사이버범죄협약 가입을 위한 이행입법 연구

The Review of Implementing Legislation for the Adoption of Convention on Cybercrime

최 혁 두*

차 례

● 국문요약 ●

정보통신기술의 발전으로 다양한 사이버범죄가 국경을 넘어 발생하고 있다. 이에 따라 사이버범죄자를 검거하기 위해서는 국제공조수사가 필수가 되었고, 수사기관은 형사사법공조, 인터폴 공조, 수사기관간 직접 공조 등을 통해 대응하고 있다. 그러나 형사사법공조는 6개월 이상 소요되어 회신을 받았을 때에는 이미 증거가 사라진 경우가 많고, 인터폴 공조와 직접 공조는 구속력이 없어 회신을 받는 것조차도 어려운 실정이다.

이러한 상황에서 사이버범죄에 효율적으로 대응할 수 있는 공조방법이 사이버범죄협약과 같은 다자간 공조 시스템에 편입되어 신속하게 국제공조를 진행하는 것이다. 협약에 가입하면 수사자료를 요청함과 동시에 컴퓨터·통신 데이터의 긴급보전을 요청하여 기간 경과로 인한 데이터의 자동삭제를 방지할 수 있고, 요청을 받은 국가가 수사과정에서 다른 경유지를 발견했을 경우, 그 경로 및 관련 데이터도 즉시 제공받을 수 있는 등 수사 효율성 측면에서 큰 도움이 될 것이다.

협약에 가입하기 위해서는 협약과 국내법이 양립 가능하여야 하고, 양립할 수 없는 조항은 이행입법을 통해 협약에서 요구하는 조건을 충족하여야 한다. 다만, 협약은 가입국의 국내법을 존중하고, 보다 많은 국가가 협약에 가입할 수 있게 하기 위하여 9개 조항에 대한 유보를 허용하고 있다. 이러한 유보 조항을 적절히 활용한다면 소폭의 국내법 제·개정으로도 협약에 가입할 수 있을 것이다.

이번 논문에서는 협약과 관련된 국내법을

* 경찰청 사이버안전국 경감

분석하여 국내법이 협약의 요구사항을 충족하는지 여부 및 이행입법 방향에 대해 연구하고, 이와 더불어 어떤 조항을 유보해야 하는지 살펴본다.

◈ 주제어 : 사이버범죄협약, 이행입법, 유보조항, 협약의 이행과 준수

Ⅰ. 서론

정보통신기술의 발전은 우리에게 경제적・교육적・사회적・문화적 측면에서 큰 혜택을 가져다주었다. 스마트폰만 있으면 집 밖으로 나가지 않아도 클릭 몇 번만으로 필요한 물건을 받을 수 있고 지구 반대편의 소식을 실시간으로 확인할 수 있다. 그러나 이러한 순기능과 더불어 역기능 또한 우리에게 큰 부담으로 다가오고 있다. 최근 논란이 되고 있는 불법촬영물 유포는 물론, 인터넷 마약거래, 해킹, 랜섬웨어 등 다양한 형태의 사이버범죄가 그 대표적인 예라고 할 수 있다.

이러한 상황에서 사이버범죄에 효율적으로 대응할 수 있는 방법 중 하나가 다자간 협약에 가입하는 것이다. 사이버범죄협약[1]에 가입하더라도 결국 형사사법공조를 통해 증거자료를 확보하여야 한다는 점에는 변함이 없지만, 수사 실무적으로 수사자료를 요청함과 동시에 컴퓨터・통신 데이터의 긴급보전을 요청하여 기간 경과로 인한 데이터의 자동삭제를 방지(협약 제16조~18조)할 수 있고, 긴급시 전자우편 등 간편 수단을 통한 공조요청도 가능(협약 제25조)하며, 요청을 받은 국가가 다른

1) 협약의 정확한 명칭은 'Convention on Cybercrime'으로 사이버범죄협약, 사이버범죄방지협약, 부다페스트 협약 등 여러 명칭으로 불리어지고 있으나, 의미상 혼동이 없다면 원문에 충실한 용어를 사용하는 게 적절하다고 판단하여 '사이버범죄협약'으로 지칭하고자 한다.

경유지를 발견했을 경우, 그 경로 및 관련 데이터도 즉시 제공(협약 제30조)받을 수 있어 수사 효율성 측면에서 큰 도움이 될 것이다.

다만, 협약의 '제출명령'은 법원의 허가나 영장을 받아야만 한다고 규정되어 있는 것이 아니기 때문에 국가가 개인의 인권을 침해하는 우회경로로 사용될 수 있고, 협약에 쌍방가벌성 원칙이 의무화되어 있지 않아 자국법상 범죄가 아닌 행위에 대해서도 타국의 요청에 의해 자국민의 개인정보를 넘겨주어야 하는 상황이 발생할 수 있다는 우려가 있다. 게다가 협약 가입 과정 자체에 상당한 시간이 소요[2]되므로 사이버범죄협약 가입의 필요성 및 실익에 대한 구체적인 논의가 필요하다.

본 논문에서는 사이버범죄협약과 관련된 국내법을 분석하여 국내법이 협약의 요구사항을 충족하는지 여부 및 어떻게 이행입법을 제정해야 할지를 확인하고, 이와 더불어 어떤 조항을 유보해야 하는지 검토하고자 한다.

Ⅱ. 사이버범죄협약의 가입 필요성

경찰청의 자료에 의하면 경찰의 사이버범죄 처리건수는 2015년 144,679건, 2016년 153,075건, 2017년 131,734건[3]으로 최근 3년간 매

2) 최근 협약 가입사례로는 범죄인인도에 관한 유럽 협약 (1957. 12. 13. 프랑스 파리에서 채택, 1960. 4. 18 발효)이 있다. 이 협약에서 2007. 11월 대한민국 정부가 유럽평의회에 협약 가입의향서를 제출, 2009. 2월 유럽평의회가 대한민국 정부를 상대로 협약 가입 초청, 2009. 8. 5 법제처 심사의뢰, 2009. 8. 28. 법제처 심사회신, 2009. 9. 15 국무회의 심의, 2009. 9. 16 대통령 재가, 2009. 11월 국회 가입동의안 제출, 2011. 3. 10 국회 가입안 통과, 2011. 9. 29 가입서 기탁, 2011. 12. 29 협약 발효가 되어 가입의향서 제출 후 약 4년이 지난 후 협약이 발효되었다.

년 10만건 이상의 사이버범죄를 처리하고 있다. 이 중에서도 해킹·랜섬웨어 등 정보통신망침해 범죄, 이메일 무역사기, 사이버 성범죄, 불법 인터넷 도박 등이 문제가 되고 있다. 이러한 범죄들은 대부분 수사기관의 추적을 피하고자 제3국에 서버를 두고 여러 나라를 경유하여, 최초 공격지의 확인을 어렵게 한다. 따라서 최초 공격지를 찾기 위해서는 서버 소재지, 경유지 국가와의 국제공조가 매우 중요하다. 또한, 범죄자들은 수사당국의 단속을 피해 법적인 처벌수단이 아직 제대로 완비되지 않은 국가에 서버를 두고 운영하는 경우가 많아 서버가 위치한 국가와의 국제공조가 필수적이다.

