형사정책연구 Korean Criminological Review
제32권 제1호(통권 제125호, 2021 · 봄)

외국의 정보통신 서비스 제공자에 대한 통신 자료 요청 방법과 형사법적 문제

박다온*

국 | 문 | 요 | 약

우리 국민 대다수가 일상생활에서 글로벌 IT 기업의 서비스를 활발히 이용함에 따라 정보통신 서비스를 이용한 범죄 또한 빈번해졌다. 이는 IT 기업이 보유하는 서비스 가입자 정보, IP 접속 기록 등 통신 자료를 확보하는 것이 수사의 관건이 된다는 것을 의미한다. 국내 서비스 제공자의 경우 수사기관은 통신자료제공요청이나 압수수색 영장 등을 통해 자료를 확보할 수 있을 것이다. 그런데 대상 서비스 제공자가 외국 법인인 경우 우리 수사기관은 어떤 방법으로 자료를 확보하고 있으며, 현행 절차는 과연 형사법적으로 적정한가? 본고에서는 이에 답하고자 경찰청의 외국 IT 서비스 제공자에 대한 통신 자료 요청 방법의 실태를 조사하고 그 적정성을 검토하였다.

먼저, 국외 소재 통신 자료를 취득할 수 있는 일반적인 방법들을 먼저 살펴보고, 그중 외국 서비스 제공자에게 직접 자료를 요청하는 방법을 구체적으로 조사하였다. 조사 대상으로는 미국 법인의 경우 페이스북, 구글, 트위터, 애플을 선정하였으며, 미국 외 법인으로는 텔레그램과 라인을 선정하였다. 나아가 현행 자료 요청 방법과 관련한 형사법적 문제로서 외국 서비스 제공자에게 제시하는 압수수색 영장 관련 문제와 회신받은 자료의 증거능력 관련 문제를 제기하였다. 즉, 우리 수사기관이 외국 서비스 제공자에 대해 영장을 제시하는 것이 형사관할권을 행사하는 강제수사인지 검토한 결과 아니라는 결론을 내었으며, 그러한 공조 방식의 법적 근거가 명확하지 않다는 점, 디지털 증거의 동일성 및 무결성을 담보하는 조치가 부재한다는 점에서 증거능력이 문제 될 여지가 있다는 점을 거론하였다. 결론에서는 현행 절차의 문제를 극복할 수 있는 현실적 대안으로서 사이버범죄협약 가입을 제시하면서 논의를 정리하였다.

DOI : https://doi.org/10.36889/KCR.2021.3.31.1.167.

❖ 주제어 : 글로벌 IT 기업, 통신 자료, 디지털 증거(전자적 증거), 국제형사사법공조, 사이버범죄협약

* 경찰대학 국제사이버범죄연구센터 전임연구관, ekdhs777@police.go.kr.

Ⅰ. 서론

스마트폰의 대중화와 소셜 미디어의 대유행은 전 세계 이용자에게 다양한 정보통신 서비스를 제공하는 이른바 '글로벌 IT 기업'을 탄생시켰다. 우리 국민 또한 대다수가 일상생활에서 정보검색부터 소셜 네트워킹 서비스, 클라우드 서비스, 쇼핑 및 간편 결제까지 글로벌 IT 기업의 서비스를 활발히 이용하고 있다. 그러나 사람들이 정보통신 서비스를 일상적으로 사용하는 만큼 이러한 서비스를 이용한 범죄 또한 빈번해졌다. 컴퓨터와 네트워크가 주요 수단인 사이버 범죄뿐 아니라, 물리적 범죄와 관련하여서도 수사기관이 IT 기업의 플랫폼에서 수사 단서를 구해야 하는 경우가 많다. 즉, IT 기업이 보유하는 서비스 이용자의 가입 정보, IP 접속 기록, 등록 기기정보 등 통신 자료를 확보하는 것이 수사의 관건이 되는 경우가 많다. 인터넷을 매개로 전 세계적 연결성이 극도로 높아지고 있는 현 추세를 볼 때 가까운 미래에 수사기관은 거의 모든 범죄의 증거가 컴퓨터 시스템에 전자적 형태로 저장된 현실에 직면할 것이다.

가입자 정보 등 통신 자료를 국내 사업자가 보유하고 있다면, 전기통신사업법에 따른 통신자료제공요청이나,[1] 통신비밀보호법에 따른 통신사실확인자료제공요청을 통해 자료를 확보할 수 있다.[2] 개인정보의 민감도가 높은 통신 내용의 경우에는 압수수색 영장을 통해 자료를 확보하며, 통신비밀보호법 제5조의 요건을 충족하는 경우 실시간 감청 등 통신제한조치도 가능하다. 그러나 서비스 제공자가 외국 법인이라면 어떤 방법으로 통신자료를 확보할 수 있는가? 법인에는 일반적으로 설립 준거법주의나 본사 소재지주의에 따른 국적이 적용되기 때문에,[3] 국내에 서비스를 제공하더라도 외국에서 설립됐거나 외국에 본사가 소재한다면 외국 법인에 해당한다. 그렇다면 수사기관의 실무상 외국 법인에 대한 통신 자료 요청은 어떤 절차와 방법으로 진행되고 있는가? 현행 절차는 과연 형사법적으로 적정한가?

본고에서는 위 의문에 답하고자 우리 경찰청의 외국 IT 서비스 제공자에 대한 통신자료 요청 방법의 실태를 조사하고 그 적정성을 검토하였다. 이를 위해 국외 소재 통신

1) 전기통신사업법 제83조 제3항.
2) 통신비밀보호법 제2조 제11호, 동법 제13조 제1항.
3) 정인섭, 「신국제법 강의(제7판)」, 박영사, 2017, 215면.

자료를 취득할 수 있는 일반적인 방법들을 먼저 살펴보고, 그중 외국 서비스 제공자에게 직접 자료를 요청하는 방법을 구체적으로 조사하였다. 조사 대상 기업으로는 우리 국민 다수가 이용하는 글로벌 IT 기업을 선정하여 미국 법인과 미국 외 국적의 법인으로 분류하였는데, 미국 법인의 경우 페이스북, 구글, 트위터, 애플을 선정하였으며, 미국 외 법인으로는 텔레그램과 라인을 선정하였다. 조사 방법으로는 해당 기업들의 통신 자료 제공 정책을 조사하는 한편 경찰청에서 글로벌 IT 기업 대상 공조 업무를 담당하는 실무자를 인터뷰하였다. 나아가 그와 관련하여 발생하는 형사법적 문제들을 국제사회의 논의에 비추어 고찰하고자 한다. 본고에서 제기하는 형사법적 문제는 크게 외국 서비스 제공자에게 통신 자료를 요청할 때 제시하는 영장 관련 문제와 회신받은 자료의 증거능력 관련 문제이다. 마지막으로 결론에서는 현행 통신 자료 요청 절차의 문제를 극복할 수 있는 현실적 대안으로서 사이버범죄협약(Convention on Cybercrime) 가입을 제시하면서 논의를 정리하고자 한다.

Ⅱ. 국외 소재 통신 자료의 취득 방법

1. 국제형사사법공조

외국 관할에 있는 형사 증거를 획득하기 위한 대표적인 방법으로 국제형사사법공조(Mutual Legal Assistance, 이하 “MLA”라고 한다)가 있다. 이는 개별 국가와 체결한 형사사법공조조약에 근거하여 형사사건의 수사 또는 재판과 관련된 소재 수사, 증거 수집, 증거물 인도, 진술 청취, 압수·수색 등 협조를 제공하거나 제공받는 것을 말한다.[4] 우리나라는 국제형사사법공조법이라는 국내법으로 공조 범위와 절차 등을 규율하나, 동법 제3조에서 공조조약에 이 법과 다른 규정이 있는 경우에는 그 규정에 따른다고 하여 조약이 우선함을 명시하고 있다. 우리나라는 2020년 기준으로 77개국과 형사사법공조조약이 체결되어 있으며(발효 74개국),[5] 조약을 체결하지 않은 국가의 경우에도 동일하거

4) 국제형사사법공조법 제2조, 동법 제5조.

5) 법무부, 「2020년 법무연감」, 2020, 269면.

나 유사한 사항에 관하여 한국의 공조 요청에 따른다는 요청국의 보증이 있는 경우에는 공조를 진행할 수 있도록 상호주의 원칙에 입각하고 있다.[6)]

MLA 절차는 개인의 권리를 보호하기 위한 일련의 법적 요건을 충족한다는 점을 보증할 수 있도록 고안되었으므로 MLA를 통해 확보한 데이터를 형사절차의 증거로 사용할 수 있다는 데 다툼이 없다.[7)] 또한 국제조약이므로 체결국 간 강제력이 있으며, 절차가 표준화되어 있다는 장점이 있다.[8)] 그러나 MLA는 법무부가 중앙기관이고 외교 경로를 통해야 하므로 수사기관에서 법무부 및 외교부를 거쳐 상대 국가로 절차가 진행되는데 평균적으로 1년 이상의 긴 시간이 소요된다.[9)] 따라서 휘발성이 강한 전자 증거를 확보하기 위한 방법으로 적합하지 않다. 글로벌 IT 기업이 접속 기록 등의 데이터를 보관하는 기간은 일반적으로 90일이므로 절차가 마무리될 즘에는 데이터가 이미 삭제돼있을 가능성이 크다.[10)] 사이버범죄협약 위원회(T-CY) 또한 2014년에 MLA의 기능을 구체적으로 평가한 결과 MLA 절차는 지나치게 복잡하고 긴 시간이 소요되므로 사이버 범죄나 전자 증거가 필요한 범죄에 대처하기에 비효율적이라는 결론을 내었다.[11)]

뿐만 아니라, 서버가 여러 국가의 관할에 있어 데이터의 위치를 알 수 없는 등 영토주의를 적용할 수 없는 경우에도 MLA는 가능한 방법이 아니다.[12)] 특히, 근래에는 여러 국가에 소재한 데이터 센터에 데이터를 분산하여 보관하는 형태의 클라우드 시스템이 발전함에 따라 어느 국가에 필요한 데이터가 있는지 수사기관이 알지 못하는 경우도 발생하고 있다.[13)]

---

6) 국제형사사법공조법 제4조.

