형사정책연구 Korean Criminological Review
제29권 제2호(통권 제114호, 2018・여름)

미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점

송영진*

국 | 문 | 요 | 약

최근 미국 의회는 2018년 종합세출법안(omnibus appropriations bill)을 통과시켰고, 도날드 트럼프 대통령은 2018년 3월 23일 동 법안에 서명하였다. 총2,000페이지가 넘는 방대한 양의 동 법안에는 "합법적인 해외 데이터 활용의 명확화를 위한 법률(Clarifying Lawful Overseas Use of Data Act, 이하 CLOUD Act)"이 포함되어 있다. 동 법률에서는 미국의 통신서비스제공자들이 보유 또는 관리하고 있는 통신 내용, 트래픽 데이터, 가입자 정보 등에 대해서 정부기관이 실제 데이터가 저장된 위치에 관계없이 제공 요청을 할 수 있도록 명시함으로써 역외 데이터에의 접근에 대한 법률적 근거를 마련하고 있다. 또한 CLOUD Act에서는 기존 국제형사사법공조 절차에 대한 대안으로써 해외 정부기관이 미국과 행정협정(executive agreement)을 체결할 경우 해당 해외 정부기관이 미국 기업에 직접 데이터를 요청할 수 있도록 규정하고 있다.

미국의 CLOUD Act는 그간 논란이 되어 온 역외 데이터에의 접근에 대해서 기존 법률에 "데이터의 위치와 관계없이" 라는 문구를 삽입하여 명쾌한 해답을 내놓았다는 점, 그리고 대부분의 수사기관에서 문제점으로 인식해 온 MLAT의 비효율성을 해결할 수 있는 대안을 제시했다는 점에서 높이 평가할만한 입법이라고 하겠다.

우리나라도 최근 5년간 수사기관에서 직접 미국의 서비스제공자를 대상으로 영장을 집행하는 사례가 증가하고 있으며 우리나라 수사기관이 미국 서비스 제공자로부터 조금 더 효율적이고 신속하게 콘텐츠 데이터를 제공받기 위해서는 미국 정부와 행정협정을 체결하는 방안을 적극적으로 검토해 볼 필요가 있다. 이를 위해서는 사이버범죄 및 디지털 증거와 관련하여 국제 기준에 맞는 실체법 및 절차법적 정비가 필요하며, 데이터를 수집, 보유, 활용, 공유하는 법적 절차, 그리고 이를 통제하기 위한 법적 장치가 마련되어 있어야 한다.

❖ 주제어 : CLOUD Act, 저장통신법, 초국경적 데이터 접근, 역외 적용, 국제형사사법공조, 사이버범죄, 디지털증거

* 경찰대학 국제사이버범죄연구센터 선임연구원, 서울대학교 법과대학 박사과정

Ⅰ. 서론

정보통신 기술의 발달로 클라우드 컴퓨팅(cloud computing)[1] 서비스가 보편화되고 있다. 클라우드 컴퓨팅의 기술적 특성상 데이터가 여러 지역의 서버에 분산되어 저장되기 때문에 데이터가 실제 저장되어 있는 위치를 알 수 없게 되는 "위치의 부재(loss of location)" 또는 "위치의 부지(不知)(loss of knowledge of location)"현상이 발생하고 있다[2].

또한 범죄자들의 소셜 네트워크 서비스 및 글로벌 기업의 이메일 서비스 이용이 증가하면서 각국 경찰에서는 관련 데이터의 소재지 국가에 공조를 요청하기 보다는 글로벌 기업, 즉 주로 미국에 본사를 둔 구글(Google), 페이스북(Facebook), 마이크로소프트(Microsoft) 등과 같은 통신서비스 제공자에게 직접 데이터 제공을 요청하고 있다[3]. 이러한 요청이 급증하자 미국의 기업들은 법집행기관을 위한 온라인 요청 채널을 운영하고 있고 데이터 요청에 대한 가이드라인을 제공하고 있다[4].

이렇듯 일국의 법집행기관이 국제형사사법공조를 거치지 않고 일방적으로 역외에 위치한 데이터에 접근하는 것은 최근 수사실무에서 보편적으로 일어나고 있는 현상이고 이러한 행위의 적법성에 대하여 각 국가마다 그 실행이 다르게 나타나고 있다[5]. 또한 이러한 현상에 대하여 국제법상 영토 주권의 침해와 개인의 프라이버

1) 클라우드 컴퓨팅(cloud computing)이란, 인터넷 기술을 활용하여 가상화된 정보 기술(IT) 자원을 서비스로 제공하는 컴퓨팅. 사용자는 IT 자원(소프트웨어, 스토리지, 서버, 네트워크 등)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼 비용을 지불하는 컴퓨팅을 말한다. 한국정보통신기술협회, 정보통신용어사전 http://word.tta.or.kr/index.jsp (최종접속일: 2018. 5. 30.)

2) Cybercrime Convention Committee (T-CY), Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Council of Europe, 2016, pp.15-17.

3) 한국 경찰의 경우에도 2014년부터 이미 기업별 정보 제공 요청 절차를 매뉴얼로 제작하여 수사에 활용하고 있으며 2017년 2차 개정 매뉴얼을 발간하여 배포한 바 있다. 경찰청 사이버안전국, 글로벌 인터넷 기업을 활용한 국제공조수사 매뉴얼(경찰청 내부자료), 2017.

4) 페이스북의 경우 온라인 요청 채널 및 가이드라인은 각각 다음의 웹사이트에서 제공하고 있다.
- 법집행기관 온라인 요청 채널 : https://www.facebook.com/records/login/ (최종접속일: 2018. 5. 30.)
- 법집행기관 가이드라인 : https://www.facebook.com/safety/groups/law/guidelines (최종접속일: 2018. 5. 30.)

5) 이러한 수사실무 사례와 법적 쟁점을 분석한 논문으로는, 전현욱 외, "사이버범죄의 수사 효율성 강화를 위한 법제 개선 방안 연구," 경제·인문사회연구회 미래사회 합동연구총서 15-17-01, 경제·

시 침해 우려 역시 제기되고 있다[6].

최근 미국 의회는 2018년 종합세출법안(omnibus appropriations bill)을 통과시켰고, 도날드 트럼프 대통령은 2018년 3월 23일 동 법안에 서명하였다[7]. 총2,000페이지가 넘는 방대한 양의 동 법안에는 "합법적인 해외 데이터 활용의 명확화를 위한 법률(Clarifying Lawful Overseas Use of Data Act, 이하 CLOUD Act)"이 포함되어 있다[8]. 동 법률에서는 미국의 통신서비스제공자들이 보유 또는 관리하고 있는 통신 내용, 트래픽 데이터, 가입자 정보 등에 대해서 정부기관이 실제 데이터가 저장된 위치에 관계없이 제공 요청을 할 수 있도록 명시함으로써 역외 데이터에의 접근에 대한 법률적 근거를 마련하고 있다[9]. 또한 CLOUD Act에서는 기존 국제형사사법공조 절차에 대한 대안으로써 해외 정부기관이 미국과 행정협정(executive agreement)을 체결할 경우, 양국이 이에 근거하여 자유롭게 광범위한 데이터를 상호 공유할 수 있도록 규정하고 있다.

