사이버범죄협약에 대한 현황 파악과 가입 실익 분석

BoB 10기 디지털포렌식 트랙 이호준

1. 사이버범죄협약이란

1.1 개요

사이버범죄협약은 일명 부다페스트 조약으로 알려져 있으며 전 세계의 국가가 초국가적인 범죄인 사이버 범죄에 공동으로 대응하기 위한 국제적인 협약이다. 2001년 11월 최초 서명식을 가졌으며 2004년 7월 1일 발효에 들어갔다. 현재 미국, 영국, 독일, 프랑스, 일본 등 세계 약 60여 개국이 가입한 상태이다.

- 협약의 목적

사이버범죄와 관련하여 각국의 형사 실체법 구성요건 및 관련된 조항들을 통일하고, 컴퓨터 시스템을 통해 저지른 기타 범죄 및 전자적 형태의 증거 수사와 기소에 필요한 형사절차법상의 권한을 규정하며, 빠르고 효과적인 국제협력 및 국제 형사사법공조 체제를 수립하는 것을 목적으로 한다.

- 규정 대상

불법감청・불법접근・시스템방해・장치의남용・데이터손괴・인터넷사기・위조・저작권침해・아동 포르노그라피 등을 규정하고 있으며, 이러한 범죄에 대하여 미수 및 방조, 교사행위와 법인의 형사상 및 행정상의 책임까지 묻도록 규정하고 있다.

- 내용

제1장 제1조에서는 협약에 들어가는 용어에 대한 정의 및 설명을 하고 있으며, 제2장 제1부 실체법에서는 가용성・기밀성・무결성 등을 해치는 컴퓨터 관련 범죄 중에서 입법해야 할 9개의 범죄행위의 실체적인 규정과 공범의 책임과 처벌에 대해 규정하고 있다. 제2장 제2부에서 절차법상 신속한 증거의 보존・압수수색・데이터 감청 등에 대하여 규정하고 있고, 제2장 제3부에서는 범죄인 송환과 인도・수사에 대한 상호협력・자발적인 정보제공・24시간 연락망 가동 등의 국제공조에 대하여 규정하고 있다.

1.2 국내 반응 및 현황

우리나라는 현재 통신비밀보호법 등 국내법과의 상충 문제로 해당 협약에 가입하고 있지 않으며 가입을 위한 이행입법에도 소극적인 태도를 보이는 상황이다. 현행법과 상충되는 조약의 여러 부분이 있지만 대표적인 것은 다음과 같다.

① 사이버범죄협약 제6조 '장치의 오남용'

해킹 등의 부정 프로그램 바이러스와 컴퓨터시스템의 전부 또는 일부의 접속을 가능하게 하는 컴퓨터비밀번호・접속코드 등을 제작・판매・수입・배포하는 범행예비 행위에 대한 처벌 규정이 있다. 그러나 국내법은 불법 감청행위 자체에 대해서만 처벌하고 있어 쌍가벌성의 원칙을 근거로 감청 데이터의 판매・유포・사용에 대한 처벌규정을 만들 필요가 있다. 하지만 범행예비행위에 대한 판단을 어떻게 할 것인가에 대한 문제와 준비란 중간에 중단이 가능하기에 처벌 조항을 만드는 것은 지나친 간섭 내지는 감시가 될 수 있다는 의견이 있다.

② 사이버범죄협약 제16조 '저장된 컴퓨터데이터의 신속한 보전'

사이버범죄협약에서 언급된 '저장된 컴퓨터데이터'는 국내 통신비밀보호법 상 통신사실 확인자료로는 대체가 불가능하기에 이에 대한 법률 개정이 필요하다. 핵심 사생활 및 국가적 비밀 관련 데이터에 대해선 보존 명령이 제한될 필요가 있는데 이에 대해 판단 기준이 애매해 악용될 여지가 있어 우려가 재기된다.