7) Jan Kleijssen and Pierluigi Perri, “Cybercrime, Evidence and Territoriality: Issues and Options.” Netherlands Yearbook of International Law 2016. The Hague: T.M.C. Asser, 2017, 147-173, 165면.

8) 정대용·김성훈·김기범·이상진, “국제협력을 통한 디지털 증거의 수집과 증거능력”, 형사정책연구 28(1), 2017, 49-77, 54면.

9) 송영진, “미국 CLOUD Act 통과와 국경 없는 데이터 접근에 대한 시사점”, 형사정책연구 29(2), 2018, 149-172, 163면.

10) 국내 사업자 또한 로그 기록 등의 보관 기간은 3개월이다(통신비밀보호법 시행령 제41조).

11) Jan Kleijssen and Pierluigi Perri, “Cybercrime, Evidence and Territoriality: Issues and Options.” Netherlands Yearbook of International Law 2016. The Hague: T.M.C. Asser, 2017. 147-173, 162면.

12) Jan Kleijssen and Pierluigi Perri,, 앞의 논문, 162면.

13) 이순옥, “인터넷서비스제공자가 보관한 정보에 대한 압수·수색 절차”, 법학논문집 제43집 제3호,

2. 외국 수사기관에 대한 공조 요청

국제형사사법공조법은 국제형사경찰기구(International Criminal Police Organization, 이하 "인터폴"이라고 한다)를 통해 국제범죄의 정보 및 자료 교환, 동일증명 및 전과조회, 사실 확인 및 조사 등 외국과 상호 협력할 수 있다고 규정하고 있다.[14] 인터폴은 우리나라를 포함하여 194개국이 가입한 세계 최대의 형사경찰 간 협력기구로서,[15] 인터폴 헌장과 각 회원국의 국내법이 허용하는 한도 내에서 국제성 범죄에 관한 정보를 교환하고, 범죄의 예방과 진압을 위해 상호 협력하는 역할을 한다.[16] 인터폴은 가입국별로 국가중앙사무국(National Central Bureau, NCB)을 지정하도록 하고, 모든 국가중앙사무국이 'I-24/7 네트워크'라는 망을 통해 직접 통신할 수 있도록 시스템을 구축하였다.[17] 한국은 경찰청 외사국에 국가중앙사무국을 설치하여 경찰, 검찰, 특별사법경찰 등 각 수사기관의 요청을 취합한 후 대상 국가에 협력을 요청하는 전문을 발송한다.[18] 수사기관끼리 직접 통신하므로 외교경로를 거치는 MLA보다 상대적으로 빠르게 회신을 받을 수 있다. 그러나 인터폴은 국제법상 협정이 아니므로 인터폴을 통한 요청은 강제성이 없으며, 공조의 범위도 한정적이다.[19] 즉 압수·수색이나 피의자 신문 등 적극적인 수사를 공조하는 데에는 한계가 있다.

이에 한국 경찰청은 미국, 영국, 네덜란드, 프랑스, 독일 등 주요 국가의 수사기관과 사이버범죄 대응 및 수사에 특화된 협력약정을 체결하여 직접 협력하기도 한다.[20] 특히 사이버 범죄는 초국경적 범죄로서 국제협력이 중요하다는 점에 국제적 공감대가 형성됨

153-190, 168면.

14) 국제형사사법공조법 제38조.

15) 인터폴 웹사이트, https://www.interpol.int/Who-we-are/Member-countries (2021. 1. 20. 최종 검색).

16) 정대용·김성훈·김기범·이상진, "국제협력을 통한 디지털 증거의 수집과 증거능력", 형사정책연구 28(1), 2017, 49-77, 53면.

17) 인터폴 웹사이트, https://www.interpol.int/Who-we-are/Member-countries (2021. 1. 20. 최종 검색).

18) 정대용·김성훈·김기범·이상진, "국제협력을 통한 디지털 증거의 수집과 증거능력", 형사정책연구 28(1), 2017, 49-77, 53면.

19) 오세연·송혜진, "초국가적 범죄의 대응강화를 위한 인터폴의 효율적 활용방안에 관한 연구", 한국재난정보학회논문집 10(4), 2014, 560-566, 562면.

20) 경찰청, 「2020 경찰백서」, 2020, 237면.

에 따라 사이버범죄 대응을 위한 국제회의, 심포지엄, 국제교육 등이 다수 개최되어왔다. 이를 통해 각국 수사기관 간 교류 협력이 증가하면서 수사기관 간 공조가 활성화되고 있다.[21] 현재 수사기관 간에는 사이버범죄 관련 정보 교류뿐만 아니라 통신 자료 보존 요청이나 디지털 증거의 제공도 이루어지고 있다.[22] 예를 들어, 최근 큰 반향을 일으킨 '텔레그램 n번방 사건'[23]의 피해 영상물이 미국의 메신저 앱인 '디스코드'를 통해 유통되었는데, 우리 경찰청은 미국 국토안보수사국(Homeland Security Investigations, HSI)의 협조를 받아 유포자를 특정할 수 있었다.[24]

한편 국제적으로는 흔히 '공조 작전(Joint Operation)'이라고 하여 특정 사건에 대해 여러 국가가 참여하여 정보를 교류하며 피의자를 검거하는 형태의 공조수사가 이미 활발히 이뤄지고 있다. 사이버범죄의 경우에는 인터폴의 사이버 퓨젼 센터(Cyber Fusion Center), 유로폴의 사이버범죄 센터(European Cybercrime Center, EC3), 국제아동음란물대응협의체(Virtual Global Taskforce, VGT)[25] 등 국제기구가 공조수사를 조율하고 지원하는 중심 역할을 하고 있다.

3. 외국의 서비스 제공자에 대한 자료 요청

사이버범죄협약 위원회의 'Cloud Evidence Group(CEG)'[26]은 일반적으로 형사당국이 범죄 수사 시 필요한 데이터의 유형을 가입자 정보(subscriber information), 트래픽 데이터(traffic data), 통신 내용(contents)으로 분류하였다.[27] 이중 서비스 이용자의 계

21) 정대용·김성훈·김기범·이상진, "국제협력을 통한 디지털 증거의 수집과 증거능력", 형사정책연구 28(1), 2017, 49-77, 55면.

22) 정대용·김성훈·김기범·이상진, 앞의 논문, 55면.

23) 텔레그램의 비밀대화방에서 피해자들을 협박해 촬영한 성착취물을 유포한 사건으로, 이렇게 개설된 대화방은 박사방, 고담방, Project N방, 1~5번방 등 수 개가 있어 n번방으로 통칭하고 있다.

24) 연합뉴스(2020. 4. 7.), "해외 메신저라 검거 안 된다?…디스코드 국제공조로 수사 확대", https://www.yna.co.kr/view/AKR20200407102400060 (2020. 12. 27. 최종 검색).

25) 온라인 아동 성착취물에 대한 수사, 정보 공유, 피해아동 구호를 위해 2003년 설립된 국제적 민관협의체로, 2020년 기준 13개 국가, 국제기구 및 19개 민간기업이 가입돼있다. 한국은 경찰청에서 2013년 가입하여 지속적으로 참여하고 있다.

26) 사이버범죄협약 위원회(T-CY)는 어떻게 국가주권 원칙과 인권을 보장하면서도 형사사법적 목적을 위한 전자적 증거를 합법적, 효과적으로 확보할 수 있는지에 대한 고민을 다루기 위해 2014년에 'Cloud Evidence Group(CEG)'을 만들었다.

정 정보 및 접속 IP주소 등 가입자 정보는 사이버 범죄 및 전자적 증거와 관련하여 국제적 수사 환경에서 가장 빈번하게 요청되는 정보이다.[28] 또한 가입자 정보는 트래픽 데이터나 통신 내용에 비해 개인정보 침해 요소가 적으므로 일부 국가에서는 수사 시 이에 접근할 수 있는 요건이 완화되어 있다.[29] 따라서 현재 다수 글로벌 IT 기업들은 서비스를 제공하는 타국의 권한 있는 형사당국이 가입자 정보를 요청하는 경우 직접 이에 회신하고 있다. 즉 통신 내용이 아닌 가입자 정보나 일부 트래픽 데이터의 경우에는 업체의 내부적 기준을 충족하면 MLA 절차를 거치지 않고도 이를 제공한다. 이 내부적 기준은 자국법이 허용하는 범위 내에서 업체마다 각기 다르게 정하고 있는데, 요청 방법과 회신 기준을 제시하기도 하며, 요청서 양식을 정해놓고 그에 따라 요청하게끔 하는 업체도 있다. 업체가 제시하는 요건을 충족하면 신속하게 자료를 획득할 수 있다. 데이터 관리 주체에게 직접적으로 필요한 데이터를 요청하고 회신받는다는 점에서 절차가 최소화되어 효율적이다.

