이학석사 학위논문

공개키 암호를 이용한 전자정보 보전처분에 관한 연구

2021년 1월

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식 전공
남 성 우

공개키 암호를 이용한 전자정보 보전처분에 관한 연구

지도교수 천 정 희

이 논문을 이학석사 학위논문으로 제출함

2020년 12월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식 전공

남 성 우

남성우의 석사 학위논문을 인준함

2021년 1월

위 원 장 _____ 국 웅 _____ (인)

부 위 원 장 _____ 박 상 준 _____ (인)

위 원 _____ 천 정 희 _____ (인)

국 문 초 록

전자정보의 생성과 저장·유통이 확대됨에 따라 전자정보가 압수수색의 대상이 되는 경우도 현저히 증가하면서, 전자정보의 훼손 용이성 등과 같은 전자정보의 특성을 반영하여 전자정보 압수수색을 위한 사전적 보전조치로서 '전자정보에 대한 보전처분 제도'를 도입하자는 논의가 계속되어 오고 있다.

전자정보 압수수색에는, 전자정보의 훼손 용이성으로 인한 '신속한 정보획득'의 필요성이라는 측면과 전자정보의 대량성 및 비가시성으로 인한 '신중한 정보보호'의 필요성이라는 측면이 공존한다. 따라서 전자정보 압수수색을 위한 사전적 보전조치로서 도입이 논의되고 있는 전자정보 보전처분 제도는 신속한 정보획득과 신중한 정보보호라는 두 가지 목표가 동시에 달성될 수 있도록 설계되어야 한다. 나아가 전자정보 보전처분 제도가 형사절차의 여러 지점에서 폭넓게 활용될 수 있도록 이를 '확장성 있는 제도'로 설계하면 형사사법 절차의 효율성을 제고하는데 도움이 될 수 있다. 이를 위하여 전자정보 보호처분 제도에 암호기술을 적용하는 기술적 접근을 시도하여 보았다.

본고에서 제안하고 있는 공개키 암호기술을 이용한 전자정보 보전처분 제도에서는, 수사기관이 보호처분된 전자정보의 내용에 임의로 접근할 수 없도록 암호기술을 통한 기술적 조치가 취하여지기 때문에 신중한 정보보호라는 목표가 충족된다. 뿐만 아니라 수사기관은 법원이 사전에 제공한 공개키 암호를 통해 전자정보 보전처분을 실시하기 때문에 신속한 정보획득이라는 목표를 달성할 수 있다. 나아가 전자정보가 암호화됨으로써, 수사기관이 보전처분된 전자정보를 보관하게 되더라도 무방하기 때문에 전자정보 보호처분 대상자가 제한 없이 확대될 수 있고, 여기에 더하여 전자정보 보전처분 제도가 별건 전자정보나 컴퓨터 생성증거의 확보 등 형사절차의 여러 지점에서 폭넓게 활용될 수 있는 확장성을 갖게 된다.

형사절차 중 신속한 정보획득의 측면과 신중한 정보보호의 측면이 공존하는 지점이라면 전자정보 보전처분 제도의 도입이 검토될 수 있게 되는 것이다.

기존에 논의되어 온 전자정보 보전처분 제도는 '자가 보전 방식'(보전처분 대상자가 스스로 전자정보를 보관하는 방식)에 기반하고 있어 그 대상자와 활용 범위가 상당히 제한되는 한계가 있다. 본고에서 제안하고 있는 공개키 암호기술을 이용한 전자정보 보전처분 제도는 기존 논의의 한계를 넘는 데에도 기여할 수 있을 것으로 기대된다.

주요어: 전자정보 보전처분(보전명령), 암호화, 공개키 암호, 압수수색, 별건 전자정보, 컴퓨터 생성증거

학 번: 2019-23359

목 차

제1장 서론

제1절 연구 배경

형사소송법은 증거 확보를 위한 대물적 강제처분으로 압수수색을 규정하고 있다. 수사기관[1]은 압수수색을 통해 물적 증거를 확보하고 이를 통해 사실관계를 확인한다. 그런데 우리 사회에서 대규모의 디지털 전환이 이루어지고 있고 휴대용 디바이스의 사용이 확산되면서 전자정보[2]의 생성과 저장·유통이 확대일로에 있으며, 이로 인하여 전자정보가 압수수색의 대상이 되는 경우도 현저히 증가하고 있다. 이에 전자정보의 훼손 용이성 등과 같은 전자정보의 특성을 반영하여 전자정보 압수수색을 위한 사전적 보전조치로서 '전자정보에 대한 보전처분 제도'(이하 '전자정보 보전처분 제도'라고 한다)를 도입하자는 의견이 대두되고 있다.

전자정보 보전처분 제도의 도입을 주장하는 견해는 전자정보의 변경과 삭제가 용이하다는 훼손 가능성에 주된 초점을 맞추고 있다. 즉 '전자정보는 훼손이 용이하기 때문에 전자정보의 주체나 보관자가 이를 훼손하기 전에 신속하게 확보하여야 한다'는 인식에 바탕을 두고 있다. 실제로 실무에서 기업의 임직원들이나 개인들이 전자정보를 훼손하는 사례를 어렵지 않게 관찰할 수 있다. 일례로 상장기업의 임직원들이 증권선물위원회의 조사를 전후로 광범위하게 전자정보를 훼손한 사실로 기소된 사례가 있고, 뇌물수수 등의 혐의를 받던 고위직 경찰공무원은 수사를 앞두고 관련자에게 휴대폰에 저장된 정보를 삭제하도록 지시하였으며 그 관련자는 수사

---

1) 수소법원이 압수수색을 실시하는 경우는 상당히 드물고, 주로 수사기관이 압수수색을 실시한다[주석 형사소송법 제5판(Ⅰ), 한국사법행정학회, 555면]. 통상적으로 법원은 수사기관의 압수수색을 통제하는 역할을 수행하고 있다. 이와 같은 이유로 본고에서는 수소법원의 압수수색이 아닌 수사기관의 압수수색을 상정하고 논의를 전개한다.

2) 대법원은 후술하는 각종 결정과 판결에서 '전자정보'라는 용어를 사용하고 있는바, 본고에서도 논의의 편의를 위하여 전자정보라는 용어를 그대로 사용한다.

기관 출석을 앞두고 휴대폰에 저장된 텔레그램 메시지 등을 모두 삭제한 후 그 휴대폰을 한강에 버린 사례도 있다. 이처럼 전자정보 훼손 행위는 기업과 개인을 가리지 않고 발생하고 있다.

이러한 현실에 비추어 보면, 전자정보 보전처분 제도를 도입하여 전자정보가 훼손되기 전에 이를 적시에 확보할 수 있도록 조치하는 것이 사실관계의 정확한 파악을 통한 적정한 형벌권의 행사를 위해 필요하다.

한편, 광범위한 전자정보의 압수수색에 따른 사생활 침해나 저인망식 수사 등에 대한 우려도 커지고 있다[3]. 이는 전자정보의 대량성과 비가시성이라는 특징에 기인하는데, 기술의 발달로 정보저장매체의 저장 용량이 급격히 증가함에 따라 통상적으로 정보저장매체에는 대량의 전자정보가 저장되어 있고, 여기에 저장된 전자정보들이 범죄혐의와 관련된 정보(이하 '유관정보'라고 한다)인지를 확인하기 위해서는 전자정보의 비가시성이라는 특성상 개별 전자정보를 일일이 살펴보아야 한다. 그 결과 수사기관이 전자장보를 압수수색하는 과정에서 범죄혐의와 무관한 정보(이하 '무관정보'라고 한다)에 대해서까지 압수수색을 실시할 수 있다는 우려가 커지고 있는 것이다. 이러한 우려는 수사기관의 행동양태에 기초하고 있기도

3) 대법원은 "오늘날 기업 또는 개인의 업무는 컴퓨터나 서버 등 정보처리시스템 없이 유지되기 어려우며, 전자정보가 저장된 저장매체는 대부분 대용량이어서 압수수색영장 발부의 사유로 된 범죄혐의와 관련이 없는 개인의 일상생활이나 기업경영에 관한 정보가 광범위하게 포함되어 있다. 이러한 전자정보에 대한 압수수색은 사생활의 비밀과 자유, 정보에 대한 자기결정권, 재산권 등을 침해할 우려가 크므로 포괄적으로 이루어져서는 아니되고 비례의 원칙에 따라 필요한 최소한의 범위 내에서 이루어져야 한다." 고 설시하면서 광범위한 압수수색에 대한 우려를 표명한바 있다(대법원 2015. 7. 16자 2011모1839 결정). 미국 연방대법원[Riley v. California, 573 U.S. (2014)]도 2014. 6. 25. 만장일치로 휴대폰에 저장된 전자정보에 대한 압수수색에 관하여 다음과 같이 판결하면서 광범위한 압수수색에 대한 우려를 표시하였다. "휴대폰은 양적으로나 질적으로나 피체포자가 소지하는 다른 유형물과 다르다. 현재 유통되고 있는 휴대폰은 거대한 저장 용량을 가지고 있다. 휴대폰이 존재하지 않던 시기에 피체포자에 대한 수색은 유형물에 국한되었고, 통상적으로 상당히 제한적인 사생활 침해를 야기할 뿐이었다. 그러나 휴대폰은 수백만 페이지의 문자정보(text), 수천 장의 사진 및 수백 편의 비디오를 저장할 수 있다."

하다. 수사기관은 사실관계를 밝혀 형사처벌의 필요성이 있는지를 살펴보아야 할 법적 권한과 의무가 있는데, 관련 정보가 많을수록 정확한 판단을 할 가능성이 높아지기 때문에 자연스럽게 다량의 정보 확보에 강한 동인을 갖게 된다. 이러한 수사기관의 행동양태는 법적 권한과 의무에 기초한 것으로 그 직분에 충실한 것이어서, 이에 대한 사법적 통제가 이루어지지 않으면 수사기관이 광범위한 압수수색으로 나아갈 개연성이 존재한다.

광범위한 압수수색으로 인한 사생활 침해 및 저인망식 수사 등에 대한 우려로 인하여, 법원은 압수수색 영장 재판 과정에서 사법적 통제를 강화하는 경향을 보이고 있다. 그런데 이와 같은 사법적 통제의 강화는 압수수색 영장 발부에 요구되는 혐의에 대한 소명의 수준을 높이는 결과로 이어지게 되고, 이는 전자정보의 훼손 용이성과 맞물리면서 전자정보의 적시 확보에는 부정적 영향을 미치게 된다.

요약하면 전자정보의 압수수색에는, 전자정보의 훼손 용이성으로 인한 '신속한 정보획득'의 필요성이라는 측면과 전자정보의 대량성 및 비가시성으로 인한 '신중한 정보보호'의 필요성이라는 측면이 공존한다. 따라서 전자정보의 압수수색을 위한 사전적 보전조치로서 도입이 논의되고 있는 전자정보 보전처분 제도는 신속한 정보획득과 신중한 정보보호라는 두 가지 목표가 동시에 달성될 수 있도록 설계되어야 한다.

나아가 전자정보 보전처분 제도가 형사절차의 여러 지점에서 폭넓게 활용될 수 있도록 이를 '확장성 있는 제도'로 설계할 필요가 있다. 형사사법 절차의 효율성을 제고할 수 있기 때문이다.

제2절 연구 방법

전자정보 보전처분 제도는 전자정보 압수수색을 위한 사전적 보전조치로서 도입이 논의되고 있다. 이처럼 전자정보 보전처분 제도는 독자적인 목적과 의미를 가지는 것이 아니라 전자정보에 대한 압수수색을 보완하는 제도로서 그 존재 의의를 갖는다. 따라서 전자정보 보전처분 제도를 논의하기에 앞서 '현행 전자정보 압수수색 실무'에 관한 검토가 선행될 필요가 있다.

현행 전자정보 압수수색 실무와 함께 이를 뒷받침하고 있는 대법원의 주요 결정 및 판결을 살펴본다. 대법원은 전자정보의 압수수색에 관한 여러 결정과 판결을 통해 관련 법규를 해석하고 전자정보 압수수색의 원칙을 제시함으로써 압수수색 실무 및 관행에 직접적인 영향을 미치고 있다. 따라서 전자정보 압수수색에 관한 대법원 판례는 전자정보 보전처분 제도를 논의함에 있어 중요한 축이 된다. 더불어 우리의 각종 법률들이 규정하고 있는 전자정보 보관의무를 바탕으로 전자정보 보전조치의 현실적 필요성을 살펴보고, 전자정보 보전처분 제도에 관한 외국 입법례와 제20대 국회에서 논의되었던 전자정보 보전처분 제도의 내용을 분석하여 기존 논의의 내용과 한계를 살펴본다.

기존 논의의 대한 정리를 바탕으로, 신속한 정보획득과 신중한 정보보호라는 두 가지 측면이 조화롭게 융합된 발전된 형태의 전자정보 보전처분 제도를 제시하고자 한다. 이를 위해 전자정보 보전처분 제도에 사용될 수 있는 암호기술들을 소개하고, 이러한 암호기술을 사용하여 전자정보 획득의 신속성을 해치지 않으면서도 신중한 정보보호라는 목표를 달성할 수 있도록 설계된 전자정보 보전처분 제도의 집행절차를 제시한다. 나아가 암호화 방식을 사용함으로써 전자정보 보전처분 제도가 형사절차의 다양한 지점에서 널리 활용될 수 있는 확정성을 갖게 될 수 있음을 살펴본다.

제2장 전자정보의 압수수색 실무

제1절 관련 규정

헌법은 신체의 자유 및 주거의 자유를 선언하면서 압수수색의 법률유보 원칙, 적법절차 원칙 및 영장주의를 명시적으로 규정하고 있고, 여기에 더하여 압수수색은 사생활의 비밀과 자유, 통신의 자유 및 표현의 자유 등 다른 기본권도 침해·제한할 수 있는 대물적 강제처분이므로 비례성 원칙과 최소 침해 원칙이 규정된 기본권 제한의 한계에 관한 일반조항(헌법 제37조 제2항)의 규율도 받는다[4].

이러한 헌법조항을 근거로 형사소송법은 압수수색을 직접적으로 규율하고 있다. 형사소송법은 제106조 내지 제138조에서 수소법원의 압수와 수색에 관한 내용을, 제215조 내지 제218조에서 수사기관의 압수와 수색에 관한 내용을 각각 규정하고 있으며, 수소법원의 압수와 수색에 관한 규정이 수사기관의 압수수색 절차에 준용되고 있다. 형사소송법 규정 중에서 앞으로 전개될 내용과 밀접한 관계가 있는 개별 조문들을 살펴본다.

먼저, 형사소송법 제106조를 살펴본다.

제106조(압수) ① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다. ② 법원은 압수할 물건을 지정하여 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다.

4) 손지영, 김주석, “압수수색 절차의 개선방안에 관한 연구”, 대법원 사법정책연구원, 2014, 24면

③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체 등"이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체 등을 압수할 수 있다. ④ 법원은 제3항에 따라 정보를 제공받은 경우 개인정보 보호법 제2조 제3호에 따른 정보주체에게 해당 사실을 지체 없이 알려야 한다.

제106조의 해석을 둘러싸고 '전자정보 자체를 압수수색 대상으로 볼 수 있는지 여부'에 관하여 견해 대립이 있다.

전자정보 자체가 압수수색의 대상의 될 수 없다고 보는 견해(부정설)는 "압수수색의 대상은 정보저장매체 등 압수물이므로, 저장매체에 저장된 전자정보에 대한 압수수색이 필요한 경우에는 저장매체 그 자체나 출력된 정보 등을 압수수색 대상으로 삼아야 하고, 저장매체와 분리된 전자정보 자체만의 압수수색은 허용될 수 없다"고 주장한다[5]. 주된 근거는 다음과 같다.

형사소송법은 압수수색과 관련하여 전자정보에 대해 다른 유체물과 달리 취급하는 규정을 두고 있지 않으므로 전자정보에 대한 압수수색이든 유체물에 대한 압수수색이든 동일한 법리가 적용되어야 한다. 즉, 형사소송법 제106조 제1항은 압수의 대상으로 유체물을 규정하고 있는데, 전자정보는 무체물이므로 전자정보 자체에 대한 압수는 허용되지 않고, 정보저장매체 등에 대한 압수방법을 규정하고 있는 형사소송법 제106조 제3항도 "압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보

5) 이완규, "디지털 증거 압수 절차상 피압수자 참여 방식과 관련성 범위 밖의 별건 증거 압수 방법", 형사법의 신동향 통권 제48호, 2015. 9., 101 내지 102면; 이경렬, "디지털 정보 관련 압수수색 규정 도입을 위한 전제적 고찰", 성균관법학 21권 2호, 2009. 8., 319면; 전승수, "디지털 정보에 대한 압수수색영장의 집행", 법조 통권 670호, 2012. 7., 252면; 남성우, "휴대용 디바이스에 연관된 전자정보의 압수수색과 영장주의", 사법연수원, 2017년도 법관연수 어드밴스(Advance) 과정 연구논문집(전문분야 소송의 주요쟁점, 조세/상사소송), 74면

저장매체인 경우"라고 규정하여 압수대상으로 유체물을 명시하고 있으며, 정보 자체를 압수대상으로 본 듯한 형사소송법 제106조 제4항은 정보 제공시 이루어지는 통지에 관한 특별규정에 불과하다.[6]

반면에 전자정보 자체가 압수수색 대상의 될 수 있다고 보는 견해(긍정설)는 다음과 같은 이유로 이를 긍정한다.

