의하도록 한다.

온라인 수색을 이렇게 정의할 때, 그 특징은 첫째, IT 시스템 안에 있는 증거를 수집하기 위해서 유체물인 컴퓨터나 휴대폰을 압수·수색하지 않고 시스템 안에 침입하여 증거를 수집하는 것, 둘째, 기술적 수단을 통하여 은밀히 이루어지는 것이다.[14)]

(2) 온라인 수색 방법

온라인 수색은 기술적으로 ①대상자와 대상 기기 탐색, ②대상자가 모르는 사이에 대상 기기에 대한 접근 실행, ③대상 기기로부터의 정보 수집이라는 3단계로 이루어진다. 구체적으로 ①탐색 단계에서는 대상자와 대상 기기의 특성을 바탕으로 적합한 해킹도구를 선택한다. ②실행 단계에서는 먼저 대상자에 대하여 은밀하게 대상자의 기기에 해킹도구를 심는 과정을 수행한다. 주로 감시 소프트웨어(해킹 프로그램)을 문자 메시지나 이메일에 첨부하거나(피싱(Phishing)) 특정 인터넷 사이트로 유인하여 대상자가 해당 사이트로 들어오면 감시 소프트웨어가 작동하도록 유도하는 방법(워터링홀(Watering hole)), 혹은 시스템의 백도어[15)]나 보안취약점을 이용하여 감시 소

14) 박희영a, 위의 글, 154쪽; 박웅신·이경렬, 위의 글, 237쪽; 정대용, 디지털 증거 수집을 위한 온라인 수색의 허용가능성에 관한 연구, 디지털포렌식연구 제12권 제1호, 2018, 69쪽.

15) 백도어(back door)란 시스템 접근에 대한 사용자 인증 등 정상적인 절차를 거치지 않고 응용 프로그램 또는 시스템에 접근할 수 있도록 하는 프로그램을 말한다. 관리자나 개발자가 시스템 유지 보수와 유사시 문제 해결 등을 위해 보안이 제거된 비밀 통로와 같은 역할을 한다. 개발한 시스템을 테스트하기 위하여 개발자가 삽입하는 백도어도 있으나, 악의적으로 사용자를 공격하기 위하여 인위적으로 만들어진 백도어를 특히 익스플로잇(exploit)이

프트웨어를 실행시키는 방법 등이 있다.[16] ③수집 단계에서는 대상 기기로부터 정보를 수집하고 이는 수사기관으로 전달된다.[17]

2. 온라인 수색의 허용 여부

형사소송법 제199조 제1항은 "수사에 관하여는 그 목적을 달성하기 위하여 필요한 조사를 할 수 있다. 다만, 강제처분은 이 법률에 특별한 규정이 있는 경우에 한하며, 필요한 최소한도의 범위 안에서만 하여야 한다."라고 하여 강제수사법정주의를 규정하고 있다. 온라인 수색은 수사의 대상이 된 사람의 의사에 실질적으로 반하여 그 사생활의 비밀과 자유라는 법익을 침해하는 강제수사에 해당하고,[18] 온라인 수색을 하기 위해서는 법률상의 근거가 필요하다.

(1) 형사소송법상의 압수·수색 규정에 따라 허용될 수 있는지 여부

전자정보는 출력·복제를 통하여 원본과 동일한 사본을 생성할 수 있기 때문에, 점유가 배타적으로 이전되는 유체물의 압수와 차이가 있다.[19] 2011. 7. 18. 법률 10864호로 개정된 형사소송법은 제106조 제3항에서 "법원은 압수의 목적물이 컴퓨

라고 하며, 공격자들은 컴퓨터 및 소프트웨어의 보안 취약점을 통해 사용자의 컴퓨터에 백도어를 만든다. 이렇게 악의적으로 생성된 백도어는 대부분 바이러스, 웜, 트로이목마 등과 같은 유해한 소프트웨어(통칭 '맬웨어(malware)'라 한다.)에 의해 생성되며, 자발적으로 생성되기보다는 사용자가 정상적인 소프트웨어라고 생각해 프로그램을 실행시키면 시스템에 백도어가 설치되도록 만들어지는 경우가 많다고 한다. (디지털타임스, 2013 5. 25. http://www.dt.co.kr/contents.html?article_no=2013050602012269795002&frommobile=1; 박상훈, IT World 용어풀이, 백도어, IT World, 2016. 2. 25. 참조. https://www.itworld.co.kr/news/98060)

16) 허황, 최근 개정된 독일 형사소송법 제100조b의 온라인 수색과 제100조a의 소스통신감청에 관한 연구, 형사법의 신동향 제58호, 2018, 101-103쪽 참조.

17) 김창섭·이상진, 안보위협 최신 암호통신에 관한 대응방안 연구, 국가안보와 전략 제21권 제3호, 국가안보전략연구원, 2021, 83-84쪽 참조. 박희영b, 위의 글, 151-152쪽에 의하면, 독일의 수사실무에서는 보안취약점을 이용하여 해킹 프로그램을 설치하는 방법이 주로 이용되고 있다고 한다.

18) 강현구, 온라인수색의 법적 성격 및 헌법적 쟁점, 형사법의 신동향 통권 제76호, 대검찰청, 2022, 134-135쪽.

19) 정대용·김기범·이상진, 수색 대상 컴퓨터를 이용한 원격 압수수색의 쟁점과 입법론, 법조 2016년 3월호(통권 714호), 법조협회, 2016, 44쪽.

터용 디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 “정보저장매체 등”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 정보저장매체 등을 압수할 수 있다”라고 규정하고 있다.[20] 전자정보가 압수·수색의 목적물이 될 수 있다고 하더라도 형사소송법 제122조는 “압수·수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단, 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 예외로 한다.”고 규정하고, 동법 제118조는 “압수·수색영장은 처분을 받는 자에게 반드시 제시하여야” 한다고 규정하고 있다.

그러나 온라인 수색은 처분대상자에게 사전에 통지하거나 영장을 제시하지 않고 당사자가 알지 못하는 사이에 이루어진다.[21] 이를 형사소송법 제122조 단서에서 규정하는 ‘급속을 요하는 때’에 해당하는 것으로 보아 온라인 수색이 허용될 수 있다고 볼 수 있는지 문제된다. 생각건대 온라인 수색은 범죄의 중대성이나 범죄가 이루어지는 사이버공간의 특성 때문에 다른 방법으로는 범죄사실을 포착할 수 없는 경우에 최후의 수단으로 실시되는 것이므로, 형사소송법 제122조 단서를 근거로 사전통지의 예외에 해당하는 경우라고 해석하는 것이 적절한지는 의문이다. 더욱이 형사소송법 제118조의 영장 제시의무는 이것이 현실적으로 불가능한 경우에 면제를 허용하고 있으나, 처분대상자 등의 부재 및 거부 등으로 인해 현실적·물리적으로 영장을 제시할 수 없는 불가피한 상황으로 인하여 불가능한 상황을 의미하는 것이지[22] 애초에 영장 제시를 배제하고 실시되는 온라인 수색이 영장 제시의무의 면제사유에 해당한다고 보기는 어렵다고 생각된다.[23]

한편, 피압수자의 참여권에 관해서도, 영장을 집행할 때는 일시와 장소를 참여권자에게 미리 통지하여 참여권을 보장하여야 한다(형사소송법 제122조, 제219조). 다

---

20) 동 조문에서는 전자정보를 압수하는 경우에도 그 목적물은 그 정보를 저장한 정보저장매체이지만 그 압수의 방법에 관한 특칙을 규정하는 방식을 취하고 있고, 명시적으로 전자정보를 압수의 목적물로서 인정하고 있지는 않다. 이재상·조균석·이창온, 형사소송법, 박영사, 2022, 238쪽.

21) 신상미, 위의 글, 178쪽.

22) 대법원 2015. 1. 22. 선고 2014도10978 판결 참조.

23) 같은 견해로 신상미, 위의 글, 179쪽 참조.

만 참여권자가 참여하지 않는다는 의사를 명시한 때 또는 급속을 요하는 때는 예외로 한다(형사소송법 제122조, 제219조). 온라인 수색의 경우 그 개념에 처분대상자가 이를 알지 못하는 것을 포함하고 있기 때문에, 원칙적으로 참여가 보장되고 예외적인 급속을 요하는 사유에 해당한다고 볼 것이 아니라 온라인 수색의 실시가 곧 처분대상자(및 변호인)의 참여권을 보장할 수 없음을 의미한다.

따라서 형사소송법상의 압수·수색 규정에 의하여 온라인 수색이 허용된다고 보기는 어렵다.

(2) 통신비밀보호법상 통신제한조치 대상에 해당하는지 여부

통신비밀보호법의 통신제한조치는 현재 진행되고 있거나 장래에 이루어질 우편물 또는 전기통신[24]의 내용을 그 대상으로 한다.[25] '통신제한조치'는 우편물의 검열 또는 전기통신의 감청을 의미하며(법 제3조 제2항), 이 법에서 감청이란 "전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것"이라고 정의하고 있다(법 제2조 제7호). 통신제한조치의 대상범죄는 법 제5조 제1항에 열거된 것에 한정되며, 주로 중범죄나 통신제한조치가 범죄 예방이나 증거수집에 적합한 범죄들이 이에 해당한다.

대법원은 '감청'의 개념에 비추어 보았을 때 감청이란 통신이 이루어지고 있는 상황에서 실시간으로 전기통신의 내용을 지득·채록하는 경우와 통신의 송·수신을 직접적으로 방해하는 경우를 의미하며, 이미 수신이 완료된 전기통신에 관하여 남아있는 기록이나 내용을 열어보는 등의 행위는 포함하지 않는다고 판시한 바 있다.[26] 즉, 감청은 전기통신의 송·수신과 동시에 이루어지는 경우만을 의미하고, 이미 수신이 완료된 전기통신의 내용을 지득하는 등의 행위는 감청에 포함되지 않는다.[27] 온라인 수색은 대상자와 제3자 사이의 통신을 실시간으로 감시하는 것이 아니라, 컴퓨

---

24) 「통신비밀보호법」의 '전기통신'이란 "전화·전자우편·회원제정보서비스·모사전송·무선호출 등과 같이 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것"을 의미한다.(동법 제2조 제3항)

25) 이주원, 위의 책, 190쪽.

26) 대법원 2012. 11. 29. 선고 2010도9007 판결; 대법원 2016. 10. 13. 선고 2016도8137 판결.

27) 대법원 2012. 10. 25. 2012도 4644 판결.

터나 휴대폰에 저장되어 있는 내용을 대상으로 감시 프로그램을 통하여 접근하여 그 내용을 수집하고 수사기관에 전달하는 것이다. 따라서 현재 진행 중인 통신만을 대상으로 하는 통신비밀보호법상의 통신제한조치와 온라인 수색은 개념상 차이가 있을 뿐 아니라, 온라인 수색으로 훨씬 더 광범위한 데이터의 수집이 가능하다.[28] 따라서 온라인 수색은 통신비밀보호법 제5조를 근거로 실시될 수는 없다.

3. 온라인 수색 도입 필요성에 관한 논의

온라인 수색과 같은 새로운 수사기법의 도입은 개인정보를 무제한적으로 수집할 수 있도록 하고, 사생활의 자유를 비롯한 헌법상 기본권을 과도하게 제한할 수 있으며, 사전 통지나 영장 제시의 어려움, 당사자 참여권 보장 제한 등으로 형사절차의 원칙에도 큰 제약을 수반하므로, 형사절차상의 법원칙과 헌법상 기본권 보장 정도의 후퇴를 가져올 수 있다는 문제가 제기될 수 있다. 이 때문에 온라인 수색이 영장주의의 근본을 흔들 수 있고, 사생활에 대한 포괄적 감시를 통하여 사생활의 핵심영역뿐만 아니라 개인정보자기결정권을 침해하며, 형사소송법이 보장하는 피의자, 변호인, 전자정보 저장장치의 소유자, 보관자 또는 관리자의 참여권을 배제하는 수사가 되기 때문에 허용될 수 없는 수사방법이라는 견해도 존재한다.[29]

그러나 지금까지 디지털 증거의 양적 증가와 중요성의 증대, IT 기술의 발전에 수반한 범죄 양상의 변화와 관련 범죄가 미치는 해악의 중대성을 감안하면, 온라인 수색이 이에 대처할 유효한 수사방법임을 부인하기는 어렵다고 생각된다.[30] 테러, 마약 거래, 아동 성착취물 거래 및 공유 등 중대 범죄의 혐의가 포착된 경우 다크웹에서 발생하는 범죄는 서버를 압수·수색하여도 IP 추적이 곤란하므로 해당 사이트의 운영자나 이용자를 찾기가 어렵다.[31] 이러한 상황을 고려해 볼 때 범죄수사에서 온라인 수색의 도입을 적극적으로 검토하여야 한다는 견해를 토대로 형사법 분야에서

---

28) 강현구, 위의 글, 138쪽에서는 “통신을 위해 저장되어 있는 데이터를 취득하는 것은 사실상 통신의 자유에 대한 제한에 해당하기 때문에 감청에 해당한다고 볼 여지도 있다.”고 하고 있는데, 이는 암호통신감청과 온라인 수색을 준별하지 않고 양자를 동일한 기회에 실행할 수 있음을 감안한 서술인 것으로 생각된다.

29) 오기두, 위의 글, 25-26쪽 참조.

30) 전현욱·윤지영, 위의 글; 윤지영·류부곤·이병욱·전현욱·김진묵·김민규·이원상, 위의 글, 279쪽.

31) 강현구, 위의 글, 129쪽.

온라인 수색의 도입 논의가 이루어져 왔던 것으로 파악된다.[32] 발전하는 IT 기술을 이용하는 범죄에 상응하는 새로운 수사기법의 도입 가능성을 검토해 보고, 만일 새로운 수사기법을 도입한다면 헌법상 기본권을 과도하게 침해하거나 형사절차의 원칙을 형해화하는 결과가 되지 않도록 적절히 입법화하는 방안을 고려할 필요가 있다.

Ⅲ. 해외 입법례

1. 독일

독일의 연방법에서 범죄 예방 및 수사를 위한[33] 온라인 수색은 연방범죄수사청법(BKAG: Bundeskriminalamtgesetz) 제49조 제1항에서 '정보기술시스템에서의 비밀침입(Verdeckter Eingriff in informationstechnische Systeme)'으로, 그리고 독일연방형사소송법(StPO: Strafprozeßordnung) 제100b조 제1항에서 '온라인수색(Online-Durchsuchung)'이라는 표제로 규정하고 있다.[34] 독일에서 온라인 수색이 위와 같이 규정되기까지 그 허용 여부와 헌법상의 요청에 적합하기 위한 요건에 관하여 연방헌법재판소의 결정에서 언급된 바 있고 그 내용이 입법에 영향을 주었다.

(1) 노르트라인 베스트팔렌 주 헌법보호법 사건

노르트라인 베스트팔렌 주 헌법보호법(das Verfassungsschutzgesetz Nordrhein-Westfalen, NWVSG)은 2006. 12. 20. 개정을 통해 특정한 범죄를 예방할 목적으로 통신장치에 대한 은밀한 관찰(heimliches Beobachten), 인터넷의 은밀한 탐지(sonstiges

32) 윤지영·류부곤·이병욱·전현욱·김진묵·김민규·이원상. 위의 글, 279쪽.

33) 독일에서 온라인 수색의 목적을 구분하는 이유는 나치의 비밀경찰에 정보수집과 수사기능이 통합되어 인권이 유린되었던 과거에 대한 반성에서 비롯되었다고 설명한다. 따라서 범죄예방 목적으로 수집된 정보는 향후 수사기관에 의해 형사소추목적으로 전용될 수 없다고 한다. 그럼에도 구체적인 경우 양자의 엄격한 구분은 쉽지 않다고 한다. 허황, 위의 글, 108쪽.

34) 박희영·이상학, 암호통신감청 및 온라인수색에서 부수처분의 허용과 한계, 형사정책연구 제30권 제2호, 한국형사정책학회, 2019, 5, 8쪽.

Aufklaeren des Internets), 기술적 수단을 통하여 인터넷 통신수단에 은밀히 접근(heimlicher Zugriff)할 수 있다고 하였다(제5조 제2항 제11호 참조). 이에 대해서 헌법소원이 제기되었는데, 연방헌법재판소는 2008. 2. 27. 해당 조항에서 규정하는 온라인 수색 자체가 기본법에 위배되는 것은 아니지만, 동 조항은 명확성 원칙과 법익균형성을 충족하지 못하여 기본법 제1조 제1항(인간의 존엄)과 제2조 제1항(일반적 인격권), 제10조 제1항(통신의 비밀), 제19조 제1항 제2문에 합치되지 않는다고 하였다.[35]

이 결정에서 연방헌법재판소는 정보자기결정권만으로는 개인의 인터넷상 정보활동을 완전하게 보호할 수 없다고 하면서, 기본법 제1조 제1항과 관련된 제2조 제1항의 일반적 인격권으로부터 도출되는 '정보기술시스템의 신뢰성과 무결성의 보장(Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systemen)'이라는 새로운 기본권(이하 'IT 기본권'으로 약칭)을 인정하고, 온라인 수색으로 제한되는 것은 이 'IT 기본권'이라고 하였다. 온라인 수색으로 얻게 되거나 관련되게 될 정보가 질적(사생활 보호 측면)으로나 양적으로나 매우 방대하고 중요하다는 점에서 높은 정도의 보호 요청이 존재하며, 온라인 수색의 대상자는 인격권을 탐지당하기 때문에, '인터넷 시스템의 신뢰성 보호'를 위하여 IT 기본권이 필요하다는 것이었다.

나아가 연방헌법재판소는 온라인 수색이 기존의 어떤 수단보다도 광범위한 정보에 접근할 수 있도록 하고 내밀한 영역까지 탐지할 수 있다는 점, 은밀한 방법으로 이루어진다는 점, 기술적으로 접근한 것만으로도 IT 기본권이 침해될 수 있다는 점에서 기본권이 중대하게 제한된다고 보았다. 이러한 온라인 수색이 정당화되기 위해서는 첫째, 매우 중요한 법익[36]에 대한 구체적인 위험이 발생했다고 볼 수 있는 근거가 있을 것, 둘째, 구체적인 위험이 실현될 충분한 개연성이 특정인에 의해 야기될 것, 셋째, 구체적 위험의 직전 단계에서 그 확인을 위해 이루어질 것을 요한다고

35) BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07. 이 판결의 전문 번역본은 박희영d, 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권(上), 법제 2008. 10, 43-68쪽; 박희영e, 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권(下), 2008. 11., 31-64쪽을 참조할 수 있다.

36) 여기서 중요한 법익이란 생명, 신체 및 사람의 자유, 국가의 토대나 존립 또는 인간존재의 기초에 있어 중요한 일반적 이익생존을 보장하는 공공급부시설의 본질적인 부분에 대한 기능도 여기에 포함된다. BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07, Rn. 247.

하였다.[37] 이를 위한 법적 보호장치로서 판사의 영장 발부, 사생활의 핵심영역 관련 정보를 수집하지 않도록 주의하고 수집된 경우 즉시 삭제될 것 등이 필요하다고 설시하였다.[38]

(2) 연방범죄수사청법(BKAG) 개정과 헌법불합치 결정

2008년 개정된 연방범죄수사청법[39]은 프로파일링, 신분위장수사, 주거 내 시각·음향 감청, 전기통신감청과 더불어, 제20k조 제1항에서 사람의 신체, 생명 또는 자유, 그리고 위협을 받을 경우 국가의 기반이나 존립 또는 사람의 존재 기반에까지 영향을 끼치는 공공급부시설에 대한 위험이 있다는 추정이 정당화되는 경우에 당사자 모르게 기술적 수단을 통해 정보기술시스템에 접근하여 시스템 내부의 정보를 수집할 수 있도록 하는 온라인 수색에 관한 내용을 규정하였다. 여기서는 온라인 수색의 대상, 시스템의 변경과 원상복구 및 무단 사용 등으로부터의 보호, 기록, 법원의 명령, 명령서 기재사항, 사생활의 핵심영역 보호 등의 내용이 규정되어 있었다(동조 제2항~제7항 참조).

그러나 온라인 수색을 비롯한 정보수집 권한을 규정한 조항들에 대한 헌법소원이 제기되었고, 연방헌법재판소는 2016. 4. 20. 주거 내 음성 감시, 온라인 수색, 전기통신감청, 통신사실확인자료 수집, 데이터를 수집하기 위한 특별한 수단을 사용한 주거 외 감시에 관한 수권규정은 일반적으로 헌법에 합치하지만, 사생활의 핵심영역의 보호에 관한 규정은 헌법에서 요청하는 조건을 충족하지 않는다고 하며 헌법불합치 결정을 하였다.[40] 이 결정에 따라 개정된 연방범죄수사청법[41] 제49조에서는 온라인 수색에 있어 사생활의 핵심 영역에 영향을 미치는 데이터는 사용할 수 없으며 지체 없이 삭제하도록 하는 등 법원의 통제에 대한 내용을 마련하였다(동조 제7항[42]).

---

37) BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07, Rn. 251, 253.

38) BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07, Rn. 258, 277.

39) 연방범죄수사청에 관한 상세는 정문식, 테러방지 감시조치에 대한 위헌심사기준, 법과 정책연구 제18집 제2호, 한국법정책학회, 2018, 5쪽 각주 7) 참조.

40) BVerfG Urteil vom 20. April 2016 - 1 BvR 966/09, 1 BvR 1140/09, Rn. 208.

41) 연방범죄수사청법은 2017년 6월 1일 '연방범죄수사청법의 새로운 체계화를 위한 법률(Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes)'에 의해서 전부 개정되어 2018년 5월 25일부터 시행되었다.

(3) 연방형사소송법 개정에 따른 온라인 수색 도입

2017. 8. 24. 시행된 개정 연방형사소송법은 온라인 수색의 법적 근거를 마련하였다.[43] 이에 따르면 일정한 중대 범죄를 저질렀거나 시도하려는 현저한 사실상의 근거가 있는 범죄자(공범 포함)에 대한 수사가 다른 방법으로는 현저히 곤란한 경우, "대상자 모르게 기술적 수단으로 대상자가 사용하는 정보기술 시스템에 침입하여 그로부터 데이터를 수집할 수 있다"(제100b조 제1항).

온라인 수색이 가능한 대상범죄는 내란, 민주적 법치국가 위험, 간첩, 외환의 범죄, 범죄·테러단체 조직, 화폐·유가증권 위조, 아동음란물 반포, 취득, 소지, 살인, 인신매매, 강제성매매·강제노동 및 자유박탈을 통한 착취, 특수절도, 특수강도, 영업적·범죄단체구성 장물취득, 금전세탁과 부정수익은닉 중 특히 중대한 범죄, 수뢰 및 증뢰 중 특히 중대한 경우, 난민·외국인체류·마약범죄 중 특히 중대한 경우, 전쟁무기통제 관련 법률·무기법 중 특히 중대한 범죄, 국제범죄 중 집단학살죄, 반인륜범죄, 전쟁범죄, 침략범죄 등으로 제한되어 있다(동조 제2항). 이는 주거 공간의 감청의 경우에도 같다(동법 제100c조 제1항 제1호). 한편, 제100a조의 소스통신감청과 제100f조의 주거 공간 밖에서 하는 감청, 제100g조 통신접속정보의 수집의 경우는 온라인 수색의 경우보다 대상범죄가 더 넓다(동법 제100a조 제2항, 제100f조 제1항, 제100g조 제1항 제1호 참조).[44]

---

42) 연방범죄수사청법 제49조(정보기술시스템에 대한 비밀 접근)
(7) 해당 조치를 통해 사생활의 핵심 영역에 관한 정보만을 알게 될 것이라는 실질적인 근거가 있는 경우 해당 조치는 허용되지 않는다. 가능한 한 사생활의 핵심 영역과 관련된 데이터가 수집되지 않도록 기술적으로 보장되어야 한다. 제1항에 따른 조치를 통해 얻은 결과는 지체 없이 이를 명령한 법원에 제출되어야 한다. 법원은 그 사용가능성 또는 삭제 여부를 지체 없이 결정하여야 한다. 사생활의 핵심 영역에 영향을 미치는 데이터는 사용할 수 없으며 지체 없이 삭제하여야 한다. 정보 수집 및 삭제 사실을 기록하여야 한다. 이 기록은 데이터 보호의 통제 목적으로만 사용할 수 있다. 이 기록은 제74조에 따른 통지 후 6개월 또는 법원이 통지의 최종 생략을 승인한 후 6개월 후에 삭제된다. 제69조 1항에 따른 데이터 보호 통제가 아직 종료되지 않은 경우 종료 시까지 기록을 보관해야 한다.

43) 연방형사소송법 조문의 원문과 번역은 독일법연구회, 독일 형사소송법, 사법발전재단 2018, 99-103쪽 참조.

44) 온라인 수색이 허용되는 범죄가 상당히 제한되어 있음에도 불구하고, 독일에서는 이 중 일부에 대해서 비판이 있다. 예컨대 "난민신청남용 유도죄(Verleitung zur missbräuchlichen Asylantragstellung)" 내지 재산권을 보호법익으로 하는 범죄들에 대해서 온라인 수색을 허용하는 것은 비례성을 잃은 것이라고 한다. 그리고 대상범죄를 "특별히 중한 경우의 범죄"로 제한한다든지 "범죄가 개별적인 경우에도 중하다"는 점을 확인하는 개별적 검토를 요

온라인 수색에 따른 기술적 변경은 정보수집에 필수적인 한도에서만 가능하고, 수사 후 자동 복구되도록 하여야 한다(제100a조 제5항 제2호·제3호 및 제100b조 제4항). 해킹 프로그램을 사용할 때는 사용한 프로그램의 명칭과 사용시점, 정보기술시스템의 식별 표시와 그 시스템에 대하여 일시적이지 않게 변경된 사항, 수집된 데이터의 확인을 가능하게 하는 표시, 집행기관을 기록해야 한다(제100a조 제6항 및 제100b조 제4항). 또한, 온라인 수색을 할 때 "가능한 한 사생활의 핵심영역과 관련되는 데이터는 수집되지 않는 것이 기술적으로 확보되어야 한다. 제100b조에 의한 조치를 통하여 확보되고 사생활의 핵심영역과 관하여 알게 된 사항은 지체 없이 삭제하거나 검찰이 데이터의 이용 가능성과 삭제에 관하여 재판하도록 그 명령 법원에 제출하여야 한다. 이용 가능성에 관한 재판은 이후의 절차에서 구속력이 있다."고 규정하고 있다(제100d조 제3항).

온라인 수색은 검찰의 신청이 있으면 검찰 소재지 지방법원 합의부에서 명할 수 있으며, 지체하면 위험할 우려가 있는 경우 재판장이 명령할 수 있다. 재판장의 (온라인 수색) 명령은 3근무일 내 형사합의부의 승인을 받지 못하면 효력을 상실한다. 최대 1개월의 제한이 있으며, 기존 수사결과를 고려하여 명령의 요건이 존속하는 한도에서 매번 1개월 이내의 연장이 허용된다. 명령 기간이 총 6개월까지 연장된 경우, 추가 연장에 관하여는 고등법원에서 결정한다.(제100e조 제2항)

사유가 종료된 후에는 지체 없이 온라인 수색을 종료하고 이를 명령한 법원이 알려야 하며(제100e조 제5항 참조), 수집한 정보는 온라인 수색을 명한 근거가 되는 범행의 규명이나 그 범행 혐의를 받는 자의 소재파악을 위해서만 사용할 수 있다(제100e조 제6항 참조). 한편, 온라인 수색의 목표인물 및 현저히 관련된 사람에게는 온라인 수색이 이루어졌음을 즉시 통지하여야 한다(제101조 제4항 제4호 및 제5항). 다만, 조사 목적, 사람의 생명, 신체의 불가침성, 개인적 자유와 중대한 재산가치를 위협하는 경우에는 통지를 보류할 수 있으나 그 사유를 기록에 기재하여야 하고(제101조 제5항), 온라인 수색 대상자 및 현저히 관련된 사람은 통지받은 때부터 2주일 내에 집행방법의 적법성에 관한 심사를 신청할 수 있으며, 그 재판에 대하여는 즉시항고를 할 수 있다(제101조 제7항). 온라인 수색을 통하여 수집한 개인정보는 형사

구하는 것만으로는 이러한 의심을 제거하지 못한다고 한다(Blechschmitt, Lisa, Zur Einführung von Quellen-TKÜ und Online-Durchsuchung, StraFo 2017, S. 361 ff. 허황, 위의 글, 120쪽에서 재인용).

소추와 이에 관한 법원의 심사에 더 이상 필요하지 않으면 지체 없이 이를 삭제해야 하고 그 사실을 기록에 기재해야 한다(제101조 제8항).

온라인 수색의 집행을 명한 사건 수(최초·연장 구분), 원인 범행, 실제 집행 건수 등을 통계로 작성하여 공개하도록 하고 있다(제101b조 제1항 및 제3항). 온라인 수색에 관한 통계는 2019년에 처음으로 작성되어, 2022년 기준 2020년 통계까지 공개되었다. 2019년에는 최초 및 연장 신청건수는 32건, 실제 집행 건수는 12건이었고, 2020년에는 최초 및 연장 신청건수는 23건, 실제 집행 건수는 8건이었다.[45]

2. 영국

영국에서 온라인 수색은 '장비 간섭(equipment interference)'이라는 이름으로 2016년 수사권한법(UK Legislation, Investigatory Powers Act 2016)에서 구체적으로 입법화되었다. 이 법에서는 정보기관이 장비 간섭을 수행하는 경우와 경찰 등 법집행기관이 수행하는 경우를 함께 규정하고 있다. 장비 간섭이란 영장을 발부받아 데이터 또는 기타 정보를 획득하기 위하여 장비, 즉 컴퓨터, 태블릿, 스마트폰, 케이블, 기타 네트워크 장치 및 이와 같은 기기와 관련하여 사용할 수 있는 것, 케이블, 와이어, 저장 장치(USB, 하드 디스크 드라이브) 등에 물리적(물리적 접근이 확보된 장비에서 데이터를 몰래 다운로드)으로 혹은 원격(장비에 소프트웨어를 설치하여 데이터를 원격으로 추출하는 것)으로 간섭하는 것을 의미한다.[46] 또한, 당사자 모르게 원격으로 감시프로그램을 설치하는 것 외에 물리적으로 대상자의 주거에 침입하여 대상 기기에 프로그램을 설치하는 것도 가능하다. 이처럼 수사권한법상의 장비 간섭은 물리적인 접근도 포함하므로 온라인 수색보다 넓은 개념이라고 할 수 있다.

장비 간섭 영장의 발부는 집행 주체가 정보기관인 경우에는 장관이, 법집행기관인 경우에는 지역경찰청장(chief constable)이 하도록 되어 있는데, 공통적으로 발부권자

45) 상세한 보고 내용은 연방사법청(Bundesamt für Justiz)의 사법통계(Justizstatistiken) 참조. (https://www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken_node.html#AnkerDokument44152 검색일: 2022. 12. 9.) 통신 감시(Telekommunikationsüberwachung) 항목의 보고서 및 관련 보도자료를 참조(2019년 통계 https://www.bundesjustizamt.de/DE/ServiceGSB/Presse/Pressemitteilungen/2020/20201218.html?nn=74788, 2020년 통계 https://www.bundesjustizamt.de/DE/ServiceGSB/Presse/Pressemitteilungen/2022/20220808.html)

46) Home Office, Equipment Interference − Code of Practice, 2018, p. 6, 10.

의 허가 후 '사법위원(judicial commissioner)'[47]의 영장 발부 동의를 필요로 한다. 사법위원은 영장의 필요성과 영장에 의하여 수행될 행위가 달성하고자 하는 목적에 비례하는지 여부를 검토하여 동의 여부를 결정한다(제106조 제1항-제5항). 사법위원은 법관의 경력이 있는 사람이 임명되나 행정부에 소속되어 있으므로, 영국에서 온라인 수색의 승인은 행정부의 권한 내에서 이루어지되, 사법위원의 동의 절차를 두어 통제를 하고 있는 것으로 볼 수 있다.

장비 간섭 영장에 관한 내용은 3년간 이를 검색할 수 있도록 하며, 수집된 정보는 필요최소한도 내에서 사용, 열람되어야 하며, 그 한도 내에서 복사할 수 있다. 그리고 수집된 정보가 더 이상 필요하지 않게 된 경우에는 즉시 삭제를 표시하고 안전하게 파기하여야 한다.[48]

3. 미국

미국에서는 온라인 수색에 대한 특별한 법적 근거가 마련되어 있었던 것이 아니라, 통상적인 압수·수색 영장에 의하여 디지털 증거를 수집하는 경우 증거수집의 방법으로 온라인 수색을 명하는 내용이 포함되어 있을 때 네트워크 수사기법 (NIT, Network Investigative Technique) 영장으로 지칭되고 있었다.[49] 이때 어떤 방법으로 디지털 증거를 수집하였는지에 관하여, FBI가 카니보어(carnivore),[50] 매직 랜턴

---

47) 수사권한법 제8편 제1장에서는 수사권한위원(Investigative Powers Commissioner)과 사법위원(Judicial Commissioner)에 관하여 규정하고 있다. 1인의 수사권한위원을 포함하여 최대 16인의 사법위원은 수사권한위원실(Investigatory Powers Commissioner's Office. 'IPCO'로 약칭)의 구성원이다. 수사권한위원은 사법위원으로서의 지위와 권한도 동시에 가지고 있다. IPCO는 수사권한법에 따라 수사권한위원과 사법위원의 직무 수행을 지원하는 기능을 수행한다. IPCO는 수사권한법이 시행되기 전에 종전의 감시 위원회(the Office of Surveillance Commissioners, OSC), 통신 감청 위원회(the Interception of Communications Commissioner's Office, IOCO), 정보국 위원회(the Intelligence Service Commissioner's Office, ISComm) 세 기관이 합쳐지면서 만들어졌다. 수사권한법에 의하여 내무부로부터 자금을 지원받지만, 내무부 소속기관이 아니며 독립적으로 업무를 수행한다. 수사권한위원과 사법위원 외에도 조사관, 변호사 및 정책 공무원을 포함하여 약 50명의 구성원이 있다.

48) Home Office, Equipment Interference − Code of Practice, 2018, pp. 30-32.

49) 김학경, 미국의 온라인수색 제도에 관한 연구 : 연방형사소송규칙 제41장 개정내용 중심으로, 시큐리티 연구 제72호, 한국경호경비학회, 2022, 6쪽.

50) 인터넷 서비스 제공자의 블랙박스에 설치되어 감시 대상 컴퓨터의 이메일이나 채팅 내용, 방문 웹사이트 등을 파악할 수 있다. 2000년에 처음으로 공개되었다. Orin S. Kerr,

(Magic Lantern),[51] CIPAV[52]와 같은 스파이웨어 프로그램을 개발하고 사용해 왔다는 것이 알려졌다.[53]

그 후 2014년에서 2015년 사이에 다크웹상의 불법 아동·청소년 성착취물 거래 사이트였던 Playpen 사이트 접속자를 검거하기 위하여 FBI가 신분위장수사 형태로 사이트를 운영하면서 악성코드를 설치하여 이용자의 IP 주소를 파악하였다. 이 사건에서 기소된 접속자 대부분이 영장 관할 지역 외의 거주자였기 때문에 역외 관할권(extraterritorial jurisdiction) 문제가 제기되었다. 온라인 수색으로 수집한 증거의 증거능력에 관한 법원의 판결이 엇갈리자, 이를 계기로 2016년 12월 1일 미국 연방형사소송규칙(Federal Rules of Criminal Procedure) Rule 41이 개정되었다. 이에 따르면, 범죄 관련 행위가 발생하였을 가능성이 있는 관할 구역에서, 권한을 가진 치안판사는 "(A) 매체나 정보가 위치한 장소가 기술적 수단을 통해 숨겨져 있는 경우, (B) 18 U.S.C. § 1030(a)(5)의 범죄를 수사함에 있어, 매체가 정당한 승인 없이 손상되고, 그러한 컴퓨터가 5개 이상의 관할 지역에 위치하는 보호되는 컴퓨터인 경우"에, 관할 구역 내부 또는 외부에 위치한 전자 저장매체를 수색하기 위하여 원격접근을 허용하거나 전자적으로 저장된 정보를 압수 수색하기 위한 영장을 발부할 수 있다.

Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't", 97 Nw. U. L. Rev. 607, 2003, p. 622.

51) 2001년에 처음 알려진 프로그램으로서, 키로깅 소프트웨어이다. 모든 키스트로크(키보드에서의 입력)을 기록하여 감시 대상자의 이메일, 대화내용, 입력한 로컬 파일의 내용을 기록할 수 있다. 매직랜턴은 위장 이메일 메시지 등을 통하여 사용자(대상자)에게 송부되어 대상자의 컴퓨터에 설치되도록 만들어졌다.

52) 후술하는 2007년 Timberland 고등학교 폭탄테러 위협 사건을 통해 알려졌다. CIPAV는 대상 컴퓨터에서 스파이웨어처럼 작용하여, 컴퓨터의 IP 주소나 현재 로그인한 사용자의 이름, 작동중인 프로그램 리스트 및 기타 이와 유사한 정보 등을 수집하여 수사기관의 컴퓨터로 그 내용을 전달하게 된다.

