형사정책연구 Korean Criminological Review
제30권 제3호(통권 제119호, 2019 · 가을)

수사기관의 클라우드 데이터 접근에 관한 비판적 고찰 : “데이터 예외주의” 논쟁과 각국의 실행을 중심으로

송영진*

국 | 문 | 요 | 약

과거에는 수사기관이 범죄를 수사할 때, 관련 증거가 대부분 유형의 물건이었고 해당 증거들도 국내의 특정 장소에 위치하는 경우가 대부분이었다. 또한 만약 증거물이나 증인이 해외에 소재한 경우, 이를 수집하기 위해서는 국제형사사법공조 절차를 통해 해당 국가의 협조를 얻는 것이 전통적인 방식이었다. 이와는 대조적으로 오늘날 범죄수사를 위해 해외 서버에 저장되어 있는 무형의 데이터를 수집해야 하는 경우가 증가하면서, 수사기관이 전통적인 국제형사사법공조 절차보다는 데이터를 실제 보유 또는 관리하고 있는 서비스 제공자들에게 직접 데이터 제공을 요청하는 관행이 보편화되었다. 그러나 클라우드 컴퓨팅 기술의 발전으로 글로벌 기업들도 대부분 데이터를 클라우드에 저장하고 있으며, 이 경우 데이터의 실제 위치를 알 수 없게 되는 문제가 발생하고 있다. 이러한 문제들이 각국 법원에서 다툼이 되고 있고 다양한 판례들이 등장하고 있으며, 학자들 사이에서도 논쟁이 되고 있다. 또한 문제의 본질적인 해결을 위해서 국가들은 이를 입법적으로 해결하기 위해 노력하고 있다. 이 논문에서는 수사기관이 해외에 저장되어 있는 데이터, 특히 클라우드 데이터에 접근함에 있어서 파생되는 문제에 대한 “데이터 예외주의” 논쟁과 이 문제를 해결하기 위한 각국의 실행을 입법과 판례를 통해 비판적으로 고찰하고자 하였다. 결론적으로 클라우드 데이터에 대해서는 데이터 관리의 특성상 기존의 영토주의 접근방식을 채택할 수 없으며, 데이터의 접근권한을 가지고 관할권의 성립을 판단하여야 하며 우리나라도 해외의 입법 노력을 참고하여 수사기관의 해외 데이터 수집에 관한 명확한 법적 근거 마련을 위해 관련 입법을 정비할 필요가 있다.

❖ 주제어 : 클라우드 컴퓨팅, 데이터 예외주의, 역외 데이터, 사이버범죄, 디지털증거

* 경찰대학 경찰학과 교수, 국제 사이버범죄 연구센터 겸임연구원

Ⅰ. 서론

오늘날 정보통신기술의 발달로 범죄수사에 있어 데이터[1]의 수집은 필수적으로 수반되고 있으며, 범죄수사 과정에서 수집되는 데이터의 양도 증가하는 추세에 있다. 특히 가입자정보, 통신사실확인자료, 통신 내용 등을 포함하는 통신데이터는 주로 통신주체들이 아닌 제3자가 보관·관리하고 있다[2]. 여기에서 제3자란 인터넷 서비스 제공자(Internet Service Provider, ISP) 또는 콘텐츠 서비스 제공자(Contents Service Provider, CSP) 등의 기업을 의미한다. 특히 구글, 페이스북, 트위터, 인스타그램과 같은 소셜 미디어 사용도 급증하면서 이러한 글로벌 기업에게 수사기관이 정보 제공을 요청하는 사례도 점점 증가하고 있다.

한편, 글로벌 기업들은 데이터 센터를 세계 각지에 설립하여 운영하고 있으며, 클라우드 컴퓨팅[3] 기술의 발달로 인해 서비스 이용자 또는 수사기관이 찾고자 하는 데이터의 정확한 위치를 알지 못하게 되는 현상(loss of location)도 발생하고 있다.

클라우드 환경에서 데이터는 위치 독립성을 가지고 있으며, 이 경우 수사기관이 데이터가 저장된 관할권이 어디인지 데이터에 어떠한 법제도가 적용되는지 판단하기 어렵다. 데이터는 여러 다른 국가에 백업이 되어 있을 수도 있고 분산되어 동시에 여러 서버에 저장될 수도 있다. 이론적으로는 데이터가 클라우드 서버에 저장되어 있는 경우에도 데이터는 언제나 특정 위치에 저장되어 있지만, 그렇다고 하더라도 수사기관의 적법한 접근에 대해 어떠한 규정을 적용해야 하는지는 분명하지 않다.

데이터에도 기존의 유무형 자산과 같이 영토 관할권이 적용되는가? 수사기관이 해외 서버에 저장되어 있는 데이터에 접근하여 이를 수집하는 경우, 해당 데이터가 저장되어 있는 서버의 소재지를 관할하는 국가의 동의를 구해야 하는가? 만약에 수

1) 데이터 자체는 여러 의미를 함축하고 있으나 본고에서 언급하는 데이터는 가입자 정보(subscriber information), 통신 내역(traffic data), 통신 내용(contents data)을 포함하는 통신 데이터에 한정하여 논의를 전개하고자 한다.

2) 박현준, 이상진, 비식별화된 통신사실확인자료의 제공 절차 도입을 통한 수사기관의 기본권 침해 최소화 방안, 형사정책연구 제30권 제1호, 2019, p.94.

3) “클라우드 컴퓨팅”이란 데이터가 특정 디바이스나 폐쇄 네트워크 내에 저장되어 있는 것이 아니라 여러 다른 서비스, 제공자, 위치, 국가에 분산되어 있는 경우를 말한다.

사기관이 데이터에 대한 접근권한은 적법하게 획득한 경우라면, 데이터 소재지 국가의 법의 규율을 받지 않아도 되는가? 수사기관이 데이터의 정확한 위치를 모르는 경우에는 어느 국가의 법에 규율을 받게 되는가?

위와 같은 여러 문제의식은 2010년대 초반부터 제기되어 왔고 특히 미국의 Microsoft Ireland 사건[4]을 계기로 소위 "데이터 예외주의(data exceptionalism)" 논쟁이 등장하게 되었다. "데이터 예외주의"란 데이터에는 영토주의의 예외가 적용된다는 주장 즉, 데이터의 관할권 성립을 판단함에 있어서 기존의 전통적인 영토주의 접근방식을 그대로 채택할 수 없다는 주장을 의미한다[5]. 데이터 예외주의에 찬성하는 학자들은 데이터가 기존의 유·무형 자산과는 다른 독특한 속성을 가지며, 이러한 특징들로 인해 클라우드 환경에서 데이터에 대해 기존의 영토주의적 접근방식을 적용하기 어렵다고 주장한다[6]. 반면, 데이터 예외주의에 반대하는 학자들은 데이터가 가진 속성들이 전혀 새로운 것이 아니며 기존 유·무형자산의 관할권 판단에 대한 법원의 접근방식을 적용할 수 있다고 주장한다[7].

위와 같은 학자들 간의 논쟁들과 더불어 각국 법원에서도 수사기관이 역외 데이터에 일방적으로 접근하는 경우, 관할권의 존부 및 수집된 데이터의 증거능력 등에

---

4) 이 사건은 미국 FBI가 법원으로부터 수색영장을 발부 받아 범죄수사 목적으로 Microsoft에 대해 특정 아웃룩 이메일에 관한 데이터 제공을 요청했으나 Microsoft는 해당 데이터가 아일랜드 더블린에 위치한 데이터 센터에 저장되어 있다는 이유로 제공을 거부한 사건으로 사실관계와 쟁점, 판결의 요지는 "Ⅳ. 데이터 접근에 대한 각국 법원의 실행"에서 후술하기로 한다. United States v. Microsoft Corp., 138 S. Ct. 1186, 1188 (2018) (per curiam).

5) 데이터 예외주의 논쟁은 1990년대 말 이루어진 사이버공간은 규제될 수 없다는 사이버 자유주의자(cyber libertarian)와 사이버공간은 규제되어야 한다는 사이버 규제주의자(cyber paternalist) 간의 논쟁과 그 맥락이 유사하다. Dan Jerker B. Svantesson, "Against 'Against Data Exceptionalism'", Masaryk University Journal of Law and Technology, Vol.10, 2016; Johnson, D. R., Post, D., Law and Borders－The Rise of Law in Cyberspace, Stanford Law Review, vol. 48, no. 5, 1996, pp. 1367-1402 ; Goldsmith, J. L., Against Cyberanarchy, The University of Chicago Law Review, vol. 65, no. 4, 1998, pp. 1199-1250 ; Post, D., Against 'Against Cyberanarchy', Berkeley Technology Law Journal, vol. 17, no. 4, 2002, pp. 1365-1388.

6) Jennifer Daskal, "The Un-Territoriality of Data", The Yale Law Journal, Vol.125, 2015; Dan Jerker B. Svantesson, "Against 'Against Data Exceptionalism'", Masaryk University Journal of Law and Technology, Vol.10, 2016; Zachary D. Clopton, "Data Institutionalism: A reply to Andrew Woods", Stanford Law Review Online, Vol.69, 2016.

7) Andrew Keane Woods, "Against Data Exceptionalism", Stanford Law Review, Vol.68, 2016.

