토론회 자료집

수사기관 전자정보 보관 문제점과 대응방안 모색을 위한 정책토론회

일시 | 2024년 7월 2일(화) 오전 10시

장소 | 국회 의원회관 제2간담회실

주최 | 더불어민주당 박주민 국회의원
참여연대
민주사회를 위한 변호사모임 사법센터

목차

프로그램

10:00	좌장	한상희 건국대 법학전문대학원 교수·참여연대 공동대표
	인사	더불어민주당 박주민 국회의원
10:05	발제	**전자정보의 압수·수색과 무관정보의 배제 – 최근의 디-넷(D-NET) 사태를 계기로**
		오병두 홍익대 법과대학 교수
10:30	발제	**전자정보의 압수 및 보관·폐기에 관한 개선방안**
		권경선 서울중앙지방법원 판사
10:55	토론	이범준 뉴스타파 객원기자
		이황희 성균관대 법학전문대학원 교수
		김면기 경찰대학 법학과 교수
		이창민 변호사_민주사회를위한변호사모임 검·경개혁소위원장
11:35	질의응답	
12:00	폐회	

전자정보의 압수·수색과 무관정보의 배제 – 최근의 디-넷(D-NET) 사태를 계기로

오병두 / 홍익대 법과대학 교수

I. 들어가며

최근 대통령 명예훼손 사건의 수사와 관련하여 언론사 '뉴스버스'를 입수·수색하는 과정에서 휴대전화, 노트북, PC를 무차별적 압수·수색하였다.[1] 압수된 휴대전화 등에 들어 있는 전자정보[2]가 '통째로' 이미지파일 형태로 장기간 보존되어 활용되고 있음[3]이 드러나면서 검찰의 '디지털 수사망', 즉 '디-넷'(D-NET)이 언론의 주목을 받았다. 특히 디지털포렌식을 위해 전자정보를

[1] '뉴스버스' 사태에서의 집행방법에 대한 사실보고와 문제제기로는 봉지욱(뉴스타파 기자), "대통령의 압수수색", 『압수된 인권, 복제되는 삶』(전자정보 압수·수색에 관한 특례법 제정을 위한 입법 토론회 자료집, 조국혁신당), 2024. 6. 17, 13-19면.

[2] '디지털증거'나 '전자정보'에 관하여는 다양한 정의가 있고 아직 확정되어 있지는 않다. 여기에서 이를 상론하기는 어렵다. 잠정적으로 우리의 논의와 직접 관련된 「디지털 증거의 수집·분석 및 관리 규정」의 정의를 활용하기로 한다. 대법원은 '전자증거'라는 용어는 사용하나, '디지털증거'라는 표현은 거의 사용하지 않는다. 검찰실무와 관련하여 하급심판결에서는 '디지털증거'라는 표현이 종종 발견된다(이를 보여주는 최근 판결로는 대법원 2023. 6. 1. 선고 2020도2480 판결 등).

＊「디지털 증거의 수집·분석 및 관리 규정」(2022. 5. 18.) 제3조(정의) 이 규정에서 사용하는 용어의 뜻은 다음과 같다.

1. "전자정보"란 정보저장매체등에 기억된 정보를 말한다.
2. "디지털 증거"란 범죄와 관련하여 디지털 형태로 저장되거나 전송되는 증거로서의 가치가 있는 정보를 말한다.

[3] 예컨대, "'디넷에 저장된 12년 전 전자 정보도 현재까지 남아'", Newsverse 2024. 4. 29, <https://www.newsverse.kr/news/articleView.html?idxno=5261>, 최종검색: 2024. 6. 20.

저장하고 수사에 활용하는 '디-넷' 서버의 존재는 '불법사찰' 논란을 야기하면서[4] 과거 검찰의 행태를 빗대어 '디지털 캐비닛'으로 불리기도 하였다.[5]

논란이 불거지자 대검찰청도 적극적으로 해명에 나섰다. 그 내용은 "'전체 이미지파일이 없으면 공소유지에 곤란을 겪을 수 있다'고 거듭 주장하며 '무관정보는 별건으로 사용하지 않으며 (이미지파일은) 해당 검사실을 포함한 어느 누구도 접근·사용할 수 없도록 기술적·절차적으로 엄격하게 통제'하고 있다"는 것이었다.[6]

그러나 언론보도에 따르면, 휴대전화나 노트북을 압수당했던 사람들의 경험은 이와 다르다. 특히 휴대전화의 경우, 수사과정에서 포렌식 절차가 끝났음에도 — 더 정확하게는 디지털포렌식을 통해 디지털증거의 선별절차가 끝났음에도, 압수목록에 넣어서 — 돌려주지 않는 일이 적지 않다고 한다.

이번 '뉴스버스 사태'로 드러난 여러 문제는 실상 새로이 발생한 것이거나, 새롭게 알려진 것은 아니다. 특히 "압수수색 영장 범위를 벗어난 전자정보까지 복제(이미징)해 보관하는 관행"[7]은 광범위한 개인의 정보가 수사기관에 넘어가는 문제가 있다. 이와 같은 전자정보에 대한 검찰·경찰의 압수·수색 실무는 이미 오래 전부터 비판의 대상이 되어 왔고 또한 그에 대한 대응도 다양하게 모색되어 왔다.

2021년 초 언론에서도 이 문제는 심도 깊게 다루어진 바 있다. 경향신문은 휴대전화의 압수·수색과 관련된 문제점을 집중적으로 다루었다.[8] 여기에서 다루어진 쟁점은 ① 예외적인 매체압수의 원칙화, ② 이미징 이후 압수된 매체의 반환 지연 내지 거부, ③ 압수된 전자정보(특히 '이미징') 무차별적, 무기한의 보관, ④ 압수된 전자정보에 대한 임의적 복제와

---

[4] "[단독] 검찰, 수사권 이용 민간인 불법사찰…휴대전화 정보 불법 수집·관리", Newsverse 2024. 3. 21, <https://www.newsverse.kr/news/articleView.html?idxno=5051>, 최종검색: 2024. 6. 20. 또한 같은 화면의 "[특종] 검찰, 조직적 민간인 불법사찰" 항목의 기사들 참고.
[5] "대법원, 검찰의 '디지털 캐비닛' 수사에 제동 판결", 경향신문 2024. 4. 26, <https://www.khan.co.kr/national/court-law/article/202404261201001>, 최종검색: 2024. 6. 20.
[6] "[단독] 검찰, 압수한 전자정보 '입맛대로' 저장했다", 한겨레 2024. 3. 25, <https://www.hani.co.kr/arti/society/society_general/1133752.html>, 최종검색: 2024. 6. 20.
[7] "압수수색 휴대폰·노트북 정보 통째 보관하는 검찰…위법 논란에 피의자 동의도 허술", 경향신문 2024. 3. 27, <https://www.khan.co.kr/national/court-law/article/202403270600171>, 최종검색: 2024. 6. 20.
[8] "(1) 영장엔 버젓이 '암호 푼 상태로'…내 정보, 풀라면 풀어야 하나", 경향신문 2021. 3. 17, <https://www.khan.co.kr/national/court-law/article/202103170600015; "(2) '죄' 밝힐 정보만? 현실은 '인생' 정보 통째로 압수", 경향신문 2021. 3. 19, <https://www.khan.co.kr/national/national-general/article/202103190600045>; "(3) 압수된 데이터는 삭제되지 않는다", 경향신문 2021. 3. 29, <https://www.khan.co.kr/national/national-general/article/202103290600005>; "(4) 지문과 홍채 정보도 압수되고 있다", 경향신문 2021. 4. 2, <https://www.khan.co.kr/national/national-general/article/202104020600005>; "(5) '네 정보 내놔'를 멈출 5가지 제안", 경향신문 2021. 4. 7, <https://www.khan.co.kr/national/national-general/article/202104070600015>, 이상 최종검색: 2024. 6. 20.

참여권이 배제된 상태의 탐색, ⑤ '우연한 발견'[9]을 내세워 압수된 전자정보를 활용한 별건수사 개시 등을 위시하여, ⑥ "지문·비번 등 통신기기 잠금 해제 압박"이나 생체정보(지문, 홍채 등)의 수집 등의 압수수색 절차상의 문제에 대한 비판[10]을 포함한다. 나아가 이에 대한 대안으로 ① "수색영장과 압수영장 분리", ② "체포 상태에서 [휴대전화] 임의제출 불법화", ③ "포렌식과 수사 과정 분리"와 함께, ④ 카카오, 네이버 등 인터넷 서비스 사업자(ISP)를 통한 "제3자 통한 우회압수 통제" 등을 다루었다.[11] 학계와 실무에서 논의되는 쟁점과 대안을 거의 망라한다.

같은 해인 2021. 10. 13.「대법원 사법행정자문위원회」(재판제도분과위원회)의 의제인 "전자증거에 관한 압수·수색 실무 개선방안"에서도 이 문제가 다루어졌다.[12] 그 구체적인 내용으로는 ① 영장 발부 단계에서 법관의 대면심리 제도를 도입할 것,[13] ② 영장 집행 단계 관련하여 (ⅰ) '정보'를 압수·수색 대상으로 명문화하고, (ⅱ) "압수방법에 관한 법원의 사전규제" 방안(검색어 등을 특정하여 영장 발부, 당사자의 참여권 보장), (ⅲ) "영장 사본 교부 제도", (ⅳ) 영장 집행시 "이해관계인이 참여하여 '의견 진술'을 할 수 있는 제도", (ⅴ) 제3자 보관정보의 압수수색 시 "정보주체의 참여권 보장 제도" 등을 도입할 것을 제안하였다. ③ 영장 집행 후의 단계에서는 (ⅰ) 압수물 또는 압수목록의 법관 제출 제도(도입 필요성이 낮다고 검토), (ⅱ) "범죄무관 정보" 폐기·삭제 필요성 등을 검토하였다. 기타 ④ "압수수색영장 양식의 개선"과 관련하여 (ⅰ) 검색어 특정 등 하여 영장발부하는 방안"을 제안하고, (ⅱ) "휴대전화 압수수색 절차의 적법성 확보 문제"[14] 등을 검토하였다.

---

[9] 대법원 2015. 7. 16. 자 2011모1839 전원합의체 결정. "전자정보에 대한 압수·수색에 있어 그 저장매체 자체를 외부로 반출하거나 하드카피·이미징 등의 형태로 복제본을 만들어 외부에서 그 저장매체나 복제본에 대하여 압수·수색이 허용되는 예외적인 경우에도 혐의사실과 관련된 전자정보 이외에 이와 무관한 전자정보를 탐색·복제·출력하는 것은 원칙적으로 위법한 압수·수색에 해당하므로 허용될 수 없다. 그러나 전자정보에 대한 압수·수색이 종료되기 전에 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우라면, 수사기관으로서는 더 이상의 추가 탐색을 중단하고 법원으로부터 별도의 범죄혐의에 대한 압수·수색영장을 발부받은 경우에 한하여 그러한 정보에 대하여도 적법하게 압수·수색을 할 수 있다고 할 것이다."

[10] "(4) 지문과 홍채 정보도 압수되고 있다", 경향신문 2021. 4. 2, <https://www.khan.co.kr/national/national-general/article/202104020600005>, 최종검색: 2024. 6. 20.

[11] "(5) '네 정보 내놔'를 멈출 5가지 제안", 경향신문 2021. 4. 7, <https://www.khan.co.kr/national/national-general/article/202104070600015>, 최종검색: 2024. 6. 20.

[12] 대법원 사법행정자문위원회, "제16차 회의자료", 2021. 10. 13, <https://www.scourt.go.kr/supreme/news/NewsViewAction2.work?pageIndex=2&searchWord=&searchOption=&seqnum=14&gubun=943>, 최종검색: 2024. 6. 20.

[13] 이에 따라 대법원은 압수수색영장 발부 시 대면심리제도 도입을 위한「형사소송규칙」개정안을 입법예고하였으나 검찰, 경찰, 공수처의 반대로 진척되지 못하고 있는 상태이다. 그 경과에 관하여는 "압수수색영장 대면심리제 도입될까", 주간경향 2024. 1. 1, <https://m.weekly.khan.co.kr/view.html?med_id=weekly&artid=202312250700001&code=115#c2b>, 최종검색: 2024. 6. 20.

[14] "피의자가 접근권한정보 등을 스스로 입력하여 수사기관이 해당 전자정보를 제한 없이 이용할 수 있는 상태에 두도록 요청하는 방법"이나 "암호화를 해제한 전자정보를 제출할 것을 요청하는 방법[을] 내용으로 하는 영장"이

여기에서 ‘디-넷’과 관련하여 특히 주목되는 것은 “범죄무관 정보” 폐기·삭제 방안이다. 이와 관련해서 「재판제도분과위원회」는 「형사소송법」 제218조의2(압수물의 환부, 가환부)[15]와 「디지털 증거의 수집 · 분석 및 관리 규정」 제54조(폐기대상)[16], 「(경찰청) 디지털 증거의 처리 등에 관한 규칙」 제35조(전자정보의 삭제 · 폐기)[17] 등의 규정이 있음을 들어 “현행 영장 별지에 수사기관에서 무관정보의 폐기 의무를 명시하고 있으므로 즉각적인 형사소송법 내지 형사소송규칙 개정의 필요성이 크지 않다고 검토”하였다.[18]

수사기관의 ‘혐의사실과 관련된 전자정보’(무관정보) 활용에 관한 「재판제도분과위원회」의 이러한 판단은 작금의 상황에 비추어보면 상당한 거리감이 느껴진다. 그 근저에는 상황과 문제 인식의 차이가 있다. 이 문제에 대한 해결방안은 그 인식 차이와 무관하지 않다. 무관정보 활용 그리고 그 법적 통제에 관한 이론과 실무 그리고 대안은 상호 연결되어 있다.
‘디-넷’(D-NET)의 문제도 마찬가지이다. 이하에서 광범한 무관정보의 사용으로 문제되고 있는 ‘디-넷’의 운영현황과 근거규정을 살펴보고, 압수·수색의 법적 규율에 비추어 무관정보 활용의 문제점과 그에 대한 대책을 이야기하고자 한다.

진술거부권을 침해한다는 주장(조성훈, “전자정보 접근 방법의 법적 문제 —진술거부권과 관계를 중심으로—”, 법조 제69권 제6호, 법조협회, 2020.12, 160면 이하)에 대하여 검토하였다.

[15] 「형사소송법」 제218조의2(압수물의 환부, 가환부) ① 검사는 사본을 확보한 경우 등 압수를 계속할 필요가 없다고 인정되는 압수물 및 증거에 사용할 압수물에 대하여 공소제기 전이라도 소유자, 소지자, 보관자 또는 제출인의 청구가 있는 때에는 환부 또는 가환부하여야 한다.

[16] 「디지털 증거의 수집·분석 및 관리 규정」(대검찰청예규 제1285호, 2022. 5. 18. 개정·시행) 제54조(폐기대상) ① 다음 각 호에 해당하는 디지털 증거는 본 장에서 규정한 절차에 따라 업무관리시스템에서 폐기한다.
1. 수사 또는 재판 과정에서 범죄사실과 관련성이 없는 것으로 확인된 경우
2. 압수의 원인이 된 사건에 대한 기소 · 불기소 등 종국처분에 따라 계속 보관할 필요성이 없다고 인정되는 경우
3. 판결이 확정되어 계속 보관할 필요성이 없다고 인정되는 경우
② 제1항에도 불구하고 다음 각 호의 사유가 있는 경우에는 압수의 원인이 된 사건의 공소시효가 완성될 때까지 디지털 증거를 폐기하지 않을 수 있다.
1. 압수의 원인이 된 사건과 형사소송법 제11조에 따라 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 경우
2. 압수의 원인이 된 사건이 기소중지처분 또는 참고인중지처분이 된 경우
3. 불기소처분을 한 사건 또는 무죄판결이 확정된 사건 중 공범 등에 대한 수사를 계속할 필요가 있다고 인정되는 경우

[17] 「(경찰청) 디지털 증거의 처리 등에 관한 규칙」(경찰청훈령 제1086호, 2023. 7. 4. 개정·시행) 제35조(전자정보의 삭제 · 폐기) ① 증거분석관은 분석을 의뢰한 경찰관에게 분석결과물을 회신한 때에는 해당 분석과정에서 생성된 전자정보를 지체 없이 삭제 · 폐기하여야 한다.
② 경찰관은 제1항의 분석결과물을 회신받아 디지털 증거를 압수한 경우 압수하지 아니한 전자정보를 지체 없이 삭제 · 폐기하고 피압수자에게 그 취지를 통지하여야 한다. 다만, 압수 상세목록에 삭제 · 폐기하였다는 취지를 명시하여 교부함으로써 통지에 갈음할 수 있다.
③ 경찰관은 사건을 이송 또는 송치한 경우 수사과정에서 생성한 디지털 증거의 복사본을 지체 없이 삭제 · 폐기하여야 한다.
④ 제1항부터 제3항까지에 따른 전자정보의 삭제 · 폐기는 복구 또는 재생이 불가능한 방식으로 하여야 한다.

[18] 대법원 사법행정자문위원회, “제16차 회의자료”, 3면과 34면.

II. 검찰의‘디-넷’(D-NET) 운영 현황

1. ‘디-넷’(D-NET) 개요

‘디-넷’(D-NET)은 그 운영실태가 검찰실무가의 논문이나 대법원 판결을 통해 단편적·간접적으로 드러날 뿐 그 전모가 잘 알려져 있지 않다. 관련 법령과 자료를 중심으로 간단히 개요를 보기로 한다.

이 ‘디-넷’은 검찰의 ‘전국 디지털 수사망’(이하 ‘디지털 수사망’이라 한다)을 말한다. 이는 검찰이 운영하는 전자정보의 저장·활용을 위한 서버이다. 이 ‘디지털 수사망’에 관해서는 「전국 디지털수사망 운영지침」[19](대검찰청예규 제1432호, 2024. 5. 31. 최종 개정·시행)에서 정하고 있다. 같은 예규 제3조 제1호는 이 ‘디지털수사망’을 “대검찰청 디지털수사과와 각 지역 거점청(디지털포렌식팀이 설치된 각 지역의 검찰청을 의미한다) 디지털포렌식팀간에 별도의 광역분석망을 통하여 운용되는 운영시스템과 디지털 증거 저장소, 디지털 증거 보관소 및 검찰망을 통하여 각 검찰청과 연계된 운영시스템”으로 정의한다.[20]

이 ‘디지털수사망’은 “디지털 수사 통합업무관리시스템(DFIS II), 디지털 증거관리시스템, 통합디지털 증거분석 시스템(IDEAS), 원격디지털수사공조시스템 등으로 구성”된다.[21] 이 ‘디지털수사망’을 구성하는 ‘디지털수사통합업무관리시스템’에 대해서는 같은 대검찰청 예규인 「디지털 증거의 수집·분석 및 관리 규정」(대검찰청예규 제1285호, 2022. 5. 18. 최종

---

[19] 이 예규는 2012년 기존 「디지털포렌식센터」(DFC)를 「국가디지털포렌식센터」(NDFC)로 명칭을 변경하고 “‘디지털 수사망”을 구축하게 되면서 2012. 7. 23. 처음 제정되었고(대검찰청예규 제608호, 제정, 2012. 7. 24. 시행), 2015. 7. 16. 대폭 개정되었다(대검찰청예규 제806호, 2015. 7. 16. 시행). 이 개정은 「디지털포렌식 수사관의 증거 수집 및 분석 규정」(대검찰청예규 제805호, 2015. 7. 16. 개정·시행)과 동시에 이루어졌다. 그 후 2020. 3. 17. 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따른 3년의 제19조(재검토기한)를 신설하였고(대검찰청예규 제1069호, 2020. 3. 17. 시행), 재검토기한에 맞춰 연장하였다.

[20] 「전국 디지털수사망 운영지침」(2024. 5. 31.) 제3조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.
1. ”디지털수사망”이라 함은 대검찰청 디지털수사과와 각 지역 거점청(디지털포렌식팀이 설치된 각 지역의 검찰청을 의미한다) 디지털포렌식팀간에 별도의 광역분석망을 통하여 운용되는 운영시스템과 디지털 증거 저장소, 디지털 증거 보관소 및 검찰망을 통하여 각 검찰청과 연계된 운영시스템을 말한다. <개정 2015.7.16.(‘디지털수사팀’->‘디지털포렌식팀)>.

[21] D-NET은 “디지털수사팀을 온라인으로 연계하여 신속한 수사지원시스템을 제공하고, 디지털 증거분석 업무의 편의성 및 증거 관리의 엄격성을 향상시키기 위한 디지털수사 네트워크”로서, “디지털 수사 통합업무관리시스템(DFIS II), 디지털 증거관리시스템, 통합디지털 증거분석 시스템(IDEAS), 원격디지털수사공조시스템 등으로 구성되어 있다.”고 한다(검찰, 국가 디지털 포렌식 센터 Brochure, [연도 미상], 20-21면: 탁희성·이원상, 디지털포렌식 통합모델 구축에 관한 연구, 한국형사정책연구원, 2016, 77면에서 재인용).

개정·시행, 이하 '관리규정'이라 한다)에서 정하고 있다. 그 제3조 제3호[22]에서는 이를 "디지털 증거의 수집 · 분석에 관한 사항과 디지털 증거의 보관 · 폐기에 관한 이력 등을 관리하는 전산시스템"으로 정의하고 있다.[23]

이 '디지털수사망'을 관리하는 부서는 대검찰청 과학수사부[24] 산하의 디지털수사과[25]이다. 대검찰청 과학수사부의 부장의 검사로 보하는데, 법과학분석과, 디엔에이 · 화학분석과, 디지털수사과 및 사이버 · 기술범죄수사과를 두고 원칙적으로 검찰사무관으로 한다.[26]

대검찰청 산하에 국가디지털포렌식센터」(National Digital Forensic Center, 약칭 NDFC)를 두고[27] 여기에 「법과학연구소」, 「디지털포렌식연구소」, 「과학수사아카데미」를 두는데, 이 중 '디-넷'과 관련된 부서는 「디지털포렌식연구소」이다.[28]

---

[22] 관리규정 제3조 (정의) 이 규정에서 사용하는 용어의 뜻은 다음과 같다.
4. "디지털수사통합업무관리시스템"(이하 '업무관리시스템'이라고 한다)이란 디지털 증거의 수집 · 분석에 관한 사항과 디지털 증거의 보관 · 폐기에 관한 이력 등을 관리하는 전산시스템을 말한다. <신설 2012. 11. 6.><개정 2016. 12. 26.><개정 2019. 5. 20.>

[23] 대검찰청은 "2009년 말부터 디지털수사와 일선수사를 온라인으로 긴밀하게 연계하는 「전국 디지털 수사망 구축사업」을 추진하여" 2012년 완료하면서 '전국디지털수사망(D-NET)'을 구축하였다. 이 '전국디지털수사망(D-NET)'은 일선 검찰의 디지털수사요청을 받아 디지털수사를 진행하고, 결과 보고를 할 수 있는 디지털수사업무와 일반관리 업무를 관할하는 '디지털수사통합업무관리시스템(DFIS II, Digital Forensic Investigation System)', 디지털증거에 대한 등록, 활용, 보관, 폐기 등 Life-Cycle관리와 디지털증거의 등록정보 등 메타데이터를 관리하는 '디지털증거관리시스템', 디지털증거로부터 추출된 디지털정보를 일선에 신속하게 제공하고, 검색, 입체분석 서비스를 제공하는 '통합디지털증거분석시스템(IDEAS, Integrated Digital Evidences Analysis System)', 디지털수사팀간의 분석 및 협업을 위한 '통합협업디지털증거분석환경', 위 시스템들의 체계적인 보안을 가능하게 하는 '디지털수사망인프라시스템'으로 구성되어 있다."고 한다(대검찰청, 검찰연감, 2023, 362면).

[24] 「검찰청 사무기구에 관한 규정」(대통령령 제34245호, 2024. 2. 27. 개정·시행) 제9조의2(대검찰청 과학수사부에 둘 과와 그 분장사무) ① 대검찰청 과학수사부에 법과학분석과, 디엔에이 · 화학분석과, 디지털수사과 및 사이버 · 기술범죄수사과를 둔다. <중략>
④ 디지털수사과장은 다음 사항을 분장한다.
1. 전자적 증거의 분석에 관한 사항
2. 전자적 증거의 분석기법에 대한 연구 · 개발에 관한 사항
3. 전자적 과학수사기법의 연구 · 개발에 관한 사항
4. 과학수사를 위한 컴퓨터프로그램의 연구 · 개발에 관한 사항
5. 제1호부터 제4호까지의 업무와 관련된 지도 · 교육에 관한 사항

[25] 「전국 디지털수사망 운영지침」(2024. 5. 31.) 제5조, 제6조.

[26] 「검찰청법」 제16조(직제) ① 대검찰청에 부(部)와 사무국을 두고, 부와 사무국에 과를 두며, 부 · 사무국 및 과의 설치와 분장사무(分掌事務)에 관한 사항은 대통령령으로 정한다.
② 제1항의 부, 사무국 및 과에는 각각 부장, 사무국장 및 과장을 두며, 부장은 검사로, 사무국장은 고위공무원단에 속하는 일반직공무원으로, 과장은 검찰부이사관 · 정보통신부이사관 · 검찰수사서기관 · 정보통신서기관 또는 공업서기관으로 보한다. 다만, 부의 과장은 검사로 보할 수 있다. <이하 생략>

[27] 2011. 11월 대검찰청에 「사이버범죄수사단」을 창설하고 2012. 11월 기존 「디지털포렌식센터」(DFC)을 「국가디지털포렌식센터」(National Digital Forensic Center, 약칭 NDFC)로 명칭을 변경하였다(대검찰청 홈페이지, "검찰활동" 중 "과학수사", <https://www.spo.go.kr/site/spo/02/1020107030000020181129 01.jsp>, 최종검색: 2024. 6. 20.).