53) 이에 관한 상세한 내용으로 윤지영, 미국 수사기관 온라인 감시에 대한 비판적 연구, 형사법의 신동향 제39호, 대검찰청, 2018, 90쪽 이하 참조.

Ⅳ. 온라인 수색으로 제한되는 기본권과 제한의 최소화

1. 제한되는 기본권

(1) 사생활의 비밀과 자유

온라인 수색으로 인하여 제한되는 주된 기본권은 헌법 제17조에서 보장하는 '사생활의 비밀과 자유'라고 할 수 있다. 전술한 바와 같이 온라인 수색을 "국가가 정보통신망에 연결되어 있는 대상자의 IT 시스템에 대상자 모르게 접근하여 그 안에 있는 데이터를 수집하는 행위"로 정의한다면, 온라인 수색에 의하여 대상자의 IT 시스템 내에 있는 정보 전체를 열람하고 그것을 수집할 수 있다는 점에서 사생활의 비밀과 자유 제한의 정도는 현재 우리나라의 현행법에서 규정한 어떤 형태의 국가기관에 의한 정보수집·탐지보다 중대하다. 정보통신 시스템이 침입하여 그 안에 저장되어 있는 정보를 모두 수집한다는 것은, 온라인상에서 상당한 부분의 일상생활이 이루어지는 현실을 감안한다면 오프라인에서의 생활과 사회적 접촉으로는 생각할 수 없을 만큼 광범위한 정보를 수집하여, 한 개인에 관하여 샅샅이 알아내는 것도 기술적으로는 가능하다. 따라서 온라인 수색으로 인한 사생활의 비밀과 자유의 제한이 심대하다는 것에는 의문의 여지가 없을 것이다. 덧붙여 사생활에 대한 침해뿐만 아니라 국가에 의한 감시로 인해 사이버공간에서 사생활을 자유롭게 영위할 권리가 위축되는 결과를 초래할 수 있다.

사생활의 비밀과 자유도 중대한 공익을 위하여 필요한 경우에는 제한될 수 있으며, 이때 과잉금지원칙을 준수해야 한다. 온라인 수색의 경우 침해되는 사생활의 비밀의 심대성에 비추어 볼 때 추구하는 공익이 매우 중대할 것을 요한다. 공익에는 중대한 범죄에 대한 효과적인 형사소추의 이익 및 형사절차에서 진실규명의 이익[54] 이 포함되며, 온라인 수색 대상자가 그 중대한 범죄혐의를 받고 있을 것을 요한다.

한편, 헌법재판소는 수사기관이 '수사의 필요성'이 있는 경우 전기통신사업자에게 가입자의 위치정보 추적자료나 통신사실 확인자료의 제공을 요청하는 것은 "수사의 신속성과 효율성을 도모하고 이를 통하여 실체적 진실발견과 국가형벌권의 적정한 행사에 기여하고자 하는 것이므로" 입법목적의 정당성은 인정할 수 있다고 하면서

54) 한수웅, 헌법학, 법문사, 2021, 717쪽.

도,[55] 보충성 등의 요건을 두지 않은 것이 침해의 최소성 요건을 충족하지 않는다고 보았다. 또한, 통신비밀보호법의 통신제한조치는 범죄를 효과적으로 규명할 수 있는 수단 중에서 기본권을 적게 침해하는 대안적 수단이 없는 경우에만 허용된다고 하여 보충성 요건을 두고 있다(통신비밀보호법 제5조 제1항 참조).[56] 결국 온라인 수색 자체가 헌법에 위배되는 것이 아니라면, 대상 범죄를 엄격하게 제한하거나 다른 수단으로는 도저히 대응하기 어려운 경우에 한하여 온라인 수색을 허용하는 등의 제도 설계를 통해 사생활의 비밀 및 자유의 제한 정도를 가급적 줄일 필요가 있을 것이다.

(2) 개인정보자기결정권

헌법재판소는 개인정보자기결정권은 "자신에 관한 정보가 언제, 누구에게, 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리"[57]를 의미하며, 이는 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 보장된다고 한다.[58] 개인정보자기결정권의 보호대상인 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보를 의미한다.[59] 이러한 개인정보는 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함하는 것으로 이해된다.[60][61] 헌법재판소는 전기통신사업자가 수사기관 등에 제공하는 통신자료에 포함되는 이용자의 성명, 주민등록번호, 주소, 전화번호, 아

---

55) 헌재 2018. 6. 28. 2012헌마191 등, 판례집 30-1하, 564, 578.

56) 한수웅, 위의 책, 717-718쪽.

57) 헌재 2005. 5. 26. 99헌마513등, 판례집 17권 1집 668, 682.

58) 헌재 2012. 12. 27. 2010헌마153, 판례집 24-2하, 537, 547; 헌재 2018. 8. 30. 2016헌마483, 판례집 30-2, 552, 561 등 참조.

59) 권건보, 개인정보보호의 헌법적 기초와 과제, 저스티스 통권 제144호, 한국법학원, 2014, 16쪽.

60) 헌법재판소 2005. 5. 26. 99헌마513, 판례집 17-1, 682.

61) 개인정보보호법 제2조 제1호 "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다.

이디, 가입일 또는 해지일과 같은 정보,[62] 발·착신 통신번호, 전기통신개시·종료시간 등의 통신사실 확인자료는 개인정보에 해당한다고 하였다.[63]

온라인 수색은 대상자의 정보통신 시스템 안에 있는 정보를 수집하는 것으로, 대상자가 사용하는 특정 기기 내부에 있는 정보 일체가 수집되고, 그 안에는 정보주체를 타인으로부터 식별가능하게 하는 개인정보 역시 포함될 수 있다. 즉, 대상자의 컴퓨터, 태블릿, 휴대폰 등 대상 기기에서의 로그기록, 아이디, 패스워드, IP 주소를 탐지하는 것도 기술적으로 가능할 뿐만 아니라, 인터넷을 이용하며 사용되는 이용자의 신상정보는 물론, 금융정보, 신용정보 등이 확인되고 수집될 수 있다. 이러한 정보는 개인정보자기결정권에 의하여 보호되는 개인정보에 해당하며, 대상 기기에서 수집한 정보에 포함되어 있는 타인의 개인정보를 통하여 그 사람을 식별할 수 있으므로 제3자의 개인정보자기결정권의 제한 역시 문제될 수 있다.

다만, 온라인 수색으로 수집되는 정보는 개인정보뿐만 아니라 사생활의 광범위한 영역이 포함될 수 있으므로, 실제 헌법재판소에서 온라인 수색과 관련된 내용이 문제될 때 제한되는 주된 기본권인 사생활의 비밀과 자유를 중심으로 판단이 이루어질 것이라고 생각된다.[64]

(3) 통신의 비밀과 자유

헌법 제18조에서 보장하는 통신의 자유는 통신의 비밀보호를 그 핵심내용으로 하며, 통신의 내용뿐만 아니라 통신에 관한 정보 일체를 그 보호대상으로 한다.[65] 헌법재판소는 “자유로운 의사소통은 통신내용의 비밀을 보장하는 것만으로는 충분하지 아니하고 구체적인 통신관계의 발생으로 야기된 모든 사실관계, 특히 통신관여자의 인적 동일성·통신장소·통신횟수·통신시간 등 통신의 외형을 구성하는 통신이용의 전

---

62) 헌재 2022. 7. 21. 2016헌마388 등, 공보 제310호, 1037, 1046.

63) 헌재 2018. 6. 28. 2012헌마538, 판례집 30-1하, 596, 606.

64) 통신감청과 관련하여 개인정보 중 개인의 사생활의 보호 필요와 중첩되는 범위의 개인정보는 헌법에 명문의 규정이 있는 사생활의 비밀과 자유의 보호대상이라고 보아야 하므로, 통신감청에 의하여 제한되는 주된 기본권은 사생활의 비밀과 자유라고 보는 견해로, 권건보, 위의 글, 21쪽. 헌법재판소는 인터넷 회선감청, 즉 소위 ‘패킷감청’이 문제된 사건에서 개인정보자기결정권을 침해하는지 여부에 대하여 판단하지 않고 사생활의 비밀과 자유를 중심으로 판단하였다(헌재 2018. 8. 30. 2016헌마263, 판례집 30-2, 481).

65) 김하열, 헌법강의, 박영사, 2021, 545쪽; 황성기, 현행 통신비밀보호법제의 헌법적 문제점, 언론과 법 제14권 제1호, 2015, 12-13쪽.

반적 상황의 비밀까지도 보장한다."[66]고 하여, 통신사업자에 대하여 통신자료를 요청하는 것이 이용자의 통신의 자유를 제한한다고 한 바 있다.

온라인 수색은 대상자의 IT 기기에 기술적 방법을 사용하여 침입한 후 그 내용을 수집·저장하는 방식으로 이루어진다. 이때 대상 기기의 정보를 망라하여 수집하기 때문에 그 중에는 전자우편이나 IT 기기를 이용한 타인과의 통신 내용이 포함될 수 있다. 온라인 수색은 감청과 같이 통신이 이루어지는 동안에 실시될 것을 요하지는 않으나, 전술한 타인과의 통신 내용뿐만 아니라, 누구와 얼마나 빈번하게 통신을 하였는지 등의 상황도 온라인 수색을 통하여 수집될 수 있으므로 통신의 비밀을 제한할 수 있다.

(4) 새로운 기본권의 도입 필요 여부-독일의 IT 기본권 논의를 소재로

전술하였듯이 노르트라인 베스트팔렌 주 헌법보호법에 대한 독일 연방헌법재판소 결정에서는 제한되는 기본권으로 IT 기본권, 즉 '정보기술시스템의 신뢰성과 무결성의 보장(Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systemen)'을 제시하였다. 정보기술의 발달로 인하여 필연적으로 발생하는 대량의 개인관련 정보 처리와 정보기술시스템의 네트워크화는 생활의 거의 모든 영역에서 원하지 않아도 자신의 행동 등이 광범위하게 추지될 수 있는 가능성을 높인다. 현대사회를 살아가는 사람들에게 정보기술시스템의 이용은 불가피하므로, 인격발전의 억압을 막기 위해서는 정보기술시스템에 대한 신뢰성과 무결성의 보장에 대한 기대를 갖게 되며 기본법은 개인의 인격 발현을 보장하기 위하여 이러한 기대를 존중하여야 한다는 생각에서 IT 기본권이 출발하였다는 것이다.[67] IT 기본권은 개인의 자기결정을 출발점으로 고려하는 패러다임이 아닌, 정보기술 시스템 전체의 신뢰성을 보장하는 것으로 개인의 자유나 인격발전이 개인으로 환원될 수 없는 사회관계 즉, 정보기술시스템을 통한 네트워크에 의존하고 있다는 사실이 개인의 인격발현에 있어 독자적인 의의를 갖는다는 생각에 기초한다.

---

66) 헌재 2018. 6. 28. 2012헌마538, 판례집 30-1하, 596, 605.

67) Wolfgang Hoffmann-Riem, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S.1014, S.1022; Gabriele Britz, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Wolfgang Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, Tübingen 2010, S.588ff.

그런데 연방헌법재판소가 새로이 창설한 IT 기본권에 대하여, 독일에서는 비판적인 견해와 독자적 의의를 인정하는 견해가 대립되고 있는 것으로 보인다. 즉, IT 기본권에 대하여 비판적인 견해는 새로운 기본권을 도출해 내지 않고도 기존에 연방헌법재판소가 인정하였던 개인정보자기결정권으로 설명하는 것이 가능하다고 한다.[68] 공권력이 광범위하게 데이터를 수집하는 것의 위험성은 정보자기결정권 관련 논의에서 이미 다뤄지고 있던 것이고, IT 기본권이 강조하는 인격 발현에 대한 위험은 새로운 기본권을 발굴해 낼 것이 아니라 기존의 정보자기결정권 침해 여부에 대한 비례심사를 강화하거나 절차적 보완을 요구하는 것으로 대응이 가능하다는 것이다.[69] 반면 연방헌법재판소가 IT 기본권을 도출한 것은 정보기술시스템의 무결성과 이에 대한 신뢰의 보장을 통해서 개인의 기본권을 충실하게 보장하기 위함이며,[70] 개인의 IT 시스템에 비밀리에 침입하였지만 아직 정보수집·열람이 이루어지지 않은 경우에는 개인정보자기결정권의 침해는 아니나 IT 기본권의 침해는 이루어졌다고 볼 수 있다는 점에서 IT 기본권을 도출한 실익을 찾는 견해도 있다.[71]

IT 기본권이라는 별도의 기본권을 도출한 것의 가장 큰 의의는 IT 시스템이라는 특정한 환경에서의 행위 및 관계를 개인의 인격발전에 불가결한 것이라고 보아 명시적으로 기본권의 보장 대상이라고 함으로써, 개인의 인격 발전을 보다 충실하게 보장하려는 시도라고 평가할 수 있다고 생각된다.

그러나 독일에서 IT 기본권이라는 별도의 기본권을 도출한 것이 일정한 의의를 갖는지에 대한 논의는 별론으로 하더라도, 과연 우리나라에서 온라인 수색으로 인한 개인의 기본권 침해가 문제된 경우 독일과 같이 새로운 기본권을 인정할 필요성이 있는지 생각해 볼 필요가 있다.[72] 2008년 노르트라인 베스트팔렌 주 헌법보호법 헌

---

68) 이권일, 헌법상 보호되는 프라이버시 개념의 변화에 관한 소고-독일 연방헌법재판소 판례 분석을 중심으로, 세계헌법연구 제25권 제1호, 세계헌법학회 한국학회, 2019, 160-161쪽에서는 IT 기본권과 개인정보자기결정권의 보호범위는 거의 일치하고 다만 개인정보자기결정권을 보충하고 세월에 맞게 부족한 부분을 개선한 것이라고 한다.

69) Gerrit Hornung, Erwiderung－Die Festplatte als ‘Wohnung’?, JZ 2007, S.301f.

70) Wolfgang Hoffmann-Riem, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S.1012f.

71) Wolfgang Hoffmann-Riem, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S.1012.

72) 국내의 선행 연구에서도 IT 기본권을 인정해야 한다는 견해가 없지 않으나(김연희, 온라인 수색 도입을 위한 문제점과 방안에 관한 소고, 법학연구 제64호, 전북대학교 법학연구소, 311쪽 이하; 명재진, "IT(정보기술) 기본권의 체계화에 관한 연구, 헌법논총 제20집, 헌법

법불합치 결정 이후 2016년 연방범죄수사청법에 대한 결정에서도 제한되는 기본권으로 IT 기본권이 언급되나 그 상세한 내용과 개인정보자기결정권과의 관계에 대해서는 명확하게 설시하고 있지 않는 것으로 보인다. 독일연방헌법재판소는 IT 기본권을 정보기술시스템에 대한 신뢰성과 무결성을 보장하는 기본권이라고 하면서 그 근거를 독일기본법 제2조 제1항 및 제1조 제1항에서 찾고 있어 기본권의 보호 대상이 IT 시스템의 신뢰성과 무결성에 대한 사용자(기본권의 주체)의 기대인지, 아니면 시스템 그 자체인지 명확하지 않고, 정보자기결정권과의 관계도 해명되지 않은 부분이 있다고 생각된다. 우리 헌법재판소의 '인터넷회선 감청' 결정에서는 헌법 제18조의 통신의 비밀과 자유 및 헌법 제17조의 사생활의 비밀과 자유를 제한하는지 여부에 대한 판단을 하면서, 정보통신기술의 발달에 따른 독자적 기본권의 인정 여부나 통신의 비밀과 자유 및 사생활의 비밀과 자유의 내용에 대한 변화의 가능성을 따로 언급하지는 않았다. 이러한 우리 헌법재판소 선례의 태도를 고려해 볼 때, 현재로서는 온라인 수색으로 제한되는 주된 기본권은 사생활의 비밀과 자유의 침해라고 보는 것이 적절하며, 온라인 수색으로 인한 침해 양상의 특수성을 감안하여 그 침해 여부를 판단하는 것으로 족하다고 생각된다.

(5) 영장주의

대상자가 알지 못하는 사이에 IT 시스템에 침입하여 그 안에 저장되어 있는 정보를 수집하는 온라인 수색은 비록 전기통신사업자가 아닌 처분대상자에 대하여 직접 이루어지고, 저장이 완료된 정보를 대상으로 한다는 점에서 차이가 있지만 대상자가 알지 못하는 사이에 그에 관한 정보를 수사기관이 대상자의 의사에 반하여 수집한다는 점에서 마찬가지로 강제처분이라 할 수 있고 영장주의가 적용된다. 입법자는 수사기관의 강제처분에 관한 법률을 제정함에 있어, 헌법 제12조 제3항을 준수하는 범위 내에서 해당 강제처분의 특수성, 그 강제처분과 관련된 우리 사회의 법 현실, 국민의 법 감정 등을 종합적으로 고려해 정책적인 선택을 할 수 있다.[73] 따라서 만일 온라인 수색이 입법화된다면 그 구체적인 내용과 허가 요건 및 통제절차에 관해

재판소, 2009, 292쪽), IT 기본권을 다룬 대부분의 선행 연구는 독일의 논의를 소개하면서 우리나라에서의 인정 여부에 대한 논의는 상세히 다루지 않고 있다.

73) 헌재 2012. 5. 31. 2010헌마672 참조; 헌재 2018. 6. 28. 2012헌마191 등, 판례집 30-1하, 564, 582.

서는 헌법에 위반되지 않는 범위 내에서 입법자가 재량을 갖는다.

헌법재판소는 헌법 제12조, 제16조 후문 등의 헌법 규정을 근거로 "형사절차와 관련하여 체포·구속·압수·수색 등의 강제처분을 함에 있어서는 사법권 독립에 의하여 신분이 보장되는 법관이 발부한 영장에 의하지 않으면 아니 된다는 원칙"으로 '영장주의'를 도출하고[74] 영장주의의 본질은 강제처분을 함에 있어서는 중립적인 법관이 구체적 판단을 거쳐 발부한 영장에 의하여야만 한다는 데에 있다고 보고 있다.[75] 온라인 수색의 경우 원칙적으로 수사기관이 영장(내지 허가장)을 사전에 청구하여 법관이 영장 발부 여부를 판단하도록 법률에 규정한다면, 헌법 제12조 제3장이 규정하는 사전영장원칙은 충족된다고 할 수 있다.

또한, 헌법상 명문의 규정은 없으나 영장주의원칙 하에서 일반영장은 허용되지 않으므로, 범죄의 내용, 온라인 수색의 목적물과 범위, 기간 등이 특정되어야 할 것이다.[76] 그런데 온라인 수색의 경우 대상자의 지배하에 있는 IT 시스템 내부의 정보를 모두 대상으로 할 수 있기 때문에 수색의 범위가 지나치게 넓어질 수 있으며 사실상 일반영장과 같이 기능할 수 있다는 비판이 있을 수 있다.[77] 이에 대해서는 가능한 범위 내에서 영장에 압수·수색 대상을 특정하고 수집된 정보의 보관, 비밀 준수, 범죄사실과 관련 없는 내용의 삭제 등 절차적 요건에 의하여 통제될 필요가 있다.

문제는 온라인 수색의 속성상 오프라인에서의 압수·수색과 달리 영장집행의 통지(형사소송법 제122조), 영장제시의무(헌법 제12조 제3항 및 형사소송법 제118조), 당사자의 참여권(형사소송법 제121조, 제219조 참조)을 준수할 수 없다는 점이다. 처분대상자가 그 집행을 모르는 상태에서 실시되는 온라인 수색은 처분대상자 등의 부재 및 거부 등으로 인해 현실적·물리적으로 영장을 제시할 수 없는 불가피한 상

---

74) 헌재 1997. 3. 27. 96헌바28등, 판례집 9-1, 313, 320; 헌재 2012. 6. 27. 2011헌가36, 판례집 24-1하, 703, 709.

75) 헌재 1997. 3. 27. 96헌바28등, 판례집 9-1, 313, 319-320; 헌재 2003. 12. 18. 2002헌마593, 판례집 15-2하, 637, 647; 헌재 2008. 1. 10. 2007헌마1468, 판례집 20-1상, 1, 35; 헌재 2012. 5. 31. 2010헌마672, 판례집 24-1하, 652, 656; 헌재 2012. 6. 27. 2011헌가36등, 판례집 24-1, 703, 709-710 등.

76) 김하열, 위의 책, 395쪽; 김종현a, 영장주의에 관한 헌법적 연구, 헌법이론과 실무 2019-A-1, 헌법재판연구원, 2019, 23-24쪽.

77) Orin S. Kerr, Searches and Seizures in a Digital World, Harvard Law Review Vol. 119, No. 2, Dec., 2005, pp. 565-566 참조.

황으로 인하여 불가능한 상황을 의미하는[78] 영장집행의 통지나 영장 제시의 예외사유에 해당한다고 보기는 어려운 것으로 생각된다. 따라서 영장 집행의 통지 및 영장제시의무가 헌법이 규정하는 영장주의의 본질적인 내용에 해당한다면, 온라인 수색은 헌법상 영장주의에 위배되는 것으로 허용되기 어렵다고 할 것이다.

영장주의는 법집행기관의 자의적인 권력행사, 특히 수사권의 행사에 의한 신체의 자유 등의 침해를 방지하고자 하는 제도라는 점에서 그 의의를 찾을 수 있다. 영장의 제시는 대상자가 강제처분의 적법성을 납득하도록 하고, 수사기관의 강제처분 남용을 심리적으로 견제하며, 대상자에게 각종 권리를 알려주고 불복신청의 기회를 보장하는 기능을 수행한다.[79] 이때, 영장의 제시나 영장 집행의 사전통지는 그 자체가 영장주의의 내용을 구성하는 것이라기보다는 영장주의 실현을 위한 수단의 하나라고 볼 수 있다.[80] 헌법재판소는 전자우편에 대한 압수수색 집행의 경우에도 급속을 요하는 때에는 사전통지를 생략할 수 있도록 한 형사소송법 제122조 단서의 위헌 여부가 문제된 사건에서, "압수수색의 사전통지나 집행 당시의 참여권의 보장은 압수수색에 있어 국민의 기본권을 보장하고 헌법상의 적법절차원칙의 실현을 위한 구체적인 방법의 하나일 뿐 헌법상 명문으로 규정된 권리는 아니"라고 설시하면서, 입법자는 압수·수색절차의 형성에 관하여 입법형성권을 가지므로, 사전통지의무와 그 예외를 정하는 것 역시 제반 사항을 고려하여 정할 수 있는 입법재량이 있다고 하였다.[81] 따라서 입법자는 적법절차원칙에 위배되지 않는 범위에서 온라인 수색의 특성을 감안한 영장 집행 절차를 마련할 수 있는 입법재량을 갖는다.[82]

그렇다면 온라인 수색을 할 때 사전영장발부, 일반영장금지원칙이 충족된다면 온라인 수색의 허용이 영장주의의 본질적 요소를 침해하는 것은 아니라고 할 수 있다.

---

78) 대법원 2015. 1. 22. 선고 2014도10978 판결 참조.

79) 문성도, 헌법상 영장 제시 조항의 문제점과 합리적 개헌방안, 경찰법연구 제16권 제1호, 한국경찰법학회, 2018, 52-53쪽.

80) 미국, 독일, 일본에서도 영장을 제시하여야 한다는 내용을 헌법에 규정하고 있지 않으며, 학계에서도 영장제시원칙의 예외를 인정하는 것이 불가피하다는 이유에서, "영장을 제시하여야 한다"는 현행 헌법의 문언보다 "영장이 있어야 한다" 내지 "영장에 의하여야 한다"는 개헌 방안을 제시하는 견해가 있다.(문성도, 위의 글, 60-62쪽). 이상의 내용은 김종현a, 위의 글, 25-26쪽 참조.

81) 헌재 2012. 12. 27. 2011헌바225, 판례집 24-2하, 467, 475.

82) "형성된 절차의 내용이 적법절차원칙에서 도출되는 절차적 요청을 무시하였는지 여부 또는 비례의 원칙이나 과잉금지원칙을 위반하여 합리성과 정당성을 상실하였는지 여부에 달려 있다."(헌재 2012. 12. 27. 2011헌바225, 판례집 24-2하, 467, 476)

그럼에도 불구하고 영장집행의 통지, 영장제시의무, 당사자 참여권 제한으로 인하여, 영장주의를 통한 적법절차원칙의 실현이 상당 부분 제한되는 것은 사실이다. 이는 아래에서 서술할 절차적 요건에 의하여 통제될 필요가 있다.

2. 기본권 제한을 최소화하기 위한 온라인 수색의 요건

(1) 온라인 수색 허용 요건

1) 대상범죄의 엄격한 제한

온라인 수색으로 인하여 침해되는 사생활의 비밀과 자유의 심각성을 고려할 때, 달성하고자 하는 공익은 매우 중대한 것이어야 한다. 이를 위하여 온라인 수색이 가능한 대상범죄는 가능한 한 엄격하게 제한될 필요가 있다. 적어도 통신비밀보호법상 통신제한조치의 대상이 되는 범죄(통비법 제5조 제1항 참조) 보다 더 좁혀서 허용할 필요가 있을 것이다.[83] 어떤 범죄에 대하여 온라인 수색을 허용할 것인지는 입법자의 재량에 속하지만, 기본권 제한을 고려한 범죄 구성요건 자체의 중대성뿐만 아니라 수사의 효율을 고려하여 대상범죄를 제한하여야 한다.

온라인 수색이 허용될 수 있는 범죄로는 그 범죄의 특성상 국가의 존립과 관련된 범죄나 은밀하게 조직적으로 이루어지는 범죄, 다수를 대상으로 하며 법익 침해의 정도도 매우 중대한 범죄, 사이버공간에서 은밀하게 이루어지는 중대한 범죄 등으로 한정하여 규정될 필요가 있다. 독일의 경우에 연방형사소송법상 온라인 수색 대상은 다른 수사기법보다 좁으며, 감청과 달리 예비·음모죄의 경우 허용되지 않는다는 점을 참고할 필요가 있다.[84]

---

83) 허황, 위의 글, 69쪽.

84) 소스통신감청을 규정하는 독일 연방형사소송법 제100a조와 온라인 수색을 규정하는 동법 제100b조의 요건을 비교하면 다음과 같다(밑줄은 필자).
제100a조 (1) 다음 각 호의 사항을 모두 충족하는 경우에는 대상자 모르게 통신의 감청과 녹음을 할 수 있다.
1. 제2항에 규정된 중대한 범죄를 정범 또는 공범으로서 저질렀다거나, 그 미수를 처벌하는 경우에는 실행에 착수했다거나 어떤 범행을 통해 이를 예비했다는 혐의가 일정한 사실에 의하여 인정되고,
(중략)
제100b조 (1) 다음 각 호의 사항을 모두 충족하는 경우에는 대상자 모르게 기술적 수단으로 대상자가 사용하는 정보기술 시스템에 침입하여 그로부터 데이터를 수집할 수 있다.
1. 제2항에 규정된 특히 중대한 범죄를 정범 또는 공범으로서 저질렀다거나, 그 미수를 처

2) 사안의 중대성

대상범죄를 제한하였다고 하여 그 범죄관련 사실이 발견되었다는 것만으로 온라인 수색을 허용하는 것을 정당화하기보다는, 온라인 수색을 허용하기 위해서는 대상범죄 관련 혐의가 상당 부분 인정되는 것뿐만 아니라 그 사안의 심각성이 명백하여 온라인 수색이 반드시 필요함을 소명하도록 하는 것이 바람직하다고 생각된다.

현재 우리 통신비밀보호법상 통신제한조치의 경우 "범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할 만한 충분한 이유가 있고, 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우"에 한하여 허가할 수 있다고 하고(제5조 제1항), 통신제한조치를 청구할 때에도 청구이유에 대한 소명자료를 첨부하도록 하고 있을 뿐(제6조 제4항), 개별 사안의 중대성에 관한 내용을 명시적으로 요구하고 있지는 않다.

이에 대하여, 독일 연방형사소송법에서는 온라인 수색을 위해서는 일정한 사실에 의하여 대상범죄에 대한 혐의가 인정될 뿐만 아니라, "그 범행이 개별 사안에서도 특히 중대하게 평가"될 것을 요한다(제100b조 제1항 제2호). 그리고 법원에 대하여 온라인 수색의 영장 발부를 요청할 때 혐의의 근거가 되는 사실 뿐만 아니라 온라인 수색 등 "조치의 필요성과 비례성에 관하여 중요한 고려사항"을 기재하도록 하고 있다(동법 제100e조 제4항)는 점이 참고가 될 수 있다.[85]

온라인 수색 영장을 신청할 때 그 사유를 상세히 기재하도록 하여 법관이 개별 사안의 심각성과 중대성을 고려하여 허가 여부를 판단할 수 있으나, 개별 사안의 중대성 요건을 명시하는 것은 온라인 수색이 일정한 중대범죄의 혐의가 있을 뿐 아니라 그 사안의 중대함이 인정되는 경우에만 허용되는 것이라는 점을 밝히는 의미가 있다.

3) 구체성(특정성)

우리 헌법은 일반영장이 금지됨을 명시하지 않지만,[86] 일반영장은 허용되지 않는

벌하는 사안에서 실행에 착수했다는 혐의가 일정한 사실에 근거하고,

85) 이는 비단 온라인 수색뿐만 아니라 통신 감청(제100a조) 및 주거 공간에 대한 감청(제100c조)의 경우에도 요구된다.

86) 미국 수정헌법 제4조에서는 "수색될 장소나 체포·압수될 사람 내지 물건을 특정하여 표시"할 것을 요하고, 일본 헌법 제33조 및 제35조 제1항에서는 각각 "이유가 되는 범죄를 명시한 영장", "수색할 장소나 압수할 물건을 명시한 영장"이라고 규정하여, 일반영장의

다고 해석된다.[87] 따라서 특정인이 범죄를 저질렀다거나 범죄의 증거가 발견되리라는 상당한 이유가 있을 때에만 영장이 발부될 것을 요한다.[88] 형사소송법 제114조에서는 압수·수색영장에 "피고인의 성명, 죄명, 압수할 물건, 수색할 장소·신체·물건, 영장 발부 연월일, 영장의 유효기간과 그 기간이 지나면 집행에 착수할 수 없으며 영장을 반환하여야 한다는 취지"를 기재하도록 하며, 통신비밀보호법 제6조 제6항에서는 법원이 발부하는 허가서에는 "통신제한조치의 종류·그 목적·대상·범위·기간 및 집행 장소와 방법을 특정하여 기재하여야 한다."라고 규정하고 있다.

온라인 수색의 경우에도 일반적인 압수·수색영장과 마찬가지로 대상자, 기간, 대상 IT 시스템, 온라인 수색이 필요한 이유 등을 명확하게 기재할 것을 요함은 물론이다. 그런데 온라인 수색의 특성상 물리적 범위로 압수·수색의 대상을 특정하는 형사소송법에 비하여 기본권 제한의 범위가 넓어질 수 있다. 온라인 수색은 해킹 프로그램 등을 사용하여 대상자의 IT 시스템 내부에 침입하는 방법을 사용하고, 그 시스템 내부에 있는 정보를 수집·저장하는 수사기법이므로, 영장에 해킹 프로그램의 설치에 관한 내용이 얼마나 구체적으로 적시되어야 하는지 문제될 수 있다. 극단적으로는 저장된 정보를 수집하는 단계에서는 범죄관련성이 있는 것만을 특정하기 어려울 수 있어, 영장에서 "대상 기기 안의 정보 일체"를 수집하는 것을 허용하게 된다면, 사실상 일반영장으로 해석될 수 있다는 우려도 충분히 제기될 수 있다.[89] 따라서 최소한 영장(허가서)에는 온라인 수색을 위하여 필요한 정보 및 혐의 범죄와의 관련성을 가능한 한 구체적으로 명시할 필요가 있다.

4) 보충성(최후수단성)

온라인 수색의 경우 대상자에 관한 방대한 정보가 수집될 수 있어 기본권 침해 가능성이 크다. 따라서 이는 다른 방법으로는 범죄의 수사가 불가능한 경우에 한하여 허용되어야 한다. 헌법재판소는 구 통신비밀보호법에서 검사 또는 사법경찰관은

금지를 헌법에서 명시하고 있다.

87) 김종현b, 영장신청권자에 관한 헌법적 연구, 법조 제68권 제4호, 법조협회, 2019, 23-24쪽 참조. 이 연구에서는 일반영장의 금지를 영장주의의 본질로 이해하고 있다. 반면, 일반영장 금지 원칙이 헌법상 영장주의에 내재된 원칙이라고 하면서도 영장주의의 본질에는 해당하지 않는다는 견해로, 황정인, 영장주의의 본질과 영장제도, 형사정책연구 제21권 제2호, 한국형사정책연구원, 2010, 215-216쪽.

88) 김종현b, 위의 글, 172쪽.

89) Orin S. Kerr, *supra note* 77, pp. 565-566.

수사에 필요한 경우 전기통신사업자에게 통신사실 확인자료의 열람이나 제출을 요청할 수 있도록 한 것이 청구인의 개인정보자기결정권과 통신의 자유를 침해한다고 하면서, "범죄수사가 어려운 경우(보충성)를 요건으로 추가하는 방안 등 수사에 지장을 초래하지 않으면서도 불특정 다수의 기본권을 덜 침해하는 수단이 존재하는 점을 고려"할 때 침해최소성 요건을 충족하지 아니하였다고 판단하였다.[90] 이 결정에 따라 현재 동법 제13조 제2항에서는 "수사를 위하여 통신사실확인자료 중 다음 각 호의 어느 하나에 해당하는 자료가 필요한 경우에는 다른 방법으로는 범죄의 실행을 저지하기 어렵거나 범인의 발견·확보 또는 증거의 수집·보전이 어려운 경우"에 통신사실확인자료를 요청할 수 있도록 개정되었다. 통신제한조치의 경우에도 역시 "...다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있다"고 하여 보충성 요건을 두고 있다(동법 제5조 제1항). 독일 연방형사소송법 제100b조 제1항 제3호에서도 역시 "사실관계의 조사 또는 범행혐의자 소재의 파악이 다른 방법으로는 본질적으로 어렵거나 가망이 없어 보이는 경우"[91]에만 온라인 수색을 실시할 수 있도록 하고 있다.

디지털 증거를 수집하는 방법 중에서도 대상 기기 자체 혹은 하드디스크를 물리적으로 압수·수색하는 경우에는 영장집행의 통지 및 영장의 사전 제시가 가능하므로 온라인 수색과 비교하여 적법절차원칙 제한의 정도가 낮다고 할 수 있다. 한편, 통신비밀보호법상의 감청, 위치정보수집, 통신사실 확인자료 제공 등은 온라인 수색과 비교하여 수집하는 정보가 상대적으로 덜 포괄적이다. 따라서 온라인 수색을 도입한다면, 어떤 수사기법으로도 대상범죄사실의 확인이나 범죄자의 소재 파악이 불가능한 경우에 한하여 허용되어야 할 것이다.

(2) 절차적 통제수단

1) 중립적이고 독립적인 법관의 판단

우리 헌법 제12조 제3항에서는 "체포·구속·압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다"고 규정

90) 헌재 2018. 6. 28. 2012헌마538, 판례집 30-1하, 596, 607.

91) 소스통신감청의 경우에는 사실관계의 조사나 피범행혐의자 소재의 파악이 다른 방법으로는 현저히 곤란하거나 성공할 가망이 없어 보이는 경우로 온라인 수색보다는 보충성을 약간 완화하여 규정하고 있다(제100a조 제1항 제3호).

하여 법관이 영장을 발부하도록 하고 있다. 형사소송법 제114조 제1항에서는 압수·수색을 할 때 이를 구체화하여 영장의 기재 사항 및 재판장이나 수명법관이 서명날인하여야 함을 명시하고 있다. 헌법재판소는 "영장주의의 본질은 강제처분을 함에 있어서는 중립적인 법관이 구체적 판단을 거쳐 발부한 영장에 의하여야만 한다는 데에 있다"고 하면서,[92] 이러한 영장주의는 사법권독립에 의하여 신분이 보장되는 법관의 사전적·사법적 억제를 통하여 수사기관의 강제적인 압수·수색을 방지하고 국민의 기본권을 보장하기 위한 것"이라고 설시한 바 있다.[93]

온라인 수색 역시 강제처분에 해당하므로 이를 실시하기 위한 법관의 허가가 필요하고, 그 허가는 영장의 발부로 이해하는 것이 타당함은 전술한 바와 같다. 영국의 예와 같이 사법부의 사전 판단 없이 행정부 내에서 이중의 동의 절차를 마련하여 온라인 수색 여부를 결정하는 입법례도 있으나, 우리 헌법 및 형사소송법상의 영장제도의 내용이 온라인 수색에도 적용된다고 이해하는 한, 법관의 허가는 반드시 필요하다고 생각된다.

법관은 온라인 수색을 허가함에 있어 우선 대상범죄에 해당하는지, 그 사안이 중대한지, 다른 방법으로는 수사가 불가한지를 검토하여야 한다. 그리고 통신제한조치를 위헌 허가절차에 준하여 온라인 수색의 경우에도 기간, 집행방법 등이 기재될 것이 요구되는바, 영장에 기재된 온라인 수색 대상자 및 대상 기기가 특정되어 있고, 대상 기기에 침입하기 위하여 어떤 프로그램을 사용하는지, 영장에 기재된 기간은 적당한지, 여러 사람이 함께 사용하는 기기를 대상으로 하는 경우 대상자에 관한 정보만 수집·저장할 수 있는 방법이 있는지 등을 종합적으로 고려하여 허가 여부 및 그 범위를 결정하여야 한다.