형사소송법 제106조 제3항은 "기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다"고 규정하고 있고, 형사소송법 제106조 제4항에서는 "법원은 제3항에 따라 정보를 제공받은 경우"라고 규정하여 명시적으로 '정보'라는 용어를 사용하면서 그 압수대상이 전자정보임을 명확히 밝히고 있다. 형법 제48조 제3항이 전자기록 등에 대한 일부 폐기 규정을 신설하여 전자정보 자체의 몰수에 관하여 규정하고 있는데 그러한 몰수대상은 압수를 통해 확보되는 것이므로 당연히 전자정보 자체를 압수대상에 포함시킬 수 있다. 전자정보를 증거로 확보하기 위하여는 그 전자정보를 유체물인 정보저장매체 등에 저장하거나 그 출력물을 압수하는 방법을 사용할 수 밖에 없지만, 이는 무체정보를 압수하기 위한 수단에 불과할 뿐이고 여전히 그 압수대상은 전자정보 그 자체이다.[7]

양 견해 모두 논리적 근거를 갖고 있으나, 대법원은 일련의 사건들에서 확고하게 '전자정보 자체가 압수수색의 대상임'을 전제로 논리를 전개하였고[8], 그러한 대법원 판례에 따라 압수수색 영장 재판을 비롯한 현행 실무는 전자정보 자체를 압수수색 대상으로 삼고 있으므로[9], 전자정보

---

6) 상동

7) 김기준, "전자우편에 대한 증거수집과 관련된 문제점", 해외연수검사 연구 논문집(Ⅱ), 17권, 169면, 원혜욱, "과학적 수사방법에 의한 증거수집-전자증서의 압수·수색을 중심으로", 비교형사법연구(제5권 제2호 특집호), 2003. 12., 174면, 남성우, "휴대용 디바이스에 연관된 전자정보의 압수수색과 영장주의", 사법연수원, 2017년도 법관연수 어드밴스(Advance) 과정 연구논문집(전문 분야 소송의 주요쟁점, 조세/상사소송), 74면

8) 손지영, 김주석, "압수수색 절차의 개선방안에 관한 연구", 대법원 사법정책연구원, 2014, 41면

9) 전자정보의 매체 독립성이라는 측면과 정보의 디지털화라는 방향에 비추어 보아도 전자정보

자체를 압수수색 대상으로 보고 논의를 전개하기로 한다.

다음으로, 형사소송법 제215조를 형사소송법 제106조와 함께 살펴본다.

제215조(압수, 수색, 검증) ① 검사는 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 지방법원판사에게 청구하여 발부받은 영장에 의하여 압수, 수색 또는 검증을 할 수 있다. ② 사법경찰관이 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 검사에게 신청하여 검사의 청구로 지방법원판사가 발부한 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.

형사소송법 제106조와 형사소송법 제215조는 압수수색의 요건으로 '관련성 요건'을 명확하게 제시하고 있다. 형사소송법 제106조 제1항의 '피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여'라는 문구와 형사소송법 제215조 제1, 2항의 '해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여'라는 문구를 통해 형사소송법은 무관정보가 압수수색의 대상이 될 수 없다는 점을 명확히 하고 있는 것이다. 이처럼 무관정보를 압수수색의 대상에서 원천적으로 배제하는 것은 신중한 정보보호의 필요성이라는 측면을 강조한 것이다. 프라이버시를 보호하고 저인망식 수사에 대한 우려를 불식시키기 위해서는 무관정보를 압수수색 실시 단계에서부터 원천적으로 배제하여야 할 필요성이 크기 때문이다.

자체를 압수대상으로 보는 것이 타당하다. 독일 연방헌법재판소가 '형사소송법 제94조는 압수대상을 물건으로 규정하고 있지만 위 조항의 압수대상에는 정보와 같은 무형적인 것도 포함된다' 설시{조대호, "각국의 디지털증거 압수절차 및 증거활용에 관한 연구", 국외훈련검사 연구논문집(Ⅰ) 미국, 793면}한 것도 이와 같은 맥락으로 보인다.

이와 관련하여 대법원은 일관되게 범죄혐의와 관련된 유관정보만을 선별해서 압수하여야 한다는 태도를 견지하면서[10] 혐의사실과의 '관련성'을 바탕으로 한 사법심사(이하 '관련성 통제'라고 한다)를 중시하는 결정과 판결을 계속하여 오고 있다. 여기에서 혐의사실과의 '관련성'은 객관적 관련성, 주관적(인적) 관련성 및 시간적 관련성을 기준으로 판단한다.

① 객관적 관련성은 압수수색 영장에 기재된 혐의사실(기본적 사실관계가 동일하거나 동종·유사의 범행을 포함한다)과 관련된 증거만을 압수하여야 한다는 것을 의미하고, ② 주관적 관련성은, 예를 들어 피의자 갑의 혐의사실에 관한 증거수집을 위하여 제3자인 을의 전자정보 내지 저장매체에 대하여 압수수색영장을 발부할 수 있는지를 살펴보는 문제인데, 을이 갑의 범죄에 대해 공범 내지 교사·방조범으로서 가담한 혐의가 있거나, 피해자 등 해당 혐의사실과 밀접하게 관련된 자가 아닌 한 을의 전자정보나 저장매체에 대한 압수수색 영장은 범죄혐의와 주관적 관련성이 없는 것으로 보며, ③ 시간적 관련성은 혐의사실 발생시점과의 관련성을 고려하여 범죄와 관련될 개연성이 있는 시기의 전자정보만으로 압수수색의 범위를 제한하는 것을 말한다[11].

---

10) 관련성 요건은 2011. 7. 8.자 형사소송법 개정을 통해 명문화되었다. 대법원은 형사소송법 개정 전부터 압수수색 영장에 기재된 범죄혐의와 관련된 유관정보만을 압수하여야 한다고 설시하여 '관련성'을 압수의 요건으로 삼아 왔다. 유관정보만을 선별해서 압수하여야 한다는 대법원 결정의 구체적인 설시 내용은 다음과 같다.
"압수의 목적물인 전자정보가 대용량 저장매체에 무관정보들과 혼재되어 저장되어 있는 경우에 수사기관은 일정한 범위를 정해 탐색하는 등으로 유관정보를 선별하여 복제하거나 출력하는 방법으로 압수수색하는 것이 원칙이고, 저장매체 또는 복제본을 그 소재지에서 외부로 반출하여 압수수색하는 것은 예외적으로만 허용된다. 예외적 방법은 수사기관이 한정된 시간 내에 압수수색 장소에서 유관정보 모두를 탐색하는 것이 현저히 곤란하다는 사정이 있기 때문에 허용되었을 뿐이고, 피압수자측이 저장매체의 외부 반출에 동의한 경우라도 이는 수사인력이 압수수색 장소에서 장시간 체류하는 것에 대한 압박감, 수사를 받고 있는 상황에서 수사기관의 요구를 거부하는 것에 대한 부담감 때문이지 수사기관이 무관정보까지 샅샅이 탐색하여 압수하는데 동의한 것이라고 볼 수는 없다. 물론 법관으로서도 그와 같은 무관정보까지 압수수색할 수 있게 하기 위해 영장을 발부해 준 것은 아니다. 따라서 탐색 결과 무관정보를 압수한 것이 밝혀진 부분에 대해서는 그 자체로 영장주의에 위반하여 위법하게 되는 것이다."(대법원 2011. 5. 26.자 2009모1190 결정 등 참조)

11) 압수수색영장 실무, 대법원 법원행정처, 2016, 73-74면; 대법원 2017. 12. 5. 선고 2017도13458 판결 참조

제2절 압수수색 실무

1. 압수수색 영장

서론에서 본 바와 같이 수사기관이 유관정보와 무관정보가 혼재된 방대한 전자정보를 압수하게 되면 프라이버시 침해는 물론이고 저인망식 수사가 진행될 우려가 있고, 이와 같은 우려를 갖는 것은 법원도 예외가 아니다[12]. 이러한 우려는 압수수색 영장 재판에서의 심사 강화로 이어지고 있다.

법원이 압수수색 영장 발부시 첨부하는 아래와 같은 별지 중 제2항을 보면, 법원의 압수수색 영장에 대한 심사강화 기조를 명확하게 확인할 수 있다. 법원은 압수수색 영장에 별지를 첨부하여 압수대상 및 압수방법을 제한하고 있는데, ① 압수대상과 관련하여 압수목적물란에 '수색·

---

12) 대법원은 관련 결정에서 아래와 같이 상세한 이유를 들어 광범위한 압수수색에 대한 우려를 나타내었다(대법원 2015. 7. 16. 2011모1839 결정 참조).
"압수의 목적물이 컴퓨터용 하드디스크나 휴대전화기 등 전자정보가 저장된 대용량의 저장매체일 경우, 그 안에는 수많은 문서, 동영상, 사진 등이 파일형태로 저장되고, 그 파일을 작성한 시간, 인터넷 접속기록 등이 세세하게 기록되어 있으며, 향후 과학기술이 발전할수록 기존의 법률이 예상조차 할 수 없었던 엄청난 양의 정보가 담기게 될 가능성이 있다. 또한 원격지 서버에 저장되어 있는 정보라도 영장에 기재된 수색장소에서 해당 서버 또는 웹사이트에 접속하여 범죄와 관련된 이메일 등 전자정보를 복제하거나 출력하는 방법으로 하는 압수수색도 가능하다. 이러한 전자정보는 개인의 행동을 시간적, 장소적으로 재구성할 수 있게 할 뿐만 아니라 개인의 내밀한 생각까지 포함하고 있는 경우가 많아 그 보유자가 대체로 타인과 공유하는 것을 원하지 않는 것인데도 그 정보의 무한 복제가 가능하다. 전자정보에 대한 압수수색에 있어서 영장주의의 정신을 살리기 위해서는 전자정보의 이러한 특성에 비추어 보다 세심한 접근이 필요하고, 수사기관이 찾고자 하는 물건이 그 물건의 외적 특성을 통해 구별되거나 문서 사본의 존재가 유한한 종전의 일반적인 물건에 대한 압수수색에 관한 제한 이론만으로는 개인이나 기업의 정보 대부분을 담고 있는 전자정보에 대한 부당한 압수수색으로부터 헌법이 보장하는 국민의 기본적 인권을 보호하고 제대로 지켜 낼 수 없다. (중략) 전자정보는 복제가 용이하여 전자정보가 수록된 저장매체 또는 복제본이 압수수색 과정에서 외부로 반출되면 압수수색이 종료한 후에도 복제본이 남아 있을 가능성을 배제할 수 없고, 그 경우 혐의사실과 무관한 전자정보가 수사기관에 의해 다른 범죄의 수사 단서 내지 증거로 위법하게 사용되는 등 새로운 법익침해를 초래할 가능성이 있으므로, 혐의사실 관련성에 대한 구분 없이 이루어지는 복제·탐색·출력을 막는 절차적 조치가 중요성을 가지게 된다."

검증 후 혐의사실과 관련된 전자정보로 압수대상을 제한함'이라는 문구를 사용하여 압수대상을 유관정보로 명확히 한정하고, ② 압수방법으로 현장에서 선별 압수하는 것을 원칙으로 하되, 예외적인 경우에 한하여 정보저장매체나 복제본의 반출을 통한 현장 외 장소에서의 압수수색을 허용하고 있다.

별지. 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 참여인1)(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 수사기관이 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·복제하는 위 (1)항 기재의 원칙적 압수 방법이 불가능하거나, 압수 목적을 달성하기에 현저히 곤란한 경우에 한하여, 저장매체에 들어 있는 전자파일 전부를 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 때에 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·복제에 의한 집행이 피압수자 등의 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.

2. 관련 판례와 그 함의

가. 관련 대법원 결정 및 판결

대법원은 2011. 5. 26.자 2009모1190 결정을 통하여 전자정보 압수수색에 관한 이정표를 제시하였다[13]. 이 결정은 전자정보에 관한 압수수색 영장 재판에 큰 영향을 미쳤고, 전항에서 본 압수수색 영장에 첨부되는

13) 결정의 주요 내용은 다음과 같다.
"전자정보에 대한 압수수색영장을 집행할 때에는 원칙적으로 영장 발부의 사유인 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 하고, 집행 현장 사정상 위와 같은 방식에 의한 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 존재하더라도 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 반출하여 해당 파일을 압수수색할 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 압수수색영장 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 압수수색영장을 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 피압수수색 당사자나 변호인의 계속적인 참여권 보장, 피압수수색 당사자가 배제된 상태의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수수색 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오남용 및 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야만 집행절차가 적법하게 된다."

별지 역시 위 결정의 영향을 크게 받았다.

대법원은 이 결정을 통해 ① 유관정보만을 선별하여 압수하여야 한다는 '선별 압수 원칙'을 확인하면서 관련성 통제의 중요성을 강조하고, ② 현장에서의 선별 압수를 원칙으로 하되, 예외적인 경우에 한하여 정보저장매체 원본(이하 '정보저장매체'라고만 한다)이나 복제본의 반출을 허용하며, ③ 유관정보와 무관정보를 선별하는 과정에 피압수자측의 참여권이 보장되지 않으면 위법한 압수수색이 된다고 설시하였다. 여기서 대법원은 피압수자측의 참여권을 특히 강조하고 있는데, 이는 선별 압수 원칙의 실효성을 제고하기 위하여 피압수자측의 참여권을 활용하고 있기 때문이다. 즉, 관련성 통제를 피압수자측의 참여권에 상당 부분 의존하는 구조이다.

위 결정의 이유 중에는 정보저장매체나 복제본의 반출과 관련하여 "정보저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수수색 영장 집행의 일환에 포함된다고 보아야 한다"라는 부분이 있는데, 이 부분이 참여권의 보장 범위와 맞물리면서 논란을 야기하였다. 대법원은 정보저장매체(복제본)의 반출과 그 반출 후에 이루어지는 전자정보의 탐색 및 출력·복사가 압수수색 영장 집행의 일환이라는 이유를 들면서 '피압수자측의 계속적인 참여권 보장, 피압수자측이 배제된 상태의 저장매체에 대한 열람·복사 금지 등의 조치가 이루어져야만 압수수색이 적법하다'라고 판단하였는데, 이에 대하여 "정보저장매체나 복제본의 압수로서 압수수색 절차가 종료되므로 압수가 종료된 후에 이루어지는 수사기관의 행위를 압수수색 영장 집행의 일부로 포섭하는 것은 부당하다"는 취지의 반론이 있다[14].

---

14) 전승수, "디지털 정보에 대한 압수수색영장의 집행(대법원 2011. 5. 26.자 2009모1190 결정에 대한 판례평석)"; 이완규, "디지털 증거의 압수수색 개념 및 증거능력 요건", 사법발전재단, 차한성 대법관 퇴임기념 논문집

대법원은 2015. 7. 16.자 2011모1839 결정에서도 위 대법원 2009모1190 결정을 재확인하였다. 특히 유관정보와 무관정보를 선별하는 작업이 이루어지기 전에 반출된 정보저장매체나 복제본에서 전자정보를 탐색하여 압수하려면 피압수자측의 참여권이 보장되어야 한다는 점도 재확인하였다.

한편 대법원은 2018. 2. 8. 선고 2017도13263 판결에서 “수사기관이 압수수색 현장에서 키워드 또는 확장자 검색 등을 통해 유관정보를 선별하여 압수하였다면 이로써 압수의 목적물에 대한 압수수색 절차는 종료된 것이므로, 수사기관이 수사기관 사무실에서 위와 같이 압수된 전자정보를 탐색・복제・출력하는 과정에서도 피압수자측의 참여 기회를 보장하여야 하는 것은 아니다”라고 판시하였다.

나. 위 결정 및 판결의 함의

앞서 본 대법원 판례들은 ‘유관정보만을 압수할 수 있다’는 압수수색의 대전제 하에서 ‘선별 압수 원칙’을 도출하고 이를 실효적으로 보장하기 위한 파생 원칙으로 ‘참여권 보장의 원칙’을 강조함으로써 전자정보 압수수색의 핵심 얼개를 형성하였다는데 그 의미가 있다. 여기에 추가하여 위 대법원 판례들을 통해 전자정보 압수수색 과정에서 일어나는 ‘정보저장매체(복제본) 반출 행위의 법적 성격’을 규명하여 볼 수 있다.