[28] 2013. 8. 설립되었다(앞의 대검찰청 홈페이지). 관련 규정으로는 「국가디지털포렌식센터 운영에 관한 규정」(대검찰청예규 제1422호, 2024. 5. 31. 개정·시행) 제2조(국가디지털포렌식센터의 설치), 제4조(국가디지털포렌식센터의 구성), 제9조(디지털포렌식연구소의 구성 및 업무).

여기에 더하여 고등검찰청 또는 지방검찰청 단위에 '거점청 디지털포렌식팀'을 두고 있다.[29] 디지털포렌식팀은 디지털포렌식 수사관으로 구성되며, 대검찰청 디지털수사망관리자[30]와 각 지역 거점청 디지털수사망 관리자를 두어 '디지털수사망'을 관리한다.[31]

2022. 12월 기준으로 대검찰청 디지털수사과에 39명의 수사관을 두고 있으며, "서울고검에 5명, 서울중앙지검에 9명, 부산고검에 8명, 대구고검에 5명, 광주고검에 6명, 대전고검에 6명, 수원고검에 6명, 서울남부지검에 4명, 서울북부지검에 4명, 인천지검에 5명, 춘천지검에 2명, 창원지검에 3명의 디지털포렌식 전문수사관을 배치하여 디지털포렌식팀을 운영하고 있다."[32]

디지털증거의 압수·수색·검증은 원칙적으로 '디지털포렌식 수사관'()이 하는데(관리규정 제14조, 예외적으로 "디지털포렌식 관련 교육을 이수한 검찰공무원"도 가능하다), 디지털포렌식 수사관은 확보된 전자증거를 '"디지털수사통합업무관리시스템'에 등록한다(관리규정 제41조, 제42조).

등록된 자료의 분석도 '디지털포렌식 수사관'이 한다(관리규정 제44조). 분석은 '이미지 파일'로 하는데(관리규정 제45조 제1항), 디지털 포렌식 수사관은 수사팀으로부터 압수된 정보저장매체의 분석을 의뢰받는 경우 "피압수자 등의 참관 하에 저장매체 원본의 봉인을 풀고 쓰기 방지장치를 장착한 후 복제(이미징) 작업을 하여 증거사본을 작성하고, 저장매체 원본을 수사팀에 반환"한다.[33] 정보저장매체를 복제(이미징)한 후 관련 정보를 탐색하는 경우 「국가디지털포렌식센터」(NDFC)의 "증거사본 서버에 그 복제본을 보관하고 디지털 포렌식 수사관이 해당 서버에 저장된 복제본의 분석 작업을 마친 후, 그 추출된 결과물을 대검찰청 '디지털수사통합업무관리시스템'에 업로드한 뒤 사건 수사팀이 위 시스템을 통해 증거를 탐색"한다.[34]

---

[29] 「전국 디지털수사망 운영지침」 제7조 (거점청 디지털포렌식팀 설치 및 운영) ① 각 고등검찰청 또는 지방검찰청에 별도의 기구로 디지털포렌식팀을 설치할 수 있다.
② 거점청 디지털포렌식팀은 디지털포렌식 수사관으로 구성한다.
③ 각 거점청 디지털포렌식팀은 해당 고등검찰청 또는 지방검찰청 관할구역내의 디지털 증거 수집·분석 및 관리 업무를 담당한다. 다만, 대검찰청 디지털수사과장이 각 거점청 디지털포렌식팀의 업무를 조정할 수 있다. <개정 2016. 12. 26.>

[30] 'D-NET'(D-NET)의 관리를 위해 '대검찰청 디지털수사망 관리자'를 지정하여 통합관리 시스템, 원격공조망, 증거관리 시스템, 디지털수사 인프라망, 연계서버 자료관리[시스템], 데이터 백업[시스템] 등을 관리한다(「전국 디지털수사망 운영지침」 제9조 제1항, [별지 2] 디지털수사망운영일지 참조).

[31] 「전국 디지털수사망 운영지침」 제7조, 제8조. 검찰조직과 관련한 소개로는 최종혁, "사이버범죄 수사와 증거수집 실무에 대한 검토", 482-482면.

[32] 대검찰청, 검찰연감, 2023, 362면.

[33] 박혁수, "디지털 정보 압수·수색의 실무상 쟁점", 86-87면.

[34] 박민우, 디지털증거 압수·수색에서의 적법절차, 186면. "경찰의 경우 검찰과 달리 별도의 통합서버 등을 운영하지는 않고 있다."(같은 곳)고 한다. 이 논문 이후에 개정된 「디지털 증거의 처리 등에 관한 규칙」(경찰청훈령 제1003호, 2021. 1. 22. 개정·시행) 제23조(디지털 증거분석 의뢰) 제2항에 의하면, 직접 운반의 원칙(제1항)의 예외로서 '업무시스템을 통한 전송'을 규정하기 시작하였다(제2항 "제1항에도 불구하고 경찰관은 분석의뢰물을 전자적 방식으로 전송하는 것이 효율적이고 적합하며 디지털 증거의 동일성 · 무결성을 담보하는

2012년 구축된 이래 '디-넷'(D-NET)에는 2021. 2월까지 "검찰이 압수해 저장한 스마트폰이나 하드디스크 등 전자정보의 이미지는 총 14만1739건에 달하고, 이 중 35.2%인 4만9942건을 지난 2월 현재 여전히 보관하고 있었"는데, 이처럼 "한번 저장된 자료는 다른 검찰청이나 검사 개인 저장장치에 복제되"어 다양하게 수사에 활용되고 있다고 한다.[35] 2023년의 경우[36]에는 검찰 디지털수사과에서 전체 3,057건의 압수·수색에 대해서 10,441건의 증거분석이 이루어졌다.[37]

2. '디-넷'(D-NET) 운영규정

가. 「디지털 증거의 수집·분석 및 관리 규정」 개정 경과와 주요 내용

'디-넷'(D-NET)의 운영과 관련한 규범은 대검찰청 예규인 「디지털 증거의 수집·분석 및 관리 규정」(관리규정)이다. 이 규정은 제정 이후 현재까지 총 7차례 개정되었다. 이 관리규정은 본래는 2006년 「디지털 증거 수집 및 분석 규정」(대검찰청예규 제410호, 2006. 11. 21. 제정·시행)으로 제정되었다.[38] 2008. 12. 17. (대검찰청예규 제438호, 같은 날 시행)[39]과 2012. 11. 6. (대검찰청예규 제616호, 같은 날 시행) 2차례 개정되었다.

경우 해시값을 기록하는 등 분석의뢰물의 동일성을 유지하는 조치를 취하고 업무시스템을 통하여 분석의뢰물을 전송할 수 있다."). 이 규칙에 의하면, '경찰청 국가수사본부 사이버수사국 디지털포렌식센터'가 '디지털 증거분석 업무'를 담당하는데(제7조), 이 '업무시스템'이 무엇인지는 이 규정에 명시되어 있지 않다.

[35] "(3) 압수된 데이터는 삭제되지 않는다", 경향신문 2021. 3. 29, <https://www.khan.co.kr/national/national-general/article/202103290600005>, 최종검색: 2024. 6. 20. 또한 다른 기사로는 "9년 묵은 압색 정보도 대검은 갖고 있다", 경향신문 2021. 4. 2, <https://www.khan.co.kr/national/court-law/article/202104020600015>, 최종검색: 2024. 6. 20.

[36] 대검찰청 홈페이지, "사전정보공표 대상", "2023년도 디지털 증거 압수수색, 증거분석 지원 현황"(디지털수사과), <https://www.spo.go.kr/site/spo/ex/announce/AnnounceInfo.do>, 최종검색: 2024. 6. 20.

[37] 2006년~2017년 사이의 대검찰청 디지털수사과 운영현황에 관하여는 오현석, 전자증거의 선별압수와 매체압수에 관한 연구, 서울대학교 석사학위 논문, 5면 이하.

[38] 그 이전에 있던 「컴퓨터 등 압수·수색 기본지침」(대검 61100-284호, 2003. 8. 11.)이 이 예규의 제정으로 폐지되었다(부칙 제2조 참조).

[39] 이 예규에 대한 소개와 분석으로는 이숙연, 형사소송에서의 디지털증거의 취급과 증거능력, 고려대학교 박사학위 논문, 2011, 78-85면. 이 개정은 제4조(디지털포렌식수사관)의 자격 등을 확대한 것이었다. 또한 2008년의 「디지털포렌식센터」(DFC) 설치와 연결된다.

2012. 11. 6. 이 관리규정은 대폭 개정되었다. 우선, 제3조(정의)[40] 조항을 신설하였는데, “디지털 증거”, “디지털수사통합업무관리시스템”, “정보저장매체등의 복제” 등을 규정하였다. 다음으로, “제4장 디지털 증거의 등록”을 신설하였는데, 이미징으로 수집된 디지털증거를 “디지털수사통합업무관리시스템”에 등록하여 분석하는 절차규정을 두었다. 여기에서 강조된 것은 디지털증거의 ‘무결성’이었고 이에 따라 제4조(디지털 증거의 무결성 유지)[41]와 제5조(디지털 증거의 신뢰성 유지)[42]도 신설하였다.

이 개정은 대법원 2007. 12. 13. 선고 2007도7257 판결<일심회 사건>과 대법원 2011. 5. 26.자 2009모1190 결정<전교조 본부 사무실 압수수색 사건> 그리고 이들 판례 법리를 반영하여 정보저장매체등에 관한 압수의 범위와 방법을 명시한 「형사소송법」 개정(법률 제10864호, 2011. 7. 18. 개정, 2012. 1. 1. 시행) 제106조 제3항으로 강화된 전자증거의 압수·수색에 대한 법원의 통제에 대응하기 위한 것이었다.

2015년 「디지털포렌식 수사관의 증거 수집 및 분석 규정」(대검찰청예규 제805호, 2015. 7. 16. 개정·시행)[43]으로 바뀌었다.[44] 예규 명칭의 변화는 있었지만 제7조(거점청 디지털포렌식팀 설치 및 운영) 등 기존 “지역 디지털 포렌식 팀”을 “거점청 디지털포렌식팀”으로 명칭을 바꾸는 등[제9조 (지원요청)] 디지털포렌식 수사인력의 역할분담에 관한 규정이 변경되는 것 이외에 큰 변화는 없었다.[45]

---

[40] 관리규정(2012. 11. 6.) 제3조 (정의) 이 규정에서 사용하는 용어의 뜻은 다음과 같다.
1. ”디지털 증거”란 범죄와 관련하여 디지털 형태로 저장되거나 전송되는 증거로서의 가치가 있는 정보를 말한다. <중략>
3. ”디지털수사통합업무관리시스템”이란 디지털 증거의 수집 및 분석에 관한 사항과 디지털 증거의 보관에 관한 이력 등을 관리하는 전산시스템을 말한다.
4. ”정보저장매체등의 복제”란 법률적으로 유효한 증거로 사용될 수 있도록 수집 대상 정보저장매체등에 저장된 디지털 정보를 동일하게 파일로 생성하거나, 다른 정보저장매체에 저장하는 것을 말한다.

[41] 관리규정(2012. 11. 6.) 제4조 (디지털 증거의 무결성 유지) 디지털 증거는 압수·수색·검증한 때로부터 법정에 제출하는 때까지 훼손 또는 변경되지 아니하여야 한다.

[42] 관리규정(2012. 11. 6.) 제5조 (디지털 증거의 신뢰성 유지) 디지털 증거는 그 수집 및 분석 과정에서 이용된 도구와 방법의 신뢰성이 유지되어야 한다.

[43] 당시의 「디지털포렌식 수사관의 증거 수집 및 분석 규정」에 대한 소개로는 탁희성·이원상, 디지털포렌식 통합모델 구축에 관한 연구, 한국형사정책연구원, 2016, 79면 이하.

[44] 공교롭게도 이 개정일은 혐의사실과 관련성이 없는 증거를 영장 없이 ‘탐색’하는 것은 위법이라고 한 <종근당 사건>(대법원 2015. 7. 16.자 2011모1839 전원합의체 결정)의 결정일이다. 또한 이 개정 이전의 주요 판결로는, 전자증거의 무결성과 동일성, 특히 해시값 이외의 무결성 확보방법을 다룬 대법원 2013. 7. 26. 선고 2013도2511 판결<왕재산 사건>이 있다. <왕재산 사건> 제1심 판결에 대한 소개와 분석 그리고 2011. 7. 18. 「형사소송법」 개정조항에 대한 분석으로는 오길영, “디지털 저장매체의 압수·수색과 그 쟁점”, 민주법학 제49권, 민주주의법학연구회, 2012.7, 13-39면.

[45] 또한 일선 검찰청 검사 등의 ‘디지털수사과장 등’에 대한 지원요청 사항에서 “디지털 증거의 압수·수색·검증”지원요청이 빠졌다[제9조 (지원요청) 제1항].

그후 2016년 「디지털 증거의 수집·분석 및 관리 규정」(대검찰청예규 제876호, 2016. 12. 26. 개정, 2017. 3. 1. 시행)으로 명칭이 변경되었다.[46] 이때 "제6장 디지털 증거의 관리"의 장이 추가되면서 제27조(디지털 증거의 폐기)[47]가 신설되었다. 또한 "제4장 디지털 증거의 등록" 중 제19조(정보저장매체 등의 이미지 등록 및 피압수자 등의 참여)가 개정되었다. 이 개정 내용은 상당 기간 이미징한 파일을 별도의 디스크에 담아서 다른 사건의 범죄사실을 '탐색'하였던 수사실무에 제동을 걸었던 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정<종근당 사건>의 법리와 관련이 깊다.

이 규정은 2019년 전면 개정되면서(대검찰청예규 제991호, 2019. 5. 20. 전부개정·시행), "디지털수사통합업무관리시스템"의 개념에 "디지털 증거의 보관·폐기에 관한 이력"의 관리에 관한 문구가 추가되고(제3조 제3호), "디지털 증거의 폐기"가 용어정의 조항에 새로이 등장하였으며(같은 조 제8호) "제8장 디지털 증거의 폐기"의 장이 신설되었다.

이 전면 개정의 배경에는 「검·경 수사권 조정 합의문」(2018. 6. 21.)[48] 당시의 "전자정보의 압수수색절차 및 사건과 무관한 전자정보 삭제 의무화" 논의가 있었던 것으로 보인다. 이에 따라 2020년 제정된 「검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정」(대통령령 제31089호, 2020. 10. 7. 제정, 2021. 1. 1. 시행, 이하 '수사준칙'이라 한다)

---

[46] 부칙 제3조(존속기한)에 따르면, 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2020. 2. 29.까지 효력을 갖도록 하였다.

[47] 관리규정(2016. 12. 26.) 제27조 (디지털 증거의 폐기) ① 디지털증거관리책임자 등은 디지털수사통합업무관리시스템에 등록된 디지털 증거에 대해 해당 사건 주임검사의 폐기 요청 또는 압수전담검사의 폐기촉탁이 있으면 해당 디지털 증거를 폐기하여야 한다.
② 제1항과 같이 디지털 증거를 폐기한 다음 해당 사건 주임검사의 폐기 요청에 따른 경우에는 별지 제7호 서식의 「디지털증거 폐기확인서」를, 압수전담검사의 폐기촉탁에 따른 경우에는 별지 제8호 서식의 「디지털증거 폐기(촉탁) 회보서」를 각각 교부하여야 한다.
③ 제9조 제3항 본문에 따라 형사사법정보시스템(KICS)과 연동하여 사건번호가 입력된 지원요청의 디지털 증거 중 주임검사 처분시까지 압수물로 수리되지 않은 디지털 증거는 지원요청 부서에 통보 후 폐기한다.
④ 제9조 제3항 단서에 따라 형사사법정보시스템(KICS)과 연동하여 사건번호가 입력되지 않고 디지털수사통합업무관리시스템에 등록된 지원요청의 디지털 증거는 6개월 이내에 형사사법정보시스템(KICS)과 연동된 사건번호의 입력이 없고 해당 사건 주임검사의 별도 보관 요청이 없을 경우 지원요청 부서에 통보 후 폐기한다.

[48] 대한민국정책브리핑, "검·경 수사권 조정", 2018. 6. 21, <https://www.korea.kr/news/policyNewsView.do?newsId=148868893>, 검색일: 2024. 5. 30. 참조.

---

6. 형사소송법 및 검찰청법 시행령 개정 내용 (2020.8.7. 입법예고)
형사소송법 시행령(검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정) 주요 개정사항
<중략>
○ 수사 과정에서 인권과 적법절차 보장을 확대함
- 기존에 인권보호수사규칙(법무부령), 범죄수사규칙(경찰청훈령) 등에 별도로 규정되어 있던 인권 및 적법절차 보장 방안을 수사준칙에 통일적으로 규정하고, 검사와 사법경찰관이 모두 이를 준수하도록 함으로써 국민의 기본권 보장에 만전을 기함
- 주요 내용 : 심야조사 제한, 장시간 조사 제한, 변호인 조력권 보장, 별건수사 금지, 내사 단계의 소환조사 및 영장청구 제한, **전자정보의 압수수색절차 및 사건과 무관한 전자정보 삭제 의무화** 등

제41조(전자정보의 압수・수색 또는 검증 방법)와 제42조(전자정보의 압수・수색 또는 검증 시 유의사항)에 그 취지가 규정되어 있다. 특히 제42조 제2항은 "검사 또는 사법경찰관은 제1항의 목록에 포함되지 않은 전자정보가 있는 경우에는 해당 전자정보를 지체 없이 삭제 또는 폐기하거나 반환해야 한다. 이 경우 삭제・폐기 또는 반환확인서를 작성하여 피압수자등에게 교부해야 한다."고 명시하고 있다. 이 수사준칙 단계에서는 아직 '전자증거'와 '디지털증거'의 구별은 나타나지 않았다(현행 규정도 동일하다).

위 수사준칙의 발효와 동시에 관리규정이 개정되었다. 관리규정에서는 수사준칙의 취지를 보다 구체화하였다. 즉, 2021. 1. 1. 개정(대검찰청예규 제1151호, 2021. 1. 1. 시행)을 통해 '디지털증거'와 이보다 넓은 범위의 '전자정보'를 개념[49]적으로 구분하고 처리절차를 달리하였다.[50] 이에 따라 '전자증거의 삭제·폐기'(제24조)[51]와 '디지털증거의 폐기'(제53조)[52]가 구별되었다.[53]

이에 따라 관련성 있는 전자정보의 압수 후에는 압수목록을 교부하여야 하고, 압수목록에 들어있지 않는 전자정보는 "해당 전자정보를 지체 없이 삭제 또는 폐기하거나 반환해야 한다."[관리규정 제23조(압수목록의 교부), 제24조(관련 있는 전자정보 압수 후 조치)]. 여기에서 전자증거의 폐기 여부를 결정함에 있어 '주임검사등'(주임검사 또는 검찰수사관)에게 관련성 판단의 재량이 인정된다. 그리고 '전자증거의 폐기'는 '디지털증거의 폐기'와 구별되며, '디-넷'(D-NET)에 저장되기 이전 단계에 무관정보를 배제할 수 있도록 한 것이다.

---

[49] 관리규정 제3조(정의) 이 규정에서 사용하는 용어의 뜻은 다음과 같다.
1. "전자정보"란 정보저장매체등에 기억된 정보를 말한다.
2. "디지털 증거"란 범죄와 관련하여 디지털 형태로 저장되거나 전송되는 증거로서의 가치가 있는 정보를 말한다.

[50] 예컨대, 관리규정은 "디지털 증거 증 전자증거"라는 문언을 사용한다.
* 관리규정 제49조(디지털 증거의 관리 시 유의사항) 디지털수사과장은 업무관리시스템에 등록된 디지털 증거 등 전자정보의 원본성·무결성 등이 훼손되지 않도록 체계적으로 보존·관리하여야 한다.

[51] 관리규정 제24조(관련 있는 전자정보 압수 후 조치) 주임검사등[주임검사 또는 검찰수사관]은 제23조[압수목록의 교부]의 목록에 포함되지 않은 전자정보가 있는 경우에는 해당 전자정보를 지체 없이 삭제 또는 폐기하거나 반환해야 한다. 이 경우 별지 제16호 서식의 "전자정보 삭제·폐기 또는 반환확인서"를 작성하여 피압수자등에게 교부해야 한다.

[52] 관리규정 제53조(디지털증거의 폐기 시 유의사항) 범죄사실과 무관한 것으로 확인된 디지털 증거는 폐기하여야 하나, 디지털 증거를 폐기하는 과정에서 향후 재판 절차에 증거로 제출되어야 하는 디지털 증거가 폐기되는 일이 없도록 유의하여야 한다.

[53] 앞서 본 2021년 경향신문 기사에서는 "법조계 관계자는 "검찰이 D-NET에 저장한 데이터 대부분을 삭제하지 않고 있다가 최근 들어 오래된 것들을 중심으로 폐기하기 시작한 것 같다"고 말했다."고 하는데("'수사 빌미' 개인정보 검찰, 5만건 보관 중", 경향신문 2021. 3. 29, <https://www.khan.co.kr/national/national-general/article/202103290600015>, 최종검색: 2024. 6. 20.), 이 폐기규정이 도입된 2021년 개정 이후를 상황을 기술하는 것으로 보인다.

한편, 디지털증거의 폐기는 '업무관리시스템', 즉 '디지털수사통합업무관리시스템'에서의 폐기만을 규정하고 있다[제54조(폐기대상)[54]]. 또한 폐기의 대상도 '디지털증거'로서 '전자증거' 일체를 말하는 것은 아니다.

디지털증거의 폐기절차는 "주임검사(주임검사가 없는 경우에는 그 승계검사) 또는 압수전담검사의 요청"이 있는 경우에 개시한다[제56조(폐기요청)[55]]. 관리규정 제53조(디지털증거의 폐기 시 유의사항)[56]는 "디지털 증거를 폐기하는 과정에서 향후 재판 절차에 증거로 제출되어야 하는 디지털 증거가 폐기되는 일이 없도록 유의하여야 한다."고 하여 공판기간을 고려할 때 장기간 보존을 염두에 두고 있다고 할 수 있다.

특히 폐기대상의 예외를 규정한 관리규정 제54조[57] 제2항은 "압수의 원인이 된 사건과 형사소송법 제11조[58]에 따라 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 경우"(제1호)를 폐기의 예외사유로 하고 있는 등 수사검사(주임검사 등)에게 디지털증거에 상당한 재량을 부여하고 있다. 이 범위는 뒤에서 보는 압수·수색의 관련성(「형사소송법」

---

[54] 관리규정 제54조(폐기대상) ① 다음 각 호에 해당하는 디지털 증거는 본 장에서 규정한 절차에 따라 업무관리시스템에서 폐기한다.
1. 수사 또는 재판 과정에서 범죄사실과 관련성이 없는 것으로 확인된 경우
2. 압수의 원인이 된 사건에 대한 기소 · 불기소 등 종국처분에 따라 계속 보관할 필요성이 없다고 인정되는 경우
3. 판결이 확정되어 계속 보관할 필요성이 없다고 인정되는 경우
② 제1항에도 불구하고 다음 각 호의 사유가 있는 경우에는 압수의 원인이 된 사건의 공소시효가 완성될 때까지 디지털 증거를 폐기하지 않을 수 있다.
1. 압수의 원인이 된 사건과 형사소송법 제11조에 따라 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 경우
2. 압수의 원인이 된 사건이 기소중지처분 또는 참고인중지처분이 된 경우
3. 불기소처분을 한 사건 또는 무죄판결이 확정된 사건 중 공범 등에 대한 수사를 계속할 필요가 있다고 인정되는 경우

[55] 관리규정 제56조(폐기요청) 제54조의 폐기대상 디지털증거에 대한 폐기절차는 주임검사(주임검사가 없는 경우에는 그 승계검사) 또는 압수전담검사의 요청으로 개시한다.

[56] 관리규정 제53조(디지털증거의 폐기 시 유의사항) 범죄사실과 무관한 것으로 확인된 디지털 증거는 폐기하여야 하나, 디지털 증거를 폐기하는 과정에서 향후 재판 절차에 증거로 제출되어야 하는 디지털 증거가 폐기되는 일이 없도록 유의하여야 한다.

[57] 관리규정 제54조(폐기대상)
① 다음 각 호에 해당하는 디지털 증거는 본 장에서 규정한 절차에 따라 업무관리시스템에서 폐기한다.
1. 수사 또는 재판 과정에서 범죄사실과 관련성이 없는 것으로 확인된 경우
2. 압수의 원인이 된 사건에 대한 기소 · 불기소 등 종국처분에 따라 계속 보관할 필요성이 없다고 인정되는 경우
3. 판결이 확정되어 계속 보관할 필요성이 없다고 인정되는 경우
② 제1항에도 불구하고 다음 각 호의 사유가 있는 경우에는 압수의 원인이 된 사건의 공소시효가 완성될 때까지 디지털 증거를 폐기하지 않을 수 있다.
1. 압수의 원인이 된 사건과 형사소송법 제11조에 따라 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 경우
2. 압수의 원인이 된 사건이 기소중지처분 또는 참고인중지처분이 된 경우
3. 불기소처분을 한 사건 또는 무죄판결이 확정된 사건 중 공범 등에 대한 수사를 계속할 필요가 있다고 인정되는 경우

[58] 형사소송법 제11조 (관련사건의 정의) 관련사건은 다음과 같다.
1. 1인이 범한 수죄
2. 수인이 공동으로 범한 죄
3. 수인이 동시에 동일장소에서 범한 죄
4. 범인은닉죄, 증거인멸죄, 위증죄, 허위감정통역죄 또는 장물에 관한 죄와 그 본범의 죄

제106조, 제215조)보다 넓다. 또한 같은 조 제3호에서는 “무죄판결이 확정된 사건 중 공범 등에 대한 수사를 계속할 필요가 있다고 인정되는 경우”까지를 포함하고 있는데, 해당 사건으로는 이미 무죄가 되었음에도 그 사건과 관련하여 압수·수색한 디지털증거를 그대로 보존할 수 있도록 하고 있다.