2) 온라인 수색 집행에 대한 관리·감독

온라인 수색의 특성상 집행의 통지 및 영장의 사전 제시, 당사자 및 관계자 참여권이 보장될 수 없다. 따라서 온라인 수색이 영장에 기재된 대로 집행되는지 여부를 집행 중에 당사나 및 관계자가 알 수 없으므로, 별도의 관리·감독 절차를 마련할 필요가 증대된다.

감청의 경우를 참고해 보면, 인터넷회선 감청 사건 결정에서 헌법재판소는 집행

92) 헌재 2012. 5. 31. 2010헌마672, 판례집 24-1하, 652, 656.
93) 헌재 2004. 9. 23. 2002헌가17등, 판례집 16-2상, 379, 387-388.

과정에서나 집행이 종료된 이후의 제3자의 정보나 범죄수사 목적과 무관한 정보까지 수사기관에 의해 수집·보관되고 있지는 않는지, 감청 집행을 통해 수사기관에 광범위하게 취득된 자료를 수사기관이 원래 허가받은 목적, 범위 내에서 제대로 이용·처리하는지 등을 감독 내지 통제할 법적 장치가 강하게 요구됨에도 이를 관리 감독할 기관이 없으므로 침해의 최소성에 반한다고 보았다.[94] 이 결정에 따라 통신비밀보호법 제12조의2를 신설하여, 수집된 전기통신의 사용이나 사용을 위해 보관하고자 할 때에는 검사가 집행종료일로부터 14일 이내 필요한 전기통신을 선별하여 법원의 승인을 청구하여야 하고(사법경찰관이 감청한 경우에는 14일 이내 검사에게 신청하고, 검사는 7일 이내 허가 법원에 승인 청구), 이 청구를 위하여 소명자료, 보관 등이 필요한 전기통신 목록을 첨부하여 통신제한조치의 집행 경위, 취득한 결과의 요지, 보관 등이 필요한 이유를 기재한 서면으로 하여야 한다고 규정하고 있다.

온라인 수색의 경우에도 감청과 마찬가지로 집행에 대한 관리·감독은 사법기관(법원)에서 하는 것이 적절하다고 생각된다. 영장에 기재된 대로 온라인 수색이 집행되었는지, 수집된 정보는 범죄수사 관련 목적으로만 사용되었는지, 관련 없는 정보가 즉시 삭제되었는지, 감시 프로그램은 대상 기기에서 효과적으로 제거하여 원상 복구시켰는지를 법원이 확인할 필요가 있고, 수사목적의 달성 후 관련 정보의 처리(즉시 삭제 혹은 일정 기간 후 삭제)에 관한 내용은 수사기관이 법원에 보고하고 기록에 남겨 둘 필요가 있다.

3) 대상자에 대한 통지 및 불복절차

온라인 수색에 관한 사후통제절차로 대상자(및 관련 제3자)에 대한 통지 및 위법한 수색에 대한 불복절차를 들 수 있다. 헌법재판소는 수사기관 등에 의한 통신자료 제공요청 사건에서, "당사자에 대한 통지는 당사자가 기본권 제한 사실을 확인하고 그 정당성 여부를 다툴 수 있는 전제조건이 된다는 점에서 매우 중요하다. 따라서 수사나 정보수집 등의 활동에 신속성, 밀행성 확보가 필요하다고 하여 그러한 이유만으로 헌법상의 절차적 요청을 외면하는 것은 허용되지 않는다"고 설시하여, 당사자에 대한 통지의 중요성을 강조한 바 있다.[95] 또한, 불복절차의 의미에 관해서도

94) 헌재 2018. 8. 30. 2016헌마263, 판례집 30-2, 481, 503. 정인경, 통신제한조치 허가 위헌 확인 등, 결정해설집 17집, 헌법재판소, 2019, 702쪽.

95) 헌재 2022. 7. 21. 2016헌마388 등, 공보 제310호, 1037, 1049.

인터넷회선 감청 위헌확인 사건에서 “수사기관의 권한 남용을 방지하고 이로 인한 관련 기본권 침해를 최소화하기 위하여, 집행 과정에서나 집행이 종료된 이후에라도 제3자의 정보나 범죄수사 목적과 무관한 정보까지 수사기관에 의해 수집·보관되고 있지는 않는지, 감청 집행을 통해 수사기관에 광범위하게 취득된 자료를 수사기관이 원래 허가받은 목적, 범위 내에서 제대로 이용·처리하는지 등을 감독 내지 통제할 법적 장치가 강하게 요구된다”고 설시하였다.[96]

온라인 수색은 밀행성을 특징으로 하여 영장주의에서 요청되는 사전 통지 및 영장 제시가 불가능하다는 특징이 있으므로, 당사자에 대한 사후 통지 및 불복절차가 갖는 의의는 매우 크다. 온라인 수색이 종료된 후 당사자 및 관련 있는 제3자에 대하여 온라인 수색이 이루어졌음을 통지할 필요가 있다. 통지 내용으로는 온라인 수색이 이루어진 사실, 기간, 사유 등이 포함되어야 하며, 수색을 위한 감시 프로그램이 삭제되어 대상 기기의 기능이 원상회복되었고 수집한 자료 중 온라인 수색과 관련 없는 내용은 즉시 삭제된다는 내용, 그리고 위법한 온라인 수색에 대해서는 불복절차를 밟을 수 있다는 내용 등을 포함할 수 있다. 통지는 원칙적으로 수색이 종료된 후 지체 없이 이루어지는 것이 바람직하나, 온라인 수색이 가능한 대상범죄의 특성상 부득이한 경우 일정한 요건 하에 법원의 허가를 얻어 통제를 유예하는 예외사유를 둘 수 있도록 하는 방법을 고려할 수 있다.

형사소송법상 압수·수색 절차에서는 불복절차로 준항고 등의 제도가 마련되어 있는데, 일반적인 압수·수색보다 기본권 침해 우려가 더 높은 온라인 수색의 경우에도 사후 불복 제도를 마련하는 것이 타당하다. 그 전제로 처분대상자에게 온라인 수색의 실시 및 그 사유, 기간, 내용 등을 통지하여야 함은 전술한 바와 같다.

V. 맺음말

우리의 생활은 이제 과거와 비교할 수 없을 정도로 IT 기술에 의존하고 있다. 사이버공간은 일정한 정보의 저장과 활용을 위한 용도를 넘어서 현실 세계가 확장된 공간이라고 볼 수 있을 정도이다. 한편으로 정보통신망을 이용한 범죄의 수법은 나

96) 헌재 2018. 8. 30. 2016헌마263, 판례집 30-2, 481, 500.

날이 진화하고 있고, 익명성이 극대화된 다크웹 등을 이용한 범죄는 국경을 넘어 광범위하게 발생하는 사례가 많고 그 해악이 매우 심대하며 기존의 수사방법으로 검거하기가 매우 어렵다. 이러한 상황에서 과거에 감청이나 위치정보추적 등이 그랬던 것처럼, 우리의 생활방식과 환경의 변화를 반영하는 새로운 수사기법으로 온라인 수색의 도입 여부와 허용 요건을 진지하게 고려해 볼 시점이다.

온라인 수색은 당사자가 모르는 사이에 해킹 프로그램 등을 이용하여 처분대상자의 정보시스템에 침입하여 디지털정보를 수집하는 것으로, 국가기관에 의한 기본권 제한의 정도가 현존하는 어떤 수사기법보다 중대하다. 우리나라에서 온라인 수색을 도입한다면, 현행 형사소송법이나 통신비밀보호법상 허용된다는 해석이 불가능하고, 그 요건과 절차를 규정하는 새로운 입법이 마련되어야 하고, 헌법상 기본권의 제한을 어떻게 완화할 것인지 여부를 고민해야 할 것이다.

해외에서는 과거 정보기관이 테러방지 등 범죄예방이나 정보수집의 목적에서 당사자가 알지 못하는 사이에 정보를 수집하는 방식의 활동이 있었음이 내부고발이나 언론 등을 통하여 알려졌지만, 그 활용 실태나 범위는 정확히 알려지지 않았다. 테러에 대한 대책 등으로 온라인 수색을 비롯한 첨단 수사기법이 기본권 침해의 위험성에도 불구하고 입법화되는 과정을 거쳤고, 최근 몇몇 국가에서는 입법화되기에 이르렀다.

온라인 수색을 통해 IT 시스템 안의 정보를 망라하여 수집할 수 있다는 점을 감안하면, 한 개인에 관한 내용을 낱낱이 들여다보는 것이 기술적으로는 불가능하지 않고, 이는 사생활의 비밀과 자유를 비롯하여 개인정보자기결정권, 통신의 비밀과 자유 등 헌법상 기본권을 중대하게 제한한다. 온라인 수색으로 인한 기본권 제한 정도가 현행법상 다른 어떤 수사기법보다 큰 만큼 그 요건 역시 엄격하게 규정될 필요가 있다.

【토론문】

“온라인 수색과 헌법상 기본권의 보호”에 대한 토론문

김 해 원*

토론의 기회를 주신 한국헌법학회와 헌법재판소 헌법재판연구원, 그리고 무엇보다도 옥고를 통해서 새로운 고민과 공부의 계기를 마련해주신 소은영 연구관님께 특별히 감사드린다. 아울러 토론에 앞서서 본 토론자는 학술대회의 대주제는 물론이고 본 발표의 주제(“온라인 수색과 헌법상 기본권의 보호”) 또한 변화무쌍한 헌법현실에서 반드시 점검되어야 할 중요한 학문적 쟁점임을 인지하고 있었음에도, 관련 공부와 관심을 등한시해온 게으른 연구자임을 고백할 수밖에 없다. 이러한 고백의 일환일 수밖에 없는 본 토론의 부족함에 대해서 미리 양해 말씀을 드린다.

토론자로서 발표자의 문제의식을 확인하고 발표문을 읽으면서 갖게 된 몇 가지 의문들을 여쭙고 관련해서 갖게 된 나름의 ‘문제 해결’이 아닌, ‘문제 해결의 방향’을 조심스럽게 밝히고자 한다. 이에 대한 소은영 연구관님의 보완설명과 평가를 통해서 제 게으름을 성찰할 수 있기를 그리고 관련 논의들이 더 풍부해질 수 있기를 기대하는 것으로 토론자의 역할을 갈음하고자 한다.

(1) 발표자께서는 온라인 수색을 “국가가 정보통신망에 연결되어 있는 대상자의 IT 시스템에 대상자 모르게 접근하여 그 안에 있는 정보를 수집하는 행위”로 정의하면서(5쪽), “ 정보통신망을 이용한 범죄의 수법은 나날이 진화하고 있고, 익명성이 극대화된 다크웹 등을 이용한 범죄는 국경을 넘어 광범위하게 발생하는 사례가 많고 그 해악이 매우 심대하며 기존의 수사방법으로 검거하기가 매우 어렵다”는 헌법현실에 대한 인식을 바탕으로(28쪽) “새로운 수사기법으로 온라인 수색의 도입 여부와 허용 요건을 진지하게 고려해 볼 시점”이라고 하면서도(28쪽) “온라인 수색은

* 부산대학교 법학전문대학원 교수

[…] 국가기관에 의한 기본권 제한의 정도가 현존하는 어떤 수사기법보다 중대하다”는 점을 지적하고 있다(28쪽). 그리고 발표자는 “우리나라에서 온라인 수색을 도입한다면, 현행 형사소송법이나 통신비밀보호법상 허용된다는 해석이 불가능” 함을 논증한 후(6-8쪽, 28쪽), 온라인 수색의 “요건과 절차를 규정하는 새로운 입법이 마련되어야” 함을 주장함과 동시에 온라인 수색으로 인한 기본권침해문제를 어떻게 해결할 수 있을 것인지를 과제로 밝힌 후(28쪽), 특히 사생활의 비밀과 자유, 재인정보자기결정권, 통신의 비밀과 자유 등과 같은 기본권을 언급하면서(15-17쪽, 28쪽), “온라인 수색으로 인한 기본권 제한 정도가 현행법상 다른 어떤 수사기법보다 큰 만큼 그 요건 역시 엄격하게 규정될 필요가 있다”는 것으로 발표문을 갈무리하고 있다(28쪽).

(2) 이러한 발표자의 문제의식에 대해서 본 토론자 또한 대부분 공감한다. 다만 관련해서 ‘온라인 수색’ 그 자체에 관한 이해가 부족한 토론자로서 발표자께 다음과 같은 점을 여쭙고 싶다: ① 우선 발표자께서는 “영장의 제시나 영장 집행의 사전통지는 그 자체가 영장주의의 내용을 구성하는 것이라기보다는 영장주의 실현을 위한 수단의 하나라고 볼 수 있다”라고 하면서 “‘영장을 제시하여야 한다’는 현행 헌법의 문언보다 ‘영장이 있어야 한다’ 내지 ‘영장에 의하여야 한다’는 개헌 방안을 제시하는 견해”를 언급하면서(21쪽 주 80) “온라인 수색을 할 때 사전영장발부, 일반영장금지원칙이 충족된다면 온라인 수색의 허용이 영장주의의 본질적 요소를 침해하는 것은 아니라고 할 수 있다”라는 입장을 피력하고 있다(21-22쪽). 그렇다면 “[…] 수색을 할 때에는 […] 영장을 제시하여야 한다”라고 규정하고 있는 헌법 제12조 제3항이 개정되기 전에는, 소위 온라인 수색 전 영장을 제시하지 않고 행해지는 온라인 수색은 현행 헌법상 용납될 수 없다는 입장인 것인지 궁금하다. 만약 그렇다면, 현행 헌법질서 하에서 온라인 수색을 통한 수사의 목적 달성을 애당초 불가능한 것으로 생각되기 때문이다.[1] 그리고 ② 발표자께서는 독일의 연방형사소송법 규정(제100d조 제3항)의 “온라인 수색을 할 때 ‘가능한 한 사생활의 핵심영역과 관련되는 데이터는 수집되지 않는 것이 기술적으로 확보되어야 한다.”는 점을 소개하고 있다

1) 발표문 5쪽: “온라인 수색은 기술적으로 ①대상자와 대상 기기 탐색, ②대상자가 모르는 사이에 대상 기기에 대한 접근 실행, ③대상 기기로부터의 정보 수집이라는 3단계로 이루어진다.”

(12쪽). 그런데 온라인 수색에 있어서 '가능한 한 사생활의 핵심영역과 관련되는 데이터는 수집되지 않는 것이 기술적으로 확보'하는 것이 현 과학기술상 가능한 것인지 여쭙고 싶습니다. 왜냐하면 특정 데이터가 사생활의 핵심영역과 관련되는 것인지 여부는 일단 소위 온라인 수색 과정을 거쳐서 데이터를 수집한 후 알 수 있는 문제라는 생각이 들기 때문입니다. 만약 그렇다면 해당 규정을 단순한 주의적 규정으로 치부할 것이 아니라면, 해당 규정은 애당초 불가능한 것을 요구한 것으로서 법치주의원칙상 그 효력을 인정치 않거나 혹은 해당 요건충족불가능으로 인한 온라인수색 금지로 해당 규정을 이해해야 하는 것 아닌가하는 의문이 들기 때문이다. ③ 나아가 발표자께서는 "일반영장은 허용되지 않는다고 해석된다"고 하시면서, "'대상 기기 안의 정보 일체'를 수집하는 것을 허용하게 된다면, 사실상 일반영장으로 해석될 수 있다는 우려"를 밝히고 있다. 관련해서 대상 기기를 구체적으로 특정하고 대상 기기에 대한 접근기간을 구체적으로 정한 영장이라면 적어도 '수색'과 관련해서는 일반영장위반여부에 대한 의심은 벗어날 수 있는 것 아닌가하는 의문이 든다. 왜냐하면 대상 기기 안의 정보 일체를 수집하는 것이 '압수'에 해당하는지는 별론으로 하더라도, 적어도 수색은 수집 이전에 행해지는 행위로 생각되기 때문이다. 같은 맥락에서 온라인 수색을 위한 영장이 일반영장에 해당되지 않도록 하기 위한 해결방안으로 발표자께서는 "최소한 영장(허가서)에는 온라인 수색을 위하여 필요한 정보 및 혐의 범죄와의 관련성을 가능한 한 구체적으로 명시할 필요가 있다"는 점을 언급하고 있는데(23-24쪽), "온라인 수색을 위하여 필요한 정보 및 혐의 범죄와의 관련성"이 적시되었다고해서 그것이 일반적/포괄적 수색의 가능성을 통제할 수 있는지는 의문이다. 왜냐하면 수색과 관련한 일반영장에 대한 통제는 결국 수색에 대한 시간적/공간적 범위 특정을 통해서 달성될 수 있는 것으로 생각되기 때문이다.

(3) 범죄에 대한 대응 및 수사 목적달성에 유용한 '온라인 수색'을 헌법적합하게 도입하는 문제와 관련해서, 실천적 차원에서 특별히 주목해야 할 것은 어쩌면 온라인 수색으로 인해 훼손될 우려가 있는 기본권들이 무엇인지에 관한 문제의식(즉 기본권보호영역에 관한 문제)보다는 '온라인 수색'이 기본권심사기준(특히 법률유보원칙, 적법절차원칙이나 영장주의, 비례성원칙 등)을 통과할 수 있는지에 관한 문제의식일 수 있다. 아마도 발표자께서도 이러한 문제의식의 일환으로서 우선 형사소송법이나 통신비밀보호법상의 규정들을 검토하면서 온라인 수색의 법률적 근거를 확인

하려는 시도를 한 것으로 보이고, 이러한 확인을 통해서 현재 상황에서는 소위 온라인 수색은 법률유보원칙을 준수하지 못한 기본권침해로 평가할 수밖에 없음을 밝힌 것으로 생각된다. 본 토론자도 이러한 이해에 동의가 된다.

다만 영장주의 위반여부와 관련해서는 개헌을 통한 문제 해결을 지향할 것이 아니라면, 헌법 제12조 제3항의 "영장을 제시하여야 한다"의 의미를 상대화하기보다는, 헌법정립권자의 의사에 기초해서(특히 오프라인과 분별되는 온라인 환경의 특수성 및 온라인 연결의 의미에 대한 검토에 기초해서) 헌법 제12조 제3항의 "수색"의 개념을 축소하거나 혹은 '적법절차원칙(특히 헌법 제12조 제3항 "적법한 절차에 따라")을 통한 사전영장주의의 통제'를 해결 방법으로 모색하는 것(즉 헌법 제12조 제3황 영장주의의 적용범위에 대한 통제)이 헌법 해석적 차원에서는 더 설득력을 얻을 수 있을 것으로 생각된다. 그리고 발표자께서 밝힌 온라인 수색 허용요건 중 대상범죄의 엄격한 제한·사안의 중대성·구체성·최수수단성(보충성) 등은 상당부분 헌법 제37조 제2항 "필요한 경우에 한하여"의 준수여부(비례성원칙 위반여부)를 통과하기위한 요소로 생각된다. 관련해서 온라인 수색은 정보통신망에 "연결되어 있는 대상자의 IT시스템"을 대상으로 한다는 점에서, 연결의 강도 및 접속의 상황 또한 함께 고려될 필요가 있으리라고 본다. 또 발가벗겨 전시되고 있는 경우와 함께 발가벗고 목욕탕에 앉아 있는 경우는 다르다는 점에서, 온라인 수색하는 공권력을 사후에라도 발가벗겨 전시할 수 있는 조치(예컨대 누가 어떤 이유로 그러한 온라인 수색을 결정했고, 또 누가 구체적으로 그 결정에 따라 온라인 수색을 어떻게 행했으며 그러한 온라인 수색에 대한 감독기관의 공식적 평가나 입장은 무엇인지를 사후에라도 구체적으로 밝혀 드러낼 수 있도록 하는 조치)들의 사전 구비 또한 검토될 필요가 있을 것이며, 만약 온라인 수색에도 불구하고 불기소처분을 받거나 무죄판결을 받은 때에는 헌법 제28조의 취지를 고려하여 국가에 정당한 보상을 청구할 수 있는 법률의 정립 또한 적극 검토될 필요가 있으리라고 본다. 이러한 제도가 구비되어 있는 헌법현실에서 행해지는 온라인 수색과 그렇지 않은 경우의 온라인 수색에 대한 기본권적 판단은 달라질 수 있을 것이기 때문이다.

【토론문】

“온라인 수색과 헌법상 기본권의 보호”에 대한 토론문

차 원 일*

온라인 수색 도입이 활발하게 논의되는 시점에서 다양한 쟁점들을 조망할 수 있는 계기를 제공해주신 발제자와 이 연구에 대해 지정토론을 할 수 있는 기회에 깊이 감사드립니다.

온라인 수색은 그 밀행성, 수집되는 정보의 광범성 등 기존의 비밀수사가 가지는 기본권 침해 태양의 특수성을 공유할 뿐 아니라, IT 시스템에 직접 접속한다는 점에서 정보자기결정권, 통신의 비밀, 사생활의 비밀과 자유 등에 대한 중첩적이면서 중대한 기본권 제한을 수반합니다. 온라인 수색은 그 성격상 정보주체가 인지할 수 없고 이로 인해 적시에 침해적 행위를 방어할 수 없기 때문에, 당사자는 일방적으로 불리한 지위에 놓이게 됩니다. 이는 법치주의의 관점에서 투명성 확보와 통제의 측면에 배치될 뿐 아니라 IT 시스템에 대한 국민들의 일반적 신뢰 나아가 인터넷 기반 소통의 양태에도 영향을 미칠 수 있습니다. 따라서 과잉금지원칙에 따른 실체적인 요건의 확립 뿐 아니라 이러한 불리한 지위를 시정 내지 보완할 수 있는 사전적·사후적인 제도상의 균형조치가 요구되며, 발제자께서 예로 들어주신 절차적 통제수단으로서의 법관유보, 온라인 수색 집행에 대한 별도의 관리·감독절차, 대상자에 대한 통지 및 불복절차 등이 이에 해당한다고 볼 수 있습니다.

먼저 위와 같은 절차적 통제수단의 이론적 근거 구성에 대해 질문을 드리고 싶습니다. 독일의 경우 적법한 절차에 대한 요청은 기본권의 객관적 성격, 이른바 절차와 조직을 통한 기본권보장 법리에 의해 발전되었습니다. 개인정보자기결정권과 관련하여, 1983년 인구조사판결에서 절차적·조직적 보호조치로서의 설명의무, 정보제공의무, 삭제의무 및 독립된 정보보호담당관의 참여 등을 그 본질적 내용으로 언급

* 헌법재판소 헌법연구원

하고 있습니다.[1] 연방헌법재판소는 2009년 통신데이터저장판결에서[2] 정보보안에 대한 상세한 절차적 입법적 요청을 과잉금지원칙에서 도출하고 있고, 이러한 입장은 발제자께서 소개하신 연방범죄수사청법에 대한 헌법불합치 판결 및 비교적 최근의 바이에른 헌법보호법에 대한 일부위헌 판결에서[3] 다시 확인되었습니다.

절차적 통제수단은 일견 적법절차원칙의 내용으로 볼 수 있습니다. 우리 헌법재판소는 "적법절차원칙에서 도출할 수 있는 가장 중요한 절차적 요청 중의 하나로, 당사자에게 적절한 고지를 행할 것, 당사자에게 의견 및 자료 제출의 기회를 부여할 것을 들 수 있으나, 이 원칙이 구체적으로 어떠한 절차를 어느 정도로 요구하는지는 일률적으로 말하기 어렵고, 규율되는 사항의 성질, 관련 당사자의 사익, 절차의 이행으로 제고될 가치, 국가작용의 효율성, 절차에 소요되는 비용, 불복의 기회, 우리 사회의 법현실 등 다양한 요소들을 형량하여 개별적으로 판단할 수밖에 없다."[4]고 설시하고 있으며, 이에 따라 적법절차원칙에서 구체적으로 도출될 수 있는 절차적 통제수단의 종류 내지 범위는 확정되기 어렵다고 볼 수 있습니다. 최근 수사기관 등에 의한 통신자료 제공요청 사건에서는 통신자료 제공으로 인한 광범위하고 포괄적인 개인정보 제한에 대하여는 과잉금지원칙 위배 여부에서, 통신자료 제공 이후의 통지절차 미비에 대하여는 적법절차원칙 위배 여부에서 판단하였는데,[5] 발제자께서 사후통지제도는 별론으로 하더라도 그 외의 사전적·사후적 통제의 헌법적 근거를 어떻게 판단하시는지에 대해서 의견을 청해 듣고 싶습니다.

온라인 수색과 관련된 핵심적인 쟁점 중 하나가 결국 형사소추의 이익을 실현하면서도 가장 내밀한 정보에 대한 보호를 어떻게 담보할지에 관한 부분일 것입니다. 설명해주신 바와 같이, 독일은 사생활의 핵심영역에 속하는 정보의 수집 금지라는 절대적인 기본권 제한의 한계를 설정하고 있습니다. 예컨대 감청의 경우 연방헌법재판소가 가장 내밀한 공간의 감청에 대해서 정당화 요건을 엄격하게 적용하고, 핵심영역정보가 수집될 경우 감청을 즉각적으로 중지하고 정보의 사후적 이용금지 및 폐기를 통해 이를 달성하고자 하였다면, 온라인 수색에 의할 경우 그 특징상 핵심영

---

1) BVerfGE 65, 1, 46.
2) BVerfGE 125, 260.
3) BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17.
4) 헌재 2018. 6. 28. 2012헌마191등, 판례집 30-1하, 564, 591.
5) 헌재 2022. 7. 21. 2016헌마388등, 판례집 34-2, 122, 140.

역정보의 수집을 피하는 것이 한층 어려울 것 같습니다. IT 시스템에 접속한 이상, 정보를 특정하여 수집할 수 있는 기술적인 방안이 존재하는지에 대한 설명을 듣고 싶습니다. 또한 수집된 정보의 이용과 관련하여, 앞서 언급한 바이에른 헌법보호법에 관한 작년 연방헌법재판소 판결에서 재판부는 수집된 정보의 분류를 위한 독립된 외부 기관을 두지 않은 점을 문제 삼았고, 변론과정에서 헌법수호청과 연방내무부 측이 외부 통제에 따른 기밀성 유지의 어려움을 들기도 하였는데, 우리의 경우 수집되는 정보의 분류를 위한 독립된 외부 기관을 둔다면, 이를 어떻게 구상할 수 있을지가 궁금합니다.

마지막으로 절차적 통제수단의 실효적 형성에 관한 질문을 드리고 싶습니다. 어떠한 절차 내지 제도를 형성하는 의무는 현존하는 사실상의 상황에 비추어 보아 결국 실현가능한 합리적 범위 내에서 그 한계성이 있다고 볼 수 있겠습니다.[6] 예컨대, 학계와 실무에서 통신제한조치 허가신청, 통신사실 확인자료 제공요청 허가신청 등에 대한 법원의 영장기각률을 실효성 측면 또는 법원의 업무부담 등 다양한 관점에서 조망하고 있는데, 연구를 진행하시면서 온라인 수색이 도입될 경우 법원의 실질적 심사를 구현할 수 있는 방안에 대한 의견이 궁금합니다.

6) 전광석, 한국헌법론, 집현재, 2023, 249면.

【제2주제】

과학기술의 발전에 따른 형사절차상 변화와 헌법적 쟁점

윤 지 영*

Ⅰ. 서 론

2050년대 미국 워싱턴을 배경으로 제작된 영화 「마이너리티 리포트(Minority Report)」에서는 예지자의 뇌에 첨단장치를 부착하여 범죄가 일어날 장소와 일시 및 범죄자를 예측하여 사전에 범죄 발생을 막는 '프리크라임 시스템(Precrime System)'이 등장한다. 2002년 개봉되었던 이 영화가 아직까지 호평을 받는 것은 '인간의 자유의지'라는 묵직한 주제와 탄탄한 구성에 기인한 측면이 크나, 영화 속에서 미래사회를 그리면서 등장했던 상상 속의 산물들이 현실에서 구현되면서 종종 회자되고 있다. IT 기술의 발전으로 인해 방대한 양의 정보들이 끊임없이 생성되고 있고, 인공지능 기술을 활용한 빅데이터 분석을 통해 보다 신뢰할 수 있는 미래 예측이 가능해지고 있다. 또한 영화가 제작된 시점으로부터 반세기 가량이나 지나서야 상용화될 것으로 그려진 홍채인식로봇이나 무인자동차 등은 이제 더 이상 상상 속의 산물이 아니다.

* 한국형사·법무정책연구원 선임연구위원

과학기술의 발전은 형사사법 분야에 다각적인 영향을 미친다. 우선 신기술을 이용한 법익침해가 문제되는데, 형사적 처벌이 필요한 경우 그 법적 공백을 최소화하며 범죄구성요건을 정비해야 할 필요성이 대두된다. 또한 처벌 규정이 존재함에도 불구하고 종래의 수사 및 재판방식으로 대응하는 것에 한계가 있는 경우에는 새로운 제도의 도입이 모색되기도 한다. 나아가 과학기술은 수사나 재판의 효율성 제고를 위해서도 활용될 수 있는데, 그 과정에서 기본권 침해 문제가 불거지기도 한다. 본 발표는 과학기술의 발전에 따른 형사절차의 변화와 이와 관련된 헌법적 쟁점에 대해 논하고자 한다. 이에 과학기술의 발전이 형사절차에 미친 영향들을 조망하고, 암호화·익명화 기술이나 자율주행기술과 같은 첨단기술이 상용화됨에 따라 형사절차에 어떤 변화가 요구되고 있는지를 검토하고자 한다. 한편 인공지능과 드론, 로봇기술, 사물인터넷, 확장현실 등의 첨단기술을 형사절차상 활용하는 과정에서 제기되는 헌법적 쟁점에 대해서도 살펴보고자 한다.

Ⅱ. 헌법적 형사절차와 과학기술

1. 헌법적 형사절차

형사절차를 통해 국가형벌권을 실현하는 과정에서는 필연적으로 기본권에 대한 제한이 수반된다. 기본권의 제한은 국회가 제정한 성문의 법률에 의해야 하는바, 형사절차의 법률유보를 두고 '형사절차법정주의'라 한다. 형사절차법은 형법의 적용이라는 공익과 개인의 자유라는 이익이 첨예하게 충돌하는 법률체계다. 이에 헌법은 국가형벌권 실현 과정에서 개인의 자유와 권리를 보호하기 위해 법률주의와 적법절차원칙, 고문금지와 불이익진술거부권, 영장주의, 변호인의 조력을 받을 권리, 체포·구속적부심사청구권, 자백배제법칙과 자백의 보강법칙, 일사부재리의 원칙, 신속한 공개재판을 받을 권리, 피고인의 무죄추정, 형사보상청구권 등을 규정하고 있다.

형사사법제도는 헌법에 합치하도록 운용되어야 하고, 피의자와 피고인의 헌법상 권리를 보장해야 하는데, 이를 두고 '헌법적 형사소송' 또는 '헌법적 형사절차'라고 한다. 헌법적 형사소송이란 형사소송법이 헌법이념을 구체화한 법이라는 것을 의미할 뿐만 아니라 법률로 구체화되지 않은 헌법규범도 형사소송의 재판규범이 된다는

것을 말한다.[1] 또한 헌법적 형사소송의 기본이념은 적법절차의 원리로 이해되는데, 이는 "법률이 정한 형식적 절차와 실체적 내용이 모두 합리성과 정당성을 갖춘 적정한 것이어야 한다는 실질적 의미를 지니고 있는 것"으로서 형사소송절차 전반을 기본권 보장의 측면에서 규율해야 한다는 기본원리가 천명된 것이다.[2]

2. 과학기술의 발전이 형사절차에 미친 영향

(1) 강제수사의 판단 기준 변화

강제력의 행사 없이 상대방의 동의나 승낙을 받아서 이루어지는 임의수사와 달리 강제수사는 강제처분에 의해 이루어진다. 형사소송법상 임의수사가 원칙이고, 강제수사는 인권침해의 위험을 방지하기 위해 법률에 특별한 규정이 있는 경우에 한해 예외적으로 허용된다. 임의수사와 강제수사를 어떻게 구분할지가 문제되는데, 종래에는 물리적 강제력이나 법적 의무 부과 여부를 기준으로 판단되었다. 그러나 과학기술이 발전하면서 새로운 수사기법이 등장하였고, 이로 인한 개인의 프라이버시 침해가 문제되었는데, 그 대표적인 것이 사진촬영과 감청이다. 전통적인 강제처분인 체포·구속·압수·수색과 달리 사진촬영이나 감청은 그 대상자에게 물리적 강제력을 가하거나 법적 의무를 부과하지 않기 때문에 대상자가 수사의 착수 여부나 진행 상황을 알지 못한 상황에서 그 권리가 침해되거나 형사절차상 중대한 결과가 초래된다. 이에 임의수사와 강제수사의 구분 기준도 변하였는바, 오늘날 양자는 중요한 권리나 이익의 침해 여부를 기준으로 구분되고 있다.

초상권이 침해되는 사진촬영은 강제수사로 파악되어 영장주의가 적용되나, 일정한

---

1) 「우리 헌법은 변호인의 조력을 받을 권리가 불구속 피의자·피고인 모두에게 포괄적으로 인정되는지 여부에 관하여 명시적으로 규율하고 있지는 않지만, 불구속 피의자의 경우에도 변호인의 조력을 받을 권리는 우리 헌법에 나타난 법치국가원리, 적법절차원칙에서 인정되는 당연한 내용이고, 헌법 제12조 제4항도 이를 전제로 특히 신체구속을 당한 사람에 대하여 변호인의 조력을 받을 권리의 중요성을 강조하기 위하여 별도로 명시하고 있다. 피의자·피고인의 구속 여부를 불문하고 조언과 상담을 통하여 이루어지는 변호인의 조력자로서의 역할은 변호인선임권과 마찬가지로 변호인의 조력을 받을 권리의 내용 중 가장 핵심적인 것이고, 변호인과 상담하고 조언을 구할 권리는 변호인의 조력을 받을 권리의 내용 중 구체적인 입법형성이 필요한 다른 절차적 권리의 필수적인 전제요건으로서 변호인의 조력을 받을 권리 그 자체에서 바로 도출되는 것이다.」 헌법재판소 2004. 9. 23. 선고 2000헌마138 결정.

2) 헌법재판소 1996. 12. 26. 선고 94헌바1 결정.

요건 하에서는 영장 없는 사진촬영이 허용된다.[3] 영장 없이 무인장비를 이용하여 제한속도 위반 차량의 번호를 촬영하는 것도 임의수사로서 허용된다.[4] 전기통신 감청은 강제력을 행사하거나 상대방에게 의무를 부과하지는 않지만 개인의 프라이버시에 대한 중대한 침해를 가져온다는 점에서 그 법적 성격을 두고 임의수사설과 강제수사설이 대립하였다. 다만 이러한 논쟁은 1994년 「통신비밀보호법」이 제정되면서 일단락되었는데, 동법에서 감청은 법원의 허가를 받아 이루어지는 강제수사로 규정되고 있다.[5]

(2) 증거능력 인정 여부 논란

1) 거짓말탐지기 검사 결과

심리생리검사라고도 불리는 '거짓말탐지기(polygraph) 검사'는 과학수사와 인권이 충돌하는 대표적인 사례다. 독일의 통설은 기계로 인간심리를 검사하는 것은 인격권을 침해하는 것으로서 독일 형사소송법 제136조의a에 규정된 금지된 신문방법에 해당한다는 입장을 취하고 있고, 판례도 거짓말탐지기 검사는 피의자의 의사결정과 의사활동의 자유를 침해하는 것으로서 피검자의 동의 여부를 불문하고 허용되지 않는다고 판시하였다.[6] 우리나라의 경우 실무상 거짓말탐지기가 사용되고 있으나 그 검

---

3) ① 현재 범행이 행하여지고 있거나 행하여진 직후이고, ② 증거보전의 필요성 내지 긴급성이 있으며, ③ 촬영방법이 상당할 것을 요구하고 있다. 대법원 1999. 9. 3. 선고 99도2317 판결.

4) 「무인장비에 의한 제한속도 위반 차량 단속은 수사 활동의 일환으로서 도로에서의 위험을 방지하고 교통의 안전과 원활한 소통을 확보하기 위하여 도로교통법령에 따라 정해진 제한속도를 위반하여 차량을 주행하는 범죄가 현재 행하여지고 있고, 그 범죄의 성질·태양으로 보아 긴급하게 증거보전을 할 필요가 있는 상태에서 일반적으로 허용되는 한도를 넘지 않는 상당한 방법에 의한 것이라고 판단되므로, 이를 통하여 운전 차량의 차량번호 등을 촬영한 사진을 두고 위법하게 수집된 증거로서 증거능력이 없다고 말할 수 없다.」 대법원 1999. 12. 7. 선고 98도3329 판결.

5) 「감청은 현재 이루어지고 있는 전기통신의 내용을 대상으로 하고, 이미 수신이 완료된 전기통신 기록이나 내용은 압수나 수색영장에 의해 취득할 수 있다. 인터넷통신망을 통한 송·수신은 전기통신에 해당하므로 인터넷 통신망을 통해 흐르는 전기신호 형태의 패킷(packet)을 중간에 확보하여 그 내용을 지득하는, 이른바 '패킷(packet) 감청'도 허용된다. 이는 패킷 감청의 특성상 수사목적과 무관한 통신내용이나 제3자의 통신내용도 감청될 우려가 있다는 것만으로 달리 볼 것이 아니다.」 대법원 2012. 10. 11. 선고 2012도7455 판결.

