Crisisonomy Vol.13 No.8, 85-100
ISSN 2466-1198 (Print) ISSN 2466-1201 (Online) http://dx.doi.org/10.14251/crisisonomy.2017.13.8.85

Crisisonomy

A Study on Improvements of the Legal System for Requesting the Third Party Information in Crime Investigation

Gi Bum Kim[+]

International Cybercrime Research Center, Korean National Police University, 100-50 Hwangsan-gil, Sinchang-myeon, Asan-si, Chungcheongnam-do, Korea

Abstract

As the importance of the third party information as an investigative lead increases, there has been a growing concern about privacy violation. Although the criminal procedure law and other related laws in Korea require a warrant issued by a judge to obtain the third party information, this warrant requirement does not properly reflect a changing investigative environment based on the ICT mechanism. This has also raised controversy over the legality of the current practices of law enforcement agencies with respect to requesting the third party information. Therefore, this paper proposes to establish a “basic law of third party information request” which requires a court’s permission in lieu of warrant; systemizes a notification structure to guarantee the rights of data subjects and third parties, and establishes procedures for information disclosure and third party objection. In terms of the effectiveness of crime investigation, this law needs to set out the procedures for urgent request of information and the system of emergency protection order and provide a non-facing/copy execution of a warrant and mandatory identification of an investigator.

Key words: third party information, communication secrets, search and seizure, criminal procedure, digital evidence

Ⅰ. 정보환경의 변화에 따른 법의 흐름

인터넷 인프라와 정보통신 서비스의 발달에 따라 개인이 생산하는 정보가 제3자에 의해 수집・보관되는 경우가 많아지고 있다(Seul, 2009: 145). 과거에는 주거지, 사무실이나 자신의 저장매체에 문서, 사진, 파일을 보관하였으나 이제는 포털, 통신사, 은행 등 제3자의 시스템에 의해 전자우편, 통화내역, 금융거래 내용이 보관되고 있다. 다가올 지능정보사회(Sung & Hwang, 2017: 4)에서 사물인터넷, 인공지능, 블록체인, 로봇에 의한 서비스가 본격화되면 제3자 정보는 기하급수적으로 증가할 것이다. 이와 같은 제3자 정보는 범죄수사에서 혐의를 입증하거나 용의자를 추적하는데 중요한 단서로 활용되기 때문에 전자우편, 금융거래내용의 압수수색뿐만 아니라 통신감청, 기지국 실시간 추적 등 다양한 수사방법이 동원되고 있다. 이로 인하여 프라이버시 침해에 대한 우려가 커지고 있다.

이에 우리 헌법은 사생활의 비밀과 자유(제17조), 통

[+] Corresponding author: Gi Bum Kim, Tel. +82-41-968-2642, Fax. +82-41-968-2689, e-mail. freekgb02@gmail.com

신비밀을 침해받지 않을 권리(제18조), 개인정보자기결정권[1] 등 다양한 형태의 기본권으로 정보에 대한 프라이버시를 보호하고, 법관이 발부한 영장에 의해서만 침해할 수 있도록 영장주의를 천명하고 있다(제12조, 제16조). 형사소송법에서도 수사기관이 영장에 의하여 정보를 취득할 수 있도록 그 요건과 절차를 엄격히 통제하여 헌법 정신을 구현하고 있다. 개별법-통신비밀보호법, 신용정보의 이용 및 보호에 관한 법률(이하 "신용정보법"이라 함), 금융실명거래 및 비밀보장에 관한 법률(이하 "금융실명법"이라 함), 국세기본법, 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률(이하 "클라우드컴퓨팅법"이라 함)-에서도 법관의 영장이나 법원의 허가에 의해서만 제3자 정보를 취득할 수 있도록 규정하고 있다.

하지만 형사소송법상 영장 규정은 유체물과 대별되는 정보의 본질적 특성, 범죄혐의와 관계없는 제3자를 대상으로 집행한다는 특성, 정보통신 기술 환경의 특성을 충분히 수용하지 못해 위법수사에 대한 논란이 제기되고 있다. 즉, 팩스・전자우편 등 비대면・사본으로 영장을 제시하고, 이때 정보주체나 변호인의 참여가 보장되지도 않는다. 제3자는 권리 침해의 직접적인 당사자가 아니라는 이유 등으로 수사기관은 압수목록이나 수색증명서를 교부하지 않고 있다. 이처럼 제3자 정보에 대한 영장집행은 형사소송법에서 규정하는 절차를 준수하지 못하거나 준수할 실익이 없는 경우가 발생하고 있다.

그런데도 정부와 국회는 2011년 형사소송법에 정보에 대한 출력・복제 원칙 신설(제106조 제3항) 등 일부만 개정할 뿐 제3자 정보에 대한 논의는 진행조차 하지 못했다. 전기통신 감청, 디지털증거, 전자우편, 위치정보, 개인정보 등 개별적 정보유형에 대한 입법적・해석적 연구만 이루어졌을 뿐 제3자 정보에 관한 연구는 거의 없었다. 형사소송법이 아닌 개별법에 제3자 정보 요청 절차를 계속 마련함에 따라 법률이 산재하고 중첩과 흠결이 발생하고 있다. 제3자 정보 요청에 있어 형사소송법상 영장제도가 적합하지 않음에도 제・개정되는 개별법에서는 관행적으로 "법관이 발부한 영장"에 의하여 정보를 취득하도록 입법화하고 있다.

따라서 본 논문에서는 제3자 정보 요청에 적합하지 않은 형사소송법상 영장제도를 대체하고, 개별법에 소관 정보별로 산재되어 있는 입법체계의 문제를 해결하기 위한 법률적 대안을 제시하고자 한다. 이를 위해 먼저 제3자 정보의 개념과 프라이버시 보호 수준을 살펴보고, 현행 입법체계와 각 개별법의 비교분석을 통해 우리법제의 문제점을 도출할 것이다. 이후 형사소송법상 영장제도는 제3자 정보 요청 절차에 부합하지 않는다는 논증을 한 후 이에 대한 입법적 개선방안을 제시하고자 한다.

II. 제3자 정보의 개념과 보호수준

1. 제3자 정보

1) 정보 개념에 대한 해석과 법해석학적 한계

통상 정보는 "양심・사상・의견・지식 등의 형성에 관련이 있는 일체의 자료"(Kwon, 2009b: 496), 내지 "어떠한 형태로든 표현된 모든 종류의 사상・의견・사실・감정・자료・지식 등이 특정한 목적을 위하여 조직화된 의사형성과 인식의 기초자료이며 판단자료가 되는 것"(Kwon, 2004: 90)으로 정의할 수 있다.

개별법을 살펴보면 형법은 컴퓨터등장애업무방해죄(제314조 제2항), 컴퓨터등사용사기죄(제347조 제2항)에서 구성요건으로 '허위의 정보'를 두고 있는데, 여기에서 정보는 "부호 또는 계속적 기능에 따라 정보처리를 위하여 코드화된 지식"(Lee, 2010: 355)을 말한다. 형사소송법은 정보의 출력・복제 원칙에서 "기억된 정보의 범위를 정하여"(제106조 제3항), 전문법칙예외의 요건 중의 하나인 자필이거나 그 서명 또는 날인의 적용을 배제하는 대상인 "문자・사진・영상 등의 정보"(제313조, 제314조), 증거법에서 "도면・사진・녹음테이프・비디오테이프・컴퓨터용 디스크, 그 밖에 정보를 담

1) 헌법재판소 2005. 5. 26. 선고 99헌마513 결정

기 위하여 만들어진 물건"(제266조의3 제6항, 제292조의3) 등에서 '정보'라는 용어를 사용하고 있다. 먼저 "기억된 정보"와 "문자・사진・영상 등의 정보"는 유체물과 대별되는 전자적(아날로그+디지털) 데이터를 의미하는 것으로 볼 수 있다. 이 중 디지털 데이터는 아날로그 데이터와 대별하여 "디지털 형태로 저장되거나 전송되는 범죄 증거로서 가치 있는 정보"(Yang, 2006: 20-21; Jo, 2010: 68), "컴퓨터 또는 기타 디지털 저장매체에 저장되거나 네트워크를 통해 전송 중인 자료로서 법정에서 신뢰할 수 있는 증거가치가 있는 정보"(Lee, 2011: 65)라고 정의되고 있다. 반면, 정보를 담기 위한 물건으로 컴퓨터용 디스크에다가 도면・사진까지 포함하는 것은 디지털 데이터뿐만 아니라 유체물에 기록・내포되어 있는 데이터, 인간의 오감에 의해 인식할 수 있는 데이터까지 포함하는 것으로 보여 진다.

