정보인권 연구소

창립토론회

<디지털 압수수색과 정보인권>

일시 : 2015년 9월 23일(수) 오후 4시-6시

장소 : 스페이스노아 커넥트홀

인사말

한국에 인터넷이 도입된 지 30년. 어느덧 정보통신 기기와 인터넷은 우리 삶의 일부분으로 자리 잡았습니다.

국가와 산업 중심의 정보화가 속에서 공공성과 정보인권 보호를 위한 사회운동도 자연스레 성장해왔습니다. 인터넷 실명제 위헌 결정, 개인정보보호위원회 설립 등 많은 성과도 있었습니다.

그러나 정보통신 기술의 급속한 발전과 이에 따른 사회 변화는 우리에게 여전히 많은 도전을 던지고 있습니다. 공공성과 인권, 그리고 민주적 거버넌스에 기반한 정보사회를 만들기 위한 심도 깊은 연구가 필요합니다. 또한, 긴급한 현안 대응에 비해, 정책 연구는 보다 긴 호흡을 가져갈 필요가 있습니다.

그래서 정보인권연구소가 출범합니다!

정보인권연구소는 현실 운동과의 긴장을 놓치지 않으면서도, 보다 장기적인 관점에서 사회의 변화를 분석하고 대안을 연구함으로써, 정보인권 운동에 자양분을 공급하고자 합니다.

정보인권연구소의 힘찬 출발에 함께 해 주세요.

정보인권연구소
이사장 이호중

행사일정

3:30 – 4:00 : **등록**

4:00 – 4:30 : **정보인권연구소 창립행사**

인사말 : 이호중 (정보인권연구소 이사)
축사 : 류은숙(인권연구소 '창' 연구활동가),
구본권(사람과디지털연구소 소장)
조영선(민주사회를위한변호사모임 사무총장)
이종회 (진보네트워크센터 대표)
설립 목적 및 주요 사업 소개
임원 소개

4:30 – 6:00 : **정보인권연구소 창립토론회**
<디지털 압수수색과 정보인권>

사회: 김기중(변호사, 정보인권연구소 이사)

주제발표: 이호중 (서강대 법학전문대학원, 정보인권연구소 이사장)

토론 :
한상훈 (교수, 연세대 법학전문대학원)
이광철 (변호사, 민주사회를위한변호사모임)
정진우 (전 노동당 부대표, 사이버사찰 피해당사자)
신훈민 (변호사, 진보네트워크센터)

※ 6시 창립행사 이후에 뒤풀이가 있습니다.

[창립토론회 발제문]

디지털 압수수색과 정보인권

이호중(서강대 법학전문대학원 교수, 정보인권연구소 이사장)

Ⅰ. 서론

우리나라에서 '정보인권'이라는 용어는 대략 2002년 교육행정정보시스템(NEIS)의 도입에 관한 논의를 계기로 하여 2003년경부터 본격적으로 사용되기 시작한 것으로 보인다.[1] 그로부터 10년 이상 경과한 오늘날 '정보인권'이라는 용어는 매우 보편화되어 있지만, 그 개념은 아직 명확하게 정의되어 있지 않은 상황이다. 대체로 정보인권이란, 인터넷 등 정보통신망과 IT 기술의 발전에 터잡아 정보통신기술시스템과 관련하여 발생하는 제반 인권문제를 아우르는 개념으로 사용되고 있다. "정보인권이란 의사소통에 필요한 정보에 손쉽게 접근하여 수집하고 이를 자유롭게 전파하고 활용할 수 있도록 하고, 나아가 자신에 관한 정보를 스스로 통제할 수 있도록 하는 기본적 인권을 총칭하는 개념"[2]이라 말하기도 하고, 국가인권위원회는 정보인권을 "정보통신기술에 의하여 디지털화된 정보가 수집·가공·유통·활용되는 과정과 그 결과로 얻어진 정보가치에 따라 인간의 존엄성이 훼손되지 않고 자유롭고 차별없이 이용할 수 있는 기본적 권리"[3]라고 정의하고 있다. 이러한 개념정의에는 사생활의 비밀과 자유, 정보통신의 비밀보장, 개인정보자기결정권 등의 헌법적 기본권이 포괄되어 있을 뿐만 아니라, 사이버상의 표현의 자유, 그리고 알권리 등 정보접근권과 더 나아가서 정보문화향유권까지 그 폭이 매우 넓다.

다소간의 개념적 불명확성에도 불구하고, 정보인권이라는 개념 하에서 다루고자 하는 문제는 정보통신기술의 발전을 기반으로 하여 디지털 정보가 생산·유통·수집되는 과정에서 야기되는 인권의 문제일 것이다. 이에 대한 접근에서는 기존의 인권 개념을 그대로 차용하는 것을 넘어설 것이 요구된다. 헌법재판소는 개인정보자기결정권이라는 개념을 프라이버시권에서 도출하고 있는데, 전통적인 프라이버시권이 개인의 사생활에 속하는 사항이 공개되지 않을 이익을 의미하는 것이었다면 개인정보자기결정권은 타인이 자신의 개인정보를 수집·이용·제공하는 경우 그 정보의 처리과정에 정보주체가 참여하고 통제할 수 있는 권리라는 개념으로 정립되었다. 더 나아가서 네트워크의 상호작용적 성격과 개인 이용자들의 정보활동의 자발성, 그리고 사회구조적 차원에서 개인과 기업, 국가 사이에 존재하는 권력 불균등의 문제를 지적하면서 정보인권의 영역에서 전통적인 프라이버시권은 수정이 불가피하다는 견해도 유력하게 제기되고 있다.[4]

정보인권의 문제지대를 크게 나누어 본다면, 아래의 세가지 차원의 서로 다른 결을 발견할 수 있다. 첫 번째 차원은 정보통신 네트워크의 공공성의 문제이다. 오늘날 정보통신망을

---

1) 오병일, "정보사회 세계정상회의를 계기로 본 정보인권", 문화과학 제35호, 2003년 가을.
2) 권건보, "정보인권의 증진과 국가인권위원회의 역할", 국가인권위원회/한국헌법학회 공동주최, 국가인권위 설립 10년 기념 공동심포지움, 2012.
3) 국가인권위원회, 정보인권보고서, 2013, 11면.
4) 우지숙, "정보통제권에서 식별되지 않을 권리로 - 네트워크 프라이버시의 새로운 개념화를 위한 연구", 언론과 사회 제13권 제4호, 2005 참조.

이용한 정보의 생산이나 유통은 개인의 인격적 삶의 형성과 뗄 수 없는 관계에 있는 만큼, 네트워크의 공공성의 문제는 네트워크 기반의 민주주의적 공공성의 문제로 제기될 수 있다. 두 번째 차원은 정보통신망을 매개로 하여 이루어지는 정보유통이 표현의 자유와 관련을 맺는 영역이다. 세 번째 차원은 정보통신망을 통해 생산·유통·수집되는 디지털정보에 대한 국가권력의 감시와 사찰의 문제이다. 이 세가지 차원은 각기 결이 다르고 각각 정보인권의 고유한 문제를 야기하고 있기는 하지만, 다른 한편으로 이 세가지 차원은 상호 영향을 주고받으면서 우리 사회의 정보인권의 실체를 형성하고 있다는 점을 인식하는 것도 매우 중요하다.

이 글에서 다루려고 하는 디지털 압수수색의 문제는 그 중에서 특히 세 번째 차원과 관련되어 있다. 압수수색은 국가 수사기관이 정보기관이 일정한 요건과 절차에 따라 개인의 디지털정보를 수집하는 문제를 다루는 것이기 때문에 그것은 일차적으로는 국가권력의 개입으로부터 개인 주체들의 정보프라이버시권의 보호의 문제로 귀착된다. 그렇지만 동시에 디지털 정보의 압수수색은 정보통신망에서 자유롭게 말하고 표현할 자유의 보장에도 상당한 정도로 영향을 미치게 된다는 점도 중요할 것이다.

Ⅱ. 디지털 압수수색 관련 형사소송법 개정 및 대법원 결정례에 대한 평가

1. 2011.7.18. 형사소송법 개정의 경과와 주요 내용

종래 형사소송법은 압수수색의 대상을 '물건'이라고만 규정하고 있었기 때문에 디지털증거의 압수·수색에 관해서는 컴퓨터에 저장된 파일(file) 자체가 압수수색의 대상이 될 수 있는가의 문제에서부터 디지털증거에 대한 압수수색의 방법과 절차, 이에 관한 법치주의적 통제의 문제 등에 대하여 많은 논란이 있어 왔다. 특히 논란이 되었던 쟁점은 압수의 대상이 컴퓨터하드디스크 등 저장매체인가 아니면 그 안에 저장되어 있는 파일인가의 문제, 그리고 압수수색의 방법과 관련하여 컴퓨터 하드디스크 등 저장매체 자체의 압수가 허용되는가, 하드디스크 카피(copy)나 이미징(Imaging)[5] 등을 압수라고 볼 수 있는가 하는 점이었다.

이론적인 논란에도 불구하고, 검찰 및 법원의 실무에서는 통상의 압수수색영장에 의하여 전자정보의 압수수색을 허용해 왔다. 영장기재의 전형적인 예를 들자면, 압수수색영장의 '압수할 물건'에는 [피의사실과 관련된 … 컴퓨터파일 및 데이터베이스 일체] 그리고 [위 자료를 보관 중인 컴퓨터, 노트북, 외장 하드디스크, 플래쉬메모리, CD … 기타 외부저장매체 및 그 출력물]이라고 기재하는 것이 일반적이다. 다만, 컴퓨터 하드디스크 등 저장매체 자체를 '통째로' 압수하는 것은 범죄사실과 무관한 정보까지 포괄적으로 압수하는 결과가 되어 영장주의 위반, 프라이버시에 대한 과도한 침해 등의 비판이 제기되고 있음을 고려하여, 법원은 최근 2-3년전부터 디지털정보의 압수방법에 대해 '하드디스크 카피·이미징 또는 문서출력후 출력물을 압수'하는 것을 원칙으로 하도록 영장에 명기하고, 컴퓨터 저장매체의 압수는 위와 같은 방법의 압수가 불가능한 경우에만 허용된다는 취지의 기재를 하는 경향을

5) '이미징(imaging)'이란 원본과 동일한 하드드라이브의 디지털 복제본을 만드는 것을 말한다. 저장매체에 저장된 모든 파일과 slack space, 마스터 파일 테이블, 메타 테이블을 포함하여 원본 드라이브 상의 모든 bit와 byte를 원래의 순서와 위치까지 그대로 복제하는 기법이다. 이숙연, 형사소송에서의 디지털증거의 취급과 증거능력, 고려대학교 법학박사학위논문, 2011,

보이고 있었다.

이런 법원의 영장실무관행이 디지털 정보에 관한 압수수색의 적법성에 관한 문제를 근본적으로 해결하는 데에는 한계가 있을 수밖에 없는 상황에서, 검찰은 검찰 나름대로 법원이 압수수색영장에 아무런 법적 근거도 없이 디지털 정보의 압수수색방법을 제한하려고 한다는 불만을 표출하고 있었다. 그렇기에 디지털 증거의 압수수색에 관한 법적 근거와 집행절차를 명확히 하는 형사소송법 개정이 필요하다는 점에는 어느 정도 공감대가 형성되고 있었다. 이런 상황에서 2009년부터 디지털증거의 압수수색에 관한 다양한 내용의 형사소송법 개정법률안들[6]이 국회에 제출된 바 있다. 국회에서는 '사법제도개혁특별위원회'의 논의를 거쳐 '위원회 대안'을 마련하였고 이렇게 마련된 형사소송법 개정안이 국회 본회의를 통과하여 2011년 7월 18일 공포되었으며 2012.1.1.부터 시행되고 있다. 주요 내용은 아래와 같다.