사이버범죄협약 가입국을 대상으로 한 조사 결과, 협약 가입국은 애플, 페이스북, 구글, 마이크로소프트, 트위터, 야후 등 미국 서비스 제공자에게 매년 100,000건 이상의 통신 자료 요청을 보내고 있으며, 이들은 60% 가량의 사건에 대하여 데이터를 공개하였다.[30] 이러한 자발적 협조는 수사에 유용하지만, 서비스 제공자가 데이터 제공요청에 관한 정책과 절차를 변경하는 경우가 잦기 때문에 예측 가능성을 저해하며, 일부 국가에서는 이러한 방식으로 얻은 데이터의 증거능력이 없다.[31] 또한, 서비스 제공자의 자발적인 데이터 제공은 데이터 보호와 기밀성에 대한 우려를 야기한다.

우리나라의 경우 경찰청이 MLA나 외국 정부기관을 거치지 않고 외국 서비스 제공자로부터 직접 통신 자료를 회신받은 것은 2012년 주한미군의 페이스북 협박 사건으로 보인다.[32] 이는 주한미군이 타인 명의 페이스북 계정을 이용하여 한국인 여성과 채팅 중

27) Jan Kleijssen and Pierluigi Perri, “Cybercrime, Evidence and Territoriality: Issues and Options.” Netherlands Yearbook of International Law 2016. The Hague: T.M.C. Asser, 2017, 147-173, 160면.

28) Cybercrime Convention Committee (T-CY), “Rules on obtaining subscriber information, report adopted by the T-CY at its 12th Plenary”, 2014, 28면.

29) Jan Kleijssen and Pierluigi Perri, 앞의 논문, 160면.

30) Jan Kleijssen and Pierluigi Perri, 앞의 논문, 164면.

31) Jan Kleijssen and Pierluigi Perri, 앞의 논문, 164면.

성관계에 응하지 않으면 나체 영상 등을 유포하겠다며 협박한 사건이었다.[33] 당시 피의자를 특정할 수 있는 단서는 페이스북 접속기록밖에 없었기 때문에 한국 경찰청은 페이스북에 이 자료를 받을 수 있는지 문의하였고, 한국 법원의 유효한 허가서가 있으면 가능하다는 답변을 들었다.[34] 이에 경찰청은 인천지방법원에서 발부한 통신사실확인허가서와 영문 번역본을 페이스북 본사에 이메일로 송부하여 해당 계정의 IP 접속기록 140건을 회신받았다.[35] 이후 경찰청은 다른 글로벌 기업에도 직접 통신 자료 요청을 보내기 시작하여 많은 사건에서 결정적인 수사 단서를 확보할 수 있었다.

Ⅲ. 외국 서비스 제공자에 대한 통신 자료 요청의 실태

1. 미국

가. 페이스북

우리 국민 다수가 이용하는 대표적인 소셜 미디어가 페이스북과 인스타그램이다. 페이스북은 미국 캘리포니아주에 본사를 둔 미국 법인이며, 2012년 인스타그램을 인수하여 양자는 데이터 제공에 관한 정책이 같다. 페이스북은 당사 서비스 약관과 연방 저장통신법(Stored Communications Act, SCA), 18 U.S.C. § 2701부터 § 2712까지 준거법에 의거하여 사법당국에 계정 기록을 공개한다고 밝히고 있다.[36] 타국의 자료요청과 관련해서는, "미국 외 지역 관할권에서의 법적 요청이 수반되고, 해당 관할권의 법에 의해 필요성이 인정되며, 그 지역 내의 사용자들에게 영향을 미침과 동시에 국제적으로 용

32) 정대용·김성훈·김기범·이상진, "국제협력을 통한 디지털 증거의 수집과 증거능력", 형사정책연구 28(1), 2017, 49-77, 60면.

33) 경인일보(2012. 7. 12.), "20대 여성에 "알몸동영상 유포하겠다" 주한미군, 이번엔 '협박'", http://www.kyeongin.com/main/view.php?key=664982 (2021. 1. 5. 최종 검색).

34) 전현욱·김기범·조성용·Emilio C VIANO, 「사이버범죄의 수사 효율성 강화를 위한 법제 개선방안 연구」, 경제·인문사회연구회 미래사회 협동연구총서, 2015, 173면.

35) 전현욱·김기범·조성용·Emilio C VIANO, 앞의 연구집, 173면.

36) 페이스북 웹사이트, https://www.facebook.com/safety/groups/law/guidelines (2021. 2. 1. 최종 검색).

인되는 기준에 부합한다고 판단될 때 해당 관할권의 요청을 받아들이는 경우" 정보를 제공할 수 있다고 밝히고 있다.[37]

페이스북과 인스타그램은 통신 자료 요청 시 요청하는 국가의 영장을 요구하는데, 법집행기관 전용 포털을 운영하며 여기에 영장의 스캔본과 영문 번역본을 PDF 파일로 업로드 하도록 하고 있다. 우리 경찰청은 압수 장소를 페이스북 본사 소재지[38]로 기재하여 법원으로부터 일반 압수수색 영장을 발부받아 위 포털에 업로드하고 있다. 포털 접속 시 초기화면에서 '권한 있는 법집행기관 또는 수사를 수행하는 정부기관 직원으로서 정식 요청을 하는 것임'[39]에 체크한 후 수사관의 이메일 주소를 입력하여야 한다. 입력한 주소로 인증 페이지에 접속할 수 있는 링크를 포함한 메일이 전송되는데, 이 인증 페이지에서 수사관의 개인정보를 입력하고 나서 요청서를 작성하거나 처리내역을 확인할 수 있다. 회신할 때에는 자료를 다운로드할 수 있는 URL을 수사관의 이메일로 전송해준다.

페이스북은 매년 투명성 보고서(Transparency Report)를 발간하여 국가별 수사기관의 요청 건수와 제공 건수를 공개하는데, 한국의 요청 건수는 지속적으로 증가하고 있으며, 2020년 상반기에 총 833건 요청하여 이중 61%에 대해 회신 받았다.[40] 경찰청 업무담당자에 의하면, 요건 충족 시 성명, 이메일, 휴대전화번호, 가입 일시 및 IP, 탈퇴 일시 및 IP 등의 가입자 정보와 요청기간 중 계정에 접속한 IP 기록을 회신해주고 있다. 그러나 페이스북은 통신 내용은 제공해주지 않으며, 통신 내용 공개를 강제하려면 MLA에 따른 요청이 필요하다는 입장이다.[41]

나. 구글

구글 검색, 전자 결제(Google Wallet), 지메일(Gmail), 유튜브(Youtube), 구글 드라이브 등 우리나라 대다수 국민들이 구글의 서비스를 이용하고 있을 것이다. 유튜브만 해

37) 페이스북 웹사이트, https://www.facebook.com/about/privacy (2021. 2. 1. 최종 검색).

38) Facebook, Inc., 1601 Willow Road, Menlo Park, CA 94025.

39) "I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request"을 의역함.

40) 페이스북 웹사이트, https://govtrequests.facebook.com/government-data-requests/country/KR (2021. 2. 1. 최종 검색).

41) 페이스북 웹사이트, https://www.facebook.com/safety/groups/law/guidelines (2021. 2. 1. 최종 검색).

도 이미 2017년에 한국 이용자 수가 2천 3백만 명으로 네이버 앱 이용자 수를 뛰어넘었다.[42] 구글은 미국 캘리포니아에 본사를 둔 미국 법인으로 전 세계 이용자에게 다양한 IT 서비스를 제공하고 있다.

구글이 2014년 한국 법집행기관에 제시한 가이드라인에 의하면, 구글로부터 사용자 정보를 받기 원하는 경우 한국 판사의 서명을 받은 유효한 수색영장을 제출하라고 기재되어 있으며,[43] 압수 장소는 본사 소재지[44]로 기재하도록 하고 있다.[45] 경찰청 업무 담당자에 의하면, 경찰청은 법원으로부터 일반 압수수색영장을 발부받아 그 스캔본과 수사관 신분증 사진을 첨부하여 법집행기관 전용 포털에 업로드 하는 방식으로 자료를 요청하고 있다. 이때 영장의 압수장소를 잘못 기재하거나 영장의 유효기간이 만료된 경우 자료 제공이 거절된다.

구글 또한 전 세계 정부기관으로부터 받은 자료 요청 건수 관련 정보를 보고서로 발간한다. 이에 따르면 한국은 2019년 하반기에 1,184건 요청하여 약 71%에 대한 자료를 받았으며, 2020년 상반기에는 더 증가한 수치인 2,958건을 요청하여 약 81%에 대한 자료를 회신 받았다.[46] 경찰청 업무 담당자에 의하면, 구글은 요건 충족 시 성명, 이메일, 휴대전화번호, 가입 및 탈퇴 일시 등 가입자 정보와 IP 접속기록을 회신해주며, 가입자가 구글 페이먼트 이용 시 결제 내역도 회신해준다. 그러나 통신 내용 및 위치정보 등은 제공해주지 않으므로 이는 MLA를 통해서만 확보할 수 있다.

