http://dx.doi.org/10.15539/KHLJ.52.4.6

개인정보의 현지화에 관한 연구*

박 훤 일*

| 국문 요약 |

개인정보의 현지화(data localization)란 개인정보를 보관·처리하는 서버를 반드시 국내에 설치해야 하는 것을 말한다. 미 정보기관의 전 세계적인 정보수집 활동이 드러남에 따라 많은 나라가 개인정보 보호, 국가안보, 자국 산업의 육성 등의 구실로 소스코드 공개를 요구하거나 데이터의 현지 보관 등 규제를 강화하는 경향을 보이고 있다.

IoT, 빅데이터 시대에 정보의 자유로운 유통으로 경제 활성화를 기대할 수 있는 반면 많은 나라가 국가안보와 국익보호 목적으로, 특히 EU의 경우 개인정보의 보호 수준이 낮은 제3국으로의 정보이전을 불허하고 미국의 IT기업들이 플랫폼을 장악하는 것에 대한 경계심이 고조되고 있다. 일부 국가는 다국적 IT기업들이 엄청난 광고 수입을 올리면서도 세금을 거의 내지 않는 것을 막기 위해 국내에 데이터 센터를 두도록 유도하고 있다. 그러나 이러한 데이터 현지화는 관련업계의 클라우드 서비스의 이용이 늘어나는 추세에 역행할 뿐만 아니라 정보유통의 장벽이 되어 외국인투자 감소로 이어질 경우 GDP가 줄어들지 모른다.

주요국 현황을 보면 중국은 핵심 정보통신 기반시설 운영자에 대한 엄격한 책임과 의무를 부과한 네트워크 안전법에서 개인정보와 중요 데이터는 현지 서버에 저장하도록 의무화했다. 베트남도 OTT통달, 정령 72호에 의해 국내에 1개 이상의 호스트 서버를 설치하도록 요구하였다. 인도네시아는 공공서비스 전자시스템 관리자의 데이터 센터 국내 설치를 의무화하였고, 러시아는 개인정보는 국내에 있는 데이터베이스로 관리하고, 데이터 센터의 소재를 당국에 신고하도록 했다.

인터넷 시대에 데이터 현지화를 요구하는 법제는 나름대로 명분이 있어 보인다. 우리나라가 구글에 대한 공간정보 반출을 불허한 것도 북한이 장거리 미사일, 무인기를 날리고 있는 상황에서 부득이했던 것으로 판단된다. 그러나 공간정보는 유통·관광산업 및 자율주행차·드론의 이용에 없어서는 안 될 인프라이다. 인터넷의 발칸화 현상은 결코 바람직하지 않으며 국경간 정보유통에 대한 확고한 신념을 가져야 한다. 그 예외 사유는 안보 목적이든 무엇이든 엄격하게 해석하는 것이 타당하다.

* 경희대학교 법학전문대학원 교수, 법학박사
(투고일자 : 2017.11.17., 심사일자 : 2017.12.01., 게재확정일자 : 2017.12.12.)

주제어 : 개인정보의 현지화, 데이터 현지규제, 데이터 센터, 정보유통, 인터넷 발칸화 현상

< 차 례 >

Ⅰ. 머리말
Ⅱ. 개인정보 로컬라이제이션의 동기
Ⅲ. 주요국의 사례
Ⅳ. 개인정보 현지화 규제에 대한 평가
Ⅴ. 맺음말

Ⅰ. 머리말[1)]

개인정보의 로컬라이제이션(data localization)은 개인정보의 '현지화' 또는 '국지화'라고 번역할 수 있는데 정보통신을 이용하는 기업이 개인정보의 보관·처리를 위한 서버를 반드시 국내에 설치하도록 의무화하는 것을 일컫는 말이다. 물리적인 데이터 보관 장소(physical data location)라는 의미보다도 정보열람에 대한 통제 등 효과적인 관할(effective jurisdiction)에 관한 문제라 할 수 있다. 그 연장선상에서 데이터의 해외 반출(data export)에 대한 규제를 뜻하는 말로 쓰이기도 한다.[2)]

최근 들어 중국, 베트남, 인도네시아, 인도, 러시아 등 여러 나라가 정보보안, 개인정보 보호, 국가안보, 제품의 안전기준, 자국 산업의 보호·육성 등을 이유로 소스코드 공개를 요구하거나 데이터의 현지 보관, 로컬 콘텐츠의 이용 등 규제를 강화(forced localization measures: FLMs)하는 경향이 늘고 있다.[3)] IT산업 발전에

1) 이 글은 NAVER의 2017년 Privacy White Paper로서 기고한 것이며 여기에 개진된 의견은 필자의 사견일 뿐이다. 이 논문의 학술지 기고를 허락해 주시고, 관련 주제에 관한 세미나 개최를 통해 인터넷과 IT법규범에 대한 관심을 환기시킨 회사 측에 사의를 표한다.

2) W. Kuan Hon, *Data Localization Laws and Policy - The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens*, Edward Elgar, 2017.

따른 이점을 충분히 살리기도 전에 클라우드 컴퓨팅, 사물인터넷(IoT) 산업에 대한 제약요인이 되고 있는 것이다.

다음 그림에서 보듯이 개인정보의 로컬라이제이션이 전세계적으로 증가하는 추세에 있기 때문에 정보의 자유로운 유통(free flow of data)의 관점에서는 우려를 낳고 있다. 왜냐하면 사물인터넷(IoT), 빅데이터 시대에는 정보가 자유롭게 흘러야 이노베이션이 활성화될 터인데 현지 규제에 따라 경제적 고려 없이 무조건 데이터 센터를 설치해야 하고 경우에 따라서는 콘텐츠의 제약도 받을 수 있기 때문이다. 반면 개인정보 보호 법제의 통일이라는 관점에서 살펴본다면 무엇이 각국의 입법자로 하여금 개인정보의 로컬라이제이션을 택하게 하는지 그 동기를 알아볼 필요가 있다.

이러한 가운데 미국과 유럽, 일본은 2013년부터 서로 손을 잡고 개인정보의 로컬라이제이션에 대한 규제에 공동 대응하기로 했다.[4] 2016년 5월 일본에서 열린 G7 정상회의에서도 개방적이고 상호운용 가능하며 신뢰할 수 있는 사이버공간에서 삶의 질을 개선하기 위한 디지털 경제를 촉진할 것을 공동선언문에 포함시킨 바 있다.[5] 한편 일본과 EU는 2015년 정보의 자유로운 유통과 사이버공간의 공평하고 평등한 확보를 위해 규제와 협력에 힘을 모으기로 했다.

이 연구는 모든 것을 인터넷으로 서로 연결하는 시대에 개인정보의 로컬라이제이션 쪽으로 입법 전환을 하는 동기가 무엇인지, 나라마다 FLMs 규제를 어떻게 실시하고 있는지 살펴본 후 국내외의 반응을 알아보고자 한다. 나라마다 특별한 사정이 있기 마련이지만 여러 이점에도 불구하고 이를 적극적으로 시행할 수 없는 속사정도 있기 때문이다. 마지막으로 우리나라는 이러한 추세에 어떻게 대응하는 것이 좋을지 생각해 보기로 한다.

---

3) 베트남, 인도네시아에서는 법률이 아주 추상적으로 규정되어 있고 그 시행세칙인 정령(Decree)과 통달(Circular)에 구체적인 규정을 두는 경우가 많다. 그러므로 FLMs가 어디에 규정되어 있는지 특정하는 것은 쉽지 않다. 베트남은 2013년 정령72호에서 대표자 또는 법인을 베트남 국내에 두도록 요구하고 있다. 엉뚱하게도 정보통신 소관부처 이외의 법률이나 시행세칙에 FLMs 규정을 두기도 한다.

4) 일례로 일본의 経済団体連合会(Keidanren)과 在日 미국상공회의소는 양국이 환태평양경제동반자협정(Trans-Pacific Partnership: TPP)에 참가한 것을 계기로 2016년 2월 25일 "日米 IED 民間作業部会共同声明2016"을 내고 Data Localization과 Cross-border Data Flow 문제를 심도 있게 다루었다. <http://www.keidanren.or.jp/policy/2016/015.html>

5) G7 이세시마 정상회담 자료는 <http://www.mofa.go.jp/ecm/ec/page4e_000457.html> 참조.

Ⅱ. 개인정보 로컬라이제이션의 동기

<그림>의 세계지도에서 보듯이 정도의 차이는 있지만 데이터 현지화를 요구하는 나라들이 더 많은 게 사실이다. 그러나 그 동기가 나라마다 조금씩 다른 것을 알 수 있다. 우선 미국 국가안보국(National Security Agency: NSA)에서 근무했던 에드워드 스노든이 미국 정보당국의 전 세계를 대상으로 한 정보수집과 감시활동(PRISM)을 폭로한 것을 계기로 국가안보와 국익보호 목적으로 국내 수집 정보의 국내 보관 및 처리를 요구하는 경우가 많아졌다.

그러나 자국민의 개인정보가 국제교역이나 해외 아웃소싱 등의 목적으로 해외 반출된 경우에 해외에서 자국민의 개인정보가 침해되는 일이 없도록 하는 개인정보 보호(data protection) 차원에서 정보의 국외이전을 불허하는 경우도 많다.

최근에는 다국적 IT 거대기업들이 국내에서 많은 수익을 얻음에도 불구하고 세금을 안 내거나 적게 내는 것을 방지하기 위해 국내에 서버를 설치하고 고정사업장(permanent establishment)을 두게 하려는 의도도 엿보이고 있다.

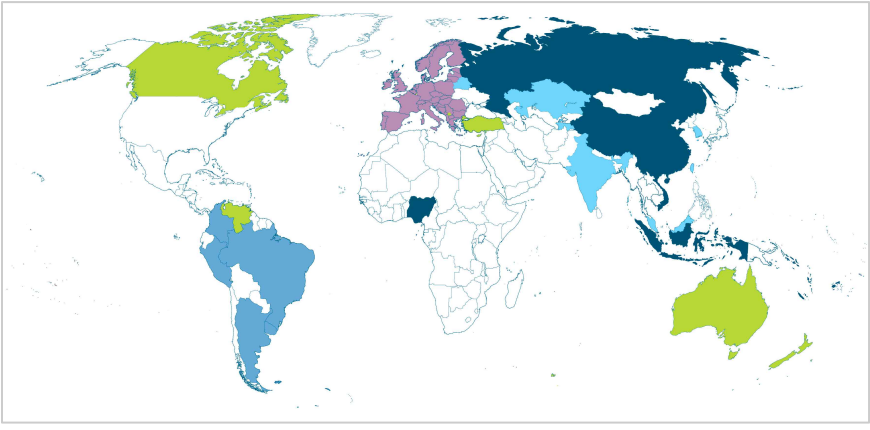
1. 국가안보와 질서유지

2013년 7월 스노든의 폭로 이후 독일에서는 연방개인정보감독기구가 나서서 외국의 정보기관들이 독일 기업들이 전송하는 데이터에 외국의 정보기관이 무단 접근하는 것을 규제할 수 있음을 밝혔다. 이와 함께 독일 정부가 지분을 갖고 있는 도이체 텔레콤에서도 독일 국내에서의 인터넷 트래픽을 최대한 국내에 유지하려는 방침을 협력업체에 시달하고, 다른 EU 회원국들에 대해서도 EU만의 유럽 데이터 네트워크를 갖출 것을 제안했다.[6] 다만, 이러한 조치는 외국 정보기관이 독일 데이터를 열람하는 것을 근본적으로 방지하기 위한 대책이 될 수 없다는 비판이 제기되었다.[7]

---

6) 독일 메르켈 정부는 유럽에서 발신되는 이메일과 전기통신의 망을 분리하는 범구주 정보통신망 구축에 앞장서고 있으며, 정부 데이터를 저장하는 클라우드 인프라(Bundes-cloud)를 2022년까지 개통하기로 했다. Albright Stonebridge Group, Data Localization: A Challenge to Global Commerce and the Free Flow of Information, September 2015, p.8 (이하 "Data Localization"라 약칭함).