첫째, 개정 전에는 "필요한 때"라고 포괄적인 요건을 규정하였던 것을 법원의 압수수색에 관해서는 "필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한하여"라고 규정하고(제106조 제1항 및 제109조 제1항 개정), 수사기관의 압수수색에 관해서는 "범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한하여"라는 요건을 규정함으로써(제215조 제1항 및 제2항 개정) 압수수색의 대상에 관하여 '피고사건과의 관련성' 요건을 명시하였다.

둘째, 디지털증거의 압수수색에 관한 규정을 신설하였다(제106조 제3항 시설). 압수의 대상이 정보저장매체인 경우에는 원칙적으로 정보의 범위를 정하여 '출력' 또는 '복사'하여 제출받도록 규정하였으며, 그러한 압수방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에 예외적으로 정보저장매체를 압수할 수 있도록 규정하였다.

셋째, 디지털정보의 압수수색이 행해진 경우에는 「개인정보보호법」에 따라 정보주체에게 해당 사실을 알리도록 하는 규정을 신설하였다(제106조 제4항 신설).

넷째, 이메일(E-mail) 등 전기통신에 관한 압수수색의 경우에는 영장에 작성기간을 기재하도록 명시함으로써 이메일 압수수색의 남용을 방지하고자 하였다(제114조 제1항 개정).

2. 2011년 전교조사건의 대법원 결정

전국교직원노동조합의 시국선언 사건의 수사과정에서 검찰과 경찰이 전교조 본부 사무실을 압수수색하면서 데스크톱 컴퓨터 3대 및 서버 컴퓨터 10대를 압수하여 수사기관 사무실로 가져갔고, 그 곳에서 저장매체 내의 파일을 복사하는 방식으로 압수수색영장을 집행한 데 대하여, 피의자와 변호인들이 압수절차 및 방법의 위법을 주장하면서 법원에 준항고를 제기한 사건이 있었다.

대법원은 준항고기각결정[7]에 대한 재항고를 기각하면서 다음과 같이 판시하였다 : 「전자정보에 대한 압수·수색영장을 집행할 때에는 원칙적으로 영장 발부의 사유인 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 하고, 집행현장 사정상 위와 같은 방식에 의한 집행이 불가능

6) 이주영 의원 대표발의 형사소송법 일부개정법률안(2009.4.1. 발의, 의안번호 4366호) ; 이종걸 의원 대표발의 형사소송법 일부개정법률안(2009.5.13. 발의, 의안번호 4839호) ; 박영선 의원 대표발의 형사소송법 일부개정법률안(2009.6.23. 발의, 의안번호 5246호) ; 조영택 의원 대표발의 형사소송법 일부개정법률안(2009.12.7. 발의, 의안번호 6880호) ; 박영선 의원 대표발의 형사소송법 일부개정법률안(2010.4.8. 발의, 의안번호 8131호) 등이 대표적인 것들이다.

7) 서울중앙지방법원 2009.9.11. 2009보5 결정(압수·수색집행에 대한 준항고).

하거나 현저히 곤란한 부득이한 사정이 존재하더라도 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 반출하여 해당 파일을 압수·수색할 수 있도록 영장에 기재되어 있고 실제 그와 같은 사정이 발생한 때에 한하여 위 방법이 예외적으로 허용될 수 있을 뿐이다. 나아가 이처럼 저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄 혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색영장 집행의 일환에 포함된다고 보아야 한다. 따라서 그러한 경우 문서출력 또는 파일복사 대상 역시 혐의사실과 관련된 부분으로 한정되어야 하는 것은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의 원칙상 당연하다. 그러므로 수사기관 사무실 등으로 옮긴 저장매체에서 범죄 혐의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위는 특별한 사정이 없는 한 영장주의 등 원칙에 반하는 위법한 집행이다. 한편 검사나 사법경찰관이 압수·수색영장을 집행할 때에는 자물쇠를 열거나 개봉 기타 필요한 처분을 할 수 있지만 그와 아울러 압수물의 상실 또는 파손 등의 방지를 위하여 상당한 조치를 하여야 하므로(형사소송법 제219조, 제120조, 제131조 등), 혐의사실과 관련된 정보는 물론 그와 무관한 다양하고 방대한 내용의 사생활 정보가 들어 있는 저장매체에 대한 압수·수색영장을 집행할 때 영장이 명시적으로 규정한 위 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우에도, 전체 과정을 통하여 피압수·수색 당사자나 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다.」[8)]

2011.7.18. 형사소송법 개정 직전에 선고된 대법원 결정은 디지털증거의 압수수색 방법 및 절차의 적법성에 관련하여 몇가지 중요한 기준을 제시해 주었다. 첫째, 전자정보의 압수는 원칙적으로 혐의사실과 관련된 부분만을 출력물의 형태로 또는 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 한다. 둘째, 하드디스크 본체를 압수하거나 하드디스크이미징을 하는 등으로 전자정보를 수사기관 사무실 등 외부로 반출하여 압수수색하는 것은 위와 같은 집행이 불가능하거나 현저히 곤란한 사정이 있어야 하고 또한 그러한 집행이 가능하다는 점이 영장에 기재되어 있는 경우에 한해서만 허용된다. 셋째, 하드디스크 본체나 이미징한 것을 수사기관에 옮겨 놓고 그 안에 저장된 전자정보를 수색하고 문서로 출력하거나 파일을 저장하는 것도 압수수색 집행에 해당한다. 따라서 수사기관의 사무실에서의 문서출력이나 파일복사는 혐의사실과 관련된 부분으로 한정되어야 한다. 같은 이유로 절차상 그 전체 과정을 통하여 피압수·수색 당사자나 그 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태에서의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색의 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 그 집행절차가 적법한 것이 된다.

3. 형사소송법 개정의 의미와 한계

1) 컴퓨터 하드디스크 등 정보저장매체는 방대한 자료를 저장하고 있으며 범죄와는 무관한

8) 대법원 2011.5.26. 2009모1190 결정 (준항고기각결정에 대한 재항고).

정보가 혼재되어 있기 때문에, 정보저장매체의 압수는 정보주체의 프라이버시권 및 당사자의 영업의 자유에 대한 침해의 강도가 일반적인 압수수색에 비하여 훨씬 크다. 저장정보의 대량성을 고려하면 정보저장매체의 압수를 손쉽게 허용하는 것은 '일괄압수'로서 헌법과 형사소송법상 요구되는 특정성의 원칙, 강제처분 비례성원칙을 무력하게 만들어 버릴 위험이 매우 높다. 이와 같은 '포괄영장(general warrant)'을 금지해야 한다는 문제의식은 디지털정보의 압수대상성에 관한 긍정설과 부정설의 대립을 넘어서서 널리 공유되어 왔다. 2011년 형사소송법의 개정과 대법원 결정도 컴퓨터하드디스크 등 정보저장매체를 통째로 압수하는 것을 원칙적으로 금지하는데 초점이 맞춰져 있다.

개정된 형소법 제106조 제3항에 의하면, 디지털정보의 압수수색에서 원칙적인 방법은 수사기관이 저장매체에 기억된 정보 중 피의사실과 관련된 정보만을 선별하여 출력 또는 복제의 방법으로 압수하는 것이다. 저장매체의 압수는 그러한 방법이 "불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에" 예외적으로 허용된다. 대법원 판례에 의하면, 하드디스크 등 저장매체 자체를 압수하기 위해서는 위와 같은 사정이 실제로 존재해야 할 뿐만 아니라 저장매체 자체를(또는 하드카피나 이미징 등의 형태로) 압수할 수 있도록 영장에 기재되어 있어야 한다.[9)]

그러나 형사소송법 제106조는 여전히 압수의 대상을 '물건'으로 규정하고 있기 때문에 해석론상으로는 디지털정보 자체가 압수의 대상이 될 수 있는가에 관한 해묵은 논쟁은 2011년 형소법 개정 이후에도 여전히 해결되지 않은 채로 남아 있다.

개정된 형소법 제106조가 디지털정보 자체를 압수대상으로 입법화한 것이라는 평가[10)]도 있다. 이 견해는 특히 제106조 제3항이 정보저장매체에 기억된 정보의 범위를 정하여 출력 또는 목제하여 제출받도록 규정한 점에서 압수대상은 전자정보이며, 제4항에서 정보주체에게 통지하도록 규정한 것도 전자정보 자체를 압수의 대상으로 상정한 때문이라고 본다. 그러나 개정된 제106조의 조문으로 볼 때, 디지털정보 자체를 압수의 대상으로 인정한 것이라는 해석론은 설득력을 얻지 못하고 있다.[11)] 2011년 개정에서 '전자정보'를 명시적으로 압수의 대상으로 포함시키지 않았을 뿐만 아니라, 신설된 제106조 제3항에서 "압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체인 경우"라고 규정하여 유체물로서 정보저장매체의 압수를 상정하고 있기 때문이다. 다만, 그 압수방법을 '출력' 또는 '복제'로 제한하는 방식을 취하면서, 컴퓨터저장매체의 압수는 예외적으로만 가능하도록 규정하고 있을 뿐이다.

한편, 전교조 사건의 대법원 판례는 디지털정보가 압수수색의 대상이 되는가에 대하여 명확한 입장을 표명하진 않았지만, 판례의 전체적인 취지를 보면 디지털정보 자체를 압수의 대상으로 파악하는 태도가 읽혀진다. 대법원 결정이 "전자정보에 대한 압수·수색영장을 집행할 때에는"이라는 표현을 쓰고 있으며, 저장매체의 압수(혹은 하드 이미징) 후에 수사기관의 사무실에 행해지는 정보검색을 압수수색영장의 집행의 일환이라고 파악한 점, 압수절차

9) 대법원 2011.5.26. 2009모1190 결정.

10) 손동권, "새로이 입법화된 디지털증거의 압수·수색제도에 관한 연구", 형사정책 제23권 제2호, 2011, 328면 ; 오기두, "전자정보의 검증 수색 압수에 관한 개정 형사소송법의 함의", 한국형사소송법학회 학술발표회(2012.2.17.) 발표문, 5면.

11) 같은 견해로는, 전승수, "디지털정보에 대한 압수수색영장의 집행 - 대법원 2011.5.26.자 2009모1190결정 -", 法曹 제670호, 2012.7., 252면 ; 이주원, "디지털 증거에 대한 압수수색제도의 개선", 安岩法學 제37권, 2012, 193면 ; 오길영, "디지털 저장매체의 압수·수색과 그 쟁점", 민주법학 제49호, 2012, 25면 ; 신동운, 신형사소송법(제4판), 2012, 343면 ; 이은모, 형사소송법(제3판), 2012, 321면.

의 종료 후에 복사대상 전자정보의 목록을 작성하여 교부해야 한다고 한 점 등에서 그러하다.