다. 트위터

트위터는 메시지 기반 소셜 네트워크 서비스를 제공하는 글로벌 기업으로 미국 캘리

---

42) Business Korea(2018. 1. 5.), “YouTube Ranks 1st in S. Korea for Number of Users”, http://www.businesskorea.co.kr/news/articleView.html?idxno=20222 (2021. 2. 1. 최종 검색).

43) “In order to obtain user information from Google, please submit a valid search warrant, signed by a judge or magistrate in Korea”을 의역함.

44) Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043, USA.

45) 경찰청 내부 자료(2014. 3. 29.), “Legal Requests for User Data, Google Inc. Process for Korean Authorities Requesting User Data”.

46) 구글 투명성 보고서, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:KR;time:&lu=user_requests_report_period (2021. 2. 14. 최종 검색).

포니아에 본사가 있다. 트위터는 한국에 트위터 코리아 유한회사를 두고 있지만, 트위터 코리아는 가입자 정보를 제공할 수 있는 권한이 없으며 관련 업무는 미국 본사에서 담당한다.[47]

트위터는 한국 법집행기관에 대한 가이드라인에서 "기본적으로 국제형사사법공조조약에 따라 미국 법원이 발부하는 가입자 정보 제공 요청에 따르나, 예외적으로 살인, 강간, 납치, 아동 유괴·성착취 등 강력범죄에 한하여 대한민국 법원의 영장에 따를 수 있다"고 하여, 구글, 페이스북 보다 제한적 범위에서 통신 자료를 제공하고 있다.[48] 경찰청 업무 담당자에 의하면, 트위터는 정당한 영장을 제시하였고, 강력범죄에 해당한다고 판단하면 가입자 정보 및 IP 접속기록을 회신해주나, 통신 내용은 MLA 절차를 거치지 않으면 제공하지 않는다.

법집행기관은 트위터의 법집행기관 전용 포털[49]을 통해 가입자 정보 등을 요청할 수 있다. 해당 포털에서 법집행기관 소속임을 인증 받은 후 요청사항을 입력하고 영장과 번역본을 스캔하여 업로드 한다. 이때, 압수 장소는 본사 소재지[50]로 기재하여 일반 압수수색 영장을 발부받아야 한다. 자료 회신은 담당 수사관의 이메일로 암호화키와 함께 URL을 전송하는 방법으로 오며, 통상 10일에서 20일이 소요된다.

트위터 또한 전 세계 법집행기관으로부터 받은 데이터 제공 요청 관련 정보를 반기마다 보고서로 발간하는데, 이에 따르면 한국은 2019년 하반기에 484건을 요청하여 이 중 약 30%에 대해 자료를 회신 받았다.[51]

---

47) 경찰청 내부 자료, "Twitter Inc.-Guidelines for Korean Law Enforcement"; 트위터 웹사이트, "Guidelines for law enforcement", https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support (2021. 2. 1. 최종 검색).

48) 경찰청 내부 자료, "Twitter Inc.-Guidelines for Korean Law Enforcement"; 트위터 웹사이트, "Guidelines for law enforcement", https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support (2021. 2. 1. 최종 검색).

49) https://legalrequests.twitter.com.

50) Twitter. Inc. c/o Legal Policy, 1355 Market Street, Suite 900, San Francisco, U.S.A.

51) 트위터 웹사이트, https://transparency.twitter.com/en/reports/information-requests.html#2019-jul-dec (2020. 12. 10. 최종 검색).

라. 애플

애플은 미국 캘리포니아에 본사가 있으며, 아이폰, 아이패드, 맥 등 하드웨어와 아이클라우드, 아이튠즈, 메일 등 소프트웨어 서비스를 제공하는 글로벌 기업이다. 애플의 경우 자료제공 요청 시 영장 첨부가 필수 요소가 아니고, 애플이 제시하는 양식을 작성하여 이메일로 송부하도록 하고 있다는 점에서 앞서 살펴본 미국 기업들과 차이가 있다.

협조가 가능한 죄종에는 특별히 제한이 없으며, 협조가 가능한 자료에는 가입자 정보와 최근 IP 접속기록을 비롯하여 등록기기 정보, 애플스토어 거래 내역, 아이클라우드 가입자 정보 등이 있다. 반면에 통신 내용 및 위치정보, 이메일 수발신 내역 등은 제공해 주지 않는다. 애플의 외국 법집행기관을 위한 가이드라인에 따르면, 통신 내용을 요청하고자 할 때에는 미국 전자통신사생활보호법(Electronic Communications Privacy Act, ECPA)에 의한 긴급정보공개 요청을 제외하고는 MLA 절차를 따라야 한다.[52]

애플 또한 전 세계 법집행기관으로부터 받은 데이터 제공 요청 건수 관련 정보를 반기마다 보고서로 발간하는데, 이에 따르면 한국은 2019년 하반기에 총 94건을 요청하여 이 중 약 53%에 대한 자료를 회신 받았다.[53]

마. 소결

미국의 대표적인 IT 기업으로서 페이스북, 구글, 트위터, 애플의 통신 데이터 제공 정책을 살펴보았다. 미국의 주요 IT 기업은 외국 형사당국이 기본적인 가입자 정보를 요청하는 경우 해당 국가의 법원이 발부한 영장 또는 허가서를 전제로 직접 자료를 제공하고 있다. 그러나 민감도가 더 높은 통신 내용을 요청할 때에는 반드시 MLA를 거치도록 하고 있다. 기업별로 통신 자료 요청 방법과 협조 범위를 정리하면 아래와 같다.

52) 애플, “Legal Process Guidelines Government & Law Enforcement outside the United States”, https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf (2020. 12. 10. 최종 검색).

53) 애플 웹사이트, https://www.apple.com/legal/transparency/kr.html (2021. 2. 10. 최종 검색).

〈표 1〉 미국의 대표적인 IT 기업별 통신 자료 요청 방법

	제공 범위	대상 범죄	영장	요청 수단	회신율*
페이스북 (인스타그램)	가입자 정보, IP 접속기록 (통신내용 불가)	제한 없음	필요	전용 포털	44%
구글	가입자 정보, IP 접속기록, 거래내역 (통신내용 불가)	제한 없음	필요	전용 포털	71%
트위터	가입자 정보, IP 접속기록 (통신내용 불가)	강력범죄에 한함	필요	전용 포털	30%
애플	가입자 정보, IP 접속기록, 거래내역 (통신내용 불가)	제한 없음	불요	이메일	53%

* 2019년 하반기 기준

2. 미국 외 국가

최근 국내에서는 해외 메신저 앱 사용이 활발해지고 있는데 이들 서비스 제공자는 미국 회사가 아닌 경우도 많다. 대표적으로 텔레그램(Telegram)과 라인(LINE)을 살펴보면, 먼저 텔레그램은 클라우드 기반의 암호화된 메신저 앱으로, 전 세계 5억여 명이 사용 중으로 추산된다.[54] 텔레그램은 러시아의 두로프 형제가 독일에 서버를 두고 개발하였으며, 이후 런던, 싱가포르 등을 거쳐 두바이에 본사가 소재하고 있다고 알려져 있으나,[55] 현 소재지는 명확히 파악된 것이 아니다.[56] 텔레그램은 가입자의 사생활 보호를 이유로 법집행기관에 비협조적인 것으로 악명 높다. 여러 국가의 사법당국이 텔레그램에 통신 자료를 요청하고 있지만, 그간 어떤 국가에도 자료를 회신한 적 없는 것으로 알려져 있다.[57] 우리 경찰청 또한 '텔레그램 n번방 사건'을 수사하면서 텔레그램에 부단히

54) 텔레그램 웹사이트, http://www.telegram.pe.kr/index.php#t002 ; 연합뉴스(2020. 12. 23.), "텔레그램 창업자 내년부터 유료 서비스 선보일 것", https://www.yna.co.kr/view/AKR20201223168700108?input=1195m (2021. 2. 4. 최종 검색).

55) 텔레그램 FAQ에 공지된 내용(telegram.org/faq).

56) 조선비즈(2020. 3. 26.), "텔레그램 본사는 어디? 세계 떠도는 창업자 형제..'데이터 공개 불가' 고수", https://biz.chosun.com/site/data/html_dir/2020/03/26/2020032602745.html (2021. 2. 4. 최종 검색).

57) 조선비즈(2020. 3. 26.), "텔레그램 본사는 어디? 세계 떠도는 창업자 형제..'데이터 공개 불가'

협조를 요청했지만, 불법 게시물 삭제 차단만 협조하고, 가입자 정보 등 통신 자료 요청에는 일절 회신하지 않았다.[58]

라인은 메신저 앱을 기반으로 커뮤니케이션, 엔터테인먼트, 핀테크 등 모바일에 특화된 다양한 서비스를 운영하며 일본 도쿄에 본사가 있다.[59] 일본의 서비스 제공자는 일본 법원이 발부한 영장만을 인정하기 때문에 타국 수사기관에 자료를 제공하지 않는다.[60] 경찰청 업무 담당자에 의하면, 라인 또한 한국 영장을 첨부한 통신 자료 요청에 협조해 주지 않으며, MLA를 전제로 한 자료 보존 요청에만 응하고 있다. 따라서 라인으로부터 통신 자료를 제공받기 위해서는 기본적인 가입자 정보라고 하더라도 MLA 절차를 거쳐야 한다.