③ 사이버범죄협약 제17조 '트래픽데이터의 신속한 보전 및 제출'

국내 통신비밀보호법 제2조에서는 부다페스트협약에 명시되어 있는 통신경로・통신크기・서비스유형 등이 규정되어 있지 않다. 따라서, 현재는 우리나라의 수사기관이 사이버범죄협약 상의 트래픽데이터를 제공하면 현행법을 위반할 소지가 있다.

2. 외국 사례

- 독일

독일은 협약이행절차 실행 준비에 일찍이 착수하고 국내법적 수용을 이행해 2009년 2월 사이버범죄협약의 비준을 완료했다. 신속한 보전을 다음과 같이 명시했는데, "(1) 심리에서 증거방법으로서 가치가 있을 수 있는 대상은 보관하거나 다른 방법으로 보전해야 한다.", "(2) 제1항의 대상은 개인이 보관하면서 자의로 제출하지 않으면 압수할 수 있다."고 규정하여 사이버방지협약에서 규정하고 있는 데이터의 보전 내지 저장 규정을 '증거의 보전'이라고 규정하여 포괄적으로 규정하고 있으며, 압수규정을 통하여 신속한 보전 제도를 이행한다.

독일 형사소송법 제95조에서는 제출의무를 규정하고 있는데, "(1) 제94조에 규정된 종류의 대상을 보관하는 자는 요구가 있으면 이를 제시하고 제출할 의무가 있다.", "(2) 거부하는 경우에는 그에게 제70조에 규정된 질서벌과 강제수단을 부과할 수 있다."고 규정해 사이버방지협약에서의 제출의무를 규정하고 있다.

뿐만 아니라 조사권한규정을 규정해 무분별한 조사를 제한하는데, 독일 형사소송법상의 제

100조g의 통신접속정보의 수집에서 통신법 제96조 제1항에 의하여 사안의 중대성에 따라서 적절한 비례성이 있는 한도에서 통신접속정보를 수집할 수 있으며, 제113조b에 의하여 저장된 통신접속정보 역시 사안의 중대성에 따라서 적절한 비례성이 있는 한도에서 통신접속정보를 수집할 수 있도록 규정하고 있다.

- 일본

2011년의 미츠비씨 중공업 사이버공격 사건과 212년 정부 네트워크에 대한 사이버 공격이 계기가 되어 내각 산하에 '국가정보보안위원회(NISC: National Information Council)'를 만들고 형사소송법 등을 개정하여 '부다페스트협약'에 가입했다.

3. 협약 가입의 장단점

3.1 장점

- 원활한 서비스공급업체 자료 요청이 가능해짐

사이버범죄방지협약은 국가간 사법공조와 더불어, 구글, 페이스북, 트위터 등 인터넷 사업자들과도 협력관계를 맺고 있다. 수사기관의 입장에서는 기존 데이터 소재지의 국가들에게 국제공조를 요청하는 것 보다는 구글이나 페이스북 등의 정보통신서비스제공자들에게 데이터 제공을 요청하는 것이 오히려 수사의 신속성이나 증거수집에 중요할 수 있다. 이 역시 해외 또는 역외에 위치하고 있는 서버이고, 서버에 저장되어 있는 데이터를 요청하는 경우가 증가하고 있기 때문에 역외 관할권의 적용 내지 국제수사공조와 밀접한 관련이 있게 된다.

- 절차적으로 효율적인 공조 가능

일반적인 국제형사사법공조(MLAT)를 통해 공조를 진행한다면 평균 10월에서 1년 이상 기간이 소요될 뿐만 아니라 국제사법공조 요청에 대한 응답의 경우는 6월에서 24개월이 걸리거나 아예 무시당하는 현실이다.

- 원활한 사이버범죄의 증거 수집이 가능해짐

테러와 같은 초국가적 범죄의 경우 SNS 등 사이버 공간을 이용하여 프라파간다, 홍보, 교육, 범행 모의가 이루어지는데 이 과정에서 전송 중인 트래픽 데이터나 저장된 데이터는 매우 중요한 정보이고 증거임에도 불구하고 국제형사사법공조를 통하여 증거를 획득하기란 매우 어렵다. 쌍가벌성의 한계로 인하여 상호주의의 충돌이 발생하게 된다면 신속한 데이터의 공유와 보전, 제공 등이 이루어지지 않게 될 수 있다. 사이버범죄방지협약은 이러한 문제를 해결해 신속한 데이터 보전과 제공을 가능하게 해줄 것이다.