이처럼 정보는 통상적인 개념과 형사법에서의 개념이 다르고, 형법과 형사소송법의 용례에서도 차이가 있을 뿐만 아니라 형사소송법 내에서도 다양하게 해석되고 있어 아직까지 체계화되지 못하고 있다. 하지만 정보의 형태가 전자적 데이터를 비롯하여 다양한 형태로 존재하고, 정보에 대한 프라이버시를 보호하기 위해 외연을 확대하여야 한다고 볼 때 "양심・사상・의견・지식 등의 형성에 관련이 있는 일체의 자료"(Kwon, 2009b: 496)를 의미하는 통상적인 정보의 의미 즉, 헌법학적 개념이 타당해 보인다. 이런 전제 하에 범죄수사에서 정보는 "범인과 범죄사실을 규명하는데 사용되는 무형의 자료"로 유체물에 기록・내포되어 있는 데이터, 아날로그와 디지털을 포함한 전자적 데이터 그리고 인간의 오감에 의해 인식할 수 있는 데이터를 모두 포함하는 것으로 정의할 수 있을 것이다.

2) 제3자 정보 개념의 의의

제3자 정보의 개념을 논의하기에 앞서, 먼저 제3자의 개념을 정의할 필요가 있다. 정보 주체 내지 대상의 범위를 확정하기 위해 선행되어야 할 해석학적 작업이다. 통상 제3자는 당사자를 제외한 나머지를 의미한다. 통신비밀보호법은 당사자에 대하여 "우편물의 발송인과 수취인, 전기통신의 송신인과 수신인"이라고 규정(제2조 제4호)하여 직접적 관련자를 의미하고 있다. 대법원은 당사자 일방의 동의를 얻어 대화내용을 녹음한 제3자의 행위를 불법감청으로 판단한 판례[2]에서 당사자를 제3자와 대별되는 개념으로 보았다. 형사소송법은 제3자 출석요구 조항(제221조)에서 제3자를 "피의자가 아닌 자"라고 규정하고 있다. 제3자와 유사한 참고인은 "피의자 이외의 제3자로서 수사기관에게 일정한 체험사실을 진술하는 자"로 정의되고 있다.(Sin, 2016: 91) 이렇게 볼 때 제3자는 "처분을 받는 자" 중 피의자 아닌 자로 범죄혐의와 관련이 없는 자로 볼 수 있다. 본 논문에서는 수사기관에게 정보를 제공해야할 법적 근거가 있는 자를 대상으로 하기 위해 사업자와 공공기관으로 제한하고자 한다(이하 '사업자'로 통칭하기로 함).

이를 바탕으로 앞서 설명한 정보의 개념과 결합하면 범죄수사에서 제3자 정보는 "사업자가 보관하거나 취득할 수 있는 범인과 범죄사실을 규명하는데 사용되는 무형의 자료"라고 정의할 수 있다. 전기통신사업자의 가입자정보, 접속기록, 전자우편, 문자메시지, 요금결제내역, 위치정보, 병원의 환자정보, 진료기록, 신용카드회사의 카드거래내역, 금융기관의 입출금내역, 인터넷뱅킹 접속기록, 국세청의 과세정보 등이 그 예가 될 것이다. 이처럼 제3자 정보의 개념을 논의하는 이유는 제3자 정보가 과거와 달리 형사법적 가치가 크고 중요한 증거능력 및 증명력을 가지고 있음에도 형사소송법상 당사자가 아니라는 점에서 절차 규정이 미흡하기 때문이다. 이하에서는 이러한 문제의식을 바탕으로 제3자 정보에 대한 법적 쟁점들을 검토할 것이다.

2) 대법원 2002.10.8. 선고 2002도123 판결; 대법원 2010.10.14. 선고 2010도9016 판결

2. 제3자 정보의 보호 수준

제3자 정보에 대하여 피의자가 직접 보관하는 정보와 동등한 수준에서 프라이버시를 보호해야 하는지에 관한 쟁점이 있다. 우리나라는 동등하게 판단하여 영장주의를 채택하고 있지만 미국에서는 프라이버시 보호 수준을 낮게 판단하여 영장주의 대상으로 보고 있지 않다.

미국 연방대법원은 1976년 United States v. Miller 판결[3]에서 자신의 정보를 제3자에게 제공한 경우 사생활에 대한 합리적 기대를 가지지 못하기 때문에 연방수정헌법 제4조에 의해 보호받을 수 없다는 제3자 원칙(The Third-Party Doctrine)을 확립한 바 있다.(Chun, *et. al.*, 2015: 329; Kwon, 2011: 239) 금융정보는 계좌명의자가 자발적으로 금융기관에 제출한 것으로, 수사기관에 제공될 위험을 감수한 것으로 보아 영장의 대상이 아니라고 보았다(Lee, 2008: 73-74). 1979년 Smith v. Maryland 판결[4]에서도 발신자가 전화번호의 착·발신기록을 전화회사에 제공한 것으로 국가에 제출될 위험을 스스로 부담하였기 때문에 수색영장이 필요없다고 판단하였다.(Kwon, 2011: 239) 이러한 입장은 1976년 이래 40년간 일관되게 유지되고 있어 제3자 정보 중 금융정보, 통화내역, 접속기록 등 비내용 정보는 영장이 아닌 제공요청(Subpoena)이나 법원의 제출명령에 의하여 제공되고 있다.

이에 반하여 디지털 시대에는 제3자 원칙이 변경되어야 한다는 주장도 제기되고 있다. Miller 판결에 부기된 반대의견은 ① 개인이 금융정보를 자발적으로 제공했다기보다 현대사회에서 살아가기 위한 불가피한 선택이고, ② 설령 자발적으로 제공했다 하더라도 수사기관에 제공될 것이라는 위험까지 감수했다고 보기는 어려우며, ③ 그 정보에 대한 비밀이 보장될 것으로 기대했을 것이라고 적시하고 있다.[5] 2012년 연방대법원은 United States v. Jones 판결[6]에서 별개의견으로 "개인이 자발적으로 제3자에게 정보를 공개하였을 경우 프라이버시에 대한 합리적 기대가 상실된다는 전제를 재고해야 한다."(Edward, 2013), "개인이 일상업무를 수행하는 과정에서 대량의 정보가 제3자에게 제공되는 디지털 시대에 부적합하다."고 판단하기도 하였다.[7] 나아가 독일은 연방헌법재판소에서 제3자 보관 전자우편에 대해 명의자는 제3자가 자신의 전자우편을 또 다른 사람에게 전달하는 것을 차단할 기술적 수단이 없기 때문에 기본권 주체를 특별히 보호해야 한다고 판결하였다.[8] 이와 같은 일련의 흐름들은 제3자 정보에 대하여 피의자 보관 정보와 동일한 수준에서 프라이버시를 보호해야 할 필요가 있다는 것을 보여주고 있다.

과거에 제3자 정보는 단순히 금융거래내역, 통화내역 등 객관적인 사실에 관한 내용이었지만 최근에는 통신내용, 위치정보 등 다양한 정보, 특히 개인의 사생활과 밀접하게 관련된 정보들이 결합되면서 보호가치가 더욱 커지고 있다. 정보주체가 제3자의 서비스를 통해 다양한 사회활동과 경제활동을 영위하고 있는 상황에서 제3자 정보에 대한 권리 보호 수준을 낮게 설정하는 것은 국민 전체의 권리보호 수준을 현저하게 떨어뜨리는 결과를 초래할 것이다. 일반적으로 정보주체가 금융기관과 거래를 할 때 자신의 정보를 공개할 의사가 있다거나 수사기관에 자발적으로 제공할 의사가 있다고 보기 어렵고, 공개될 위험을 인수하였다고 볼 수도 없다.(Oh, 2015: 392) 금융실명법에서도 금융회사 종사자에게 명의인 요구나 동의 없이 금융정보를 제공·누설하지 못하도록 규정하고 있어 단순히 금융기관만의 정보라고 볼 수도 없는 상황이다. 따라서 금융정보, 통화내역정보 등 비내용적 정보는 지금처럼 법관의 영장

3) United States v. Miller, 425 U.S. 435 (1976)
4) Smith v. Maryland, 442 U.S. 735 (1979)
5) United States v. Miller, 425 U.S. 435 (1976)
6) United States v. JONES, 615 F. 3d 544 (2012)
7) 소토마이어 대법관 별개의견(Justice Sotomayor concurring opinion in Jones), p.957
8) BVerfGE 120, 43 (Rn. 46 ff.)

에 의해서만 제공할 수 있도록 사법적 통제 하에 두는 것이 바람직할 것이다.