대한 판례들이 등장하고 있다. 전통적이고 공식적인 국제형사사법공조 절차를 거치지 않고 직접 수사기관이 데이터에 접근하거나 서비스 제공자를 통해 데이터에 접근하는 경우, 각국 법원은 서로 다른 접근방식을 취하고 있다.

여기에서는 데이터 예외주의에 대한 학자들의 의견 대립과 각각의 논거를 살펴보고, 수사기관이 역외 데이터에 접근하는 경우에 대한 법원의 판단을 중심으로 각국의 실행을 분석하여 역외 데이터 접근에 대한 시사점을 도출하고자 한다.

Ⅱ. 데이터 예외주의 논쟁

1. 찬성론

데이터 예외주의를 주장하는 대표적 학자인 Daskal 교수는 기존의 유무형 자산과 데이터를 비교하면서 데이터가 가진 고유한 속성이 있다고 주장한다. "데이터는 유형의 물건 또는 자산과는 다르다"는 전제하에 데이터의 비영토성(un-territoriality)을 주장하고 있는 것이다. Daskal 교수는 논문에서 데이터의 속성을 데이터의 이동성, 데이터의 가분성, 위치 독립성, 데이터의 혼합, 제3자 이슈 등 5가지로 제시하고 있으며, 여기에서는 Daskal 교수가 제시한 .데이터의 속성에 대해서 살펴보고자 한다.

1) 데이터의 이동성(data's mobility)

유형의 물건을 이동시키는 경우에는 그 물건의 이동이 관찰 가능하고 어디로 이동할 지에 대한 예측이 가능하다. 또한 대부분의 경우에 물건의 이동에 관한 의사결정은 소유자 또는 점유자에 의해 이루어지고 물건의 소유자나 점유자는 물건의 위치를 쉽게 알 수 있다[8]. 그러나 데이터의 경우 네트워크 내에서 계속 이동하는 특성을 가지기 때문에 데이터의 소유자가 데이터의 위치를 예측하기가 어렵다. 특히 데

8) Jennifer Daskal, "The Un-Territoriality of Data", The Yale Law Journal, Vol.125, 2015, p.366.

이터가 클라우드에 저장되는 경우, 이는 고정된 위치에 저장되지 않고 기술적 처리 또는 서버 유지보수 등의 이유로 이동될 수 있으며, 데이터가 복사되거나 분할되어 여러 장소에 분산될 수 있다.[9)]

이러한 유형재산과 데이터의 차이는 두 가지 측면에서 중요하다. 첫째, 어느 규범이 적용될지에 대한 판단기준으로 삼는 데이터 위치가 변경될 가능성이 있다[10)]. 데이터는 A 지점에서 B 지점으로 순식간에 이동할 수 있는데, 만약 정부가 데이터에 접근할 경우 서비스제공자가 해당 시점에 데이터를 어느 장소에 보관하는지에 따라 상반된 결과가 나올 수 있다. 둘째, 데이터의 이동 경로는 이용자가 알지 못한 상태로 또는 이용자의 선택과는 무관하게 결정된다[11)]. 이용자가 데이터를 클라우드에 저장할 경우, 이용자는 데이터가 실제 보관되는 위치를 통제할 수도 없고 이를 알 수도 없게 된다. 통상적으로 데이터의 위치는 컴퓨터 알고리즘에 의해 결정되며 이용자는 해당 데이터에 어느 규범이 적용될 것인지 알기 어렵다.

2) 데이터의 가분성(divisibility) 및 데이터 분할(data partitioning)

클라우드에 저장된 데이터는 복제되어 여러 위치에 보관되는 경우가 많은데, 이는 서버 오작동에 따른 데이터 손실을 방지하고 사용자가 백업 위치에서 자신의 데이터에 계속 액세스할 수 있도록 보장하기 위해서 취해지는 관리적 조치이다.

관리가능성과 이용의 효율성을 증대시키기 위해 단일 데이터베이스가 여러 파트로 나뉘게 되는 데이터 분할은 또 다른 측면에서의 복잡성을 야기한다[12)]. 분할된 데이터베이스의 다양한 구성요소는 각기 다른 위치에 보관될 수 있다. 데이터 가분성 또는 데이터 분할이라는 특성으로 인해서 규범 적용의 판단기준이 되는 데이터의 저장 위치를 판단하기 어려워진다[13)]. 데이터의 위치는 조작이 가능하며, 해당 위치를 특정하기 어려운 경우도 있다. 이러한 데이터의 독특한 특성들로 인해 과연

9) Jennifer Daskal, 앞의 논문, p.366.

10) Jennifer Daskal, 앞의 논문, p.367.

11) Jennifer Daskal, 앞의 논문, p.367.

12) 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, p.3.

13) Jennifer Daskal, “The Un-Territoriality of Data”, The Yale Law Journal, Vol.125, 2015, p.369.

데이터의 위치가 데이터에 적용되는 규범을 결정함에 있어 판단기준이 되어야 하는가에 대한 의문이 제기되고 있다.

3) 위치 독립성

과거 전통적인 수사 방식과 비교하여 가장 큰 변화 중 하나는 데이터에 접근하는 수사기관의 위치와 데이터의 저장 위치 사이에 단절이 있다는 것이다[14]. 현대 기술의 발달로, 수사관은 더 이상 압수수색대상과 같은 장소에 있을 필요가 없다. 또한 A국의 수사관이 B국의 서버에 원격으로 접속하여 저장되어 있는 데이터를 복사할 때, B국에서는 이를 인식할 수도 없고, 데이터 이용자의 데이터 접근권한이나 데이터의 가용성에도 변화가 없는 경우가 많다[15]. 일부 학자들은 서버의 원격 접근이 사용자의 데이터 접근 권한을 변경하거나 방해하지 않기 때문에, 데이터의 복사는 헌법에서 규정하고 있는 압수에 해당하지 않는다고 주장하기도 한다[16].

또한 위치 독립성은 데이터와 데이터 이용자와의 단절, 즉 데이터가 이용자와 동일한 또는 근접한 위치에 저장될 필요가 없다는 것을 의미한다[17]. 이를 통해 이용자는 어디에서나 데이터에 액세스할 수 있으며 클라우드 효율성의 핵심이 된다. 위치 독립성은 공급자가 데이터를 이동하여 피크 시간에 스토리지 센터의 사용을 최적화하고 서버 다운이나 정전을 방지하며 사용자 접근을 방해하지 않고 서버 정비를 수행할 수 있도록 한다. 클라우드 서비스의 경우 통상적으로 서비스제공자가 데이터의 위치를 관리한다[18]. 서비스제공자들은 데이터가 한 곳에서 다른 곳으로 이동할

14) Jennifer Daskal, 앞의 논문, p.369.

15) Jennifer Daskal, 앞의 논문, p.372.

16) Orin S. Kerr, “Searches and Seizures in a Digital World”, Harvard Law Review Vol.119, 2005, pp.557-558.

17) Jennifer Daskal, “The Un-Territoriality of Data”, The Yale Law Journal, Vol.125, 2015, p.373.

18) 여기에서 특기할만한 점은 클라우드 유형에 따라 데이터를 관리하는 방식의 차이가 발생하게 된다는 것이다. 특히 Schwartz 교수는 클라우드의 유형을 데이터 조각 모델, 데이터 국지화 모델, 데이터 신탁 모델 등 세 가지로 구분하여 각각의 법적 효과에 대하여 달리 판단하여야 한다고 주장하고 있다. Paul M. Schwartz, “Legal Access to the Global Cloud”, Columbia Law Review, Vol.118, No.6, 2018.

때마다 이용자에게 통지하거나 그의 동의를 얻지 않고 그러한 의사 결정을 한다[19]. 실제로 이용자는 자신의 데이터가 특정 시점에 어디에 저장되어 있는지 알지 못하는 경우가 많다.

데이터의 위치 독립성으로 인해 수사기관은 데이터에 접근함에 있어서 실질적인 어려움에 직면하게 되는데 우선 수사기관은 스마트폰, 컴퓨터 등의 디지털 기기를 압수할 때조차도, 해당 매체와 연동된 데이터가 실제 어디에 저장되어 있는지 알지 못하게 된다[20]. 따라서 디지털 기기와 이에 접근할 수 있는 암호 키를 확보한 상태라고 하더라도, 기기와 연동된 데이터가 수사기관의 관할 내에 저장되어 있는지 아니면 역외에 저장되어 있는지 알기 어렵다. 또한 수사관이 데이터의 위치를 알고 있다고 하더라도 데이터 사용자의 위치에 대해서 알지 못하는 경우가 발생할 수 있다[21]. 특히 익명화 도구의 사용은 이러한 식별의 어려움을 가중시키고 있다.

4) 데이터의 혼합(intermingling)

데이터는 복수의 사용자가 생성한 데이터가 혼합될 수 있다는 점에서 유형의 아날로그와는 다르다. 네트워크에서 전송되는 통신은 다중 통신 트랜잭션으로 함께 묶이게 되는데, 수사기관은 이러한 통신을 별도의 구성요소로 분리할 수 있는 기술적 능력이 부족하다[22]. 따라서 통신 감청을 위해서는 감청 대상에게 또는 그 대상으로부터 송수신되는 모든 통신 데이터를 분석하기 위해서 수사기관은 전체의 트랜잭션을 획득해야 한다. 이러한 데이터의 혼합으로 인해서 데이터 수집 단계에서 사용자 또는 ID 기반 구분이 어려워지고 있고, 영토주의를 기반으로 관할권 성립을 결정하기 위해서 관련 데이터 사용자를 확인하고 적용될 규범을 판단하는 것을 어렵게 만들고 있다[23].