<그림> 데이터 현지화의 국가별 현황



지도상의 색	데이터 해외 이전에 대한 제한의 정도	해당 국가
	[매우 엄격] 개인정보는 국내 설치된 서버에 보관되어야 함	러시아, 중국, 인도네시아, 베트남, 브루네이, 나이지리아
	[사실상 엄격] 개인정보의 국외 이전을 법령으로 제한함으로써 사실상 데이터 현지화가 이루어지고 있음	유럽연합(EU)
	[부분적 제한] 국외 이전할 수 없는 정보의 종류를 지정하거나 정보의 국외 이전에 정보주체의 동의를 요함	한국, 인도, 말레이시아, 카자흐스탄, 벨라루스
	[완 화] 일정한 조건하에서만 정보의 국외 이전을 제한함	아르헨티나, 브라질, 콜롬비아, 페루, 우루과이
	[특정분야 제한] 헬스케어, 이동통신, 금융, 국가안보 등의 분야에 한하여 정보의 국외 이전을 제한함	타이완, 캐나다, 오스트레일리아, 뉴질랜드, 터키, 베네수엘라
	[제한 없음] 데이터 현지화 의무가 없음	미국, 일본 등 기타 국가

자료: Albright Stonebridge Group, Data Localization: A Challenge to Global Commerce and the Free Flow of Information, September 2015, p.5.

주: 개인정보의 국외 이전을 제한하고 데이터 현지화를 요구하는 법령은 수시로 바뀔 수 있으므로 명확히 분류하기 어려운 점이 있으며 저자가 작성시점을 기준으로 평가하여 소개한 것임

7) 허진성, "데이터 국지화(Data Localization) 정책의 세계적 흐름과 그 법제적 함의", 언론과 법 제13권 2호, 2014. 295~296면.

이와 관련하여 브라질의 호세프 대통령도 미국을 우회하는 남미와 유럽 간의 정보통신망을 연결하는 해저 광섬유 케이블 설치 계획을 제안하면서, 브라질 우정국에 암호화된 이메일 시스템 개발을 지시하였다. 의회에 대해서는 구글, 마이크로소프트 등 미국의 IT기업들이 브라질 이용자에 대한 데이터를 국내 서버에 보관할 것을 의무화하는 입법을 요구했으나 거센 반대에 부딪혔다. 그래서 이것은 제외한 채 2014년 4월 인터넷 이용자의 권리와 서비스 제공자의 의무를 규정한 마르코 시빌 법(Marco Civil da Internet Law)을 제정·공포하였다.[8]

중국에서도 자국민들에 대한 사상통제와 정치적 안정을 위해 외부 인터넷 연결을 막지는 않아도 일정한 경우 정부당국이 인터넷 트래픽의 국내 유입과 국외 유출을 통제할 수 있는 정보장벽[9]을 설치하였다. 이는 후술하는 2017년의 네트워크 안전법에서 보다 구체화되었다. 이란에서도 중국에서 전문가들을 불러와 종교적으로 허용되는 인터넷을 구축하는 작업을 진행하였다.

그러나 안보 목적의 데이터 현지화는 오히려 해킹 등 공격 목표를 명확히 하는 것이 되어 더 위험에 처할 수 있다는 비판이 가해지고 있다.

2. IT 거대기업에 대한 종속 탈피

유럽에서는 구글, 아마존, 마이크로소프트, 페이스북 등 미국의 IT기업들이 플랫폼[10]을 장악하고 정보유통 시장을 지배하는 것에 대한 경계심이 고조되었다.

---

8) Dan Cooper, “Brazil Enacts “Marco Civil” Internet Civil Rights Bill”, Covington & Burling LLP April 28, 2014. <https://www.insideprivacy.com/international/brazil-enacts-marco-civil-internet-civil-rights-bill/>. 호세프 대통령의 이 조치는 그가 수세에 몰린 국내정치 상황에서 국면전환용이라는 비판이 많았다.

9) 중국은 1994년 외부 웹과 연결된 이래 1998년에는 인터넷 트래픽의 유·출입을 통제할 수 있는 황금방패(Golden Shield) 시스템을 설치하여 세계에서 가장 정교한 정보장벽 이른바 ‘Great Firewall’(정보의 만리장성)을 구축하였다.

10) 이러한 플랫폼은 중세 시대에는 봉건영주와 교회, 길드조합 등 중간조직에 속하였고 개인의 인권은 도외시되기 일쑤였다. 기본적 인권이 강조되는 21세기의 정보사회에서도 플랫폼을 누가 지배하느냐에 따라 이러한 사정은 마찬가지다. 개인이 정보사회에서 자율적으로 활동하고, 이러저러한 플랫폼에서 조각난 인격을 스스로의 의사로 재통합하기 위해서는 자신의 정보를 소유하고 이전할 수 있는 정보이동권이 앞으로 정보사회의 불가결한 인권으로 인식될 것이다. 生貝直人, “自律·分散·協調社会とデータポータビリティーの権利”, 経済産業省分散戦略ワーキンググループ 第6回, 2016.7.27, 24面.

2017년 초까지 유럽의회 의장을 역임한 독일 사민당 대표 슐츠(Martin Schulz)는 거대 IT기업(Digital Giants)에 의한 데이터 시장의 지배는 경제문제에 한하지 않고 사회질서의 문제로 직결될 것이라고 경고하기도 했다.[11]

이러한 유럽인들의 심리는 EU의 개인정보보호규정(General Data Protection Regulation: GDPR 2018.5.25 EU회원국내 법률로서 발효)에 정보이동권(right to data portability: RDP)을 규정함으로써 구체화되었다.[12] 만일 정보이동이 안 된다면 어느 한 사람의 개인정보는 특정 정보처리자의 서버에 갇혀(lock-in) 있거나 다양한 사업자와 정부기관에 분산 보관될 것이다. 인터넷 환경에서는 구글과 페이스북, 애플, 아마존[13] 사례에 비추어 플랫폼 기업에 정보가 집중될 것임이 명약관화하다. 특히 인공지능, IoT, 빅데이터, 로봇 등에 의한 4차 산업혁명 시대에 플랫폼을 장악한 거대 IT기업에 정보가 집중되는 상황은 가상공간뿐만 아니라 이러한 정보가 이용되는 제조업, 의료 및 교통 서비스 산업, 사회 전반에 걸쳐 중대한 영향을 미치게 될 것이라는 점은 쉽게 짐작할 수 있다. 이에 따라 EU에서는 주로 미국계 IT 플랫폼 기업에 대한 데이터 시장을 탈환하기 위한 무기로 EU내 유통 정보의 역내 보관을 의무화하기보다[14] 정보이동권을 강조하고 나왔던 것이다.

그리고 일부 동남아 국가에서는 자국 내 하이테크 경제활동을 촉진한다는 의도하에 로칼 콘텐트를 요구하고 해외 콘텐트에 대해서는 높은 세율을 부과하기도 한다. 이를테면 '디지털 중상주의(Digital Mercantilism)'의 도래라 할 만하다.[15]

---

11) EU의회의 슐츠 전 의장은 2016년 1월 유럽의 CPDP(컴퓨터, 프라이버시, 개인정보보호) 컨퍼런스에서 다음과 같이 말했다. "만일 개인정보가 21세기의 가장 중요한 상품이 되고 있다면 자신의 정보에 대한 개개인의 소유권을 강화하는 것은 정치인과 사법부의 임무이다. 이러한 상품에 아무도 대가를 지불하지 않고 이용만 하려 드는 상황에서 디지털 자이언츠가 새로운 세계질서를 형성하는 것을 허용하여서는 아니 된다."

12) GDPR Article 20 and para. 68 of Preamble. 박훤일, "정보이동권의 국내 도입 방안 - EU GDPR의 관련 규정을 중심으로", 경희법학 제52권 3호, 2017.9.30., 214~221면 참조.

13) 세계 정보유통시장의 플랫폼을 지배하는 이들 IT기업의 머리글자를 따서 'GFAA'라고 부른다.

14) EU의 데이터보관지침(EU Data Retention Directive, Directive 2006/24/EC)은 2014년 4월 유럽사법재판소(Court of Justice of the European Union: CJEU)로부터 사생활에 대한 기본적 인권 및 개인정보 보호를 광범위하고 심각하게 침해하므로 소급하여 위법 무효라고 선고받았다. Covington, "EU Data Retention Directive Declared Invalid by CJEU", *Inside Privacy*, April 8, 2014. <https://www.insideprivacy.com/international/european-union/eu-data-retention-directive-declared-invalid-by-court-of-justice-of-the-eu/>

3. 공정 과세의 실현

다국적 IT기업들이 국내에서 엄청난 광고 수입을 올리면서도 세금을 내지 않거나 아주 적은 금액만 납부하는 행태가 많은 나라에서 문제가 되고 있다. 2013년 5월 EU 정상회담에서도 다국적기업의 조세회피 문제를 거론하고 EU 차원에서 공동대처하기로 의견을 모았다. 실제로 프랑스 정부는 구글, 페이스북, 아마존과 같은 IT기업에 대해 수익이 아닌 매출액(turnover) 기준으로 과세하기로 한 바 있으며, 2017년 9월 EU 집행위에서도 다국적 IT기업들이 현지법인 같은 물리적 실재가 없다는 이유에서 일반 기업의 23.2%에 비해 크게 낮은 10.1% 세율의 법인세만 납부하는 것을 시정하기로 방침을 굳혔다.[16] 애플과 구글 같은 IT기업들은 이른바 'Double Irish with Dutch Sandwich' 전략[17]을 구사하여 미국 외 매출에 대한 원천지 과세를 회피해 온 것으로 알려져 있다.

이러한 실정에 비추어 정교한 세법 규정을 갖추지 못한 동남아 국가에서는 세계적인 검색·사회관계망 서비스(SNS) 운영기업에 대해 자국 내에 서버를 두도록 하고 이를 근거로 과세하는 방법을 택하고 있다. 우리나라에서도 구글은 유한회사인 구글 코리아가 소규모 벤처기업으로 분류되어 있어 외부감사나, 매출액을 공시할 의무가 없다. 2016년 중 구글은 우리나라에서 구글 플레이 앱을 통한 유료

---

15) Stuart Lauchlan, "Data localization rules damage the global digital economy, says US tech thinktank", Diginomica, May 3, 2017. <http://diginomica.com/2017/05/03/data-localization-rules-damage-global-digital-economy-says-us-tech-thinktank/>

16) The Guardian, "EU to find ways to make Google, Facebook and Amazon pay more tax", 21 September 2017. <https://www.theguardian.com/business/2017/sep/21/tech-firms-tax-eu-turnover-google-amazon-apple>

17) 구글(2015.8.부터는 지주회사인 알파벳)은 아일랜드에 자회를 설립한 후 연구개발비의 일부만 받기로 하고 지적재산권을 자회사에 이전한다. 이 자회사는 직접 영업을 하지 않고 100% 자회사를 만들어 지재권을 사용하는 영업을 유럽과 아프리카에서 수행하도록 한다. 이때 네덜란드에 세 번째 자회사를 만들어 지재권의 사용과 그 사용료를 중개하는 역할을 맡긴다. 아일랜드 세법 및 조세조약에 따라 EU 역내의 모회사나 자회사에 지급한 사용료에 대해 원천과세를 하지 않는 것을 이용한 편법이다. 그 결과 대부분의 국외 영업이익은 구글이 아일랜드에 처음 만든 자회사에 쌓이지만 아일랜드 세법상 미국 본사(버뮤다에 설립된 또 다른 구글 자회사)의 지배를 받는 비거주자로 취급되므로 아일랜드에서 법인세를 신고 납부할 필요가 없는 것이다. 안종석, "다국적 IT기업의 조세회피 행태와 시사점: 애플·구글의 사례를 중심으로", 재정포럼 2013.7, 8～10면.

