사단법인 한국토지공법학회
토지공법연구 제78집 2017년 5월
Korea Public Land Law Association
Public Land Law Review
Vol. 78, May, 2017

데이터 속성과 국지화 규범의 법적 쟁점에 대한 고찰

A Study on the Legal Issues of Data Attributes and Localization Norms

김 현 경 (서울과학기술대학교 조교수, 법학박사)
Kim, Hyun-Kyung / Professor of Seoul National University of Science and Technology, Ph.D. in Law.

국문초록

최근 각국의 정부는 디지털 주권(digital sovereignty)을 주장하기 위한 광범위한 노력의 일환으로 데이터국지화 규범을 추진하고 있다. 데이터의 속성은 탈영토성(un-territoriality)을 기반으로 한다. 그러나 주권은 영토를 기반으로 하는 국민국가를 단위로 하여 절대성과 항구성을 특질로 하는 권력이다. 데이터가 생성·유통되는 공간으로서 인터넷을 기반으로 하는 공간은 주권이 미치는 영역이다. 따라서 인터넷 공간의 데이터에 대하여 주권의 실행으로서 관할권을 행사하기 위해서는 우선 데이터에 대하여 관리/지배가능성이 있어야 한다. 이러한 데이터의 속성을 영토주의 원칙에 부합하게 제약 하려는 규범적 시도가 바로 데이터의 위치를 제한하는 '데이터 국지화(Data Localization)' 조치라고 할 수 있다. 데이터국지화 규범 자체는 사실상 데이터의 기술적 속성에 위배되는 것이다. 따라서 규범설정만으로 기술적 효과를 완전히 막기에는 분명히 한계가 존재한다. 그러나 규범이 반드시 기술적 속성에 종속되어 기술적 속성을 따라야 하는 것은 아니며, 오히려 기술적 속성이 인간의 삶에 유익하게 작동할 수 있도록 제도가 구축되는 것이 바람직하다. 모든 데이터에 대한 국지화 정책은 데이터의 기술적 속성에 완전히 위배되며 현실적으로 가능할지도

의문이다. 그러나 국민의 프라이버시, 국가안보, 공공기록물 등 국가주권 보장에 불가결한 일정한 데이터에 대하여는 국지화 정책이 일정부분 추구되어야 한다. 그 이외의 데이터에 대한 국지화 규범은 경제적 파급효과, 데이터 협력필요성 등에 비추어 볼 때 모든 국가를 상대로 일률적으로 정할 수 있는 것은 아니다. 대외적 주권실현의 가장 기본원칙인 상호주의에 입각한 데이터 국지화 규범이 타당하다. 또한 데이터 국지화 규범설정은 오히려 정부감시 및 통제의 수단으로 활용하기 용이하고 이는 국민주권을 기본원리로 하는 민주주의의 발전에도 저해된다. 따라서 데이터국지화 규범 설정 시 자의적 공권력에 의한 부당한 결과가 초래되지 않도록 하는 수단이 반드시 함께 마련되어야 할 것이다.

Abstract

Governments in recent years are making efforts to legislate data localization as part of a broader effort to advocate digital sovereignty. The attributes of the data are based on un-territoriality. However, sovereignty is the power that characterizes the absoluteness and permanence of a nation based on territory. The Internet-based space as a space where data is generated and circulated is the domain of sovereignty. Therefore, in order to exercise jurisdiction as the exercise of sovereignty over data in the Internet space, it must first be possible to manage and control data. The normative attempt to constrain the attributes of such data in accordance with the principle of territoriality is called 'data localization', which restricts the location of data. The data localization norm itself is in fact contrary to the technical nature of the data. Therefore, there is a limit to completely prevent the technical effect only by setting the norm. However, norms are not necessarily dependent on technical attributes and does not necessarily conform to the technical attributes, rather, it is desirable that institutions be designed so that technical attributes can work in a way that is beneficial to human life. Localization of all data is completely contrary to the technical nature of the data and is realistically questionable. However, localization should be pursued for specific data indispensable for national sovereignty, such as the privacy of citizens, national security, and public records. The localization norms for other data are not uniformly set for all countries in view of the economic ripple effects, the necessity of data cooperation, and so on. The principle of localization based on reciprocity, which is the most basic principle for the realization of external sovereignty, is reasonable. In addition, data localization is rather easy to utilize as a means of government

monitoring and control, which also hinders the development of democracy, which is the institutional guarantee of national sovereignty. In addition, data localization can be exploited as a means for the government to monitor and control the people. This is also detrimental to the development of democracy to institutionalize popular sovereignty. Therefore, when setting the data localization norm, a means for not causing the improper result by the arbitrary public power will have to be necessarily provided with.

(주제어) 데이터 규범(The Norm for Data), 데이터의 탈영토성(Un-Territoriality of Data), 데이터 주권(Data Sovereignty), 데이터 국지화(Data Localisation), 개인정보 국외이전(Cross-Border Transfer of Personal Information)

Ⅰ. 문제의 제기

전 세계에 걸쳐 자유로운 정보 흐름의 중요성은 누구도 부인할 수 없다. 국경을 초월한 데이터의 자유로운 흐름으로 인해 지난 20여 년간 인터넷은 경제 발전의 핵심 요소로 작동되어 왔다. McKinsey에 의하면 인터넷산업은 선진국의 GDP 성장률의 1/5을 차지하고 있으며,[1] 인터넷에 의한 경제적 가치의 대부분은 오히려 기술 분야 외에서 창출되고 있다. 전통적인 산업 분야에서 얻은 이익의 75%가 인터넷을 통한 경제적 가치, 생산성 향상, 국내외 시장 진출 기회의 확대, 혁신적 제품 개발, 그리고 아이디어의 신속한 배포 등에서 비롯된다고 한다.[2]

그러나 최근 각국의 정부는 '디지털 주권(digital sovereignty)'을 주장하기 위한 광범위한 노력의 일환으로 데이터에 대한 통제권을 행사하려고 노력한다. 이러한 노력의 기저에는 정보의 자유로운 흐름이 공공질서, 소비자 개인 정보 또는 국가 안보에 위협이 될 수 있다는 우려가 전제되어 있다. 또한 국내 기업에 대한 외국 기업의 경쟁우위에 대한 우려도 포함된다. 특히 많은 국가들은 법률을 통하여 일정한 유형의 데이터는 반드시 자국 내 서버에서 저장되고 운영되어야 한다고 규정하고 있다. 예를 들어 개인정보의 경우 자국 내 서버에서 처리되고 저장되어야만 함을 원칙으로 하며, 예외적인 경우에만 해외 유통을 허용한다. 이러한 규범을 '데이터 국지화'라 한다. '데이터 국지화' 규정은 중국 및 러시아를 비롯한 아시아·태평양 국가에서 뿐만 아니라 유럽의 다수 국가들도 포함하고 있다.

---

1) McKinsey Global Institute. Internet matters: The Net's sweeping impact on growth, jobs, and prosperity, May 2011; McKinsey Global Institute. The great transformer: The impact of the Internet on economic growth and prosperity, Oct. 2011.

2) McKinsey, Internet Matters at 7.

원칙적으로 ‘데이터 국지화’ 는 데이터의 자유로운 흐름을 전제로 하는 인터넷의 기술적·본질적 속성에는 부합하지 않는다. 그럼에도 불구하구 각 국은 이를 제도적으로 운영하고 있는 바, 본 고에서는 데이터의 기술적·서비스적 속성을 우선적으로 분석하여 데이터를 규율하는 현행 규범과의 충돌가능성을 밝히고, 각국의 ‘데이터 국지화’에 대한 입법추진 현황을 검토한 뒤 데이터 국지화 규범의 법적 쟁점과 과제에 대하여 모색해 보고자 한다.

Ⅱ. 데이터의 속성과 규범의 충돌

1. 데이터의 속성

(1) 이동성

유체물은 한 지점에서 다른 지점으로 이동함에 있어서 일반적인 물리 법칙에 의해 제한을 받는다. 그리고 이동방식은 일반적으로 관찰 가능하며 의식적으로 선택할 수 있다. 예를 들어 워싱턴 DC에서 필라델피아로 여행하는 사람은 일반적으로 메릴랜드와 델라웨어를 횡단하여 가장 직접적인 경로를 택할 것이다. 만약 여행자가 프랑스로 우회한다면 이는 특별히 계획된 별도의 의도에 의한 것일 것이다. 데이터와 가장 가까운 유형의 ‘우편’도 마찬가지이다. 미국 우편 서비스가 워싱턴 DC에서 필라델피아로 가는 길에 파리를 통해 우편을 보낼 가능성은 거의 없다. 유사하게, 누군가 유형 자산을 안전 금고 또는 저장 장치에 저장하면, 이러한 유형자산은 인지될 수 있으며, 관찰 가능하고 고정 된 위치를 가지게 된다. 절도나 압류조치가 없다면, 주인이 다른 곳으로 이동하기로 결정하기 전까지는 그 자리에 존재하게 된다.[3)]

반면 데이터의 이동은 데이터 사용자의 의지와 무관하게 자의적으로 발생할 수 있다. 데이터의 이동성, 특히 그 이동 속도와 예측 불가능성은 장소 간 물체의 이동에 대한 의미와 재산을 “저장”한다는 것의 의미에 대하여 의문을 제기하게 된다. 예를 들어 독일에서 보낸 전자 메일은 이웃 프랑스에 있는 수신자의 장치에 표시되기 전에 미국을 비롯한 여러 국가를 통과 할 수 있다. 뉴욕에서 생성되고 관리되는 데이터는 네덜란드의 데이터 센터에 저장 될 수 있다. 클라우드에 저장되고 Washington D.C.에서 액세스 한 문서는 아일랜드의 데이터 저장 센터에 일시적으로 저장되며 한 번에 여러 곳에서 복사 및 보관 될 수도 있다. 유사하게 미국에 거주하는 두 명의 미국인이 전자 메일을 보내면 일반적으로 국내정보통신망을 통과하게 된다. 그러나 종종 일부 중요하지 않은 주파수로 수신자의 컴퓨터 화면에 나타나기 전에 국경 내 있는 국내네트워크를 벗어났다가 되돌아오기도 한다.[4)]

3) Jennifer Daskal, the un-territoriality of data, the yale law journal 125:326 2015.

일례로 구글챗(Google chats)이용자가 필라델피아에 있는 친구와 함께 채팅하거나 캘리포니아에 출장 중인 배우자와 FaceTime을 사용하는 경우 당사자도 알지 못하는 사이에 데이터는 프랑스를 경유할 수 있다. 유사하게 데이터가 클라우드에 보관되는 경우 데이터는 하나의 고정된, 관찰가능 한 위치에 놓여있지 않다. 기술적 조치와 서버 유지보수 등의 이유로 옮겨질 수 있으며 복제되거나 여러 파트로 나누어져서 여러 장소에 저장될 수 도 있다. 저장장소는 반드시 자국 영역일수도 그렇지 않을 수도 있다. 특정 순간에 사용자는 그의 데이터가 어디에 저장되어 있는지, 어디로 이동되는지, 이동 경로는 어디인지 알지 못하며 알 수도 없다.

유체물과 데이터의 이러한 차이는 적용되는 법규를 결정할 때 데이터 위치가 임의적으로 결정될 수 있음을 의미한다. 사람과 유체물의 위치는 유체물이 공간을 이동하는 방식에 기반하여 일반적으로 이해되는 규칙이 적용된다. 반면 데이터는 엄청난 속도를 가지고 점진적이며 임의적 방식으로 이동할 수 있다. 또한 이용자의 선택이나 인지 또는 인위적 작동과 무관하게 데이터의 이동경로가 결정될 수 있다. 이는 데이터 주체의 '동의' 및 '고지'의 목적과 관련하여 중요한 문제이다.[5] 누군가 외국의 관할이 미치는 영역을 여행하거나 그 영토 내에 재산을 보유하고 있다면, 해당 국가의 법 적용을 받게 된다. 그러나 누군가 캘리포니아에서 필라델피아에 사는 친구에게 이메일을 보내는데 이러한 이메일이 다른 나라를 경유하게 된다면, 이러한 사실을 아는 한 그는 특정 외국법의 적용을 받기를 선택하지 않을 것이다. 또한 데이터가 미국 외부로 이동한다고 해서 사용자가 의식적으로 미국 수정헌법 제4조[6]에 의해 보장된 보호를 포기하거나 미국 내 재산 검색 및 압류에 관한 법적인 보호를 포기하는 것도 아니다. 마찬가지로 클라우드에 데이터를 저장하는 경우, 이용자는 데이터가 보관되는 장소를 결정할 수 있는 권한을 가지고 있지 못하며 그러한 장소가 어디인지 조차도 알 수 없는 경우가 다반사이다. 이러한 결정들은 일반적으로 컴퓨터 알고리즘에 위탁되어 있다. 따라서 사용자는 적용되는 규칙에 대한 지식과 선택할 수 있는 여건이 부족할 수밖에 없다.[7] 이러한 문제는 데이터의 위치를 규정하는 서비스계약조건을

---

4) Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary, 109th Cong. 4 (2006) (statement of Michael V. Hayden, Director, Central Intelligence Agency).

5) John M.Cauthen, Executing Search Warrants in the Cloud, FBI L. ENFORCEMENT BULL. (Oct. 7, 2014),

6) 국민의 사생활 침해를 막는 법을 제정해 놓은 것으로, 정부에 의한 부당한 수색, 체포, 압수에 대하여 신체, 가택, 서류 및 동산의 안전을 보장받는 국민의 권리는 침해될 수 없다는 것을 기본 골자로 하고 있다. 사인에 의한 부당한 수색, 체포, 압수 등에는 적용되지 않는다. : The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized

7) Anupam Chander & Uyên P. Lê, Data Nationalism, 64 EMORY L.J. 677(2015)

통해 해결될 수 있으며, 특정 데이터는 자국 내 보관하도록 입법적 조치를 취함으로서 해결하고자 하는 국가도 있다.

(2) 가분성 및 분할성(Divisibility and Partitioning)

클라우드에 저장된 데이터는 종종 하나 이상의 위치에 저장되고 복제된다. 이렇게 하면 서버 오작동을 방지하고 사용자가 백업 위치에서 자신의 데이터에 지속적으로 접근할 수 있다. 일부 저장위치는 자국 내 영토가 될 수도 있고 그렇지 않을 수도 있다.[8] 이는 문서 사본을 여러 개 만들어 저장하는 것과 유사하다. 따라서 이러한 관행은 데이터에만 존재하는 것은 아니다. 그러나 데이터는 복제 및 이동 속도가 매우 빠르고 쉽기 때문에 여러 사이트 및 다국적 스토리지의 기하급수적인 증가를 초래하였다. 데이터 분할성(Data partitioning)은 단일 데이터베이스를 여러 부분으로 나누어 관리와 이용효율성을 높이고자 하는 것이다. 이러한 데이터 분할성은 또 다른 복잡성을 야기한다. 분할된 데이터베이스의 다양한 구성 요소는 여러 위치에 보유 될 수 있다. 경우에 따라 소위 "관계형 데이터베이스(relational databases)"는 해당 응용 프로그램을 사용하여 끌어 올 경우에만 이해할 수 있다.[9] 예를 들어 건강관리서비스제공자는 환자의 의료기록을 사무실에서 가져올 수 있다. 그러나 환자이름, 약력정보 및 약물내역 등의 구성요소가 각각 다른 위치에 분산·저장되어 있다면 적정한 소프트웨어가 없이 관련 정보를 사용 가능한 형태로 조립할 수 없다. 이러한 데이터의 분할성은 적용될 법규를 결정하는 데이터의 위치를 결정함에 있어서 복잡성과 임의성을 야기한다. 미국정부가 미국 영토 밖의 백업 시스템에 저장된 복사본을 압수수색함으로서 미국 영역 내에 저장된 외국인의 데이터에 대하여 수정헌법 제4조를 회피할 수 있는가 라는 문제가 제기될 수 있다. 또한 관계형 데이터베이스에서 관련된 위치라 함은 그 데이터가 접근되고 다시 재구성되어 이용가능 한 형태로 되는 위치를 의미하는 것인지에 대한 의문도 제기될 수 있다. 이러한 질문들에서 알 수 있듯이 데이터 위치는 매우 조작하기 쉽고 경우에 따라 정의하기가 어렵다. 따라서 데이터의 이러한 조작가능성과 불확정성은 데이터 위치와 관련하여 적용 규율을 결정할 때 규범적 불안정성을 가져오게 된다.

---

8) Sasha Segall, Note, Jurisdictional Challenges in the United States Government' Move to Cloud Computing Technology, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1105, 1114-15(2013).

9) Ian Walden, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent 3 (Queen Mary Univ. of London, Sch. of Law, Research Paper No. 74, 2011), http://ssrn.com/abstract=1781067 [http://perma.cc/SA7K-J83V] ("echniques widely used in cloud computing, such as 'harding' or 'artitioning,' mean that the data will likely be stored as fragments across a range of machines, logically linked and reassembled on demand, rather than as a contiguous data set."; Tony Morales, Oracle Database VLDB and Partitioning Guide, ORACLE 1-2 (July 2007), http://docs.oracle.com/cd/B28359_01/server.111/b32024.pdf [http://perma.cc/488S-RZK8].

(3) 독립성

데이터의 위치는 법집행자 및 데이터 이용자의 위치로부터 독립, 단절되어 있다. 압수수색을 집행하는 법집행자는 더 이상 압수수색대상인 데이터 소재지와 동일한 구역에 있지 않다. Riley v. California사건에서 법원은 클라우드컴퓨팅으로 인해 수색하려는 데이터의 위치와 그러한 수색을 담당하는 법집행관의 소재지가 같을 수 없다고 한 바 있다.[10] 최근 미국과 멕시코 국경에 있는 미국 측 국경통제요원이 국경의 멕시코 측에 있는 비시민권자들을 사살한 두 건의 사건이 발생하였다.[11] 이 사안에서 죽은 아이들의 부모는 수정헌법 제4조에 위반되는 과도한 집행이라는 주장을 하였다. 한 사건인 Hernandez v. United States 판결에서 제5항소법원은 이에 대하여 미국 영토 밖에 소재지이며 미국시민이 아니라는 이유로 이러한 청구를 기각하였다.[12] 반면 Rodriguez v. Swartz 판결에서 아리조나 법원은 피고가 미국과 근접하며 가족적 연계성이 있다고 하며 수정헌법 제4조의 적용을 인용하였다.[13] 두 법원이 결과는 다른 것 같아도 영토에 대하여 동일한 분석을 하였다. 두 법원 모두 사건 체포는 사망자가 사망한 멕시코에서 발생하였으며, 총기 발사요원의 위치는 모두 미국이라고 분석하였다. 두 경우 모두 “영토성”은 총기발사요원의 위치가 아니라 체포대상의 위치에 기반 하여 판단하였으며, 두 판결 모두 영토외의 체포와 관련이 있음을 전제로 하였다. 드론의 경우 법집행자와 집행대상의 위치가 단절된 또 하나의 사례이다. 드론 작동자는 버지니아의 랭글리에 있다. 이들은 원격으로 드론을 조종하여 예멘, 소말리아, 이라크 등에 폭탄을 터트린다. 그러나 실제로 모든 법적 분석에 의하면 국경 총기사건과 일관되게 영토는 목표대상의 위치에 의해 결정된다고 한다.[14] 총격과 드론의 사건을 유추적용하면, 데이터의 초기 압수·수색은 그 데이터가 접근되고 검토된 장소가 아니라 저장되고 조작된 장소에서 이루어지는 것으로 이해할 수 있다. 즉 이러한 사례는 정부와 법원이 일반적으로 개인 컴퓨터에 대한 데이터의 검색과 압류를 어떻게 고려하고 있는지를 보여준다. 우선 데이터에 대한 집행을 담당하는 집행관의 위치보다는 그러한 데이터가 저장된 컴퓨터의 위치를 고려한다. 예를 들어 United States v. Gorshkov사건[15]에서 시애틀에

10) Riley v. California, 134 S. Ct. 2473, 2491 (2014).

11) Hernandez v. United States, 757 F.3d 249, 255 (5th Cir. 2014) (involving a scenario in which a border agent in Texas shot and killed a fifteen-year-old Mexican), rev' en banc, rev' per curiam, 785 F.3d 117 (5th Cir. 2014), petition for cert. filed, No. 15-118 (U.S. July 27, 2015); Rodriguez v. Swartz, No. 4:14-CV-02251 (D. Ariz. July 9, 2015) (involving a scenario in which a border agent in Arizona shot and killed a sixteen-year-old Mexican).

12) Hernandez, 785 F.3d at 119; see also Hernandez, 757 F.3d at 266-67.

13) Rodriguez, slip op. at 12-16.

14) Memorandum from David J. Barron, Acting Assistant Att' Gen., Office of Legal Counsel, U.S. Dep' of Justice, to Eric Holder, Att' Gen. 38 (July 16, 2010), http://www.justice.gov/sites/default/files/olc/pages/attachments /2015/04/02/2010-07-16_-_olc_aaga_barron_-_al-aulaqi.pdf [http://perma.cc/T55C-CVSW].

