Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전연구센터 연구위원 워킹페이퍼 No.14.(발간일: 2025.2.3.)

데이터 거버넌스와 개인정보보호

김현경 서울과학기술대학교 IT정책전문대학원 교수

1. 서론

그간 민간영역의 데이터 안보는 글로벌 경쟁 관계에 있는 기업 간에 있어서 영업비밀 등 기업의 핵심 혹은 주요 전략 보호 차원에서 다루어진 것으로 보인다. 그러나 인공지능과 데이터를 기반으로 한 글로벌 플랫폼 기업이 국제경제에서 차지하는 영향력과 비중이 높아지면서 민간 기업이 보유하고 있는 '데이터' 역시 국가안보 차원에서 논의되는 경향이다. 특히 개인정보는 자국민의 프라이버시권 · 개인정보자기결정권이라는 헌법상 기본권의 원천이 되므로 자국민의 기본권 보호 차원에서 개인정보의 보호체계에 대한 관심이 고조되고 있다. 무엇보다도 지난 10년간 데이터는 전 세계적으로 가장 가치 있는 경제적 자산 중 하나로 부상했다고 해도 과언이 아니다. 아마 산업혁명 이후 처음으로 전 세계 국가들이 데이터의 부가가치를 최대한 창출하기 위한 노력에 매진하고 있다고 볼 수 있을 것이다. 따라서 전 세계 국가들이 각기 다른 데이터 거버넌스를 도입하여 자국 내에서 데이터 활용을 극대화하려는 시도를 하는 것은 지당한 일이다. 러시아 · 중국 등은 자국민의 개인정보가 국경 밖으로 이전되지 못하도록 하는 규범체계를 원칙으로 삼고 있으며, 유럽의 경우 유럽이 인정한 개인정보 보호 수준에 미치지 못하는 국가 또는 기업에게 유럽시민의 개인정보 이전을 엄격히 제한하는 입법을 완료하여 시행중이다. 반면 구글·아마존·메타 등 거대 데이터 공룡기업을 보유하고 있는 미국은 국경 간 개인정보의 자유로운 이동을 허용하되, 오히려 자국의 안보를 위해 해외에 있는 데이터에 대한 접근 권한을 강화하는 규범을 추진하였다. 그러나 데이터의 국경 이동은 클라우드컴퓨팅, 생성형 인공지능 등의 해외 서비스 이용에서 보듯 각국

의 규범을 집행하는 것 자체가 곤란한 상황을 발생시킨다.

무엇보다도 EU-미국 간 프라이버시 실드(Privacy Shield)를 무효로 하는 유럽사법재판소(이하 "CJEU"라 한다)의 슈렘스II 결정(이하 "Schrems II"라 한다)[1] 이후 EU 국가들의 데이터 감독기구(European data protection authorities, 이하"DPA"라 한다)는 국경 간 데이터 이전을 규정하고 있는 GDPR 제5장[2]과 관련하여 "위험 제로(zero risk) 접근방식"을 발전시켰다. 이러한 접근방식은 외국의 정보기관 및 법 집행 기관이 유럽의 개인정보에 접근할 수 있는 모든 위험을 '제거'하도록 요구하는 것으로, "유럽 주권 해결책(European sovereign solutions)"이라는 엄격한 집행방식을 클라우드 서비스 제공자(이하 CSP라 한다)를 비롯한 데이터 처리 기업에게 요구하고 있다. 특히 이러한 해결책에는 데이터 국지화가 필수 요건으로 포함된다. 그러나 이러한 "위험 제로 접근방식"이 보안 친화적이며, 실효적인지에 대하여는 의문인 바, 본 고에서는 개인정보 국외 이전과 관련하여 각 국가가 취하고 있는 데이터 거버넌스를 검토한 후, 향후 개인정보 국외 이전 규범에 있어서 고려해야 할 쟁점을 도출하고자 한다.

2. 개인정보 보호의 이념과 거버넌스 유형

2-1. 통합 · 독립기관형 : 유럽

유럽의 정치 전통은 사회 전체를 통합하여 국가를 창설하는, 그리하여 사회 내 권력을 국가에 포괄적이고 절대적으로 이양하는 이른바 "사회계약"(Social Contract) 이론에 기초하고 있다. 이러한 체계에서는, 개인이 자아 발전을 도모하게 되는 사회공동체가 구체적으로 조직되고 형성됨에 있어서 국가는 핵심적인 역할을 수행하는 것으로 본다(Yves Poullet, 1990). 그리고 시민의 자율은 법적 권리의 뒷받침으로 확보될 수 있다고 인식된다. 이러한 정치철학에서, 개인정보 보호는 기본적 인권보호의 관점에서 요구되는 정치적 명령이다.[3] 시민들은 개인정보보호와 관련해서 민간의 기업보다 정부를 더 신뢰하는 경향을 보이기도 한다(Herbert J. Spiro, 1971). 따라서 여기서 개인정보보호의 문제는 주로 공법의 영역에서 다루어지게 된다.