6) BGHSt. 5, 332.

사결과의 증거능력 인정 여부를 두고는 견해가 대립한다.[7] 대법원은 피검자의 동의를 전제로 증거능력이 인정될 수 있는 까다로운 요건을 제시하며[8] 사실상 증거능력을 부정하고 있고, 설령 그러한 요건을 갖추어 증거능력이 인정되는 경우라고 하더라도 그 결과는 피검자의 신빙성을 가늠하는 정황증거로서 기능하는 데 그친다고 밝혔다.[9]

2) 영상녹화물

피의자나 참고인 및 피해자의 진술을 녹화한 영상물을 재생시키는 것도 과학적 증거방법 중 하나이다. 형사소송법은 피의자와 참고인 진술의 영상녹화제도를 인정하고 있는데(형사소송법 제221조 제2항, 제244조의2 제1항), 영상녹화물의 독립된 증거능력 인정 여부를 두고는 찬반양론이 대립한다. 실무상 영상녹화물은 녹화와 편집 과정에 조작의 위험이 있고, 수사과정에서 작성된 영상녹화물의 상영에 의해 법관의 심증이 좌우될 수 있다는 이유로 독립된 증거능력이 부정되고 있다. 현재 영상녹화물은 피의자신문조서와 참고인 진술조서의 진정성립을 인정하는 방법으로 활용되며(동법 제312조 제2항 제4항), 진술자의 기억이 불명확한 경우에 기억환기용으로

---

7) 인격침해나 신용성 결여를 이유로 증거능력을 부정하는 견해가 있는가 하면, 피검자의 동의나 적극적 요구를 요건으로 증거능력을 인정하는 견해도 있다.

8) 「거짓말탐지기의 검사 결과에 대하여 사실적 관련성을 가진 증거로서 증거능력을 인정할 수 있으려면, ① 거짓말을 하면 반드시 일정한 심리상태의 변동이 일어나고, ② 그 심리상태의 변동은 반드시 일정한 생리적 반응을 일으키며, ③ 그 생리적 반응에 의하여 피검사자의 말이 거짓인지 아닌지가 정확히 판정될 수 있다는 세 가지 전제요건이 충족되어야 할 것이며, ④ 특히 마지막 생리적 반응에 대한 거짓 여부 판정은 거짓말탐지기가 검사에 동의한 피검사자의 생리적 반응을 정확히 측정할 수 있는 장치이어야 하고, ⑤ 질문사항의 작성과 검사의 기술 및 방법이 합리적이어야 하며, ⑥ 검사자가 탐지기의 측정내용을 객관성 있고 정확하게 판독할 능력을 갖춘 경우라야만 그 정확성을 확보할 수 있는 것이므로, 이상과 같은 여러 가지 요건이 충족되지 않는 한 거짓말탐지기 검사 결과에 대하여 형사소송법상 증거능력을 부여할 수는 없다.」 대법원 2005. 5. 26. 선고 2005도130 판결.

9) 「거짓말탐지기의 검사는 그 기구의 성능, 조작기술 등에 있어 신뢰도가 극히 높다고 인정되고 그 검사자가 적격자이며, 검사를 받는 사람이 검사를 받음에 동의하였으며, 검사서가 검사자 자신이 실시한 검사의 방법, 경과 및 그 결과를 충실하게 기재하였다는 등의 전제조건이 증거에 의하여 확인되었을 경우에만 형사소송법 제313조 제2항에 의하여 이를 증거로 할 수 있는 것이고 위와 같은 조건이 모두 충족되어 증거능력이 있는 경우에도 그 검사결과는 검사를 받는 사람의 진술의 신빙성을 가늠하는 정황증거로서의 기능을 하는데 그치는 것이다.」 대법원 1987. 7. 21. 선고 87도968 판결.

사용될 수 있다(동법 제318조의2 제2항). 다만 일부 특별법은 영상녹화물의 독립적 증거능력을 인정하고 있었는데, 최근 헌법재판소는 영상물에 수록된 19세 미만 성폭력범죄 피해자 진술에 관한 증거능력을 인정한 「성폭력범죄의 처벌 및 피해자보호 등에 관한 법률」 규정이 원진술자에 대한 피고인의 반대신문권을 실질적으로 배제하여 피고인의 방어권을 과도하게 제한하는바, 과잉금지원칙에 반한다는 위헌결정을 내렸다.[10)]

(3) 신빙성 있는 증거 확보

과학기술의 발전은 DNA와 같은 신빙성 있는 증거를 확보할 수 있도록 한다. 1985년에 처음 발표된 DNA를 이용한 개인 식별은 과학 수사 및 재판 분야의 산업혁명에 비유될 만한 정도의 기술 혁신으로 평가되었다. 우리나라에서는 1986년 국립과학수사연구소가 DNA 분석기법을 도입한 후 성폭력 사건이나 강력범죄 사건의 범인을 식별하거나 대형재난이나 재해 발생 시 피해자의 신원확인을 위해 활용되었다. 1990년대에 들어서는 범죄현장의 인체유래물을 개별적으로 분석하는 기법의 한계[11)]가 지적되면서 DNA 데이터베이스화의 필요성이 제기되었다. DNA 데이터베이스 구축에 대한 치열한 찬반논쟁이 진행되던 가운데, 1994년 영국은 세계 최초로 유전자 정보 은행을 구축하기 위한 근거법을 마련하였다. 우리나라는 강력범죄를 저지른 사람의 DNA 신원확인정보를 미리 확보 및 관리하는 DNA 신원확인정보 데이터베이스 제도를 도입함으로써 강력범죄가 발생하였을 때 등록된 DNA 신원확인정보와의 비교를 통하여 신속히 범인을 특정·검거하고, 무고한 용의자를 수사선상에서 조기에 배제하며, 더 나아가 DNA 신원확인정보가 등록된 사람의 재범 방지 효과를 제고시키고자 2010년 1월 25일에 「디엔에이신원확인정보의 이용 및 보호에 관한 법률」이 제정되어 같은 해 7월 26일부터 시행되고 있다. DNA 분석은 높은 신뢰성을 가지는 보편적인 과학수사기법으로 자리 잡고 있으나, DNA 데이터베이스의 확장에

---

10) 헌법재판소 2021. 12. 23. 선고 2018헌바524 결정.

11) 종래의 방법이 효과적이기 위해서는 범인이 실제 그 지역에 거주하는 사람이어야 하고, 검체를 얻고자 하는 대상자의 동의를 얻지 못할 경우 이를 강제할 방법이 없으며, 투입되는 인력과 비용에 비해 그 검거율이 상대적으로 낮아서 비경제적이라는 비판이 제기되었다. Kenneth Jost, “DNA Database: Does expanding them threaten civil liberties?”, CQ Researcher Vol. 9 Issue 20, CQ Press, May 28, 1999, https://library.cqpress.com/cqresearcher/document.php? id=cqresrre1999052800 (2023년 5월 8일 최종검색).

대해서는 민감한 개인정보의 오남용 등 시민의 자유와 권리에 관한 침해 문제가 지적되고 있다.

(4) 증거확보 과정의 정교화

1) 전자정보

정보통신기술이 발전하고 디지털 기기의 사용이 일상화됨에 따라 형사절차상 실체적 진실을 발견하는 데 전자증거의 역할이 커졌다. 그러나 전자정보는 복제가 쉽고, 조작이나 변경 및 삭제 등이 용이하기 때문에 법정에서 유효한 증거로 인정받기 위해서는 어떠한 조작이나 흠결이 없었다는 사실이 입증되어야 한다. 또한 비가시성을 특징으로 하는 대량의 전자정보에는 혐의사실과 관련된 정보와 무관한 정보가 혼재되어 있어서 압수·수색 과정에서 이를 선별하고, 피압수자나 변호인에게 참여의 기회를 보장하는 것이 중요해졌다. 대법원은 참여권 보장 문제와 관련하여 '실질적 피압수자'[12]라는 개념을 사용하고 있는데, 최근 '카카오톡 사건'에서 제3자인 인터넷서비스업체가 보관하고 있는 전자정보의 압수·수색 과정에 실질적 피압수자인 피의자의 참여권을 보장하지 않은 것은 위법하다고 판단했다.[13]

2) 통신감청 및 통신사실 확인자료

통신감청이나 통신사실 확인자료 취득은 범죄를 밝혀내는 효율적인 수단이다. 다만 그로 인해 통신 및 대화의 비밀과 자유가 제한되는바, 「통신비밀보호법」을 통해 그 대상을 한정하고 엄격한 법적 절차를 거치도록 하고 있다. 동법은 헌법재판소의 헌법불합치 결정을 통해 개선되어왔는데, 종래 ① 통신제한조치기간의 연장을 허가함에 있어 총연장기간이나 총연장횟수의 제한을 두지 않았던 규정,[14] ② 수사가 장기간 진행되거나 기소중지결정이 있는 경우에는 정보주체에게 통신사실 확인자료 제공에 대한 통지 의무를 규정하지 않고, 그 외 통신사실 확인자료 제공을 통지할

12) 실질적 피압수자란 "압수·수색 당시 또는 이와 시간적으로 근접한 시기까지 해당 정보저장매체를 현실적으로 지배·관리하면서 그 정보저장매체 내 전자정보 전반에 관한 전속적인 관리처분권을 보유·행사하고, 달리 이를 자신의 의사에 따라 제3자에게 양도하거나 포기하지 않은 경우로서, 그 정보저장매체에 저장된 전자정보에 대하여 실질적인 압수·수색 당사자로 평가할 수 있는 사람"이다. 대법원 2022. 1. 27. 선고 2021도11170 판결.

13) 대법원 2022. 5. 31.자 2016모587 결정.

14) 헌법재판소 2010. 12. 28. 선고 2009헌가30 결정.

때에도 그 제공사유는 통지되지 않으며, 수사목적 달성 이후 해당 자료의 파기 여부를 확인할 수 없었던 규정,[15] ③ 인터넷회선 감청의 특성을 고려하여 수사기관의 권한 남용을 통제하고 관련 기본권의 침해를 최소화하기 위한 제도적 조치가 마련되어 있지 않은 상태에서, 범죄수사 목적을 이유로 한 인터넷회선 감청을 통신제한조치 허가 대상 중 하나로 정하고 있었던 규정[16] 등이 개선되었다.

2022년 7월 21일에는 전기통신사업자가 수사기관 등의 통신자료 제공요청에 따라 수사기관 등에 제공하는 이용자의 성명, 주민등록번호, 주소, 전화번호, 아이디, 가입일 또는 해지일 정보를 제공할 수 있도록 한 「전기통신사업법」 규정이 통신자료 취득에 대한 사후통지절차를 두지 않아 적법절차원칙에 위배된다는 헌법재판소의 결정이 있었다.[17] 이 사안에서 헌법재판소는 법적 공백을 방지하기 위해 헌법불합치 결정을 내리면서 늦어도 2023년 12월 31일까지 개선입법이 이루어져야 한다고 적시했다. 다만 이와 관련해서는 동 결정이 내려지기 전부터 입법논의가 전개되었는바, 전기통신사업자가 수사기관 등에 제공하는 정보는 통신 행위와는 직접 관련성이 없고, 「통신비밀보호법」상 '통신사실 확인자료'와 혼동될 우려가 있다는 점에서 '통신

---

15) 헌법재판소는 이 사건 통지조항이 적법절차원칙에 위배되어 청구인들의 개인정보자기결정권을 침해한다고 판단하였다. 헌법재판소 2018. 6. 28. 선고 2012헌마191 등 결정.

16) 헌법재판소는 패킷감청의 방식으로 이루어지는 인터넷회선 감청은 해당 인터넷회선을 통하여 흐르는 불특정 다수인의 정보가 패킷 형태로 수집되어 수사기관이 다른 통신제한조치와는 비교할 수 없을 수준의 방대한 자료를 취득하게 된다는 점에 주목하였다. 이에 대한 법적 통제수단이 미비한 상황에서 인터넷회선 감청을 허용하는 것은 개인의 통신 및 사생활의 비밀과 자유를 침해한다고 보았다. 헌법재판소 2018. 8. 30. 선고 2016헌마263 결정.

17) 이 사건 법률조항(전기통신사업법(2010. 3. 22. 법률 제10166호로 전부개정된 것) 제83조 제3항 중 '검사 또는 수사관서의 장(군 수사기관의 장 포함), 정보수사기관의 장의 수사, 형의 집행 또는 국가안전보장에 대한 위해 방지를 위한 정보수집을 위한 통신자료 제공요청'에 관한 부분)에 의한 통신자료 제공요청이 있는 경우 통신자료의 정보주체인 이용자에게는 통신자료 제공요청이 있었다는 점이 사전에 고지되지 아니하며, 전기통신사업자가 수사기관 등에게 통신자료를 제공한 경우에도 이러한 사실이 이용자에게 별도로 통지되지 않는다. 그런데 당사자에 대한 통지는 당사자가 기본권 제한 사실을 확인하고 그 정당성 여부를 다툴 수 있는 전제조건이 된다는 점에서 매우 중요하다. 효율적인 수사와 정보수집의 신속성, 밀행성 등의 필요성을 고려하여 사전에 정보주체인 이용자에게 그 내역을 통지하도록 하는 것이 적절하지 않다면 수사기관 등이 통신자료를 취득한 이후에 수사 등 정보수집의 목적에 방해가 되지 않는 범위 내에서 통신자료의 취득사실을 이용자에게 통지하는 것이 얼마든지 가능하다. 그럼에도 이 사건 법률조항은 통신자료 취득에 대한 사후통지절차를 두지 않아 적법절차원칙에 위배된다. 헌법재판소 2022. 7. 21. 선고 2016헌마388 등 결정.

자료'라는 용어를 '통신이용자정보'로 변경해야 할 필요성이 제기되었다. 또한 통신이용자정보제공 후 통지 제도의 신설도 논의되었는데, 이 경우 수사실무상 문제가 고려되어야 하며, 통지 주체와 통지 시한 등이 명시되어야 한다.

(5) 원격 수사·공판 진행 및 형사절차의 전자화

1) 원격영상시스템 활용

전자통신 및 인터넷 분야의 획기적인 기술 발전은 재판관계인이 직접 법정에 출석하지 않더라도 비대면 방식으로 각종 재판절차를 진행하는 것을 가능하게 만들었는데, 이는 재판관계인의 편의 증진과 재판 비용 절감 및 분쟁 해결의 효율성 제고 등의 장점이 있다. COVID-19 확산 시기였던 2021년 8월 17일에 개정된 「형사소송법」이 같은 해 11월 18일부터 시행되면서 영상재판의 대상이 획기적으로 확대되었다. 다만 민사재판[18]에 비해 형사재판의 경우에는 그 활용 범위나 이용 장치가 제한된다. 구속이유를 고지할 때나 공판준비기일, 증인신문, 감정인신문, 통역 등이 영상재판으로 진행될 수 있는데, 공판준비기일에만 인터넷 화상장치가 활용될 수 있고, 그 이외의 절차는 모두 비디오 등 중계장치에 의한 중계시설이 이용되어야 한다. 형사법정은 피고인의 유무죄를 가리는 엄숙한 장이고, 형사소송법상 직접주의 원칙이나 피고인의 방어권 보장 측면 등이 고려되어야 한다는 점에서 영상재판의 활용 범위가 제한적이다.[19] 또한 영상재판은 법원이 자체적으로 구축한 '원격영상재판 시스

---

18) 민사재판의 경우에는 변론기일, 변론준비기일, 심문기일, 증인신문, 당사자신문, 감정인신문, 통역 등에 인터넷 화상장치 또는 비디오 등 중계장치에 의한 중계시설이 폭넓게 활용될 수 있다.

19) 영상재판과 관련하여 형사절차상 출석이라는 개념을 어떻게 해석하고, 직접주의나 피고인의 방어권과의 관계를 어떻게 규명할 것인지에 관한 문제는 모두 밀접한 관련성을 가진다. 현행 형사소송법상 출석은 "보이거나 들리는 범위 내"가 아닌 "물리적 출석"을 의미하는 것으로 파악되고, 이는 용어의 근본적 의미와 일반적·상식적 이해에 부합한다. 형사소송법상 피고인이나 증인은 관련절차 진행을 위해 공판정에 출석해야 하는 것이 원칙이고 일정한 경우 그 예외가 인정되고 있을 뿐, "물리적 출석"이라는 출석의 개념 자체가 "보이거나 들리는 범위 내"로 확대된 것은 아니다. 또한 공판정에서 직접 조사한 증거만을 재판의 기초로 삼을 수 있는 직접주의와 피고인의 방어권과 관련해서는 원격영상시스템을 통해 얼마나 생동감 있게 현장에서와 같은 상황이 연출될 수 있는지에 관한 기술적 문제가 검토되어야 한다. 한편 형사절차상 원격영상시스템의 활용은 모든 절차관계인들이 매체를 통해 대면하여 구두로 진행되고, 사전에 녹화된 영상물을 방영하는 것이 아니라 실시간으로 생중계된다는 점에서, 직접주의의 원칙과 피고인의 방어권 보장에 친화적이다. 그러나 원격영상시스템이 이용되려면 동 시스템의 활용으로 인한 이익과 직접주의 또는 피고인의

템’에 접속하여 진행되는데, 형사재판의 경우 상대적으로 보안이 취약한 개인의 인터넷 화상장치 보다는 비디오 등 중계장치에 의한 중계시설을 이용하도록 하고 있다.

수사과정에서도 원격영상시스템이 활용될 수 있다. 2009년 「공직선거법」상 재외국민선거제도가 도입되면서 해외에서 선거범죄가 발생할 경우 사실상 법 집행의 사각지대가 될 수 있다는 우려가 제기됨에 따라, 2012년 「공직선거법」에 재외선거사범에 대한 인터넷화상조사 규정이 신설되었다. 증인의 보호 또는 수사의 효율성 제고를 통해 실체적 진실을 발견하고자 비디오 등 중계장치에 의한 증인신문제도와 재외선거사범에 대한 인터넷화상조사제도가 도입된 것이다. 비단 선거사범이 아니더라도 범죄혐의를 받고 있는 피의자나 참고인이 해외에 있을 때 원격화상시스템을 활용해서 이들을 조사할 수 있는 근거 규정을 마련할 필요가 있다. 향후 수사 단계에서 피의자 또는 참고인이 원거리에 있거나 보복 우려 등으로 인해 수사기관에서 진술하지 못할 경우에 이들의 동의를 전제로 원격화상시스템을 활용할 수 있는 근거 규정이 형사소송법을 통해 체계적으로 정비되어야 할 것이다.

2) 형사절차의 전자화

민사재판의 경우 2011년 5월 2일부터 전자소송이 시행되면서 그 효율성이 제고되었으나, 형사재판은 전자화된 증거의 원본성 인정 문제 등으로 인해 음주운전 등 일부 약식사건에만 전자소송이 도입되었다. 2021년 10월 19일 「형사사법절차에서의 전자문서 이용 등에 관한 법률」이 제정되어 2024년 10월 20일부터 시행될 예정인데, 동법으로 인해 형사소송의 효율성과 투명성이 강화될 것으로 기대되고 있다. 특히 동법을 통해 전자영장제도가 도입된 것이 주목되는데, 영장이나 감정유치장, 허가장, 허가서 및 요청서 등이 전자문서로 발부된 경우에는 전자문서를 제시하거나 전송하는 방법으로 영장 등을 집행할 수 있다(형사사법절차에서의 전자문서 이용 등에 관한 법률 제17조).

방어권을 비교형량하여 전자의 이익이 후자의 가치를 훼손하지 않는 범위에서 그 효용성이 입증될 수 있을 정도로 커야 한다.

Ⅲ. 첨단기술 상용화에 따른 범죄 대응과 형사절차 변화

1. 암호화·익명화 기술

(1) 프라이버시 보호 기술 발전

정보통신기술의 발전으로 인해 사람들은 다양한 서비스와 편익을 향유하고 있지만, 그로 인한 프라이버시 침해 우려도 커졌다. 특히 궁극의 디지털 제품이라 불리는 스마트폰이 대중화되면서 이용자의 통화내역이나 위치정보는 물론이고, 문자메시지나 이메일 등 디바이스에 담긴 수많은 정보가 유출될 위험이 커지면서, 프라이버시 보호 기능 강화를 요구하는 목소리도 높아졌다. 이에 스마트폰 제조사들은 보안 수준을 제고시킨 암호화 장치를 구축하기 위해 경쟁적으로 기술을 개발하였는데, 일례로 단순히 비밀번호를 설정하던 방식은 잘못된 번호를 입력한 횟수에 따라서 일정시간 동안 잠금 해제를 시도하는 것이 불가능한 방식으로 변하였다. 또한 인공지능 기술의 발전에 힘입어 생체정보 인식률이 개선되면서 지문을 비롯해서 홍채나 얼굴을 인식해서 잠금 장치가 해제되는 기술도 이미 적용되었다.

모바일 디바이스나 그 운영체제에 암호화 장치가 구축되면서 범죄수사나 기소를 담당하는 사법당국이 전자통신 기기나 시스템에 접근하는 것 자체가 어려워지고 있다. 실제로 2016년 미국에서는 연방수사국(FBI)과 애플이 아이폰 잠금 해제를 두고 첨예하게 대립한 바 있다.[20] 당시 아이폰은 잘못된 비밀번호를 입력한 횟수에 따라서 일정시간 동안 잠금 해제의 시도가 불가능했다. 만약 비밀번호가 6자리 수에 대문자, 소문자 및 숫자로 구성되었다면 총 568억 개의 조합수를 입력해야 했기 때문에 잠금장치 해제에 소요되는 시간이 최장 144년에 이른다고 계산된 것이다.[21]

2015년 12월 2일에 발생했던 ‘샌 버나디노(San Bernardino) 총격 사건’에서 연방수사국은 용의자의 아이폰을 입수했고, 고속입력기를 이용해 단말기의 암호를 풀려고 하였으나 실패했다. 이에 연방수사국은 애플을 상대로 이른바 ‘백도어(Backdoor

20) “Apple opposes order to help FBI unlock phone belonging to San Bernardino shooter”, L.A. Times 2016.2.17., https://www.latimes.com/local/lanow/la-me-ln-fbi-apple-san-bernardino-phone-20160216-story.html (2023년 5월 8일 최종검색).

21) “Why even the FBI can’t hack the iPhone”, The Washington Post 2016.2.17., https://www.washingtonpost.com/news/wonk/wp/2016/02/17/how-long-it-takes-to-crack-an-iphone/ (2023년 5월 8일 최종검색).

)’[22]를 열어 줄 것을 요구했으나, 개인정보 보호를 이유로 애플이 이를 거부하자 연방수사국이 법원에 소송을 제기하였다. 이 사건을 맡은 미국 캘리포니아 주 리버사이드(Riverside) 연방지방법원은 2016년 1월 16일 애플에게 총기 테러 용의자의 스마트폰 잠금장치 해제를 지원하라고 명령했고,[23] 이에 애플은 항소를 제기하였다.[24] 반면 2016년 2월 29일 뉴욕 주 브루클린(Brooklyn) 연방지방법원은 연방수사국이 애플에게 마약거래 용의자의 아이폰 잠금장치 해제를 지원해달라고 요청한 사건에서 애플이 그 요청에 응하지 않아도 된다고 판단했다.[25] 이 판결에서 제임스 오렌스타인(James Orenstein) 판사는 당국이 잠금장치 해제 지원을 요청하는 것은 기업에게 지나친 부담을 지우는 것인바, 기술의 발전 현황을 고려해서 안보와 개인정보 보호 간에 균형점을 어떻게 설정할 것인지는 향후 의회에서 다루어져야 할 문제라고 밝혔다.[26] 용의자의 범죄 유형을 고려하지 않고 두 사건을 평면적으로 비교하는 것은 적절하지 않지만, 연방수사국이 애플을 상대로 범죄 용의자의 아이폰 잠금장치 해제 지원을 요청한 두 사건에서 상반된 입장의 판결이 내려지면서 이후 상급심 법원의 논리 전개에 이목이 집중되었다. 그러나 2016년 3월 28일 연방수사국이 아이폰 잠금장치를 해제하면서 애플을 상대로 제기한 소송을 취하하였고, 이에 양측 간의 법적 공방은 일단락되었다. 그러나 프라이버시 보호를 위한 기술적 조치를 두고 벌어지는 수사당국과 기업의 갈등 양상은 지금도 재현되고 있다.

---

22) 백도어(Backdoor)란 정상적인 인증절차를 우회하여 시스템에 접근할 수 있도록 하는 프로그램을 말한다.

23) “Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman”, The New York Times 2016.2.16., https://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html (2023년 5월 8일 최종검색).

24) “‘Too dangerous’: Apple blasts court order over San Bernardino shooter’s iPhone”, RT News 2016.2.17., https://www.rt.com/usa/332707-judge-orders-apple-unlock-iphone/ (2023년 5월 8일 최종검색).

25) “Apple Wins Ruling in New York iPhone Hacking Order”, The New York Times 2016.2.29., https://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.html (2023년 5월 8일 최종검색).

26) “Magistrate Judge James Orenstein’s Order”, The New York Times 2016.2.29., https://www.nytimes.com/interactive/2016/02/29/technology/document-Orenstein-Order.html (2023년 5월 8일 최종검색).

(2) 다크넷 수사

접속 기록이 남고, 추적이 가능한 통상의 인터넷과 달리 익명화가 보장되는 기술도 개발되었다. 1990년대 중반 미국의 해군연구소(Naval Research Laboratory)는 'The Onion Routing(TOR)' 프로젝트를 통해 웹사이트를 방문해도 익명성이 보장되는 '어니언 라우팅(Onion Routing)'이라는 기술을 개발했고,[27] 이후 무상으로 소스코드가 공개되었다.[28] 이는 인터넷과 같은 일반적 네트워크가 아닌, 가상의 오버레이 네트워크(Overlay Network)[29]를 통해서 같은 웹페이지를 방문할 때 강력한 익명성을 보장해주는 기술이다. 토르(TOR)로 대표되는 다크넷(Dark Net)은 첩보 작전 등의 군사활동이나 내부고발 등에 이용될 수 있으나, 마약이나 총기, 아동성착취물이나 불법 소프트웨어의 거래나 살인청부 등이 이루어지는 범죄의 온상이 되고 있다. 2013년 미국 연방수사국이 마약 암거래 웹사이트인 '실크로드(Silk Road)'를 수사하면서 다크넷의 실상이 널리 알려졌고, 우리나라에서도 2018년 아동성착취 영상물을 거래하는 다크웹 사이트인 '웰컴 투 비디오(W2V)'에 대한 수사가 진행되기도 했다. 이 사건들은 관련자들의 실수에 기인하여 범죄자를 특정해서 추적할 수 있었던 매우 이례적인 사례이며, 암호화·익명화라는 다크넷의 기술적 특징으로 인해 웹사이트 운영자나 이용자를 찾아내기란 불가능에 가깝다. 이로 인해 일부 권위주의 국가에서는 다크넷 접속을 금지하고 있으나, 다크넷이 범죄에 악용된다고 해서 접속 자체를 막을 수는 없는 노릇이다. 다크넷 상에서 벌어지고 있는 범죄에 대응하는 것은 오늘날 전 세계 수사기관이 직면한 과제인바, 우리나라도 잠입수사 제도[30]의 개

---

27) "International Raids Target Sites Selling Contraband on the 'Dark Web'", The New York Times 2014.11.7., https://www.nytimes.com/2014/11/08/world/europe/dark-market-websites-operation-onymous.html (2023년 5월 8일 최종검색).

28) The Tor Project 웹페이지, https://www.torproject.org/about/overview.html.en (2023년 5월 8일 최종검색).

29) 오버레이 네트워크(Overlay Network)는 기존의 네트워크를 바탕으로 다른 필요에 의해 그 위에 재구성되는 또 다른 가상의 컴퓨터 네트워크이다. 기존의 네트워크 위에 별도의 노드(node)와 논리적 링크(logical link)를 구성하므로 기존의 네트워크를 활용하여 성능을 개선하고 효율성을 높인 네트워크 서비스를 제공할 수 있다. ScienceDirect 웹페이지, Overlay Network, https://www.sciencedirect.com/topics/computer-science/overlay-network (2023년 5월 8일 최종검색).

30) 2021년 3월「아동·청소년의 성보호에 관한 법률」개정을 통해 아동·청소년 대상 디지털 성범죄에 대한 신분비공개수사 및 신분위장수사 제도가 도입되었다. 현행 제도는 아동·청소년을 대상으로 한 디지털 성범죄에 한정되어 적용되기 때문에 성인 대상 디지털 성범죄

선과 온라인 수색 제도의 도입이 전향적으로 검토되어야 한다는 주장이 제기되고 있다.

2. 자율주행기술

(1) 자율주행자동차에 대한 압수·수색

자율주행자동차에 대해 압수·수색을 할 경우에도 영장주의가 적용되어야 하는바, 그 영장은 차량번호 등 다른 차량과 구별될 수 있는 사항을 특정하여 발부받을 수 있다. 문제는 종래의 영장 집행방법이 자율주행자동차에도 적용될 수 있는가이다. 사람이 탑승하고 있는 유인 자율주행자동차의 경우, 탑승자가 해당 자동차의 관리인(간수자)인 경우에는 일반적인 자동차에 대한 영장 집행과 다를 바 없다. 그러나 인간 운전자가 없는 무인택시에 승객이 탑승한 경우, 해당 차량에 대한 영장제시 및 영장집행 사실 통보를 어떻게 진행할 것인지 정리되어야 한다. 즉 차량에 대한 수색이 필요한 경우 영장을 승객에게 제시할 것인지, 승객은 차량 내부에 대해서만 점유하는 방실에 대한 권리와 유사한 권한을 가지는 것인지, 잠겨 있는 트렁크에 대한 수색까지 가능한 것인지 등에 대한 논의가 요구된다. 요컨대, 이 경우 수사기관은 관리자에게 영장집행 사실을 통보하고 참여하게 하는 절차를 진행해야 하며, 승객이 탑승하고 있는 승객 칸이 수색의 대상이 된 때에는 수색영장을 탑승객에게 제시해야 한다. 한편 미국 판례에 의할 때, 자동차에 대한 합법적인 영장 집행이 이루어지면 트렁크를 포함한 자동차의 모든 부분이 수색의 대상이 되고,[31] 승객 칸[32]은 물론이고 차 안에 있는 승객의 소지품[33]도 수색의 대상이 될 수 있다. 승객이 미처

를 비롯해 다크웹에서 벌어지는 수많은 범죄에 대응할 수 없다는 한계가 있다.

31) United States v. Ross, 456 U.S. 798 (1982).

32) New York v. Belton, 453 U.S. 454 (1981).

33) 1999년 Wyoming v. Houghton 판결에서 연방대법원은 차량 안에 있는 승객의 소지품에 대한 수색을 정당화하는 두 가지 이유를 제시했는데, ① 승객의 축소된 프라이버시에 대한 기대(승객은 운전자와 마찬가지로 차량으로 운송되는 재물에 대해 축소된 프라이버시에 대한 기대를 가지게 됨)와 ② 승객의 소지품을 수색할 수 없는 경우, 상당한 정도로 손상될 수밖에 없는 효과적인 법률 집행에 대한 정부의 이익(영장 발부를 기다리는 사이, 자동차의 기동성으로 인해 증거나 금제품을 영구적으로 상실하게 될 위험이 창출되기 때문)이 그것이다. Rolando Del Carmen/Craig Hemmens, Criminal Procedure: Law and Practice, CENGAGE Learning, 2017, p.234.

알지 못하는 사이에 범인이 승객의 소지품에 금제품을 은닉할 수 있다는 가능성이 고려된 것이나, 차량에 대한 수색 영장으로 승객에 대한 수색까지 이루어지는 것은 비판받을 만하다.

한편 사람이 탑승하지 않은 상황에서 주행 중인 무인 자율주행자동차의 경우에는 피처분자의 부재로 인해 영장을 제시하는 것이 현실적으로 불가능하므로 영장제시 없이 압수·수색을 할 수 있다고 해석될 수 있다.[34] 법은 불가능을 요구할 수 없는 바, 형사소송법상 영장제시 의무가 영장의 제시가 불가능한 경우에도 요구되는 것은 아니라는 점은 원론적으로 타당하다. 그러나 일정한 의무가 조건 없이 부여된 경우에는 법적 불가능의 상태에 대한 판단을 엄격히 해석해야 하고, 그것이 개인의 기본권에 대한 침해를 정당화하기 위한 요건이라면 더욱 더 그러하다. 그러한 측면에서 볼 때 단순히 피처분자가 현장에 부재한다는 것을 영장제시 의무가 면제되는 상황으로 설명하는 것은 지나치게 형식적인 판단이며, 영장제시 의무가 가지는 법적 의미의 중대성을 간과한 것이라고 할 수 있다. 즉 영장제시 의무가 가지는 법적 의미를 고려한다면 피처분자가 부재중이고, 그가 현장에 참여하는데 소요되는 시간이 당해 압수·수색의 수사상 목적과 효과를 현저히 저해할 정도에 이를 때에야 비로소 영장제시 없이도 압수·수색을 할 수 있다고 보아야 한다.

다만 이러한 해석론은 영장의 제시라는 요건에 대해 '직접성'을 고수하는 것을 전제로 한다. 즉 압수·수색의 현장에서 피처분자가 직접 영장의 원본을 인지할 수 있도록 하는 것을 영장제시의 유일한 방법이라고 이해하는 것이다. 하지만 이에 대해서는 2017년 대법원 판결[35]에서 언급된 영장제시의 입법취지, 즉 영장제시 요건의 실질적 의미는 영장의 내용과 범위를 피처분자에게 인지하게 하는 것이라는 점에 주목하면서 보다 효율적인 방식을 고려해 볼 수 있다. 이에 전자영장제도의 도입 필요성이 제기되었는데, 2021년 10월 19일 「형사사법절차에서의 전자문서 이용 등에 관한 법률」 제정을 통해 도입된 전자영장이 이용될 경우 피처분자가 부재중인 상황에서도 압수·수색의 적법요건을 충족하면서 수사상의 목적이 달성될 수 있을 것으로 기대된다.

---

34) 대법원 2015. 1. 22. 선고 2014도10978 전원합의체 판결.

35) 대법원 2017. 9. 21. 선고 2015도12400 판결.

(2) 자율주행자동차 운행 정보 취득

자율주행자동차는 카메라, 레이더, 초음파 센서 등을 통해 외부환경을 인식하여 운행되는바, 대량의 정보를 수집 및 활용하게 된다. 향후 자율주행자동차는 다른 자동차나 교통 및 통신 기반시설과 연결되어 네트워크의 한 축으로서 양방향 소통을 하게 될 것으로 전망되는데, 이 경우 특정 차량의 운행 정보는 그 차량의 소유자뿐만 아니라 전기통신사업자나 위치정보사업자는 물론이고 기반시설 운영 주체에 의해 보유될 수 있다. 또한 딥러닝 기반의 인공지능이 탑재된 자율주행자동차의 운행 정보는 차량 제조사에 의해서도 수집되어 기술 개선 등에 활용될 것이다. 이때 수사기관은 법원의 허가를 받아서 「전기통신사업법」에 의한 전기통신사업자에게 통신사실 확인자료 제공을 요청할 수 있고, 통신사실 확인자료에는 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적 자료가 포함된다.

2018년 6월 22일 미국 연방대법원은 정부기관이 사전에 영장을 발부받지 않고 휴대전화에 기반한 개인의 위치에 대한 과거 셀 사이트(cell-site) 기록에 접근하는 것은 부당한 압수·수색을 금지한 수정헌법 제4조에 위배된다고 판단하였다.[36] 그러나 자동차라는 객체의 특성을 고려할 때[37] Carpenter v. United States 판결이 휴대전화 위치정보가 아닌 자율주행자동차의 위치정보에도 적용될 수 있을지는 의문이다. 1983년 United States v. Knotts 판결[38]에서 미국 연방대법원은 “공공 도로에서 자동차를 타고 이동하는 사람은 한 장소에서 다른 장소로 이동하는데 있어 프라이버시에 대한 합리적인 기대가 없기 때문에 시각적인 감시가 수색은 아니다”라고 결론지었다.[39] 공공 도로상 차량 및 그 이동 상황은 누구라도 볼 수 있으므로 프라

---

36) Carpenter v. United States, 138 S.Ct. 2206 (2018).

37) 미국 연방대법원은 자동차의 기동성에 주목하였는바, 영장을 발부받을 수 있는 시간적 여유가 없을 때에는 영장 없이 자동차를 수색할 수 있다고 판시하였다(Carroll v. United States, 267 U.S. 132 (1925)). 자동차 수색에 있어서 영장주의의 예외가 광범위하게 인정되는 것과 관련해서는 수사기관으로 하여금 국민들의 기본권을 침해하는 강제수사를 하기에 앞서 독립적이고 중립적인 판사로부터 사전에 그 적절성에 대한 심사를 받도록 하는 헌법의 취지를 몰각시킬 수 있다는 비판이 제기되고 있다. 다만 자동차가 대중화·일반화하면서 범죄 도구로 활용될 가능성 또한 높아졌고, 이에 수반하여 자동차에 대한 수색의 필요성도 한층 증대되었는바, 자동차 수색 시 영장주의의 예외가 여전히 광범위하게 인정되고 있다.