15) United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

위치한 법집행관들은 러시아에 있는 컴퓨터에 원격으로 접근하여 데이터를 저장하였다. 관할법원은 법집행관의 위치가 아니라 데이터의 위치를 '영토성'을 판단하는 결정요인으로 삼았기 때문에 이를 '영토 외 수색'으로 간주하였다.[16] 법원은 러시아 컴퓨터에 대한 영토 외 접근과 데이터의 저장은 미국 영역 밖에 위치한 외국 거주자에 대한 영토외적 집행이기 때문에 수정헌법 제4조가 적용되지 않는다고 하였다.

그러나 드론이나 총격에 대한 법집행과 데이터에 대한 법집행은 매우 중요한 차이가 있다. 국경에서 총을 쏘거나 소말리아에서 드론을 띄우는 것은 영공에 대한 명백한 침공이며 다른 국가의 경토에 대한 물리적 효과(폭발, 재산 파괴, 살상 등) 또한 명백하다. 그러나 A라는 국가의 정부가 원격으로 B라는 국가에 위치한 서버에 접근하여 거기에 있는 데이터를 복제한다고 할 때 B국가에서는 어떠한 명백한 물리적 변화도 없으며 데이터 이용자의 데이터 활용 및 접근에도 어떠한 장애 혹은 변화를 초래하지 않는다.[17] 종종 데이터에 대한 원격 접근은 사용자의 데이터 접근성을 제약하지 않으므로 데이터 복제는 수정헌법 제4조가 규율하는 압수에 해당되지 않는다는 견해도 있다.[18] 그러나 이러한 견해를 주장한 Kerr는 이후 견해를 바꾸어 "비합리적인 압수/수색을 금지하는 수정헌법 제4조는 무엇보다도 정보를 통제하고 압수할 정부의 능력을 규제하기 위한 것이므로, 데이터 복제가 정부의 이용가능한 정보들에 추가되는 한 그러한 데이터 복제는 수정헌법상의 '압수'에 해당된다고 한다.[19] 그밖에 다른 학자들과 법원도 이러한 Kerr의 견해와 유사하게 데이터 복제는 헌법상 압수를 구성한다고 한다.[20] 즉 총이나 미사일의 폭발과는 달리 영토 밖에서 디지털 데이터를 복제하는 것은 해당국가가 인지할 수 없이 비밀리에 이루어질 수 있다. 이는 데이터의 위치가 아니라 접근의 소재지(the location of access)가 중요하다는 정부의 입장에 논란을 제기할 여지를 줄 수 있다.

다음으로 데이터는 데이터이용자와 단절된다. 데이터의 위치 독립성 이라 함은 데이터가 사용자와 동일한 또는 가까운 위치에 저장될 필요가 없다는 것과 관련된다. 사용자는 어디에 있던 관계없이 데이터에 접근할 수 있다. 또한 위치 독립성은 데이터 이용시간이

16) Id. at 3.

17) 그러나 특정 유형의 클라우드에 기반 한 인터페이스나 알려지지 않은 아키텍처를 통해 접근될 경우 원격으로 이루어지는 데이터 검색은 데이터 변동을 야기할 수 있다.

18) Orin S. Kerr, Searches and Seizures in a Digital World, 119 HARV. L. REV. 531, 557-58 (2005). 그러나 이 논문에서 Kerr는 데이터의 복제에 요구되는 컴퓨터 조작 그 자체는 헌법적으로 인식가능한 수색에 해당되므로 여전히 영장이 필요하다고 한다. 즉 데이터의 단순한 복제가 아니라 기계적 조작에 기반하여 이루어진 경우 수색에 해당한다.; In re Warrant To Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 472 (S.D.N.Y. 2014). 이 사건에서 치안판사 역시 데이터의 단순한 복제는 수정헌법 제4조의 압수에 해당되지 않는다고 하였다.

19) Orin S. Kerr, Fourth Amendment Seizures of Computer Data, 119 YALE L.J. 700, 704 (2010).

20) Amici Curiae Brennan Center for Justice at NYU School of Law et al. in Support of Appellant at 4 ; Susan W. Brenner & Barbara A. Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, 8 MICH. TELECOMM. & TECH. L. REV. 39, 113 (2002); Paul Ohm, The Fourth Amendment Right To Delete, 119 HARV. L. REV. F. 10, 12(2005).

최고조에 달했을 때 스토리지 센터의 이용을 최소화하기 위하여 서비스 제공자는 데이터를 이동시킨다. 이러한 데이터 이동을 통해 서버 다운이나 정전을 피할 수 있고 사용자 접근을 중단하는 등의 이용자 불편을 초래하지 않고 서버 유지보수를 수행할 수 있다.[21] 현재 관행상 서비스제공자는 데이터의 위치를 통제한다. 데이터 이동에 대하여 이용자에게 고지하거나 동의를 득하지 아니하고 데이터 위치를 결정한다. 사실 이용자는 자기 데이터가 특정 시점에 어디에 저장되는지에 대하여 그다지 관심을 가지지 않기도 한다.

(4) 혼합성(Data' Intermingling)

데이터는 여러 사용자의 데이터와 섞일 수 있다. 네트워크를 통과하는 통신은 종종 다중통신송신으로 묶여진다. NSA조차도 현재 이러한 통신을 분리된 구성요소로 분리할 수 있는 기술적 역량이 부족하다.[22] 그러므로 이러한 번들링된 통신 중 일부에 감시 대상인 외국인에 대한 부분이 속해 있다면, 정부는 그 송신 전체를 획득할 수밖에 없을 것이다. 데이터의 이러한 속성으로 인해 데이터의 수집 단계부터 사용자 식별을 수행하는 것이 곤란하다. 즉 이러한 데이터의 '혼합성'은 영토를 기반으로 적용되는 법을 결정하기 위하여 관련된 사용자 데이터를 확인하는 현재의 방식에 의문을 제기할 수밖에 없다. 예를 들어 아직 일반에게 공개되지 않았으나 몇몇 개인들이 접근가능 한 Google문서를 가정해 보자. 또는 이러한 문서를 공유하는 채팅방을 운영함에 있어서 여러 사용자가 모두 암호화를 사용하여 그러한 채팅을 비공개로 유지하려는 의도가 있다고 가정해 보자. Google문서에 액세스하는 각 사용자의 위치 및 ID 또는 다중 참여자 채팅의 모든 참가자의 위치 및 ID를 확인할 수 있다고 하더라도, 적용법규를 결정함에 있어서 누구의 신분과 위치를 기준으로 할 것인가라는 문제가 제기된다. 예를 들어, 수정헌법 제4조의 적용과 관련하여 사용자 중 한 명이 미국에 있거나 미국 시민권자나 또는 이 조문의 적용이 가능한 자인 경우 Google 문서에는 수정헌법 제4조가 적용되는 것인지, 아니면 검색대상이나 사용자 모두가 수정헌법 제4조의 적용대상이 되는 경우에만 구글문서는 보호될 수 있는 것인지 불명확하다.[23]

(5) 제3자 관련성

유체물의 소유자는 해당 소유물에 대하여 부분적으로 제3자에게 유지관리를 부탁하기도 하지만 대부분은 스스로 보유하려 한다. 그러나 우리는 우리의 디지털재산의 상당부분에 대하여 다른 사람에게 통제권 혹은 지배권을 부여한다. 데이터의 상당부분은 제3자에 의해

21) Damon C. Andrews & John M. Newman, Personal Jurisdiction and Choice of Law in the Cloud, 73 MD. L. REV. 313, 325-28(2013).

22) Memorandum Opinion, [Caption Redacted], [Docket No. Redacted], 2011 WL 10945618, at *10 (FISA Ct. Oct. 3, 2011)https://www.clearinghouse.net/chDocs/public/NS-DC-0057-0002.pdf (2017.4.10. 확인) at 31-41.

23) Orin S. Kerr, The Fourth Amendment and the Global Internet, 67 STAN. L. REV. 285(2015) at 317.

보유되거나 통제된다. 그러한 제3자에는 ISP, 클라우스서비스제공자, 그리고 유선망을 운영·관리하는 기업 등이 모두 포함된다. 더욱이 데이터가 유통되는 경로와 데이터 저장장소에 대하여 중요한 결정을 내릴 수 있는 자는 일반적으로 데이터 사용자가 아니라 그러한 제3자 이다. 또한 정부관료가 요구하는 데이터를 수집하고 생산하도록 요구되는 자도 이용자가 아니라 이러한 제3자 이다. 미국에서는 제3자 원칙에 따라서, 제3자에게 공개된 데이터는 프라이버시의 합리적 기대에 의해 보호받지 못한다.[24] 그러한 원칙은 1970년대의 2개의 대법원 판결 즉 Smith v. Maryland사건[25]과 United States v. Miller사건[26]에서 비롯되었다. 그러나 Smith v. Maryland사건 당시 기술적 수준이 그다지 정교하지 못한 상태에서 데이터의 양은 지극히 제한적이었다.[27] 그러나 오늘날은 제3자에게 엄청난 양의 개인의 사적인 정보를 노출시키지 않고는 디지털 세계에 참여한다는 것은 불가능하다. 따라서 이러한 제3자 원칙에 의해 문제를 해결하는 것은 곤란하다.[28] 오히려 이러한 제3자 이슈는 데이터와 다른 유형의 유체물 간의 차이점이 명확하다는 것을 확인시켜 줄 뿐이다.

2. 인터넷 공간과 데이터 주권

(1) 주권과 인터넷 공간

주권은 영토를 기반으로 하는 국민국가를 단위로 하여 절대성과 항구성을 특질로 하는 권력으로 이해되고 있다. 즉 고대나 중세의 국가와는 구별되는 입헌적 주권국가로서 근대적 의미의 국민국가를 개념적 전제로 하는 것이다.[29] 주권은 어떤 공동체이건 권력이 미치는 일정한 공동체를 배경으로 하는 것이어야 하고 그 공동체 내에서의 지배력 또는 통치권능이 인정되는 권위일 수 있어야 한다.[30]

주권에 관한 논의가 매우 혼란스럽게 전개되고는 있지만,[31] 대외적 독립성과 대내적 최고성을 주권개념의 핵심적 징표로 인정하는 것은 대체로 일치하고 있다.[32] 여기서 대내적

---

24) Smith v. Miller, 425 U.S. 435, 443 (1976) 당시 이 판례는 "수정헌법 제4조는 제3자에게 공개된 정보를 획득하여 정부에게 제공하는 것을 금지하지 않는다. 이러한 정보가 제한된 목적을 위해서만 사용되고 제3자에 대한 신뢰의 원칙이 지켜질 것이라는 전제 하에 공개된 것이라 할지라도 이러한 제한이 적용된다"고 판시하고 있다.

25) 442 U.S. 735 (1979).

26) 425 U.S. 435 (1976).

27) Smith, 442 U.S. at 737 (여기서 데이터량은 단 하루 동안 걸려 진 전화번호의 수집량이다) Miller, 425 U.S. at 437-38 (여기서의 데이터량은 4달 동안의 은행기록이다).

28) Jennifer Daskal, The un-territoriality of data, the yale law journal 125:326 2015.

29) 이성환, 국민국가의 변천과 헌법의 과제, 법학논총, 제10호, 1998, 281면-282면.

30) 주권의 개념과 주권이론의 변천에 관하여는 '박경철, 보댕, 홉스, 루소의 주권이론과 주권론, 강원법학 제23권(2006. 12), 73-102면' 참조.

31) 주권의 개념과 본질에 관한 논의는 완전히 통일되어 있지 않다. 주권의 개념과 본질을 둘러싼 다양한 논의에 대하여는 Hermann Heller/김효전 역, 주권론(Ⅰ), 동아법학, 제29호, 2001; Hermann Heller/김효전 역, 주권론(Ⅱ), 동아법학, 제32호, 2003 참조.

최고성이란 한 국가 내에서 국가의사를 전반적이고 최종적으로 결정할 힘을 의미하며, 대외적 독립성이란 국가의 의사를 결정하는 경우에 외세의 영향력으로부터 자유로워야 한다는 것을 의미한다.[33] 그러나 국가가 외부로부터의 강제적 압력을 배제하지 못한다면 대내적 문제에 대해서도 외적 간섭을 수용할 수밖에 없으며, 일정한 영역에 대한 배타적 주권을 대외적으로 주장하기 위해서는 내부의 이질적인 세력을 배척할 수 있어야 하므로 양자는 서로 다른 개념이 아니라 상호 밀접하게 연계된다.

인터넷이 창출한 공간에 주권이 미치는 영향에 대하여는 국가주권을 해체하는데 기여한다는 견해와 이를 부정하는 견해가 있다. 우선 국가주권의 해체에 기여한다는 견해에 의하면 국내문제에 대한 외부의 간섭을 배제할 수 있는 국가의 권력인 주권은 경계를 알지 못하는 인터넷의 영향으로 매우 빠른 속도로 침식되고 있다고 한다. 인터넷은 경제, 인권, 환경 등을 주제로 활동하는 국제기구나 국제적 비정부기구의 역할증대 등과 같이 주권에 위협을 주는 요소들과 합세하여 주권을 해체한다는 것이다.[34]

이를 부정하는 견해는 인터넷이 국내적 차원에서 법의 지배를 강화하기 위한 수단으로 이용될 수 있는 것과 마찬가지로 세계적 차원에서도 주권을 침식하는 것이 아니라 오히려 주권의 가치를 증대시킬 수 있는 가능성을 가진다고 주장하기도 한다.[35] 또한 인터넷 공간 자체는 주권의 가치를 떨어뜨리거나 더욱 확고히 하는 것이 아니며, 단지 중립적인 성격을 가지는 것으로 보아야 한다는 견해도 있다.[36]

최근 세계화의 현상들은 국민국가의 위상에 변화를 초래하는 요인이 되고 있으며, 이에 전통적인 주권이론에 바탕을 둔 국가의 독립적 존속가능성에 대해서까지 의문이 제기되고 있다. 국경과 일치하는 것으로 이해되던 국가권력의 외적인 경계가 세계화에 따라 점차 융통성 있게 변화하고 있는 상황에서는 영토를 기반으로 한 근대국가의 형성에 중심적 역할을 수행했던 주권개념이 그 실질적인 전제조건을 상실한 것으로 파악될 수 있기 때문이다.[37] 이러한 세계화에 인터넷이 매우 중요한 역할을 하고 있다. 인터넷은 경제에 대한 법적규제, 도덕적·이념적 가치의 보호, 국가적 동질성의 확보 등과 같은 국가의 전통적 기능에 위협이 되고 있지만, 이는 곧 그만큼 국가 간의 경제적 상호의존성과 적합한 규제를 위한 협력의 필요성을 증대시키는 결과를 가져온다는 점에서 세계화의 주요한 동력이 된다.[38]

---

32) 김명재, 헌법상의 국민주권의 개념, 공법학연구, 제7권 제1호, 2006, 86-87면.
33) 김종서, 한미FTA와 민주주의, 민주법학, 제32호, 2006, 113면.
34) Walter B. Wriston, Bits, Bytes, and Diplomacy, Foreign Affairs, Vol.76 No.5, 1997, 174면~175면.
35) Henry H. Perritt, The Internet as a Threat to Sovereignty?, Indiana Journal of Global Legal Studies, Vol.5 No.2, 1998, 423면.
36) Georgios Zekos, Internet or Electronic Technology, The Journal of Information, Law and Technology, Issue3, 1999.
37) Dieter Grimm (Hrsg.), Staatsaufgaben, Baden-Baden: Nomos, 1994, 9면.
38) 홍석한, 세계화에 따른 주권의 변화에 관한 헌법적 고찰, 公法學硏究 第10卷 第2號, 2009, 193면.

(2) 인터넷 공간에서의 데이터 주권

데이터는 인터넷이 창출한 공간을 통해 유통된다. 데이터 주권의 문제는 결국 데이터의 창출, 유통 등의 행위가 이루어지는 '인터넷 공간에서 주권이 미치는가' 하는 문제라고 할 수 있다.

영토는 국가임을 나타내는 우선적 기준이고 국제사회 참여에 있어서 필수불가결한 선결요건이[39] 된다. 다른 국가가 국경을 넘어서 자국영토 내에 들어오거나 국경을 넘어가는 데이터의 전달과 자신의 영토 내에서 개인이 자국의 기준에 합치되지 않는 데이터를 사용하는 것을 규제할 수 있는 권한을 갖는다는 것이 '현실주의적 주권개념'이다.[40] 이러한 주권개념은 규제를 위한 관할권을 주장함에 있어서 영토 원칙(the territoriality principle)과 효과원칙(the effects principle)을 근거로 한다.[41] 즉 인터넷을 통해서 유해한 데이터가 자국 영토 내에 전파되는 것을 방지할 수 있는 국가의 권한이 인정된다. 또한 자국 내에서 발생한 불법적 결과의 원인이 되는 인터넷상의 데이터 활동이 자국 영토 이외의 지역에서의 인터넷 이용자나 서비스 제공자에 의한 경우일 때, 불법적 결과와 견련성 있다면 효과적인 해결을 위해 그들에 대한 규제관할권을 주장하는 것이다.

한편 국가는 그 자체의 의지를 갖는 것이 아니라 각 구성원들의 다양한 이해관계를 대변하는 역할을 수행하는 대표기관이며[42] 주권을 이러한 대의 또는 대표의 개념으로 분석하는 것이 '대의주의적 주권개념'이다.[43] 이러한 견해에 의할 경우 인터넷 공간에서의 특정한 활동들이 국민을 대표하는 주권국가의 기능을 저해하고, 국민들의 의지에 유해한 내용을 전파하는 경우라면 국민의 대표로서의 주권국가는 그러한 문제점들을 당연히 앞장서서 규제할 수 있다. 다만 주권국가가 대표해야 하는 국민의 일반의지가 전제되어야 한다. 이러한 전제 없이 온라인상에서 뿐만 아니라 오프라인 상에서도 어떠한 규제도 행사할 수 없다.

결국 주권개념에 의거할 때 인터넷 공간에서도 데이터 규제와 관련된 관할권이 인정된다. 그러나 국가주권에 기초한 관할권-입법, 사법, 행정적 관할권-의 영역에서 국가들은

---

39) Paul R. Viotti & Mark V. Kauppi, INTERNATIONAL RELATIONS THEORY: REALISM, PLURALISM, GLOBALISM(2d ed. 1993) pp. 723-724.

40) 조소영, 인터넷 주권과 통제에 관한 연구, 公法學硏究 第12卷 第4號, 2009, 363-364면.

41) Stephan Wilske & Teresa Schiller, International Jurisdiction in Cyberspace: Which States May Regulate the Internet?, 50 Fed. Comm. L.J. 117, 1997, pp.129-142.

42) Paul R. Viotti & Mark V. Kauppi, INTERNATIONAL RELATIONS THEORY: REALISM, PLURALISM, GLOBALISM(2d ed. 1993), pp.230-231.

43) 진정한 주권국가가 되기 위해서는 국민들의 일반의지를 대표해야 하므로 대의주의적 주권 개념 하에서는 "오직 인권과 민주주의 대표원칙을 존중하는 국가만이 합법적인 국가인 것이고 이러한 국가만이 그 국민을 대표할 수 있는 권한으로서의 주권을 부여받는다"고 함으로써 그들의 주권국가를 정의하고 있다. Roxanne Lynn Doty, SOVEREIGNTY AND THE NATION: CONSTRUCTING THE BOUNDARIES OF NATIONAL IDENTITY(Thomas J. Biersteker & Cynthia Weber eds.,1996) pp. 121-122.

독자적인 법체계를 가지고 있으며 이를 통하여 자국의 안보, 경제, 사회문화적 가치를 지키고, 인터넷의 위협적 효과 및 인터넷에 의한 부가가치 생산에도 대처하고 있다. 즉 국가들은 국가주권에 기초하여 국제법상 정당한 관할권을 가지는 한도 내에서 독자적 법체계를 구축하고 있다.[44] 그 결과 한 국가에서는 적법한 활동이 동시에 유효한 관할권을 가진 다른 국가에서는 위법할 수가 있는 것이다.

3. 데이터와 규범의 충돌, 그리고 데이터 국지화

(1) 데이터와 규범의 충돌

데이터의 속성은 탈영토성(un-territoriality)을 기반으로 한다. 따라서 영토에 기반 하여 주권 및 관할을 전제 하고 있는 현재의 규범체계를 그대로 데이터 규범에 적용하는 것은 규범의 집행을 불안정하게 만든다. 즉 데이터의 탈영토성은 영토를 기준으로 시민과 국가를 연계하여 헌법과 법규의 적용을 결정하는 기준에 의문을 제기한다.