앱 판매액과 유튜브 동영상 광고 매출, 검색 광고료 등으로 2조 원 이상의 매출을 올리는 것으로 추정된다. 그럼에도 한국 내 구글 매출액은 광고 판촉만 벌이는 구글 코리아가 아닌 법인세가 낮은 싱가포르 소재 구글 아시아퍼시픽의 수입으로 잡히며, 최종적으로는 법인세율이 낮고 조세감면 혜택도 많은 아일랜드에서 세금을 내는 것으로 되어 있다. 정부는 2017년 1월 구글을 비롯한 다국적 기업의 현지 세금회피를 막기 위해 비상장 유한회사의 경영내용을 공시하도록 하는 관련법 개정안을 발의했지만 법안 심리는 무기한 연기된 상태이다.[18]

그러나 현지에 서버를 구축하게 하는 FLMs 정책이 단기적으로는 데이터 센터의 설치, 정보통신 기술직 채용의 증가를 가져와 지역경제에 도움이 될 수 있을 것이다. 그러나 장기적으로는 정보흐름의 단절은 외국인투자 의욕을 저상시키고 유망한 프로젝트에 대한 외국 기업과의 협력사업을 방해하는 등 역효과가 더 크다는 비판도 만만치 않다.[19]

4. 국내기업의 역차별 방지

우리나라의 경우 한·미 FTA에서 미국은행 고객의 금융거래 정보를 해외에서 처리하는 문제를 둘러싸고 논란이 많았다. 그 결과 한·미 FTA 제13부속서에서 각 당사국은 상대국의 금융기관이 일상적인 영업과정에서 개인정보의 처리가 요구되는 경우 그의 처리를 위해 자국 영역 안과 밖으로 정보를 전자적 또는 그 밖의 형태로 이전하는 것을 허용하기로 했다. 다만, 금융정보의 해외이전을 허용한다고 하여 금융정보의 생성·저장을 위한 IT 설비, 금융 전산망 등 본질적 요소들의 해외 이전까지 허용하는 것은 아니다.[20]

한편 구글은 구글 맵 제작을 위해 2007년부터 공간정보의 반출을 줄곧 요구해 왔다. 2016년에도 정식으로 공간정보 반출을 요청하여 외국인투자 담당 부처에서는 긍정적인 의견을 보였으나[21] 최종적으로 국가안보에 지장을 줄 수 있고, 이를

---

18) 조선일보, "한국 게임으로 1兆 챙긴 구글… 세금은 '깜깜'", 2017.9.15; Insight, "'구글', 국내서 2조 버는데 세금은 한 푼도 안 낸다", 2017.5.15. <http://www.insight.co.kr/newsRead.php?ArtNo=105579>

19) Albright Stonebridge Group, *Data Localization*, p.7.

20) 박훤일, 「개인정보의 국제적 유통에 따른 법적 문제와 대책」, 집문당, 2015, 177~178면.

21) Google Maps가 전 세계적으로 관광산업 및 무인자동차 사업에 널리 이용되고 있음에

허용하면 엄격한 보안규정을 적용받고 있는 국내기업들에 대한 역차별이 된다는 이유에서 국내 서버 설치를 조건으로 내걸었다. 그러나 해외의 클라우드 서비스를 이용하고, 앞서 설명한 바와 같이 글로벌한 관점에서 세금을 줄이려는 구글 측이 이를 거부함으로써 그 해 11월 최종 불허 결정이 내려졌다.[22]

5. 클라우딩 서비스의 이용 추세에서 U턴

세계적인 데이터 로컬라이제이션 추세와는 반대로 우리나라에서는 클라우드컴퓨팅 도입은 이제 거스를 수 없는 대세가 되었다.[23] IT 기업은 물론 가장 보수적인 은행들도 클라우드 도입에 적극적이다. 인공지능(AI)과 사물인터넷(IoT), 빅데이터 등 클라우드 인프라 및 플랫폼이 각광을 받으면서 클라우드 도입율도 현재의 20%대에서 크게 높아질 것으로 보인다.[24] 아마존 같은 해외 클라우딩 서비스 업체를 이용할 경우 데이터는 해외에 소재하는 서버에 보관될 것이다.

금융권에서도 챗봇과 같은 AI 기반 신기술 수용 사업을 클라우드 기반에서 운영하는 사례가 늘고 있다. KB국민은행의 경우 2017년 9월에 오픈한 대화형 뱅킹 플랫폼 '리브똑똑'에 아마존 웹서비스의 인프라를 이용하고 있으며, 신한금융그룹도 오는 11월부터 아마존의 음성인식 AI를 통해 파일럿 서비스를 개발하기로 했다.

제조업체들은 스마트 팩토리와 관련하여, 의료부문은 정밀의료나 원격진료 등

비추어 공간정보 분야 국내기업의 경쟁력 향상과 외국인투자를 통한 기술제휴 및 협업을 기대할 수 있다는 의견도 있었지만, 그 효과는 일부 하청업체에만 해당되고 장기적으로는 기술종속의 우려가 있다는 반론도 만만치 않았다. 오마이뉴스, "구글의 지도 국외반출 요구에 포털·네비 업체 '역차별' 반발", 2016.6.20. <http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0002219482>

22) 2016년 11월 18일 경기도 수원 국토지리원에서 열린 기본측량성과 국외반출협의체 3차 회의에서 협의체는 국가안보를 이유로 구글의 기본측량성과 반출 요청에 대해 불허 결정을 내렸다.

23) 일반적으로 외국에 있는 클라우드컴퓨팅 서비스 업체의 약관에 동의하는 방식으로 서비스 이용이 개시되나 개인정보가 포함되어 있는 경우에는 개인정보보호법, 정보통신망법과 관련하여 주의를 요한다(클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제4조).

24) 디지털 데일리, "[주간 클라우드 동향] 2017 국내 클라우드 도입, 어디까지 왔나", 2017.10.16. <http://www.ddaily.co.kr/cloud/news/article.html?no=161209>

여러 분야에서 클라우드 서비스 및 기술의 도입을 적극 검토하고 있다. 클라우드 주무부처인 과학기술정보통신부에서도 전국 산업단지에 입주한 기업을 대상으로 다양한 클라우드 서비스 요금을 최대 70%까지 지원해 중소 규모 제조기업의 경쟁력을 높이기로 했다. 조달청 나라장터의 종합쇼핑몰에도 2개의 클라우드 인프라 서비스(IaaS)가 정식 등록됨에 따라[25] 클라우드 서비스가 확대될 전망이다.

이에 따라 국제적인 정보유통에 로컬라이제이션이라는 장벽이 설치된다면 경제적으로 심각한 타격을 주게 될 것임이 틀림없다. 미국의 IT분야 씽크탱크인 ITIF (Information Technology and Innovation Foundation)에 의하면 미국에서는 데이터 로컬라이제이션의 결과 GDP가 0.1~0.36% 줄어드는 효과가 발생할 것으로 전망했다. 이미 데이터 현지화법을 시행하고 있는 브라질, 중국, EU, 인도, 인도네시아, 한국, 베트남에서도 정도의 차이는 있지만 GDP가 0.7~1.7% 감소할 것으로 내다보았다.[26]

Ⅲ. 주요국의 사례

이하에서는 위에서 설명한 정책적 동기에 비추어 우리나라가 참조할 수 있는 데이터 현지화를 의무화하고 있는 중국, 베트남, 인도네시아, 인도, 러시아 등의 FLMs 규제 현황과 대응책을 살펴보기로 한다.

---

25) IaaS (Infrastructure as a Service)란 서버, 네트워크 장비, 스토리지 등 인프라 자원을 구매하지 않고 인터넷을 통해 서비스 형태로 임대해 이용하는 서비스를 말한다. 조달청의 종합쇼핑몰 나라장터에는 NAVER 비즈니스플랫폼과 케이티가 IaaS를 클라우딩으로 제공하는데 이를 이용하려면 KISA가 발급하는 보안 인증을 받아야 한다. IaaS 사용료는 서비스를 사용한 만큼 청구되며, 웹 방화벽, 데이터관리시스템(DBMS), 백업 등 부가서비스도 함께 제공된다. 전자신문, "'나라장터에서 인프라 클라우드 서비스 이용하세요", 2017.9.27. <http://www.etnews.com/20170927000385>

26) Stuart Lauchlan, *op.cit.*, <http://diginomica.com/2017/05/03/data-localization-rules-damage-global-digital-economy-says-us-tech-thinktank/>

1. 중국

가. 규제의 현황

중국은 거대한 인구를 기반으로 알리바바, 바이두, 탄센트와 같은 세계적인 IT 대기업을 둔 나라이지만 개인정보 보호에 관한 한 국제적인 흐름에 크게 뒤져 있다. 그런데 스노든 사건 이후 중국 정부가 국가안보법(国家安全法)과 테러방지법의 제정을 서두르면서 개인정보 보호 관련 규정을 마련하여 주목을 받았다. 지금까지 개인정보 보호를 위한 포괄적인 법 규정이 시행된 적이 없기에 이들 법안에 들어 있는 개인정보보호에 관한 규정과 다른 한편으로는 이를 제약하는 규정들이 관심을 끌었다.

중국의 입법기관인 전국인민대표대회(全国人民代表大會)[27]는 2016년 11월 7일 인터넷에 대한 통제를 강화하고 네트워크 설비와 시설, 정보데이터 등에 관한 보안조치 등을 망라한 네트워크 안전법(中国网络安全法, PRC Cybersecurity Law)을 채택했다. 새 법률은 준비기간을 거쳐 2017년 6월 1일부터 시행되었다.[28] 미국의 스노든 사건이 계기가 되었지만 사이버보안을 이유로 국가기관에 대한 정보제공 및 기술협력 의무, 데이터의 로컬라이제이션 등 개인정보 보호가 뒤로 밀리는 현상이 벌어지게 된 것이다.

네트워크 안전법의 초안은 2015년 6월 발표되었고, 이후 두 차례의 심의 및 의견수렴 과정을 거쳤다. 2016년 6월 진행된 제2차 심의 및 의견수렴 과정을 거친 최종안에는 인터넷 범죄에 대한 처벌 내용을 담은 4개 조항이 추가되었으며, 이후 최종안은 수정 없이 통과되었다.

나. 주요 내용

① 중국의 네트워크 안전법과 개인정보보호 이슈

네트워크 안전법의 입법 취지는 인터넷 공간의 주권과 국가안보의 유지, 공민과

27) 중국 전국인민대표대회는 중국의 형식상 최고 권력기관으로서 22개 성·자치구·직할시, 홍콩(香港)·마카오(澳門) 특별행정구(特別行政區), 인민 해방군에서 선출되는 대표로 구성된다.