통상적으로 압수수색이라는 표현이 사용되고 있으나, 개별 압수물을 기준으로 볼 때 수색이 선행하고 압수는 후행한다. 이는 전자정보 압수수색의 경우에도 동일한데, 정보저장매체에서 유관정보를 찾는 수색 행위가 앞서고 유관정보를 찾았을 때 그 유관정보를 압수하는 행위가 일어난다. 이처럼 유관정보로 판명되어야 비로소 압수 행위로 넘어갈 수 있으므로, 유관정보인지 여부가 확인될 때까지 이루어지는 수사기관의 행위는 수색 행위에 포섭된다. 이처럼 유관정보와 무관정보를 선별하는 작업이

이루어져야 압수가 이루어질 수 있으므로, 유관정보와 무관정보의 선별이 이루어지지 않은 상태에서 이루어지는 정보저장매체나 복제본의 반출 행위는 전자정보의 압수 행위에 해당한다고 볼 수 없고, 압수 행위에 선행하는 수색 행위의 일부에 해당한다. 보다 정확히 말하면, 정보저장매체나 복제본 반출은 현장에서의 수색 활동이 곤란한 경우에 예외적으로 수색 활동 장소를 변경하기 위한 조치로서 수색 활동의 일환(수색 집행에 필요한 처분)이다. 그리고 유관정보와 무관정보를 선별한 후에 유관정보만을 출력하거나 복제하여 이를 압수하면 압수수색이 종료된다.

위 대법원 결정들은 '유관정보와 무관정보와의 선별이 이루어지지 아니한 상태에서 정보저장매체나 그 복제본이 반출된 것만으로는 압수수색이 종료되지 않는다'는 취지의 설시를 하고 있는데 이는 당연한 설시이다. 정보저장매체나 복제본의 반출은 현장에서의 수색 활동이 곤란한 경우에(현장에서 유관정보와 무관정보를 선별하기 어려운 경우에) 예외적으로 현장이 아닌 다른 장소에서 수색 활동을 실시할 수 있도록 허용하는 '수색 활동을 위한 보전처분'이기 때문이다. 이와 같은 수사기관의 반출 행위가 허용되는 법적 근거는 형사소송법 제120조 제1항, 제219조와 이를 허용하는 내용이 기재된 압수수색 영장이다. 다만 대법원은 관련 결정을 하면서 그 이유에 반출 행위의 법적 성격을 명확히 설시하지 않은 채 다소 모호한 표현을 사용하였다.

위 2017도13263 판결은 '수사기관이 현장 수색 활동을 통해 무관정보와 유관정보를 선별하고 현장에서 유관정보를 저장매체에 담는 방식으로 선별된 유관정보를 압수하게 되면 이로써 전자정보의 압수수색 절차는 종료된 것이므로, 그 후에 수사기관이 압수한 유관정보를 분석할 때에는 피압수자의 참여권을 보장할 필요는 없다'는 취지의 설시를 하고 있다. 이와 같은 설시를 통하여 '수색을 위한 보전처분으로서 정보저장매체나 복제본을 반출하는 행위'와 '선별 작업을 통해 압수된 유관정보를 담고

있는 정보저장매체나 복제본을 반출하는 행위'의 법적 성격이 상이함을 확인할 수 있다.

이처럼 형사소송법에 따라 압수수색 영장의 발부 권한을 가진 법원이 '수색을 위한 보전처분'을 허용하고 있는 이상, 여기서 한 걸음 더 나아가 법률을 개정하여 '압수수색을 위한 보전처분 제도'를 도입하려는 시도는 상당히 자연스럽다. 보전처분으로서, 민사소송법에 보전처분 제도가, 행정법에 집행정지 제도가 규정되어 있는 점에 비추어 보아도 형사소송법에서 전자정보 압수수색을 위한 보전처분 제도를 도입한다고 하여 이례적이라고 평가되지 않는다. 실제로 여러 법제에서 전자정보 보전처분 제도를 도입하고 있다.

3. 압수수색 영장 집행 실무

수사기관은 압수수색 현장에서의 선별 압수가 가능한 경우 디지털 포렌식 도구를 이용하여 조건 검색[15] 등으로 유관정보를 선별한 다음 이를 출력하거나 복사하는 방식으로 압수수색을 실시하고 있다.

압수수색 현장에서의 선별 작업이 곤란하여 정보저장매체나 복제본을 반출하는 경우에는 현장 수사관이 정보저장매체나 복제본을 피압수자측의 참여하에 봉인한 다음 이를 수사기관 사무실이나 디지털 포렌식 센터 등으로 옮긴다. 이후 수사관은 피압수자측이 참여한 상태에서 정보저장매체나 복제본의 봉인을 해제하고 쓰기방지 장치를 부착하여 복제본을 생성한 다음 무관정보와 유관정보를 선별하여 유관정보만을 압수한다. 이렇게 압수수색 절차가 종료되면 수사관은 압수된 유관정보에 대한 분석 작업에 착수하게 된다.

---

15) 검색 조건으로 검색어나 파일의 생성·변경 시점 및 파일 형식 등을 설정하여 유관정보를 선별해 내고 있다.

한편 전자정보 처리를 위한 인적·물적 자원을 보유하고 있는 정보통신서비스 제공자[16] 등은 수사기관으로부터 압수수색 영장을 제시받으면 자신의 서버에서 해당 전자정보를 찾아 이를 수사기관에 제공하고 있다. 이처럼 수사기관이 제3자 보관의 전자정보에 대하여 압수수색 영장을 집행하는 경우 형사소송법 제219조, 제122조 본문에 따라 이를 피의자 등에게 사전통지하여야 하는지 여부에 관하여 논란이 있다. 실무에서는 통상 '급속을 요할 경우에는 예외로 한다'는 형사소송법 제122조 후단을 근거로 삼아 사전통지를 실시하지 않고 있는데, 이러한 실무관행에 대하여 '피압수자의 전자정보 훼손 가능성을 고려하여 보면, 이와 같은 실무 관행이 위법하다고까지는 할 수 없다'는 것이 실무가들의 대체적인 견해인 것으로 보인다. 그러나 정보통신서비스 제공자가 수사기관에 제공하는 정보에 무관정보가 혼재되어 있을 가능성을 배제하기 어렵고, 제3자의 지위에 있는 정보통신서비스 제공자가 무관정보와 유관정보를 선별하는 작업을 적극적으로 수행할 것이라고 기대하기도 어려우므로, 이 경우에도 피의자 등의 참여권이 보장될 수 있는 방안이 강구될 필요가 있다.

16) '정보통신서비스 제공자'의 정의는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 제3호에 규정되어 있는데, 전기통신사업법 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 의미한다.

제3장 전자정보 보전처분 제도의 입법화 및 기존 논의

제1절 전자정보 보전처분 제도의 입법화

1. 사이버범죄방지조약[17]

유럽평의회 사이버범죄방지조약은 사이버범죄에 관한 최초의 국제적 협약으로 사이버범죄에 대한 국제적 공조를 목적으로 2001. 11. 8. 의결되었고 2004. 7. 1. 발효되었으며, 유럽평의회 회원국은 물론 미국과 일본 등 비회원국들도 가입하고 있고, 실체법적인 규정과 절차법적인 규정을 모두 갖고 있다.[18] 여기에서는 전자정보 보전처분 제도와 관련된 제16조와 제17조를 살펴보기로 한다.

사이버범죄방지조약 제16조(저장된 전자정보의 신속한 보전)
1. 컴퓨터시스템에 의해서 저장되어 있는 통신데이터를 포함한 특정한 전자정보가 특히 손실되거나 변경될 수 있다고 믿을 만한 근거가 있는 경우에는 가입국은 이러한 전자정보의 신속한 보전을 자국의 권한 있는 기관이 명령하거나 이와 유사한 방법으로 취득할 수 있도록 필요한 입법적 조치와 그 밖의 조치를 취하여야 한다. 2. 어떤 자가 보유하거나 관리하고 있는 특정한 전자정보를 보전하게 하는 명령을 통하여 제1항을 실행한다면, 가입국은 필요한 만큼의 기간 동안, 최장 90일 동안 그 자가 이러한 전자정보의 무결성을 보전하고 유지하여 이를 권한 있는 기관에게 전달할 수 있도록 필요한 입법적 조치와 그 밖의 조치를 취하여야 한다. 가입국은 그러한 명령이 연속하여 연장

17) Convention on Cybercrime; Budapest Convention
18) 박희영, “사이버범죄방지조약의 형사절차법 규정의 평가와 현행 형사절차법 관련 규정의 개정방향”, 인터넷법률 통권 제46호, 157-158면

될 수 있도록 규정할 수 있다. 3. 각 가입국은 국내법에 의해 규정된 기간 동안 이러한 절차의 수행을 비밀리에 할 수 있도록 보관자 또는 전자정보를 확보해야 할 자에게 의무를 부과하기 위해 필요한 입법적 조치와 그 밖의 조치를 취하여야 한다. (이하 생략) 사이버범죄방지협약 제17조(통신데이터의 신속한 보전과 일부 제출) 1. 각 가입국은 제16조에 의하여 보전되어야 하는 통신데이터와 관련하여, a) 하나 또는 그 이상의 서비스제공자가 당해 통신의 중개에 참여하고 있는지에 관계 없이 통신데이터의 신속한 보전이 가능하도록 하고, b) 가입국이 서비스제공자 및 통신의 전송 경로를 확정할 수 있도록 충분한 양의 통신데이터가 가입국의 관할기관이나 이 기관으로부터 지정받은 자에게 즉시 제출되도록 필요한 입법적 조치와 그 밖의 조치를 취하여야 한다. (이하 생략)

사이버범죄방지조약에 첨부된 설명서(Explanatory Report)에 따르면 위 규정에서의 '보전'이란 저장 중인 전자정보가 향후 변경되거나 삭제되지 않도록 현 상태 그대로 이를 보호하는 것을 의미한다. 보전처분의 특성을 반영하여 위 설명서에 수사기관은 보전처분된 전자정보의 '내용'에 접근할 수 없다는 내용이 명기되어 있다.

전자정보 보전조치의 주체에 대하여 위 규정은 '권한 있는 기관'이라는 표현을 사용하고 있을 뿐이고 이를 구체화하고 있지 않다. 또한 전자정보 보전조치의 대상에 관하여도 '어떤 자가 보유하거나 관리하고 있는 특정한 저장 컴퓨터데이터'라는 표현을 사용하고 있어, 전자정보 보전조치의 대상

자는 '전자정보의 주체나 관리자'로 폭넓게 해석되고 있다. 한편 보전조치의 구체적인 집행 방법에 대하여는 침묵하고 있다.

2. 일본

일본은 사이버범죄방지조약 가입국으로서 동 조약에 따라 형사소송법을 개정하였는데, 그 개정 내용 중에는 사이버범죄방지조약상의 전자정보 보전처분 제도에 대응되는 전자정보 보전처분 제도도 포함되어 있다[19]. 구체적인 내용은 아래와 같다.

형사소송법 제197조 ③ 검찰관, 검찰사무관 또는 사법경찰원은 압수 또는 기록명령부 압수를 하기 위하여 필요한 때에는 전기통신을 하기 위한 설비를 타인의 통신용으로 제공하는 사업을 영위하는 자 또는 자기의 업무를 위하여 불특정 또는 다수의 자의 통신을 매개할 수 있는 전기통신을 하기 위한 설비를 설치하고 있는 자에 대하여, 그 업무상 기록하고 있는 전기통신의 송신원, 송신처, 통신일시 그 밖의 통신이력의 전자적 기록 중 필요한 것을 특정하여 30일을 초과하지 아니하는 기간을 정하여 이를 소거하지 아니하도록 서면으로 요구할 수 있다. 이 경우 해당 전자적 기록에 대하여 압수 또는 기록명령부 압수를 할 필요가 없다고 인정된 때에는 해당 요구를 취소하여야 한다. ④ 전항의 규정에 따라 소거하지 아니하도록 요구하는 기간에 대하여는 특히 필요한 때에는 30일을 초과하지 아니하는 범위 내에서 연장할 수 있다. 다만, 소거하지 아니하도록 요구하는 기간은 총 60일을 초과할 수 없다.

위 조문에 따르면, 전자정보 보전처분의 주체는 수사기관이고, 전자정보

19) 이용, "디지털 증거 수집에 있어서의 협력의무", 2016, 50-57면

보전처분의 대상자는 전기통신사업자나 업무상 전기통신 매개 설비를 갖춘 자이다. 전자정보 보전처분은 임시적으로 전자정보의 보전을 구하는 것이므로 그 전자정보의 '내용'을 입수하기 위해서는 압수수색 영장이 필요하다[20]. 한편 전자정보 보전처분 제도와 관련하여 비용의 부담에 관한 문제제기가 있어 왔는데, 보전기간 동안 발생하는 비용이 전기통신사업자 등에게 부담이 될 수 있다는 지적이다[21].

3. 미국

미국의 저장통신법(The Stored Communications Act; SCA)은 저장된 전자정보(이하 '저장정보'라고 한다)를 획득하는 절차를 마련하고 있는데, 저장정보는 크게 ① 이용자에 관한 기초정보(basic subscriber and session information)[22], ② 이용자에 관한 추가정보(records or other information pertaining to a customer or subscriber)[23], ③ 내용(contents)으로 구분되고, 수사기관은 저장정보를 ① 제공명령(subpoena), ② 사전통지를 동반한 제공명령(subpoena with prior notice to the subscriber or customer), ③ 법원의 제공명령(court order), ④ 사전통지를 동반한 법원의 제공명령(court order with prior notice to the subscriber or customer), ⑤ 수색영장(search warrant)을 받아 확보할 수 있으며, 프라이버시와 밀접한 저장정보일수록 후순위의 방법이 요구된다(수사기관은 전자정보의 보전을 위하여 서비스 제공자에게 최대 90일의 범위 내에서 보전명령을 할 수 있고, 1회에 한하여 이를 연장할 수 있다)[24].

---

20) 손지영, 김주석, "압수수색 절차의 개선방안에 관한 연구", 대법원 사법정책연구원, 2014, 69면
21) 상동
22) 성명, 주소, 가입기간, 전화번호, 결제 관련 정보(신용카드 번호나 계좌번호) 등
23) 이용자에 관한 기초정보를 제외한 이용자에 관한 정보로서 내용(contents)이 아닌 정보를 말하는데, 로그 정보, 기지국 위치 정보 등이 있다.
24) 전현욱, 이자영, "사이버범죄방지조약과 형사절차상 적법절차원칙: 저정된 데이터의 보존 및 일부 공개를 중심으로", 형사정책연구 제25권 제2호, 2014년 여름, 76면

4. 독일

독일 형사소송법은 아래와 같이 '증거대상의 보전을 위한 압수'를 규정하고 있는데, 이는 최초혐의(Anfangsverdacht)의 요건을 갖출 경우에 가능하고, 여기서 최초혐의란 수사절차의 개시를 정당화할 정도의 혐의로서 정확한 사실관계의 구체화를 요하는 것은 아니나 범행이 저질러졌을 가능성을 나타내는 사실적 근거는 필요하며, 압수명령은 원칙적으로는 법원에 의해서만 가능하나, 예외적으로 지체되면 위험한 경우에는 검사와 수사요원에 의해서도 가능하다고 알려져 있다[25].

독일 형사소송법 제94조(증거대상의 보전) ① 증거방법으로서 심리에 중요할 수 있는 대상은 유치하거나 또는 다른 방법으로 보전해야 한다. ② 그러한 대상을 개인이 소지하고 있고 이를 자발적으로 인도하지 않는 때에는 압수를 요한다. 제95조(제출 및 인도의무) ① 전술한 종류의 대상을 소지하고 있는 자는 요구가 있으면 이를 제출하고 인도할 의무가 있다. ② 전항의 의무이행을 거부하는 경우에는 제70조에 규정된 질서벌 및 강제수단을 부과할 수 있다. 단 증언거부권이 있는 자에게는 적용되지 않는다.

이처럼 독일에서는 긴급한 경우 수사기관이 자체 판단으로 압수수색을 실시할 수 있으므로 전자정보 보전처분 제도의 필요성이 비교적 크지 않은 것으로 보인다. 그러나 우리의 경우에는 헌법 제12조 제3항에서 사전영장

25) 손지영, 김주석, "압수수색 절차의 개선방안에 관한 연구", 대법원 사법정책연구원, 2014, 150면

주의를 규정하고 있으므로[26], 전자정보 압수는 긴급한 상황인지 여부와 관계 없이 압수수색 영장을 발부받아 실시하여야 한다. 따라서 독일과 같은 방식으로 압수수색 관련 제도를 운용하는 것은 어려워 보인다.

제2절 우리 사회의 도입 논의

1. '전자정보 보관의무 부과' 상황

우리의 경우 일부 전자정보에 대하여 법률상 보관의무가 부과되어 있는데 그 구체적인 내용은 다음과 같다.

