형사정책연구 Korean Criminological Review
제34권 제3호(통권 제135호, 2023 · 가을)

부다페스트 협약 제2 추가의정서 가입을 위한 국내 입법 정비방안 연구
– CLOUD Act와 비교하여 –

이지우* · 이경렬**

국 | 문 | 요 | 약

디지털증거 역외 압수·수색은 수사기관이 해외서버에 있는 증거에 대한 영장을 발부받아 해당 IP에 접속하여 관련 증거를 수집하는 압수·수색 방법을 의미한다, 우리나라는 2022년 10월 11일 역외 압수·압수수색을 위한 부다페스트 협약 가입의향서를 제출하였다. 그러나 이미 2021년 11월 제2 추가의정서가 제정되었으므로, 제2 추가의정서 가입 여부 또한 별도로 논의해야 한다.

제2 추가의정서는 역외 압수·수색의 효율성 확보 및 확장을 위해 타국 정부를 거치지 아니하고 ISP에 직접 정보 제공요청을 하거나 기존 형사사법공조절차 중 일부를 생략할 수 있도록 하는 것을 주된 내용으로 하였다. 비록 개인정보 보호 강화를 위한 일부 조항이 있었으나, 결과적으로 역외 압수수색의 확장만을 강조하였다.

우리나라가 제2 추가의정서에 가입하게 되면 역외 압수·수색 관련 국내 법률제도 재검토가 불가피하다. 특히 역외 압수·수색의 확장과 관련하여 역외 압수·수색의 명문화, 트래픽 데이터 및 통신사실 확인 자료 제공, 법적 책임 규정 등에 대한 고민이 필요하다. 이 중 트래픽 데이터 및 통신사실 확인 자료 제공과 법적 책임 규정은 부다페스트 협약과 제2 추가의정서간 배치되는 부분이 있으므로 양자를 조화롭게 달성할 수 있는 입법·정책적 방안을 모색해야 한다.

사이버범죄에 적절하게 대처해야 하기 위한 국가 간 상호 협력과 역량 강화가 중요하고 급변하는 ICT 환경에 대응해야 한다는 점을 고려하면, 제2 추가의정서에 언젠가는 가입해야 한다. 그러나 제2 추가의정서의 문제점 및 부다페스트 협약과의 조화에 대한 고민이 선행되어야 한다. 그리고 미국의 CLOUD Act는 제2 추가의정서와 마찬가지로 수사기관이 직접 ISP에 정보공개 요청을 할 수 있게 했다는 점에서 우리의 연구에 시사하는 바가 있다. 따라서 미국의 사례가 우리나라에 시사하는 바가 무엇인지 알아보는 것은 역외 압수·수색 확장 관련 문제들을 해결하는데 중요한 역할을 할 것이다.

DOI : https://doi.org/10.36889/KCR.2023.9.30.3.225.

❖ 주제어 : 역외 압수·수색, 부다페스트 협약, 제2 추가의정서, 개인정보 보호, CLOUD Act

* 주저자: 성균관대학교 일반대학원 법학과 박사과정
** 교신저자: 성균관대학교 법학전문대학원 교수, 법학박사

Ⅰ. 들어가는 말

디지털증거 역외 압수·수색(Trans-border Access)은 수사기관이 해외서버에 있는 증거에 대한 영장을 발부받아 해당 IP에 접속하여 관련 증거를 수집하는 압수·수색 방법을 의미한다.[1] 수사 과정에서 해외서버에 대한 계정과 비밀번호를 알게 되었을 때, 수사기관 사무실 등에서 해외서버에 접속하여 관련 증거를 확보하겠다는 내용을 기재한 영장을 발부받아 집행하는 방법이다.[2]

역외 압수·수색은 수사상 그 필요성이 인정됨에도 불구하고 이를 명시하는 규정이 없어 그동안 형사사법관할 등 합법성 논란이 있었으며, 이에 대한 해결책으로써 우리나라는 2022년 10월 11일 부다페스트 협약 가입의향서를 제출하였다. 하지만 부다페스트 협약의 내용을 보충하고 지난 20년간의 정보통신환경변화를 반영할 필요가 생겼다. 즉, 2021년 11월 제2 추가의정서[3](Second Additional Protocol)가 제정되었다는 점이 고려되어야 한다.[4] 부다페스트 협약에 가입되었다고 하더라도 그 효력이 자동으로 제2 추가의정서의 채택과 가입으로 바로 미치는 것은 아니다. 제2 추가의정서의 채택과 가입은 별도로 논의되어야 한다.

부다페스트 협약은 사이버범죄 수사를 위한 국가 간 디지털증거 수집 협조를 규정한 유일한 국제적 조약이다.[5] 비록 2001년 부다페스트 협약에는 디지털증거의 보존, 생산

1) 이지우·이경렬, "디지털 역외 압수·수색에 관한 비교연구", 비교형사법연구 제24권 제4호, 한국비교형사법학회, 2023, 379-380면.

2) 정대웅·김기범·권헌영·이상진, "디지털증거의 역외 압수·수색에 관한 쟁점과 입법론", 법조 제65권 제9호, 법조협회, 2016, 136면.

3) 제2 추가의정서 원문은 웹사이트 https://search.coe.int/cm/pages/result_details.aspx?objectid=09000001680a48e4d(최종 검색일: 2023.7.31.) 참조.

4) 부다페스트 협약은 실행 단계에서 많은 문제점을 드러냈고, 이에 따라 현재까지 2개의 의정서가 추가로 제정되었다. 특히 인터넷을 통한 인종차별 및 외국인 혐오범죄를 명확하게 언급하지 않았다는 비판을 받았으며 [Vagia Polyzoidu, "Combating the Cybercrime: Thoughts Based on the Second Additional Protocol (Draft) to the Budapest Convention on Cybercrime", EU Internet Law in the Digital Single Market (2021), 360면], 이에 따라 2003년 제1 추가의정서가 채택되었다. 제1 추가의정서는 "Concerning the Criminalization of Acts of a Racist and Xenophobic Nature committed through Computer Systems"라는 명칭에서 알 수 있듯이, 인터넷에서 발생하는 인종차별과 혐오범죄에 대응하기 위한 목적으로 제정되었다.(https://ccdcoe.org/uploads/2018/11/CoE-030128-Additional/Protocol-1.pdf. (최종검색일: 2023.07.06.)

5) Markko Künnapu, "Challenges Related to Fight Against Cybercrime. A Need to Strengthen

및 실시간 데이터 접속에 관한 절차적 조치를 규정하고 있으나, 빠르게 발전하는 기술에 효과적으로 대응할 수 없다는 비판이 제기되었다.[6] 정보통신기술의 발달과 그에 따라 변모하는 사이버범죄에 효과적으로 대응하기에는 2001년에 채택된 협약의 규정만으로는 부족하다는 말이다. 그 결과 지난 2017년에 부다페스트 협약 제2 추가의정서에 대한 논의가 촉발되었다.[7]

이하에서는 부다페스트 협약 제2 추가의정서의 주요 내용을 살펴보고 관련 쟁점들을 검토함으로써 추가의정서의 채택 여부를 연구하고자 한다. 제2 추가의정서는 역외 압수·수색의 효율성을 확보하기 위해 타국의 국가기관을 거치지 않고 ISP에 직접 정보공개 요청을 할 수 있게 하는 것을 주된 내용을 하고 있다. 제2 추가의정서에 가입하게 되면 역외 압수·수색 확장에 따른 명문 규정 마련 및 책임소재의 문제를 명확하게 정해야 한다. 미국의 CLOUD Act는 제2 추가의정서와 마찬가지로 수사기관이 직접 ISP에 정보공개 요청을 할 수 있게 했다는 점에서 우리의 연구에 시사하는 바가 있다. 따라서 본 연구는 제2 추가의정서의 가입을 위해 별도로 논의될 국내법적 쟁점 사항을 검토한 뒤, 국내법의 개정 방향과 관련하여 CLOUD Act의 시사점도 함께 논의하도록 한다.

Ⅱ. 제2 추가의정서의 주요 내용과 쟁점

1. 제2 추가의정서의 채택

부다페스트 협약이 체결·발효된 이래로 정보통신의 사용이 폭증하였을 뿐만 아니라 정보통신기술도 비약적으로 발전하였고, 또한 이를 이용한 사이버범죄의 양상도 변모되어왔다. 수사기관이 외국 소재의 서버에 있는 디지털증거를 수사하기 위해서는 해당 국가의 협조를 구해야 한다. 그러나 디지털증거는 국경의 제약을 받지 않으며, 관련 과학기

International Cooperation", International Journal of Criminal Justice 제3권 제2호, 한국형사·법무정책연구원, 2021, 39면.

6) Markko Künnapu, 앞의 논문, 40면.

7) 박재성, "사이버범죄 국제조약의 동향 - 부다페스트 협약 제2 추가의정서 및 유엔 사이버범죄 조약을 중심으로 -", 저스티스 제185호, 2021, 251면 참조.

술이 발전함에 따라 더욱 빠르고 쉽게 복사, 이동 또는 삭제되는 특성을 지니고 있다. 또한, 형사사건 중 절반 이상이 해외에서의 디지털증거를 확보하기 위하여 형사사법공조가 필요하다고 할 만큼 사이버범죄가 폭증하였고, 그와 함께 부다페스트 협약보다 더욱 효율적으로, 더 신속하게 디지털증거를 확보하는 방안이 필요하다는 목소리가 커지게 되었다.[8] 이에 따라 2017년 타국 소재 서버의 디지털증거를 더욱 빠르게 수집할 수 있도록 하는 내용의 제2 추가의정서 발의가 시작되었다.