28) 개인정보보호포럼·한국인터넷진흥원, 「지능정보사회 선도를 위한 개인정보보호 이슈 및 동향」, 2017. 2.

법인 및 기타 조직의 합법적 권익을 보호하기 위한 것이다. 이 법은 사이버 공간에서의 프라이버시와 보안 관련 사안에 대해 포괄적으로 다룬 중국 최초의 법규라는 점에서 의의가 있다. 개인정보를 비롯한 데이터의 보안을 강화한 측면도 있으나 시민들의 온라인 활동에 대한 감시 및 해외기업에 대한 차별을 가져올 수 있는 규정을 포함하고 있다.

중국 네트워크 안전법은 중국 내 정보통신망의 구축·운영·유지보호·사용 및 그의 보안에 대한 감독 및 관리와 관련된 사항을 규정하고 있다. 이에 따라 개인 컴퓨터를 비롯한 정보 단말기부터 온라인 서비스 제공 기업에 이르기까지 인터넷과 관련된 제반 영역이 규제의 대상이다.

네트워크 안전법은 △총칙(总则), △네트워크 보안 전략·기획·촉진(网络安全支持与促进), △네트워크 운영 보안(网络运行安全), △네트워크 정보 보안(网络信息安全), △모니터링 경보와 응급조치(监测预警与应急处置), △법적 책임(法律责任), △부칙 등 총 7장 79조로 구성되어 있다.

네트워크 안전법은 '핵심 정보통신 기반시설(關鍵信息基礎施設, Critical Information Infrastructures: CII)' 운영자에게 엄격한 책임과 의무를 부과하고 있다. 이 법 제31조에서 '핵심 정보통신 기반시설'이란 에너지, 교통, 수리시설, 금융, 의료, 방송, 공공서비스, 전자정부 등 국가 중점시설 분야와 네트워크의 기능 파괴 또는 데이터 유출 시 국가안전과 공공이익에 영향을 미치는 정보통신 시설을 의미한다'고 정의하였다. 주요 정보통신 기반시설의 운영자는 각종 보안심사와 안전평가를 받아야 하며, 제37조에서는 중국에서의 사업수행 과정 중 수집되거나 창출된 중국 국민들의 개인정보(Citizens' Personal Information)와 중요 데이터(Important Data)는 반드시 중국 현지에 소재한 서버에 저장하도록 의무화하고 있다. 그러나 합법적인 사업상의 이유로 인해 이 같은 데이터를 중국 외부에 있는 해외 법인이나 조직 등에게 제공해야 하는 경우에는 중국의 사이버보안관리 당국 및 중국 국무원이 공동으로 마련한 보안평가(Security Assessment)[29]를 거치면 된다.

---

29) 네트워크 안전법에는 보안평가의 의미와 구체적인 내용이 명시되어 있지 않다. 당초 데이터 현지화 의무도 국내외 비판이 일자 모든 네트워크 운영자에서 CII로 범위를 좁혔는데 최종 시행시기도 18개월 연기한 것으로 알려졌다. Adam Golodner, et al., China's New Cybersecurity Law Imposes Heightened Restrictions on Company Computer Networks, Arnold Porter Kaye Scholer, July 20, 2017.

② 네트워크 안전법과 개인정보보호 관련 사항

네트워크 안전법은 중국 정보통신산업부(MIIT)가 2011년 12월 정보통신망 보호 규정을 제정한 이래 정부 차원에서 추진해 온 개인정보 보호의 원칙을 법률로써 구체화한 성과물이라 할 수 있다.[30] 특히 개인정보 보호와 관련하여 다음 사항들을 규정함으로써 개인정보 보호에 관한 의지를 표명하고 있다.

- 네트워크 운영자가 법규를 위반하거나 개인정보 수집·이용과 관련한 계약사항을 위반한 경우 정보주체가 해당 운영자에게 개인정보의 삭제를 요구할 수 있고, 수집되거나 저장된 정보에 오류가 있을 때에는 이에 대한 수정을 요구할 수 있다(제43조).
- 개인이나 조직은 개인정보 획득을 목적으로 불법적인 수단을 동원하거나 개인정보를 절취해서는 안 되며, 개인정보를 제3자에게 불법적으로 판매하거나 불법적으로 제공해서는 안 된다(제44조).
- 네트워크 보안 감사 및 관리 의무를 가진 조직이나 담당자는 업무과정에서 획득한 개인정보와 상업적 비밀 정보에 대해 엄격한 보안을 유지해야 하며 제3자에게 이를 누설, 판매 또는 불법적으로 제공해서는 안 된다(제45조).

이 법은 기존 법령에 비하면 진일보하여, 이른바 글로벌 스탠더드라 할 수 있는 개인정보 침해 사실의 이용자에 대한 고지의무를 규정하였고 벌칙도 다소 강화되었다. 그러나 이용자의 정보열람권, 정보의 질(quality)이나 민감정보에 관한 규정은 빠져 있으며, 개인정보 보호와 감독을 담당하는 국가기관도 명시되어 있지 않다.[31] 더욱이 중요 정보의 국내 처리·보관을 의무화하고 정보의 반출을 규제하고 있어 국제적인 흐름에 역행하고 있다.

입법취지를 보더라도 네트워크 안전법은 온라인상에서의 검열과 통제를 크게 강화하고 있으며, 인터넷 활동에 대한 정부의 개입을 합리화하고 있는 것이 특색이다.

- 네트워크 안전법은 인터넷 서비스 제공업체에 대해 온라인 서비스를 제공하는 계약관계를 맺을 때 반드시 실명정보(real identity information)를 요구하도록 했다.

---

30) Graham Greenleaf and Scott Livingston, “China’s Cybersecurity Law – also a data privacy law?”, Privacy Laws & Business International Report, December 2016, p. 7.

31) *Ibid*., p. 3.

- ○ 인터넷 서비스 제공업체 등이 당국에 기술 제공과 수사에 협력하도록 의무화하고, 사용자가 게시한 정보에 대한 관리를 강화해 불법정보 발견 시 전송 중단, 제거, 확산 방지, 기록 보관 등의 조치를 수행하고 유관기관에 보고하여야 한다.
- ○ 인터넷 서비스 제공업체는 수사기관에 대해 의무적으로 협조하도록 했으며 주관부처는 국가안보, 사회질서 유지 등을 위해 인터넷 서비스 제공업체에게 그 사용을 제한하는 임시조치를 내릴 수 있다.
- ○ 네트워크 로그 기록은 데이터 보관 규정에 따라 6개월 이상 보관하여야 한다.
- ○ 국가는 네트워크 운영자들이 네트워크 안전에 관한 정보를 수집·분석·신고하고 대응능력을 증진함에 있어서 상호 협력하는 것을 지원한다.

또한 네트워크 안전법은 법적 책임을 규정하는 제5장에서 법인이나 이와 관련된 책임자가 해당 법률조항을 준수하지 않을 경우 경고, 과징금 부과, 부당이익 환수, 영업정지, 사업면허 박탈 등의 처벌을 가할 수 있도록 규정하고 있다.

네트워크 보안책임 등을 이행하지 않은 경우 1만 위안~10만 위안의 과징금이 부과되며, 직접적인 관리 책임자에 대해서는 5천 위안~5만 위안의 과징금이 부과된다.

그 밖에 제59조부터 제75조에서는 다양한 상황에 대한 법적 책임을 부여하고 그에 상응한 과징금을 규정하고 있다.

③ 중국의 네트워크 안전법과 데이터의 로컬라이제이션 이슈

시진핑 정부에서는 사이버보안을 강조하면서 개인정보의 국내 보관·처리를 의무화할 것으로 예견되었다. 연혁적으로 중국 정부는 국가기밀이나 일정한 금융정보, 의료정보 같은 민감정보는 외국으로 이전하거나 외국에 보관하는 것을 금지시켜 왔다. 명백히 데이터의 국내 보관·처리를 의무화한 것은 아니었지만 그러한 효과를 가져오도록 만들었다.

최근 들어서 중국 정부는 적극적으로 광범위한 개인정보 법제의 중요한 구성요소인 전자정보의 국내 보관·처리를 의무화하고 있으며, 이러한 취지로 네트워크 안전법 규정이 마련되었다. 중국이 이처럼 민감하게 반응한 것은 에드워드 스노든이 미국 정보기관의 PRISM 첩보수집을 폭로한 것을 계기로 중국 공산당이 사이버보안을 강조하였기 때문이다. 그 당시만 해도 국가의 기간전산망이 외국 업체에 의존하는 사례가 적지 않았다. 스노든 폭로를 계기로 중국은 인터넷 정책

결정기구를 정비하고 시진핑 주석을 위원장으로 하는 중앙 사이버보안 및 정보화 지도소조(中央网络安全和信息化领导小组, Central Leading Group for Cybersecurity and Informatization)를 설치하였다. 인터넷 정책을 총괄조정하는 중앙정부 조직(国家互联网信息办公室, Cyberspace Administration of China: CAC)도 만들었다.

그러니 이들 정부조직이 사이버 주권을 강조하면서 영토 안에서 전송되는 인터넷 콘텐츠를 감독하고 통제하는 권한을 갖는 것은 당연한 귀결이었다. 그러니 인터넷 정책은 국내에서 외국 기술이 안전하고 통제 가능할 것을 요구함과 아울러 정부의 통제와 감독을 기반으로 하는 것이었다. 그 중심은 인터넷 정보를 국외로 이전하는 것을 금하고 국내에 보관하도록 하는 정보처리의 로컬라이제이션였다.

전통적으로 중국의 인터넷 법령은 정보의 국외 이전을 금하고 일정한 민감정보는 국내에 저장하도록 했다. 중국 국가기밀법(国家机密法, China Secrets Law)에서 광의로 정의되는 국가기밀(State Secrets)의 국외이전은 금지되었다. 최근에는 산업별로 특화된 규정이 신설되어 다른 유형의 민감정보를 여기에 포함시켰다.

- ○ 중국 인민의 개인신용정보의 해외 처리·저장을 금지하는 2011년 은행 및 금융기관의 개인정보 보호를 촉구하는 중국인민은행 통지[32]
- ○ 은행업무의 사이버 안전보장 능력과 정보화 건설 수준을 향상시키도록 하는 안전하고 제어가능한 정보기술을 응용한 은행업 네트워크 보안 및 정보화 건설 강화에 관한 지도의견[33]
- ○ 개인정보의 국외이전에 정보주체의 동의를 요하는 2013년 자율적 가이드라인[34]
- ○ 중국에서 수집된 인구 건강정보의 국외 저장을 금지하는 2014년 전인민 건강정보 관리조치[35]

---

32) 中国人民银行关于金融机构进一步做好客户个人金融信息保护工作的通知(Notice of the People's Bank of China on Urging Financial Institutions to Further Effectively Protect Clients' Personal Financial Information) 2011.

33) 2014년 9월 중국은행업감독관리위원회(CBRC), 국가발전개혁위원회, 과학기술부, 공업정보화부가 공포한 关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见(文書番号: 銀監発 [2014] 39号) <http://www.cbrc.gov.cn/govView_115696B8621049099A0B880DAB133A33.html>

34) Information Security Technology - Guidelines for Personal Information within Public and Commercial Services Information Systems 2013.