현재 국내 수사기관이 국제공조수사를 위하여 일반적으로 활용하고 있는 절차는 형사사법공조이다. 그런데 각 국가는 형사사건에 관한 사법공조에 응해야 할 의무가 없고, 요청받은 국가는 쌍방가벌성과 적법성 등을 판단해 공조여부를 결정하게 된다. 따라서 형사사법공조조약에 가입되어 있고 국내법상 공조를 할 수 있는 근거가 마련되어 있다고 하더라도 요청받은 국가의 결정으로 사법공조가 이루어지지 않을 수 있다.

또한 통상적으로 형사사법공조는 수사공조가 이루어지기까지 적게는 6개월, 많게는 2년이라는 상당한 시간이 소요된다. 이러한 문제점을 보완하고자, 수사기관은 인터폴망,[4] G7 24/7망[5]을 활용하거나 외국 법집행

3) 사이버안전국 홈페이지에서 '사이버범죄 통계자료', cyberbureau.police.go.kr/share/sub3.jsp?mid=030300.

4) 인터폴의 공식명칭은 국제형사경찰기구(International Criminal Police Organization)로, 194개 회원국으로 구성(2018. 11월 현재)된 세계 최대의 국제경찰조직이다. 인터폴 회원국들은 국제범죄의 예방과 진압을 위해 인터폴 헌장과 자국의 국내법이 허용하는 한도 내에서 국제범죄에 관한 각종 정보를 교환하고 범죄자 체포, 인도에 대해 상호 협력한다. 국제공조수사가 가능한 범위는 수사 관련자에 대한 정보(인적사항, 범죄경력 등), 도피사범에 대한 소재수사(출입국 기록 확인 등), 사실 확인(문서진위 여부 등)이 있고, 한국의 컨택포인트는 경찰청

기관과 직접 협력관계를 구축하여 국제공조수사를 진행하고 있다. 그러나 이러한 공조망을 이용한 국제공조는 회원국간 비강제적 수사(사실확인, 소재수사 등)에 한해 가능한 경우가 대부분이고, 구속력이 없어 회신을 받지 못하는 경우가 상당수이다. 직접 협력관계 구축을 통한 국제공조는 신속한 공조가 가능하지만 협력망 구축 및 유지에 많은 시간과 비용이 소요되어 직접 협력국의 수가 제한적이라는 점에서 비효율적이다.

이러한 점을 고려할 때 기존의 국제공조 수단만으로는 수사공조가 신속하게 이루어지기 어렵고, 사이버범죄협약과 같은 이미 구축[6]되어 있는 공조체제에 편입되어 국제공조가 효율적으로 이루어져야 할 필요가 있다.

Ⅲ. 협약 가입을 위한 이행입법 검토

1. 개요

2001년 유럽평의회(Council of Europe) 주도로 시작된 사이버범죄협약은 2018년 7월 현재 61개국이 비준하였고 4개국이 서명하였다. 비준국으로는 유럽평의회 회원국 47개국 중 43개국과 미국, 호주, 일본

외사수사과 인터폴계이다.

5) 각 회원국들이 긴급하게 필요한 전자적 증거를 수집하기 위해 제공되는 네트워크로, 1997년 G7 법무부 장관회의(첨단범죄분과)에서 미국 주도로 창설되어, 83개 회원국(2018년 7월 현재)으로 구성되었다. 한국의 컨택포인트는 대검찰청 사이버수사과이다.

6) 유럽평의회(Council of Europe)는 1995년 '사이버범죄에 대한 형사절차 및 국제협력에 관한 원칙'을 채택한 후, 1997년 전문가위원회를 설치하였고, 2001년 사이버범죄협약 초안이 유럽범죄문제위원회(European Committee on Crime Problems)에서 의결되었다.

등 비유럽 18개국[7]이 포함되어 있다. 2018년에 파라과이(7.30), 모로코(6.29), 카보베르데(6.19), 아르헨티나(6.5) 등 4개국이 비준하는 등 신규 가입국도 증가하는 추세이다.

사이버범죄협약은 원칙적으로 사이버범죄 영역에서 각국의 형사 실체법의 구성요건 및 연결된 조항들을 통일하고, 컴퓨터 시스템을 통해 저지른 기타 범죄 및 전자적 형태의 증거 수사와 기소에 필요한 형사절차 법상의 권한을 규정하며, 신속하고 효과적인 국제협력 체제를 수립하는 것을 목적으로 한다. 이러한 목적을 바탕으로 협약은 실체법, 절차법, 국제공조 절차 등 4개의 장, 48개 조문으로 구성되어 있다. 협약은 제1장에서 컴퓨터 시스템, 컴퓨터 데이터, 서비스 제공자, 트래픽 데이터에 대해 정의한다. 제2장은 불법접속, 불법감청, 데이터 침해, 시스템 방해, 장치 남용, 컴퓨터 관련 위조, 컴퓨터 관련 사기, 아동 음란물 관련 범죄, 저작권 및 관련 권리에 대한 범죄 등 실체법과 저장된 데이터의 신속한 보전, 제출명령, 데이터의 수색과 압수, 감청 등 절차법 및 관할에 대해 규정한다. 제3장은 국제공조 절차로 전통적 범죄, 컴퓨터 범죄와 관련한 공조 및 범죄인 인도 규칙에 관해 규정한다. 제4장에서는 유럽평의회 조약의 표준조항과 유보조항을 규정한다.

7) 유럽평의회 회원국 및 협약 성안 과정에 참여한 비회원국(미국, 일본 등)의 경우, 서명 후 비준하게 되나, 그외 국가의 경우, 서명 없이 국내 비준절차 완료 후 가입서를 기탁함으로써 협약에 가입하게 된다. 우리나라의 경우, 유럽평의회 회원국이 아니고, 협약 성안에도 참여하지 않았기 때문에 가입서를 기탁하는 방식으로 협약에 가입할 수 있다. 사이버범죄협약의 가입절차는 ① 유럽평의회에 가입의향서를 제출 ② 유럽평의회에서 가입국 의견 수렴 및 각료이사회 회의를 거쳐 가입 여부를 결정 ③ 유럽평의회에서 협약 가입 초청서 발송 ④ 법제처 심사 ⑤ 국무회의 ⑥ 대통령 재가 ⑦ 국회심의·동의 ⑧ 조약·법률 공포와 동시에 가입서(Instrument of Accession) 기탁 순이다.