본 논문에서는 우선 CLOUD Act의 결정적인 입법배경이 된 Microsoft 사건과 CLOUD Act의 주요 내용을 살펴보고, 이러한 미국의 CLOUD Act의 통과가 역외 데이터에의 접근과 관련하여 법집행기관에 주는 시사점을 도출하고자 한다.

인문사회연구회, 2015, pp.169-176 참조. 이외에도 수사기관의 일방적인 역외 데이터 접근에 대한 유형과 그 법적 평가에 대해서는, 정소연, 디지털 증거의 역외 압수수색에 대한 법적 고찰, 디지털 포렌식 연구 제11권 제1호(제17호), 2017 참조.

6) Walden, Ian. "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent." Queen Mary School of Law Legal Studies Research Paper No. 74/2011, 2011, p. 1. 이인곤, 강철하, 클라우드컴퓨팅 환경에서 전자정보 압수수색의 문제점과 개선방향, 형사법의 신동향 통권 제54호, 2017, pp. 345-347.

7) Laura Huatala, CLOUD Act Becomes Law, Increased Government Access to Online Info, CNET (Mar. 23, 2018), https://www.cnet.com/news/cloud-act-becomes-law-increases-government-access-to-email-internet-microsoft/. (최종접속일: 2018. 5. 30.)

8) 동 법안의 전체 텍스트는 미국 의회 홈페이지에서 찾아볼 수 있다. https://www.congress.gov/bill/115th-congress/house-bill/4943 (최종접속일: 2018. 5. 30.)

9) CLOUD Act 이전에도 오린 해치(Orrin Hatch) 상원 의원이 주도한 의회는 SCA를 개정하여 해외에 저장된 데이터에 접근할 수 있는 법적 근거의 마련을 시도한 적이 있다. 2015년 "해외에 저장된 데이터에 대한 법집행기관의 접근에 관한 법률(Law Enforcement Access to Data Stored Abroad Act, LEADS Act)"과 2017년 "국제 통신 프라이버시 법(International Communications Privacy Act, ICPA)"은 모두 SCA를 개정하기 위한 법안이었으나 의회에서 통과되지는 못했다.

Ⅱ. 입법배경 : 저장통신법과 Microsoft 사건

1. 저장통신법(Stored Communications Act)

저장통신법(Stored Communications Act, "저장통신법")는 미국 연방법전 제18장 제2701조 내지 제2712조의 규정을 통칭하는 법으로, 1986년 전기통신 프라이버시법(Electronic Communications Privacy Act, ECPA)의 한 부분으로 제정되었다[10]. 동 법률은 컴퓨터네트워크 서비스 제공자의 고객 및 가입자의 법적 프라이버시 권리에 대하여 규정하고 있다[11]. 저장통신법 제2703조는 법집행기관들이 네트워크 서비스 제공자들로부터 저장된 통신 데이터의 공개를 강제할 때 반드시 따라야 하는 형사절차적 규정을 포함하고 있다. 또한 제2702조에서는 정부와 비정부단체에 대한 네트워크 서비스 제공자의 자발적인 데이터 공개에 관한 사항들을 다루고 있다[12].

여기에서는 이하에서 살펴볼 마이크로소프트 사건의 쟁점이자 CLOUD Act의 입법 배경이 된 미국 저장통신법 제2703조의 내용을 살펴보고자 한다. 저장통신법 제2703조에 의하여 수사기관이 취득할 수 있는 정보는 콘텐츠 정보, 로그기록 등 가입자와 관련된 비내용 정보, 그리고 제2703조(c)(2)[13]에 구체적으로 명시된 가입자 정보 및 세션정보 등 세 가지로 나누어 볼 수 있다. 또한 제2703조에서는 "정부기관(government entity)[14]"이 제공자에게 저장된 전자통신의 내용, 그리고 계정 기록과

10) Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," George Washington Law Review, Vol. 72, No. 6, 2004, p.1. 최성진, 수사기관의 전자우편 압수수색의 한계에 관한 연구 - 미국의 판례 및 법제도를 중심으로 -, 홍익법학 제11권 제2호, 2010, pp.141-142.

11) U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual (2009), p.115.

12) 일례로, 콘텐츠 정보의 경우 사람의 생명·신체에 급박한 위험이 있다고 생각되는 경우, 아동보호 등을 위한 경우에 공개될 수 있다. 18 U.S.C. § 2702(b)(6), § 2702(b)(8).

13) 제2703조(c)(2)에서는 기본 가입자정보 및 세션정보의 범주를 다음과 같이 제시하고 있다.
(A) 이름; (B) 주소; (C) 지역 내 전화와 장거리 전화 연결 기록, 또는 세션 시각과 지속시간 기록; (D) 서비스 사용기간의 길이(시작일자 포함)와 이용한 서비스의 종류; (E) 전화번호 및 기타 기기번호 또는 임시적으로 배정된 모든 네트워크 주소를 포함한 기타 가입자번호 또는 신원; 그리고 (F) 그러한 서비스에 대한 이용료 지불수단 및 지불원천

기본 가입자정보 및 세션정보와 같은 각각의 정보 공개를 강제하기 위해 밟아야 하는 절차를 규정하고 있다[15].

제2703조에서는 정부기관이 제공자에게 특정 정보의 공개를 강제하는 데 사용할 수 있는 다섯 가지 방법을 제시하고 있다. 이 다섯 가지 방법은 1) 제출명령(subpoena), 2) 가입자에 대한 사전통지 후 제출명령, 3) § 2703(d)에 따른 법원 명령(court order), 4) 가입자에 대한 사전통지 후 § 2703(d)에 따른 법원 명령; 그리고 5) 수색 영장(search warrant)이 그것이다[16]. 제출명령(subpoena)은 가장 법적 요건이 약하며 발부절차가 간소한 증거 수집 절차로[17], 정부기관은 제출명령을 통해 기본 가입자정보 및 세션정보의 공개를 강제할 수 있다.[18] 또한 정부기관은 제2703조(d)에 따른 법원 명령을 통해서 가입자정보 외에도 계정의 로그나 거래기록을 수집할 수 있다. 정부기관이 법원으로부터 수색 영장을 발부받은 경우, 전기통신서비스의 '전자적 저장공간'의 콘텐츠 중 180일 이내의 콘텐츠 데이터를 포함하여 가입자정보 및 로그기록 등 가장 광범위한 데이터의 공개를 강제할 수 있다[19]. 수색영장 집행에 있어 특이할만한 점은 미국 연방법 제3105조에서는 일반적인 영장 집행 시에 법집행관이 영장집행 장소에 반드시 임장할 것을 규정[20]하고 있으나, 저장통신법 제2703조(g)에서는 이 법에 따른 영장 집행 시에는 법집행관의 임장이 요구되지

14) 18 U.S.C § 2711
(4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.