④ 중국의 FLMs 규제에 대한 외국의 반응

2014년 테러방지법안에서도 국내에서의 정보처리 및 보관을 요구하였다. 이에 따르면 인터넷 콘텐트 제공자, 즉 웹사이트 또는 스마트폰 앱은 정부가 접속할 수 있는 백도어[36]를 만들고 비밀 암호키를 공안당국에 제출하도록 했다. 더욱이 이 법안에서는 이들 사업자가 중국 내에 서버를 설치하고 국내 이용자들의 모든 데이터를 보관하도록 했다.

그러자 새 법률안의 의무사항은 외국 정부나 무역단체의 반발을 불러일으켰다. 미국의 오바마 대통령은 시진핑 주석과 회담할 때 심각한 우려를 표명했다. 이에 따라 중국 정부는 2015년 12월에 제정한 테러방지법(恐怖活动防止法, PRC Anti-Terrorism Law)에서는 논란이 많았던 일부 조항을 삭제하거나 수정했다. 최종적으로 데이터의 국내 보관·처리 조항이 전부 빠졌고, 암호화 요건도 완화되어 공안당국이 요청하면 인터넷 콘텐트 사업자가 암호화 키를 곧바로 제공하는 대신 기술적 지원을 하도록 완화했다.

네트워크 안전법에서도 정보의 국내 보관·처리를 의무화하는 조항이 들어갔다. 테러방지법에서 이러한 조항이 빠졌으나 전국인민대표대회에서는 네트워크의 안전을 도모하고 사이버공간에서의 주권을 확보하기 위해서는 중요 정보의 국내 보관·처리가 긴요하다고 여겼다. 그리하여 중요정보 인프라(CII) 운영자는 중국 국내에서 운영하고 수집·생성된 개인정보 및 중요 데이터는 중국 국내에서 보관하도록 하고, 업무의 필요성에서 국외로의 제공할 필요가 있는 경우 국가 네트워크 정보부문은 국무원 관련부서에서 제정한 방법에 따라 보안성 평가를 받도록 했다. 법률, 행정법규로 별도의 규정이 있는 것은 그 규정에 따른다(제37조). 하지만 막판에 이 조항의 시행시기를 늦춘 것으로 알려졌다.

네트워크 운영자는 치안 및 국가안전 담당기관이 법에 의하여 국가의 안전유지 또는 범죄수사 활동을 함에 있어 기술적 지원과 협력을 하여야 한다(제28조).

그 밖에 온라인 출판, 자동차 함께 타기(ride sharing), 인터넷 지도 서비스, 인터넷 뱅킹·증권 서비스도 관련 규정에 따라 이용자의 개인정보를 중국 내에 보관·처리할 것을 요구하고 있다.

---

35) 人口健康信息管理办法-试行 (Measures for Administration of Population Health Information – Trial Implementation) 2014.

36) 백도어(back door)란 제품, 컴퓨터 시스템, 암호시스템 등에서 정상적인 인증 절차를 우회하여 정식 승인을 받지 않고 시스템에 접속하는 것을 말한다.

요컨대 중국 네트워크 안전법은 온라인 데이터의 해외 이전 및 저장에 대한 제약(FLMs)을 강화하고 개인정보 보호를 위한 규정을 명시한 점에서 주목된다.

중국 정부는 스노든의 폭로로 드러난 사이버 위협의 증가 추세를 이유로 사이버보안 강화 및 온라인 정보에 대한 주권 강화의 필요성을 역설하고 있다. 이것은 현재도 중국 정부가 사이버 공간에서 취하고 있는 여러 조치들의 법적인 근거를 마련한 것이라 볼 수 있다. 개인정보 보호와 관련하여 글로벌 스탠더드에 따라 정보주체의 권리를 명시하는 등 진일보한 측면도 있으나 개인의 정보통신망에서의 활동에 대하여 정부의 검열을 강화하겠다는 의지를 표명하고 있다. 중국 내 정보통신망을 통해 세계 최대의 온라인 시장에 접근하려는 외국의 기업들로서는 여러 채널을 통해 FLMs는 기업활동을 크게 제약하고 중국경제의 발전에도 유익하지 않다는 점을 설득하는 한편[37] 이 법률의 주요 개념과 규제·시행에 관한 사항, 그에 따른 효과를 관심 있게 지켜볼 필요가 있다.

2. 베트남

가. 규제의 현황

베트남에서는 다음과 같은 법령에 의하여 서버의 국내설치 의무가 규정되어 있다.

① 인터넷 통화, SM서비스의 제공 및 이용의 관리에 관한 규정(OTT통달)

2013년 이후 인터넷을 이용한 통화·메시지(Over the Top: OTT)[38] 서비스가 발달함에 따라 정보통신부가 처음으로 OTT에 대한 규제를 도입하기로 했다. 업계의 의견수렴도 끝났으나 아직 정식으로 조문화되어 되어 있지는 않다. 현지 OTT 사업자와 단체들이 일관되게 반대를 하고 있어 통달의 시행 여부는 불투명한 실정이다.

---

37) 野村総合研究所,「ＥＵとの規制協力：サイバー空間及びIoTに係る規制等に関する調査報告書」, 2017.3, 14面.

38) Over the Top에서 Top은 TV셋톱박스 같은 단말기를 뜻하므로 OTT는 셋톱박스 같은 단말기를 넘어서서 인터넷과 모바일을 이용한 영화·방송·교육 등 각종 미디어 콘텐츠를 제공하는 서비스를 말한다.

통달의 주요 내용은 다음과 같다.[39]

- 국내법인은 OTT 서비스 사업인가를 받은 경우에 한하여 유상으로 서비스를 제공할 수 있다.
- 유상의 OTT 서비스를 제공하는 해외사업자는 (i) 유상으로 OTT 서비스 제공에 관한 사업인가를 취득한 베트남 국내사업자와 계약을 체결하거나 (ii) 베트남 국내에 최소한 하나의 호스트 서버를 설치하고 유상으로 OTT 서비스 제공에 관한 사업인가를 취득한 베트남 국내의 사업자와 업무협약을 체결하여야 한다.
- 무상으로 OTT 서비스를 제공하는 사업자는 국내/해외 사업자와 사업인가를 취득할 필요가 없으나 서비스 가입 이용자 수가 100만을 초과하는 경우에는 그 사업자는 정보통신부(MIC)에 대하여 본사의 소재지, 도메인이름, 호스트서버의 주소, 취급 통화/메시지 수 등의 정보를 제공하여야 한다.
- 인터넷 서비스 제공자는 OTT 서비스 제공자와 그 이용자를 방해해서는 아니된다.

② 정보기술 서비스 정령

베트남 정보통신부(MIC)가 IT기기·서비스에 대한 승인·등록, 데이터의 현지보관을 의무화하는 정령의 제정을 추진하고 있다.

③ 정령 72호(No.72/2013/ND-CP)

베트남에서는 2013년 정령 72호에 따라 일반 웹사이트나 사회관계망 웹사이트를 서비스하는 사업자는 베트남에 감독당국의 검사를 받는 하나 이상의 서버를 두어야 한다.[40] 데이터 보관의 요건은 일반 웹사이트의 경우 적어도 일반 정보를 사이트에 게시된 날로부터 90일간, 처리된 정보의 로그 기록은 2년 이상 보관하여야 하며, 사회관계망 웹사이트의 경우 계정 및 로그인-로그아웃 시간, 이용자의 IP주소, 처리된 정보의 로그 기록을 2년 이상 보관하여야 한다. 그리고 테러,

39) 노무라 종합연구소, 앞의 보고서, 15면.

40) 정령 72호의 적용범위는 아주 광범위한 바, 베트남에서 등록하고 운영하는 기업은 물론 베트남 밖에 소재하더라도 베트남 이용자들에게 서비스를 하거나 베트남어로 서비스하거나, 베트남 도메인 주소(.vn)를 쓰거나 베트남과 어떤 형태로든 관련이 있는 사업자들이 그에 해당한다.

범죄, 위법행위와 관련이 있는 이용자에 대해서는 관할 행정청의 요구가 있으면 그의 인적 사항과 사적인 정보를 제공하여야 한다.[41]

2015년에는 공개정보의 국경간 제공을 규율하는 통달[42]의 시안이 공표되었다. 여기서 공개정보의 국경간 제공이란 외국의 기관, 기업 또는 개인이 외국에 하드웨어를 설치하거나 외국의 클라우딩 서비스를 이용하여 베트남 국내 이용자에 대하여 뉴스 웹사이트, 소셜네트워킹, 검색엔진, 이용자가 열람 또는 다운로드할 수 있는 공개정보에 관한 앱 또는 그와 유사한 것을 제공하는 것을 말한다. 이에 따라 뉴스 사이트, 검색엔진 등을 국외의 하드웨어 또는 클라우딩 서비스를 통해 운영하는 경우, SNS 가입 회원이 5천명을 넘을 경우에는 법적인 대표자를 베트남 국내에 두어야 한다.

예외적으로 순전히 상업적인 웹사이트로서 특성화된 응용(specialized application) 사이트인 경우에는 데이터 처리 및 보관의 현지화 의무가 없다. 통신, 정보기술, 방송, 텔리비전, 상거래, 금융, 은행, 문화, 헬스케어, 교육 기타 일반적인 정보제공이 아닌 전문 분야에 속한 웹사이트가 이에 해당한다.[43]

나. 국내외의 반응

베트남 IT업계에서는 정부의 현지화 정책에 반대의 입장을 분명히 하였다. 이러한 규제는 베트남 산업의 경쟁력을 떨어트리고 규제가 없는 싱가포르 등지로 떠나기 때문에 산업 공동화가 우려된다는 의견을 내놓았다. 이와 관련하여 구글, 이베이 등 미국계 대형 OTT 사업자들도 맹렬히 반대 로비를 펼치고 있다. 다만, 현지법인의 설립을 의무화하는 것에 대하여 외국의 OTT 사업자들이 납세를 회피하려고 반대하는 게 아닌가 하는 의혹을 사고 있다.[44]

요컨대 베트남의 FLMs 조치는 크게 국방과 사상통제, 과세, 국내산업의 육성

41) Scott Livingston and Graham Greenleaf, “Data localisation in China and other APEC jurisdictions”, *Privacy Laws & Business International Report* Issue 143, October 2016, pp. 22-26.

42) Draft circular on detailed regulation on cross border provision of public information (No.72/2013/ ND-CP)

43) Livingston and Greenleaf, *op.cit*.

44) 베트남에서 서버의 현지설치 의무화 등 FLMs에 관한 집행사례는 아직 없다. 노무라 연구소, 앞의 보고서, 18면.

세 가지 측면에서 살펴볼 필요가 있다. 국방·사상통제에 관하여는 국방부가 적극적인 반면 정보통신부, 산업무역부에서는 베트남 경제에 도움이 되지 않는다는 이유에서 이에 소극적이다. 과세 문제는 비단 베트남에 한하지 않고 국가 간의 전자상거래 전반에 관하여 제기되고 있으므로 국제적 논의의 추이를 보아가며 해결될 전망이다. FLMs와 관련 산업의 육성은 산업공동화를 초래할 수 있다는 점에서 특히 주목을 요한다. 베트남에 진출하려는 국내기업이 늘어나는 추세인 만큼 우리 정부 차원에서도 기술 및 자금협력을 함에 있어서 FLMs가 상호간에 득이 안 된다는 것을 설명하고 베트남 측의 이해를 구해야 할 것이다.