부다페스트 협약 가입국의 협약 이행 현황을 감독하고 개선 방향을 연구하기 위하여 설립된 유럽평의회 산하 사이버범죄 협약 위원회(Cybercrime Convention Committee)는 2017년 6월 8일 위원회 총회에서 기존의 부다페스트 협약의 미비점들을 보완하기 위한 제2 추가의정서 초안 작성을 결의하였다. 2021년 5월 사이버범죄 협약 위원회는 추가의정서 최종안을 확정하고, 이후 유럽평의회의 의사결정 기구인 각료 위원회(Committee of Ministers)에 이를 회부되어 2021년 11월 추가의정서가 채택·승인되었다. 2022년 5월 프랑스 스트라스부르에서 열린 유럽평의회에서 제2 추가의정서는 공식적으로 서명되었으며, 2023년 6월 기준 총 39개국이 가입하였다.[9]

제2 추가의정서는 초기부터 “증진된 공조 및 디지털증거 제공을 위한 사이버범죄 협약 제2 추가의정서(Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence)”로 안을 제시하였으며 국가 간 수사 공조 촉진에 목표를 두고 있음을 분명히 알 수 있다.[10] 타국에 위치한 인터넷서비스 제공자를 상대로 가입자 정보(Subscriber Information)와 트래픽 데이터(Traffic Data)를 더욱 효율적으로 확보할 수 있는 제도, 즉 타국 정부를 거치지 아니하고 직접 공조 요청하거나 기존 형사사법공조절차 중 일부를 생략할 수 있도록 하는 제도를 만들고자 한 것이다.[11] 나아가 제2 추가의정서는 수사 공조의 효율성을 추구하는 동시에 그 남용을 방지하고 개인정보 보호를 위한 추가적인 조항들을 규정하고자 하였다. 따라서 제2 추가의정서는 역외 압수·수색의 확장 및 절차 간소화와 더불어 사생활

8) 박재성, 앞의 논문, 252면.
9) 유럽평의회 웹사이트 https://www.coe.int/en/web/cybercrime/second-additional-protocol(최종 검색일: 2023.8.26.) 참조.
10) 박재성, 앞의 논문, 254면 참조.
11) 박재성, 앞의 논문, 253면.

보호 강화도 지향했다고 평가할 수 있다.[12)]

2. 주요 내용

가. 역외 압수·수색 절차 간소화

제2 추가의정서의 가장 핵심적인 조항은 역외 압수·압수수색 절차 간소화를 규정한 제6조 및 제7조다. 제2 추가의정서는 타국 정부를 거치지 아니하고 권한 있는 기관이 직접 공조 요청을 하거나 기존 형사사법공조절차 중 일부를 생략할 수 있도록 하는 제도를 만들고자 의도하였다. 이에 관한 내용은 제6조 및 제7조에 규정되어 있다.

제6조는 "도메인 이름 등록 정보 요청(Request for Domain Name Registration Information)"이라는 제목 아래[13)] 권한 있는 기관(Competent Authority)[14)]이, 또한 제7조는 "가입자 정보 제공(Disclosure of Subscriber Information)"이라는 제목 아래, 권한 있는 기관이 타국에 위치한 ISP에 직접 사건 수사에 필요한 가입자 정보를 제공할 것을 요청할 수 있다고 제1항에 규정하고 있다.[15)] 제6조와 달리 '수사에 필요한' 범위

---

12) Melissa L. Ken, "The Real Cost of 5G Technology: National Security Implications of 5G Implementation and Impact on the U.S.-China Relationship", 9 Nat'l Sec. L. J. 119 (2022), 15면: AP II consists of the following elements: more efficient mutual legal assistance; increased direct cooperation; extended trans-border searches; and increased rule of law and data protection safeguards.

13) 도메인 네임(Domain Name)이란 인터넷 사이트의 주소를 기억하기 어려운 연속된 숫자 형태의 IP 주소 대신 사용하기 쉬운 영문으로 표현한 것이다. 흔히 사용하는 'www.naver.com'과 같은 형태의주소로 등록된다. (박재성, 앞의 논문, 255면)

14) 권한 있는 기관이란 특정 범죄 수사 또는 절차와 관련된 증거의 수집 또는 생산을 목적으로 제2 추가의정서에 따른 조치의 실행을 명령, 승인 또는 수행할 권한이 있는 사법, 행정 또는 기타 법 집행 기관을 의미한다. 제2 추가의정서 제3조 제2항 제b호: "Competent Authority" means a judicial, administrative or other law-enforcement authority that is powered by domestic law to order, authorize or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

15) 제2 추가의정서 제7조 제1항: Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or

내에서만 가입자 정보를 요청할 수 있는데, 이는 도메인 이름과 달리 가입자 정보가 좀 더 개인정보의 성격을 가지기 때문에 제공 범위를 제한하였다고 볼 수 있다.

제6조 제2항[16] 및 제7조 제1항은 모두 "필요한 입법 및 기타 조치를 해야 한다(Shall adopt such legislative and other measures as maybe necessary)"라고 규정하고 있다. 따라서 제2 추가의정서 가입국은 자국 소재 서비스 제공자가 타국 정부로부터 직접 요청을 받고 정보공개를 할 수 있도록 관련 규정 및 제도를 마련할 의무가 있다. 예를 들어 제2 추가의정서 가입국인 A는 또 다른 가입국 B 소재 ISP에 직접 정보공개 요청을 할 수 있을 뿐만 아니라 B가 자국 ISP에도 직접 공개요청을 할 수 있도록 국내법적 제도를 마련해야 하는 것이다. 역외 압수·압수수색 절차 간소화를 규정하는 동시에 절차의 실효성 확보를 위해 이러한 입법적 조치의무를 부여하였다고 해석된다.

나. 개인정보 보호 강화

제14조는 개인정보보호(Protection of Personal Data)라는 제목 아래 개인정보보호 조치를 강화하기 위한 15개 조항을 규정하고 있다. 예를 들어 제2항은 제공된 정보가 제공된 목적 내에서만 사용되어야 한다고 규정하고 있으며, 제4항은 인종, 정치적 성향, 종교, 유전적 정보, 건강 상태 등 민감정보(Sensitive Data) 보호장치 없이 수집되어 불이익을 받는 일이 없어야 한다고 규정하고 있다. 또한, 제11항은 개인정보가 수집되면 당사자에게 통보가 이뤄져야 한다고 규정하고 있으며, 더 나아가 제12항 및 제14항은 이러한 조치를 취하지 않거나 개인정보를 부당하게 취득한 국가에 대해 정정 조치를 요구하거나 정보 제공을 중단할 수 있도록 규정하고 있다.

다. 일부 조항의 선택적 유보

부다페스트 협약 제42조에는 특정 조항들에 대하여 유보할 수 있음을 명시하고 있다. 제2 추가의정서 역시 부다페스트 협약과 마찬가지로 일부 조항의 선택적 유보 조항을

proceedings.

16) 제2 추가의정서 제6조 제2항: Each party shall adopt such legislative and other measures as maybe necessary to permit an entity in its territory do disclose such information in response to a request under paragraph 1, subject to reasonable conditions provided by domestic law.

두고 있다. 제2 추가의정서에 따르면 가입국은 비준 시 일부 조항의 적용을 유보할 수 있다. 예를 들어 제7조 제9항 제a호는 가입국이 필요시 제7조 적용을 배제할 수 있다고 규정하고 있으며, 제8조 제13항은 트래픽 데이터에 한하여 제8조의 적용을 유보할 수 있다고 규정하고 있다. 이는 제7조의 남용에 의한 주권 및 개인정보 침해의 우려를 불식시키고 추가의정서에 최대한 많은 국가가 가입하도록 유도하기 위한 규정이라고 볼 수 있다.[17)]

부다페스트 협약이 일부 규정에 대한 유보 조항을 규정하고 있음에도 불구하고 추가의정서가 협약과 반대로 모든 조항의 적용을 강제할 수는 없기 때문이다. 또한, 국가마다 법체계가 다르므로 최대한 자신들의 체계와 상황에 맞게 의정서를 조정할 수 있도록 했다고도 할 수 있다.

3. 관련 쟁점

가. 정보공개 주체의 전환 및 권한의 정당성 의문

제2 추가의정서에 따라 디지털증거가 타 국가 소재 서버에 있으면 수사기관은 해당 국가가 아닌 해당 인터넷서비스 제공자(ISP)에게 정보공개를 직접 요청할 수 있다. 그러나 이에 대해 일부에선 국가가 자국민의 정보공개에 대한 권한을 외국 기관과 ISP에 과도하게 이양했다고 비판한다.[18)] 외국 수사기관이 자국법에 따라 수사에 필요한 증거를 요청할 수 있으나, 그렇다고 하여 ISP가 무슨 권한을 근거로 정부의 허가 없이 개인정보가 포함된 증거를 임의로 외국 기관에 제출할 수 있는지가 문제 되는 것이다.

물론 이에 대해선 ① 외국 수사기관이 정보공개를 요청한다고 하여 ISP가 모든 요청에 의무적으로 공개해야 하는 건 아니라는 점,[19)] ② Microsoft 판결[20)]에서 알 수 있듯

17) 박재성, 앞의 논문, 258-259면.

18) Courtney Christensen, “Who Decides? Speech and Privacy Risks in the Draft Second Additional Protocol to the Budapest Convention”, 52 Geo. J. Int'l L. 1031 (2021): 1036면: The proposed protocol shifts too much power to foreign law enforcement agencies and the private sector to make determinations about speech and privacy rights.

19) 유럽 사이버범죄 협약 위원회에 따르면 정보공개 요청에 응하는 비율은 약 76%다. Cybercrime Convention Committee(T-CY), supra note 33, at 24. (박재성, 앞의 논문, 265면 재인용)

20) U.S. v. Microsoft, 138 S. Ct. 1186 (2018)

이 ISP는 최대한 정보를 공개하지 않는 방향을 지향할 것이라는 점[21]을 근거로 ISP 권한 이양이 문제 되지 않을 것이라 주장한다. 그러나 이에 대해선 다음과 같은 재반박이 가능하다.

우선 ①과 관련하여 과연 ISP의 선택적 정보공개가 실질적으로 가능할 수 있을지 의문을 가질 수 있다. 제2 추가의정서 제7조 제5항에 따르면 만약 ISP가 외국 수사기관의 정보공개 요청에 응하지 않으면 수사기관에 그 이유를 설명해야 한다. 즉, 정당한 사유로 정보공개 요청을 거부하더라고 그 '정당한 사유'가 무엇인지에 대한 해명을 추가로 해야 하는 것이다. ISP로선 요청을 거부한 사안마다 사유서를 작성해야 하므로 많은 법적 및 인적 자원이 요구될 수밖에 없다. 그러나 특히 규모가 작은 ISP의 경우 정보공개 요청에 맞서거나 대응하지 않는데 필요한 법적 또는 인적 자원이 부족하므로 사실상 모든 요청에 응하게 될 가능성이 더욱 크다.[22] 분쟁을 피하고, 법적 불확실성을 줄이고, 정부와 안정적인 관계를 유지하려는 ISP로선 정보공개 요청을 모두 준수할 유인이 더 큰 것이다.[23]

또한, 설령 ISP가 선택적으로 정보공개 요청에 응할 수 있다고 하더라도 그 자체가 문제될 수 있다. 국가기관이 아닌 민간 ISP가 개별 사안마다 구체적으로(case by case) 판단하여 정보공개 여부를 결정하는 것이 과연 정당한지 의문을 가질 수밖에 없다. 또한, ISP가 case by case 판단을 하게 되면 과연 무엇을 근거로 판단하는지도 불투명하다. 제2 추가의정서 역시 각 ISP에 별도의 판단 기준을 마련하거나 공개할 것을 요구하지 않기 때문이다. 각 ISP가 타국 정부로부터 직접적인 요청을 받았을 때 정보공개를 할 수 있도록 국내 제도를 마련할 것을 가입국에 요구하는 반면, 정작 ISP에게는 별도의 기준 마련을 요구하지 않는 것이다. 따라서 국가기관보다 더욱 불투명하고 비일관적인

21) 박재성, 앞의 논문, 265면. 이에 따르면 Microsoft 판결과 CLOUD Act가 도입된 배경도 마이크로소프트가 자사 해외서버에 저장된 데이터에 대한 압수수색을 거부했기 때문이라고 한다. 즉, ISP는 개인정보를 보호하기 위해서 국가와 대립각을 세우는 것도 주저하지 않는다는 것이다.