---

19) Jennifer Daskal, 앞의 논문, p.373.
20) Jennifer Daskal, 앞의 논문, p.374.
21) Jennifer Daskal, 앞의 논문, p.374.
22) Jennifer Daskal, 앞의 논문, p.375.
23) Jennifer Daskal, 앞의 논문, p.376.

5) 제3자(third-party) 이슈

유형재산의 소유자들은 대부분 자신의 재산을 직접 보관하고 관리하고, 예외적인 경우에 이를 제3자에게 양도하여 대신 보관하거나 관리하도록 한다. 이와는 대조적으로, 데이터의 경우에는 데이터를 생성한 주체가 아닌 ISP, 클라우드 서비스 제공자 등 제3자가 대부분의 데이터를 보유 또는 관리하고 있다[24].

또한 상술한 바와 같이 데이터가 이동하는 경로나 데이터가 저장되는 위치에 대해 일반적으로 중요한 결정을 내리는 것은 사용자가 아니라 제3자다. 또한 정부에서도 사용자가 아닌 제3자에게 데이터의 제공을 요청하고 있다. 1970년대 Smith v. Maryland과 United States v. Miller 사건에서 도출된 "제3자 원칙(third-party doctrine)"에 따르면, 제3자에게 자발적으로 데이터를 제공한 개인은 해당 데이터에 대한 합리적인 프라이버시 보호를 기대할 수 없게 된다.

제3자 이슈는 데이터와 유형재산의 또 다른 차이점을 만드는 요인이 된다. 우선 데이터의 경우, 제3자의 위치가 관할권 성립을 결정짓는 요소가 될 수 있다[25]. 또한 제3자의 통제로 인해 사용자는 데이터와 그 데이터의 저장 위치에 대한 직접적인 통제를 행사할 수 없게 된다[26]. 물론 제3자와 계약을 체결하거나 데이터 국지화(data localization) 법을 통과시켜 데이터를 특정 위치에 저장하는 것은 가능하다. 그러나 현재 대부분의 데이터 사용자는 자신의 데이터에 대한 그러한 통제권을 보유하고 있지 않다. 기본적으로 클라우드와 글로벌 인터넷의 효율성은 제3자가 사용자 선호와 통제에 구속되지 않고 가장 빠른 방법으로 데이터를 이동할 수 있도록 설계되었기 때문이다.

2. 반대론

반대론을 주장하는 Woods 교수는 이동형, 분할형, 위치 독립형 자산으로서 데이터의 고유한 특성에 대한 주장이 대부분 과대평가되고 있으며, 오히려 데이터는 물

24) Jennifer Daskal, 앞의 논문, p.377.
25) Jennifer Daskal, 앞의 논문, p.378.
26) Jennifer Daskal, 앞의 논문, p.378.

리적 자산과 무형 자산 모두와 유사성을 가지고 있다고 주장한다. 따라서 데이터는 기존의 자산과 크게 다르지 않으며, 법원의 기존 접근방식을 적용 가능하다고 주장한다[27].

Woods 교수는 데이터의 특징들 중 어떤 것도 사실 새로운 것이 아니며, 실제로 데이터는 저장되는 모든 곳에 물리적 위치가 있기 때문에 관할권 성립을 결정하기가 오히려 더 쉬울 수도 있다고 주장한다. 또한 법원이 클라우드 내 데이터에 대한 관할권 판단을 위해 두 가지의 기준을 활용할 수 있다고 하면서, 데이터를 무형자산으로 간주하여 돈, 부채, 주식 및 기타 유사한 물품에 대한 처리 방식과 동일하게 취급하거나 데이터를 데이터가 저장된 매체 즉, 물리적 자산으로 취급하여 접근할 수 있다고 주장한다. 아래에서는 무형자산으로서의 데이터와 물리적 자산으로서의 데이터를 나누어 Woods 교수의 주장과 논거를 정리해보고자 한다.

1) 무형자산으로서의 데이터

첫째, 데이터에 영토주의 원칙이 적용되지 않을 것이라는 주장은 데이터의 무형적인 속성에서 기인한다. 그러나 법원은 그간 주식이나 부채와 같이 무형자산에 대한 분쟁에 대한 사법적인 판단을 내려왔기 때문에 이러한 데이터의 무형성은 새로운 문제가 아니다[28]. 실제로 법원은 무형자산의 위치에 대한 다양한 접근방식을 제시해 왔는데, 예를 들어 상표권과 같은 지적 재산권은 그것이 창작되고 등록되는 모든 곳에서 발견할 수 있다. 부채는 전형적으로 부채와 관련된 조치가 취해질 수 있는 채무자의 거주지에 위치하게 된다.

미국 대외관계법 제3차 Restatement에서는 무형재산은 각각 다른 목적에 따라 다른 위치를 가질 수 있다고 설명하고 있다. 범죄수사와 관련된 데이터의 위치를 결정지을 때 법원이 적용할 수 있는 적절한 기준은 과세 목적 또는 민사분쟁에서의 위치 결정 기준과는 다를 수 있지만 실제로 많은 경우에 법원이 자산을 통제할 수 있는 자에 대해 관할을 갖는 한 무형자산의 위치는 중요하지 않다[29]. 국가가 클라우드

27) Andrew Keane Woods, “Against Data Exceptionalism”, Stanford Law Review, Vol. 68, 2016.
28) Andrew Keane Woods, 앞의 논문, p.756.
29) Andrew Keane Woods, 앞의 논문, p.757.

데이터에 대한 권한을 주장하기 위한 관할권적 근거를 살펴보기 전에 데이터와 무형 자산 사이에 상당 부분 유사성이 있으며 법원이 이러한 무형 자산과 관련된 다수의 분쟁을 경험했다는 사실은 언급할 필요가 있다.

둘째, 데이터 예외주의자들은 데이터가 이동하기 때문에 위치에 기반한 관할권이 데이터에 대해서는 적용하기 어렵다고 주장한다[30]. 그러나 이동성은 데이터에만 독특한 특징이 아니다. 금전의 경우 한 장소에서 다른 장소로 즉시 이체될 수 있으며, 법원이 금전에 대한 관할권을 주장하기 위해 금전의 위치를 결정짓는 데 문제가 없다. 법원은 사람, 물자 및 이동적인 자산의 관할을 결정할 때 특별한 어려움을 겪지 않는다. 따라서 데이터의 이동성으로 인해 영토주의 관할권을 적용하기 어려울 것이라는 우려는 불필요한 것이다[31].

셋째, 데이터의 가분성과 대체가능성은 이용자의 데이터가 여러 파트로 분할되어 각각 다른 위치 또는 국가에 있는 서버에 분산될 수 있다는 것을 의미한다[32]. 그러나 이러한 특징은 데이터에만 독특한 것은 아니다. 은행계좌에 들어있는 현금을 예로 들어보면, 고객이 5달러 지폐 2매를 은행에 입금한 경우, 은행은 돈을 은행의 다른 지점에 분산해서 보관하고 만약 고객이 현금을 인출할 경우에 10달러를 지급하게 된다. 돈이 계좌에 입금되면 이 돈은 다른 돈들과 혼합되어 예치된다[33].

넷째, 이용자는 자신의 데이터와 동일한 위치에 있지 않을 수도 있고 위치를 알지 못할 수도 있다. 이러한 점으로부터 데이터가 영토주의의 적용을 받지 않는다는 주장이 도출된다. 그러나 이러한 위치의 분리는 데이터에 고유한 특성이 아니다. 현금의 경우, 스위스 은행과 같은 역외 은행 계좌에 저장될 수 있다. 누군가 다른 관할권에 위치한 뮤추얼 펀드에 주식을 보유할 수 있으며, 뮤추얼 펀드는 많은 관할권에 분산된 회사의 주식을 보유할 수 있다[34].

2) 물리적 자산으로서의 데이터

30) Andrew Keane Woods, 앞의 논문, p.758.
31) Andrew Keane Woods, 앞의 논문, p.758.
32) Andrew Keane Woods, 앞의 논문, p.759.
33) Andrew Keane Woods, 앞의 논문, p.760.
34) Andrew Keane Woods, 앞의 논문, p.760.

데이터에 영토관할권을 적용하기 어렵다는 주장은 데이터를 찾기가 어렵다는 아이디어를 전제로 한다. 그러나 부채나 주식과 달리 데이터는 저장되어 있는 곳마다 물리적이며 영토적인 위치를 가지기 때문에 법원이 무형 자산보다 데이터에 대한 관할권을 주장하는 것이 여러 면에서 쉽다[35]. 주식, 부채 및 은행과 달리 데이터는 압수가능한 물리적 드라이브에 저장되어 있다. 실제로 데이터는 사실 물리적 위치, 일반적으로 이용자의 위치와 가까운 곳에 저장된다. Microsoft의 선서진술서(affidavit)에 따르면 데이터 센터는 가능한 한 최종 이용자(end user)에 가까운 곳에 위치한다[36].