이 규정은 2022년 존속기한 연장을 위한 개정(대검찰청예규 제1285호, 2022. 5. 18. 개정·시행)을 거쳐 현재에 이르고 있다.[59]

나. 비교 규정: 「(경찰청) 디지털 증거의 처리 등에 관한 규칙」

향후 다른 관련사건의 수사상의 필요성을 이유로 한다면, 비교할 만한 규정이 있다. 같은 업무를 수행하는 「(경찰청) 디지털 증거의 처리 등에 관한 규칙」(경찰청훈령 제1086호, 2023. 7. 4. 개정·시행) “제5장 디지털 증거의 관리”이다. 수사와 관련된 업무가 종결된 이후에는 “지체없이 삭제·폐기”하도록 한다[제35조(전자정보의 삭제 · 폐기)]. 삭제 대상은 수사과정에서 생성된 복사본을 포함하며, 삭제한 후 그 취지를 피압수자에게 통지하도록 하고 있다.

한편, 미제사건의 경우 “압수를 계속할 필요가 있는 경우 해당 사건의 공소시효 만료일까지 보관 후 삭제·폐지”하도록 하고 있다[제36조(입건 전 조사편철 · 관리미제사건 등록 사건의 압수한 전자정보 보관 등)[60] 제1호]. 보관의 범위는 ‘해당사건’에 제한되며, 이를 위 관리규정과 같이 형사소송법 제11조와 같은 관련성 있는 사건 등으로까지 확장하지는 않는다.

---

[59] 부칙 제2조(존속기한)에 따르면, 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2025. 5. 18.까지 효력을 갖도록 하였다.

[60] 「(경찰청) 디지털 증거의 처리 등에 관한 규칙」(2023. 7. 4.) 제36조(입건 전 조사편철 · 관리미제사건 등록 사건의 압수한 전자정보 보관 등) 경찰관은 입건 전 조사편철 · 관리미제사건 등록한 사건의 압수한 전자정보는 다음 각호와 같이 처리하여야 한다.

1. 압수를 계속할 필요가 있는 경우 해당 사건의 공소시효 만료일까지 보관 후 삭제 · 폐기한다.
2. 압수를 계속할 필요가 없다고 인정되는 경우 삭제 · 폐기한다.
3. 압수한 전자정보의 삭제 · 폐기는 관서별 통합 증거물 처분심의위원회의 심의를 거쳐 관련 법령 및 절차에 따라 삭제 · 폐기한다.
4. 압수한 전자정보 보관 시 충격, 자기장, 습기 및 먼지 등에 의해 손상되지 않고 안전하게 보관될 수 있도록 별도의 정보저장매체등에 담아 봉인봉투 등으로 봉인한 후 소속부서에서 운영 또는 이용하는 증거물 보관시설에 보관하는 등 압수한 전자정보의 무결성과 보안 유지에 필요한 조치를 병행하여야 한다.

3. 소결

검찰의 '디-넷'(D-NET) 운용의 상황과 관련 규범은 앞으로 보는 「형사소송법」과 대법원 판례의 전자정보 규율에 맞추어 조금씩 개선되고 있다고 보인다. 즉, 관리규정은 지속적으로 개정되면서 점차로 대법원 판례에 보조를 맞추어 전자정보에 관한 규율을 풍부하게 하였다.

특히 2012년과 2016년의 개정은 2011년 개정 「형사소송법」과 대법원의 판례 법리의 영향을 받은 것이다. 동시에 「검·경 수사권 조정 합의문」(2018. 6. 21.)의 영향도 보인다. 그럼에도 불구하고 대법원에 의한 통제의 사각은 여전히 남은 것으로 보인다.

우선, 「디지털 증거의 수집·분석 및 관리 규정」(관리규정)은 '전자증거'와 '디지털증거'를 증거를 구별하여, 전자증거의 폐기는 '디-넷'(D-NET)에 저장되기 이전 단계의 폐기를 정하고 디지털증거의 폐기는 이미 '디-넷'(D-NET)에 저장된 '디지털증거'의 폐기만을 정하고 있다. 여기에서 검사나 검찰수사관이 수사 목적으로 개별적으로 자신의 하드디스크나 이동식 저장장치에 보유하는 복제본이 있는 경우 이에 관하여까지는 정하고 있지 않다. 다음으로, 이 관리규정 제54조 제2항의 지나치게 넓은 예외사유는 '디-넷'(D-NET)에 등록된 디지털증거를 장기간 보존할 수 있는 여지를 여전히 남겨 놓고 있다.

검찰이 보유한 전자증거나 디지털증거는 보통 법원의 압수·수색영장의 집행을 통해 획득한 것이다. 따라서 이러한 과도한 전자정보의 획득과 무관정보의 취득과 활용에 대한 법적 평가를 일차적으로 전자정보 압수·수색 그리고 무관정보 처리에 관한 「형사소송법」의 규정과 판례를 통해 평가해볼 수 있을 것이다.

III. 전자정보의 압수·수색과 무관정보 처리에 관한 법적 규율

1. 「형사소송법」상 압수·수색 개관

가. 개관

현행 「형사소송법」상 전자정보의 압수와 수색에 관한 규율은 일반적인 압수·수색의 경우와 크게 다르지 않다. 압수·수색에 관하여 「형사소송법」은 법원이 주체가 되는 압수·수색을 제106조부터 제138조까지에서 규정하는 한편, 수사기관의 압수·수색을 제216조부터 제220조까지 정하면서, 수사기관의 압수·수색에 법원의 압수·수색 규정 대부분을 준용하도록 하였다(제219조).

압수·수색에 대해서는 헌법 제12조 제1항 제1문(“누구든지 법률에 의하지 아니하고는 체포·구속·압수·수색 또는 심문을 받지 아니하며, 법률과 적법한 절차에 의하지 아니하고는 처벌·보안처분 또는 강제노역을 받지 아니한다.”) 그리고 제3항(“체포·구속·압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다.”)에 따라 강제처분법정주의와 영장주의가 적용된다.

특히 영장주의는 일반영장의 금지에서 출발하므로 영장의 특정성이 요구된다. 압수·수색에 관하여 이를 구현하는 조문이 「형사소송법」 제114조이다. 이 취지를 압축적으로 기술하고 있는 것으로는, 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정에서 다수의견에 대한 대법관 이인복, 대법관 이상훈, 대법관 김소영의 보충의견을 들 수 있다. 즉, “우리 헌법은 제12조에서 (…) 압수·수색에 관한 (…) 영장주의의 원칙을 선언하고 있다. 이에 따라 압수·수색 여부를 수사기관의 전적인 재량에 맡기는 영장의 발부는 금지되고, 압수·수색영장에는 피의자의 성명, 죄명 외에도 압수할 물건, 수색할 장소, 신체, 물건, 발부연월일, 유효기간, 압수·수색의 사유 등을 기재하여야 하며, 영장의 청구서에도 위 사항을 기재하여야 한다(형사소송법 제219조, 제114조 제1항, 형사소송규칙 제58조, 제107조).”

나. 압수·수색의 범위: '관련성 요건'

「형사소송법」은 압수·수색의 범위를 제한하는 요건으로 '관련성 요건'을 요구하고 있다. 즉, 「형사소송법」에 따르면, 수사기관(검사, 사법경찰관)은 "범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여" 그리고 "지방법원판사가 발부한 영장에 의하여 압수, 수색 또는 검증을 할 수 있다"(형소법 제215조 제1항, 제2항).

여기에서 "해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여"를 '관련성 요건'이라 한다. 대법원은 "영장 발부의 사유로 된 범죄 혐의사실"과 관련된 증거를 이를 ① 객관적 관련성과 ② 인적 관련성(주관적 관련성)으로 나누어 검토한다.[61] ① 혐의사실과의 객관적 관련성란 "압수·수색영장에 기재된 혐의사실의 내용과 수사의 대상, 수사 경위 등을 종합하여 구체적·개별적 연관관계가 있는 경우"를 말한다. "혐의사실과 단순히 동종 또는 유사 범행이라는 사유만으로" 족하지는 않지만, "압수·수색영장에 기재된 혐의사실 자체 또는 그와 기본적 사실관계가 동일한 범행과 직접 관련되어 있는 경우"를 넘어 "범행 동기와 경위, 범행 수단과 방법, 범행 시간과 장소 등을 증명하기 위한 간접증거나 정황증거 등으로 사용될 수 있는 경우"에도 인정된다.[62] 그리고 ② "압수·수색영장 대상자와 피의자 사이에 인적 관련성"은 보통 "압수·수색영장에 기재된 대상자의 공동정범이나 교사범 등 공범이나 간접정범은 물론 필요적 공범 등에 대한 피고사건에 대해서도 인정"된다.[63]

다. 압수·수색의 절차적 통제: '당사자의 참여권'과 '압수목록의 교부'

「형사소송법」은 압수·수색을 절차적으로 통제하기 위하여 압수·수색 시에 검사 이외에 피고인·변호인이 참여할 수 있도록 하고(「형사소송법」 제121조[64]), 그 권리를 보장하기 위해 집행에 앞서 집행 일시·장소를 피고인·변호인에게 통지하도록 하였다(같은 법 제122조[65] 본문). 다만 피고인·변호인이 "참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때"에는

---

[61] 대표적인 판결로는 대법원 2020. 2. 13. 선고 2019도14341, 2019전도130 판결<통신매체이용음란 혐의 사건>. "압수·수색영장의 범죄 혐의사실과 관계있는 범죄라는 것은 압수·수색영장에 기재한 혐의사실과 객관적 관련성이 있고 압수·수색영장 대상자와 피의자 사이에 인적 관련성이 있는 범죄를 의미한다."
[62] 대법원 2020. 2. 13. 선고 2019도14341, 2019전도130 판결.
[63] 대법원 2017. 12. 5. 선고 2017도13458 판결.
[64] 「형사소송법」 제121조(영장집행과 당사자의 참여) 검사, 피고인 또는 변호인은 압수 · 수색영장의 집행에 참여할 수 있다.
[65] 「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.

예외로 한다(같은 조 단서). 또한 사후적인 통제수단으로 “압수한 경우에는 목록을 작성하여 소유자, 소지자, 보관자 기타 이에 준할 자에게 교부”하도록 하고 있다(「형사소송법」 제129조[66]).

2. 전자정보의 압수·수색에 관한 「형사소송법」 규정과 대법원 판례

가. 현장 선별압수의 원칙 그리고 매체·복사본 반출 후 선별(‘선반출-후선별 압수’)의 예외

전자정보의 압수·수색도 위에서 다룬 일반적인 규범적 틀 내에서 허용된다. 따라서 영장에 의하여야 함은 당연하다. 그러나 형식적으로는 법관에 의하여 발부된 영장에 의하여 집행이 되더라고 전자증거나 정보저장매체의 특성상 영장주의의 한계, 특히 ‘영장의 특정성’을 잃기 쉽다. 여기에서 전자정보에 관하여 「형사소송법」에서는 특칙을 두고 있으며, 대법원의 그 해석에 특별한 의미를 부여하고 있다.

우선, 전자정보의 압수·수색[67]과 관련해서 특별히 규율하는 조문으로는 「형사소송법」 제106조[68] 제3항이 유일하다. 이에 따르면 “컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체”(“정보저장매체등”)를 압수·수색하는 경우 “기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받”는 것을 원칙으로 하되, 이 방법에 의한 “출력 또는 복제”가 불가능한 경우나 이 방법에 의하여 “압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때”에만 예외적으로 ‘정보저장매체등’ 자체를 압수할 수 있도록 하였다. 이 조항은 「형사소송법」 제209조에 의하여 수사기관에 준용된다.

이처럼 ‘정보저장매체등’의 압수는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받”는 것을 원칙으로 하고 예외적으로 “범위를 정하여 출력 또는 복제하는 방법이

---

[66] 「형사소송법」 제129조(압수목록의 교부) 압수한 경우에는 목록을 작성하여 소유자, 소지자, 보관자 기타 이에 준할 자에게 교부하여야 한다.
[67] 이에 관한 개괄적 서술로는 박병민·서용성, 디지털 증거 압수수색 개선방안에 관한 연구 —법률 개정에 관한 논의를 중심으로—, 사법정책연구원, 2021, 155면 이하.
[68] 「형사소송법」 제106조(압수) 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.

불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있"도록 하고 있다.

대법원은 「형사소송법」 제106조 제3항의 해석과 관련하여, "영장 발부의 사유로 된 범죄 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복제하는 방식"을 원칙으로 하고, "저장매체 자체를 직접 반출하거나 그 저장매체에 들어 있는 전자파일 전부를 하드카피나 이미징 등 형태(이하 '복제본'이라 한다)로 수사기관 사무실 등 외부로 반출하는 방식"을 예외적으로 허용된다고 한다.[69] 개별적인 '파일복제' 그리고 저장매체 또는 파일 전체에 대한 복제본(하드카피 또는 이미징[70]의 '반출'로 대비하면서, 전자('현장 선별압수')를 원칙으로 하고 후자('선반출-후선별 압수')를 예외로 한다.[71] [72]

이러한 판례에 따르면, 예외적인 '반출'은 "현장의 사정이나 전자정보의 대량성으로 인하여 관련 정보 획득에 긴 시간이 소요되거나 전문 인력에 의한 기술적 조치가 필요한 경우 등 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에 한"하여 허용된다.[73]

---

[69] 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정<종근당 사건> "수사기관의 전자정보에 대한 압수·수색은 원칙적으로 영장 발부의 사유로 된 범죄 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복제하는 방식으로 이루어져야 하고, 저장매체 자체를 직접 반출하거나 그 저장매체에 들어 있는 전자파일 전부를 하드카피나 이미징 등 형태(이하 '복제본'이라 한다)로 수사기관 사무실 등 외부로 반출하는 방식으로 압수·수색하는 것은 현장의 사정이나 전자정보의 대량성으로 인하여 관련 정보 획득에 긴 시간이 소요되거나 전문 인력에 의한 기술적 조치가 필요한 경우 등 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에 한하여 예외적으로 허용될 수 있을 뿐이다."

[70] '이미징'에는 "저장매체 전체를 파일 형태로 생성하는 '물리이미징'과 저장매체 중 선별된 폴더나 파일만을 대상으로 생성하는 '논리이미징'이 있다."[홍진표, "디지털 증거에 대한 압수수색 영장제도의 실무적 개선방안 고찰", 사법 제1권 제50호, 사법발전재단, 2019.1, 115면 각주 10)].

[71] 법원 실무에서는 ① '복사(copy)'는 "원본파일 또는 디렉토리를 단순히 사본 저장매체에 복사하는" 것, ② '복제(hard copy)'란 "특수장비를 이용하여 하드디스크를 물리적으로 그대로 복사하는" 것, ③ '이미징(imaging)'은 "소프트웨어를 사용하여 대상 하드디스크 전체를 하나의 파일 형태로 복사하는" 것으로 각각 구별한다는 설명도 있다[홍진표, "디지털 증거에 대한 압수수색 영장제도의 실무적 개선방안 고찰", 114면 각주 9)].

[72] 실무상으로는 전자 '파일'로 복제하거나 '이미징'('물리이미징'과 '논리이미징')의 형태로 이루어지는데, 수사(검찰) 실무상 이를 '선별압수'('증거파일', '물리이미징'과 '논리이미징'), 후자는 '매체압수'(정보저장매체등에 대한 압수)로 부르기도 한다(예컨대, 오현석, 전자증거의 선별압수와 매체압수에 관한 연구, 4-5, 15면).

[73] 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정.

나. '선반출-후선별 압수'에 대한 규제 법리

(1) '관련성 있는 정보'(유관정보와 무관정보의 구별)

전자정보의 압수·수색을 위해 압수·수색장소 외부로 '반출'한 저장매체나 복제본에 대해서는 수사관서에서 혐의사실을 입증할 증거('디지털증거')를 '탐색'하고 발견한 경우 이를 '출력'하는 작업을 거쳐야 한다. 이 '탐색'행위도 대법원[74]은 "압수·수색의 일환"으로 보며, 그 범위도 "혐의사실과 관련된 부분으로 한정되어야" 한다는 입장이다.

"수사기관 사무실 등으로 반출된 저장매체 또는 복제본에서 혐의사실 관련성에 대한 구분 없이 임의로 저장된 전자정보를 문서로 출력하거나 파일로 복제하는 행위는 원칙적으로 영장주의 원칙에 반하는 위법한 압수"가 된다. 앞서의 「디지털 증거의 수집·분석 및 관리 규정」(관리규정)의 용어로 설명하면, '반출' 이후 이미징한 파일 등 '전자정보'에서 관련성이 없는 '디지털증거'를 출력·복제하는 것은 위법한 수사가 된다는 것이다. 이러한 법리는 유관정보('혐의사실과 관련된 전자정보')와 무관정보('혐의사실과 무관한 전자정보')가 "혼재된 정보저장매체를 임의제출받은 경우"에도 동일하다.[75]

(2) '탐색'과 '출력'의 과정에서 당사자의 참여권

대법원은 이 '탐색'과 '출력'의 과정에서 당사자의 참여권을 강화하고 있다. 대법원[76]은 '선반출-후선별 압수'의 경우, "피압수·수색 당사자(이하 '피압수자'라 한다)나 그 변호인에게 참여의 기회를 보장하고 혐의사실과 무관한 전자정보의 임의적인 복제 등을 막기 위한 적절한 조치를 취하는 등 영장주의 원칙과 적법절차를 준수하여야 한다."고 본다. 따라서 "피압수자 측이 참여하지 아니한다는 의사를 명시적으로 표시하였거나 절차 위반행위가 이루어진 과정의 성질과 내용 등에 비추어 피압수자 측에 절차 참여를 보장한 취지가 실질적으로 침해되었다고 볼 수 없을 정도에 해당한다는 등의 특별한 사정이 없는 이상" 그 압수·수색이 위법하게 된다. "수사기관이 저장매체 또는 복제본에서 혐의사실과 관련된 전자정보만을 복제·출력하였다"고 해도 마찬가지이다. 즉, 유관정보만을 추출했다고 해서 참여권 배제의 위법성이 치유되지는 않는다.

---

[74] 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정.
[75] 대법원 2021. 11. 18. 선고 2016도348 전원합의체 판결.
[76] 대법원 2011. 5. 26.자 2009모1190 결정; 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정

(3) '우연한 발견'의 경우: 무관정보 탐색을 위한 별건 영장의 청구

문제는 '탐색'·'출력' 과정을 다른 범죄의 수사를 위한 수단으로 활용하는 경우이다. 압수·수색 영장을 발부하는 계기가 되었던 '특정한' 범죄혐의와 무관한 범죄수사에 이용되는 경우를 대법원은 다른 범죄혐의에 대한 별건 영장을 청구하도록 하고 있다. 즉, "전자정보에 대한 압수·수색이 종료되기 전에 유관정보를 적법하게 탐색하는 과정에서 무관정보를 우연히 발견한 경우라면, 수사기관으로서는 더 이상의 추가 탐색을 중단하고 법원으로부터 별도의 범죄혐의에 대한 압수·수색영장을 발부받은 경우에 한하여 그러한 정보에 대하여도 적법하게 압수·수색을 할 수 있"도록 하는 예외를 대법원은 인정하고 있다.[77]

[77] 대법원 2015. 7. 16. 자 2011모1839 전원합의체 결정.

IV. 수사기관의 전자정보 압수·수색 행태에 대한 대응방안

1. 수사기관의 전자정보 압수·수색 실무

가. '선반출-후선별 압수'의 원칙화

수사 실무에서는 포렌식작업의 편의성 때문에서 현장에서 선별압수를 하는 것('현장 선별압수')보다는 '선반출-후선별 압수'가 선호된다. 이에 관련하여, 수사실무에서는 전자증거의 '무결성'(integrity)[78]을 확보하여 공판에서 증거능력 시비에 대비할 필요성이 크고, 사안에 따라서는 삭제된 정보까지 디지털포렌식을 통하여 복원하여 살펴볼 필요가 있다는 점을 강조한다.[79]

특히 휴대전화의 경우에는 '선반출-후선별 압수'의 비율이 압도적으로 높다. 그 비율은 PC의 경우와 비교할 때, 실무상 휴대전화(모바일)의 경우 예외적인 '매체압수'의 비율이 압도적으로 높아서 2006년~2017년 사이의 대검찰청 디지털수사과의 '디-넷'(D-NET) 통계를 보면, PC의 경우 선별압수가 80% 초과함에 반하여 모바일의 경우 선별압수가 거의 없어 매체압수가 100%에 가깝다고 한다.[80] 원칙과 예외가 뒤바뀌어 운영되고 있는 것이다. (게다가 압수한 휴대전화를 이미징하여 '디-넷'(D-NET)에 등록한 이후에도 '범행도구'라는 이유로 공판이 끝날 때까지 반환하지 않는 경우도 많다고 한다).[81]

---

[78] "압수물인 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체(이하 '정보저장매체'라고만 한다)에 입력하여 기억된 문자정보 또는 그 출력물(이하 '출력 문건'이라 한다)을 증거로 사용하기 위해서는 정보저장매체 원본에 저장된 내용과 출력 문건의 동일성이 인정되어야 하고, 이를 위해서는 정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 사정, 즉 무결성이 담보되어야 한다. 특히 정보저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다." 이는 대법원 2007. 12. 13. 선고 2007도7257 판결<일심회 판결>을 따르면서, 재진술한 대법원 2013. 7. 26. 선고 2013도2511 판결<왕재산 사건>의 일부이다.

[79] 예컨대, "(2) '죄' 밝힐 정보만? 현실은 '인생' 정보 통째로 압수", 경향신문 2021. 3. 19, <https://www.khan.co.kr/national/national-general/article/202103190600045>, 최종검색: 2024. 6. 20.

[80] 오현석, 전자증거의 선별압수와 매체압수에 관한 연구, 6-11면

[81] "(2) '죄' 밝힐 정보만? 현실은 '인생' 정보 통째로 압수", 경향신문 2021. 3. 19, <https://www.khan.co.kr/national/national-general/article/202103190600045>, 최종검색: 2024. 6. 20.

나. 수사상 무관정보 탐색의 관행

(1) 판례에 나타난 수사상 무관정보 탐색의 관행

‘선반출-후선별 압수’에 대한 대법원의 규제 법리가 실무에서는 잘 작동하지 않은 것으로 보인다. 이 ‘혐의사실과 관련된 전자정보’(무관정보)의 ‘탐색’ 사례는 판례에서 종종 확인되기 때문이다.

대표적인 예가 전자정보의 압수·수색과 관련하여 수사상 무관정보 탐색에 제동을 건 <종근당 사건>(대법원 2015. 7. 16.자 2011모1839 전원합의체 결정)이 있다. 이 사건에서 담당검사는 2011. 업무상 배임 등의 혐의로 제약회사 빌딩에 있는 대표이사 사무실을 압수·수색영장(이하 ‘제1 영장’이라고 한다)을 발부받아 압수수색하였다. ‘선반출-후선별 압수’의 절차를 거쳐 저장매체에 저장되어 있는 전자정보파일 전부를 ‘이미징’의 방법으로 다른 저장매체로 복제(이하 ‘제1 처분’이라 한다)”하고 이를 ‘디-넷’(D-NET, 더 정확하게는 그 일부인 ‘원격디지털수사공조시스템’)에 등록한 후, 복제본을 “자신이 소지한 외장 하드디스크에 재복제(이하 ‘제2 처분’이라 한다)하고 (…) 제1 영장에 기재된 혐의사실과 무관한 정보들도 함께 출력(이하 ‘제3 처분’이라 한다)하였”고, 이를 토대로 1달여 지나서 “ 별도의 압수·수색영장(이하 ‘제2 영장’이라 한다)을 발부받아 외장 하드디스크에서 별건 정보를 탐색·출력하는 방식으로 압수·수색”하였다. 제2·3 처분 시에 피고인측의 참여권은 배제되었다.

이 사건에서 검찰은 강력부검사가 “임의로 이미징 복제본을 재복제해 둔 외장 하드디스크에서 제1 영장 기재 혐의사실[의] 혐의와 관련된 전자정보를 탐색하던 중 우연히 [다른 범죄] 위반 혐의에 관련된 전자정보[를] 발견하”고 제2 영장을 청구하였다고 주장하였다.

이에 대해 대법원은 “제1 영장에서 예외적으로나마 저장매체 자체의 반출이나 그 전자정보 전부의 복제가 허용되어 있으나, 제2 영장 청구 당시 압수할 물건으로 삼은 정보는 제1 영장의 피압수자에게 참여의 기회를 부여하지 않은 상태에서 임의로 재복제한 외장 하드디스크에 저장된 정보로서 그 자체가 위법한 압수물이어서 앞서 본 별건 정보에 대한 영장청구 요건을 충족하지 못한 것이므로, 비록 제2 영장이 발부되었다고 하더라도 그 압수·수색은 영장주의의 원칙에 반하는 것으로서 위법하다”고 보았다.