22) Courtney Christensen, 앞의 논문, 1037면: Smaller-and medium-sized internet service providers will likely be more susceptible to this control, as they are unlikely to have access to the legal or human resources that would allow them to fight these requests or endure the potential punishment for non-compliance.

23) Courtney Christensen, 앞의 논문, 1037면: Companies who are attempting to avoid conflict, reduce legal uncertainty, and maintain a stable relationship with governments will have a large incentive to comply with these requests.

기준으로 정보공개가 이루어질 가능성이 매우 높다고 볼 수 있다.

그리고 ②의 해석과 반대로 오히려 Microsoft 판결로 인해 ISP가 정당한 사유가 있다 하더라도 정보공개에 응하지 않을 가능성이 작아졌다고 볼 수 있다. Microsoft가 정보공개 요청을 거부하는 적극적인 행동을 취했음에도 불구하고 결과적으로 판결로 인해 정보공개가 강제되었기 때문이다. 따라서 Microsoft 판결은 ISP의 정보공개 요청 거부를 방지하는 결과를 가져왔다고 할 수 있다. 추후 ISP가 정보공개 요청을 거부하면 국가기관은 Microsoft 판결을 근거로 정보공개를 강제할 수 있는 것이다.

나. 쌍방 가벌성(Dual Criminality) 부재

쌍방 가벌성이란 외국 수사기관의 정보공개 요청 근거인 범죄사실이 상대 국가에서도 범죄로 규정되어야 한다는 원칙이다.[24] 범죄인 인도에서 적용되었던 원칙이 디지털증거 수집에도 적용되었다고 할 수 있다. 이 원칙은 수사기관의 자의적이고 정치적 편향에 따른 부당한 기소를 방지하고 정보공개의 일관된 기준을 제시하는 데 의의가 있다.[25]

그러나 정의에서 알 수 있듯이 쌍방 가벌성은 국가 간 정보공개 협조에만 적용되는 원칙이다. ISP로선 자기가 공개하는 정보가 자기가 속한 국가에서도 범죄에 해당하는지를 판단할 이유가 없다. 따라서 쌍방 가벌성이 없으면 ISP의 개인정보 공개 여부의 근거가 될 수 있는 법적 기준 또한 사라지게 된다.[26] 즉, ISP의 더욱 자의적인 개인정보 공개가 가능해진 것이다. 이에 따라 민주주의와 정보통신센터(Center for Democracy and Technology, CDT)[27] 등 일부 국제기구는 제2 추가의정서에 쌍방 가벌성이 명시되어야 한다고 주장한다.

---

24) Vagia Polyzoidu, 앞의 논문, 363면: The offence prosecuted in one State must also constiute a crime in the State in which the data is being requested.

25) Vagia Polyzoidou, 앞의 논문, 363면: It provides legal certainty for individuals and prevents politically motivated or otherwise unjust prosecutions.

26) Courtney Christensen, 앞의 논문, 1045면: The lack of dual criminality requirement removes legal standards by which companies can base their decisions about whether or not to release user's data, making their decisions all the more arbitrary.

27) 제2 추가의정서에 대한 CDT 비판 성명서 웹사이트: https://rm.coe.int/cdt-comments-2nd-additional-protocol/168098c93e (마지막 검색일 2023.8.14.)

다. 가입자 정보 개념 및 기준의 모호성

1) 개념의 모호성

제2 추가의정서를 지지하는 견해는 ① 제2 추가의정서가 모든 개인정보가 아닌 가입자 정보 등 일부 정보만을 선택적으로 공개한다는 점,[28] ② 가입자 정보만으로는 관련 개인의 사생활과 일상 습관에 대한 정확한 결론을 내릴 수 없다는 점[29]을 근거로 개인정보 침해를 최소화했다고 주장한다. 그러나 이는 가입자 정보와 트래픽 데이터 등의 개념이 명확하다는 전제하에 가능한 주장이다. 하지만 미국의 Jones 판결[30]에서도 알 수 있듯이, 트래픽 데이터 등 법률이 규정한 기술 관련 개념은 실무상 적용하는 과정에서 명확하지 않을 수 있다. 프런티어전자재단(Electronic Frontier Foundation, EFF)[31]은 가입자 정보로서의 IP 주소와 트래픽 데이터로서의 IP 주소가 구분되어야 하지만 제2 추가의정서가 양자를 구분하지 못한다고 비판한다.[32] 유럽의회(European Parliament) 또한 어떠한 정보가 제2 추가의정서가 규정한 '가입자 정보'에 해당하는지 모호하다고 비판한다.[33]

---

28) 박재성, 앞의 논문, 266면.

29) 박희영, "유럽평의회: 전자 증거의 협력 및 공개 강화에 관한 사이버범죄 협약 제2차 추가의정서(CETS No.224)", 유럽 법제동향, 톰슨로이터코리아, 2023, 9면.

30) U.S. v. Jones, 565 U.S. 400 (2012). 경찰이 마약범죄 혐의자 존스의 지프차에 무단으로 위치추적 장치를 사용한 조치가 수정헌법 제4조의 위반인가가 쟁점이 된 사안에 대하여, 연방대법원은 하급심의 판단을 긍정하면서 영장 없이 존스의 차량에 GPS 추적 장치를 설치한 것은 수정헌법 제4조에 따라 불법 수색에 해당한다고 판단하였다. 존스 판결에서 법원은 개인의 고속도로 이용에 있어서 사생활에 대한 합리적인 기대가 존재하지 않는다는 정부의 주장을 기각하고, 수정헌법 제4조가 개인의 프라이버시 침해를 어느 정도 보호하고 있다고 강조하였다. 해당 판결에서 특히 Alito 대법관은 보충의견(Concurring Opinion)을 통해 "장기간의 감시는 사람이 반복적으로 하는 것, 하지 않는 것, 합주하는 것과 같은 단기 감시에 의해 드러나지 않는 정보의 유형을 보여준다. 이러한 유형의 정보는 각각 격리된 상태에서 본 어떤 개별 여정보다 한 사람에 대해 더 많은 정보가 드러나게 할 수 있다"고 하여 장기간의 감시로 축적된 정보를 통해 한 사람에 대한 사실상 모든 정보를 알 수 있다고 강조하였다.

31) 제2 추가의정서에 대한 EFF 비판 성명서 웹사이트: https://www.eff.org/document/eff-comments-additions-budapest-protocol-cybercrime (마지막 검색일 2023.8.13.)

32) 각주 31의 성명서, 4-8면.

33) Birgit Sippel & Nuno Melo, "2nd Working Document(B) on the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters", 유럽의회 정기보고서, 2019, 5면: There is no agreement among Parties to the Convention on the demarcation between subscriber information and traffic data.

개념의 모호성은 결국 정보 수집 주체 혼선을 일으킨다. 일부 국가는 IP 주소와 가입자 정보를 동일시하기도 하며, 더 나아가 일부 국가에서는 가입자 정보를 경찰이나 검찰이 수집하나 다른 국가에선 법원 명령에 따른 수집만이 허용된다.[34] 즉, 가입자 정보의 성격을 어떻게 해석할 것인지에 따라 정보 수집의 주체가 달라지는 것이다. 이는 결국 제2 추가의정서가 국가별 법체계의 다양성을 포섭하기 위해 규정한 '권한 있는 기관'이라는 포괄적인 개념조차 실무 단계에서 혼란을 가져온다는 비판[35]으로 이어진다.

가입자 정보든 트래픽 데이터든 상관없이 어떠한 유형의 정보를 수집하더라도 결국 IP 주소는 필연적으로 수집된다. 그리고 IP 주소가 공개되면 개인의 위치, 네트워크 접속 기록 등의 정보가 공개될 뿐만 아니라 명시적으로 공개되지 않은 정보들에 대한 힌트도 제공된다.[36] 일정 정보들을 명시적으로 공개할 뿐만 아니라 공개되지 않은 정보들도 무엇인지 암시하는 것이다. 정보 수집을 통해 이러한 '힌트'들이 누적되면 결국 명시적으로 요청하지 않은 정보들까지 수집할 수 있게 되어 과도한 개인정보 수집, 즉 침해가 발생할 수 있다. 비슷한 맥락에서 Jones 판결 또한 단일 정보 자체는 많은 개인정보를 담고 있지 않다고 하더라도 해당 정보가 지속적으로 축적되면 사실상 개인정보 전부 공개와 다름없는 결과가 발생한다고 판시하였다.[37] 따라서 제2 추가의정서에 규정된 모호하고 불명확 정의 조항들로 인해 개인정보의 침해사안으로 비하될 우려가 있다.

---

34) Birgit Sippel & Nuno Melo, 앞의 보고서, 5-6면: In some Member States, subscriber data can be gathered by police or prosecutors, whilst in others, the data gathering has to be based on a court order. Moreover, some Member States treat IP addresses as subscriber data.

35) Veridiana Alimonti, "Assessing New Protocol to the Cybercrime Convention in Latin America", EFF 단행 보고서, 2022, 10-11면.

36) Veridiana Alimonti, 앞의 보고서, 12면: Police can request your name, the subscriber data linking your identity to your online activity, and that can be used to create a nicely detailed police profile of your daily habits, and may also provide relevant hints regarding the content of your communications.

37) U.S. v. Jones, 565 U.S. 400 (2012): Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. [...] A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts.

2) 기준의 모호성

전술한 바와 같이 제2 추가의정서는 권한 있는 기관이 타국에 위치한 ISP에게 직접 사건 수사에 필요한 가입자 정보를 제공할 것을 요청할 수 있도록 하고 있다. 그러나 "수사에 필요한"이라는 기준을 제시했음에도 불구하고 제2 추가의정서는 정작 해당 수사에 관한 사실관계를 ISP에 설명할 것을 요구하지 않는다.[38] 즉, 수사에 필요하다는 추상적인 요건만 제시하고 그에 대한 구체적인 기준을 제시하지 않은 것이다. 비록 정보 공개 요청은 어디까지나 특정 형사사건 또는 재판에 관련된 긴급한 상황에서 이루어져야 하기에 수사 중인 사건의 죄명, 근거 법률도 제시되어야 하지만,[39] 제9조에 따라 이는 긴급상황(Emergency)에만 적용될 뿐, 긴급상황이 아닌 경우에는 이러한 제시 의무가 없다.