그러나 일반적인 클라우드 사용자에게 데이터가 저장되는 위치는 중요한데, 그 이유는 데이터의 위치가 액세스 할 수 있는 속도에 영향을 미치고 결정적으로는 특정 정부가 그 데이터에 액세스 할 수 있기 때문이다[37]. 예를 들어 Google이 고객 데이터에 대한 중국의 접근을 원하지 않으면 Google은 홍콩으로 이전해야 한다고 판단한다. Google은 고객 데이터를 홍콩이나 중국이 아닌 가까운 대만 및 싱가포르의 서버에 저장한다. 이를 통해 Google은 중국 고객에게 일부 서비스를 제공할 수 있지만 데이터를 중국 당국의 손이 닿지 않는 곳에 보관할 수 있다. 이러한 조치는 데이터의 물리적 위치가 중요하다는 것을 의미한다.

3. 소결

영토주권은 계속해서 인터넷을 지배해왔으나 무엇이 영토적이고 무엇이 역외적인지에 대해서는 아직 논쟁이 계속되고 있다[38]. 데이터의 독특한 특성과 데이터가 취급되는 방식으로 인해 특수한 고려가 필요하며, Woods 교수의 주장과 같이 단순히 다른 유형자산과 무형자산에 적용되는 규정을 그대로 적용하는 것은 부적절하다.

데이터와 유형자산 및 무형자산의 다른 형태의 유사성에 초점을 맞추는데 있어서

35) Andrew Keane Woods, 앞의 논문, p.761.

36) Microsoft E-mail Search Warrant Case, 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014).

37) Andrew Keane Woods, “Against Data Exceptionalism”, Stanford Law Review, Vol. 68, 2016, p.761.

38) Jennifer Daskal, “Border and Bits”, Vanderbilt Law Review, Vol.71, 2018, p.221.

Woods는 주요 차이점에 대해 분명히 언급하지 못하고 있다. 수많은 정부, 학계, 사법 기관들이 데이터에 대한 집행 및 입법 관할권에 대한 관할의 한계를 정의하기 위해 적극적으로 노력하고 있는 것만 보더라도 데이터와 유형자산이 다르다는 점을 알 수 있다[39].

데이터의 이동성과 관련하여 사람과 일부 유형재산들도 국경을 넘나들며 이동하지만 그것들은 상대적으로 예측가능하고 관찰가능하게 이동한다. 그러나 데이터의 이동은 예측이 불가능하고 일반적으로 데이터의 주체나 정부기관이 알 수 없는 방식으로 이동한다. 이러한 특징으로 인해 데이터의 저장 위치를 영토적 관할권을 결정짓는 근거로 삼기 어렵게 된다.

또한 이것은 데이터가 저장된 장소와 해당 데이터에 대해 이해관계가 있는 국가와의 불일치성을 야기하게 된다. 결국 국가뿐만 아니라 데이터의 주체도 어떤 특정 시점에 해당 데이터의 위치를 알 수 없게 되는 "위치의 부재(loss of location)" 현상이 발생하게 된다.

Woods 교수는 금전이나 부채와 같은 다른 자산들도 가분성을 가진다고 보고 있다. 그러나 빠르게 이동하는 통신 내용과 빠르게 이동하는 금전과는 중요한 차이가 존재한다. 금전이나 부채는 경쟁적(rivalrous) 자산이다. 그러나 이와 대조적으로 데이터는 비경쟁적(non-rivalrous) 자산이다. 데이터는 그 데이터의 속성이나 데이터 주체의 접근 또는 수정 권한에 전혀 영향을 미치지 않으면서 일방적으로 복제되어 동시에 여러 관할 내에 존재할 수 있다.

금전의 경우 정부에 의해 압수되면 더 이상 그 소유자가 금전을 사용할 수 없게 되지만, 데이터는 기존 데이터 주체의 권리를 해치지 않은 채로 다수의 당사자들에 의해서 분할·배포·복제·접근이 가능하다[40]. 데이터를 A국가에서 압수하더라도 그 데이터는 여전히 다른 B국가에서 접근하고 이용할 수 있다.

또한 데이터는 원격에서 액세스 및 변경이 가능하다. 이는 데이터 주체가 데이터와 분리될 수 있고 다른 국가에서 데이터를 변경할 수 있다는 것을 의미한다. 또한 이는 수사기관과 서비스 제공자 모두가 해외에 직접 가지 않더라도 역외에 위치한

39) Jennifer Daskal, 앞의 논문, p.222.

40) Jennifer Daskal, 앞의 논문, p.223.

데이터에 접근할 수 있음을 의미한다. 수사기관은 데이터 주체의 접근권한을 배제하거나 방해하지 않고서 데이터에 접근하고 복제할 수 있다.

마지막으로 데이터의 저장 위치가 제3자에 의해 통제되는 경우가 점점 증가하고 있다. 이용자는 일반적으로 데이터가 저장될 위치를 결정하지 않는다. 또한 데이터 주체와 데이터가 저장될 위치와의 규범적인 연관성 역시 없다[41].

데이터에 대해서는 다른 부동산 또는 재산 소유자에 의한 선택과 같은 의사결정이 이루어지지 않고 데이터 주체에 대해서 데이터 접근에 대해 어떠한 규정이 적용될지에 대한 통지가 이루어지지 않고 데이터 주체는 이를 통제할 수 없게 된다.

이러한 각각의 데이터 속성들은 주권과 관할권, 주요 이해관계를 평가함에 있어서 중요하게 작용하며, 적용할 규범을 판단할 때 고려되어야 한다.

Ⅲ. 데이터 접근에 대한 각국의 입법

1. 미국

2018년 미국 의회는 “합법적인 해외 데이터 활용의 명확화를 위한 법률(Clarifying Lawful Overseas Use of Data Act, 이하 CLOUD Act)”를 통과시켰다[42]. CLOUD Act는 수사기관이 통신서비스제공자가 보유하고 있는 데이터를 수집하기 위한 절차를 규정하고 있는 저장통신법(Stored Communications Act)을 개정하기 위한 법이다[43]. 기존 저장통신법에는 정부가 서비스제공자에게 미국이 아닌 해외에 저장된 데이터의 제공을 요청할 수 있는지 여부에 대한 명시적 규정을 두고 있지 않았기 때문에 해외에 저장된 데이터에 대한 수사기관의 접근이 법적으로 가능한지 여부가 논란이 되어 왔다[44]. 이에 미국 정부는 CLOUD Act를 통해 실제

41) Jennifer Daskal, 앞의 논문, p.225.

42) Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018).

43) CLOUD Act의 제정 배경과 세부적인 입법 내용에 대해서는, 송영진, 미국 CLOUD Act의 통과와 역외 데이터 접근에 대한 시사점, 형사정책연구 제29권 제2호, 2018 참조.

데이터가 저장된 위치에 관계없이 정부기관이 서비스제공자들에게 통신 데이터를 제공 요청할 수 있도록 규정하여 이러한 문제를 입법적으로 해결하였다. 즉 제2713조에서 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[45].

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. CLOUD Act 제2523조는 미국의 전자 통신 서비스 제공자가 저장통신법을 위반하지 않고 행정협정에 따라 외국 정부의 정보 제공요청에 응할 수 있도록 법적 근거를 제공하고 있다[46].

제2523조는 특정 외국 정부의 국내법 및 그 실행이 데이터 수집과 관련하여 기본권과 프라이버시를 강력하게 보장하는 등 일정한 요건을 충족하는 경우, 미국 법무장관에게 해당 정부와 행정 협정을 체결할 수 있는 권한을 부여하고 있다. 이러한 요건에는 외국 정부가 유럽평의회의 사이버범죄협약 당사국이거나 사이버범죄협약 상의 규정이 국내법과 일치하는 경우와 같이 외국정부가 사이버범죄 및 전자증거에 관한 적절한 실체법과 절차법을 가진 경우, 외국 정부기관이 데이터를 수집, 보유, 활용, 공유하는 절차 및 그러한 활동의 효과적 통제를 포함한 분명한 법적 권한 및 절차를 갖춘 경우 등이 포함된다. 만약 외국 정부가 이러한 요건을 충족시킨다면, 미국과 외국 정부 사이에 체결된 행정 협정은 상호 정보 공유를 허용하고, 이에

44) 송영진, 미국 CLOUD Act의 통과와 역외 데이터 접근에 대한 시사점, 형사정책연구 제29권 제2호, 2018, p.157.

45) § 2713. 통신 및 기록에 대한 보존 및 공개 의무
"전자 통신 서비스 제공자 또는 원격 컴퓨팅 서비스 제공자는 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."

46) 송영진, 미국 CLOUD Act의 통과와 역외 데이터 접근에 대한 시사점, 형사정책연구 제29권 제2호, 2018, p.160.

따라 미국과 다른 외국 국가들이 해외에 저장된 데이터에 접근하는 것을 허용하게 된다[47].

2. 영국

영국은 CLOUD Act 제정 이전부터 이미 미국과 데이터 상호 제공에 관한 논의를 시작한 국가로, 위에서 언급한 미국 CLOUD Act 제2523조에 따른 행정협정을 체결하는 최초의 국가가 될 것으로 언론이나 학계에서 언급되어 왔다[48]. 영국 의회는 미국과의 행정협정 체결을 염두에 두고 국외 제출명령에 관한 내용을 포함한 “Crime (Overseas Production Order) Act 2019”를 통과시켰고 동 법안은 2019년 2월 12일 영국 왕실의 재가(royal assent)를 받았다.