먼저, 통신 관련 전자정보에 대하여 법률상 보관의무가 부과되어 있다. 통신비밀보호법 제15조의2에 따르면, 전기통신사업자는 검사・사법경찰관 또는 정보수사기관의 장이 전기통신사업법에 따라 집행하는 통신제한조치 및 통신사실 확인자료제공의 요청에 협조하여야 한다. 또한 통신제한조치의 집행을 위하여 전기통신사업자가 협조할 사항과 통신사실확인자료의 보관기간 그 밖에 전기통신사업자의 협조에 관하여 필요한 사항은 대통령령으로 정하도록 규정되어 있다. 이에 동법 시행령 제41조는 동법 제15조의2에 따라 '전기통신사업자는 살인・인질강도 등 개인의 생명・신체에 급박한 위험이 현존하는 경우에는 통신제한조치 또는 통신사실 확인자료 제공 요청이 지체없이 이루어질 수 있도록 협조하여야 한다'고 규정하면서 ① 가입자의 전기통신일시, 전기통신개시・종료시간, 발・착신 통신번호 등 상대방의 가입자번호와 사용도수는 12개월간[27] 보관하고, ② 컴퓨터 통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터

---

26) 체포・구속・압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다. 다만, 현행범인 경우와 장기 3년 이상의 형에 해당하는 죄를 범하고 도피 또는 증거인멸의 염려가 있을 때에는 사후에 영장을 청구할 수 있다.

27) 다만, 시외・시내전화역무와 관련된 자료인 경우에는 6개월로 한다.

통신 또는 인터넷의 로그기록 자료와 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료는 3개월간 보관하도록 정하고 있다.

다음으로, 금융거래 관련 전자정보에 대하여 법률상 보관의무가 부과되어 있다. 전자금융거래법 제22조에 따르면, 금융회사 등은 전자금융거래의 내용을 추적·검색하거나 그 내용에 오류가 발생할 경우에 이를 확인하거나 정정할 수 있는 기록을 생성하여 5년의 범위 안에서 대통령령이 정하는 기간 동안 보존하여야 하고, 금융회사 등이 보존하여야 하는 전자금융거래기록의 종류, 보존방법, 파기절차·방법 및 상거래관계가 종료된 날의 기준 등은 대통령령으로 정하도록 규정하고 있다. 이에 동법 시행령 제12조가 보전의무에 관한 구체적인 사항을 정하고 있는데, 중요 전자금융거래내역에 대하여 5년간의 보존의무가 부과되고 있다. 또한 자본시장과 금융투자업에 관한 법률 제60조에 따르면, 금융투자업자[28]는 금융투자업 영위와 관련한 자료를 대통령령으로 정하는 자료의 종류별로 대통령령으로 정하는 기간 동안 기록·유지하여야 한다. 이에 동법 시행령 제62조가 보전의무에 관한 구체적인 사항을 정하고 있는데, 주요 자료에 관하여 3년 내지 10년간의 기록유지 의무를 정하고 있다.

이처럼 통신 관련 전자정보는 보관기간이 그리 길지 않고, 보관의무가 부과되는 통신 및 금융거래 관련 전자정보의 범위도 제한되어 있다. 그 결과 상당 부분의 통신 및 금융 관련 전자정보가 훼손될 가능성이 있다. 더욱이 위와 같은 일부 전자정보에만 보관의무가 부과되어 있을 뿐이고, 그 외의 전자정보에는 보관의무가 아예 부과되고 있지 않아, 현재 생성·저장·유통되고 있는 전자정보의 상당 부분은 쉽게 훼손될 수 있는 상

28) 자본시장과 금융투자업에 관한 법률 제6조 제1항이 규정하고 있는 "금융투자업"이란 이익을 얻을 목적으로 계속적이거나 반복적인 방법으로 행하는 행위로서 투자매매업, 투자중개업, 집합투자업, 투자자문업, 투자일임업, 신탁업의 어느 하나에 해당하는 업을 말한다.

태에 놓여 있다. 이러한 현실 상황을 고려하여 우리 국회에서 전자정보 보전처분 제도의 도입이 논의된 바 있다. 항을 바꾸어 살펴본다.

2. 전자정보 보전처분 제도의 도입 시도

제20대 국회에 제출된 형사소송법 일부 개정안[29]이 전자정보 보전처분 제도를 담고 있었는데, 위 개정안은 임기 만료로 폐기되었다. 위 개정안의 구체적인 내용을 살펴보고, 이를 두고 이해관계자들이 어떠한 의견을 개진하였는지에 관하여 본다.

가. 개정안의 내용

형사소송법 개정안은 법원을 보전처분의 주체로, 정보통신서비스 제공자를 보전처분의 대상자로 규정하고 있었다. 그 개정안에 규정되어 있던 구체적인 내용은 아래와 같다.

형사소송법 개정안 제108조의2(정보의 보존요청 등) ① 법원은 정보를 압수할 필요가 있는 경우 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 제1항 제3호에서 정한 정보통신서비스 제공자에게 30일의 범위 내에서 당해 정보가 삭제·변경되지 않도록 보존할 것을 서면으로 요청할 수 있다. 다만, 상당한 이유가 있다고 인정되는 경우 30일의 범위 내에서 1회에 한해 연장할 수 있다. ② 제1항의 경우 당해 정보를 압수할 필요가 없다고 인정되는 때에는 지체없이 보존 요청을 취소하여야 한다.

29) 의안번호 2001352, 제안일자 2016. 8. 2., 제안자 김도읍, 정갑윤, 권성동, 김성원, 경대수, 김태흠, 권석창, 홍철호, 이우현, 성일종 의원(10인)

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 이 법에서 사용하는 용어의 뜻은 다음과 같다. ① "정보통신서비스 제공자"란 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다. 전기통신사업법 제2조 6. "전기통신역무"란 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말한다. 8. "전기통신사업자"란 이 법에 따라 등록 또는 신고(신고가 면제된 경우를 포함한다)를 하고 전기통신역무를 제공하는 자를 말한다.

나. 이해관계자들의 의견

국회 법제사법위원회 수석전문위원은 검토보고를 통해 “위 개정안은 정보통신서비스 제공자에 대하여 정보 보존요청을 할 수 있도록 함으로써 증거가치 있는 정보의 상실을 방지하려는 취지”[30]라고 밝히면서 아래와 같은 개정안의 문제점을 지적하였다.

개정안은 법원의 정보 보존요청에 대하여 정보통신서비스 제공자의 보존의무를 규정하고 있지 않아 정보통신서비스 제공자가 법원의 보존요청을 거부할 경우 제도의 실효성이 반감될 우려가 있다고 봄. 정보통신서비스 제공자가 정보 보존을 위하여 지출한 비용을 보전하여 주는 등 협력을 이끌어 낼 수 있는 방안을 마련할 필요가 있음[31].

법원(법원행정처)는 위 개정안에 대하여 아래와 같은 내용의 의견을 국회에 전달하면서 반대의사를 표시하였다.

개정안은 보존요청의 요건으로 ‘압수할 필요가 있는 경우’를 규정하고

30) 법제사법위원회 수석전문위원 남궁 석, 형사소송법 일부 개정 법률안(김도읍 의원 대표발의, 제1352호) 검토보고, 2016. 11., 13면
31) 위 검토보고(각주 28), 13면

있는데, 압수할 필요가 있는 경우에는 압수영장을 발부·집행하면 족하고 별도로 정보통신서비스 제공자에게 보존요청을 할 필요성이 있는지 의문이고, 전기통신서비스 사업자에게 불필요한 부담을 지울 수 있다는 점을 들어 보존요청 제도의 도입에 반대함. 보존요청 제도를 도입한다 하더라도, 보존요청 제도의 취지는 압수수색 영장 청구를 하기 전에 해당 압수수색 영장 청구를 위한 시간적 여유를 확보하는 데 있으므로 보존기간은 1주일 정도의 시간이면 충분하고, 수사기관의 남용 가능성에 대한 사법적 통제가 필요하므로 제도를 도입한다 하더라도 통신비밀보호법상 통신사실 확인자료제공요청 허가와 같이 법원의 허가를 받도록 할 필요가 있음[32].

대한변호사협회는 위 개정안에 대하여 "법원의 정보 보존요청은 영세한 기업들에게는 상당한 업무상 부담이 있으므로, 정보 보존요청제도의 적용범위를 일정 규모 이상의 정보통신서비스 제공자로 한정할 필요가 있다"[33]는 의견을 제시하였다.

위 의견들을 종합하여 보면, 공통적으로 보전의무를 이행하여야 하는 제3자에게 부담이 가해질 수 있다는 점을 언급하고 있다. 특히 대한변호사협회는 보전의무를 이행하는데 필요한 인적·물적 자원이 부족할 수 있는 영세업자들에게 상당한 부담이 될 수 있다는 점을 지적하고 있다. 이는 전자정보 보전처분 제도의 실효적인 이행 가능성에 의문을 제기하는 것으로 전자정보 보전처분 제도를 설계함에 있어 감안되어야 할 점이다.

나아가 위 개정안에 따르면 전자정보 보전처분과 압수수색 사이의 차이가 모호할 수 있다는 법원의 문제제기도 고려해 보아야 한다. 위 개정안은 신속한 정보획득의 측면을 받아들여 전자정보 보호처분 제도를

32) 위 검토보고(각주 28), 13면
33) 위 검토보고(각주 28), 14면

도입하면서도, 신중한 정보보호의 측면도 감안하여 '압수 필요성'이라는 요건을 추가함으로써 사법적 통제를 강화하려고 한 것으로 보인다. 그런데 위 개정안에 따르면 전자정보 보전처분 과정에서 법원이 압수 필요성이라는 요건을 심사하여야 되는데, 그렇게 되면 전자정보 보전처분과 압수수색이 거의 동일한 모습을 갖게 된다. 그렇다면 굳이 개정안이 제시하고 있는 형태의 전자정보 보전처분 제도를 도입할 필요성이 있는지에 대해 의문이 드는 것은 당연하다.

제4장 공개키 암호를 활용한 전자정보 보전처분 제도의 도입

제1절 전자정보 보전처분 제도에 관한 기존 논의의 한계

1. 기존 논의의 내용 및 한계

제3장에서 본 바와 같이 기존에 논의되어 온 전자정보 보전처분 제도는 '신속한 전자정보 확보'라는 측면에 기반하고 있다. 전자정보가 훼손될 우려가 있는 경우 압수수색을 실시하기 전에 미리 전자정보에 대한 보전처분을 실시할 실무적 필요성이 크다는 것이다. 이처럼 실무적 필요에 따라 해외에서 이미 도입되었거나 도입 논의가 진행 중인 전자정보 보전처분 제도는 '압수수색을 위한 보전처분'으로서의 법적 성격을 갖는다. 한편 제2장 제2절에서 본 바와 같이 법원은 압수수색 영장을 발부하면서 수색을 위한 임시조치로서 정보저장매체나 복제본의 반출을 허가하고 있는데, 이 역시도 법적으로 '수색을 위한 보전처분'의 성격을 갖는다. 이처럼 영장을 발부하는 법원(法院)의 허가에 따라 수색을 위한 보전처분도 이루어지고 있는 현실에서, 법원(法源)인 법률 차원에서 압수수색을 위한 보전처분 제도(전자정보 보전처분 제도)를 도입하는 것에 어떠한 법적인 문제가 있다고 보기 어렵다. 나아가 우리 헌법은 '기본권은 법률로 제한할 수 있다'고 규정하고 있으므로, 전자정보 보전처분 제도를 포함한 압수수색을 위한 보전처분이 법률에 근거하여 실시되는 것이 바람직하다.

사전적·잠정적 처분인 '보전처분의 특성상' 압수수색 영장이 발부되기 전에는 수사기관이 보전처분된 전자정보의 내용에 접근할 수 없어야 한다. 이와 같은 전자정보 보전처분의 필요조건을 충족시키고자, 기존의 전자정보 보전처분 제도는 그 대상자를 제3자 중 일정 규모 이상의 정보통신사업자로 국한하는 경향성을 보이고 있다. 구체적인 이유를 아래에서 살펴본다.

보전처분의 특성상 압수수색 영장이 발부되기 전에는 수사기관이 보전처분된 전자정보의 내용에 접근할 수 없어야 하기 때문에, 기존 논의는 '전자정보 보전처분 단계에서 전자정보의 주체나 보관자는 수사기관에게 해당 전자정보를 넘기지 않고 자신이 스스로 해당 전자정보를 계속 보유·보관하면서 그 전자정보의 현상을 그대로 유지할 의무를 부담하는 방식'으로 제도를 설계하였거나 설계하고 있다.

그런데 이와 같은 방식으로 전자정보 보전처분 제도를 설계하게 되면, 먼저 피혐의자에 대한 전자정보 보전처분은 상정하기 어렵다. 피혐의자에 대한 전자정보 보전처분이 이루어진다고 하더라도 피혐의자가 본인에게 불리한 전자정보를 현상 그대로 보전하기를 기대하기는 어렵고, 이를 훼손하더라도 증거인멸죄가 성립하지 않아 법적인 제재를 가하는 것도 어렵기 때문이다. 따라서 기존 논의는 통상 피혐의자를 전자정보 보전처분의 대상자에서 아예 제외하여 왔다. 피혐의자에 대한 전자정보 보전처분은 실효성이 없다고 보는 것이다.

또한 제3자에 대한 전자정보 보전처분에 있어서도, 기존 논의는 영세한 기업이나 개인을 전자정보 대상자에서 제외하고 일정 규모 이상의 정보통신사업자 등으로 대상자를 한정하는 경향을 보이고 있다. 일정 규모 이상의 정보통신사업자 등과는 달리 영세한 기업이나 개인은 인적·물적 자원의 부족으로 인하여 해당 전자정보를 보전할 능력이 없다는 이유이다. 보전처분을 이행할 능력이 부족한 자를 상대로 법적인 보전의무를 강제하는 것은 현실성이 떨어질 뿐만 아니라 부적절하다는 점을 고려한 것으로 보이는데, 앞서 본 바와 같이 제20대 국회에서 형사소송법 개정안을 심사할 당시 대한변호사협회도 국회에 이러한 취지의 의견을 전달하였다. 일본 형사소송법이 전자정보 보전처분 대상자를 전기통신사업자나 업무상 전기통신 매개 설비를 갖춘 자로 제한하고 있는 것도 이러한 맥락으로 보인다.

이처럼 전자정보 보전처분 대상자에서 피혐의자와 일정 규모 이하의 기업 및 개인을 제외하고 나면, 전자정보 보전처분 대상자의 범위는 현저히 축소된다. 그러나 서론에서 기술한 바와 같이 피혐의자가 자신에게 불리한 전자정보를 적극적으로 훼손하는 경우가 적지 않을 뿐만 아니라, 일정 규모의 이하의 기업이나 비영리법인 및 단체 등이 보유하고 있는 전자정보도 훼손되기 전에 확보하여할 필요성이 있다. 그럼에도 불구하고 '수사기관이 전자정보 보전처분 단계에서 전자정보의 내용에 접근할 수 없어야 한다'는 필요조건을 충족시키고자, 전자정보 보전처분 대상자가 해당 전자정보를 스스로 보전하는 것을 제도 설계의 전제로 삼아, 제3자 중 보관능력이 있는 자로 전자정보 보전처분 대상자를 제한하는 방식으로 전자정보 보전처분 제도를 설계·운용하고 있는 것이다.

2. 전자정보 보전처분 대상자의 확장을 위한 기술적 조치 가능성

전자정보 보전처분 대상자의 확장 가능성을 타진하여 보기 위하여 전자정보 보전처분 제도의 필요조건을 면밀히 살펴본다. 전자정보 보전처분 제도의 필요조건은 보전처분의 성격상 "전자정보 보전처분 단계에서는 수사기관이 전자정보의 '내용'에 접근할 수 없어야 한다"는 것이다. 이러한 필요조건을 만족시키기 위하여 기존 논의는 해당 전자정보의 주체나 보관자가 스스로 그 전자정보를 보전하는 방식을 고수하고 있다.

그런데 수사기관이 해당 전자정보의 주체나 보관자로부터 보전처분된 전자정보를 넘겨받더라도 전자정보의 내용에는 접근할 수 없도록 기술적 조치를 취할 있다면, 그와 같은 기술적 조치를 전제로 '수사기관이 피혐의자나 일정 규모 이하의 기업 및 개인으로부터 해당 전자정보를 위탁받아 이를 보전하는 방식'으로 전자정보 보전처분 제도를 설계·운용함으로써 전자정보 보전처분 대상자를 확장할 수 있다는 결론에 이르게 된다.

요약하면, 전자정보 보전처분 대상자 확장의 문제는, 전자정보 보전처분 단계에서 수사기관에 전자정보를 맡기되, 수사기관이 그 전자정보의 내용에는 접근할 수 없도록 기술적 조치를 취할 수 있는지 여부에 달려 있다. 이러한 기술적 조치로써 암호기술의 도입을 제안하고자 한다.

제2절 공개키 암호기술의 도입

1. 압수수색 과정에서의 암호기술

압수수색 과정에서 암호기술을 활용하는 것은 새로운 아이디어가 아니다. 앞서 본 압수수색 영장의 별지 중 '전자정보 압수시 주의사항' 부분에는 이미 다음과 같은 기재가 있다.

"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."*

암호기술은 압수수색에 활용할 수 있는 유용한 도구이다. 왜냐하면 전자정보 저장매체에 대한 물리적 봉인 방법으로는 수사기관의 임의 접근을 근본적으로 방지할 수 없는 한계가 존재하기 때문이다. 수사기관과 피압수자측이 서로를 신뢰할 수 없는 상황에서 암호기술은 쌍방의 임의 접근을 기술적으로 불가능하게 함으로써 수사기관과 피압수자측 모두 수긍할 수 있는 방식으로 해당 전자정보가 증거로 확보될 수 있게 한다. 이러한 암호기술은 아래와 같이 대칭키 암호방식과 공개키 암호방식으로 크게 나눌 수 있다.