2) 수사실무상 디지털정보의 압수수색은 대개 아래와 같이 진행된다 : 「① 하드디스크 이미징(또는 저장매체의 압수) → ② 수사기관 사무실에서 파일 내용에 대한 수색 혹은 탐색 → ③ 피의사실에 관련된 파일만을 골라 수사기관의 점유취득(CD에 저장하여 압수)」. 형사소송법 제106조 제3항 및 전교조 사건의 대법원 결정은 압수수색의 현장에서 범죄사실과 관련성이 인정되는 파일들만을 선별하여 출력하거나 복제하는 것이 디지털 정보 압수수색의 원칙이라고 천명하고 있지만, 이러한 원칙적인 압수수색은 대부분의 사건에서는 현실적으로 불가능하다.[12] 컴퓨터 하드디스크에는 많게는 수만개에서 수십만개의 파일이 저장되어 있을 뿐만 아니라, 파일 이름이나 형식이 다양하고 암호화되어 있는 경우라든가 피의자가 파일이름이나 형식을 교묘하게 위장하여 은닉해 놓았을 가능성도 있으며, 수사기관의 입장에서는 경우에 따라서 삭제된 파일을 복구하는 기술을 사용할 필요가 있을 수도 있기 때문이다. 이런 이유로 수사기관에서는 하드디스크 자체의 압수나 이미징을 우선적으로 활용하려는 경향이 있다.[13] 형사소송법 제106조 및 대법원 판례는 저장매체의 압수나 이미징을 예외적으로 허용된다고 선언하고 있음에도 불구하고, 실무상 대부분의 경우에 그 예외의 요건을 충족시키란 그리 어렵지 않다. 또한 영장실무에서도 법원은 압수수색영장에 '피의사실과 관련성이 있는 정보의 출력 또는 복제'를 원칙적인 압수방법으로 기재하면서도 '그러한 방법이 불가능하거나 현저히 곤란한 경우에는 저장매체 자체의 압수나 이미징을 할 수 있다'고 기재하고 있다. 결국 법에서 정한 원칙과 예외는 선언적인 의미에 그칠 뿐이고, 저장매체의 압수를 통한 디지털정보의 포괄적인 압수관행을 실질적으로 통제하는데에는 역부족일 수밖에 없다.

3) 뿐만 아니라, 압수수색의 절차와 방법에 대한 통제의 문제에 대하여도 개정 형사소송법 제106조의 규정은 지나치게 단순하고 미흡한 수준이어서 명확한 해결책을 제시해 주지 못하고 있는 실정이다.

일반 물건의 경우 수색 후 압수가 이루어지는 것과는 달리, 컴퓨터 파일의 경우 우선 '복사'가 선행되고, 그 다음에 '수색'과 '파일의 점유취득'의 순으로 진행된다. 위와 같이 진행되는 디지털정보의 압수수색에서 무엇이 압수이고 무엇이 수색인가를 해명하는 것은 매우 중요하다. 이에 따라 압수수색의 절차가 영장주의 위반인가의 판단이 달라질 수 있기 때문이다. 또한 이 문제는 압수의 대상을 무엇으로 이해할 것인가의 문제와 관련되어 있다.

전교조 사건의 대법원 결정은 수사기관이 저장매체 자체를 압수하거나 하드디스크 이미징 사본을 외부로 반출한 후의 정보검색 및 분석의 과정도 압수수색영장 집행의 일환임을 분명하게 적시하고 있다. 따라서 이 경우에도 수사기관은 피의사실과 관련성이 있는 파일만을 추출하여 출력하거나 복사해야 하고, 그와 같은 정보검색과정에서 임의적인 복제나 오남용

12) 오길영, 전게논문, 18-21면 참조. 컴퓨터 하드디스크 1대만이 압수대상인 경우라 하더라도 그 저장용량의 방대함과 파일의 다양성을 고려하면 현장에서 범죄혐의와 관련된 파일만을 추출해 낸다는 것은 현실적으로 쉽지 않는데, 요즘은 PC 뿐만 아니라 USB, 스마트폰, 태블릿 등 다양한 디지털 기기들을 동시에 사용하는 것이 일반적임을 고려하면 두말할 나위가 없다.

13) 노명선, "디지털증거의 수집절차와 입법적 개선", 포렌식논문지 제1권 제1호, 2010, 10-12면 참조. 다만, 저장매체 자체를 압수하면 영업의 계속 등에 지장을 준다는 비판을 의식해서 최근에는 이미징 기법을 선호하는 추세이다.

을 방지하기 위하여 '당사자나 변호인의 계속적인 참여권 보장', '피압수수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지', '복사대상 전자정보 목록의 작성·교부' 등의 조치가 이루어져야 영장집행의 적법성이 인정된다고 판시하고 있다.

대법원은 [①저장매체의 압수(또는 하드 이미징) → ② 수사기관 사무실에서 정보검색 → ③ 피의자실과 관련성있는 파일만 선별하여 정보취득]의 방식으로 이루어지는 과정 전부를 압수수색영장의 집행이라고 이해한다. 대법원의 이러한 태도는 이미징 후의 정보검색의 남용을 억제하고 당사자의 참여권을 보장한다는 점에서 획기적인 것으로 평가할 만하다.[14] 그렇지만 이러한 해석이 개정된 형사소송법 제106조와 조화될 수 있는가에 대해서는 다소 논란이 있다.

앞서 언급한 것처럼, 형사소송법 제106조는 디지털 정보 자체를 압수의 대상이라고 명시하지 않은 채로, 저장매체 자체의 압수를 엄격한 요건으로 통제하는데 초점을 두고 개정되었다. 그렇다 보니, 형사소송법 제106조로부터는 위 ①~③의 절차 중에서 무엇이 압수인지, 압수영장의 집행절차가 종료되는 시점이 언제인지에 대한 명확한 해석을 도출해 내기 어렵다. 디지털 증거에 관한 압수수색의 전형적인 방법인 위 ①~③의 절차를 상정해 놓고 이 문제에 접근해 보자.

먼저 디지털정보 자체가 압수의 대상이 될 수 없다고 해석하면서 위 절차의 흐름에서 ①의 과정이 압수라고 이해하는 견해가 있다.[15] 저장매체의 압수가 유체물 압수임은 물론이고, 하드 이미징의 경우에도 마치 수색현장에서 관련자의 입회 하에 종이서류를 복사하여 그 사본을 압수하는 것과 동일하게 이미징 자체를 압수라고 보면서, 저장매체 자체 또는 하드 이미징한 것은 수사기관의 사무실로 옮기는 것으로 압수절차는 종료한다는 것이다. 이렇게 보면, 수사기관의 사무실에서 관련 파일을 검색하는 행위는 압수절차의 종료 이후에 행해지는 압수물의 분석에 불과하며,[16] 분석결과 관련성 있는 파일만을 복사하는 행위는 "압수물을 가환부하는 과정에서 관련성 있는 정보에 대한 원형보존조치의 일환"[17]으로 보게 된다. 이 견해는 저장매체의 압수(또는 하드 이미징) 이후 수사기관의 정보검색과정도 압수수색의 집행이라고 파악한 대법원의 결정에 대하여 형사소송법 제106조와 괴리된 해석론이라고 비판하고 있다.

그러나 이 견해는 컴퓨터에 저장된 모든 디지털정보를 통째로 압수하는 것을 허용함으로써 '범죄관련성' 요건을 무시하고 포괄압수를 일반적으로 승인하게 되는 문제를 안고 있다. 이는 형사소송법 제106조의 개정취지에 명백히 반한다. 저장매체의 압수를 허용하는 예외요건은 실무상 비교적 쉽게 충족될 수 있다는 사정을 고려할 때, 저장매체의 압수로 압수집행이 종료한다는 해석은 '범죄 관련성이 인정되는 파일만을 출력·복사의 방법으로 압수'하도록 한 형사소송법 제106조 제3항의 규정을 무력하게 만들어 버리는 것이기 때문에 동의하기 어렵다.

종래의 견해 중에는 디지털 정보 자체가 압수의 대상이 된다는 전제에서, 디지털정보를 압수수색함에 있어서 저장매체 자체 또는 하드 이미징한 것을 수사기관의 사무실로 가져가는 것은 수색의 과정으로 형사소송법상 수색에 부수한 '필요한 처분'(형사소송법 제219조,

---

14) 오길영, 전게논문, 21면.

15) 그와 같은 논지는 대표적으로, 전승수, 전게논문, 272-273면 ; 노명선, 전게논문, 12면 ; 조석영, "디지털 정보의 수사방법과 규제원칙", 형사정책 제22권 제1호, 2010, 94면.

16) 예를 들어, 압수한 장부나 수첩 등을 수사기관의 사무실에서 면밀하게 분석하는 것과 성질상 같다고 보는 것이다.

17) 전승수, 전게논문, 272면.

제120조)으로 허용된다고 보면서, 정보검색 결과 수사기관이 피의사실과 관련성이 인정되는 디지털정보를 취득하는 것을 압수라고 이해하는 입장이 있다. 이 견해는 저장매체 압수 후에 행해지는 수사기관의 정보검색을 '수색'에 해당한다고 보고 그러한 정보검색 후에 범죄사실과 관련된 파일만을 CD 등 저장매체에 담아 그 저장매체를 압수하는 것으로 압수수색절차가 종결된다고 본다.[18] 이에 따르면, 저장매체를 압수한 이후에 진행되는 정보검색도 압수수색의 집행에 해당하기 때문에 형사소송법상의 피의자·변호인의 참여권(제219조, 제121조) 및 간수자 참여규정(제219조, 제123조)을 준수해야 영장집행의 적법성이 인정된다. 그렇지만 이 견해는 압수수색의 현장에서 일단 저장매체의 압수 또는 하드 이미징을 폭넓게 허용할 수밖에 없다는 약점을 지니고 있다.

대법원 판례는 이 두가지 입장을 절묘하게 조합하였다. 대법원 판례는 일응 저장매체의 압수나 하드 이미징을 '1차 압수'로 파악하는 것으로 보인다. 물론 여기에는 압수수색의 현장에서 피의사실과 관련성이 있는 정보만을 출력하거나 복제하는 방식으로 압수수색영장을 집행하는 것이 불가능하거나 현저히 곤란하는 사정이 전제되어야 한다. 앞서 언급한 것처럼 수사실무상 이러한 요건을 충족하기란 그리 어렵지 않다. 아무튼 대법원 판례에 의하면 이와 같은 '1차 압수' 이후에 수사기관의 사무실에서 행해지는 정보검색 '수색'에 해당하고 최종적으로 관련성 있는 파일만을 선별하여 복사하는 것은 '최종적인 압수'라고 이해할 수 있다. 결국 저장매체의 압수(혹은 하드 이미징)라는 예외적인 방식의 압수절차는 "압수-수색-압수"의 단계를 밟아 이루어지는 셈이다. 압수수색의 절차에 관한 대법원의 이러한 이해는 피의자와 변호인의 참여권 보장에 보다 적합하고 포괄압수의 남용을 통제하는데 기여한다는 점에서 수응할 만하다. 그렇지만 이는 디지털 정보 자체를 압수의 대상으로 파악하는 입장에서는 자연스러운 논리이겠지만, 여전히 유체물 압수의 연장선에서 디지털 정보의 압수수색을 규율하고 있는 개정 형사소송법 제106조 하에서 보면 논리적 모순의 문제를 야기시키게 된다. 대법원 결정이 디지털 정보의 압수수색에 관한 형사소송법 개정보다 시기적으로 두달 정도 앞서 나왔고 형사소송법 제106조의 개정에 동력을 실어 준 것은 분명하지만, 대법원 판례가 함축하고 있던 고민을 개정된 제106조는 온전히 담아내지 못하고 있다.