부동산이나 동산의 경우 그 소재지에 의해 관할 및 적용법규가 정해진다. 즉 현재의 규범(유체물 규범)은 규범대상의 위치 및 이동에 대하여 수범주체의 인지를 전제로 그의 의지를 존중한다. 그러나 데이터의 이동성과 독립성은 데이터의 소재지가 적용법을 결정한다는 전제에 중요한 의문을 제기한다. 프라이버시권 또는 증거에 접근하려는 법집행은 데이터가 거의 실시간 무작위적으로 이동되고 있음에도 불구하고 특정시점에 데이터가 어디에 있는지에 대하여만 초점을 맞추고 있다. 그러나 데이터의 이동은 임의적이기 때문에 데이터의 주체라 할 수 있는 데이터 생성자 혹은 이용자가 데이터의 위치 및 이동에 대하여 인식할 수 없다. 따라서 데이터를 기준으로 적용법규를 결정하는 것이 무리이다. 적용법규를 명확히 하는 규범적 방법은 데이터 이동의 임의성이라는 속성에 제한을 가하는 것이다. 즉 데이터의 위치를 규정하는 서비스계약조건이나 입법 조치를 통해 특정 데이터는 반드시 특정 국가 혹은 지역 내에 보관하도록 조치를 취하는 것이다.

또한 데이터의 '분할성'은 광대한 양의 데이터 저장 및 이용의 효율을 높일 수 있는 데이터의 중요한 속성이다. 그러나 이러한 데이터 분할성으로 인해 데이터 위치를 데이터 주체가 인지하는 것은 매우 곤란하며, 그 소재를 인지할 수 없으므로 권리주장은 더욱 어렵다. 데이터의 '분할성'을 존중하는 한 기존 유체물의 공간을 중심으로 한 분할에 대한 규범을 그대로 데이터에 대한 관할 또는 적용법규에 적용하는 것은 곤란하다.

뿐만 아니라 데이터와 데이터 이용자 간의 단절은 법 집행에 있어서 실질적 문제를 불러일으키게 된다. 법 집행관이 집행대상자의 스마트 폰, 컴퓨터 또는 기타 전자 장치를 찾은 경우에도 장치에 저장된 데이터가 실제로 보관되는 위치를 알 수 없는 경우가 종종

44) Henkin et al, International Law: Cases and Materials, St.Paul: West Publishing, 1993 3rd ed, Ch12; 김대순, 국제법론, 삼영사, 2001, 제9장.

발생한다. 데이터를 찾고 있는 집행관이 보고 있는 스마트폰의 데이터가 집행시점의 그 장소에 저장 되어 있다고 보아야 하는지, 클라우드에서 끌어온 것인지 알 수 없다. 데이터를 볼 수 있는 디바이스와 필요한 패스워드가 있는 경우에도 클라우드 덕분에 영토내에 저장된 데이터에 접근하고 있는 것인지, 영토 밖의 데이터에 접근하고 있는 것인지 확신할 수 없다.[45] 그리고 법집행관이 데이터의 위치를 알아냈다고 할지라도 데이터 사용자의 위치를 알 수 있는 것은 아니다. 퍼레이드에서 폭발물을 원격으로 터뜨릴 계획을 기술한 이메일 작성자의 위치와 신원을 추적하고자 한다고 가정해 보자. 이를 추적하는 집행관은 이메일을 보낸 디바이스와 데이터를 연계시켜야 한다. 이를 위해 우선 디바이스의 위치를 확인한다. 그 다음 디바이스 사용자의 위치를 확인하여야 하는 데 실시간 추적이 없으면 디바이스의 사용자의 위치는 디바이스 자체의 위치와 다를 수 있다. 그 다음 디바이스 사용자의 신원을 확인하여야 한다. 법 집행을 목적으로 추상적 목표를 다룰 때 식별이 가능할 수도 있지만(어렵긴 하지만) 현재 감시 프로그램에서 수집되는 엄청난 양의 데이터로 인해 이러한 개별화 된 분석을 수행하는 것은 거의 불가능하다.[46] 한편, 익명화 도구를 사용하면 법 집행 기관 및 정보 요원 모두에게 식별 어려움이 발생한다. 이러한 식별은 반드시 데이터에만 존재하는 것은 아니다. FedEX가 수상해 보이는 포장물품을 조사한 결과, 코카인을 발견하였고 정부에 보고하여 수사관이 그 포장물품의 발신자를 추적한다고 가정해 보자. 아마도 발신자에게 보낼 수 있는 반송주소는 있지만 그러한 주소는 잘못되었거나 정확하지 않을 것이며, 하물며 발신주소가 없을 수도 있다. 이처럼 식별추적의 문제는 유체물에서도 어렵다. 그러나 방대한 양의 데이터와 익명화 도구들, 그리고 데이터를 전송함에 있어서 순회방식 등은 데이터의 이용자를 식별하는 것을 더 어렵게 만든다. 이러한 데이터의 단절적/독립적 성격은 법 적용의 기준으로 작용하고 있는 사용자 위치와 기타 주요 구성요소 등에 대하여 의문을 제기할 수밖에 없다.

그리고 데이터의 혼합적 성격으로 인해 법이 요구하는 바에 따라 데이터를 미세하게 조정해서 식별 및 위치에 기반 한 형태로 만드는 것이 거의 불가능하다. 다중송신(multi-communication transactions)의 문제가 없다 할지라도, 우리가 상호 연결된 글로벌한 네트워크 사회에 살고 있는 한 자국민과 외국인의 데이터는 불가피하게 섞여 있을 수밖에 없다. 결국 광범위한 감시 프로그램과 대량 수집이라는 방법은 부수적인/의도하지 않은 데이터를 수집하게 된다.

한편 통상적으로 유체물에 대하여는 그 소유 또는 점유할 정당한 권한을 가지는 자가 그 유체물에 대하여 지배력을 행사하도록 규범이 설정되어 있다. 그러나 현실적으로 데이터에 대하여는 그 데이터의 창출/이용에 정당한 권한을 가지는 데이터 이용자가 아니라,

45) Riley v. California, 134 S. Ct. 2473, 2491, 2495 (2014).
46) William C. Banks, Programmatic Surveillance and FISA: Of Needles in Haystacks, 88 TEX. L. REV. 1633 (2010) at 1639, 1645.

데이터서비스제공자, 클라우드컴퓨팅 서비스제공자 등 제3자가 데이터에 대한 관리지배력을 가지게 된다. 데이터의 위치는 데이터이용자의 소재지와 단절되며 데이터 위치에 대한 이용자의 인지가능성도 떨어지기 때문이다. 결국 제3자가 데이터에 대한 통제권을 가지며 이용자는 그들의 데이터에 대해 특정 시점에서 직접적인 통제권을 결하게 된다. 이러한 데이터의 특성은 적용 법규를 결정함에 있어서 데이터의 위치를 특정해야 한다는 규범적 문제에 봉착하게 된다. 통상적으로 유체재산의 위치는 재산권자의 선택이며 그 유체물이 위치하고 있는 장소와 관련된다. 그러나 데이터에 대하여는 소유자의 의도와 물건의 위치가 연계된다는 기본적 가정이 적용될 수 없다. 사용자는 그의 데이터가 특정 시점에 어디에 있는지 알 수 없으므로 데이터의 위치가 이용자에게 많은 의미가 있다고 주장하는 것이 어렵다. 따라서 특정 시점의 데이터 위치는 특정 위치에 대한 데이터 사용자의 유대를 잘 나타내지도 않을뿐더러, 사용자의 관점에서 볼 때 적용해야하는 규칙을 정하는 공정한 요인이라고 볼 수도 없다.[47]

특히 이러한 데이터의 제3자 지배와 관련된 속성은 몇 가지 중요한 규범적 문제를 발생시킨다. 우선, 제3자의 위치(그러한 재산의 위치가 아니라)가 잠재적으로 어떠한 법을 적용할 것인지를 결정할 수 있는 요인이 될 수 있다는 것이다. 예를 들어 MS는 미국에 소재하고 있기 때문에 정부는 MS의 통제 하에 있는 데이터의 생산을 데이터의 소재와 관계없이 강제할 수 있다. 데이터에 대한 제3자(MS)의 통제권은 영토 밖에 있는 데이터에 대한 정부의 입장을 조율할 수 있는 가능성을 제시한다고 볼 수 있다. 즉 데이터가 영토 밖에 있어서 법집행관의 접근이 불가능하다 할지라도, 정부는 제3자(MS)를 통하여 데이터를 조사하도록 할 수 있다.[48]

(2) 데이터주권과 데이터 국지화

앞서 논의하였듯이 주권은 영토를 기반으로 하는 국민국가를 단위로 하여 절대성과 항구성을 특질로 하는 권력이다. 영토는 국가임을 나타내는 우선적 기준이고 국제사회 참여에 있어서 필수불가결한 선결요건이 된다. 데이터가 생성·유통되는 공간으로서 인터넷을 기반으로 하는 공간은 주권이 미치는 영역이다. 따라서 인터넷 공간의 데이터에 대하여 주권의 실행으로서 관할권을 행사하기 위해서는 우선 데이터에 대하여 관리/지배가능성이 있어야 한다. 이러한 관리/지배가능성은 유체물 및 영토기반의 규범하에서는 소재의 인지를 전제로 한다. 관할의 대상이 되는 물건 혹은 사람에 대한 위치의 인지가 없이는 주권의 행사로서 적절한 관할권 행사가 곤란하다. 그러나 앞서 언급하였듯이 데이터에 대하여는

47) Jennifer Daskal, the un-territoriality of data, the yale law journal 125:326, 2015.

48) Brief for Appellant at 16, In re Warrant To Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985-CV (2d Cir. Dec. 8. 2014) at 30-32. 본 결정문에 의하면 MS는 본질적으로 정부입찰을 수행하기 위해 정부의 요구에 따라야 하므로 정부의 대리인으로서 정부의 규율에 의해 활동한다고 한다.

이동성·독립성·혼합성·분할성·제3자 관련성 등의 속성으로 인해 데이터의 소재를 파악한다는 것이 매우 힘든 일이며 정보주체 혹은 이용자는 그들의 데이터에 대해 특정 시점에서 직접적인 통제권을 상실하게 된다. 사실 클라우드 컴퓨팅이나 글로벌 인터넷의 효율성에 비추어 볼 때 상당 부분 데이터 유통에 대한 권한은 가장 신속한 방법으로 제3자에게 의존할 수밖에 없다. 그 결과 대부분 데이터 유통에 대하여 제3자는 자국민인 이용자의 선호도나 통제에 의해 제약을 받지 않으며 데이터 이용자인 국민들은 데이터에 대한 통제권을 상실하게 된다.

또한 데이터의 위치는 법집행자의 소재지로부터 독립/단절된다. 법 집행대상이 총격이나 미사일의 폭발등인 경우에도 법집행자와 법집행대상이 독립/단절된다. 그러나 이와 달리 영토 밖에서 디지털 데이터를 복제하는 것은 해당국가가 인지할 수 없이 비밀리에 이루어질 수 있다. 정부가 얻고자 하는 대상 데이터와 정부기관이 접근하는 데이터 간의 위치가 각각 독립되어 있으므로 A국가는 B국가에 대한 어떠한 물리적 침해 없이 B국가에 있는 데이터를 압수 수색할 수 있다. 그러나 압수수색의 시기 및 범위와 방법 등은 A국가가 결정한 것이기 때문에 B국가의 입장에서는 주권 침해를 주장할 수 있다. 이러한 일방적인 데이터 압류는 많은 국가들이 자국 영토 내의 데이터에 대한 주권통제력과 규제를 수립하려는 오랜 노력을 무시하는 결과와 법률 간의 충돌가능성을 초래한다.

따라서 이러한 데이터의 속성을 영토주의 원칙에 부합하게 제약 하려는 규범적 시도가 바로 데이터의 위치를 제한하는 '데이터 국지화(Data Localization)' 조치라고 할 수 있다. 데이터 국지화는 말 그대로 데이터의 국가 간, 지역 간 이동에 제약을 두려는 움직임으로 널리 이해할 수 있다.[49] 여기에는 다양한 방식이 포함되는바, 정보가 국외로 전송되는 것을 금지할 수도 있고, 정보가 국경 너머로 이전되기에 앞서 정보 주체의 사전 동의 혹은 정보의 승인을 요구할 수도 있으며, 정보의 사본이 국내에 저장될 것을 요구할 수도 있고, 데이터 수출에 세금을 부과할 수도 있다.[50] 국경을 넘어서 자국영토 내에 들어오거나 국경을 넘어가는 데이터의 전달에 대하여 국가가 주권에 기반 하여 직접적으로 규제를 하고자 하는 것이다. 자신의 영토 내에서 자국의 기준에 합치되지 않는 데이터를 사용하는 경우도 마찬가지다. 입법을 통해 혹은 계약을 통해 특정 데이터가 특정 지역에 저장 또는 이동되어야 함을 정하는 것이다.

49) 허진성, 데이터 국지화(Data Localization) 정책의 세계적 흐름과 그 법제적 함의, 언론과법 13(2), 한국언론법학회, 2014.12, 290면.

50) Chander, Anupam and Le, Uyen P., Breaking the Web: Data Localization vs. the Global Internet 3 (April 2014). Emory Law Journal, Forthcoming; UC Davis Legal Studies Research Paper No. 378.

Ⅲ. 데이터 국지화 규범 현황 및 분석

1. 국가별 규범 동향

(1) 유럽

1) 프랑스

프랑스 정부는 외국의 감시 및 경쟁력에 대한 우려를 기반으로 지난 몇 년간 주권 클라우드(the sovereign cloud 또는 le cloud souverain)라고 불리는 "지역 데이터 센터 기반시설"을 홍보하기 위해 노력해 왔다. 정부는 2개의 클라우드 컴퓨팅 기업 Numergy와 Cloudwatt에 직접 투자하여 각각에 3분의 1지분을 보유하고 있다.[51] 2013년 2월 Arnaud Montebourg 산업부 장관은 프랑스 자국 내 고용을 지원하기 위해 프랑스영역 내에서 데이터 처리하는 것을 지지한다고 공개적으로 선언한 바 있다.[52] 국내기업에 대한 보조금이 교역조건 위반인지 아닌지는 매우 복잡한 문제이다. 특히 스노든의 폭로는 프랑스 정부가 데이터 국지화를 추진할 것을 촉구시켰다. Fleur Pellerin 디지털 경제 장관은 "PRISM 주장이 사실로 밝혀진다면 프랑스 자국 영역내에 데이터 센터와 서버를 두는 것이 데이터 보안을 위해 매우 중요하다"고 밝히기도 하였다.[53] 프랑스에 있는 사용자에 의해 만들어진 개인정보를 상업적으로 이용하거나 관리, 수집하는 것에 대하여 세금을 부과하자는 제안은 당연히 자국밖에 위치한 외국에서 제공하는 서비스를 억제시키는 방향으로 시행될 수도 있다. 그러나 실제로 그러한 세금부과를 찬성하는 사람들에 의하면 세금의 목표중 하나는 국내 경제에서의 생산성 향상과 가치 창조를 증진하는 것이라고 한다.[54] 소위 "데이터 세금"은 "사용자의 활동을 정기적으로 체계적으로 모니터링 하여 얻은 데이터"에 적용된다.[55] 또한 이러한 데이터세금제에 따르면 세율은 프라이버시와 관련된 법규준수의 수준에 따라 달라진다. 서비스제공자가 프라이버시 보호와 관련된 준수의무를 다한다면 세율은

51) David Meyer, A Guide to the French National Cloud(s), GIGAOM (Nov. 18, 2013, 7:55 AM PST), http://gigaom.com/2013/11/18/a-guide-to-the-french-national-clouds/.

52) Arnaud Montebourg: «Google et Facebook agissent ainsi car il n' a pas de règles» [Arnaud Montebourg: Google and Facebook are Doing this Because There are No Rules], 20 MINUTES.FR (Feb. 28, 2013 09:29), http://www.20minutes.fr/politique/1109303-arnaud-montebourg-nous-faisons-tous-jours-loiscitoyens-pourquoi-contre-geants-linternet.

53) Valéry Marchive, France Hopes to Turn PRISM Worries into Cloud Opportunities, ZDNET (June 21, 2013, 9:02 GMT), http://www.zdnet.com/france-hopes-to-turn-prism-worries-into-cloud-opportunities-7000017089/ (second alteration in original).

54) PIERRE COLLIN & NICHOLAS COLIN, TASK FORCE ON TAXATION OF THE DIGITAL ECON., REPORT TO THE MINISTER FOR THE ECONOMY AND FINANCE, THE MINISTER FOR INDUSTRIAL RECOVERY, THE MINISTER DELEGATE FOR THE BUDGET AND THE MINISTER DELEGATE FOR SMALL AND MEDIUM-SIZED ENTERPRISES, INNOVATION AND THE DIGITAL ECONOMY at 122 (2013).

55) Id. at 123.

거의 제로에 이르게 된다.[56] 미국에서의 데이터 처리가 세이프하버에 따라 수행되고 있다 할지라도 프랑스법 준수에 어긋난다고 판단한다면, 그러한 세금은 데이터 수출에 대한 세금으로 효율적으로 기능하게 될 것이다.[57] 이에 대하여 어떤 보고서는 과세의 탈을 쓴 글로벌 무역전쟁이 발생할 수 도 있다고 주목하고 있다.[58] 프랑수아 올랑드(Francois Hollande) 전 대통령은 미국의 스파이 행동에 대한 분노를 표명하면서, 프랑스는 2013년 12월 10일 프랑스 애국자법(the French Patriot Act)으로 명명된 군사방위법(Military Programming Law)을 채택하였으며 이 법은 방위부, 내무부, 경제부, 예산담당 부처 등 여러 부처들이 전자적·디지털 통신을 실시간으로 볼 수 있도록 허용하고 있다.[59]

2) 독일

스노든의 폭로 이후, 독일 데이터보호위원회는 독일 정부가 외국의 첩보활동이 데이터 보호법의 기본원칙을 준수하고 있다고 보증할 때까지 모든 국가 간 데이터 이동을 승인하지 않겠다고 발표하였다.[60] 위원회는 NSA의 위법행위가 일어날 수 있었던 것이 결국 독일기업에 의해 이전된 데이터가 NSA를 비롯한 여러 다른 외국의 정보기관에 의해 접근될 수 있었기 때문이라고 판단하였다. 특히 독일 프라이버시 규제당국은 2010년에 미국의 세이프 하버(Safe Harbor)를 통해 자기 인증이 이루어지는 것 자체가 저절로 적절한 보호조치의 결정적 증거로 간주되어서는 안 된다며 문제를 제기한 바 있다.[61] 위원회는 유럽 영역

56) Id. at 123.
57) Id. at 123 - 4
58) Ian Allison, Europe Cracks Down on Google, Apple, Facebook and the Data-Driven Tax Black Hole, INT'L BUS. TIMES (Dec. 12, 2013, 09:18 GMT), http://www.ibtimes.co.uk/tax-internet-ec-oecd-googlefacebook-apple-529601 (internal quotation marks omitted); see also Bruno Waterfield, UK Braced for Battle with France over Google Data Tax, TELEGRAPH (Oct. 23, 2013, 3:42 PM BST), http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/10399840/UK-braced-for-battle-with-France-over-Google-data-tax.html.
59) Loi 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale [Law No. 2013-1168 of December 18, 2013 on the Military Budget for the Years 2014 - 019 and Miscellaneous Provisions for Defense and National Security], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Dec. 19, 2013, p. 20570 (Fr.); Kim Willsher, French Officials Can Monitor Internet Users in Real Time Under New Law, GUARDIAN (Dec. 11, 2013, 13:18 EST), http://www.theguardian.com/world/2013/dec/11/french-officials-internet-users-real-time-law.
60) Press Release, Die Landesbeauftragte für Datenschutz und Informationsfreiheit [State Commissioner for Data Protection and Freedom of Information], Conference of Data Protection Commissioners Says that Intelligence Services Constitute a Mass Threat to Data Traffic Between Germany and Countries Outside Europe (July 24, 2013), available at http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile.
61) BESCHLUSS DER OBERSTEN AUFSICHTSBEHÖR DEN FÜR DEN DATENSCHUTZ IM NICHT-ÖFFENTLICHEN BEREICH AM 28./29. APRIL 2010 IN HANNOVER, PRÜFUNG DER SELBST-ZERTIFIZIERUNG DES DATENIMPORTEURS NACH DEM SAFE HARBOR-ABKOMMEN DURCH DAS DATEN EXPORTIERENDE UNTERNEHMEN [DECISION OF THE BOARD OF

밖으로의 데이터 유출을 멈출 것을 촉구하였고, 일부는 독일 내부에서의 데이터 유통만 허용하자는 의견도 제안되었다. 2013년 10월 도이치 텔레콤(Deutsche Telekom, 지분의 1/3 국가 소유)은 독일인 간의 데이터 유통은 독일 네트워크안에서만 이루어지도록 하자고 제안한 바 있다.[62] 이미 그 이전인 8월 초에 도이체 텔레콤(Deutsche Telekom)은 국내 서버를 통해 서만 데이터를 독점적으로 전송하려는 "독일 전자 메일(E-mail made in Germany)"을 출시한 바 있었다.[63] 2014년 2월, 독일 메르켈 총리는 보안상의 이유로 유럽 내에서 데이터를 보관하도록 설계된 자체 유럽 인터넷 인프라를 구축 할 것을 제안하기도 하였다.[64] 그러나 이러한 제안에 대하여는 네트워크 구축 및 운영비용 문제와 함께 과연 외국의 감시로부터 데이터를 보호할 수 있을지에 대하여 의문의 제기하면서 단시 국내 지역 사업자의 수익만 증대시켜줄 뿐이라는 비판도 제기된다.[65]

3) 스칸디나비안 국가들

스칸디나비안 데이터 보호를 담당하는 국가기관은 외국 클라우드 컴퓨팅 서비스의 이용에 대한 우려를 표명하여 왔다. 그러나 법원을 통해 이러한 당국의 우려가 검증된 바는 없다. 2011년 덴마크 데이터 보호국(Danish Data Protection Agency)은 보안 우려를 이유로 Odense가 "건강, 심각한 사회 문제 및 기타 사적인 문제와 관련된 데이터"를 Google Apps으로의 이전허가요구를 거부하였다.[66] 2012년 노르웨이 데이터 보호국(Norwegian data authority)은 해당 시는 서버가 유럽 연합(EU)내에 위치하지 않는 한 클라우드 컴퓨팅 서비스를 사용할 수 없다고 하였으나 얼마 후에 Google Apps 사용 금지를 해제하였다.[67]

SUPERVISORY AUTHORITIES FOR PROTECTION IN NON-PUBLIC AREAS ON 28/29TH APRIL 2010 IN HANNOVER, CONSIDERATION OF SELF-CERTIFICATION OF DATA IMPORTER TO THE SAFE HARBOR AGREEMENT BY THE DATA EXPORTING COMPANY] (Apr. 28, 2010).