또한 최근 대법원 판결(대법원 2024. 4. 16. 선고 2020도3050 판결<무관정보 이용 청탁금지법 수사 사건>)은 무관정보를 적극적 활용한 별건 압수·수색에 대해

위법수집증거배제법칙(형소법 제308조의2)을 적용하여 증거능력 배제하였다.[82] 이 사건의 사실관계는 <종근당 사건>과 많이 다르지 않다. 수사기관은 「국토의 계획 및 이용에 관한 법률」(국토계획법) 위반 등 "제1 영장 기재 혐의사실과 관련된 전자정보를 탐색하[여] 관련된 혐의사실 부분을 정리하여 이를 CD에 복제한 다음 수사기록에 편철"한 후(제1 영장 집행), 약 3개월에 걸쳐 영장 없이 '디-넷'(D-NET, 대검찰청 서버)에 저장된 전자정보를 탐색하여, 청탁금지법 관련 디지털증거를 추출하여 "무관정보를 우연히 발견하였음에도 더 이상의 추가 탐색을 중단하고 법원으로부터 압수 · 수색영장을 발부"받는 것처럼 하여 제2 영장을 청구하여 집행하였다.

이 사건에서 대법원은 "수사기관이 새로운 범죄혐의의 수사를 위하여 ['디-넷'(D-NET, 대검찰청 서버)에 저장되어 있고] 무관정보가 남아 있는 복제본을 열람하는 것은 압수 · 수색영장으로 압수되지 않은 전자정보를 영장 없이 수색하는 것과 다르지 않다."고 보아 "제1 영장 집행 종료 후 무관정보를 삭제 · 폐기 · 반환 등의 조치를 취하지 않고 계속 보관하면서 이를 탐색 · 복제 · 출력하는 [행위를] 비롯한 일련의 수사상 조치"와 이에 기초한 제2 압수는 모두 위법하다고 하였다. 앞의 <종근당 사건>과 다른 것은 별도의 저장매체를 사용하지 않고 '디-넷'(D-NET)을 열람하여 '탐색'하였다는 점이다. 이에 대해서도 대법원은 제한을 가한 것이다.

(2) 수사상 무관정보 탐색과 '디-넷'(D-NET)의 운영규정

위 2개의 대법원 판결은 무관정보 탐색을 위한 별건 영장의 청구라는 대법원의 기본 법리를 수사 실무에서 어떻게 '적응'하고 있는가를 잘 보여주는 사례이다. 이상과 같은 광범한 무관정보 '탐색'이 가능한 것은 영장의 특정성이 제대로 기능하기 어려워 전자정보에 대한 포괄적 압수·수색이 이루어질 수 있고 그와 함께 한 번 수집된 피의자의 전자정보가 장기간 보존되기 때문이다.

앞서 본 「디지털 증거의 수집·분석 및 관리 규정」(관리규정) 제54조 제2항의 '디지털증거의 폐기'에 관한 예외사유에서도 이 점은 잘 확인된다.

> 관리규정 제54조(폐기대상)
> ② 제1항에도 불구하고 다음 각 호의 사유가 있는 경우에는 압수의 원인이 된 사건의 공소시효가 완성될 때까지 디지털 증거를 폐기하지 않을 수 있다.

[82] 관련 기사로는 "대법원, 검찰의 '디지털 캐비닛' 수사에 제동 판결", 경향신문 2024. 4. 26, <https://www.khan.co.kr/national/court-law/article/202404261201001>, 최종검색: 2024. 6. 20.

1. 압수의 원인이 된 사건과 형사소송법 제11조에 따라 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 경우
2. 압수의 원인이 된 사건이 기소중지처분 또는 참고인중지처분이 된 경우
3. 불기소처분을 한 사건 또는 무죄판결이 확정된 사건 중 공범 등에 대한 수사를 계속할 필요가 있다고 인정되는 경우

우선, 예외사유가 지나치게 넓어서 사실상 무관정보와 유관정보의 구별을 무색하게 한다. 특히, 같은 조 제2항 제1호는 "압수의 원인이 된 사건과 형사소송법 제11조[83]에 따라 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 경우"를 예외사유로 하고 있다. 전자증거의 압수·수색에서 적용되는 '관련성 요건'은 이보다는 훨씬 좁다. 「형사소송법」 제11조 제1호는 인적 관련성만 요구한다. 즉, 「형사소송법」 제11조 제1호의 "1인이 범한 수죄"를 기준으로 할 경우, '인적 관련성'과 인정되면 거의 무제한하게 해당 피압수자 사건에 대해 '디지털증거'를 보유할 수 있게 된다. 둘째, 제3호의 경우에도 "공범 등에 대한 수사"가 명확하지 않다. 특히 "무죄판결이 확정된 사건"의 경우에도 폐기의 예외가 된다면 검사의 판단에 따라 보관되어야 할 증거의 범위가 어디까지인지 알기 어렵다. 다음으로, 시간적으로도 "해당 사건의 "압수의 원인이 된 사건의 공소시효가 완성될 때"까지로 상당히 장기이다.

보다 근본적으로는, 관리규정 제54조 제2항가 예정하는 모든 경우가 무관정보를 함께 보관하는 경우를 정당화할 수 있는 사유가 되기 어렵다는 점에서 문제이다. 무관정보는 예외 없이 폐기해야 한다는 것은 앞에서 살펴본 대법원의 법리와 이 법리를 토대로 작성된 압수·수색 영장의 기재 취지에 부합한다. 법원의 영장발부 실무에서는 대법원 판례 법리에 따라 압수·수색영장의 별지에 "압수대상 및 방법의 제한"을 기재하여 발부하는데, 여기에는 '무관정보의 삭제·폐기·반환'의 취지를 기재하고 있다.[84] 위와 관리규정 제54조 제2항은 이에 위배된다.[85]

---

[83] 「형사소송법」 제11조 (관련사건의 정의) 관련사건은 다음과 같다.
1. 1인이 범한 수죄
2. 수인이 공동으로 범한 죄
3. 수인이 동시에 동일장소에서 범한 죄
4. 범인은닉죄, 증거인멸죄, 위증죄, 허위감정통역죄 또는 장물에 관한 죄와 그 본범의 죄

[84] "혐의사실과 관련된 전자정보의 탐색·복제· 출력이 완료된 후에는 지체없이, 피압수자 등에게 ① 압수 대상 전자정보의 상세목록을 교부하여야 하고, ② 그 목록에서 제외된 전자정보는 삭제·폐기 또는 반환하고 그 취지를 통지하여야 함" 법원의 영장실무상 영장 기재양식의 변천에 관하여는 오현석, 전자증거의 선별압수와 매체압수에 관한 연구, 16면 이하. 그리고 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정 이후 서울중앙지방법원 영장전담판사의 실무 개선안(2015. 8. 1.자 시행)에 관하여는 손지영·김주석, 압수·수색 절차의 개선방안에 관한 연구, 사법정책연구원, 2016, 211면 이하, 또한 "2019. 6. 21. 기준 서울중앙지방법원 영장재판부의 '압수대상 및 방법의 제한' 별지"의 기재례는 박병민·서용성, 디지털 증거 압수수색 개선방안에 관한 연구 —법률 개정에 관한 논의를 중심으로—, 192면 이하.

[85] 박병민·서용성, 디지털 증거 압수수색 개선방안에 관한 연구 —법률 개정에 관한 논의를 중심으로—, 266면.

2. 전자정보의 압수·수색 실무에 대한 통제 방안

가. 개관

전자정보의 압수·수색에 관한 수사기관의 실무를 통제하거나 개선하기 위한 노력은 다각도에 이루어지고 있다. 대법원와 법원 실무에서는 영장주의(특히 영장의 특정성, 집행방법)에 의한 통제와 위법수집증거배제법칙(「형사소송법」 제308조의2)에 의한 통제가 주된 것이다. 「형사소송법」 제417조의 준항고에 의한 통제[86]도 생각할 수 있으나 '디-넷'(D-NET)에 이미 전자정보가 등록된 상황에서는 이를 통한 수사활동을 알기 쉽지 않아 역시 제한적이다. 법원 입장에서는 법정에 나온 증거 이외에는 통제할 방법이 마땅하지 않다. 결국 입법에 의한 통제가 강조될 수밖에 없다. 이에 따라 다양한 입법적 제도적 제안이 나와 있는 이유이다.[87]

제도적 개선방안으로는, 법원을 중심으로 해서 보면, ① 압수수색 대상으로서 '정보'의 명문화, ② 영장 발부시 집행방법에 관한 구체적·개별적 사전 규제 도입(전자 증거 압수·수색 사전심문제도[88] 포함), ③ 현장 선별압수 원칙의 강화(신속한 환부와 예외적 원본 보관)[89], ④ 수색영장·압수영장의 분리 발부, ④ 유관정보 선별과정에서의 참여권 강화[90], ④ 집행결과의 법원 보고의무 명시, ④ 저장매체 반환의무와 무관정보 폐기 및 통보 의무 명시 등이 대표적이다.[91] 또한 수사기관에 대한 것으로는 ① 독립한 포렌식기관의 설치, ② 저장매체

---

[86] 앞서 본 <종근당 사건>(대법원 2015. 7. 16.자 2011모1839 전원합의체 결정)이 준항고 사건이다.
[87] 이미 「형사소송법 일부개정법률안」(의안번호 1913878, 김도읍의원 등 10인), 「형사소송법 일부개정법률안」(의안번호 2001352, 김도읍의원 등 10인, 앞의 법안과 동일), 「형사소송법 일부개정법률안」(의안번호 2114302, 이수진의원 등 10인) 등이 제안된 바 있고, 제22대 국회에서는 단행법률로도 준비되고 있다. 예컨대, 조국혁신당의 「전자정보 압수·수색에 관한 특례법안」[조국 의원 대표발의, 2024. 6. 0.(예정)](🥷압수된 인권, 복제되는 삶👩🏿(전자정보 압수·수색에 관한 특례법 제정을 위한 입법 토론회 자료집, 조국혁신당), 2024. 6. 17, 29-39면).
[88] 이원상, "암호화된 스마트폰 압수·수색 규범의 법률화 필요성", 232면.
[89] 곽병선, "디지털 증거의 압수 · 수색절차상 문제점과 개선방안", 259-260면.
[90] 관련하여, 휴대전화 압수시 고지의무를 규정하여 체포구속이유고지제도와의 유사한 '권리고지'를 강화하는 방안도 도입할 필요가 있다. 권리고지는 진술거부권과 마찬가지로 그 불고지 자체가 그 증거에 대한 배제로 이어져야 한다.
[91] 전자증거의 압수·수색 개선방안에 관한 포괄적인 연구로는 박병민·서용성, 디지털 증거 압수수색 개선방안에 관한 연구 —법률 개정에 관한 논의를 중심으로—, 221면 이하.

반환의무와 무관정보 폐기 및 통보 의무 위반 시의 형사처벌[92] 등이 있다. 대체로 현재의 수사실무를 개선할 수 있는 합리적 제안으로 생각된다.

나. 무관정보의 수집·보관에 대한 통제 방안

전자정보의 압수·수색 관련하여 무관정보의 취득으로 인한 문제점은 학계와 실무계에서 오래 전부터 지적되어 왔다. 문제는 현행 「형사소송법」 제도로는 ―수사활동이라고 하면서― 은밀하고 광범위하게 이루어지는 특정인에 대한 정보수집 활동을 통제할 마땅한 방도가 없다는 점이다. 무관정보 활용 수사에 대해서는 검찰에게 위법수집증거배제라는 제재만으로는 무관정보의 장기간 보관 및 이용을 억제할만한 충분한 실효성이 없다. 검찰이 그 위험을 기꺼이 감수할 가능성이 있다.

압수·수색 대상범죄의 유죄 입증에는 제한이 없고 새로 '탐지'한 증거를 토대로 전자증거로부터 파생하는 다른 증거를 찾으면 되기 때문이다. 대법원 판례에서 다른 처분이 문제 되는 이유는 해당 전자정보 이외에 다른 유력한 증거가 없었기 때문이다. 이를 '우연한 발견'의 법리에 기대어 적법한 증거로 활용하고자 했으나 법원에 의해 제동이 걸린 것이다. 다른 유력하고 독립적인 증거가 있다면 이 증거를 위법수집증거배제법칙 적용이라는 부담을 안고서 법정에 증거로 현출할 필요는 없었을 것이다. 최근 무관정보 '탐색'에 기초한 후속 압수·수색영장의 효력을 부인하는 일련 대법원 판결은 이 지점에 서 있다. 앞서 본 바와 같이, 그 의미가 큰 것을 사실이지만, 그것으로도 한계가 있다. 따라서 결국 무관정보의 폐기 나아가 무관정보 수집과 보전에 관한 수사기관의 동기를 억제하고 기회를 제거하는 것은 이와는 다른 길을 택해야 한다.

여기에서는 기존에 제안된 방안 중에서 2가지 주요한 제도적 제안을 중심으로 검토하고자 한다. 형사절차상의 사법작용상의 대응은 개별 사안별로 법관이 통제하는 것에 주력을 두는 것으로 생각된다. 여기에 더하여 무관정보의 확보 가능성과 활용 가능성을 통제하기 위해서는 보다 일반적·체계적으로 접근할 필요가 있을 것이다. 그러한 제안 중 주목되는 것으로, 하나는

---

[92] 예컨대, 조국혁신당의 「전자정보 압수·수색에 관한 특례법안」[조국 의원 대표발의, 2024. 6. 0.(예정)](💂‍♀️압수된 인권, 복제되는 삶💁🏿‍♀️(전자정보 압수·수색에 관한 특례법 제정을 위한 입법 토론회 자료집, 조국혁신당), 2024. 6. 17, 29-39면).
* 법안 제15조(무관정보 미삭제 · 폐기죄) 제9조 제1항을 위반하여 무관정보를 삭제 · 폐기 또는 반환하지 아니한 자는3년 이하의 징역 또는 5년 이하의 자격정지에 처한다.
* 법안 제9조(무관정보의 삭제 · 폐기등) ① 수사기관등은 제8조 제4항의 목록에 포함되지 않은 전자정보(이하"무관정보"라 한다)가 있는 경우 해당 전자정보를 지체 없이 삭제 또는 폐기하거나 반환하여야 한다.

압수영장과 수색영장의 분리발부와 집행 제도이고, 다른 하나는 독립한 포렌식기관의 설치이다.

(1) 압수영장과 수색영장의 분리

「형사소송법」은 전자증거의 압수·수색에 관하여 현장 선별압수를 원칙으로 하고, 매체·복사본 반출 후 선별을 예외로 규정하고 있지만, 수사 실무는 '선반출-후선별 압수'를 원칙화하고 있다. 이러한 상황은 규범적 선언만으로 개선되기 쉽지 않아 보인다.

실무상으로는 '선반출-후선별 압수'의 경우 영장 전담 재판부에서 시행되고 있는 영장 별지의 "압수 대상 및 방법의 제한"에 사후 소명의무를 추가하고 그 소명이 부족한 경우 (영장 없는 압수의 경우) 사후영장을 기각하거나 (사전 영장의 경우) 본안에서 압수된 증거의 증거능력을 배제하자는 제안도 있다.[93]

여기에서 더 나아가 '반출'한 경우에는 —긴급한 필요나 수사의 효율성을 고려한 예외적인 사유 등 특별한 사정이 없는 한,— '반출' 이후의 '탐색'은 별도의 영장을 발부 받도록 하는 것이다. '반출' 자체를 하나의 영장[수색영장]으로 하고, 다시 반출 이후의 절차를 또 다른 영장[압수 또는 검증영장[94]]을 발부하도록 하자는 것이다. 법원 실무에서도 하급심에 이러한 제한적 범위 영장을 발부하기도 하였다.[95]

학설로는 현장에서의 디지털증거의 선별이 어려운 사정을 고려하여, 전자증거의 압수·수색 절차를 증거수집단계(1단계)와 증거분석단계(2단계)로 나누어 2단계에서 엄격한 선별압수가 이루어질 수 있도록 하자는 견해[96]도 동일한 문제의식으로 이해된다. 또한 수색대상(물리적 공간 대 비물리적 공간)과 압수대상(유체물 대 무체물)의 차이를 고려하여 압수·수색영장을 단계별로 청구하고 집행하여야 한다는 견해[97]도 비슷하다.

---

[93] 이기리, "디지털증거의 압수·수색 개선방안", 형사법 실무연구II, 제133집, 법원도서관, 2016, 421면.
[94] 디지털증거의 성격상 검증영장에 의한 규율도 함께 고려해야 한다.
[95] 실무상 사례로, "수색 영장만을 발부하고, 수색결과를 반영하여 추후 압수 영장을 재청구하라"고 한 사건에 관하여는 박병민·서용성, 디지털 증거 압수수색 개선방안에 관한 연구 —법률 개정에 관한 논의를 중심으로—, 241면. "서울중앙지방법원 영장재판부는 2007년 기술유출사건(서울중앙지방법원 2007영장번호6497호), 제이유그룹로비사건(서울중앙지방법원 2007영장번호11822호), 재벌 회장 폭행사건(서울중앙지방법원 2007영장번호11901호)에 관한 압수수색영장 청구에 대해 압수 청구 부분을 기각하고, 수색영장만 발부하여 준 적이 있다."(같은 곳).
[96] 곽병선, "디지털 증거의 압수 · 수색절차상 문제점과 개선방안", 법학연구 제51집, 한국법학회, 2013.9, 258면. "영장심사단계나 집행단계에서 선별적 압수의 원칙을 실현할 수 없다면, 영장집행후 단계에서 선별적 압수의 원칙을 실현하면 된다. 즉, 1단계 증거수집 단계에서는 선별적 압수의 원칙을 유연하게 적용하되, 2단계 증거분석단계에서 선별적 압수의 원칙이 실현될 수 있도록 제도적 장치를 마련하는 것이다."
[97] 박세영, 디지털 정보의 수사상 강제처분에 관한 연구, 한양대학교 박사학위논문, 2021, 143면 이하.

(2) 독립한 디지털포렌식 기관의 설치

미국의 경우 전자증거의 사후분석과정에서 수사 담당부서와 분리된 별도의 필터팀을 운영하는 경우가 있다고 한다. 필터팀이란 수사 담당부서와 디지털포렌식 부서 사이에 일종의 차이니스 월(chinese wall)[98]을 두는 것이다. 수사상 프라이버시의 유지와 제3자에 의한 디지털증거 분석을 통한 과도한 정보수집을 기하자는 취지의 제도이다.[99] 미국의 실무에서는 이미 활용되고 있으며 긍정적인 평가를 받고 있다고 한다.[100]

우리의 경우, 수사기관인 검찰과 경찰에 디지털포렌식 기관이 소속되어 있다.[101] 특히 검찰은 공판에서 일방 당사자가 되는 주체이면서 동시에 디지털포렌식 기관도 보유하고 있다. 이 때문에 디지털포렌식의 중립성과 공정성이 충분히 담보될 수 있는가가 문제될 수 있다. 여기에서 독립한 디지털포렌식기관의 필요성이 강조된다.[102]

미국의 경우처럼, 필터팀을 두거나 필터링 기능을 하는 기관을 두자는 제안이 있다. 즉, "법원에서 포렌식 인력 양성을 통해 필터링 업무를 수행하든지 아니면 대학이나 중립적인 제3의 기관에서 업무를 위탁 받아 필터링을 수행하는 방법으로 제도를 발전시키"자는 것이다.[103] 수사 실무에서 유관증거와 무관증거가 혼재된 경우에 대응하여, 강제처분인 「형사소송법」의 압수·수색 제도가 가지는 침해성이 전자증거의 경우에 극히 심화된다는 점 그리고 기술의 발달에 효율적으로 대응하는 전문기구는 수사기관도 수사와는 다른 기술적 차원에서 전자증거의 수집과 관리를 전담할 수 있다는 점[104] 등을 고려할 때, 수긍할 수 있는 제안으로 생각된다. 현실적으로는 법원의 부담과 관리비용을 고려할 때 독립기관으로 설치하여 다양한 수사기관의 존재와 향후 발전가능성을 고려할 때 —기존 경찰과 검찰의 디지털포렌식 기구를 통폐합하여— 수사기관과도 분리된 독립기구로 함이 바람직할 것이다.

---

98 이에 관한 소개로는 오현석, 전자증거의 선별압수와 매체압수에 관한 연구, 144면 이하.
99 곽병선, "디지털 증거의 압수 · 수색절차상 문제점과 개선방안", 261면.
100 이에 관한 상세 소개로는 모성준, "미국의 압수수색절차에 대한 사법적 통제의 단계구조 -디지털 증거를 중심으로 -", 207-211면. 판례로는 United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir., 2010)(같은 글, 208면), 실무사례로는 FBI의 윌리엄 제퍼슨(William J. Jefferson) 사건 수사(같은 글, 209면)가 소개되어 있다.
101 민간에 의한 포렌식의 경우도 없는 것은 아니나 공신력 등을 이유로 대부분의 포렌식은 수사기관 소속의 포렌식 기관에서 이루어진다.
102 박세영, 디지털 정보의 수사상 강제처분에 관한 연구, 151면 이하.
103 곽병선, "디지털 증거의 압수 · 수색절차상 문제점과 개선방안", 260-262면; 홍진표, "디지털 증거에 대한 압수수색 영장제도의 실무적 개선방안 고찰", 165-166면.
104 디지털증거의 '무결성'과 '동일성'은 증거능력의 요건 자체는 아니며 증거능력을 인정하기 위한 전제라고 할 수 있다. 따라서 독립한 기관을 두어 디지털증거에 대한 디지털포렌식을 별도로 수행하게 한다면 이에 따라 '무결성'과 '동일성' 등의 요건은 굳이 수사기관에게 입증하게 하지 않아도 되므로 법정에서의 절차도 달리 구성할 수 있다. 공판에서 소추기관이 증거능력의 입증에만 집중할 수 있게 된다면 공판의 효율성도 제고될 수 있을 것이다.

정리하자면, 전자증거의 경우에 수사기관과 독립된 '제3의 서버관리기관'을 두어 무관정보 반환·폐기와 통보 절차를 담당하게 할 필요가 있다. 디지털포렌식 전문가에 의한, 선별 작업이 끝난 모든 파일도 그 포렌식센터가 일정 기간 보관했다가 바로 폐기하든지 아니면 선별 작업 끝나면 바로 폐기하도록 하는 것이다. 수사기관은 디지털포렌식 전문가를 경유하거나 그 조력을 받아서만 디지털증거에 접근할 수 있도록 하는 것이다.

V. 나오며

무관정보를 활용한 검찰의 수사 사례들은 전자증거의 압수·수색 과정을 강제처분임에도 법원의 영장에 의한 통제가 쉽지 않음을 보여준다. 형사작용법으로 「형사소송법」에 의한 통제나 헌법적 통제가 실효적으로 작동하기 어려운 국면에 놓여 있기 때문이다. 과학기술의 발달이 전자증거에 대한 법적 통제가 용이하지 않다는 점에서나 유체물에 대한 집행을 염두에 두고 만들어진 압수·수색의 관념과 규정이 전자증거의 특수성을 제대로 반영하기 쉽지 않다는 점에서나[105] 기존의 규율방식만으로 한계가 있다.

최근의 '디-넷'(D-NET) 사태는 전자증거 압수·수색에 관한 수사실무를 적나라하게 드러내주었다. 무관정보와 관련된 수사실무는 「형사소송법」의 명문과 대법원의 판례 법리에서 벗어나 있다. 법적 규율을 벗어난 실무는 그 자체로 헌법상 적법절차와 영장주의의 가치에 대한 이해의 차이를 보여준다. 모든 국가기관은 헌법적 가치의 실현 그리고 최대한의 법치실행의 의무를 지고, 검찰, 경찰 등 수사기관도 예외가 되지는 않는다는 점에서 현재의 전자증거 압수·수색 관련 실무는 개선되어야 한다.

현재의 실무를 교정하기 위해서는 영장제도가 가지는 가치를 유지하면서 전자정보의 압수·수색 실무에 대한 통제를 강화하는 동시에 수사기관의 위법수사 동기를 제어할 수 있는 제도가 필요하다. 여기에서는 압수영장과 수색영장의 분리와 독립한 포렌식기관의 설치와 운영을 검토하였으나 이에 한정되지 않고 전자정보의 구조와 특수성을 고려한 다양한 제도적 통제방안이 고민되고 또 입법적으로 도입되어야 한다.

[105] 압수·수색의 대상으로서 '유체물'과 '정보'의 차이와 여기에 개입한 법적 규율상 '아날로드 마인드'와 '디지털 마인드'의 차이에 대해서는 오길영, "디지털 저장매체의 압수·수색과 그 쟁점", 27면 이하.

참고문헌

대검찰청, 검찰연감, 2023.

박병민·서용성, 디지털 증거 압수수색 개선방안에 관한 연구 —법률 개정에 관한 논의를 중심으로—, 사법정책연구원, 2021.

손지영·김주석, 압수·수색 절차의 개선방안에 관한 연구, 사법정책연구원, 2016.

오현석, 전자증거의 선별압수와 매체압수에 관한 연구, 서울대학교 석사학위 논문, 2019.

이숙연, 형사소송에서의 디지털증거의 취급과 증거능력, 고려대학교 박사학위 논문, 2011.

탁희성·이원상, 디지털포렌식 통합모델 구축에 관한 연구, 한국형사정책연구원, 2016.

곽병선, “디지털 증거의 압수·수색절차상 문제점과 개선방안”, 법학연구 제51집, 한국법학회, 2013.9, 249-265면.

모성준, “미국의 압수수색절차에 대한 사법적 통제의 단계구조 —디지털 증거를 중심으로—”, 법학연구 제27권 제2호, 연세대학교 법학연구원, 2017.6, 191-221면.

봉지욱(뉴스타파 기자), “대통령의 압수수색”, 🙅‍♀️압수된 인권, 복제되는 삶🙅🏿‍♀️(전자정보 압수·수색에 관한 특례법 제정을 위한 입법 토론회 자료집, 조국혁신당), 2024. 6. 17, 13-19면.