---

1) CJEU는 유럽연합(EU)에서 제3국으로 전송되는 개인정보에 대한 높은 수준의 보호 수준을 유지하는 것이 중요하다는 점을 강력하게 확인하면서 미국뿐만 아니라 다른 국가의 데이터 접근 문제를 포괄적으로 다루었다. CJEU, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Case C-311/18), ("Schrems II"), Judgment of July 16th, 2020

2) Chapter 5 Transfers of personal data to third countries or international organisations :제44조부터 제49조

3) 프랑스 개인정보보호법 제1조는 그 첫머리에서 "컴퓨터처리는 시민에게 봉사하여야 한다."고 선언하고 있다. Law No. 78-17 of Jan 6, 1978, art. 1 〈http://www.cnil.fr/textes/text02.htm〉

이 유형에서는, 포괄적인 입법을 통해 공공부문이든 민간부문이든 모든 개인정보처리에 관해 총체적이고 전반적인 권리와 의무를 규정한다. 그리고 그 권리와 의무의 집행은 전문적이고 독립된 감독기구를 통해 이루어진다(이인호외, 2014).

2-2. 분산형 : 미국 등

미국은 개인정보 보호와 관련하여 공공부문과 민간부문을 분리하여 이원적으로 접근하는 방식을 취하고 있다. 민간부문에 있어서는 유럽의 접근 방식과는 달리 시장 중심의 경제적 관점을 채택하고 있다. 즉 개인정보보호는 정치적으로 보호되어야 할 권리의 문제라기보다 경제적 역학관계의 문제로 취급된다. 그리고 개인정보보호에 관한 논의는 "시민"(citizens)이라기보다 "소비자"(consumers)라는 관점에서 주로 이루어진다.[4] 미국에서 민간부문의 소비자정보를 감독하고 민원을 해결하기 위한 목적에서 특별히 설립된 감독기구는 없다. 그러나 공정한 경쟁을 통한 시장기능의 유지와 불공정한 거래 또는 사업 관행으로부터 소비자를 보호하기 위해 1914년부터 독립규제위원회로서 설립된 연방거래위원회(FTC: Federal Trade Commission)가 소비자정보를 보호하기 위한 감독기능을 함께 수행하고 있다. 따라서 모든 소비자의 개인정보를 연방 차원에서 감독하고 보호하는 기구는 연방거래위원회[5]라고 할 수 있다. 연방거래위원회가 소비자의 개인정보를 보호하는 기능과 권한은 연방거래위원회법(Federal Trade Commission Act)[6] 제5조(15 U.S.C. Sec. 45)에 근거한다. 이는 "상거래에 있어서 또는 상거래에 영향을 미치는 불공정하거나 기만적인 행위나 관행"(unfair or deceptive acts or practices in or affecting commerce)을 금지하고 있고, 다만 여기서 "불공정하거나 기만적인 행위나 관행"이라는 개념은 "소비자 자신이 합리적으로 피할 수 없고 또한 그것을 상쇄시킬만한 소비자 또는 경쟁에의 우월적인 이익이 없는 그러한 중대한 피해(substantial injury)를 소비자에게 야기하거나 야기 할 가능성이 있는 행위나 관행"을 의미하는 것이다.[7]

---

4) 그렇기 때문에 미국의 경우 인터넷에서의 상거래와 관련한 개인정보보호의 문제는 주로 시장의 공정거래질서를 확보하기 위해 설립된 연방거래위원회(FTC)의 소관사항이며, 기업이 개인정보처리원칙을 위반한 경우 불공정거래행위로 취급되어 규율된다.

5) 연방거래위원회는 시장에서의 공정경쟁을 확보하기 위하여 행정부로부터 분리되어 이 부문에서 독자적으로 일정한 행정기능을 수행하는 독립규제위원회이다. 연방거래위원회는 상원의 동의를 받아 대통령이 7년의 임기로 임명하는 5인의 위원으로 구성되어 있다.

6) 연방거래위원회법은 현재 연방법률집 제15편 제41조 내지 제58조에 수록되어 있다. 15 U.S.C. Sec. 41-58.