Crime Act에 따르면 경찰관(constable) 등 법에서 정하는 공무원(appropriate officer)은 형사법원(Crown Court)에 국외 제출 명령(overseas production order, “OPO”)을 신청하여 해외에 있는 자로부터 데이터의 저장 위치와 관계없이 ‘전자데이터(electronic data)’를 제출하거나 접근 가능하게 하도록 요구할 수 있다. 동법에서는 ‘전자 데이터’를 ‘전자적으로 저장된 모든 데이터’로 광범위하게 정의하고 있다. 다만, OPO는 변호사 특권에 의해 보호되는 기록이나 개인의 의료기록과 같은 비밀기록에는 적용되지 않는다[49].

형사법원 판사는 다음의 여섯 가지 사항을 모두 충족한다고 믿을만한 합리적인 근거가 있는 경우에 OPO를 발부할 수 있다.

1. 제출명령의 대상이 되는 자가 영국 밖에 있는 국가에서 활동하거나 해당 국가

47) 송영진, 미국 CLOUD Act의 통과와 역외 데이터 접근에 대한 시사점, 형사정책연구 제29권 제2호, 2018, p.161.

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

49) 동법에서는 이를 전자데이터와 구분하여 “예외적 전자데이터(excepted electronic data)”라고 정의하고 있다.

에 기반을 두고 있으며, 해당 국가가 영국과 '지정된 국제협력 약정(designated international cooperation arrangement)[50]'을 체결한 당사국인 경우;

2. 수사 또는 형사절차가 기소가능 범죄와 관련된 경우, 또는 제출명령이 테러리스트 수사 목적인 경우;
3. 제출명령의 대상이 되는 자가 전자 데이터의 전체 또는 일부를 보유 또는 관리하는 경우;
4. 전자 데이터의 전체 또는 일부가 수사 또는 형사절차에 상당한 중요성을 가지는 경우;
5. 전자 데이터의 전체 또는 일부가 범죄와 관련된 증거가 될 경우;
6. 전자 데이터의 전체 또는 일부가 제출되는 것이 사법정의에 부합하는 경우

OPO에는 명령에 명시되거나 서술된 전자데이터를 제출하거나 접근가능하게 하여야 하는 대상자 및 전자데이터를 제출해야 하는 기한이 명시되어 있어야 한다. 여기에서의 기한은 영장이 제시된 날로부터 "7일"이며, 특정한 상황에서는 판사가 판단하여 적절하다고 판단되는 경우 7일의 기간보다 단기 또는 장기의 기간을 정하여 명시할 수 있다.

동법의 제출명령을 받은 자는 제출명령에 명시되어 있거나 서술되어 있는 전자데이터를 수사기관이 반출할 수 있는(can be taken away) 형태 또는 가시적이고 가독한(visible and legible) 형태로 해당 데이터를 제출하여야 한다.

3. 유럽연합(EU)

미국 CLOUD Act가 발효한 후 얼마 지나지 않아, 2018년 4월 17일 EU 집행위원회(the European Commission, EC)는 전자증거 규칙(e-Evidence Regulation) 및

50) 동법에서는 '지정된 국제 협력 약정(designated international cooperation arrangement)'을 범죄수사 또는 기소와 관련된 국제사법공조 규정과 관련이 있으며 국무장관이 법률에 의해 지정한 관련 조약이라고 정의하고 있다. 2019년 7월 현재까지 영국과 약정을 체결한 국가는 없으며, 따라서 동법의 해당 부분은 아직 발효되지 않은 상태이다. 영국은 현재 미국과 관련 약정을 체결하기 위한 협상을 진행하고 있으나 약정의 초안은 아직 공개되지 않고 있다.

전자증거 지침(e-Evidence Directive) 초안을 발표하였고[51], 이에 대한 수정 법안이 2018년 12월 7일 채택되었다. EU의 법안은 유럽의 경찰과 사법기관에 의한 초국경적 전자증거의 접근을 가능하게 하고, 데이터 접근에 대한 기본적인 원칙과 초국경적인 분쟁의 해결방안을 제시하기 위하여 마련되었다.

EU의 전자증거 규칙은 EU 회원국의 수사기관이 다른 EU 회원국 내에 설립된 서비스 제공자에 의해 보관 중인 데이터를 제출하도록 강제할 수 있는 법적 근거를 규정하고 있고 그러한 수단으로 법적 구속력이 있는 유럽 제출 명령(European Production Orders, EPO)과 유럽 보존 명령(European Preservation Orders, EPO-PR) 제도를 도입하고 있다.

또한 지침 초안에서는 모든 온라인 서비스 제공자들로 하여금 EU 회원국 중 해당 서비스 제공자가 설립되었거나 "상당한 연관성(substantial connection)"을 갖는 최소한 하나의 회원국에 법적 대리인을 지정할 것을 요구하고 있다. 이러한 대리인들은 모든 회원국의 법집행기관에게 형사절차상 증거를 제공할 수 있도록 제출명령을 준수할 수 있는 역량을 갖춰야 한다. 역외에 위치한 글로벌 서비스 제공자들은 EU 시민들과 거주자들의 데이터를 점점 더 많이 통제, 관리하고 있으며, 이러한 데이터에 대한 접근권한을 갖고 있기 때문에 이에 대응하기 위해서 지침 초안은 이러한 글로벌 기업들에 대해서 EU가 관할권을 행사할 수 있도록 근거를 마련하고 있다.

규칙 초안은 미국의 CLOUD Act와 상당부분 유사점을 갖는다. 규칙 초안에서는 관할권의 주요한 결정요소로서의 데이터의 저장 위치라는 개념을 버리고, 요청국가가 서비스 제공자가 위치한 다른 회원국의 협력이나 형사사법공조 없이도 다른 회원국 내에 위치한 서비스 제공자에게 직접 데이터의 제출을 강제할 수 있도록 규정하였다[52].

---

51) Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, COM (2018) 225 final (Apr. 17, 2018); Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings, COM (2018) 226 final (Apr. 17, 2018)

52) Jennifer Daskal, "Privacy and Security Across Borders", Yale Law Journal Online, Vol.128, 2019, p.1040.

또한 규칙 초안은 모든 명령이 형사절차의 목적상 필요하며 비례할 것 등의 요건을 포함한 기본적인 요건을 규정하고 있다. 통신 내용 및 송수신 데이터(transactional data)[53]에 관한 제출명령의 경우, 판사, 법원 또는 수사판사에 의해 발부되어야 하고 내용이나 송수신 데이터의 요청은 최소 3년의 징역형으로 규정되어 있는 범죄 및 규칙 초안에 명시된 범죄 유형[54]에만 적용된다[55]. 제출명령과 달리, 보존 명령의 경우 모든 범죄에 대해서 발부가 가능하다.

규칙 초안은 제공자에 대해서 엄격한 기한을 부여하고 제출명령에 대하여 이의제기를 할 수 있는 법적 근거를 제공하고 있다. 특히 초안에서는 서비스 제공자들이 일반적으로 10일 이내에 응답을 할 것을 요구하고 있고, 긴급한 경우에는 6시간 내에 응답할 것을 요구하고 있다[56]. 이는 통상 국제형사사법공조가 10개월, 유럽 수사명령(European Investigation Order)이 120일이 소요되는 것과 비교했을 때 상당히 시간을 단축할 수 있는 제도라고 할 수 있다. 만약 서비스 제공자들이 제출명령 또는 보존명령을 준수하지 않을 경우에는 벌금을 부과하도록 하고 있다. 이의제기의 근거로는 3가지를 규정하고 있는데 여기에는 명령이 불완전하고 "명백한 오류(manifest errors)"를 포함하고 있거나 명령을 집행할만한 충분한 정보를 제공하지 못하는 경우, 명령을 준수하는 것이 불가능한 경우, 또는 해당 명령이 법률 간의 충돌을 야기하는 경우가 포함된다. 이러한 이의제기는 10일 이내에 이루어져야 한다.

4. 유럽평의회 사이버범죄협약

유럽평의회(Council of Europe)의 사이버범죄협약(Convention on Cybercrime)

53) 규칙 초안에서는 데이터의 유형을 가입자 정보, 접근 데이터(서비스 사용 일시, 로그 기록, IP주소 등과 같은 접속기록), 송수신 데이터(메세지의 송수신, 기기의 위치, 날짜, 시간, 기간, 크기, 경로, 포맷, 프로토콜, 압축유형 등 메타데이터) 및 내용 데이터 4가지로 구분하고 있다.

54) 여기에는 온라인 사기, 온라인 아동성착취 및 아동음란물, 정보시스템에 대한 불법 접속, 시스템 방해, 데이터 침해, 불법 감청, 악성 프로그램 등 유럽평의회 사이버범죄협약에서 규정하고 있는 범죄 대부분과 테러리즘 관련 범죄가 포함된다.

55) Jennifer Daskal, "Privacy and Security Across Borders", Yale Law Journal Online, Vol.128, 2019, p.1041.

56) Jennifer Daskal, 앞의 논문, p.1042.

제18조[57]는 두 가지의 제출명령을 규정하고 있는데 하나는 일정한 컴퓨터데이터를 소유 또는 지배하고 있는 사람에 대한 제출명령이고, 다른 하나는 서비스제공자에 대한 가입자 정보의 제출명령에 관한 것이다[58]. 이는 제19조에서 규정하고 있는 압수수색과는 구별되는 것으로, 후자의 경우 수사기관이 해당 컴퓨터데이터에 직접 접근하여 이를 확보하는 수단인 반면 전자는 컴퓨터 데이터를 소유하거나 지배하고 있는 자에게 데이터의 제출을 요구하는 것이다.