오길영, “디지털 저장매체의 압수·수색과 그 쟁점”, 민주법학 제49권, 민주주의법학연구회, 2012.7, 13-39면.

이기리, “디지털증거의 압수·수색 개선방안”, 형사법 실무연구II, 제133집, 법원도서관, 2016, 389-429면.

조성훈, “전자정보 접근 방법의 법적 문제 —진술거부권과 관계를 중심으로—”, 법조 제69권 제6호, 법조협회, 2020.12, 142-183면.

홍진표, “디지털 증거에 대한 압수수색 영장제도의 실무적 개선방안 고찰”, 사법 제1권 제50호, 사법발전재단, 2019.1, 107-172면.

「전자정보 압수·수색에 관한 특례법안」[조국 의원 대표발의, 2024. 6. 0.(예정)](『압수된 인권, 복제되는 삶』(전자정보 압수·수색에 관한 특례법 제정을 위한 입법 토론회 자료집, 조국혁신당), 2024. 6. 17, 29-39면.

대법원 사법행정자문위원회, “제16차 회의자료”, 2021. 10. 13,
<https://www.scourt.go.kr/supreme/news/NewsViewAction2.work?pageIndex=2&searchWord=&searchOption=&seqnum=14&gubun=943>, 최종검색: 2024. 6. 20.

대검찰청 홈페이지, “검찰활동” 중 “과학수사”,
<https://www.spo.go.kr/site/spo/02/10201070300002018112901.jsp>, 최종검색: 2024. 6. 20.

대검찰청 홈페이지, “사전정보공표 대상”, “2023년도 디지털 증거 압수수색, 증거분석 지원 현황”(디지털수사과), <https://www.spo.go.kr/site/spo/ex/announce/AnnounceInfo.do>, 최종검색: 2024. 6. 20.

“[단독] 검찰, 수사권 이용 민간인 불법사찰…휴대전화 정보 불법 수집·관리”, Newsverse 2024. 3. 21,
<https://www.newsverse.kr/news/articleView.html?idxno=5051>, 최종검색: 2024. 6. 20.

“(1) 영장엔 버젓이 ‘암호 푼 상태로’…내 정보, 풀라면 풀어야 하나”, 경향신문 2021. 3. 17,
<https://www.khan.co.kr/national/court-law/article/202103170600015>, 최종검색: 2024. 6. 20.

“(2) ‘죄’ 밝힐 정보만? 현실은 ‘인생’ 정보 통째로 압수”, 경향신문 2021. 3. 19,
<https://www.khan.co.kr/national/national-general/article/202103190600045>, 최종검색: 2024. 6. 20.

“(3) 압수된 데이터는 삭제되지 않는다”, 경향신문 2021. 3. 29,
<https://www.khan.co.kr/national/national-general/article/202103290600005>, 최종검색: 2024. 6. 20.

“(4) 지문과 홍채 정보도 압수되고 있다”, 경향신문 2021. 4. 2,
<https://www.khan.co.kr/national/national-general/article/202104020600005>, 최종검색: 2024. 6. 20.

“(5) ‘네 정보 내놔’를 멈출 5가지 제안”, 경향신문 2021. 4. 7,
<https://www.khan.co.kr/national/national-general/article/202104070600015>, 최종검색: 2024. 6. 20.

“[단독] 검찰, 압수한 전자정보 ‘입맛대로’ 저장했다”, 한겨레 2024. 3. 25,
<https://www.hani.co.kr/arti/society/society_general/1133752.html>, 최종검색: 2024. 6. 20.

“‘디넷에 저장된 12년 전 전자 정보도 현재까지 남아’”, Newsverse 2024. 4. 29,
<https://www.newsverse.kr/news/articleView.html?idxno=5261>, 최종검색: 2024. 6. 20.

“‘수사 빌미’ 개인정보 검찰, 5만건 보관 중”, 경향신문 2021. 3. 29,
<https://www.khan.co.kr/national/national-general/article/202103290600015>, 최종검색: 2024. 6. 20.)

“9년 묵은 압색 정보도 대검은 갖고 있다”, 경향신문 2021. 4. 2,
<https://www.khan.co.kr/national/court-law/article/202104020600015>, 최종검색: 2024. 6. 20.

“대법원, 검찰의 ‘디지털 캐비닛’ 수사에 제동 판결”, 경향신문 2024. 4. 26,
<https://www.khan.co.kr/national/court-law/article/202404261201001>, 최종검색: 2024. 6. 20.

"압수수색 휴대폰·노트북 정보 통째 보관하는 검찰…위법 논란에 피의자 동의도 허술", 경향신문 2024. 3. 27, <https://www.khan.co.kr/national/court-law/article/202403270600171>, 최종검색: 2024. 6. 20.

"압수수색영장 대면심리제 도입될까", 주간경향 2024. 1. 1, <https://m.weekly.khan.co.kr/view.html?med_id=weekly&artid=202312250700001&code=115#c2b>, 최종검색: 2024. 6. 20.

발제문2

전자정보의 압수 및 보관·폐기에 관한 개선방안

권경선 / 서울중앙지방법원 판사

I. 들어가며[106]

- 2021. 3. 28. '대검찰청 전국디지털수사망(D-NET, 이하 '디넷') 스토리지 활용도' 자료를 보면, 검찰은 2012. 4. 디넷 구축 이후 전자정보 이미징 데이터 14만 1,739건을 서버에 저장했고, 이 중 35.2%인 4만 9,942건은 2021. 2. 기준으로 여전히 서버에 남아 있다. 이 가운데 스마트폰 데이터는 총 5만 441건이 저장돼 1만 4,550건이 남아 있다.[107]

- 주식회사 케이티의 대표이사였던 이○○에 대한 2012년 상반기 대졸 신입사원 부정채용관련 업무방해 사건[108]에서, 서울중앙지방검찰청 과학기술지원단 사무실에 보관 중이던 모바일 포렌식 자료가 압수되었다. 그러나 압수된 자료는 이미 무죄판결이 확정된 특정경제범죄가중처벌등에관한법률위반(배임) 등 사건에 관한 압수.수색영장으로 압수한 피고인의 아이패드 미니 등에서 추출한 것으로, 압수가 있었던 사건에서 무죄판결이 확정되었음에도 검찰은 사건 관련 전자정보를 폐기하지 않고 계속 보관하고 있다가 별건의 증거로 삼기 위해 다시 압수.수색영장을 청구하였다.

- 뉴스버스 이○○ 대표의 스마트폰과 뉴스버스 사무실에 있는 업무용PC 등을 2023. 12. 압수수색하는 과정에서 검찰이 이대표의 동의 없이 범죄혐의와 관련 없는 전자정보 등 스마트폰 전체를 복제해 디넷에 저장한 사실이 보도되었다.[109]

---

[106] 이하의 내용은 발제자 개인의 의견으로 법원의 공식적인 입장이 아님을 밝혀둡니다.
[107] 경향신문, [단독]'수사 빌미' 개인정보 검찰, 5만건 보관 중, 2021. 3. 29. 자 https://v.daum.net/v/20210329060209574?x_trkm=t (2024. 6. 19. 최종 확인).
[108] 서울남부지방법원 2019고합169, 181, 182(병합) 사건.
[109] 뉴스버스, "[단독] 검찰, 수사권 이용 민간인 불법사찰…휴대전화 정보 불법 수집·관리", https://www.newsverse.kr/news/articleView.html?idxno=5051 (2024. 6. 19. 최종 확인).

이와 같이 압수된 전자정보가 압수된 전자정보가 판결이 확정된 후에도 폐기되지 않고 계속해서 보관되고 있고, 보관되고 있던 전자정보가 별건 수사에 활용되고, 별건에서 증거로 제출되어 문제가 되고 있다.

전자정보의 압수와 관련하여, 압수.수색영장에 기재된 '범죄혐의사실과 관련된 전자정보'(이하 '유관정보')의 범위를 넘어서는 전자정보까지 압수되는 경우가 빈번히 발생한다. 특히 휴대폰의 경우 범죄혐의사실과 관련 없는 전자정보(이하 '무관정보')를 포함한 휴대폰에 저장된 전체 전자정보를 이미징한 다음 복제한 전체 이미지파일(이하 '전체 이미지파일')을 디넷에 업로드하여 보관하는 것이 오히려 일반적이다.

아래에서는 전자정보의 압수·보관·폐기에 관한 실무를 살펴보고, 이러한 실무의 문제점과 검찰이 전자정보의 압수·보관·폐기 실무의 근거로 삼는 대검찰청 예규인 「디지털 증거의 수집 분석 및 관리 규정」의 문제점에 관하여 검토한다. 그리고 전자정보 압수 방법에 대한 개선안을 제시한다. 다음으로 압수한 전자정보의 보관·폐기의 원칙을 살펴보고 이러한 원칙이 지켜지지 않는 이유가 무엇인지, 이에 대한 개선방안은 무엇이 있는지를 본다.

Ⅱ. 전자정보 압수, 보관·폐기 실무의 문제점

1. 전자정보 압수, 보관·폐기 실무

헌법 제12조에서 "누구든지 법률에 의하지 아니하고는 … 압수·수색 … 을 받지 아니하며"(제1항), "… 압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다."(제3항)라고 정하여 압수.수색에 관한 적법절차와 영장주의의 원칙을 선언하고 있고, 이에 따라 압수.수색 여부를 수사기관의 전적인 재량에 맡기는 영장의 발부는 금지된다. 형사소송법 제106조 제3항 본문에서는 "압수의 목적물이 정보저장매체등인 경우 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다"고 규정함으로써 선별압수를 원칙으로 하고 있다. 대법원 결정 역시 현장에서의 선별압수를 원칙으로 하고, 정보저장매체 또는 이미징한 파일의 압수를 예외로 하고 있다.[110] 그러나 현재의 압수 실무는 원칙이 오히려 예외가 된 상황이다.

특히 휴대폰의 경우 전체 이미지파일을 복제하여 디넷에 업로드한 다음, 이 전체 이미지파일에 대하여 선별작업을 거쳐 유관정보만으로 선별 이미지파일을 만드는 절차를 거치는 것이 일반적이다. 그런데 휴대폰과 같은 경우 수많은 문서, 동영상, 사진 등이 파일의 형태로 저장되고, 파일을 작성한 시간, 인터넷 접속기록 등이 세세하게 기록되어 있다. 이러한 전자정보는 개인의 행동을 시간, 장소적으로 재구성할 수 있게 할 뿐만 아니라 개인의 내밀한

[110] 대법원 2011. 5. 26.자 2009모1190 결정(전교조 사건), 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정(종근당 사건).

생각까지 포함하고 있는 경우가 많아 그 보유자가 대체로 타인과 공유하는 것을 원하지 않는 것인데도 그 정보의 무한 복제가 가능하다.[111] 전자정보의 특성상 다른 정보저장매체에 비해 형사소송법 제106조 제3항 본문에서 정한 선별압수의 원칙이 지켜져야 할 필요성은 더욱 크지만, 사실상 실무는 휴대폰에 저장된 무관정보를 포함한 이미지파일이 일단 수사기관이 가져가는 방식으로 운영되고 있다.

2. 이에 대한 통제수단

대법원은 2023. 5. 1. 수사기관이 새로운 범죄 혐의를 수사하기 위해 무관정보가 남아있는 복제본을 열람하는 것은 압수되지 않은 전자정보를 영장 없이 수색하는 것과 마찬가지이고, 복제한 전체 이미지파일은 더 이상 수사기관의 탐색, 복제 또는 출력의 대상이 될 수 없음을 명확히 하였다(대법원 2023. 5. 1. 선고 2018도19782 판결).[112] 이에 따라 수사기관이 보관하고 있던 전체 이미지파일에 대하여 별도의 압수.수색영장을 발부받더라도 증거능력이 없고, 당사자의 동의가 없더라도 증거능력이 없다. 그러나 이는 사후적 통제수단으로, 이것만으로는 효과적인 통제수단이 된다고 보기 어렵다. 수사기관이 보관하고 있던 무관정보를 별도 범죄사건에서 증거로 활용하지 않는 이상, 외부로 드러나지 않아 알 수 없고 실질적으로 통제할 방법이 없다.

3. 전자정보의 압수.·보관 관련 대검찰청 예규와 실무의 문제점

대검은 2024. 3. 23. "검찰은 형사소송법 제313조 2항에 따른 '과학적 분석결과에 기초한 디지털포렌식 자료를 통한 증거능력'을 보장하기 위해 2019. 5. 20. 대검 예규를 개정해 공판에서의 증거가치 보전을 위해 사후 검증 등에 필요한 이미지파일을 보관할 수 있도록 했다"고 밝혔다. 또 대검은 "전자저장매체에 저장된 정보를 압수한 경우 범죄사실과 관련성 있는 부분을 선별해 압수하고 있는데, 특히 휴대전화에 저장된 정보를 선별, 추출할 경우 전자정보의 기술적 특성상 선별, 추출한 편집본의 형식을 취할 수밖에 없다"고 했다. 대검은 "피고인, 변호인 측에서 공판절차 진행 중 전자정보의 편집본 형식에 대해 기술적 오류, 조작, 위변작, 작성자 불명, 내용 부지, 해킹 등 다양한 주장과 이의를 제기하고 있"는데, "공판

---

[111] 2015. 7. 16. 자 2011모1839 전원합의체 결정의 제1·2·3 처분에 관한 다수의견에 대한 대법관 이인복, 대법관 이상훈, 대법관 김소영의 보충의견.

[112] 수사기관이 유관정보를 선별하여 압수한 후에도 무관정보를 삭제·폐기·반환하지 않은 채 그대로 보관하고 있다면 무관정보 부분에 대하여는 압수의 대상이 되는 전자정보의 범위를 넘어서는 전자정보를 영장 없이 압수.수색하여 취득한 것이어서 위법하고, 사후에 압수.수색영장이 발부되었다거나 피고인이나 변호인이 증거로 함에 동의하였다고 하여 위법성이 치유된다고 볼 수 없다(대법원 2022. 1. 24. 자 2021모1586 결정). 무관정보가 남아있는 복제본은 더 이상 수사기관의 탐색, 복제 또는 출력 대상이 될 수 없고, 수사기관은 새로운 범죄혐의의 수사를 위해 필요한 경우에도 기존 압수.수색과정에서 출력하거나 복제한 유관정보의 결과물을 열람할 수 있을 뿐이다. 따라서 사후 법원으로부터 복제본을 대상으로 압수.수색영장을 발부받아 집행하였다 하더라도 이는 압수.수색절차가 종료됨에 따라 당연히 삭제·폐기되었어야 할 전자정보를 대상으로 한 것으로 위법하다(대법원 2023. 6. 1. 선고 2018도19782 판결, 대법원 2023. 10. 18. 선고 2023도8752 판결).

과정에서의 증거능력 다툼의 소지에 대비해 형사소송법, 대검 예규에 따라 사후 검증 등에 필요한 전자정보 이미지파일 일시 보관이 필요하게 된 것"이라며 "이미지파일은 기술적으로 그 자체로는 내용을 알 수 없도록 돼 있고, 만약 이러한 이미지파일을 보관하지 못한다면 피고인 등의 여러 주장과 사후 검증에 대비할 수 없으며, 부득이 휴대전화 자체를 반환하지 않고 보관해야만 하는데 이는 압수대상자에게 더 큰 불편을 초래하게 된다"고 강조했다.[113]

가. 전자정보의 압수.·보관 관련 대검찰청 예규의 문제점

전자정보의 압수.보관과 관련하여 법무부령인 「검찰보존사무규칙」, 대검찰청 예규인 「디지털 증거의 수집 분석 및 관리 규정」, 경찰청 훈령인 「디지털 증거의 처리 등에 관한 규칙」, 대통령령인 「검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정」 등이 있다. 이하에서는 대검찰청 예규인 「디지털 증거의 수집 분석 및 관리 규정」(이하 '대검 예규')의 전자정보 압수.보관 관련 규정의 내용을 중심으로 살펴본다.

(1) 2019. 5. 20. 개정 전 대검 예규

2019. 5. 20. 개정 전 대검 예규는 디지털 증거의 등록에 관하여, 선별압수된 이미지파일만을 등록하도록 규정하고 있었다.[114] 이 규정은 형사소송법 제106조 제3조의 선별압수 원칙에 따른 내용이지만, 실무는 예규와는 달리 전체 이미지파일을 계속 보관하는 경우가 있었던 것으로 보인다. 한편 디지털 증거의 폐기와 관련하여, 2019. 5. 20. 개정 전 대검 예규에서는 폐기의 연한 등을 정하지 않고 있었다.[115]

---

[113] 대검, '전자정보 이미지파일 저장' 형소법 따른 공판 대비용…뉴스버스 보도 반박, 2024. 3. 23. 아시아경제, 최석진 기자.

[114] 디지털 증거의 수집·분석 및 관리 규정 [시행 2017. 3. 1.] [대검찰청예규 제876호, 2016. 12. 26., 일부개정] (이하 '2019. 5. 20. 개정 전 대검 예규')
제18조 (선별 이미지파일 등의 등록) 제15조 제1항 본문에 따라 정보저장매체 등에 기억된 정보의 범위를 정하여 선별 압수된 증거파일 또는 선별 이미지파일을 디지털수사통합업무관리시스템에 등록한다. 다만, 제15조 제1항 단서의 경우에는 예외로 한다.<개정 2016. 12. 26.>
제19조 (정보저장매체 등의 이미지 등록 및 피압수자 등의 참여)
① 제15조 제1항 단서 중 정보저장매체 등을 직접 압수한 경우 또는 제9조 제2항의 분석 의뢰를 받은 경우에는 대상 정보저장매체 등의 봉인을 해제한 후 해당 사건 주임검사 주도하에 사건과 관련성이 있는 전자정보를 선별하여 증거파일 또는 선별 이미지파일을 만든 다음 디지털수사통합업무관리시스템에 등록하고, 대상 정보저장매체 등은 재봉인하여 지원요청자에게 인계한다. <개정 2016. 12. 26.>
② 제15조 제1항 단서 중 정보저장매체 등에 기억된 전자정보 전부를 이미지파일로 압수한 경우에는 해당 사건 주임검사 주도하에 사건과 관련성이 인정되는 전자정보를 선별하여 증거파일 또는 선별 이미지파일로 만든 다음 디지털수사통합업무관리시스템에 등록한다. <개정 2016. 12. 26.>
③ 제1항 내지 제2항의 선별 과정에서 피압수자 등의 참여를 보장하여야 한다. 피압수자 등이 참여한 경우에는 별지 제5호의 서식에 따라 확인서를 작성토록 한다. <개정 2016. 12. 26.>
④ 피압수자 등이 참여를 하지 않겠다는 의사표시를 한 경우에는 신뢰성과 전문성을 담보할 수 있는 상당한 방법으로 사건과 관련성이 있는 정보를 선별하여 압수한다. <신설 2016. 12. 26.>

[115] 2019. 5. 20. 개정 전 대검 예규
제27조 (디지털 증거의 폐기)
① 디지털증거관리책임자 등은 디지털수사통합업무관리시스템에 등록된 디지털 증거에 대해 해당 사건 주임검사의 폐기 요청 또는 압수전담검사의 폐기촉탁이 있으면 해당 디지털 증거를 폐기하여야 한다.

(2) 2019. 5. 20. 개정된 제991호[116]

2019. 5. 20. 개정으로 전체 이미지파일 등록의 근거가 마련되었고, 나아가 이미지파일을 업무관리시스템에 등록하지 않을 수 있도록 하는 규정도 두고 있었다.[117] 한편 디지털 증거의 폐기에 관한 규정을 구체화하였다.[118] 즉 범죄사실과 무관한 디지털 증거와 유죄판결이 확정된

---

② 제1항과 같이 디지털 증거를 폐기한 다음 해당 사건 주임검사의 폐기 요청에 따른 경우에는 별지 제7호 서식의「디지털증거 폐기확인서」를, 압수전담검사의 폐기촉탁에 따른 경우에는 별지 제8호 서식의「디지털증거 폐기(촉탁) 회보서」를 각각 교부하여야 한다.
③ 제9조 제3항 본문에 따라 형사사법정보시스템(KICS)과 연동하여 사건번호가 입력된 지원요청의 디지털 증거 중 주임검사 처분시까지 압수물로 수리되지 않은 디지털 증거는 지원요청 부서에 통보 후 폐기한다.
④ 제9조 제3항 단서에 따라 형사사법정보시스템(KICS)과 연동하여 사건번호가 입력되지 않고 디지털수사통합업무관리시스템에 등록된 지원요청의 디지털 증거는 6개월 이내에 형사사법정보시스템(KICS)과 연동된 사건번호의 입력이 없고 해당 사건 주임검사의 별도 보관 요청이 없을 경우 지원요청 부서에 통보 후 폐기한다.

[116] 부칙 <제991호,2019.5.20.>
제1조(시행일) 이 규정은 2019. 5. 20.부터 시행한다.
제2조(존속기한) 이 예규는「훈령 · 예규 등의 발령 및 관리에 관한 규정」에 따라 이 예규를 발령한 후의 법령이나 현실 여건의 변화 등을 검토하여야 하는 2022. 5. 20.까지 효력을 가진다.

[117] 2019. 5. 20. 개정 예규
제24조 (이미지파일 등의 등록)
① 제18조제1항에 따라 생성된 이미지파일과 증거파일(이하 '이미지파일 등'이라고 한다) 및 제23조에 따라 생성된 이미지파일은 다음 각 호의 구분에 따라 업무관리시스템에 등록한다. 다만, 정보저장매체 등으로부터 기억된 전자정보 전부에 대하여 생성한 이미지파일의 등록은 다음 각 호의 절차에 따른다.
1. 정보저장매체 등으로부터 기억된 전자정보 전부에 대하여 생성한 이미지파일을 업무관리시스템에 등록한다.
2. 제1호와 같이 생성한 이미지파일에서 사건과 관련성이 인정되는 전자정보만을 선별하여 이미지파일을 생성한 경우에는 제1호에 따라 등록된 이미지파일을 삭제하고 선별하여 생성한 이미지파일을 등록한다.
3. 제2호에도 불구하고 사건관련 전자정보를 선별하여 압수하는 과정에서 발생하는 전자정보의 변경·손실이 증거가치를 훼손할 우려가 있는 경우에는 제1호에 따라 등록된 이미지파일을 삭제하지 않도록 한다.
② 제19조 및 제23조에 따라 피압수자 등에게 교부한 전자정보 상세목록파일의 사본을 업무관리시스템에 등록한다.
③ 대용량 기타 기술적 사유 등으로 업무관리시스템에 이미지파일 등을 등록하는 것이 현저히 곤란한 경우에는 업무관리시스템에 등록하지 않고 압수물에 준하여 별도로 관리할 수 있다.

[118] 2019. 5. 20. 개정 예규
제8장 디지털 증거의 폐기
제34조 (디지털 증거의 폐기 시 유의사항) 범죄사실과 무관한 디지털 증거는 폐기를 원칙으로 하되 디지털 증거를 폐기하는 과정에서 향후 재판 절차에 증거로 제출되어야 하는 디지털 증거가 폐기되는 일이 없도록 유의하여야 한다.
제35조 (폐기대상)
① 다음 각 호에 해당하는 디지털 증거는 본 장에서 규정한 절차에 따라 폐기하는 것을 원칙으로 한다.
1. 해당사건에 대한 기소·불기소 등 종국처분에 따라 계속 보관할 필요성이 없다고 인정되는 경우
2. 유죄판결이 확정된 사건의 경우
② 제1항에도 불구하고 압수대상사건과 형사소송법 제11조에 따라 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 디지털 증거에 대하여는 폐기하지 않을 수 있다.
제36조 (폐기요청) 수사 또는 재판 중인 사건에서 디지털 증거의 폐기는 주임검사 는 승계검사가 요청할 수 있고, 재판이 확정된 사건에서 디지털 증거의 폐기는 압수전담검사가 요청할 수 있다.
제37조 (폐기절차)
① 수사 또는 재판 중인 사건에서 디지털 증거의 폐기를 요청하는 경우에는 다음 각 호의 절차에 따라 폐기를 진행한다.
1. 주임검사는 기소 또는 불기소 처분 시 계속 보관할 필요성이 없는 디지털 증거에 대하여 폐기촉탁지휘를 한다.
2. 사건 처분 결과가 기소중지 및 참고인 중지에 해당하는 디지털 증거는「검찰압수물사무규칙」제62조(기소중지처분·참고인중지처분 사건의 압수물처분)를 준용하여 공소시효가 완성된 이후에 폐기하여야 한다.
3. 불기소처분을 한 사건 또는 무죄판결이 확정된 사건 중 수사를 계속할 필요가 있는 사건의 디지털 증거로서 법원의 결정이나「형사소송법」의 규정에 의하여 폐기되지 아니한 디지털 증거는「검찰압수물사무규칙」제62조(기소중지처분·참고인중지처분 사건의 압수물처분)를 준용하여 공소시효가 완성된 이후에 폐기하여야 한다.

사건의 디지털 증거는 폐기하는 것을 원칙으로 규정하였다. 그러나 형사소송법 제11조의 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 디지털 증거, 유죄판결이 확정된 사건에서 수집된 디지털 증거는 재심청구 기회 보장을 위해 형이 확정된 때부터 10년간 보존할 수 있도록 규정함으로써 넓은 범위의 예외를 두어 원칙이 지켜지지 않을 여지가 크다.

(3) 2021. 1. 1. 개정된 제1151호[119]

2021. 1. 1. 개정으로 새로운 내용이 다수 등장하였다. 이는 현재 시행 중인 2022. 5. 18. 개정된 제1285호[120]의 내용과 대동소이하다.