15) U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual (2009), p.127.

16) U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual (2009), p.127.

17) 최성진, 수사기관의 전자우편 압수수색의 한계에 관한 연구 - 미국의 판례 및 법제도를 중심으로 -, 홍익법학 제11권 제2호, 2010, pp.147-148.

18) 18 U.S.C. § 2703(c)(2).

19) 18 U.S.C. § 2703(a).

20) 18 U.S. Code § 3105 - Persons authorized to serve search warrant
A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution.

않는다고 명시적으로 규정하고 있다는 점이다[21].

2. United States v. Microsoft Corp. 사건

2013년 12월 미국 연방정부는 마약밀매 사건과 연관이 있는 이메일 계정에 대해 뉴욕남부지방법원으로부터 수색 영장을 발부받아 마이크로소프트를 상대로 해당 이메일 계정의 내용을 포함한 관련 정보를 제출할 것을 요청하였다. 그러나 마이크로소프트는 미국 내 서버에 저장되어 있는 일부 정보만을 제출하였고, 내용 데이터의 경우 데이터가 아일랜드 더블린에 위치한 데이터 센터에 저장되어 있다는 이유로 정보 제출을 거부하였다. 이에 2014년 4월 25일 뉴욕남부지방법원 치안판사는 마이크로소프트가 미국에서 사업을 수행하고 있으며, 아일랜드 서버에 접근권한을 가진 미국 법인이라는 점을 근거로 마이크로소프트가 수색 영장 집행에 응해야 한다고 판시[22]하였으나, 마이크로소프트는 이에 항소하였다.

이 사건의 주된 쟁점은 미국 법집행기관이 마이크로소프트에게 미국 외에 위치한 서버에 저장된 통신 내용 정보를 제출하도록 한 저장통신법상 영장의 집행이 법률의 역외 적용에 해당하는지 여부이다. 이 쟁점을 분석하기 위해서 항소법원은 역외적용 추정 금지의 원칙(Presumption against Extraterritoriality)의 위반 여부를 검토하였다. "역외적용 추정 금지의 원칙"이란, 역외적용에 대한 입법기관의 의사가 법률에 명시적이고 분명하게 나타나 있지 않은 한, 해당 국내법은 역외적용 되어서는 안 된다는 원칙[23]이다.

---

21) 18 U.S.C. § 2703 (g) Presence of Officer Not Required.—
Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

22) In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, No. 13 Mag. 2814, 2014 WL 1661004 (S.D.N.Y. Apr. 25, 2014).

23) 연방대법원은 미국 증권거래법(Securities Exchange Act)의 역외적용과 관련된 사건에서 역외적용 추정 금지의 원칙을 처음 명시적으로 언급하였다. Morrison et al. v. National Australia Bank Ltd. et al., 561 U.S. 247 (2010)(이하 "Morrison 사건"), p.13. 백범석, 김유리,

연방대법원은 Morrison 사건에서 특정 법률의 역외 적용 여부를 분석하기 위한 2단계의 기준을 발전시켜왔다. 법원은 우선 역외적용 추정 금지의 원칙이 반증될 (rebuttable) 수 있는지 여부 즉, 해당 법률이 역외적으로 적용된다는 명시적 규정이 있는지 여부를 판단하여야 한다[24]. 그 다음으로 법원은 사건이 법률의 국내적 적용과 관련되는지 여부를 판단해야 하며 이를 판단하기 위해서 법원은 해당 법률의 주된 보호법익(focus)이 무엇인지 그러한 보호법익과 관련 있는 행위가 어디에서 일어났는지를 파악해야 한다[25].

결론적으로 2016년 7월 미국 제2순회항소법원은 마이크로소프트 사건에서 국내 서비스 제공자에게 미국 밖에 저장된 정보를 공개하도록 요구하는 저장통신법상 영장을 집행하는 것은 법률의 역외 적용에 해당한다고 판시하였다[26][27]. 첫 번째 단계에서, 항소법원은 입법 당시 의회가 저장통신법에 따라 발부된 영장이 역외 적용될 것을 의도하지 않았다고 보았다[28]. 두 번째 단계에서 항소법원은 저장통신법의 제2703조(a) 조항의 초점은 "사용자의 저장된 통신 내용의 프라이버시를 보호"하는데 있다고 보았고 이와 관련된 행위는 사용자의 프라이버시에 대한 서비스 제공자의 침해이며, 이러한 행위는 영장에 의해 마이크로소프트가 정부의 대리인으로써 사용자의 보호된 콘텐츠를 압수하는 경우에 발생된다고 보았다.

또한 항소법원은 영장의 대상인 내용이 아일랜드 더블린(Dublin) 소재 데이터센터에 저장되어 있었고 해당 데이터센터에서 압수되었기 때문에 법률의 초점과 관련된 행위가 미국 밖에서 일어난 것이라고 판단하였다. 따라서 그러한 영장의 집행은 법률의 불법적인 역외 적용에 해당한다고 판시하였다[29].

[판례평석] 미연방대법원 Kiobel 판결의 국제인권법적 검토, 국제법학회논총 제58권 제3호, 2013, pp.256-257에서 재인용.

24) Dodge, William S. "The Presumption Against Extraterritoriality in Two Steps." AJIL Unbound, Vol. 110, 2016, p.45.

25) Dodge, William S. "The Presumption Against Extraterritoriality in Two Steps." AJIL Unbound, Vol. 110, 2016, p.46.

26) Microsoft v. United States, No. 14-2985 (2d Cir. 2016).

27) In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., Case No. 14-2985 (2d Circuit July 14, 2016).

28) In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., Case No. 14-2985 (2d Circuit July 14, 2016).

이에 법무부는 항소법원의 결정에 불복하여 상고하였고 동시에 이 사건이 연방대법원에 계류 중일 당시, 저장통신법을 개정하는 법안을 제출하였다[30]. 2018년 법무부가 제안한 역외 적용 조항이 포함된 CLOUD Act가 양원에 상정되었다. 이후 동 법안이 2018년 통합세출법안에 포함되어 국회를 통과하였고 최종적으로 대통령이 동 법안에 서명하였다.

이에 법무부는 CLOUD Act를 근거로 새로운 영장을 발부받아 마이크로소프트에 집행하였고, 미국 정부와 마이크로소프트 양 당사자는 새로운 영장이 기존의 영장을 대체하였다는 점에 동의하였다[31]. 결국 연방대법원에서는 동 사건이 더 이상 소의 이익이 없다(moot)고 판단하고 하급심 법원의 결정을 파기하고 기각 결정을 하였다[32].