Ⅲ. 제3자 정보 요청 입법체계 및 법제분석

1. 입법체계 개관

1) 개별법 중심의 입법

형사소송법에서 압수수색 규정은 2007년 위법수집 증거배제법칙 명문화(제308조의2), 2011년 압수수색 요건에 관련성 추가(제106조 제1항, 제109조 제1항, 제215조 등), 정보의 출력·복제 원칙 명문화(제106조 제3항), 영장작성 시 전자우편의 작성기간 표기(제114조 제1항) 등에 관한 사항만 개정되었을 뿐 제정 이래 지난 60년 동안 거의 변경되지 않았다. 이처럼 형사소송법의 개정이 어렵자 제3자 정보 요청 절차는 비교적 입법이 용이한 개별법 제·개정을 통해 이루어졌고, 그 결과 통신비밀보호법, 신용정보법, 금융실명법, 전기통신사업법 등 다양한 법률에 만들어지게 되었다. 즉, 1993년 전기통신 감청은 형사소송법상 압수수색 형태로 집행될 수 없다고 보아 통신비밀보호법을 제정하여 법원의 허가를 받도록 하였다(Oh, 2015: 69). 1995년 수사기관이 개인신용정보를 요청 할 경우 영장에 의하도록 신용정보법을 제정하였고, 1997년 그간 형사소송법 상 사실조회에 근거하여 처리하던 금융거래정보를 영장에 의해서만 제공할 수 있도록 금융실명법을 만들었다. 통신사실 확인자료는 2001년에 지방검찰청 검사장의 승인을 받도록 하였다가 2005년에 다시 법원의 허가를 받도록 통신비밀보호법을 개정하였다. 2009년 전기통신 압수수색은 형사소송법에 근거하면서도 집행통지는 통신비밀보호법에 규정을 신설하는 기이한 입법이 이루어지기도 하였다(Im, 2016: 205). 2015년 클라우드컴퓨팅법에도 제3자 정보 요청을 영장에 의하도록 규정하는 등 개별법을 제·개정하는 입법 방식은 지금까지 계속되고 있다.

2) 형사소송법상 영장 절차 고수

제3자 정보 요청 법제는 크게 법관의 영장제도와 법원의 허가제도로 나눌 수 있다. 법관의 영장제도는 형사소송법, 개별법에서 '법관의 영장'에 의하도록 규정한 경우, 개별법에 근거가 없어 결국 형사소송법상 영장 절차를 따라야 하는 경우로 나눌 수 있고, 법원 허가제도는 통신비밀보호법에 규정된 통신제한조치와 통신사실 확인자료 절차가 있다. 개별법에서 법관의 영장에 의하도록 규정한 경우는 금융실명법, 신용정보법, 국세기본법, 지방세기본법, 관세법, 복권및복권기금법, 본인서명사실확인등에관한법률, 의료법, 자유무역협정의 이행을 위한 관세법의 특례에 관한 법률, 정치자금법, 클라우드컴퓨팅법 등이 있고, 개별법에 근거가 없는 경우는 개인정보보호법, 위치정보법, 지능형전력망의 구축 및 이용촉진에 관한 법률(이하 "지능형전력망법"이라 함) 등이 있다.

이와 별도로 형사사법절차 전자화 촉진법(이하 "형사절차전자화법"이라 함)에서는 정보 자체가 형사사법 목적으로 수집한 만큼 영장 대상이 안 된다고 보았고, 특정 금융거래정보의 보고 및 이용 등에 관한 법률(이하 "특정금융정보법"이라 함)에서는 영장 없이 제공할 수 있도록 법률에 명시한 반면, 전기통신사업법은 통신자료 요청에 관하여 영장이 아닌 관서장 승인에 의하도록 규정하고 있다. 이처럼 법원의 허가제도를 채택하는 통신비밀보호법과 영장주의가 적용되지 않는 형사절차전자화법, 특정금융정보법, 전기통신사업법을 제외한 대부분의 법률들은 형사소송법상 압수수색 영장의 절차를 따르고 있다.

2. 현행법률 비교분석

1) 요청 요건

형사소송법을 비롯한 각 개별법에서 제3자 정보 요청 요건을 다르게 규정하고 있다. 형사소송법 상 전기통신 압수수색은 일반 압수수색과 동일하게 범죄정황, 관련성, 필요성을 요건으로 하고 있다. 통신비밀보호법상 통신사실 확인자료 요청은 "수사 또는 형의 집행을

위하여 필요한 경우"를 요건으로 하고(제13조 제1항), 통신제한조치는 "범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우"로 제한하고 있다(제5조 제1항). 금융실명법은 "사용 목적에 필요한 최소한의 범위"에서 제공하도록 범위만을 규정하고(제4조 제1항), 신용정보법은 이에 대한 별다른 규정(제32조 제6항)이 없어 결국은 형사소송법상 압수수색 요건과 동일하다고 해석해야 할 것이다. 전기통신사업법은 "재판, 수사, 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여"라고 목적만 규정하고 있을 뿐 별도의 요건은 없다(제83조 제3항).

통신비밀보호법 상 통신제한조치는 비공개적으로 이루어지고 침해의 정도가 크기 때문에 압수・수색・검증보다 요건이 엄격한 것은 타당하다. 내용정보를 대상으로 하는 전기통신 압수수색이 비내용 정보를 대상으로 하는 통신사실 확인자료보다 엄격한 요건을 요구하는 것 또한 수긍할 수 있다. 하지만 똑같은 비내용 정보를 대상으로 하고 있는 금융실명법, 신용정보법 상 영장과 통신비밀보호법상 통신사실 확인자료 간의 요청 요건의 차이는 납득하기 어렵다.

2) 집행방법

형사소송법은 처분 받는 자에게 영장을 제시하고(제118조), 검사나 사법경찰관리가 이를 집행하도록 규정(제115조 제1항)하고 있다. 전자우편・팩스를 이용한 비대면・사본 제시에 대해서 2015년 서울고등법원은 "이메일은 압수・수색 당시 영장 원본이 피압수・수색 당사자에게 제시되었다고 볼 수 없을 뿐만 아니라 나아가 압수조서와 압수목록이 작성되어 압수목록이 피압수・수색 당사자에게 교부되었다고 볼 수 없는 이상, 헌법과 형사소송법 제118조, 제129조가 정한 절차를 위반하여 수집한 위법수집증거로 원칙적으로 유죄의 증거로 삼을 수 없다."고 판결하여 부정적으로 보고 있다.[9)]

통신비밀보호법, 금융실명법, 신용정보법, 국세기본법, 지방세기본법 등 대부분 개별법에서도 서면 또는 문서로 요청하도록 규정하면서도 비대면・사본집행이 허용되는지에 대해서는 모호하다. 통신제한조치 및 통신사실 확인자료는 통신비밀보호법 시행령에 사본을 발급하거나 신분에 관한 증표를 제시하는 경우 모사전송에 의할 수 있다고 규정하고 있어 논란은 없다(제37조 제5항). 금융실명법과 신용정보법은 전국은행연합회의 금융실명거래 업무해설에서 팩스 집행을 허용하고 있다.[10)] 국세기본법, 지방세기본법은 별도의 법률적 근거나 규정 없이 수사현장에서는 관행적으로 팩스・전자우편 또는 공문서에 첨부하는 방식으로 비대면・사본집행을 하고 있다.

정보통신의 발달에 따라 영장을 집행할 때 강제력 행사보다 덜 침해적인 비대면・사본 제시방법이 허용될 필요가 있음에도 통신비밀보호법을 제외하고 대부분의 법률에서 이에 대한 명시적 근거를 두지 않아 논란이 계속되고 있다.

3) 긴급집행

형사소송법은 원칙적으로 사후영장을 불허하면서 예외적인 경우에 한하여 영장 없는 압수수색을 허용하고 사후영장을 받도록 규정하고 있다(제216조, 제217조). 통신비밀보호법은 "국가안보를 위협하는 음모행위, 직접적인 사망이나 심각한 상해의 위험을 야기할 수 있는 범죄 또는 조직범죄 등 중대한 범죄의 계획이나 실행 등 긴박한 상황에 있고 제5조 제1항 또는 제7조 제1항 제1호의 규정에 의한 요건을 구비한 자에 대하여 제6조 또는 제7조 제1항 및 제3항의 규정에 의한 절차를 거칠 수 없는 긴급한 사유"가 있는 때에 긴급통신 제한조치를 할 수 있고(제8조), "관할 지방법원 또는 지원

9) 서울고등법원 2015. 6. 25. 선고 2014노2389 판결

10) 은행연합회. 2016. 금융실명거래 업무해설. http://www.kfb.or.kr/new_data/etc.html?S=GAE&m=view& table=PDS3&no=274&start=0&mode=&field =&s_que(2017.7.20. 최종방문)

의 허가를 받을 수 없는 긴급한 사유"가 있는 때에 통신사실 확인자료를 요청할 수 있다(제13조 제2항). 금융실명법에는 긴급집행에 대한 별도의 규정이 없는 반면, 신용정보법은 "범죄 때문에 피해자의 생명이나 신체에 심각한 위험 발생이 예상되는 등 긴급한 상황"에서 영장을 발부받을 시간적 여유가 없을 경우에 영장 없이 제공할 수 있도록 규정하고 있다(제32조 제6항 제6호). 전기통신사업법도 긴급한 사유가 있는 때에는 서면이 아닌 방법으로 긴급집행하고 사후에 승인을 받아 송부하도록 규정하고 있다(제83조 제4항).