2. 현행 국내법과의 부합 여부 및 이행입법 검토

대부분의 협약 조항이 「형법」, 「형사소송법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「통신비밀보호법」 등 현행 국내법과 양립 가능하지만 일부 이행입법이 필요한 조항도 발견된다. 협약에 모순되는 입법을 하는 것이 국내법 체계상으로는 문제가 없다[8]고 하더라도, 그러한 내용으로 입법하게 된다면 협약 사무국 및 가입국의 반발이 예상되며 국제관계상 마찰이 발생할 수 있다. 따라서 사이버범죄협약이 국내법에 수용되기 위한 이행입법을 요구할 뿐 가입국에 곧바로 효력이 발생되는 것이 아니라고 하더라도 특별한 사정이 없는 한 국회는 협약에 모순되는 방향의 입법은 자제하는 것이 바람직하다.

아래에서는 협약 조문과 현행 국내법 사이에 괴리가 있어 이행입법이 필요하거나 검토가 필요한 조항에 대해 기술하겠다.

1) 저장된 컴퓨터 데이터의 보전

협약 제16조(저장된 컴퓨터 데이터의 보전)[9]는 대상 데이터의 삭제를

8) 「헌법」 제6조 제1항의 국제법 존중주의는 우리나라가 가입한 조약과 일반적으로 승인된 국제법규가 국내법과 같은 효력을 가진다는 것으로 조약이나 국제법규가 국내법보다 상위의 효력을 가진다는 것은 아니다. 즉, 국제법 또한 국내법 질서체계에서는 헌법의 하위규범에 불과하다.(헌법재판소 2001. 4. 26. 99헌가13 결정) 따라서 헌법에 의해 보장된 국회의 입법권이 법률과 동일한 효력을 가진 협약에 의해 제한된다고 볼 수는 없다.

9) 제16조(저장된 컴퓨터 데이터의 신속한 보전)
① 컴퓨터 시스템을 통해 저장된 특정한 컴퓨터 데이터(트래픽 데이터가 포함)가 특별히 손실되거나 변경될 수 있다고 인정될 만한 특별한 사정이 있는 경우, 각 당사국은 자국의 권한 있는 기관이 이러한 컴퓨터 데이터를 신속히 보전할 수 있도록 명령하거나 이와 유사한 방법으로 확보할 수 있도록 필요한 입법 및 그밖의 조치를

방지하기 위한 긴급처분이다. 이 조항에 대해 국내 ISP 등 서비스 제공자들은 현행 국내법상 정당한 사용자에 의해 보전된 데이터에 대하여 보전명령을 할 수 있는 일반규정이 없다는 입장이다. 국제형사사법공조법 제17조에서 검사와 사법경찰관의 처분을 규정[10]하고 있지만 공조요청에 따른 수사처분에서 컴퓨터 데이터의 신속한 보전은 포함되어 있지 않다는 것이다.[11]

이기수 등[12]은 협약 제16조의 데이터 보전명령은 현행법상의 압수 및 증거보전제도와 차이가 있고, 통비법상 통신사실확인자료는 통신데이터를 의미하는 것이지 협약에서 규정한 '보전되어야 할 자료'로서 컴

취해야 한다.
② 전항과 관련하여 당사국이 어떤 자에게 그가 소유하거나 관리하고 있는 저장된 특정 컴퓨터 데이터를 보전하도록 명령하는 경우, 해당 당사국은 최대 90일까지 필요한 기간 동안 그가 해당 컴퓨터 데이터의 무결성을 유지한 채 보전하도록 하고 권한있는 기관에게 제공할 수 있도록 필요한 입법 및 그밖의 조치를 취해야 한다. 각 당사국은 그러한 명령이 연속하여 연장되게 규정할 수 있다.

10) 「국제형사사법공조법」(시행 2017. 7. 26) 【법률 제14839호, 2017. 7. 26., 타법개정】 제17조(검사 등의 처분)
① 검사는 공조에 필요한 자료를 수집하기 위하여 관계인의 출석을 요구하여 진술을 들을 수 있고, 감정·통역 또는 번역을 촉탁할 수 있으며, 서류나 그 밖의 물건의 소유자·소지자 또는 보관자에게 그 제출을 요구하거나, 행정기관이나 그 밖의 공사단체에 공조에 필요한 사실을 조회하거나 필요한 사항의 보고를 요구할 수 있다.
④ 검사는 사법경찰관리를 지휘하여 제1항의 수사를 하게 할 수 있고, 사법경찰관은 검사에게 신청하여 검사의 청구로 판사가 발부한 영장에 의하여 제2항에 따른 압수·수색 또는 검증을 할 수 있다.

11) 이경렬·하경우, "유럽평의회 사이버범죄조약의 가입·비준을 위한 국내 이행법률의 마련과 준비 비교", 비교형사법연구 제19권 제4호, 한국비교형사법학회, 2018.1, 527쪽.

12) 이기수·민수현, "한국과 중국의 사이버범죄 형사사법공조 강화를 위한 법개정 검토 – 유럽 사이버범죄협약을 기준으로 –", 비교형사법연구 제19권 제4호, 2018. 1, 543-544쪽.

퓨터 데이터는 아니라며 이에 대한 보완이 필요하다는 입장이다. 전현욱 등[13]도 이 조항에 대한 국내법상 규정이 없다며 보존명령 제도를 도입해야 한다고 주장한다.

협약 제16조는 권한 있는 기관이 데이터의 신속한 보존을 '명령하거나 이와 유사한 방법으로 확보(order or similarly obtain)'하도록 규정하고 있다. 여기에서 '유사한 방법으로 확보'라는 표현을 쓴 것은 꼭 입법적 조치를 취하지 않더라도 다른 방법으로 데이터의 신속한 보전을 할 수 있다면 협약 제16조에 부합하는 것으로 인정하겠다는 취지이다.

현행 국내법에서 데이터의 신속한 보존을 위한 '유사한 방법'으로 고려해볼 수 있는 것이 압수수색이다. 현행법상 데이터의 압수수색은 이러한 관점에서 보면 데이터의 무결성을 확보할 수 있는 보전명령에 해당한다고 볼 수 있다.

또한, 통비법시행령[14]상 통신사업자들의 보전의무규정에 따라 협약 가입국 수준의 보존조치가 이루어지고 있고 통비법 제13조 제2항 단서에 따라 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 먼저 통신사실 확인자료 제공을 요청하여 필요한 자료를 제출받고 사후에 허가를 받아 통신사업자에게 송부할 수 있기 때문

13) 전현욱・이자영, "사이버범죄협약과 형사절차상 적법절차원칙 : 저장된 데이터의 보존 및 일부 공개를 중심으로", 형사정책연구 제25권 제2호, 2014, 93-94쪽.