38) United States v. Knotts, 460 U.S. S. 276 (1983).

39) United States v. Knotts, 460 U.S. S. 276 (1983) at 281, 282.

이버시 보호를 주장할 수 없다는 것이다.[40] 또한 Carpenter v. United States 판결의 법정의견은 위치추적 장치가 부착된 자동차[41]와 달리 휴대전화는 그 소유자의 이동 상황을 거의 정확하게 추적할 수 있도록 하는 것으로서 "사람을 해부하는 것과 같은 특징"[42]을 가진다고 언급하였다.[43] 일반적으로 자동차의 경우 기동성을 가지고 있어서 신속하게 구역 밖으로 도주할 수 있고, 주택에 비해 프라이버시에 대한 기대가 낮은 공간으로 평가되며, 이미 교통법규 등을 통해 정부의 규제를 받고 있기 때문에 자동차에 대한 영장 없는 수색이 광범위하게 인정되는 것으로 파악된다.[44] 요컨대 운행 중인 자율주행자동차에 대해서는 영장 없는 수색이 이루어질 수 있는 가능성이 보다 넓게 열릴 수 있을 것이다.

(3) 기타

사법경찰관 등이 현실적으로 주행 중인 자동차에 대한 영장을 집행하기 위해서는 이를 정지시킬 수 있는 기술적인 조치가 선행되어야 한다. 즉 일반적인 자동차의 경우 운전자에 대한 일정한 표시나 고지행위로 자동차를 정지시킬 수 있으나, 자율주행자동차의 경우 이를 인지할 주체가 없으므로, 자율주행시스템이 즉시 정차가 필요한 경우 등을 인지할 수 있도록 공통의 신호체계를 만들어서 탑재하거나 영장을 집행하는 사법경찰관 등이 자율주행시스템을 즉시 정지시킬 수 있는 기술적인 수단을 갖추도록 하는 조치가 필요하다. 아울러 모든 무인 방식의 자율주행자동차의 경우에는 영장을 집행하는 사법경찰관 등이 신속하게 해당 자동차의 관리자 등에게 연락을 취할 수 있는 기술적 수단도 갖추어져야 한다.

한편 방대한 양의 자율주행자동차 운행 정보는 클라우드 서버에 집적될 가능성이 크고, 글로벌 자동차 제조업체가 관리하는 해당 서버는 해외에 구축되어 있을 수 있

---

40) United States v. Knotts, 460 U.S. S. 276 (1983) at 281. James W. Osterburg/Richard H. Ward, Criminal Investigation: A Method for Reconstructing the Past, Anderson Publishing, 2014, p.205.

41) United States v. Jones, 132 S.Ct. 945 (2012).

42) Riley v. California, 573 U.S. ___ (2014), 134 S.Ct., at 2484.

43) Carpenter v. United States, No. 16-402, 585 U.S. ____ (2018), at 2218.

44) Robbins v. California, 453 U.S. 420(1981); Rolando Del Carmen/Craig Hemmens, Criminal Procedure: Law and Practice, CENGAGE Learning, 2017, p.243; Steven G. Brandl, Criminal Investigation, SAGE Publications, Inc., 2014, pp.65-67.

다. 2018년 3월 미국은 연방법인 「합법적인 해외 데이터 활용의 명확화에 관한 법률(Clarifying Lawful Overseas Use of Data Act, CLOUD Act)」(이하 '클라우드법'이라 함)[45]을 입법화하였는데,[46] 클라우드법에 의할 때 전자통신서비스 및 원격 컴퓨팅 서비스 관련 미국 기업은 영장이나 자료 제출 명령이 있으면 그 대상이 된 정보 등이 외국 서버에 저장되어 있다고 하더라도 이를 제출해야 한다.[47] 이러한 입법적 조치로 인해 미국 기업이 해외 서버에 저장되어 있는 데이터를 수사기관에 제출할 경우 발생할 수 있는 손해배상 부담과 같은 법적 책임 문제가 어느 정도 해결될 수 있다는 평가가 내려지고 있다.[48] 또한 클라우드법은 미국 법무부와 행정협정(executive agreements)을 맺은 국가에게 호혜적 정보 공유를 허용하는바,[49] 행정협정 체결국은 미국의 전자통신서비스 기업 등에게 직접 전자정보 등을 요청할 수 있다.[50] 유럽 사이버범죄 협약도 일정한 요건을 갖추면 국제형사사법 공조가 없더라도 직접 전자정보를 받아볼 수 있도록 규정하고 있는데, 우리나라는 2022년 10월에서야 사이버범죄 협약 가입의향서를 유럽평의회에 제출하였다.

---

45) H.R.1625 - Consolidated Appropriations Act, 2018(115th Congress), 03/23/2018 Became Public Law No: 115-141, DIVISION V—CLOUD Act, https://www.congress.gov/bill/115th-congress/house-bill/1625/text (2023년 5월 8일 최종검색).

46) Jean Galbraith(Edit.), "Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data", American Journal of International Law Vol.112 Issue3, American Society of International Law, 2018, p.487.

47) Ilana Hope Eisenstein/Jim Halpert/Lindsay R. Barnes, "CLOUD Act bolsters US government powers to obtain data stored abroad", DLA Piper, April 12, 2008, https://www.dlapiper.com/en/us/insights/publications/2018/04/us-cloud-act-authorizes-search-warrants-for-data-stored-abroad/ (2023년 5월 8일 최종검색).

48) "'클라우드 서버' 압수수색 방안 논의 필요", 세계일보 2018년 11월 9일자, http://www.segye.com/newsView/20181109001490 (2023년 5월 8일 최종검색).

49) CLOUD Act § 105(a); to be codified at 18 U.S.C. § 2523 - Executive agreements on access to data by foreign governments; "CLOUD Act Establishes Framework To Access Overseas Stored Electronic Communications", Cleary Gottlieb, April 4, 2018, p5, https://www.clearygottlieb.com/-/media/files/alert-memos-2018/cloud-act-establishes-framework-to-access-overseas-stored-electronic-communications.pdf (2023년 5월 8일 최종검색).

50) Stephen P. Mulligan, Cross-Border Data Sharing Under the CLOUD Act, Congressional Research Service(CRS) Report, 2018, p.2.

Ⅳ. 형사절차상 첨단기술 활용과 헌법적 쟁점

1. 인공지능

(1) 수사지원 및 범죄예측 프로그램

수사과정에서 용의자 검거나 증거확보를 위하여 다양한 과학기술이 활용되고 있는데, 지문이나 DNA 매핑, CCTV 분석이나 GPS 위치추적 등이 대표적이다. 인공지능이 딥러닝을 통해 패턴분석을 하여 인식의 정확도를 제고시키면서 종래의 장치들은 한층 더 지능화되고 있다. 또한 문자나 음성인식, 홍채인식[51]이나 얼굴인식 등에 대한 분석도 패턴인식에 의해 정확도가 높아지고 있으며, 데이터 분석 시스템을 이용해서 대용량 디지털 데이터로부터 유의미한 결과를 도출할 수 있다.[52] 즉 인공지능 기술을 활용할 경우 비정형파일이나 대용량의 이메일, 통화 내역, 계좌나 전자결제 내역, 모바일 데이터나 회계 데이터 등을 사용자나 시간 또는 관계를 중심으로 분석할 수 있다.[53] 인공지능 기술의 발전은 범죄자들 사이의 관계는 물론이고 범죄자와 데이터, 데이터와 데이터 사이의 관계 및 그 패턴을 분석할 수 있도록 하였는바, 동 기술을 통해 빅데이터 기반 처리시스템이 고도화되면서 범죄자의 행적이나

51) 미국의 생체인식·식별 기술 기업인 BI2 Technologies(Biometric Intelligence and Identification Technologies)사가 아이폰 기반으로 개발한 홍채인식 스캐너 '모리스(MORIS)'가 수사에 활용되고 있는데, 경찰은 모리스로 특정인의 홍채를 스캔한 후 범죄기록 데이터베이스에 접속해서 범죄용의자인지 여부를 확인할 수 있다. Zach Howard, "Police to begin iPhone iris scans amid privacy concerns", Reuters, July 21, 2011, https://www.reuters.com/article/us-crime-identification-iris/police-to-begin-iphone-iris-scans-amid-privacy-concerns-idUSTRE76J4A120110720 (2023년 5월 8일 최종검색).

52) 예컨대, 살해된 피해자의 몸에서 피의자의 DNA가 검출되었다는 과거사실을 알려주는 것에 그치지 않고, 피의자가 피해자의 옆집에 살고 있었다는 사실이나 피의자의 자동차에 피해자를 태운 사실 등을 찾아내어 그가 범인일 가능성이 있다고 수사관에게 알려주는 것이다. Michael L. Rich, "Machine learning, Automated Suspicion Algorithms and the Fourth Amendment", University of Pennsylvania Law Review Vol.164, University of Pennsylvania Law School, 2016, p.892.

53) FBI는 패턴일치 여부 확인에 기반한 수사기술을 활용하고 있는데, 실제로 강도범인을 추적하면서 범행기간 전에 급증한 통화량과 범행기간 이후에 폐쇄적으로 사용된 선불통화전화의 패턴을 이용해서 범인을 검거하기도 했다. FBI, Next Generation Identification (NGI), https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (2023년 5월 8일 최종검색).

범죄행위에 대한 추적이 효율적으로 이루어지게 된 것이다.

2012년 뉴욕 경찰청이 마이크로소프트(Microsoft)사와 함께 개발한 'DAS(Domain Awareness System)'는 뉴욕 내에 설치된 방범용 CCTV나 차량번호판 판독기 등을 통해 수집된 데이터와 911 신고 내역이나 전과 기록 및 톨게이트 통행 정보 등을 통합·분석하여 용의자나 용의 차량 추적 등을 지원한다.[54] 또한 DAS는 범죄용의자의 생년월일과 전화번호, 주소, 신용카드나 금융거래 내역, 차량의 종류와 색상 및 번호 등은 물론이고 고용정보나 신용정보 및 판결기록 등을 포함하는 빅데이터를 분석해서 용의자의 동선이나 생활패턴 등 다양한 정보를 파악할 수 있다.[55] 아울러 의심 상황이 포착되면 즉시 경보가 발령되고, 이때 일선 경찰관들은 모바일 기기를 통하여 사건 발생 위치와 용의자 동선 및 전과 기록 등의 정보를 제공받는다.[56] DAS는 수사의 효율성을 증진시켰으나, 이로 인한 개인의 사생활 침해와 인권 침해의 우려가 제기되었다. 이에 뉴욕 경찰청은 동 시스템에 관한 가이드라인을 마련하였는바, DAS는 적법한 법집행과 공공의 안전을 증진시키기 위해 24시간 운영되나, 사적 영역이 아닌 장소나 공공활동을 대상으로 하며, 누구라도 성별·나이·인종·국적·종교·혼인여부·장애·성적지향·시민권 보유 여부·병역 및 정치적 성향 등을 이유로 그 목표가 되거나 감시받지 않는다. 나아가 경찰이 CCTV를 이용할 때에는 표지를 부착하여 사람들이 그 촬영 사실을 인식할 수 있도록 해야 한다.[57]

한편 인공지능 기술은 범죄발생 예측도구 개발에도 이용되고 있다. 2011년 미국 로스앤젤레스 경찰국은 캘리포니아 대학과 공동으로 'PredPol(PREDictive POLicing)'이라는 범죄예측 소프트웨어를 개발했다.[58] 인공지능 알고리즘을 이용해서 종래 발

54) Andrew Guthrie Ferguson, "Big Data and Predictive Reasonable Suspicion", University of Pennsylvania Law Review, Vol.163, University of Pennsylvania Law School, 2015, pp.378-379.

55) Andrew Guthrie Ferguson, Id., p.378.

56) E. S. Levine/Jessica Tisch/Anthony Tasso/Michael Joy, "The New York City Police Department's Domain Awareness System", Journal Interfaces, Vol. 47, Iss. 1, INFORMS Institute for Operations Research and the Management Sciences, 2017, pp.70-84.

57) NYPD Domain Awareness System Public Security Privacy Guidelines, p.3, Public Intelligence, July 30, 2012, https://publicintelligence.net/nypd-domain-awareness-system-public-security- privacy-guidelines/ (2023년 5월 8일 최종검색).

58) Ishmael Mugari/Emeka E. Obioha, "Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing", Social Sciences, Vol.10, Iss.6, 234, MDPI, 2021. 6., p.5.

생했던 범죄의 유형이나 발생 위치 및 일시 등과 같은 데이터를 분석한 후 향후 발생할 범죄의 형태와 장소 및 시간 등을 알려주는[59] PredPol은 경찰력의 효율적 배치를 통해 범죄율을 감소시킨 것으로 평가된 바 있다.[60] 그러나 인공지능 알고리즘과 그 데이터에 대해서는 편향성과 검증 가능성의 문제가 제기된다. 특히 인공지능 알고리즘은 특정한 판단에 대해 그 설계자조차도 알기 어려운 블랙박스가 문제되어 설명의무의 부과가 함께 논의된다.

(2) 재판 지원 프로그램

인공지능 시스템은 유무죄 및 형량을 결정하는 판사의 업무를 지원할 수 있다. 2013년 미국 위스콘신 주 라크로스에서 발생한 총격 사건으로 두 명의 용의자가 체포되었는데, 그 중 에릭 루미스(Eric L. Loomis)에 대한 재판에서 주 검찰은 노스포인트사(Northpoint Inc)가 개발한 컴퍼스(Compas)를 활용하여 루미스의 재범 위험성이 높다고 주장했다. 이를 인정한 판사는 루미스가 공동체에 큰 위협이 되는 인물이라며 6년 징역형을 선고했다. 이에 루미스는 인공지능 분석을 근거로 중형을 선고한 것이 부당하다고 항소했는데, 인공지능의 판단에 대해서는 알고리즘을 확인하거나 이의를 제기할 수 없기 때문에 적법한 절차에 따를 권리가 침해되었다고 주장한 것이다. 이 사건에서 위스콘신 주 대법원은 “알고리즘의 한계와 그 비밀을 고려해야 하지만 소프트웨어가 양형 법원에 활용 가능한 정보를 제공하는 데 도움을 준 것은 사실이고, 컴퍼스 보고서는 가치 있는 정보를 제공했다”고 밝히면서 “컴퍼스 보고서를 제외해도 전과가 있는 루미스가 자신의 범죄 차량 운전 혐의 등을 인정한 만큼 동일한 형량(징역 6년)을 선고받았을 것”이라면서 항소를 기각하였다.[61]

재범예측 프로그램인은 컴퍼스는 피고인에게 137개의 질문에 답하게 하고 과거의 범죄 데이터와 대조하여 다시 범죄를 저지를 위험을 10단계의 점수로 산출하고 있

---

59) PredPol 홈페이지, https://www.predpol.com/about/, https://www.predpol.com/results (2023년 5월 8일 최종검색).

60) “UCLA Study Proves Predictive Policing Successful in Reducing Crime Over Several Months of Deployment with The LAPD”, PredPol, 2015. 11. 11., http://www.predpol.com/ucla-predictive-policing-study (2023년 5월 8일 최종검색).

61) “Sent to Prison by a Software Program’s Secret Algorithms”, The New York Times, 2017. 5. 1. https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?_r=0 (2023년 5월 8일 최종검색).

다. 그 질문에는 범죄나 보석 이력, 나이, 고용이나 생활 상황, 교육 수준, 지역사회와의 관계, 약물 사용, 신념, 심지어 가족의 범죄 이력이나 마약 사용 경력 등도 포함된다. 루미스의 경우 과거 성폭행 전과로 인해 성범죄자 데이터베이스에 등록되어 있던 인물이었고, 이로 인해 컴퍼스에 의한 재범위험 점수도 높게 산출된 것으로 판단된다. 그동안 미국 법원은 재판의 효율성 등을 위해 암묵적으로 인공지능을 활용하기도 했으나 인공지능의 판단을 형사판결의 타당성 근거로 인용한 것은 처음이었다. 최근 인공지능 기기는 판결문을 다듬거나 보석금을 설정하고, 심지어 유무죄 결정에까지 관여하는 등 미국 여러 주의 사법 시스템에서 중요한 역할을 수행하고 있다.[62] 상기의 컴퍼스는 주 정부의 교정국에서도 사용되고 있고, 그 데이터가 판사에게 제공되고 있는바, 형사재판의 양형 단계는 물론이고 가석방의 결정 여부를 판단하는 등 교정의 영역에서도 활용되고 있다.

한편 위스콘신 주 이외에도 애리조나, 콜로라도, 델라웨어, 켄터키, 루이지애나, 오클라호마 버지니아, 워싱턴 주에서도 형사재판에 재범예측 프로그램을 도입하였는데, 이와 관련해서는 전술한 바와 같이 알고리즘의 비공개로 인하여 예측 기능의 정확성을 외부에서 검증할 수 없다는 비판이 제기되었다. 이에 '프로 퍼블리카(PRO PUBLICA)'라는 언론매체가 컴퍼스를 도입하고 있는 플로리다 주의 정보공개법을 활용하여, 2013년부터 2014년에까지 브로워드 카운티에서 재범예측의 평가를 받았던 1만명 가량의 데이터를 확보한 후 독자적 검증을 진행했다. 플로리다 주는 컴퍼스를 공판 전에 보석 여부를 판단하는 과정에 활용하고 있는데, 재범예측 전반의 정확성에서는 백인 59%, 흑인 63%로 큰 차이는 없는 것으로 보이나, 면밀히 살펴보면 흑인이 백인에 비해서 위험도가 더 높게 나오는 경향이 있다고 지적하였다. 즉 재범예측 후, 실제로는 2년 동안 재범이 없었던 인물이 높은 위험도 평가를 받는 비율은 흑인이 45%, 백인은 23%로 2배 가까이 차이가 났고, 반대로 재범예측 후 2년 이내에 재범이 있었던 인물이 낮은 위험도 평가를 받은 비율은 백인이 48%, 흑인 28%로 이 또한 2배 가까이 차이가 있었다고 한다.[63]

---

62) "Sent to Prison by a Software Program's Secret Algorithms", The New York Times, 2017. 5. 1. https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?_r=0 (2023년 5월 8일 최종검색).

63) PRO PUBLICA 웹사이트, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (2023년 5월 8일 최종검색).

2. 드론과 로봇기술

(1) 드론

드론은 범죄수사에 활용될 수 있는데, 그 수사의 법적인 성격을 판단함에 있어서는 드론의 특징과 활용 방법이 함께 고려되어야 한다.[64] 먼저 수사과정에서 사진 또는 동영상 촬영에 드론을 이용하는 것의 법적 성격을 규명할 때에는 사진촬영의 법적 성격을 두고 전개되는 형사소송법상 논의를 참고할 수 있는바, 이는 강제수사로 파악되어야 한다. 다음으로 드론은 실시간 관찰 업무에 투입될 수 있는데, 이 경우 드론은 탑재된 영상장비를 통해서 사진이나 동영상을 촬영한 후 저장하는 것이 아니라 육안이나 망원경을 대신하는 것이다.[65] 다만 기술의 특징상 넓은 시야각을 확보해서 사각지대를 해소할 수 있고, 근접 촬영을 할 수 있기 때문에 사생활 침해의 위험성은 보다 높게 평가된다. 특히 드론이 수사에 활용될 경우 수사 대상자는 물론이고 그 주변인이나 불특정 다수의 프라이버시도 침해될 우려가 있으므로 사법부의 통제가 이루어질 필요가 있다. 다만 통신감청과 마찬가지로 드론을 이용한 수사도 그 밀행성이 유지될 필요가 있으므로 법률에 정해진 일정한 요건을 구비하여 법원의 허가를 얻은 경우에는 통상적인 영장집행 절차를 거치지 않고 드론을 활용할 수 있도록 해야 한다. 다만 통신감청과 같이 드론을 투입한 경우에도 해당 사건에 대하여 공소가 제기되거나, 불기소 또는 불입건 처분이 있은 날로부터 일정한 기간 내에 대상자에게 드론을 이용한 수사가 이루어진 사실과 함께 그 집행기관 및 집행일시 등이 통지될 필요가 있다.

---

64) 드론을 이용한 범죄수사에 영장주의가 적용되는지가 직접적으로 다루어진 국내외 사례는 발견되지 않는다. 다만, 미국에서는 항공감시의 법적 성격을 두고 영장이 요구되는 수색으로 보아야 할지가 문제되었는데, 항공감시와 관련된 미국의 판례들은 항공기의 운행 고도나 촬영된 사진의 화질 등을 고려해서 수정헌법 제4조가 적용되는 수색인지를 판단하고 있다. 즉, 헬리콥터나 비행기가 통상적으로 운행되는 고도에서 육안이나 성능이 낮은 카메라를 이용하여 이루어진 항공감시는 수색으로 파악하지 않고 있는 것이다. 이러한 법원의 입장에 대해서는 기술이 발달함에 따라 물리적 침입 없이 야기되는 시민의 사생활 침해를 제대로 막지 못한다는 비판이 제기되고 있다.

65) 예컨대, 대마가 재배되는 것으로 의심되는 고층 아파트 베란다나 건물 옥상을 관찰하기 위하여 인근 건물에서 고성능 망원렌즈를 이용하는 것과 드론을 투입하는 것은 본질적으로 그 성격이 다르지 않다.

(2) 로봇기술

지능형 로봇이 경찰의 순찰 업무에 투입되기도 하는데, 미국의 나이트스코프(Knightscope)사가 개발한 'K5'는 자율주행이 가능하고, 부착된 카메라를 이용해 360도 회전하면서 자동차 번호판을 판독할 수 있으며, 적외선 열화상 센서가 탑재되어 야간에도 사람이나 사물을 인식할 수 있다. 또한 네트워크에 연결되어 메시지나 인식 정보를 송·수신할 수 있고, 긴급한 상황이 발생하면 경찰을 호출할 수 있어서 사전에 입력된 지역을 주기적으로 순찰할 수 있다.[66] 순찰업무의 위험성과 강도를 고려할 때 지능형 로봇의 투입은 순찰업무의 효율성을 높일 수 있을 뿐만 아니라 기존에 순찰업무에 투입되었던 경찰인력을 취약지역에 재배치하여 그 활용도를 제고시킬 수 있다.[67]

한편 로봇은 범죄수사에도 활용될 수 있는데, 2016년 7월 8일 미국 텍사스 주 댈러스 경찰은 경찰관을 저격한 범인을 사살하는 과정에서 '폭탄 로봇(bomb robot)'을 투입하였는데, 로봇팔에 폭발물을 장착하여 용의자가 숨어있는 자리에 가져다 놓고 폭파시킨 것이다.[68] 또한 2016년 12월 8일 러시아에서도 폭발물을 탑재한 장갑차 모양의 킬러로봇을 범죄자의 은신처로 접근시켜 출입물을 폭파하고 내부로 진입하여 IS 조직원을 사살한 사건이 있었다.[69]

---

66) Knightscope 홈페이지, https://www.knightscope.com/k5/, https://www.knightscope.com/blog-1 (2023년 5월 8일 최종검색).

67) 아랍에미리트 두바이에서도 경찰 로봇이 도입되었는데, 인공지능 기술을 기반으로 한 로봇은 범인 얼굴을 식별하고, 실시간으로 주변 정보를 수집하여 경찰에 보고한다. 두바이는 2030년까지 경찰력의 25%를 로봇으로 대체하는 방안을 추진하고 있다. "Robocop joins Dubai police to fight real life crime", https://www.reuters.com/article/us-emirates-robocop/robocop-joins-dubai-police-to-fight-real-life-crime-idUSKBN18S4K8. (2023년 5월 8일 최종검색)

68) "When Can Police Use a 'Bomb Robot' to Kill a Suspect?", Time 2016. 7. 8., http://time.com/4398196/dallas-shooting-bomb-robot/(2023년 5월 8일 최종검색).

69) "Dramatic moment Russian special forces use a machinegun ROBOT as they 'take out' ISIS warlord behind deadly bombings", Daily Mail, 2016. 12. 8., http://www.dailymail.co.uk/news/article-4013864/Dramatic-moment-Russian-special-forces-use-machinegun-ROBOT-ISIS-war-lord-deadly-bombings.html (2023년 5월 8일 최종검색).

3. 사물인터넷과 확장현실

(1) 사물인터넷

가. 사물인터넷

우리나라에 비해 총기 소지가 자유로운 미국에서는 총기사용 범죄 발생 시에 신속하게 피해자를 구조하고 수사의 효율성을 제고하고자 사물인터넷 기반의 '샷 스포터(Shot Spotter)' 시스템이 이용되고 있다.[70] 이는 대학 캠퍼스와 같은 특정 장소에 설치된 음향감지장치가 총성을 감지하여 데이터를 전송하면, 총성이 개별 음향감지장치들에 도달한 각각의 시간을 토대로 삼각 측량법을 이용해 총기의 발사 위치를 알아내는 것이다.[71] 2017년에 샷 스포터 시스템을 도입한 일리노이주의 록포드(Rockford) 경찰은 2018년 10월 말 기준으로 이 시스템을 이용해서 총기 사건 용의자 16명을 체포했다고 한다.[72] 2016년 캘리포니아주 샌디에고(San Diego)시 경찰국은 업무 수행 중에 경찰이 총기를 발포하거나 경찰을 향해 총격이 가해지는 상황에 신속하게 대응하고자 샷 스포터(Shot Spotter) 장비[73]가 장착된 경찰복을 지급하여 1년 동안의 시범 운영을 거쳐 이 시스템을 도입하기도 했다.[74]

2015년에는 '야르담 테크놀로지스(Yardarm Technologies)'사가 총기 자체에 센서와 위치추적 장치를 부착해서 그 발사 정보를 경찰 클라우드로 전송하는 '스마트 총(Smart Gun)'을 출시하였다.[75] 이 총은 공식 출시 전에 캘리포니아주의 산타크루즈(Santa Cruz)와 텍사스주의 캐롤튼(Carrollton) 경찰서에서 시험 사용되었는데,[76] 당

---

70) ShotSpotter 웹페이지, ShotSpotter Cities, https://www.shotspotter.com/cities/ (2023년 5월 8일 최종검색).

71) ShotSpotter, ShotSpotter FAQ, 2019, https://www.shotspotter.com/wp-content/uploads/2019/06/FAQ-June-2019_v2.pdf (2023년 5월 8일 최종검색).

72) "Rockford Police say ShotSpotter detection system has led to 16 arrests", WTVO Channel 17/WQRF Fox 39 2018. 10. 30., https://www.mystateline.com/news/rockford-police-say-shotspotter-detection-system-has-led-to-16-arrests/ (2023년 5월 8일 최종검색).

73) 음향 감지 센서와 GPS 기반의 위성판독 시스템이 탑재된 이 장비는 총기나 기타 화기의 발포 위치를 추적하도록 한다.

74) "San Diego police to continue using gunshot detection system, despite some criticism", The San Diego Union-Tribune, 2017. 10. 7., https://www.sandiegouniontribune.com/news/public-safety/sd-me-sdpd-shotspotter-20171005-story.html (2023년 5월 8일 최종검색).

75) 네트워크에 연결된 스마트 총 이외에도 방아쇠에 지문센서가 탑재되었거나 RFID 칩이 장착된 총도 스마트건으로 개발되었다.

시 현장 경찰들은 검증되지 않은 신기술이 적용된 스마트 총에 대해 회의적인 입장을 취하기도 했다.[77] 그럼에도 불구하고 스마트 총은 경찰에 의한 총기 사용의 투명성을 확보하고, 위험 상황에서 지원 요청 위치를 알릴 수 있다는 장점이 있다.[78]

한편 우리나라에서는 2015년 10월부터 시범 운영된 '웨어러블 폴리스 캠'이 2019년 발생한 '버닝썬 클럽 사건' 등을 계기로 하여 그 필요성이 강조되었으나, 정작 폴리스 캠의 활용 건수는 감소한 것으로 알려졌다.[79] 폴리스 캠은 화질이나 배터리 용량 등의 성능이 떨어지고 그 장착이 불편하며, 녹화된 영상이 실시간으로 전송되지 않기 때문에 일일이 수동으로 녹화 영상을 전송 및 등록해야 하는 번거로움이 크다고 한다. 이러한 문제를 해소하기 위해서는 폴리스 캠의 성능을 개선하고, 해당 디바이스가 네트워크로 연결되어 그 영상이 자동으로 전송되는 시스템을 구축할 필요가 있다. 아울러 폴리스 캠의 이용 활성화를 위해서는 관련 법률의 정비도 요청된다. 경찰청은 폴리스캠을 시범 운영하기 위해 경찰청 내부 훈령인 「웨어러블 폴리스캠 시스템 운영 규칙」을 제정하였다.[80] 그러나 폴리스 캠의 경우 근접 촬영으로 인한 사생활 침해나 촬영된 영상의 외부 유출 등이 문제되고 있으므로, 그 우려를 해소할 수 있도록 운영에 대한 근거 법률이 마련되어야 한다. 또한 종래에는 「개인정보 보호법」상 '영상정보처리기기'가 CCTV와 같은 고정형 영상기기로 한정되어 이동형 영상촬영기기의 활용 근거가 없다는 문제가 있었다. 그러나 2023년 3월 14일 동법이 개정되면서 이동형 영상정보처리기기 운영 기준이 마련되었는바,[81] 이는 2023년 9월 15일부터 시행될 예정이다.

---

76) Dara Kerr, "Can these gun sensors keep cops safer?", CNET, 2014. 11. 8., https://www.cnet.com/ news/can-these-gun-sensors-keep-cops-safer/ (2023년 5월 8일 최종검색).

77) Colin Neagle, "How the Internet of Things is transforming law enforcement", Network World, 2014. 11. 3., https://www.networkworld.com/article/2842552/how-the-internet-of- things-is-transforming-law-enforcement.html (2023년 5월 8일 최종검색).

78) Yardarm Technologies 홈페이지, http://www.yardarmtech.com/ (2023년 5월 8일 최종검색).

79) 증거자료로 활용하기 위해 폴리스 캠 영상을 다운로드한 건수는 2015년 141건에서 2016년 180건, 2017년 63건, 2018년 13건, 2019년 31건, 2020년 2건, 2021년 7월 기준으로 0건을 기록하였다. "현장경찰 수요 커진 '바디캠'…사비로 해결하는 이유는", THE FACT, 2022년 2월 6일자, http://news.tf.co.kr/read/life/1916708.htm (2023년 5월 8일 최종검색).

80) 경찰청 훈령 제778호, 웨어러블 폴리스캠 시스템 운영 규칙, 법제처 국가법령정보센터, https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2100000030521 (2023년 5월 8일 최종검색).

81) CCTV와 같은 고정형 영상정보처리기기 외에 드론, 자율주행자동차 등을 이용한 이동형 영상정보처리기기의 사용이 증가함에 따라 개정법은 이동형 영상정보처리기기의 정의 규

(2) 확장현실

아랍에미리트와 중국 등에서는 증강현실(AR) 기술이 적용된 스마트안경이 용의자 수색 및 수배차량 식별에 이용되고 있다. 또한 범죄현장이나 시신에 대한 3D 스캐닝을 통해 가상의 사건현장 지도가 구축되는가 하면, 가상부검[82]이 이루어지기도 한다. 2016년 독일에서는 나치 전범 재판에서 VR 기술로 아우슈비츠 수용소를 재현한 영상을 활용해 유죄판결이 내려졌다.[83] 2018년 중국 베이징에서도 살인사건 재판 과정에서 유일한 목격자의 증언을 듣는 데에 VR이 활용되면서 이목이 집중된 바 있다.[84][85] VR을 통해 범죄현장을 재현하여 재판에 활용하는 것을 넘어 메타버

정을 두었고(개인정보 보호법 제2조 제7호의2), 이동형 영상정보처리기기로 공개된 장소에서 업무를 목적으로 사람 또는 그 사람과 관련된 사물의 영상을 촬영할 수 없도록 원칙적으로 금지하되, 정보주체의 동의를 받은 경우나 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우 등에는 예외적으로 촬영할 수 있도록 하고, 촬영 시에는 불빛이나 소리 및 안내판 등으로 촬영 사실을 표시하도록 하는 등 이동형 영상정보처리기기의 운영 기준 등을 정하였다(개인정보 보호법 제25조의2).

82) 가상부검(Virtopsy)은 '가상'을 뜻하는 'virtual'과 '부검'을 의미하는 'autopsy'가 조합된 신조어이다. Sabine Dobel, "Mit Virtual Reality dem Verbrechen auf der Spur", Welt 2017. 1. 23., https://www.welt.de/regionales/bayern/article161438809/Mit-Virtual-Reality-dem-Verbrechen-auf-der-Spur.html (2023년 5월 8일 최종검색).

83) 1942년부터 1944년 6월까지 수용소의 경비원으로 일하면서 17만여 명의 유대인 학살을 방조한 혐의로 기소된 라인홀트 하닝(Reinhold Hanning)은 자신의 지위나 근무 지역을 고려할 때 아우슈비츠 내 다른 지역에서 발생한 범죄사실을 알 수 없었다고 주장했다. 그러나 실제 아우슈비츠 수용소의 시설과 주변 환경 및 주변 도로와 철도까지 3차원으로 구현된 영상에 의할 때 그가 근무했던 감시탑에서 수용소 내 화장터를 볼 수 있었다는 점이 입증되면서 징역 5년형을 선고받았다. 실제 아우슈비츠의 가스실과 화장터는 모두 사라졌으나 제작자들은 아우슈비츠 기록 보관소에서 파괴된 건물들의 설계도를 찾아냈고, 이에 기반하여 VR 영상을 구현할 수 있었다고 한다. 특히 판결 당시 재판장은 VR 영상으로 구현된 3D 모델 덕분에 피고인이 감시탑에서 근무하면서 무엇을 보았는지를 파악할 수 있었다고 말했다. Marc Cieslak, "Virtual reality to aid Auschwitz war trials of concentration camp guards", BBC, 2016. 11. 20., https://www.bbc.com/news/technology-38026007 (2023년 5월 8일 최종검색.

84) 증인이 VR 헤드셋을 착용하고 컨트롤러를 조작하면 법정 내 사람들은 스크린을 통해 VR 속 화면을 확인하는 방식이었다. Jonathan Nafarrete, "Chinese Courtroom Uses VR to Revisit Crime Scene", VRScout, 2018. 3. 2., https://vrscout.com/news/chinese-courtroom-vr-crime-scene/ (2023년 5월 8일 최종검색).

85) 이와 관련해서는 피고인이 자해를 하거나 피해자를 찌르는 등의 세부 사항이 증인의 진술에 의해 밝혀진 것이 아니라 이미 VR 영상에 포함됨으로써 증인의 진술을 부당하게 유도했다는 문제가 지적되었다. 梁雅丽, "VR技术对法庭审判和刑事辩护的可能影响", 北京法和家网络科技有限公司, 2019. 7. 26., https://www.fahejia.com/view?id=95b97ad0dc834c6a8f1ce3

스 내에서 재판이 이루어질 가능성도 고려해볼 수 있다. 이는 영상재판의 차세대 버전으로 논의될 수 있는데, 향후 법원이 안정적인 메타버스 플랫폼을 구축할 수 있다면, 현존감과 몰입감이 높은 메타버스에서 재판이 진행될 수 있을 것이나, 형사재판의 경우 그 범위는 여전히 제한적일 것이다.

한편 2020년 8월 정부는 수사기관이 용의자 및 수배차량 조회를 효율적으로 수행할 수 있도록 증강현실 기술이 적용된 스마트 안경 도입 방안을 모색할 것이라고 밝혔다.[86] 스마트 안경의 효시격인 구글 글래스에 대해서는 무단 사진이나 동영상 촬영 등으로 인한 사생활 침해 우려가 제기되었고, 시야에 영향을 주기 때문에 안전성의 문제가 지적되었다. 그러나 이미 대중화된 스마트폰을 가지고도 동의 없는 사진 촬영이나 녹음 등이 가능하고, 운전 중에 손으로 작동시켜야 하는 기기를 사용하는 것에 비해 구글 글래스를 착용하는 것이 덜 위험하다는 반론도 제기될 수 있다. 2012년 구글 글래스가 출시된 지 10여 년이 지난 지금, 새로운 디바이스에 대한 시민들의 거부감이 얼마나 감소되었는지는 알 수 없으나, 스마트 안경은 이미 성장 정체기에 접어든 스마트폰을 이을 차세대 IT 기기로 거론되고 있다. 양 손을 자유롭게 사용할 수 없는 상황에서 업무 매뉴얼이나 긴급 자료 등을 확인하고, 수배차량을 조회하는 기능 등은 사생활 침해의 논란 없이 활용될 수 있다. 다만 현행 규정상 신원확인이나 수배차량 조회 등과 같은 긴급사실 조회는 관계 경찰관서간 직접 경찰전화나 전신 등으로 해야 하는바,[87] 현장 경찰이 스마트안경을 이용하여 수배차량 조회 등을 할 수 있도록 관련 규정이 정비되어야 한다. 경찰업무에 스마트 안경을 활용하고 있는 중국이나 두바이에서는 이 장비가 안면인식을 통한 신원확인 조회에 탁월한 성과를 내고 있는 것으로 알려져 있다. 우리나라의 경우 경찰이 스마트 안경을 활용해 수배차량의 조회를 넘어 안면인식을 통한 신원확인 조회까지 하는 것은 거센 국민적 반발에 가로막혀 시행될 수 없으리라 예상된다. 아울러 스마트 안경에 어느 정도의 기능을 탑재할 것인지에 따라 관련 법규의 정비 범위도 달라질 것이다.

