형사정책연구 Korean Criminological Review
제25권 제2호(통권 제98호, 2014 · 여름)

사이버범죄협약과 형사절차상 적법절차원칙 : 저장된 데이터의 보존 및 일부 공개를 중심으로

전 현 욱* · 이 자 영**

국 | 문 | 요 | 약

유럽평의회 사이버범죄협약(Convention on Cybercrime)은 초국가적 사이버범죄에 대한 국제사회의 효율적 대처를 목적으로 2001년 채택되고 2004년 발효된 국제규범이다. 그러나 실체적 진실발견에 지나치게 편향된 협약의 절차법적 규정들이 정보적 자기결정권을 비롯한 개인의 인권에 심각한 위협이 될 수도 있다는 비판적 관점이 협약을 거부하는 논거가 되고 있다. 협약 제16조와 제29조는 수사기관에게 저장되어 있는 컴퓨터 데이터가 보존될 수 있도록 강제하는 형사절차적 권한을 부여하는 것을 내용으로 한다. 그러나 제16조가 규정하고 있는 데이터의 신속한 보존은 압수 · 수색의 실효성을 확보하기 위한 전단계 절차이며, 따라서 압수 · 수색이 허용되어서는 안 되는 사생활의 핵심적인 부분이나 국가적 비밀 등에 대해서는 보존명령이 제한될 필요가 있다. 또한 보존기간은 영장청구 등의 적법절차를 밟기 위해 필수적으로 소요되는 시간을 확보하는 것에서 그쳐야 하며 이을 국내법에 도입함에 있어 기간의 상한은 제한적으로 해석되어야 한다. 협약 제17조와 제30조는 트래픽 데이터에 한정하여 신속한 보존을 확보하기 위하여 추가적으로 필요한 조치를 규정하고 있으며, 통신의 전송경로를 확인하기에 충분한 트래픽 데이터를 수사기관에게 공개하도록 한다. 그러나 사이버범죄를 수사하는 수사기관은 이 두 조항에 근거하여 자국은 물론 타국의 서비스 제공자에게도 트래픽 데이터를 받아낼 수 있게 되며, 이는 결국 아무런 적법절차의 통제를 거치지 않은 채 정보적 자기결정권의 본질을 심각하게 침해하는 것이 될 수도 있음을 유의해야 한다. 우리나라 국내법에는 제16조와 제17조에 해당하는 제도가 없으며, 디지털 증거의 특성을 고려한다면 사이버범죄 수사의 효율성을 높이기 위해 신속한 보존명령 및 트래픽 데이터의 일부공개 제도를 도입하는 것을 검토해 볼 필요가 있다. 그러나 앞에서 언급한 점을 고려하여 적법절차 원칙을 준수하는 가운데, 꼭 필요한 범위 내에서만 정보적 자기결정권을 제한할 수 있도록 해야 한다.

❖ 주제어 : 사이버범죄협약, 저장된 컴퓨터 데이터의 신속한 보존, 트래픽 데이터의 부분적 공개, 디지털 증거, 압수 · 수색, 적법절차 원칙

* 한국형사정책연구원 부연구위원, 법학박사.
** 아주대학교 대학원, 석박사통합과정.

Ⅰ. 서론

유럽평의회 사이버범죄협약(Convention on Cybercrime)은 정보통신기술로 인해 새롭게 등장한 문제현상인 초국가적 사이버범죄에 대한 국제사회의 효율적 대처를 목적으로 2001년 11월 8일 채택되고 2004년 7월 1일 발효된 국제규범이다. 이 협약은 사이버범죄에 대한 국가간 형사사법 공조를 보다 강화하기 위하여, 각 국가마다 서로 다소간 차이가 있었던 주요 사이버범죄의 표준 구성요건을 제시하는 실체법적 부분과, 디지털 증거에 대한 수사방법 및 강제수사의 국제공조에 관한 절차법적 부분으로 구성되어 있다. 그러나 사이버범죄협약이 처음 제정되었던 2001년 당시와 비교해 10여년의 세월이 지난 현재, 정보통신 기술의 급속한 발전, 인터넷 사용인구의 급증, 이용자의 인식변화 등으로 인하여 협약 제정 당시에는 미처 생각하지 못했던 많은 문제점들이 지적되고 있는 것도 사실이다.[1)]

특히 절차법적 영역에서는, 기존의 수사절차와 방법으로는 적절하게 대응하는데 한계가 있을 수밖에 없다는 문제의식 아래에서 디지털 증거에 대한 수사의 효율성 측면이 보다 강조되었기 때문에 상당히 강력한 강제수사절차를 도입하는 것을 내용으로 하고 있으나, 오늘날에는 이러한 점이 오히려 이 협약이 세계적인 보편규범으로 자리 잡지 못하게 만드는 원인이 되고 있는 것으로 평가되고 있다. 국경을 넘는 수사권 행사에 수반될 수밖에 없는 주권의 충돌과 이에 대한 여러 국가들의 서로 다른 다양한 이해관계로 인하여 상당수의 국가가 협약 제정 이래 지금까지도 협약 가입을 명시적으로 거부하고 있는데, 실체적 진실발견에 지나치게 편향된 협약의 절차법적 규정들이 정보적 자기결정권을 비롯한 개인의 인권에 심각한 위협이 될 수도 있다는 비판적 관점이 협약 거부의 정당성을 지지하는 강력한 논거가 되고 있기 때문이다.

실제 이 협약에 따르면 각 가입국은 개인이나 기업 소유의 컴퓨터 데이터[2)]와 트래픽 데이터(traffic data)[3)]는 물론 가입자 정보의 신속한 보존과 제출을 명령할 수 있

1) 정보통신기술발전과 사이버범죄의 변화에 대해서는 이원상, 해킹미수 처벌 논의에 대한 고찰, 비교형사법연구, 제13권 제2호, 2011, 211쪽 이하 참고.

2) 사이버범죄협약 제1조 b. “컴퓨터 데이터”란 컴퓨터 시스템을 작동하게 하는데 적합한 프로그램을 포함하여 컴퓨터 시스템에서 처리되기에 적합한 형태의 모든 사실, 정보 또는 개념 등을 의미한다.

3) 사이버범죄협약 제1조 d. “트래픽 데이터”란 통신망의 부분을 구성하는 컴퓨터 시스템에 의하여

으며, 더 나아가 각 가입국은 온라인 수색과 트래픽 데이터의 실시간 수집·기록을 위한 법적 제도를 마련하고 다른 나라의 요청에 협조해야 한다. 정보사회에서 개인의 삶의 대부분이 정보화되어 기록되고 저장된다는 점을 고려한다면, 디지털 증거의 수집 및 보존이라는 명목 하에 수사기관에 국경을 넘는 과도한 권한을 부여하는 부작용을 낳고 있다는 우려가 상당한 설득력을 갖는 것이다. 이 글에서는 사이버범죄협약의 절차법적 규정들 중에서 특히 우리 형사소송법에서 유사한 내용을 찾기 어려운 데이터의 보존 및 공개에 관한 절차규정으로 논의를 한정하여 이에 대한 사이버범죄협약 규정을 살펴보고 관련 조항들이 제정 목적에 부합하는지, 그리고 어떠한 문제가 있는지에 대하여 검토하고, 우리나라의 현행법상 절차규정과 비교해 보고자 한다.

Ⅱ. 사이버범죄협약 개요

1. 제정 경위

전세계적으로 컴퓨터 및 컴퓨터 시스템을 이용한 범죄, 즉 사이버범죄가 점차 확대됨에 따라 1985년 유럽평의회(Council of Europe)는 전문가위원회의 하나로 '유럽형사문제위원회(ECCP; European Committee on Crime Problems)를 구성하고 '통신방해 관련 형사사법공조에 관한 유럽협약의 실질적 적용에 관한 권고[4]'를 발표하였다. 이어 1989년 제428차 각료위원회 회의에서는 '국내법상 컴퓨터 범죄의 입법을 위한 가이드라인 제공을 목적으로 한 컴퓨터 관련 범죄에 대한 권고[5]'를 승인하였다. 이후 유럽형사문제위원회는 점차 심각해지는 사이버범죄문제에 보다 적극적으로 대응하기 위하여 1996년 11월 '증거서류의 요건 및 복제서류와 복제전자데이터의 증거능력에 관한 권고[6]', '통신방해에 대한 형사사법공조에 관한 유럽협

생성된 것으로 컴퓨터 시스템을 이용한 통신에 관련된 모든 컴퓨터 데이터를 의미하며, 통신의 발신, 수신, 경로, 시간, 일시, 크기, 지속기간, 또는 기반이 된 서비스의 유형을 나타내는 데이터를 말한다.