ISP로선 자신들이 타국에서 진행되고 있는 수사와 자신들이 공개해야 할 정보의 관련성을 판단할 수 없으므로 타국 기관이 수사에 필요하다는 이유로 요청하면 그에 따를 수밖에 없다. 따라서 수사기관은 사실상 모든 정보의 공개를 요청할 수 있게 된다. "수사의 필요한"이라는 기준 자체가 추상적이므로 사실상 모든 정보의 공개요청을 기준에 포섭시킬 수 있는 것이다.

또한, 제6조 제2항 및 제7조 제1항은 모두 "필요한(Necessary) 입법 및 기타 조치를 해야 한다"라고 규정되어 있으나, 국가마다 '필요한'이라는 기준을 다르게 해석하여 협약에 따르더라도 국가마다 똑같은 범죄에 대한 처벌을 다르게 할 가능성이 있다는 견해[40]가 있다. 더 나아가 일부에선 이미 규정 자체가 모호하므로 굳이 일부 조항의 적용 제외가 아니더라도 충분히 회피할 수 있다고 비판한다.[41]

---

38) Courtney Christensen, 앞의 논문, 1050면: Governments are not required to provide a summary of the facts regarding the crime for which they are gathering evidence.

39) 박재성, 앞의 논문, 261면.

40) Mickellea M. Tennis, "A United Nations Convention on Cybercrime", 48 Cap. U. L. Rev. 189 (2020), 201면: This language leaves open many options for parties to decide what is "necessary," creating the potential for conflicting laws and uneven application of the Convention in practice.

41) Allison Peters & Amy Jordan, "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime", 10 J. Nat'l Security L. & Pol'y 487 (2020), 13면 참조: Even when countries have acceded to the Budapest Convention, some have criticized the treaty because of the vagueness of its provisions that have allowed governments to skirt their obligations.

라. 개인정보 보호와 공개의 비례 문제

1) 비례성 원칙

역외 압수·압수수색 절차 간소화는 결국 개인정보 보호 문제와 직결된다. 물론 개인정보 보호권은 다른 권리들과 마찬가지로 국가에 의해 필요에 따라 제한될 수 있으며, 제한의 범위는 사안의 중요성 및 필요성에 비례해야 한다.[42] 또한, 제14조가 명시한 바와 같이 당사자 통보 등의 절차를 통해 정보공개의 투명성 또한 보장되어야 한다.

그러나 역외 압수·압수수색 절차가 간소화로 인해 국가가 아닌 ISP가 정보공개 판단 주체가 되면 비례성 원칙이 제대로 지켜지지 않을 확률이 높아진다. ISP가 국가기관만큼 사안별 비례원칙을 판단할 역량을 가지거나 관련 절차 및 규정을 마련할 수 있을지 의심되기 때문이다. 제2 추가의정서가 각 ISP에 별도의 판단 기준을 마련하거나 공개할 것을 요구하지 않는 상황에서 ISP가 자발적으로 기준을 제시하여 비례원칙을 제대로 지킬지 의심스러울 수밖에 없다. 즉, ISP가 무엇을 근거로 정보공개 여부를 결정할지, 그 기준은 과연 국가가 적용하는 수준의 비례원칙 기준일지가 문제 되는 것이다.

2) 행위와 책임 주체의 불일치에 따른 무분별한 공개 가능성

개인정보 보호를 명시한 제14조 역시 개인정보를 보호하는데 효과적이지 않을 수 있다. 제14조 제12항 및 제14항은 개인정보 보호 조치를 취하지 않거나 개인정보를 부당하게 취득한 국가에 대해 정정 조치를 요구하거나 정보 제공을 중단할 수 있도록 규정하고 있다. 그러나 독일처럼 기본적으로 존재하는 압수의 공개성 원칙에 대한 예외로서 디지털증거 등 일부 증거에 대해 법원 명령을 통해 압수하더라도 통지를 유보할 수 있으면,[43] 개인정보가 공개되었다는 사실조차 인지할 수 없게 되므로 그에 대한 조치를 요구

---

42) Christine Galvagna, “The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform”, 9 Notre Dame J. Int’l & Comp. L. 57 (2019), 62면: Government interference with privacy or data protection rights must, first, be necessary to achieve a legitimate aim. Second, the interference must be proportionate to that aim, in that it appropriately balances the state's interest in obtaining data with the seriousness of the interference with the subject's privacy and data protection rights.

43) 박희영, “형사소송법 제95a조의 도입: 제3자가 보관 중인 증거의 비밀 입수”, 독일 법제동향, 톰슨로이터코리아, 2021, 3면.

하기가 어려워진다. 그리고 이러한 조항은 제2 추가의정서와 마찬가지로 증거 수집의 효율성 확보를 목표로 하고 있으므로[44] 제2 추가의정서에 따르더라도 관련 규정이 국내 이행법률로 마련되어 있지 않다면 위법으로 해석될 여지가 있다.

또한 문제가 될 수 있는 개인정보 공개의 주체는 ISP임에도 불구하고 그에 대한 입법적 책임을 국가가 부담하게 한다는 점에서 해당 조항의 실효성이 의심받는다. 국가 입장에선 자신들이 공개하지도 않은 정보에 대해 공개를 중지하거나 관련 조치를 취할 명분이 약하기 때문이다.

그럼에도 불구하고 "필요한 입법 및 기타 조치를 해야 한다"라는 조항은 결국 ISP가 추가의정서에 따라 정보 제공요청 준수에 대한 책임으로부터 면제되도록 당사국에 관련 법률을 만들도록 강제한다.[45] 따라서 제2 추가의정서는 정보공개 행위 주체는 ISP지만 그에 대한 책임은 국가가 부담하므로 행위와 책임 주체의 불일치가 발생한다. 그리고 이에 따라 ISP는 책임이라는 부담이 없으므로 더욱 무분별한 개인정보 공개를 할 위험이 있다.

마. 실효성 의문

1) 일부 조항 선택적 유보의 문제

전술한 바와 같이 제2 추가의정서는 각 국가의 법체계 다양성을 인정한다는 명분 아래 일부 조항을 채택하지 않을 수 있도록 하였다. 그러나 채택하지 않을 수 있는 조항들은 몇몇 조항과 같이 제2 추가의정서의 핵심적인 내용을 규정한 조항들이다. 각 국가의 법체계 다양성을 인정한다는 취지는 긍정적이나, 이에 따라 추가의정서의 실효성이 문제될 수 있는 것이다.

또한, 제7조 제9항 제a호에 따라 가입국은 필요시 제7조 적용을 유보할 수 있으나,

---

44) 박희영, 앞의 논문, 3면에 따르면, 소위 다크넷 등 사이버범죄 영역에서 피의자에게 통지해야 하는 것은 추가 비밀 처분을 더 어렵게 하므로 통지 유보 조항이 마련되어야 한다고 주장한다. 한편 통신비밀보호법에서는 통신사실 확인자료의 제공과 관련하여 '통지유예제도'를 마련하고 있다(통신비밀 보호법 제13조의3 제2항 참조).

45) Courtney Christensen, 앞의 논문, 1035면: The protocol requires that party states to create implementing legislation to ensure that ISPs "give effect" to the request for evidence by shielding them from liability for complying with evidentiary requests under the protocol.

이는 서명 시 또는 그 비준, 승낙 또는 승인의 문서를 보관할 때에만 적용된다. 제7조를 유보한 국가가 다른 국가에 있는 ISP에 제7조 제1항에 따른 직접적인 정보공개 요청을 할 수 없는 것이다.[46] 결국 다른 국가 소재 ISP에 정보공개 요청을 하기 위해선 사실상 제7조를 비준해야 하는 것과 마찬가지이다. 따라서 일부 선택적 유보 조항 자체가 명분상으로만 있을 뿐 사실상 모든 조항의 적용을 강제하는 것과 다름없다고 해석될 수 있다. 더 나아가 일부에서는 제2 추가의정서의 실효성을 확보하기 위해서라도 제7조가 반드시 필요하다고 주장한다.[47]

2) 국가 간 분쟁 가능성

가) 중국 및 러시아의 반발

이미 부다페스트 협약이 서방 국가 중심으로 규정되어 있는 상황에서 제2 추가의정서 또한 같은 문제가 있다고 보는 견해[48]도 있다. 비록 각 국가의 법체계 다양성을 인정하려고 하나 기본적으로 구조 자체가 서방 국가 위주라는 것이다. 실제로 중국과 러시아는 부다페스트 협약과 추가의정서가 서방 국가 중심적이라고 비판하면서 가입을 거부하고 있으며, 이에 따라 기존 협약 대신 새로운 "진정한 국제 협약(Truly Global Agreement)"이 제정되어야 한다고 주장한다.[49] 이미 부다페스트 협약에 대응하기 위해 중국 - 러시아 사이버범죄 협약(Russia-China Cyber Treaty) 제정이 양국 간 논의되고 있는 상황에서 제2 추가의정서 또한 서방 국가 위주라는 비판으로부터 자유롭지 못한 것이다. 중국과 러시아의 국제적 영향력을 고려하면 그들의 반대는 부다페스트 협약 및

46) Veridiana Alimonti, 앞의 보고서, 11면: Paragraph 9(a) of Article 7 allows Parties to reserve the right not to apply Article 7 in its entirety, but only at the time of signature or when depositing its instrument of ratification, acceptance, or approval. A Party that reserves Article 7 is not permitted to issue direct cooperation orders under Article 7, paragraph 1, to service providers in other Parties' territories.

47) 대표적으로 박재성, 앞의 논문, 266면.

48) Melissa L. Ken, 앞의 논문, 24면: One of the main attacks against the Convention is that it was drafted by Western nations and thus does not reflect the interests of non-Western nations. The keys to these reforms lie in a new proposal amending membership procedures and heeding current calls to revise the proposed additional Protocol.

49) Melissa L. Ken, 앞의 논문, 24면: China and Russia regularly argue that the Convention should be replaced by a truly global agreement.