이처럼 개별법마다 긴급집행 절차의 존부와 긴급성의 요건이 다르고, 개별법에 별도의 규정이 없는 경우 형사소송법이 준용되는지도 해석에 맡겨져 있다. 나아가 사후 승인절차, 허가시간, 승인 기각 시 정보의 처리 등에서 많은 차이를 보이고 있다.

4) 협조의무

형사소송법상 영장은 강제력을 전제하기 때문에 실무상 협조의무를 논할 실익은 없다. 통신비밀보호법에서는 법원의 허가 제도를 두어 통신제한조치 및 통신사실 확인자료에 대한 협조의무를 규정(제15조의2)하고 있는 반면 금융실명법, 신용정보법에는 협조의무에 관한 언급이 없다. 지능형전력망법에서는 "성실히 협의에 응하여야 한다."(제23조 제4항), "협의를 할 수 없거나 협의가 성립되지 아니하는 경우에는 산업통상자원부장관에게 대통령령으로 정하는 바에 따라 조정을 요청"할 수 있다고 규정(제23조 제5호)하여 다양한 입법 형태를 보여주고 있다.

형사소송법에 제3자의 협조의무가 규정되어 있지 않지만 대부분의 경우 제3자의 협조에 의하여 영장이 집행되고 있다고 볼 때 수사현장과 법률 간의 괴리가 있는 것은 사실이다. 똑같은 전기통신사업자라도 영장에 의해 전기통신을 압수수색하면 협조의무가 없지만 법원 허가에 의해 통신제한조치와 통신사실 확인자료 요청을 하면 협조의무가 발생하고 있다.

5) 통지제도

형사소송법 상 압수수색에서는 원칙적으로 통지제도가 없었으나, 2011년 개정을 통해 정보를 압수수색한 경우 침해를 당하는 정보주체에게 통지하고(제106조 제4항), 전기통신 압수수색을 한 경우에는 발신인이나 수신인에게 통지하도록 규정하였다(제107조 제3항). 하지만 아직까지 세부절차를 마련하지 못해 수사현장에서 집행되지 않고, 전기통신 압수수색에 대해서는 통신비밀보호법에 규정된 압수・수색・검증 집행통지 조항에 따라 이행하고 있다(제9조의3). 통신비밀보호법(제9조의2, 제13조의3), 금융실명법(제4조의2), 신용정보법(제32조 제7항)에서 통지제도를 두고 있는 반면, 국세기본법 등 국가기관을 대상으로 집행하는 경우나 의료법・클라우드컴퓨팅법 등 기타 개별법에서 영장제도를 준용하는 경우에는 통지제도를 두고 있지 않다. 그래서 국세청을 대상으로 과제정보를 압수수색한 경우 금융실명법, 신용정보법과 달리 정보주체가 집행사실을 알 수 있는 절차가 없다.

통지 주체에 관하여 형사소송법상 정보 압수수색에 따른 정보주체 통지(제106조 제4항)와 전기통신 압수수색(통신비밀보호법 제9조의3), 통신비밀보호법 상 통신제한조치(제9조의2)와 통신사실 확인자료(제13조의3), 신용정보업법 상 개인신용정보(법 제32조 제7항, 시행령 제28조 제12항 별표2의2)는 수사기관이 통지해야 하는 반면, 금융실명법 상 금융거래정보는 제3자인 금융기관이 통지하도록 규정(제4조의2)하고 있다. 또한 통신비밀보호법(제17조 제2항 제3호)은 통신제한조치에 대한 집행통지를 불이행한 경우 형사처벌하고 있으나, 송・수신이 끝난 전기통신의 압수・수색・검증이나 통신사실 확인자료의 경우에는 벌칙규정이 없다(Im, 2016: 217). 통지제도의 기산점과 기간에 관하여 통신비밀보호법은 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지 결정을 제외한다)을 한 경우 그 처분을 한 날부터 30일 이내(제9조의2, 제9조의3, 제13조의3), 금융실명법은 제공한 날로부터 10일 이내(제4조의2), 신용정보법은 제공한 날로부터 6개월 이

내에 통지하도록 규정(법 제32조 제7항, 시행령 제28조 제12항 별표2의2)하고 있다. 신용정보법은 통지가 불가피할 경우에는 인터넷 홈페이지 게재 등을 활용하여 고시하는 방법도 허용하고 있다(제32조 제7항).

통지유예 제도에 관하여 형사소송법(전기통신 압수수색 포함)은 관련규정이 없고 금융실명법과 신용정보법은 동일하게 규정되어 있으나 이들은 통신비밀보호법과는 다르다. 통신비밀보호법(통신제한조치와 통신사실 확인자료)은 ① 국가의 안전보장・공공의 안녕질서를 위태롭게 할 현저한 우려가 있는 때 ② 사람의 생명・신체에 중대한 위험을 초래할 염려가 현저한 때에는 그 사유가 해소될 때까지 유예할 수 있다(제9조의2 제4호, 제13조의3 제2항). 이는 별다른 유예기간의 제한을 두고 있지 않다는 비판이 있다(Im, 2016: 205). 금융실명법과 신용정보법은 동일하게 ① 사람의 생명이나 신체의 안전을 위협할 우려가 있는 경우 ② 증거인멸, 증인 위협 등 공정한 사법절차의 진행을 방해할 우려가 명백한 경우 ③ 질문・조사 등의 행정절차의 진행을 방해하거나 과도하게 지연시킬 우려가 명백한 경우로 규정하고 있다(금융실명법 제4조의2 제2항, 신용정보법 제32조 제7항, 시행령 제28조 제12항). 다만, 금융실명법은 ①항의 경우에는 유예 기간에 제한이 없고, ②항, ③항의 경우에는 최대 6개월까지 유예할 수 있는 반면, 신용정보법은 금융위원회의 고시 기간 동안 유예할 수 있도록 규정하고 있다.

이처럼 개별법에서 통지(유예) 제도의 존부, 통지주체, 통지유예 사유와 기간 등이 모두 상이하게 규정되어 법집행에서 혼선이 발생하고, 피의자의 권리 보호에도 한계가 있다.

6) 행정통제

형사소송법 상 압수수색은 영장을 제시만하기 때문에 제3자에게 정보요청 및 제공 내역에 대한 보관의무가 없다. 통신비밀보호상 수사기관은 통신제한조치 집행 대장을, 전기통신사업자는 여기에 통신제한조치허가서, 긴급감청서 표지 사본을 더하여 3년간 보관하여야 한다. 수사기관과 법원은 통신사실 확인자료 요청사실을 기재한 대장과 통신사실 확인자료 요청서 등을 비치하여야 하고(제13조 제5항, 제6항), 전기통신사업자는 이를 7년간 비치하여야 한다(제13조 제7항). 통신제한조치에 관한 각종 기록의 보관기관은 법률이 아닌 대통령령에 3년으로 규정한데 반하여 통신사실 확인자료는 해당법률에 7년으로 규정한 것은 프라이버시 침해 정도를 고려했을 때 적절하다고 볼 수 없다. 금융실명법에서는 금융기관에게 관련정보를 5년간 보관(제4조의3 제1항)하도록 강제하는 반면 신용정보법에서는 별다른 규정이 없다.

형사소송법은 국회 또는 부처에 영장 집행결과를 보고하는 제도가 없다. 반면, 통신비밀보호법 상 전기통신사업자는 수사기관 등에 통신사실 확인자료를 제공한 때에는 자료제공현황 등을 연 2회 과학기술정보통신부장관에게 보고하여야 하고(제13조 제7항), 보고하지 아니하였거나 관련 자료를 비치하지 아니한 경우 벌칙규정을 두고 있다(제17조 제2항 제4호). 하지만 검사 또는 사법경찰관은 관련 자료에 대한 비치기간도 정해져 있지 아니하고 위반에 따른 벌칙규정도 없다(Kim, 2014: 19). 국회 의 상임위원회와 국정감사 및 조사를 위한 위원회는 특정한 통신제한조치에 대하여 통신제한조치를 청구하거나 신청기관의 장 또는 집행한 기관의 장에게 보고를 요구할 수 있다(제15조 제1항). 금융실명법은 금융위원회에 금융거래정보 제공 등에 관한 통계자료를 매년 정기국회에 보고하도록 규정하고 있다(제4조의4).