2b4166da2b&userid=&type=1 (2023년 5월 8일 최종검색).

86) "정세균 국무총리, 제1차 규제혁신 현장대화 개최- 정총리 규제혁신 10대 의제(아젠다) 첫 현장대화, 가상·증강현실 선제적 규제혁신 이행안(로드맵) 발표 -", 관계부처 합동 보도자료, 2020년 8월 3일자, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&bbsSeqNo=94&nttSeqNo=3008738 (2023년 5월 8일 최종검색).

87) 범죄수사자료 조회규칙 제4조(조회처) 범죄수사자료 조회는 전국 경찰관서의 각종 수사조회 시스템을 이용하고, 긴급사실조회는 관계 경찰관서간 직접 경찰전화·전신 등으로 한다.

V. 결 론

4차 산업혁명 시대에 신기술은 형사사법 분야에 다양한 도전 과제를 던지고 있다. 첨단기술의 발전은 인간의 삶을 보다 풍요롭게 만들고 다양한 편의를 제공해주지만, 그 기술이 범죄에 악용될 경우 사회의 안녕과 질서 유지를 위협하는 새로운 위험요소로 작용한다. 일례로 개인 식별의 수단으로 이용되기 시작했던 DNA 감식은 기술이 발전함에 따라서 동식물과 미생물에까지 확대되어 수사에 이용되고 있고, 대조할 DNA가 없더라도 사건 현장에서 발견된 DNA만으로 그 해독 정보를 담은 mRNA를 분석함으로써 범인을 추정할 수 있게 되었다.[88] 나아가 2012년 크리스퍼 기술이 개발되면서 DNA 정보를 자르고 붙여서 문제를 해결할 수 있는 유전자 편집(genome editing) 기술이 본격적으로 발전하고 있는데, 향후 성폭력범죄를 저지른 용의자가 자신의 유전자를 편집한다면 형사절차에서 DNA는 더 이상 신뢰성 높은 증거로 활용될 수 없을 수 있다. 반면 범죄수사 및 재판 과정에 첨단기술이 활용될 경우 실체적 진실 발견이 용이하게 이루어질 수 있다. 다만 국민들의 인권의식이 높아지면서 형사사법 분야에 새로운 기술이 도입될 때마다 프라이버시 등 각종 권리나 자유 침해 논란이 야기되고 있다. 이에 해당 기술의 특징과 활용 목적 등을 분석하여 적용 가능 여부를 평가하고, 권리 보호와의 균형점을 찾아서 이를 제도화시키는 일은 앞으로도 형사사법 분야의 과제로 남게 될 것이다. 한편 2018년 Carpenter v. United States 판결에서 법원은 1944년 Northwest Airlines, Inc. v. Minnesota 판결[89]에서 비행기와 라디오의 새로운 혁신을 감안할 때, 법원은 “미래를 당황스럽게(embarrass the future)” 만들지 않도록 그러한 혁신과 관련된 사안들을 신중히 다루어야 한다고 했던 프랭크푸르터(Frankfruter) 대법관의 말을 인용하였다.[90] 과학기술의 발전에 따른 형사절차의 변화와 헌법적 논의를 전개함에 있어서도 미래를 당황스럽게 만들지 않아야 할 것인바, 기술에 대한 이해와 그 발전 동향에 대한 면밀한 분석을 토대로 보다 적극적이고 선도적인 헌법적·형사법적 논의가 이어지기를 기대한다.

---

88) “‘최후의 목격자’ DNA, 범인 몽타주도 그린다: 사람의 얼굴 3차원으로 촬영…얼굴 특징과 DNA 차이 분석: 노화에 따른 외형변화도 추정…범행 방식도 알 수 있어 기대”, 한국경제 2017년 9월 3일자, http://news.hankyung.com/article/2017090388461 (2023년 5월 8일 최종검색).

89) Northwest Airlines, Inc. v. Minnesota, 322 US 292 (1944), at 300.

90) Carpenter v. United States, No. 16-402, 585 U.S. (2018), at 2220.

【토론문】

“과학기술의 발전에 따른 형사절차상 변화와 헌법적 쟁점”에 대한 토론문

이 재 홍*

1. 들어가는 말

Chat GPT를 비롯하여 과학기술 발전에 따른 새로운 산물들이 우리사회에 연일 놀라움을 안겨 주는 상황에서, 윤지영 선임연구위원님의 발표문을 통해 형사절차 역시 예외가 아님을 알게 되었습니다. 또한 헌법적인 관점에서 그러한 변화를 어떻게 평가하여야 하는지에 관해서도 생각해볼 수 있는 계기가 되어 감사드립니다.

발표문을 읽는 동안 처음 가보는 여행지를 다니는 듯한 신기함을 느끼는 시간이 많았습니다. 지정토론을 통해 선임연구위원님의 발표문을 통해 생각해 본 내용 몇 가지를 공유해 보고자 합니다.

2. 아이폰의 압수 관련(발표문 9-11면)

발표문 9-11면에는 수사기관이 아이폰의 비밀번호를 풀지 못하여 압수의 목적을 달성하지 못하는 경우 수사기관이 ‘법원을 통해 아이폰 잠금 해제를 강제할 수 있는지’라는 흥미로운 쟁점에 관한 내용이 소개됩니다. 미국의 경우 소송이 이루어졌다가 연방수사국의 취하로 종결되어 아쉬움이 남습니다만, 이 부분을 읽으면서 든 근본적인 의문은 종래의 전통적인 압수물에 관한 관점에서 이 문제에 접근하는 것이 가능하지는 않을지입니다.

* 이화여자대학교 법학전문대학원 교수

가. 압수영장의 효력 범위 관련

만약 자물쇠로 잠금장치가 된 일기장(예전에 초등학교에 다닐 무렵에 이런 것이 유행을 했습니다)에 대한 압수영장이 발부되었다면, 그 영장의 효력 범위에는 일기장 자물쇠를 여는 열쇠가 포함된다고 보아야 할 것입니다. 일기장의 압수는 그 안에 있는 정보를 지득하기 위한 것인데, 잠금장치가 되어 있는지 여부를 수사기관이나 영장을 발부하는 법원이 미리 알 수는 없는 노릇이므로, 수사관이 "일기장"에 대해 발부된 영장을 집행하면서 일기장에 자물쇠가 걸려 있는 것을 발견했고, 열쇠가 옆에 놓여 있었다면 그 열쇠까지 압수할 수 있다고 보는 것이 통례일 것입니다.[1)]

마찬가지 이치로 휴대전화에 잠금 기능이 설정되어 있는지 여부는 압수의 집행에 나아가기 전까지는 수사기관이나 법원이 알 수가 없는 노릇이므로, 휴대전화에 대해 발부된 압수영장의 효력 범위에는 그 비밀번호까지 포함되는 것으로 구성할 수는 없을런지요. 물론 휴대전화를 상해의 도구로 활용한 범죄처럼 휴대전화라는 물리적 실체가 압수의 대상인 것이 아니라 그 안에 저장된 정보가 필요해서 발부된 압수영장임을 논의의 전제로 합니다.

구체적으로 아래와 같은 의문들이 생깁니다. ① 피의자가 휴대전화 비밀번호를 적어 둔 메모지가 책상 안에서 발견된 경우 이것을 압수하는 것을 위법으로 볼 수 있을지요. ② 애플이나 삼성 등 휴대전화 제조사가 비밀번호 정보를 보관하고 있다면, 이는 비밀 일기장 판매 회사가 판매한 일기장 각각의 열쇠의 복사본을 보관하고 있는 상황과 유사합니다. 법관이 애플이나 삼성 등 휴대전화 제조사가 보관하고 있는 비밀번호가 저장된 서버에 대한 압수영장을 발부한다거나 입법자가 그러한 정보를 강제로 취득하는 것을 목적으로 하는 특수한 영장제도(발표문 15-16면에 소개된 미국의 클라우드법에 유사한 제도)를 만드는 것이 가능할지요.

나. 생체정보를 활용한 잠금해제 관련

한편 휴대전화의 잠금이 비밀번호가 아니라 안면인식, 지문인식 등 생체정보를 이용해 설정된 경우에는 아래와 같은 의문이 생깁니다. 수사기관이 휴대전화 잠금을 해제할 수 있는 생체정보에 대하여 별도의 압수영장을 발부받는 방법이나 혹은 경찰이 보관하고 있는 지문정보를 이용하여 3D 프린팅 기술을 통해 모형 손가락을 만

1) 법리 구성은 주물-종물 관계 등 여러 가지로 가능할 것 같습니다.

들어 내어 휴대전화의 잠금해제를 하는 것이 현행 형사소송 관련 법령상 위법인지 의문입니다.[2)]

다. 비밀번호 진술의무 부과와 진술거부권 관련

조금 더 진술거부권에 직접 관련된 주제로는, 만약 입법자가 휴대폰 소유자(반드시 피의자인 것은 아닙니다)에게 비밀번호 정보를 제공할 의무를 부과하고 미이행시 일정한 불이익을 주는 가상의 법률(이하 '가상의 비밀번호제공법')을 입법자가 만든다면, 그러한 법률이 진술거부권을 침해하는지를 상정해 볼 수 있습니다. 이는 그러한 법률에 의해 헌법 제12조 제2항의 진술거부권의 제한이 있는지,[3)] 있다면 그러한 제한이 헌법상 정당화되는지의 문제가 됩니다.[4)]

혈중알콜농도는 자신에게 형사상 불리한 정보이지만 이를 제공하는 음주측정행위는 진술이 아니어서 음주측정 강제에 의해서는 진술거부권의 제한 자체가 없다는 결정례에서 알 수 있듯이,[5)] 어떠한 행위가 진술거부권의 보호영역에 들어오려면 "자신에게 형사상 불리한 정보의 제공"만으로는 부족하고 그 정보제공의 형태가

---

2) 이환우, 생체정보 취득을 통한 스마트폰 전자정보 접근방안 연구, 서울대학교 대학원 석사학위논문(2019. 2.), 32-33면은 아래와 같은 내용의 형사소송법 제120조 제1항을 근거로 이것이 허용되어야 한다는 견해입니다.
형사소송법 제120조(집행과 필요한 처분) ①압수·수색영장의 집행에 있어서는 건정을 열거나 개봉 기타 필요한 처분을 할 수 있다.
②전항의 처분은 압수물에 대하여도 할 수 있다.

3) 진술거부권의 제한이 있는지의 문제는 진술거부권의 보호영역의 문제입니다. 이에 관해서는 "진술거부권의 보호대상이 되는 진술이라 함은 언어적 표출 즉, 개인의 생각이나 지식, 경험사실을 정신작용의 일환인 언어를 통하여 표출하는 것을 의미하고, 형사상 자신에게 불이익이 될 수 있는 진술이므로 범죄의 성립과 양형에서의 불리한 사실 등을 말하는 것이며, 그 진술내용이 자기의 형사책임에 관련되는 것일 것을 전제로 한다."는 결정례(헌재 2014. 9. 25. 2013헌마11, 판례집 26-2상, 593, 604-605)를 참조할 수 있습니다.

4) 이는 결국 과잉금지원칙(헌법 제37조 제2항) 위반의 문제가 될 것입니다.

5) "헌법 제12조 제2항은 진술거부권을 보장하고 있으나, 여기서 "진술"이라함은 생각이나 지식, 경험사실을 정신작용의 일환인 언어를 통하여 표출하는 것을 의미하는데 반해, 도로교통법 제41조 제2항에 규정된 음주측정은 호흡측정기에 입을 대고 호흡을 불어 넣음으로써 신체의 물리적, 사실적 상태를 그대로 드러내는 행위에 불과하므로 이를 두고 "진술"이라 할 수 없고, 따라서 주취운전의 혐의자에게 호흡측정기에 의한 주취 여부의 측정에 응할 것을 요구하고 이에 불응할 경우 처벌한다고 하여도 이는 형사상 불리한 "진술"을 강요하는 것에 해당한다고 할 수 없으므로 헌법 제12조 제2항의 진술거부권이 제한되는 것은 아니다."(헌재 1997. 3. 27. 96헌가11, 판례집 9-1, 245, 257-258)

“진술”이어야 합니다.[6] 휴대전화 소유자에게 비밀번호 정보를 제공할 의무를 부과하는 것은 진술 이외의 형태로는 상정하기 어려우므로 가상의 비밀번호제공법에 의한 진술거부권의 제한은 인정할 수 있을 것 같습니다.

한편, 헌법재판소 결정례에 따르면 정치자금에 관한 장부를 진실하게 기재할 의무를 부과하고 그에 위반할 경우에 형사처벌을 하는 조항은 진술거부권의 제한이지만 과잉금지원칙에 반하지 않아 진술거부권 침해는 아니므로 합헌입니다.[7] 즉, 정치자금법 위반이라는 범죄사실을 장부에 기록하고 선관위에 보고하는 방식으로 진술할 의무를 부과하고, 불이행시 형사처벌을 하는 법률조항이 진술거부권을 침해하지 않는다는 것입니다. 그렇다면 가상의 비밀번호제공법이 사회적 해악이 큰 특정 범죄, 예컨대 마약이나 인신매매에 사용된 전화번호에 해당하는 휴대전화 단말기에 한하여 휴대전화기 소유자에게 그 비밀번호를 진술하도록 하고 이에 응하지 않을 경우 형사처벌을 하도록 하고, 수사기관은 소유자가 그와 같이 진술한 비밀번호를 이용해 해당 휴대전화에 저장된 정보 중 마약, 인신매매에 관한 정보만을 지득할 수 있도록 한다고 규율한다면 이것을 과잉금지원칙에 위반되어 진술거부권을 침해하는 법률로

---

6) 즉, 진술거부권은 자기부죄금지뿐 아니라 자유로운 의사형성과 표현을 보호하는 권리이고 양자는 OR 관계가 아니라 AND 관계에 있습니다. 이러한 관점에서 진술거부권의 본질은 사상의 자유, 표현의 자유에도 닿아 있습니다.

7) 정치자금의 수입·지출에 관한 내역을 회계장부에 허위 기재하거나 관할 선거관리위원회에 허위 보고한 정당의 회계책임자를 형사처벌하는 조항이 진술거부권을 침해하는 지에 관하여, “구 정치자금에관한법률(2004. 3. 12. 법률 제7191호로 개정되기 전의 것, 이하 ‘정치자금법’) 제31조 제1호 중 제22조 제1항의 허위 기재 부분과 같은 호 중 제24조 제1항의 허위보고 부분은 궁극적으로 정치자금의 투명성을 확보하여 민주정치의 건전한 발전을 도모하려는 것으로서 그 입법목적이 정당하고, 위 조항들이 규정하고 있는 정치자금에 대한 정확한 수입과 지출의 기재·신고에 의하여 정당의 수입과 지출에 관하여 정확한 정보를 얻고 이를 검증할 수 있게 되므로, 이는 위 입법목적과 밀접한 관련을 갖는 적절한 수단이다. 또한, 정치자금에 관한 사무를 처리하는 선거관리위원회가 모든 정당·후원회·국회의원 등의 모든 정치자금 내역을 파악한다는 것은 거의 불가능에 가까우므로 만일 불법 정치자금의 수수 내역을 기재하고 이를 신고하는 조항이 없다면 ‘정치자금의 투명성 확보’라는 정치자금법 본연의 목적을 달성할 수 없게 된다는 점에서 위 조항들의 시행은 정치자금법의 입법목적을 달성하기 위한 필수불가결한 조치라고 할 것이고, 달리 이보다 진술거부권을 덜 침해하는 방안을 현실적으로 찾을 수 없다. 마지막으로, 위 조항들을 통하여 달성하고자 하는 정치자금의 투명한 공개라는 공익은 불법 정치자금을 수수한 사실을 회계장부에 기재하고 신고해야 할 의무를 지키지 않은 채 진술거부권을 주장하는 사익보다 우월하다. 결국, 정당의 회계책임자가 불법 정치자금이라도 그 수수 내역을 회계장부에 기재하고 이를 신고할 의무가 있다고 규정하고 있는 위 조항들은 헌법 제12조 제2항이 보장하는 진술거부권을 침해한다고 할 수 없다.”라고 판시한 결정례(헌재 2005. 12. 22. 2004헌바25, 판례집 17-2, 695, 706-708)를 참고할 수 있겠습니다.

볼 수 있을런지요. 또는 형사처벌보다 가벼운 불이익을 가한다면 합헌이라고 볼 수 있을런지요. 예컨대, 마약, 인신매매에 사용된 휴대전화기의 비밀번호를 제공하지 않으면, 기소될 경우 비밀번호 미제공 사실을 피고인에게 불리한 정황증거로 사용할 수 있다는 식의 증거법 규정을 두거나 혹은 과태료나 이행강제금 부과 규정을 둔다면 진술거부권의 침해에 해당되지 않을런지요.

3. 사물인터넷 관련(발표문 22-23면)

발표문 22-23면에는 사물인터넷 중 미국의 Shot Spotter 시스템과 Smart Gun에 대한 내용이 소개되어 있습니다. 특히 Shot Spotter 시스템은 놀랍고도 무릎을 치게 하는 기술이었습니다. 이는 피의자 스스로 공개한 정보인 '총성'이라는 음파 정보를 수집하여 총기발사위치를 추적하므로, 임의수사에 해당됩니다. 따라서 영장주의/진술거부권이나 사생활의 비밀과 자유, 혹은 개인정보자기결정권 침해 등의 문제는 발생하지 않을 것입니다. 그러나 사물인터넷에 의해 수집된 정보 중 정보주체가 공개하지 않은 정보를 수사기관이 취득하는 경우에는 위와 같은 문제가 발생합니다.

Shot Spotter 시스템이 그러한 문제 상황의 단초를 제공합니다. 이 사물인터넷 시스템은 경찰관들을 대상으로 한 것이지만, 만약 이를 사인을 대상으로 시행한다면 그것이 헌법상 허용될 것인지 허용된다면 그 한계는 어떠한지가 문제되리라 생각합니다. 예컨대 총기와 같은 위험성이 있는 물건에 대해서는 그 소유자가 누구인지를 불문하고 위치정보를 파악할 수 있는 장치를 반드시 부착하도록 하고, 그 위치정보에 국가가 수사 목적으로 접근하는 것이 허용될지의 문제입니다. 위험성의 범위를 어떻게 설정하는지에 따라 총기와 같은 무기뿐 아니라 자동차까지도 그 범주에 들어갈 수 있으리라 생각이 됩니다.

현행법 체계의 관점에서 보자면, 사물인터넷도 정보통신망에의 접속을 필수적인 요소로 할 것이므로 사물인터넷 장치가 부착된 물건을 '정보통신기기'로 볼 수 있다면, 그 물건의 위치정보는 통신비밀보호법상 통신사실확인자료 중 위치(접속지) 추적자료(법 제2조 11호 바목[8])에 대한 통신사실확인자료제공허가 절차의 대상이 될

8) 11. "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다.
사. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신

수도 있어 보입니다. 이에 관한 실무례나 학계의 논의가 있는지 궁금합니다.

4. 맺는 말

발표문을 통해 새로운 내용을 많이 알 수 있었습니다. 감사드립니다. ‘새로운 변화를 기존의 틀로 설명해 볼 수는 없는지’라는 관점에서 몇 가지 생각해 본 점을 토론문에 담았습니다. 미래지향적인 해결을 도모하는 데에는 부족할 수 있겠지만, 이 주제에 관한 선임연구위원님의 향후 연구에 도움이 되시기 바라며 지정토론을 마칩니다. 감사합니다.

기기의 위치를 확인할 수 있는 접속지의 추적자료

【토론문】

“과학기술의 발전에 따른 형사절차상 변화와 헌법적 쟁점”에 대한 토론문

김 현 귀*

과학기술의 발전에 따른 형사절차의 변화와 헌법적 쟁점에 대해 망라적으로 정리해 주신 발표자의 노고에 감사드립니다. 망라해주신 주제 하나하나가 좋은 논문주제가 될 것으로 보입니다. 저는 각 주제에 관하여 제가 가진 생각을 몇 가지 덧붙이는 것으로 이 토론을 갈음하고자 합니다.

과학기술발전을 대하는 자세

먼저 미래를 당황스럽게 만들지 않도록 혁신과 관련된 사안들을 신중히 다루어야 한다는 프랑크푸르터 연방대법관의 말은 이 모든 주제를 관통할 수 있는 핵심적인 교훈이라고 생각합니다. 가령, 프라이버시 보호기술과 익명화 기술이 중요한 범죄수사, 특히 다크넷 수사에 있어서 큰 장애물이 된다는 것은 공지의 사실입니다. 그렇다고 이를 극복하기 위해 법으로 백도어 제공을 강제한다거나 익명화 기술을 금지시킨다면 이는 과학기술의 발전으로 발생한 장애물을 법을 이용하여 극복하려고 하는 것입니다. 물론 그런 장애물을 제거하는 것이 실체적 진실을 발견하려는 데 도움이 될 것 같아 보이지만, 이건 너무 뻔하고 쉬운 잘못된 해결책이 될 가능성이 큽니다. 정책이 있으면 항상 대책이 있듯이, 이는 그저 이용자들의 소위 ‘사이버 망명’ 같은 물의를 일으킬 수 있습니다. 또 법적 규제를 회피하는 더 교묘한 기술과 방법을 발전시켜서 결국은 그 규제는 그저 광범위한 프라이버시 침해만 유발할 가능성이 큽니다. 그러니 과학기술의 발전과 혁신에 대해서는 신중하게 대응해야만 합니다.

* 한국해양대학교 해사법학부 부교수

효율성이 아니라 적법한 절차

과학기술이 발전하더라도 변하지 않는 것이 있다면, 그것은 국가의 법집행과정은 국민의 자유와 권리를 보호하기 위하여 법치국가원리와 적법절차원리에 의하여 제한되어야 한다는 것입니다. 이는 우리 헌법이 요구하고 있는 것이고 과학기술이 발전하였다고 하여도 결코 소홀하게 취급될 내용은 아니라는 것입니다. 그런 의미에서 거짓말탐지기나 범죄예측 프로그램 또는 Compas 같은 재범예측 프로그램이 아무리 정확도나 신뢰도가 높다고 하더라도 법관의 자유심증의 범위에서 활용되는 정황증거에 머물러야 합니다. 알고리즘에 의한 판단은 효율적일지는 몰라도 우리는 그것이 공정한 재판이나 적법한 절차에 의한 판단이라고 보지 않기 때문입니다. 공정한 재판이나 적법한 절차는 판단의 효율성이나 정확성이 아니라 당사자에게 공평한 기회와 절차를 제공하고 중립적이고 독립적인 법관에 의한 판단 등으로 구성되기 때문입니다.

정보권력의 문제와 법의 지배

DNA가 확실한 증거수단이 될 수 있다고 하더라도 그런 이유만으로 전 국민을 상대로 그런 데이터베이스를 구축하는 것이 정당화 될 수 없습니다. 그리고 DAS가 수사의 효율성을 증진시킬 수 있다고 하더라도 국민생활에 대한 광범위한 감시망으로 작동하여서는 안됩니다. 또 폴리스캠이나 드론, 로봇기술, 스마트 안경 등을 활용한 경찰장비에 있어서 혁신적인 변화도 국민의 안전을 확보하기 위한 경찰행정과 수사에 있어서 도움이 되고 필요하겠지만, 역시 그것이 광범위한 데이터베이스에 기초하여 국민생활을 감시하는 수단이 되어서는 안 됩니다. 그 이유는 그것이 정보권력의 문제와 연결되기 때문입니다.

우리의 법치주의는 기본적으로 국민의 자유와 권리를 보호하기 위하여 정부의 권력을 제한하는 데 그 목적이 있습니다. 법의 지배는 ‘법을 이용한 지배’가 아니라 ‘법에 의한 지배’입니다. 그런데 정부에게 너무나 강력하고 효율적인 그래서 반론이 불가능한 무기가 쥐어진다면, 법으로 이 권력을 통제할 수 없습니다. 반론가능성은 민주주의와 건전한 토론의 전제조건입니다. 그런데 정보의 불균형은 반론을 불가능하게 만들고 시민들을 수동적인 피지배자로 만듭니다. 과학기술을 이용한 수사나 공

권력 행사가 효율적일지는 몰라도, 그것이 정보와 지식에 대한 국가의 독점에서 출발한다면 법의 지배를 위협할 수 있습니다.

영장주의와 적법한 절차

헌법상 적법한 절차의 보장은 핸드폰과 같은 전자기기에 저장된 정보에 대한 압수수색이 단순히 물건을 압수수색하는 것과 달리 취급되어야 하는 이유이고, 메일서버에 대한 압수수색에서 피의자 등의 참여권을 보장해야 하는 이유이며, 패킷감청이나 통신사실 확인자료 제공요청을 통한 기지국 수사가 기존의 전화에 대한 통신감청이나 통신사실 확인자료 제공요청과 달리 취급되어야 하는 이유이면서, 전기통신망법상 통신자료가 제공된 자에게 적절한 고지를 해야 하는 이유이기도 합니다.

이 모든 사건에서 영장주의보다는 적법한 절차가 더 주목을 받는 이유는, 제3자가 보유 또는 운영하는 정보 및 기기에 접근하여 정보를 얻는 것이 강제수사로 보기에 애매한 상황인데다 이 상황에서 법관에게 그 판단을 유보하는 것보다 당사자가 이를 알고 직접 대응하게 하는 것이 더 효과적인 기본권 보장수단이기 때문이라고 봅니다. 강제수사로 보고 영장주의를 적용하는 것은 정보주체의 권리를 보호하는 것이 아니라 오히려 수사기관에게 정당화 할 수 있는 절차를 제공하고 정보를 관리하는 제3자에게 면책을 제공할 뿐입니다. 이들에게 정보를 취득하고 제공할 절차를 마련해 주는 게 중요한 것이 아니라 정보주체의 권리를 보장하는 것이 더 중요하니, 이 상황에서는 정보를 관리하는 제3자가 정보주체를 의식하도록 하고 그들의 고객인 이용자의 반응을 두려워하도록 만드는 것이 차라리 정답입니다. 그래서 정보주체가 자신의 정보에 대해 통제할 수 있도록 적법한 절차를 보장하는 것이 정보주체의 권리를 보호하는 가장 기본이 되는 방법이라고 생각합니다.

헌법적 형사절차

헌법상 적법한 절차의 보장은 헌법적 형사절차의 가장 핵심적인 내용이라고 생각합니다. 물론 적법한 절차의 보장이 때로는 실체적 진실을 발견하기 위한 수사에 있어서 장애물이 되는 것으로 보일 수도 있습니다. 그러나 기본적으로 모든 국가의 공권력은 국법에 근거하고 적법한 절차에 의하여 행사되어야 합니다. 실체적 진실을

발견하기 위한 수사도 기본적으로 적법한 절차에 의하여야 합니다. 그리고 여기서 법은 법집행자도 입법자도 모두 구속하는 규범입니다. 그러니 적법한 절차가 실체적 진실의 발견에 방해가 될 수는 없습니다.

【제3주제】

모바일 전자증거 압수수색과 적법절차, 최근 쟁점과 법원 판례의 동향

오 현 석*

1. 서론

전자정보 수집절차가 적법하다 하려면, 영장에 의한 압수의 경우 영장의 집행 이전에 영장을 제시하여야 하고, 그 영장 기재에 부합하고 혐의사실과 '관련성' 있는 정보에 한하여 집행이 이루어져야 한다. 임의제출에 의한 압수의 경우라면 전자정보 제출의 임의성이 있어야 할 뿐만 아니라 그 제출의 범위에 관해 제출자의 의사가 불분명할 때에는 압수의 동기가 된 범죄혐의사실과의 관련성이 있는 최소한의 전자정보만을 압수하여야 한다. 이러한 전자정보의 압수과정에 피압수자의 실질적 참여권이 보장되어야 하고, 전자정보의 파일 명세가 상세히 기재된 목록을 교부하여야 한다.

* 부장판사, 대전지방법원

본고는, 모바일 전자증거 압수수색의 적법절차에 관하여 최근 다양하게 등장한 쟁점들이 무엇인지 일람하고, 관련된 법원 판결례를 함께 살펴본다.

2. 무관정보 혼재의 문제

2011. 7. 18. 개정된 형사소송법 제106조 제1항 및 제109조 제1항은 '피고사건과의 관계가 있다고 인정할 수 있는 것에 한정'하여 압수 또는 수색할 수 있다고 규정하고, 제215조는 '해당 사건과 관계가 있다고 인정할 수 있는 것에 한정'하여 압수, 수색할 수 있다고 규정하여, 범죄혐의 관련성 원칙을 명문화하였다.

전자정보는 방대함, 대량성, 풍부함을 특징으로 한다. 오늘날 개인·단체·기업은 시시각각 막대한 양의 개인정보, 업무 정보를 생성하며, 저장매체는 대량의 정보를 저장하기 쉽도록 매우 작아졌고 극히 저렴하다. 인터넷 기업들은 온라인에서 고객 개개인의 활동을 면밀히 추적하여 성향파악 광고 등에 활용하려고 방대한 정보를 수집하기에 개인정보보호법 쟁점들이 다수 제기되며, 수사기관이 압수·수색하는 저장매체에 사건과 무관한, 영업비밀, 사생활 등이 대량으로 혼재되어 있기에 영장주의 위반 문제가 자주 제기된다. 영장 실무는 오래전부터 전자정보상세목록을 반드시 피압수자에게 제공토록 명하고 있으나[1], 전자정보상세목록에 파일 단위로 path/filename이 나열되는데, 비할당영역의 전부 또는 일부에서 어떤 무관 정보가 압수되었는지는 이 목록에서 드러나지 아니한다는 점, 사람이 복잡한 path/filename을 식별하기가 쉽지 아니하여 그 목록을 받아도 방어권 행사에 활용하기 어려운 경우가 많다는 점, 예컨대 모바일 카카오톡 앱은 모든 대화 정보를 하나의 파일(SQLite DB 형식인 KakaoTalk.db 파일) 안에 집중적으로 저장하므로 그 파일명 KakaoTalk.db만으로는 해당 대화가 무엇인지는커녕 해당 대화방이 무엇인지조차 특정되지 아니한다는 점에서 그 목록의 효능에 일정한 한계도 있다.[2]

---

1) 서울중앙지법 영장전담판사들은 적어도 2011. 8. 이래로 그렇게 해 왔다. 압수된 정보의 상세목록에는 정보의 파일 명세가 특정되어 있어야 한다는 대법원 2018. 2. 8. 선고 2017도13263 판결, 대법원은 2020. 11. 17. 자 2019모291 결정, 대법원 2022. 1. 14. 자 2021모1586 결정 참조.

2) 예컨대 문자메시지 앱은 mmssms.db 파일에, 카카오톡 앱은 KakaoTalk.db 파일에 모두 저장한다.

스마트폰이 성범죄 영상물 촬영 등의 범행에 직접적인 범행도구로 사용된 경우에는, 휴대전화 자체가 법 제219조, 제106조에 규정된 '증거물 또는 몰수할 것으로 사료하는 물건'에 해당하여 이를 압수할 수 있다는 데에 의문의 여지가 없다.

그러나 일반적으로는 스마트폰에 저장된 전자정보는 그것이 압수 대상에 해당하는지 별도로 신중히 보아야 하며, 무관 정보가 문제된다. 컴퓨터 하드디스크, 휴대용 플래시메모리장치 등 다른 유형의 정보저장매체와 달리 스마트폰에는 개인의 전화·문자메시지·SNS, 일정, 인터넷 검색기록, 전화번호부, GPS위치정보 등 사생활에 밀접히 관련된 많은 정보가 한데 모여 있다. 혐의사실과 관련성 없는 정보 또는 혐의사실과 무관한 제3자에 관한 정보가 무차별적으로 함께 압수될 위험이 크다. 해당 사용자뿐 아니라 SNS 등으로 연결된 제3자의 기본권, 즉 사생활 비밀·평온, 통신의 자유, 개인정보 자기결정권 등을 과도하게 침해할 우려가 있다. 강제수사에 관한 비례의 원칙이나 범죄혐의 관련성 원칙 등의 법리에 입각하여 압수에 신중을 기하고, 개인정보의 유출이나 별건 수사를 억제할 필요가 있다.

스마트폰 등 모바일 기기의 사용자 데이터 파티션(UserData partition)[3]의 이미지 파일에는 무관 정보, 즉 혐의사실과 무관한 정보가 다량으로 포함되어 있는 경우가 많다. 이미지 파일 저장의 위법성, 장기 보유의 위법성, 별건 압수의 적법 여부 등이 문제된다. 스마트폰은 현장 선별이 곤란한 경우가 많아서 현장 외 선별을 용인할 경우가 많다고는 하겠으나, 수사기관이 무관 정보를 보유하는 것은 압수의 위법성 문제로 직결된다.

수사기관이 무관 정보를 폐기하지 아니한 사안에서, 준항고를 기각한 원심결정을 파기하고 압수가 위법하니 취소되어야 한다고 명한 대법원 2022. 1. 14. 자 2021모1586 결정도 참고할 만하다. 삭제·폐기의무를 위반한 전자정보에 대하여 새롭게 압수·수색영장을 받아 압수할 경우 그 위법성이 치유되는지 여부에 대하여 이를 부정한 결정이기도 하다.

대법원 2022. 1. 14. 자 2021모1586 결정
법원은 압수·수색영장의 집행에 관하여 범죄 혐의사실과 관련 있는 전자정보의 탐

3) 스마트폰, 태블릿 등 모바일 기기의 저장공간은 여러 파티션(분할된 영역)들로 나뉘어 관리되는데, 그중 디지털 포렌식의 대상이 되는 파티션은 사용자 데이터가 저장되는 파티션이다(안드로이드 OS에서는 USERDATA라는 이름의 파티션이다).

색·복제·출력이 완료된 때에는 지체 없이 영장 기재 범죄 혐의사실과 관련이 없는 나머지 전자정보에 대해 삭제·폐기 또는 피압수자 등에게 반환할 것을 정할 수 있다. 수사기관이 범죄 혐의사실과 관련 있는 정보를 선별하여 압수한 후에도 그와 관련이 없는 나머지 정보를 삭제·폐기·반환하지 아니한 채 그대로 보관하고 있다면 범죄 혐의사실과 관련이 없는 부분에 대하여는 압수의 대상이 되는 전자정보의 범위를 넘어서는 전자정보를 영장 없이 압수·수색하여 취득한 것이어서 위법하고, 사후에 법원으로부터 압수·수색영장이 발부되었다거나 피고인이나 변호인이 이를 증거로 함에 동의하였다고 하여 그 위법성이 치유된다고 볼 수 없다.

수사기관이 압수·수색영장에 기재된 범죄 혐의사실과의 관련성에 대한 구분 없이 임의로 전체의 전자정보를 복제·출력하여 이를 보관하여 두고, 그와 같이 선별되지 않은 전자정보에 대해 구체적인 개별 파일 명세를 특정하여 상세목록을 작성하지 않고 '….zip'과 같이 그 내용을 파악할 수 없도록 되어 있는 포괄적인 압축파일만을 기재한 후 이를 전자정보 상세목록이라고 하면서 피압수자 등에게 교부함으로써 범죄 혐의사실과 관련성 없는 정보에 대한 삭제·폐기·반환 등의 조치도 취하지 아니하였다면, 이는 결국 수사기관이 압수·수색영장에 기재된 범죄 혐의사실과 관련된 정보 외에 범죄 혐의사실과 관련이 없어 압수의 대상이 아닌 정보까지 영장 없이 취득하는 것일 뿐만 아니라, 범죄혐의와 관련 있는 압수 정보에 대한 상세목록 작성·교부의무와 범죄혐의와 관련 없는 정보에 대한 삭제·폐기·반환의무를 사실상 형해화하는 결과가 되는 것이어서 영장주의와 적법절차의 원칙을 중대하게 위반한 것으로 봄이 상당하다(만약 수사기관이 혐의사실과 관련 있는 정보만을 선별하였으나 기술적인 문제로 정보 전체를 1개의 파일 등으로 복제하여 저장할 수밖에 없다고 하더라도 적어도 압수목록이나 전자정보 상세목록에 압수의 대상이 되는 전자정보 부분을 구체적으로 특정하고, 위와 같이 파일 전체를 보관할 수밖에 없는 사정을 부기하는 등의 방법을 취할 수 있을 것으로 보인다). 따라서 이와 같은 경우에는 영장 기재 범죄 혐의사실과의 관련성 유무와 상관없이 수사기관이 임의로 전자정보를 복제·출력하여 취득한 정보 전체에 대해 그 압수는 위법한 것으로 취소되어야 한다고 봄이 상당하고, 사후에 법원으로부터 그와 같이 수사기관이 취득하여 보관하고 있는 전자정보 자체에 대해 다시 압수·수색영장이 발부되었다고 하여 달리 볼 수 없다.

2011. 7. 18. 신설된 형사소송법 제106조 제3항은 "법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는

때에는 정보저장매체등을 압수할 수 있다.”고 규정한다. 전자정보에 대한 압수·수색 영장 집행은 원칙적으로 영장 발부의 사유인 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 정보저장매체에 해당 파일을 복제하는 방식으로 이루어져야 한다.