14) 「통신비밀보호법 시행령」(시행 2017. 7. 26) 【대통령령 제28211호, 2017. 7. 26., 타법개정】 제41조(전기통신사업자의 협조의무 등).
② 법제15조의2 제2항에 따른 전기통신사업자의 통신사실확인자료 보관기간은 다음 각 호의 구분에 따른 기간 이상으로 한다.
1. 법 제2조 제11호 가목부터 라목까지 및 바목에 따른 통신사실확인자료 : 12개월
2. 법 제2조 제11호 마목 및 사목에 따른 통신사실확인자료 : 3개월

에 지연의 우려는 크지 않을 것으로 보인다. 실무적으로 통신사실확인자료 제공요청의 경우 통상 법원의 허가까지 1~2일이 소요되나, 시간적으로 긴급을 요하는 경우 담당판사에게 이러한 사유를 설명하고 1시간만에 허가를 받은 경우도 있기 때문에 법원의 심사절차가 느려 데이터 보전이 늦어지는 것을 우려할 필요는 없다.

이렇듯 형사소송법상 압수수색 절차나 통비법상 보전의무규정 등으로 데이터의 신속한 보전이라는 목적은 어느 정도 달성할 수 있다. 다만, 데이터 보존명령 제도의 도입을 권고하는 협약 주석서의 취지[15]를 고려하여 데이터 보존명령에 대한 이행입법이 필요한지에 대해서는 보다 심도깊은 논의가 이루어져야 한다.

2) 트래픽 데이터의 보전

협약 제17조(트래픽 데이터의 신속한 보전 및 일부 제공)[16]는 제16

15) 협약 주석서 160(Explanatory Report, para 160)
'명령하거나 이와 유사한 방법으로 확보'라는 표현은 단순히 법원 또는 행정부의 명령이나 지시에 의한 것 이외에 보존을 달성하는 다른 법적 방법의 사용을 허용하기 위한 것이다. 일부 국가의 경우, 보존 명령이 그들의 절차법에 존재하지 않으며, 데이터는 압수수색 또는 제출명령을 통해서만 보존, 획득할 수 있다. 유연성의 목적은 이들 국가들이 이 수단을 사용하여 본 조항을 이행할 수 있도록 하기 위한 것이나 국가는 데이터를 보존하라는 명령을 받는 사람에 대해 실제로 명령하는 권한과 절차의 수립을 고려하는 것이 바람직하다.

16) 제17조(트래픽 데이터의 신속한 보전 및 일부 제공)
① 각 당사국은 제16조에 따라 보전되어야 할 트래픽 데이터와 관련하여, 각 호의 사항을 위해 필요한 입법 및 그 밖의 조치를 취해야 한다.
가. 하나 또는 그 이상의 서비스 제공자가 해당 통신 중개에 관여하고 있는지 여부와 관계없이 트래픽 데이터의 신속한 보전이 가능하도록 보장, 그리고
나. 당사국이 해당 서비스 제공자와 통신 경로를 확인할 수 있는데 충분한 트래픽 데이터를 당사국의 권한 있는 기관이나 그 기관이 지명한 자에게 신속히 제공될 수 있도록 보장

조에 대한 특별규정으로 이해할 수 있다. 컴퓨터 통신망은 수많은 중간 단계를 거쳐 전달되기 때문에 다양한 서비스 제공자에게 트래픽 데이터를 신속하게 보존하게 할 필요가 있고, 이 조항으로 보존 명령 권한을 수사기관에게 부여한 것이다. 협약상 트래픽 데이터는 통신의 발신지 및 착신지, 통신경로, 시간, 날짜, 크기, 기간, 이용한 서비스의 유형[17] 이다. 이에 반해, 협약상 트래픽 데이터에 상응하는 통비법 제2조 11호의 통신사실확인자료는 가입자의 전기통신일시, 전기통신개시·종료시간, 발·착신 통신번호 등 상대방의 가입자번호, 사용도수, 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록 자료, 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료, 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료[18]이다. 그렇다면 협약상 트래픽 데이터와 통비법상 통신사실확인자료가 완벽히 일치하는 것은 아니다.

박희영,[19] 이기수[20] 등은 통신경로, 통신의 크기, 이용한 서비스의 유형이 통신사실확인자료에 포함되지 않아 이행입법이 필요하다는 입장이다.

그러나 착·발신 통신번호, 컴퓨터통신의 로그기록, 발신기지국의 위

17) 협약 주석서 30(Explanatory Report, para 30)

18) 박희영 외, "사이버범죄협약 이행입법 연구", 2015 연구용역 결과보고서(대검), 2015. 12., 86쪽.

19) 앞의 연구용역 결과보고서, 86-87쪽.

20) 이기수·민수현, "한국과 중국의 사이버범죄 형사사법공조 강화를 위한 법개정 검토 - 유럽 사이버범죄협약을 기준으로 -", 비교형사법연구 제19권 제4호, 2018. 1, 544-555쪽.

치추적자료 등을 종합, 분석하여 통신경로와 이용한 서비스의 유형을 확보할 수 있고, 통신의 크기는 통신사실확인자료를 통해서는 확보하기 어렵지만 실무적으로 압수영장을 통해 확보할 수 있다. 따라서 협약이 요구하는 조건은 현행 국내법으로도 충족되기에 이행입법은 필요하지 않다.

3) 트래픽 데이터에 대한 '제출명령' 제도의 도입 실효성

협약 제18조(제출명령)[21]와 관련하여 협약 주석서는 제출명령 제도를 독자적인 제도로 규정한 것은 더 침해적이거나 부담스러운 조치를 대신해 수사기관이 유연하게 적용할 수 있는 제도를 마련한 것으로 이러한 절차의 구현으로 ISP 등 서비스 제공자 역시 자신이 관리하는 데이터를 자발적으로 제공함으로써 자신의 계약상 또는 계약외 책임을 면제받게 되어 유익할 것이라고 설명하고 있다.[22] 이러한 협약상 취지는 수사기관이나 서비스 제공자 양측 모두의 입장에서 긍정적이라고 평가될 수 있으나, 현행 국내법상 협약 제18조와 명확하게 일치하는 절차법 규정은 없다.

이와 관련, 박희영 등[23]은 이 조항이 「형사소송법」상의 통상적인 압

---

21) 제18조(제출명령)
① 각 당사국은 권한 있는 기관에게 다음 각 호의 사항을 명령할 수 있는 권한을 부여하는데 필요한 입법 및 그 밖의 조치를 취해야 한다.
가. 자국 내에 있는 자가 컴퓨터 시스템 또는 컴퓨터 데이터 저장매체에 저장되어 있는 컴퓨터 데이터를 보유하거나 관리하고 있는 경우 그 컴퓨터 데이터의 제출
나. 서비스 제공자가 자국 내에서 제공하는 서비스와 관련하여 보유 또는 관리하고 있는 가입자 정보의 제출

22) 협약 주석서 171(Explanatory Report, para 171).