4. 2015년 종근당사건의 대법원 결정

2011년 전교조사건의 대법원 결정에 이어 2015.7.16. 전자정보의 압수수색에 관한 대법원 전원합의체 결정[19]이 있었다. 이 결정은 기본적으로 2011년 대법원 결정의 연장선에 있는데, 여기에서는 두가지 쟁점이 특별히 문제되었다.

첫째는, 디지털 저장매체의 본체 내지 이미징한 것을 수색하는 과정에서 다른 범죄혐의와 관련된 정보를 우연히 발견한 경우에 수사기관이 그 정보를 압수하기 위한 절차가 무엇인가 하는 점이다. 이에 관하여 대법원은 "전자정보에 대한 압수·수색에 있어 저장매체 자체를 외부로 반출하거나 하드카피·이미징 등의 형태로 복제본을 만들어 외부에서 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."고 전제하면서, "그러나 전자정보에 대한 압수·수색이 종료되기 전에 혐

18) 박경신, "E-메일 압수수색의 제문제와 관련 법률개정안들에 대한 평가", 법학연구(인하대 법학연구소 발간) 제13집 제2호, 2010, 274-275면.
19) 대법원 2015.7.16. 2011모1839 전원합의체 결정.

의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우라면, 수사기관은 더 이상의 추가 탐색을 중단하고 법원에서 별도의 범죄혐의에 대한 압수·수색영장을 발부받은 경우에 한하여 그러한 정보에 대하여도 적법하게 압수·수색을 할 수 있다.”고 판시하였다. 또한 그 경우에도 “별도의 압수·수색 절차는 최초의 압수·수색 절차와 구별되는 별개의 절차이고, 별도 범죄혐의와 관련된 전자정보는 최초의 압수·수색영장에 의한 압수·수색의 대상이 아니어서 저장매체의 원래 소재지에서 별도의 압수·수색영장에 기해 압수·수색을 진행하는 경우와 마찬가지로 피압수·수색 당사자(이하 ‘피압수자’라 한다)는 최초의 압수·수색 이전부터 해당 전자정보를 관리하고 있던 자라 할 것이므로, 특별한 사정이 없는 한 피압수자에게 형사소송법 제219조, 제121조, 제129조에 따라 참여권을 보장하고 압수한 전자정보 목록을 교부하는 등 피압수자의 이익을 보호하기 위한 적절한 조치가 이루어져야 한다.”고 판시함으로써 피의자의 참여권 등 적법절차의 보장을 준수해야 함을 분명히 하였다.

2015년 전원합의체 결정이 다룬 두 번째 쟁점은 디지털 정보의 압수수색 과정이 위법한 경우에 – 이 사건에서는 검사가 피의자나 변호인의 참여 없이 임의로 이미징한 파일을 다시 복제한 것과 영장에 기재된 범죄혐의와 무관한 정보를 임의로 출력·복제한 것이 문제되었다 – 준항고에 의하여 압수수색의 전 과정을 위법한 것으로 취소할 수 있는가하는 점이었다. 이에 관한 대법우너 다수의견은 “ 전자정보에 대한 압수·수색 과정에서 이루어진 현장에서의 저장매체 압수·이미징·탐색·복제 및 출력행위 등 수사기관의 처분은 하나의 영장에 의한 압수·수색 과정에서 이루어진다. 그러한 일련의 행위가 모두 진행되어 압수·수색이 종료된 이후에는 특정단계의 처분만을 취소하더라도 그 이후의 압수·수색을 저지한다는 것을 상정할 수 없고 수사기관에게 압수·수색의 결과물을 보유하도록 할 것인지가 문제 될 뿐이다. 그러므로 이 경우에는 준항고인이 전체 압수·수색 과정을 단계적·개별적으로 구분하여 각 단계의 개별 처분의 취소를 구하더라도 준항고법원은 특별한 사정이 없는 한 구분된 개별 처분의 위법이나 취소 여부를 판단할 것이 아니라 당해 압수·수색 과정 전체를 하나의 절차로 파악하여 그 과정에서 나타난 위법이 압수·수색 절차 전체를 위법하게 할 정도로 중대한지 여부에 따라 전체적으로 압수·수색 처분을 취소할 것인지를 가려야 한다. 여기서 위법의 중대성은 위반한 절차조항의 취지, 전체과정 중에서 위반행위가 발생한 과정의 중요도, 위반사항에 의한 법익침해 가능성의 경중 등을 종합하여 판단하여야 한다.”고 판시하였다.

Ⅲ. 정보통신망에 의해 수집·유통되는 디지털정보의 압수수색 관련 문제

1. 문제 제기

위에서 언급한 대법원 결정은 컴퓨터 하드디스크와 같은 컴퓨터 정보저장매체(내지 그 안에 저장된 디지털정보)의 압수수색에 관한 것이다. 개인이나 회사의 PC에 저장된 디지털정보의 압수수색에 관해서 제기되었던 포괄압수의 문제, 당사자의 참여권 보장 등의 문제는 두차례에 걸친 대법원 결정에 의하여 거의 정리된 것으로 보이며, 디지털 압수수색에 관하여 대법원이 정립한 원칙들은 지지할 만하다.

그런데 위 대법원 결정은 컴퓨터 하드디스크 등 정보저장매체의 압수수색에 관한 것일 뿐, 디지털정보의 압수수색의 문제 전반을 포괄하고 있는 것이 아니다. 대법원의 결정에서는 정보통신 네트워크에 기반하여 디지털정보가 생산, 유통되는 상황, 즉 네트워크화되어

있는 디지털정보의 유통이라는 맥락을 고려한 것이 아니다. 오늘날 집이나 사무실에 있는 컴퓨터 하드디스크나 USB와 같은 저장매체의 압수는 디지털 압수수색에서는 차라리 고전적인 문제에 속한다.

이와 관련하여 두가지 사례를 주목할 필요가 있다. 하나는 카카오톡 등 메신저서비스의 압수수색문제이다. 메신저 대화내용의 압수수색은 실무상 압수수색영장에 의하여 집행되고 있는데, 이 사례는 메신저서비스의 대화적 특성이 사실상 감청과 유사하여 그로 인한 정보인권의 침해강도를 일반적인 하드디스크 압수수색과 동일하게 볼 수 없다는 문제의식을 일깨워준다. 다른 하나는 RCS와 같은 해킹툴을 이용한 감시의 문제이다. 최근 불거진 국정원의 RCS 사용의혹의 문제가 그것인데, 이는 디지털정보의 압수수색에서 정보주체에 대한 포괄적이고 전면적인 감시와 사찰의 문제를 제기해 주고 있다.

2. 전기통신에 대한 압수수색

1) 카카오톡 압수수색 사례

2014년 가을 당시 노동당 부대표였던 정00씨의 카카오톡 압수수색 사건을 계기로 하여 카카오톡과 같은 메신저서비스에 의해 송수신된 대화내용의 압수수색 문제가 불거진 바 있다. 사건의 개요를 요약하면 아래와 같다.

정00씨는 2014년 9월 16일자로 종로경찰서로부터 「전기통신에 대한 압수·수색·검증 집행사실 통지」를 받았다. 거기에 적힌 것은 [2014년 5월 1일부터 6월 10일까지 '카카오톡 메시지 내용, 대화 상대방 아이디 및 전화번호, 대화일시, 수발신 내역 일체, 그림 및 사진 파일' 전체를 압수수색]하였다는 내용이었다. 경찰이 다음카카오 회사의 서버에 저장된 카카오톡 메시지 내용 등을 압수수색한 것은 2014년 6월 17일이었다고 한다. 압수수색영장을 집행할 당시에 경찰과 검찰은 피의자인 정00나 변호인에게 압수수색 사실을 전혀 통지하지 않았다. 그 결과 카카오톡 압수수색의 과정에 피의자 정00씨나 변호인의 참여가 전혀 보장되지 않은 채로 압수수색이 진행되었다. 게다가, 2014년 6월 말 검찰은 정00씨를 기소하였는데, 검찰은 정00씨 카카오톡 압수수색으로 취득한 대화내용이나 기타 정보를 증거목록에 포함시키지 않았다. 증거목록에 대해서는 피의자나 변호인의 소송기록열람등사권이 보장되지만(형소법 제266조의3 이하), 카카오톡 압수수색으로 경찰과 검찰이 취득한 정보내용이 이 목록에 포함되지 않았으니, 정00씨나 변호인의 입장에서는 이 시점에서도 카카오톡 압수수색의 집행사실을 전혀 알 수 없었다.

카카오톡 등 메신저서비스는 그 특성상 수많은 개인들이 대화방에 참여하게 된다. 정00씨의 경우 카카오톡 압수수색 당시에 정씨가 참여하고 있던 대화방의 참여자는 약 3,000명 정도였다고 한다. 그 대화내용은 학교 동창들과의 대화와 같은 지극히 사적인 내용도 있었고, 신용카드 번호와 비밀번호, 재판과 관련하여 변호사와 나눈 이야기, 노동당의 업무에 관련한 대화내용 등 내밀한 이야기들이 담겨 있었다고 한다. 이러한 상황은 비단 카카오톡만의 문제는 아니다. 네이버톡이나 밴드, 구글톡 등 사이버상의 다양한 메신저 서비스가 모두 그러하다.

2) 전기통신에 관한 감청과 압수수색의 모호한 경계

현행 법체계 상 전기통신의 내용을 수사기관이 확보하는 방법으로는 통신비밀보호법상 감청과 형사소송법에 의한 압수수색의 두가지가 존재한다.

통신비밀보호법상 감청이란 "전기통신[20]에 대하여 당사자의 동의없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것"을 말한다(제2조 제7호). 대법원은 감청의 개념 및 그 대상에 관하여 다음과 같이 말한다 : "통신비밀보호법에 규정된 '통신제한조치'는 '우편물의 검열 또는 전기통신의 감청'을 말하는 것으로(제3조 제2항), 여기서 '전기통신'이라 함은 전화·전자우편·모사전송 등과 같이 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것을 말하고(제2조 제3호), '감청'이라 함은 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 것을 말한다(제2조 제7호). 따라서 '전기통신의 감청'은 위 '감청'의 개념 규정에 비추어 현재 이루어지고 있는 전기통신의 내용을 지득·채록하는 경우와 통신의 송·수신을 직접적으로 방해하는 경우를 의미하는 것이지 전자우편이 송신되어 수신인이 이를 확인하는 등으로 이미 수신이 완료된 전기통신에 관하여 남아 있는 기록이나 내용을 열어보는 등의 행위는 포함하지 않는다 할 것이다."[21]

판례에 의하면, 이메일이나 메신저의 통신내용은 발신자의 발신 후 수신자가 "읽을 수 있는 상태"에 도달하면 송수신이 완료된 것으로 보게 된다. 수신자가 통신내용을 실제 읽어야 송수신이 완료되는 것이 아니다. 수신자의 개봉 여부와는 무관하게 통신내용을 수신자가 읽을 수 있는 상태가 되는 송수신이 완료된 것으로 보기 때문에, 이처럼 송수신이 완료된 전기통신은 통비법상 감청의 대상이 아니다. 결국 수사기관은 '송수신이 완료된 전기통신'에 대해서는 형소법상의 압수수색영장을 발부받아 그 통신내용을 취득할 수 있게 된다.