Ⅲ. CLOUD Act의 주요 내용

CLOUD Act 제102조에 따르면, 동 법의 역외적용 규정 신설의 목적 중 하나는 법집행기관의 수사에 대한 장벽을 없애는 것이다. CLOUD Act의 전문에서도 동 법의 입법 취지에 대해서 설시하면서, 테러리즘을 포함한 심각한 범죄에 대응하기 위해서는 통신서비스제공자가 보유하고 있는 데이터에 적시에 접근하는 것이 필요하며, 그간 이러한 데이터가 해외에 저장된 경우에는 데이터에 대한 접근이 어려웠다

29) 이와는 대조적으로 미국 연방수사국(FBI)가 구글(google)을 상대로 저장통신법 제2703조에 따른 영장을 발부받아 집행한 사건에서 구글 역시 해당 데이터가 아일랜드에 저장되어 있다는 이유로 정보 제공을 거부하였는데, 펜실베니아 동부 지방법원은 구글에게 해외에 저장된 데이터를 제공하도록 요구하는 SCA 영장의 집행이 적법하다고 판시하였다. 법원은 제2703조의 초점은 서비스 제공자가 전자통신 및 기타 가입자정보를 정부에 공개하는 것이며, 영장을 집행하는 모든 절차가 국내에서 이루어진다고 보았다. 즉 저장된 통신에 접근하는 법적 위치는 데이터센터의 물리적 위치가 아니라 서비스 제공자가 전자적으로 해당 데이터에 접근할 수 있는 위치라고 이해하는 것이 더 바람직하다고 판단하였다. In re Search Warrant No. 16-960-M-01 to Google, 232 F.Supp.3d 708 (E.D.Pa. 2017).

30) Mulligan, Stephen P. “Cross-Border Data Sharing Under the CLOUD Act,” Congressional Research Service Report, 2018, p. 7.

31) Mulligan, Stephen P. “Cross-Border Data Sharing Under the CLOUD Act,” Congressional Research Service Report, 2018, p. 8.

32) United States v. Microsoft Corp., No. 17-2, 584 U.S. ___ (2018).

는 점을 인정하고 있다.

또한 외국 정부에서도 미국의 통신서비스제공자가 보유한 데이터에 대한 접근 요청이 증가하고 있고 통신 내용과 같이 미국 법률이 해당 데이터의 공개를 금지하는 경우 서비스제공자들의 입장에서는 법적 의무가 충돌할 수 있는 문제가 발생하였다. CLOUD Act 전문에서는 이러한 문제를 해결하기 위하여 미국과 외국 정부가 프라이버시 및 기본권 보호에 대한 상호 존중을 바탕으로 국제 협정을 체결하는 것이 하나의 대안으로 작용할 것이라는 점을 언급하고 있다.

1. 역외적용의 명시적 근거 마련

CLOUD Act 이전의 저장통신법에는 정부가 서비스제공자에게 미국 밖에 저장된 데이터의 제출을 요구할 수 있는지 여부와 그 상황에 대한 명시적 규정을 두고 있지 않았다. 그로 인해 위에서 살펴본 Microsoft 사건에서와 같이 미국에 본사를 둔 기업이 미국 밖에 저장하고 있는 데이터에 대한 접근 가능성 여부 등이 논란이 되었고 미국 의회는 CLOUD Act를 통해 저장통신법 제2713조를 신설하여 이를 입법적으로 해결하였다. 즉 제2713조에 "서비스제공자는 해당 통신, 기록 또는 기타 정보가 미국 내 또는 미국 밖에 저장되어 있는지 여부와 관계없이 해당 제공자가 보유, 보관 또는 통제하고 있는 유선 또는 전자통신의 내용 및 기타 기록 또는 고객 또는 가입자의 정보를 보존, 백업(backup), 또는 공개할 법적 의무를 준수하여야 한다[33]."라고 규정함으로써, 저장통신법이 역외적으로 적용된다는 점을 분명히 하였다.

최근 유럽평의회(Council of Europe)의 사이버범죄협약 위원회(Cybercrime Convention Committee, T-CY)에서도 클라우드 내 증거에 대한 초국경적 접근 문제에 대하여 연구하였고 이러한 문제의 해결방안 중 하나로써 제출명령(production

33) § 2713. Required preservation and disclosure of communications and records
"A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

order)에 관한 사이버범죄협약(Convention on Cybercrime) 제18조 해설서(guidance note)를 발표하였다[34]. 사이버범죄협약 제18조 제1항 b호에서는 당사국은 자국 영토 내에서 서비스를 제공하는 서비스제공자에게 서비스제공자가 보유 또는 관리하고 있는 가입자정보를 제출하도록 명령할 권한을 부여하여야 한다고 규정하고 있다[35]. 동 조문과 관련하여 해설서에서는 CLOUD Act의 입법취지와 같은 맥락에서 당사국은 자국 영토 내에 서비스 제공자가 법적으로 또는 물리적으로 소재하지 않는 경우에도 동 조항을 적용할 수 있다고 해석하고 있다[36]. 즉 데이터는 여러 관할권에 걸쳐 저장되어 있을 수도 있고 여러 관할권을 이동할 수도 있기 때문에, 데이터의 위치가 관할 성립을 결정짓는 요소는 아니라고 언급하면서 데이터가 서비스제공자의 보유 또는 관리 하에 있는 한, 가입자정보가 타국 관할 내에 저장되어 있다고 하더라도 제18조를 적용할 수 있다고 보고 있다[37].

---

34) Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10 - Production orders for subscriber information(Article 18 Budapest Convention), T-CY(2015)16, 1 March 2017.

35) 제18조(제출명령) 1. 각 당사국은,
   a. 어떤 자가 자국의 영토 내에서 컴퓨터 시스템 또는 컴퓨터 데이터 저장매체에 저장되어 있는 특정 컴퓨터를 보유하고 있거나 관리하고 있는 경우 이를 제출하고,
   b. 서비스제공자가 당사국의 영토 내에서 보유하고 있거나 관리하고 있는 자신의 서비스와 관련한 가입자정보를 제출하도록 명령할 권한을 관할 기관에게 부여하도록 필요한 입법조치 및 그 밖의 조치를 취하여야 한다.
   2. 동 조에 의한 권한과 절차는 제14조 및 제15조를 기초로 하여야 한다.
   3. 동 조에서 의미하는 가입자정보란 서비스 제공자가 보유하고 있는 서비스 이용자에 관한 정보 중 트래픽데이터 또는 콘텐츠 데이터를 제외한 컴퓨터 데이터의 형태로 되어 있거나 기타 다른 형태로 되어 있는 모든 정보로서 다음을 확인할 수 있는 정보를 말한다.
   a. 이용 중인 통신 서비스의 종류, 이 통신서비스를 위해서 행해진 기술적 조치 및 서비스의 이용기간;
   b. 가입자의 신원, 주소, 전화번호 및 그 밖의 접속번호, 통신서비스와 관련한 계약이나 협정에 근거해서 이용될 수 있는 요금의 청구 및 지급에 관한 정보;
   c. 서비스 계약 또는 협정에 근거한 통신기기 설치 장소에 관한 그 밖의 정보.

36) Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10 - Production orders for subscriber information(Article 18 Budapest Convention), T-CY(2015)16, 1 March 2017, p.6.

37) Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10 - Production orders for subscriber information(Article 18 Budapest Convention), T-CY(2015)16, 1 March 2017, p.7.