(가) 범죄혐의와의 관련성

개정 대검 예규는 제22조에 관련성의 판단기준에 관한 조항을 신설하면서, 제1항에서 "주임검사등은 압수 · 수색시를 기준으로 압수 · 수색 · 검증영장에 기재된 피의자나 진범 및 공범의 범죄혐의와 기본적인 사실관계가 동일하거나 동종 · 유사 범행과 관련된다고 의심할 만한 상당한 이유가 있는 범위 내의 전자정보, 이들의 범행 동기나 목적 그 밖에 형법 제51조(양형의 조건)에서 규정한 사항에 해당한다고 인정되는 범위 내의 전자정보, 이러한 전자정보의 출처증명 기타 법정에서 디지털 증거의 정확성과 신뢰성의 입증에 필요한 범위 내의 전자정보 등을 함께 압수할 수 있다"고 규정하였다.

한편 대법원 판례가 인정하는 관련성의 범위는 다음과 같다.

"형사소송법 제215조 제1항은 "검사는 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 지방법원판사에게 청구하여 발부받은 영장에 의하여 압수·수색 또는 검증을 할 수 있다."라고 규정한다. 여기에서 '해당 사건과 관계가 있다'는 것은 압수·수색영장에 기재한 혐의사실과 관련되고 이를 증명할 수 있는 최소한의 가치가 있는 것으로서 압수·수색영장의 혐의사실과

---

4. 폐기촉탁지휘를 받은 압수물담당직원은 KICS의 압수물관리시스템을 통하여 디지털수사과장에게 해당 디지털 증거에 대한 폐기를 요청한다.
5. 디지털수사과장은 폐기를 요청 받은 디지털 증거를 지체 없이 폐기하고 별지 제12호 서식의 "디지털증거 폐기(촉탁) 회보서"를 업무관리시스템을 통하여 입력하는 방법으로 작성하여 압수물담당직원에게 회보한다.
제38조 (유죄확정 판결에 대한 특례)
① 유죄판결이 확정된 사건에서 수집된 디지털 증거는 유죄의 확정판결을 받은 피고인의 재심청구의 기회를 보장하기 위하여 형이 확정된 때로부터 10년간 보존할 수 있다.
② 판결 확정 이후 당사자의 폐기요청이 있는 경우에는 디지털 증거를 폐기한다. 다만, 유죄의 확정판결을 받은 자가 수인인 경우에는 당사자 전원의 폐기요청이 있을 경우에 폐기한다.
③ 내란죄, 외환죄 등 「검찰보존사무규칙」 제8조제3항에 해당하는 죄의 디지털 증거는 「검찰보존사무규칙」 제8조제3항을 준용하여 영구 또는 준영구로 보존한다.

[119] 부칙<제1151호, 2021.1.1.>
제1조(시행일) 이 규정은 2021. 1. 1.부터 시행한다.
제2조(존속기한) 이 규정은 「훈령 · 예규 등의 발령 및 관리에 관한 규정」에 따라 발령 후 법령이나 현실 여건의 변화 등을 검토하여야 하는 2024. 1. 1.까지 효력을 가진다.

[120] 부칙 <제1285호, 2022.05.18.>
제1조(시행일) 이 규정은 2022. 5. 18.부터 시행한다.
제2조(존속기한) 이 규정은 「훈령 · 예규 등의 발령 및 관리에 관한 규정」에 따라 발령 후 법령이나 현실 여건의 변화 등을 검토하여야 하는 2025. 5. 18.까지 효력을 가진다

사이에 객관적, 인적 관련성이 인정되는 것을 말한다. ① **혐의사실과의 객관적 관련성**은 압수·수색영장에 기재된 혐의사실 자체 또는 그와 기본적 사실관계가 동일한 범행과 직접 관련되어 있는 경우를 의미하지만, 범행 동기와 경위, 범행 수단과 방법, 범행 시간과 장소 등을 증명하기 위한 간접증거나 정황증거 등으로 사용될 수 있는 경우에도 인정할 수 있다. 이때 객관적 관련성은 압수·수색영장에 기재된 혐의사실의 내용과 수사의 대상, 수사 경위 등을 종합하여 구체적·개별적 연관관계가 있는 경우에만 인정할 수 있고, 혐의사실과 단순히 동종 또는 유사 범행이라는 사유만으로 객관적 관련성이 있다고 볼 수는 없다. 그리고 ② **피의자 또는 피고인과의 인적 관련성**은 압수·수색영장에 기재된 대상자의 공동정범이나 교사범 등 공범이나 간접정범은 물론 필요적 공범 등에 대한 사건에 대해서도 인정할 수 있다."

2021. 1. 1. 개정된 대검 예규에서 정한 '관련성'은 대법원이 인정하는 관련성의 범위에 비해 훨씬 넓다. 즉 개정 대검 예규 제22조의 '동종·유사 범행과 관련된다고 의심할 만한 상당한 이유가 있는 경우'만 하더라도 혐의사실과의 객관적 관련성을 혐의사실과 단순히 동종 또는 유사 범행이라는 사유만으로는 인정할 수 없고, 구체적.개별적 연관관계가 있는 경우에만 인정하고 있다고 보는 법원의 관련성 기준보다 넓은 범위이다. 그런데 위 규정에서는 나아가 양형자료와 원본성 입증에 필요한 전자정보 역시 관련성이 있는 것으로 규정하고 있다. 이는 압수.수색영장에서 정하는 유관정보의 범위를 초과하는 것으로, 사실상 모든 전자정보의 압수에서 전체 이미지파일을 보관하는 근거로 활용될 위험성이 있다.

나아가 대검 예규 제26조 제1항에서는 "주임검사등은 전자정보에 대한 압수 · 수색 · 검증을 하는 경우에 별지 제13호의 '전자정보 압수 · 수색 · 검증 안내문'에 따라 전자정보에 대한 압수 · 수색 · 검증 과정을 설명하는 등으로 참여권의 실질적 보장을 위하여 노력하여야 한다."고 정하고 있다. 별지 제13호 서식 [전자정보 압수.수색검증 안내문]에서는 '사건과 관련 있는 전자정보'가 압수 대상이라고 하면서, 검찰에서는 관련성 있는 전자정보를 다음과 같은 기준으로 판단하고 있다고 적고 있다. 이는 개정된 대검 예규 제22조에서 규정한 관련성의 범위와 동일하다.

[5] '사건과 관련 있는 전자정보'가 압수 대상이며 검찰에서는 다음과 같은 기준으로 관련성을 판단하고 있습니다.

1. 수사란 범인을 발견, 확보하고 증거를 수집, 보전하기 위한 수사기관의 활동이므로, 전자정보의 압수도 큰 틀에서는 이러한 필요성을 기준으로 합니다.

2. 검찰은 수사과정에서 양형에 대한 정상자료도 수집해야 하며, 법정에서 디지털 증거의 정확성, 신뢰성 검증을 위해 재현이 필요한 경우에는 증거의 증거로서 복제본 전체가 필요할 수도 있습니다.

3. 위와 같은 기준에 따라 관련성 있는 전자정보를 정리하면 아래와 같습니다.

【관련성 있는 전자정보】

① **(사건 관련성)** 압수·수색 시를 기준으로 압수·수색·검증영장에 기재된 피의자나 진범 및 공범의 범죄혐의와 기본적인 사실관계가 동일하거나 동종·유사 범행과 관련된다고 의심할

만한 상당한 이유가 있는 범위 내의 전자정보

② **(양형자료)** 피의자나 진범 및 공범의 범행 동기나 목적 그 밖에 형법 제51조(양형의 조건)에서 규정한 사항에 해당한다고 인정되는 범위 내의 전자정보

③ **(원본성 입증)** 위와 같은 전자정보의 출처증명 기타 법정에서 디지털 증거의 정확성과 신뢰성의 입증에 필요한 범위 내의 전자정보

이에 따를 때 '사건과 관련 있는 정보'의 범위는 대법원 판례의 인정 범위보다 훨씬 넓고, 전체 이미지파일에 대해서도 관련성을 인정할 수 있다.

(나) 전체 이미지파일 보관의 근거 마련

개정 대검 예규는 제41조에서 전체 이미지파일을 업무관리시스템에 등록할 수 있는 절차를 구체화함으로써 전체 이미지파일을 보관, 등록할 근거를 마련하였다. 한편 개정 대검 예규 제35조, 제36조에서 '전자정보의 탐색 · 복제 · 출력을 완료한 경우에는 지체 없이 피압수자등에게 전자정보 상세목록을 교부하고 담당 디지털포렌식 수사관에게 별지 제15호 서식에 따라 전자정보의 삭제 또는 폐기를 요청한다'고 규정하고 있다. 별지 제15호 서식(목록에 없는 전자정보에 대한 지휘)은 압수한 전자정보의 목록에 포함되지 않은 전자정보에 대한 주임검사등(주임검사 또는 검찰수사관)의 삭제·폐기 지휘 양식인데, 이 양식에는 지휘내용으로 "① 정보저장매체 등에 기억된 전자정보 전부를 복제한 파일과 사건과 관련 있는 전자정보만 선별하여 복제한 파일 모두 업무관리시스템에 등록하여 보존하고, 등록하지 않은 대상 전자정보는 삭제·폐기하기 바람"이라고 기재되어 있다. 그리고 '전부 이미지' 보존 필요성과 관련하여 예시로, "'전부 이미지'를 보존하지 않을 경우 법정에서 동일성을 재현하거나 검증하는데 상당한 지장을 초래할 우려가 있음"이라고 기재하고 있어 이 규정이 전자정보 상세목록에 기재하지 않은 압수대상과 전체 이미지파일을 디넷에 보관할 근거로 활용될 여지가 있다.

(다) 전체 이미지파일에 대한 추가 탐색 및 분석 가능성

개정 대검 예규는 제37조에서 "법정에서 디지털 증거의 재현이나 검증을 위해 필요한 경우 이미지파일의 보관을 요청할 수 있다"고 한 다음, 제38조 제2항에서 "제37조에 따라 업무관리시스템에 등록한 이미지 파일에 대한 추가 탐색이나 분석을 위해 접근권한을 새로 부여받고자 하는 경우 소속 청의 인권보호관으로부터 승인을 받아 디지털수사과장에게 공문으로 이미지파일에 대한 접근권한의 부여를 요청할 수 있다"고 규정하면서, 제3항에서 "주임검사등이 제2항에 따라 접근 권한을 부여받아 이미지파일에서 추출된 파일을 탐색하는 경우에는 피압수자등이나 변호인에게 제32조에 따른 참관의 기회 등을 제공하여야 한다. 다만, 법정에서 디지털 증거의 동일성이나 분석 결과의 정확성, 신뢰성 등을 검증하기 위하여 필요한 분석 등을 수행하는 경우에는 그러하지 아니하다."라고 규정하였다. 제38조 제2항과 제3항의

내용을 종합해 보면, 법정에서 디지털 증거의 재현이나 검증을 위해 보관한 전체 이미지파일이 무결성·동일성 입증 목적이 아닌 별건 수사 등의 목적을 위해 활용될 위험성이 있다.

(라) 폐기 관련 규정

개정 대검 예규 제38조 단서는 전체 이미지파일을 "분석결과의 정확성, 신뢰성 등에 대한 검증을 위해 계속 보관할 수 있다"고 규정하고 있고, 제54조 제2항 제1호에서 "압수의 원인이 된 사건과 형사소송법 제11조에 따라 관련성이 인정되는 사건에서 증거로 사용될 것이 예상되는 경우, 불기소처분을 한 사건 또는 무죄판결이 확정된 사건 중 공범 등에 대한 수사를 계속할 필요가 있다고 인정되는 경우 압수의 원인이 된 사건의 공소시효가 완성될 때까지 디지털 증거를 폐기하지 않을 수 있다"고 정하고 있다. 나아가 "유죄판결이 확정된 사건에서 압수된 디지털 증거는 피고인에게 재심청구의 기회를 보장하기 위하여 확정된 때로부터 10년간 보존할 수 있다"는 규정을 2019. 5. 20. 개정 예규에서부터 계속해서 유지하고 있어, 넓은 범위에서 폐기의 예외 규정을 두고 있다.[121]

(4) 경찰청의 「디지털 증거의 처리 등에 관한 규칙」과의 비교

경찰청의 「디지털 증거의 처리 등에 관한 규칙」의 경우, 2023. 7. 4. 일부 개정되었으나 2019. 5. 20. 개정 전 대검 예규와 같이 제19조 제2항에서 "제15조제1항에 따라 복제본을 반출한 경우 범죄혐의와 관련된 부분만을 선별하여 탐색 · 출력 · 복제하여야 한다"고 규정하는 등으로 선별압수 원칙에 부합하는 규정을 두고 있다. 또한 대법원 판례의 설시와 유사하게 제20조에서 "경찰관은 제14조부터 제17조, 제19조까지의 규정에 따라 혐의사실과 관련된 전자정보를

---

[121] 디지털 증거의 수집·분석 및 관리 규정 [시행 2022. 5. 18.] [대검찰청예규 제1285호, 2022. 5. 18., 일부개정]
제48조(생성 이미지파일 등 삭제) 제43조에 의한 분석을 위해 생성한 이미지파일이나 분석 과정에서 생성된 일체의 전자정보는 분석결과 회신 후 지체 없이 삭제하여야 한다. 다만, 제42조 및 제45조에 따라 업무관리시스템에 등록한 전자정보와 분석보고서는 분석결과의 정확성, 신뢰성 등에 대한 검증을 위해 계속 보관할 수 있다.
제54조(폐기대상)
① 다음 각 호에 해당하는 디지털 증거는 본 장에서 규정한 절차에 따라 업무관리시스템에서 폐기한다.
1. 수사 또는 재판 과정에서 범죄사실과 관련성이 없는 것으로 확인된 경우
2. 압수의 원인이 된 사건에 대한 기소 · 불기소 등 종국처분에 따라 계속 보관할 필요성이 없다고 인정되는 경우
3. 판결이 확정되어 계속 보관할 필요성이 없다고 인정되는 경우
② 제1항에도 불구하고 다음 각 호의 사유가 있는 경우에는 압수의 원인이 된 사건의 공소시효가 완성될 때까지 디지털 증거를 폐기하지 않을 수 있다.
1. 압수의 원인이 된 사건과 형사소송법 제11조에 따라 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 경우
2. 압수의 원인이 된 사건이 기소중지처분 또는 참고인중지처분이 된 경우
3. 불기소처분을 한 사건 또는 무죄판결이 확정된 사건 중 공범 등에 대한 수사를 계속할 필요가 있다고 인정되는 경우
제58조 (유죄확정 판결에 대한 특례)
① 유죄판결이 확정된 사건에서 압수된 디지털 증거는 피고인에게 재심청구의 기회를 보장하기 위하여 형이 확정된 때로부터 10년간 보존할 수 있다.
② 판결 확정 이후 당사자의 폐기요청이 있는 경우에는 디지털 증거를 폐기한다. 다만, 유죄의 확정판결을 받은 자가 수인인 경우에는 당사자 전원의 폐기요청이 있을 경우에 폐기한다.
③ 내란죄, 외환죄 등 「검찰보존사무규칙」 제8조제3항에 해당하는 죄의 디지털 증거는 「검찰보존사무규칙」 제8조제3항을 준용하여 영구 또는 준영구로 보존한다.

탐색하는 과정에서 별도의 범죄 혐의(이하 "별건 혐의"라 한다)를 발견한 경우 별건 혐의와 관련된 추가 탐색을 중단하여야 한다. 다만, 별건 혐의에 대해 별도 수사가 필요한 경우에는 압수 · 수색 · 검증영장을 별도로 신청 · 집행하여야 한다."고 규정하고 있다.

또한 전자정보의 폐기와 관련하여서는, 제35조 제2항에서 "경찰관은 제1항의 분석결과물을 회신받아 디지털 증거를 압수한 경우 압수하지 아니한 전자정보를 지체 없이 삭제 · 폐기하고 피압수자에게 그 취지를 통지하여야 한다", 제3항에서 "경찰관은 사건을 이송 또는 송치한 경우 수사과정에서 생성한 디지털 증거의 복사본을 지체 없이 삭제 · 폐기하여야 한다.", 제4항에서 "제1항부터 제3항까지에 따른 전자정보의 삭제 · 폐기는 복구 또는 재생이 불가능한 방식으로 하여야 한다"는 규정을 두고 있다.

나. 현재의 전자정보 압수 실무의 문제점

압수.수색영장에서는 유관정보에 한하여 보관하고 무관정보는 폐기할 것을 정하였음에도 실제로는 수사기관이 유관정보뿐만 아니라 무관정보를 포함한 전체 이미지파일을 보관하고 있는 경우가 많다. 공판절차 진행 중 동일성.무결성을 입증해야 할 필요성을 이유로 하는 것이 대표적이다.

한편 피압수자는 유관정보 외에 무관정보, 전체 이미지파일을 수사기관이 계속 보관 중이라는 점을 인식하지 못하는 경우가 많다. 압수수색영장에는 범죄혐의사실과 관련이 있는 정보를 압수대상으로 하고 압수대상 전자정보 상세목록에서 제외된 전자정보는 삭제·폐기 또는 반환하고 그 취지를 통지해야 한다고 기재되어 있기 때문이다. 따라서 수사기관이 전체 이미지파일을 대상으로 선별작업을 마친 후 피압수자에게 압수물 목록이나 전자정보 상세목록과 전자정보 삭제·폐기 또는 반환 확인서를 교부하면, 피압수자는 나머지 전자정보는 폐기된 것이라고 생각하기 쉽다. 설령 무관정보가 공판 절차가 진행되는 중에 계속 보관된다는 사실까지는 인식했다 하더라도, 해당 정보가 판결이 확정된 이후에도 계속해서 폐기되지 않고 수사기관에 보관될 수 있다는 점까지 인식하는 경우는 드물 것이다.

나아가 수사주체이자 압수 집행의 주체인 수사기관이 압수한 전자증거의 보관까지 담당하고 있기 때문에, '본래 압수.수색영장의 취지에 따라 삭제·폐기되어야 하지만 유관정보의 증거가치 유지를 위하여 부득이하게 보관하는 것에 불과'한 무관정보[122]가 새로운 수사를 위해 활용되는 것이 아닌지에 대한 불안감을 불식시키기 어렵다.

[122] 서울고등법원 2022. 8. 12. 선고 2022노594 판결. 쌍방 상소하였으나 2022. 12. 15. 상고기각판결(무변론)로 확정되었다.

Ⅲ. 전자정보 압수 방법의 개선안

1. 유관정보를 넘어선 전자정보를 보관할 경우 압수.수색영장에 기재할 필요

수사기관이 정보저장매체에 저장된 전자정보를 압수하는 경우, 정보저장매체를 가져가는 대신 전체 이미지파일을 복제한 다음 이를 가지고 가서 선별작업을 거치는 것이 필요한 경우가 많을 것이다. 이때 수사기관이 전체 이미지파일에서 유관정보를 선별하는 것은 압수절차의 일부이고, 압수가 종료된 것이 아니다. 따라서 선별작업을 마친 후 유관정보만을 보관하고 전체 이미지파일 중 무관정보에 해당하는 부분은 폐기하는 것이 현재 전자정보 압수의 경우 일반적으로 발부되는 압수수색영장의 내용에 비추어 예정된 압수절차이다(별지2 참조).

그러나 현재 실무는 동일성·무결성 입증을 위해, 혹은 압수대상 파일에서 유관정보만을 가려내는 것이 어렵다는 이유 등으로 수사기관이 선별작업을 마치고 전자정보 상세목록을 피압수자에게 교부한 후에도 전체 이미지 파일을 계속 보관하는 경우가 많다. 결국 압수수색영장의 내용과 실무의 실제 운영방식 사이에 간극이 존재한다. 따라서 수사기관이 압수수색영장을 청구할 당시부터 전체 이미지파일을 계속 보관해야 할 상황이 예상될 경우 압수.수색영장을 청구할 때 전체 이미지파일을 압수할 필요성을 구체적으로 소명하여, 유관정보 외에 전체 이미지파일의 보관을 함께 구하거나, 현재 실무와 같이 유관정보에 대한 압수수색영장만이 발부되었는데 이후 압수.수색과정에서 무관정보까지 계속 보관할 필요가 발견되었다면, 해당 시점에 추가 수색을 멈추고 무관정보에 대한 압수.수색영장을 청구하는 방식으로 운영되어야 한다. 한편 이때의 압수수색영장은 동일성·무결성 입증을 위한 제한적인 용도를 위해 '보관'하는 것이므로, 실제로는 영장이 발부되더라도 일반적 압수수색영장의 경우와는 달리 수사기관이 이에 대하여 탐색할 수 있는 것은 아님을 영장 기재를 통해 명확히 할 필요가 있다.

현재와 같이 전체 이미지파일을 디넷이 저장하는 것은 동일성·무결성 입증 등 제한적인 용도로 파일을 '보관'하는 것이지 '압수'하는 것이 아니므로 '범죄혐의와 관련 있는 전자정보'에 한정하여 발부된 압수.수색영장으로 전체 이미지파일까지 계속 보관할 수 있다고 보는 것은, 영장의 기재 내지 법리와 실무 사이의 괴리를 만든다.

2. 이와 함께 필요한 조치

가. 압수물 목록 기재 실질화

수사기관은 무관정보나 전체 이미지파일에 대한 압수.수색영장을 발부받은 경우 압수물 목록이나 전자정보 상세목록에 유관정보와 무관정보를 구별하여 구체적으로 기재함으로써 무관정보 또는 전체 이미지파일까지 수사기관이 보관한다는 점을 피압수자에게 명확하게 고지할 필요가 있다. 이렇게 함으로써 피압수자는 어떠한 전자정보를 수사기관에서 압수한

것인지 알 수 있고, 이에 따라 준항고를 하는 등 권리행사를 할 수 있다. 나아가 피압수자가 공판절차에서 동일성.무결성을 다투지 않을 것이고 해당 전자정보가 자신의 휴대폰에 저장되어 있던 정보라는 점을 명확하게 하는 등으로 전체 이미지파일 보관의 필요성을 불식시킴으로써 전체 이미지파일에 대해서는 곧바로 폐기를 요구할 여지도 있을 것이다.

나. 긴급 압수.수색에 대한 사후영장에 대한 사법적 통제

사전영장에 의하지 않은 압수.수색이 허용되는 경우로는, 체포, 구속에 수반한 체포현장에서의 압수.수색(형사소송법 제216조 제1항 제2호, 제2항), 범행 중 또는 범행 직후 범죄장소에서의 압수.수색(형사소송법 제216조 제3항), 긴급체포 피의자의 소유물 등에 대한 24시간 내 압수.수색(형사소송법 제217조 제1항)이 있다. 이와 같은 경우 사후영장을 발부할 때 압수방법의 제한을 사전영장에 준하게 할 필요가 있다. 현재 사후영장의 경우 사전영장에 비해 간략한 양식의 별지를 사용하고 있다(별지2, 별지3 참조). 그러나 압수되는 대상의 성격은 달라지지 않을 뿐만 아니라 수사기관은 법원에서 사후영장이 발부되기 전까지 별다른 제한 없이 정보저장장치에 저장된 전자정보에 접근할 수 있으므로, 사후영장을 발부하는 경우에도 사전영장과 동일한 정도의 압수방법의 제한을 정할 필요가 있다.[123]

다. 별건에 대한 압수.수색영장 청구에 대한 사법적 통제

압수수색영장에 기재된 범죄사실과 관련성이 없는 범죄사실에 대한 증거물을 우연히 발견한 경우 그 증거물이 디지털 증거인지와 관계없이 원칙적으로 영장 없이 압수수색할 수 없다. 따라서 유체물이 아닌 전자정보에 대한 압수수색이 종료되기 전에 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우에는, 수사기관은 더 이상의 추가 탐색을 중단하고 법원에서 별도의 범죄혐의에 대한 압수수색영장을 발부받은 경우에 한하여 그러한 정보에 대하여 적법하게 압수수색을 할 수 있다(대법원 2015. 7. 16. 자 2011모1839 전원합의체 결정).

별건에 대한 압수수색영장 청구시 전자정보에 대한 압수수색이 종료되기 전에 우연히 발견한 것인지, 추가 탐색을 중단한 것인지 등에 관한 구체적인 소명 없이 압수수색영장을 발부받은 때로부터 몇 달이 경과한 후에 별건에 대한 압수수색영장을 청구하는 경우가 있다. 이러한 경우 이미 당초의 압수수색영장에 따른 압수가 종료된 이후일 가능성, 검찰이 디넷에 보관 중이던 무관정보에 대하여 탐색 후 압수수색영장을 청구하는 경우일 가능성 등을 배제할 수 없으므로, 구체적인 소명을 할 필요가 있다. 대법원 판례가 이와 같은 경우 위법수집증거로 증거능력을 배제한다 하더라도 이는 공소제기 후 사후통제수단에 불과하다.

나아가 별건에 대한 압수수색영장 청구를 너무 쉽게 허용할 경우, 수사기관이 더 많은 전자정보를 일단 입수하려고 할 유인이 커지고, 다른 범죄혐의를 목적으로 하고 다른 종류의 범죄에 대한 소명 후 휴대폰의 전체 이미지파일을 복제하려는 가능성도 배제할 수 없다.

---

[123] 홍진표, “디지털 증거에 대한 압수수색 영장제도의 실무적 개선방안 고찰”, 사법 통권 50호(2019), 사법발전재단, 145-146.