62) Telecoms Plan Shielded European Internet, DEUTSCHE WELLE (Nov. 10, 2013), http://www.dw.de/telecoms-plan-shielded-european-internet/a-17217304.

63) Will It Work? German Email Companies Adopt New Encryption to Foil NSA, RT.COM (Aug. 11, 2013, 10:54), http://rt.com/news/german-email-encryption-nsa-312/. 2017.4.10.확인.

64) Merkel and Hollande Mull Secure European Communication Web, DEUTSCHE WELLE (Feb 16, 2014), http://www.dw.de/merkel-and-hollande-mull-secure-european-communication-web/a-17435895.

65) Weighing a Schengen Zone for Europe' Internet Data, DEUTSCHE WELLE (Feb. 20, 2014), http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482. 2017.2.5. 확인.

66) Processing of Sensitive Personal Data in a Cloud Solution, DATATILSYNET (Feb. 3, 2011), http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/.

67) Norwegian Data Inspectorate, Notification of Decision - New E-mail Solution Within Narvik Local Authority (Narvik Commune) - Google Apps, DATATILSYNET (Jan. 16, 2012), http://www.datatilsynet.no/Global/english/2012_narvik_google_eng.pdf (decision to ban service); Use of Cloud Computing Services, DATATILSYNET (Sept. 26, 2012), http://www.datatilsynet.no/English/Publications/cloud-computing/ (reporting on the decision to lift the ban); see also Loek Essers, Norway Ends Nine-Month Ban on Google Apps, COMPUTERWORLD (Sept. 26, 2012, 2:27 PM PT), http://www.computerworld.com/article/2491685/cloudcomputing/norway-ends-nine-month-ban-on-google-apps-use.html.

4) 러시아

2013년 여름 NSA폭로 이후, 러시아 하원 의장은 이메일 또는 소셜네트워크 기업들이 러시아 고객의 데이터를 러시아 영역안의 서버에 보유하도록 하는 입법을 통해 "디지털 주권(digital sovereignty)"을 강화하여야 할 것을 요구하였다.[68] 2014년 7월 21일 러시아인들의 개인정보를 러시아 연방 영토 밖에 저장하는 것을 금지하는 법 개정안이 통과되었다.[69] 더욱이 데이터베이스의 운영자는 데이터센터의 물리적 위치를 공개하여야 한다.[70] 이를 위반하는 온라인 웹사이트는 Roscomnadzor(연방 통신 감독 기관)의 블랙리스트 명단에 기재되며 마약이나 아동포르노 등과 유사하게 취급된다.[71]

이 법에 의하면 인터넷 이용자들 간의 정보 교환이나 유포를 매개/운용하는 개인 또는 법인은 음성, 서면, 이미지, 소리 등 정보의 종류를 불문하고 모든 정보를 러시아 영토에서 6개월 간 저장하여야 한다.[72]

(2) 아시아

1) 중국

중국은 2015년 7월 사이버상에서의 공격과 범죄, 유해정보 확산 위협으로부터 사이버주권과 국가안보를 수호하기 위한 「중화인민공화국 네트워크 안전법」(사이버안전법)을 제정하였으며, 2017년 6월 1일부터 시행될 예정이다. 이는 네트워크 전반을 망라한 규제법으로서 네트워크에 대한 통제를 강화하는 한편, 사이버공격을 방어하고, 중국의 이용자에 관한 정보를 보호하는 정부의 역량을 강화하고자 만들어 졌다. 이 법은 네트워크 보안 지원과 촉진, 네트워크 운영 안전(제1절 일반 규정, 제2절 중요 정보 인프라의 운행 안전), 네트워크 정보 보안, 모니터링 경보와 비상 대응 등으로 구성되어 있는바, 결과적으로 '사이버 만리장성'을 구축하였다는 평가를 받고 있다.

특히 네트워크 중요 설비와 네트워크 보안 전용 제품인 경우, 관련 국가 기준의 필수요구에 따라 자격을 갖춘 기관에서 보안 인증 혹은 보안 테스트 요구에 부합한 후에야 판매

68) Andrew E. Kramer, N.S.A. Leaks Revive Push in Russia to Control Net, N.Y. TIMES, July 15, 2013, at B1, available at http://www.nytimes.com/2013/07/15/business/global/nsa-leaks-stir-plans-in-russia-to-controlnet.html; Maria Makutina, Lawmakers Seek to Bolster Russia' Internet Sovereignty, RUSS. BEYONDHEADLINES (June 21, 2013), http://rbth.ru/politics/2013/06/21/lawmakers_seek_to_bolster_russias_internet_sovereignty_27365.html.

69) 이는 기존 2006년의 제152호 연방법(Federal Law No. 152 "n Personal Data")을 개정한 것으로 제242호 연방법(Federal Law No. 242)이다.

70) Federal Amendments to Certain Legislative Acts of the Russian Federation, art. 2.2.

71) Max Smolaks, Russian Government Will Force Companies to Store Citizen Data Locally, TECHWEEKEUROPE (July 4, 2014, 17:22), http://www.techweekeurope.co.uk/news/russian-government-will-forcecompanies-store-citizen-data-locally-148560.

72) Federal Law of May 5, 2014, art. 1.1; see also Russia' Parliament Prepares New "Anti-Terrorist" Laws for Internet, GLOBAL VOICES (Jan. 16, 2014, 5:51 GMT), http://advocacy.globalvoicesonline.org/2014/01/16/russias-parliament-prepares-new-anti-terrorist-laws-for-internet-censorship-putin/.

혹은 제공이 가능하다. 국가 인터넷 통신 부서는 국무원의 관련 부서와 함께 네트워크 중요 설비와 네트워크 보안 전용 제품 목록을 제정하고 발표하며 보안 인증 및 보안 검사의 결과를 서로 인정하여 중복 인증과 테스트를 피한다(제23조). 또한 네트워크 제품, 서비스는 관련 국가 기준의 필수 요구에 부합하여야 한다. 네트워크 제품, 서비스의 제공자는 악성 프로그램을 설치해서는 안 되고 해당 네트워크 제품, 서비스에 안전 결함, 취약점 등 위험이 있다는 것을 발견하였을 경우 즉시 보완 조치를 취한 후 규정에 따라 즉시 사용자에게 고지하고 또 관련 주관 부서에 보고해야 한다. 네트워크 제품, 서비스 제공자는 네트워크 제품 서비스에 대해 지속적으로 보안 유지 보호를 제공하고 당자사가 약정한 기간 내에 보안 유지 제공을 중지해서는 안 된다. 사용자의 정보를 수집하는 기능을 가지고 있는 네트워크 제품, 서비스는 반드시 사용자에게 명시하고 또 동의를 얻어야 한다. 사용자 개인 정보에 관련되는 경우에는 본 법과 관련 법률, 행정 법규에서 개인 정보 보호에 관한 규정을 지켜야 한다(제22조).

중요 정보 인프라의 운영 보안에 관하여도 ① 중요 정보 인프라에 대한 네트워크 보안 등급 보호 제도와 중점적인 보호의 실행 ② 중요 정보 인프라의 운영 보안 보호 업무를 지도 및 감독 ③ 중요 정보 인프라의 구축의 업무 안정성 및 지속적 운영성능 구비 ④ 중요 정보 인프라의 운영자의 보안 보호 의무 이행 ⑤ 중국 국내에서 운영하면서 수집하고 생성된 개인 정보와 중요 데이터의 중국 국내 저장 의무 ⑥ 중요 정보 인프라의 운영자의 네트워크의 보안성에 대한 검사와 평가 의무 ⑦ 국가 인터넷 부서의 중요 정보 인프라의 보안 보호 조치 의무 등을 규율하고 있다. 국가는 공공 통신과 정보 서비스, 에너지, 교통, 수력, 금융, 공공 서비스, 전자 민원 등 중요한 업계와 분야가 파괴되었거나 기능을 상실하였거나 혹은 데이터가 유출이 되어 국가 안보, 국민 생계, 공공 이익에 심각한 해를 끼치게 될 수 있는 중요 정보 인프라에 대해 네트워크 보안 등급 보호 제도를 바탕으로 중점적인 보호를 실행한다. (제31조).

2) 인도

2011년 4월, 인도 통신 기술부(the Indian Ministry of Communications and Technology)는 「2000년 정보기술법 (Information Technology Act of 2000)」의 특정 조항을 구현하는 개인 정보 보호 규칙을 발표하였다.[73] 이 규칙은 “합리적인 보안관행과 절차 및 민감 개인정보에 관한 규칙”으로 민감 개인정보의 해외 이전을 제한하고 있다. 민감 개인정보의 해외이전은 오직 그 이전이 필수불가결하거나, 정부주체가 해외이전에 동의한 경우에만 해외이전이 가능하다.[74] 여기서 민감 개인정보는 ‘①패스워드, ②은행계좌·신용카드 등 지불수단과

73) 2000년 정보기술법(Information Technology Act 2000, No.21)은 컴퓨터 오용에 초점을 맞추었으나, 데이터 보안과 관련된 부분을 다루지 못하였다. 따라서 2008년 개정법(Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009)은 개인정보의 보호 문제를 다루기 위해 두 개의 조문(43A 및 72A)을 추가하였다.

관련된 금융정보, ③신체적·생리적·정신적 건강 정보, ④성적 취향, ⑤의료기록, ⑥생체정보, ⑦ 서비스 제공과정에서 기업에게 제공된 ① 내지 ⑥과 관련된 모든 세부정보, ⑧ 합법적인 계약 기타 합법적 방법으로 처리, 저장 또는 처리하기 위해 기업이 받은 정보'를 의미한다. 다만 2005년 정보권리법 또는 다른 법률에 의해 공공 누구나 접근가능하거나 자유롭게 이용할 수 있는 정보는 이 규칙에서 민감정보로 보지 않는다.[75] 법인이나 개인은 민감한 개인정보를 인도 내에 위치한 또는 다른 국가에 위치한 법인 또는 개인에게 이전할 수 있다. 다만 이 규칙에서 정하는 데이터 보호 수준을 준수하고 있어야 한다. 또한 합법적 계약의 이행을 위해서 필요한 경우 또는 정보주체가 정보이전에 동의한 경우에만 민감 개인정보의 이전이 허용된다.[76] 사실 개인정보의 국외 이전이 "반드시 필요"하다는 것을 입증하는 것은 어렵기 때문에 정보주체의 동의를 득하지 않는 한 실질적으로 민감 개인정보의 이전은 곤란하다.

그러나 이 규칙은 정보수집자가 정보처리자에게 이전하는 과정에서 '동의'를 어떻게 획득하여야 하는지에 대하여 명확하지 않다. 우선 개인정보를 수집할 때, 서면, 팩스, 이메일 등의방식으로 동의를 받을 것을 요구하고 있다. '서면'의 의미를 어떻게 해석하느냐에 따라 달라지겠지만 전형적인 웹페이지상의 "동의버튼" 조차도 이 규정의 "동의요건"에서 배제될 수 있다.[77] 이러한 동의요건은 미국이나 유럽의 법제보다도 훨씬 더 제한적이다.[78] 유럽의 경우 통상적으로 데이터의 수집과 처리에 대하여 일반적으로 동의를 받도록 되어 있으며, 국외 이전에 대한 특별한 동의를 요구하는 것은 아니다.[79] 다만 데이터 국외이전에 있어서 특별한 동의를 필요로 하는 경우는 데이터가 이전되는 국가의 법률상 데이터의 안전수준이 유럽에 비해 덜 한 경우이다. 이러한 경우 정보주체에게 특별히 인식할 수 있도록 고지하고 동의를 받아야 한다.

2011년 8월 인도의 정보통신기술부(the Ministry of Communications & Information Technology)는 이 규정이 인도인들의 정보를 수집하는 기업에게만 적용되며 그러한 기업들은 인도에 위치하여야 함을 의미한다고 밝힌 바 있다.[80] 이는 외국기업의 인도 투자를

74) Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India.subsection II(3)(i) (Apr. 11, 2011).
75) Id. at Rule 3.
76) Id. at Rule 7.
77) MIRIAM H. WUGMEISTER & CYNTHIA J. RICH, MORRISON & FOERSTER, INDIA'S NEW PRIVACY REGULATIONS 3(2011),available at http://www.mofo.com/files/Uploads/Images/110504-Indias-New-Privacy-Regulations.pdf.
78) Id. at 1.
79) Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281), at 40.
80) Press Note, Press Info. Bureau, Gov' of India, Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Under Section 43A of the Information Technology ACT, 2000, (Aug. 24, 2011), available at

억제시킬 수 있다는 비판도 있다.[81] 데이터 국지화를 유발할 수 있는 또 다른 강력한 법은 「공공기록물법(Public Records Act of 1993)」이다. 이 법 제4조는 공공기록물이 "공익적 목적"인 경우를 제외하고는 인도 영토 밖으로 이전되는 것을 금지하고 있다.[82] 중앙정보의 승인 없이는 어떠한 사람도 공공기록물을 인도 영역 밖으로 이전할 수 없다. 다만 공적 목적을 위한 경우에는 그러한 중앙정부의 사전 승인은 요구되지 않는다.[83] 이 법은 컴퓨터에 의해 생성된 어떠한 것도 "공공기록물"에 해당되며, 2013년 인도 델리 고등법원(the Delhi High Court)은 정부 이메일을 인도 밖으로 이전하는 것을 금지하는 것도 포함한다고 해석하였다. 즉 공식적인 정부이메일은 공공기록물법을 따라야 한다.[84] 인도정부 이메일 정책에 의하면 공무원은 가정에서 또는 해외에 기반 한 이메일을 사용하여서는 안되며 반드시 정부이메일서비스만을 이용해야만 한다.[85] 하물며 일부 주 정부는 모든 정부 웹사이트가 인도영역 안에서만 특히 정부 소유 서버를 통해서만 호스팅 되어야 한다고 하기도 한다.[86]

한편 2014년 2월 국가안보회의(National Security Council, NSC)는 정부 분만 아니라 인도 시민들을 위한 데이터 국지화 정책을 제안한 바 있다. 이러한 정책제안에는 모든 인도의 이메일서비스사업자는 인도 영역 안에 서버를 호스팅하도록 의무화하여야 한다고 담겨있다. 또한 내국서버에 있는 데이터를 해외의 메인서버를 통해 그대로 미러링(mirroring)하는 것을 금지한다.[87]

또한 국가안보보좌관(National Security Advisor)은 통신부(Department of Telecom)에게 모든 통신 및 인터넷 기업들이 '국가 인터넷 교환소(National Internet Exchange of India)'를 통하여 국내 데이터를 라우팅 할 것을 의무화 하도록 요구하였다. 이러한 조치는 국내 인터넷 패킷이 대부분 인도 영역에 남도록 보장하기 위함이다.[88] 그러나 2014년 2월

---

http://pib.nic.in/newsite/erelease.aspx?relid=74990; Deepa Christopher & Praveen Thomas, India - WelcomeClarification on Sensitive Personal Data Rules, LINKLATERS (Sept. 20, 2011), http://www.linklaters.com/Insights/Publication1403Newsletter/TMT-newsletter-September-2011/Pages/India-data-security-laws.aspx.

81) Anupam Chander, DATA NATIONALISM, EMORY LAW JOURNAL [Vol. 64:677] available at: http://ssrn.com/abstract=2577947 at 696.

82) The Public Records Act, No. 69 of 1993, § 4, INDIA CODE (1993).

83) Id.

84) Delhi HC Asks Government to Formulate an Email Policy Within 4-weeks, IBN LIVE (Oct. 30, 2013, 3:06 PM IST); see also Delhi High Court Seeks Clear-cut Answers from Centre on Its Email Policy, ECON. TIMES (Oct. 1, 2014, 07:19 PM IST).

85) STANDING COMMITTEE ON INFORMATION TECHNOLOGY, CYBER CRIME, CYBER SECURITY AND RIGHT TO PRIVACY 21 (2014).

86) Letter from Rajesh Aggarwal, Sec'y of Info. Tech., Directorate of Info. Tech., to all Gov. Depts. in Maharashtra, India 2 (Sept. 30, 2013).

87) Thomas K. Thomas, National Security Council Proposes 3-Pronged Plan to Protect Internet Users, HINDU BUS. LINE (Feb. 13, 2014).

88) Thomas K. Thomas, Route Domestic Net Traffic via India Servers, NSA Tells Operators, HINDU

정보부의 정보기술위원회(The Standing Committee on Information Technology of the Ministry of Information)는 여전히 대부분의 인도내의 웹사이트는 인도 영역 밖에서 호스팅 되고 있음을 지적한 바 있다.[89]

3) 인도네시아

2012년 인도네시아 정부는 공공서비스를 제공하는 서비스사업자로 하여금 데이터센터를 반드시 인도네시아 영토 안에 둘 것을 요구하였다. 즉 인도네시아 국민의 데이터에 대한 국가 주권의 보호와 집행, 그리고 법 집행을 위하여 공공서비스를 위한 정보시스템 운영자는 반드시 데이터센터와 재난대비센터를 인도네시아 영역 안에 두어야 한다.[90] "공공서비스"와 관련된 전자적 시스템의 범위가 모호함에 대한 비판이 존재한다. 번들링 서비스의 특성상 언론이나 정보서비스와 관련된 모든 온라인 어플리케이션과 웹사이트, 소셜플랫폼 등이 모두 포함되는지 등이 불분명하다. 따라서 인도네시아 전자상거래 협회(Indonesian Association of E-commerce, idEA)는 이러한 규정이 공공서비스에 대한 규정과 양립하지 않는다는 비판을 제기하고 있다.[91]

2014 년 1월 7일 통신부(the Ministry of Communication)는 데이터 센터에 대한 기술 가이드라인 초안을 배포하였다. 이 가이드라인은 보다 광범위한 기관을 대상으로 하는 '국내 재해 복구 데이터 센터'를 요구하고 있다.[92] 이러한 기관에는 정보기술에 기반 한 서비스를 제공하는 모든 기관이 포함될 수 있으므로 구글과 야후 뿐만 아니라 항공사, 호텔, 은행 등의 서비스까지 광범위하게 포함될 수 있다.[93]

4) 말레이시아

2010년 말레이시아는 개인정보보호법(Personal Data Protection Act, PDPA)을 제정하였다. 이 법은 말레이시아 국민에 대한 데이터는 국내 서버에 저장되어야 함을 규정하고 있다. 제129조제1항에 의하면 데이터 이용자는 어떠한 개인정보도 말레이시아 영역 밖으로

BUS. LINE (Aug. 14, 2013).

89) STANDING COMMITTEE ON INFORMATION TECHNOLOGY, supra note 87, at 61.

90) Regulation Concerning Electronic System and Transaction Operation, Law No. 82 of 2012, art. 17(2)(Government Gazette of the Republic of Indonesia Year 2012 No. 189) (Indon.), translation available at TECHNICAL COOPERATION PROJECT FOR CAPACITY DEVELOPMENT FOR TRADE-RELATED ADMINISTRATION IN INDONESIA.

91) Enricko Lukman, Is the Indonesian Government Hurting or Helping the E-Commerce Industry?, TECH IN ASIA (May 9, 2013, 5:12 PM).

92) Rancangan Peraturan Menteri(RPM) tentang Pedoman Teknis Pusat Data [Draft Regulation Concerning the Technical Guidelines for Data Centers] (2013) (Indon.); Press Release, Kominfo, Siaran Pers Tentang Uji Publik RPM Data Center [Press Release About Public Test RPM Data Center] (Jan. 7, 2014) (Indon.).

93) Indonesia May Force Web Giants to Build Local Data Centers, ASIA SENTINEL (Jan. 17, 2014); Vanesha Manuturi & Basten Gokkon, Web Giants to Build Data Centers in Indonesia?, JAKARTA GLOBE (Jan. 15, 2014, 9:35 AM).