7) 한편 미국의 공공부문의 개인정보 보호는 1974년 세계에서 두 번째로 「프라이버시법」(Privacy Act of 1974)을 제정한 국가다. 미국은 유럽처럼 그 의무와 권리를 집행하는 독립된 감독기구를 별도로 두고 있지는 않지만, 공공부문에 있어서는 대통령 직속의 관리예산처(OMB)가 그 집행책임을 지고 있고, 나아가 법원에 의한 효과적인 권리구제절차를 마련해 놓고 있다. 미국의 개인정보보호법제의 특징 등 상세한 소개는, 김일환, "미국 개인정보보호법규에 관한 연구", 『미국헌법연구』 제10호 (미국헌법학회, 1999), 325-400면 참조.

특히 미국은 자유로운 정보유통(free flow of information)을 제1의 원리로 삼는 강한 표현의 자유 전통을 가지고 있다. 자유로운 정보유통이 사적 활동과 자율을 촉진하는 것이기 때문에, 정부 규제보다는 사적 계약이야말로 개인정보보호의 일차적인 法源이 되어야 하고, 이에 따라 개인은 자기 자신의 권리를 스스로 주장하고 요구하여야 한다는 것이다(J. R. Reidenberg, 2000).

그러나 최근 미국 내에서도 개인정보 남용에 대한 시민들의 관심과 우려가 커지면서, 규제에 대한 여론이 강화되고 주 차원의 개별 규제체계가 등장하고 있다. 캘리포니아주는 2020년 1월 「캘리포니아주 소비자 프라이버시 보호법(California Consumer Privacy Act: CCPA)」을 시행하였는데, 이는 미국 최초의 광범위한 데이터를 대상으로 하는 포괄적인 프라이버시 보호법이라고 할 수 있다. 동 법은 2020년 11월 「캘리포니아주 프라이버시권법(California Privacy Rights Act: CPRA)」을 통하여 개정되었다. CPRA는 2023년 1월부터 시행되고 있다(김현수, 2023). 주요한 개정사항으로는 민감한 개인정보의 신설, 보안에 관한 의무 강화, 소비자의 사적 소권 대상의 확대가 포함된다. 이와 함께, 데이터와 보안에 관한 조사나 집행을 담당하는 미국 최초의 규제기관으로 평가되는 캘리포니아주 프라이버시 보호국(California Privacy Protection Agency)을 설립하는 규정을 두었다.[8] 그 외에도 버지니아주에서는 포괄적인 프라이버시 보호법인 「소비자 데이터 보호법(Consumer Data Protection Act: CDPA)」이 2023년 1월부터, 콜로라도 주에서는 「콜로라도주 프라이버시법(Colorado Privacy Act: CPA)」[9]이 2023년 7월부터, 코네티컷주에서는 「코네티컷주 데이터 프라이버시법(Connecticut Data Privacy Act: CTDPA)」[10]이 2023년 7월부터, 유타주에서는 「유타주 소비자 프라이버시법」(Utah Consumer Privacy Act)[11]이 2023년 12월 12일부터 각각 시행되었다.[12]

뿐만 아니라 연방 차원에서도 통일적 입법 움직임이 시도되고 있다. 2021년 11월 4일 연방 상원에서는 민주당 Maria Cantwell 의원에 의해 「소비자 온라인 프리이버시권법(Consumer Online Privacy Rights Act: COPRA)[13]이 제안되었다. 그리고 공화당 Roger Wicker 의원에 의해 제안된 「안전한 데이터법(Safe Data Act)」[14] 역시 유력한 법안이었으나 최종적으로 법률로 제정되지는 못했다. 그밖에, 2022년 6월 21일 공화당 Frank Pallone 의

8) Cal. Civ. Code § 1798.199.10 (2022) 참조.
9) 2021 Colo. Ch. 483.
10) Senate Bill 6: An Act Concerning Personal Data Privacy and Online Monitoring.
11) Utah Code Ann. § 13-61-102.
12) 2024년 3월 20일 현재 캘리포니아, 콜로라도, 코네티컷, 델라웨어, 플로리다, 인디애나, 아이오와, 몬태나, 뉴햄프셔, 뉴저지, 오리건, 테네시, 텍사스, 유타, 버지니아를 포함하여 최소 15개 주에서 자체 데이터 개인 정보 보호법을 제정했다.
13) S.3195 – Consumer Online Privacy Rights Act, 117th Congress (2021–2022).
14) S.2499 – SAFE DATA Act, 117th Congress (2021–2022).

원에 의해 제출된 「미국 데이터 프라이버시 및 보호법(American Data Privacy and Protection Act: ADPPA)」[15] 등이 있다.