4) No. R(85)10. 본 권고안은 1985년 6월 28일 제387차 장관회의에서 채택되었다.

5) No.R(89)9.

6) No. R(81)20.

약의 실질적 적용에 관한 권고[7]', '경찰의 개인정보이용에 관한 권고[8]' 및 '국내법상 컴퓨터범죄 입법을 위한 가이드라인 제공을 목적으로 한 컴퓨터관련 범죄에 대한 권고' 등에 근거하여 사이버범죄 전문가 위원회(Committee Experts on Crime in Cyberspace)를 설치하기로 결정하였다.[9]

본 결정에 따라 1997년 2월 4일 개최된 제583차 회의에서 '사이버범죄에 관한 전문가회의'를 설치하기로 결의[10]하였으며, 1997년 4월부터 사이버범죄에 관한 최초의 국제협약을 제정하기 위한 협의가 시작되었으나 그 과정은 그리 순탄치 않았으며, 당초 기한은 1999년 12월 31일까지였으나 형사법적 쟁점 중 일부 사항에 대한 협의가 이루어 지지 않아 기한을 다음해인 2000년 12월 31일로 연장해야 했다.[11] 마침내 전문가회의는 유럽형사문제위원회의 도움을 받아 협약안을 완성하였고, 2001년 6월 22일 제50차 유럽형사문제위원회에 수정된 최종 협약안이 제출되어 승인을 받았다. 같은 해 11월 8일 각료위원회는 이 협약안을 채택했고, 2001년 11월 23일 헝가리 부다페스트에서 열린 가입행사에서 유럽평의회 비회원국 4개국 포함하여 30개국의 가입을 받았고, 5개국 이상이 비준을 완료한 2004년에 비로서 발효될 수 있었다.[12]

2006년 협약위원회(T-CY; The Convention Committee)는 스마트폰, PDA, 태블릿 등 새로운 정보통신기기를 포함할 수 있도록 협약 제1조에서 명시하고 있는 '컴퓨터 시스템'에 대한 정의를 수정하였으며, 수정안은 2012년 12월 제8차 총회에서 채택되었다. 이후 2012년, 협약위원회는 기준설정, 모니터, 역량구축 세 가지를 주축으로 하는 부다페스트 협약의 이행 평가를 시작했고, 같은 해 12월 제8차 총회에서 16조(데이터의 신속한 보존), 17조(국내절차)와 29조, 30조(국제공조)에 관한 제

7) No. R(85)10.

8) No. R(87)15E.

9) Decision CDPD/103/211196.

10) Decision No. CM/Del/Dec(97)583

11) Decision No. CM/Del/Dec(99)679

12) 제정 경위에 관해서 상세한 내용은 유럽평의회, 사이버범죄협약 주석보고서(Explanatory Report to the Convention on Cybercrime; http://conventions.coe.int/Treaty/en/Reports/Html/185.htm) 참조; 이영준/금봉수/정완, 사이버범죄방지조약에 관한 연구, 형사정책연구, 형사정책연구원, 2001, 11쪽 이하; 김한균/김성은/이승현, 사이버범죄방지를 위한 국제공조방안 연구, 대검찰청 연구용역 보고서, 2009, 11쪽 이하 참조.

1차 평가를 진행한 바 있다.[13]

본 협약은 다수 국가가 사이버범죄에 대한 수사와 처벌을 위한 협력의 틀을 마련한 최초의 국제협약이며 인터넷상의 모든 범죄행위 및 그에 대한 처벌과 관련하여 상세한 규정을 두고 있다는 점에서 중요한 의미를 갖는다 할 수 있다. 그러나 2013년 현재까지도 유럽평의회 47개국 중 협약을 비준한 국가는 36개국에 이르지만 미국 일본 등 비회원국 4개국에 불과하다. 다시 말해, 사이버범죄협약은 아직 보편적 국제규범으로 확대되지 못하고 있다.[14]

2. 주요 내용

사이버범죄협약은 사이버범죄와 관련하여 각 가입국의 국내 형사실체법상의 구성요건 및 관련 규정간의 조화, 컴퓨터 시스템을 이용하거나 전자 증거와 관련된 범죄의 수사와 기소에 필요한 각 가입국의 국내 형사절차법적 권한 규정, 빠르고 효과적인 국제 형사사법공조의 기반 정립을 목적으로 한다.[15] 이를 위해 사이버범죄협약은 서문 및 4장 48개조의 규정으로 구성되어 있다. 제1장은 이 협약에서 사용되는 용어의 정의, 제2장은 형사실체법, 절차법, 관할권 등에 관하여 가입국이 취해야 할 법제도적 조치, 제3장은 국제 형사사법공조의 일반원칙 및 사이버범죄에 관한 구체적 형사사법공조를 위한 절차규정, 제4장은 협약의 서명·비준·발효 등에 관한 유럽의회 협약 표준규정을 내용으로 한다.

이 중 제2장이 본 협약의 핵심이라고 할 수 있을 것이다. 제2장의 제1절은 실체법에 관한 것으로 컴퓨터 시스템 및 데이터에 관한 범죄 또는 컴퓨터 및 컨텐츠 관련 범죄의 구성요건에 관하여 규정하고 있다. 다만 정보통신기술발전에 따라 계속 변화

13) 각 가입국의 이행입법 현황에 관해서는 유럽평의회 사이버범죄협약위원회 이행평가 보고(http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2012_10_Assess_report_v30_public.pdf), 2013, 참조.

14) 서명 및 비준국 명단은 유럽평의회 홈페이지(http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG) 참조.

15) 유럽평의회, 사이버범죄협약 주석보고서(Explanatory Report to the Convention on Cybercrime; http://conventions.coe.int/Treaty/en/Reports/Html/185.htm); 김한균/김성은/이승현, 사이버범죄방지를 위한 국제공조방안 연구, 대검찰청 연구용역보고서, 2009, 16쪽 참조.

· 확장하고 있는 사이버범죄에 대한 포괄적인 개념을 직접 정의하고 있지 않으며[16] 구체적인 행위유형을 구성요건으로 정하는 방법을 이용하고 있다. 협약 제2장 제1절은 9개 유형의 범죄 행위를 4개 군으로 분류하고 이를 국내법상 형사실체법으로 규정하여 처벌하도록 의무화하고 있다.[17] 제1군은 컴퓨터 데이터와 시스템에 대한 침해로 불법접속, 불법감청, 데이터 침해, 시스템 이용 방해, 시스템 및 데이터 부정이용 등 다섯 가지 구성요건을 포함한다. 제2군은 컴퓨터 관련 범죄라는 표제 아래 컴퓨터 관련 위조, 컴퓨터 사용 사기를 규정하고 있다. 제3군은 콘텐츠 관련 범죄로 아동 음란물 관련 구성요건이 이에 해당한다. 제4군은 저작권 및 관련 권리에 대한 침해이며 컴퓨터 시스템을 이용한 저작권 침해를 구성요건으로 구체화하고 있다.[18]

제2장의 제2절은 절차법과 관련한 것으로 제1절의 실체법에서 규정하고 있는 범죄를 효과적으로 수사하여 처벌하기 위한 절차규정을 상세하게 명시하고 있다. 여기에는 저장된 데이터의 신속한 보존, 트래픽 데이터의 신속한 보존 및 공개, 가입자 정보에 대한 제출명령, 컴퓨터 데이터의(온라인) 압수 및 수색, 트래픽 데이터의

16) 정보통신 기술발전과 이를 규율하는 형사법적 개념의 모호성에 대한 분석으로는 전현욱, 개인정보 보호에 관한 형법정책, 고려대학교 박사학위논문, 2010, 37쪽 이하 참조.

17) 사이버범죄협약상 사이버범죄의 유형에 관하여 상세한 해설은 김한균/김성은/이승현, 사이버범죄 방지를 위한 국제공조방안 연구, 대검찰청 연구용역보고서, 2009, 17쪽 이하 참조.