이전하여서는 안 되나, 다만 관보에 공표된 바에 따라 커미셔너(Commissioner)의 권고에 기반 하여 장관에 의해 특정된 장소의 경우에는 예외를 인정한다.[94] 그밖에 정보주체의 동의가 있는 경우, 정보주체와 정보이용자간 계약의 이행을 위해 필요한 경우, 정보주체의 요청 또는 정보주체의 이익을 위하여 정보이용자와 제3자간의 계약을 체결한 경우 그 계약의 이행을 위해 필요한 경우, 법적 권리를 방어하거나 수행하기 위해 필요한 경우, 데이터 이전이 정보주체에 대한 소송의 대응을 위해 필요한 경우, 법 준수를 위한 합리적인 예방조치 및 모든 예정된 조치를 취한 경우, 정보주체의 치명적 이익을 보호하기 위하여 또는 장관이 정하는 공익을 위하여 데이터 이전이 필요한 경우 등은 예외적으로 허용된다.[95]

5) 카자흐스탄

카자흐스탄은 국내 등록 된 모든 도메인 이름(즉, ".kz" 최상위 도메인에 있는 도메인 이름)은 내국영토에 있는 물리적 서버에서 작동하도록 강제하였다.[96] 정부는 2010년 말에 이러한 규제를 시행하였고, 이러한 규제를 우회하기 위해 Google은 "Google.kz"에서 "Google.com"으로 트래픽을 전환하도록 유도하였다. 이러한 트래픽 전환으로 인해 구글은 카자흐스탄 사용자들에게 적합하지 않은 검색 결과를 도출하게 되었다.[97] 이에 카자흐스탄 IT기업 협회는 국내 서버 요건을 2010년 9월 7일 이후에 새로이 등록된 도메인에만 적용되도록 요구하였고, 이러한 요청이 받아들여져서 Google은 "Google.kz"사이트를 운용할 수 있게 되었다. 다만 2010년 9월 7일 이후에 도메인이 등록된 국내외 기업들은 더 이상 글로벌 클라우드 서비스를 이용할 수 없다.

(3) 북미, 오세아니아

1) 캐나다

캐나다의 「개인정보 보호 및 전자문서법(the Personal Information Protection and Electronic Documents Act, PIPEDA)[98]」은 캐나다 영역 밖으로 개인정보를 이전하는 것을 금지하지는 않았다. 다만 지역 간 이동에 대한 제한을 두고 있다. 이러한 지역 간 정보이전 제한은 미국에 기반을 둔 사업자들에게 지방정부의 정보기술서비스를 아웃소싱하려는 시도에서 비롯된 것이다. 이러한 제한이 스노든 폭로 이전에 이미 공식화되었지만, 미국 애국법(USA PATRIOT Act)에 의해 미국의 감시가 증가하면서 오히려 더 정당화되고 있다.[99]

94) Personal Data Protection Act 2010 § 129 (Act No. 709) (Malay.).
95) Id. art. 129(3).
96) FREEDOM HOUSE, FREEDOM ON THE NET 2013: A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA 441 (Sanja Kelly et al. eds., 2013), available at http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf. at 441(2017.4.10. 확인).
97) Bill Coughran, Changes to the Open Internet in Kazakhstan, GOOGLE OFFICIAL BLOG (June 14, 2011,7:40 PM).
98) Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.).
99) FRED H. CATE, CTR. FOR INFO. POLICY LEADERSHIP, PROVINCIAL CANADIAN

두 개의 캐나다 주 즉 브리티시 컬럼비아 주(British Columbia)와 노바 스코샤 주(Nova Scotia)는 학교, 대학, 병원, 정부 소유 공공시설 및 기관과 같은 공공 기관이 보유한 개인정보는 지극히 예외적인 경우를 제외하고는 캐나다에서만 보관하고 접근 할 것을 요구하는 법률을 제정하였다.[100] 브리티시 컬럼비아 주의 1996년 「정보자유 및 프라이버시 보호법(Freedom of Information and Protection of Privacy Act)」에 의하면, 공공기관은 자신의 관리에 있거나 통제에 있는 개인정보가 캐나다 영역에서만 저장되고 접근가능 하도록 보장하여야 한다.[101] 다만 정보주체가 그러한 정보를 명확히 인식하고 캐나다 영역 밖에서 저장·접근하는 것에 동의한 경우에만 예외가 허용된다.[102] 노바스코샤 주(Nova Scotia) 역시 유사한 개인정보 국지화 규정을 두고 있다.[103] 다만 "공공 기관의 장"이 공공 기관의 운영을 위해 필요하다고 경정한 경우에는 캐나다 영역 밖에서 저장 또는 접근을 허용한다.[104] 외국에서 제공하는 이메일 서비스의 사용에 이러한 브리티시 컬럼비아 주의 규정을 적용한다고 가정해 보면, 어떤 개인이 구글Gmail(미국을 기반으로 하고 있는 서비스라 가정해 볼 때)을 사용한다면 그는 미국에 개인정보를 이전하는 것에 동의해야 할 뿐만 아니라 그가 Gmail 메시지에서 이야기하는 모든 캐나다사람들 또한 미국에 개인정보를 이전하는 것에 동의하여야 한다.

2) 호주

호주는 전자적 형태인 개인건강정보기록(Personally Controlled Electronic Health Records, PCEHR)이 국가 영토 밖으로 이전되는 것을 막고 있다. 즉 전자적 형태로 된 개인건강정보기록은 영토 밖으로 이전되어서는 아니 되며, 영토 밖에서 그러한 정보가 처리되어서도 안 된다.[105] 다만 그러한 개인건강정보기록에 소비자와 관련된 개인정보 또는 개인을 식별할 수 있는 정보가 포함되어 있지 않는 한 영토 밖에서 처리되거나 영토 밖으로 이전되는 것을 허용한다.[106] 호주의 헬스케어서비스 제공업체는 이 법으로 인해 호주인들이 해외

GEOGRAPHIC RESTRICTIONS ON PERSONAL DATA IN THE PUBLIC SECTOR 3 - 4 (2008).

100) Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165, s. 30.1 (Can.), ; Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3, s. 5(1) (Can.).

101) Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, at c. 165, s. 30.1.

102) Id. s. 30.1(a).

103) Personal Information International Disclosure Protection Act, S.N.S. 2006, at c. 3, s. 5(1)(a) - b).

104) Id. s. 5(2).

105) Personally Controlled Electronic Health Records Act 2012 (Cth) Section 77(Austl.).Subsection 1 "The System Operator, a registered repository operator, a registered portal operator or a registered contracted service provider that holds records for the purposes of the PCEHR system (whether or not the records are also held for other purposes) or has access to information relating to such records, must not: (a) hold the records, or take the records, outside Australia; or (b) process or handle the information relating to the records outside Australia; or (c) cause or permit another person: (i) to hold the records, or take the records, outside Australia; or (ii) to process or handle the information relating to the records outside Australia"

106) Id. S77(2).

여행에서 모바일 디바이스를 통해 헬스케어서비스를 제공받기 힘들다고 한다.[107] 소비자는 해외 모바일 장치를 통해 데이터에 액세스하게 되며 사실상 데이터가 액세스되고 잠재적으로 호주 외부에 보관되거나 캐싱 될 수 있기 때문이다. 즉 호주에서 건강관련 정보를 취급하는 외국기업은 데이터센터를 호주 영역 안에 설립하거나 호주 영역 내 있는 기업의 아웃소싱을 통해서만 건강관련 정보를 취급할 수 있다.

2. 국제협정 분석

(1) 다자간 서비스협정(TRADE IN SERVICES AGREEMENT, TISA)[108]

TISA는 EU, US, 파키스탄, 대한민국, 터키 등 24개 국가가 참여한 다자간 협약이다. TISA 협상 당사국은 약 16억 명의 인구를 대표하며, 세계 경제 GDP의 거의 3분의2를 포괄한다.[109] TISA는 GATS를 기반으로 하되, 통신, 운송 및 기술 영역을 포함한 서비스 부문을 더욱 자유화를 추구한다. 전자 상거래에 관한 부속서에는 캐나다, 콜롬비아, 일본, 대만 및 미국의 제안이 포함되어 있으며 그 내용에는 데이터 국지화를 강제하는 규율을 억제하고자 하는 내용이 포함되어 있다. 즉 서비스 제공 업체의 비즈니스와 관련된 활동이 수행되기 위하여 필요한 정보 등(개인정보를 포함하여)의 국경 간 전송을 차단하는 것을 금지하고 있다.[110] 이러한 TISA의 의무규정은 서비스제공자로 하여금 특정 국가에 데이터서버를 설치하도록 강제할 수 없으며 예외적으로 국가 안보, 생계 및 천연 자원 보존의 경우에만 가능하다.[111]

전자 상거래 장에서 설명 된 정보의 자유로운 흐름을 보장할 의무는 여전히 협상의 여지가 있으며 그 범위가 좁혀질 수도 있다. 예를 들어, 한국은 개인정보의 자국 외 이전의 경우 개인 정보의 사용과 관련하여 법에 의거한 완전한 보호 조치를 다 이행한 경우에만 정보주체의 “고지된 동의”에 의해 가능하다.

---

107) CSC, CSC’S SUBMISSION TO THE STANDING COMMITTEE ON COMMUNITY AFFAIRS: INQUIRY INTO THE PROVISIONS OF THE PERSONALLY CONTROLLED ELECTRONIC HEALTH RECORDS BILL 2011 AND A RELATED BILL 7 (2011).

108) 2012년 초 부터 미국과 호주의 주도로 논의되고 있는 TISA 추진은 세계무역기구(WTO)의 도하개발아젠다(DDA) 협상이 지지부지한 데 따른 것이며, 건설, 문화, 유통 등 서비스시장 무역장벽을 없애는 것이 주 목적이므로 ‘서비스 분야의 자유무역협정(FTA)’으로도 불리기도 한다. (한경 경제용어사전, 한국경제신문/한경닷컴).

109) European Commission, Trade in Services Agreement http://ec.europa. eu/trade/policy/in-focus/tisa/.

110) TISA Annex on Electronic Commerce https://wikileaks.org/tisa/ ecommerce/05-2015/page-3.html.

111) On the national security exceptions to the WTO agreements, see Abdel-Latif, Ahmed. How to deal with the security exception in the digital economy, E15 Initiative paper (2015).

(2) 환태평양 경제동반자 협정(TRANS-PACIFIC PARTNERSHIP, TPP)[112]

호주에서 베트남에 이르기까지 태평양 12개 국가가 참여한 협약이며 전 세계 GDP의 39%를 차지한다.[113] 그 협상의 주제는 매우 광범위하며 농업, 관세, 전자상거래 등을 포함하여 국가 간 이슈를 다루고 있다.[114] TPP국가들은 무역거래를 위한 데이터 유통과 관련하여 두 가지 의무를 지닌다. 우선, 국경 간 정보의 유통을 허용하여야 하며, 다름으로 TPP 국가의 기업에게는 해당 지역에 서버를 사용할 것을 강제하는 규제를 부여하여서는 안 된다. 특히 제14.11조에 의하면 가입국은 원칙적으로 국경 간 데이터 유통을 보장하되, 1) 합법적일 공공정책적 목적을 달성하기 위해 필요한 경우 2) 부당한 차별을 구성하지 않는 경우 3) 목표 달성에 필요한 것보다 과도한 수단이 아닌 경우(즉 비례원칙에 어긋나지 않는 경우) 예외를 허용한다. 그러나 이러한 조문은 회원국 정부가 수집하거나 정부 조달에 관련된 정보에는 적용되지 않는다.[115]

결론적으로 프라이버시등과 같은 합법적인 공공정책적 목적을 위해서는 데이터 국지화 또는 자국 인프라 사용 강제 등을 요구할 수 있다. 그러나 소비자 프라이버시 보호가 유지될 수 있는 한 정보의 유통은 허용되어져야 함이 인터넷과 전자거래의 활성화를 위해 도입된 본 협약의 취지에 부합된다.

(3) 범대서양 무역 투자 동반자 협정(THE TRANSATLANTIC TRADE AND INVESTMENT PARTNERSHIP, TTIP)[116]

TTIP는 미국과 유럽을 가로질러 대서양 지역의 자유무역지역을 만들기 위한 노력의 일환으로 논의되었다. 동 협정은 세계 재화 및 서비스 교역의 약 3분의1을 차지한다.[117] TTIP는 TISA 및 TPP와 유사하게 논의가 진행될 것으로 보인다. 다만 EU의 데이터보호법과

112) 원래 TPP는 05년 싱가포르, 뉴질랜드, 칠레, 브루나이 등 환태평양 4개국이 다자간 무역자유화 협정을 체결한 것이 기원이다. 2008년 미국이 환태평양 무역자유화 협정에 참여함으로써 협상이 본격화되었고 2015년 10월 협상이 타결 됐다.(한경 경제용어사전, 한국경제신문/한경닷컴).

113) United States Trade Representative, The Trans-Pacific Partnership: Economic Benefits, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2013/December/TPP-Economic-Benefits.

114) Stoller, Matt. Trans-Pacific Partnership: The biggest trade deal you've never heard of, Oct. 23, 2012.

115) TPP Art. 14.2.

116) 2013년 논의가 시작되었으나, TTIP 체결을 위해서는 EU 이외에 각 회원국 의회의 동의가 필요한데, TTIP가 임금을 떨어뜨리고 환경 규제를 약화시키며 노동권에도 부정적인 영향을 미칠 것이라는 전망에 따라 유럽 각국에서 반대 시위가 일어났다. 또한 투자자국가분쟁해결(ISDS) 조항(공공정책에 다국적기업의 제도적 간섭을 허용하는 제도)을 유럽의회가 반대하고 있어 타결이 어려울 것으로 전망되고 있다. [네이버 지식백과] 범대서양 무역투자동반자협정 [汎大西洋貿易投資同伴者協定, Transatlantic Trade and Investment Partnership] (시사상식사전, 박문각).

117) Office of the United States Trade Representative, Fact Sheet: United States to Negotiate Transatlantic Trade and Investment Partnership with the European Union https://ustr.gov/about-us/policy-offices / press-office/fact-sheets/2013/february/US-EU-TTIP 2017.4.7. 확인.

관련하여 여전히 논쟁의 여지가 있다. 유럽 의회는 TTIP의 정보유통이 EU프라이버시법과 양립 가능할 것을 권고한 바 있다.

3. 소결

데이터 국지화를 위한 조치들은 다양한 방식을 보인다. 국외 데이터 국지화 규범은 국지화의 강도에 따라 세 가지 유형으로 나누어 볼 수 있다. 첫째, 분리된 네트워크를 원칙으로 하는 유형이다. 이러한 경우 언제든 정부에 의한 데이터 통제가 가능하므로 가장 강력한 데이터 국지화 유형이라고 할 수 있다. 둘째, 모든 데이터에 대한 국지화를 원칙으로 하되, 예외적으로 국외이전을 허용하는 경우이다. 세 번째는 개인정보 등 특정 데이터에 대한 국지화를 원칙으로 하는 유형이다.

우선 분리된 네트워크를 원칙으로 하는 경우에는 중국과 이란, 북한과 쿠바 등이 해당된다. 북한과 쿠바가 중국과 이란의 경우와 구별되는 점이 있다면 전자의 경우 인터넷과의 연결을 전적으로 거부하지는 않지만 대다수 주민들은 통제된 인트라넷에 가 둬두려고 하는 반면, 후자는 위의 이유로 인터넷과 격리된 국가 네트워크를 구축하고자 한다.[118] 중국은 1994년에 웹에 연결되었는데 4년 후 황금방패(Golden Shield) 시스템을 도입함으로써 트래픽의 국내유입과 국외유출을 통제하게 되었는바, 이 시스템은 세계에서 가장 정교한 정보장벽으로 발전하였고 이른바 '만리장성'(Great Firewall)으로 불리운다.[119] 이란은 보수적인 마흐무드 아흐마디네자드(Mahmoud Ahmadinejad)가 대통령으로 당선된 후 2005년에 국가 인터넷 네트워크 프로젝트(National Internet Network project)를 시행하였는데 2013년 한층 온건한 하산 로우하니(Hassan Rouhani)가 당선되었는데도 이란은 중국으로부터 전문가들을 불러와 이른바 할랄(Halal), 즉 종교적으로 허용되는 인터넷을 구축하기 위한 계획을 지속적으로 시행해나갈 것을 선언하였다. 북한은 2000년에 폐쇄된 인트라넷을 도입하였는데 이는 이른바 '광명'으로 불리우며 이메일과 소수의 필터링된 웹사이트를 지원할 뿐이었고 이후 2010년에 인터넷에 연결되었으나 트래픽이 여전히 정부 부처를 통해 라우팅되고 있으며 단지 소수의 학문 집단에게만 이용가능하다.[120]

다음으로 모든 데이터에 대한 국지화를 원칙으로 하되, 예외적으로 국외이전을 허용하는 경우이다. 이는 자국 내 데이터 유통을 원칙으로 하되, 지극히 예외적인 경우에 국외유통을 허용하는 방안이다. 대표적으로 러시아는 2014년 7월 21일 법 개정을 통해 러시아

118) Charlotte Alfred, Web At 25: Will Balkanization Kill The Global Internet?, The Huffington Post, http://www.huffingtonpost.com/2014/03/19/web-balkanization-national-internet_n_4964240.html 2017.4.10.확인.

119) Charlotte Alfred, Web At 25: Will Balkanization Kill The Global Internet?, The Huffington Post,http://www.huffingtonpost.com/2014/03/19/web-balkanization-national-internet_n_4964240.html 2017.4.10.확인.

120) 허진성, 데이터 국지화 정책의 세계적 흐름과 법제적 함의, 언론과 법 제13권 제2호, 2014, 298-299면.

인들의 개인정보를 러시아 연방 영토 밖에 저장하는 것을 금지하는 법을 통과시켰으며,[121] 더욱이 데이터베이스의 운영자는 데이터센터의 물리적 위치를 공개하여야 한다.[122] 2013년 독일 도이치 텔레콤이 독일인 간의 데이터 유통은 독일 네트워크안에서만 이루어지도록 하자고 제안한 사례라든지,[123] 2014년 독일 메르켈총리가 유럽 내에서만 데이터를 보관하도록 설계된 자체 유럽 인터넷 인프라를 구축 할 것을 제안한 것.[124] 등이 이러한 경우에 해당될 수 있다. 인도의 경우에도 2014년 2월 인도의 국가안보회의(National Security Council, NSC)는 모든 인도의 이메일서비스사업자가 인도 영역 안에 서버를 호스팅하도록 의무화하도록 하는 정책을 제안한 바 있으며 이는 내국서버에 있는 데이터를 해외의 메인 서버를 통해 그대로 미러링(mirroring)하는 것을 금지하는 내용을 포함한다.[125] 더불어 이러한 정책제안에는 국내 인터넷 패킷이 대부분 인도 영역에 남도록 보장하기 위해 모든 통신 및 인터넷 기업들이 '국가 인터넷 교환소(National Internet Exchange of India)'를 통하여 국내 데이터를 라우팅 할 것을 의무화 하도록 요구하는 내용도 포함하고 있다.[126]

세 번째 유형인 개인정보 등 특정 데이터에 대한 국지화를 원칙으로 하는 경우는 국민의 사적인 생활과 밀접하게 관련된 건강정보, 개인정보 또는 국가기관이 보유하고 있는 정보 등 특정 정보의 국외 이전을 엄격히 제한하는 경우이다. 대부분의 서구유럽과 북미 국가들이 채택하고 있다. 인도의 경우 민감 개인정보의 해외이전은 오직 그 이전이 필수불가결하거나, 정부주체가 해외이전에 동의한 경우에만 해외 이전이 가능하다.[127] 뿐만 아니라 인도는 「공공기록물법(Public Records Act of 1993)」을 통해 공공기록물이 "공익적 목적"인 경우를 제외하고는 인도 영토 밖으로 이전되는 것을 금지하고 있다.[128] 인도네시아의 경우에도 공공서비스를 제공하는 서비스사업자는 데이터센터를 반드시 인도네시아 영토

121) 이는 기존 2006년의 제152호 연방법(Federal Law No. 152 "n Personal Data")을 개정한 것으로 제242호 연방법(Federal Law No. 242)이다.

122) Federal Amendments to Certain Legislative Acts of the Russian Federation, art. 2.2.

123) Telecoms Plan Shielded European Internet, DEUTSCHE WELLE (Nov. 10, 2013), http://www.dw.de/telecoms-plan-shielded-european-internet/a-17217304.

124) Merkel and Hollande Mull Secure European Communication Web, DEUTSCHE WELLE (Feb 16, 2014), http://www.dw.de/merkel-and-hollande-mull-secure-european-communication-web/a-17435895. 2017.4.10.확인.

125) Thomas K. Thomas, National Security Council Proposes 3-Pronged Plan to Protect Internet Users, HINDU BUS. LINE (Feb. 13, 2014), http://www.thehindubusinessline.com/features/smartbuy/national-securitycouncil-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece (internal quotation marks omitted.2017.4.10.확인.)