제2 추가의정서 가입률 저하, 더 나아가 국제 협약으로서의 실효성 문제를 일으킬 수밖에 없다.[50] 이에 따라 일부에서는 협약의 실효성을 확보하기 위해서라도 중국과 러시아 등 非서방 국가들도 가입할 수 있도록 제2 추가의정서를 개정해야 한다고 주장한다.[51]

나) 새로운 국제조약 논의를 위한 UN 결의[52]

2019년 12월 27일 유엔 총회는 정보통신기술(Information and Communications Technologies, "ICT")을 이용한 범죄행위에 대응하기 위한 새로운 국제조약을 논의하기 위해 전문가들로 구성된 특별위원회를 설치할 것을 결의하였다.[53] 그리고 러시아 등 부다페스트 협약과 제2 추가의정서에 반대했던 국가들은 UN 결의에 동의하는 태도를 보인다.

비록 새로운 조약에 어떠한 내용이 담길 것인지 등 구체적인 부분은 전혀 언급되지 않았으나, 결의에 동의하는 러시아의 견해에 비추어 새로운 조약에 담길 내용을 짐작할 수 있다는 견해[54]가 있다. 러시아는 이미 2017년 유엔 총회에서 새로운 국제조약의 초안을 제시한 바 있다. 그리고 초안은 국가체제 보호를 위한 사이버범죄는 엄벌하되 부다페스트 협약과 달리 형사사법공조가 내정간섭에 이르면 안 된다는 점을 강조하고 있으며, 더 나아가 범죄행위에 대한 형사사법공조 요청 또는 범죄인인도 요청이 이루어지는 경우 요청받은 국가는 수사 대상 범죄가 정치범죄(Political Offence)라는 이유만으로는 협조를 거부할 수 없도록 규정하고 있다.[55]

따라서 러시아를 필두로 한 UN 결의는 부다페스트 협약 및 제2 추가의정서와 배치되는 새로운 국제조약을 입안하려는 시도로 볼 수 있다. 그리고 이러한 입안 시도는 기존 공조 노력과 중복되어 실효성을 저해할 가능성이 있다.[56]

---

50) Melissa L. Ken, 앞의 논문, 29면: The delay will allow new member-nations (such as China and Russia) to provide meaningful input to Additional Protocol II which will allow the protocol to reflect global concerns and priorities.
51) 대표적으로 Melissa L. Ken, 앞의 논문, 27-29면.
52) https://digitallibrary.un.org/record/3847855?ln=en(최종 검색일: 2023.8.26.)
53) 박재성, 앞의 논문, 266면.
54) 박재성, 앞의 논문, 269면.
55) 박재성, 앞의 논문, 270-271면.
56) 박재성, 앞의 논문, 276면.

다) 유럽인권재판소 판결과 상충

중국과 러시아뿐만 아니라 정작 제2 추가의정서가 제정된 유럽에서조차 갈등의 소지가 있다. 2018년 유럽인권재판소(European Court of Human Rights)는 Benedik 판결을 통해 경찰이 법원 명령을 받지 않고 가입자 IP 주소와 가입자 정보를 수집하는 것은 불법이라고 하였다.[57] 제2 추가의정서가 가입자 정보 등을 타국 ISP에 직접 요청할 수 있다고 규정한 것과 달리 법원 명령이 요구된다고 판결한 것이다.

비록 서유럽 국가들에만 국한되어 있으나, 유럽인권재판소 판결은 구속력을 가진다. 따라서 제2 추가의정서가 실효성을 확보하기 위해서라도 유럽인권재판소 판결과의 불일치 문제를 해결해야 한다. 디지털증거 압수에 대해 통지가 유보된 압수와 마찬가지로 비법원에 의해 수행하고 사후에 법원의 승인을 받는 독일의 사례[58]를 참고하여, 가입자 정보 등을 타국 ISP에 우선 요청한 뒤 사후에 법원 명령을 받는 방법도 고려할 수 있다.

57) Benedik v. Slovenia (Application no. 62357/14). 판결문 원본 웹사이트(http://www2.gov.si/dp-rs/escp.nsf/e868d16f2fedf171c1256bdd004936b6/ee2cda44f07c7756c12582cf0045c390/$FILE/CASE%20OF%20BENEDIK%20V.%20RS..pdf.; 최종방문일: 2023.9.28.)

사건 진행	슬로베니아 경찰은 특정 P2P 파일공유 사이트를 통해 아동음란물과 파일을 주고받은 정보를 근거로 특정 시점에 IP 주소가 할당된 사용자에 대한 정보공개를 법원 명령 없이 ISP에 요청하였다. 이 요청에 따라 ISP는 경찰에게 해당 IP 주소와 관련된 인터넷 서비스가입자인 Benedik의 아버지의 이름과 주소를 경찰에 전달했다. 이후 경찰은 Benedik 아버지의 개인정보와 교통정보에 대한 법원 명령을 받아 냈고, 이를 통해 Benedick 아버지의 가정집을 수집하여 미성년자가 연루된 음란물이 포함된 것으로 확인된 컴퓨터를 압수·수색했다. 그러나 경찰은 이후 Benedik의 아버지가 아닌 Benedik를 음란물 전시·제조·소지·유통한 혐의로 기소하였다. IP에 따른 가입자는 아버지였으나, IP를 접속한 컴퓨터, 즉 음란물이 있는 하드디스크는 Benedik의 소유였기 때문이다. 이에 대해 Benedik는 서신 및 기타 통신수단의 프라이버시는 법원의 명령에 의해서만 제한될 수 있으므로 위법하게 취득한 정보는 증거로서 배제되어야 한다고 항변하였다. 즉, 경찰이 영장을 받은 대상은 자신이 아닌 자신의 아버지이며, 설령 자신을 대상으로 하였다 하더라도 처음에 영장 없이 ISP로부터 받은 정보를 근거로 음란물 소지 등 관련 증거를 수집했으므로 위법하게 취득했다는 것이다. 이에 대해 슬로베니아 헌법재판소는 IP 주소의 사용자 신원에 관한 정보는 헌법상 프라이버시로 보호된다는 점을 인정하면서도 Benedik가 자신이 인터넷에 접속한 IP 주소를 어떠한 방법으로도 숨기지 않았으므로 해당 권리를 보호받을 합리적 기대를 어느 정도 포기한 것과 같다고 판단하였다. 국내 법원에서 유죄 판결을 받은 Benedik는 이를 다시 유럽인권재판소에 제소하였다.
쟁점	Benedik의 개인정보를 수집하는 과정에 경찰의 위법이 있는가? Benedik를 비롯한 인터넷 사용자는 자신의 온라인 활동이 익명으로 남아있을 것으로 기대하는 것이 합리적 기대인가?
결론	유럽인권재판소는 Benedick가 자신의 IP 주소와 파일 공유 네트워크에서 통신한 내용을 공개함으로써 사실상 사생활에 대한 권리를 포기했기 때문에 경찰이 법원의 명령을 받을 필요가 없었다는 헌법재판소의 판단은 사생활에 대한 권리를 침해하는 결정이라고 판단하였다. 또한 유럽인권재판소는 사생활에 대한 권리 포기가 없으므로 경찰이 법원의 명령을 받지 않고 Benedik의 IP 주소와 가입자 정보를 수집하는 것은 위법하다고 판단하였다.

58) 박희영, 각주 43의 논문, 3면.

4. 소결

제2 추가의정서는 ① 정보공개 주체의 전환 및 권한의 정당성, ② 쌍방 가벌성 부재, ③ 개념 및 기준의 모호성, ④ 개인정보 보호, ⑤ 실효성의 문제가 있다.

제2 추가의정서의 가장 핵심적인 부분은 역외 압수·수색의 효율성과 용이성을 확보하기 위하여 타국의 국가기관을 거치지 않고 ISP에 직접 정보공개 요청을 할 수 있게 했다는 점이다. 그러나 ISP에 정보공개의 권한을 부여하면서 ISP가 무슨 권한과 기준을 가지고 정보공개를 하는지 모호하다는 문제가 발생했으며, 불명확한 기준에 따른 정보공개는 결국 개인정보 보호와 더불어 의정서 자체의 실효성 문제로 이어졌다. 따라서 제2 추가의정서의 문제점들은 역외 압수·수색의 확장으로부터 서로 연결되었다고 할 수 있다.

제2 추가의정서는 역외 압수·수색의 확장과 개인정보 보호의 조화를 이루기 위해 노력하였으나, 일부 비판적 견해에 따르면 결과적으로 전자만을 강조한 것으로 보고도 있다. 개인정보를 보호하고 법체계의 다양성을 존중하기 위해 규정한 일부 조항만으로는 충분하지 않다는 것이다. 따라서 우리는 국제공조를 강화하고 급변하는 기술 발전에 대응해야 할 필요가 있으므로 언젠가는 제2 추가의정서에 가입해야 할 것이지만, 제2 추가의정서 가입 여부에 대해서는 더욱 신중하게 접근해야 한다.

Ⅲ. 제2 추가의정서 가입을 위한 국내 법률 정비

부다페스트 협약 가입을 위한 이행 입법으로서 형사소송법, 통신비밀보호법, 전기통신사업법, 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 등의 개정이 필요하다는 논의가 진행 중이다.[59] 부다페스트 협약과 제2 추가의정서의 공통된 주요 쟁점 중 역외 압수·수색의 확장과 관련된 개별 법률 개정 논의는 다음과 같다.

59) 신용우, "유럽 사이버범죄 방지협약 체결 현황과 우리나라 입법·정책적 대응 방향", 국제관계 동향과 분석 제77호, 국회입법조사처 정기보고서, 2020, 5면.

1. 역외 압수·수색의 명문화

부다페스트 협약과 제2 추가의정서 모두 역외 압수·수색의 명문화 및 확장에 관한 규정이며, 특히 부다페스트 협약 제19조 제2항은 역외 압수·수색을 명시적으로 허용하고 있다. 이에 따라 부다페스트 협약 가입을 위해 우리나라 또한 역외 압수·수색을 법률에 명시해야 한다는 견해[60]가 있다. 최근 대법원에서 역외 압수·수색을 인정하였으나,[61] 강제처분 법정주의에 따라 명문화가 필요하다는 것이다. 비록 부다페스트 협약 및 제2 추가의정서가 역외 압수·수색 명문화를 요구하지는 않으나, 규정에 명시되지 않는 증거 수집은 위법수집증거 배제원칙 및 강제처분 법정주의에 반할 수 있다. 더 나아가 절차가 법률에 규정되지 않은 증거 수집 절차를 과연 무엇을 근거로 확장할 수 있을지도 불분명하다. 국내법에도 명시되지 않은 역외 압수·수색을 제2 추가의정서만을 이유로 확장하기에는 무리이다. 따라서 부다페스트 협약, 더 나아가 제2 추가의정서 가입하기 위해선 역외 압수·수색을 명시적으로 규정해야 한다.[62]

2. 트래픽 데이터 제공

부다페스트 협약 제17조와 관련하여, 협약과 달리 통신비밀보호법 제2조에는 부다페스트 협약에 명시되어 있는 통신경로·통신 크기·서비스 유형 등이 규정되어 있지 않다.[63] 또한, 우리나라 수사기관이 부다페스트 협약 상의 트래픽 데이터를 제공하려면 국

60) 이경렬·하건우, "유럽평의회 사이버범죄 조약의 가입·비준을 위한 국내 이행법률의 마련과 준비 비교", 비교형사법연구 제19권 제4호, 한국비교형사법학회, 2018, 524-525면;

61) 대법원 2017.11.29. 선고 2017도9747 판결.