18) 2013년 OECD가 발간한 Comprehensive Study on Cybercrime도 사이버범죄의 개념은 각각의 다양한 개별 범죄의 행위양태를 통해서 구체화되며 모든 사이버범죄를 포괄하는 일반 개념으로는 정의될 수 없음을 확인하였다. 이 보고서는 사이버범죄인지 여부를 확인하기 위해서는 우선 실질적인 위법행위를 시행할 의도를 확인하고, 컴퓨터를 이용한 행위가 개별적인 구성요건에 해당되는지 판단해야 한다고 설명하고 있다. 이러한 관점에서 UNODC 보고서는 사이버범죄의 구성요건을 14가지 3개군으로 분류하였다. 제1군은 컴퓨터 데이터 시스템의 기밀, 완전성 및 이용가능성 관련 범죄로 1) 컴퓨터 시스템에 대한 불법 접근, 2) 컴퓨터 데이터에 대한 불법 접근 및 손괴, 3) 컴퓨터 시스템 및 데이터에 대한 불법적 개입, 4) 컴퓨터를 악용할 수 있는 도구의 생산, 유포 및 소지, 5) 사생활 침해 및 데이터 보호 조치 위반을 포함한다. 제2군은 개인적·경제적 이익 및 손해야기를 목적으로 하는 컴퓨터 관련 행위로 1) 컴퓨터 관련 사기 또는 위조, 2) 컴퓨터 관련 신원도용, 3) 컴퓨터 관련 저작권 또는 상표권 침해, 4) 스팸 발송 또는 관리, 5) 개인적 피해를 가하게 되는 컴퓨터 관련 행위, 6) 컴퓨터를 이용한 성행위를 위한 아동의 그루밍(grooming) 또는 유인 등이 이에 해당한다. 제3군은 컴퓨터 콘텐츠 관련 행위로 1) 컴퓨터를 이용하여 특정 인종이나 그룹에 대한 경멸 또는 증오 등 차별적 의사표현, 2) 컴퓨터를 이용한 아동 포르노 생산 및 유포, 3)컴퓨터를 이용한 테러 지원 행위를 말한다. 이는 사이버범죄협약과 유사한 방법이나, 10여년의 시간이 흐름에 따라 사이버범죄에 해당하는 구성요건의 유형과 범위가 넓어졌음을 알 수 있다. 상세한 내용은 UNODC, Comprehensive Study on Cybercrime, 2013, 16쪽 참조.

실시간 수집 콘텐츠 데이터의 감청 등이 포함된다. 이 외에도 절차 규정의 범위에 대한 지침과 함께 시행해야 할 권리보장 조치와 조건에 대한 내용을 추가로 규정하고 있으며, 마지막으로 관할권과 관련한 조항을 명시하고 있다. 제3장은 형사사법공조의 일반원칙으로 호혜성, 범죄인 인도, 협력의무, 그리고 이 협약 제2절의 수사절차를 국경을 넘어 신속하게 집행하는데 필요한 국가간 권리와 의무에 관한 사항을 규정하고 있으며, 또한 가입국간 신속한 공조를 위한 24/7 네트워크 구축에 대해 규정하고 있다.

Ⅲ. 저장된 데이터의 신속한 보존

1. 근거 규정 – 제16조, 제29조

제16조(저장된 컴퓨터 데이터의 신속한 보존)

1. 각 가입국은 컴퓨터 시스템에 저장되어 있는 트래픽 데이터를 포함한 특정한 컴퓨터 데이터가 특히 손실되거나 변조될 수 있다고 믿을 만한 근거가 있는 경우 자국의 권한 있는 기관의 명령 또는 이와 유사한 방법으로 이러한 데이터의 신속한 보존을 확보하기 위해 필요한 입법 및 그 밖의 조치들을 도입하여야 한다.
2. 가입국이 제1항을 실행하여 저장된 특정 컴퓨터 데이터를 소지하거나 관리하는 자에게 그 데이터를 보존할 것을 명령하는 경우, 가입국은 최대 90일 이내의 범위에서 필요한 기간 동안 그 데이터의 소지 또는 관리자가 컴퓨터 데이터의 무결성을 유지하여 보관하도록 하기 위해 필요한 입법과 그 밖의 조치들을 도입하여야 한다. 가입국은 이러한 명령이 연속하여 연장될 수 있도록 규정할 수 있다.
3. 각 가입국은 간수자(看守者) 또는 컴퓨터 데이터를 보존해야 하는 자가 이러한 절차가 진행되고 있다는 사실을 비밀로 하도록 하기 위해 필요한 입법과 그 밖의 조치들을 도입하여야 한다.
4. 동조에 의한 권한과 절차는 제14조와 제15조의 적용을 받는다.

협약 제16조와 제29조는 저장되어 있는[19] 컴퓨터 데이터가 보존될 수 있도록 강제하는 형사절차적 권한을 수사기관에 부여하는 것을 내용으로 한다. 제16조는 국내 수사절차에서 필요한 입법적 조치에 관해서, 그리고 제29조는 저장된 컴퓨터 데이터의 신속한 보존과 관련한 국제 수사공조의 절차 및 방법에 관해서 규정하고 있다. 데이터의 보존이란 저장된 데이터의 내용뿐만 아니라 현재의 상태를 변경할 수 있는 모든 가능성으로부터 보호하는 것을 말하며[20], 보존명령의 대상에는 트래픽 데이터뿐만 아니라 콘텐츠 데이터도 포함된다. 보존 의무를 지는 자는 개인은 물론 법인을 포함한다.[21] 제16조는 수사대상의 범위를 전통적인 유체물에서 컴퓨터 데이터로 확대하였을 뿐만 아니라, 제2항에서 무결성(Integrity)[22]을 보장할 것을 요구하는 등, 일정한 형태가 없는 디지털 증거의 특성을 반영한 수사절차규정으로 평가되고 있다.[23]

디지털 데이터는 변조와 인멸이 매우 용이할 뿐만 아니라[24], 대체로 일정기간이 경과하면 자동으로 삭제되도록 되어있다.[25] 그런데 압수·수색이나 제출명령 등 적법한 강제수사의 전제가 되는 법원의 영장 또는 허가장을 발부받는 절차는 상당한 시간이 소요될 수밖에 없는 것이 현실이다. 또한 영장청구 등 공식절차가 진행되고 있다는 사실이 피의자 등 이해관계인에게 알려지기 쉬우므로, 이러한 적법절차를 모두 거치는 과정에서 증거가 훼손될 가능성이 높다. 그래서 협약 제16조는 이러한

19) 통신 중인 데이터의 실시간 감청은 협약 제20조와 제21조에서 규정하고 있다. 이 글은 저장된 데이터의 신속한 보존 및 일부 제공에 한정해서 논의하고자 한다.

20) 노명선, 사이버범죄 대처를 위한 EU사이버범죄협약 가입 필요성과 가입에 따른 협약이행 방안, 대검찰청 연구용역보고서, 2011, 103쪽.

21) 유럽평의회 사이버범죄협약위원회 이행평가 보고서 (http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2012_10_Assess_report_v30_public.pdf), 2013, 6쪽.

22) 무결성이란, 처리, 저장, 소통되는 정보가 비인가자에 의해 변경 및 파괴되지 않도록 정확성, 안전성이 보장되어야 한다는 원칙이다. 정필운, 유비쿼터스 컴퓨팅 환경에서 정보보안관련입법의 현실과 지향, 인터넷법률, 제40호, 2007, 166쪽.

23) 박희영, 사이버범죄방지협약의 형사절차법 규정의 평가와 현행 형사절차법 관련 규정의 개정방향, 인터넷법률, 제46호, 2009, 165쪽.

24) 증거로서 디지털 데이터의 특징에 관하여 상세한 내용은 전현욱/윤지영, 디지털 증거 확보를 위한 수사상 온라인 수색제도 도입 방안에 대한 연구, 대검찰청 연구용역보고서, 2012, 7-11쪽 참조.

25) 특히 컴퓨터 데이터는 이용자의 개인정보가 되는 경우가 대부분이며, 따라서 개인정보 보호와 관련하여 법률이나 약관을 통해 이용목적을 달성한 경우 즉시 복구 불가능한 방법으로 파기되도록 되어있는 경우가 많다. 개인정보보호법 제21조(개인정보의 파기) 참조.