126) Thomas K. Thomas, Route Domestic Net Traffic via India Servers, NSA Tells Operators, HINDU BUS. LINE (Aug. 14, 2013), http://www.thehindubusinessline.com/industry-and-economy/info-tech/route-domestic-net-traffic-via-india-servers-nsa-tells-operators/article5022791.ece 2017.4.10.확인.

127) Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India.subsection II(3)(i) (Apr. 11, 2011).

128) The Public Records Act, No. 69 of 1993, § 4, INDIA CODE (1993), available at http://nationalarchives.nic.in/writereaddata/html_en_files/html/public_records93.html. 2017.4.10.확인.

안에 두도록 규율하고 있다. 다만 “공공서비스”와 관련된 전자적 시스템의 범위가 모호하므로 공공서비스와 관련된 데이터가 실제로 자국민의 모든 데이터로 확대될 우려가 있다. 말레이시아는 내국민의 개인정보는 법에서 규정된 예외적인 사유가 아닌 한 국내 서버에 저장되어야 함을 원칙으로 규정하고 있다.[129] 캐나다의 경우에도 공공 기관이 보유한 개인정보는 지극히 예외적인 경우를 제외하고는 캐나다에서만 보관하고 접근 할 것을 요구하는 규율체계를 가지고 있다. 호주의 경우에도 전자적 형태인 개인건강정보기록이 국가 영토 밖으로 이전되는 것을 막고 있다. 즉 전자적 형태로 된 개인건강정보기록은 영토 밖으로 이전되어서는 아니 되며, 영토 밖에서 그러한 정보가 처리되어서도 안 된다. 그밖에 2011년 덴마크 데이터 보호국(Danish Data Protection Agency)은 “건강, 심각한 사회 문제 및 기타 사적인 문제와 관련된 데이터”를 Google Apps로 이전하는 것에 대하여 보안 우려를 이유로 거부한 바 있다.

그밖에 TISA, TPP 등 다자간 협정의 경우 명확히 데이터 이전과 관련된 특정 협의안을 담고 있기 보다는 비즈니스, 무역거래 등을 과정에서 이루어지는 정보유통을 억제하지 말자는 취지를 반영한 것이며, 다양한 해석과 예외의 여지를 남기고 있다.

우리나라의 경우 세 번째 유형에 해당된다고 볼 수 있다. 국민의 사적인 생활과 밀접하게 관련된 건강정보, 개인정보 또는 국가기관이 보유하고 있는 정보 등 특정 정보의 국외이전을 제한하는 경우이다. 「개인정보 보호법」은 개인정보의 국외이전 전반을 금지하거나 규제하고 있지는 않다. 다만 개인정보처리자가 개인정보를 국외의 제3자에게 “제공”할 때에는 정보주체에게 그 사실을 알리고 동의를 받아야 한다. 제3자 제공에 대해서만 동의를 받으면 되므로 해외 수집, 위탁, 보관 등의 경우에는 동의를 받을 필요가 없다. 그러나 정보통신서비스 제공자등이 이용자의 개인정보를 국외에 제공(조회 포함)·처리위탁·보관하려면 이용자의 동의를 받아야 한다. 「개인정보 보호법」의 경우와 달리, 「정보통신망 이용촉진 및 정보보호등에 관한 법률」(이하 “정보통신망법”이라 한다)은 국외 제3자 제공의 경우뿐만 아니라 국외 처리위탁, 보관 등의 경우도 동의를 받도록 규정하고 있다(제63조 제2항). 다만 중국, 유럽 등의 강한 데이터 국지화 움직임에 대하여 국내에서도 이에 대응하는 입법적 방안 마련이 필요하다는 논의가 진행 중이다.

Ⅳ. 데이터 국지화 규범쟁점과 과제

1. 국가안보

데이터 국지화 정책은 스노든 사태[130]에 대한 반응으로 미국과 같은 외국의 정보기관의

129) Personal Data Protection Act 2010 § 129 (Act No. 709) (Malay.), available at http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf. 2017.4.10.확인.

감시로부터 자유와 안전을 확보하려는 시도의 일환으로 본격화 되었다. 즉 외국의 감시에 대한 우려, 데이터 보안 등의 관점에서 그 타당성이 인정된다. 그러나 일정국가 내에서 데이터를 저장해야 하는 의무로 인해 해당 데이터가 데이터를 해킹하려는 범죄자들에게는 오히려 손쉬운 대상이 될 수 있다는 점 때문에 데이터에 대한 위험을 초래할 수 있다.[131] 기술적으로 데이터 국지화 정책이 외국의 감시활동을 방지할 수 있는가에 대하여는, 치열한 경쟁에 노출되어 있는 글로벌 기업의 보안서비스에 미치지 못하는 수준의 국내 보안서비스로 보호함으로써 결과적으로 데이터를 한데 모아놓고 취약한 보안장치로 이를 보호하려고 시도하다가 더 큰 위험에 빠뜨리게 될 우려가 있다는 견해도 있다.[132] 또한 악성소프트웨어(malware)의 사용은 데이터를 국지화로 막을 수 있는 성질의 문제가 아니다. 네덜란드 신문인 NRC Handelsblad는 NSA가 악성 소프트웨어 네트워크를 통해 세계 곳곳에 침투했다고 전한 바 있다.[133] 최근 미국에서 발생한 수백만 명의 고객이 엄청난 보안 침해를 겪은 것은 아마도 매장의 POS장치에 악성 코드가 설치되어 미국인의 신용 카드 데이터가 러시아의 서버로 전송 된 것이라고 추정된다.[134] 따라서 인터넷이라는 기술적 속성상 지속적으로 모니터링 되고 보안조치 되는 방화벽 안에 정보를 유지하는 것이 국경너머의 누군가가 접근할 수 없다는 것을 의미하지 않는다.

한편 데이터 국지화의 타당성 중의 하나가 외국의 감시체계로부터 벗어나려는 것이라면, 사실 데이터 국지화는 외국의 감시를 더 용이하게 할 수 있다는 견해도 제기된다. 기업이 글로벌 서비스가 아닌 로컬 서비스를 사용하도록 강제함으로써 보안 조치가 약한 회사를 선택할 확률이 높아지게 된다. 본질적으로 글로벌 서비스는 전 세계적으로 치열한 경쟁을 겪고 있으나, 지역서비스는 이러한 글로벌 규모의 기업에 비할 때 특히 데이터 국지화요건에 의해 보호될 경우 고객을 유인하기 위해 더 강력한 보안을 제공할 필요가 없게 된다. 이렇듯 보안 수준이 낮게 되면 결국 외부의 공격에 취약해 질 수 밖에 없다.[135]

또한 특정 지역에 거주하는 이용자들의 정보를 그 지역에 중앙집중화 한다면 특정 국가 국민들의 감시를 더 용이하게 집중할 수 있도록 해주므로 외국의 첩보부담을 줄여주는 결과를 초래할 수도 있다고 한다(이를 "Jackpot" 문제라 한다).[136]

---

130) 미국 중앙정보국(Central Intelligence Agency, CIA)과 국가안보국(National Security Agency, NSA)에서 근무했던 에드워드 스노든(Edward Snowden)이 국가안보국의 개인정보 수집과 감시활동에 대한 폭로를 한 후 국제사회에서는 이에 대해 상당한 반향이 일었다.

131) Bert Verschelde, The Impact of Data Localisation on Korea's Economy, http://www.ecipe.org/media/publication_pdfs/ECIPE_bulletin1014_dataloc_korea.pdf, 2017.4.10.확인.

132) Chander & Le, supra note 52 at 30.

133) Floor Boon, Steven Derix & Huib Modderkolk, NSA Infected 50,000 Computer Networks with Malicious Software, NRC.NL (NETH.) (Nov. 23, 2013, 02:40).

134) Brian Krebs, Hacker Ring Stole 160 Million Credit Cards, KREBS ON SECURITY (July 13, 2013, 3:39 PM ET), http://krebsonsecurity.com/2013/07/hacker-ring-stole-160-million-credit-cards/.

135) Anupam Chander & Uyên P. Lê, supra note 7 at 716-717.

136) Id at 717.

2. 프라이버시/개인정보

해외 대부분 입법의 데이터 국지화 사유가 프라이버시와 정보보안이다. 특히 개인의 프라이버시를 명목으로 개인정보가 국경 밖으로 이전되는 것을 막고 있다. 이러한 법률들은 명백히 데이터 국지화 자체를 위해 고안된 것은 아니지만, 데이터 유통에 중요한 장벽을 만듦으로서 데이터 국지화 수단으로 작동하고 있다. 그러나 이러한 프라이버시나 정보보안을 위한 데이터 이전의 제한이 오히려 프라이버시나 정보보안을 약화시킨다는 견해가 있다.[137] 데이터 국지화 서버는 여러 지역에 있는 여러 서버에 데이터를 분산시킬 기회를 감소시킨다. 이러한 경우 위에서 검토한 바와 같이 한곳에 모여진 데이터는 "Jackpot"을 유발시키며 범죄의 이상적인 대상이 될 수 있다. 일부 컴퓨터 전문가들에 의하면 데이터국지화는 클라우드서비스제공자가 인터넷의 분산된 인프라를 활용함으로서 세계적 규모로 샤딩(sharding)과 난독화(obfuscation)를 활용하는 것을 막는다고 한다.[138] 샤딩(sharding)은 전 세계의 서버에서 데이터베이스 테이블의 행을 개별적으로 보관하는 프로세스로, 데이터를 작동하기에 충분한 각각의 파티션을 만들지만, 개개인을 재식별하기에 충분하지는 않다.[139] 오히려 개인정보/보안을 위한 가장 정확한 해결책은 모든 데이터가 한 장소에 집중되어 저장되지 않도록, 탈-중앙집중화 시키며 종단 간 암호화된 서비스의 생성과 사용을 장려하는 것이다.[140] 한편 스토리지와 정보처리서비스를 제공하는 지역서비스사업자는 보안에 국제적 서비스제공업자보다 취약할 수밖에 없다. 국제적 서비스제공자는 끊임없이 증가하는 사이버 공격의 정교함에 대응하기 위하여 보안능력을 향상시키기 때문이다. 클라우드컴퓨팅 환경에서 데이터에 대한 가장 일반적인 위협은 부적절한 시스템 보호에 의한 해커의 위법행위, 사용자 부주의, 엔지니어링 오류 등을 모두 포함한다. 유럽, 일본, 미국 등의 정보기술협회는 보안은 상품이 어떻게 만들어지고, 사용되며, 관리되는가와 관련된 기능의 문제이지, 누가 또는 어디서 그러한 상품이 만들어지는가에 대한 장소의 문제가 아니라고 한다.[141] 비슷한 맥락에서 호주가 개인건강기록을 국내에 보유할 것을 규율하는 법을

137) Daniel Castro, The False Promise of Data Nationalism, INFO. TECH. & INNOVATION FOUND. 1 (Dec.2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf 2017, 4,10 확인.

138) Patrick S. Ryan, Sarah Falvey & Ronak Merchant, When the Cloud Goes Local: The Global Problem with Data Localization, COMPUTER, Dec. 2013, at 54, 56.

139) David Geer, Big Data Security, Privacy Concerns Remain Unanswered, COMPUTERWORLD (Dec. 5, 2013, 22:43), http://news.idg.no/cw/art.cfm?id=B1920F48-0FD6-A5E7-5685FC364B81ECBB. 2017.4.10. 확인.

140) Rohin Dharmakumar, India' Internet Privacy Woes, FORBES INDIA (Aug. 26, 2013), http://forbesindia.com/article/checkin/indias-internet-privacywoes/35971/1#ixzz2r0zriZTF. 2017.4.10. 확인.

141) Statement, Digital Eur., U.S. Info. Tech. Indus. Council (ITI) & Japan Elecs. & Info. Tech. Indus. Assoc. (JEITA), Global Information and Communications Technology (ICT) Industry Statement: Recommended Government Approaches to Cybersecurity (June 2012), available at http://www.jeita.or.jp/english/topics/2012/0622/release_2012_en.pdf. This idea is echoed in submissions from a range of IT consortia.

추진할 당시 MS는 결국 그러한 규율이 개인건강기록에 대한 보안을 약화시킬 것이라고 주장한 바 있다.

특히 소비자의 선택권 보장 차원에서 데이터국지화에 대한 의문을 제기하기도 한다. 소비자는 그들의 개인건강데이터를 통제할 수 있어야 하며, 이는 소비자가 그들의 수요에 부합하는 서비스를 제공받을 수 있다고 믿는 기업이라면 그러한 기업이 호주의 영토내에 있는지 여부와 관계없이 그러한 기업에 의한 본인의 건강데이터 보유여부를 선택할 수 있어야 한다.[142] 그러나 소비자의 올바른 선택권을 보장하기 위해서는 보안수준에 대한 정확한 정보를 제공받고 소비자가 그 준수여부에 대하여 이의제기 할 수 있어야 한다. 그러나 정보보안의 성격상 기업의 보안에 대한 정보가 제대로 소비자에게 제공, 인식되기 곤란하며 자국의 감독과 법 집행력이 미치지 못하는 한 소비자의 알권리 실현도 요원하므로 소비자 보호 차원에서 데이터 국지화를 반대하는 견해는 한계가 있다.

또한 데이터국지화에 대하여 회의를 제기하는 견해는 데이터국지화를 추진하는 국가들은 종종 그 국가 자체가 사이버범죄의 온상지이기도 하므로 오히려 개인정보나 프라이버시보호에 취약하다고 한다. 인도네시아는 해커의 천국이라고 일컬어질 만큼 사이버범죄에 취약하다.[143] 브라질 역시 악성소프트웨어와 피싱의 주요 목표가 되는 국가이며,[144] 때대로 사이버범죄는 외부로부터의 공격이 아니라 자국 내에서 자행되는 경우도 많다. 즉 데이터 보안과 데이터를 어디에 보관하여야 하는가가 밀접한 관련을 가진다고 확언할 수는 없다는 것이다. 브리티시 컬럼비아 주민들의 개인 정보가 뱅쿠버에서 몇 마일 떨어진 IBM이 아니라 뱅쿠버의 정부 컴퓨터에 저장되어 있기 때문에 더 안전하다고 믿을만한 정당한 이유가 없다.[145]

3. 경제적 영향

많은 정부는 데이터 국지화를 추진함으로서 국내 기업에 대한 투자를 증가시킬 수 있다고 생각할 수 있다. 즉 데이터국지화 조치는 종종 자국 지역경제 활성화를 위한 동기유발이 될 수 있다. 그러나 이에 대하여는 오히려 데이터국지화는 지역 비즈니스의 비용을 높이고 소비자를 위한 글로벌 서비스 접근을 감소시키며 현지 창업을 방해하고 최신 기술 발전에 저해된다고 한다.[146]

---

142) Richard Chirgwin, Microsoft to Aussie Gov: Privacy Rules Stifle e-Health, REGISTER (Nov. 25, 2011, 00:01), http://www.theregister.co.uk/2011/11/25/ms_threatens_au_gov_over_ehealth/. (2017.2.9. 확인).

143) Jonathan Vit, Hacker' Paradise or Host Nation? Indonesian Officials Weigh Cyber Threat, JAKARTAGLOBE (Oct. 25, 2013, 6:34 PM).

144) Ricardo Geromel, Hackers Stole $1 Billion in Brazil, The Worst Prepared Nation to Adopt Cloud Technology, FORBES (Mar. 2, 2012, 8:45 AM).

145) Anupam Chander & Uyên P. Lê, supra note 7 at 721.

유럽의 일부 국가에서는 해외 데이터 이전에 대한 우려를 제기하였음에도 불구하고 EU 집행위원회는 대서양 경제에 있어서 데이터흐름이 매우 중요함을 깊이 인식하고 있음을 밝힌바 있다.[147] 위원회는 국제 데이터 이전이 소셜 미디어 또는 클라우드 컴퓨팅과 같이 새로운 성장하는 디지털 비즈니스를 포함하여 대서양을 가로 질러 상거래의 필수적인 부분을 형성하고 있다는 점을 인식하고 있다. 경제협력기구(OECD)역시 글로벌 정보공유와 경제발전에 있어서 데이터 흐름을 제약함으로서 나타날 수 있는 역효과에 대하여 우려를 표명한 바 있다. OECD는 각 국가들은 다른 기본권과 양립되는 한 비용 및 기타 효율성을 보장하기 위해서는 국경 간 데이터 설비의 접근, 위치 등에 대한 장벽을 없애도록 노력하여야 할 것이라고 밝힌바 있다.[148]

국가경제에 있어서 인터넷의 가치는 매우 중요하다. 그러나 데이터의 흐름이 없이 이러한 경제적 가치가 구현되기 곤란하다. 스웨덴 정부 기관인 National Board of Trade는 최근 각 부문에서 다양한 규모의 현지 기업 15곳을 인터뷰한 결과 "한 곳에서 다른 곳으로 데이터가 이동하지 않으면 무역이 일어날 수 없다"는 결론을 도출한 바 있다.[149]

데이터국지화는 보호주의적 조치로서 단지 몇 개의 지역기업에는 이익이 될 수 있으나 전체적인 경제에는 부정적 영향을 미치게 된다는 견해가 제기된다. 즉 데이터 국지화가 가져다주는 국내 이점은 소수의 데이터 센터 소유자와 직원 및 이 센터에 서비스를 제공하는 소수의 기업에 국한되며 중소기업 및 대기업은 생산성을 향상시킬 수 있는 글로벌 서비스에 대한 접근이 거부되므로 그 부정적 영향이 매우 크다고 한다. 최근 통과 된 러시아의 데이터 국지화 추진 법에 대하여, NGO로 활동 중인 러시아 전자 통신 협회(Association for Electronic Communications)는 글로벌 서비스 철수를 지적하면서 잠재적으로 부정적 경제적 결과를 강조한 바 있다.[150] 예를 들어, 국제 소셜 미디어 플랫폼의 철수뿐만 아니라, 데이터 국지화로 인해 러시아는 온라인 서비스를 통해 항공권이나 소비재를 주문할 수 없게 된다. 특히 에로플로트(Arioflot)와 같은 러시아 항공회사들은 외국 발권 예약 시스템에 의존하므로 그러한 영향은 더욱 크다고 한다.[151]

---

146) Id at 721.

147) Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, at 3, COM(2013) 847 final (Nov. 27, 2013).

148) ORG. FOR ECO. CO-OPERATION & DEV., OECD COUNCIL RECOMMENDATION ON PRINCIPLES FOR INTERNET POLICY-MAKING 7 (2011), http://www.oecd.org/sti/ieconomy/49258588.pdf. 2017.4.10. 확인.

149) KOMMERSKOLLEGIUM [SWED. NAT'L BD. OF TRADE], NO TRANSFER, NO TRADE: THE IMPORTANCE OF CROSS-BORDER DATA TRANSFER FOR COMPANIES BASED IN SWEDEN 23 (2014), available at http://www.kommers.se/Documents/dokumentarkiv/publikationer/2014/No_Transfer_No_Trade_webb.pdf. 2017.4.10. 확인.

150) The Russian Association for Electronic Communications stated, "assing similar laws on the localization of personal data in other countries has led to withdrawal of global services and substantial economic losses." New Russian Law Bans Citizens'Personal Data Being Held on Foreign Servers, RT (July 5, 2014, 10:50).

또한 데이터국지화는 기업가가 해외 기반의 최정상 글로벌 서비스를 기반으로 구축할 능력을 갖지 못하게 함으로서 국내 혁신에 영향을 미친다고 한다. 브라질의 정보 기술 커뮤니케이션 연합(Brasscom, the Brazilian Association of Information Technology and Communication Companies)은 데이터 국지화 의무는 “인터넷의 적절한 사용으로 인해 일자리를 창출하고 혁신하며 세금을 징수 할 국가의 능력에 손상을 끼치게 될 것”이라고 주장한 바 있다.[152]

그밖에 데이터 국지화는 ‘비용’ 효율화 측면에서 부정적인 영향을 미치게 된다고 한다. 정부는 데이터 국지화로 인해 자국에서 사용되는 다양한 글로벌 서비스가 자국 내에 인프라를 구축하게 될 것이라고 기대할 수 있다. 그러나 특정 지역에 로컬서버를 구축하는 것이 비경제적이며 더 위험한 경우가 많다고 한다.[153] 데이터 센터는 최고 수준의 보안을 유지하는 경우 비용이 많이 든다. 브라질은 서반구에서 데이터센터를 구축하는데 가장 비싼 국가라는 연구도 있다. 브라질에 데이터 센터를 짓는 데는 평균 6천 9백 억 달러가 들지만, 칠레와 미국에서는 1천 2백 5십만 달러와 4천 3백만 달러의 비용이 든다.[154] 데이터 센터 운영 역시 막대한 에너지와 기타 비용으로 인해 많은 지출이 소요되는데, 평균적으로 매월 브라질에서는 95만 달러, 칠레에서는 71만 달러, 미국에서는 51만 달러이다. 이러한 비용의 불일치는 주로 전기 요금, 데이터 센터에 구축에 필요한 장비를 수입하는데 부여되는 세금 등의 차이로 인한 것이다.[155] 한편 운영비용의 4분의 3이 에너지 비용이므로 인건비 비중이 높지 않으며 결국 데이터 센터의 고용효과는 미비하다.[156] 2013년 데이터 센터 위험도 지수에 따르면, 호주, 러시아, 중국, 인도네시아, 인도 및 브라질은 데이터 센터를 운영하는 데 있어 가장 위험한 국가에 해당된다.[157]

데이터 국지화에 따른 경제적 비용뿐만 아니라 그 잠재적 이익 역시 정부가 예측한 것

151) Upper House Obligates Internet Companies to Retain Information on Russians Only in Russia, SPUTNIK NEWS (July 9, 2014, 16:58).