사이버범죄협약 제18조 제1항 b호에서는 당사국은 자국 영토 내에서 서비스를 제공하는 서비스제공자에게 서비스제공자가 보유 또는 관리하고 있는 가입자정보를 제출하도록 명령할 권한을 부여하여야 한다고 규정하고 있다. 동 조문과 관련하여 해설서에서는 당사국은 자국 영토 내에 서비스 제공자가 법적으로 또는 물리적으로 소재하지 않는 경우에도 동 조항을 적용할 수 있다고 해석하고 있다[59].

또한 유럽평의회의 사이버범죄협약 위원회(Cybercrime Convention Committee, T-CY)에서는 클라우드 내 데이터에 대한 초국경적 접근 문제에 대하여 연구하기 위하여 2015년 1월부터 클라우드 내의 전자증거에 관한 워킹 그룹(Cloud Evidence Group, 이하 “CEG”) 구성되어 활동을 시작하였다. CEG는 클라우드 및 해외 관할

---

57) 제18조(제출명령) 1. 각 당사국은
a. 어떤 자가 자국의 영토 내에서 컴퓨터 시스템 또는 컴퓨터 데이터 저장매체에 저장되어 있는 특정 컴퓨터데이터를 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. 이 조에서 의미하는 가입자정보란 컴퓨터데이터의 형태로 또는 그 밖의 다른 형태로 포함되어 있는 모든 정보로써, 트래픽데이터나 내용관련데이터 (이외의 것으로)를 제외한, 서비스제공자의 서비스 이용자에 관한 것으로써 서비스제공자에게 보관되어 있고, a) 이용 중인 통신서비스의 종류, 이 서비스에 관련되는 기술적 조치 및 서비스의 기간; b) 가입자의 신원, 주소, 전화와 그 밖의 접속번호, 통신서비스와 관련한 계약이나 협약에 근거해서 이용될 수 있는 요금의 청구 및 지급에 관한 정보; c) 통신서비스와 관련한 계약 또는 협정에 근거하여 존재하는 전기통신시설이 있는 장소에 관한 그 밖의 정보를 통해서 확정될 수 있는 모든 정보를 의미한다.

58) 박희영, “사이버범죄방지조약의 형사절차법 규정의 평가와 현행 형사절차법 관련 규정의 개정방향.”, p.169.

59) 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.

내의 서버에 저장된 디지털 증거 수집에 관한 해결방안에 대한 연구를 수행하였고 이에 대한 결과물로 2016년 9월 T-CY에 "클라우드 내 전자증거에 대한 형사사법적 접근: T-CY에 대한 권고안"이라는 제목의 보고서를 제출하였다[60].

동 보고서에서는 실무상의 문제점으로 국제형사사법공조 절차가 너무 복잡하고 비효율적이라는 점, 국제사법공조는 데이터의 위치를 알고 있다는 것을 전제로 하고 있는데, 클라우드 컴퓨팅에서는 데이터의 위치를 알기가 어렵다는 점, 서비스제공자와 법집행기관 간의 협력이 어렵다는 점 등을 제시하였다. 보고서에서는 이러한 문제에 대한 해결방안 중 하나로 제출명령에 대하여 규정하고 있는 협약 제18조의 해설서(guidance note)에 따른 문언적 해석을 제시하였다. 이에 따르면, 데이터는 여러 관할권에 걸쳐 저장되어 있을 수도 있고 여러 관할권을 이동할 수도 있기 때문에, 데이터의 위치가 관할 성립을 결정짓는 요소는 아니며 데이터가 서비스제공자의 보유 또는 관리 하에 있는 한, 가입자정보가 타국 관할 내에 저장되어 있다고 하더라도 제18조를 적용할 수 있다[61].

Ⅳ. 데이터 접근에 대한 각국 법원의 실행

1. 미국

1) Microsoft Ireland 사건

2013년 12월 미국 연방수사국(Federal Bureau of Investigation, FBI)은 마약밀매 사건과 연관이 있는 이메일 계정에 대해 뉴욕남부지방법원으로부터 수색 영장을 발부받아 마이크로소프트(Microsoft)를 상대로 해당 이메일 계정의 내용을 포함한 관련 정보의 제출을 요청하였다. 그러나 마이크로소프트는 미국 내 서버에 저장되어

60) Cybercrime Convention Committee (T-CY), "Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY," September (2016).

61) Cybercrime Convention Committee (T-CY), "Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY," September (2016).

있는 일부 정보만을 제출하였고, 이메일의 내용과 같은 콘텐츠 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 판시하였으나, 마이크로소프트는 이에 항소하였다.

이 사건의 주된 쟁점은 미국 법집행기관이 마이크로소프트에게 미국 외에 위치한 서버에 저장된 통신 내용 정보를 제출하도록 한 저장통신법 상 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 원칙이다[62].

2016년 7월 미국 제2순회항소법원은 마이크로소프트 사건에서 국내 서비스 제공자에게 미국 밖에 저장된 정보를 공개하도록 요구하는 저장통신법상 영장을 집행하는 것은 법률의 역외 적용에 해당한다고 판시하였다[63]. 첫 번째 단계에서, 항소법원은 입법 당시 의회가 저장통신법에 따라 발부된 영장이 역외 적용될 것을 의도하지 않았다고 보았다. 두 번째 단계에서 항소법원은 저장통신법의 제2703조(a) 조항의 초점은 "저장된 통신 내용의 프라이버시를 보호"하는데 있다고 보았고 이와 관련된 행위는 서비스 제공자에 의한 사용자의 프라이버시 침해이며, 이러한 행위는 영장

62) 이는 미국 연방대법원 판례에 의해 성립된 원칙으로, 동 원칙에 따라 역외적용에 대한 입법기관의 의사가 법률에 명시적이고 분명하게 나타나 있지 않은 한, 해당 국내법은 역외적용 되어서는 안 된다. 연방대법원은 역외 적용을 분석하기 위하여 다음과 같이 2단계의 판단기준을 발전시켜왔는데 첫째, 법원은 역외적용 추정 금지의 원칙이 반증될 수 있는지 여부 즉, 법률에 해당 법률이 역외 적용된다는 명확하고 분명한 표현이 있는지 여부를 판단하여야 한다. 둘째, 사건이 법률의 국내 적용과 관련되는지 여부, 달리 말하면, 사건의 국내 연관성이 역외적용 추정 금지 원칙을 촉발시키지 않기에 충분한지 여부를 판단해야 한다. 법원은 법률의 주된 입법취지가 무엇인지 그러한 주된 취지와 관련된 행위가 어디에서 일어났는지를 파악해야 한다. Dodge, William S. "The Presumption Against Extraterritoriality in Two Steps." AJIL Unbound, Vol. 110, 2016, pp.45-46.

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

에 의해 마이크로소프트가 정부의 대리인으로서 통신 내용을 압수할 때 이루어진다고 보았다.

또한 항소법원은 영장의 대상인 내용이 아일랜드 더블린에 위치한 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[64].

2) Google 사건

FBI는 2건의 온라인 사기 사건 수사 중 발견된 4건의 구글 계정에 대해서 저장통신법 제2703호에 따라 관련 정보를 제출하라는 내용의 영장을 발부받아 이를 집행하였다. 구글은 미국 내에 저장되어 있는 관련 정보를 제출하였지만, 미국 내에 저장되어 있는지 알 수 없는 데이터는 제공하지 않았다. 구글은 해외에 저장된 데이터를 요구하는 영장의 집행은 저장통신법의 불법적인 역외 적용(an unlawful extraterritorial application)을 구성한다고 주장하면서, 해당 명령이 미국 외에 위치한 서버에 저장되어 있는 데이터를 제출하라고 요구하는 한 해당 명령을 거부하겠다고 주장하였다[65].

이 사건에서의 쟁점은 구글에게 미국 외에 위치한 서버에 저장된 통신 및 기타 가입자정보를 제출하도록 한 저장통신법 영장의 집행이 법률의 역외 적용에 해당하는지 여부였으며, 이 쟁점을 분석하기 위해서 법원은 역외적용 추정 금지의 원칙부터 검토하였다.

이 사건에서 법원은 첫 번째 단계에서 저장통신법 제2703조가 역외 적용된다는 명시적 표현이 없다는 점에 대해서 양 당사자가 모두 인정하여 논쟁의 여지가 없다고 보았다. 그러나 법원은 이 사건이 저장통신법의 국내 적용과 관련이 있는지, 즉 법률의 초점과 관련된 행위가 어디에서 발생하였는지를 판단하는 것이 이 사건의

64) 항소심 판결 이후 미국 정부는 상소하였으나 연방대법원에 사건이 계류 중일 당시, 상술한 CLOUD Act가 통과되어 연방대법원에서 사건이 각하되었다. 결국 CLOUD Act를 근거로 마이크로소프트는 FBI에 아일랜드 데이터센터에 저장된 데이터를 제출하였다.

65) In re Search Warrant No. 16-960-M-01 to Google, 232 F.Supp.3d 708 (E.D.Pa. 2017).

쟁점이라고 판단하였다.

정부는 저장통신법 영장은 전통적인 수색영장이 아닌 절차의 한 형태라고 주장하였다. 특정 장소에서 집행되는 전통적인 영장과 달리 저장통신법 영장은 서비스 제공자라는 개인 또는 법인을 대상으로 하며, 따라서 집행 법원이 서비스제공자에 대한 인적 관할권을 가지는 한, 영장은 정보의 위치와 관계없이 제공자가 보유 또는 관리하는 정보에 대해 집행가능하다고 보았다.