디지털 사회에서 프라이버시 문제의 다양성 및 그 규모에 비추어 보면 FTC의 권한 강화나 다른 감독기관과의 협동의 필요성이 높아지고 있다. 더불어 FTC는 개인정보 보호를 위한 감독기관으로 적절하게 기능할 수 있다고 하는 견해가 있는 한편 새로운 감독기관의 필요성을 지적하는 견해도 존재한다(Priscilla M. Regan, 2020).

2-3. 우리나라 : 혼합형

우리나라는 통합 감독기구인 '개인정보보호위원회'가 존재하므로 통합 독립기관형 체계를 취하고 있는 것으로 볼 수 있으나, 엄격히 영역별 개인정보 보호체계가 별도로 존재하고 있는바, 혼합형으로 보는 것이 타당하다. 2011년 공공과 민간에 모두 적용되는 개인정보 보호의 일반법 · 기본법으로서 「개인정보 보호법」이 제정되었다. 이후 데이터 3법의 개정을 통해 법령 간 중복 또는 충돌 적용이 문제가 되었던 「정보통신망 이용촉진 및 정보보호등에 관한 법률」(이하 "정보통신망법)의 개인정보 보호 규정을 「개인정보 보호법」으로 이관함으로서 개인정보 보호 영역의 법률간 체계정합성을 다지고자 하였다. 또한 개인정보 보호의 집행체계 역시 행정안전부와 방송통신위원회의 기능을 개인정보 보호위원회로 이관하고, 개인정보 보호위원회의 독립성과 집행기관으로서 위상을 강화함으로서 감독기관의 실효성을 담보하고자 하였다. 그러나 여전히 금융영역은 「신용정보의 이용 및 보호에 관한 법률」(이하 "신용정보법")에 따라 금융위원회를 중심으로 독자적으로 집행되고 있으며, 의료영역, 교육영역, 위치정보 등은 각각 복지부, 교육부, 방통위 등이 주된 역할을 하고 있다.

2-4. 소결

앞서 언급한 바와 같이 유럽의 경우, 개인정보 보호에 대한 권리를 기본적 권리 또는 인권으로 파악[16]해 온 반면, 미국에서는 개인정보를 수집하고 활용하는 데 있어 전통적으로 기업에게 유리한 접근 방식을 취해 왔다(김민호, 2016). 한편 유럽은 개인정보보호수준이 "적절하지"(adequate) 못한 역외 국가에 개인정보의 이전을 금지시킴으로써 역외 국가의 개

15) H.R.8152 – American Data Privacy and Protection Act, 117th Congress (2021–2022).

16) 「EU 기본권 헌장(Charter of Fundamental Rights of the European Union)」제8조, 「유럽 인권 조약(European Convention on Human Rights)」제8조 및 「EU 운영 조약(Treaty on the Functioning of the European Union)」제16조에서 개인 데이터 보호에 대한 권리가 기본적 인권으로서 다루어지고 있다. 그 배경에는 나치가 유대인을 박해할 때 개인 데이터를 악용한 데 대한 반성이 깔려 있다.

인정보보호체계에 대한 심사를 강요하고 있다. 이러한 미국과 유럽의 집행모델의 불일치는 개인정보의 국가 간 이전에 있어서 미묘한 갈등 상황을 야기하고 있다.

개인정보나 프라이버시보호 법제는 각각의 가치관을 바탕으로 세계 각국에서 발전해 왔지만, 세계화가 진행되면서 관련 상대국의 법제도를 의식하고 자국의 법제도를 현행화는 움직임이 활발해지고 있다(김현수, 2024). 그리고 개인정보 보호에 관련한 상황은 기술환경과 주변 통상국들의 변화에 영향을 받아 지속적으로 변화할 것이기 때문에 개인정보의 적절한 보호를 위해서는 계속적으로 거버넌스 및 법제도의 재검토가 필요하다.

3. 개인정보 국외 이전 규범의 유형

개인정보 국외이전을 규율하는 유형은 국가의 개입 정도에 따라, 사적자치의 원칙을 우선시 하는 '자유주의 모델', 이전 자체는 허용하되, 국가가 정한 기준에 부합하는 경우에만 허용하는 '상호적정성 모델', 원칙적으로 국경 밖 이전을 허용하지 않되, 지극히 예외적인 경우에만 허용하는 '국가통제 모델'로 나누어 볼 수 있다.

3-1. 자유 이전형

미국은 앞서 언급하였듯이 민간영역을 포괄적으로 규율하는 연방 차원의 개인정보 보호법은 존재하지 않는다. 공공부문의 프라이버시 보호법(the Privacy Act, 1974)이 존재하고, 민간부문의 아동온라인 프라이버시 보호법,[17] 건강보험법,[18] 전자통신에서 프라이버시 보호법[19] 등 영역별 법제를 취하고 있다.