통비법상 감청은 일반 압수수색에 비하여 적용대상 범죄가 제한되어 있고 요건도 상당히 까다롭다. 그 이유는 감청은 통신비밀의 자유에 대한 직접적인 침해를 가져오는 조치이기 때문이다. 그런데 감청과 압수수색의 구별에 관한 대법원 판례에 의하면, 감청은 "송·수신이 진행 중인 동안"에만 가능하다는 결과가 된다. 전통적인 전화감청이나 인터넷 패킷감청[22]은 그 전형적인 예가 된다.

문제는 메신저 서비스의 특성을 고려하면 감청과 압수수색의 경계가 상당히 모호해진다는 점이다. 메신저 서비스는 서비스 제공의 기술적 방식에 따라 감청의 기술적 가능성이 달라질 수 있다.[23] 카카오톡의 경우 발신자가 보낸 메시지는 서버에 저장되었다가 수신자의 단말기와 서버가 연결되면 수신자에게 전달되는 방식으로 통신이 이루어진다. 이는 카카오톡

---

20) 통신비밀보호법 상 '전기통신'은 "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 말한다(제2조 제3호).

21) 대법원 2012.11.29. 선고 2010도9007 판결.

22) 인터넷 패킷감청의 허용 여부에 대해서는 많은 비판이 제기되고 있으며, 현재 헌법재판소에 헌법소원이 계류 중이기도 하다. 하지만, 대법원은 통비법상 허용되는 감청의 한 방법으로 용인된다는 입장이다. 대법원은 "인터넷 통신망을 통한 송·수신은 통신비밀보호법 제2조 제3호에서 정한 '전기통신'에 해당하므로 인터넷 통신망을 통하여 흐르는 전기신호 형태의 패킷(packet)을 중간에 확보하여 그 내용을 지득하는 이른바 '패킷 감청'도 같은 법 제5조 제1항에서 정한 요건을 갖추는 경우 다른 특별한 사정이 없는 한 허용된다고 할 것이고, 이는 패킷 감청의 특성상 수사목적과 무관한 통신내용이나 제3자의 통신내용도 감청될 우려가 있다는 것만으로 달리 볼 것이 아니다."라고 말한다(대법원 2012.10.11. 선고 2012도7455 판결).

23)

뿐만 아니라 네이버톡이나 다음의 마이피플 등도 유사하다. 카카오 측은 메시지가 전송되는 과정에서는 SSL 암호화 방식을 이용하고 있어 감청이 불가능하다고 말한다. 그렇지만, 메시지가 카카오톡 서버를 경유하는 과정에서 메시지의 복호화가 기술적으로는 얼마든지 가능하다. 따라서 메시지가 "서버에 저장되는 순간과 동시에" 특정 계정의 메시지를 실시간으로 추출하는 것은 기술적으로 얼마든지 가능하다. 만약 수사기관이 이러한 방식으로 메신저 서비스 상의 대화내용을 수집하였다면 이는 감청에 해당한다고 말할 수 있다.[24)]

결국 메시지가 카카오톡 서버에 저장되는 '바로 그 순간 혹은 직전에' 정보를 취득하면 감청이고 서버에 저장된 '직후에' 취득하는 것이라면 압수수색의 대상이 된다는 식으로 감청과 압수수색의 대상이 구별되는 셈인데, 통신비밀의 보호라는 관점에서 보면 그 기술적 차이는 무시해도 무방할 정도일 것이다. 반면에, 감청이냐 압수수색이냐의 형식적 구별에 따른 수사기관의 정보수집의 용이성, 즉 감청영장과 압수수색영장의 발부요건은 커다란 차이가 있다. 그리고 메신저서비스의 경우 기술적으로 감청이 개입할 시간적 범위는 점점 협소해지므로, 상대적으로 압수수색영장의 완화된 요건이 적용되는 범위는 넓어지게 되어 결국 수사기관의 정보취득이 보다 수월해지는 결과가 된다. 그러므로, 다음카카오 측의 감청영장 집행협조가 감청의 집행이냐 아니냐의 논란은 법제도적 개선에 관련해서는 전기통신의 감청과 압수수색의 법적 간극을 좁혀야 하는 과제로 재등장해야 한다. 즉, 실시간이라는 '현재성과 동시성'을 기준으로 한 현행법체계의 "감청과 압수수색의 이분법" 틀을 넘어서는 법제도의 개선이 필요함을 시사해 주고 있다.

3) 전기통신 정보의 압수수색의 규율 방향에 대하여

(1) 영장 발부요건의 문제

현행 법제에서 전기통신의 내용을 수사기관이 취득하는 방식은 감청과 압수수색으로 이원화되어 있다. 카카오톡 등 메신저 대화내용 중 "송수신이 완료된 것"은 현재 통신비밀보호법상의 감청이 아니라 형사소송법상의 압수수색 대상으로 취급된다. 우선 형사소송법에 의한 압수수색영장이 실제로 매우 광범위하게 그리고 손쉽게 발부되고 있다는 점이다. "피의자가 죄를 범하였다고 의심할 만한 정황"이라는 요건은 체포나 구속사유로 규정된 "상당한 이유"보다 완화된 요건이며, 이러한 요건이 없었던 구 형소법 시절에도 압수수색영장을 발부받기 위해서는 법원은 수사기관이 관련 범죄사실을 소명할 것을 요구하였기 때문에 이러한 요건이 2011년 형소법 개정에서 새롭게 도입된 것은 실무상 압수수색영장의 남발을 규제하기는 어려워 보인다.

이처럼 형사소송법상 압수수색의 요건은 유체물의 압수수색이건 전기통신의 압수수색이건 동일한 조문에 의하여 규율되고 있으며, 압수수색영장은 구속영장의 "상당한 이유"보다 요건이 완화되어 있어 보다 쉽게 발부되는 것이 현재의 상황이다.

그런데 이 하나의 조문으로 사이버 정보통신망을 기반으로 해서 제공되는 다양한 형태의 전기통신 내용에 대한 압수수색을 규율하는 것은 상당히 심각한 문제를 낳고 있다. 여기에서는 컴퓨터 하드디스크의 압수수색, 이메일의 압수수색 그리고 메신저 대화의 압수수색이 지니고 있는 특성과 기본권침해 효과가 질적으로 상이하다는 것을 상기해 볼 필요가 있다.

---

24) 물론 서버를 경유하지 않는 비밀대화나 1:1채팅의 경우에는 메신저서비스 업체의 서버에 기록이 남지 않기 때문에 업체의 협조를 얻어 감청하거나 압수수색하는 것은 불가능하다.

우선 디지털정보의 압수수색은 - 컴퓨터 하드디스크, 일정 기간 동안의 이메일이나 메신저 대화내용 등의 경우 모두에서 - 방대한 자료를 저장하고 있으며 범죄혐의와는 무관한 정보가 혼재되어 있기 때문에, 정보저장매체의 압수라든가 일정 기간 동안의 이메일이나 메신저 대화내용의 포괄적인 압수 방식을 취할 수밖에 없다. 정보주체의 프라이버시권 및 통신비밀에 대한 침해의 강도가 일반적인 압수수색에 비하여 훨씬 크다. 저장정보의 대량성을 고려하면 포괄압수를 손쉽게 허용하는 것은 헌법과 형사소송법상 요구되는 특정성의 원칙, 강제처분의 비례성원칙을 무력하게 만들어 버릴 위험이 매우 높다. 이와 같은 '포괄영장(general warrant)'을 금지해야 한다는 문제의식은 디지털정보의 압수수색 전반에 걸쳐 가장 근본적인 문제의식이 되어야 한다.

그러나 다른 한편으로, 인터넷 통신망을 통해 송수신되는 전기통신(이메일이나 메신저 대화 등)의 경우에는 컴퓨터 하드디스크 등 정보저장매체의 압수와는 또 성격이 다르다. 첫째, 그것은 단순히 컴퓨터 하드디스크에 정보를 저장하는 것과는 달리, 통신비밀의 보호대상이 된다는 점에서 다르다. 둘째, 발신자와 수신자 사이에 오고가는 메시지의 경우 사실상 감청과 압수수색의 대상을 '송수신의 완료 여부'로 구별하는 현행 법시스템이 타당한가 하는 점이다. 메시지가 상대방에게 전달되었으나 아직 상대방이 이를 읽지 않은 채로 서비스회사의 서버에 저장되어 있는 경우에도 여전히 통신비밀로서 보호되어야 할 필요성이 크다고 보아야 한다. 그렇다면 송수신의 완료 여부에 따라 감청과 압수수색의 대상을 구별하면서 감청영장의 요건보다 훨씬 완화된 요건으로 전기통신의 압수수색이 가능하도록 하는 현재의 규율방식은 재고되어야 한다.

마지막으로 이메일과 메신저의 차이도 중요하다. 양자는 프라이버시 및 통신비밀이 침해되는 상대방이 여럿 존재할 수 있다는 점에서는 공통적이나, 메신저의 경우 이메일을 압수수색하는 경우보다 프라이버시나 통신비밀에 대한 침해당사자의 수가 비교할 수 없을 정도로 크다는 점에서는 커다란 차이가 있다. 정00씨 카카오톡 압수수색에서도 3,000여명의 지인들의 대화내용이 수사기관에 그대로 노출되었다.

이처럼 디지털 정보라도 그 대상이 하드디스크 등 저장매체인가, 이메일인가, 메신저 대화내용인가 따라 관련 당사자의 범위 및 기본권 침해의 강도가 서로 다르다는 점을 고려하면, 이 모든 경우를 일반적인 압수수색과 동일한 요건에 의하여 압수수색이 가능하도록 한 현행 규율방식은 비례성원칙의 헌법적 요구에 반하는 결과를 초래하고 있다고 보아야 한다.

그러므로 디지털정보의 압수수색에 관해서는 압수수색의 대상이 무엇인가에 따라 압수수색의 요건과 절차 등을 보다 세분하여 규정하는 방향으로 관련 법제도를 개혁해 나가야 한다. 특히 이메일과 메신저 대화내용의 압수수색은 사실상 통신감청에 준하는 엄격한 요건을 규정하여 통제할 필요가 있다. 송수신이 완료된 경우라도 아직 그 메시지를 읽지 않은 수신자가 있다면 통신비밀의 보호필요성은 더욱 크다고 보아야 하기 때문이다.

이러한 문제의식에 따라 시민사회단체는 이메일이나 메신저 등 전기통신에 대한 압수수색을 통신감청에 준하여 그 대상범죄를 제한하고, 영장발부의 요건에 있어서도 감청영장에 준하여 "다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우일 것"(보충성 요건)을 요건으로 하는 방향으로 통신비밀보호법 개정안을 입법청원한 바 있다.

(2) 포괄압수에 따른 남용 위험에 대한 통제

수사실무상 디지털정보의 압수수색은 대개 아래와 같이 진행된다 :「① 하드디스크 이미징(또는 저장매체의 압수) → ② 수사기관 사무실에서 파일 내용에 대한 수색 혹은 탐색 → ③ 피의사실에 관련된 파일만을 골라 수사기관의 점유취득(CD에 저장하여 압수)」.