법원은 제2703조의 초점은 서비스 제공자가 전자통신 및 기타 가입자정보를 정부에 공개하는 것이라고 보았다. 또한 미국 내 기업 고용자가 미국에 있는 사무실을 벗어나지 않고도 관련 정보를 검토하고 이를 정부에 제출할 수 있기 때문에 영장을 집행하는 모든 절차가 국내에서 이루어진다고 보았고, 저장된 통신에 접근하는 법적 위치는, 데이터센터의 물리적 위치가 아니라 "서비스 제공자가 전자적으로 해당 데이터에 접근할 수 있는 위치"라고 이해하는 것이 더 바람직하다고 보았다[66]. 결론적으로 법원은 구글에게 미국 외에 저장된 데이터를 제공하도록 요구하는 저장통신법 영장의 집행이 적법하다고 판시하였다.

2. 벨기에

1) Yahoo! 사건

벨기에의 경우 미국과 유사한 사건이 있었는데, 2007년 11월 벨기에 검사는 온라인 사기 사건을 수사하면서 Yahoo!를 상대로 IP주소와 이메일 주소, 특정인에 대한 개인 식별가능 정보를 제공할 것을 요청하였다[67]. Yahoo!는 벨기에 국적의 회사가 아니며 현지 사무소도 없으므로 그러한 요청은 국제형사사법공조 절차를 따라야 한다는 이유를 들어 정보 제공을 거부하였다. 그러자 벨기에 검사는 Yahoo!를 사법기관에 대한 협력의무 불이행을 이유로 자국법에 근거하여 기소하였다. 1심에서 Yahoo!는 유죄판결을 받았고 법원에서는 Yahoo!에게 55,000 유로의 벌금을 부과

66) In re Search Warrant No. 16-960-M-01 to Google, 232 F.Supp.3d 708 (E.D.Pa. 2017).

67) Franssen, V. "The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?", European Data Protection Law Review, Volume 3, Issue 4, 2017, p. 538.

하고 해당 데이터를 제공하지 않을 경우, 1일당 10,000유로를 추가로 지불하라고 명령하였다. Yahoo!는 이에 항소했다. 항소의 요지는 3가지였는데 첫째, Yahoo!는 벨기에의 전자통신네트워크도 아니며 전자통신서비스 제공자도 아니므로 벨기에 법의 적용을 받지 않는다. 둘째, Yahoo!는 미국의 기업으로 벨기에에 주둔하는 회사가 아니므로, 벨기에 법의 적용을 받지 않는다. 셋째, Yahoo!가 비록 벨기에의 법의 적용을 받는다고 하더라도, 제출명령은 벨기에의 집행 관할권의 허용되지 않는 역외 적용에 해당한다.

2015년 12월 벨기에 파기원(court of cassation)에서는 모든 Yahoo!의 주장을 배척하고 유죄판결을 확정하였다[68]. 특히 파기원은 Yahoo!가 관련 벨기에 법의 적용을 받는 전자통신 서비스 제공자라고 보았으며, 법적인 정보공개의무는 비록 해당 기업이 벨기에에 물리적으로 존재하지 않더라도 "벨기에 고객에 대해서 경제적인 활동을 목적으로 하는 모든 서비스 운영자 또는 제공자"에게 적용된다고 판시하였다[69].

또한 벨기에의 파기원은 역외 집행에 관한 쟁점에 대해서 이러한 조치가 벨기에 경찰관이나 치안판사 또는 그들의 대리인이 정보를 제공받기 위해서 외국에 직접 갈 필요가 없고, 해외에서의 어떠한 물리적인 행위도 요구하지 않는다고 보았다. 따라서 이는 제한된 범위 내에서의 강제적 조치이며, 이를 집행하는 것은 벨기에 영토 외에서의 어떠한 간섭에도 해당하지 않는다고 판시하였다.

2) Skype 사건

Yahoo! 사건에서는 사법당국이 요청한 정보가 가입자정보에만 한정되어 있었으나, Skype 사건에서 벨기에 법원은 Yahoo! 사건에서의 법원의 입장을 통신 내용에까지 확장하여 적용하였다[70]. 벨기에 검사는 조직범죄 사건을 수사하면서 두 명의 벨기에 거주자 간의 통신과 관련하여 Skype를 상대로 트래픽 데이터와 위치 데이

68) Belgian Court of Cassation 1 December 2015, No.P.13.2082.N.

69) Belgian Court of Cassation 1 December 2015, No.P.13.2082.N.

70) Court of Appeal Antwerp, 15 November 2017, Case No 2016/CO/1006 ; Court of First instance Antwerp, Division Mechelen 27 October 2016, Registry No 1286, Case No 20.F1.105151-12.

터를 제출하고 통신내용을 실시간으로 감청하도록 명령하였다[71]. 또한 이 명령에는 Skype에게 이러한 통신내용을 획득하도록 기술적 지원을 요청하는 내용도 포함되어 있었다.

Skype는 가입자정보는 제공하였으나, 통신 내용의 경우 이를 보유하고 있지 않고 이에 대한 접근권한이 없다고 주장하였다. 또한 Skype의 본사는 룩셈부르크에 있으므로, 통신 내용에 대한 제공 요청은 룩셈부르크 정부에게 하여야 한다고 주장하였다. 1심과 2심 모두 Skype의 주장을 배척하였다. 1심 법원에서는 Skype가 룩셈부르크 회사라고 할지라도, 벨기에에서 서비스를 제공하고 있고 경제활동에 적극적으로 참여하고 있기 때문에 벨기에 관할권의 대상이 된다고 보았다[72].

또한 Yahoo! 사건에서의 벨기에 파기원의 판결을 참조하여, 1심 법원은 벨기에의 수사관이 타국에 가지 않았고, 관련 정보는 벨기에에서 수신한다는 점을 강조하면서 관련 집행 행위가 역외적인 것이 아니라 국내에서 이루어진 것이라고 보았다. 또한 법원은 룩셈부르크 법과의 충돌 가능성이나 룩셈부르크의 주권 침해에 대한 우려 역시 배척하였다. 법원은 Skype가 룩셈부르크가 아닌 벨기에의 영토 내에서 기술적 협력을 제공해야 한다는 점을 들어 룩셈부르크 법과의 충돌 가능성은 이 사건과 관련이 없다고 판시하였다. 항소법원에서도 1심 법원의 입장을 받아들여 원심을 확정하였고 Skype에게 30,000 유로의 벌금을 부과하였다.

3. 우리나라

아직까지 우리나라 법원에서 글로벌 기업에 대해 수사기관이 직접적으로 제공요청을 하여 확보한 데이터의 증거능력이나 이러한 수사관행의 적법성에 대해 다툰 사례는 없다. 그러나 최근 우리나라 대법원에서는 국제형사사법공조 절차를 거치지 않고 중국에 위치한 서버에 저장된 데이터에 수사기관이 직접 접근한 사안에서 이러한 방법이 압수수색의 한 방법으로 허용되는지 여부에 대해서 판단하였

71) Franssen, V. “The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?”, European Data Protection Law Review, Volume 3, Issue 4, 2017, p. 539.

72) Court of First instance Antwerp, Division Mechelen 27 October 2016, Registry No 1286, Case No 20.F1.105151-12.

다. 비록 위의 미국이나 벨기에의 사례와는 사실관계나 쟁점에 있어 차이가 있지만 데이터의 역외 접근을 허용한 사례라는 점에서 본 논문에서 살펴보고자 한다.

1) 국가보안법 위반 사건

이 사건은 수사기관이 적법하게 취득한 인터넷서비스이용자(이하 '이용자')의 이메일 주소와 암호를 이용하여 한국인터넷진흥원의 PC에서 이용자의 중국 이메일 계정에 접속한 뒤 화면캡쳐나 내려받기의 방법으로 전자정보를 압수수색한 사안이다.

이 사건에서는 이용자의 이메일 계정에 대한 접근권한에 갈음하여 발부받은 압수·수색영장에 따라 원격지의 저장매체에 적법하게 접속하여 내려받거나 현출된 전자정보를 대상으로 하여 범죄 혐의사실과 관련된 부분에 대하여 압수·수색하는 것이 허용되는지 여부 및 형사소송법 제120조 제1항에서 정한 '압수·수색영장의 집행에 필요한 처분'에 해당하는지 여부 그리고 이러한 법리가 원격지의 저장매체가 국외에 있는 경우라도 마찬가지로 적용되는지 여부가 문제 되었다.

대법원은 "이용자는 전자정보의 소유자나 소지자로서 압수수색의 대상자가 되고, 이용자의 접근권한에 갈음하여 발부받은 영장에 따라 통상적인 방법으로 원격지 서버에 접속하여 압수수색하는 것은 제공자의 의사에 반하지 아니하며, 압수수색장소도 단말기가 있는 한국인터넷진흥원이라는 점을 들어 원격 압수수색이 적법하다"고 하면서, "원격지 서버가 국외에 있는 경우라도 달리 볼 것이 아니"라 하여 역외 압수수색도 적법하다고 하였다. 즉 대법원은 피의자의 이메일 계정에 대한 접근권한에 갈음하여 발부받은 압수수색영장에 따라 원격지 저장매체에 적법하게 접속하여 내려받거나 현출한 전자정보를 대상으로 하여 영장사실과 관련된 부분에 대하여 압수수색하는 것은 대물적 강제처분 행위로서 허용되며, 영장의 집행에 필요한 처분에 해당한다고 보았으며, 이러한 법리는 원격지 저장매체가 국외에 있는 경우에도 마찬가지로 적용된다고 판시하였다[73].