이처럼 통신 자료 요청에 응하지 않는 외국 업체들의 경우 협조적인 업체보다 수사가 까다로울 수밖에 없고, 그 결과 범죄자의 도피처로 악용될 우려가 있다. n번방 사건 또한 디지털 성범죄물 유통을 위해 텔레그램의 보안성과 수사기관에 대한 비협조적 측면을 적극적으로 이용한 사례라고 할 수 있다.

한편, 유럽의 경우 2018년 발효된 '일반 데이터 보호 규정(General Data Protection Regulation, GDPR)'에 의해 개인정보 보호 정책이 더욱 강화됨에 따라 유럽권 IT 서비스 제공자는 일반적으로 유럽연합 회원국이 아닌 타국 법집행기관에 통신 자료를 직접 제공하지 않는다.[61] 특히, GDPR 제48조는 EU 회원국과 외국 정부 간에 체결된 "국제형사사법공조조약과 같은 국제협정에 근거한" 경우에만 외국의 영장이나 법원 명령을 인정하므로,[62] 우리나라 영장이 인정될 여지가 없다. 이는 우리나라의 서비스 제공자도

고수", https://biz.chosun.com/site/data/html_dir/2020/03/26/2020032602745.html (2021. 2. 4. 최종 검색).

58) 김한균 외, 「첨단 과학수사 정책 및 포렌식 기법 종합발전방안 연구(Ⅲ)」, 경제·인문사회연구회 협동연구 총서, 2020, 352면.

59) 라인 웹사이트, https://linepluscorp.com/company/info (2021. 2. 4. 최종 검색).

60) 전현욱·김기범·조성용·Emilio C VIANO, 「사이버범죄의 수사 효율성 강화를 위한 법제 개선방안 연구」, 경제·인문사회연구회 미래사회 협동연구총서, 2015, 172면.

61) Jan Kleijssen and Pierluigi Perri, "Cybercrime, Evidence and Territoriality: Issues and Options." Netherlands Yearbook of International Law 2016. The Hague: T.M.C. Asser, 2017, 147-173, 164면.

62) 송영진, "미국 CLOUD Act 통과와 국경 없는 데이터 접근에 대한 시사점", 형사정책연구 29(2), 2018, 149-172, 165면.

마찬가지로, 개인정보보호법 제18조 제1항에 의해 개인정보의 제3자 제공이 제한되며, 동조 제2항 제6호의 예외규정 또한 '조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우'라고 정하고 있으므로, MLA 절차에 의하지 않고서는 외국 사법당국에 통신 자료를 제공할 수 없다.

Ⅳ. 현행 통신 자료 요청 방법의 형사법적 문제

1. 사이버 공간에서의 형사관할권과 영장 집행의 성질

앞서 우리나라 수사기관이 외국 서비스 제공자에 대해 통신 자료를 요청할 때 일반적으로 압수수색 영장을 발부받아 제시하고, 그 집행 장소를 본사 주소로 기재하고 있음을 살펴보았다. 그렇다면 이러한 절차는 우리나라가 외국 서비스 제공자에 대하여 형사관할권을 행사하는 것이고, 그들의 본사에 대하여 압수수색 영장을 집행하는 강제수사인 것인가? 이 문제를 검토하기 위해서는 먼저 사이버 공간에서의 영토 개념과 형사관할권을 둘러싼 국제적 논의를 정리할 필요가 있다.

가. 사이버 공간에서의 영토 개념과 형사관할권

전통적으로 국가는 영토를 기반으로 관할권을 행사하며, 특히 형사법은 영토주의 관념에 필연적으로 기반한다.[63] 그러나, 데이터의 무형성, 이동성, 가분성, 복제 용이성 등 특수한 성질로 인해 사이버 공간에서의 영토 개념이 도전을 받고 있다.[64] 즉, 본고에서 다루는 상황과 같이 업체의 본사나 데이터 서버가 자국의 영토에 있지 않더라도 일정 요건하에 데이터에 대한 형사관할권을 행사할 수 있는지 문제 된다. 이에 대한 학계의 논쟁은 데이터 예외주의와 비예외주의로 나뉘는데, 데이터 예외주의파는 사이버 공간은 기존의 법률이 적용되는 지리적 공간과 근본적으로 다른 것이며, 정보 그 자체는 물질적

63) Jonathan Clough. 「Principles of Cybercrime, Cambridge university press」, 2015, 475면.

64) 송영진, "수사기관의 클라우드 데이터 접근에 관한 비판적 고찰: "데이터 예외주의" 논쟁과 각국의 실행을 중심으로", 형사정책연구 30(3), 2019, 149-180, 152-155면.

인 성질이 없고 경계도 없으므로 사이버 공간에서 관할권을 행사하기 위해서는 기존과 다른 법적 체제가 필수적이라고 본다.[65] 반면에, 후자는 사이버 공간에서의 행위도 언제나 어떤 국가의 영토에 기반한 서버나 장비를 사용하여 이루어지는 것이며, 그 행위의 영향도 어떤 국가에서 나타나므로 현존하는 법으로 규율할 수 있다고 본다.[66]

사이버 공간에서 국가주권의 범위와 전쟁에 관한 사안을 다룬 탈린 매뉴얼은 첫 장에서 "전문가들은 만장일치로 국제법의 일반원칙이 사이버 공간에 적용된다고 결론 내렸다"[67]라고 시작하여 데이터 비예외주의 입장에서 쓰였다.[68] 탈린 매뉴얼은 어떤 국가도 사이버 공간 그 자체에 대한 주권을 주장할 수는 없으며, 기술적 도전과제로 인해 사이버 공간에서 사법관할을 결정하는 것이 어려울 수는 있지만 그럼에도 국가는 자국의 영토에 위치한 사이버 기반시설과 그 시설과 관련한 활동에 대하여 관할을 행사할 수 있다고 서술하고 있다.[69] 그러나, 오늘날 사이버 공간에서의 관할권 행사에 관한 국제법적 질서는 아직 확립된 바 없으며, 학계의 논쟁과 더불어 각국 법원에서도 다른 판단을 내리고 있다.

예컨대 벨기에 검찰은 2007년 국내 형사사건에서 미국의 서비스 제공자인 '야후(Yahoo!)'를 상대로 가입자 정보를 요청하였는데, 야후는 벨기에 국적의 회사가 아니므로 MLA에 따라야 한다며 정보 제공을 거부한 사건이 있었다. 이에 벨기에 검찰은 야후를 사법기관에 대한 협력의무 불이행으로 기소하였으며, 벨기에 법원은 야후에게 55,000 유로의 벌금을 부과하였다.[70] 야후는 이에 항소하며 벨기에에 주둔하는 회사가 아니므로 벨기에 법의 적용을 받지 않으며, 설령 벨기에 법의 적용을 받는다고 하더라도 데이

65) 송영진, 앞의 논문, 151면.

66) Lianne J.M. Boer, "Spoofed Presence Does not Suffice: On Territoriality in the Tallin Manual", Netherlands Yearbook of International Law 2016, The Hague: T.M.C. Asser, 2017, 131-145, 134면.

67) "the Experts unanimously concluded that general principles of international law applied to cyberspace"을 번역함.

68) Lianne J.M. Boer, "Spoofed Presence Does not Suffice: On Territoriality in the Tallin Manual", Netherlands Yearbook of International Law 2016, The Hague: T.M.C. Asser, 2017, 131-145, 136면.

69) Lianne J.M. Boer, 앞의 논문, 137면.

70) 송영진, "수사기관의 클라우드 데이터 접근에 관한 비판적 고찰 : "데이터 예외주의" 논쟁과 각국의 실행을 중심으로", 형사정책연구 30(3), 2019, 149-180, 171면.

터 제출 명령은 벨기에의 집행관할권의 허용되지 않는 역외 적용이라고 주장하였다.[71] 그러나 벨기에 파기원(Court of Cassation)에서는 야후의 주장을 배척하고 유죄판결을 확정하였다.[72] 파기원은 벨기에에 물리적으로 존재하지 않더라도 벨기에 국적의 고객에 대해 서비스를 제공하고 경제적 활동을 하는 모든 서비스 제공자에게 데이터 공개 의무가 적용된다고 판시하였다.[73] 이러한 접근 방식에 따르면 데이터 위치나 서비스 제공자의 위치 등과 관계없이 데이터 제출명령의 집행관할권이 인정되므로 사이버 공간에서의 영토주의를 지나치게 확장하게 되며, 타국민의 프라이버시를 침해하거나 타국의 주권을 침해할 우려가 있다.[74]

우리나라에서는 아직 외국 서비스 제공자에 대해 수사기관이 직접 통신 자료를 요청하는 관행의 적법성을 다투거나 서비스 제공자에 대해 자료 제출을 강제할 집행관할권이 있는지를 다툰 판례는 없다. 그러나 서울고등법원 2012나63832 판결에서 국가의 집행관할권은 자국 영토 등에 한정되어 미치므로 외국에 있는 재산에 관하여 강제집행권을 행사하기 위하여는 조약 또는 상대국 동의가 있거나 외국판결 승인 등 절차를 거쳐야 하고, 그러한 절차 없이 곧바로 외국 소재 재산에 강제집행권을 행사하는 것을 허용되지 않는다는 것이 일반적으로 승인된 국제관습법이라고 판시한 바 있다.[75] 따라서 국내법적 근거가 명확히 있다거나 국제법적 합의가 형성되지 않은 현시점에서는 한국이 일방적으로 타국의 서비스 제공자에 대하여 통신 자료 제출을 강제할 수 있는 집행관할권이 있다고 볼 수 없다.