이메일이나 메신저 대화내용의 압수수색도 절차상으로 이와 다를 것이 없다. 일반론으로 말하면, ≪영장에 적시된 해당기간 동안 송수신된 이메일을 통째로 복사 → 사무실에서 이메일 내용에 대한 수색 혹은 탐색 → 피의사실 관련 파일만을 골라 수사기관의 점유취득(저장매체인 CD의 압수)≫의 절차로 진행된다. 소위 '하드디스크 이미징'의 경우에도 우선 하드디스크에 저장된 파일을 통째로 복사한 다음에 그 파일 내용을 수색한다는 점에서 압수수색의 절차는 위와 기본적으로 동일하다.

그러므로 포괄압수에 대한 적법절차적 통제를 목표로 한 형사소송법 제106조 제3항 및 대법원 결정은 컴퓨터 하드디스크 등 정보자정매체에 대한 압수수색에 대해서 뿐만 아니라, 인터넷서비스회사의 서버에 저장된 일정 기간 동안의 이메일이나 메신저 대화내용을 압수수색하는 경우에도 동일하게 적용되어야 마땅하다.

그런데 형사소송법 제106조 제3항 및 전교조 사건의 대법원 결정은 압수수색의 현장에서 범죄사실과 관련성이 인정되는 파일들만을 선별하여 출력하거나 복제하는 것이 디지털 정보 압수수색의 원칙이라고 천명하고 있지만, 이러한 원칙적인 압수수색은 대부분의 사건에서는 현실적으로 불가능하다. 형사소송법 제106조 및 대법원 판례는 저장매체의 압수나 이미징을 예외적으로 허용된다고 선언하고 있음에도 불구하고, 실무상 대부분의 경우에 그 예외의 요건을 충족시키란 그리 어렵지 않다. 또한 영장실무에서도 법원은 압수수색영장에 '피의사실과 관련성이 있는 정보의 출력 또는 복제'를 원칙적인 압수방법으로 기재하면서도 '그러한 방법이 불가능하거나 현저히 곤란한 경우에는 저장매체 자체의 압수나 이미징을 할 수 있다'고 기재하고 있다. 결국 법에서 정한 원칙과 예외는 선언적인 의미에 그칠 뿐이고, 저장매체의 압수를 통한 디지털정보의 포괄적인 압수관행을 실질적으로 통제하는 데에는 역부족일 수밖에 없다.

이 때 포괄적인 압수수색으로 인한 남용가능성을 규제하는 원칙적인 방식은 피의자 등 당사자의 참여권을 확고하게 보장하는 방향이어야 한다.

(3) 참여권 등 절차적 통제

① 압수수색 전의 사전통지

형사소송법상 피의자 또는 변호인은 압수수색영장의 집행에 참여할 수 있다(제121조, 제219조). 이는 압수수색절차의 공정성을 확보하기 위한 것으로, 참여권을 보장하기 위하여 수사기관은 압수수색영장을 집행할 때에는 미리 집행의 일시와 장소를 참여권자에게 통지해야 한다(제122조, 제219조).

다만, 참여권자가 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 예외로 한다는 단서규정이 있다(제122조 단서). '급속을 요하는 때'라 함은 압수수색영장의 집행사실을 미리 알려주면 증거물을 은닉할 염려가 있어 압수수색의 실효를 거두기 어려운 경우를 말한다.[25] 사실 경찰과 검찰은 압수수색영장을 집행하는 경우에 거의 대부분 관행적으로 참여권자에게 통지하지 않는다.

25) 대법원 2012.10.11. 선고 2012도7455.

그러나 전기통신사업자의 서버에 저장된 디지털정보의 경우에 수사기관의 관행처럼 '급속을 요하는 경우'에 해당한다고 말할 수는 없다. 특히 카카오톡과 같은 메신저서비스의 경우에는 피의자나 변호인에게 압수수색의 집행에 대하여 사전통지하더라도 피의자·변호인이 서비스제공회사의 서버에 저장된 메시지내용을 임의로 삭제할 가능성은 없다. 따라서 다음 카카오의 서버에 저장된 카카오톡 대화내용을 압수수색하는 경우에는 형소법의 원칙적인 규정에 따라 압수수색영장의 집행일시와 장소를 피의자나 변호인에게 사전통지해야 한다. 피의자나 변호인에게 압수수색 집행을 사전에 통지하지 않고 집행하는 것은 위법한 집행에 해당한다고 보아야 한다.

앞으로의 입법방향은 전기통신의 성격에 따라 사전통지제도를 보다 구체적으로 규정함으로써 당사자의 참여권을 보다 분명하게 보장하는 방향이어야 한다.

② 일정기간 동안의 메신저를 포괄압수한 후 범죄와의 관련성 선별절차에의 참여권 보장

전교조 사건의 대법원 판례는 일응 저장매체의 압수나 하드 이미징을 '1차 압수'로 파악하는 것으로 보인다. 물론 여기에는 압수수색의 현장에서 피의사실과 관련성이 있는 정보만을 출력하거나 복제하는 방식으로 압수수색영장을 집행하는 것이 불가능하거나 현저히 곤란하다는 사정이 전제되어야 한다. 앞서 언급한 것처럼, 수사실무상 이러한 요건을 충족하기란 그리 어렵지 않다. 아무튼 대법원 판례에 의하면 이와 같은 '1차 압수' 이후에 수사기관의 사무실에서 행해지는 정보검색 '수색'에 해당하고 최종적으로 관련성 있는 파일만을 선별하여 복사하는 것은 '최종적인 압수'라고 이해할 수 있다. 결국 저장매체의 압수(혹은 하드 이미징)라는 예외적인 방식의 압수절차는 "압수-수색-압수"의 단계를 밟아 이루어지는 셈이다. 압수수색의 절차에 관한 대법원의 이러한 이해는 피의자와 변호인의 참여권 보장에 보다 적합하고 포괄압수의 남용을 통제하는데 기여한다는 점에서 기본적으로 타당한 방향이다.

이러한 참여권 보장은 이메일이나 메신저의 대화내용에 대하여 일정 기간을 정하여 압수수색영장을 발부하는 경우에도 동일하게 적용되어야 한다. 아래의 내용은 대법원 판례의 취지를 이메일이나 메신저의 대화내용에 대한 압수수색에 적용한 결론이 될 테지만, 보다 근본적으로는 아래와 같은 압수수색 절차를 법규정으로 세밀하게 명시하는 방향으로 나아가야 한다.

첫째, 영장에 기재된 대상기간 동안에 송수신된 이메일·메신저의 내용을 통째로 복사(CD복사건 수사관의 보안용 이메일로 수신한 경우건 간에)하는 것은 범죄사실과 관련성이 없는 파일을 포괄적으로 압수하는 결과가 되어 원칙적으로 위법하다고 보아야 한다. 그것은 예외적으로 압수수색의 현장에서 범죄와 관련성있는 정보를 추출하여 압수하는 것이 실제로 불가능하고, 또 그러한 요건 하에서 일정 기간의 이메일·메신저의 내용을 포괄적으로 압수(1차 압수)할 수 있다는 취지가 영장에 기재된 경우로 한정해야 한다.

둘째, 대법원판례의 취지를 이메일·메신저 압수수색에 적용하면 해당 기간 동안의 이메일·메신저 전체를 복사해 가는 것은 하드디스크이미징과 성질상 같은 것이라고 볼 수 있다. 따라서 대법원판례에 의하면, 피의사실과의 관련성을 무시한 채로 해당 기간 동안의 이메일을 통째로 압수하는 것은 하드디스크이미징의 경우처럼 영장에 그러한 압수가 가능하다고 기재된 경우로서 예외적인 요건을 충족한 경우에 한하여만 허용되어야 한다.

세째, 대법원 판례에 의하면, 수사기관의 사무실에서 압수한 파일을 열어 분석하는 것도 압수수색의 계속된 과정이다. 그러므로 판례의 취지를 살리면, 메신저서버에서 일정 기간

동안의 메신지를 통째로 CD에 담거나 이를 수사기관의 보안메일로 송부받았다고 해서 압수수색절차가 종료한 것이 아니다. 압수의 대상은 어디까지나 범죄와 관련성이 인정되는 정보에 한정되어야 하므로, 우선 수사기관은 일정 기간 동안의 메신지를 통째로 압수했다면 우선 그 파일들을 봉인해야 하고 피의자나 변호인의 참여 하에 개개의 파일이나 내용을 열어보고 범죄와 관련성 없는 정보는 즉시 삭제하고 관련성있는 것들만 추출하여 최종적으로 압수하는 조치를 취하도록 해야 한다.

네째, 이메일·메신저의 포괄 압수 이후에 수사기관의 사무실에서 진행된 수색절차에 당사자 참여권은 "제한없이" 보장되어야 한다. 이 경우의 수색절차는 '급속을 요하는 경우'에 해당하지 않음이 분명하기 때문이다. 수사기관은 이미 서버회사로부터 해당 기간의 이메일·메신저 내용을 통째로 복사해 가지고 있기 때문에 피의자나 변호인에게 참여통지를 하더라도 증거인멸의 우려는 없기 때문이다.

2. RCS와 온라인수색의 문제[26)]

1) 국정원의 RCS 구입 및 사용 의혹

최근 국정원이 이탈리아 Hacking Teams라는 회사로부터 RCS(Remote Control System)를 구입하여 사용했다는 의혹이 논란이 된 바 있다. 2015년 7월 5일 인터넷상에 공개된 이탈리아 Hacking Teams의 자료에 의하면, 국정원은 RCS의 구입 고객이었다. 의혹이 불거지자 국정원은 이탈리아 해킹팀으로부터 RCS를 구입했다는 사실은 마지 못해 시인하면서도 대북·대테러용으로만 사용했다고 해명했다. 그렇지만, 유출된 400기가 분량의 Hacking Team 자료에 대한 분석 결과, 국정원이 RCS를 국내에서 사용했음을 추정케 하는 사실들이 밝혀졌다. 국정원은 이탈리아 해킹팀에 카카오톡 해킹 기능을 요구했으며, 백신프로그램인 안랩을 피하는 방법을 주문했고, 삼성에서 신형 핸드폰이 출시될 때 그것을 해킹하는 '맞춤해킹' 방법을 이탈리아 해킹팀에 문의하였다. '미디어오늘' 기자를 사칭한 메일의 첨부 워드파일에 스파이웨어를 심어달라고도 요청하기도 했다. 스파이웨어를 침투시키기 위하여 특정 공간에서 가상의 와이파이망을 만드는 TNI 프로그램을 구입했다는 의혹도 있고, 앱의 다운로드를 통해 스파이웨어를 감염시키려 했던 정황도 포착되었다.

RCS는 해킹프로그램의 일종으로, 사용자의 PC나 스마트폰에 원격조종을 가능하게 하는 스파이웨어를 침투시킨 다음, 그것과 연결된 컴퓨터시스템을 통하여 사용자의 PC나 스마트폰을 원격조종하여 정보를 빼내는 방식으로 작동한다. RCS 해킹프로그램은 컴퓨터나 스마트폰에 해당 스파이웨어를 침투시키는데 성공한다면 감시자는 컴퓨터나 스마트폰을 통해서 유통되거나 저장되어 있는 거의 모든 정보를 검색하고 수집할 수 있다. 컴퓨터나 스마트폰의 사용자가 인터넷에 접속하는 경우에 정보통신망을 통해서 이루어지는 전화통화나 메시지 송수신의 내용은 실시간으로 감시자에 전달되거나 지정된 서버에 저장된다. 또한 감시자는 스마트폰에 내장된 카메라를 원격조종하여 사용자 몰래 사용자의 상태나 주변상황에 관한 화상정보를 전송받을 수 있으며, 통화내용을 몰래 녹음하여 전송하는 것도 가능하다. 더 나아가서, 감시자는 컴퓨터나 스마트폰에 저장된 정보도 사용자 몰래 검색하고 수집할 수 있

26) 이 부분 서술은, 이호중, "국정원의 해킹프로그램 구입 및 사용(의혹)에 관한 법리 분석과 국정원 정보수집의 한계", 서울지방변호사회 인권위원회 주최, 「정보기관의 정보수집 권한의 한계와 견제 방안 등에 대한 강연회 및 토론회」(2015.7.30.) 자료집 9-39면의 내용을 요약, 발췌한 것이다.