73) 대법원 2017. 11. 29. 선고 2017도9747 판결.

Ⅴ. 시사점 및 결론

이상에서 데이터 예외주의를 둘러싼 학자들의 찬반대립을 살펴보고 데이터와 관할권에 대한 각국의 실행을 분석하였다. 여기에서는 각국 법원의 실행과 데이터 예외주의 논쟁을 종합하여 시사점을 도출하고자 한다.

위에서 살펴본 벨기에의 Skype와 Yahoo! 사건은 Microsoft 사건에서는 다루어지지 않은 쟁점을 다루었다. Microsoft 사건에서는 미국 법집행기관이 Microsoft에 대한 명확한 관할권을 가진 반면에 Yahoo!나 Skype는 모두 벨기에에 물리적으로 소재하지 않았다. 그럼에도 불구하고 벨기에 법원은 두 회사가 벨기에에서 경제적 활동에 참여하고 서비스를 제공하고 있다는 점을 들어 관할권을 인정하였다. 이 접근방식에 따라서 벨기에에서 광고를 하고 벨기에 국민들에게 맞춤형 기술적 지원을 제공하는 기업들은 벨기에 관할권의 대상이 된다.

Microsoft 사건에서 취해진 접근방식과는 반대로 벨기에 법원은 영토주의는 데이터가 실제 위치한 장소가 아니라, 데이터에 접근하거나 데이터를 수신하는 장소에 따라 결정된다고 보았다. 즉 벨기에 법원은 관련 서비스 제공자가 정보를 제공받는 국가의 영토 내에 물리적으로 소재하지 않더라도 데이터를 제공받는 장소를 영토주의를 결정짓는 요소로 판단하였다. 이러한 접근방식은 영토주의를 잠재적으로 무한정 확장시킬 수 있는 접근 방식이다.

Microsoft 사건에서 쟁점은 영토주의가 데이터가 위치하는 곳에 따라 결정되는지 아니면 서비스 제공자의 위치와 데이터에 접근하는 위치에 따라 결정되는지에 관한 것이었다. 그러나 Yahoo! 사건에서는 데이터와 서비스 제공자 모두 역외에 위치하고 있었음에도 불구하고 벨기에 파기원은 요청한 데이터를 요청 국가의 영토적 경계 내에서 수신하였기 때문에 제출 명령이 국내에서 집행되었다고 보았다. 이러한 접근방식에 따르면 데이터의 위치나 서비스제공자의 위치 등과는 관계없이 모든 제출명령이 국내적으로 집행되었다고 판단할 수 있다. 따라서 이 접근방식에서는 해당 제출명령이 법적인 근거에 따라 이루어졌는지에 대한 쟁점만이 남게 된다.

데이터의 비영토성(un-territoriality)은 데이터 자체의 속성이라기보다는 데이터 관리의 속성이라고 보는 것이 적절하다. 이상에서 살펴본 바와 같이 클라우드 컴퓨

팅의 보편화로 인해서 데이터는 위치 독립성을 가지고 제3자에 의해 그 위치가 통제된다는 점에서 기존의 유무형 자산들과는 차이가 있다. 따라서 데이터가 실재하는 물리적 위치에 따라 관할권 성립을 결정짓는 접근방식을 취하는 것은 현실적으로 무리가 있다.

그러나 서비스제공자의 위치와 관계없이 데이터에 접근하는 위치를 근거로 영토적 관할권의 성립을 결정한 벨기에 법원의 접근 방식 역시 문제가 있다. 이러한 국내 관할권의 무제한적인 확장으로 인해 타국의 주권을 침해할 우려가 있고 타국의 법률과의 충돌 가능성도 배제할 수 없다. 또한 이러한 접근방식은 국가가 타국의 충돌되는 이해관계는 고려하지 않고 모든 데이터에 대한 접근을 정당화시킬 우려가 있다.

즉, 자국민의 데이터에 대한 접근을 규제하고 있는 다른 국가의 주권을 침해할 수 있고 타국 국민의 프라이버시나 기본권을 침해할 소지도 있다. 또한 미국이나 대부분의 유럽 국가들에서 법으로 규정하고 있는 대항입법(blocking provisions)을 위반할 소지도 있다.

데이터는 적법하고 유효한 접근권한을 가진 자(개인 또는 서비스제공자)라면 언제든지 세계 어디에서나 접근이 가능하다. 따라서 데이터에 대해 관할권 성립을 주장할 때에는 기존의 영토주의적 접근방식을 따르기보다는 데이터의 “접근권한”의 개념으로 접근하는 것이 바람직하다. 다만 국가보안법 사건에 대한 대법원 판결 사례에서와 같이 수사기관이 해외에 저장된 데이터에 대한 접근권한을 획득하여 직접 접근한 경우, 수사기관이 저장된 데이터를 조작하거나 변조할 가능성이 있다는 우려가 제기될 수 있다. 따라서 이러한 우려를 불식시키고 데이터의 위변조를 사전에 예방하기 위해서는 제3의 기관에 의한 사법적 통제 방안에 대한 연구도 후속적으로 수행되어야 할 것이다.

참고문헌

1. 국내문헌

Jihyun Park, International trend against cybercrime and controversy over the F.B.I.'s practice of “Extra-territorial Seizure of Digital Evidence”, 국제법학회논총 제49권 제3호, 2004.

송영진, 미국 CLOUD Act의 통과와 역외 데이터 접근에 대한 시사점, 형사정책연구 제29권 제2호, 2018.

이수용, 임규철, 역외 압수수색의 절차적 위법성에 대한 비판적 소고 - 대법원 2017. 11. 29. 선고 2017도9747 판결을 중심으로, 비교법연구 제18권 제2호, 2018.

이순옥, 디지털 증거의 역외 압수·수색 - 대법원 2017. 11. 29. 선고 2017도9747 판결을 중심으로, 중앙법학 제20집 제1호(통권 제67호), 2018.

정대용·김성훈·김기범·이상진, 국제협력을 통한 디지털 증거의 수집과 증거능력, 형사정책연구 제28권 제1호, 2017.

정소연, 디지털 증거의 역외 압수수색에 대한 법적 고찰, 디지털포렌식연구 제11권 제1호, 2017.

2. 해외문헌

Ahmed Ghappour, “Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web”, Stanford Law Review, Vol.69, 2017.

Andrew Keane Woods, “Against Data Exceptionalism”, Stanford Law Review, Vol.68, 2016.

Dan Jerker B. Svantesson, “Against ‘Against Data Exceptionalism’”, Masaryk University Journal of Law and Technology, Vol.10, 2016.

Franssen, V. “The Belgian Internet Investigatory Powers Act - A Model to

Pursue at European Level?", European Data Protection Law Review, Volume 3, Issue 4, 2017.

Jennifer Daskal, "The Un-Territoriality of Data", The Yale Law Journal, Vol.125, 2015.

Jennifer Daskal, "Border and Bits", Vanderbilt Law Review, Vol.71, 2018.

Jennifer Daskal, "Privacy and Security Across Borders", Yale Law Journal Online, Vol.128, 2019.

Orin S. Kerr & Sean D. Murphy, "Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?", Stanford Law Review Online, Vol.70, 2017.

Paul M. Schwartz, "Legal Access to the Global Cloud", Columbia Law Review, Vol.118, No.6, 2018.

Zachary D. Clopton, "Data Institutionalism: A reply to Andrew Woods", Stanford Law Review Online, Vol.69, 2016.

A Critical Review on the Government Access to Cloud Data : "Data Exceptionalism" Debate and Legal Practice

Song, Young-jin*

In the past, when law enforcement agencies investigated crimes, most of the relevant evidence was tangible and the evidence was also located in their jurisdiction. In addition, if evidence or witnesses are located in another jurisdiction, it has been a traditional method to obtain the cooperation of the relevant country through the Mutual Legal Assistance(hereinafter "MLA") process to collect them. However, with the increasing need to collect intangible data stored abroad for criminal investigations today, it has become common practice for law enforcement agencies to request service providers who actually hold or manage data rather than traditional MLA procedures. However, advances in cloud computing technology are also causing most global companies to store data in the cloud, making it impossible to know the physical location of data. These issues are being raised in courts of different countries, various precedents are emerging, and even among scholars are being debated. In addition, countries are trying to resolve the issue by law-making. In this paper, it was intended to critically review the "data exceptionalism" debate on the issue of deriving in accessing extraterritorial data, particularly cloud data, and the implementation of each country to solve this problem through legislation and precedent. In conclusion, due to the nature of data management, it is not possible to apply traditional territoriality approach to cloud data, and the establishment of jurisdiction should be judged with access authority of data. In addition, referring to other legislative examples, Korean government also needs to amend or enact relevant legislation to provide clear legal basis for access to extraterritorial data by

* Department of Police Science, International Cybercrime Research Center, Korean National Police University

law enforcement agencies.

❖ Key words: Cloud Computing, Data Exceptionalism, Extraterritorial Data, Cybercrime, Digital Evidence

투고일 : 8월 30일 / 심사일 : 9월 20일 / 게재확정일 : 9월 20일