위험을 제거하여 휘발성이 높은 디지털 증거에 대한 "신속한 보존"을 확보함으로써 이어질 제출명령(제18조) 및 압수·수색(제19조) 절차의 실효성을 확보하기 위한 규정이다. 이러한 관점에서 제16조 제3항은 보관자 등에게 보존 절차가 진행되고 있다는 사실에 대한 비밀엄수(기밀성)의 의무를 부과하고 있다.[26] 특히 초국가적 사이버범죄에 대한 국제공조수사의 경우 형사사법공조 과정에 더 많은 시간이 필요할 수밖에 없기 때문에 협약 제29조는 제7항에서 국제공조를 위한 보존명령의 경우 요청국이 압수·수색 또는 이와 유사한 적법절차를 밟을 수 있도록 60일 이상의 기간으로 할 것을 명시하고 있다.

컴퓨터 데이터의 보존 방법에 대해서는 구체적으로 규정되어있지 않으며, 각 국가의 입법재량에 맡기고 있다. 다만 제16조는 데이터의 보존을 명령하는 권한만을 수사기관에 부여할 뿐이며, 그 내용에 접근하는 것은 허용하지 않는 것으로 보아야 한다. 사이버범죄협약은 데이터의 내용을 확인하려면 제출명령 또는 압수·수색의 절차를 별도로 거치도록 하고 있다. 컴퓨터 데이터의 신속한 보존조치는 그 긴급성으로 인하여 현실적으로 사법적 통제가 쉽지 않을 수밖에 없다는 점을 고려하여 기본권 제한의 한계가 설정된 것이다. 따라서 제16조의 보존명령은, 남용되지 않는 것을 전제로 하면, 원칙적으로 정보적 자기결정권에 대한 침해 우려가 높지 않은 것으로 볼 수 있다.

2. 신속한 보존과 적법절차 원칙

가. 수인의무 또는 협력의무

협약 제16조는 수사기관의 보존명령에 대해서만 규정하고 있을 뿐, 보존명령에 대한 당사자의 수인의무나 서비스제공자의 협력의무에 관해서는 명확하게 규정하고 있지 않다는 비판[27]이 있다. 수범자의 명령 준수의무에 관하여 명백한 법령이 마련되지 않으면 보존명령의 실효성을 담보하기 어려울 뿐만 아니라, 타인의 컴퓨

26) 유럽평의회, 사이버범죄협약 주석보고서(Explanatory Report to the Convention on Cybercrime; http://conventions.coe.int/Treaty/en/Reports/Html/185.htm).

27) 이러한 비판은 박희영, 사이버범죄방지협약의 형사절차법 규정의 평가와 현행 형사절차법 관련 규정의 개정방향, 인터넷법률, 제46호, 2009, 163쪽 참조.

터 데이터를 보관하고 있는 ISP 등의 경우 개인정보 삭제 의무와 충돌하여 민사상 손해배상 책임은 물론 형사책임을 지게 될 가능성도 있기 때문이다. 그러나 제16조는 컴퓨터 데이터의 신속한 보존명령에 관한 국내법 제정의 지침일 뿐이며, 더욱이 "필요한 입법과 그 밖의 조치"를 할 것을 내용으로 하고 있으므로 이러한 내용은 보존명령 제도를 국내법에 도입하는 각 가입국이 고려해야 할 내용일 뿐이다. 또한 별도의 의무규정을 두지 않아도 명령규정의 해석상 수범자의 의무나 면책은 당연히 수반된다 할 것이다.

나. 모든 데이터의 동등취급과 비례성 원칙

협약 제16조는 보존명령의 객체가 될 컴퓨터 데이터의 종류를 구분하지 않는다. 데이터의 내용과 상관없이 다만 "손실되거나 변경될 수 있다고 믿을 만한 근거가 있는 경우" 보존명령을 내릴 수 있도록 하고 있다. 그러나 수사절차에서 실체적 진실발견은 무조건 달성되어야 하는 절대적 가치가 아니며, 당연히 비례성 원칙이 준수되는 범위 내에서만 허용될 수 있다. 강제수사를 통해 얻어질 이익과 이로 인해 침해되는 국익 및 인권 등 다른 중요한 이익들과의 관계에서 균형성이 요구되는 것이다. 우리 형사소송법도 제110조 내지 제112조에서 군사상·공무상·업무상 비밀에 대한 압수의 한계를 규정하고 있다. 협약 제16조가 규정하고 있는 데이터의 신속한 보존은 압수·수색의 실효성을 확보하기 위한 전단계 절차이며, 따라서 압수·수색이 허용되어서는 안 되는 사생활의 핵심적인 부분이나 국가적 비밀 등에 대해서는 보존명령이 제한될 필요가 있다.[28)]

사이버범죄협약은 데이터의 종류에 따른 보존명령의 한계를 설정하고 있지 않으나, 다만 다음과 같은 두 가지 한계를 확인할 수 있다. 첫째, 협약 제16조 제4항은 보존명령과 관련하여 제15조를 준수하도록 하고 있는데, 제15조 제1항은 유럽평의회의 1950년 "인권과 기본적 자유의 보호에 관한 유럽협약"과 UN의 1966년 "시민적 정치적 권리에 관한 국제규약"에 따라 인권과 자유를 보장할 것을 내용으로 하고 있다. "인권과 기본적 자유의 보호에 관한 유럽협약" 제8조[29)]와 "시민적 정치적

28) 박희영, 사이버범죄방지협약의 형사절차법 규정의 평가와 현행 형사절차법 관련 규정의 개정방향, 인터넷법률, 제46호, 2009, 165쪽 참조.

권리에 관한 국제규약" 제17조[30]는 모두 사생활의 자유를 보장하고 있으며, 특히 통신비밀에 대한 권리를 명시하고 있다. 물론 사생활 또는 통신비밀에 대한 권리 역시 절대적인 것은 아니므로, 당연히 범죄수사를 위하여 제한될 수 있어야 하겠지만, 필요한 범위를 넘는 그리고 상대적으로 중요한 권리에 대한 침해는 정당화 될 수 없다.[31] 그러므로 가입국은 부당한 기본권 침해의 여지를 최소화하기 위하여, 데이터의 신속한 보존과 관련하여 국내법적 제도를 마련함에 있어 협약 제16조 제4항에 근거하여 컴퓨터 데이터의 중요도와 유형에 따라 세분하여 차별화된 규정을 마련해야 할 것이다.

둘째, 신속한 보존과 관련된 국제공조절차를 규정하고 있는 제29조 제5항은 "정치범죄 또는 정치범죄와 연관된 범죄라고 판단되는 경우"와 "주권, 안보, 공공질서 또는 다른 중요한 이익을 침해하는 경우"에는 타국의 보존요청을 거절할 수 있는 것으로 하고 있다. 따라서 가입국은 협약 제29조 제5항에 근거하여 사생활의 중대한 이익에 대한 보호뿐만 아니라 군사상·공무상 비밀을 이유로 국제공조를 거부할 수 있다. 그러므로 적절하게 만들어진 국내법과, 실무상 적극적인 주권행사를 전제로 한다면, 제16조 및 제29조의 컴퓨터 데이터의 신속한 보존명령과 관련하여 국가의 주권이나 개인의 인권이 부당하게 침해될 우려는 크지 않다고 할 것이다.

다. 보존기간 연장의 상한

협약 제16조는 데이터 보존기간을 90일 이내에서 필요한 범위로 정할 수 있도록 함으로써, 원칙적으로 보존기간의 상한을 90일로 정하고 있다. 그러나 제2문에서

29) 제8조(사생활 및 가족생활을 존중받을 권리) 1. 모든 사람은 그의 사생활, 가정생활, 주거 및 통신을 존중받을 권리를 가진다. 2. 법률에 합치되고, 국가안보, 공공의 안전 또는 국가의 경제적 복리, 질서유지와 범죄의 방지, 보건 및 도덕의 보호, 또는 다른 사람의 권리 및 자유를 보호하기 위하여 민주사회에서 필요한 경우 이외에는, 이 권리의 행사에 대하여는 어떠한 공공당국의 개입도 있어서는 안 된다. 원문은 유럽평의회 홈페이지(http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm) 참조.

30) 제17조 1. 어느 누구도 그의 사생활 가정 주거 또는 통신에 대하여 자의적이거나 불법적인 간섭을 받거나 또는 그의 명예와 신용에 대한 불법적인 비난을 받지 아니한다. 2. 모든 사람은 그러한 간섭 또는 비난에 대하여 법의 보호를 받을 권리를 가진다. 원문은 UN OHCHR 홈페이지 (http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx) 참조.

31) 범죄자의 프라이버시권 보호의 기준과 한계에 관해서는 박혜진, 형법적 관점에서 바라 본 피의사실 공표죄의 제문제, 비교형사법연구 제13권 제2호, 2011, 159-160쪽 참조.