으며, 사용자가 사용하는 아이디나 비밀번호도 수집할 수 있다. 사용자가 데이터를 암호화 행태로 저장하는 경우에도 감시자는 사용자가 특정 시점에 데이터를 사용하는 것과 동일한 방법으로 그 데이터에 접근할 수 있기 때문에 암호화되기 전 단계에서 정보를 수집할 수 있다는 점도 RCS의 특징이다.

2) 감청도, 압수수색도 아닌 RCS

국정원이 사용한 것으로 보이는 RCS 해킹이 구체적으로 어떠한 기술적 방식으로 작동하는지는 아직 명확하게 해명되어 있지 않다. RCS가 감청에 해당하는가에 관하여, 국정원은 지난 7월 27일 국회 정보위원회 보고에서 RCS에 의한 "실시간 감청은 불가능하며 서버에 자동으로 녹음되어 녹취록을 만든다"고 해명한 것으로 알려지고 있다.[27] 감청의 개념은 송수신 중에 기술적 개입을 통하여 통신의 내용을 지득하는 것을 말하며, 그것이 녹음의 방식인지 아니면 감청하는 수사기관이 실시간으로 그 내용을 지득하는 것인지는 중요하지 않다. 스마트폰의 통화 내용을 실시간으로 서버에 저장하는 것도 감청의 개념에 해당한다. 그러므로 위와 같은 국정원의 해명은 법을 왜곡하는 것이다.

중요한 점은 RCS 프로그램이 단지 대상자가 송·수신하는 전기통신 과정에 실시간으로 개입하여 전기통신의 정보를 감청하는 것에 한정되지 않는다는 점이다. RCS는 통화내용이나 메시지에 대해 실시간으로 내용을 확보하는 기능(이것은 '감청'에 해당한다)뿐만 아니라, 스마트폰의 카메라를 작동시켜 사용자의 모습 또는 주변상황에 관한 정보를 취득할 수 있으며, 더 나아가서 대상자의 컴퓨터나 스마트폰에 저장·사용되는 모든 정보를 사실상 사용자 몰래 취득할 수 있다. 그러므로 해킹프로그램으로 국정원이 취득할 수 있는 정보의 범위는 단순히 '감청'으로 획득할 수 있는 정보의 범위를 넘어서는 광범위한 것이다.

이를 기본권보호의 관점에서 바라본다면, RCS 해킹프로그램의 사용은 시민들이 기본권으로 향유하는 통신비밀 및 프라이버시의 자유를 침해하는 것을 훨씬 넘어서는 기본권 침해효과를 수반한다. 사실 RCS 해킹프로그램은 기술적으로 수집가능한 정보의 범위를 특정하기 어렵다는 문제를 안고 있다. 그것은 스파이웨어에 감염된 사용자의 컴퓨터나 스마트폰에서 다양한 정보를 검색하고 수집할 수 있는 기술적 가능성을 지니고 있지만, 어느 수준의 정보까지 해킹이 가능한지는 일률적으로 특정할 수 없다는 한계가 있다. 해킹프로그램이 업데이트됨에 따라 이전에 가능하지 않던 정보의 검색과 수집이 가능하게 될 수 있기 때문이다. 어쨌거나 RCS 해킹프로그램은 기존의 감청제도에 의하여 보호되는 통신비밀과 프라이버시를 넘어서는 광범위한 정보인권 침해를 가져오는 것은 분명하다.

오늘날 핸드폰이나 컴퓨터는 단순한 통화매체 또는 정보저장매체의 기능을 넘어서서 사실상 사용자의 모든 생활에 관한 정보를 담고 있다. 사용자들은 카카오톡 등 메신저서비스를 통하여 다양한 정보를 주고받으며, 페이스북, 블로그 등에 자신의 생활에 관한 다양한 정보를 올리기도 한다. 수많은 사진과 동영상, 일기와 같은 지극히 사적인 정보도 핸드폰이나 컴퓨터에 저장된다. 그러므로 핸드폰이나 컴퓨터는 사용자의 인격과 긴밀하게 결합된 매체라는 특성을 지니고 있다.

만약 국정원이나 기타 정보기관·수사기관이 시민들이 사용하는 핸드폰이나 컴퓨터에 사용자 몰래 임의로 접근하여 사용·저장되는 정보를 수집한다면, 그 수집정보의 범위는 사용자의 일상생활의 동선, 취미, 취향, 신체적 특성, 사회적 관계 등 개인의 인격에 관한 거의

27) http://www.hani.co.kr/arti/politics/politics_general/701989.html?_fr=mt1

모든 정보를 망라한다. RCS의 본질은 따라서 '감청'이 아니라 시민 개개인에 대한 '인격사찰'이다.

3) 소위 "IT-기본권"

독일 연방헌법재판소는 해킹사찰의 이러한 특성을 고려하여 "정보기술 시스템의 기밀성과 무결성을 보장받을 수 있는 권리(Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)"라는 개념을 도입하였다.[28] 이는 통상 "IT-기본권"이라 부르는데, 이 IT 기본권은 독일 기본법 제1조 및 제2조 제1항의 인격권보호로부터 도출된다고 한다.

독일 연방헌법재판소가 'IT-기본권'이라는 새로운 개념을 창설한 것은 사용자의 컴퓨터시스템에 스파이웨어를 설치하는 방식으로 비밀리에 사용자의 정보기술시스템에 접근하여 정보를 검색·수집하는 행위(이를 통상 온라인수색이라고 부른다)에 대해 헌법적으로 인정되는 통신비밀의 자유, 프라이버시권, 개인정보자기결정권 등으로는 인격권보호에 충분하지 못하다는 문제의식에 기반하고 있다.

우선 개인용 PC나 스마트폰은 시민들의 생활에 매우 중요한 의미를 지니고 있으며, 그 정보기술시스템이 인터넷 등 정보통신망으로 연결된 경우에 그것은 인격권 발현에 있어서 더욱 커다란 중요성을 지닌다고 한다. 특히 인터넷통신서비스를 이용하여 시민들은 적극적으로 사회적 관계를 형성하고 촉진할 수 있는 반면에, 네트워크화된 정보기술시스템에의 침입은 인격에 대한 새로운 침해의 위험 또한 증가시키고 있다고 한다.

네트워크를 통하여 사용자는 개인 컴퓨터나 스마트폰에서 다양한 데이터를 수집하고 저장할 수 있다. 만약 누군가가 네트워크를 통하여 사용자의 컴퓨터나 스마트폰에 비밀리에 접속할 수 있다면, 그것에 의해 검색·수집되는 정보의 범위는 매우 광범위하며, 그것은 사용자가 의식적으로 사용하거나 저장한 정보에 국한되지 않는다. 사용자가 어떤 사이트를 자주 방문하는지, 거기에서 어떤 정보를 게시하고 어떤 정보를 수집하는지에 관한 정보도 수집될 수 있으며, 누구와 연락하는지, 어떤 장소를 방문하는지 등 개인의 사회적 관계 및 활동에 관하여 엄청난 양의 정보를 수집할 수 있게 된다. 독일 연방헌법재판소는 이렇게 수집된 정보들이 평가된다면 이는 사용자의 인격을 추론케 할 정도의 것이라고 말한다.

또한 사용자가 SNS 서비스에 접속하는 경우에 해킹프로그램에 의하여 그 관련정보를 수집하는 행위는 수많은 대화참여자에 관한 정보를 무한정하게 수집한다는 점에서 그 기본권 침해는 매우 광범위하게 확산될 수 있다고 한다.

이렇게 RCS를 통해서 수집되는 정보는 송·수신 중인 전기통신의 내용을 넘어서는 것이다. 독일 연방헌법재판소는 감시자가 네트워크 비밀접속을 통하여 사용자의 컴퓨터나 스마트폰에 저장된 정보를 수집하는 경우에는 통신비밀의 보호라는 기본권으로는 충분히 보호될 수 없다고 한다. 또한 해킹 프로그램에 의하여 비밀리에 수집되는 정보는 프라이버시에 속하는 정보에 국한되는 것도 아니기 때문에, 프라이버시 보호라는 기본권으로 포괄하는 것도 한계가 있을 수밖에 없다고 한다. 같은 이유에서, 개인정보에 관한 정보적 자기결정권이라

28) BVerfG v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07. 이 결정은 노르트라인-베스트팔렌 주의 헌법보호법률(Gesetz über den Verfassungsschutz in Nordrhein-Westfalen) 제5조 제2항에서 헌법보호청에게 정보기술시스템에의 비밀 접근을 허용하는 규정을 도입한 것(이 규정은 2006년 12월 20일 발효)에 대한 헌법소원 사건에 대한 것이다.

는 기본권 테제로도 인격권 침해에 대한 충분한 보호가 불가능하다고 말한다.

이러한 검토에 따라 독일 연방헌법재판소는 '정보기술시스템의 기밀성과 무결성을 보장받을 권리'라는 기본권이 독일 헌법 제1조와 제2조 제1항으로부터 도출될 수 있다고 보았다. 독일 연방헌법재판소의 말을 인용하면, "정보기술시스템에의 접근은 개인의 생활형성의 중요한 부분을 보게 하거나 심지어는 인격에 대하여 내용이 풍부한 표상을 가질 수 있게 하는 경우에 적용될 수 있다."

독일 연방헌법재판소는 노르트라인-베스트팔렌 주의 헌법보호법률(Gesetz über den Verfassungsschutz in Nordrhein-Westfalen) 제5조 제2항 제11호에 대해서는 위헌결정을 내렸다. 그렇지만, 독일 연방헌법재판소는 스파이웨어를 통한 해킹 방법이 국가정보기관의 헌법보호나 테러위험의 방지 등의 목적을 위한 수단으로 사용될 가능성을 완전히 차단한 것은 아니었다. 과잉금지 원칙에 비추어 독일 연방헌법재판소는 스파이웨어 침투에 의한 해킹이 허용될 수 있는 엄격한 요건을 설정하여, 첫째, 매우 중대한 보호법익에 대한 매우 구체적인 위험이 존재하는 경우로 한정되어야 하며, 둘째, 절차적으로는 판사의 허가에 의해야 국가기관이 집행해야 하고, 셋째, 프라이버시의 핵심영역을 보호하기 위한 보호조치가 마련되어야 한다는 점을 지적하였다.