행정통제는 정보의 성격상 소관부처는 다를 수 있겠지만 보고의 내용, 방법, 주기, 위반 시 벌칙규정 등에 있어서 차이를 두어야할 이유를 찾기 어렵다.

7) 불복제도

형사소송법 상 검사 또는 사법경찰관의 구금, 압수 또는 압수물의 환부에 관한 처분과 형사소송법 제243조의2에 따른 변호인의 참여 등에 관한 처분에 불복이 있는 경우 준항고(제417조)와 재항고(제415조)를 통해

처분을 취소할 수 있다. 영장 제도를 채택하는 금융실명법, 신용정보법 등은 준항고와 재항고를 통해 다툴 여지가 있지만, 법원의 허가제도 등을 채택하는 통신비밀보호법과 전기통신사업법은 다툴 수 없고, 위법수집증거배제법칙에 의지할 수밖에 없다. 이렇게 볼 때 통신비밀호보법 상 전기통신사업자는 수사기관의 요청에 대한 협조의무를 부담하면서도 불복절차가 없어 영장제도에 비하여 제3자의 권리 보호가 미흡하다고 할 것이다.

3. 소결

제3자 정보 요청 법제는 형사소송법이 아닌 개별법제·개정 방식을 선호하여 산재되어 있고, 통신비밀보호법 등을 제외한 대부분의 개별법에서 형사소송법상 영장 제도를 채택하고 있다. 제3자 정보는 유체물 이상으로 범죄수사에서 활용되는 비중이 높지만 아직까지 입법적으로 미흡한 부문이 많다. 하지만, 개별법 입법방식은 요청 요건, 집행방법, 긴급집행, 협조의무, 통지제도, 행정통제, 불복제도 등에서 상이하게 규정하고 있어 법률 해석에 혼선을 유발하고, 피의자의 권리보호에도 한계를 보이고 있다. 개별법에서 법관의 영장에 따르도록 할 뿐 다른 절차에 대한 언급이 없어 형사소송법에 준용되는지 아니면 개별법에 근거가 없어 형사소송법을 준용할 필요가 없는지도 모호하다. 이러한 상황임에도 개별법을 제·개정할 때 "법관이 발부한 영장"이라는 문구를 입법 관행적으로 계속 사용되고 있다는 점이다.

Ⅳ. 제3자 정보 요청 절차와 영장 제도 간의 불합치성

1. 압수 개념의 제3자 정보 포섭 여부

무체물인 정보가 압수 대상이 될 수 있는지에 대한 논란이 있다.(Oh, 2015: 51) 학설은 ① 민법상 무체물이 물건에 포함된다는데 견해에 따라 압수 대상이 된다는 긍정설(Kim & Kim, 2006: 109; Park, 2007: 138-139), ② 정보는 유체물로 볼 수 없어 압수가 불가능하다는 부정설(Kang, 2010: 165-166; Park, 2009: 35; Tak, 2004: 26-28; Kwon, 2009a: 368-369), ③ 법규가 흠결된 상황에서 현실적 필요성이 절박하기 때문에 범죄사실에 대한 관련성이 인정되는 경우에 인정해야한다는 절충설(Won, 2004: 174), ④ 범죄와 관련된 정보만 저장된 컴퓨터는 압수할 수 있지만 관련없는 정보까지 저장하고 있는 컴퓨터는 압수할 수 없고, 수색만 할 수 있다는 일부 절충설(Oh, 1997: 76-80; Cho, 2010: 105) 등 다양하다(Kim, *et. al.*, 2011: 87).

미국은 연방형사소송절차규칙(Federal Criminal Rules of Procedure)에서 압수 대상에 정보를 추가하여 입법적으로 해소하였으나 혼란은 여전하다(Oh, 2015: 53). 잔존하는 점유의 이익에 손상이 없어도 정보를 복사할 당시 정보의 전송을 위해 케이블 연결 등 장비를 설치하기 때문에 유의미한 방해가 있다는 견해(Orin, 2005: 561)가 있는가 하면, 점유자 스스로가 컴퓨터 작동을 위해 접촉하는 행위도 유의미한 방해에 해당되는 오류가 발생한다며 반박하는 견해도 있다(Josh, 2011: 159).

판단컨대, 압수는 복사 또는 복제와 같이 점유권의 이전을 수반하지 않는 처분을 포함하는데 한계가 있다(Kim, *et. al.*, 2011: 88). 유체물에 대한 점유 획득을 전제로 하는 대륙법계 체제에서 압수대상으로 정보를 수용하는 법리구성은 어렵다(Oh, 2015: 52). 실제 우리나라 형사소송법도 정보에 관한 압수규정을 신설할 때 압수 대상인 증거물과 몰수물에 정보를 포함시키지 못하고(제106조 제1항), 결국 정보의 압수방법과 범위를 규정하는 방법으로 우회하였다(제106조 제3항). 금융거래내용을 추적할 때 일반영장이 아닌 금융정보추적용 영장을 사용하는 것도 일반적인 압수와는 다르다는 것을 시사한다(Oh, 2015: 386). 수사기관의 전기통신 감청도 형사소송법 상 영장제도에서 포섭할 수 없다고 보아 결국은 통신비밀보호법 상 허가제도로 해결하였다. 이렇게 볼 때 제3자 정보 역시 형사소송법 상 압수방식만을 고집할 것이 아니라 다양한 입법적 대안을 고려해볼 필요가 있을 것이다.

2. 영장 제도와의 괴리

1) 적법절차 위반 소지

제3자 정보 요청은 영장에 의하더라도 동의 또는 협조에 의해 집행되고 있다는 점(제106조), 검사 또는 사법경찰관리가 아닌 사실상 제3자에 의해 집행되고 있다는 점(제115조 제1항), 전자우편・팩스 등 비대면・사본으로 영장을 제시하고 있다는 점(제118조), 영장집행 과정에서 피의자나 변호인의 참여가 어렵다는 점(제121조), 권리 침해의 직접적인 당사자가 아닌 제3자에게 압수목록이나 수색증명서를 교부해야 하고, 이에 대한 실익이 크지 않다는 점(제128조, 제129조) 등에서 현행 형사소송법 절차와 상이한 측면이 많다. 새로운 정보나 수사방법이 등장하였으나 관련 법률에 근거가 없는 경우 형사소송법상 영장에 의하여 집행되는 경우가 있는데 이때 적절한 통제수단이 되지 못하거나 법률에 근거가 없는 집행이 될 수 있다. 또한 수사기관이 제3자의 협조로 충분히 집행이 가능함에도 강제적 집행권한을 사용하는 것은 비례성 원칙, 특히 상당성에 반한다는 비판을 면하기 어려울 것이다.

2) 범위의 과잉확대 및 과잉축소 등

용의자가 금원을 출금하는 CCTV 영상은 개인정보보호법상 범죄수사 목적만 입증되면 영장 없이 확보할 수 있지만 금융기관에서 금융거래내용으로 확대 해석하여 영장을 요구하는 경우가 많다. 신용카드회사가 보관하고 있는 정보 중에서 카드거래내역에 대한 정보를 제외한 해외출입내역, 택시 탑승기록, 톨게이트 통과내역이나 출금 위치・장소정보 또한 영장대상이 되고 있다.

한편, 형사소송법상 영장은 집행 시점 직후의 정보나 실시간 정보는 압수할 수 없기 때문에 집행대상과 범위가 과잉축소 되는 문제도 발생한다. 개별법에서 영장제도를 규정하고 있는 경우 제3자 정보에 대한 실시간 정보는 제공받을 수 없게 된다. 법원 허가제도를 채택하는 전기통신 감청과 통신사실 확인자료는 실시간 정보를 제공받을 수 있는 반면 영장제도를 채택하는 금융거래내용이나 신용카드 사용내용은 실시간 정보를 받을 수 없다.[11] 금융기관의 인터넷뱅킹 접속기록은 보관주체가 전기통신사업자가 아니기 때문에 통신비밀보호법 적용대상이 아니고, 접속기록은 금융거래정보가 아닌 통신사실 확인자료에 해당하기 때문에 금융실명법을 적용할 수 없다. 결국 인터넷뱅킹 접속기록을 금융거래정보로 해석하여 영장으로 집행할 경우 실시간 정보는 제공받을 수 없게 된다. 과거에는 전기통신사업자만이 실시간 정보를 제공할 수 있었으나 이제는 대부분의 서비스가 정보통신망에서 운용되고 있어 은행 등 다양한 사업자가 실시간 정보를 제공할 수 있음에도 영장의 한계에 묶여 활용되지 못하고 있다.