2. 서비스제공자의 영장 각하신청 제도 신설

CLOUD Act는 저장통신법의 제2703조를 개정하여 서비스 제공자가 저장통신법 영장에 대해서 사전에 법원을 상대로 이를 각하 또는 변경해줄 것을 청구할 수 있는 메커니즘을 제공하고 있다[38]. 이러한 메커니즘은 예양(comity)을 근거로 이루어지는데 이러한 예양에 대한 분석(comity analysis)은 커먼로(common law)에 그 기원을 두고 있으며, 국내법과 외국법 간의 충돌이 발생한 경우 법원으로 하여금 미국과 해외 정부의 관련 이해관계를 검토하도록 하는 절차이다[39].

저장통신법 영장이 아닌 일반 수색영장의 경우, 영장집행의 대상자 즉, 피압수자는 영장이 무엇을 압수수색하기 위함인지 대부분 알기가 어렵고, 영장은 일반적으로 영장에 기재된 항목을 압수하는 법집행관에 의해 집행된다. 그러나 저장통신법 영장의 경우, 통상 법집행기관이 이메일이나 온라인으로 영장을 제시하면 서비스제공자가 영장에 기재된 범위의 데이터를 제공해주는 형태로 집행된다. 제출 명령(subpoena)의 경우 집행되기 전에 이에 대해 이의를 제기할 수 있는 법적 절차가 정립되어 있지만, 영장의 경우에는 그러한 절차가 마련되어 있지 않았기 때문에 전통적으로, 서비스제공자들이 영장에 이의를 제기하는 유일한 방법은 영장의 집행을 거부하고 소송을 제기하는 것이었다.

이러한 문제를 해결하기 위해 CLOUD Act는 전자통신서비스 제공자가 가입자 또는 고객의 통신 내용을 공개하라는 요구를 받은 경우에, "가입자 또는 고객이 미국인이 아니며 미국 내에 거주하지 않고 그러한 공개로 인해 서비스제공자가 자격 있는 외국정부(qualifying foreign government)의 법률을 위반할 중대한 위험을 발생시킬 것이라고 합리적으로 믿는 경우"에는 영장을 변경 또는 각하(quash)해 줄 것을 법원에 청구할 수 있도록 법적 근거를 마련하였다[40]. 또한 그러한 청구는 정보공개 요구를 받은 날로부터 14일 이내에 이루어져야 한다.

이러한 청구를 받은 법원은 영장을 집행한 정부기관에 이에 대응할 기회를 주어

38) CLOUD Act, H.R. 1625, 115th Cong. div. V, § 103(b) (2018) (18 U.S.C. § 2703(h)).

39) Jennifer Daskal, *Microsoft Ireland*, the CLOUD Act, and International Lawmaking 2.0, Stanford Law Review Online, Vol. 71, 2018, p.11.

40) 18 U.S.C. § 2703(h)(2)(A).

야 한다. 법원은 "정보의 공개로 인해 서비스제공자가 자격 있는 외국 정부의 법을 위반할 소지가 있는 경우, 모든 정황을 종합해 보았을 때 사법정의에 따라 그러한 영장이 변경되거나 기각되어야 한다고 판단되는 경우[41], 그리고 고객 또는 가입자가 미국인이 아니고 미국 내에 거주하지 않는 경우"에는 영장을 변경하거나 각하할 수 있다[42].

즉 CLOUD Act는 미국 정부에 의해 발부된 영장의 집행이 외국의 법률을 위반할 소지가 있는 경우, 그리고 대상자가 미국인이 아닌 경우에는 서비스제공자가 영장 각하 또는 변경 청구를 할 수 있는 장치를 두어 서비스제공자가 우려하는 외국 법률과의 충돌 문제를 사전에 예방하고자 하였다.

3. 외국 정부와의 행정협정 체결을 통한 정보제공절차 마련

CLOUD Act는 저장통신법에 제2523조를 신설하여 초국경적 정보 제공요청을 위한 미국과 외국 정부 간의 행정 협정(executive agreement)에 대한 규정을 마련하고 있다[43]. 제2523조는 미국의 전자 통신 서비스 제공자가 저장통신법을 위반하지 않고 행정협정에 따라 외국 정부의 정보 제공요청에 응할 수 있도록 법적 근거를 제공하고 있다.

제2523조는 특정 외국 정부의 국내법 및 그 실행이 데이터 수집과 관련하여 프라이버시 및 자유권을 실체적·절차적으로 강력하게 보장하는 등 법률에서 정한 요건을 충족하는 경우, 미국 법무장관에게 해당 정부와 행정 협정을 체결할 수 있는 권한을 부여하고 있다[44].

---

41) 특히 이 경우를 판단할 때 법률에서는 법원이 고려해야 사항을 규정하고 있는데, 여기에는 미국의 이익, 자격 있는 외국 정부의 이익, 고객 또는 가입자의 위치와 국적, 서비스제공자의 미국과의 연관성의 정도와 그 성격, 수사의 중요성 등이 포함된다. 18 U.S.C. § 2703(h)(3).

42) 18 U.S.C. § 2703(h)(2)(B).

43) CLOUD Act § 105(a) (18 U.S.C. § 2523 신설).

44) 특히, 제2523조는 법무장관이 특정 외국 정부와의 행정협정 체결 여부를 판단 할 때 고려해야 할 사항 6가지를 다음과 같이 제시하고 있다.
- 외국 정부가 유럽평의회의 사이버범죄협약 당사국이거나 사이버범죄협약상의 규정이 국내법과 일치하는 경우와 같이 외국정부가 사이버범죄 및 전자증거에 관한 적절한 실체법과 절차법을

만약 외국 정부가 이러한 요건을 충족시킨다면, 미국과 외국 정부 사이에 체결된 행정 협정은 상호 정보 공유를 허용하고, 이에 따라 미국과 다른 외국 국가들이 해외에 저장된 데이터에 접근하는 것을 허용하게 된다.

그러나 제2523조에서는 외국 정부가 접근할 수 있는 데이터의 범위에 대한 제한 규정을 두고 있다. 예를 들어, 제2523조에서는 외국 정부가 "의도적으로 미국인이나 미국 내에 거주하는 사람을 대상으로 하는 것"을 금지하고 있다. 또한 외국 정부는 미국인이나 미국 내에 거주하는 사람과 관련된 정보를 획득하기 위한 목적으로 미국 밖에 위치한 비(非) 미국인을 대상으로 명령을 발부해서는 안 되며, 외국 정부에 의해 발부된 명령은 테러리즘을 포함한 중범죄의 예방, 탐지, 수사, 기소와 관련한 정보를 획득할 목적이 있어야 하고 특정 개인, 계정, 주소 등 개인을 식별할 수 있는 표지를 명확히 특정하여야 한다. 외국 정부에 의해 발부된 명령은 표현의 자유를 침해하기 위해 이용되어서는 안 된다.