수규정의 범위를 벗어나고, 「형사소송법」 제106조 제2항에서 압수의 일종으로 제출명령을 규정하고 있지만 이는 법원의 권한일 뿐, 수사기관의 독자적인 제출명령 권한은 인정되지 않기에[24] 이 조항에 대한 이행입법이 필요하다고 주장한다. 이기수[25]와 이경렬[26] 등도 제출명령에 상응하는 법률규정이 한국에 없다는 입장이다.

그러나 현행 국내법으로도 협약상 취지를 달성할 수 있다. 「통신비밀보호법」 제13조에서 수사기관이 법원의 허가를 받아 전기통신사업자에게 통신사실확인자료의 제공을 '요청할 수 있다'고 규정하고 있어 이 조항을 원용할 수 있기 때문이다. 법문상 '요청'이라고 표현하였지만, 수사기관이 법원의 허가를 받아 자료를 제공받고 전기통신사업자가 협조해야 할 의무를 부담한다는 점에서 협약 제18조에 상응하는 제도라고 할 수 있다. 또한 개정 「형사소송법」에서 제106조 제3항[27]이 입법될 때의 사법제도개혁특별위원회의 회의록을 보면 제3항의 본문은 제출

23) 앞의 연구용역 결과보고서, 94-96쪽.

24) 「형사소송법」 제219조는 수사기관의 압수, 수색에 제106조를 준용하도록 규정하고 있으나, 법원의 제출명령에 관한 제106조 제2항은 준용되지 않는다는 것에 학계의 견해가 일치한다.

25) 이기수·민수현, "한국과 중국의 사이버범죄 형사사법공조 강화를 위한 법개정 검토 - 유럽 사이버범죄협약을 기준으로 -", 비교형사법연구 제19권 제4호, 2018. 1, 545쪽.

26) 이경렬·하경우, "유럽평의회 사이버범죄조약의 가입·비준을 위한 국내 이행법률의 마련과 준비 비교", 비교형사법연구 제19권 제4호, 한국비교형사법학회, 2018.1, 523쪽.

27) 「형사소송법」 제106조(압수)
③ 법원은 압수의 목적물이 컴퓨터용 디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체 등을 압수할 수 있다.

명령을 포함한다는 것이 입법자의 취지[28]이다. 그렇다면 현행법상 압수에 의해서도 협약 제18조를 충족할 수 있다. 이러한 점을 고려할 때 현행 국내법은 협약 제18조의 요건을 충족하므로 제출명령 제도를 새로 도입할 필요가 없다.

현행 국내법이 제18조에 상응할 수 있다는 점을 차치하고, 제출명령 제도를 새로 도입해야 할 실익이 있는지를 분석해보면 협약의 트래픽 데이터에 상응하는 통신사실확인자료에 대해서는 이미 통신비밀보호법상의 제공요청제도가 시행되고 있으므로 제출명령 제도를 새로 도입할 필요가 없고, 데이터 제출명령이 새롭게 필요하다면 그것은 컨텐츠 데이터에 대해서만 의미가 있을 것이다. 그런데 실제로 컨텐츠 데이터의 경우 서비스 제공자들은 서버에 데이터를 저장하지 않거나 저장하더라도 극히 짧은 기간 동안만 저장하는 경우[29]가 많기 때문에, 제출명령이라는 새로운 제도를 도입한다고 하더라도 데이터를 실효적으로 확보하기란 쉽지 않다. 제출명령이라는 제도를 도입한다고 하더라도 실효성이 없는 것이다.

또한 대법원의 판례에 의해 수사기관은 범죄혐의와 관계있는 컴퓨터 데이터만을 선별해서 압수해야 한다. 문제는 컴퓨터 데이터를 직접 들여다보기 전까지는 어떤 자료가 범죄혐의와 관계가 있는지 알 수 없다는 것이다. 실무적으로는 관련된 컴퓨터 데이터를 압수한 후 이 중 범죄혐의와 관계있는 데이터를 선별하는 과정을 거치고 있다. 따라서 제출되어야 할 데이터를 미리 특정하여 제출하는 방식의 제출명령은 그

28) 이윤제, 디지털 증거 압수·수색영장의 집행에 있어서의 협력의무, 형사법연구 제24권 제2호, 2012, 317쪽.

29) 카카오톡의 경우 비밀대화의 경우 내용은 저장되지 않고, 일반대화의 경우 2~3일 정도만 저장되고 있어 실무적으로 컨텐츠 정보를 확보하기가 쉽지 않다.

제도 자체에 근본적인 한계가 있어 도입할 실효성이 없다.

결국 협약상 제출명령 제도는 현행 국내법으로도 충족된다는 점, 제출명령 제도를 도입할 실효성이 없다는 점에서 제출명령 제도에 대한 이행입법은 필요하지 않다.

4) 원격수색의 허용 필요성

협약 제19조(저장된 컴퓨터 데이터의 수색과 압수)[30]를 국내법과 비교했을 때 검토가 필요한 조항은 제19조 제2항이다. 협약 제19조 제2항은 압수·수색 대상자의 컴퓨터 시스템에서 정보통신망으로 연결되어 있는 다른 컴퓨터 시스템에 접속하는 원격수색을 허용하는 조항으로 '다른 컴퓨터 시스템 또는 그 일부'와 관련하여 클라우드 서비스나 웹하드 등의 데이터 저장공간을 이용하는 경우는 원격수색이 허용된다고 볼 수 있다. 그런데 이용자가 이메일 서비스를 사용하는 과정에서 어떤 정보가 이메일 서비스 제공자의 서버에 보관되어 있는 경우, 이 서버도 '다른 컴퓨터 시스템 또는 그 일부'로 볼 수 있을지는 명확하지 않다.

---

30) 제19조(저장된 컴퓨터 데이터의 수색과 압수)
① 각 당사국은 자국의 권한있는 기관에게 자국 내에서 다음 각 호의 대상을 수색하거나 이와 유사한 방식으로 접근할 수 있는 권한을 부여하는데 필요한 입법 및 그 밖의 조치를 취해야 한다.
가. 컴퓨터 시스템 또는 그 일부, 그곳에 저장된 컴퓨터 데이터
나. 컴퓨터 데이터가 저장될 수 있는 컴퓨터 데이터 저장매체
② 각 당사국은 권한있는 기관이 제1항에 따라 특정 컴퓨터 시스템 또는 그 일부를 수색 또는 이와 유사한 방식으로 접근한 결과, 찾고자 하는 데이터가 자국 내 다른 컴퓨터 시스템 또는 그 일부에 저장되어 있고, 이 데이터가 최초 접근한 컴퓨터 시스템을 통해 정당하게 접근하거나 이용할 수 있다고 믿을만한 사정이 있는 경우, 권한 있는 기관이 다른 컴퓨터 시스템에 대해 신속히 수색 또는 이와 유사한 방식으로 접근하는데 필요한 입법 및 그밖의 조치를 취해야 한다.