62) 물론 이러한 역외 압수·수색 규정의 법정만인 관련 수사상 실무의 문제점을 모두 해결하지는 않는다. 부다페스트협약에 가입하고 유관 규정을 형사소송법에 명시적으로 입법한 일본의 경우에도 최근의 최고재판소의 결정(最高裁判所令和3年2月1日 決定, https://www.courts.go.jp/app/files/hanrei_jp/995/089995_hanrei.pdf; 최종검색일: 2023.9.30.)에 따르면 역외 압수는 여전히 위법적이라는 취지인데 반해, 이 문제를 사법실무상 해결하고 있는 우리의 대법원 판결(대법원 2017.11.29. 선고 2017도9747 판결)에서는 합법이라고 판단하고 있다. 이에 대한 자세한 논의는 이경렬·박제민. "역외 압수·수색 수사에 관한 한일 최고법원판례 비교연구", 비교형사법연구 제24권 제3호, 한국비교형사법학회, 2022, 121면 이하참조.

63) 정태진·이광민, "사이버범죄 대응을 위한 부다페스트 협약 가입과 국제공조 연구", 경찰학논총 제14권 제2호, 원광대학교 경찰학연구소, 2019, 72면.

내 통신비밀보호법을 위반할 소지가 있으며, 협약에 가입한 회원국에 직접 트래픽 데이터를 요구하여 얻을 수 있기에 적법절차에 의한 통제가 없어서 정보적 자기결정권을 훼손할 우려가 있다는 지적[64]이 있다. 가입국들이 마음만 먹으면 우리나라 국민들의 개인 통신정보까지도 접근이 가능하고 이를 정부를 거치지 않고 직접 자료요청을 할 수 있기에 문제의 소지가 있다는 것이다.[65] 이를 다르게 해석하면 제2 추가의정서에 따라 수사기관이 해외 ISP에 직접 정보공개를 요청하는 것 역시 위법할 수 있다. 따라서 제2 추가의정서는 부다페스트 협약 비판론이 위법하다고 주장한 직접 자료요청을 역외 압수·수색의 확장을 이유로 명시적으로 규정했다고 볼 수 있다.

물론 부다페스트 협약의 적용 범위가 사이버범죄 수사에 한정되어 있으므로 트래픽 데이터 수집으로 인한 개인정보 침해나 정보제공 피요청국가의 주권의 침해가 크지 않다는 견해[66]도 있다. 그러나 전술한 바와 같이 제2 추가의정서는 트래픽 데이터의 개념을 불분명하게 정의하여 개인정보 침해의 위험이 있을 뿐만 아니라 수사 관련성(Facts related to the Investigation)이라는 사실관계를 ISP에 제공할 의무 규정 또한 두고 있지 않다. 수사 관련성은 부다페스트 협약과 제2 추가의정서에 공통으로 명시되어 있는 요건이자 역외 압수·수색의 확장에 따른 트래픽 데이터 수집의 전제 조건이라 할 수 있다. 따라서 수사 관련성 요건 및 사실관계 제공 의무가 규정되어야만 간소화된 역외 압수·수색에 의한 개인정보 침해나 정보자 주권의 침해가 우려가 낮아진다. 관련 규정이 제2 추가의정서에 없으면 추가의정서와 충돌하지 않는 범위에서 국내 입법을 검토할 수 있다.

3. 범죄 수사를 위한 통신사실 확인 자료 제공

부다페스트 협약 제17조와 관련하여 통신비밀보호법 제13조는 범죄 수사를 위한 통신사실 확인 자료 제공 절차를 두고 있으며, 제15조의2와 동법 시행령 제41조에서 전기통신사업자의 협조 의무 및 통신사실 확인 자료의 제공·보관 의무를 규정하고 있다. 그

64) 전현욱·이자영, "사이버범죄 협약과 형사절차상 적법절차원칙: 저장된 데이터의 보존 및 일부공개를 중심으로", 형사정책연구 제25권 제1호, 한국형사법무정책연구원, 2014, 84면.
65) 정태진·이광민, 앞의 논문, 72-73면 참조.
66) 정태진·이광민, 앞의 논문, 72면.

리고 이에 대해 통신비밀보호법상 통신사실 확인 자료는 협약에서 규정하는 통신 데이터와 일치하지 않아 보완이 필요하다는 견해[67]가 있다. 또한, 부다페스트 협약 제18조의 컴퓨터 데이터 제출명령과 관련하여 통신비밀보호법 제13조의 통신사실 확인 자료 제공 절차 또는 형사소송법 제106조 제3항으로 대응이 가능한지 여부에 대해서도 검토가 필요하다는 견해[68]도 있다. 따라서 부다페스트 협약에 가입하면 협약에 맞게 통신비밀보호법과 형사소송법에 규정된 통신사실 확인 자료 조항들을 개정 혹은 재검토해야 한다.

그러나 제2 추가의정서는 통신사실 확인 자료 같은 기존 형사사법공조절차가 비효율적이기 때문에 새로운 제도를 도입하고자 제정된 것과 마찬가지다.[69] 기존 절차가 충분히 효율적이었으면 역외 압수·수색의 효율성 확보를 위한 별도 규정을 신설할 이유가 없기 때문이다. 따라서 부다페스트 협약에 따라 통신사실 확인 자료 제공 등의 형사사법공조절차를 개정 및 재마련하더라도 제2 추가의정서에 가입하면 해당 절차가 비효율적이라는 점을 인정하는 것과 마찬가지이게 되는 것이다.

또한, 통신비밀보호법 제13조 제3항에 따르면 수사기관은 통신사실 확인 자료 제공을 요청하는 경우 요청 사유 및 해당 가입자와의 연관성을 관할 법원에 서면으로 허가를 받아야 하는데, 이러한 '요청 사유 및 연관성'이 제2 추가의정서에 명시된 '수사 관련성'에 해당되는지 여부에 대한 검토도 필요하다. '수사 관련성'에 해당되면 제2 추가의정서와 달리 통신비밀보호법은 수사 관련 사실을 정보 제공자에게 제시할 의무를 부여하기 때문이다. 따라서 부다페스트 협약에 따라 통신사실 확인 자료 제공 절차를 개정하더라도 제2 추가의정서 가입에 따른 추가적인 재검토가 필요할 수 있다.

4. 법적 책임 규정

부다페스트 협약 제12조는 협약을 위반한 자연인이 속한 법인의 법적 책임을 규정하고 있다. 이에 대해 우리나라는 협약 제7조와 제8조의 컴퓨터 관련 위조·사기 범죄에 대응하는 양벌규정이 존재하지 않아 개정이 필요하다는 견해[70]가 있다. 더 나아가 국내

67) 정태진, "유럽 사이버범죄 협약과 사이버범죄 대응을 위한 국제공조", 국제문제연구소 워킹페이퍼 제98호, 서울대학교 국제문제연구소, 2018, 11면
68) 신용우, 앞의 보고서, 6면.
69) 박재성, 앞의 논문, 266면.

법에는 법인에 대한 처벌 조항 및 규정이 없으므로 신설이 필요하다는 견해[71]도 있다.

이와 달리 제2 추가의정서는 개인정보를 제공한 ISP의 면책 조항을 규정하고 있으며, 오히려 이에 대한 책임은 국가가 부담하도록 하고 있다. ISP의 책임 부담을 줄여 더욱 빠르고 자유롭게 정보를 공개할 수 있도록 한 것이다.

그러나 책임 주체 측면에서 부다페스트협약과 제2 추가의정서가 배치된다고 볼 수 있다. 따라서 부다페스트협약 가입에 따라 법인에 대한 처벌 조항을 마련하게 되면 추후 제2 추가의정서와의 조화를 어떻게 이뤄야 할 것인지를 고민해야 한다. 비록 부다페스트 협약 제42조는 특정 조항들에 대하여 유보할 수 있다고 명시하고 있으나, 제12조는 유보 대상에 포함되지 않기 때문이다.[72] 여기서는 ① 법인에 대한 처벌과 더불어 국가적 책임도 같이 규정하는 방안, ② 법인을 처벌하되 제2 추가의정서의 유보 조항을 적용하여 트래픽 데이터 제공에 한해 법인의 책임을 완화 또는 면제하는 방안, ③ 원칙적으로 정보 제공자인 법인의 책임을 완화 또는 면제하되 협약을 위반한 경우에만 처벌하도록 하는 방안 등을 예시로 제시할 수 있다. 물론 구체적인 방안은 추후 제2 추가의정서에 가입할 때 우리나라의 상황을 고려하여 마련해야 한다. 그러나 어떠한 방식이던 부다페스트협약과 제2 추가의정서의 조화를 위한 방안 마련을 마련해야 한다.

5. 소결

역외 압수·수색은 수사상 그 필요성이 인정됨에도 불구하고 우리나라는 이를 명시하는 규정이 없어 합법성 논란이 있었다. 이에 대한 해결책으로써 부다페스트 협약 가입의 향서를 제출하였으나, 협약에 가입하면 이행 입법으로서 관련 법률을 개정해야 한다. 그

70) 이경렬·하건우, 앞의 논문, 523면.

71) 차진아, "사이버범죄에 대한 실효적 대응과 헌법상 통신의 비밀보장: 사이버범죄 협약 가입에 따른 통신비밀보호법의 개정 방향을 중심으로", 공법학연구 제14권 제1호, 한국비교공법학회, 2013, 55면.

72) 부다페스트 협약 제42조: By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

리고 제2 추가의정서도 가입하게 되면 역외 압수·수색의 명문화, 트래픽 데이터 및 통신사실 확인 자료 제공, 법적 책임 규정문제를 검토해야 하며, 이는 제2 추가의정서의 문제점으로 지적되었던 부분과 마찬가지로 역외 압수·수색의 확장과 관련된다. 역외 압수·수색을 명문으로 규정하지 않은 상태로 강제처분을 확장할 수는 없으며, 더 나아가 역외 압수·수색의 확장에 따른 자료 제공 절차가 책임 문제로 이어졌기 때문이다. 또한, 트래픽 데이터 및 통신사실 확인 자료 제공과 법적 책임 규정은 부다페스트 협약과 제2 추가의정서 간 모순되는 부분이 있으므로 양자를 조화롭게 달성할 수 있는 입법·정책적 방안을 모색해야 한다.