3. 인도네시아

가. 규제의 현황

① 전자시스템과 거래조직에 관한 규정(2012년 정부규정 제82호)[45]

인도네시아 2012년 정부규정 제82호에 따르면 공공서비스 전자시스템 관리자는 데이터 센터를 법 집행 및 국가주권의 보호와 집행을 목적으로 반드시 인도네시아 국내에 두어야 한다. 공공 서비스와 관련된 정보 외에도 건강정보는 보건부장관이 관리하는 데이터 센터와 연결되어 있는 국내의 데이터 센터에서 처리해야 한다. 보건부장관의 허가가 있으면 외국에서도 처리할 수 있다. 이러한 현지화 정책은 경제발전에 도움이 안 된다는 반론도 있었으나 공공의 이익을 위한 것이라는 주장에 묻혀버렸다.[46]

② 통신정보부 규정(2015년 정부규정 제27호)[47]

4G 스마트폰에 대하여 30~40%의 로컬 콘텐츠를 싣도록 하였다. 이 규정에 의하면 인도네시아에서 제조·이용 또는 수입된 LTE 제품에 대하여 다음과 같은

45) Organization of Electronic Systems and Transactions Regulation (82/2012)

46) Livingston and Greenleaf, *op.cit*.

47) Regulation No. 27 of 2015 regarding Technical Requirement of Equipment and/or Telecommunication Devices in Long Term Evolution Technology Basis (Permenkominfo 27/2015)

로칼 콘텐츠 요구를 충족하여야 한다. 기지국의 송신기는 30%, 스마트폰 수신기는 20%에서 시작하여 2017년부터는 각각 40%, 30%로 인상되었다. 여기서 로칼 콘텐츠는 소프트웨어를 포함하므로 현지 업계는 반기는 분위기였다.

③ 개인정보보호법

2015년 7월 정부기관에 대한 개인정보보호 규정이 공포되었다. 인도네시아에서는 개인정보보호에 관한 일반법은 없고 개별 법령에 개인정보보호에 관한 조항이 들어 있다. 일반 사업자에 대한 규제는 아직 검토된 바 없다.

④ OTT 규정

인도네시아에서도 OTT 서비스가 발전함에 따라 정부가 새로운 규제를 내놓았다. 외자계 기업에 관해서는 OTT 서비스를 제공할 때 인도네시아 국내에 항구적 시설(BUT)을 설치할 의무가 부과되었다. 이는 외자계 기업의 OTT 서비스 제공에 따른 영업수익에 과세를 하기 위한 것으로 풀이된다.

나. 국내외의 반응

인도네시아의 경우 데이터 현지화에 관한 법규정이 복잡하고 예외 규정이 많으므로 현지기업들이 많이 참여하는 업계단체를 통하여 사정을 파악하는 경우가 많다. 아직은 기업에 대한 FLMs 집행사례도 많지 않다. 인도네시아 정부 역시 과도한 FLMs는 인근 싱가포르 등지로 기업들이 빠져나갈 가능성을 염두에 두고 있는 것 같다.

현지 기업들은 대체로 정부의 FLMs 시책을 지지하고 있으며, 스마트폰의 로컬 콘텐츠 요구에 대해서도 적극적으로 받아들이고 있다.

그러나 외국 기업을 비롯하여 일부 현지 기업들은 해외의 클라우드 서비스를 이용하여 사업을 벌이고 결제를 하는 만큼 지나친 FLMs에 반대하는 입장을 보이고 있다.

4. 유럽연합(EU)

가. 규제의 현황

① 제3국의 적절한 개인정보 보호 수준

유럽연합(European Union: EU)에서 역내에서 데이터를 보관·처리해야 하는 경우란 개인정보 이전 대상인 정보처리자가 속한 나라의 개인정보 보호의 수준이 EU 기준에 비추어 적절하지 못할 때이다. 이에 관한 근거는 EU 개인정보보호지침(Data Protection Directive 95/46/EC) 제25조 및 제26조이다. EU 회원국의 개인정보감독기구들로 구성되어 있는 개인정보보호작업반(Article 29 Working Party)에서는 동 규정에 따른 실무작업보고서(Working Document)[48]에 열거되어 있는 12가지 기준[49]에 비추어 적절한 보호 수준(adequate level of protection)인지 여부를 평가하게 된다. 이 기준은 GDPR 제45조에도 그대로 반영되어 있어 GDPR 시행 후에도 정기적으로 재심사를 받는 것 외에는 당분간 계속 적용될 것으로 보인다.

그러므로 개인정보를 수집하고 이를 보관·처리하는 기업이라면 EU에서 요구하는 개인정보 보호의 안전대책(safeguards)을 갖추지 못한 경우[50] 정보를 역외로 반출할 수 없으므로 현지에 서버를 둘 수밖에 없다. EU 입장에서는 EU 역내 시민들의 프라이버시권을 보장하고 미국계 다국적 기업에 의한 정보의 지배를 막기 위한 고육지책이라 할 수 있다. 스노든이 폭로한 대로 미국 정보당국이 독일, 브라질 등 외국 정상의 통화를 감청하고 있었던 상황에서 다른 대안이 없었던 것이다.

---

48) Article 29 Working Party, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf>.

49) 12개 기준은 다음과 같다: 1) 기본원칙 ① 목적제한의 원칙 ② 정보의 질, 비례성의 원칙 ③ 투명성의 원칙 ④ 안전성의 원칙 ⑤ 열람·정정·거부의 권리 ⑥ 제3자 전송 제한 2) 추가기준 ⑦ 민감정보 ⑧ 다이렉트 마케팅의 제한 ⑨ 자동화된 의사결정 3) 절차/집행/구제의 방법 ⑩ 양호한 수준의 준수 ⑪ 정보주체에 대한 지원 ⑫ 피해자에 대한 적절한 구제

50) 이러한 안전조치에는 자율규제와 표준계약서, 구속력 있는 기업규칙(Binding Corporate Rules: BCRs) 등이 있다. 미국은 EU와 세이프하버 협약(Safe Harbor Agreement)에 의하여 이 문제를 해결하였으나 쉬렘스 판결로 무효가 선언됨에 따라 이를 프라이버시 방패(Privacy Shield)로 대체하였다.

마침 페이스북의 아일랜드 현지법인에서도 유럽 이용자들의 정보를 세이프하버 협약에 따라 미국 본사로 전송하여 처리하여 왔는데 유럽사법재판소(CJEU)는 2015년 10월 쉬렘스 사건[51]에서 EU-미국 간 세이프하버 협약을 무효로 선언하였다. 왜냐하면 EU 시민이 페이스북에 올린 개인정보가 미국 내에서 처리되는 과정에서 미국 정보기관에 제공될 수 있음을 간과한 협약은 무효라고 한 것이다. 이에 따라 세이프하버 협약을 대체한 프라이버시 방패[52]에서는 미국 기업이 EU 주민의 개인정보를 다룰 때 보다 엄중한 의무를 지게 하고 미국 정부기관도 명백한 안전조치와 투명한 처리를 약속[53]하게 하는 한편 침해를 입은 EU 시민에 대한 구제에 만전을 기하도록 했다.

그리고 EU 집행위에서도 프라이버시 보호를 최우선 과제로 내세워 데이터의 보관과 소유 문제를 다룰 기관을 설치하고 새로운 직책을 만들었다. 디지털 경제를 담당하는 귄터 외팅어(Günther Oettinger) 집행위원은 미국 기업들로부터 정보통제권을 되찾는 것이 그의 임무라고 공언하기도 했다.[54]

② 잊힐 권리

2014년 5월 유럽사법재판소의 또 다른 판결[55]은 다국적 IT 기업의 유럽 내 콘텐츠를 특별히 관리할 필요성을 야기했다. 검색 엔진의 결과물이 부적합하고 부적절하거나 더 이상 타당하지 않은 정보(inadequate, irrelevant or no longer relevant information)라면 그의 삭제를 원하는 이용자의 요구를 들어줘야 한다는 것이다.[56] 그 결과 구글은 1백만 건 이상의 신청을 접수하여 독일, 프랑스 등 유럽 도메인에서 40% 이상의 정보를 삭제하지 않을 수 없었다.

---

51) Court of Justice of the European Union, Maximilian Schrems v. Data Protection Commissioner, C-362/14, 6 October 2015.

52) EU Commission, "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield", Press release, 2 February 2016. <http://europa.eu/rapid/press-release_IP-16-216_en.htm>

53) 미 정부는 국가안보 목적이라고 했으나 CJEU는 개인정보보호에 대한 예외 사유는 엄격히 해석할 필요가 있다고 보았다.

54) Albright Stonebridge Group, *Data Localization*, p.6.

55) Court of Justice of the European Union, Google v. Spain AEPD, C-131/12, 13 May 2014.

56) 이것은 GDPR 제17조에 '삭제권'(right to erasure) 또는 '잊힐 권리'(right to be forgotten)로 성문화되었다.

프랑스 정보와 자유 국가위원회(CNIL)는 한 걸음 더 나아가 구글 같은 다국적 검색엔진이 잊힐 권리를 제대로 보장하려면 유럽 내 도메인뿐만 아니라 전 세계의 도메인에서 관련 정보를 삭제해야 한다고 요구하고 나섰다.[57]

나. 국내외의 반응

EU에 명시적으로 개인정보의 로컬라이제이션을 요구하는 법규범은 없다. 그러나 개인정보 보호수준이 EU보다 낮은 제3국으로의 개인정보 유출이 금지되는 만큼 복잡한 허가 절차를 밟지 않고 역내에 서버를 설치하여 개인정보를 처리하고 보관하는 것도 개인정보 로컬라이제이션임에는 틀림없다.

EU에서는 프라이버시권을 기본적 인권의 수준으로 파악하고 있어 개인정보 보호의 수준도 다른 나라에 비해 그 만큼 엄격하다고 볼 수 있다. 그럼에도 EU 회원국들이 세계경제에서 차지하는 비중이 크기 때문에 EU의 기준에 맞춰 자국의 개인정보보호 법제를 개선하고 복잡한 절차를 거쳐서라도 EU로부터 적정성 평가를 받고자 하는 나라[58]가 늘고 있다. 이러한 현상은 2018년 5월 GDPR 발효 후에도 멈추지 않을 것으로 보인다. 이에 따라 OECD의 프라이버시 보호 8원칙[59]을 충실히 이어 받은 EU의 개인정보 보호의 기준은 오늘날 개인정보 보호에 관한 한 글로벌 스탠더드의 하나로 자리잡게 되었다.

5. 러시아

가. 규제의 현황

러시아의 블라디미르 푸틴 대통령은 우크라이나 사태 이후 러시아가 서방

57) Albright Stonebridge Group, *Data Localization*, p.8.

58) EU로부터 적정성 평가(Adequacy assessment)를 받은 나라를 'Whitelisted Countries'라 부르거니와 2017년 6월 현재 역외금융센터 포함하여 12개 나라가 그 판정을 받았으며, 현재 일본과 한국에 대한 EU 측의 적정성평가(Adequacy assessment) 작업이 진행 중이다. <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>

59) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>

세계에 포위되었다는 인식 하에 외세에 영향을 받지 않고 정치적인 비판을 잠재우기 위해 정보에 대한 통제를 강화하고 있다. 러시아 정부는 이러한 정치논리에 입각하여 데이터 로컬라이제이션 정책을 펴고 있다.

러시아에서는 연방산업기술·수출관리국(Federal Service for Technical and Export Control: FSTEC)에서 정보통신 인프라의 안전, 러시아 국내에서 외국인의 산업기술 스파이 활동 단속, 국가기밀정보의 보호, 정보통신기기의 개발·제조·운용 및 폐기기술의 정보보호, 수출관리 등을 담당하고 있다. 국가안보에 관한 정책운용 및 부처 간의 조정·협력업무를 수행하기도 한다.