152) Angelica Mari, New Data Storage Demands May Put Companies Off Brazil, ZDNET(Nov. 4, 2013, 17:18PST), http://www.zdnet.com/new-data-storage-demands-may-put-companies-off-brazil-7000022790/ 2017.4.10.확인.

153) Anupam Chander & Uyên P. Lê, supra note 7 at 723.

154) Loretta Chao & Paulo Trevisani, Brazil Legislators Bear Down on Internet Bill, WALL ST. J. (Nov. 13, 2013, 6:45 PM ET), http://online.wsj.com/news/articles/SB10001424052702304868404579194290325348688(according to a government-commissioned study seen by The Wall Street Journal).

155) FROST & SULLIVAN, DOING BUSINESS IN BRAZIL: HOW TO REDUCE YOUR RISKS THROUGH IT INFRASTRUCTURE OUTSOURCING 7 (2012), available at http://www.alog.com.br/wp-content/uploads/2012/12/Brazilian_IT_Infrastructure.pdf at 10

156) RACHEL A. DINES, FORRESTER RESEARCH, INC., BUILD OR BUY? THE ECONOMICS OF DATA CENTER FACILITIES (2011), available at https://www.forrester.com/Build+Or+Buy+The+Economics+Of+Data+Center+Facilities/-/E-WEB7855. 2017.4.10.확인.

157) CUSHMAN & WAKEFIELD, DATA CENTRE RISK INDEX (2013), http://www.cushmanwakefield.com/~/media/global-reports/data-centre-risk-index-2013.pdf. at7. 본 연구는 30개 국가를 대상으로 성공적인 데이터 센터 운영에 영향을 미치는 위험요인에 대한 분석을 기반으로 하고 있다.

보다는 훨씬 제한적이라고 한다. 데이터서버는 고용창출에 기여하는 바가 그다지 크지 않다. 수천대의 컴퓨터에 의해 밀집되어 있으나 이를 운영하기 위한 인력은 소수에 불과하다. 데이터 서버 구축의 초기 비용은 대부분 자본재이며, 그 대부분은 서버가 구축되는 국가로 수입된다. 디젤 발전기, 냉각 시스템, 서버 및 전원 공급 장치는 글로벌 공급 업체로부터 수입된다.[158] 따라서 모순되게도 데이터 국지화 규율의 수혜자는 오히려 서버와 장비를 공급하는 외국의 글로벌 업체인 경우가 많다.[159] 브라질의 경우에도 오히려 수입산이 서버장비시장을 지배하고 있기 때문에 내국의 장비업체는 이러한 데이터국지화 규정으로부터 혜택을 받지 못한다고 한다.[160] 외국으로부터 자본구매를 늘리면서 데이터 국지화 규정은 사실상 상품무역적자를 증가시킬 수 있다. 게다가 거대한 데이터팜은 엄청난 에너지의 소비자이므로 종종 에너지 그리드에 엄청난 부담을 준다. 따라서 더 높은 가격을 지출하면서 에너지를 위해 경쟁하여야 하는 다른 산업에 피해만 입히고 이는 잠재적으로 이미 부족한 전력 공급에 한계로 작동할 수 있다.[161]

또한 이러한 비용상의 문제는 많은 인터넷 기업들로 하여금 외국의 데이터센터를 이용하게 한다. 인도네시아 전자 상거래 협회(Indonesian E-Commerce Association, IdEA)의 다니엘 투미와(Daniel Tumiwa) 소장은 “인도네시아에서 비용이 두 배로 늘어날 수 있다”고 주장한 바 있다.[162] 이로 인해 인도네시아의 인터넷 창업 기업들은 그들의 서비스를 호스트하기 위해 종종 호주, 싱가포르 또는 미국과 같은 외국으로 방향을 돌리고 있다. 한 보고서는 “스타트업 온라인 미디어가 서비스하기 위해 의존하고 있는 상당부분의 도구들이 아직 인도네시아에서는 충분하지 않다”고 언급하고 있다.[163] 또한 인도네시아의 자국 내 약한 호스팅 인프라는 자국 내 호스팅 된 사이트의 로딩 시간을 지연시킴으로서 서비스 불편을 초래한다. 마찬가지로 베트남 정부 역시 기업가 정신과 혁신을 육성하려고 데이터국지화 규제를 실시하였지만[164] 스타트업 기업들이 해외의 값 싸고 강력한 플랫폼을

158) FROST & SULLIVAN, DOING BUSINESS IN BRAZIL: HOW TO REDUCE YOUR RISKS THROUGH IT INFRASTRUCTURE OUTSOURCING 7 (2012), available at http://www.alog.com.br/wp-content/uploads/2012/12/Brazilian_IT_Infrastructure.pdf(emphasis omitted). at 10.

159) Press Release, Gartner, Gartner Says Worldwide Server Shipments Market Grew 1.3 Percent in the Second Quarter of 2014 While Revenue Increased 2.8 Percent (Aug. 27, 2014), available at http://www.gartner.com/newsroom/id/2833020 (noting that US multinational HP, IBM, Dell, Oracle, and Cisco together make up about 76.4 percent of the server market share during the second quarter of 2014).

160) Brazil Data Center Power Supplies Market Size Report by Frost & Sullivan, INFOTECH LEAD (Dec. 12, 2013).

161) Anupam Chander & Uyên P. Lê, supra note 7 at 725.

162) Avi Tejo Bhaskoro, Indonesia Ministry Still Insists on Local Data Centers for Online Companies, DAILYSOCIAL (May 8, 2013, 16:28:27).

163) Ross Settles, Indonesia: A Hotbed of Innovative Online Publishing Start-ups, CLICKZ (Mar. 30, 2011), http://www.clickz.com/clickz/column/2281593/indonesia-a-hotbed-of-innovative-online-publishing-startups. 2017.4.10. 확인.

164) On June 4, 2013, the Ministry of Science and Technology launched the Silicon Valley Project to

이용하는 것을 차단함으로서 잠재적으로 베트남을 기술 경쟁에 참여시키는 데 장애가 될 수 있다고 한다.

그러나 이러한 주장은 이미 서버 등 장비기술이 우세한 국가나, 인프라가 잘 구축되어 있는 국가에는 해당되지 않는다. 또한 중국의 경우 오히려 외산 운용체계나 네트워크 장비에 의존하지 않음으로써 외부 침입에 강력한 방어 기반을 갖추었다고 평가되는 바 있으며, 이러한 기술력을 바탕으로 중국의 바이두·알리바바·텐센트가 미국의 구글·아마존·페이스북 벤치마킹 수준을 뛰어넘어 양자 간 대칭구도를 형성했고, 화웨이(하드웨어)·샤오미(소프트웨어) 등 자수성가형 성공사례도 잇따르고 있다.[165]

한편 대부분의 정부는 자국의 데이터를 해외로 이전하는 것에 대하여는 우려하지만, 역으로 해외의 데이터를 자국 영토 내에 가져오는 것에 대하여는 긍정적이다. 많은 국가들은 기업들의 데이터센터 유치를 원한다. 말레이시아의 경우 2010년에 경제변혁프로그램(Economic Transformation Program)을 발표하면서 아시아태평양 지역을 위한 세계적 규모의 데이터세터 허브를 만들겠다고 발표한 바 있다.[166] 브라질이나 프랑스 역시 이러한 정책의지를 표명한 바 있다.[167] 그러나 데이터 국지화 조치는 이러한 자국 내 데이터센터 유치를 위한 투자로 작동하기 보다는 이러한 규제 회피로 인해 투자의 감소와 국가 집행력의 손상만 초래할 것이라는 예측이 있다. 우선 보복효과가 있을 수 있음을 지적한다. 일례로 Brasscom은 다른 국가들이 데이터국지화를 위해 브라질과 유사한 대응정책을 취하여 데이터센터를 다른 국가로 이전한다면 브라질 인터넷 산업은 큰 타격을 받을 수 있다고 지적한 바 있다.[168] EU의 디지털 어젠다의 유럽 위원장인 Neelie Kroes역시 각국이 별도의 인터넷을 보유하게 될 경우 유럽의 글로벌 경쟁력에 대하여 우려를 제기한 바 있다.[169]

---

stimulate the growth of technology startups in Vietnam. See VIETNAM SILICON VALLEY PROJECT, http://www.siliconvalley.com.vn/ (last visited Feb. 6, 2015).

165) 중국은 미국의 인터넷 기술종속에서 벗어나기 위해 지난 20년간 안간힘을 쏟아 왔다. 그간 중국 정부 인터넷 정책은 외국 하드웨어와 소프트웨어를 국산으로 대체하는 데 초점을 맞추고 있었다. 외산 소프트웨어에의 지나친 의존으로 생기는 위험성은 2008년 마이크로소프트가 윈도 운용체계 무단 사용을 막기 위해 해적 방지 프로그램을 보급하면서 부각됐다. 당시 소프트웨어 80%가 해적판이어서 마이크로소프트의 새 프로그램이 설치되자 컴퓨터 수백만대가 다운되는 큰 혼란이 발생한 적이 있다. 손영동, "[손영동의 사이버세상]<8>기반기술 국산화 주도하는 중국", 전자신문 2015년 9월 1일자칼럼 참조.

166) Overview of ETP, ECON. TRANSFORMATION PROGRAMME, http://etp.pemandu.gov.my/About_ETP-@-Overview_of_ETP.aspx. 2017.4.7.확인.

167) MINISTÈRE DU REDRESSEMENT PRODUCTIF [MINISTRY OF ECON. REGENERATION], THE NEW FACE OF INDUSTRY IN FRANCE (2013), at 1 available at http://www.entreprises.gouv.fr/files/files/directions_services/secteurs-professionnels/industrie/nfi/NFI-anglais.pdf 2017.4.10.확인.

168) Angelica Mari, New Data Storage Demands May Put Companies Off Brazil, ZDNET (Nov. 4, 2013, 17:18 PST), http://www.zdnet.com/new-data-storage-demands-may-put-companies-off-brazil-7000022790/ 2017.4.10.확인.

169) Chiponda Chimbelu, No Welcome for Deutsche Telekom National Internet Plans from EU Commission, DEUTSCHE WELLE (Nov. 11, 2013), http://www.dw.de/no-welcome-for-deutsche-telekomnational-internet-plans-from-eu-commission/a-17219111. 2017.4.10.확인.

또한 국지화 규제는 외국 기업들로 하여금 국지화 조치를 취하고 있는 국가를 피하도록 할 뿐만 아니라 자국기업들도 이러한 규제를 피하기 위해 외국으로 이전함으로서 결국 의도했던 투자효과와는 반대로 기업들로 하여금 나가게 만드는 효과를 초래하게 된다고 한다.[170]

데이터 국지화의 부정적 효과는 인터넷기업과 그 소비자에 국한되는 것이 아니며, 전통산업에까지 미치게 된다고 한다. 맥킨지에 의하면 인터넷과 데이터 흐름에 의해 창출된 부가가치의 75%는 전통산업에 있으며 따라서 부분적으로 전통산업의 생산성 증대에 기여한다고 한다.[171] 의료, 제조, 전기, 도시 기반 구조, 보안, 농업, 소매 등 주요 부문의 잠재적 경제효과는 연간 2.7 내지 6.2 조 달러로 추산된다고 한다.[172] 이는 전통 산업이 여전히 우세한 신흥 경제에서는 특히 중요하다. 인터넷은 또한 수입 증대, 판매비용 및 관리 비용 절감으로 인해 이익을 창출시킨다. 따라서 데이터국지화로 인해 전통적 산업은 외국 영토에서 정보를 저장 또는 처리하는 많은 글로벌서비스에의 접근이 차단되게 된다고 한다.

그밖에 데이터국지화 정책은 IoT, 클라우드컴퓨팅, 빅데이터 등 새로운 인터넷·컴퓨팅 기술을 제약한다. 이는 인프라가 잘 갖추어져 있지 않은 신흥 경제국가의 기업가에게 특히 중요하다.

결국 데이터 국지화 정책이 경제적 효과에 부정적으로 작동할지 그렇지 않을 지는 모든 국가에 일률적으로 동일하게 적용할 수는 없다. 글로벌 경쟁력을 가지고 있는 기업을 보유한 국가와 그렇지 못한 국가, 이미 발달된 인프라와 설비기술을 보유한 국가와 그렇지 않은 국가에 따라 긍정적/부정적 요소로 작용할 수 있는 요인이 각각 다르다. 글로벌 경쟁력을 갖추고 있는 기업을 다수 보유하고 있는 국가의 경우 기술 우위효과에 의해 당연히 데이터 국지화 정책이 부정적 효과를 미칠 수밖에 없다. 기술력을 전혀 보유하지 못한 국가 역시 서비스에의 접근가능성이 배제되는 한 혁신의 기회를 놓치게 될 수 있다. 그러나 자국의 경쟁력이 갖추어지지 않은 상태에서 타국 기업에 의해 기술이나 서비스지배력이 확장될 경우, 자국민의 데이터 지배력 전이로 자국이 소비시장으로만 전락하며 기술경쟁력에서 열세에 빠질 수 있다. 즉 데이터국지화 정책이 경제적 효과에 부정적 혹은 긍정적이라고 단언할 수 없으며, 오히려 경제적 효과와 관련하여서는 정책적으로 적절한 국지화와 적절한 개방화의 묘미가 필요하다.

---

170) Esteban Israel & Alonso Soto, Brazil' Anti-Spying Internet Push Could Backfire, Industry Says, REUTERS, Oct. 2, 2013.

171) MATTHIEU PÉLISSIÉ DU RAUSAS ET AL., MCKINSEY GLOBAL INST., INTERNET MATTERS: THE NET'S SWEEPING IMPACT ON GROWTH, JOBS, AND PROSPERITY 22 (2011), available at http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters. 2017.4.10.확인.

172) JAMES MANYIKA ET AL., MCKINSEY GLOBAL INST., DISRUPTIVE TECHNOLOGIES: ADVANCES THAT WILL TRANSFORM LIFE, BUSINESS, AND THE GLOBAL ECONOMY 55 (2013), available at http://www.mckinsey.com/insights/business_technology/disruptive_technologies. 2017.4.10.확인.

4. 자국법의 집행

정부는 범죄를 예방하고 범죄자에게 응당한 형벌을 부과함으로서 국민을 보호할 의무가 있다. 이러한 법집행요구의 필요성으로 인해 데이터 국지화 필요성이 제기된다. 그러나 이러한 필요성에 대하여는 이미 정보공유협약으로 가능하므로 다분히 과장되었다는 비판이 제기될 수 있다. 예를 들어 미국, 독일, 프랑스 등 40여개 국가가 체결한 사이버범죄협약은 해당국가에게 사이버범죄에 대한 법률을 채택하고 집행하며 서로 "상호원조"를 제공할 의무를 부여하고 있다.[173] 많은 국가들이 외국과의 상호법적지원조약(Mutual Legal Assistance Treaties, MLATs)을 체결해 오고 있다. 이러한 조약은 정부에게 외국 관할에 있는 데이터에 대한 접근권을 부여함으로서 개개인의 권리를 보호하기 위한 절차를 확립하고자 한다. 미국은 오십 여 개 이상의 국가와 이러한 조약을 시행중에 있으며,[174] 중국·태국과는 '상호법적지원약정(Mutual Legal Assistance Agreement, MLAA)'을 체결하였다.[175] 일반적으로 MLATs는 어떤 유형의 조력을 제공하여야 하는지, 어떠한 경우에 이러한 조력을 거부할 수 있는지 구체적으로 규정하고 있다. 이러한 조력의 요청은 주로 법집행이 그 해당국가의 보안이나 공익에 편파적인 경우, 정치적 공격에 해당되는 경우, 합리적 이유가 없는 경우, MLATs에서 정하는 요건을 충족하지 못하는 경우, 조력을 요청받은 국가의 법률에 어긋나는 경우 거절될 수 있다.[176] 동시에 정보의 수집이 적절한 정부의 조사를 지원하는 것이라는 것을 확인하기 위한 절차적 요건이 있다. 예를 들어, 미국-독일 MLATs 제17조는 지원을 요청하는 정부가 서면으로 지원을 요청하여야 하며, 요구되는 증거 또는 정보, 관련 당국, 관련 형법 조항 등을 명시해야한다고 규정하고 있다.[177] MLATs는 가입국의 정부가 다른 국가에 있는 서버에 저장된 정보를 모을 수 있게 해준다. 국제 상공 회의소(The International Chamber of Commerce) 역시 국경 간 데이터 흐름의 합법적 차단을 용이하게 하기위해 MLATs의 중요한 역할을 인정하고, 국지화 조치 대신 MLAT에 집중할 필요성을 강조한 바 있다.[178]

---

173) Convention on Cybercrime art. 25(1), Nov. 23, 2001, T.I.A.S. No. 13,174, E.T.S. No. 185, available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. 2017.4.10.확인.

174) 2 BUREAU FOR INT'L NARCOTICS & LAW ENFORCEMENT AFFAIRS, U.S. DEPT. OF STATE, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT: MONEY LAUNDERING AND FINANCIAL CRIMES 20 (2012), available at http://www.state.gov/documents/organization/185866.pdf 2017.4.10.확인.

175) 2012 INCSR: Treaties and Agreements, U.S. DEP'T OF STATE (Mar. 7, 2012), http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm.

176) THE ALLEGED TRANSNATIONAL CRIMINAL: THE SECOND BIENNIAL INTERNATIONAL CRIMINAL LAW SEMINAR 372 - 3 (Richard D. Atkins ed., 1995).

177) Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Ger., art. 17, Oct. 14, 2003, T.I.A.S. No. 09-1018.

178) INT'L CHAMBER OF COMMERCE, USING MUTUAL LEGAL ASSISTANCE TREATIES (MLATS) TO IMPROVE CROSS-BORDER LAWFUL INTERCEPT PROCEDURES 3 (2012),

그럼에도 불구하고 테러에 대한 두려움은 몇몇 국가로 하여금 국가의 범죄감시기능을 강화시키며 데이터 국지화를 추구하고 있다. 2008년 뭄바이 테러에서 테러범이 블랙베리 디바이스를 사용하여 공격한 이후 인도 정부는 통신사업자의 데이터에 접근할 수 있으며, 특정 통신사업자의 서버는 인도에 둘 것을 요청할 수 있다.[179] 특히 NSA의 스파이 행위가 밝혀지면서 인도의 '인터넷 서비스 공급 업체 협회(Internet Service Providers Association of India)'는 소비자의 프라이버시에 대한 우려를 표명하면서 외국 인터넷 회사들이 자국내 서버를 통해 국내에 서비스를 제공하도록 할 것을 정부에 요청한 바 있다.[180] 프랑스는 최근에 특정 부처가 "전자 및 디지털 통신"을 "실시간"으로 볼 수 있도록 군사 프로그램에 관한 법률을 채택한 바 있다.[181] 한편 미국도 테러공격에 대응한 애국법[182]을 비롯하여 지속적으로 테러 감시를 위한 입법을 강화하였다. 또한 미국정부는 이미 경우에 따라 미국 통신 인프라에 대한 해외 투자를 검토하여 일부 통신 회사에게 데이터 국지화를 요구할 권한을 행사하였음이 밝혀진 바 있다.[183] 이러한 데이터 국지화에 대한 검토는 법무부, 국방부, 국토 안보부 및 연방수사국(FBI)의 대표로 구성된 "팀 텔레콤(Team Telecom)"이라는 비공식적 절차로 진행되었다.[184] 데이터 국지화 의무는 때로는 외국 서비스 사용에 대한 사전 통지 형태로 또는 미국에서의 데이터 저장 요구 형태로 이루어진다. 정보공유협약에 의한 국제적 공조체계가 존재함에도 불구하고 결국 데이터국지화

---

http://www.iccindiaonline.org/policystatement/3.pdf. at 6.

179) Praveen Dalal, Big Brother Must Not Overstep the Limits, TEHELKA.COM (Mar. 3, 2012), http://www.tehelka.com/big-brother-must-not-overstep-the-limits/.

180) Vikas SN, Foreign Internet Companies May Be Asked to Setup Local Servers in India, MEDIANAMA(June 10, 2013), http://www.medianama.com/2013/06/223-foreign-internet-companies-may-be-asked-to-setuplocal-servers-in-india/; Thomas K. Thomas, Indian Net Firms Want Google, Facebook to Go "ocal,"HINDUBUS. LINE (June 8, 2013), http://www.thehindubusinessline.com/industry-and-economy/info-tech/indian-netfirms-want-google-facebook-to-go-local/article4795367.ece.