물론 이러한 우려를 줄이기 위해 부다페스트 협약과 제2 추가의정서를 동시에 가입하는 방안도 고려할 수 있으나, 전술한 제2 추가의정서의 문제점을 고려하면 부다페스트 협약에 먼저 가입하고 제2 추가의정서 가입을 좀 더 시간을 두고 고민하는 방안이 타당하다. 또한, 제2 추가의정서 가입을 안 하는 방안도 있으나, 사이버범죄에 적절하게 대처해야 하기 위한 국가 간 상호 협력과 역량 강화가 중요하고 급변하는 ICT 환경에 대응해야 한다는 점을 고려하면,[73] 언젠가는 제2 추가의정서에 가입해야 한다. 그러나 제2 추가의정서의 문제점 및 부다페스트 협약과의 조화에 대한 고민이 선행되어야 한다.

Ⅳ. 국내 법률 정비와 관련된 CLOUD Act의 주요 쟁점 사항

CLOUD Act[74]는 기존 저장통신법(Stored Communications Act, SCA)[75]의 일부 조항을 개정한 법률이다. 물론 미국이 부다페스트 협약 가입을 이유로 CLOUD Act를 제정한 것은 아니다. 그러나 CLOUD Act와 제2 추가의정서 모두 수사기관이 직접 ISP에 정보공개 요청을 할 수 있게 했다는 공통점이 있다. 또한, CLOUD Act와 제2 추가의정서를 동일선상에서 논의해야 한다는 견해[76]도 있는 만큼, 양자의 비교 논의는 중요

73) 정명현, "유엔 사이버범죄 대응 국제조약의 논의 동향과 전망", 국제법 동향과 실무 통권 제62호, 외교부 국제법률국, 2021, 19면.
74) 18 U.S. Code § 2523
75) 18 U.S. Code § 2701-2712
76) Christine Galvagna, 앞의 논문, 65면: Recently proposed or enacted legal instruments designed

한 의미가 있다. 따라서 아래에서는 CLOUD Act가 전술한 역외 압수·수색 확장을 위한 국내 법률 정비 관련 쟁점들을 어떻게 해결하고 있는지 논의해본다.

1. 역외 압수·수색 명시

CLOUD Act는 역외 압수·수색(Trans-border Access) 명시적으로 규정하지 않고 있다. 오히려 SCA를 통해 원격 압수·수색이 처음 규정되었으며, CLOUD Act를 근거로 한 Microsoft 판결[77]이 처음으로 역외 압수·수색을 명시적으로 허용했다고 봐야 한다.[78] Microsoft 판결이 역외 압수·수색을 규정하였으므로 판결의 근거 법률인 CLOUD Act 또한 역외 압수·수색에 관한 규정이라고 해석할 수 있는 것이다.

2. 정보 제공

CLOUD Act에 따라 국가기관이 요청할 수 있는 정보는 "특정인, 계정, 주소 또는 개인기기, 기타 특정 식별자"로 식별될 수 있어야 한다.[79] 또한 국가기관은 ISP에 "조사 대상에 대한 명백하고 신뢰할 수 있는 사실, 특수성, 적법성 및 경중에 근거한 합리적인 정당성"을 설명할 의무가 있다.[80]

---

to streamline cross-border data access include the U.S. CLOUD Act, the EU's e-Evidence proposal, the Council of Europe's potential Second Additional Protocol to the Budapest Convention, and a proposal for an International Data Access Warrant by the U.N. Special Rapporteur on the right to privacy.

77) U.S. v. Microsoft, 138 S. Ct. 1186 (2018)

78) Yanqing Hong, "Game of Laws: Cross-Border Data Access for Law Enforcement Purposes", Yale Law School Paul Tsai China Center 단행 보고서, 2021, 6면: The SCA is the primary legal ground for U.S. law enforcement agencies to forcefully access individuals' or enterprises' private electronic communications. It is mainly applied in the United States and does not give clear instructions on overseas data. The dispute between the parties in Microsoft Corp. v. United States involved jurisdiction over data stored abroad.

79) Christine Galvagna, 앞의 논문, 70면: The subject of a data request must be described by "a specific person, account, address, or personal device, or any other specific identifier."

80) Christine Galvagna, 앞의 논문, 70면: Additionally, a request must include "a reasonable justification based on articulable and credible facts, particularity, legality, and the severity regarding the conduct under investigation."

그러나 CLOUD Act는 정보공개의 범위를 테러 등 “중대 범죄(Serious Crime)”로 제한하지만, 중대 범죄가 무엇인지에 관한 정의 조항이 없어 광범위하게 해석될 수 있다는 문제가 있다.[81] 비록 범죄 통제 및 집행법(34 U.S. Code: Crime Control and Law Enforcement) 제11103조가 중대 범죄를 정의하고 있으나,[82] 이는 CLOUD Act가 규정된 연방 형법(18 U.S. Code)에 규정된 정의 조항이 아니므로 해당 조항을 근거로 CLOUD Act를 집행할 수는 없다. 따라서 CLOUD Act는 정보 제공과 관련하여 일부 조항이 불명확하다는 문제가 있다.

3. 법적 책임

정보공개 요청을 받은 ISP는 해당 정보를 공개할 수 있으며, CLOUD Act에 따라 미국과 CLOUD Act 협약에 합의한 국가 또한 미국 소재 ISP를 상대로 정보공개 요청을 할 수 있다.[83] 더 나아가 CLOUD Act는 적법한 요청에 의한 적법한 정보공개는 추후 민·형사 책임으로부터 면제된다는 기존 SCA 조항[84]을 그대로 남겨두었으며, 판례 또한 해당 조항이 합헌이라고 판시했다.[85] 따라서 미국의 ISP는 CLOUD Act 및 SCA

81) Christine Galvagna, 앞의 논문, 70면: The CLOUD Act limits the purposes for which orders can be sent by foreign governments to “serious crime[s], including terrorism. Yet the term “serious crime” is undefined, and absent further clarification may be interpreted too liberally.

82) 34 U.S. Code § 11103(14): The term “serious crime” means criminal homicide, forcible rape or other sex offenses punishable as a felony, mayhem, kidnapping, aggravated assault, drug trafficking, robbery, larceny or theft punishable as a felony, motor vehicle theft, burglary or breaking and entering, extortion accompanied by threats of violence, and arson punishable as a felony

83) 18 U.S. Code § 2702(b): A provider described in subsection (a) may divulge the contents of a communication—
(9) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

84) 18 U.S. Code § 2703(e): No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

85) Alexander v. Verizon Wireless Services, LLC, No. 16-31227 (5th Cir. 2017): Thus, § 2703(e) provides immunity to a service provider when it makes a disclosure in accordance with a

에 따라 적법한 요청에 자유롭게 정보공개를 할 수 있다. 그리고 이러한 관계를 '선의의 신뢰(Good Faith Reliance)'라고 하여 사실상 모든 민·형사 책임으로부터의 면제를 제공한다고 보는 견해[86]도 있다.

물론 이러한 조항들은 공개적으로 ISP의 책임을 면제하고 더 나아가 ISP를 보호하려는 목적을 가진다.[87] 그러나 이러한 면책 조항으로 인해 국가 간 분쟁이 발생할 가능성 또한 낮아졌다는 견해[88]도 있다. 이 견해는 ①정보공개 요청에 대해 ISP가 법의 충돌 혹은 위법의 가능성을 이유로 공개요청을 거부할 수 있었으나 해당 조항으로 인해 법의 충돌 및 위법의 소지가 낮아졌다는 점, ②면책 조항으로 인해 적법한 요청에 따른 공개로 인해 추후 문제가 발생해도 책임의 소재가 명확해졌다는 점을 근거로 분쟁 가능성 또한 간접적으로 낮아졌다고 본다. 물론 이는 적법한 요청에 따른 적법한 공개에만 적용되며, 적법하지 않은 공개에 대해선 정보를 공개한 ISP가 책임을 져야 한다.

4. 국내 시사점

CLOUD Act는 ① 역외 압수·수색 명시, ② 정보 제공, ③ 법적 책임 측면에서 제2 추가의정서 도입 시 우리나라에 발생할 수 있는 쟁점들에 대해 시사하는 바가 있다. 우선 CLOUD Act는 Microsoft 판결을 통해 역외 압수·수색을 간접적으로 명시했다고 볼 수 있다. 이는 영미법 국가 특성상 판례가 법률과 동일시되기 때문에 가능했던 부분이기도 하다. 따라서 CLOUD Act를 근거로 우리나라 또한 역외 압수·수색을 명문화할 이유가 없다고 주장해선 안 될 것이다. 우리나라는 시민법 국가이며, 강제처분 법정주의를 따르기 위해서라도 법률에 명시된 절차가 필요하기 때문이다.

정보 제공과 관련하여 CLOUD Act 또한 제2 추가의정서와의 충돌 문제가 발생할 수 있다. CLOUD Act에 규정된 '사실 및 합리적인 정당성'이 제2 추가의정서의 '수사

provision of the SCA.

86) Tim Cochrane, "Hiding in the Eye of the Storm Cloud: How CLOUD Act Agreements Expand U.S. Extraterritoral Investigatory Powers", 32 Duke J. Comp. & Int'l L. 153 (2021), 171면: A mere "good faith reliance" on 18 U.S.C. § 2702(b)(9) provides "a complete defense to any civil or criminal action brought under this chapter or any other law."

87) Tim Cochrane, 앞의 논문, 171면: These provisions are expressly designed to protect providers.

88) Tim Cochrane, 앞의 논문, 171-175면.

관련성'에 해당한다면, CLOUD Act 또한 우리나라 통신비밀보호법 제13조 제3항과 마찬가지로 수사 관련 사실을 ISP에 제시할 의무를 부여하기 때문이다. 그러나 아직 이러한 충돌 문제를 어떻게 해결해야 할지에 대한 논의를 미국에서도 찾아볼 수 없다. 추후 관련 논의가 어떻게 진행되고 어떠한 결론으로 귀결되는지 지켜볼 필요가 있으며, 이는 우리나라에도 시사하는 바가 있을 것이다.