가. 대칭키 암호방식

대칭키 암호방식은 암호화와 복호화에 동일한 키를 이용하는 방식으로 과거부터 널리 활용되어 온 암호방식이어서 이를 이해하는데 별다른 어려움이 없다. 암호화와 복호화에 동일한 암호키를 사용하기 때문에 대칭키 암호방식에서는 암호화하는 자와 복호화하는 자가 사전에 암호키를 공유하여야 하는 어려움(이하 '암호키 공유 문제'라고 한다)이 존재한다. 또한 암호화할 사건이 증가할수록(또는 암호화에 개입하는 인원이 증가할수록) 거기에 비례하여 관리하여야 하는 암호키의 수가 증가하는 어려움도 존재한다.

나. 공개키 암호방식

공개키 암호방식은 암호키 공유 문제를 해결하기 위하여 고안된 암호기술이다. 1970년대에 등장한 공개키 암호방식은 단방향 함수(one-way function)의 특성을 활용하는데[34], 누구든지 공개된 암호키를 이용하여 암호화할 수 있으나 복호화는 복호화키를 소지하고 있는 자만이 할 수 있도록 설계되어 있다. 여기서 단방향 함수란 일방향에서는 계산이 용이하나 타방향에서는 계산이 어려운 함수를 의미하는데, 소인수분해 함수가 대표적인 예이다. 아주 큰 두 개의 소수를 곱하는 것은 그리 어렵지 않으나 그 곱셈의 결과를 두고 역으로 소인수분해하는 것은 극히 어렵다. 이러한 소인수분해 함수는 공개키 암호방식의 대표격인 RSA 암호방식에서 활용되고 있다. 이러한 공개키 암호방식은 대칭키 암호방식과 함께 사용되고 있다. 이를 하이브리드 암호화 방식(Hybrid Encryption)이라고도 부르기도 하는데, 효율성을 제고하기 위하여 사용된다. 시간과 데이터량의 측면에서 보면 대칭키 암호방식이 공개키 암호방식보다 효율적이기 때문에, 대량의 전자정보를 암호화할 때에는 대칭키 암호방식을 사용하고, 대칭키의 교환 등과 같은 중요 전자정보의 전달에만 공개키 암호방식을 사용하는 것이다.

34) 최초의 공개키 암호방식은 RSA이다. 현재 공개키 암호방식은 웹 프로토콜, 인터넷 상거래 등에서 널리 활용되고 있다.

2. 압수수색에서의 암호기술에 관한 기존 논의

압수수색에 암호기술을 접목하는 방법에 대한 논의가 계속되어 오고 있다. 특히 피압수자의 참여권 보장과 관련하여 '수사기관이 피압수자에게 참여권을 보장하지 아니한 채 임의로 반출 전자정보에 대한 불법 수색 및 압수를 실시할 수 없도록 하는 기술적인 조치'로써 암호기술의 사용이 집중적으로 논의되어 오고 있다. 그 중 대표적인 논의를 살펴봄으로써 전자정보 보전처분 제도에 암호기술을 활용할 수 있는 방법을 모색해 본다.

가. 이론적 구성

1) 수사기관과 피압수자가 동시에 암호화에 참가하는 방식

앞서 본 압수수색 별지에 "봉인 및 개봉은 물리적인 방법 또는 수사기관과 피압수자 등[35] 쌍방이 암호를 설정하는 방법 등에 의할 수 있고" 라는 내용으로 암호화가 언급되고 있다. 여기서 언급되고 있는 암호화가 수사기관과 피압수자가 동시에 암호화에 참가하는 방식(이하 '당사자 동시 암호화 방식'이라 한다)이다. 이 경우 피압수자가 복호화에 협조하지 않는 이상 수사기관이 임의로 전자정보에 접근할 수 없다. 그 결과 피압수자의 참여권이 보장되지 않는 상황에서는 수사기관이 임의로 전자정보의 내용에 접근할 수 없으므로 피압수자의 참여권이 확실히 보장된다. 그런데 실무적으로 당사자 동시 암호화 방식을 어떻게 설계할 수 있을 것인지는 분명하지 않다(이에 대한 구체적인 내용은 아래 나.항 '실무적 방안' 부분에서 후술한다). 나아가 이 방식을 사용할 경우에 논리필연적으로 피압수자의 참여 거부 등 피압수자가 압수수색에 비협조적인 경우에는 압수수색 자체가 이루어질 수 없는 중대한 단점이 존재한다. 따라서 당사자 동시 암호화 방식을 그대로 실무에서 활용하기는 쉽지 않다.

---

35) 별지에 따르면, 피압수자 등은 피압수자 또는 형사소송법 제123조에 정한 참여인을 의미한다.

2) 수사기관, 피압수자 및 제3자가 암호화에 참여하는 방식

당사자 동시 암호화 방식의 단점을 보완하기 위하여, 암호화에 제3자를 참여시켜 제3자의 암호키로 피압수자의 암호키를 대신할 수 있게 하는 방식(이하 '삼자 구도 방식'이라 한다)이다[36]. 위 방식에 따르면, 수사기관과 피압수자 및 제3자가 암호화에 참여하여 각자의 암호키로 암호화하되, 3개의 암호키 중에서 2개의 암호키만 있으면 암호를 풀 수 있도록 하는 Shamir의 '임계 암호기술'을 활용하며, 이 경우 수사기관은 단독으로 해당 전자정보에 접근할 수 없고, 동시에 피압수자가 압수수색 자체에 협조하지 않는 상황에서는 제3자의 암호화키를 사용하여 압수수색을 실시할 수 있으므로 당사자 동시 암호화 방식의 단점을 해결할 수 있다.

나. 실무적 방안

1) 당사자 동시 암호화 방식에 기반한 방안

당사자 동시 암호화 방식에 기초하여 '수사기관과 피압수자가 각자의 암호키로 해당 전자정보를 암호화하고 그 암호화된 자료와 암호키들을 제3의 중립적인 기관에 보관하는 내용'의 실무적 방안[37](이하 '강상형 방안'이라 한다)이 제안된 바 있다. 그런데 이 방안은 복제본 반출시 복제본을 암호화하는 방안으로 제시된 것은 아니고, 유관정보의 선별이 종료된 후부터 복제본이 삭제·폐기될 때까지 수사기관이 그 복제본을 임의로 압수수색할 수 없도록 방지하는 기술적 조치로서 제시되었으나[38], 이 방안은

36) 강석한, "전자정보 압수수색에서의 참여권 보장을 위한 기술적 조치 연구 - 임계 암호기술을 이용하여", 2017, 서울대학교 석사학위논문

37) 강상형, "사생활 정보를 고려한 디지털 증거처리 모델", 2016, 디지털포렌식연구, 10(1), 21 내지 37면{이하 '강상형(2016)'이라 한다}

38) 무관정보와 유관정보의 선별을 통해 유관정보만이 압수되면 그 즉시 나머지는 폐기하여야 하는 것이 원칙이므로 유관정보의 압수 후에 이루어지는 나머지 정보의 보관은 위법이다. 따라서 강상형 방안은 위법 상황을 전제하고 있는 것으로 보이기는 하나, 이 방안에서 논의되는 기술적 조치를 참여권 보장을 위한 기술적 조치로서 전용할

복제본의 반출시의 참여권 보장을 위한 기술적 조치로 사용될 수 있는 여지가 있다. 그 결과 참여권 보장을 위한 기술적 조치의 하나로서 인용되어 오고 있다.

강상형 방안에 따르면, 전자정보를 암호화로 봉인할 필요가 있는 경우 수사기관과 피압수자측은 각각 암호화하여 이를 봉인하고 중립적인 기관에 암호화로 봉인된 전자정보를 보관한다. 이후 수사기관과 피압수자의 동의하에 이를 열람할 수 있게 한다. 피압수자측이 복호화에 동의하지 않을 경우 수사기관은 법원에 열람을 청구하는 절차를 거치게 되고, 법원의 승인이 있는 경우 중립적인 기관이 강제로 복호화한다.

이 방안은 암호기술을 압수수색에 접목하려고 한 측면에서 상당한 의미가 있으나, 현재 존재하지 않는 제3의 중립기관을 상정하고 있어 현실성이 떨어진다는 문제를 내포하고 있다. 더욱이 강상형 방안은 '전자정보를 암호화로 봉인할 필요가 있는 경우 수사기관과 피압수자측은 각각 암호화하여 이를 봉인한다'고 제안하고 있는데, 이러한 제안을 기술적으로 구현하는 방법에 대하여는 제대로 밝히지 않은 채 수사기관과 피압수자측이 Secret Sharing System을 사용하여 더욱 안전하게 봉인할 수 있다고 설명하고 있다. 그런데 현실적으로 각자의 암호키로 전자정보를 독립적으로 암호화하는 것은 성립하기 어렵고, 상정할 수 있는 구현방법은 예를 들어 수사기관과 피압수자측이 각각 생성한 128비트 키를 암호 프로그램에 입력하여 암호 프로그램이 이들을 조합하여 하나의 암호키를 만들어(2개의 키를 Exclusive OR 시키는 것이 하나의 예이다) 그 암호키로 전자정보를 암호화하게 하고, 수사기관과 피압수자는 각자가 생성한 키를 중립기관에 보관하는 방법이 있을 수 있는데, 강상형 방안에서는 수사기관과 피압수자측의 Secret Sharing System 활용이 언급되고 있어 강상현 방안의 구체

수 있으므로, 그와 같은 전용을 염두에 두고 기술적 조치에 초점을 맞추어 이 방안을 살펴본다.

적인 기술적 구현방법은 위 논문만으로는 유추해 보기도 쉽지 않다. 나아가 위 방안에 대하여 제3의 중립기관에서의 전자정보 유출 위험을 문제삼는 견해도 있다[39]. 여러 모로 위 방안을 현행 실무에 그대로 적용하기는 어려울 것으로 보인다.

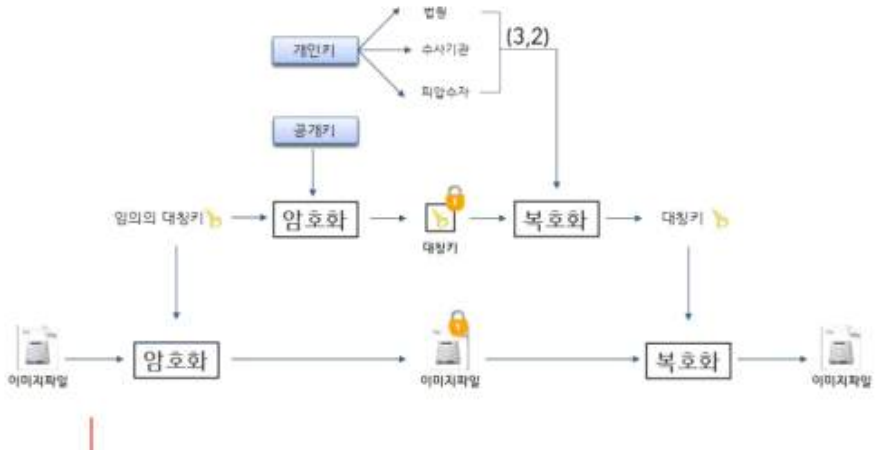
2) 삼자 구도 방식에 기반한 방안

삼자 구도 방식에 임계 암호기술과 공개키 암호기술을 접목시킨 방안(이하 '강석한 방안'이라 한다)도 제시되고 있다[40]. 강석한 방안에 따르면, 해당 사건을 위하여 공개 암호방식에 따른 개인키(비밀키)와 공개키 한 쌍을 만든 다음 개인키를 Shamir의 임계 암호 방식에 따라 3개의 조각으로 나누고, 3개의 조각 중 첫 번째 조각은 수사기관, 두 번째 조각은 피압수자, 그리고 마지막 세 번째 조각은 법원 또는 제3의 신뢰기관이 하나씩 나누어 갖는다. Shamir 임계 암호 방식에 따라 3개의 조각 중 2개의 조각이 모이면 개인키를 복원할 수 있다. 이제 전자정보의 압수수색에 참여하는 수사관에게 암호화 프로그램과 공개키를 제공한다. 수사관은 반출 대상 전자정보가 결정되면, 암호화 프로그램으로 대칭키를 자동 생성하여 반출 대상 전자정보를 대칭키로 암호화하고 그 대칭키는 다시 공개키로 암호화한다. 이 경우 반출 대상 전자정보에는 사건 관련 정보를 포함한 포괄적인 정보가 포함될 수 있다. 이후 암호화된 전자정보를 수사기관 서버에 업로드하여 보관하고, 인증된 사용자에게만 위 서버에 접속하여 암호화 된 전자정보를 내려 받을 수 있도록 한다. 이제 수집된 전자정보로부터 사건 관련 데이터를 선별하기 위해 선별 과정에 피압수자의 참여를 요청한다. 이때 피압수자가 선별 과정에 참여하면, 수사기관의 키 조각과 피압수자가 가지고 있는 키 조각을 Shamir 임계 암호 방식에 따라 조합하여 개인키를 복구한다. 그리고 복구된 개인키로 상기 공개키로 암

39) 강석한, "전자정보 압수수색에서의 참여권 보장을 위한 기술적 조치 연구 - 임계 암호기술을 이용하여", 2017, 서울대학교 석사학위논문, 46면
40) 위 논문

호화된 대칭키를 복호화하여 평문 대칭키를 구하고, 다시 대칭키로 암호화된 반출 대상 전자정보를 복호화한다. 이를 통하여 수사기관과 피압수자는 평문 상태의 반출 대상 전자정보에서 사건 관련 정보를 선별하는 선별 작업을 할 수 있다. 그러나 상기 과정에서 수사기관의 참여 요청에도 불구하고 피압수자가 선별 과정에 참여하지 않으면, 수사기관은 단독으로 개인키를 복구할 수 없으므로 나머지 한 조각을 가지고 있는 법원 또는 제3의 신뢰기관의 협조를 얻어 Shamir 임계 암호방식에 의해 개인키를 복구할 수 있다. 이렇게 복구된 개인키를 이용하여 수사기관은 암호화된 대칭키를 복호화하고 다시 대칭키로 암호화된 반출 대상 전자정보를 복호화하여, 피압수자의 참여 없이 단독으로 선별 작업을 한다.

강석한 방안에 따르면, 법원은 피압수자가 참여를 거부한 경우에 수사기관의 단독열람을 허용할 것인지 여부를 결정하는 역할을 수행하는데, 먼저 피압수자의 참여 거부 의사를 확인하고 압수수색이 영장에서 허용하는 방법과 절차에 따라 이루어졌는지를 심사한 다음에 법원 몫의 개인키 조각을 사용할 것인지를 결정하게 되며, 이를 도식화하여 아래와 같이 제시하고 있다.



그런데 강석한 방안은 대칭키를 생성하는 시점, 대칭키 생성 방법, 암호화 프로그램 내에서 대칭키가 노출될 가능성에 대한 보호 대책 등을 구체적으로 제시하지 않고 있다. 뿐만 아니라 개인키를 누가 어떻게 공정하게 나누어 가질 것인가에 대해서도 언급이 없다. 가장 간명한 방법은 법원이 개인키를 3조각으로 나누어 분배하는 것인데, 이 경우 법원이 수사기관은 물론 피압수자에게까지 개인키 조각을 나누어 주어야 하므로 법원의 업무 부담이 지나치게 높아질 뿐만 아니라, 사실상 법원이 중립기관으로서의 역할을 전부 떠안게 되는 셈이어서 강상형 방안과 사실상 큰 차이가 없게 된다.

3. 전자정보 보전처분 제도에서의 암호화 기술 도입 방안

제1, 2항에서 본 암호기술을 전자정보 보전처분 제도에 도입하게 되면, "전자정보 보전처분 단계에서는 수사기관이 전자정보의 '내용'에 접근할 수 없어야 한다"는 전자정보 보전처분 제도의 필요조건이 충족될 수 있다. 다만, 전자정보 보전처분 제도의 특성에 맞추어 앞서 본 암호기술과 암호화 방안을 아래와 같이 일부 변형하여 도입하는 것이 바람직하다.

가. 전자정보 보전처분의 발령 주체

암호기술이 전자정보 보전처분 제도에서 사용되는 양태는 전자정보 보전처분의 발령 주체를 어느 기관으로 정하는지에 따라 일정 부분 달라지므로, 선결적 쟁점인 전자정보 보전처분의 발령 주체에 관하여 먼저 살펴본다.

전자정보 보전처분의 발령 주체에 관한 논의는 수사기관과 법원 중 어느 기관을 발령 주체로 할 것인지의 문제이다. 수사기관과 법원 모두 발령 주체로서의 장단점을 갖고 있는데, 이는 전자정보에, 전자정보의 훼손

용이성으로 인한 '신속한 정보획득의 필요성'이라는 측면과, 전자정보의 대량성 및 비가시성으로 인한 '신중한 정보보호의 필요성'이라는 측면이 동시에 존재하는 것과 궤를 같이 한다. 따라서 전자정보 보전처분 제도의 특성을 면밀히 고려하여 발령 주체를 선택하여야 한다.