나. 영장 집행의 성질과 문제점

외국의 서비스 제공자에 대해 통신 자료 제출을 강제할 수 있는 집행관할권이 없다면, 수사기관이 압수수색 영장을 발부받아 이들에게 제시하는 것은 강제수사인 영장 집행이 아닐 것이다. 그러나 현 관행이 영장의 집행이 아니라면 무엇으로 보아야 하는가? 앞서

71) 송영진, 앞의 논문, 172면.

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

73) 송영진, "수사기관의 클라우드 데이터 접근에 관한 비판적 고찰 : "데이터 예외주의" 논쟁과 각국의 실행을 중심으로", 형사정책연구 30(3), 2019, 149-180, 172면.

74) 송영진, 앞의 논문, 172면.

75) 서울고등법원 2013. 4. 18. 선고 2012나63832 판결.

살펴본 IT 기업들은 왜 영장을 요구하는가? 이를 검토하기 위해 우리나라가 주로 통신 자료를 요청하는 미국의 서비스 제공자가 어떠한 법적 근거로 자료를 제공하는지 살펴보았다.

미국 서비스 제공자의 통신 데이터 제공 정책은 미국 전자통신사생활보호법(Electronic Communication Privacy Act, ECPA)[76]의 Title Ⅱ에 해당하는 저장통신법(Stored Communication Act, SCA)[77]에 근거한다. 동법 §2702는 전자통신 서비스(Electronic Service Provider)와 원격 컴퓨팅 서비스(Remote Computing Service) 제공자(이하 "서비스 제공자"로 통칭하기로 한다)의 자발적인 정보 공개를 다루고, §2703은 의무적인 정보 공개를 다룬다.

§2703(a),(b)에 의해 정부기관이 서비스 제공자에게 통신 내용 공개를 강제하고자 할 때 그 저장기간이 180일 이하인 경우에는 영장에 의해서만, 180일이 넘거나 오로지 저장 목적인 경우에는 영장 또는 제출 명령(subpoena) 또는 법원 명령에 의해야 하며, §2703(c)에 의해 '가입자나 고객과 관련된 기록 및 기타 정보(내용 정보 제외)' 공개를 강제하고자 할 때에는 영장, 법원 명령, 가입자 동의, 텔레마케팅 사기 수사 시 법집행기관의 서면 요청 등의 방법이 있다. 이때, 영장, 제출 명령, 법원 명령은 모두 "권한 있는 관할(competent jurisdiction)"의 법원이 발부할 것을 요하고 있다. 우리 법집행기관이 미국 서비스 제공자에 제시하는 우리 법원이 발부한 영장, 통신사실확인 허가서 등은 이에 해당하지 않으므로 §2703이 적용된다고 보기 어렵다.

한편, 미국의 트럼프 정권은 2018년 "합법적인 해외 데이터 활용의 명확화를 위한 법률(Clarifying Lawful Overseas Use of Data Act, CLOUD Act)"을 제정하였는데, 동 법률에서는 외국 정부기관이 미국과 행정협정을 체결할 경우 미국 서비스 제공자에게 직접 데이터 공개를 명령할 수 있도록 하고 있다.[78] 그러나, 한국은 미국과 행정협정을 체결하지 않았으므로 CLOUD 법이 적용될 여지도 없다.

그렇다면, 미국의 서비스 제공자가 우리나라에 통신 자료를 제공하는 것은 §2702에 의거한 자발적 정보 공개에 해당할 것이다. §2702(a)는 서비스 제공자는 원칙적으로 통

76) 18 U.S.C. § 2510 et seq.
77) 18 U.S.C. Chapter 121 § 2701-2712.
78) 18 U.S.C. § 2523.

신 내용을 '누구에게도' 누설할 수 없고, 가입자나 고객과 관련된 기록 및 기타 정보(내용 정보 제외)의 경우에는 '정부기관'에 누설할 수 없다고 규정하고 있다. §2702(b),(c)에서는 (a)의 예외규정을 두고 있는데, 이중 §2702(c)(6)에서 통신 내용이 아닌 가입자 관련 정보의 경우에는 "정부기관 이외의 자"에게 제공할 수 있다는 예외규정이 있다. SCA에서 말하는 "정부기관(governmental entity)"이란, 미국 연방의 부처 또는 주 또는 정치적 구획을 의미하므로,[79] 외국 정부는 포함되지 않는 개념이다. 따라서 미국 서비스 제공자가 외국 법집행기관에 통신 내용을 제외한 가입자 관련 정보 요청에 협조해 주고 있는 근거는 §2702(c)(6)로 보아야 할 것이다.

정리하면, 미국 서비스 제공자가 외국 정부에 대하여 가입자 관련 정보를 공개하는 것은 §2702(c)(6)을 근거로 한 미국 정부기관 이외의 자에 대한 자발적인 공개에 해당하며, 업체별 정책과 개인정보보호 약관을 함께 고려하여 요청마다 개별적으로 검토하는 것이다. 따라서 애플의 경우에는 영장 첨부 없이도 가입자 정보를 제공해주나, 텀블러의 경우에는 영장을 제시하여도 자료를 회신받기 쉽지 않은 것처럼 미국 내에서도 업체마다 통신 자료 제공 요청에 대한 협조 범위가 다르다. 그러나 자발적인 공개에 앞서 영장을 요구하는 이유는 요청하는 국가에서 적법한 범죄 수사를 위해 요청하는 자료가 필요하고 이에 대해 법원의 허가가 있었다는 것을 증명하는 공신력 있는 문서가 필요하기 때문으로 판단된다.

그러나 현 관행은 강제수사가 아님에도 압수수색 영장을 발부받는 것 자체에 문제가 있으며, 나아가 영장 집행의 절차를 준수하지 않는다는 문제가 있다. 현 관행은 형사소송법 제118조의 영장 원본 제시, 동법 제121조 및 제122조의 참여권 보장, 동법 제129조의 압수목록 교부 등 압수수색 절차를 모두 무시하고 있기 때문이다. 아직까지 법원에서 영장 집행 절차를 지키지 않았다고 하여 회신받은 자료의 증거능력을 다툰 적은 없으나, 이러한 자료가 위법수집증거 배제의 원칙으로부터 자유롭다고 볼 수 없다. 따라서 압수수색 영장은 외국의 서비스 제공자에게 제시하는 수단으로 적합하지 않으며, 공신력을 증명할 수 있는 법원의 허가서 등 다른 방법으로 대체해야 할 것이다.

79) 18 USC § 2711(4)의 정의.

2. 회신받은 자료의 증거능력 인정 여부

외국 서비스 제공자에게 직접 요청하여 통신자료를 제공받는 현 관행은, 그러한 공조 방식의 법적 근거가 명확하지 않다는 점, 디지털 증거의 동일성 및 무결성을 담보하는 조치가 부재한다는 점에서 증거능력이 문제 될 여지가 있다.

먼저 법적 근거와 관련하여, 국제형사사법공조법 제38조 제2항에 의하여 국가 간 형사사법공조에 관한 사항은 동법에 의해야 하나, 동법에는 형사사법공조조약에 근거한 공조와 인터폴을 통한 공조에 대해서만 규정하고 있을 뿐, 우리 법집행기관이 외국 정부를 거치지 않고 민간에 직접 요청하여 수사자료를 제공받는 방식에 대해서는 규율하고 있지 않다. 경찰관직무집행법 또한 제8조의 2에서 경찰관의 직무 범위를 "외국 정부기관, 국제기구 등과 자료 교환, 국제협력 활동"으로 국한하고 있으므로, 민간업체와의 자료 교환에 적용하기에는 무리가 있다. 그렇다면 최종적으로, 임의수사의 원칙을 담고 있는 형사소송법 제199조 제1항[80]을 근거로 삼아야 할지 문제 될 것이나, 본 사안을 규율하기에는 지나치게 포괄적이다. 결국, 현 관행은 법적 근거가 명확하지 않다.

둘째로, 디지털 증거 혹은 전자적 증거란 디지털 매체에 보관되어 있거나 디지털 매체를 통해 전송되는 증거로서 가치가 있는 정보이므로,[81] 외국 서비스 제공자로부터 확보한 자료는 디지털 매체에 보관되어 있던 데이터를 서비스 제공자가 발췌하여 디지털 매체(본안에서는 이메일 또는 법집행기관 전용 포털)를 통해 전송하는 것으로서 디지털 증거라고 볼 수 있다. 디지털 증거는 자체적으로 가시성이 없고 복제, 위·변조가 용이하므로, 증거능력이 인정되기 위해서는 동일성 및 무결성이 인정되어야 한다. 대법원은 저장매체에서 출력한 문건 또는 복제본은 저장매체 원본에 저장된 내용과 동일성이 인정되어야 하며, 압수 절차에서 변경되지 않았음이 담보되어야 한다고 판시하여 디지털 증거의 동일성, 무결성 원칙을 선언하였으며,[82] 이는 피압수수색 당사자가 원본과 복제본의 해시값이 동일하다는 취지에 대한 확인서명을 받아 법원에 제출하여 증명하는 것이 원칙이고, 그러한 방법이 불가능하거나 현저히 곤란하면 참여 수사관, 전문가 등의 증언에 의해

80) 형사소송법 제199조 ① 수사에 관하여는 그 목적을 달성하기 위하여 필요한 조사를 할 수 있다.