이러한 명령이 연장될 수 있도록 규정할 수 있다고 하여, 결국 보존기간의 상한을 명시하지 않은 것으로 해석된다. 사이버범죄협약은 보존기간의 연장과 관련하여 얼마의 기간을 그리고 몇 번이나 연장할 수 있는 지에 대해서는 명시하지 않고 있고, 오직 가입국이 입법적 조치를 통해 기간을 정하도록 하고 있다. 다만 제29조 제7항에서 국제공조에 의한 신속한 보존명령에 따른 보존기간의 하한을 60일 이상으로 정하고 있을 뿐이다. 그런데 신속한 보존명령은 이후의 강제수사절차 즉, 제출명령 또는 압수·수색의 효율성을 확보하기 위한 전단계 조치이며 영장청구 등의 적법절차를 밟기 위해 필수적으로 소요되는 시간 동안 인멸 등에 취약한 디지털 증거의 보존을 확보하기 위한 절차일 뿐이다. 따라서 오로지 기술적으로 영장 청구 등에 소요되는 시간을 확보하는 것에서 그쳐야 하며, 그 이상의 데이터 보존은 유럽평의회의 1950년 "인권과 기본적 자유의 보호에 관한 유럽협약"과 UN의 1966년 "시민적 정치적 권리에 관한 국제규약"을 위반하는 부당한 기본권 제한이 되는 것으로 보아야 할 것이다.

그러므로, 신속한 보존명령을 국내법에 도입함에 있어 기간의 상한은 제한적으로 해석되어야 하며, 제2문을 전체 90일의 범위 내에서만 연장 가능한 것으로 해석하는 것도 방법이 될 수 있을 것으로 생각한다.[32] 현실적으로 강제수사 절차에 소요되는 시간을 모든 경우에 90일 이내로 제한하는 것이 어려운 한계가 있다면 법이 허용하는 기간은 총 90일 이상으로 정하더라도, 실제 필요한 기간 동안에만 데이터를 보존하도록 하고 형사사법기관에게 절차를 신속히 마칠 의무를 부과하는 것이 대안이 될 수 있을 것이다. 사이버범죄협약을 비준한 미국의 경우 ISP에게 수사기관(Guvernmental entity)의 요청에 의해 최대 90일의 범위 내에서 영장 청구 등의 절차에 필요한 기간 동안 데이터를 보존하도록 하고 있으며 1회에 한하여 연장할 수 있도록 규정하여 총 180일을 보존기간의 상한으로 정하고 있다.[33] 프랑스는 정보통신기술자에게 그가 보존하는 사용자에 대한 정보를 1년 이하의 기간 동안 보존할 수 있도록 하고 있으나 판사의 허가를 받은 검사의 지휘에 따르도록 하여 요건을 엄격하게 제한하고 있으며, 또한 수사기관에게 해당 정보를 최단기간 내에 처리할 의무를 부과하고 있다.[34] 독일

32) 90일로 충분하다는 견해로 박희영, 사이버범죄방지협약의 형사절차법 규정의 평가와 현행 형사절차법 관련 규정의 개정방향, 인터넷법률, 제46호, 2009, 164쪽.

33) 18 U.S.C §2703(f).

은 신속한 보존명령에 관하여 별도의 규정을 두고 있지는 않으나 유럽평의회의 이행평가 보고서[35]는 검찰과 경찰의 수사권과 관련하여 정보제공을 비롯한 모든 명령을 내릴 권한이 있음을 선언하고 있는 형사소송법상의 일반규정과 트래픽 데이터에 대한 조사권한규정[36]을 보존명령과 유사한 조치로 해석하고 있다.[37]

라. 데이터 보관(retention)과의 관계

보존명령이 컴퓨터 데이터에 대한 강제수사의 실효성을 높여주는 전단계 절차임은 분명하다. 다만 보존명령이 실제 기능하기 위해서는 보존할 데이터가 존재해야 한다는 한계가 있다. 그러나 정보보호법은 개인정보를 법이 허용하는 요건을 충족하는 경우에만 수집할 수 있도록 하고 있으며, 더 나아가 수집 목적이 달성되면 복구 불가능한 방법으로 파기하도록 하는 경우가 대부분이다. 또한 데이터 저장에는 비용이 발생하기 때문에, 영업을 목적으로 서비스를 제공하는 ISP는 비용과 위험부담을 최소화하기 위하여 많은 양의 데이터를 보관하려 하지 않는다. 일부 ISP는 과금 등에 필요 없는 트래픽 데이터를 발생 즉시 삭제하기도 한다.

그래서 데이터 보존명령에 앞서 ISP에게 수사에 필요한 데이터에 대한 일반적인 보관(retention) 의무를 부여하는 것이 보존명령의 실효성을 높이기 위해 필요하다는 지적이 있다. 트래픽 데이터 보관에 관해서는 EU의 2006년 "통신사실확인자료의 보관에 관한 지침(the Data Retention Directive)"[38]에 근거하여 유럽연합의 대부분의 가입국이 법제화한 바 있다. 이 지침에 따르면 트래픽 데이터, 즉 인터넷 접속, 인터넷 이메일 및 인터넷 전화통신은 물론 유무선 전화통신과 관련된 가입자 정보와 위치 데이터를 6개월 이상, 2년 이하의 기간 동안 보관해야 한다(지침 제6조). 그러나

34) 프랑스 형사소송법 제60-2조 제2항, 제3항.

35) 유럽평의회 사이버범죄협약위원회 이행평가 보고서 (http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2012_10_Assess_report_v30_public.pdf), 2013, 28-31쪽 참조.

36) 독일 형사소송법 제161조 제1항, 제163조, 트래픽 데이터에 대해서는 제100조의g.

37) 독일에서 전통적인 법치국가 원칙이 약화되고 있다는 분석으로 김정환, 테러예비행위와 보호감호의 규정을 통해 살펴본 독일형법의 유럽화와 기능화, 비교형사법연구, 제14권 제1호, 2012, 31쪽 이하 참조.

38) Directive 2006/24/EC.

통신 콘텐츠에 관한 데이터나 URL, 수신 IP 주소, 이메일 헤더 등은 보관대상에 포함되지 않는다(지침 제3조).[39] 이러한 법제를 통해 일반적으로 통용되는 데이터 보관과 사이버범죄협약상 데이터 보존(preservation)의 차이는 다음 표와 같다.[40]

	신속한 보존	데이터 보관
목적	휘발성 디지털 증거의 적법한 강제수사를 위해 필요한 시간 확보	중대 범죄의 수사와 체포, 기소 가능성 확보
특성	특정 데이터에 대한 특별한 명령 필요	대상 데이터에 일반에 대한 자동화된 보관
데이터의 유형	모든 데이터(콘텐츠 데이터 포함)	트래픽 데이터, 가입자 정보와 위치 데이터(통신 콘텐츠에 관한 데이터나 URL, 수신 IP 주소, 이메일 헤더 등 불포함)
대상의 제한	디지털 증거에 관련된 모든 범죄	중대 범죄
수범자	모든 자연인 또는 법인	서비스 제공자
기간	유동적 : 90일 이내(연장 가능)	6개월 이상 2년 이하의 기간 중에서 국내법에 의해 정해진 기간.

그러나 사이버범죄협약은 데이터의 보관에 관한 국내법 규정을 제정할 의무를 각 국가에 부과하는 것은 아니다.[41] 따라서 가입국은 사이버범죄협약의 컴퓨터 데이터 신속한 보존을 위하여 모든 데이터의 보관의무에 관한 규정을 새로 만들어야 하는 것은 아니며, 반대로 EU의 지침에 의하여 이미 트래픽 데이터에 대한 보관의무가 국내법에 입법되어있다 하더라도, 신속한 보존명령을 위해서 필요한 추가적인 입법적 조치를 취해야 하는 것이다. 다만 보존명령의 실효성을 확보할 목적으로 보관의무의 내용을 확대하는 것은 신중해야 한다. ISP의 트래픽 데이터 보관의무를 규정하고 있는 EU의 지침은 제한적인 트래픽 데이터에 대한 보관의무만을 규정하고 있으며 매우 중대한 범죄에 한하여 이를 이용할 수 있도록 하고 있음에도 불구하고 제정 당

39) 이는 우리나라의 통신비밀보호법 제15조의2와 같은 법 시행령 제41조 제2항에서 규정하고 있는 통신사실확인자료의 보관의무와 유사한 것으로 다만 우리법제는 "상대방의 가입자번호"까지 저장해야 하는 것으로 정하고 있다. 다만 통신은 대체로 상호적으로 발생하는 것이므로, 발신자는 동시에 수신자가 되며, 수신자의 상대방이 된다.