먼저, 신속한 정보획득의 필요성 측면(효율성 측면)에서 본다. 전자정보 보전처분 제도의 핵심은 신속한 전자정보의 획득이고, 신중한 전자정보의 보호를 위해 전자정보 보전처분 제도를 실시하는 것은 아니다. 신속한 정보획득을 목표로 삼되, 신중한 정보보호 측면이 고려되도록 제도를 설계하여야 하는 것이다. 이러한 점에서 수사기관이 전자정보 보전처분의 발령 주체가 되는 것이 효율적이다. 수사를 진행하면서 긴급히 전자정보를 보전하여야 할 필요성이 확인될 때 즉시 전자정보 보전조치로 나아가기 위해서는 수사기관이 발령 주체가 되는 것이 효율적이고, 법원의 심사를 거쳐 전자정보 보전처분을 실시하게 되면 그만큼 전자정보 보전처분이 지체되게 된다.

다음으로, 수사기관이 보전처분의 발령 주체가 될 경우 신중한 정보보호 측면이 도외시 되는지에 관하여 본다. 전자정보 보전처분 제도의 필요조건('압수수색 영장이 발부되기 전까지 전자정보 보전처분 단계에서 수사기관의 전자정보 내용에 대한 임의 접근을 차단하는 것')이 기술적으로 달성되면, 전자정보 보전처분 단계에서의 정보보호에 대한 우려는 사라지게 된다. 또한 전자정보 보전처분 제도는 전자정보의 보전에 국한되는 조치로서 내용에 대한 접근은 차단되므로 기본권이 침해되는 정도도 비교적 작다. 따라서 기술적인 보호조치를 전제로 전자정보 보전처분에 대한 사법통제의 수준은 압수수색에 대한 사법통제 수준보다 낮게 설정하여도 무방하다.

이처럼 신속한 정보획득의 필요성 측면과 신중한 정보보호의 필요성

이라는 양 측면을 종합적으로 살펴본 결과, 기술적인 보호조치를 전제로 전자정보 보전처분 제도의 발령 주체는 수사기관이 되는 것이 바람직하다고 판단된다. 이에 발령 주체를 수사기관으로 하여 전자정보 보전처분 제도를 설계할 것을 제안한다.

나. 전자정보 보전처분 제도에서의 암호화 방안

1) 피압수자의 암호화 참여 여부

압수수색시의 암호화 방안에서는 통상 피압수자가 암호키를 나누어 갖는다. 이는 압수수색시 피압수자에게 참여권이 보장되어야 하므로, 피압수자가 참여권을 행사하지 않기로 결정하지 않는 이상 피압수자의 참여가 없는 상태에서 수사기관이 임의로 해당 전자정보에 접근하는 것을 차단하기 위한 기술적 조치이다.

그런데 전자정보 보전처분 단계에서는 유관정보 선별 작업이 이루어지지 않으므로 피압수자의 참여권이 문제될 여지가 없다. 따라서 피압수자가 암호키를 나누어 갖는 조치가 전자정보 보전처분 제도에서는 필수적이지 않다. 즉, 전자정보 보전처분 제도에서는 '제3의 기관이 암호키를 갖고, 피압수자는 암호키를 갖지 않는 방식'으로 제도를 설계하여도 수사기관이 보전처분된 전자정보에 임의로 접근하는 것을 차단할 수 있다.

오히려 피압수자가 암호화에 참가하여 암호키를 나누어 갖는 방식은 현재로서는 현실성이 부족하다. 개인이나 기업의 임직원인 일반 시민이 압수수색이나 전자정보 보전처분을 받게 되는 경우 암호에 관한 별다른 지식을 갖추지 못한 상태에서 암호화의 주체로서 암호화에 참가한다는 것은 쉽지 않다. 압수수색 영장에 암호화 방식으로 봉인할 수 있다고 기재되어 있지만, 현 실무에서 암호화 방식이 사실상 사장되어 온 현실이 이를

뒷받침한다. 향후 (압수수색이나 전자정보 보전처분에) 암호에 관한 일정한 지식을 갖춘 변호사 등의 조력이 일상화되지 않는 이상, 피압수자의 암호화 참가는 다소 비현실적이다. 또한 앞서 제2항에서 본 바와 같이 피압수자가 암호화키를 나누어 갖는 방안을 기술적으로 구현하는 방법을 찾기도 쉽지 않다. 법원이 피압수자에게까지 암호화키를 나누어 주는 것은 현실적으로 실무에 적용하기 어려운 방법이다.

이와 같은 사정들을 종합하여 보면, 전자정보 보전처분 제도는 제3의 기관이 암호키를 갖고 피압수자는 암호키를 나누어 갖지 않는 것으로 제도를 설계하는 것이 현실성이 높고, 제3의 기관은 압수수색의 적법성을 심사하여 온 법원이 되는 것이 효율적이다. 또한 전자정보 보전처분에서의 암호화에는 3자 이상의 다자 구도가 발생하지 않으므로 임계 암호기술을 사용하지 않고 보다 단순하게 암호화 방안을 설계할 수 있다.

2) 공개키 암호기술의 활용

대칭키 암호방식은 압수수색이나 전자정보 보전처분 제도에서 다음과 같은 현실적인 문제를 일으킨다. 대칭키 암호방식을 사용하는 경우, 수사기관이 암호키를 만들거나 혹은 타 기관에서 만들더라도 이를 수사기관에 교부하게 되면, 수사기관이 암호화와 복호화를 모두 할 수 있게 되어 수사기관의 반출 전자정보에 대한 임의 접근이 가능해지는 문제점이 발생한다. 그렇다고 하여 법원이 매번 보전처분 대상자에게 암호키를 전달하는 것도 비효율적이고 비현실적이다. 법원이 전자정보 보호처분 사건별로 매번 대칭키를 생성하여 이를 보전처분 대상자에게 교부하여야 한다면, 그만큼 전자정보 보전처분 제도의 신속성이 희생되어 비효율적일 뿐만 아니라, 법원은 암호키에 관한 업무를 상당한 수준으로 수행하여야 하고 사건마다 별도의 암호키를 생성·관리하여야 하기 때문에 암호키 관리에도 어려움을 겪게 된다.

그런데 이러한 문제점은 앞서 본 공개키 암호기술을 사용함으로써 어렵지 않게 해결할 수 있다. 법원의 공개키로 암호화가 이루어지면 암호화와 복호화 과정이 분리되어 법원의 암호키 없이는 수사기관이 해당 전자정보의 내용에 접근할 수 없게 된다. 동시에 법원은 사전에 공개키를 공개하는 것으로써 전자정보 보전처분에서의 역할이 끝나므로 전자정보 보전처분 제도의 신속성이 희생될 여지가 없을 뿐만 아니라, 법원의 기존 업무인 압수수색 영장 재판 단계에 이르러서야 비로소 법원이 복호화 업무를 수행하게 되므로 전자정보 보전처분 제도의 도입으로 인하여 추가되는 법원의 업무량도 최소화할 수 있다.

3) 구체적인 실천 모델

전자정보 보전처분 제도에 앞서 논의한 암호기술과 암호방식을 도입되면, 법원은 사전에 전자정보 보전처분에 필요한 공개키를 공개하여 두고, 수사기관이 보전처분을 실시하는 방식으로 그 집행이 이루어진다. 그 집행 과정을 구체적으로 살펴본다.

먼저, 전자정보 보전처분 대상자가 현재의 정보통신서비스 사업자와 같은 제3자로서 자체적으로 해당 전자정보를 보전하는데 별다른 어려움이 없는 경우, 수사기관이 전자정보 보전처분 대상자에게 해당 전자정보의 보전을 요구함으로써 집행은 종료된다. 여기에는 암호기술이 사용되지 않는다.

다음으로, 전자정보 보전처분 대상자가 피혐의자이거나 자체적으로 전자정보를 보전하는데 어려움을 겪는 제3자인 경우, 수사기관은 보전처분 대상자로부터 해당 전자정보의 복제본을 제출받아 즉시 이를 법원 제공의 공개키로 암호화한다. 이때 필요에 따라 하이브리드 방식으로 암호화할

수 있다. 공개키로 대량의 전자정보를 암호화하면 효율성 저하로 상당히 많은 시간이 소요될 수 있으므로, 보전처분 현장에서 전자정보의 복제본은 대칭키로 암호화하고, 그 대칭키만을 공개키로 암호화하는 하이브리드 방식이 효율적이다. 다만 하이브리드 방식으로 암호화를 진행할 경우 대칭키를 누가 생성할 것인가를 둘러싸고 기술상 문제가 발생한다. 수사기관이 대칭키를 생성하는 경우에는 수사기관이 그 대칭키를 복사하여 둔 다음 해당 전자정보에 임의로 접근할 수 있는 위험성이 있다. 반면에 법원이 대칭키를 생성하는 경우에는 전자정보 보전처분이 실시될 때 마다 사건별로 대칭키를 만들어 피압수자에게 교부하여야 하므로 전자정보 보전처분 제도의 신속성이 저하되고 법원의 업무 부담이 증가한다는 단점이 있다. 이 문제를 해결하기 위하여 "수사기관의 포렌식 도구인 암호화 프로그램에서 난수 형태의 일회용 대칭키를 발생시킨 다음 그 대칭키를 법원 제공의 공개키로 즉시 암호화하는 방법"을 제안한다. 이 정도로도 대칭키 보호를 위한 기술적 조치로 부족함이 없을 것으로 보이나, 극단적인 경우 메모리 덤프 방식 등으로 대칭키를 알아 낼 수 있는 여지가 없는 것은 아니므로, 하드웨어 차원에서 분리된 메모리 영역의 보안구역에 암호키를 보관하는 기술적인 조치[41]를 취하면 그 안전성을 배가시킬 수 있다.

전자정보 보전처분을 한 이후 수사기관은 해당 사건을 수사한 다음 법원에 소명자료를 제시하면서 압수수색 영장을 청구하는데, 이때 보전처분된 전자정보가 존재하는 경우에는 복호화를 함께 신청한다. 법원은 압수수색 영장을 발부하는 경우에 복호화를 실시한다. 한편 법원이 압수수색 영장을 기각하는 경우 수사기관은 즉시 보전처분된 전자정보를 폐기한다.

---

41) 대표적인 예로 인텔사(Intel Corporation)의 Software Guard Extensions(SGX)을 들 수 있다. 인텔사는 이를 통해 하드웨이 기반 제어를 사용함으로써 특정 응용프로그램 코드와 메모리의 데이터를 분리하는 하드웨어 기반 메모리 암호화가 가능하다고 밝히면서, 사용자 수준 코드를 사용하여 인클레이브(프라이빗 메모리 영역)를 할당할 수 있다고 설명하고 있다.

제3절 전자정보 보전처분 제도의 확장

1. 보전처분 대상자의 확장

가. 보전처분 대상자의 확장과 그 절차

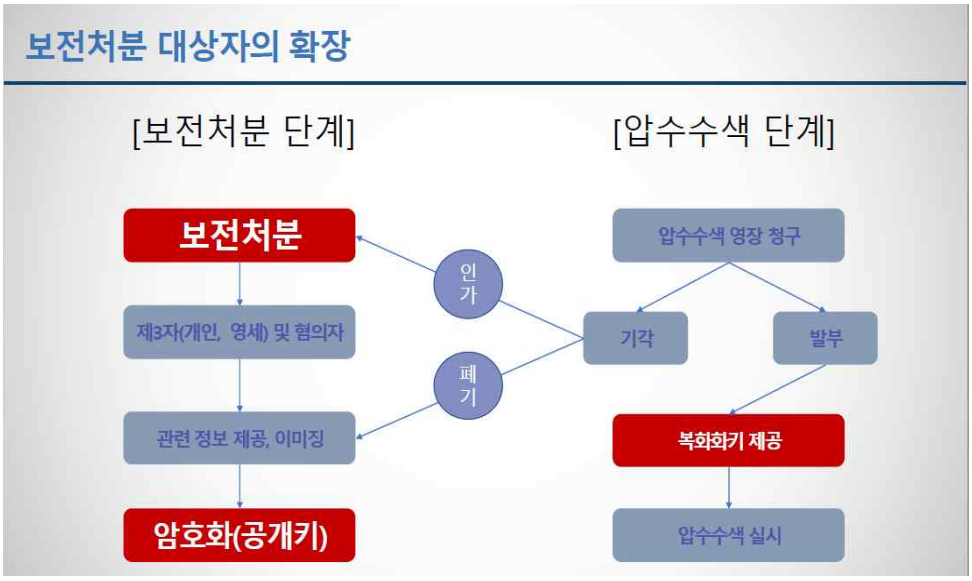
기존 논의가 일정 규모 이상의 정보통신사업자를 전자정보 보전처분 대상자로 삼고 있는 것을 앞서 본 바와 같다. 이들은 전자정보를 보전하는데 필요한 인적·물적 자원을 보유하고 있으므로, 전자정보 보전처분으로 이들에게 해당 전자정보를 보관하도록 의무를 부과하고, 압수수색 영장이 발부된 후에 이들로부터 해당 전자정보를 넘겨받아 압수수색을 실시하면 된다. 이들을 대상으로 실시되는 전자정보 보전처분은 이처럼 간명하게 처리된다.

반면에 피혐의자의 경우 자신에게 불리한 전자정보를 스스로 현 상태대로 보관할 것이라고는 기대하기 어렵고, 제3자 중 영세한 기업이나 개인은 전자정보를 보관할 인적·물적 자원이 부족하므로, 이들을 대상으로 한 전자정보 보전처분은 자가 보관 형태가 될 수 없다. 이에 이들에 대하여는 '공개키 암호기술을 이용한 암호화 방식을 통해 수사기관이 보전처분된 전자정보를 보관하는 형태'[42]로 전자정보 보전처분을 실시할 것을 제안하였다.

이처럼 공개키 암호기술을 이용한 암호화 방식으로 전자정보 보전처분을 실시하게 되면, 기존 방식으로는 대상자로 삼지 못한 피혐의자를 비롯하여 일정 규모 이하의 기업이나 각종 비영리법인, 단체 및 개인 등도 대상자로 삼을 수 있게 된다. 즉 공개키 암호기술을 이용한 암호화 방식을 도입함으로써 '대상자에 대한 제한'이 사라지게 되는 것이다. 이는 전자

42) 제3의 기관이 설립된다면, 제3의 기관이 보관을 맡는 형태도 상정해 볼 수 있다.

정보의 훼손 가능성이 기업과 개인을 가리지 않고 모든 영역에서 상존하고 있는 현실을 감안하여 볼 때 전자정보 보전처분과 뒤따르는 압수수색의 효율성을 제고하는데 상당한 역할을 할 것으로 기대된다. 전자정보 보전처분 대상자를 피혐의자나 일정 규모 이하의 기업 및 개인으로 확대하는 경우 이들에 대한 전자정보 보전처분과 압수수색의 절차는 아래 표와 같이 진행된다.



위 표에서 보듯이 압수수색 영장이 기각되었을 경우에는 암호화된 복제본을 폐기하는 것이 원칙이다. 그러나 압수수색 영장을 소명 부족으로 기각하는 경우에도, 지방법원판사가 보완 수사 후 압수수색 영장을 재청구할 수 있을 만한 사안이라고 판단하는 경우에는 직권으로 일정 기간 그 보전처분의 효력을 계속 유지시키도록 하는 내용의 인가 결정을 할 수 있도록 하는 것이 합리적이라고 본다.

나. 피혐의자에 대한 보전처분 제도의 타당성

전자정보 보전처분에 암호화 방식을 사용하는 기술적 조치를 취할 경우 피혐의자에 대한 전자정보 보전처분이 가능하게 된다. 그러나 한편, 기술적 가능성의 측면이 아닌 수사비례의 원칙에 비추어 피혐의자를 전자정보 보전처분 대상자로 삼는 것이 적절한지에 관하여 논란이 있을 수 있다. 즉, 압수수색 영장이 발부되지도 않은 상태에서 신속한 전자정보 보전을 이유로 피혐의자에 대한 전자정보 보전처분을 할 수 있게 하는 것이 피혐의자의 기본권을 과도하게 침해하는 행위가 될 수 있다는 우려이다[43].

이와 같은 우려는 신중한 정보보호의 측면에서 충분히 이해할 수 있으나, 아래와 같은 이유로 피혐의자를 보전처분 대상에서 제외할 필요는 없다고 본다. 다만, 그와 같은 우려를 반영하여 전자정보 보전처분 제도의 도입 초기에는 피혐의자를 보전처분 대상자에서 제외하고 제3자만을 보전처분 대상자로 삼는 것도 고려하여 볼 만하다.