이러한 법률에서도 자국민의 개인정보 국외 이전을 제한하기보다, 오히려 정부의 국외 정보에 대한 접근을 허용하여 국가안보 차원의 개인정보 규율을 강화하고자 한다. 미국 정부는 마이크로소프트사(이하 MS라 한다)의 이메일계정이 마약밀매에 이용된다는 이유로 관련 자료를 열람하고자 하였다. 뉴욕남부 연방지방법원은 '전자통신 프라이버시 보호법'에 근거하여 MS에게 이메일계정 관련 자료를 제출하도록 하는 수색영장을 발부하였다.[20] MS는

---

17) the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§6501–6506)

18) the Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.);

19) the Electronic Communications Privacy Act(ECPA)(18 U.S.C. §2510). 미국 의회는 이 법의 제2장에서 저장통신법(Stored Communications Act; SCA)을 제정하며 전자통신 이용에 있어 개인의 사생활보호 권리를 인정하였다. 이 법은 감청법(Wiretap Act,arts. §2510–§2522), 저장통신법(Stored Communications Act; SCA, arts. §2701–§2712), 통신이용상황기록장치법(Pen Register Statute, arts.§3121–§3127) 등 3개의 주요 장으로 구성된다.

20) 18 U.S.C. art. 2703(c)(1)(A); 미국 정부기관의 통신이용 기록이나 정보에 대한 수집권 및 그 허용범위에 관해서는 최창수, "수사·정보기관의 통신이용 정보수집권에 관한 미국의 입법례와 그 함의", 「정보법학」 제20권

해당자료는 미국 영토 밖 즉 외국(아일랜드의 데이터센터)에 보관되어 있으므로 미국법원이 강제할 수 없다고 하였고 이러한 수색영장을 무효화하기 위한 소송을 제기하였다. 항소법원은 아일랜드에 저장된 자료를 제출하도록 하는 것은 역외적용 문제이나, 법률에 의해 명시적으로 역외적용을 규정하지 않고 있다고 하였다. 따라서 아일랜드 정부가 사법공조조약에 의거 해당자료를 제출하도록 요청하는 것과는 별론으로 '전자통신 프라이버시 보호법'에 따라 영장을 발부할 권한이 없다고 하였다(이하 "MS사건").[21] 이어서 미국정부는 제2순회 항소법원에 전원합의체 재심리(en banc rehearing)를 신청하였으나 거부되었고, 이러한 과정에서 일부 재판관들은 항소법원의 판결에 대하여 별도로 반대의견을 표명하였다(박선욱, 2019).

이러한 일련의 과정을 겪으면서 미국 의회는 합법적인 해외정보 활용을 위한 해외정보이용 합법화법(Clarifying Lawful Overseas Use of Data Act; CLOUD Act)[22]을 통과시켰다. 동법은 2018년 3월 22일 시행되었는데 동법에 의하면 미국의 통신서비스제공자들이 보유 또는 관리하고 있는 통신내용, 트래픽 데이터, 가입자 정보 등에 대해 미국 정부기관이 실제 데이터가 저장된 위치에 관계없이 제공 요청을 할 수 있도록 명시한 것이다.

즉 미국은 개인정보의 국외 이전을 자유롭게 허용하되, 오히려 자국의 역외데이터 접근에 대한 법적 근거를 마련함으로서 데이터 경제의 부흥과 데이터 보안의 조화를 추구하고자 한 것이라고 볼 수 있다.

3-2. 상호적정성 유형

2018년 5월 시행된 유럽연합 일반개인데이터보호규칙(General Data Protection Regulation; 이하 'GDPR')은 지리적 적용범위에 대하여 "본 규정은 유럽연합 역내의 개인정보처리자 또는 수탁처리자의 사업장의 활동에 수반되는 개인정보의 처리에 적용되고, 이 때 해당 처리가 유럽연합 역내 또는 역외에서 이루어지는지 여부는 관계없다(제3조 제1항)"고 규정하고 있다. 또한 유럽 연합 역내에 있는 정보주체에 대한 개인정보를 유럽연합 역외지역에 설립된 개인정보처리자 또는 수탁처리자가 처리하는 경우에도 이 법의 적용을 받아야 하며, 유럽연합 역내 정보주체에게 재화나 서비스를 제공하는 것과 관련한 처리활동인 경우 이에 대한 실제 비용 지불과 관련이 있는 지의 여부와 무관하게 이 법이 적용된다.[23] 즉 대

제1호, 2016, 122-125면 참조.

21) Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (Microsoft I), 829 F.3d 197 (2d Cir. 2016).

22) Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 4943, 115th Cong. (2018). 동법은 전자통신에서 프라이버시 보호법(18 U.S.C.)에 art. 2713을 신설한 것이다.

한민국의 기업이라 할지라도 EU시민의 개인정보를 처리하는 경우에는 GDPR이 적용된다.

한편 유럽시민의 개인정보를 제3국으로 이전할 수 있는 경우는 다음과 같다. 우선 1) GDPR 제45(3)조에 따른 적정성 결정을 득한 경우(이하 "적정성 결정"이라 한다), 2) 표준데이터보호조항(Standard Data Protection Clauses: SDPC, 舊SCC) (제46조제2항c), 구속력 있는 기업규칙(Binding Corporate Rules: BCR) (GDPR 제47조)[24] 등 제46조에 따른 적절한 안전조치에 이루어지고 있다고 인정된 경우(이하 "적절한 안전조치"라 한다), 3) 1)과 2)에 해당하지 않지만 '적정성 결정'과 '적절한 안전조치'가 결여되어 정보주체에 대해 발생할 수 있는 위험을 고지 받은 후, 정보주체가 자신의 개인정보를 제3국으로 이전되는 것에 대하여 '명시적으로 동의한'(explicitly consented) 경우(이하 "정보주체의 명시적 동의"라 한다)에 가능하다.[25]

'적절한 안전조치(2)'와 '정보주체의 명시적 동의(3)'의 경우 유럽진출 기업이 개별적으로 대응해야 한다는 한계가 있다. 유럽연합과 경제적인 교류가 늘고 있는 제3국 입장에서는 개별적인 계약체결을 통한 이전은 각 국의 법률적용 및 검토비용 등 상당한 비용을 지불해야 한다(오태현, 2018). 그러나 '적정성 결정(1)'의 경우 개인정보 이전에 대하여 추가적인 인가를 받을 필요 없다. 즉 유럽은 개인정보의 자유로운 국외이전을 허용하기 보다는, EU가 개인정보 보호수준이 적정하다고 인정한 국가 및 국외 개인정보처리자에게로의 이전만 원칙적으로 허용 하되 예외적으로 정보주체의 강력하고 명확한 동의를 득한 경우 국외 이전이 가능하도록 규율한 것이다. 그러나 EU 국가들의 데이터 감독기구(DPA)는 역외 데이터 이전에 있어서 기존의 "위험 기반(risk-based) 접근방식"이 아닌 "위험 제로(zero risk) 접근방식"을 발전시키고 있다. "외국 정부가 유럽 데이터에 접근할 수 있는 이론상의 위험이 존재한다면 어떠한 데이터 이전도 허용될 수 없다"는 "위험 제로 접근 방식(zero risk approach)을 집행하기 위한 "유럽 주권 해결책(European sovereign solutions)"을 시행하고 있는바, 이는 일정부분 GDPR의 국외 이전 규범보다 더 강력하다.

한편 이러한 유럽과의 교역을 고려하여 일본, 우리나라 등이 이러한 모델을 입법화한 바 있다. 일본「개인정보 보호법」은 은 개인정보의 국외이전과 관련하여 제24조는 외국에 있는 제3자에게 개인정보를 제공하는 것을 제한하는 규정을 마련하였다.[26] 이 규정에 의하면 개

---

23) 제3조제2항, Recital 23

24) 다국적 기업 내부에 구속력을 갖는 보호지침 마련 및 당국 승인이 필요하다.

25) GDPR 제49조제1항(a).

26) 제24조(외국에 있는 제3자에의 제공의 제한) ① 개인정보취급사업자는, 외국(일본의 역외에 있는 국가 또는 지역을 말한다. 이하 같다)(개인의 권리이익을 보호하는 가운데 우리나라와 동등한 수준에 있다고 인정되는 개인정보의 보호에 관한 제도를 가지고 있는 외국으로서 개인정보보호위원회규칙으로 정하는 외국을 제외한다. 이하 이 조에서 동일하다)에 있는 제3자(개인데이터의 취급에 대하여 이 節의 규정에 의해 개인정보취급사업자가 취하여야 할 조치에 상당하는 조치를 계속적으로 취하기 위하여 필요한 것으로서 개인정보보호위원회규칙으로 정하는 기준에 적합한 체제를 정비하고 있는 자를 제외한다. 이하 이 조에서 동일하다)에게 개인