3) 피의자 권리보호 미흡

제3자 정보를 제공받을 경우 형사소송법에서 규정하는 변호인의 참여권 보장이 어렵다. 개별법에 참여권에 관한 규정이 없어 허용되지 않는다는 해석과 결국은 영장으로 집행하기 때문에 참여권이 보장되어야 한다는 해석이 대립할 수 있지만 제3자에게 집행할 경우, 어떤 경우에도 참여권 보장에 한계가 있다. 전기통신 압수수색은 형사소송법에 근거하기 때문에 참여권이 보장된다고 볼 수 있지만 수사실무에서는 영장집행에 급속을 요하는 때로 보아 피의자 또는 변호인에게 집행사실을 통지하지 않는 경우가 많아 사실상 보장되지 않고(제121조, 제122조), 통신비밀보호법에서는 참여권에 대한 별도의 언급이 없고 집행통지에 관한 규정만 두고 있을 뿐이다.

4) 입법의 사각지대 발생

개별법 중심의 입법체계는 상이한 규정과 적용 영역의 차이로 인해 일관된 법해석을 어렵게 하고, 궁극적으로는 입법적 흠결을 가져오게 된다. 이러한 문제는 죄형법정주의의 유추해석을 금지하고 있는 형사법 영

11) 수사현장에서는 일부 금융기관과 신용카드 회사에서 중요사건인 경우에 한하여 제한적으로 수사관의 휴대폰 문자메시지로 실시간 이용내역의 일시, 장소 등을 제공하고 있으나 역부족이다.

역에서 더욱 두드러지게 나타난다. 일단 개별법 중심의 입법체계는 특정한 제3자가 보관하고 있는 특정정보에 대한 요청이 있는 경우에 적용되기 때문에 주체인 "제3자"와 대상인 "정보"가 불일치할 경우에는 개별법을 적용할 수 없어 결국은 형사소송법 상 영장으로 집행해야 한다.

통신비밀보호법은 전기통신사업자가 보관하는 통신사실 확인자료, 금융실명법은 금융기관이 보관하는 금융거래내용, 신용정보법은 신용정보회사가 보관하는 개인신용정보에서만 적용된다. 오픈마켓(Open Market)이나 비트코인 거래소가 금융거래정보를 보관할 경우 금융기관이 아니기 때문에 금융실명법을 적용할 수 없고, 금융거래정보는 통신사실 확인자료에 해당되지 않기 때문에 통신비밀보호법을 적용할 수 없다. 한국정보통신진흥협회가 이동통신사로부터 도난신고를 받은 휴대폰의 이동통신사, 국제이동단말기식별번호(IMEI)를 받아 통신을 차단하고 있으나 법정법인으로 전기통신사업자가 아니기 때문에 통신비밀보호법이나 전기통신사업법의 적용을 받지 않는다. 이 경우 대부분 형사소송법상 영장에 의하거나 간혹 수사관서의 공문에 의해 확보하기도 한다. 또한, 전기통신사업자가 보유하고 있는 서비스 결제정보, 온라인 아이템 거래내역, 사이버머니 거래내역, USIM 번호, 국제이동단말기식별번호(IMEI), GPS 정보 등은 전기통신사업자가 보관하는 정보이지만 통신자료 또는 통신사실 확인자료에 해당하지 않기 때문에 결국 영장에 의하여 취득할 수밖에 없다.

이처럼 개별법의 입법적 흠결은 형사소송법상 영장주의 등 강제처분 규정에 의존할 수밖에 없는 상황에서 문언 의미의 확장을 통한 해결은 유추해석이라는 비판을 받게 된다. 결국 입법적 해결이 불가피한 지점인 것이다.

3. 시사점

제3자 정보 요청은 기본적으로 형사소송법상 영장제도와 어울리지 않음에도 우리 법제는 소관 법률을 제·개정할 때 "법관이 발부한 영장"이라는 문구를 관행적으로 사용하고 있다. 이로 인하여 위법한 수사로 증거능력이 배제될 가능성 역시 높아지고 있다. 나아가 영장제도를 채택함에 따라 수사에 필요한 실시간 정보를 획득하지 못하는 경우도 발생하고, 정보주체나 변호인의 참여권도 보장되지 못해 피의자의 권리보호가 미흡해지는 경우도 발생한다. 영장주의의 확대에 형식적 절차뿐만 아니라 실효성 확보를 위한 제도적 개선이 이루어지지 않는다면 광범위한 형식적 영장주의가 적용됨에도 실질적으로는 적용되지 않은 결과를 초래할 것이다(Seul, 2009: 200). 따라서 제3자 정보에 맞는 집행절차와 피의자 권리 보호에 관한 입법적 대안을 모색해야 한다. 수사기관이 합법과 불법의 모호한 경계 속에서 법집행을 해서도 안 되고, 통제의 범위에서 벗어나도 안 될 것이다.

V. 제3자 정보 요청 법제 개선 방안

1. 가칭 '제3자 정보 요청 기본법' 제정

제3자 정보 요청에 관하여 개별법에 규정된 각각의 조항을 통합하여 일관되고 체계적인 입법체계를 마련해야 한다. 제3자는 직접적인 수사대상자가 아니고, 정보 제공에 관한 사무를 객관적으로 처리할 수 있는 지위에 있기 때문에 제3자 정보에 대해서 유체물이나 피의자·참고인이 보관하는 정보와 다른 법률상 지위를 부여하여야 한다. 그 대안으로 형사소송법에 포함시키는 방안과 특별법 형태의 기본법을 제정하는 방안을 검토할 수 있는데 전자는 독일과 일본에서 채택하는 입법방식으로 체계적이지만 우리나라의 특별법 중심의 입법 문화를 고려할 때 실현 가능성은 높아 보이지 않는다. 반면, 후자는 입법 과정이 비교적 용이하나 형사소송법 외에 또 다른 특별법을 만든다는 비난을 피하기 어려울 것이다. 따라서 우선 제3자 정보 요청에 대한 특별법 형태의 기본법, 가칭 '제3자 정보 요청 기본법'을 제정하고, 궁극적으로는 이를 형사소송법에 편입하는 방안을 고려하여야 할 것이다.

구체적으로 기본법은 제3자 정보 요청에 가장 최적화되어 있는 통신비밀보호법을 중심으로 형사소송법 중 제3자 정보에 관한 압수수색(주로 전기통신 등), 전기통신사업법 중 통신자료 제공절차, 금융실명법, 신용정보법을 비롯하여 영장제도를 준용하는 모든 법률의 내용을 포함하여야 한다. 개별법에서 제3자 정보 요청에 관한 입법이 필요한 경우 기본법을 준용하도록 하는 규정을 신설하여 입법의 일관성과 체계성을 갖춰 나가야 한다. 적용대상이 되는 제3자는 개별법에서 수사기관 등에 정보제공에 대한 의무가 규정되어 있는 사업자로 제한하는 것이 필요할 것이다.

2. 법원 허가제도 도입

제3자 정보 요청 절차는 법관의 영장제도 대신 법원의 허가제도를 채택하는 것이 바람직할 것이다. 형사소송법의 입법체계상 별도로 규정하기 어려운 비대면・사본 집행, 긴급집행, 정보 보관 및 폐기, 부처의 관리감독 및 국회 통제 등을 규정하기에도 용이하다. 법원의 허가제도는 영장이나 제출명령에 비해 일반적이지 않지만 독립적인 사법부의 심사를 받는다는 측면에서 헌법상 영장주의에 부합한다.[12] 이렇게 되면 제3자 정보는 법원 허가제도로, 피의자・참고인 등 수사대상자의 정보는 형사소송법상 영장제도에 의하여 집행되는 것이다.