1) 먼저 현실적 필요성이다. 사실관계(실체적 진실)를 정확하게 밝히기 위해서는 피혐의자가 보유하고 있는 정보를 신속하게 보전할 필요성이 있다. 사실관계 파악에 있어 직접적이고 실효적인 정보는 사건 당사자인 피혐의자가 소지하고 있을 가능성이 높다. 따라서 정보보전 필요성의 관점에서 볼 때 피혐의자가 보관하고 있는 전자정보는 우선적으로 보전하여야 할 중요 정보에 해당한다. 따라서 피혐의자를 전자정보 보전처분 대상자에 포함하는 것이 사실관계를 정확하게 파악하여 적정한 형벌권을 행사하는데 필요하다.

2) 다음으로, 전자정보 보전처분의 법적 성격상 피혐의자를 포함시

43) 이러한 견해는 수사비례의 원칙에 기반하고 있는 것으로 보인다. 형벌권은 국가권력 중 가장 강력한 권력 중 하나이며 이러한 형별권 행사를 준비하기 위한 수사권도 그 목적 달성을 위해 국민의 기본권을 침해하는 요소가 강하므로, 비례의 원칙에 따라 수사권 행사가 이루어져야 한다는 인식이 보편화되어 있다.

키는 것이 논리적이라는 점을 들 수 있다. 전자정보 보전처분 제도는 압수수색을 위한 사전적 보전처분이므로, 전자정보 보전처분의 범위를 압수수색의 범위와 동일하게 설정하는 것이 논리적 정합성을 갖는다. 즉, 전자정보 보전처분의 범위와 압수수색의 범위가 동일한 것이 원칙적인 모습이고, 예외적인 경우에 그 범위를 다르게 설정할 수 있다고 보는 것이 논리적이다. 따라서 압수수색 대상자에 포함되는 피혐의자(피의자)를 전자정보 보전처분 대상자에서는 제외한다면 이는 상당히 부자연스럽다. 기존에 전자정보 보전처분 제도를 논의하면서 피혐의자를 제외한 것은 피혐의자에게 불리한 정보의 보전을 요구해도 그 이행을 기대하기 어렵고, 피혐의자가 그 요구에 따르지 아니하더라도 피혐의자를 형사처벌할 수 없는 이상 보전처분의 실효성이 크지 않다는 것이 주된 이유였는데, 공개키 암호기술을 이용한 암호화 방식의 도입으로 피혐의자가 스스로 전자정보를 보전하지 않아도 무방한 방식으로 전자정보 보전처분 제도를 설계할 수 있으므로, 더 이상 실효성의 부재를 이유로 삼아 피혐의자를 그 대상자에서 제외할 필요가 없다.

3) 수사기관이 전자정보의 내용에는 접근할 수 없도록 하는 전자정보 보전처분의 특성에 비추어 볼 때, 전자정보 보전처분의 기본권 침해 정도가 비교적 높지 않으므로, 피혐의자를 대상자에 포함시키는 것이 비례의 원칙상 과도하다고 볼 수 없다. 물론 전자정보의 대량성과 비가시성으로 인하여 전자정보 압수수색은 프라이버시 침해와 저인망식 수사에 대한 우려를 낳고 있으므로, 수사기관의 전자정보 확보에 있어 이러한 우려가 현실화되지 않도록 신중을 기하여야 하나, 전자정보 보전처분의 경우에는 그 필요조건으로 수사기관이 당해 전자정보의 내용에 접근할 수 없도록 하고 있고 공개키 암호기술을 이용한 암호화 조치를 취함으로써 그 필요조건이 충실히 달성되므로 신중한 정보보호의 측면에서도 별다른 우려가 있을 수 없다. 수사기관은 압수수색 영장을 발부받기 전까지는 전자정보를 보전만 할 뿐이고, 압수수색 영장을 발부받은 후에야 피압수자측의 참여

하에 수색 과정을 거쳐 유관정보만을 압수할 수 있다. 이처럼 암호화 방식을 이용한 전자정보 보전처분 단계에서는 프라이버시 침해와 저인망식 수사에 대한 우려가 발생하지 않으므로, 피혐의자에 대한 전자정보 보전처분이 수사 초기 단계에 압수수색 영장 없이 이루어진다고 하더라도 기본권 침해의 정도는 크지 않는 반면에, 이를 통해 사실관계 파악에 필요한 중요 전자정보를 확보할 수 있는 공익을 달성할 수 있으므로 수사비례의 원칙을 충족한다.

2. 보전처분 활용범위의 확장

가. 사법통제의 유연성 제고

현행 압수수색 영장 재판에서, 수사기관이 압수수색 영장의 발부를 확신하면서 영장을 청구하나, 법원이 견해를 달리하여 소명 부족으로 압수수색 영장을 기각하는 일이 종종 발생한다. 그러나 소명부족이라는 법원의 판단이 확정적인 것은 아니다. 기각 결정 후에 소명자료가 보완되거나 추가 소명자료가 제출되면, 법원은 압수수색 영장을 발부할 수 있다. 그런데 최초의 압수수색 영장이 기각되고 재청구된 압수수색 영장이 발부되는 사이에 중요한 전자정보가 훼손될 수 있다. 따라서 향후 추가 소명과 함께 압수수색 영장이 재청구되면 영장이 발부될 수 있을 만한 사안에서는 법원으로서도 '영장을 기각하되 해당 전자정보는 현 상태로 유지하도록 하는 보전조치를 취할 수 있는 제3의 선택지'가 존재하면 압수수색 영장 재판을 보다 유연하게 가져갈 수 있을 것이다. 전자정보 보전처분 제도가 도입된 상황에서도 이러한 상황은 여전히 발생할 수 있다. 수사기관이 전자정보 보전처분을 실시하지 않은 채 바로 압수수색 영장을 청구할 수 있기 때문이다.

이처럼 소명 정도에 따라 압수수색 영장의 발부와 기각만이 가능한

현행 압수수색 영장 재판에 제3의 선택지로 전자정보 보전처분 제도를 도입할 수 있다. 법원이 소명 부족으로 압수수색 영장을 기각하되 직권으로 전자정보 보전처분을 명령할 수 있도록 하면, 법원이 보다 유연하게 압수수색에 대한 사법적 통제를 실시할 수 있다. 즉 압수수색 영장을 기각하는 경우, 지방법원판사가 직권으로 전자정보 보전처분을 명령하고 수사기관이 그 명령을 집행함으로써 전자정보가 보전되도록 설계하는 것이다. 이 경우 압수수색 영장의 피압수자가 피의자인 경우나 피압수자가 자체적으로 전자정보를 보전할 능력이 없는 제3자인 경우에는 앞서 본 바와 같이 공캐키 암호기술을 이용한 암호화 방식으로 해당 전자정보의 복제본을 암호화하여 전자정보 보전처분을 실시한다. 이후 수사기관이 소명자료를 보완·추가하여 압수수색 영장을 재청구하면, 지방법원판사는 재청구된 영장을 발부하는 경우 복호화를 허가하면 된다. 이렇게 압수수색 영장 제도를 운영하게 되면, 법원은 신중한 전자정보 보호의 필요성이라는 관점에서 사법적 통제 강화 기조를 유지하면서도 전자정보의 훼손 가능성은 낮출 수 있고, 압수수색 영장을 발부받지 못한 수사기관으로서도 추후 소명자료를 보완·추가하여 전자정보를 확보할 수 있는 기회를 갖을 수 있게 된다. 즉 신속한 전자정보의 확보와 신중한 전자정보의 보호라는 두 가지 목표가 모두 고려된 실무 운용이 가능하게 된다.

나. 관련성 통제의 취약점 보완 - 별건 전자정보에 관하여

1) 별건 전자정보의 압수 방법

형사소송법상 무관증거는 압수할 수 없다. 이는 압수수색 영장을 집행하는 과정에서 별건 전자정보를 우연히 발견한 경우에도 그대로 적용되어 기존 압수수색 영장으로는 별건 전자정보를 압수할 수 없다. 일례로 수사기관이 피의자 갑의 공직선거법 위반 범행을 영장 범죄사실로 하여 발부받은 압수수색 영장의 집행 과정에서 을, 병 사이의 대화가 녹음된

녹음파일을 압수하여 을, 병의 공직선거법 위반 혐의사실을 발견한 사안에서 대법원은 “압수수색 영장에 기재된 ‘피의자’인 갑이 녹음파일에 의하여 의심되는 혐의사실과 무관한 이상, 을과 병 사이의 대화가 담긴 녹음파일은 형사소송법 제219조에 의하여 수사기관의 압수에 준용되는 형사소송법 제106조 제1항이 규정하는 ‘피고사건’ 내지 같은 법 제215조 제1항이 규정하는 ‘해당 사건’과 ‘관계가 있다고 인정할 수 있는 것’에 해당하지 않으며[44], 이와 같은 압수에는 헌법 제12조 제1항 후문, 제3항 본문이 규정하는 영장주의를 위반한 절차적 위법이 있으므로, 녹음파일은 형사소송법 제308조의2에서 정한 ‘적법한 절차에 따르지 아니하고 수집한 증거’로서 증거로 쓸 수 없고, 그 절차적 위법은 헌법상 영장주의 내지 적법절차의 실질적 내용을 침해하는 중대한 위법에 해당하여 예외적으로 증거능력을 인정할 수도 없다”고 판시하였다(2014. 1. 16. 선고 2013도7101판결 참조).

법원은, 압수수색 영장을 집행하는 과정에서 별건 전자정보가 발견된 경우 수사기관이 그 별건 전자정보를 압수하기 위하여는 추가 탐색을 중단하고 별도의 영장을 발부받아야 한다는 태도를 확고히 하고 있다[45]. 이러한 법원의 태도에 대하여 “법원이 별건 전자정보에 관하여 추가 압수수색 영장을 발부받아 이를 압수할 수 있다고 설시하고는 있으나, 추가

44) 제2장 제1절에서 살펴 본 ‘관련성 요건’에 관한 기술 중 주관적 관련성 부분 참조

45) 대법원 2017. 11. 14. 선고 2017도3449 판결, 대법원 2015. 7. 16.자 2011모1839 결정 등 참조. 위 결정의 이유 중 중요 부분은 다음과 같다. “전자정보에 대한 압수수색이 종료되기 전에 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우라면, 수사기관은 더 이상의 추가 탐색을 중단하고 법원에서 별도의 범죄혐의에 대한 압수수색영장을 발부받은 경우에 한하여 그러한 정보에 대하여도 적법하게 압수수색을 할 수 있다. 나아가 이러한 경우에도 별도의 압수수색 절차는 최초의 압수수색 절차와 구별되는 별개의 절차이고, 별도 범죄혐의와 관련된 전자정보는 최초의 압수수색영장에 의한 압수수색의 대상이 아니어서 저장매체의 원래 소재지에서 별도의 압수수색 영장에 기해 압수수색을 진행하는 경우와 마찬가지로 피압수수색 당사자는 최초의 압수수색 이전부터 해당 전자정보를 관리하고 있던 자라 할 것이므로, 특별한 사정이 없는 한 피압수수색 당사자에게 형사소송법 제219조, 제121조, 제129조에 따라 참여권을 보장하고 압수한 전자정보 목록을 교부하는 등 피압수자의 이익을 보호하기 위한 적절한 조치가 이루어져야 한다.”

압수수색 영장을 발부받기 위하여 필요한 절차나 소명자료의 확보에 필요한 시간 등을 고려하여 볼 때 그 과정에서 전자정보가 위조·변제·삭제될 가능성이 크다'라는 비판적인 견해[46]가 존재한다. 그러나 앞서 대법원 2013도7101 판결에서 본 바와 같이 관련 규정 등에 따라 압수수색 영장에 기재된 혐의사실과 관련 있는 유관정보의 압수만이 적법한 점에 비추어 보면, 별건 전자정보의 압수에 추가 압수수색 영장을 요구하는 법원의 태도는 논리필연적이므로, 별다른 사정이 없는 한 이러한 법원의 태도가 변경되기는 쉽지 않을 것으로 보인다.

2) 추가 압수수색 영장 발부를 둘러싼 실무상 문제점

이처럼 대법원은 수사기관이 별건 전자정보를 압수하려면 추가로 압수수색 영장을 발부받아야 한다고 밝히면서도 구체적인 방법은 제시하고 있지 않아 수사 실무 및 영장 재판상 그 적용에 혼란이 있을 수 있다. 실무가들이 제시하고 있는 구체적인 쟁점들을 보면, 우연히 발견한 최초의 별건 전자정보를 기존의 압수수색 영장으로 압수할 수 있는지 여부, 우연히 발견한 최초의 별건 전자정보 역시 기존의 혐의사실과는 관련성이 없는 무관정보이므로 기존의 압수수색 영장으로는 압수할 수 없다고 본다면 최초의 별건 전자정보를 추가 압수수색 영장을 청구하기 위한 소명자료로는 사용할 수는 있는지 여부, 수색 과정에서 별건 전자정보를 우연히 발견하였다는 내용의 수사기관 작성의 보고서 등이 추가 압수수색 영장의 청구시에 소명자료로 사용될 수 있는지 여부, 추가 압수수색 영장을 청구하려고 하는데 최초로 발견된 별건 전자정보만으로는 소명이 부족한 경우에는 어떻게 처리할 것인지 여부, 소명 부족으로 별건 전자정보에 대한 압수수색 영장을 즉시 발부받을 수 없는 경우에는 신속하게 별건 전자정보를 압수하지 못하게 되므로 그 정보주체가 별건 전자정보를 훼손

46) 박래옥, "클라우드 스토리지의 효율적인 압수수색을 위한 방안", 서울대학교 석사학위 논문, 2016, 78면

하는 행위를 차단할 수 없게 되는 것이 타당한지 여부와 같은 실무상 문제점들이 쟁점으로 부상하고 있다.

나아가 위와 같은 실무상 문제점들이 법원의 압수수색 영장에 대한 심사 강화 기조와 맞물리게 되면, 법원의 관련성 통제 강화가 신속한 전자정보의 획득을 상당히 어렵게 만드는 결과를 초래할 수 있다. 따라서 법원의 관련성 통제 강화가 실체적 진실의 발견에 필요한 전자정보 획득에 장애가 되지 않도록 적절한 방안을 강구하여야 한다.

3) 전자정보 보전처분 제도의 활용

기존에 논의되어 온 전자정보 보전처분 제도는, 혐의사실을 포착한 수사기관이 그 혐의사실에 관한 전자정보를 압수수색하기 전에 실시하는 사전적 보전처분으로 고안된 것이다. 그런데 이와 같은 사전적 보전처분으로서 고안된 전자정보 보전처분 제도는 수사기관이 우연히 발견한 별건 전자정보로 새로운 혐의사실을 포착하게 된 경우에도 활용할 수도 있다. 즉, 혐의사실 포착시점과 전자정보의 취득시점이 뒤바뀐 별건 전자정보의 경우에도 전자정보 보전처분 제도를 적용함으로써[47] 법원의 관련성 통제 강화가 실체적 진실 발견에 필요한 전자정보의 획득에 장애가 되지 않도록 운용할 수 있는 것이다.

별건 전자정보에 관한 전자정보 보전처분도 공캐키 암호기술을 이용한

---

47) 독일 형사소송법은 아래와 같이 별건 정보를 우연히 발견한 경우 임시적으로 압수를 할 있다는 규정을 두고 있다. 검사가 적절한 기간 내에 판사에게 압수수색을 구하지 않은 경우에는 임시 압수는 취소되고 압수물은 환부된다(최진안, “독립적 긴급압수수색제도의 도입가능성과 한계, 아주법학 제7권 제1호, 2013. 6., 121면). 이러한 가압수는 보전처분과 일맥상통한다.
제108조
① 조사와는 직접적 관련이 없지만 수색의 기회에 다른 범행의 혐의근거가 되는 대상을 발견한 때에는 이를 가압수(임시 압수)할 수 있다. 당해 사실은 검사에게 통지하여야 한다. (이하 생략)

암호화 방식으로 실시한다. 즉, 별건 전자정보를 암호화하는 방식으로 전자정보 보전처분을 실시하고, 이후 수사기관이 소명자료를 모아 별건 전자정보에 대한 압수수색 영장을 청구하며, 지방법원판사가 영장 발부와 함께 복호화를 허가하게 된다. 법원이 별건 전자정보에 대한 압수수색 영장 청구를 기각하는 경우 직권으로 전자정보 보전처분에 대한 인가 결정을 할 수 있도록 설계할 수 있다는 점도 동일하다. 이를 통해 사법적 통제 강화 기조를 훼손하지 않으면서도 동시에 전자정보의 훼손 가능성을 낮출 수 있다.

다. 관련성 통제의 취약점 보완 - 컴퓨터 생성증거에 관하여

1) 컴퓨터 생성증거의 의의 및 보존 필요성

컴퓨터는 시스템 자원 관리 등의 목적으로 컴퓨터에 일정한 행위가 발생했을 때 그 행위와 관련된 부가 정보를 기록하는데, 이때 기록되는 부가 정보는 사람의 개입 없이 컴퓨터가 내장 알고리즘에 따라 기록하는 것으로서 컴퓨터 생성증거(Computer Generated Evidence)라고 하고, 반면에 사람이 기록한 것으로 컴퓨터에 저장된 증거는 통상 '컴퓨터 저장증거'라고 부른다[48]. 컴퓨터 생성증거는 비진술증거에 해당하므로 전문법칙이 적용되지 않는다. 이에 반하여 컴퓨터 저장증거가 전문증거에 해당하는지 여부는 개별적으로 따져 보아야 한다.