이와 관련, 이러한 수색을 명시적으로 허용하는 현행법은 없다. 원격수색은 전통적인 압수수색에서 정립되어 있는 '압수수색 장소의 특정성'이 아닌 '데이터에 대한 접근 권한 유무'로 그 허용 여부를 결정한다는 점에서 기존 압수수색의 법리를 넘어서는 것이다.

박희영 등[31]은 원격수색을 허용하는 국내법은 발견되지 않아 입법이 필요하다는 입장이지만 입법 방향에 대해서는 언급하지 않았다.

수사실무상 이메일 압수 등에서 원격수색 없이는 수사 자체가 진행되기 어렵다. 원격수색이 필요한 때는 피의자에 의한 데이터 삭제, 변경의 가능성이 있어 피의자보다 먼저 중요 정보를 확보할 필요가 있을 때인데, 중요 데이터가 네트워크로 연결된 다른 컴퓨터 시스템에 저장되어 있음을 수사과정에서 알게 된 경우 그 데이터를 압수하기 위해서는 압수수색 영장을 다시 발부받아야 하고 압수수색 영장을 발부받는 동안 그 데이터가 삭제될 수 있기 때문이다. 그동안의 이메일 압수수색은 인터넷서비스 제공자를 대상으로 하는 경우가 많아 외국 인터넷 서비스 제공자에게는 영장 집행이 쉽지 않을 뿐만 아니라 소재국과의 주권 문제도 발생하였다. 최근 원격수색을 인정한 판례(2017도9747[32])가 나왔

31) 박희영 외, "사이버범죄협약 이행입법 연구", 2015 연구용역 결과보고서(대검), 2015. 12, 111쪽.

32) 이 판결은 수사기관이 적법하게 취득한 인터넷 서비스 이용자의 이메일 주소와 암호를 이용하여 한국인터넷진흥원의 PC에서 이용자의 중국 이메일 계정에 접속한 뒤 화면캡처나 내려받기의 방법으로 전자정보를 압수수색한 사안에 대한 것이었다.
대법원은 이용자는 전자정보의 소유자나 소지자로서 압수수색의 대상자가 되고, 이용자의 접근권한에 갈음하여 발부받은 영장에 따라 통상적인 방법으로 원격지 서버에 접속하여 압수수색하는 것은 제공자의 의사에 반하지 아니하며, 압수수색한 장소도 단말기가 있는 한국인터넷진흥원이라는 점을 들어 원격 압수수색이 적법하다고 판시하였다. 이와 더불어, 원격지 서버가 국외에 있는 경우도 달리 볼 것이 아니라고 하여 역외 압수수색도 적법하다고 판시

지만, 「형사소송법」에 명확한 규정을 적시하는 것이 협약의 요건 충족은 물론, 적법한 수사를 통한 수사의 정당성 확보를 위해서도 필요하다.[33] 제19조 제2항에 대한 이행입법은 별도의 영장을 발부받을 시간적 여유가 없을 경우 예외적으로 허용하되, 사후영장을 발부받는 방식으로 제정되어야 할 것이다. 독일[34]과 일본[35]도 원격수색의 허용범위를 형사소송법에 규정함으로써 입법적으로 해결하였다.

3. 유보 조항

위와 같이 협약상 대부분의 조항은 현행 국내법으로도 협약에서 요구

하였다. 이는 대단히 파격적인 판결로 평가되고 있는데, 이전에 원격 압수수색에 대한 일관된 판결이 없었기 때문이다. 2015년 '종근당 판결(2011모1839)'의 보충의견에서 원격수색이 허용된다고 판시한 이후 2017년 'PC방 간첩사건(2017노23)'에서 원격수색을 인정하지 않았지만, 2017년 국가보안법 위반 혐의에 대한 항소심(2017노146)에서는 원격수색을 인정하였다.

33) '유럽평의회 사이버범죄조약의 가입·비준을 위한 국내 이행법률의 마련과 준비 비교'에서도 협약 제19조에 상응하는 국내 규정이 없다며 이행입법이 필요하다는 입장이다.(524쪽)

34) 독일「형사소송법」제110조
③ 수색하고자 하는 데이터의 상실이 우려되는 경우에는 수색대상인 자의 전자 저장매체에 대한 수색은 그로부터 그것과 공간적으로 분리되어 있는 저장매체에 접속할 수 있는 한 그 저장매체에까지 확장될 수 있다. 수사에 중요한 의미가 있는 데이터는 보존될 수 있다.

35) 일본「형사소송법」제99조
② 압수할 것이 전자계산기인 때에는 당해 전자계산기에 전기통신회선으로 접속하고 있는 기록매체로서, 당해 전자계산기로 작성 또는 변경한 전자적 기록이나 당해 전자계산기로 변경 또는 삭제할 수 있는 전자적 기록을 저장하는데 사용하고 있다고 인정할 만한 상황이 있는 때에는 그 전자적 기록을 당해 전자계산기나 다른 기록매체에 복사한 후, 해당 전자계산기나 다른 기록매체를 압수할 수 있다.

하는 조건을 충족할 수 있다는 점에서 대폭의 국내법 제·개정은 필요하지 않을 것으로 보인다. 게다가 사이버범죄협약은 조약 준수에 대한 동의표시 시 조약의 일부조항에 대해 효력을 배제 또는 변경하기 위해 행하는 일방적 선언으로 유보를 인정하고 있기에 유보를 적절히 활용한다면 소폭의 제·개정만으로 협약에 가입할 수 있을 것이다.

협약 주석서에 따르면, 유보는 각 국이 자국 국내법상의 접근법 및 개념을 유지하도록 허용하면서, 보다 많은 국가가 협약에 가입할 수 있게 하는데 그 목적이 있다. 즉, 유보를 허용함으로써 협약의 의의를 심각하게 훼손하는 것을 방지하면서, 다른 한편으로는 협약상 필수적인 조항에 대해서는 가입국간 통일성을 유지하게 한 것이다.

협약 제42조에서는 '모든 국가는 유럽평의회 사무총장에 대한 서면 통지를 통해, 서명하거나 비준, 수락, 승인 또는 가입서를 기탁할 때 제4조 2항, 제6조 제3항, 제9조 제4항, 제10조 제3항, 제11조 제3항, 제14조 제3항, 제22조 제2항, 제29조 제4항, 제41조 제1항에 규정된 유보를 선언할 수 있다. 기타 다른 조항에 대한 유보는 허용되지 아니한다'고 하여 9개 조항에 대해서만 유보를 허용하고 있다.

미국, 일본, 독일 등 주요 가입국은 자국법과의 충돌 등의 이유로 일부 조항을 유보하는 등 2018년 9월 현재 61개 회원국 중 31개국이 일부 조항을 유보하였다. 각 국이 유보한 조항은 상이하나 협약 제29조 제4항(쌍방가벌성 요건 미충족시 협약 제29조에 따른 저장된 컴퓨터 데이터의 신속한 보전을 거절할 권리)이 다수 발견[36]된다.