Ⅳ. 압수한 전자정보의 보관 · 폐기

1. 압수한 전자정보 보관 · 폐기에 관한 원칙

가. 판결이 확정된 경우

(1) 형사소송법과 대법원 판례

형사소송법 제332조에서 “압수한 서류 또는 물품에 대하여 몰수의 선고가 없는 때는 압수를 해제한 것으로 간주한다”고 규정하고 있으므로, 압수한 물건에 대해 몰수 선고가 없는 경우 환부하는 것이 원칙이다. 대법원 판례 역시 “압수물에 대한 몰수의 선고가 포함되지 않은 판결이 선고되어 확정되었다면 검사에게 압수물을 제출자나 소유자 기타 권리자에게 환부하여야 할 의무가 당연히 발생한다”고 판시하였다.[124] 따라서 유죄, 무죄를 불문하고 몰수 선고 없는 확정판결이 있는 경우 압수물을 환부할 의무가 발생하고, 수사기관이 보관할 수 없다.

전자정보의 경우 수사기관이 압수한 전자정보는 정보저장매체에 저장되어 있는 전자정보의 복제본이므로 피압수자에게 환부하는 것이 큰 의미가 없을 뿐만 아니라 돌려준다는 의미에서 환부의 대상이라고 보기 어렵다. 따라서 환부의 의미로 이를 폐기하여야 한다. 판결이 확정된 경우 폐기의 대상은 유관정보, 무관정보를 불문한다. 판결이 확정되기 전이라도 필요성이 소멸한 경우에는 즉시 폐기하여야 한다.

(2) 검찰보존사무규칙, 대검 예규의 폐기 제외 규정

그런데 검찰보존사무규칙 제62조는 기소중지처분 및 참고인중지처분을 하는 경우 압수물을 공소시효가 완성할 때까지 계속 보관해야 한다고 규정하고 있고, 제87조에서는 불기소처분을 한 사건이나 무죄판결이 확정된 사건 중 수사를 계속할 필요가 있는 사건의 압수물의 경우 제62조를 준용한다고 규정하고 있어 문제된다. 무죄판결이 확정된 사건의 경우 공소시효가 완성할 때까지 보관할 수 있다고 규정한 것은 위법하다. 다만 형사소송법 제218조의2 제1항은 “검사는 압수를 계속할 필요가 없다고 인정되는 압수물 및 증거에 사용할 압수물에 대하여 공소제기 전이라도 소유자나 기타 권리자의 청구가 있는 때에는 환부 또는 가환부하여야 한다”고 규정하고 있으므로, 불기소처분의 경우 형사소송법 제218조의2 제1항에서 규정한 압수를 계속할 필요가 있는지에 따라 허용될 여지가 있다.

다음으로 검찰보존사무규칙 제8조 제1항에서는 “형을 선고하는 재판이 확정된 사건기록은 형의 시효가 완성될 때까지 보존한다”라고, 제4항에서는 “무죄, 면소, 형의면제, 공소기각 또는 선고유예의 재판이 확정된 사건기록은 공소시효기간 동안 보존”하고, 내란죄, 외환죄, 뇌물죄 등 주요 사건기록은 준영구로 보존한다고 규정하고 있다. 이 규칙 제2조 제1호 가목에서는 ‘사건기록’을 “수사, 재판 등에 관한 문서와 기록, 그 밖의 관계 서류 또는

[124] 대법원 1995. 3. 10. 선고 94누14018 판결, 대법원 2022. 1. 14. 선고 2019다292197 판결.

물건(도면·사진·디스크·테이프·필름·슬라이드·영상녹화물·전자기록 등의 특수매체기록을 포함한다)"고 규정하고 있으므로, 제8조 제1항, 제4항의 경우 전자정보까지 함께 보존되는 것으로 볼 여지가 있다.

또한 대검 예규는 제54조 제2항과 제58조 제1항, 제3항에서 앞서 본 것과 같이 넓은 범위의 폐기에 대한 예외규정을 두고 있다. 특히 제54조 제1항 제1호, 제3호에서 "압수의 원인이 된 사건과 형사소송법 제11조에 따라 관련성이 인정되는 사건에서 증거로 사용될 것으로 예상되는 경우(제1호), 불기소처분을 한 사건 또는 무죄판결이 확정된 사건 중 공범 등에 대한 수사를 계속할 필요가 있다고 인정되는 경우(제3호)", 제58조 제1항에서 "유죄판결이 확정된 사건에서 압수된 디지털 증거는 피고인에게 재심청구의 기회를 보장하기 위하여 형이 확정된 로부터 10년간 보존할 수 있다"고 정하여 검찰보존사무규칙에서 규정하지 않은 폐기 제외 사유도 규정하고 있다.

형사소송법 제332조에서는 예외 규정을 별도로 두고 있지 않음에도 검찰보존사무규칙과 대검 예규에서 다수의 예외 규정을 두어 판결이 확정된 후에도 계속해서 전자정보를 보관할 수 있도록 규정한 것은 형사소송법에 반한다고 볼 여지가 있다. 또한 압수수색영장의 별지에 무관정보는 삭제, 폐기, 반환하도록 하였음에도 검찰보존사무규칙과 대검 예규에서 무관정보를 공소시효 만료시까지 혹은 공범에 대한 수사, 재심 청구 보장 등의 이유로 장기간 동안 보관할 수 있게 규정하고 있는 것 또한 위법의 소지가 있다.

나. 판결의 확정 전

수사기관이 판결의 확정 전 유관정보를 보관하는 것은 수사와 공소유지를 위해 반드시 필요하다. 문제는 유관정보를 넘어서는 범위의 전자정보를 보관할 필요가 있는지이다. 이는 일률적으로 결정할 수 없고 사안에 따라 결정되어야 하며, 수사기관이 무관정보를 보관할 필요성이 있는 경우가 있는지에 대해서 향후 충분히 검토할 필요가 있다. 따라서 앞서 본 것과 같이 전자정보를 압수하는 경우 유관정보를 압수하는 것을 원칙으로 하되, 그 이상을 보관할 필요가 있는 경우 이러한 사유를 소명하여 압수수색영장을 청구하고, 압수수색영장을 발부받은 범위에서 보관할 수 있다.

2. 실무상 원칙이 준수되지 않는 이유

우리 법상 수사의 주체와 압수 집행의 주체, 압수한 전자정보 보관.폐기의 주체가 일치하므로, 수사 주체가 압수를 집행하고 이후 압수된 전자정보를 보관하게 된다. 이 때문에 수사기관이 유관정보에 대한 선별작업을 거친 후 압수수색영장에서 허가받은 범위를 초과하여 무관정보를 계속 보관하더라도 외부에서는 알기 어렵고, 판결 확정 후 또는 압수의 필요성이 소멸한 이후에도 전자정보를 폐기하지 않고 계속 보관하더라도 이를 외부에서 알기 어렵다. 또한 대검 예규, 검찰사건사무규칙이나 검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정에서 폐기에 관한 규정을 두고 있으나 예외사유를 넓은 범위에서 규정하고 있어 판결 확정 후에도 전체 이미지파일까지 계속 보관될 가능성이 있을 뿐만 아니라 외부의 통제 수단 없는 수사기관 내부의 절차에 불과하다.

3. 개선방안: 법원 등 제3의 기관의 전자정보 보관

가. 제3의 기관에 의한 전자정보 보관의 방법

수사기관이 압수수색영장에 따라 전체 이미지파일을 압수한 경우, 현재와 같이 검찰이 관리하는 디넷이 아닌 제3의 기관이 관리감독권한을 가진 서버에 올리도록 할 필요가 있다. 전체 이미지파일은 현재와 같이 디넷에 일단 등록하도록 하되, 압수수색영장의 집행이 끝나는 시점 또는 추가 압수수색영장의 집행 종료 시점에 제3의 기관에 무관정보만을 이전하도록 할 경우, 전체 이미지파일을 수사기관이 보유하는 것을 막을 수 없기 때문이다. 전체 이미지파일을 수사기관이 아닌 제3의 기관이 보관하면서 선별작업을 하는 검찰수사관들에게 접근권한만을 일시적으로 부여하는 방식으로 운영하되, 선별작업이 끝나면 검찰수사관은 유관정보만을 보관하고 무관정보는 폐기해야 한다. 전체 이미지파일 또는 일부 무관정보를 계속 보관할 필요가 인정되어 압수수색영장이 발부된 경우라도 이 부분은 제3의 기관이 보관한다.

제3의 기관이 보관하는 정보를 수사기관이 사용할 필요가 있는 경우 법원의 허가를 받아 해당 목적으로만 사용하도록 하여야 한다. 수사기관이 무관정보의 압수가 필요한 사유로 압수수색영장에 기재했던 내용은 법원이 허가 여부를 결정할 때 주요 자료가 될 수 있을 것이다. 필요성이 소명된 경우 해당 무관정보에 대한 접근권한을 수사기관에 일시적으로 부여함으로써 해당 전자정보를 사용할 수 있도록 하여야 한다. 압수의 필요성이 소멸하는 경우 전체 이미지파일이나 무관정보를 보관하고 있는 제3의 기관이 폐기하고, 수사기관은 수사기관이 보관하고 있는 유관정보의 범위에서 압수의 필요성이 소멸될 경우 이를 폐기해야 한다. 판결이 확정된 이후 전자정보를 보관할 필요가 있는 예외적인 경우 유관정보와 무관정보를 불문하고 모든 전자정보를 제3의 기관이 보관한다.

보관장소는 한 군데로 하되, 접근권한만을 제3의 기관으로 이전하거나 수사기관에도 복수 부여하는 등의 방식으로 운영하는 것이 바람직하다. 전자정보의 복제본을 만들어 이전하는 등의 방식은 전자정보의 유출이나 유용의 위험성이 커질 수 있으므로, 타당하지 않다.

나. 기대 효과

전자정보의 보관을 제3의 기관이 하도록 함으로써, 수사와 압수 집행의 주체와 전자정보 보관·폐기 주체가 구별되는 효과가 발생한다. 수사 및 압수 집행의 주체는 수사기관, 전자정보 보관·폐기의 주체는 제3의 기관이 되도록 함으로써 수사기관이 압수한 무관정보를 별건 수사에 활용할 가능성을 차단할 수 있다. 나아가 압수가 압수수색영장의 기재에 따라 집행되는지, 무관정보가 별건 수사 등에 활용되지 않는지, 압수의 필요성이 소멸된 후에도 폐기하지 않고 계속 보관하는 것이 아닌지에 대한 우려를 불식시킬 수 있고, 압수의 필요성이 소멸된 전자정보의 폐기를 확실히 할 수 있다.

4. 법률 개정 필요

현재로서는 제3의 기관이 전자정보를 보관하게 할 근거가 없으므로, 법률에 근거를 만들 필요가 있다. 나아가 이 방안과 병행하여, 제3의 기관이 보관하는 전자정보에 대한 정기적 감사, 보관 중인 전자정보의 열람·사용 내역, 폐기한 전자정보를 공개하도록 하는 근거규정을 신설하는 것에 대해서도 검토할 필요가 있다.

Ⅴ. 나가며

형사소송법은 정보저장매체에 저장된 전자정보가 압수의 목적물인 경우 선별압수를 원칙으로 규정하고 있다. 이에 따라 전자정보를 현장 선별압수하는 것이 가능하다면 좋을 것이나, 전자정보의 특성, 기술의 발전 등으로 인하여 선별압수가 어려운 경우가 많다. 이로 인하여 특히 휴대폰의 경우 현장에서 전체 이미지파일이 반출되는 경우가 많고, 이후 유관정보를 선별하는 작업을 거친 후에도 공판절차에서 동일성·무결성 입증을 위해 필요할 가능성 등 유관정보 이상의 전자정보를 보관할 필요성이 있음으로 인하여, 범죄혐의사실과 관련성이 인정되는 범위를 넘어서는 전자정보가 수사기관에 보관되어 왔다.

현재의 실무는 압수수색영장의 발부시 법관은 유관정보의 압수만을 허가하지만, 실질적으로는 유관정보 이상의 전자정보를 수사기관이 취득하고, 이중 일부 또는 전부를 계속 보관하는 방식으로 운영되어 괴리가 존재한다. 이에 대하여 유관정보 외에 동일성·무결성 입증 등을 위해 무관정보를 보관할 필요성이 있다면, 압수수색영장 청구시 또는 압수수색영장 집행 중 추가 영장을 청구함으로써 수사기관이 해당 사건과 관련하여 어떠한 내용의 전자정보를 어떠한 범위에서 보관하고 있는지를 명확히 하는 것이 필요하다. 나아가 수사기관이 무관정보를 별건 수사에 활용할 수 있다는 우려를 차단하고, 필요성이 소멸한 전자정보의 폐기를 담보하기 위하여, 현재와 같이 수사기관이 아닌 제3의 기관이 전자정보를 보관하게 할 필요가 있다. 이를 통하여 실체적 진실 발견과 법치주의, 적법절차 준수라는 어렵지만 중요한 가치를 좀 더 잘 지켜나갈 수 있을 것이다.

[별지1] [별지 제16호 서식] 전자정보 삭제 · 폐기 또는 반환 확인서

전자정보 삭제·폐기 또는 반환 확인서

○○검찰청 0000형제 호 사건의 압수·수색·검증 과정에서 확보한 전자정보 중 압수한 전자정보의 목록에 포함되지 아니한 전자정보를 아래와 같이 삭제·폐기하거나 반환하였음을 확인함

0000. 0. 0.

○○검찰청 검사 (인)

■ 대상 전자정보

사건번호	형제 호	지원번호	지원 호
주임검사	검사 ○○○	압수일시	0000. 0. 0.
압수장소			
압수된 전자정보	*매체 단위로 특정하되 다수인 경우 별지 사용, 전자정보 상세목록 활용 가능*		

■ 삭제·폐기 또는 반환 대상 확인 *대상에 「」 표시하거나 「■」로 변경*

(삭제·폐기) □ 수사기관의 정보저장매체에 저장되어 반출된 전자정보, □ 탐색·복제·출력 과정에서 부수적으로 남겨진 전자정보

(매체반환) □ 반출된 정보저장매체 원본 내 전자정보, □ 피압수자의 정보저장매체등에 저장되어 반출된 전자정보

□ 삭제·폐기 확인 *삭제·폐기인 경우 앞 기호를 「■」로 변경*

전자정보	*이미지파일로 특정하되 다수인 경우 별지 사용, 전자정보 상세목록 활용 가능*
일시	0000. 0. 0. 00:00경
장소	
삭제·폐기 방법	

디지털포렌식 수사관 ○○○은 주임검사의 지휘에 따라 정보저장매체에 저장되어 있던 삭제·폐기 대상 전자정보를 위와 같이 삭제·폐기하였음

0000. 0. 0.

확인자 : 디지털포렌식 수사관 ○○○

□ 반환 확인 *반환인 경우 앞 기호를 「■」로 변경*

전자정보(매체)	*매체 단위로 특정하되 다수인 경우 별지 사용, 압수목록 활용 가능*
일시	0000. 0. 0. 00:00경
장소	
수령자	(성명) (연락처)

검찰주사(보) ○○○은 주임검사의 지휘에 따라 반환 대상 전자정보가 저장되어 있는 정보저장매체등 원본/복제본을 반환하는 방식으로 위와 같이 반환하였음

0000. 0. 0.

확인자 : 검찰주사(보) ○○○

[별지2] 압수 대상 및 방법의 제한 (일반용)

압수 대상 및 방법의 제한

1. 문서에 대한 압수

가. 해당 문서가 몰수 대상물인 경우, 그 원본을 압수함.

나. 해당 문서가 증거물인 경우, 피압수자 또는 참여인[1](이하 '피압수자 등'이라 한다)의 확인 아래 사본하는 방법으로 압수함 (다만, 사본 작성이 불가능하거나 협조를 얻을 수 없는 경우 또는 문서의 형상, 재질 등에 증거가치가 있어 원본의 압수가 필요한 경우에는 원본을 압수할 수 있음).

다. 원본을 압수하였더라도 원본의 압수를 계속할 필요가 없는 경우에는 사본 후 즉시 반환하여야 함.

2. 컴퓨터용 디스크 등 정보저장매체에 저장된 전자정보에 대한 압수·수색·검증

가. 전자정보의 수색·검증

수색·검증만으로 수사의 목적을 달성할 수 있는 경우, 압수 없이 수색·검증만 함.

나. 전자정보의 압수

(1) **원칙** : 저장매체의 소재지에서 수색·검증 후 **혐의사실과 관련된 전자정보만을 범위를 정하여 문서로 출력하거나 수시기관이 휴대한 저장매체에 복제하는 방법으로 압수할 수 있음.**

(2) **저장매체 자체를 반출하거나 하드카피·이미징 등 형태로 반출할 수 있는 경우**

(가) 저장매체 소재지에서 하드카피·이미징 등 형태(이하 "복제본"이라 함)로 반출하는 경우

- 혐의사실과 관련된 전자정보의 범위를 정하여 출력·복제한 위 (1)항 기재의 원칙적 압수 방법이 불가능하거나 압수 목적을 달성하기에 현저히 곤란한 경우[2]에 한하여, 저장매체에 들어 있는 전자 파일 정부를 하드카피·이미징하여 그 복제본을 외부로 반출할 수 있음.

(나) 저장매체의 원본 반출이 허용되는 경우

1) 위 (가)항에 따라 집행현장에서 저장매체의 복제본 획득이 불가능하거나 현저히 곤란할 때[3]에 한하여, 피압수자 등의 참여 하에 저장매체 원본을 봉인하여 저장매체의 소재지 이외의 장소로 반출할 수 있음.

2) 위 1)항에 따라 저장매체 원본을 반출한 때에는 피압수자 등의 참여권을 보장한 가운데 원본을 개봉하여 복제본을 획득할 수 있고, 그 경우 원본은 지체 없이 반환하되, 특별한 사정이 없는 한 원본 반출일로부터 10일을 도과하여서는 아니됨.

(다) 위 (가), (나)항에 의한 저장매체 원본 또는 복제본에 대하여는, 혐의사실과 관련된 전자정보만을 출력 또는 복제하여야 하고, 전자정보의 복구나 분석을 하는 경우 신뢰성과 전문성을 담보할 수 있는 방법에 의하여야 함.

(3)전자정보 압수시 주의사항

(가) 위 (1), (2)항에 따라 혐의사실과 관련된 전자정보의 탐색·복제·출력이 완료된 후에는 지체 없이, 피압수자 등에게 **① 압수 대상 전자정보의 상세목록을 교부하여야 하고, ② 그 목록에서 제외된 전자정보는 삭제·폐기 또는 반환하고 그 취지를 통지하여야 함**[위 상세목록에 삭제·폐기하였다는 취지를 명시함으로써 통지에 갈음할 수 있음].

(나) 봉인 및 개봉은 물리적인 방법 또는 수사기관과 피압수자 등 쌍방이 암호를 설정하는 방법 등에 의할 수 있고, 복제본을 획득하거나 개별 전자정보를 복제할 때에는 해시 함수값의 확인이나 압수·수색과정의 촬영 등 원본과의 동일성을 확인할 수 있는 방법을 취하여야 함.

(다) **압수·수색의 전체 과정(복제본의 획득, 저장매체 또는 복제본에 대한 탐색·복제·출력 과정 포함)에 걸쳐 피압수자 등의 참여권이 보장되어야 하며**, 참여를 거부하는 경우에는 신뢰성과 전문성을 담보할 수 있는 상당한 방법으로 압수·수색이 이루어져야 함.

---

1) **피압수자** – 피의자나 변호인, 소유자, 소지자 // **참여인** – 형사소송법 제123조에 정한 참여인
2) ① 피압수자 등이 협조하지 않거나, 협조를 기대할 수 없는 경우, ② 혐의사실과 관련될 개연성이 있는 전자정보가 삭제·폐기된 정황이 발견되는 경우, ③ 출력·복제의 의한 집행이 피압수자 등이 영업활동이나 사생활의 평온을 침해하는 경우, ④ 그 밖에 위 각 호에 준하는 경우를 말한다.
3) ① 집행현장에서의 하드카피·이미징이 물리적·기술적으로 불가능하거나 극히 곤란한 경우, ② 하드카피·이미징에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 현저히 침해하는 경우, ③ 그 밖에 위 각 호에 준하는 경우를 말한다.

[별지3] “계속 압수할 물건” 관련 일부 기각 기재례

“계속 압수할 물건” 관련 일부 기각

- 휴대전화에 저장된 범죄혐의 관련 전자정보로 계속 압수할 물건을 제한함
- 위 휴대전화에서 해당 전자정보를 복제·출력하여 압수한 후, 휴대전화는 피의자에게 반환하여야 함
- 압수·수색의 전체 과정(정보저장매체 또는 그 복제본의 탐색·출력·복제 포함)에 걸쳐 피압수자의 참여권을 보장할 것
- 전자정보의 탐색·복제·출력 완료 후 지체 없이 압수대상 전자정보의 상세목록을 교부할 것

토론문1

이범준 / 뉴스타파 객원기자

저는 두 발제자께서 발제문에 인용해 주신 2021년 경향신문 기획 기사를 취재·작성하였습니다. 이 기획 기사에서 전자정보 압수·수색 여러 문제를 다뤘는데, 디넷 존재를 밝혀낸 것이 다소 주목받았습니다. 그러나 이후 디넷에 대해 법원도 국회도 별달리 견제하지 못했습니다. 오히려 위헌적인 디넷 운용을 입법화하는 법안 발의가 나와, 이를 비판한 적이 있습니다. 이러한 문제를 다만 위임입법 한계로 파악했다는 것이 놀라웠습니다. 저는 오늘 이황희 교수 말씀대로 디넷의 근거가 검찰 예규에 있으나, 형사소송법에 있으나 위헌이라는 점은 달라지지 않는다고 생각합니다.

그러다 지난해 제가 함께 일하고 있는 뉴스타파, 저의 친정인 경향신문 등 언론사에 대한 압수·수색이 시작되면서 다시 이 문제가 논란이 됐습니다. 2021년 기획 기사 취재 당시 검찰의 디지털 정보 압수·수색이 어떠한 것인지 조금 알게 되었는데, 이번에 가까이서 지켜보니 상상을 뛰어넘는 고통과 두려움을 주는 것이었습니다. 그나마 말 많은 기자들이라고 봐준 것인데도 그 정도였다고 짐작하고 있습니다. 얘기를 들어보면, 위법한 압수·수색에 대한 분노, 이를 거부하지 못했다는 자책, 검찰에 내 모든 정보가 있다는 두려움이 차례로 찾아오는 것 같았습니다.

저는 검찰의 전자정보 압수·수색을 취재해 온 기자로서, 동료 언론인의 피압수·수색을 간접 경험한 시민으로서 두 발제자께 세 가지를 여쭈어보려고 합니다.

1. 디바이스 압수를 쉽게 허용하는 법원의 영장 관행이, 검찰의 별건 압수와 불법 저장, 이에 따른 별건 수사로 이어지는 계기가 되는 것은 아닌지.

법원 압수·수색 영장이 정한 원칙은 혐의사실 관련 정보 출력 또는 복사이고, 예외가 저장매체 반출과 이미징입니다. 하지만 검찰은 원칙과 예외를 뒤집어 놓았습니다. 가령 피압수·수색자 스스로 휴대전화 비밀번호를 해제한 사례에서도 이런저런 이유를 들어 디바이스를 반출하고 이미징하고 있습니다. 이렇게 반출된 디바이스를 수사관이 며칠 동안 검색해 수사와 무관한 정보까지 찾아내고, 피압수자를 설득하고 압박해 임의 제출 형태로 확보하고 있습니다.

이렇게 검찰이 다바이스를 무차별 압수하지만, 디바이스 압수가 위법하다고 준항고라도 해서 받아들여진 사례가 있을지 의문이 듭니다. 아마도 없을 것입니다. 그렇다면 이유는 법원 영장이 애초 예외를 너무나 넓게 허용한 탓은 아닌지 의심이 듭니다. 영장에 붙어 있는 '압수 대상 및 방법의 제한(권경선, 전자정보의 압수 및 보관·폐기에 관한 개선방안, 2024, 별지2 참조)'을 보면, 검찰의 자의적인 판단으로 예외로 넘어갈 수 있다는 걸 알 수 있습니다. 이 때문에 예외적 반출을 확인한 대법원 판결(2011모1839)도 별다른 의미가 없는 것 아닌지 의문이 듭니다.

2. 위법적인 무관정보 수집·보관의 출발점인 저장장치 비밀번호 취득용 압수·수색 영장 발부에 신중해야 하는 것 아닌지.

두 발제자께서 지적하신 무관정보 수집·보관의 시작은 디바이스 잠금장치 해제입니다. 그런데 잠금장치가 해제된 전자정보는 그렇지 않은 전자정보와 성격이 다릅니다. 그래서"'암호 해제된 전자정보'는 이미 압수된 '파일 자체'와 별개의 것으로 위법하게 수집한 접근권한정보 등을 기초로 새롭게 획득한 2차적 증거에 해당하는 것이므로, 암호 해제되기 전의 파일을 적법하게 압수하였다는 사정은 '암호 해제된 전자정보'의 증거능력을 판단함에 유의미한 사항은 아니다(조성훈, 역외 전자정보 압수·수색에 관한 연구, 2020, 164쪽)"라고 합니다.

이와 관련해 검찰의 영장 청구서에서 빠지지 않는 압수·수색 항목이 '위 각 항의 자료의 소재를 파악하거나 증거를 인멸한 정황을 확인할 수 있는 폐쇄회로 촬영물 및 관련 자료'입니다. 이를 근거로 수사기관은 아파트 엘리베이터 폐쇄회로 텔레비전 화면, 지하철역과 버스정류장에서 집까지 폐쇄회로 텔레비전 화면 등을 압수합니다. 그리고 이들 화면에서 휴대전화 비밀번호 해제 모습이 많이 포착된다고 합니다. 애초 손바닥보다 작은 디바이스 인멸 과정을 폐쇄회로 텔레비전 화면으로 확인할 수 있는지 의문이 듭니다. 이를 비롯해 여러 위법적인 디바이스 잠금장치 해제를 통제해야 하는 것 아닌지 궁금합니다.