40) 보존과 보관의 차이에 관한 표는 유럽평의회, 사이버범죄협약위원회 이행평가 보고서 (http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2012_10_Assess_report_v30_public.pdf), 2013, 76쪽에서 인용.

41) 이러한 취지는 유럽평의회, 사이버범죄협약 주석보고서(Explanatory Report to the Convention on Cybercrime; http://conventions.coe.int/Treaty/en/Reports/Html/185.htm).

시부터 프라이버시 침해에 대한 우려로 시민의 저항이 상당하였으며, 현재 개정작업이 진행 중이다.[42] 더 나아가 모든 이용자의 콘텐츠 데이터를 자동화된 시스템을 이용하여 보관하는 것은 그 자체로 프라이버시의 중요한 내용을 심각하게 침해하는 것으로 비례성 원칙을 충족할 수 없으므로 규범적으로 정당화될 수 없을 뿐만 아니라, 엄청난 저장용량이 필요하게 되므로 경제적으로도 불가능[43]할 것으로 생각된다.

IV. 트래픽 데이터의 일부 공개

1. 근거 규정 – 제17조, 제30조

제17조(트래픽 데이터의 신속한 보존과 부분적 공개)

1. 각 가입국은 제16조에 의하여 보존되어야 할 트래픽 데이터에 관하여 다음과 같은 조치를 확보하는데 필요한 입법과 그 밖의 조치를 취해야 한다.
   a. 다수의 서비스 제공자가 통신의 전송에 관여하였더라도 신속한 보존이 가능하도록 해야 한다.
   b. 서비스 제공자와 해당 통신의 전송 경로를 확인하기에 충분한 양의 트래픽 데이터를 가입국의 정당한 권한을 가진 기관이나 그 기관이 지명한 자에게 신속하게 공개할 수 있도록 해야 한다.
2. 이 조에 의한 권한과 절차는 제14조와 제15조의 적용을 받는다.

---

42) 상세한 내용은 유럽위원회(European Commission), 통신사실확인자료의 보관에 관한 지침 평가보고서(Evaluation report on the Data Retention Directive; http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/ com2011_225_data_retention_evaluation_en.pdf), 2011, 특히 프라이버시와 관련해서는 28쪽 이하 참조.

43) 통신사업자의 저장비용에 관하여 참고할만한 객관적인 자료를 찾는 것은 쉽지 않다. 다만 2003년을 기준으로 세계적인 서비스제공자인 AOL은 하루에 3억9천2백만 사용자가 약 5억9천7백만 개의 이메일을 전송하고 있으며, 시스템을 구축하는데 약 4천만 달러의 비용이 들고 이를 유지하는데 연간 1천4백만 달러가 소요될 것으로 추정되었다. All Party Internet Group, Communications Data - Report of an Inquiry by the All Party Internet Group (http://www.steptoe.com/assets/attachments/2162.pdf), 2003, 22쪽 참조.

사이버범죄협약 제17조는 제16조의 특칙이며 제30조는 제17조와 관련한 국제 수사공조에 관한 규정이다. 제16조는 트래픽 데이터를 포함한 모든 컴퓨터 데이터에 대한 보존명령을 규정하고 있으나 제17조는 신속한 보존을 확보하기 트래픽 데이터에 한정하여 위하여 추가적으로 필요한 조치를 규정하고 있다. 발신자와 수신자가 일대일로 연결되는 전통적인 통신과는 달리, 인터넷으로 대표되는 컴퓨터 통신은 패킷으로 쪼개져 다수의 중간단계를 거쳐 전달되며, 그 과정에서 각각의 전산망에 걸리는 부하에 따라 다양한 경로를 이용하게 된다.[44] 사이버범죄와 관련한 통신도 역시 마찬가지이며, 범죄자는 의도적으로 경로를 복잡하게 하거나 중간의 트래픽 데이터에서 흔적을 지우는 방법을 이용하여 추적을 회피하기도 한다.

인터넷 통신에서 트래픽 데이터는 패킷이 경로로 삼은 다수의 서버에서 모두 발생할 수밖에 없으며, 따라서 신속한 보존명령의 대상이 되는 ISP를 모두 특정하여 이들에게 데이터의 보존을 명령하기 위해서는 범죄자에 의해서 이용된 것으로 확인된 ISP로부터 최소한 패킷의 통신 경로에 관한 트래픽 데이터를 신속하게 확보할 수 있어야만 한다. 트래픽 데이터를 통해 통신에 관여한 ISP를 순차적으로 확인하여 최종 서비스 제공자를 발견하고 이를 통해 가입자 정보 및 위치정보를 특정해야 하기 때문이다. 그러나 단순히 중계(routing)만 담당한 서버의 트래픽 데이터는 일반적으로 그리 오래 보관되지 않는다.[45] 그래서 제17조 제1항 a는 통신의 전송에 다수의 서비스 제공자가 관여한 경우에도 모든 서비스 제공자에게 신속한 보존명령을 내릴 수 있어야 한다고 규정하고 있으며, 이를 가능하게 하기위해 제1항 b는 해당 통신의 전송경로를 확인하기에 충분한 트래픽 데이터를 수사기관이 확보하는데 필요한 입법적 조치를 취할 것을 규정하고 있다.

이 과정에서 다른 가입국의 영역 내에 있는 서비스 제공자가 통신의 전송에 관여하였음이 확인되는 경우 협약 제29조에 의하여 그 가입국에 저장된 데이터의 신속한 보존을 요구할 수 있으며, 피요청국은 제16조와 제17조에 관한 국내법절차에 의하여 자국 내의 컴퓨터 데이터에 대한 신속한 보존과 트래픽 데이터에 대한 일부

44) 박희영, 사이버범죄방지협약의 형사절차법 규정의 평가와 현행 형사절차법 관련 규정의 개정방향, 인터넷법률, 제46호, 2009, 166쪽.

45) 유럽평의회, 사이버범죄협약 주석보고서(Explanatory Report to the Convention on Cybercrime; http://conventions.coe.int/Treaty/en/Reports/Html/185.htm).

공개를 확보해야 한다. 이때 일부 공개된 트래픽 데이터를 통해 제3의 가입국의 서비스 제공자가 데이터의 전송과 관련되었다는 사실이 확인된 경우 피요청국은 협약 제30조에 의거해 요청국에게 서비스 제공자와 해당 통신의 전송 경로를 확인하기에 충분한 양의 트래픽 데이터를 공개해야 한다. 다만 제17조는 서비스 제공자가 일정한 종류의 트래픽 데이터를 의무적으로 수집하여 보관할 것을 내용으로 하는 것은 아니다.[46] 상술한 바와 같이 사이버범죄협약은 데이터 보관의 의무를 규정하기 위한 것이 아니기 때문이다.

2. 영장 없는 초국가적 강제수사

협약 제17조는 데이터의 보존을 명령하는 것에서 그치지 않고, 트래픽 데이터를 수사기관에 일부 공개하도록 하고 있으며, 제30조에 따르면, 다른 가입국에게도 공개해야 한다. 비록 경유 서버에 저장된 트래픽 데이터의 휘발성이 디지털 증거 중에서도 특히 높은 편에 속하며, 따라서 연속된 통신경로를 확인하는 것이 매우 시급하게 이루어져야 한다는 점에는 동의한다 하더라도, 그 방법을 구체화하고 있는 협약 제17조와 제30조의 내용에 대해서는 비판적으로 검토해 볼 필요가 있다. 사이버범죄를 수사하는 수사기관은 이 두 조항에 근거하여 자국은 물론 타국의 서비스 제공자에게도 트래픽 데이터, 즉 통신사실확인자료를 받아낼 수 있게 되며, 이는 결국 아무런 적법절차의 통제를 거치지 않은 채 정보적 자기결정권의 본질을 심각하게 침해하는 것이 될 수도 있기 때문이다.