36) 주요국이 유보한 조항을 살펴보면 미국은 제4조, 제6조 제1항, 제9조 제2항 2·3호, 제10조 제1항·제2항, 제22조 제1항 2·3·4호, 제41조, 오스트리아는 제29조 제4항, 프랑스는 제9조 제2항 2호, 제22조 제1항 4호, 독일은 제6조 제3항, 제9조 제2항 2호, 제29조 제4항, 일본은 제6조 제3항, 제9조 제4항, 제11조 제3항, 제22조 제2항, 영국은 제9조 제4항, 제22조 제2항, 제

아래에서는 현행 국내법으로는 협약에서 요구하는 절차법, 실체법을 충족시킬 수 없어 유보가 필요한 2개 조항에 대해서 검토하겠다.

1) 아동·청소년 이용 음란물의 판단기준(협약 제9조 제4항)[37]

아동음란물 관련, 「아동청소년의 성보호에 관한 법률」은 '알면서 이를 단순 소지하는 행위'까지 처벌하고, 「정통망법」은 정보통신망을 통한 배포·판매·임대·공공연한 전시를 처벌하고 있으므로 협약의 요건을 충족하여 유보는 필요하지 않다. 다만, 아동음란물의 범위와 관련하여 아청법은 아동·청소년이용 음란물을 판단할 때 '아동·청소년으로 명백하게 인식될 수 있는 사람'인지 여부를 그 기준으로 하고 있어 협약의 '미성년자로 보이는 자' 및 '사실적 이미지로서 묘사된 미성년자'가 위 기준에 부합하는지는 해석상 문제될 소지[38]가 있다. 따라서 제9조 제2항 2, 3호는 아청법상 아동·청소년이용 음란물에 포섭되는 경우에 한하여 적용되는 것으로 일부 유포할 필요가 있다.

29조 제4항이다.

37) 주요 유보국으로는 미국, 독일, 프랑스, 일본, 스위스 등이 있다.

38) 헌재 2015.6.25. 선고 2013헌가 17·24, 2013헌바85(병합) 결정 <아동·청소년의 성보호에 관한 법률 제2조 제5호 등 위헌제청 등>
아동·청소년의 성보호에 관한 법률의 입법목적, 가상의 아동·청소년이용음란물의 규제 배경, 법정형의 수준 등을 고려할 때, '아동·청소년으로 인식될 수 있는 사람'은 일반인의 입장에서 실제 아동·청소년으로 오인하기에 충분할 정도의 사람이 등장하는 경우를 의미함을 알 수 있고, '아동·청소년으로 인식될 수 있는 표현물' 부분도 아동·청소년을 대상으로 한 성범죄를 유발할 우려가 있는 수준의 것에 한정된다고 볼 수 있으며, 기타 법관의 양식이나 조리에 따른 보충적인 해석에 의하여 판단 기준이 구체화되어 해결될 수 있으므로, 위 부분이 불명확하다고 할 수 없다.

2) 데이터 보전시의 쌍방가벌성 적용(협약 제29조 제4항)[39]

「국제형사사법공조법」 제4조에서 상호주의를 규정하고 있듯이 상호주의는 사법공조의 근간이다. 협약 제29조 제3항[40]과 관련, 협약 주석서에서는 보전조치가 압수수색 및 감청 등 통상의 공조방법에 비해 덜 침해적이고 쌍방가벌성의 입증에 오랜 시간이 소요되어 그동안 데이터가 삭제, 제거, 수정될 수 있으므로 쌍방가벌성을 요건으로 삼을 수 없다고 설명한다. 협약 제29조 제5항에서 보전요청 거절사유를 규정하고 있고, 신속한 증거보전은 사이버수사의 기본이라는 점을 감안하더라도 아직 우리나라에서 법제화되지도 않은 보전조치에 대해, 국내에서 처벌받지 않는 사유임에도 불구하고 원칙적으로 공조요청을 거절할 수 없다는 것은 일견 받아들이기 어렵다.

그러나 성인음란물 등 우리나라에서는 처벌하지만 외국에서는 처벌법규가 없는 경우와 같이 우리나라의 입장에서 데이터 보전이 필요한 경우도 발생할 수 있는 만큼, 상호주의 측면에서 이 조항을 받아들일 필요가 있다. 데이터가 보전되면 추후 적용법률을 수정하는 등의 방법으로 요청국이 피요청국의 법제에 맞게 공조요청을 할 수 있게 된다. 피요청국 입장에서는 데이터 보전을 한다고 하더라도, 추후 데이터를 요청국에 회신할 지 여부는 국내법 등을 고려해서 결정할 것이므로 국가주권 차원에서도 문제가 되지는 않을 것이다.

협약 제29조 제4항에서는 컴퓨터 데이터의 수색, 압수 등에 대해 유

39) 주요 유보국으로는 독일, 영국, 스위스 등이 있다.

40) 제29조(저장된 컴퓨터 데이터의 신속한 보전)
③ 요청을 받은 다른 당사국은 자국법에 따라 그 데이터의 신속한 보전을 위한 적절한 모든 조치를 취해야 한다. 공조 요청에 대해 회신을 할 경우, 쌍방가벌성이 그 보전을 이행하기 위한 요건으로 되어서는 아니 된다.

보할 수 있다고 규정하고 있다. 데이터의 보전을 넘어서는 압수 등에 대해서도 쌍방가벌성 요건을 요구하지 않는 것은 국가주권 및 인권보호 차원에서 납득할 수 없다. 따라서 제29조 제4항에 대해서는 유보할 필요가 있다.

Ⅳ. 결론

사이버범죄협약은 여러 방면에서 비판이 제기되고 있다. 스마트폰 등 전자기기가 보편화된 현대사회에서 대다수의 형사 절차가 전자증거의 수집과 연관될 수밖에 없어 사이버범죄협약이 사이버범죄만이 아닌 모든 범죄를 규율하는 포괄적인 협약으로 확대될 수 있다는 우려가 있다. 또한 협약 가입국 관련, 중국, 러시아,[41] 동남아시아 등 사이버범죄의 주요 발생국 또는 경유국이 협약에 가입하지 않았기에 협약 가입의 실효성이 떨어진다는 비판도 있다.

이러한 우려와 비판이 있음에도 불구하고, 사이버범죄협약에 가입해야 하는 이유는 앞서 살펴본 바와 같이 사이버범죄협약에 가입하여 얻는 이익이 이러한 문제점보다 크기 때문이다. 사이버범죄는 국경을 초월하여 발생하고 범죄증거는 전자적 형태로 존재하여 조기 소멸된다는 점을 감안하면 형사사법공조, 인터폴 공조와 같은 기존의 공조 체계와

41) 중국, 러시아는 사이버범죄협약이 서구 중심적이며, 협약 제32조가 '국가주권'을 침해한다는 이유로 사이버범죄협약 가입에 반대하면서 UN차원의 신규 협약 제정을 주장하고 있다. 그러나 협약 제32조에서 해당국의 동의 없이 데이터에 접속하기 위해서는 공개된 컴퓨터 데이터이거나 정보 주체의 동의가 있어야만 한다. 따라서 사이버 주권 침해 우려는 과도한 면이 있다.