인정보취급사업자는, 외국(일본의 역외에 있는 국가 또는 지역을 말한다. 이하 같다)에 있는 제3자에게 개인정보를 제공하는 경우에는, 前條 제1항 각 호에 열거된 경우를 제외하고,[27] 미리 외국에 있는 제3자에게 개인정보를 제공하는 것에 대하여 정보주체의 동의를 얻어야만 한다. 그러나 '외국'의 범위와 관련하여 "개인의 권리이익을 보호하는 가운데 일본과 동등한 수준에 있다고 인정되는 개인정보의 보호에 관한 제도를 가지고 있는 외국으로서 개인정보보호위원회규칙으로 정하는 국가를 제외"하고 있다. 즉 사전 동의를 받는 것을 원칙으로 하면서도, 동등한 보호수준을 가진 외국을 적용대상에서 제외시키고 있다. 또한 '제3자'의 범위와 관련하여 "개인정보의 취급에 대하여 일본 「개인정보 보호법」상 개인정보취급사업자가 취하여야 할 조치에 상응하는 조치로서 「개인정보보호위원회규칙」으로 정하는 기준에 적합한 체제를 정비하고 있는 자"를 제외하고 있다.

우리나라 역시 유럽과의 적정성 결정을 위해 개인정보 국외이전 규범을 비롯 개인정보 감독기구 등 법체계 및 규정 내용을 정비를 한 바 있다.

3-3. 이전 금지형(국가통제모델)

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. 이후에도 중국의 개인정보의 역외이전을 제한하는 입법을 추진한 바 있다. 러시아 역시 2013년 여름 NSA폭로 이후, 하원 의장은 이메일 또는 소셜네트워크 기업들이 러시아 고객의 데이터를 러시아 영역안의 서버에 보유하도록 하는 입법을 통해 "디지털 주권(digital sovereignty)"을 강화하여야 할 것을 요구하였고. 2014년 7월 21일 러시아인들의 개인정보를 러시아 연방 영토 밖에 저장하는 것을 금지하는 법 개정안이 통과되었다.[28] 더욱이 데이터베이스의 운영

데이터를 제공하는 경우에는, 前條 제1항 각 호에 열거된 경우를 제외하고, 미리 외국에 있는 제3자에의 제공을 인정하는 취지의 본인의 동의를 얻어야만 한다. 이 경우에는 同條의 규정은 적용하지 아니한다.

27) 제23조(제3자제공의 제한) ① 개인정보취급사업자는, 다음 각 호의 어느 하나에 해당하는 경우를 제외하고, 미리 본인의 동의를 얻지 않고서는 개인데이터를 제3자에게 제공하여서는 아니된다.
1. 법령에 근거한 경우
2. 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때
3. 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위하여 특히 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때
4. 국가기관 혹은 지방자치단체 또는 그 위탁을 받은 자가 법령이 정하는 사무를 수행하는 것에 대하여 협력할 필요가 있는 경우로서, 본인의 동의를 얻음으로써 당해 사무의 수행에 지장을 줄 우려가 있는 때

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

자는 데이터센터의 물리적 위치를 공개하여야 한다.[29] 이를 위반하는 온라인 웹사이트는 Roscomnadzor(연방 통신 감독 기관)의 블랙리스트 명단에 기재되며 마약이나 아동포르노 등과 유사하게 취급된다.[30] 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 6개월간 저장하여야 한다.[31]

4. 개인정보 국외 이전 규범 쟁점

4-1. 데이터 주권과 역외적용의 한계

데이터 주권은 데이터에 대한 관할 즉 집행력 확보를 통해 실현되므로 속지주의에 기반한 현행의 법체계로는 데이터의 물리적 소재에 따라 달라질 수밖에 없다. 우선 자국 내에 데이터센터 등을 두고 개인정보를 자국 내에서 처리하는 경우 내국민 개인정보의 보호와 관련된 법집행에 있어서는 크게 문제가 될 것이 없다. 영토는 국가임을 나타내는 우선적 기준이고(Viotti & Kauppi, 1993) 자신의 영토 내에 소재한 정보가 자국의 법적 기준에 합치되지 않게 될 경우 집행력을 확보할 수 있는 권한을 갖는다. 그러나 사업자가 국외에 데이터센터 등을 두고 자국민의 개인정보를 국외에서 처리하는 경우 데이터 주권을 위한 국내법의 집행이 문제될 수 있다. 개인정보의 물리적 위치는 해외에 있다 할지라도 해당 사업자가 그나마 국내 사업자인 경우(국내기업인 카카오가 서버 혹은 데이터 센터를 아일랜드에서 운영하는 경우 등) 개인정보처리자에 대한 인적 관할을 기반으로 데이터에 대한 집행이 어느 정도 가능할 수 있으나, 이 역시 미국의 MS사건에서 보듯 명확한 것은 아니다. 특히 내국인의 개인정보를 처리하는 사업자가 외국에 데이터센터를 두고 외국에서 대한민국 국민의 개인정보를 처리하는 외국사업자인 경우(현재 구글/페이스북 등) 온전히 자유주의 모델에만 의존할 경우, 법의 집행력 실현은 거의 요원하다.