3. 앞으로 기소청·공소청을 신설하고 검찰의 수사 기능을 완전히 없앨 경우, 전자정보 포렌식 주체를 어디로 해야 하는지.

두 발제자께서 모두 전자정보 포렌식이나 이미징 파일 보관을 수사기관이 아닌 제삼 기관이 맡아야 한다고 지적했습니다. 이와 관련해 국회에서는 검찰의 수사 기능을 완전히 없애는 형사소송법 등 개정을 추진하고 있습니다. 이렇게 되면 법무부의 외청인 검찰청은 수사는 하지 않고, 공소제기와 유지를 담당할 것으로 예상됩니다. 이때 포렌식과 전자정보 보관을 기소청·공소청이 해도 되는지, 아니면 다른 기관이 해야 하는지 궁금합니다.

토론문2

이황희 / 성균관대 법학전문대학원 교수

들어가며

‘대검찰청 전국디지털수사망’(D-NET, 이하 ‘디넷’)과 관련한 문제들을 논의하는 이번 토론회에서 토론자로 참여하게 되어 뜻 깊게 생각합니다. 저는 헌법을 공부하는 사람으로서, 근래 드러난 검찰의 디넷 활용 방식이 갖는 문제점을 헌법적 관점에서 말씀드리고자 합니다. 간략히 말씀드리면, 디넷의 문제는 법치주의와 민주주의의 각 측면에서 모두 위헌적인 피해를 초래한다는 것입니다. 이하에서는 편의상 경의를 생략합니다.

법치주의: 자유 보장의 측면

먼저 법치주의의 측면이다. 권리보장과 질서유지를 수행하기 위하여 포괄적인 공권력을 독점하게 된 국가권력은 개인이 넘볼 수 없는 강한 힘을 갖게 되었다. 그러나 이는 개인과 국가권력 간의 지위를 불균형하게 만들었고, 이로 인해 개인의 자유는 역으로 국가권력으로부터 침해될 수 있는 상시적인 위험 속에 놓이게 되었다. 이러한 힘의 격차를 경계해 온 근대 헌법이 따라서 공권력으로부터 개인의 권리를 보호하는 데 큰 관심을 가지게 된 것은 자명한 귀결이다.

헌법의 그 같은 관심은 특히 형사절차에 대한 규율에서 각별하게 나타난다. 형사절차는 공권력에 의한 개인의 권리 침해 위험이 구조적으로 내재되어 있는 대표적인 국가작용 영역이기 때문이다. 우리 헌법에 존재하는 사법절차적인 조항들이 기본적으로 (민사절차가 아닌) 형사절차에 관한 것(제12조, 제13조, 제27조 등)인 이유가 바로 여기에 있다. 이는 형사절차에 내재한 구조적 불균형 문제에 대한 우리 헌법의 적극적인 경계심을 잘 보여준다.

영장주의, 적법절차, 변호인의 조력을 받을 권리, 진술거부권 등의 헌법적 내용들은 이러한 불균형을 보완하기 위한 제도적 성취들이다.

특히 이러한 불균형을 보완하기 위한 대표적인 장치로, 법률유보가 있다. 개인은 자유의 주체이고, 국가는 공권력의 주체인데, 후자는 전자에 큰 위협이 되므로 양자의 지위는 근대 헌법 속에서 대조적으로 설정되어 왔다. 즉 헌법은, '자유의 주체'에게는 원칙적으로 모든 행위를 허용하되, 예외적으로 공익을 위한 제약 가능성을 부분적으로 인정하고 있을 뿐인 반면, '공권력의 주체'에게는 원칙적으로 자유에 개입하는 모든 행위를 금지하되, 예외적으로 공익을 위한 개입 가능성을 부분적으로 인정하고 있을 뿐이다. 따라서 공권력에 의한 자유의 제약 가능성은 입법자가 공익을 위한 개입이라고 예외적으로 인정한 것들에만 한정된다(법률유보 원칙). 이러한 대조적인 지위가 명확히 준수되지 않으면, 개인의 자유는 국가권력 앞에서 그야말로 바람 앞의 등불에 지나지 않는다.

검찰은 법정에서 디지털 증거의 무결성을 소명하기 위하여 스마트폰의 전체 추출정보를 디넷에 보관해 왔고, 해당 수사에 기초한 재판이 종료 후에도 여러 이유에서 상당기간 폐기하지 않아 왔는데, 이는 기본적으로 헌법이 위와 같이 구상해 온 '대조적인 지위 구분'과 충돌한다. 영장주의 위반 문제도 있겠으나, 무엇보다도 공권력의 주체에게 설정된 근본적인 제약, 즉 '개인의 자유에 개입하기 위해서는 법률이 공익을 위해 허용한 것만을 행할 수 있다는 제약'을 무시하고 있다는 측면을 지적하지 않을 수 없다. 검찰의 관행은 「디지털 증거의 수집·분석 및 관리 규정」이라는 행정규칙에 근거한 것일뿐, 명확한 법률적 근거는 존재하지 않기 때문이다. 이러한 법률적 근거의 부재는, 2021년 디넷에 관한 언론 기사가 보도된 이후 2021년 4월 전주혜 의원이 대표발의한 형사소송법 일부개정안의 제안이유에서도 표현되었다.[125]

만 아니라, 디넷의 문제는 사법(대법원 판례)의 취지를 존중하지 않는다는 점에서, 헌법상 권력분립 및 견제와 균형의 원리에도 충실하지 않다.

민주주의: 공적 참여의 측면

다음으로 민주주의의 측면이다. 먼저, 개인적 자유로 표상되는 사적 자율성이 보장되지 않을 때, 공적 참여로 표상되는 공적 자율성 역시 온전하지 않다. 이는 두 자율성이 동등하게 근원적이며 상호 참조적인 관계에 있다는 하버마스(『사실성과 타당성』) 등의 유명한 주장이다.

---

[125] 위 형사소송법 일부개정법률안의 <제안이유 및 주요내용> 중 일부는 다음과 같다: "검찰은 2012년 4월 전국디지털수사망(이하 "D-NET"이라 한다)을 구축한 이래 피의자나 참고인 등으로부터 압수하거나 임의제출받은 정보저장매체등에서 복제한 전자정보 데이터 14만 1,739건을 저장했고, 이 중 35.2%인 4만 9,942건은 2021년 2월 기준 여전히 서버에 저장되어 있는 상황으로, 검찰이 압수한 전자정보를 D-NET에 저장하는 근거는 대검찰청 예규인 「디지털 증거의 수집·분석 및 관리 규정」뿐이고, 이를 직접적으로 통제하는 법률규정은 존재하지 않는 상황임."

다음으로, 디넷이 초래하는 바와 같은 국가에 의한 개인정보의 과잉취득은 국가와 개인 간 불균형한 관계를 더욱 악화시키는 결과를 가져온다. 그리고 이러한 결과는 시민의 공적 참여 가능성을 제약하는 요인이 될 수 있다. 일찍이 이 문제를 인식한 독일 연방헌법재판소는 '정보에 관한 자기결정권'(Recht auf informationelle Selbstbestimmung)을 인정한 유명한 판례에서 이 문제를 다음과 같이 해명하였다.

> *사회적 환경의 특정한 영역에서 자신에 관한 어떤 정보가 알려져 있는지 충분히 파악할 수 없는 사람, 잠재적인 의사소통 상대방의 지식을 일정 부분 평가할 수 없는 사람은 자기결정을 통해 계획하거나 결정할 자유가 현저하게 제한될 수 있다. … 만약 일탈적인 행동이 언제든 기록되고 정보로서 영구히 저장, 사용 또는 전수될 수 있음을 우려하는 사람은 그러한 행동을 통해 눈에 띄지 않으려고 노력할 것이다. 예컨대, 집회나 주민발안에 참여하는 것이 당국에 의해 등록되고 이로 인해 위험에 처할 수 있다고 예상하는 사람은 집회·결사의 자유 행사를 자제할 가능성이 높다. 이는 자기결정이 시민의 행위능력과 참여능력에 기초한 자유롭고 민주적인 공동체의 본질적인 기능적 조건이기 때문에, 개인의 개성발현 기회뿐만 아니라 공익에도 해를 끼칠 것이다.*[126]

오늘날 개인의 핸드폰은 일상적 삶을 포괄적으로 기록하게 되므로, 자신이 기억하지 못하는 많은 내용들까지 담겨 있다. 이러한 정보가 국가의 수중에 존재한다는 것을, 혹은 한때라도 존재했다는 것을 의식하는 사람은 그로 인해 자신이 언제든 위험에 처할 수 있음을 우려하게 되므로, 국가권력에 대한 비판적 목소리를 내거나 그러한 활동을 펼치는 데 주저할 가능성이 있다. 이러한 가능성은, 특히 정부와 대립하는 야당 정치인이나 비판적 언론인, 시민운동가 등에게 더 심각하게 작동할 수 있다. 이는 시민들의 자발적 참여에 기초한 민주주의라는 헌법의 기획에 유해한 상황을 초래한다.

마치며

디넷 관행은 이처럼 여러 측면에서 위헌적인 피해를 산출한다. 이는, 단지 표면적으로 헌법의 규정에 저촉된다는 수준이 아니라, 근대 헌법의 중심적 기획을 훼손한다는 측면에서 그 위헌성이 더욱 심층적이다. 수사와 재판에서 디지털 증거의 무결성을 소명하는 일은 중요하지만, 이것은 헌법이 설정한 제약 속에서 이루어져야 한다. 이 문제에 관한 해법이 조속히 모색될 수 있기를 기대한다.

[126] BVerfGE 65, 1, 43(밑줄은 필자에 의함).

토론문3

김면기 / 경찰대학 법학과 교수

오병두 교수님과 권경선 판사님의 발제문 잘 들었습니다. 최근 들어 치열하게 논의되고 있는 수사기관 전자정보 보관의 문제점을 명확히 분석하고, 합리적인 대응방안을 제시하신 것을 보입니다. 두 분의 분석과 견해에 적극 동의하며, 가장 핵심적인 쟁점으로 보이는 '디지털 증거 무결성·동일성 입증을 위한 무관정보(이미지 파일)의 보관' 문제에 대하여 제 의견을 가미하는 형태로 토론에 갈음하고자 합니다.

무관정보 보관과 관련하여 수사기관의 입장과 법원(판례)의 태도가 충돌하는 것으로 보입니다. 수사기관에서는 디지털 증거의 동일성·무결성을 입증하기 위해서는 전체 이미지 파일을 보관할 필요성이 높다고 주장합니다. 2010년대 접어들면서 법원이 위법수집증거배제법칙 등을 통해 여러모로 엄격히 증거능력을 심사하고 있기 때문에, 수사기관의 입장이 일견 이해가 갑니다. 반면 판례는 전자정보 압수과정에서 개인의 내밀한 정보가 포함될 우려가 높으므로, 관련성 있는 증거를 찾기 위한 선별·탐색이 종료된 후 무관정보는 폐기될 것을 요구합니다. 최근 대법원은 폐기되지 않고 남아있는 무관정보는 설사 수사기관이 영장을 발부받아 압수하였더라도 증거로 사용할 수 없다고 판시한 바 있습니다.[127]

디지털 증거의 무결성·동일성 입증은 상당히 복잡한 문제입니다. 단지 형사법(증거법)적인 문제를 넘어 첨단 기술에 대한 이해도 수반되어야 하기 때문입니다. 기술은 끊임없이 발전하고 진화하기 때문에 섣불리 판단을 하기도 쉽지 않습니다. 수사기관의 입장은 나름 설득력이 있지만, 판례와의 괴리를 좁히기는 쉽지 않아 보입니다. 그렇다고 섣불리 답을 내리려 할 경우, 각각의 입장만 강변하는 반복이 이어질 것으로 보입니다.

따라서 논의의 쟁점을 보다 좁힐 필요가 있다고 봅니다.

[127] 대법원 2022. 1. 24. 자 2021모1586 결정; 대법원 2023. 5. 1. 선고 2018도19782 판결

순수하게 기술적인 측면만 고려하면, '완벽한 입증'을 위해서는 이미지 파일을 보관하는 것이 필요합니다. 수사기관은 선별·탐색을 거쳐 최종적으로 관련성있는 증거만을 압수합니다. 그런데 전자정보는 그 특성상 위조·변조가 용이하기 때문에, 수사기관이 보관·제출하는 디지털 증거가 과연 압수할 당시의 그것과 동일한가에 대해 의문이 생길 수 있습니다. 만약 이미지 파일이 남아있지 않은 경우, 동일성·무결성 입증을 위해 대조할 대상 자체이 존재하지 않습니다. 수사기관은 증거의 동일성·무결성이 침해받는 일이 없도록 이미지 파일을 보관하려는 것으로 보입니다.

형사절차에서 '완벽한 입증'은 중요합니다. 그러나 문제는 완벽한 입증이 결코 '공짜'가 아니라는 것입니다. 스마트폰 속에 있는 특정 디지털 증거에 대한 완벽한 동일성·무결성 입증이라는 공익은, 대상자의 스마트폰 전체 이미지 파일이 (당사자가 알기 어려운) 상당한 기간 동안 수사기관에 보관된다는 '프라이버시 침해'에 기반해 있다는 점입니다. 결국은 두 가치에 대한 비교형량의 문제가 될 것입니다.

그렇다면 동일성·무결성 입증에 실패함으로서 훼손되는 정의 실현이라는 공익과 수사기관이 무관정보를 보관함으로서 침해되는 사익을 현실적·경험적으로 보다 세밀하게 분석해볼 필요가 있습니다.

현재 법원은 기술적으로 '완벽한 입증'만을 요구하고 있지 않습니다. 잘 알려져 있듯, 법원은 전자정보의 증거능력과 관련하여, "[전자정보]의 생성과 전달 및 보관 등의 절차에 관여한 사람의 증언이나 진술, 원본이나 사본 파일 생성 직후의 해쉬(Hash)값과의 비교, [전자정보]에 대한 검증·감정 결과 등 제반 사정을 종합하여 판단할 수 있다"고 판시한 바 있습니다.[128]

현재까지 이미지 파일이 존재하지 않기 때문에, 즉 기술적으로 완벽한 동일성 입증이 되지 않았기 때문에, 법원이 증거능력을 배제한 판례가 있는지 의문입니다. 법원이 이미 '완벽한' 입증을 기준으로 요구하지 않고 있기 때문에, '완벽한' 입증이 아니어도 수사기관이 동일성·무결성을 인정받는 것에는 큰 어려움이 없는 것으로 보입니다. 즉, 수사기관이 주장하는 '동일성·무결성 입증에 실패함으로서 훼손되는 정의 실현이라는 공익'은 경험적으로 크지 않습니다.

그렇다면, '수사기관이 무관정보를 보관함으로서 침해되는 사익'은 어느정도 일까요. 수사기관에서 내 스마트폰의 이미징 파일을 장기간 보관하는 것은 그 자체로 두렵습니다. 아마 가장 극단적인 형태의 프라이버시 침해라고 볼 수 있습니다. 2021년 경향신문 기사에 따르면,

> *검찰은 2012년 4월 D-NET 구축 이후 전자정보 이미징 데이터 14만1739건을 서버에 저장했고, 이 중 35.2%인 4만9942건은 지난 2월 기준으로 여전히 서버에 남아 있다. 이 가운데 스마트폰 데이터는 총 5만441건이 저장돼 1만4550건이 남아 있다.*

[128] 대법원 2015. 1. 22. 선고 2014도10978 전원합의체 판결 [내란음모·국가보안법위반(찬양·고무등)·내란선동] [공2015상,357]

고 합니다. 엄청난 숫자입니다. 그런데 이미 3년전의 통계수치입니다. 2024년 7월 현재는 과연 얼마나 더 많은 이미징 파일이 저장되어 있을까요.

완벽한 입증의 대가는 이처럼 혹독합니다.

그러나 앞서 언급했듯이 우리 형사사법시스템은 결코 수사기관에게 완벽한 입증을 요구한 적이 없습니다. 수사기관은 필요성을 자의적으로 해석·판단하여 과도한 전자정보를 보관하고 있습니다. 대검 예규에서는 법률적 근거도 없이 대법원 판례와도 어긋나게, 보관범위를 상당히 넓히고 있습니다. 공익은 불분명합니. 사익침해는 광범위합니다. 그리고 과거와 최근의 주요 사례에서 보듯, 그 저의는 의심받기에 충분합니다.

소위 '디지털수사망'이라는 D-NET은 저인망식 광범위한 위헌적 수사를 일컫는 '드래그넷(Dragnet)'이 더 어울립니다.[129] 변화가 필요합니다.

이상으로 금일의 토론을 마치겠습니다. 감사합니다.

[129] 드래그넷(Dragnet)은 기다란 어망을 바다 밑바닥 등에서 가로질러 끌고가는 낚시 기술에서 유래한 용어입니다. 범죄수사와 관련하여, 모든 사람을 대상으로 과도하게 유죄 증거를 찾기 위해 수색하는 행위에 비유됩니다. 미국에서는 1950년대 이후 이러한 '드래그넷'을 부당한 수색 및 압수 행위로 보아 위헌적인 수사로 평가하고 있습니다. https://en.wikipedia.org/wiki/Dragnet_(policing)

토론문4

이창민 / 민주사회를 위한 변호사모임 검·경개혁소위원장

이번 여름은 날씨만큼이나 검찰개혁 열기가 뜨겁습니다. 권위주의 검찰 정권이 들어선 지 채 2년밖에 지나지 않았지만, 시민들은 검찰 권한의 오남용을 지켜보면서 검찰개혁의 필요성에 대해 공감하고 있는 분위기입니다. 최근 검찰은 자체 디지털수사망(D-NET)에 범죄혐의와 관련이 없는 개인정보도 보관하고 있다는 사실이 언론을 통해 보도되면서 시민들의 검찰개혁에 대한 열망은 더 높아졌습니다. 그리고 오늘의 주제이기도 합니다.

이러한 검찰권 오남용에 대해 살펴보기 위하여, 우선 한국 검찰 제도의 내재적 문제점을 짚고 넘어갈 필요가 있습니다. 바로 비대한 검찰권에서부터 이러한 문제가 시작되기 때문입니다. 주지하다시피 한국 검찰의 권한은 너무나도 막강합니다. 정보의 수집·보관, 수사, 기소, 영장청구 등의 권한을 갖고 있습니다. 위 개개의 권한이 너무나도 강력한 권한인지라 국가 기관 간 힘의 균형 및 견제 차원에서 살펴보면, 한 기관이 위의 권한 모두를 갖고 있다는 사실 자체가 모순인 상황이라 할 수 있습니다.

그런데 한국의 검찰은 위 권한을 모두 갖고 있습니다. 쉽게 표현하자면 절대 권력과 유사하다고 할 수 있습니다. 그러니 일부 검사들이 때로는 집행 권력에 편승하여, 때로는 스스로가 집행 권력이 되어 국정을 쥐락펴락하는 사태까지 발생하는 것입니다. 여기에 더하여 그 많은 권한과 재량은 검찰 퇴직 후에도 '우리가 남이가'의 형태로 남아 '전관 비리'로 이어집니다. 고위직은 퇴직 후 2년간 수십억 원은 벌 수 있는 구조가 고착화 되었습니다.

오늘의 주제인 검찰의 정보수집 및 보관 역시 검찰의 막강한 권한 중 하나입니다. 그중 검찰이 수집한 정보를 저장해 두는 장소, 특히 디지털 정보를 보관하는 장소를 D-NET이라고 합니다. 발제자들이 지적한 바와 같이 D-NET의 문제점은 크게 세 가지로 요약할 수 있습니다. ① 혐의사실과 무관한 '무관정보'는 디지털포렌식을 통해 증거 선별절차가 끝나면 즉각 삭제되어야 함에도, D-NET에서 삭제·폐기되지 않고 보관되고 있으며, ② 혐의사실과 관련한 유관정보 역시 공판이 끝나 그 목적이 달성되면 삭제되어야 하는데, 삭제하지 않는 경우가 상당히 많으며, ③ 피압수자 입장에서는 선별절차 끝에 무관정보를 검찰이 삭제하였는지, 공판이 끝나 유관정보를 검찰이 삭제하였는지에 대해 사실상 알 수 없다는 것입니다.

이러한 D-NET의 문제점을 해결하기 위해서는 규범적인 접근과 제도적인 접근이 모두 필요합니다. 규범적으로 디지털 정보에 대한 압수 시 유관정보만을 수사기관이 압수하여야 한다는 원칙이 지켜져야 합니다. 실무상 기술적·시간적 한계가 있다는 이유로, 휴대전화 등 저장매체 자체를 압수장소나 피압수자로부터 반출하여 D-NET에 이미징 등의 형태로 정보를 저장하는, 지극히 예외적인 방식이 원칙인 것처럼 영장이 집행되면 안 됩니다. 즉 수사기관이 피압수자의 휴대전화를 통째로 가져가, 혐의사실과 무관한 정보까지 들여다보고, 이를 저장하게 하는 방법은 별건 수사 등은 차치하고라도 위법의 소지가 다분한 수사 방식에 해당합니다.

규범적인 측면에서, 발제자들의 지적과 같이 「형사소송법」을 위시하여 하위 규범들의 정리가 필요합니다. 특히 우리 「형사소송법」은 압수·수색에 관하여 법원이 주체가 되는 압수·수색을 제106조부터 제138조까지 규정하고 있는 한편, 수사기관의 압수·수색을 제216조부터 제220조까지 규정하면서, 수사기관의 압수·수색에 법원의 압수·수색 규정을 대부분 준용하도록 규정하고 있습니다. 이렇게 관련 규정이 준용의 형식으로 되어 있는 것도 문제지만, 압수수색 대상으로서 '정보'가 규정되어 있지 않은 것이 더 큰 문제입니다. 저장매체가 아닌 정보에 대한 압수수색 관련 법률 규정조차 부재한 것입니다. 수사 절차에 관한 통합적인 법률을 제정하면서 정보에 대한 압수수색 과정과 절차를 세밀히 규정할 필요가 있습니다.

다음으로 제도적으로는 발제자의 지적대로 수사의 주체, 압수·수색영장 집행의 주체, 압수물(정보) 보관의 주체, 압수물(정보) 분석의 주체가 모두 동일하여 선별압수의 원칙이 지켜지지 않고 있으며, 외부에서는 이를 알 수 없다는 문제가 있습니다. 나아가 검찰의 경우는 수사·영장 집행·압수된 정보보관·정보분석·기소·공소 유지의 주체가 모두 같아 혐의사실과 무관한 정보까지 보관할 유인이 크다는 문제가 있습니다.

D-NET 문제에 국한하여 보면, 수사 및 압수·수색 집행 주체와 디지털 정보보관의 주체를 달리할 필요가 있습니다. 즉, 독립된 디지털포렌식 기관이 설치되어야 합니다. 검찰을 비롯한 수사기관이 디지털 정보를 압수하면 독립된 디지털포렌식 기관이 이를 보관하고, 선별절차 시 디지털포렌식 기관이 압수된 정보에 대한 접근 권한을 해당 수사기관이나 수사관에게 부여하는 방식으로 운영되어야 합니다. 물론 디지털포렌식 기관은 선별절차 이후에는 혐의사실과 무관한 정보는 즉시 폐기하게 하여야 합니다. 이러한 제도적 장치가 갖추어 지면, 수사·영장 집행

기관과 정보 관리 기관이 분리되어 권한 집중도 해소될 수 있으며, 상호 견제 하에 보관된 정보가 투명하게 관리될 것입니다. D-NET 문제의 규범적·제도적 해결 방안을 요약하면 아래 표와 같습니다.

D-NET 문제의 규범적·제도적 해결 방안

- 수사 절차에 관한 통합적인 법률을 제정하면서, 정보에 대한 압수·수색 과정과 절차를 세밀히 규정할 필요가 있음
- 수사 및 압수·수색의 집행 주체와 디지털 정보보관의 주체를 달리해야 함. 즉, 독립된 디지털포렌식 기관이 설치되어야 함

규범적 통제의 경우 정보에 대한 압수·수색 절차를 세밀히 규정하고, 혹여 공백이 있으면 이를 판례의 법리로 메워 나가면 될 것입니다. 그런데 문제는 제도적 해결 방안입니다. 독립된 디지털포렌식 기관 설치로 D-NET의 문제는 해결할 수 있지만, 독립된 디지털포렌식 기관이 또 다른 권력 기관화될 우려가 있습니다. 이른바 정보 권력이 탄생할 수도 있습니다. 이는 독립된 디지털포렌식 기관의 통제 방법과도 연관이 있습니다.

마지막으로 발제자들에게 간단히 두 가지만 질의하고 토론문을 마칩니다. 첫째, 독립된 디지털포렌식 기관이 또 다른 권력 기관화될 우려가 있다고 보시는지, 만일 그렇다면, 해결 방안은 무엇인지 궁금합니다. 둘째, 정보에 대한 압수·수색 관련 법령이 정비되어, 수사기관이 휴대전화 등 정보 저장매체 자체를 반출하지 못하고, 검색어 입력 등의 방법으로 혐의사실과 관련된 정보만을 압수할 수 있다고 한다면, 실무에서 이러한 원칙이 얼마나 지켜질 수 있을지, 다른 해결 방법이 있는지 궁금합니다.

수사기관 전자정보 보관 문제점과 대응방안 모색을 위한 정책토론회

발행일 2024. 07. 02.
발행처 국회의원 박주민 · 참여연대 · 민주사회를 위한 변호사모임 사법센터
문 의 참여연대 사법감시센터
02-723-0666 jw@pspd.org

※ 본 자료는 참여연대 웹사이트에서 다시 볼 수 있습니다.