형사소송법 제106조 제3항 단서에서 정한 예외적인 사정이 존재하였다는 점에 대하여는 영장의 집행기관인 수사기관이 이를 구체적으로 증명하여야 하며, 압수목록을 작성할 때에는 준항고 등을 통한 권리구제가 신속하면서도 실질적으로 이루어질 수 있도록 압수방법, 장소, 대상자별로 명확히 구분하여 압수물의 품종, 종류, 명칭, 수량, 외형상 특징 등을 최대한 구체적으로 정확하게 특정하여 기재하여야 한다(대법원 2022. 7. 14. 자 2019모2584 결정).

3. 참여권

검사, 피고인 또는 변호인은 압수·수색영장의 집행에 참여할 수 있다(형사소송법 제121조, 제219조). 압수·수색영장을 집행할 때에는 미리 집행의 일시와 장소를 검사, 피고인 또는 변호인에게 통지하여야 한다.[4] 단, 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 예외로 한다(제122조, 제219조).

전자정보에 대한 압수·수색절차에 참여권 보장이 최초로 논의된 대법원 2011. 5. 26. 자 2009모1190 결정, 그리고 대법원 2015. 7. 16. 자 2011모1839 전원합의체 결정 등이 대표적이고 이미 널리 알려진 판례라고 할 수 있다.

위와 같은 사전 통지는 적법절차에 중요한 의의가 있다. 그런데 제118조는 영장을 반드시 제시해야 한다면서 그 상대방을 ‘처분을 받는 자’라고 달리 표현하였다. 제106조 제2항의 소유자, 소지자 또는 보관자를 가리키는 것으로 보인다. 소유자, 소지자, 보관자 기타 이에 준할 자에게는 압수목록을 교부해야 한다(제129조). 검사 또는 사법경찰관의 압수수색에 위 규정들 모두가 준용된다(제219조; 피고인→피의자).

그런데 2011. 7. 신설된 형사소송법 제106조 제4항의 사후 통지 규정은 ‘정보주

4) 변호인의 참여권에 관하여는, 조은별, “디지털 증거의 압수·수색에 있어 변호인의 참여권”, 경찰법연구 제20권 제3호(2022), 31-61.

체’에게 하라고 하였다. 2011. 3. 제정된 개인정보 보호법에 정의된 용어이다. 형사소송법 제106조 제4항 ‘정보주체’에게 사후 통지해야 한다는 규정에 의하여 ‘정보주체’는 참여권을 가지는가? 2009. 5. 신설된 통신비밀보호법 제9조의3에 의한 한참 나중의 통지만으로 족한가[5], 아니면 그 후 신설된 규정인 제106조 제4항이 우선하는가? 제107조 제3항 본문에 따라서 발신인이나 수신인에게 사전(동시) 통지해야 하는가?

영장이나 수사기관 내부 규정 등에, 정보주체의 참여권은커녕 정보주체에 관하여 명시적 언급이 없다. 종합적이고 정확한 해석이 필요하다.

영장 양식을 보면, 2011년 이래로 지금까지 압수수색영장의 전형적인 기재례는 피압수자(피의자나 변호인, 소유자, 소지자)[6], 참여인(형사소송법 제123조의 책임자, 간수자 등)에게 참여권을 보장한다고만 하였다. 정보주체에 관하여는 언급이 없다.

수사기관 내부 규정을 보자. 대검예규 「디지털 증거의 수집·분석 및 관리 규정」을 살펴보면 제19조 제3항 “제1항 내지 제2항의 선별 과정에서 피압수자 등[7]의 참여를 보장하여야 한다. 피압수자 등이 참여한 경우에는 별지 제5호의 서식에 따라 확인서를 작성토록 한다.”고만 규정했다. 경찰청훈령 「디지털 증거 수집 및 처리 등에 관한 규칙」을 살펴보아도 제11조 제4항 “수사관은 제1항부터 제3항까지의 규정에 따라 디지털 데이터를 압수하는 경우에는 피의자나 변호인, 소유자, 소지자 또는 형사소송법 제123조에 정한 참여인(이하 "피압수자등"이라고 한다)의 참여권을 보장하여야 한다.”고만 정하였다.

정보주체, 즉 ‘이메일 계정 사용자’는 위 소유자, 소지자, 보관자 또는 간수자의 어느 하나에 포섭된다고 보는 것이 옳은가?[8]

---

5) 박경신, “이메일 압수수색의 제문제와 관련 법률개정안들에 대한 평가”, 사법개혁과 세계의 사법제도 [VII], 사법발전재단 (2010), 878; 박경신, “E-메일 압수수색의 제문제와 관련 법률개정안들에 대한 평가”, 인하대학교 법학연구소 법학연구 제13집제2호 (2010. 8.), 278은 메일계정소유자에게 영장제시가 이뤄지지 않는 것은 명백한 불법이라 지적하였고, 여러 입법 개선안을 제시했었다.

6) “법원은 압수할 물건을 지정하여 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다.”고 정한 형사소송법 제106조 제2항에 의한 것이므로, 위 괄호에는 ‘또는 보관자’도 포함되는 것으로 보아야 한다.

7) 같은 대검예규 제9조 제4항 제2호에 피압수자, 형사소송법 제123조에 정한 참여인을 ‘피압수자 등’이라고 한다고 했다. ‘피압수자’에 관한 정의규정은 두지 않았다.

8) ‘이메일 계정 소유자’라는 표현에 대하여는, 정보는 민법 제98조의 물건이 아니어서 엄밀히 말한다면 소유권의 대상은 아니라는 물권법 측면의 지적이 가능해 보이기는 한다. 헌법

① 전기통신사업자인 경우를 보자. 예컨대 웹메일 서비스 회사가 보관하는 참고인의 이메일 정보를 압수하려 할 때의 참여권 보장 대상은, 개인정보처리자·송신자·수신자(공동수신인, Cc, Bcc 참조인 포함 또는 불포함 등 매우 다양한 경우가 나타날 수 있다)·피의자 중 누구라고 보는 것이 가장 합당할 것인가? 대체로 현행 실무는 그 웹메일 서비스 회사의 직원이 영장을 제시받고 집행에 참여한다.[9] 그런데 이메일 계정 사용자가 '처분을 받는 자'에 해당한다고 보아서 현행 실무를 변경해야 올바른 것일까?[10] 추가인가, 대체(교환)인가? 실무를 바꾼다면, 압수의 실효성을 담보할 방안은 무엇인가?[11]

② 경우를 달리 하여, 전기통신사업자가 아니라 임직원이 소속된 회사의 사내메일 계정이나 PC에 파일로 저장된 참고인 이메일을 압수하는 사안을 생각해보자. 영장 제시, 상세목록 교부의 상대방은 회사인가 그 이메일 계정 사용자인 임직원인가? 영장에 이메일 계정 사용자에게 참여권을 보장하도록 기재하여 집행방법을 제한한 사례가 최근 소개되었는데[12], 그런 기재가 있어야만 비로소 그 이메일 계정 사용자의 참여권이 생기는가? 반대로, 그 제한의 법령상 근거는 무엇인가?

재판소 2012. 12. 27. 선고 2011헌바225 결정이 계정 소유자, 정보의 소유자라는 표현을 쓰기는 했으나 의문이 있다.

9) 이숙연, "디지털증거의 압수수색", 법원도서관 재판자료 제123집 (2012), 710 참조.
실제로 대법원 2017. 9. 7. 선고 2015도10648 판결은 '영장 제시는 원본이라야 한다'는 판례인데, 2010. 1. 11. 집행 당시의 사실관계에 관한 3쪽을 읽어보면 제시 상대방이 네이버 주식회사라고 보는 것을 전제하고 있다. 역시 2017. 9. 7. 선고된 2016도11272 판결 사안에서는 1심 판결인 수원지방법원 2016. 1. 14. 선고 2015고단3204 판결의 34쪽 2013. 6. 7. 집행에 관하여 읽어보면 피압수당사자가 주식회사 다음커뮤니케이션이라고 보는 것을 전제하고 있다. 서울중앙지방법원 2016. 7. 14. 선고 2015노2544 판결(상고심: 대법원 2018. 7. 11. 선고 2016도11597 판결) 사안도 마찬가지이다.

10) 오기두는, 정보주체의 참여권을 배제하면 안된다고 지적하면서, 이메일 보전조치를 하도록 전기통신사업자에게 협조요청을 먼저 시도하는 등 가능한 노력을 다해야 하고 그럼으로써 정보주체 참여권을 보장하고 그에게 영장을 제시하는 것이 바람직하다고 한 바 있다. 오기두, "전자정보의 수색·검증, 압수에 관한 개정 형사소송법의 함의", 한국형사소송법학회 형사소송 이론과 실무 제4권 제1호(2012. 6.), 144 [2012. 2. 17. 제1회 한국형사소송법학회 발표자료집, 18]

11) 이메일 계정 사용자의 참여권 보장을 주장하는 조아람, "전자정보에 대한 압수수색절차에서 참여권 보장의 의의", 사법연수원 2017년도 법관연수 어드밴스(Advance) 과정 연구논문집 형사법 신종증거론, 191은 이숙연과 비슷하게 인터넷서비스제공자에 대한 보전명령을 들고 있다.

12) 압수·수색영장 실무 집필위원회, 압수·수색영장 실무 (개정2판) (2016. 6.), 93 (그 사례는 2010년 개정판에는 없었던 내용이며, 전기통신사업자 사안이 아니라고 한다)

어느 경우든 만약 백업본이 있어서 이를 획득했거나 1차적인 추출·이미징을 마침으로써 삭제 위험이 없어진 때부터는 위 관련 계정 사용자들에게 선별에 참여할 권리를 보장해야 하는가? 그 후에라도 계정 사용자들에게 그들의 정보를 왜 보았는지 영장 제시하고, 무슨 정보를 보았는지 상세목록 교부해야 하는 것일까? 과연 언제까지 해야 하는가? 안했다면 위법성이 중한가? 전원에게 해야 하는가? '이메일 계정 사용자'의 범위는 어디까지인가? 그 범위를 정할 때 수색과 압수를 구분하여 정할 것인가?

대법원 2021. 11. 18. 선고 2016도348 판결은 '실질적 피압수자'라는 개념을 도입하였는데, 참여권 보장을 누구에게 해야 하는가 하는 참여권자의 인적 범위가 해결 곤란한 실무상 주요 쟁점인 가운데에 나온 판결이어서 주목된다.[13]

---

13) 이러한 대법원 2021. 11. 18. 선고 2016도348 전원합의체 판결이 있기 전의 논문으로, 박용철, "디지털 증거 중 카카오톡 대화의 압수ㆍ수색영장 집행에 대한 참여권", 한국비교형사법학회『비교형사법연구』제20권 제4호 (2019. 1.) 23~42.
재판연구관의 위 대법원 판결 해당 논문으로, 장석준, "임의제출된 정보저장매체에 저장된 전자정보의 증거능력", 사법 59호(2022. 3.), 815-855.
위 판결 선고 후의 논문으로, 전치홍, "대법원의 참여권 법리에 대한 비판적 검토-대법원 2021. 11. 18. 선고 2016도348 전원합의체 판결을 중심으로-",「형사소송 이론과 실무」제14권 제1호 (2022. 3.), 33은 임의제출 현장에서 정보 저장매체를 탐색하지 않고, 정보 저장매체를 수사기관의 사무실로 일단 반출한 후 탐색(포렌식)하는 방식(이른바 2단계의 방식)으로 압수수색 영장의 집행이 이뤄지고 있는바 전자의 단계에서 급속을 요하여 참여권 보장이 없었다 하더라도 후자의 단계에서는 별도로 참여권이 보장되어야 한다고 타당하게 지적하고 있다. 같은 취지로 이규봉, "디지털 증거 압수·수색 과정에서 피압수자 등의 참여 범위", 석사학위 논문(고려대학교 2021), 73-75; 조성훈,『역외 전자정보 압수·수색 연구』, (박영사, 2020), 131; 방경휘, "정보저장매체의 반출 후 전자정보의 탐색·선별에서의 참여권 보장에 관한 연구", 홍익법학 제21권 제3호 (2020).
구길모, "디지털 증거 압수·수색과 참여권보장 - 피의자와 피압수자가 일치하지 않는 경우를 중심으로", 형사법연구 제34권 제4호(2022 겨울)는 아예 '피압수자'가 아니라 '피의자'가 참여권의 주체라는 입장에 서서 대법원이 '피압수자'라고 표현하는 데 대하여 비판적 논의를 전개한다. 이흔재, "제3자 보관 전자정보에 대한 압수·수색영장의 집행과 피의자의 절차적 권리", 형사법의 신동향 통권 제76호(2022·가을)는 입법론을 전개한다. 박중욱, "전자정보의 압수수색과 피의자의 참여권 -대법원 입장의 비판적 수용 및 독일 논의의 참고-", 형사정책연구 제34권 제1호(통권 제133호, 2023 ·봄)는, 대법원 2021도11170 판결이 피의자가 실질적 피압수자가 아니라는 이유로 그의 참여권을 인정하지 않은 것에 대하여, 이는 법률상 인정된 피의자의 권리를 부당하게 제한하는 해석이라는 점에서 적법절차 원칙에 반한다고 비판한다.
소재환·이선화, "디지털 증거 압수·수색 시 참여권자 관련 실무상 문제 - 대법원의 '실질적 피압수자' 법리 중심으로", 형사법의 신동향 통권 제77호(2022·겨울)는 수사 현실을 들어 비판적 입장을 보인다.

대법원 2021. 11. 18. 선고 2016도348 전원합의체 판결
피해자 등 제3자가 피의자의 소유·관리에 속하는 정보저장매체를 영장에 의하지 않고 임의제출한 경우에는 실질적 피압수자인 피의자가 수사기관으로 하여금 그 전자정보 전부를 무제한 탐색하는 데 동의한 것으로 보기 어려울 뿐만 아니라 피의자 스스로 임의제출한 경우 피의자의 참여권 등이 보장되어야 하는 것과 견주어 보더라도 특별한 사정이 없는 한 형사소송법 제219조, 제121조, 제129조에 따라 피의자에게 참여권을 보장하고 압수한 전자정보 목록을 교부하는 등 피의자의 절차적 권리를 보장하기 위한 적절한 조치가 이루어져야 한다.

대법원 2022. 1. 27. 선고 2021도11170 판결은 피의자나 제3자가 압수·수색의 대상이 되는 전자정보에 의하여 식별되는 정보주체에 해당한다는 사정만으로 참여권이 인정되는 것은 아니라고 보았다.[14] 물론 정보주체에게 형사소송법 제106조 제4항에 따른 압수 후 통지는 이루어져야 한다.

대법원 2022. 1. 27. 선고 2021도11170 판결
나아가 피해자 등 제3자가 피의자의 소유·관리에 속하는 정보저장매체를 영장에 의하지 않고 임의제출한 경우에는 실질적 피압수자인 피의자가 수사기관으로 하여금 그 전자정보 전부를 무제한 탐색하는 데 동의한 것으로 보기 어려울 뿐만 아니라 피의자 스스로 임의제출한 경우 피의자의 참여권 등이 보장되어야 하는 것과 견주어 보더라도 특별한 사정이 없는 한 형사소송법 제219조, 제121조, 제129조에 따라 피의자에게 참여권을 보장하고 압수한 전자정보 목록을 교부하는 등 피의자의 절차적 권리를 보장하기 위한 적절한 조치가 이루어져야 한다(위 대법원 2016도348 전원합의체 판결 등 참조).
이와 같이 정보저장매체를 임의제출한 피압수자에 더하여 임의제출자 아닌 피의자에게도 참여권이 보장되어야 하는 '피의자의 소유·관리에 속하는 정보저장매체'라 함은, 피의자가 압수·수색 당시 또는 이와 시간적으로 근접한 시기까지 해당 정보저장매체를 현실적으로 지배·관리하면서 그 정보저장매체 내 전자정보 전반에 관한 전속적인 관리처분권을 보유·행사하고, 달리 이를 자신의 의사에 따라 제3자에게 양도하거나 포기하지 아니한 경우로써, 피의자를 그 정보저장매체에 저장된 전

14) 헌법상 보장되는 주거권, 개인정보자기결정권, 사생활의 비밀과 자유, 통신의 비밀, 재산권 등이 강제적 수사행위로 인하여 침해되는 기본권이라면 해당 기본권의 향유 주체가 강제처분절차에의 참여자가 되어야 한다는 김혜경, "영장주의의 본질을 기초로 한 전자정보 압수·수색의 참여권의 범위", 연세법학 제35호(2020. 6.) 35~38은 원론적으로는 타당한 면이 없지 아니하나, 실무상 신중한 검토를 필요로 한다.

> 자정보에 대하여 실질적인 압수·수색 당사자로 평가할 수 있는 경우를 말하는 것이다. 이에 해당하는지 여부는 민사법상 권리의 귀속에 따른 법률적·사후적 판단이 아니라 압수·수색 당시 외형적·객관적으로 인식 가능한 사실상의 상태를 기준으로 판단하여야 한다. 이러한 정보저장매체의 외형적·객관적 지배·관리 등 상태와 별도로 단지 피의자나 그 밖의 제3자가 과거 그 정보저장매체의 이용 내지 개별 전자정보의 생성·이용 등에 관여한 사실이 있다거나 그 과정에서 생성된 전자정보에 의해 식별되는 정보주체에 해당한다는 사정만으로 그들을 실질적으로 압수·수색을 받는 당사자로 취급하여야 하는 것은 아니다.

피압수자 등 참여권자가 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 미리 집행의 일시·장소를 통지하지 않고 압수·수색을 할 수 있다(형사소송법 제122조, 제219조). 형사소송법 제122조의 '급속을 요하는 때'라 함은 압수·수색영장 집행 사실을 미리 알려주면 증거물을 은닉할 염려 등이 있어 압수·수색의 실효를 거두기 어려울 경우를 의미한다(대법원 2012. 10. 11. 선고 2012도7455 판결).

> 헌법재판소 2012. 12. 27. 선고 2011헌바225 결정
> 압수·수색 집행에 대한 사전통지를 분별없이 일률적으로 적용하게 되면, 범죄수사와 실체적 진실발견이라는 형사소송법의 다른 중요한 목적을 달성할 수 없게 된다는 점을 고려한 이 사건 법률조항의 취지와 문언의 의미 등을 종합하여 보면, 이 사건 법률조항의 '급속을 요하는 때'라 함은 압수수색 집행사실을 피의자에게 미리 통지하여 줄 경우 압수수색의 대상이 된 증거를 인멸하거나 훼손하여 압수수색의 목적을 달성할 수 없게 되는 때를 의미하는 것으로 합리적으로 해석할 수 있고, 그와 같이 압수수색의 목적을 달성할 수 없게 되는 예외 사유를 구체적으로 나열하거나 세부적으로 특정하는 것은 압수수색의 집행과 관련하여 다양하게 나타날 수 있는 사실관계에 비추어 바람직하다고 할 수 없으므로, 위 조항이 명확성원칙에 위배된다고 할 수 없다.
> 이 사건 법률조항[15]에 의하여 피의자 등이 압수수색 사실을 사전 통지받을 권리 및 이를 전제로 한 참여권을 일정 정도 제한받게 되기는 하지만, 그 제한은 '사전

15) 아래 밑줄 그은 부분을 준용하는 법 제219조 해당 부분을 가리킨다: 형사소송법 제122조 (영장집행과 참여권자에의 통지) 압수·수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단, 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 예외로 한다.

> 통지에 의하여 압수수색의 목적을 달성할 수 없는 예외적인 경우'로 한정되어 있고, 전자우편의 경우에도 사용자가 그 계정에서 탈퇴하거나 메일 내용을 삭제·수정함으로써 증거를 은닉·멸실시킬 가능성을 배제할 수 없으며, 준항고 제도나 위법수집증거의 증거능력 배제 규정 등 조항 적용의 남용을 적절히 통제할 수 있는 방법이 마련되어 있는 점, 반면에 이와 같은 제한을 통해 압수수색 제도가 전자우편에 대하여도 실효적으로 기능하도록 함으로써 실체적 진실 발견 및 범죄수사의 목적을 달성할 수 있도록 하여야 할 공익은 매우 크다고 할 수 있는 점 등을 종합해 보면, 이 사건 법률조항에 의하여 형성된 절차의 내용이 적법절차원칙에서 도출되는 절차적 요청을 무시하였다거나 비례의 원칙이나 과잉금지원칙을 위반하여 합리성과 정당성을 상실하였다고 볼 수 없다.

대법원 2022. 5. 31. 자 2016모587 결정은 수사기관이 정보통신서비스제공자를 상대로 발부받은 압수·수색영장에 기하여 피의자인 서비스이용자의 아이디, 대화내용 등 전자정보를 압수·수색한 사안에서, '서비스이용자로서 실질적 피압수자이자 피의자인 준항고인에게 참여권을 보장하지 아니한 위법'이 있다고 판단하였다. 그리고 원심(서울중앙지방법원 2016. 2. 18. 자 2015보6 결정)은 법 122조 단서의 급속을 요하는 때에 해당하지 않는다고 보았으나, 대법원은 원심의 그 판단이 잘못이라고 언급하였으니, 대법원의 언급은 급속을 요하는 때여서 참여권자 통지를 생략할 수 있다는 취지이다. 이는 사용자가 카톡 삭제 내지 카톡방 나가기를 해버리면 카카오톡 서비스 운영 회사의 서버에서도 정보가 삭제되며 복구가 어려워질 수 있다는 데에 주목하면서 한 언급으로 이해된다. 물론 카카오톡 서비스 운영 회사의 서버에서 삭제가 되는 경우와 되지 않고 백업이 그대로 남아 있는 경우가 나뉘므로, 사실심 법원이 면밀한 현황 확인을 하여야 하는 심리 대상이다.

참여권이 보장되지 않은 경우 압수·전자증거의 증거능력에 관하여 보면, 수사기관이 피압수자 측에 참여의 기회를 보장하거나 압수한 전자정보 목록을 교부하지 않는 등 영장주의 원칙과 적법절차를 준수하지 않은 위법한 압수·수색 과정을 통하여 취득한 증거는 위법수집증거에 해당하고, 사후에 법원으로부터 영장이 발부되었다거나 피고인이나 변호인이 이를 증거로 함에 동의하였다고 하여 위법성이 치유되는 것도 아니다(대법원 2022. 7. 28. 선고 2022도2960 판결). 피고인이 수사단계에서 이 사건 공소사실을 모두 인정하면서 압수절차의 위법성을 다투지 않았다거나, 영장 혐의사실과 비교할 때 범행 방법이 동일하여 피고인의 방어권이 침해되지 않았다는

사유만으로는 유죄의 증거로 사용할 수 있는 예외적인 경우에 해당한다고 보기도 어렵다(대법원 2021. 12. 30. 선고 2019도10309 판결).

4. 정보의 독자적 대상성 및 영장 기재 해석의 엄격성, 이메일과 클라우드

정보는 저장매체로부터 독립한 것으로 취급되어야 한다. 그래서 예컨대 압수영장이나 압수목록에 매체 압수라고만 적혀 있으면 그 매체에 저장된 정보를 포함하는 뜻이라고 보는 것이 기존의 수사·재판 실무상 통념적 이해였다고 한다면, 요즘에는 "매체와 정보를 구분해서 보아야 하며 정보는 독자적인 대상성을 갖기에 정보는 불포함이라고 보아야 한다."는 반론이 빠르게 설득력을 얻어 이제는 판례로 자리잡았다고 하여도 과언이 아니다.[16] 하물며, 자동로그인 설정된 앱을 사용하여 그 연결된 클라우드 개인저장소를 탐색하는 것까지 포함한다고는 보기 어려운 경우가 많을 것이다.

> 대법원 2022. 6. 30. 자 2020모735 결정
> 압수할 전자정보가 저장된 저장매체로서 압수·수색영장에 기재된 수색장소에 있는 컴퓨터, 하드디스크, 휴대전화와 같은 컴퓨터 등 정보처리장치와 수색장소에 있지는 않으나 컴퓨터 등 정보처리장치와 정보통신망으로 연결된 원격지의 서버 등 저장매체(이하 '원격지 서버')는 소재지, 관리자, 저장 공간의 용량 측면에서 서로 구별된다. 원격지 서버에 저장된 전자정보를 압수·수색하기 위해서는 컴퓨터 등 정보처리장치를 이용하여 정보통신망을 통해 원격지 서버에 접속하고 그곳에 저장되어 있는 전자정보를 컴퓨터 등 정보처리장치로 내려 받거나 화면에 현출시키는 절차가 필요하므로, 컴퓨터 등 정보처리장치 자체에 저장된 전자정보와 비교하여 압수·수색의 방식에 차이가 있다. 원격지 서버에 저장되어 있는 전자정보와 컴퓨터 등 정보처리장치에 저장되어 있는 전자정보는 그 내용이나 질이 다르므로 압수·수색으로 얻을 수 있는 전자정보의 범위와 그로 인한 기본권 침해 정도도 다르다. 따라서 수사기관이 압수·수색영장에 적힌 '수색할 장소'에 있는 컴퓨터 등 정보처리장치에 저장된 전자정보 외에 원격지 서버에 저장된 전자정보를 압수·수색하기 위

16) 대법원 2022. 6. 30. 자 2020모735 결정 참조.

해서는 압수·수색영장에 적힌 '압수할 물건'에 별도로 원격지 서버 저장 전자정보가 특정되어 있어야 한다. 압수·수색영장에 적힌 '압수할 물건'에 컴퓨터 등 정보처리장치 저장 전자정보만 기재되어 있다면 컴퓨터 등 정보처리장치를 이용하여 원격지 서버 저장 전자정보를 압수할 수는 없다.

대법원 2022. 6. 30. 선고 2022도1452 판결

위와 같은 사실관계를 앞서 본 법리에 비추어 살펴보면, 이 사건 압수·수색영장을 집행하면서 이 사건 휴대전화를 이용하여 구글클라우드에 저장된 불법촬영 사진, 동영상을 압수·수색한 것은 위법하고, 위 (5) 증거[17]는 증거능력이 없다. 그 구체적인 이유는 다음과 같다.

(1) 이 사건 압수·수색영장에 적힌 '압수할 물건'에는 '여성의 신체를 몰래 촬영한 것으로 판단되는 사진, 동영상 파일이 저장된 컴퓨터 하드디스크 및 외부저장매체'가, '수색할 장소'에는 피고인의 주거지가 기재되어 있다. 이 사건 압수·수색영장에 적힌 '압수할 물건'에 원격지 서버 저장 전자정보가 기재되어 있지 않은 이상 이 사건 압수·수색영장에 적힌 '압수할 물건'은 피고인의 주거지에 있는 컴퓨터 하드디스크 및 외부저장매체에 저장된 전자정보에 한정된다.

(2) 그럼에도 경찰은 이 사건 휴대전화가 구글계정에 로그인되어 있는 상태를 이용하여 원격지 서버에 해당하는 구글클라우드에 접속하여 구글클라우드에서 발견한 불법촬영물을 압수하였다. 결국 경찰의 압수는 이 사건 압수·수색영장에서 허용한 압수의 범위를 넘어선 것으로 적법절차 및 영장주의의 원칙에 반하여 위법하다.

(3) 따라서 이 사건 압수·수색영장으로 수집한 불법촬영물은 증거능력이 없는 위법수집증거에 해당하고, 이 사건 압수·수색영장의 집행 경위를 밝힌 압수조서 등이나 위법수집증거를 제시하여 수집된 관련자들의 진술 등도 위법수집증거에 기한 2차적 증거에 해당하여 증거능력이 없다.

라) 결국 이 사건에서 증거능력이 없는 증거를 제외한 나머지 증거들만으로는 이 부분 공소사실이 합리적인 의심을 배제할 정도로 입증되었다고 보기 어렵다.

마) 그런데도 원심은 이 부분 공소사실을 유죄로 판단하였다. 이러한 원심판결에는 압수·수색영장의 효력, 위법수집증거 배제법칙에 관한 법리를 오해하여 판결에 영향을 미친 잘못이 있다. 이를 지적하는 피고인의 상고이유 주장은 이유 있다.

---

17) 판결의 위 (5) 증거라는 언급은, 이 사건 휴대전화와 연동된 구글클라우드를 수색한 결과를 가리킨다.

대법원 2021. 7. 29. 선고 2020도14654 판결
피의자가 휴대전화를 임의제출하면서 휴대전화에 저장된 전자정보가 아닌 클라우드 등 제3자가 관리하는 원격지에 저장되어 있는 전자정보를 수사기관에 제출한다는 의사로 수사기관에게 클라우드 등에 접속하기 위한 아이디와 비밀번호를 임의로 제공하였다면 위 클라우드 등에 저장된 전자정보를 임의제출하는 것으로 볼 수 있다.

대법원은 외국계 이메일 계정을 이용한 이메일에 대한 압수·수색에 대한 대법원 2017. 11. 29. 선고 2017도9747 판결(이른바 SINA.COM 사안)에서 이메일 원격 압수·수색, 나아가 역외 압수·수색을 허용하는 견해를 채택하였다. 실체적·절차적으로 적법절차나 영장주의의 실질에 반하는 측면이 없는 점이 고려된 것으로 볼 수 있다.

서울고등법원 2022. 12. 7. 선고 2020노367 판결은, 영장 발부 판사가 '사무실, 전산실' 앞에 '위 건물 내'의 기재를 추가하고, 그 뒤에 있는 '외부에 위탁한 경우 외부 업체 포함'이라는 기재는 삭제하는 것으로 수정하여 발부한 데에 주목하고, '압수할 물건'란에 기재된 '서버'에는 원격지에 존재하는 외부 업체의 서버인 아마존 클라우드 시스템 서버가 포함된다고 볼 수 없다고 판단하였다(상고심 2022도16718 계속 중). 유사한 취지의 수원고등법원 2022. 6. 15. 선고 2022노145 판결이 있다(상고심 2022도8203 계속 중).[18]

대법원 2021. 10. 14. 선고 2021도2485 판결은 법원이 지정한 특정 검색어가 아닌 특정 검색어를 분할한 키워드를 사용하여 탐색한 결과를 촬영한 컴퓨터 모니터 화면 사진에 대하여 압수수색영장에 기재된 '압수할 물건'에 포함되지 아니하고, '압수수색의 방법 제한'을 위반하여 수집된 증거로서 위법수집증거에 해당하므로 증거능력이 없다고 판단한 원심을 수긍하였다.

18) 관련 논문에 장진환, "핸드폰 압수·수색영장으로 행한 클라우드 압수·수색의 타당성 - 대법원 2022도8203 사건을 중심으로", 형사법연구 제35권 제1호(2023 봄).

5. 접근권한정보 관련 쟁점

안티포렌식은 디지털포렌식을 방해하는 활동이다. 디지털 사용 흔적(artifacts[19])의 파괴, 데이터 은닉과 암호화, 흔적 난독화, 포렌식도구 분석 방해 등의 여러 기법들이 있다. 이러한 안티포렌식 기법이 비교적 생소하게 들릴지 모르지만, 모바일에서는 암호화라는 강력한 안티포렌식 기법이 전국민 누구나 일상적으로 사용하고 있는 스마트폰에 이미 보편적으로 적용된 지 여러 해가 지났다. 전체 디스크 암호화(FDE, Full Disk Encryption)는 모바일 기기의 메모리 중 사용자 데이터 파티션(UserData partition)에 저장된 정보 전체를 하나의 암호키로 통째로 암호화하는 기술이며, 모든 파일들을 파일별 암호키로 암호화하는 기술(FBE, File-based Encryption)이 최근에 표준 적용되고 있다. 그 외에도 애플, 삼성 등의 기기 제조 회사들은 정보 보안과 사생활 보호를 위하여 부팅시스템 무결성 검사, 보안 전용의 별도 프로세서 장착을 비롯하여 다양하고 한층 강화된 보안 기술들을 모바일 기기에 기본 탑재시켜놓고 있다.

그래서 오늘날 화면잠금번호(PIN, 숫자 패스코드), 비밀번호(문자 또는 숫자의 로그인 패스워드), 화면잠금패턴 등의 접근권한정보를 끝내 확보하지 못한다면 포렌식 수사관뿐만 아니라 법원을 포함한 어느 국가기관도 스마트폰 압수를 통하여 얻을 수 있는 정보는 거의 아무 것도 없다고 하여도 과언이 아니다. 요즘(대략 2017년 이후 출시) 스마트폰에 대한 획득 방법은, 획득 도구의 문제, 강화된 보안 기술의 적용 등으로 인하여 '라이브 획득'의 방법뿐인 경우가 많다. 잠금해제·복호화 수단인 접근권한정보를 준비하지 못하면 포렌식 작업은 불가능해진 또다른 이유이다. 다른 획득 방법, 즉 리커버리 모드, 다운로드 모드 등에 의하여 사용자 데이터 파티션(UserData partition)을 물리이미징하는 방식은, 설령 획득 도구가 그 모델·버전의 스마트폰에 대하여 이러한 방식을 지원한다 하더라도, 암호화 때문에 그 비밀번호 등 접근권한정보를 준비하지 못하면 역시 포렌식 작업이 아예 불가능하다.

수사기관은 피압수자로 하여금 예컨대 '정보저장매체 제출 및 이미징 등 참관여부 확인서'에 화면잠금번호, 비밀번호, 화면잠금패턴, 백업데이터 비밀번호를 기재하도록 하여 받고 있으며, 이 부분은 사실상 임의제출로 받는 것에 가깝다.

---

19) 맥락(분야)에 따라서 다양한 의미를 갖는 용어인바, 디지털 포렌식의 맥락에서는 부산물, 흔적 등을 가리킨다.

접근권한정보 관련하여 최근 법적 쟁점은 진술, 입력행위, 생체정보 등으로 나누어 살펴볼 수 있는데, 진술에 관하여는 진술거부권 쟁점[20] 등이, 입력행위는 영장 강제집행이 과연 가능한지 등이, 생체정보는 관련 특별법상의 쟁점 등이 검토될 수 있다.

6. 임의제출

영장주의 관련 논의에서 임의제출에 의한 압수와 영장에 의한 압수의 둘은 종래 비교적 분명하게 구분지어지고 있었지만, 오늘날 수사기관 압수 대상물의 과반을 차지하는 모바일 기기에서는 그러한 종래의 사고방식이 재검토되어야 할 것이다. 암호화 등 안티포렌식 기술이 오늘날의 모바일 기기에 보편적으로 적용되어 있으므로 잠금해제·복호화를 위하여 화면잠금번호, 비밀번호, 화면잠금패턴 등의 접근권한정보를 확보하지 못하면 압수는 실패한다. 영장을 발부받았다고 하여 언제나 이러한 접근권한정보를 확보할 수 있는 것은 아니므로 사실상 임의제출과 유사하게 피압수자의 협조에 의하여야 그러한 정보를 확보할 수 있게 된다. 이런 맥락에서, 영장집행 시 접근권한정보의 제출거부를 할 수 있음을 먼저 고지해야 비로소 임의제출의 임의성이 담보될 수 있다는 의견이 있다. 진술거부권 고지 의무가 있는지 연구검토 필요하다는 의견도 있다. 그래서 특히 '모바일' 기기의 압수에서 불거지는 여러 재판상 쟁점을 올바르게 해결하기 위해서는 영장에 의한 압수와 임의제출에 의한 압수를 통합하는 법리 체계를 모색할 필요가 있을 수 있다.

임의제출물 압수와 관련하여 제3자가 피의자의 소유·관리에 속하는 정보저장매체를 영장에 의하지 않고 임의제출한 경우에 그 피의자에게 참여권이 인정될 수 있다고 판단한 대법원 2021. 11. 18. 선고 2016도348 전원합의체 판결은 앞서 본 바와 같다. 이는 임의제출 압수에서도 압수·수색영장에 의한 집행과 마찬가지로 선별압수 원칙이 적용된다고 판단하고, 임의제출자의 임의제출의 제출범위를 한정하는 것은 가능하나 이때 의사표시는 엄격하게 해석하여야 하며, 임의제출자의 의사가 명확하지 않은 경우에는 압수·수색영장에 의한 집행과 마찬가지로 압수의 동기가 된 범죄

---

20) 조성훈, "전자정보 접근 방법의 법적 문제 - 진술거부권과 관계를 중심으로", 법조 제69권 제6호(통권 제744호), 2020년, 142～183.

혐의사실과의 관련성이 있는 전자정보에 한하여 압수의 대상이 된다고 한 점에서도, 주목할 만한 주요 판결이다.[21][22]

7. 맺음말

이상으로, 모바일 전자증거 압수수색의 적법절차에 관하여 최근 다양하게 등장한 쟁점들을 일람하고, 관련 판례를 소개하였다. 본고는 ① '관련성' 요건에 관한 대법원 판례의 변화[23], ② 관련성 요건 중 하나로 대법원이 제시한 인적 관련성 요건의 문제점을 둘러싼 논의, ③ 적법하게 압수한 전자증거의 별건 사용을 제한할 수 있는가 하는 쟁점에 관한 논의, ④ 최근 논의되고 있는 형사소송규칙 개정안[24] 등에 관하여는 언급을 생략하는데, 비록 본고에서는 생략하지만, 법원 재판실무상 중요한 현안들이라는 데 대하여는 두말할 나위가 없을 것이다.