4) RCS에 대한 규제의 문제

독일에서 2006년 노르트라인-베스트팔렌 주의 헌법보호법률(Gesetz über den Verfassungsschutz in Nordrhein-Westfalen) 제5조 제2항 제11호에 해킹프로그램의 사용이 명시적으로 규정되기 전에, 독일에서는 해킹프로그램에 의한 온라인수색이 감청(독일 형사소송법 제100a조)에 의하여 허용될 수 있는지에 대하여 많은 이론적인 논란이 있었던 것으로 보인다. 감청규정을 근거로 해서 해킹프로그램에 의한 정보수집이 허용될 수 있다는 일부 견해가 있었지만, 독일 연방대법원은 2006년 판례 이후로 해킹프로그램의 사용이 독일 형사소송법상의 감청 규정에 의하여 정당화될 수 없다는 점을 분명히 하였다.[29] 개인 사용자의 컴퓨터에 저장된 정보는 감청의 대상이 되는 전기통신의 범위를 넘어서는 것으로 감청으로 허용될 수는 없으며, 다른 한편으로 그것은 '비밀수색'이라는 점에서 공개된 혐의자수색을 규정한 독일 형소법 제102조에 의하여도 허용될 수 없다고 하였다.[30] 독일에서도 '감청'은 송·수신 중인 전기통신에 대해서만 허용되는 정보수집행위라는 점에서 우리의 통비법상의 감청과 개념적으로 거의 동일하기 때문에, 독일 연방대법원 판례와 이론적인 논의는 우리에게 시사해주는 바가 크다.

RCS에 의한 정보수집의 범위가 통비법상의 감청제도에 의하여 허용되는 범위를 넘어서는 것이라는 점에서 RCS는 통비법상의 감청으로 허용될 수 있는 정보수집행위라고 볼 수 없다. 이렇게 보면, 현재 우리나라의 법체계에서 RCS와 같은 해킹툴을 이용한 온라인수색을 가능하게 하는 법규정은 존재하지 않는다.

외국에서는 이미 RCS와 같은 해킹툴을 이용한 온라인수색을 허용하는 법적 근거를 마련한 경우도 있고 법규정의 도입에 관해 논의하고 있는 나라도 있다. 독일의 경우를 예로 들면, 독일에서는 RCS와 같은 트로이목마 프로그램을 통한 감시를 허용하는 규정을 das Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der

29) BGH v. 31.1.2007 - StB 18/06 ; BGH v. 25.11.2006 - 1 BGs 184/06.
30) Röwer, in : Radtke/Hohmann, Strafprozessordnung Kommentar, §100a, Rn.19ff.

Länder in kriminalpolizeilichen Angelegenheiten(연방수사국 및 범죄수사 업무에 관한 연방과 각 주의 협력에 관한 법률) 제20k조(정보기술시스템에 대한 비밀침입)[31], 그리고 연방

31) § 20k Verdeckter Eingriff in informationstechnische Systeme
(1) Das Bundeskriminalamt darf ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für
1. Leib, Leben oder Freiheit einer Person oder
2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.
Eine Maßnahme nach Satz 1 ist auch zulässig, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in Satz 1 genannten Rechtsgüter hinweisen. Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.
(2) Es ist technisch sicherzustellen, dass
1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.
Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.
(3) Bei jedem Einsatz des technischen Mittels sind zu protokollieren
1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.
Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 2 genannten Zweck noch erforderlich sind.
(4) Die Maßnahme darf sich nur gegen eine Person richten, die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.
(5) Die Maßnahme nach Absatz 1 darf nur auf Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht angeordnet werden.
(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben
1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie
4. die wesentlichen Gründe.
Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.
(7) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erhobene Daten sind

과 주의 헌법보호청법률들에 이미 도입되어 있다. 위 연방헌법재판소의 위헌결정에 따라 그 허용요건은 매우 엄격하게 설정되어 있기는 하다. 위 독일 연방수사국 및 범죄수사 업무에 관한 연방과 각 주의 협력에 관한 법률 제20k조를 보면, 해킹툴을 이용한 비밀감시의 요건은 대체로 "개인의 생명·신체나 자유에 대한 구체적인 위험을 방지하기 위한 목적 또는 공공 법익에 대한 구체적인 위험이 존재하고 그것이 국가의 존립과 기본질서 내지 인류의 존립기반을 위협하는 경우"로 규정되어 있다.

현행법상 RCS의 사용이 법적 근거가 없는 불법적인 범죄행위라는 것을 지적하고 문제제기하는 것 못지 않게, 이 사건은 앞으로 그러한 RCS 해킹툴의 사용을 허용하는 법제도를 용인할 것인가 하는 지극히 어려운 정책적 과제를 우리에게 던져주고 있다.

Ⅳ. 맺음말에 대신하여 - 던져진 숙제

1. 압수대상으로서 '정보', 그리고 수색의 공간

디지털정보의 압수수색에서 압수의 대상이 '유체물'인가 '정보'인가에 관한 고전적인 논란은 법이론상으로는 아직 명쾌하게 결판나지 않았다. 앞서 언급한 것처럼, 판례는 디지털정보 자체를 압수의 대상으로 파악하고 그에 따라 디지털정보의 압수수색에 관하여 범죄혐의와 무관한 정보의 포괄적인 압수의 위험을 법치주의적으로 통제하기 위한 방안으로 당사자의 참여권을 강조하고 있다.

디지털 압수수색에서 압수의 대상을 '유체물'로 바라보는 견해는 이메일이나 메신저서비스의 압수수색에서 당장 그 난점을 드러낼 수밖에 없다. 컴퓨터 하드디스크나 USB 저장매체의 압수수색을 넘어서서 정보통신망을 통하여 생산되고 유통되는 정보가 수사기관이나 정보기관의 수집대상이 될 수 있음을 부인하기 어려운 현 상황에서, 디지털 압수수색의 규율을 위해서는 압수의 대상이 '정보'라는 관점을 유지하는 것이 보다 유용하다. 특히 카카오톡 압수수색의 사례에서 언급한 것처럼, 디지털정보 그 자체를 압수수색의 대상으로 포착하는 방향은 압수대상인 디지털정보의 성격과 인권침해적 속성을 고려하여 압수수색의 요건과 절차 등을 보다 엄격하게 세분화하는 방향으로 나아갈 수 있다는 장점이 있다.

그런데 디지털정보의 압수수색에서 이처럼 '정보' 그 자체가 압수의 대상이라고 보는 관점은 또 다른 차원에서 우리에게 어려운 문제를 안겨주고 있다. 전통적인 압수수색의 개념은 '유체물' 그리고 '그 유체물이 존재하는 물리적 공간'을 전제로 하고 있다. 유체물을 압수하기 위해서 그 물건이 존재할 것으로 보이는 물리적 공간 - 집이나 사무실 - 이 수색의 대상이 되는 것이다. 그 때 수색의 장소는 대개 피의자 또는 제3자의 프라이버시권이 미치는

---

unter der Sachleitung des anordnenden Gerichts nach Absatz 5 unverzüglich vom Datenschutzbeauftragten des Bundeskriminalamtes und zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen. Der Datenschutzbeauftragte ist bei Ausübung dieser Tätigkeit weisungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Abs. 3 des Bundesdatenschutzgesetzes). Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen nicht verwertet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

공간임을 전제로 한다.

그러나 압수물을 '정보'라고 하면, 사정이 다르다. 디지털 정보는 개인이나 회사의 컴퓨터 하드디스크나 USB처럼 누군가의 소유·소지가 법적으로 보호되는 공간에 존재할 수도 있지만, 이메일이나 메신저서비스의 경우를 보면 디지털정보는 그 서비스를 제공하는 기업의 서버에 저장되는데 정작 그 서버를 물리적으로 관리하는 회사는 해당 정보의 저장에 관하여 프라이버시권 보호의 이해관계를 갖고 있지 않다.[32] 즉 인권법적 이해관계에서 볼 때, 디지털 정보의 주체에게 참여권을 인정하는 등 정보주체의 인권보호가 점점 더 중요해 지는 이 면에서는, 디지털정보가 존재하는 물리적 공간에 대한 프라이버시 보호의 이익은 상대적으로 미약하다고 평가될 수도 있다. 이 문제는 외국의 서버를 이용하는 이메일이나 메신저의 경우에 수사기관이 국내에서 아이디와 비밀번호 접속의 방법에 의해서 해당 서버에 접속함으로써 디지털 정보를 압수하는 방법 – 소위 '원격 압수' – 의 허용가능성을 열어줄 수 있다. 당사자인 피의자의 참여권만 보장된다면, 수사기관이 외국이나 국내의 서비스제공 기업이 피의자에게 할당한 서버의 일정 부분에 접속하여 디지털정보를 압수하는 방법이 허용되어야 하는가의 문제가 매우 어려운 난제로 등장하게 될 것이다.

2. '수색'과 '사찰'

우리가 통상 '압수수색'이라고 말할 때 전통적으로 방점은 '수색'이 아니라 '압수'에 두어져 왔다. 디지털정보의 압수수색에서도 포괄적인 압수의 금지가 핵심적인 쟁점을 형성해 왔으며, 컴퓨터 하드디스크의 압수수색에 관한 대법원 결정에서도 '범죄혐의와 무관한 정보의 포괄적인 압수'를 어떻게 제어할 것인가가 주요 쟁점이 되었다. 반면에, '수색'은 '압수'를 위한 절차적 과정이라는 인식이 아직도 강하게 지배하고 있는 듯하다. 디지털정보의 수색 그 자체에 의한 정보인권의 침해에 관해서는 아직 문제의식이 미약한 편이다.

그러나 우리가 향후 보다 주목해야 할 쟁점은 압수가 아니라 수색에 놓여 있다. 디지털정보의 포괄적인 압수의 위험을 효과적으로 규제하는 문제는 그 자체로 매우 중요한 쟁점인 것은 분명하지만, 정보인권의 관점에서 볼 때, 그것이 디지털정보의 압수수색에 관련한 정보인권 침해의 문제를 모두 해결해 주지는 못한다. 디지털 정보의 압수수색의 특징은 사실 디지털정보에 대한 광범위한 수색이 허용될 수밖에 없다는 점에 있다. 대법원 결정에 따라 디지털 정보의 압수수색절차에 피의자나 변호인의 참여를 허용한다면 포괄압수의 남용에 대해서는 어느 정도 통제가 가능하지만, 엄청난 양의 디지털 정보를 일일이 탐색하는 과정 자체를 금지하기는 어렵다는 치명적인 약점을 안고 있다.

수사기관의 광범위한 정보탐색은 영장주의에 의해 제어할 수 있는 문제가 아니다. 더구나 RCS 해킹툴의 사용에서 문제된 것처럼 시민의 컴퓨터나 스마트폰의 모든 정보를 국가권력이 탐색할 수 있게 된다면 그것은 인격권에 대한 전방위적 사찰이라는 결과에 이르게 된다. 이 문제는 디지털 압수수색에서 우리가 직면하게 될 현실적인 문제가 단지 포괄압수의 남용을 제어하는 문제를 넘어서 네트워크화되어 유통·수집되는 디지털정보에 관한 포괄적인 탐색을 어떻게 제어할 것인가의 문제임을 분명하게 보여주고 있다.

Ⅳ. 맺음말

32) 이는 클라우드 서비스 등 웹하드를 이용하는 경우에도 동일하게 나타난다.

정보인권연구소

- 홈페이지 : http://idr.jinbo.net
- 전화 : 02-774-4551
- 팩스 : 02-701-7105
- 이메일 : digitalrights2015@gmail.com
- 주소 : 서울시 서대문구 독립문로8길 23 3층 (03745)