FSTEC는 정부기관, 금융, 정보통신, 전력, 운수, 에너지, 방재 등의 시스템에 이용되는 기술과 제품에 대한 인증을 담당하며, 요건을 미비한 경우에는 제재를 가하고 집행기관을 감사할 수 있는 권한을 갖고 있다.[60]

나. FSTEC 감독 하의 개인정보 보관

FSTEC는 직접적으로 FLMs의 법령이나 규제를 수행하지는 않지만, 정보 시스템 처리에 있어서 개인정보의 안전 강화를 위한 조직적·기술적 조건의 확인에 관한 명령(2013.2.18) 제11조에 의하여 개인정보의 보호를 목적으로 정보 시스템에 대한 검열을 할 수 있다.

2015년에 공표된 "EU와의 규제협력: IT 전자분야에 있어서 제3국의 규제에 관한 조사보고서"에 의하면 연방법 제242호-FZ[61]는 러시아 국민의 개인정보는 러시아 국내에 설치된 데이터베이스로 관리하고, 데이터 센터의 소재를 당국에 신고하여야 한다. 구체적으로 초기 데이터의 수집, 기록, 시스템화, 축약, 집적, 갱신, 복구 등의 작업은 러시아 국내에 설치된 데이터베이스를 이용하여야 한다. 하지만 개인정보를 동시에 러시아 국외에서도 보관하는 것을 막지는 않고 있다.

FLMs를 직접 관장하는 기관은 전기통신·매스컴부 산하의 연방통신정보기술·매스미디아 감독국(Roskomnadzor, 이하 "연방통신감독국")이다. 러시아 국내의 서버에 모든 개인정보를 수록한다면 그와 같은 분량 또는 그보다 적은 분량의 개인정보를 국외의 서버에 보관하는 것이 금지되지는 않는다. 요컨대 러시아에 있어서 FLMs는 러시아 국민의 개인정보를 국외에서 관리하는 것을 금하는 것은

60) 노무라 연구소, 앞의 보고서, 27면.

61) 연방법 No.242-FZ는 「정보통신망에 의한 개인정보 처리절차 조사에 있어서 개개의 러시아 연방법령의 수정에 관한 연방법」으로 2015년 9월 1일 발효되었다.

아니지만 러시아 정부의 감독이 미치는 범위에서 반드시 개인정보를 국내에 보관하도록 하고 있는 것이다.[62] 연방통신감독국은 최근 들어 연방법규에 따라 러시아 이용자의 개인정보가 해외 데이터베이스에 보관되고 있는지, 이용자의 동의를 받았는지, 개인정보처리방침을 제대로 공시하고 있는지 단속과 규제를 강화하고 있는데 러시아 내 SNS 서비스 길이 막힌 LinkedIn 사례가 대표적이다.[63]

6. 그 밖의 나라들

가. TPP 체약국

데이터 보관·처리의 현지화는 널리 보편화되는 추세에 있다. 인도네시아, 베트남 뿐만 아니라 캐나다, 호주 등지에서도 개인정보보호법 등은 일정 종류의 정보는 반드시 국내 서버에 저장하고 처리할 것을 의무화하고 데이터를 국외 이전하는 경우에는 일정 조건을 충족할 것을 요구하고 있다.[64] 미국의 트럼프 대통령이 철회함으로써 무산되고 말았지만, 환태평양 경제동반자(Trans-Pacific Partnership: TPP) 조약에서도 일부 APEC 회원국들은 일정한 정보의 국내 처리를 의무화하고자 하였다.

이와 반대로 유럽회의(Council of Europe: CoE) 108호 협약은 체약국 간의 개인정보의 자유로운 이전을 규정[65]하고 있는 바 주요 정보를 국내에서 보관·처리하라고 하는 것은 무슨 문제를 야기하게 되는가?

---

62) 노무라 연구소, 앞의 보고서, 28면.

63) 연방통신감독국은 2016년 모스크바 Taganskiy 지방법원에 LinkedIn을 제소하여 승소하였다. LinkedIn은 러시아내 약 600만명의 회원이 현지에서 LinkedIn서비스를 받지 못하게 됨에 따라 항소를 하였으나 항소법원은 1심판결을 그대로 유지함으로서 러시아 내 LinledIn 접속은 계속 불가능한 실정이다. Dmitry V. Nikiforov, et al, "Russia 2016: Personal Data & Cybersecurity", D&P Client Update, Debevoise & Plimpton, February 14, 2017.

64) Livingston and Greenleaf, op. cit., pp.22-26.

65) CoE Privacy Convention Article 12 (Transborder flows of personal data) 개인정보의 국경간 유통 (1) 각 당사국은 개인정보보호의 한 가지 목적을 위하여 또는 특별허가를 얻는 조건으로 이 협약의 다른 당사국의 관할에 속하는 제3자에게 개인정보를 이전하는 것을 금지하여서는 아니 된다. 다만, 그 당사국은 지역적인 국제기구에 속하는 국가들이 공유하는 조화를 이룬 보호규칙에 구속된다면 그리할 수 있다

TPP 조약 전자상거래 편의 제14.13조를 보면 '컴퓨터 시설의 소재지'(Location of Computing Facilities)라는 제하에 각 당사국이 정당한 공공정책목표를 달성할 수 있도록 컴퓨터 시설의 이용 또는 설치에 대한 제한을 부과할 수 있음을 예외적으로 인정하였다. 그리고 TPP 회원국에서 온 서비스 제공자가 자국에서 영업을 하는 조건으로 자국 내에 있는 컴퓨터 시설을 이용하거나 설치할 것을 의무화하는 것을 금지하였다. 일견 자국 내 정보의 보관·처리는 금지되고 투자자-국가분쟁(Investor-State Dispute: ISD)에 의해 해결하도록 하고 있으나, 여기서의 컴퓨터 시설은 상업적 용도로 제한하는 데다 광범한 예외를 인정함으로써 금지를 피할 수 있게 하였다.

나. 한국

한국에서는 정보처리자가 개인정보를 국외의 제3자에게 이전하려면 정보주체의 동의를 받도록 하고 있다(개인정보보호법 제17조 3항, 정보통신망법 제63조 2항). 그러므로 정보통신망 이용 계약을 체결함에 있어 약관상으로 이용자 즉 정보주체의 동의를 받을 수 없다면 예외 사유에도 해당되지 않는 한 당해 정보는 국외의 제3자에게 이전할 수 없고 국내에 보관하여야 하는 것이다.

앞에서 구글 맵과 관련하여 설명한 바와 같이 한국 정부(국토교통부장관)는 국가안보나 그 밖에 국가의 중대한 이익을 해칠 우려가 있다고 인정되는 경우에는 공간정보(기본측량성과 및 기본측량기록)를 복제하게 하거나 그 사본을 발급할 수 없으며(공간정보의 구축 및 관리 등에 관한 법률 제14조 3항 1호), 이 경우 기본측량성과를 국외로 반출해서도 안 된다(동법 제16조 2항 본문). 다만, 특정 외국정부와 기본측량성과를 서로 교환하기로 하였거나(동법 제16조 1항 단서에 의한 상호주의), 국토교통부장관이 국가안보와 관련된 사항에 대하여 과학기술정보통신부장관, 외교부장관, 통일부장관, 국방부장관, 행정안전부장관, 산업통상자원부장관 및 국가정보원장 등 관계 기관의 장과 협의체[66]를 구성하여 국외로 반출하기로 결정한 경우에는 예외로 하였다(동법 제16조 2항 단서).

66) 공간정보관리법 제16조는 기본측량성과의 국외반출을 금지하고 있는데, 이 문제를 심의하기 위한 관계기관장 협의체에 민간부문의 사정을 반영할 수 있게끔 1인 이상의 민간전문가를 포함하도록 의무화했다(제16조 제3～5항, 2018. 4. 25 발효).

다. 오스트레일리아

오스트레일리아에서는 '나의 건강기록(My Health Records) 시스템'[67] 관련 법규정에 의하면 시스템 운영자는 등록된 포털 운영자 또는 등록된 계약 서비스 제공자로서 나의 건강기록 시스템의 목적 상 그 기록을 오스트레일리아 밖에서도 보유하거나 처리하는 것이 금지된다. 그러나 시스템 운영자는 그 정보가 개인정보 또는 식별정보를 포함하지 않는다면 이를 국외에서 보유하거나 처리할 수 있다.

보건부 홈페이지에서는 나의 건강기록이 생성된 곳에서 건강기록이 국내에 보관되어야 하며, 보건부에서는 국민의 건강기록이나 개인정보를 국외에서 밝히지 않는다고 한다. 그 밖의 데이터 처리의 현지화를 명시한 규정은 없다.

Ⅳ. 개인정보 현지화 규제에 대한 평가

데이터를 보관·처리함에 있어서 현지에 있는 서버를 이용하도록 요구하는 것은 정보기술의 발전에 역행하는 처사이다. 국경이 없는 매체(borderless medium)로서 개방적이고 분권화된 네트워크인 인터넷의 본질에 반하다고 할 수 있다. 정보는 수요처를 찾아 유통하게 마련이고 이것을 사이버공간의 참여자들이 신속하고 적은 비용으로 실현 가능하게 만드는 것이 정보통신 기술이기 때문이다. FLMs 규제는 개방적인 인터넷의 기능과 자원을 조각(fragmentaion) 내고 비효율적으로 만드는 것이다.[68] 특히 신생기업·중소기업은 외부 클라우딩이나 데이터 센터의 컴퓨터 설비를 빌려서 영업을 하는 터에 FLMs 규제는 적잖은 타격이 될 것이다. 데이터 로컬라이제이션은 IT산업의 발전을 위축시키고 해당 국가는 물론 글로벌한 경제성장에도 차질을 빚게 된다.[69] 중국이 네트워크 안전법에서 국가안보 등을

67) 종전에 개인적으로 지배할 수 있는 전자적 건강기록(personally controlled electronic health record) 시스템으로 부르던 것이다. 근거법률의 명칭도 Personally Controlled Electronic Health Records Act.

68) Albright Stonebridge Group, *Data Localization*, p.3.

69) *Ibid.*, p.9.

이유로 중요정보 인프라(CII) 운영자에 대해 개인정보 및 중요 데이터의 국내 보관 및 국외 제공 데이터의 보안성 평가를 요구한 것에 대해 국내외의 반발이 거셌다. 막판에 시행시기를 늦추기는 했지만, 이러한 데이터에 대한 정부기관의 감시와 열람(back door)을 전제로 한 것이 아닌가 의심을 샀던 것이다. 이러한 의혹의 눈길은 러시아에 대해서도 마찬가지였다.

다만, 개인정보 보호의 견지에서 보호의 수준이 자국에 비해 뒤떨어지는 나라에 개인정보를 포함한 데이터의 반출을 일정 조건 하에 불허하는 것은 프라이버시권이 기본적 인권으로 보장하는 오늘날에는 당연한 처사라 볼 수 있다. 인터넷의 특성에 비추어 정보가 유통되는 어느 채널 한 곳이라도 허점이 있으면 데이터의 보안이 제대로 이루어질 수 없다는 점에서 나름대로 정당성을 갖는다.