또한 CLOUD Act는 통신에 대한 불법 감청 또는 공개를 금지하는 저장통신법 제2511조를 개정하여 제2511조 (2)항 (j)호를 신설하였다. 제2511조 (2)항에서는 불법감청에 대한 각종 예외규정을 나열하고 있는데, CLOUD Act는 (j)호에 전자통신서비스 제공자가 제2523조에 따라 미국과 행정협정을 체결한 외국 정부의 명령에 따라 유선 또는 전자 통신의 내용을 감청하거나 공개하는 것은 동 법에 따라 '위법하지 않다(not be unlawful)'고 명시적으로 규정[45]하고 있다.

가진 경우;

- 법치와 차별금지원칙에 대한 존중을 나타내는 경우;
- 적용가능한 국제인권법상 의무 및 약속을 준수하거나, 자의적이고 불법적인 프라이버시 침해로부터 보호, 공정한 재판을 받을 권리, 표현의 자유, 집회시위의 자유, 자의적인 체포 및 구금 금지, 고문 및 잔인한, 비인도적 대우 또는 처벌 금지 등을 포함한 국제 보편적 인권의 존중을 나타내는 경우;
- 외국 정부기관이 데이터를 수집, 보유, 활용, 공유하는 절차 및 그러한 활동의 효과적 통제를 포함한 분명한 법적 권한 및 절차를 갖춘 경우;
- 데이터의 수집 및 활용과 관련하여 책임성 및 적절한 투명성을 제공하는 충분한 메커니즘을 갖춘 경우;
- 세계적인 정보의 자유로운 이동과 인터넷의 공개되고 분산되고 상호연결된 특성을 촉진하고 보호하겠다는 의지를 나타내는 경우

45) (j) It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject

CLOUD Act에 의해 승인된 행정협정은 기존의 국제 데이터 공유 방법을 보완하는 것이지 대체하는 것이 아니다[46]. 따라서 공조 요청은 여전히 기존의 국제형사사법공조 조약(Mutual Legal Assistance Treaty, 이하 “MLAT”) 등의 절차를 통해 가능할 것이다.

미국 정부와 CLOUD Act 협정을 체결한 국가는 “중대한 범죄”가 있는 경우, 그리고 해당 요청이 미국인이나 미국 내 거주자를 대상으로 하지 않는 한, 그리고 위에서 언급한 CLOUD Act에서 규정하고 있는 특정 요건을 충족할 경우에 미국 서비스 제공 업체로부터 직접 데이터를 요청할 수 있다. 미국과 MLAT이 체결되어 있지만 CLOUD Act 협정이 체결되어 있지 않은 국가의 경우 또는 CLOUD Act의 범위를 벗어나는 데이터 요청의 경우에 외국 정부는 기존의 MLAT 프로세스를 활용할 수 있다[47].

Ⅳ. 역외 데이터 접근에 대한 시사점

이상에서는 미국의 CLOUD Act의 입법 배경과 주요 내용을 살펴보았다. 여기에서는 CLOUD Act가 법집행기관에게 주는 시사점과 다른 국내법 및 국제법 등 법률과의 충돌 가능성에 대해서 검토하고자 한다.

1. MLAT에 대한 보완책 : 새로운 형태의 데이터 공유 메커니즘

미국에 본사를 둔 IT 기업들이 세계 전자통신의 대다수를 자사의 서버에 보유하고 있기 때문에 각국의 법집행기관이 미국의 통신서비스제공자에게 요청하는 데이

---

to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

46) Mulligan, Stephen P. “Cross-Border Data Sharing Under the CLOUD Act,” Congressional Research Service Report, 2018, p. 23.

47) Mulligan, Stephen P. “Cross-Border Data Sharing Under the CLOUD Act,” Congressional Research Service Report, 2018, p. 23.

터는 상당하고 데이터 제공 요청 건수도 해마다 증가하고 있다[48].

2014년 12월 채택된 유럽평의회(Council of Europe)의 국제사법공조에 대한 이행평가 보고서[49]에 따르면, MLAT의 절차는 평균적으로 1년 이상 소요된다[50]. 전자증거의 초국가적이고 휘발적인 특성으로 인해 신속한 국제사법공조는 사이버범죄와 전자증거와 관련된 범죄에 대응하기 위해 매우 중요한 요소임에도 절차가 너무 복잡하고 장시간이 소요되는 등 비효율적으로 운영되고 있다. 또한 동 보고서에 따르면 통상 국제사법공조 요청에 대한 응답에 걸리는 시간은 6개월에서 24개월로 나타났고 다수의 요청이 무시되는 사례도 있다[51].

CLOUD Act의 행정협정 관련 규정은 이러한 MLAT 프로세스의 문제를 해결할 수 있는 입법적 대안으로 작용할 것으로 기대된다. 또한 CLOUD Act의 통과에 따라 미국에 본사를 둔 구글, 페이스북, 트위터, 마이크로소프트 등 서비스제공자가 보유한 데이터를 제공받기 위해 더 많은 정부들이 미국과 행정협정을 체결하려고 시도할 것으로 예상된다[52].

우리나라도 최근 5년간 수사기관에서 직접 미국의 서비스제공자를 대상으로 영장을 집행하는 사례가 증가하고 있다. 다만, 가입자정보나 로그기록 등은 미국 국내법을 근거로 직접 미국 서비스 제공자로부터 제공받을 수 있었으나 이메일 내용과 같은 콘텐츠 데이터의 경우, 해당 기업은 국제형사사법공조(MLAT) 절차를 거칠 것을 요구해 왔다. 따라서 우리나라 수사기관이 서비스 제공자로부터 조금 더 효율적

48) Lin, Tiffany, and Mailyn Fidler. “Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement.” A Berklett Cybersecurity publication, Berkman Klein Center for Internet & Society (2017), p.4.

49) Cybercrime Convention Committee (T-CY), T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Council of Europe, 2014.

50) Clarke, Richard A., Liberty and Security in a Changing World: Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies, 2013, p. 227.에서도 MLAT에 따른 절차가 평균 10개월 정도 소요된다고 지적한 바 있다.

51) Cybercrime Convention Committee (T-CY), T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Council of Europe, 2014, p.123.

52) 영국의 경우 이미 미국 정부와 협정 체결에 대한 논의를 하고 있으며, CLOUD Act에 따른 행정협정을 최초로 체결하는 국가가 될 것으로 예상되고 있다. Jennifer Daskal, *Microsoft Ireland*, the CLOUD Act, and International Lawmaking 2.0, Stanford Law Review Online, Vol. 71, 2018, p.14.

이고 신속하게 콘텐츠 데이터를 제공받기 위해서는 미국 정부와 행정협정을 체결하는 방안을 적극적으로 검토해 볼 필요가 있다.

물론 이를 위해서는 우리나라가 CLOUD Act에서 규정하고 있는 "자격 있는 외국 정부(qualifying foreign government)"에 해당하기 위한 요건을 갖추었는가를 먼저 검토해볼 필요가 있다. 이를 위해서는 우리나라가 유럽평의회의 사이버범죄협약 당사국이거나 협약 상의 규정을 국내적으로 이행한 경우와 같이 사이버범죄와 디지털 증거에 대한 실체법 및 절차법을 갖추고 있어야 한다. 그러나 아직 우리나라는 유럽평의회의 사이버범죄협약 당사국이 아니며, 협약의 내용이 국내법에 완전히 수용되었다고 보기 어렵기 때문에 국제 기준에 맞는 실체법 및 절차법적 정비가 필요하다.