한편 앞서 본 바와 같이 형사소송법 규정 및 법원의 관련성 통제 강화로 인하여 선별 압수를 실시하고 있는데, 그 구체적인 양태를 살펴보면 파일 단위로 압수하는 경향을 보이면서 사이버 및 인터넷 범죄 사건을 제외한 대부분의 일반 사건에서는 혐의사실과 관련 있는 '파일'에 한정하여 압수수색을 진행하고 있다[49]. 이렇게 파일 단위로 증거를 압수

48) 김영철, "디지털 본래증거 수집 방안 연구", 서울대학교 석사학위 논문, 2018, 6면

하는 경향이 컴퓨터 생성증거의 압수에 있어 기술적 측면에서는 문제를 일으키지 않는다. 메타데이터를 비롯하여 이벤트로그와 레지스트리 등 컴퓨터 생성증거는 파일의 형태로 존재하는 경우가 대부분이기 때문이다[50]. 그러나 법적 측면에서는 컴퓨터 생성증거 압수의 적법성 여부가 명확하지 않다. 관련성 통제 측면에서 볼 때 컴퓨터 생성증거와 혐의사실과의 관련성이 인정되는지 여부가 불분명한 경우가 발생하기 때문이다. 항을 바꾸어서 살펴본다.

2) 컴퓨터 생성증거와 전문법칙

컴퓨터 생성증거와 혐의사실과의 관련성이 주로 문제되는 지점은 전문증거의 증거능력 인정 여부이다. 이를 논의하기 위하여 먼저 전자정보와 전문법칙에 관하여 본다.

정보저장매체에 담긴 전자정보나 그 출력물을 진술증거로 사용하는 경우, 그 기재 내용의 진실성에 관하여는 전문법칙이 적용되므로, 공판준비기일이나 공판기일에서 작성자나 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다[51]. 다만 어떤 진술이 기재된 서류가, 그 내용의 진실성이 범죄사실에 대한 직접증거로 사용될 때는 전문증거가 된다고 하더라도, 그와 같은 진술을 하였다는 것 자체 또는 그 진술의 진실성과 관계 없는 간접사실에 대한 정황증거로 사용될 때는 반드시 전문증거가 되는 것은 아니다[52]. 예를 들어 피압수자가 그와 같은 내용의 문서 또는 그러한 문서파일이 들어있는 저장매체를 소지 또는 보관하고 있었다는 점에 대한 증거로 사용될 때에는 전문법칙이

49) 원용기, “디지털증거에 대한 계층적 접근 방안 연구”, 서울대학교 석사학위 논문, 2016, 4면
50) 김영철, “디지털 본래증거 수집 방안 연구”, 서울대학교 석사학위 논문, 2018, 30면
51) 대법원 2015. 7. 16. 선고 2015도2625 판결, 대법원 2007. 12. 13. 선고 2007도7257 판결 등 참조
52) 대법원 2000. 2. 25. 선고 99도1252 판결 등 참조

적용될 것이 아니어서 증거능력이 인정될 수 있다[53].

이처럼 정보저장매체에 담긴 전자정보나 그 출력물을 진술증거로 사용하는 경우작성자나 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있으나(형사소송법 제313조 제1항), 형사소송법은 '진술서의 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하는 경우에는 과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있다는 규정(형사소송법 제313조 제2항[54])'을 통해 과학적 분석결과에 기초하여 증거능력을 인정하는 길을 열어 두고 있다. 다만, 피고인 아닌 자가 작성한 진술서는 피고인 또는 변호인이 공판준비 또는 공판기일에 그 기재 내용에 관하여 작성자를 신문할 수 있었을 것을 요한다.

따라서 사건에 따라 작성자나 진술자가 향후 공판 과정에서 진술증거인 전자정보나 그 출력물에 관하여 성립의 진정을 인정하지 않는 경우를 대비하여, 수사기관으로서는 과학적 분석결과에 기초하여 증거능력을 인정받기 위하여 컴퓨터 생성증거를 확보해 두어야 할 필요성이 있을 수 있다. 그런데 관련성 통제 측면에서 볼 때 수사단계에서 컴퓨터 생성증거와 혐의사실과의 직접적인 관련성이 인정되는지 여부가 확실하지 않은 경우 '향후 공판 단계에서 필요성이 있을 수 있다'라는 점을 들어 컴퓨터 생성증거를 압수할 수 있는지 여부가 불분명하다. 따라서 컴퓨터 생성증거를 일시적으로 보관할 수 있는 방안이 마련되는 것이 바람직하다.

3) 전자정보 보전처분 제도의 활용

전자정보 보전처분 제도는 컴퓨터 생성증거를 일시적으로 보관할

53) 대법원 2013. 6. 13. 선고 2012도16001 판결 등 참조
54) 2016. 5. 29. 개정되었다.

수 있는 방법으로 유효적절하게 활용될 수 있다. 수사기관은 압수수색 과정에서 컴퓨터 생성증거를 분리한 다음, 이를 법원의 공개키로 암호화 하는 방식으로 전자정보 보전처분을 실시함으로써, 컴퓨터 생성증거를 안전하게 확보할 수 있다. 향후 작성자나 진술자가 공판준비기일이나 공판 기일에서 진술증거인 전자정보나 그 출력물에 관하여 성립의 진정을 인정 하지 않는 경우, 수소법원은 보전처분된 컴퓨터 생성증거에 대한 압수수색 영장을 발부하면서 컴퓨터 생성증거를 복호화함으로써 이를 증거능력 판단에 활용할 수 있게 된다.

라. 소결

공개키 암호기술을 이용한 암호화 방식의 전자정보 보전처분 제도는 사법통제 강화 기조를 유지하면서도 그 대상자를 확대하고 관련성 통제의 취약점을 보완하며, 인가 결정을 통한 유연성 있는 사법통제를 가능하게 한다.

특히 관련성 통제의 취약점 보완과 관련하여 별건 전자정보 및 컴퓨터 생성증거에 관하여 살펴보았는데, 이는 공개키 암호기술을 이용한 암호화 방식의 전자정보 보전처분 제도가 확장 적용될 수 있는 형사절차적 지점을 예시적으로 제시한 것으로써 이와 같은 방식의 전자정보 보전처분 제도는 형사절차의 다양한 지점들에서 폭넓게 활용될 수 있다.

제4절 형사소송법 개정안

향후 공개키 암호를 이용한 암호화 방식의 전자정보 보호처분 제도를 도입한다면 구체적으로 형사소송법 개정안이 어떻게 마련될 수 있을지 제시하여 본다.

형사소송법 개정안

제215조의2(전자정보의 보전처분)

① 검사 또는 사법경찰관은 피의자가 죄를 범하였다고 의심할 만한 정황이 있는 경우 해당 사건과 관계가 있는 전자정보를 보유하고 있거나 관리하고 있는 자(이하 '보전처분 대상자'라고 한다)에게 30일의 범위 내에서 당해 전자정보가 삭제·변경되지 않도록 보전할 것을 서면으로 요구할 수 있다. 다만, 상당한 이유가 있는 경우 30일의 범위 내에서 1회에 한하여 서면으로 연장을 요구할 수 있다.

② 피의자인 보전처분 대상자는 보전처분 대상인 전자정보의 복제본을 검사 또는 사법경찰관에게 제출하여야 하고, 그 외의 보전처분 대상자는 보전처분 대상인 전자정보의 복제본을 검사 또는 사법경찰관에게 제출할 수 있다. 복제본을 교부받은 검사 또는 사법경찰관은 즉시 보전처분 대상자의 참여하에 법원의 승인이 있을 경우에만 열람할 수 있도록 암호기술을 포함하는 기술적 보호조치를 취하여야 하고, 그 과정에서 어떠한 이유로도 전자정보 내용을 확인하여서는 아니된다.

③ 검사 또는 사법경찰관이 제1항에 따라 전자정보의 보전을 요구하는 경우에는 범죄사실 요지가 기재된 전자정보 보전처분서에 의하여야 하고, 소속기관에 전자정보 보전처분대장을 비치하여야 한다. 사법경찰관이 제1항에 따라 전자정보의 보전을 요구한 경우 검사에게 지체없이 전자정보 보전처분서 등본을 송부하여야 한다.

④ 검사는 제215조 제1항에 따라 발부받은 영장에 의하여, 사법경찰관은 제215조 제2항에 따라 발부받은 영장에 의하여 보전처분한 전자정보에 대한 압수·수색·검증을 실시할 수 있다. 전자정보의 복제본에 대하여 제2항에 따른 기술적인 보호조치가 이루어진 경우, 검사는 영장을 청구하면서 압수수색 영장의 발부와 동시에 기술적인 보호조치에 대한 해제를 법원에 신청할 수 있다.

⑤ 지방법원판사는 보전처분된 전자정보에 대한 압수·수색·검증 영장을 기각하는 경우 직권으로 30일의 범위 내에서 해당 전자정보의 보전

처분을 연장하는 인가 결정을 할 수 있다. 검사 또는 사법경찰관은 인가 결정 없이 압수수색검증 영장이 기각된 경우 지체 없이 보전처분을 취소하여야 한다.

⑥ 지방검찰청검사장은 이에 대응하는 지방법원법원장에게 매월 1회 이상 전자정보 보전처분을 한 검사 및 사법경찰관이 작성한 전자정보 보전처분서의 목록을 제출하여야 한다.

⑦ 보전처분 대상자가 검사 또는 사법경찰관의 보전처분에 응하지 아니하는 경우, 검사 또는 사법경찰관은 해당 전자정보가 저장되어 있을 것으로 예상되는 정보저장매체를 직접 복제할 수 있고, 그 복제본은 제2항에서 기술한 동일한 방식으로 기술적 보호조치를 하여야 하며, 그 과정에서 어떠한 이유로도 전자정보의 내용을 확인하여서는 아니 된다. 이 경우 검사는 지체 없이 지방법원판사의 허가를 받아야 하고, 사법경찰관은 검사에게 신청하여 검사의 청구로 지방법원판사의 허가를 받아야 하며, 72시간 이내에 지방법원판사의 허가를 받지 못한 때에는 복제본을 즉시 폐기하여야 한다.

제5장 결론

급격한 디지털 전환이 이루어지면서 전자정보의 생성·저장·유통도 전례 없이 증가하고 있다. 그 결과 압수수색에서 전자정보가 차지하는 비중도 꾸준히 증가하고 있다. 이러한 상황에서 전자정보의 훼손 용이성을 외면한 채 현 압수수색 제도의 틀을 고수할 수만은 없다. 현 압수수색 제도에 대한 계속적인 보완이 이루어져야 하고, 전자정보 보전처분 제도의 도입은 그 보완의 시발점으로서 어떤 형태로든지 필연적으로 도입될 것으로 보인다.

전자정보 보전처분 제도를 도입한다면, 그 적용 범위를 가능한 한 확대하여 전자정보의 훼손 가능성을 최대한 차단할 수 있도록 설계되어야 한다. 그럼에도 전자정보 보전처분 제도에 관한 기존 논의는 그 대상자를 일부 정보통신사업자로 국한하고 있고, 전자정보 보호처분 제도가 사용되는 시점도 압수수색 실시 전으로 한정하고 있다. 이와 같이 기존 논의에 따른 전자정보 보전처분 적용범위는 상당히 협소하다. 즉 확장성이 부족한 제도로 전자정보 보호처분 제도가 설계되고 있는 것이다.

하지만 공개키 암호기술을 이용한 암호화 방식을 도입함으로써 전자정보 보호처분 제도는 기존 논의를 훨씬 뛰어넘는 확장성을 확보할 수 있다. 암호화 방식이 적용되면 수사기관이 보호처분된 전자정보의 내용에는 접근할 수 없기 때문에 수사기관이 보전처분된 전자정보를 보관하게 되더라도 무방하다. 그 결과 전자정보 보호처분 대상자가 스스로 전자정보를 보관할 수 없는 상황에서도 수사기관 보관 형태로 전자정보 보전처분을 실시할 수 있는 길이 열리는 것이다. 이 경우 전자정보를 보전하는데 소요되는 비용도 수사기관이 부담하게 되므로 비용 논란 역시 해소된다. 이로써 전자정보 보호처분 대상자는 제한 없이 확대될 수 있다. 나아가 공개키 암호기술을 사용한 암호화 방식이 활용됨으로써 수사기관은 전자정보 보전

처분을 실시할 때마다 법원으로부터 암호키를 교부받는 절차를 생략할 수 있어 전자정보 보전처분 제도의 신속성을 제고할 수 있고, 법원으로서도 공개키를 제공하는 역할에 머무르게 되어 업무상 부담을 최소화할 수 있다. 이렇게 효율성이 제고됨에도 보전처분된 전자정보의 보호에는 별다른 문제가 발생하지 않는다. 여기에 더하여 전자정보 보전처분 제도는 별건 전자정보나 컴퓨터 생성증거의 확보 등 형사절차의 여러 지점에서 폭넓게 활용될 수 있는 확장성을 갖게 된다. 형사절차 중 신속한 정보획득의 측면과 신중한 정보보호의 측면이 공존하는 지점이라면 전자정보 보전처분 제도의 도입이 검토될 수 있는 것이다. 이처럼 암호화 방식을 도입함으로써 얻는 이점은 매우 크다.

새로운 기술과 제도의 도입은 여러 우려를 낳는다. 그러나 디지털 전환이라는 사회의 큰 흐름을 직시하여 보면 공개키 암호기술을 이용한 암호화 방식의 전자정보 보전처분 제도의 도입이 필요하다는 주장을 배척하기 어렵다. 만약 전자정보 보전처분 제도를 형사소송법에 전면적으로 도입하는 것이 어렵다면, 우선적으로 전자정보의 생성・저장・유통이 현저하고 관련자들이 증거인멸을 시도할 가능성이 높은 영역에 시범적으로 도입하여 보는 것도 하나의 방법이다. 예를 들어 자본시장과 금융투자업에 관한 법률이나 독점규제 및 공정거래에 관한 법률과 같은 개별 법률에 시범적으로 전자정보 보전처분 제도를 규정하여 위 법률들을 위반한 형사사건에서부터 이를 활용하여 보는 것이다.

[참고문헌]

1. 손지영, 김주석, “압수수색 절차의 개선방안에 관한 연구”, 대법원 사법정책연구원, 2014
1. 김영철, “디지털 본래증거 수집 방안 연구”, 서울대학교 석사학위논문, 2018
1. 강상형, “사생활 정보를 고려한 디지털 증거처리 모델”, 디지털포렌식연구, 10(1), 2016
1. 이완규, “디지털 증거 압수 절차상 피압수자 참여 방시과 관련성 범위 밖의 별건 증거 압수 방법”, 형사법의 신동향 통권 제48호, 2015. 9.
1. 전승수, “디지털 정보에 대한 압수수색영장의 집행”, 법조 통권 670호, 2012. 7.
1. 조대호, “각국의 디지털증거 압수절차 및 증거활용에 관한 연구 - 관련성 있는 정보의 선별 범위 및 당사자 참여권의 인정 범위를 중심으로”, 국외훈련검사 연구논문집(Ⅰ) 미국
1. 원용기, “디지털증거에 대한 계층적 접근 방안 연구”, 서울대학교 석사학위 논문, 2016
1. 박희영, “사이버범죄방지조약의 형사절차법 규정의 평가와 현행 형사절차법 관련 규정의 개정방향”, 선진상사법률연구, 제46호, 2009
1. 박래옥, “클라우드 스토리지의 효율적인 압수수색을 위한 방안”, 서울대학교 석사학위 논문, 2016
1. 남성우, “휴대용 디바이스에 연관된 전자정보의 압수수색과 영장주의”, 사법연수원, 2017년도 법관연수 어드밴스(Advance) 과정 연구논문집(전문 분야 소송의 주요쟁점, 조세/상사소송)
1. 강석한, “전자정보 압수수색에서의 참여권 보장을 위한 기술적 조치 연구 - 임계 암호기술을 이용하여”, 서울대학교 석사학위논문, 2017
1. 오미경, “디지털 증거 선별 압수수색에 다른 문제점 해결을 위한 기술적 방안 연구 - 동형암호를 이용하여, 서울대학교 석사학위논문, 2019
1. 압수수색영장 실무, 대법원 법원행정처, 2016

1. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations(3rd ed.), OLE (2009)

<Abstract>

A study on expedited preservation of digital evidence using public key cryptography

Because of advancements in digital technology, search and seizure for electronically stored information have become essential to criminal investigation. Data vulnerability such as loss or modification has made data retention more important. Meanwhile, there are growing concerns over the possibility of the intrusion on privacy caused by search and seizure for electronically stored information, owing to the massiveness and invisibility of such forms of information.

This study dealt with expedited preservation of digital evidence using public key cryptography, which enables securing personal privacy. This study also showed that expedited preservation of digital evidence using public key cryptography can be applied at various points in criminal proceedings.

Keywords: expedited preservation of digital evidence, data retention, public key cryptography, search and seizure, electronically stored information, data vulnerability