그러나 아쉽게도 최근 들어 세를 불리고 있는 개인정보 로컬라이제이션에 맞설 수 있는 세력은 단독이든 연합이든 가시화되지 않고 있다. 그만큼 외국 정보기관에 의한 감시(foreign surveillance)의 우려, 개인정보 보호의 필요성이 강조되고 있는 탓이다. 외국 기업들이 데이터 현지화에 반대하는 것 못지않게 국내기업들은 데이터 현지화에 따른 이익을 양보하려 들지 않고 있다.[70] 그러나 데이터 현지화가 많아질수록 데이터 이용자들은 데이터 이용범위가 그 만큼 줄어들고 제조업이나 서비스업 종사자들은 유용한 정보에 대한 접근 기회를 놓칠 수 있음을 알아야 한다. 만일 현지 정부가 정보의 자유로운 유통을 정치적인 위협으로 간주하고 비민주적인 목적을 위해 데이터를 이용하거나 가공하려 들 경우에는 표현의 자유나 프라이버시마저 침해될 공산이 크다.

Ⅴ. 맺음말

오늘날 개방된 네트워크인 인터넷을 통해 모든 일이 이루어지는 시대에 데이터의 보관·처리의 현지화를 요구하는 법제는 일견 모순되고 시대착오적인 것처럼 보인다. 그러나 이를 시행하는 각국의 사정을 들여다보면 나름대로 명분이 있다.

70) *Ibid.*, p.3.

우리나라도 구글에 대하여 공간정보의 제공을 불허함으로써 데이터 로컬라이제이션 국가 리스트에 올랐지만 북한이 장거리 미사일과 무인기를 날리고 있는 작금의 현실에 비추어 상세한 지리정보를 공개하는 것은 매우 위험한 일이 아닐 수 없다. 다른 한편으로 해외여행을 하면서 스마트폰으로 구글이 제공하는 지도 및 교통정보 서비스<https://maps.google.com>를 이용해본 사람이라면 그러한 공간정보가 얼마나 유용하며 유통업이나 관광 서비스업 등에 부가가치를 창출하는지 체험적으로 알게 된다. 앞으로 도래할 자율주행차와 드론의 이용에는 없어서는 안 될 인프라가 되고 있다.

결국은 서로 충돌하는 가치를 놓고 선택을 해야 하는 문제로 바뀌게 된다. 국가안보의 명분도 절대불변이 아니며 남북긴장 완화의 상황에 따라 달라질 수 있다. 반면 개방·협조·책임을 앞세우는 인터넷 속성을 강조하는 것이나 정보의 분절화·파편화(fragmentation)를 초래하는 로컬라이제이션은 원활한 정보의 국제유통을 저해하므로 바람직하지 않다는 주장[71]도 피상적으로 들릴 수 있다. 그보다는 국가안보 및 공정과세에 중점을 두고 다국적 거대 IT기업에 주도권을 뺏기지 않는데 역점을 두거나, 아니면 시대적 조류에 맞게 국내 IT산업을 보호하고 경제적 실리를 취하자는 것이 피부와 와 닿을 수 있다.

인터넷이 세계의 모든 기업과 개인이 활발히 참여함으로써 그로 인한 시장이 지속적으로 확대되고 이노베이션이 촉발되었다는 점을 감안한다면 이른바 인터넷의 발칸화(Internet balkanization)[72]를 몰고 오는 데이터 로컬라이제이션은 결코 바람직하지 않다는 결론에 도달하게 된다. 일단 세계경제의 발전을 도모할 수 있는 국경간 정보유통(transborder data flow)의 원활화에 목표를 두고 그에 대한 예외 사유는 그것이 국가안보 목적이든 공정과세 원칙이든 정부의 이익을 좁게 제한(narrowly tailored)하고 엄격히 해석하여야 한다. 그리 함으로써 장기적으로 세계경제의 고른 발전을 도모할 수 있고 정보통신 기술의 발전을 통해 새로운 시대를 맞이할 수 있을 것이다.

---

71) 월드와이드웹(World Wide Web)의 창시자로 알려진 팀 버너스-리(Tim Berners-Lee)는 최근 모두에게 열려 있는 분권화된 인터넷(Re-decentralized Web)이라는 처음의 구상을 다시 강조하고 나섰는데, 그는 인터넷의 발전적 미래상에 대한 최대의 위험요소는 이른바 발칸화된 웹의 등장이라고 말했다. 허진성, 앞의 논문, 290면.

72) 인터넷 발칸화(Internet Balkanization)란 인터넷이 국가적으로 지역적으로 폐쇄된 네트워크들로 분열되는 것을 말한다. 19세기 말 오스만 제국이 붕괴되는 과정에서 발칸 반도가 여러 작은 나라들로 분열됨으로써 1차대전의 원인을 제공한 현상을 사이버공간에 빗대어 표현한 것이다. 허진성, 위의 논문, 290~291.

참고문헌

박훤일, “정보이동권의 국내 도입 방안 - EU GDPR의 관련 규정을 중심으로”, 경희법학 제52권 3호, 2017.9.30.

_____, 「개인정보의 국제적 유통에 따른 법적 문제와 대책」, 집문당, 2015.

안종석, “다국적 IT기업의 조세회피 행태와 시사점: 애플·구글의 사례를 중심으로”, 재정포럼 2013.7.

허진성, “데이터 국지화(Data Localization) 정책의 세계적 흐름과 그 법제적 함의”, 언론과 법 제13권 2호, 2014.

개인정보보호포럼·한국인터넷진흥원, 「지능정보사회 선도를 위한 개인정보보호 이슈 및 동향」, 2017.2.

生貝直人, “自律·分散·協調社会とデータポータビリティーの権利”, 経済産業省分散戦略ワーキンググループ 第6回, 2016.7.27.

野村総合研究所,「ＥＵとの規制協力：サイバー空間及びIoTに係る規制等に関する調査報告書」, 2017.3.

日本経済団体連合会·在日米國商工會議所, “日米 IED民間作業部会共同声明 2016”, 2016.2.25.

Article 29 Working Party, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf>.

Draft circular on detailed regulation on cross border provision of public information (No.72/2013/ ND-CP).

Adam Golodner, et al., China's New Cybersecurity Law Imposes Heightened Restrictions on Company Computer Networks, Arnold Porter Kaye Scholer, July 20, 2017.<https://www.apks.com/en/perspectives/publications/2017/07/hinas-w-cybersecurity-law-imposes>

Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Information*, September 2015.

Covington & Burling, “EU Data Retention Directive Declared Invalid by CJEU”, *Inside Privacy*, April 8, 2014.

Covington & Burling, “Brazil Enacts “Marco Civil” Internet Civil Rights Bill”, *Inside Privacy*, April 28, 2014.

Dmitry V. Nikiforov, et al, “Russia 2016: Personal Data & Cybersecurity“, D&P Client Update, Debevoise & Plimpton, February 14, 2017. <https://www.debevoise.com/insights> Russia 2016: personal data

EU Commission, “EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield”, Press release, 2 February 2016. <http://europa.eu/rapid/press-release_IP-16-216_en.htm>

Graham Greenleaf and Scott Livingston, “China’s Cybersecurity Law – also a data privacy law?”, *Privacy Laws & Business International Report* Issue 144, December 2016

W. Kuan Hon, *Data Localization Laws and Policy - The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens*, Edward Elgar, 2017.

The Guardian, “EU to find ways to make Google, Facebook and Amazon pay more tax”, 21 September 2017. <https://www.theguardian.com/business/2017/sep/21/tech-firms-tax-eu-turnover-google-amazon-apple>

Scott Livingston and Graham Greenleaf, “Data localisation in China and other APEC jurisdictions”, *Privacy Laws & Business International Report* Issue 143, October 2016.

Information Security Technology – Guidelines for Personal Information within Public and Commercial Services Information Systems 2013.

디지털 데일리, “[주간 클라우드 동향] 2017 국내 클라우드 도입, 어디까지 왔나”, 2017.10.16. <http://www.ddaily.co.kr/cloud/news/article.html?no=161209>

조선일보, “한국 게임으로 1兆 챙긴 구글… 세금은 '깜깜'”, 2017.9.15. <http://biz.chosun.com/site/data/html_dir/2017/09/14/2017091403574.html>

Insight, “'구글', 국내서 2조 버는데 세금은 한 푼도 안 낸다”, 2017.5.15. <http://www.insight.co.kr/newsRead.php?ArtNo=105579>

오마이뉴스, “구글의 지도 국외반출 요구에 포털·네비 업체 ‘역차별’ 반발”, 2016. 6.20. <http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0002219482>

전자신문, "'나라장터에서 인프라 클라우드 서비스 이용하세요", 2017.9.27.
<http://www.etnews.com/20170927000385>
G7 이세시마 정상회담 자료 <http://www.mofa.go.jp/ecm/ec/page4e_000457.html>
NAVER Privacy Whitepaper 2017년 게재 논문
<https://privacy.naver.com/protection_activity/privacy_white_paper?menu=protection_activity_report_privacy_whitepaper>
(이상의 웹사이트는 2017.12.12 최종 접속)

Abstract

The Merits and Demerits of Data Localization

Park, Whon-Il*

Data localization requires personal data of citizens or residents be processed and stored within the border of the country. When such data are transferred overseas, they are required to meet local privacy or data protection laws. After revelations by Edward Snowden regarding United States global surveillance programs in 2013, an increasing number of countries have introduced data localization laws and data export restrictions.

In this Age of IoT and big data, data localization laws worldwide are threatening digital globalization and inhibiting cloud computing's adoption despite acknowledged benefits. There are various motivations for nations to adhere to data localization and restrict the transfer of personal data to a third country. Those restrictions are implemented for the purpose of national security, prevention of cybercrime, or protection of privacy of citizens, in particular, of the EU Member States.

In some countries, it is to prevent the global IT Giants like Google and Facebook from evading local taxes on the huge advertisement profits in those countries by requiring the presence of local data centers. As such, local IT businesses are complaining of reverse discrimination from foreign providers of identical services. Other countries believe data localization offers a quick way to force high-tech economic activity to take place within their borders.

It is also true that data localization and other barriers to data flows impose significant costs: reducing GDP by 0.7 to 1.7 percent in China, EU, Indonesia, South Korea, and Vietnam, which have all either proposed or enacted data localization policies.

Statutory grounds in the above countries are found at:

- China : Cybersecurity Law, the People's Bank of China Notice on Urging Financial

* Professor of law at Kyung Hee University.

Institutions to Protect Clients' Personal Financial Information (2011), and Measures for Administration of Population Health Information (2014)
- Vietnam : Decree of Information Technology Services and OTT Circular
- Indonesia : Organization of Electronic Systems and Transactions Regulation (82/2012) and Regulation No. 27 of 2015 regarding Technical Requirement of Equipment and/or Telecommunication Devices in LTE Technology Basis
- European Union : Data Protection Directive (95/46/EC) and GDPR effective May 2018
- Russia : Federal Law 242-FZ
- Korea : Act on the Establishment, Management, etc. of Spatial Data.

There seem to be diverse rationales, one of which is national security or surveillance concerns. The Korean government is afraid of the detailed Google maps would be utilized by the belligerent North Koreans who have already developed long range missiles and unmanned aircraft systems. However, such mapping data are indispensable to local retail vendors, logistics and tourism enterprises and the operation of unmanned vehicles and drones in the near future.

The so-called Internet balkanization and any barrier to free flows of data would hinder such burgeoning high-tech services. Therefore, the derogations of the primary aim of the Internet as an open network should be subject to strict scrutiny even for the compelling government interest such as national security.

Key Words : data localization, forced localization measures (FLMs), data center, trans-border data flow, Internet balkanization