또한 우리 정부기관에서 데이터를 수집, 보유, 활용, 공유하는 법적 절차, 그리고 이를 통제하기 위한 법적 장치가 마련되어 있어야 한다. 이러한 국내법적 장치는 개인정보의 수집, 이용, 제공, 관리 등에 대해 규정하고 있는 개인정보보호법 제15조 내지 제34조에서 찾아볼 수 있으며, 통신비밀보호법 상 통신제한조치(제5조 내지 제9조), 통신사실 확인자료 제공 절차(제13조) 및 전기통신사업법 상 통신자료 제공 절차(제83조 제3항) 등에서도 관련 규정을 찾아볼 수 있다. 그러나 이러한 국내법과 제도가 미국에서 요구하는 기준에 부합하는 것인지에 대해서는 보다 세부적인 검토가 필요할 것이다.

또한 만약 미국과 행정협정을 체결하면 상호주의 원칙에 따라 우리나라 기업이 보유 또는 관리하고 있는 데이터에 대해 미국이 직접 기업을 상대로 제공 요청을 할 수 있게 되므로 이에 따른 대비도 역시 필요하다. 현재 우리나라에는 외국 수사기관의 데이터 제공 요청에 대응할 구체적인 법제나 가이드라인이 마련되어 있지 않다[53]. 이 때문에 실무상으로는 해외 수사기관이 우리나라 수사기관에게 수사협조를 요청하거나 형사사법공조 절차를 통하는 경우에 한하여, 우리 수사기관이 자체적으로 수사에 착수하여 서비스제공자에게 관련 정보를 제공받고 이를 다시 해외 수사기관에 제공하고 있다[54]. 따라서 우리나라 서비스 제공자가 외국 수사기관이

53) 전현욱 외, "사이버범죄의 수사 효율성 강화를 위한 법제 개선 방안 연구," 경제·인문사회연구회 미래사회 합동연구총서 15-17-01, 경제·인문사회연구회, 2015, p.176.

54) 전현욱 외, "사이버범죄의 수사 효율성 강화를 위한 법제 개선 방안 연구," 경제·인문사회

국제공조절차를 통하지 않고 국내 서비스제공자에게 직접 정보 제공을 요청하고 이를 제공받을 수 있도록 하는 법제도적 근거를 마련할 필요가 있다.

또한 개인정보보호법 제17조 제3항에 따르면, 개인정보를 국외의 제3자에게 제공할 때에는 정보주체에게 개인정보를 제공받는 자 및 개인정보 이용 목적 등을 통지할 의무가 있고 동의를 받아야 하는데, 이러한 개인정보 국외 이전에 대한 규정과 행정협정이 충돌할 우려가 있다[55]. 따라서 국내 서비스 제공자가 범죄수사를 목적으로 해외의 정부기관에 정보를 제공하는 경우에 적용할 수 있는 개인정보의 국외 이전에 대한 예외 규정을 신설할 필요가 있다.

이상에서 언급한 모든 절차는 국내 기업에 대한 비용적 부담과 프라이버시에 대한 우려를 수반하기 때문에, 국내 기업 및 시민단체들과의 논의와 공감대 형성이 선행되어야 할 것이다.

2. 다른 법률과의 상충 문제

최근 유럽연합(European Union, EU)에서는 2018년 5월 25일 "일반 데이터 보호 규정(General Data Protection Regulation, GDPR)"이 발효되었다. 이로 인해서 데이터 전송 및 처리에 관한 EU의 GDPR 규정과 CLOUD Act 규정이 상충될 가능성이 있다[56].

GDPR은 EU 비회원국에 의해 발부된 법원의 영장에 따른 데이터 제공과 같이 EU 내에 저장된 데이터를 EU 외부로 이전(transfer)할 경우 여러 가지의 제한규정을 두고 있다. 특히 GDPR 제48조는 외국의 영장이나 법원의 명령이 EU 회원국과 외국 정부 간에 체결된 "국제형사사법공조 조약과 같은 국제협정에 근거한" 경우에만 이를 인정한다[57]. 그러나 CLOUD Act에 근거한 행정협정이 GDPR 제48조 상

연구회 미래사회 합동연구총서 15-17-01, 경제·인문사회연구회, 2015, p.176.

55) 제17조(개인정보의 제공) ③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

56) Jennifer Daskal, *Microsoft Ireland*, the CLOUD Act, and International Lawmaking 2.0, Stanford Law Review Online, Vol. 71, 2018, p.12.

57) EU GDPR Article 48 "Transfers or disclosures not authorised by Union law"

의 "국제협정"에 해당하는지 여부는 불분명하다. 미국은 2017년부터 영국과 데이터 공유에 관한 행정협정 체결을 논의하고 있는데, 이러한 GDPR과의 충돌 문제 역시 검토되어야 할 것이다.

또한 CLOUD Act는 GDPR의 영향을 받는 EU 회원국의 국내법과도 상충될 소지가 있다. 마이크로소프트 외에도 구글, 아마존, 페이스북 등 대부분의 미국 IT 기업들은 아일랜드에 데이터 센터를 두고 있다. CLOUD Act에 따르면 미국이 서비스 제공자에게 아일랜드 소재 데이터 센터에 있는 데이터를 요구하더라도 아일랜드 정부가 이러한 사실을 알기 어렵고 통제도 사실상 불가능하다. 아일랜드는 마이크로소프트 사건에서 법원에 제출한 법정조언자 의견서(amicus curiae brief)에서 미국 정부는 해당 데이터를 미국과 아일랜드 간에 체결되어 있는 국제형사사법공조 조약을 통해서 획득하는 것이 가장 적절하며, 그렇게 하지 않는 경우, 사건에서 문제된 영장은 아일랜드의 주권을 침해하는 것이라고 주장한 바 있다[58]. 따라서 아일랜드나 싱가포르와 같이 미국 기업들의 데이터 센터가 모여 있는 국가들의 입장에서는 CLOUD Act가 해당 국가의 주권을 침해하는 일방적인 입법으로 간주될 수 있다. 이러한 문제는 인터넷 상의 국가관할권에 대한 확립된 국제 원칙이 없기 때문에 발생하는 법적 충돌로, 향후 해당 국가들이 CLOUD Act에 대해서 어떠한 반응을 보일지 지켜볼 필요가 있으며 CLOUD Act가 과연 해당 국가의 주권을 침해하는지 여부는 차후 연구 과제로 남겨두기로 한다.

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

58) Brief amicus curiae of Ireland in support of neither party, Microsoft Ireland, No. 17-2, 2017.