허가는 해당 요건을 충족하면 이행해야 하는 '기속행위'(Kil, 2011: 116; Oh, 2015: 41)로 보아 법관에 의해 절차적・형식적 심사만 이루어질 뿐 실질적 심사가 무력해지는 결과를 가져올 수 있다는 비판(Oh, 2015: 41)이 있지만 법원 허가 역시 영장보다는 낮지만 기각되는 사례가 존재하는 만큼 실질적 심사를 하지 않는다고 보기 어렵다. 법원행정처에서 발행한 사법연감에서 2015년 발부율을 살펴보면 압수수색검증 영장은 89.7%이고, 통신제한조치허가서 89.0%, 통신사실 확인자료요청서 94.1%인 점을 볼 때 대동소이하다는 것을 확인할 수 있다.[13]

3. 정보주체 및 제3자 권리보호 확대

허가제도의 특성상 정보주체 및 변호인의 참여권 보장이 어렵기 때문에 다양한 형태의 권리보호 방안이 마련되어야 한다. 먼저 정보주체에게 집행통지와 유예에 관한 절차, 시점, 방법, 주체, 사유를 체계화하여야 한다. 집행통지의 시점은 "공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지 결정을 제외한다)을 한 때에는 그 처분을 한 날부터"가 아니라 통신제한조치, 송・수신이 완료된 전기통신의 압수・수색・검증 등이 종료된 시점으로 앞당겨야 한다(Im, 2016: 212; Kim, 2005: 228; Park, 2010: 280). 수사기관과 제3자의 오남용을 통제하기 위해 허가서 등을 일정기간 보관하도록 의무화하고(Kim, 2014: 18), 정보주체에게 정보제공사실열람청구권을 명시적으로 부여하여 제3자가 수사기관에게 제공한 자신의 정보를 확인할 수 있도록 하여야 한다.

또한 법원의 심사를 받았다고 해서 그 집행이 모두 정당화되는 것은 아니기 때문에 제3자에게 협조의무를 부여함과 동시에 불복절차를 마련하여 방어권을 보장해 주어야 한다. 그래서 제3자가 업무상 비밀에 관한 정보, 기술적・물리적으로 협조가 현저히 곤란한 정보, 과도한 비용부담이 초래되는 정보 등에 대한 제공요청을 받았을 때 법원에 이의를 제기하고, 법원에서 제출여부 및 그 범위를 결정하도록 하여야 할 것이다(Baik, 2010: 56-57). 나아가 필요한 경우 정부부처나 국회에 의한 통제장치도 마련하여야 할 것이다.

4. 범죄수사의 실효성 확보

수사기관의 집행에 대한 제3자의 협조의무를 규정하여 수사기관의 강제력은 지금보다 완화시키고 제3자의 협력은 지금보다 강화하여 중간지점에서 범죄수사의 실효성을 확보하여야 한다. 수사기관이 제3자에게 정보를 요청할 때 서면뿐만 아니라 전자우편, 팩스 등 비대면・사본으로도 할 수 있도록 허용하고, 비대면 집행

12) 헌법재판소 1997.3.27. 선고 96헌바28 결정
13) 법원행정처. 2016. 사법연감. 583.

에서 논란이 되는 신원확인 문제를 해소하기 위해 집행자의 신분을 증명할 수 있는 절차를 두어야 한다. 범죄수사에서 제3자 정보 요청에 긴급한 사유가 발생하는 경우 긴급집행을 허용하고, 사후에 법원의 승인을 받는 절차를 마련하여야 한다. 나아가 검사 또는 사법경찰관이 제3자에게 정보에 대한 긴급보존명령을 할 수 있는 법적 근거도 마련하여야 한다(Kim, *et. al.*, 2016: 481-483). 이는 유럽평의회 사이버범죄방지협약(제29조)에서 규정하고 있지만 우리나라에는 아직 입법화되지 않았다(Park, *et. al.*, 2015: 135-136).

Ⅵ. 결 론

이상에서 살펴본 바와 같이 제3자 정보 요청 절차가 형사소송법과 개별법에 산재되어 있고, 통신비밀보호법, 전기통신사업법을 제외한 대부분 법률에서 형사소송법상 영장절차를 활용하고 있다. 하지만, 제3자 정보요청은 정보와 보관주체의 특성에 따라 형사소송법상 영장절차를 준수하는데 한계가 있다. 이에 따라 수사현장과 법률 간의 괴리가 커져가면서 법집행의 적법성에 대한 논란이 끊임없이 제기되고 있고, 위법한 수사절차라고 판단하여 증거능력을 배제시키는 사례도 종종 등장하고 있다.

따라서 본 논문에서는 이러한 문제를 해결하기 위해 제3자 정보 요청에 관한 각종 법률을 통합한 기본법 제정과 법관의 영장이 아닌 법원의 허가제도를 채택할 것을 제안하였다. 정보주체 및 제3자에 대한 권리보장을 위해 정보제공사실열람청구권을 명문화하고, 제3자의 정보제공 이의신청제도를 신설할 것도 제시하였다. 또한 수사의 효율성 확보를 위해 긴급집행 절차 및 긴급보존 명령제도를 마련하고, 허가서의 비대면・사본집행을 허용함과 동시에 신분증명 절차를 의무화할 것도 제안하였다. 향후 제3자 정보 요청에 관한 형사소송법, 통신비밀보호법 등 관련 법률을 제・개정 시 본 논문에서 제안한 입법안이 반영되기를 바라고 나아가 제3자 정보 요청에 관한 기본법이 제정되기를 촉구한다.

알리는 글

이 논문은 저자의 2017년 박사학위(고려대) 논문인 “범죄수사에서 제3자 정보 취득법제 통합방안 연구”의 내용을 수정・보안한 것임.

References

Baik, Kang Jin. 2010. The Search and Seizure of E-mail Data Stored in the Server of the Internet Service Provider. A Proposal for New Type of Warrant. *Law & Technology*. 6(4): 46-58.

Cho, Kuk. 2010. Requirements for the Legitimate Warrants for Searches and Seizures of Computer Data. *Korean Journal of Criminology*. 22(1): 99-123.

Chun, Hyun Wook, Gi Bum Kim, Sung Yong Cho, and Emilio C. Viano. 2015. A Study on Legislative Reform for Enhancing Effective Cybercrime Investigation. *National Research Council for Economics, Humanities and Social Sciences Future Policy Focus Cooperative Research Series*. 15-17-01.

Edward, Felton. 2013.10.2. Statement for the Record, Hearing Before the Senate Judiciary Committee, Continued Oversight of the Foreign Intelligence Surveillance Act. http://www.cs.princeton.edu/~felten/testimony-2013-10-02. pdf (last visit 2016.11.26).

Im, Seok Soon. 2016. Inhaltliche Sowie Strukturelle Probleme der Regelungen der Durchsetzungsmitteilung im Gesetz zum Schutz des Kommunikationsgeheimnisses und deren Verbesserung: Mit der Diskussion über das Doppelte System der Durchsetzungsgrundlage der Kommunikationsbegrenzungsmaßnahmen etc. *Korean Criminological Review*. 27(2): 203-230.

Jo, Sang Su. 2010. Integrity Assurance Method for Improving Legal Status of Digital Evidence. *Prosecution Service*. 27: 64-109.

Josh, Goldfoot. 2011. The Physical Computer and the Fourth Amendment. *Berkeley Journal of Criminal Law*. 16: 159.

Kang, Dong Wook. 2010. A Study on the Revisionist Bills of Criminal Procedure Act about the Collecting of Digital Evidence. *The Journal of Legal Studies*. 8(3): 161-188.

Kil, Joon Kyu. 2011. *Introduction to Administrative Law*. Parkyoungsa.

Kim, Dae Keun, Seok Soon Im, Sang Wook Kang, and Ki Bum Kim. 2016. Analysis of New Financial Frauds and Research on Criminological Measures: Cyber-financial Fraud Using Technology. *Korean Institute of Criminology(KIC) Report*.

Kim, Gi Bum, Kwan Hee Lee, Yun Sik Jang, and Sang Jin Lee. 2011. The Study on Development of Digital Information Warrant. *The Journal of Police Science*. 11(3): 85-116.

Kim, Hyung Joon. 2005. Problems of Current Telecommunication Protection Act in Korea and Their Improvements. *Journal of Criminal Law*. 24: 228.

Kim, Hyung Sung and Hak Shin Kim. 2006. A Study on Legal Issues of Computer Forensics. *SungKyunKwan Law Review*. 18(3): 213-236.

Kim, Jae Yoon. 2014. The Prosecutor's Monopoly Claims of a Warrant and the Right to Request of Communication Confirmed Data. *Korean Journal of Comparative Criminal Law*. 16(2): 1-23.

Kwon, Hyung Jon. 2004. A Study on the Right to Control the Personal Information. *Constitutional Law*. 10(2): 89-116.

Kwon, Soon Min. 2011. Protections for E-Mail Stored Internet Service Provider's Server in Criminal Procedure. *Journal of Criminal Law*. 23(4): 227-259.

Kwon, Yang Sub. 2009a. Establishing Legal System of Digital Forensics. *Law Review*. 35: 357-382.

Kwon, Yeong Seong. 2009b. *Constitutional Theory*. Bobmunsa.

Lee, Chang Soo. 2008. Account Tracking in the United States. *Prosecution Service*. 15: 56-124.