CLOUT Act는 제2 추가의정서와 마찬가지로 개인정보를 제공한 ISP의 면책 조항을 규정하고 있으며, 면책 조항으로 인해 국가 간 분쟁이 발생할 가능성 또한 낮아졌다고 보고 있다. 제2 추가의정서의 문제점으로 지적된 면책 조항이 또 다른 문제점인 국제분쟁 가능성의 해결책이라고 본 것이다. 또한, CLOUD Act는 적법한 요청에 대한 적법한 정보공개에 대해서만 책임을 면제한다고 하여 협약을 위반한 법인의 법적 책임을 규정한 부다페스트 협약 제12조와의 균형도 맞췄다고도 할 수 있다. 우리나라 또한 CLOUD Act와 마찬가지로 적법한 정보공개와 그렇지 않은 정보공개를 구별하여 전자에 대해서만 제2 추가의정서의 면책 조항을 적용하고 후자에 대해선 부다페스트 협약에 따라 처벌하는 방안을 검토할 필요가 있다. 따라서 CLOUD Act는 부다페스트 협약 제2 추가의정서의 법적 책임 문제에 대한 해결책을 제시하였다고 볼 수 있다.

Ⅴ. 나가는 말

디지털증거 역외 압수·압수수색은 수사기관이 해외서버에 있는 증거에 대한 영장을 발부받아 해당 IP에 접속하여 관련 증거를 수집하는 압수·수색 방법을 의미한다, 우리나라는 2022년 10월 11일 역외 압수·압수수색을 위한 부다페스트 협약 가입의향서를 제출하였다. 그러나 이미 2021년 11월 제2 추가의정서가 제정되었으므로, 제2 추가의정서 가입 여부 또한 별도로 논의해야 한다.

제2 추가의정서는 역외 압수·수색의 효율성 확보 및 확장을 위해 타국 정부를 거치지 아니하고 ISP에 직접 정보 제공요청을 하거나 기존 형사사법공조절차 중 일부를 생략할 수 있도록 하는 것을 주된 내용으로 하며, 더 나아가 일부 조항들을 통해 개인정보를 더욱 강력하게 강화하려 하였다. 그러나 제2 추가의정서는 역외 압수·수색의 확장과 개

인정보 보호의 조화를 이루기 위해 노력하였음에도 불구하고 결과적으로 전자만을 강조하게 되었다. 문제점으로 지적된 ① 정보공개 주체의 전환 및 권한의 정당성, ② 쌍방 가벌성 부재, ③ 개념 및 기준의 모호성, ④ 개인정보 보호, ⑤ 실효성 모두 역외 압수·수색의 확장으로부터 서로 연결되었다고 할 수 있다.

우리나라가 제2 추가의정서에 가입하게 되면 역외 압수·수색 관련 국내 법률제도 재검토가 불가피하며, 역외 압수·수색의 명문화, 트래픽 데이터 및 통신사실 확인 자료 제공, 법적 책임 규정 등에 대한 고민이 필요하다. 특히 트래픽 데이터 및 통신사실 확인 자료 제공과 법적 책임 규정은 부다페스트 협약과 제2 추가의정서간 배치되는 부분이 있으므로 양자를 조화롭게 달성할 수 있는 입법·정책적 방안을 모색해야 한다. 그리고 미국의 CLOUD Act는 제2 추가의정서 도입 시 우리나라에 발생할 수 있는 문제들을 미리 보여준 대표적인 사례라고 할 수 있다.

사이버범죄에 적절하게 대처해야 하기 위한 국가 간 상호 협력과 역량 강화가 중요하고 급변하는 ICT 환경에 대응해야 한다는 점을 고려하면, 언젠가는 제2 추가의정서에 가입해야 한다. 그러나 제2 추가의정서의 문제점 및 부다페스트 협약과의 조화에 대한 고민이 선행되어야 한다. 제2 추가의정서가 앞으로 어떻게 발전하는지 지켜보면서 우리나라 실정에 맞는 도입 방안이 마련되길 기대해본다.

참고문헌

[국내 문헌]

가. 단행본

신용우, “유럽 사이버범죄 방지협약 체결 현황과 우리나라 입법·정책적 대응 방향”, 국제관계 동향과 분석 제77호, 국회입법조사처 정기보고서, 2020

나. 논문

박재성, “사이버범죄 국제조약의 동향 - 부다페스트 제2 추가의정서 및 유엔 사이버범죄 조약을 중심으로-”, 저스티스 통권 제185호, 한국법학원, 2021

박희영, “유럽평의회: 전자 증거의 협력 및 공개 강화에 관한 사이버범죄 협약 제2차 추가의정서(CETS No.224)”, 유럽 법제동향, 톰슨로이터코리아, 2023

박희영, “형사소송법 제95a조 도입: 제3자가 보관 중인 증거의 비밀 압수”, 독일 법제동향, 톰슨로이터코리아, 2021

이경렬·박제민. “역외 압수·수색 수사에 관한 한일 최고법원판례 비교연구”, 비교형사법연구 제24권 제3호, 한국비교형사법학회, 2022

이경렬·하건우, “유럽 사이버범죄 협약의 가입·비준을 위한 국내 이행법률의 마련과 준비 비교”, 비교형사법연구 제19권 제4호, 한국비교형사법학회, 2018

이지우·이경렬, “디지털증거 역외 압수·수색에 관한 비교연구”, 비교형사법연구 제24권 제4호, 한국비교형사법학회, 2023

전현욱·이자영, “사이버범죄 협약과 형사절차상 적법절차원칙: 저장된 데이터의 보존 및 일부공개를 중심으로”, 형사정책연구 제25권 제1호, 한국형사법무정책연구원, 2014

정대웅·김기범·권헌영·이상진, “디지털증거 역외 압수·수색에 관한 쟁점과 입법론”, 법조 제65권 제9호, 법조협회, 2016

정명현, “유엔 사이버범죄 대응 국제조약의 논의 동향과 전망”, 국제법 동향과 실무 통권 제62호, 외교부 국제법률국, 2021

정태진, “유럽 사이버범죄 협약과 사이버범죄 대응을 위한 국제공조”, 국제문제연구소 워킹페이퍼 제98호, 서울대학교 국제문제연구소, 2018

정태진·이광민, “사이버범죄 대응을 위한 부다페스트 협약 가입과 국제공조 연구”, 경찰학논총 제14권 제2호, 원광대학교 경찰학연구소, 2019

차진아, “사이버범죄에 대한 실효적 대응과 헌법상 통신의 비밀보장: 사이버범죄 협약 가입에 따른 통신비밀보호법의 개정 방향을 중심으로”, 공법학연구 제14권 제1호, 한국비교공법학회, 2013

다. 판례

대법원 2017.11.29. 선고 2017도9714 판결

[해외 문헌]

가. 단행본

Birgit Sippel & Nuno Melo, “2nd Working Document(B) on the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters”, 유럽의회 정기보고서, 2019

Veridiana Alimonti, “Assessing New Protocol to the Cybercrime Convention in Latin America”, EFF 단행 보고서, 2022

Yanquing Hong, “Game of Laws: Cross-Border Data Access for Law Enforcement Purposes”, Yale Law School Paul Tsai China Center 단행 보고서, 2021

나. 논문

Allison Peters & Amy Jordan, “Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime”, 10 J. Nat'l Security L. & Pol’y 487 (2020)

Christine Galvagna, “The Necessity of Human Rights Legal Protections in Mutual

Legal Assistance Treaty Reform", 9 Notre Dame J. Int'l & Comp. L. 57 (2019)

Courtney Christensen, "Who Decides? Speech and Privacy Risks in the Draft Second Additional Protocol to the Budapest Convention", 52 Geo. J. Int'l L. 1031 (2021)

Markko Künnapu, "Challenges Related to Fight Against Cybercrime. A Need to Strengthen International Cooperation", International Journal of Criminal Justice 제3권 제2호, 한국형사법무정책연구원, 2021

Melissa L. Ken, "The Real Cost of 5G Technology: National Security Implications of 5G Implementation and Impact on the U.S.-China Relationship", 9 Nat'l Sec. L. J. 119 (2022)

Mickellea M. Tennis, "A United Nations Convention on Cybercrime", 48 Cap. U. L. Rev. 189 (2020)

Tim Cochrane, "Hiding in the Eye of the Storm Cloud: How CLOUD Act Agreements Expand U.S. Extraterritoral Investigatory Powers", 32 Duke J. Comp. & Int'l L. 153 (2021)

Vagia Polyzoidu, "Combating the Cybercrime: Thoughts Based on the Second Additional Protocol (Draft) to the Budapest Convention on Cybercrime", EU Internet Law in the Digital Single Market (2021)

다. 판례

Alexander v. Verizon Wireless Services, LLC, No. 16-31227 (5th Cir. 2017)

Benedik v. Slovenia (Application no. 62357/14)

U.S. v. Jones, 565 U.S. 400 (2012)

U.S. v. Microsoft, 138 S. Ct. 1186 (2018)

A Study on the Domestic Legislation for Joining the Second Additional Protocol to the Budapest Convention

Jiwoo Lee* · Kyung-Lyul Lee**

Trans-border access of digital evidence refers to a search and seizure in which investigative agencies obtain warrants for evidence on overseas servers and access the IP to collect related evidence. Korea submitted a letter of intent to join the Budapest Convention on October 11, 2022. However, since the second additional protocol has already been enacted in November 2021, joining the second additional protocol should be discussed separately as well.

In order to secure and expand the efficiency of trans-border access, the second additional protocol was mainly about requesting information directly from ISP without going through other governments or without following some of the existing criminal justice cooperation procedures. Although there were some provisions to strengthen personal information protection, only the expansion of trans-border access was emphasized in the end.

If Korea joins the second additional protocol, revision of domestic legisltion is inevitable. In relations to trans-border access in particular, it is necessary to consider stipulating trans-border access, providing traffic and communication data, and regulating legal responsibility. Among them, the provision of traffic and communication data and legal responsibility regulations contradict the Budapest Convention. Thus, legislative and policy measures should be sought to achieve both in harmony.

Considering that mutual cooperation between countries is important to cope with cybercrime that changes rapidly in ICT environment, joining the second additional

* Ph.D. Student, Department of Law, Graduate School of Sungkyunkwan University
** Professor, Law School of Sungkyunkwan University, Ph.D. in Law

protocol is inevitable. However, concerns about the problems of the second additional protocol in relations to the Budapest Convention must precede. The CLOUD Act has implications for our study in that it also allows investigative agencies to directly request ISP to disclose information like the second additional protocol does. Therefore, implications of U.S. case to Korea will play an important role in solving problems related to trans-border access.

❖ Key words: Trans-border Access, Budapest Convention, Second Additional Protocol, Protection of Personal Information, CLOUD Act

투고일 : 8월 30일 / 심사일 : 9월 22일 / 게재확정일 : 9월 30일