Ⅴ. 결론

이상에서 살펴본 미국의 CLOUD Act는 그간 논란이 되어 온 역외 데이터에의 접근에 대해서 기존 법률에 "데이터의 위치와 관계없이"라는 문구를 삽입하여 명쾌한 해답을 내놓았다는 점, 그리고 대부분의 수사기관에서 문제점으로 인식해 온 MLAT의 비효율성을 해결할 수 있는 대안을 제시했다는 점에서 높이 평가할만한 입법이라고 하겠다.

CLOUD Act에 대해서 양자 협정 체결을 통한 데이터 공유 프로세스가 프라이버시를 침해할 것이라는 우려도 제기되고 있다[59]. 그러나 장기적으로 보면, 전 세계 데이터의 대다수를 보유한 미국과 CLOUD Act에 따른 행정협정을 체결하려는 국가들이 늘어나고 그러한 국가들은 법에서 정하고 있는 일정 요건을 충족시키기 위해 노력할 것이다. 그렇게 되면 CLOUD Act가 종국적으로 국가들 간의 법제 조화를 촉진시키고 전 세계적으로 프라이버시 보호를 강화시키는 순기능으로 작용하게 될 것이라고 생각한다. 미국의 Jennifer Daskal 교수 역시 이러한 CLOUD Act가 국내법을 통해 국제법을 제정하는 새로운 형태의 국제 입법이 될 것이라고 보았다[60].

다만, CLOUD Act에 따른 행정협정과 관련하여, 우리 정부는 중대범죄에 대한 수사의 효율성과 신속성, 국민의 기본권과 프라이버시 보호, 법제 정비 등에 수반되는 비용·노력 및 시간 등을 종합적으로 고려하여야 하고, 미국과 행정협정을 체결함으로써 얻는 득과 실을 비교 형량하여 행정협정을 체결할지 여부에 대한 정책적 판단을 내려할 것이다.

---

59) Robyn Greene, Somewhat Improved, the CLOUD Act Still Poses a Threat to Privacy and Human Rights, Just Security, March 23, 2018. https://www.justsecurity.org/54242/improved-cloud-act-poses-threat-privacy-human-rights/ (최종접속일: 2018년 5월 30일)

60) Jennifer Daskal, *Microsoft Ireland*, the CLOUD Act, and International Lawmaking 2.0, Stanford Law Review Online, Vol. 71, 2018, p.15.

참고문헌

Ⅰ. 국내문헌

이원상·이성식, “클라우드 컴퓨팅 환경에서의 사이버범죄와 대응방안 연구”, 한국형사정책연구원 연구총서 12-AA-07, 2012.

이인곤·강철하, 클라우드컴퓨팅 환경에서 전자정보 압수수색의 문제점과 개선방향, 형사법의 신동향 통권 제54호, 2017

전현욱 외, “사이버범죄의 수사 효율성 강화를 위한 법제 개선 방안 연구,” 경제·인문사회연구회 미래사회 합동연구총서 15-17-01, 경제·인문사회연구회, 2015.

정대용·김기범·권헌영·이상진, “디지털 증거의 역외 압수수색에 관한 쟁점과 입법론: 계정 접속을 통한 해외서버의 원격 압수수색을 중심으로.” 법조 제 65권 제9호, 2016.

최성진, 수사기관의 전자우편 압수수색의 한계에 관한 연구 - 미국의 판례 및 법제도를 중심으로 -, 홍익법학 제11권 제2호, 2010.

Ⅱ. 구미문헌

1. 단행본

Millard, Christopher, ed. Cloud Computing Law. Oxford University Press, 2013.

U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual (2009).

2. 논문

Brier Thomas F., Jr. “Defining the Limits of Governmental Access to Personal Data Stored in the Cloud: An Analysis and Critique of Microsoft Ireland.” Journal of Information Policy, Vol. 7 (2017).

Cybercrime Convention Committee (T-CY), T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Council of Europe, 2014.

Cybercrime Convention Committee (T-CY), Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Council of Europe, 2016.

Currie, Robert J. “Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the ‘Next Frontier’?” Canadian Yearbook of International Law/Annuaire Canadien de Droit International 54, no. March (2017).

Daskal, Jennifer. “The Un-Territoriality of Data.” Yale Law Journal 125, no. 2 (2015).

Daskal, Jennifer, “Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0”, Stanford Law Review Online, Vol. 71, 2018.

Dodge, William S. “The Presumption Against Extraterritoriality in Two Steps.” American Journal of International Law(AJIL) Unbound, Vol. 110, 2016, p.45.

Lin, Tiffany, and Mailyn Fidler. “Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement.” A Berklett Cybersecurity publication, Berkman Klein Center for Internet & Society (2017).

Mulligan, Stephen P. “Cross-Border Data Sharing Under the CLOUD Act,” Congressional Research Service Report, 2018.

Orin S. Kerr, “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It,” George Washington Law Review,

Vol. 72, No. 6, 2004.

Walden, Ian. “Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent.” Queen Mary School of Law Legal Studies Research Paper No. 74/2011, 2011.

William S. Dodge, “The Presumption Against Extraterritoriality in Two Steps.” AJIL Unbound, Vol. 110, 2016.

Woods, Andrew K. “Against Data Exceptionalism.” Stanford Law Review 68, no. April (2016).

Passage of the CLOUD Act and Its Implications for Law Enforcement Access to Extraterritorial Data

Song, Young-jin*

Recently, the US Congress passed the 2018 omnibus appropriations bill, and President Donald Trump signed the bill on March 23, 2018. The bill encompasses over 2,000 pages, including the “Clarifying Lawful Overseas Use of Data Act(hereinafter ‘CLOUD Act’)”.

CLOUD Act explicitly stipulates that government agencies should be able to make requests for communications, traffic data, and subscriber information that are owned or managed by US telecommunications service providers regardless of where the data is located. CLOUD Act therefore provides a legal basis for transborder access to data.

In addition, the CLOUD Act provides that foreign government agencies can request data directly from US companies when an executive agreement is signed with the US government as an alternative to the existing international cooperation process based on the Mutual Legal Assistance Treaty(MLAT).

The CLOUD Act provides clear answers to the recent controversial issue of transborder access to data by introducing the phrase "regardless of whether such [...] information is located" in the existing law. This is a worthy legislative measure in that it presents an alternative to solve the inefficiency of MLAT process, which has been recognized as an investigative barrier by most law enforcement agencies around the world.

In Korea, the number of cases in which law enforcement agencies are directly

* International Cybercrime Research Center, Korean National Police University

executing a warrant against US service providers is increasing in recent 5 years. In order for Korean law enforcement agencies to receive content data from US service providers more efficiently and promptly, it is necessary to actively review ways to conclude executive agreements with the US government. This requires substantive and procedural laws that are in line with international standards in relation to cybercrime and digital evidence. In addition, Korean government should be able to assure that there are clear legal mandates and procedures, including procedures through which the authorities collect, retain, use, and share data, and effective oversight of these activities.

❖ Keyword: CLOUD Act, Stored Communications Act, transborder access to data, extra-territoriality, mutual legal assistance, cybercrime, digital evidence

투고일 : 5월 31일 / 심사일 : 6월 21일 / 게재확정일: 6월 21일