Lee, Jae Sang. 2010. *Criminal Law*. 7th Edition. Parkyoungsa.

Lee, Sang Jin. 2011. *Introduction to Digital Forensics*. Yiroon.

Oh, Gi Du. 1997. (A) Study on the Investigating and Use of the Computer-related Evidences in Criminal Procedure Law. Ph.D. Dissertation. Seoul Natioanl University.

Oh, Gi Du. 2015. *Electronic Evidence Act*. Parkyoungsa.

Oh, Ki Young. 2015. A Critique on current Communication Privacy Act and Related Arguments. *Journal of Media Law, Ethics and Policy Research*. 14(1): 41-53.

Orin, S. Kerr. 2005. Searches and Seizures in a Digital World. *Harvard Law Review*. 119: 561.

Park, Hee Young, Ho Jin Choe, and Seong Jin Choi. 2015. Research on Implementing the Cybercrime Convention. *Supreme Prosecutors' Office Research Service Report*.

Park, Jong Keun. 2009. Seizure of Digital Evidence and Legislation. *Prosecution Service*. 18: 32-100.

Park, Kyung Sin. 2010. Problems of and Legislative Solutions to Searching and Seizing Electronic Mails. *InHa Law Review*. 13(2): 265-314.

Park, Soo Hee. 2007. Sammlung von Elektronischen Beweismitteln und Zwangsermittlung. *Korean Associatin of Public Safety and Criminal Justice Review*. 29: 126-154.

Seul, Min Soo. 2009. Effectiveness of Prior Warrant Preference Doctrine against Third Parties in the Constitution: Case of Internet Service Provider. *Lawyers Association Journal*. 58(8): 144-203.

Sin, Dong Un. 2016. *Brief New Criminal Procedure Law*. 8th Edition. Bobmunsa.

Sung, Wook Joon and Sung Soo Hwang. 2017. A Review of Intelligent Society Studies: A Look on the Future of AI and Policy Issues. *Informatization Policy*. 24(2): 3-19.

Tak, Hee Sung. 2004. A Study on Searching and Seizing Electronic Evidence. *Korean Criminological Review*. 15(1): 21-62.

Won, Hye Wook. 2003. Beschlagnahme und Durchsuchung von Elektronischen Beweismitteln. *Korean Journal of Comparative Criminal Law*. 5(2): 165-191.

Yang, Kun Won. 2006. A Study on Collection and Admissibility of Digital Evidence in Criminal Procedure. Ph.D. Dissertation. Kyung Hee University.

Korean References Translated from the English

강동욱. 2010. 디지털증거 수집에 관한 형사소송법 개정안에 대한 검토. 법학연구. 경상대 법학연구소. 8(3): 161-188.

권순민. 2011. 형사절차에서 인터넷서비스 제공자 서버에저장된 이메일 보호. 형사법연구. 23(4): 227-259.

권양섭. 2009. 디지털 포렌식 법률체계 구축방안. 법학연구. 35: 357-382.

권영성. 2009. 헌법학원론. 법문사.

권형준. 2004. 자기정보통제권에 관한 고찰. 헌법학연구. 10(2): 89-116.

길준규. 2011. 행정법입문. 박영사.

김기범, 이관희, 장윤식, 이상진. 2011. 정보영장 제도 도입방안 연구. 경찰학연구. 11(3): 85-116.

김대근, 임석순, 강상욱, 김기범. 2016. 신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구: 기술적 수단을 사용한 사이버 금융사기를 중심으로. 한국형사정책연구원 보고서.

김재윤. 2014. 검사의 독점적 영장청구권과 통신사실 확인자료 요청허가청구권. 비교형사법연구. 16(2): 1-23.

김형성, 김학신. 2006. Computer Forensics의 법적문제 연구. 성균관법학. 18(3): 97-125.

김형준. 2005. 현행 통신비밀보호법의 문제점과 개선방안: 통신제한조치와 대화감청을 중심으로. 형사법연구. 24: 213-236.

박경신. 2010. E-메일 압수수색의 제문제와 관련법률개정안들에 대한 평가. 법학연구. 13(2): 265-314.

박수희. 2007. 전자증거의 수집과 강제수사. 한국공안행정학회보. 29: 126-154.

박종근. 2009. 디지털증거의 압수수색과 법제. 형사법의 신동향. 18: 32-100.

박희영, 최호진, 최성진. 2015. 사이버범죄협약 이행입법 연구. 대검찰청 연구용역보고서.

백강진. 2010. 인터넷서비스제공자 보관 이메일에 대한 압수수색: 이른바 통신내용제출영장 제도의 신설 제안. Law & Technology. 6(4): 46-58.

설민수. 2009. 인터넷서비스제공자를 통해서 본 제3자 보유정보에 대한 영장주의의 실효성. 법조. 58(8): 144-203.

성욱준, 황성수. 2017. 지능정보시대의 전망과 정책대응 방향 모색. 정보화정책. 24(2): 3-19.

신동운. 2016. 신형사소송법(제8판). 법문사.

양근원. 2006. 형사절차상 디지털 증거의 수집과 증거능력에 관한 연구. 경희대학교 박사학위논문.

오기두. 1997. 형사절차상 컴퓨터관련 증거의 수집 및 이용에 관한 연구. 서울대학교 박사학위논문.

오기두. 2015. 전자증거법. 박영사.

오길영. 2015. 현행 통신비밀보호법의 문제점과 개선방향. 언론과 법. 14(1): 33-69.

원혜욱. 2003. 과학적 수사방법에 의한 증거수집: 전자증거의 압수・수색을 중심으로. 비교형사법연구. 5(2): 165-191.

이상진. 2011. 디지털 포렌식 개론. 이룬.

이재상. 2010. 형법각론(제7판). 박영사.

이창수. 2008. 미국에서의 계좌추적. 형사법의 신동향. 15: 56-124.

임석순. 2016. 통신비밀보호법상 집행통지규정의 내용적・구조적 문제점과 개선방안: 통신제한조치 등 집행근거규정의 이원체계에 대한 논의와 함께. 형사정책연구. 27(2): 203-230.

전현욱, 김기범, 조성용, Emilio C. Viano. 2015. 사이버범죄의 수사효율성 강화를 위한 법제 개선방안 연구. 미래사회협동연구총서 15-17-01. 경제・인문사회연구회.

조국. 2010. 컴퓨터 전자기록에 대한 대물적 강제처분의 해석론적 쟁점. 형사정책. 22(1): 99-123.

조상수. 2010. 디지털 증거의 법적 지위 향상을 위한 무결성 보장 방안. 형사법의 신동향. 27: 64-109.

탁희성. 2004. 전자증거의 압수・수색에 관한 일고찰. 형사정책연구. 15(1): 21-62.

Received: Jul. 24, 2017 / Revised: Aug. 21, 2017 / Accepted: Aug. 29, 2017

범죄수사에서 제3자 정보 요청에 관한 입법체계

국문초록 본 연구는 범죄수사에서 제3자 정보 요청에 관한 입법적 개선방안을 제시하고자 한다. 인터넷 발달로 제3자 정보가 중요한 수사단서가 되면서 프라이버시 침해에 대한 우려가 커지고 있다. 우리나라의 형사소송법과 개별법 대부분은 수사기관이 제3자 정보를 요청할 경우 '법관의 영장'에 의하도록 규정하고 있지만, 이러한 영장제도는 정보통신으로 인한 수사변화를 충분히 반영하지 못해 위법수사에 대한 논란이 계속되고 있다. 이러한 문제를 해결하기 위해 법관의 영장 대신 법원의 허가제도 도입을 골자로 한 제3자 정보 요청에 관한 기본법 제정을 제안하고자 한다. 나아가 정보주체와 제3자의 권리를 보장하기 위해 통지제도를 정비하고, 정보제공사실에 대한 열람청구권과 제3자 이의신청 제도를 입법화하여야 한다. 또한 수사의 효율성 확보를 위해 긴급집행 절차와 긴급보존 명령제도를 신설하고, 비대면·사본집행 도입과 신원확인 절차의 의무화도 필요할 것이다.

주제어 : 제3자 정보, 통신비밀, 압수수색, 형사소송, 디지털증거

Profiles **Gi Bum Kim** : He received his B.A. from Korean National Police University, and his M.S. and Ph.D. from Korea University. He is a police superintendent, a professor of the Department of Police Science and the Director of the International Cybercrime Research Center at Korean National Police University. He worked in the Department of Cybercrime, Seoul Metropolitan Provincial Agency and National Police Agency from 2000 to 2012. His area of research and education is investigation of cybercrime, digital forensics and cybersecurity policy(freekgb02@gmail.com).