81) 김윤섭·박상용, "형사증거법상 디지털 증거의 증거능력 - 증거능력의 선결요건 및 전문법칙의 예외요건을 중심으로" 형사정책연구 26(2), 2015, 165-214. 168면.

82) 대법원 2007. 12. 13. 선고 2007도7257 판결.

해시값이 동일하다거나 저장매체 원본이 압수 시부터 밀봉되어 증거 제출 시까지 전혀 변경되지 않았다는 사정을 증명하는 방법 등으로 입증할 수 있다고 하였다.[83]

비록 본안에서 다루는 사안이 디지털 증거의 '압수·수색'은 아니지만, 외국 서비스 제공자가 우리 수사기관에 제공하는 자료는 일반적으로 그 획득 절차에서 동일성과 무결성이 지켜졌다는 인증이 없다. 아직까지 이러한 자료의 동일성 및 무결성을 다툰 판례는 없지만, 우리 대법원이 디지털 증거의 동일성, 무결성을 엄격히 요구하고 있음에 비추어 볼 때 외국 수사기관의 확인이나 보증을 거치지 않았음은 물론, 서비스 제공자의 구체적인 인증도 없는 자료의 증거능력이 문제 될 소지는 충분하다.

이를 전문증거로 보더라도, 전문법칙의 예외규정인 형사소송법 제313조 및 제314조의 요건을 충족시키기 어렵다. 현 관행상 외국 서비스 제공자는 당사가 제공한 자료에 대하여 우리나라 공판준비나 공판기일에서 성립의 진정을 증명하고 있지 않다. 제314조의 "공판준비 또는 공판기일에 진술을 요하는 자가 외국거주로 인하여 진술할 수 없는 때"에 해당한다고 보더라도, 진술 또는 작성이 특신상태에서 행해졌음이 증명되어야 한다.[84] 특신상태의 인정 요건은 우리 법에서 명확히 규정하고 있지 않아 법관의 재량 영역에 속하게 되는데,[85] 대법원은 특신상태의 판단기준에 관하여 '특히 신빙할 수 있는 상태 '란 진술 내용이나 조서 작성에 허위개입의 여지가 거의 없고, 진술 내용의 신빙성이나 임의성을 담보할 구체적이고 외부적인 정황이 있는 것을 말한다고 판시하였다.[86] 아직까지 본 쟁점과 유사한 사안을 다룬 판례는 없지만, 외국 거주자의 작성 서류에 대한 특신상태 불인정으로 인해 증거능력을 부정한 판례가 존재한다(대법원 2011. 7. 14. 선고 2011도3809 판결, 대법원 2006. 9. 26. 선고 2006도3922 판결).[87] 또한, 동법 제315조의 '당연히 증거능력이 있는 서류' 관련, 본 사안의 회신 자료는 외국 공무원이 작성한 문서에 해당하지 않고, 평소에 업무상 필요로 작성한 통상문서도 아니며, 기타

83) 대법원 2013. 7. 26. 선고 2013도2511 판결.

84) 조규철, "국제범죄수사에 있어 외국에서의 증거수집 및 수집한 증거의 증거능력에 대한 고찰" 한국공안행정학회보 20(3), 2011, 272-303, 293면.

85) 안성훈·김민이·김성룡, 「국제범죄수사에 있어서 외국에서 수집된 증거의 증거능력에 대한 연구」, 한국형사정책연구원 연구총서, 2017, 89면.

86) 대법원 2012. 7. 26. 선고 2012도2937 판결.

87) 안성훈·김민이·김성룡, 「국제범죄수사에 있어서 외국에서 수집된 증거의 증거능력에 대한 연구」, 한국형사정책연구원 연구총서, 2017, 130면.

특히 신용할 만한 정황에 의하여 작성되었다는 인증도 없으므로 이에 해당한다고 볼 수도 없다.

정리하면, 우리 수사기관이 외국 업체에 직접 요청하여 획득한 디지털 증거물은 당연히 증거능력이 인정된다고 볼 수 없다. 외국 서비스 제공자에 대한 통신 자료 요청 건수가 매년 증가하는 현실을 볼 때 이러한 방식의 공조에 대한 법적 근거를 명확히 마련할 필요가 있으며, 회신 자료의 동일성과 무결성을 담보할 수 있는 조치가 필요하다.

Ⅴ. 시사점 및 결론

전 세계적으로 통신 자료를 비롯한 전자적 증거를 확보하는 것이 수사의 관건이 되고 있다. 오늘날 "모든 범죄가 사이버범죄화"됨에 따라 사이버범죄 뿐만 아니라 비(非) 사이버범죄 또한 수사단서 및 증거를 외국의 서비스 제공자가 보유하는 경우가 늘어나고 있다. 유럽 위원회가 2018년 발표한 보고서에 따르면 모든 수사 사건의 절반 이상이 전자적 증거에 대한 초국경적 접근 요청을 포함한다.'[88]

해외에 소재한 전자적 증거를 확보하기 위한 기존의 공조 방식으로는 대표적으로 MLA와 인터폴 공조가 있지만, 두 방법 모두 큰 한계가 있다. MLA는 요청부터 회신까지 절차가 복잡하고 긴 시간이 소요되어 휘발성을 특징으로 하는 전자적 증거 획득에 적합하지 않다. 인터폴 공조 또한 강제성이 없으며 협력 범위가 한정적이라는 한계가 있다.

이에 우리 경찰청은 실무적으로 외국 서비스 제공자에게 직접 가입자 정보 등 통신 자료를 요청하는 사례가 늘고 있지만, 앞서 살펴본 것과 같은 중요한 형사법적 문제가 있다. 즉, 영장을 발부받아 집행하지만 실제로는 데이터 제공을 강제할 수 있는 형사관할

88) European Commission, "Commission Staff Working Document: Impact Assessment, Accompanying the Document, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules of the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings", 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN. (2021. 1. 4. 최종 검색).

권 행사가 아닌 점, 영장 집행의 절차 관련 형사소송법 규정을 준수하지 않는 점, 법적 근거의 불명확성 및 무결성 입증 미비로 인해 회신받은 자료의 증거능력이 문제된다는 점 등이 있다. 또한 업체가 데이터 제공에 관한 정책과 절차를 변경하는 경우가 있기 때문에 예측 가능성을 저해하며, 중요한 증거물의 확보가 민간업체의 임의적 협조 여부에 의존한다는 문제도 있을 것이다.

따라서 우리는 사이버범죄협약을 가입하여 현행 방식의 근거와 절차를 확립할 필요가 있다. 사이버범죄협약은 사이버범죄 이슈를 다룬 최초의 구속력 있는 다자 협약으로서 사이버범죄가 아닌 일반 범죄라도 전자적 형태의 증거물과 관련하여 적용될 수 있다.[89] 협약 제18조 제1항 b호[90]는 당사국의 관할관청이 '자국 영토에서 서비스를 제공하는' 자에게 해당 서비스와 관련하여 보유 또는 관리하는 가입자 정보를 제출하도록 명령할 수 있도록 하는 제도를 갖출 것을 규정하고 있다.[91]

제18조의 해석에 관하여 사이버범죄협약위원회(Cybercrime Convention Committee, T-CY)가 2017년 3월에 채택한 해설서(Guidance Note)에 따르면, 서비스 제공자가 법적으로나 물리적으로 당사국 영토 내에 소재하지 않더라도, 자국 영토에서 서비스를 제공한다면 관할관청이 이 서비스 제공자에게 직접 제출명령을 할 수 있다.[92] '자국 영토에서 서비스를 제공'하는 경우에는 서비스 제공자가 당사국 영토에 있는 사람으로 하여금 그 서비스를 이용할 수 있도록 하는 경우, 또는 서비스 제공자가 가입자를 향해 활동하거나, 가입자 정보를 그 활동 과정에서 사용하거나, 가입자와 상호작용하는 경우, 또는 당사국 영토 내에서 제공된 서비스와 관련하여 가입자 정보가 생성된 경우 등이 포함된다.[93] 즉, 해설서에서는 서비스 제공자가 자국 내에서 서비스를 제공하는 경우를 넓게 해석하여 제18조 제1항 b호의 적용범위를 확대하고 있다. 이 해설서는 법적 구속력이

89) 유민종, "사이버범죄협약과 국내 법제의 양립 가능성 연구", 2019, 10면.

90) Article 18(1)(b) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: (...) service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

91) 유민종, "사이버범죄협약과 국내 법제의 양립 가능성 연구", 2019, 110면.

92) Cybercrime Convention Committee(T-CY), "T-CY Guidance Note #10 Production orders for subscriber information(Article 18 Budapest Convention)", 2017, 6면.

93) Cybercrime Convention Committee(T-CY), 앞의 자료, 8면.