---

21) 위 2016도348 전원합의체 판결 선고 이후 임의제출한 전자증거(압수물)의 '관련성'과 관련된 판례로는 대법원 2021. 11. 25. 선고 2019도6730 판결, 대법원 2021. 11. 25. 선고 2019도9100 판결, 대법원 2021. 11. 25. 선고 2019도7342 판결, 대법원 2021. 11. 25. 선고 2016도82 판결, 대법원 2021. 11. 25. 선고 2020도3796 판결, 대법원 2021. 12. 30. 선고 2018도7994 판결, 대법원 2022. 1. 13. 선고 2016도9596 판결, 대법원 2022. 2. 17. 선고 2019도4938 판결 등이 있다.
관련 논문에 박정란, "임의제출된 휴대폰 내 전자정보의 압수범위 및 피압수자의 참여권 보장 - 대법원 2021. 11. 18. 선고 2016도348 판결 -", 법조 제71권 제2호(통권 제752호)(2022. 4.), 371~398; 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 62호(2022. 12.), 225-264 등.

22) 위 판결 선고 전의 관련 논문에 박석훈·함영욱·백승철, "전자증거의 압수수색 및 임의제출 과정에서의 데이터 범위 한정가능성에 대한 고찰", 법조 2015년 6호(통권 705호).

23) 오현석, "압수수색의 관련성 심사방식에 관한 판례의 문제점", 한국형사소송법학회 월례세미나(2021. 7. 23.) 발표자료; 김웅재, "압수·수색의 '관련성' 요건에 관한 대법원 판례의 진화", 법학평론 제12권 (2022. 4.), 9-66면.

24) 다음과 같은 네 가지를 골자로 하는 개정안이다: ① 압수수색 영장 관련 판사 대면심문기일 도입, ② 피의자 등의 압수수색영장 집행 참여 시 의견진술권 등 참여권 강화, ③ 압수수색의 대상으로 정보를 명문화, ④ 전자정보에 대한 압수수색 영장 청구서의 기재사항에 집행계획을 추가.

【토론문】

“모바일 전자증거 압수수색과 적법절차, 최근 쟁점과 법원 판례의 동향”에 대한 토론문

성 중 탁*

1. 서설

먼저, 스마트폰 압수수색에 관한 최근 주요 쟁점과 관련 최신 판례들을 깔끔하게 잘 정리해주신 발제자의 노고에 경의를 표합니다. 스마트폰의 기능과 품질이 크게 향상되면서 휴대전화의 기능이 단순 통화나 문자·음성메시지를 전송·수신을 넘어 사진·동영상의 촬영, 보관, 각종 메모, 인터넷 검색 내역 등을 포함하는 광범위한 정보를 집약적으로 저장·취급하는 것으로 확장되었습니다. 그에 따라 휴대전화에 저장된 각종 데이터에 관한 수색은 경우에 따라서는 개인용 컴퓨터를 수색하는 것에 상응하거나 그 이상의 의미를 가지게 되었습니다. 또한 수사 실무에서 체포에 수반하여 피의자의 휴대전화를 사실상 압수한 후 그 내용을 뒤져 증거를 찾거나 체포의 대상이 된 범죄혐의 이외에 다른 사건을 인지하거나(예를 들어, 조세포탈 혐의를 수사하는 과정 중에 휴대전화에 저장된 데이터를 사실상 수색하여 미성년자와 모텔에 가서 찍은 사진이나 전화번호를 발견하고 아동청소년 성매매 사건을 인지하는 경우 등) 이를 이유로 당해 사건의 자백을 받아내는 등의 사례가 일어날 가능성도 배제할 수 없습니다. 이에 아래에서는 본 발제문을 보충하는 취지에서 관련 쟁점과 그에 관한 짧은 사견을 말씀드리는 것으로 부족한 토론자의 임무를 다하고자 합니다.[1)]

* 경북대학교 법학전문대학원 교수

1) 이하, 아래에서는 편의상 경어를 생략한 점 널리 양해 부탁드립니다.

2. 정보프라이버시권 내지 개인정보자기결정권 침해 최소화 필요성

수사기관이 형사소송법 제217조에 따른 긴급 압수수색 시 핸드폰의 경우 일단 영장 없이 압수한 다음 사후 영장 대상으로 삼아 이를 청구하는 경우가 있다. 핸드폰의 경우 다른 정보저장매체에 비해 그 청구 빈도가 월등하게 많은 것으로 파악된다. 또한 발제문을 통해서도 알 수 있는 바와 같이 수사기관이 체포된 피의자의 스마트폰에서 영장도 없이 그 안에 담긴 문자메시지, 사진, 동영상, 전화번호부, 주소록, 통화 내역, 각종 사회관계망서비스(SNS)와 연결된 대화 내용·친구 목록, 클라우드 등 사생활 정보를 수색하는 점에 대해 법원 내부에서도 강한 문제의식을 갖고 있는 것으로 보여진다.[2)]

전자정보 수집·이용과 전자감시 맥락에서 수집되는 스마트폰 저장 개인정보는 개인의 사생활과 밀접하게 관련된 매우 민감한 정보로서, 수사기관에 의해 강제수집된 후 일반 대중에게는 공개되지 않는다 하더라도 정부기관 상호간에는 공유될 수 있어 정보프라이버시권 침해가능성이 크기 때문에 더욱 문제가 아닐 수 없다. 이와 관련하여, 2018년 헌법재판소는 체포·구속영장을 집행할 때 수색영장 없이 제3자의 주거지 등을 '수색'할 수 있도록 한 형사소송법 조항(제216조 제1항)에 대해 재판관 전원일치 의견으로 헌법불합치 결정했다[3)]. 위 사건에서 헌재는 '피의자가 해당 장소에 있을 개연성이 인정되고', '수색영장을 발부받기 어려운 긴급한 사정이 있을 때만' 헌법 제16조가 정한 영장주의의 예외가 인정될 수 있다고 밝힌 바 있다.

3. 관련 정책의 개선방안

피의자의 범죄 혐의가 소명되고 주거지, 사무실 등에서 각종 장부 등의 압수수색 필요성이 인정된다 하더라도 곧바로 같은 장소에 있는 PC나 휴대전화 등 정보저장매체의 압수수색 필요성까지 인정되는 것은 아니다. 수사기관은 피의자, 참고인 등을 상대로 출석을 요구하면서 사전에 출석대상자의 휴대전화 압수수색영장을 청구

---

2) 과거 법원은 일반 구속영장과 달리 압수수색영장은 연구자료 부족 등으로 객관적 기준이 마련되지 않아 업무처리에 어려움이 있었고, 심지어 아무런 검토 없이 수사기관이 청구하는 대로 발부하는 경우까지 있었다.

3) 헌법재판소 2018. 4. 26. 2015헌바370 결정

하는 경우가 있는데 수사기관의 출석요구에 따른 피의자신문, 참고인신문 등 수사는 기본적으로 임의수사 성격을 갖는다는 점에서 분명 문제가 있는 부분이다. 즉 범죄혐의의 내용, 범죄의 성격이나 소명 정도, 대상자의 수사상 위치, 통화 내역에 관한 통신사실 확인자료 제공 요청 허가 등 기본권 제한 정도가 덜한 수사 방법에 의해 소기의 목적을 달성할 수 있는지 여부 등을 보다 신중히 고려해야 하는 것이다. 무엇보다 체포나 압수수색 대상이 아닌 사람은 휴대전화를 수사기관에 제출할 의무가 전혀 없다.

다만, 범죄의 규명과 처벌에 있어 전자증거의 중요성은 날로 커지고 있고, 이에 따라 전자증거의 수집을 위한 압수수색이 대물적 강제처분의 대종을 이루게 되었다. 그에 따라 디지털 환경이 개별적이고 PC로부터, 인터넷과 클라우드 컴퓨팅 시대로 이행되면서, 전자증거에 대한 수집은 사생활영역 및 정보자기결정권의 보호와 영장주의 등 다양한 법적 쟁점과 마주하고 있다.

향후에는 이러한 헌법상 기본권 보장과 적법절차 및 영장주의 원칙을 제대로 반영하여 형사소송법을 개정하여야 하고 그 기회에 '전자정보' 그 자체가 압수수색의 대상임을 명시하는 것으로 정비되고, 수사기관이 저장매체 원본 또는 그 복제본을 압수할 수 있는 명확한 요건을 명문화하여야 할 것이다. 또한, 전자정보에 대한 압수 후 범죄와 관련 없는 개인 민감 정보가 발견될 경우 이를 폐기하거나 삭제할지 여부에 대해 피압수자의 확인을 받는 절차를 명문화하고, 수사기관이 이와 같은 노력을 게을리 할 경우 범죄와 관련된 증거를 포함하여 전체 증거의 증거능력을 박탈함으로써, 적법절차를 실질적으로 준수하는 한편 피압수자 등의 기본권 제한을 최소화하는 방안이 강구될 필요가 있다.

결국, 전자정보에 대한 압수수색은 영장주의 원칙에 따라 저장매체의 압수에서부터 전자정보를 복제, 출력하는 전체 과정이 적법하게 집행되어야 한다. 특히, 혐의사실과의 관련성과 피압수자의 절차 참여 기회 보장은 영장주의 원칙의 핵심요소이고, 그 절차상 위법이 중대하여 전체 압수수색절차를 위법한 것으로 평가할 수 있을 경우 압수수색처분 전체가 취소되어야 하며, 수집된 전자정보의 증거능력은 배제되어야 한다. 이런 측면에서 발제문에서 소개하고 있는 대법원 2015. 7. 16. 자 2011모1839 전원합의체 판결은 큰 의미가 있다고 하겠다.[4)]

---

4) 한편, 위 대법원 전합 판결 이후에도 대법원은 "수사기관이 정보저장매체에 기억된 정보 중에서 키워드 또는 확장자 검색 등을 통해 해당 사건의 혐의사실과 관련 있는 정보를 선

무엇보다, 휴대폰 등에 대한 전자정보 압수수색의 경우에도 그 전 과정에서 적법절차원칙과 영장주의 원칙을 준수하여야 한다. 그동안 수사실무 관행상 휴대폰 등 모바일기기는 특정 장소에 비치되어 사용되는 정보저장매체와 달리 통상적으로 사람의 신체에 휴대된다는 특성 때문에 임의 제출물의 압수 또는 체포현장에서의 압수수색 등 영장주의 예외의 적용을 너무나 쉽게 받아 온 것이 사실이다. 그와 같은 잘못된 수사관행을 바로 잡기 위해서라도 휴대폰 등을 임의 제출받는 경우에도 그에 저장된 전자정보까지 임의로 제출하는 것이 당사자 본인의 자의에 기한 의사 인지를 명확히 확인하고, 정보 탐색, 복제, 출력 등 전 과정에서 임의성이 확보되도록 당사자의 참여기회를 철저히 부여 하여야 한다. 특히, 체포현장에서 영장 없이 휴대폰 등을 압수수색하는 경우 휴대폰 등 기기 자체와 그에 저장된 전자정보를 구별하여, 전자정보를 영장 없이 압수하여야 할 긴급한 상황이 아닌 경우 사전 압수수색영장을 발부받아야 함이 상당하다.

또한, 제3자로부터 정보를 제공받은 경우 정보주체에게 지체 없이 통지하도록 한 개정 형사소송법 제106조 제4항에 대하여는 수사목적상 필요한 경우 유예기간을 둘 수 있도록 보완할 필요가 있는 한편, 위와 같은 통지 및 전자우편 압수수색시 사후통지(통신비밀보호법 제9조의 3[5])를 흠결한 경우 해당 증거물의 증거능력을 박탈하

별한 다음, 정보저장매체와 동일하게 비트열 방식으로 복제하여 생성된 파일을 제출받아 압수하였다면 이로써 압수의 목적물에 대한 압수수색절차는 종료된 것이므로 수사기관이 수사기관 사무실에서 위와 같이 압수된 이미지 파일을 탐색·복제·출력하는 과정에서도 피의자 등에게 참여의 기회를 보장하여야 하는 것은 아니다."라고 판시하였다. 이는 수사기관이 압수수색 현장에서 범죄사실과 관련성이 있는 전자정보만을 압수수색하였을 경우에는 그 후에 절차에서는 피압수자 등의 참여권을 보장하지 않아도 된다고 본 최초의 법리를 설시한 판례로 평가할 수 있다. 즉 수사기관의 최초 압수수색 현장에서 해당 범죄사실과 관련성 있는 전자정보를 선별한 후 해당 부분만을 압수하였다면 그 이후 절차에서는 피압수자에게 참여권을 보장하지 않더라도 적법절차에 위배된다고 보지 않겠다는 취지로 해석된다(대법원 2018. 2. 8. 선고 2017도13263 판결, 조광훈, "전자정보의 압수수색절차에서 관련성·동일성·참여권 -대법원 2018. 2. 8. 선고 2017도13263 판결에서 제기된 쟁점을 중심으로 Relatedness", 법제논단, 한국법제연구원, 2018. 8, 15면 이하.).

5) 제9조의3(압수·수색·검증의 집행에 관한 통지) ① 검사는 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우 그 사건에 관하여 공소를 제기하거나 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정을 제외한다)을 한 때에는 그 처분을 한 날부터 30일 이내에 수사대상이 된 가입자에게 압수·수색·검증을 집행한 사실을 서면으로 통지하여야 한다. ② 사법경찰관은 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우 그 사건에 관하여 검사로부터 공소를 제기하거나 제기하지 아니하는 처분의 통보를 받거나 내사사건에 관하여 입건하지 아니하는 처분을 한 때에는 그 날부터 30일 이내에 수사대상이 된 가입자에게 압수·수색·검증을 집행한 사실을 서면으로 통지하여야

는 명문의 규정을 둘 필요가 있다.

그럼에도 불구하고 이러한 입법적 보완을 통하여 디지털 증거에 대한 압수와 그 방법이 모두 해결된 것은 아닐 것이다. 여전히 '수사 비례성' 원칙에 의한 제한 문제가 남아 있기 때문이다. 과거 기업에 대한 압수·수색의 경우 필요하지 않은 자료까지도 모두 압수해 가서 정상적인 업무를 유지할 수 없었던 사례가 디지털 증거의 압수에서도 마찬가지로 발생할 수 있다. 오늘날과 같은 대량 정보처리 시대에 대상자의 중앙 메인 서버와 같은 정보처리장치가 몇 시간 동안 멈춰있다면 그 피해를 산출하기조차 힘들게 되기 때문이다. 수사 목적 달성에 필요한 압수·수색을 수행하되, 가급적 그 이상의 손해를 남기지 않도록 수사목적 달성에만 충실하도록 엄격한 수사 비례성원칙도 반드시 지켜져야 할 것이다.

4. 결론

"잡히면 '폰'부터 던져 부순다"라는 어느 신문기사의 제목은 최근의 수사공권력 집행과정에서 파생되는 스마트폰 압수수색이 새로운 법적, 사회적, 정치적 논란이 되고 있음을 단적으로 대변한다. 현대사회에 있어서 디지털 정보의 생성과 저장이 일상화 됨에 따라 범죄행위자가 사용하던 스마트폰과 컴퓨터 및 그 정보가 저장된 서버에 대한 압수수색은 수사에 있어서 필수적인 절차가 되었고, 전자증거의 수집 여부가 수사의 성패를 가르는 결정적인 요소가 되기도 한 반면, 대량 생산된 전자정보의 보관상 취약성 등으로 말미암아 수사기관이 우연한 기회에 취득한 전자정보에 대한 포괄적 압수수색의 문제가 빈번히 야기된다. 특히 전자정보가 대량 생산되고 이를 보관할 수 있는 대용량 저장장치의 발달로 말미암아, 수사기관이 법원에 발부받은 압수수색영장에 기재된 범죄사실과 관련이 없는 전자정보를 수집할 우려는 점점 더 커지고, 이렇게 수집한 정보에 관하여 수사기관이 이를 반환하지 아니하거나 반환하더라도 사본을 남겨 피의자 또는 제3자에 대한 다른 범죄 수사의 단서 내지 증거로 사용할 경우 필연적으로 새로운 법익침해가 발생할 가능성이 있다.

이러한 전자증거의 수집은 주거의 자유(제16조), 사생활의 비밀과 자유(제17조), 그리고 통신의 비밀(제18조), 그로부터 파생되는 새로운 유형의 기본권으로서 정보

한다.

프라이버시와 정보자기결정권 등 국민의 기본권에 대한 중대한 제한을 수반하지 않을 수 없으며, 그 한계는 헌법상 적법절차, 영장주의 및 비례원칙이 될 것이다.

즉, 실체적 진실발견과 국가형벌권의 적정한 행사를 위하여 전자증거에 대한 적시의 그리고 효과적인 수집은 필수적이라 할 것이나, 비례원칙을 넘어서 과도한 양의 전자정보가 수사기관에게 입수되게 됨으로써 개인의 사생활과 기업의 운영에 심대한 타격을 입힐 우려가 항상 존재하고 있다. 이런 현실에서 미연방대법원 판결과 우리 대법원 판결은 수사기관의 안전 확보 및 증거인멸의 방지라는 공익과 영장주의 원칙 및 개인의 사생활 보호라는 사익이 충돌하는 사안에서, 스마트폰이 사생활에 미치는 영향, 기술적 특수성 등에 대한 고찰을 토대로, 체포에 인접한 스마트폰 수색의 경우, 긴급한 상황의 예외를 제외하고는 적법한 절차에 따른 사전영장을 발부받도록 하였다. 이러한 동향들은 향후 우리나라 수사실무에서 피의자 체포시의 스마트폰 압수, 수색에 관한 법리를 정립하고 입법을 진행하는 데 큰 시사점을 제공한다. 이런 추세에 비추어 현재 거듭된 관련 법 개정과정에서 압수수색의 요건이 강화되고, 전자정보에 대한 압수수색 방법과 절차 등이 점차 정비되고 있는 것은 다행스러운 일이다.

다만, 이러한 제도적 개선에 더하여 앞으로 모든 IT 관련 부서와 기업, 국가와 지자체, 공공기관과 사기업체, 개인 등 너나 할 것 없이 모든 업계, 특히 해외 출장에 나서는 사람들은 스마트폰 속 데이터가 공식적인 조사 과정에서 모두 추출될 수 있다는 것을 가정하고 대비해야 한다. 더불어 스마트폰 개인정보보호에 관한 대국민 의식을 강화하는 국가차원의 교육과 홍보도 적극 행해져야 한다.[6)]

---

6) 성중탁, 스마트폰 압수, 수색에 대한 헌법상 쟁점, IT와 법연구, 경북대학교 IT법연구소, 2019. 3.

【토론문】

“모바일 전자증거 압수수색과 적법절차, 최근 쟁점과 법원 판례의 동향”에 대한 토론문

김 종 현*

먼저 토론의 기회를 주신 헌법재판연구원과 한국헌법학회에 깊이 감사드립니다.

결국 찾기는 했지만, 스마트폰을 잃어버리고 크게 당황했던 일이 기억납니다. 누군가 제 스마트폰을 습득할 경우 그 동안 촬영한 사진·동영상, 다른 사람들과의 소통기록, 각종 거래내역, 문서작업내역 등이 한꺼번에 노출될까봐 우려하였습니다. 약간의 과장을 보탠다면 모바일 전자기기는 소유자의 발자취 그 자체라고도 볼 정도로 다양하고 많은 정보를 가지고 있으며, 그렇기에 이를 압수·수색할 때에는 특히나 기본권을 침해하지 않고 적법절차원칙을 준수해야 한다는 생각을 가져 봅니다.

몇 년 전 영장주의를 연구하고 최근 적법절차원칙에 관한 연구를 수행하였음에도 모바일 전자증거 압수수색의 쟁점과 동향을 잘 알지 못하고 있었습니다. 발표문을 읽으면서, 모바일 전자증거의 압수수색에 관한 최신 판례의 동향 및 일선 실무에 관하여 많이 배울 수 있었습니다. 부족한 견문을 넓혀주신 발표자님께 감사의 말씀을 드립니다. 이하에서는 발표문을 읽고 가지게 된 몇 가지 생각을 말씀드리도록 하겠습니다. 다만 토론자가 영장실무 경험이 없고 수사·재판에 관한 세세한 지식이 부족하기에, 일반 독자로서 큰 틀에서 말씀드릴 수밖에 없다는 점 양해를 구합니다.

1. 무관정보 혼재의 문제에 관하여: 영장주의와 적법절차

소개해주신 2021모1586 결정에서는 “범죄 혐의사실과 관련 있는 정보를 선별하여 압수한 후에도 그와 관련이 없는 나머지 정보를 삭제·폐기하지 아니한 채 그대로 보관하고 있는 것”이 위법하며, 그러한 위법성이 치유될 수 없다고 판단하였습니다.

* 헌법재판소 헌법재판연구원 책임연구관

대법원에 따르면 이는 (1) 압수 대상이 아닌 정보까지 영장 없이 취득하는 것이며 (2) 상세목록 작성·교부의무와 삭제·폐기·반환의무를 형해화하여 영장주의 및 적법절차원칙을 중대하게 위반한 것입니다.

영장주의의 본질은 그것이 헌법상 원리로 자리매김한 역사적 배경으로부터 도출할 수 있을 것입니다. 영장주의가 영국에서 형성되어 미국 수정헌법 제4조에 규정된 경과를 살펴보면, 영장주의는 무엇보다도 일반영장의 남용에 따른 폐해를 방지하는 데 주된 도입목적이 있었다고 생각합니다. 일반영장은 사람, 장소, 사물 등 대상을 특정하지 아니한 채 영장소지자로 하여금 원하는 사람과 장소를 무제한적으로 압수·수색할 수 있게 하였으며, 영장이라는 형식만으로는 기본권을 충실히 보호하기 어렵다는 역사적 경험이 일반영장금지원칙의 등장으로 이어졌습니다.[1)]

일반영장의 금지가 헌법상 영장주의의 요체임을 인정한다면, 압수수색의 대상이 되는 전자정보를 구체적으로 특정하지 아니한 채 압수·수색영장을 청구하여 발부받아 집행하는 것은 헌법상 영장주의에 반한다고 생각합니다. 그런데 만약 (1) 영장을 청구하여 발부받는 단계에서는 압수·수색의 대상이 되는 전자정보를 구체적으로 특정하였으나, (2) 기술적인 문제 등으로 부득이 범죄 혐의사실과 무관한 정보까지 일단 탐색·복제·출력하였고,[2)] (3) 이후 나머지 전자정보를 삭제·폐기·반환하지 아니한 경우에(2021모1586 사안) 이를 헌법상 영장주의 위반이라고 평가해야 할지 고견을 듣고 싶습니다. 학계에서는 영장 발부 이후인 강제처분의 집행과정이나 집행 이후의 단계에서, 수사기관의 집행 남용을 방지하는 통제규범을 두고 기본권을 보호하는 것이 영장주의의 범위 내인지 아니면 범위 밖인지가 논의되고 있기도 합니다.[3)]

관점에 따라서는 영장 청구 및 발부가 헌법상 영장주의 원칙에 부합하게 이루어졌으나, 사후적으로 (절차적) 적법절차원칙을 위반하고 및 과잉금지원칙에 반하여 기본권을 과도하게 침해한 것[4)]으로 볼 여지도 있을 것 같습니다. 2021모1586 결정은 영장주의 원칙을 중대하게 위반하였다고 보았는바, 영장주의는 영장의 신청·발부

---

1) 김종현, 영장신청권자 규정에 관한 헌법적 연구, 법조, 제68권 제4호, 2019, 164-170쪽.

2) 혹은 형사소송법 제106조 제3항에 따라 정보저장매체 등을 압수할 수도 있겠습니다.

3) 이흔재, 제3자 보관 전자정보에 대한 압수·수색영장의 집행과 피의자의 절차적 권리, 형사법의 신동향, 제76호, 2022, 164쪽.

4) 범죄 혐의사실과 관련된 정보만을 추려 보관할 수도 있다는 측면에서, 개인정보자기결정권, 사생활의 비밀과 자유 등 기본권이 과잉금지원칙(특히 침해의 최소성 원칙)에 반하여 과도하게 이루어졌다고 볼 여지가 있겠습니다.

뿐만 아니라 집행 단계에서도 관철되어야 한다는 입장으로 생각됩니다.[5)]

어떠한 입장을 취하든 2021모1586 결정에서와 같이 압수·수색하여 취득한 전자정보가 위법수집증거이며 위법성이 치유되지 않는다는 결론에 있어서는 다르지 않겠습니다. 다만 헌법상 영장주의가 신청 및 발부 단계에 그치며 이후의 문제는 적법절차원칙 위반(절차적 측면)과 과잉금지원칙 위반(실체적 측면)으로 평가해야 하는지, 아니면 영장주의는 영장의 집행 및 후속처리과정(상세목록 작성교부, 무관정보의 삭제·폐기·반환 등)까지 관철하는지에 관하여 상이한 입장이라 하겠습니다.

2. '실질적 피압수자', '피의자의 소유·관리에 속하는 정보저장매체'에 관하여

2016도348 전원합의체 판결에서는 피해자 등 제3자가 '피의자의 소유·관리에 속하는' 정보저장매체를 임의제출한 경우 실질적 피압수자인 피의자에게 참여권을 보장하고 절차적 권리 보장을 위한 적절한 조치가 이루어져야 한다고 하였습니다.

2021도11170 판결에 따르면, 피의자가 해당 정보저장매체를 현실적으로 지배·관리하며, 그 정보저장매체에 저장된 전자정보에 대하여 실질적인 압수·수색의 당사자로 평가될 수 있어야 '피의자의 소유·관리에 속하는 것'으로 인정됩니다. 그리고 그 해당 여부는 민사법상 권리의 귀속에 따른 법률적·사실적 판단이 아니라, 압수·수색 당시 외형적·객관적으로 인식 가능한 사실상의 상태를 기준으로 판단한다고 합니다.

그런데 제3자가 외장하드나 USB와 같은 정보저장매체를 임의제출하였을 때, 외형적·객관적으로 누가 해당 정보매체를 현실적으로 지배·관리하는지를 어떻게 판단할 수 있을지 궁금하였습니다. 일반적으로 제3자(특히 피해자)의 임의제출은 피의자의 의사에 반하여 혹은 피의자가 잘 모르는 가운데 이루어질 터이므로, 피의자가 압수·수색 당시 해당 정보저장매체를 현실적으로 지배·관리하고 있다고 보기는 쉽지 않을 것 같습니다.

또한 발표문에 언급되었듯 전자정보 저장매체는 매우 작아졌고 스마트폰의 경우 데이터의 현장 선별이 곤란한 경우가 많을 것입니다.[6)] 그렇다면 (저장매체 외부에

---

5) 다만 이 사안의 경우 압수·수색영장이 휴대전화 등에 있는 전자정보의 압수 대상 및 방법에 대해 '저장매체 자체를 반출하거나 복제본으로 반출하는 경우에도 혐의사실과 관련된 전자정보만을 출력 또는 복제하여야 하고, 완료된 후에는 지체 없이 피압수자 등에게 압수 대상 전자정보의 상세목록을 교부하여야 하고, 그 목록에서 제외된 전자정보는 삭제·폐기 또는 반환하고 그 취지를 통지하여야 한다.'고 제한하였다는 점이 고려되어야 하겠습니다.

스티커 등에 소유자의 이름을 표시하여 부착한 경우 등이 아니라면) 외형적·객관적으로 해당 정보저장매체에 저장된 전자정보와 관련하여 실질적인 압수·수색 당사자가 누구인지를 파악하는 것도 용이하지만은 않을 수 있다는 생각이 들었습니다.

3. 임의제출과 접근권한정보의 제출에 관하여

발표문에 따르면 모바일 기기가 오늘날 수사기관 압수대상물의 과반을 차지하며, 비밀번호나 화면잠금패턴 등 접근권한정보를 확보하지 못하면 압수는 실패합니다.[7] 관련하여, 휴대전화의 비밀번호 제출을 거부하는 피의자를 처벌하는 법안(일명 '휴대전화 비밀번호 강제해제법')이 검토되었으나 법조계에서 거센 비판이 제기된 바도 있습니다. 자기부죄금지원칙에 반하며 피의자의 방어권을 크게 위축시킬 수 있다는 이유에서였습니다.[8]

헌법재판소에 따르면 진술거부권은 자기부죄거부의 특권(privilege against self-incrimination)에서 유래하는 권리입니다.[9] 그런데 헌법상 진술거부권이 질문과 답변이라는 언어적 영역이라면, 자기부죄거부특권은 자신의 죄를 입증할만한 서류, 자료, 증거 등을 제출하지 않는 것도 포함하는 증거법상의 원칙이라고 합니다.[10]

최근 수사기관의 스마트폰 비밀번호 해제를 구체적으로 검토한 선행연구가 있어 주목됩니다. 그에 따르면 사안의 진실규명과 유죄의 증명책임은 검사가 부담하므로, 수사기관은 입수한 스마트폰의 접근권한정보를 해제하기 위하여 여러 방법을 동원

---

6) 사견으로는 스마트폰뿐만 아니라 외장하드, USB에도 다양한 정보가 대용량 저장되어 있는 경우가 많기에, 현장에서 선별하기가 쉽지만은 않을 것 같습니다.

7) 최근 우리나라에서는 피의자가 스마트폰 비밀번호를 함구하거나 잠금해제 요구를 거부하여, 수사기관이 잠금을 해제하려 했으나 실패하고 무혐의 처분 때 환부한 사례가 널리 알려져 있습니다. 손현성, 검찰, 2년간 못 푼 한동훈 아이폰 돌려줘... "무혐의 처분시 반환이 원칙", 동아일보, 2022. 8. 7, https://www.hankookilbo.com/News/Read/A2022080712540005866(최종방문일 2023. 5. 12.).

8) 강한, 법률가들 "휴대전화 비밀번호 제출 강제는 위헌", 법률신문, 2020. 11. 14, https://m.lawtimes.co.kr/Content/Article?serial=165705(최종방문일 2023. 5. 12.).

9) 헌재 2001. 11. 29. 2001헌바41, 판례집 13-2, 699, 705. 진술거부권은 형사소송법 제244조의3(진술거부권 등의 고지), 제283조의2(피고인의 진술거부권), 민사소송법 제314조, 형사소송법 제148조, 국회에서의 증언·감정 등에 관한 법률 제3조에 의하여 구체화됩니다. 김하열, 헌법강의, 박영사, 2023, 406쪽.

10) 이정민, 스마트폰 비밀번호 해제 관련 자기부죄거부특권 고지의 필요성, 법학논총, 2022, 114쪽.

할 수 있습니다.[11] 그런데 형사소송법 제120조 제1항은 “압수·수색영장의 집행에 있어서는 건정을 열거나 개봉 기타 필요한 처분을 할 수 있다.”라고 규정하는바, ‘필요한 처분’은 수사기관이 집행과정에서 하는 적극적 행위를 의미하며 피압수자 등은 그에 대한 수인의무가 있을 뿐이라고 합니다. 따라서 수사기관이 피압수자에게 비밀번호를 요구할 권리나 피압수자의 협조의무는 인정되지 않는다는 것입니다.[12]

이 연구는 검찰의 “디지털 증거의 수집·분석 및 관리규정”[대검찰청예규 제1151호](별지3)에 의한 ‘정보저장매체 제출 및 이미징 참관여부 확인서’에 비밀번호 제출을 거부할 수 있다거나 동의를 철회할 수 있다고 고지하는 내용이 없다고 합니다.[13] 이 연구는 (1) 수사기관이 비밀번호, 암호 등이 진술거부권 대상임을 구체적으로 고지해야 하며, (2) 매스미디어나 교육 등을 통해 스마트폰 비밀번호 협조의무가 없으며 수사는 수사기관에서 하다는 점을 각인시킬 필요가 있다고 제안합니다. 또한 비밀번호를 제출했다고 하여 스마트폰 내 모든 정보를 제출한 것은 아니며, 정보를 탐색·복제·수집할 때 피의자·피고인·변호인의 참여권을 보장해야 한다고 합니다.[14] 현행 “정보저장매체 제출 및 이미징 참관여부 확인서”에도 비밀번호 등이 진술거부권 대상이라거나 동의를 철회할 수 있다는 고지는 없는 듯합니다.

한편 영국의 「수사권한규제법(Regulation of Investigatory Powers Act 2000」 제49조 제2항, 프랑스 형법 제434-15-2조, 호주 형법(Crimes Act 1914 (Cth)) 제3LA조는 일정한 요건 하에 스마트폰 잠금해제에 협조하도록 강제하고 있다고 합니다. 공개를 거부하는 경우 처벌까지 하는 규정들로 파악됩니다.[15] 현재 우리나라 수사기관의 디지털 증거 수집분석 관련 서식에 개선이 필요하다고 보시는지, 영국·프랑스·호주와 같이 잠금해제 협조를 강제하는 입법이 이루어질 경우 진술거부권 침해라고

11) 이정민, 스마트폰 비밀번호 해제 관련 자기부죄거부특권 고지의 필요성, 법학논총, 2022, 119쪽.

12) 이정민, 스마트폰 비밀번호 해제 관련 자기부죄거부특권 고지의 필요성, 법학논총, 2022, 121쪽. 또 스마트폰 압수수색은 집행과정에서 필요성, 비례성, 관련성이 인정되는 범위에서 이루어져야 하며, 특히 침해되는 프라이버시와 수사로 얻을 수 있는 공익을 비교형량해야 한다고 합니다. 같은 글, 122쪽.

13) 이정민, 스마트폰 비밀번호 해제 관련 자기부죄거부특권 고지의 필요성, 법학논총, 2022, 135쪽.

14) 이정민, 스마트폰 비밀번호 해제 관련 자기부죄거부특권 고지의 필요성, 법학논총, 2022, 136쪽.

15) 허순철, 미국법상 스마트폰 잠금 해제 거부와 법원모욕, 원광법학, 제39권 제1호, 2023, 5쪽.

보아야 할 것인지[16]에 관한 발표자의 고견을 여쭙습니다.

[별지 제3호 서식] 정보저장매체 제출 및 이미징 등 참관여부 확인서

[정보저장매체 제출 및 이미징 등 참관여부 확인서]

피압수자 (임의제출자)	성 명 : 생년월일 : 연 락 처 :		
기기의 종류 등	기기의 종류 : 제조사 및 모델 (S/N) : (모바일의 경우) 전화번호 :		
[현장] 정보저장매체 제출	피압수자 또는 변호인은, ■선별 압수 및 전부 복제본을 압수하는 것이 불가능하거나 현저히 곤란하여 매체 반출을 해야 하는 사유에 대한 설명을 [☐ 고지받았습니다. (서명) ☐ 고지받지 못했습니다. (서명)] ■이미징 및 유관 정보의 선별 과정에 자유롭게 참여할 수 있고, 참관 후 선별 압수 절차 전반에 대한 의견을 제출할 수 있음을 [☐ 고지받았습니다. (서명) ☐ 고지받지 못했습니다. (서명)]		
이미징 등 참관	■위와 같이 압수 또는 임의제출 된 정보저장매체에 대한 전부 복제·이미징, 전자정보의 탐색 및 복제(출력) 등 과정에 [☐ 참관하겠습니다. (서명) ☐ 참관하지 않겠습니다. (서명)]		
	참관 희망시	참관 범위	정보저장매체 전부복제·이미징 【 】 전자정보탐색 및 복제(출력) 【 】
		참관 예정자	성 명 : 생년월일 : 연 락 처 :

※ (참관의 경우) 유의사항

- 정당한 사유 없이 예정된 참관 기일에 출석하지 않는 경우에는 신뢰성과 전문성을 담보할 수 있는 상당한 방법으로 집행할 수 있음

※ (모바일 기기의 경우) 유의사항

- 기기의 이미징 과정에서 분해, 재조립, JTAG 연결, 펌웨어 체인지 등의 방법이 필요한 모델의 경우에는 기기의 손상 또는 데이터가 초기화 될 가능성이 있음
- 이미징 후 일부 기기는 보안 솔루션 기반 앱(삼성knox, 삼성페이 등)을 사용할 수 없게 되거나, 그와 관련된 기존 데이터는 유실 될 가능성이 있음
- 애플 기기(iOS 11버전 이상)의 경우 백업 암호 분실 시 모든 설정이 재설정 될 수 있음

보안 솔루션 기반 앱의 사용 여부

보안폴더 ☐	삼성페이 ☐	기타 ( )

- **자동 잠금 해제, 모바일 기기 및 백업 파일(아이폰 등)의 비밀번호 등 표시**

▣ 화면잠금번호(4자리이상 숫자) : *1234* ▣ 비밀번호(4자리이상 문자 또는 숫자): *spo1234*
▣ 패턴 : *0-1-2-5-8* ▣ 백업데이터 비밀번호 : *123456*

위 정보저장매체의 제출 및 참관 등 절차를 확인하고, 압수된 전자정보는 수사 또는 재판 목적 소멸 시 폐기됨을 고지받았음을 확인합니다.

20 . . .

피압수자, 임의제출자 등 : (서명)

검찰수사관 : (서명)

16) 한국에서 피의자나 피고인에게 스마트폰 비밀번호를 말하라고 강요한다면 헌법 제12조 제2항 후문의 진술거부권을 침해하는 것이라는 평가로 허순철, 스마트폰 비밀번호 해제와 진술거부권, 공법연구, 제48집 제1호, 2019, 215쪽.

4. 토론을 마치며

첨단수사 및 그에 대한 사법적 통제에 관하여 잘 알지 못하던 차에 발표문을 읽고 토론문을 작성하며 부족한 견문을 넓힐 수 있었습니다. 또한 지난 몇 년 동안 모바일 전자증거 압수수색과 관련하여 의미 있는 판결이 많았음을 알게 되었습니다. 과학기술의 급속한 발전 속에서도 형사절차상 인권이 두터이 보호될 수 있기를 기대하며 토론을 마칩니다. 감사합니다.