제16조에 의한 데이터의 보존은 다만 데이터의 변경이나 삭제를 금지하는 것일 뿐, 그 내용을 수사기관이 확인하는 것을 허용하지는 않는다. 그러나 제17조와 제30조에 의한 트래픽 데이터의 일부 공개는 수사기관이 그 구체적인 내용을 신속하게 지득하고 후속수사에 활용하는 것까지를 허용한다. 특히 앞에서 살펴본 바와 같이 우리나라와 EU가입국을 포함한 상당수의 국가가 이미 ISP의 통신사실 확인자료의 자동적 보관의무에 대한 국내법 제도를 마련하여 시행하고 있다는 점을 고려하면,

46) 노명선, 사이버범죄 대처를 위한 EU사이버범죄협약 가입 필요성과 가입에 따른 협약이행 방안, 대검찰청 연구용역보고서, 2011, 104쪽.

사실상 사이버범죄협약 제17조는 수사기관에 의해 사법적 통제 없이 거의 모든 인터넷 통신 이용자의 실명과 접속지의 위치를 확인하기 위한 방법으로 이용될 우려가 있다. 협약 제1조의 d가 정의하고 있는 트래픽 데이터의 개념이 명확하지 않아 통신의 발신 또는 수신자의 정보도 이에 포함되는 것으로 해석될 여지가 있기 때문이다. 따라서 의도적으로 발신자의 정보를 숨기기 위한 특별한 수단을 이용하지 않는 한 모든 인터넷 이용자는 자신의 인터넷 이용 내역 및 접속 위치에 관한 정보를 국가에 의해 모두 파악당할 수밖에 없는 상황에 놓이게 된다.

특히 현대 정보사회에서 인터넷은 스마트폰 단말기를 통해 매일 매일의 삶 속에 깊이 들어와 있으며, 단지 통신사실확인자료 만으로도 개인의 이동경로와 하루 일정을 재구성하는 것이 가능할 정도라고 할 수 있다. ISP는 자신의 이윤을 극대화하기 위하여 별다른 통제 없이 DPI(Deep Paket Inspection) 등의 장비를 이용하여 가입자로부터 수많은 통신 관련 정보들을 수집하고 있는 것이 현실이다. 특히 대부분 후불제로 이용되는 우리나라의 통신시장구조에서 이미 통신서비스제공자는 "이용된 통신 서비스의 형태, 서비스를 위한 기술제공 및 서비스 기간, 서비스 약관이나 협정에 따라 활용할 수 있는 이용자의 신원, 주소, 전화번호 및 기타 다른 접속 번호, 청구와 수납 정보, 통신 장비의 설치 장소에 관한 기타 정보" 등을 완벽하게 확보[47]하고 있다. 이러한 상황에서 협약 제17조에 의해 발신자 또는 수신자 정보를 포함한 트래픽 데이터가 수사기관에 제공된다면, 이는 결국 사생활의 비밀의 중요 부분을 심각하게 침해하는 것이 된다.

따라서 협약 제17조가 일부 공개를 명령하고 있는 트래픽 데이터는 오직 경유된 서버와 서비스 제공자에 관한 정보로 한정해서 해석되어야 한다. 협약 제17조는 제16조에서 규정하고 있는 보존 명령의 대상이 되는 데이터 보관자, 즉 서비스 제공자를 특정하기 위한 것이며, 따라서 통신의 경로를 확인하기 위한 목적으로만 이용될 때 일부 공개가 정당화될 수 있다. 이를 넘는 내용의 트래픽 데이터를 공개하는 것은 불필요한 기본권 침해가 되며 협약 제17조 제2항이 준용하고 있는 제15항 제1호를 위반하는 것이 된다.[48] 협약 제30조 제2항은 "정치범죄 또는 정치범죄와 연관된 범죄라

47) 이영준, 유럽의회의 사이버범죄방지를 위한 국제협약 소고, 형사정책연구 제12권 제2호, 2001, 형사정책연구원, 20쪽.

48) 불필요한 데이터 공개는 유럽평의회의 1950년 "인권과 기본적 자유의 보호에 관한 유럽협약"제8조와

고 판단되는 경우"와 "주권, 안보, 공공질서 또는 다른 중요한 이익을 침해하는 경우"에는 데이터 공개를 보류할 수 있도록 하여 인권과 주권의 보호를 우선하고 있다.

V. 국내 형사절차법상 관련 규정 검토

지금까지 사이버범죄협약의 절차규정 중 사이버범죄 수사의 효율성을 높이기 위해 마련된 저장된 데이터의 신속한 보존 및 트래픽 데이터의 일부 공개절차에 관하여 살펴보았다. 디지털 증거의 휘발성과, 사이버범죄의 초국가성을 고려한다면, 이러한 절차를 국내법에 도입하는 것을 신중하게 고려해야 할 필요가 있을 것으로 생각된다. 다만 그 과정에서 정보적 자기결정권의 불필요한 침해 여지가 없도록 해야 할 것이다. 이하에서는 지금까지의 논의를 바탕으로 국내법상 유사한 규정을 확인하고 법제화를 위해 고려해야 할 사항에 대하여 검토하는 것으로 결론을 대신하고자 한다.

1. 저장된 컴퓨터 데이터의 신속한 보존명령

우리나라의 현행법상, 사이버범죄협약 제16조에서 명시하고 있는 저장된 컴퓨터 데이터의 신속한 보존에 해당하는 규정은 찾을 수 없다. 간접적으로라도 이와 관련이 있는 것으로 볼 수 있는 규정은 압수에 관한 규정인 형사소송법 제106조와 215조를 들 수 있을 것이다. [49] 증거를 보존하고 인멸이나 변조를 막는다는 점에 있어서는 일단 보존명령과 압수의 기능을 유사한 것으로 볼 수 있다. 그러나 압수는 수사기관이 증거를 완전히 확보하고 그 내용을 확인하는 것을 의미한다는 점에서, 협약 제16조가 규정하고 있는 보존명령과는 전혀 다른 제도라고 할 것이다. 따라서 형사소송법 제217조에서 규정하고 있는 "긴급"압수의 경우 신속한 조치라는 점에서는 유사하다 할지라도 다른 제도로 보아야 한다. 게다가 형사소송법 제217조는 체포된 자의 소지 또는 소유물에 대한 압수로 경우가 제한되어 있다.

UN의 1966년 "시민적 정치적 권리에 관한 국제규약"제17조를 위반하는 부당한 프라이버시 침해이다.

49) 박희영, 사이버범죄방지협약의 형사절차법 규정의 평가와 현행 형사절차법 관련 규정의 개정방향, 선진상사법률연구, 제46호, 2009, 183쪽.

오히려 보존명령은 상술한 바와 같이 압수의 실효성을 확보하기 위한 전단계 절차에 해당한다. 그러므로 협약 제16조가 명령뿐만 아니라 이와 유사한 방법을 데이터의 보존을 위한 수단으로 인정하고 있지만, 해석상 적법절차를 준수하기 위해 필수적으로 상당한 시간이 소요될 것이 전제된 영장에 의한 압수는 원칙적으로 이와 유사한 방법에 포함되는 것으로 볼 수 없다. 다만 유럽평의회의 사이버범죄협약 주석보고서는 압수를 이와 유사한 방법에 해당하는 것으로 설명하고 있다.[50] 그러나 2013년 발간된 유럽평의회의 사이버범죄협약 이행평가보고서에 따르면 법원의 압수영장은 24시간 이내에도 발부되지기도 하지만 때로는 몇 주가 걸리기도 하므로, 압수가 이와 유사한 방법에 포함되기 위해서는 절차가 지나치게 제한적이거나 복잡해서는 안 된다고 한다.[51]

디지털 증거의 휘발성을 고려한다면 국내법에 보존명령 제도를 도입할 필요가 있을 것으로 생각된다.[52] 저장된 컴퓨터 데이터에 대한 신속한 보존명령은 높은 실효성이 기대됨에도 불구하고 수사기관에게 그 내용이 전해지지지 않는 다는 점에서 기본권 침해 우려가 비교적 낮은 것으로 평가될 수 있다. 다만 이 경우에도 앞에서 검토한 바와 같이 비례성 원칙에 따라 압수가 제한되는 비밀 등에 대해서는 보존명령 또한 제한될 수 있도록 해야 하며, 보존기간도 꼭 필요한 범위 내로 한정해야 할 것이다.

2. 트래픽 데이터의 일부 공개

협약 제17조에서 규정하고 있는 트래픽 데이터의 일부공개에 관한 규정과 가장 유사한 국내법은 통신비밀보호법 제13조(범죄수사를 위한 통신사실 확인자료제공의 절차)라고 할 수 있을 것으로 생각된다. 통신비밀보호법 제13조에 따르면 수사기관은 전기통신사업자에게 통신사실 확인자료를 요청할 수 있다. 또한 법 제15조의2

50) 유럽평의회, 사이버범죄협약 주석보고서(Explanatory Report to the Convention on Cybercrime; http://conventions.coe.int/Treaty/en/Reports/Html/185.htm).