3.2 단점

- 실효성에 대한 의문

우리나라의 국가안보에 영향을 미치는 사이버공격은 주로 북한으로부터 시작되기에 다른 회원국들로부터 지원받을 만한 유용한 정보들이 많이 없어서 협약 가입의 필요성에 의문을 가지는 의견이 있다. 뿐만 아니라, 이미 2011년 말에 유럽평의회 형사사법공조협약에도 가입되어 있고 다른 비공식라인을 통해서 필요한 수준의 국제공조가 되기에 실효성이 높지 못하다는 의견이 제기된다.

- 우리나라의 정보자산에 대한 외부의 접근 증대

제17조 '트래픽 데이터의 신속한 보전 및 제출'과 제32조에 '국경을 초월한 데이터정보의 접근' 같은 조항이 국가안보에 직결되는 문제를 발생시킬 수 있다는 정보기관의 우려가 있다.

- 개인정보 이슈

사이버범죄협약에는 "수사기관이 추적하는데 필요한 충분한 데이터를 제공하여야 한다", "회원국 통신사에 직접 트래픽 데이터를 요구하여 얻을 수 있다"는 내용이 존재하는데 이는 회원국들이 정부를 거치지 않고 우리나라 국민들의 개인통신정보까지도 접근이 가능하다는 문제의 소지가 있다.

4. 결론

현재 다양한 국가가 사이버범죄협약을 통해 상호 공조를 통해 사이버범죄의 수사뿐만 아니라 예방에 대해서도 방향을 같이하여 효과적인 성과를 보이고 있다. 2014년에 발표된 사이버범죄협약을 통한 사법공조 평가 보고서(T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime)에 의하면 미국과 일본 등은 사이버범죄방지협약을 통한 사법공조가 매우 빈번하게 활용되고 있는 것을 알 수 있다. 또한 루마니아, 터키, 호주 등의 국가들 역시 연간 100건 이상의 사이버범죄방지협약을 통한 사법공조 요청을 하거나 다른 국가에 제공한 것으로 나타났다. 우리나라도 현행법을 개정 및 보완하여 사이버범죄방지협약을 비준하는 것이 필요할 것이다. 현재 사이버범죄는 초국가적인 양상을 띈다. SNS을 통한 테러 모의 뿐만 아니라 콜로니얼 파이프라인 사건과 같이 국가적으로 중요한 민간 기업에 대해서도 공격을 감행하는 양상을 보인다. 이에 대해 사이버범죄협약은 애플, 구글 등의 초국가적 인터넷서비스공급자와도 협력관계를 맺고 있다. 위의 보고서에 따르면 미국, 독일, 일본 등 주요국은 약 60% 이상 관련 사이버정보를 위의 인터넷서비스공급자로부터 제공받는다고 한다. 비록, 회원국이 무분별하게 개인의 통신정보에 접근할 수 있지 않겠냐는 우려가 있으나 조사권한규정을 엄밀히 정비하여 사안의 중대성에 따라서 적절한 비례성이 있는 한도에서 통신접속정보를 수집할 수 있도록 한다면 이러한 우려는 해소할 수 있을 것이다. 전자통신기술이 발전하고 있는 오늘날 사이버범죄의 규모와 그 심각도는 날로 커져간다. 사회적 합의를 통해 적절한 한도를 정하여 프라이버시를 보장하는 선을 정해 현행법을 정비한 후 사이버범죄협약에 가입하는 것이 필요하다.

참고자료

사이버범죄 대응을 위한 부다페스트협약 가입과 국제공조 연구 – 정태진, 이광민 (경찰학연구소/ 경찰학논총 제14권 제2호(2019))

사이버범죄협약(일명 '부다페스트' 조약) 가입을 위한 선결과제 – 윤해성, 라광현 (가천법학 제12권 제3호)