181) Loi 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale [Law No. 2013-1168 of December 18, 2013 on the Military Budget for the Years 2014 - 019 and Miscellaneous Provisions for Defense and National Security], art. 20, JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Dec. 19, 2013, p. 20570 (Fr.).

182) USA PATRIOT Act of 2001, Pub. L. No. 107-56, tit. II, 115 Stat. 272, 278 - 6.

183) Network Security Agreement between U.S. Dep' of Justice, U.S. Dep' of Homeland Sec., U.S. Dep' of Def., and Level 3 Commc's, Inc. § 2.5 (2011), available at https://info.publicintelligence.net/US-NSAs/US-NSAs-Level3.pdf; Network Security Agreement between U.S. Dep' of Justice, U.S. Dep' of Homeland Sec., and TerreStar Corp. § 2.4 (2009), available at https://info.publicintelligence.net/US-NSAs/US-NSAs-TerreStar.pdf ; Network Security Agreement between U.S. Dep' of Def., U.S. Dep' of Justice, Fed. Bureau of Investigation, AT&T Corp., British Telecomm. PLC, TNV (Neth.) BV, VLT Co. LLC, and Violet License Co. LLC § 2.5.2 (1999), available at https://info.publicintelligence.net/US-NSAs/US-NSAs-ATT.pdf.

184) Spencer E. Ante & Ryan Knutson, U.S. Tightens Grip on Telecom, WALL ST. J., Aug. 27, 2013, http://online.wsj.com/articles/SB10001424127887324906304579037292831912078.

제도를 입법화 하려는 각국의 움직임이 지속되고 있는 것은 결국 현행의 공조체계로는 데이터에 대한 법집행이 상당부분 곤란하다는 것을 반증한다.

5. 정보의 자유

정보의 통제는 권위주의적 정권 생존의 핵심이다. 그러한 정권은 권위를 유지하기 위해 정보를 억제할 것을 요구한다. 이는 독재정부조차 정부가 국민의 이익을 위해 행동하고 있음을 주장함으로서 공공의 위임을 이끌어내기를 원하기 때문이다.[185] 이러한 유익한 정부라는 주장을 방해함으로서 그 위임에 부정적 영향을 미치는 정보를 모든 비용을 들여서라도 제거하길 원한다. 이견을 제기하는 미디어는 전형적으로 데이터 추적의 대상이 되어 그 면허가 취소되거나 설비가 몰수된다. 인터넷은 많은 반체제 인사들이 정보를 공유하기 위해 전 세계에 기반을 둔 서비스를 사용할 수 있게 하므로 이러한 정보의 통제 프로세스를 훨씬 어렵게 한다. 인터넷은 독재정권이 시민들 간 정보를 습득하고 공유하는 것을 막음으로서 시민을 압박하는 것을 더 어렵게 만들었다. 따라서 데이터국지화는 인터넷의 자유향상 기능을 침식시킬 수 있다. 결국 데이터 국지화는 초기 본래의 의도와는 상관없이 수많은 정보를 정권의 통제하게 두게 되는 결과를 초래하게 된다. 이로 인한 위험은 명백하다. 이란의 경제 문제 담당 알리 아가 모하 마디(Ali Aghamohammadi)가 제시한 바와 같이 이란 인터넷에 대한 공식적인 동기는 “윤리적이고 도덕적인 수준에서 무슬림을 겨냥한 진정한 할랄 네트워크”라는 인터넷을 창안하는 것이었다. 이러한 네트워크는 사이버 공격으로부터도 그리고 외국의 네트워크를 사용함으로 인해 야기되는 위험으로부터 안전한 것이다.[186] 그러나 인권운동가들은 외설정보 등을 이유로 한 정부의 추적감시행위는 정부의 진정한 의도를 감추기 위한 것이며, 결국 반대의견을 억누르고 국제적 소통을 막기 위한 것이라고 한다.[187] 언론은 이란인들이 허가된 웹사이트만 방문하도록 허용하는 것은 정권에 의한 책략이라고 비판한다.[188]

이러한 국가에 의한 체제유지에 이용될 가능성을 잘 인식하고 있는 인터넷 기업들은 반체제 인사들을 대상으로 사용된 정보를 피하기 위해서 종종 서버를 자국 영토 밖에 놓기도 한다. Vietnam, Yahoo! 는 국가의 감시체계와의 갈등을 피하기 위하여 서버를 영토밖에 설치하는 결정을 한 바 있다.[189]

---

185) Anupam Chander, Googling Freedom, 99 CALIF. L. REV. 1, 20 (2011).
186) Christopher Rhoads & Farnaz Fassihi, Iran Vows to Unplug Internet, WALL ST. J., May 28 - 9, 2011, at A1, available at http://www.wsj.com/articles/SB10001424052748704889404576277391449002016.
187) Jillian C. York, Is Iran' Halal Internet Possible?, ALJAZEERA (Oct. 2, 2012, 08:18), http://www.aljazeera.com/indepth/opinion/2012/10/201210263735487349.html. 2017.4.10확인
188) Government Blocks Google and Gmail, While Promoting National Internet, REPS. WITHOUT BORDERS (Sept. 24, 2012), ttp://en.rsf.org/iran-islamic-republic-poised-to-launch-21-09-2012,43431.html.
189) VN Digital Content Firms Find Home Disadvantage, VIỆT NAM NEWS (Sept. 22, 2008),

아마도 데이터국지화의 가장 큰 위험은 독재국가들이 정보에 대한 통제를 확장하는 것이다. 자유주의 국가들이 독재체계에 의한 정보의 통제를 비판할 때, 독재국가는 자유주의 국가들 역시 데이터국지화룰 위해 노력하였다는 것을 인용할 수 있다. 자유주의 국가가 데이터 통제를 정당화하기 위해 보안, 개인 정보 보호, 법 집행 및 사회 경제적 이유로 인용할 수 있다면 독재 국가도 마땅히 그렇게 할 수 있다.[190]

자유주의 국가에 의한 데이터국지화가 독재정권이 모방하기 좋은 선례로 작동하는 것은 바람직하지 않다.[191] 자유주의 국가 조차도 시민을 감시함으로서 시민의 권리를 약화시킨 바 있다. 독일의 "Internetz"제안에 대하여는 국가 라우팅이 심층적인 패킷 검사를 필요로 하므로 광범위한 감시가 있을 수 있다는 우려를 불러일으킨 바 있다.[192] 일부 언론은 이러한 국가 공인 네트워크는 외국의 감시로부터 벗어나는데 그다지 도움이 되지 않고, 오히려 독일 감시기관의 "감시기능의 중앙집중화"를 초래할 것이라고 밝힌 바 있다.[193]

감시 및 검열에 근거한 인권 침해에 대한 우려 외에도 데이터 국지화 조치는 표현의 자유, 특히 국경에 상관없이 모든 종류의 정보와 아이디어를 추구하고 수령하고 전달할 자유에 저해된다.[194] 해외에서 개인 정보가 저장되거나 처리 될 수 있으므로 시민들이 외국 정치 포럼을 사용하는 것을 방지하는 것은 지식에 대한 개인의 권리를 방해하는 것이다.[195] 데이터가 외부로 나가는 것을 차단하고 들어오는 데이터를 걸러내는 기능으로 무장 한 데이터 국지화는 감시 및 검열을 위한 인프라를 제공함으로써 정부의 데이터 통제권을 더욱 결집, 강화 시킬 수 있다.[196]

---

http://vietnamnews.vn/economy/business-beat/180617/vn-digital-content-firms-find-home-disadvantage.html(베트남에서 서비스되고 있는 Yahoo!' 서버는 싱가포르에 있다.

190) Anupam Chander & Uyên P. Lê, supra note 7 at 737.

191) Natsu Taylor Saito, Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and Unlawful Repression of Political Dissent, 81 OR. L. REV. 1051, 1059 - 0 (2002).

192) Richard Adhikari, Deutsche Telekom Pitches NSA-Free German Internet, TECH NEWS WORLD (Oct. 26, 2013, 5:00 AM PT), http://www.technewsworld.com/story/79286.html. On deep packet inspection, see Hal Abelson, Ken Ledeen & Chris Lewis, Just Deliver the Packets, OFFICE OF THE PRIVACY COMM'R OFCAN., http://www.priv.gc.ca/information/research-recherche/2009/ledeen-lewis_200903_e.asp (last modified Mar. 25, 2009).

193) Alex Evans, Can Germany Really Keep Bytes Within Its Borders?, LOCAL(Nov. 29, 2013, 10:10GMT), http://www.thelocal.de/20131129/german-email-providers-unite-german-internet-against-nsa.

194) International Covenant on Civil and Political Rights, art. 19(2), opened for signature Dec. 19, 1966, 999 U.N.T.S. 171 (entered into force, Mar. 23, 1976); see also Molly Land, Toward an International Law of the Internet, 54 HARV. INT'L L.J. 393, 438 (2013).

195) Molly Beutz Land, Protecting Rights Online, 34 YALE J. INT'L L. 1 (2009).

196) Anupam Chander & Uyên P. Lê, supra note 7 at 739.

Ⅴ. 결 론

주권개념에 의거할 때 인터넷 공간에서도 데이터 규제와 관련된 관할권이 인정된다. 각 국가들은 국가주권에 기초하여 국제법상 정당한 관할권을 가지는 한도 내에서 독자적 법체계를 구축하고 있으며 그 결과 한 국가에서는 적법한 활동이 동시에 유효한 관할권을 가진 다른 국가에서는 위법할 수가 있는 갈등이 나타나게 된다. 따라서 인터넷 공간에서 데이터 관할권에 근거한 갈등상태를 극복하는 방안은 인터넷 규제법을 조화시켜 가급적 법률충돌이 발생하지 않도록 하거나, 분쟁 시 우선적 재판관할권을 부여하는 조약을 체결하는 것이다. 그러나 인터넷 공간의 데이터 갈등 문제는 대부분 인터넷 공간에서 끝나지 않는다. 프라이버시 침해, 국가안보, 명예훼손, 음란물, 공정경쟁 등 인터넷 공간의 데이터 규범의 차이에 따른 갈등은 결국 각 나라의 사회문화 뿐만 아니라 실물경제에 영향을 미치며 그 결과는 현실공간에서 드러나게 된다. 세계 모든 국가는 서로 고유한 법체계와 문화를 가지고 있으며 이를 형성해 온 정치·사회·경제적 배경이 각각 다르므로 인터넷 공간에서 전 세계적으로 통일된 규제를 만든다는 것은 현실적으로 불가능하다. 하지만 인터넷 공간에서 데이터 규범의 국제적 합의의 실패는 국가 간에 논쟁과 갈등을 일으킬 수 있다. 이러한 갈등 속에서 우리의 데이터주권을 얼마만큼 지켜낼 수 있는가 하는 문제는 독립국가로서의 위상과 국민적 자부심에 영향을 미칠 수 있는 만큼 민감하면서도 중요할 수밖에 없다.

데이터국지화 규범 자체는 사실상 데이터의 기술적 속성에 위배되는 것이다. 따라서 규범설정 만으로 기술적 효과를 완전히 막기에는 한계가 존재한다. 그러나 규범이 반드시 기술적 속성에 종속되어 기술적 속성을 따라야 하는 것은 아니며, 오히려 기술적 속성이 인간의 삶에 유익하게 작동할 수 있도록 제도가 기술의 방향을 이끄는 것이 바람직하다. 이러한 관점에서 이미 많은 정부는 자국 관할 하에서 운영되고 있는 기업들에 대하여는 그 기업이 보유하고 있는 국적자에 대한 데이터를 공유하도록 강제하는 입법적 조치를 마련하였다. 절차는 각각 다르지만 대부분의 국가들은 어떤 특정한 상황에서 클라우드컴퓨팅 서비스 제공자에게 그들이 보유하고 있는 고객정보를 공개하도록 요구할 수 있는 권한을 가지고 있으며, 대부분의 경우 이러한 권한으로 인해 정부는 물리적으로 국경밖에 저장된 정보에 대하여도 접근이 가능하다.[197]

모든 데이터에 대한 국지화 정책은 데이터의 기술적 속성에 완전히 위배되며 현실적으로 가능할지도 의문이다. 그러나 국민의 프라이버시, 국가안보, 공공기록물 등 국가주권 보장에

197) WINSTON MAXWELL & CHRISTOPHER WOLF, HOGAN LOVELLS, A GLOBAL REALITY: GOVERNMENT ACCESS TO DATA IN THE CLOUD 3 (rev. ed. 2012), available at http://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf at 2 - 3(2017.4.10.확인).

필수불가결한 일정한 데이터에 대하여는 국지화 정책이 일정부분 추구되어야 한다. 이러한 경우 국가주권의 최소한의 관할권 행사로서의 데이터 국지화 조치가 필요하다. 그 이외의 데이터에 대한 국지화 규범은 경제적 파급효과, 데이터 협력필요성 등에 비추어 볼 때 모든 국가를 상대로 일률적으로 정할 수 있는 것은 아니다. 따라서 대외적 주권실현의 가장 기본원칙인 상호주의에 입각한 데이터 국지화 규범이 타당하다. 상호주의 원칙하에 우리나라에 대한 상대국의 정책을 반영하여 차별화 될 필요가 있다. 그리고 이러한 원칙을 「개인정보 보호법」 등 데이터 관련 법률에 명확히 규정할 필요가 있다. 또한 우리나라가 정한 데이터 보호 조치를 준수할 것을 약정하고 그에 어긋난다면 한국법의 집행을 받는다는 전제하에 데이터의 자유로운 흐름을 보장하는 방안도 함께 강구되어야 한다.

집안 침대 밑에 숨겨둔 돈처럼, 내 집에 보관해 둔다고 해서 데이터가 마냥 안전한 것만은 아니다. 데이터가 그 집안, 그 나라 안에 보관되어 있다고 할지라고 범죄자들은 결국 불법적인 접근을 시도한다. 뿐만 아니라 데이터 국지화 규범설정은 오히려 정부 감시 및 통제의 수단으로 활용하기 용이하고 이는 국민주권의 제도적 보장인 민주주의의 발전에도 저해된다. 따라서 데이터국지화 규범 설정시 자의적 공권력에 의한 부당한 결과가 초래되지 않도록 하는 수단이 반드시 함께 마련되어야 할 것이다.

(투고일 : 2017. 5. 1 / 심사일 : 2017. 5. 17 / 확정일 : 2017. 5. 23)

참 고 문 헌

김현경, 기술혁신환경에서 프라이버시와 공권력의 충돌과 조화, 가천법학 제9권 제3호 , 2016.9. pp.81~124

_____, ICT규제원칙에 기반한 온라인서비스 비대칭규제의 개선방안에 관한 연구, 성균관법학 제26권제3호, 2014.9. pp.487~521

윤재석, 유럽연합과 미국의 개인정보 이전 협약 (프라이버시 쉴드)과 국내 정책 방향, 정보보호학회논문지 26(5), 2016.10. pp.1269-1277.

조소영, 인터넷 주권과 통제에 관한 연구, 공법학연구 제12권 제4호, 2009.

함인선, EU의 2016년 일반정보보호규칙(GDPR)의 제정과 그 시사점, 법학논총 36(3), 2016.9. pp. 411-453.

허진성, 데이터 국지화((Data Localization) 정책의 세계적 흐름과 법제적 함의, 언론과 법 제13권 제2호, 2014. pp. 289-309.

홍석한, 세계화에 따른 주권의 변화에 관한 헌법적 고찰, 公法學硏究 第10卷 第2號, 2009. pp.187-212.

Alves Jr., Sergio, Internet Governance 2.0.1.4: The Internet Balkanization Fragmentation (June 29, 2014). Available at SSRN: http://ssrn.com/abstract=2466222

Anupam Chander & Uyên P. Lê, Data Nationalism, 64 EMORY L.J. 677(2015)

Bert Verschelde, The Impact of Data Localisation on Korea's Economy http://www.ecipe.org/media/publication_pdfs/ECIPE_bulletin1014_dataloc_korea.pdf

Bellia, Patricia L., Chasing Bits Across Borders. University of Chicago Legal Forum, pp. 35-101, 2001. Available at SSRN: https://ssrn.com/abstract=556471

Brown, Ian and Korff, Douwe, Foreign Surveillance: Law and Practice in a Global Digital Environment (April 30, 2014). European Human Rights Law Review 3: 243-251. Available at SSRN: https://ssrn.com/abstract=2521433

Chander, Anupam and Le, Uyen P., Breaking the Web: Data Localization vs. the Global Internet (April 2014). Emory Law Journal, Forthcoming; UC Davis Legal Studies Research Paper No. 378. Available at SSRN: http://ssrn.com/abstract=2407858

Charlotte Alfred, Web At 25: Will Balkanization Kill The Global Internet?, The Huffington Post http://www.huffingtonpost.com/2014/03/19/web-balkanization-national-internet _n_4964240.html

Damon C. Andrews & John M. Newman, Personal Jurisdiction and Choice of Law in the Cloud, 73 MD. L. REV. 313, 325-28(2013)

Deeks, Ashley, Confronting and Adapting: Intelligence Agencies and International Law

(April 12, 2016). Virginia Law Review, Vol. 102, No. 59, 2016; Virginia Public Law and Legal Theory Research Paper No. 2016-31. Available at SSRN: https://ssrn.com/abstract=2768339

De Hert, Paul and Boulet, Gertjan, Cloud Computing and Trans-Border Law Enforcement Access to Private Sector Data. Challenges to Sovereignty, Privacy and Data Protection (September 10, 2013). Workshop paper collection: 'Big data & Privacy. Making Ends Meet', organised by the 'Future of Privacy Forum' and the 'Center for Internet and Society' at Stanford Law School, pp. 23-26. Available at SSRN: https://ssrn.com/abstract=2530465

Irion, Kristina, Government Cloud Computing and National Data Sovereignty (June 30, 2012). Irion, Kristina (2012). "Government Cloud Computing and National Data Sovereignty". Policy and Internet Vol. 4 [2012] issues 3-4, pp. 40-71. Available at SSRN: https://ssrn.com/abstract=1935859 or http://dx.doi.org/10.2139/ssrn.1935859

Jennifer Daskal, the un-territoriality of data, the yale law journal 125: 326, 2015.

Jeanette Seiffert, Weighing a Schengen zone for Europe's Internet data http://www.dw.de /weighing-a-schengen-zone-for-europes-internet-data/a-17443482

Joshua Bleiberg and Darrell M. West, How to Stop the Internet from Breaking Apart, Oct.6, 2014 http://www.brookings.edu/blogs/techtank/posts/2014/10/6-preventing -internet-balkanization

Jonah Force Hill, Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers(2012)http://belfercenter.ksg. harvard.edu/files/internet_fragmentation_jonah_hill.pdf

Jonah Force Hill, The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders(May 1, 2014). The Hague Institute for Global Justice, Conference on the Future of Cyber Governance, 2014. Available at SSRN:http://ssrn.com/abstract=2430275

Kobrin, Stephen J., The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance (November 2002). Available at SSRN: https://ssrn.com /abstract=349561 or http://dx.doi.org/10.2139/ssrn.349561

McKinsey Global Institute. Internet matters: The Net's sweeping impact on growth, jobs, and prosperity, May 2011; McKinsey Global Institute. The great transformer: The impact of the Internet on economic growth and prosperity, Oct. 2011.

Michael Birnbaum, Germany looks at keeping its Internet, e-mail traffic inside its borders http://www.washingtonpost.com/world/europe/germany-looks-at-keepingits-inter

net-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html

Molly Beutz Land, Protecting Rights Online, 34 YALE J. INT'L L. 1 (2009).

Natsu Taylor Saito, Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and Unlawful Repression of Political Dissent, 81 OR. L. REV. 1051, 1059 - 0 (2002).

Nugraha, Yudhistira and ., Kautsarina and Sastrosubroto, Ashwin Sasongko, Towards Data Sovereignty in Cyberspace (April 17, 2015). Third International Conference of Information and Communication Technology, May 2015. Available at SSRN: https://ssrn.com/abstract=2610314 or http://dx.doi.org/10.2139/ssrn.2610314

Orin S. Kerr, Searches and Seizures in a Digital World, 119 HARV. L. REV. 531, 557-58 (2005).

Stephan Wilske & Teresa Schiller, International Jurisdiction in Cyberspace: Which States May Regulate the Internet?, 50 Fed. Comm. L.J. 117, 1997.

Tim Berners-Lee: We need to re-decentralize the Web http://arstechnica.com/tech-policy/2014/02/tim-berners-lee-we-need-to-redecentralize-the-web/

U.S. Chamber of Commerce, Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity (2014) https://www.uschamber.com/sites/default/files/021384_BusinessWOBorders_final.pdf

Vaile, David and Kalinich, Kevin P. and Fair, Patrick V. and Lawrence, Adrian, Data Sovereignty and the Cloud: A Board and Executive Officer's Guide (December 16, 2013). UNSW Law Research Paper No. 2013-84. Available at SSRN: https://ssrn.com/abstract=2369660

William C. Banks, Programmatic Surveillance and FISA: Of Needles in Haystacks, 88 TEX. L. REV. 1633 (2010)