관할 개념, 압수수색 방식만으로는 진화하는 사이버범죄에 효과적으로 대응할 수 없다. 구속력 있는 다자간 협약을 통해 사이버범죄에 보다 체계적으로 접근해야 할 이유가 바로 여기에 있다.

정부는 2010년 이후로 사이버범죄협약 가입의 필요성 검토를 위해 관계부처 회의를 진행하였고, 문재인 정부 출범 후 협약 가입을 적극적으로 추진하고 있는 것으로 보인다. 다만, 현행 국내법이 사이버범죄협약에서 요구하고 있는 실체법과 절차법을 모두 충족하고 있다고 볼 수는 없어 이에 대한 사회적 합의가 필요하다. 그러나 국내법과 협약의 불일치는 가입의향서 제출 후 국내비준 과정에서 이행 입법을 마련함으로써 해결할 수 있다. 물론 이행입법을 마련하더라도 협약에서 요구하는 규정을 모두 충족하기가 쉽지 않을 것이다. 다행인 것은 협약에 규정된 모든 조항을 충족하여야만 협약에 가입할 수 있는 것은 아니라는 점이다. 사이버범죄협약 가입국인 일본의 이행입법을 살펴보면 유보할 수 있는 조항이 아님에도 불구하고, '보존대상 컴퓨터데이터'에 '통신내용'을 제외하였고, 트래픽 데이터의 공개 및 실시간 수집 규정이 없으며, 통신감청법의 중대범죄에 사이버범죄를 포함시키지 않는 등 협약과 불일치하는 조항이 다수 존재한다.

결국 사이버범죄협약 가입 여부는 협약에 가입함으로써 국민 권익이 증진되는지 여부로 결정될 것이다. 사이버범죄협약에 가입하게 되면 효율적인 국제공조를 통해 수사력이 강화될 것이고, 궁극적으로는 국민의 권익 보호라는 결과로 이어질 것이다. 사이버범죄협약 가입을 긍정적으로 검토할 시기이다.

〈논문접수 : 2018. 10. 31, 심사개시 : 2018. 11. 19, 게재확정 : 2018. 12. 11.〉

참 고 문 헌

Ⅰ. 국내문헌

1. 단행본

경찰청, 경찰통계연보, 2016, 2017.

장윤식・김기범, 사이버범죄수사론, 경찰대학, 2013.

전현욱 외, “사이버범죄의 수사 효율성 강화를 위한 법제 개선 방안 연구”, 경제인문사회연구회, 2015.

2. 논문

강수진, “국가 사이버범죄 대응전략 설계”, 경찰청・고려대학교 사이버법센터, 2013.

노명선, “사이버범죄 대처를 위한 EU 사이버범죄협약 가입 필요성과 가입에 따른 협약이행 방안”, 대검찰청 연구용역보고서, 2011.

박희영 외, “사이버범죄협약 이행입법 연구”, 2015 연구용역 결과보고서(대검), 2015.

이경렬・하경우, “유럽평의회 사이버범죄조약의 가입・비준을 위한 국내 이행법률의 마련과 준비 비교”, 비교형사법연구 제19권 제4호, 한국비교형사법학회, 2018.

이기수・민수현, “한국과 중국의 사이버범죄 형사사법공조 강화를 위한 법개정검토 - 유럽 사이버범죄협약을 기준으로 - ”, 비교형사법연구 제19권 제4호, 한국비교형사법학회, 2018.

이윤제, “디지털 증거 압수・수색영장의 집행에 있어서의 협력의무”, 형사법연구 제24권 제2호, 2012.

정완, “사이버범죄의 방지를 위한 국제협력방안”, 형사정책연구 통권 제70호, 한국형사정책연구원, 2007.

정재준, “국제 사이버범죄에 대한 대응방안 -부다페스트(Budapest) 조약 10년의 성과와 반성-”, 형사법의 신동향 통권 제39호, 대검찰청, 2013.

조기영, “최근 주요 쟁점과 관련한 통신비밀보호법 개정방향”, 형사법연구 제26권 제4호, 2014.

차진아, “사이버범죄에 대한 실효적 대응과 헌법상 통신의 비밀보장 - 사이버범죄협약 가입에 따른 통신비밀보호법의 개정방향을 중심으로 -”, 공법학연구 제4권 제1호, 2013.

3. 기타

사이버안전국 홈페이지, ‘사이버범죄 통계자료’ cyberbureau.police.go.kr/share/sub3.jsp?mid=030300(2018. 10. 27. 검색).

유럽평의회 홈페이지(https//www.coe.int).

통신비밀보호법 ‘기지국 수사’ 사건 보도 자료, 2018. 6. 28.

통신비밀보호법 ‘위치정보 추적 자료’ 사건 보도 자료, 2018. 6. 28.

Ⅱ. 외국 문헌

Alexander Seger, "The Budapest Convention on Cyberrmime 10 years on : Lessons learnt or the web is web", the International Conference on Cybercrime, version 16 Feb 2012(https://rm.coe.int/16802fa3e0)

< ABSTRACT >

The Review of Implementing Legislation for the Adoption of Convention on Cybercrime

Choi, Hyeok-Doo

Advances in information and communication technology have resulted in a variety of new cyber crimes. As a result, international cooperation is required in order to arrest cyber criminals. Investigators are responding to cyber crimes through MLAT, Interpol channel and direct cooperation among law enforcement agencies. However, MLAT often took more than six months to take replies and Interpol channel and direct cooperation are not binding, making difficult to secure evidence.

Under these circumstances, a multi-party cooperation system such as Convention on Cybercrime is needed to effectively respond to cyber crimes. Joining the convention would prevent automatic deletion of data due to expiration time by requesting data at the same time as requesting data preservation. In addition, if the country finds other stops in the investigation process, the route and related data will be immediately provided to the requesting country. These will greatly help in terms of investigation efficiency and speed.

In order to join the convention, the convention should be compatible with the existing domestic laws and, if not compatible, the implementation legislation should meet the requirements of the convention.

By the way, in order to allow more countries to join the convention,

the convention respects domestic laws of the member countries and allows the reservation of 9 provisions in the convention. If the reservation clauses are properly enforced, Korea will be easily able to join the convention with a small number of amendments and enactments in domestic laws.

In this study, domestic laws related to the convention are analyzed to identify whether or not domestic laws meet the requirements of the convention, how implementation legislation should be enacted and what provisions should be reserved.

◈ Key words : Cyber crime, Convention on Cybercrime, Implementing legislation, Joining the convention, Reservation clause, Fulfillment and observation on the Convention