51) 유럽평의회, 사이버범죄협약위원회 이행평가 보고서 (http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2012_10_Assess_report_v30_public.pdf), 2013, 10쪽.

52) 양근원, 형사절차상 디지털 증거의 수집과 증거능력에 관한 연구, 경희대학교 박사학위논문, 2006, 205쪽 이하 참조.

는 전기통신사업자의 협조의무를 규정하고 있으며, 시행령 제41조는 통신사실 확인자료의 유형에 따라 각각 보관기간을 정하고 있다. 그러나 원칙적으로 통신사실 확인자료를 요청하기 위해서는 관할 법원의 허가를 받아야 하며, 또한 이러한 요청은 통신사실 확인자료를 확보하는 것 그 자체를 목적으로 한다. 따라서 이렇게 확보된 통신사실은 범죄자의 위치를 특정하기 위해 이용되거나, 또는 그 자체로 유죄입증의 증거가 되기도 한다.

그러나 협약 제17조는 사이버범죄의 통신경로를 확인하기 위한 것이며, 이렇게 공개된 트래픽 데이터는 통신경로에 있는 서버의 관리자에게 제16조에 의한 보존명령을 발령하기 위해 이용된다는 점에서 본질적인 차이가 있다. 상술한 바와 같이 트래픽 데이터의 일부 공개는 그 자체로 범죄자의 위치를 특정하거나 유죄를 입증하기 위한 증거로 사용하기 위한 것이 아니라, 압수의 실효성을 달성하기 위한 보존명령의 대상이 되는 ISP를 특정하기 위한 것이다. 즉 압수의 전단계인 보존명령의 전단계로서 이중의 전단계 수사방법이라고 할 수 있을 것이다. 그러므로 통신비밀보호법 시행령 제41조는 컴퓨터 데이터의 신속한 보존에 관한 규정이 아니라, 오히려 데이터의 자동적 보관에 관한 규정으로 보아야 한다.

다만 통신비밀보호법 제13조 제2항 단서는 법원의 허가를 받을 수 없을 정도로 긴급한 사유가 있는 경우에는 통신사실 확인자료를 먼저 요청하고 사후에 법원의 허가를 받도록 하고 있다. 통신사실 확인자료는 통신의 전송경로를 추적하여 또 다른 증거를 확보하기 위해 이용될 수도 있다는 점에서 긴급 통신사실 확인자료 요청절차는 트래픽 데이터 일부공개를 포함하는 수사방법으로 볼 수 있다. 다만 열람하는 자료의 범위가 더 넓고, 프라이버시를 침해할 우려가 크기 때문에 법원의 사후적 통제는 필수적이라 할 것이다. 다만 사이버범죄 수사의 효율성을 높이기 위해 국내법에 법원의 통제 없이도 가능한 범위의 트래픽 데이터 일부 공개에 관한 규정을 마련할 필요는 있을 것으로 생각된다. 다만 이때 공개될 수 있는 트래픽 데이터는 통신비밀보호법상의 통신사실 확인자료보다는 훨씬 제한된 것으로, 단지 통신 경로상 연결된 서버와 그 관리주체를 확인하는데 필요한 것으로 한정되어야 하며, 이 또한 저장된 컴퓨터 데이터의 신속한 보존명령의 대상을 확인하기 위해서만 이용될 수 있도록 해야 한다.

참고문헌

국내문헌

김정환, 테러예비행위와 보호감호의 규정을 통해 살펴본 독일형법의 유럽화와 기능화, 비교형사법연구, 제14권 제1호, 2012

김한균.김성은.이승현, 사이버범죄방지를 위한 국제공조방안 연구, 대검찰청 연구용역보고서, 2009

노명선, 사이버범죄 대처를 위한 EU사이버범죄협약 가입 필요성과 가입에 따른 협약이행 방안, 대검찰청 연구용역보고서, 2011

박혜진, 형법적 관점에서 바라 본 피의사실공표죄의 제문제, 비교형사법연구 제13권 제2호, 2011

박희영, 사이버범죄방지협약의 형사절차법 규정의 평가와 현행 형사절차법 관련 규정의 개정방향, 선진상사법률연구, 제46호, 2009

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

이영준, 유럽의회의 사이버범죄방지를 위한 국제협약 소고, 형사정책연구 제12권 제2호, 2001

이영준.금봉수.정완, 사이버범죄방지조약에 관한 연구, 형사정책연구, 형사정책연구원, 2001

이원상, 해킹미수 처벌 논의에 대한 고찰, 비교형사법연구, 제13권 제2호, 2011

전현욱, 개인정보 보호에 관한 형법정책, 고려대학교 박사학위논문, 2010

전현욱.윤지영, 디지털 증거 확보를 위한 수사상 온라인 수색제도 도입 방안에 대한 연구, 대검찰청 연구용역보고서, 2012

국외문헌 및 기타

All Party Parliamentary Internet Group, “Communications Data: Report of an Inquiry by the All Party Internet Group”, 2003.

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.

Council of Europe, Decision No. CM/Del/Dec(97)583, 1997.

Council of Europe, Decision No. CM/Del/Dec(99)679, 1999.

Council of Europe, Explanatory Report to the Convention on Cybercrime, 2001.

Cybercrime Convention Committee, Assessment report Implementation of the preservation provisions of the Budapest Convention on Cybercrime, 2012.

European Commission, Evaluation report on the Data Retention Directive, 2011.

European Committee on Crime Problems “decision CDPC/103/211196”, 1996.

European Parliament and of the Council, “Directive 2006/24/EC”, 2006.

UNODC, Comprehensive Study on Cybercrime, 2013.

UN OHCHR, International Covenant on Civil and Political Rights, 1996.

* 각주의 URL은 모두 2014, 5. 6. 최종 확인하였음.

Convention on Cybercrime and Due Process of Law : on Preservation and Partial Disclosure of Stored Data

Chun, Hyun Wook* · Lee, Ja Young**

The Convention on Cybercrime(CoC) was adopted by the Committee of Ministers of the Council of Europe at its 109th Session (8 November 2001). It was signed in Budapest in 2001 and entered into force in 2004. It is noteworthy that the Convention is the first and currently the only international instrument to respond to cybercrime committed via internet and network. The Convention, however, is not sufficient to deal with new types of cybercrime as the level of Information Technology development at that time was not comparable to the present day and cybercrime becomes more sophisticated in types and forms. Those who are against the Convention argue that provisions of the Convention, only intended to find substantial truth may infringe fundamental rights as well as personal information control right of people. It is widely regarded that the Article 16 (Expedited preservation of stored computer data) and 19 (search and seizure of stored computer data) of the Convention provide procedure power against cybercrime. Given that expedited preservation of stored computer data provided in the Article 16 is a measure to carry out search and seizure effectively, it is required to limit scope of administering preservation order in order to protect essential privacy of a person or state' confidentiality. In addition, duration of preservation should be confined as the purpose of preservation order is to get enough time to carry out legal procedures such as issuing warrant. States should interpret the article narrowly before they introduce the provision into the law. The Article 17 (Expedited preservation and partial disclosure of traffic data) and 30

* First Author, Ph.D in Criminal Law, Korean Institute of Criminology.
** Second Author, Doctoral Candidate, College of Law, Ajou University.

(Expedited disclosure of preserved traffic data) set out necessary measures to secure expedient preservation of traffic data and require traffic data to be disclosed to the investigation agency so that they could identify route of transmission. However, these two provisions allow the investigation agency to request traffic data to internet service both at home and abroad which may result in infringe the fundamental rights as well as personal information control right of people. Korea doesn't have any legal institutions amount to the Article 16 and 17. Characteristics of cybercrime and digital evidence, it should consider to introduce similar provisions to improve efficiency of investigation on cybercrime. It should be in mind that it must respect due process principle and minimize limitation of personal information control right of people.

❖ Key words: Convention on Cybercrime, Expedited Preservation of Stored Computer Data, Partial disclosure of Traffic Data, Digital Evidence, Search and Seizure, Due Process of Law

투고일 : 5월 30일 / 심사(수정)일 : 6월 18일 / 게재확정일 : 6월 18일