있는 것은 아니지만, 협약 해석과 적용에 관한 당사국 간 공통적 이해를 반영하는 연성법(Soft Law)의 성격을 띤다.[94]

나아가 2021년 2월 기준으로 아직 논의가 진행되고 있는 사이버범죄협약 제2차 추가의정서(2nd Additional Protocol)에서도 가입자 정보 관련 타국 서비스 제공자와의 직접 협력과 법집행기관의 국경을 넘어선 전자적 증거 확보 문제를 집중적으로 다루고 있다.[95] 추가의정서 제4조에 의하면 관할관청은 타국의 서비스 제공자에 대하여 MLA를 거치지 않고 그가 보유하거나 관리하는 가입자 정보를 제출하도록 직접 명령할 수 있고 해당 서비스 제공자가 이에 30일 이내에 응답하지 않으면 다른 방법으로 명령을 집행할 수 있다.[96] 이 의정서가 채택된다면 협약 제18조는 최소한 가입자 정보와 관련해서는 한 국가의 서비스 제공자가 서비스를 제공하는 타국의 법집행기관에 데이터를 공개하는 행위의 법적 근거를 제공할 것이다.[97]

사이버범죄협약은 유럽평의회의 이니셔티브로 탄생하였지만, 전 세계적 적용을 의도하여 만들어졌으며,[98] 2021년 2월 기준 65개국이 가입돼있다.[99] 우리나라도 하루빨리 협약에 가입하여 사이버범죄 대응을 위한 국제적 논의에 참여하고 통신 자료 요청과 관련한 현행 방식의 불확실성을 제거할 필요가 있다.

---

94) Paul de Hert, Cihan Parlar, Juraj Sajfert, “The Cybercrime Convention Committee’s 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law”, Computer Law & Security Review, Volume 34, Issue 2, 2018, 329면.

95) Jennifer Daskal, DeBrae Kennedy-Mayo(2020. 7. 2), “Budapest Convention: What is it and How is it Being Updated?”, https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/?cn-reloaded=1#_edn27(2021. 2. 2. 최종 검색).

96) Cybercrime Convention Committee (T-CY), “Draft Text Version 10, Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime”, 2020, 15면.

97) Jan Kleijssen and Pierluigi Perri, “Cybercrime, Evidence and Territoriality: Issues and Options.” Netherlands Yearbook of International Law 2016. The Hague: T.M.C. Asser, 2017, 147-173, 166-167면.

98) Jonathan Clough.「Principles of Cybercrime, Cambridge university press」, 2015, 24면.

99) 유럽평의회 홈페이지, “Chart of signatures and ratifications of Treaty 185”, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=bl9q9MUJ (2021. 2. 15. 최종 검색).

참고문헌

1. 국내문헌

경찰청, 「2020 경찰백서」, 경찰청, 2020.

경찰청 내부 자료, 「Legal Requests for User Data, Google Inc. Process for Korean Authorities Requesting User Data」, 「Twitter Inc.-Guidelines for Korean Law Enforcement」, 2014.

김한균 외, 「첨단 과학수사 정책 및 포렌식 기법 종합발전방안 연구(Ⅲ)」, 경제·인문사회연구회 협동연구 총서, 2020.

법무부, 「2020년 법무연감」, 법무부, 2020.

안성훈·김민이·김성룡, 「국제범죄수사에 있어서 외국에서 수집된 증거의 증거능력에 대한 연구」, 한국형사정책연구원 연구총서, 2017.

전현욱·김기범·조성용·Emilio C VIANO, 「사이버범죄의 수사 효율성 강화를 위한 법제 개선방안 연구」, 경제·인문사회연구회 미래사회 협동연구총서, 2015.

정인섭, 「신국제법 강의(제7판)」, 박영사, 2017.

김윤섭·박상용, "형사증거법상 디지털 증거의 증거능력 - 증거능력의 선결요건 및 전문법칙의 예외요건을 중심으로" 형사정책연구 26(2), 2015.

송영진, "미국 CLOUD Act 통과와 국경 없는 데이터 접근에 대한 시사점", 형사정책연구 29(2), 2018.

송영진, "수사기관의 클라우드 데이터 접근에 관한 비판적 고찰: "데이터 예외주의" 논쟁과 각국의 실행을 중심으로", 형사정책연구 30(3), 2019.

오세연·송혜진, "초국가적 범죄의 대응강화를 위한 인터폴의 효율적 활용방안에 관한 연구", 한국재난정보학회논문집 10(4), 2014.

유민종, "사이버범죄협약과 국내 법제의 양립 가능성 연구", 2019.

이순옥, "인터넷서비스제공자가 보관한 정보에 대한 압수·수색 절차", 법학논문집 43(3), 2019.

정대용·김성훈·김기범·이상진, "국제협력을 통한 디지털 증거의 수집과 증거능력", 형사

정책연구 28(1), 2017.
조규철, "국제범죄수사에 있어 외국에서의 증거수집 및 수집한 증거의 증거능력에 대한 고찰", 한국공안행정학회보 20(3), 2011.

2. 국외문헌

Clough, Jonathan「Principles of Cybercrime」, Cambridge university press, 2015.
Cybercrime Convention Committee (T-CY), "Draft Text Version 10, Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime", 2020
Cybercrime Convention Committee (T-CY), "Rules on obtaining subscriber information, report adopted by the T-CY at its 12th Plenary", 2014.
Cybercrime Convention Committee(T-CY), "T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention)", 2017.
European Commission, "Commission Staff Working Document: Impact Assessment, Accompanying the Document, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules of the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings", 2018.
J.M. Boer, Lianne, "Spoofed Presence Does not Suffice: On Territoriality in the Tallin Manual", Netherlands Yearbook of International Law 2016, The Hague: T.M.C. Asser, 2017.
Kleijssen, Jan and Perri, Pierluigi, "Cybercrime, Evidence and Territoriality: Issues and Options." Netherlands Yearbook of International Law 2016.

The Hague: T.M.C. Asser, 2017.

Paul de Hert, Cihan Parlar, Juraj Sajfert, “The Cybercrime Convention Committee’s 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law”, Computer Law & Security Review, Volume 34, Issue 2, 2018.

3. 기타

경인일보(2012. 7. 12.), “20대 여성에 "알몸동영상 유포하겠다" 주한미군, 이번엔 ‘협박’”, http://www.kyeongin.com/main/view.php?key=664982 (2021. 1. 5. 최종 검색).

연합뉴스(2020. 12. 23.), “텔레그램 창업자 내년부터 유료 서비스 선보일 것”, https://www.yna.co.kr/view/AKR20201223168700108?input=1195m (2021. 2. 4. 최종 검색).

조선비즈(2020. 3. 26.), “텔레그램 본사는 어디? 세계 떠도는 창업자 형제..‘데이터 공개 불가’ 고수”, https://biz.chosun.com/site/data/html_dir/2020/03/26/2020032602745.html (2021. 2. 4. 최종 검색).

연합뉴스(2020. 4. 7.), “해외 메신저라 검거 안 된다?…디스코드 국제공조로 수사 확대”, https://www.yna.co.kr/view/AKR20200407102400060 (2020. 12. 27. 최종 검색).

Jennifer Daskal, DeBrae Kennedy-Mayo(2020. 7. 2.), “Budapest Convention: What is it and How is it Being Updated?”, https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/?cn-reloaded=1#_edn27(2021. 2. 2. 최종 검색).

https://govtrequests.facebook.com/government-data-requests/country/KR (2021. 2. 1. 최종 검색).

https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support (2021. 2. 1. 최종 검색).

https://linepluscorp.com/company/info (2021. 2. 4. 최종 검색).

https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:KR;time:&lu=user_requests_report_period (2021. 2. 14. 최종 검색).

https://transparency.twitter.com/en/reports/information-requests.html#2019-jul-dec (2020. 12. 10. 최종 검색).

https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf (2020. 12. 10. 최종 검색).

https://www.apple.com/legal/transparency/kr.html (2020. 2. 10. 최종 검색).

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=bl9q9MUJ (2021. 2. 15. 최종 검색).

https://www.facebook.com/about/privacy (2021. 2. 1. 최종 검색).

https://www.facebook.com/safety/groups/law/guidelines (2021. 2. 1. 최종 검색).

https://www.interpol.int/Who-we-are/Member-countries (2021. 1. 20. 최종 검색).

http://www.telegram.pe.kr/index.php#t002 (2021. 2. 4. 최종 검색).

Legal Issues on Investigative Authority's Data Request to Foreign IT Service Providers

Park, Da-On*

As the majority of Koreans actively use the services of global IT companies in their daily lives, crimes taking advantage of their services have also become common. This means that obtaining communication data such as subscriber information and IP logs possessed by IT companies will be the key to the investigation of many cybercrimes as well as conventional crimes. In the case of domestic service providers, investigative authorities may obtain data through data production requests or warrants. However, if the data is possessed by a foreign service provider, how should our investigation authority obtain the data, and is the current practice appropriate under the criminal procedural law? This paper was intended to critically review the current practice of the National Police Agency's requests to foreign IT service providers and its issues.

First, the general methods of acquiring foreign-based data, including Mutual Legal Assistance, are reviewed, among which is then reviewed more thoroughly how to request data directly to a foreign service provider. Facebook, Google, Twitter, and Apple were selected for U.S. service providers, while Telegram and Line were selected for non-U.S. service providers. As a legal issue related to the current practice of direct requests, search and seizure warrants presented to foreign service providers and the admissibility at the court of the data received are discussed. It is concluded that presenting warrants to foreign service providers is not a compulsory investigation based on criminal jurisdiction, and that the evidence obtained this way might be inadmissible at court, because there is no clear legal

* Researcher, International Cybercrime Research Center, Korean National Police University.

basis for such request and no measures to guarantee the integrity of the data received. The conclusion summarized the discussion by suggesting that the accession to the Cybercrime Convention can be a realistic alternative to overcome the challenges of current practices.

❖ key words: IT Service Provider, Subscriber information, electronic evidence, Mutual Legal Assistance, Convention on Cybercrime

투고일 : 2월 22일 / 심사일 : 3월 23일 / 게재확정일 : 3월 23일