이러한 데이터에 대한 주권 실행의 어려움을 극복하기 위해 유럽 등에서 대표적으로 채택한 방식이 '역외적용'이다. EU 국경 외부에서 발생하는 데이터 보호 위협으로부터 보호하기 위한 주요 메커니즘으로, EU 역외의 데이터 처리에도 적용될 수 있는 GDPR 제3조의 영

---

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

30) 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.

31) 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/ (2024.8.29.최종확인)

토적 범위에 관한 규정(GDPR 제3조)과 제3국으로 이전되는 개인정보를 보호하는 개인정보 이전 제한 규정(GDPR 제5장)이다.

GDPR의 지역적 범위를 규정하고 있는 제3조제1항에 의하면 GDPR의 적용은 유럽연합 내 정보주체의 데이터를 처리하는 경우 데이터 처리가 유럽연합 내에서 이루어지는지 여부에 관계없이 적용된다.[32] 이전의 개인정보 규범인 개인정보 보호지침(DPD)이 EU 외부에서 처리되거나 저장된 개인정보에 대하여 충분한 보호를 제공하지 못한다는 우려가 있었고,[33] 이로 인해 EU 외부에 설립된 자의 개인정보 처리에 대한 법 적용을 다루는 규칙이 변경된 것이다. 이는 현재 GDPR 제3조(2)에 규정되었다. 제3조(2)(a)에 따라 GDPR은 '유럽연합 내 정보주체에 대한 대가 지급 여부와 관계없이 상품 또는 서비스의 제공'과 관련된 경우 유럽연합에 설립되지 않은 데이터 컨트롤러[34] 또는 데이터 프로세서[35] 의 데이터 처리에 적용되며, 제3조(2)(b)에 따라 유럽연합 내 정보주체의 행동 모니터링과 관련하여 유럽연합에 설립되지 않은 컨트롤러 및 프로세서의 처리 활동은 그러한 행동이 유럽연합 내에서 발생하는 한 적용된다.

이러한 GDPR의 지역 범위 규정은 전 세계적으로도 영향을 미치게 된다. 이 규정은 EU 영토 경계 밖의 데이터 처리에도 적용되므로 제3국에서 이러한 처리에 관여하는 당사자뿐만 아니라 해당 국가 자체도 일정한 의무를 부과하게 된다. 이러한 EU 개인정보 보호법의 역외적용 또는 영토 확장을 초래하여 제3국과의 충돌이 발생할 수 있다(Ryngaert and Taylor, 2020).

또한 내국인의 개인정보에 대하여 해외사업자가 관리 · 지배력을 가지는 경우 그 집행이 용이하지 않다. 따라서 이러한 역외적용의 실효성 확보를 위해, 즉 해외사업자에 대한 실효성 확보를 위해 국내 대리인제도가 도입되었다(김현경,2019). GDPR 제27조 제1항은 제3조 2항에 따라 데이터 처리에 GDPR이 적용되는 EU 사업장이 없는 컨트롤러 및 처리자에게 유럽연합 내 대리인을 임명하도록 요구함으로써 이들의 책임을 강화하고자 하였다. 대리인 지정은 '해당 컨트롤러 및 처리자가 GDPR을 준수하지 않을 경우 정보주체의 보호 수준이 저하되지 않도록 보장'하고, 특히 이들에 대한 집행을 용이하게 하기 위해 고안된 것이다 (Millard and Kamarinou, 2020). 따라서 대리인 지정은 비(非)EU 데이터 컨트롤러 및 처리

---

32) EDPB, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Version 2.0' (12 November 2019), at 10

33) European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World—A European Data Protection Framework for the 21st Century', COM(2012) 9/3, 25 January 2012, at 10–11,

34) A data controller determines the purposes and means of processing personal data. See Article 4(7) GDPR.

35) A data processor processes personal data on behalf of the data controller. See Article 4(8) GDPR.

자에 대한 GDPR의 법적 집행의 어려움을 보완하기 위한 시도라고 할 수 있다. 그러나 비 EU 당사자에 대한 GDPR의 집행을 개선하기 위한 방법으로 대리인을 임명하는 것은 지금까지 대체로 효과가 없는 것으로 입증되었다(EC, 2020).

오히려 미국은 안보 차원에서 이러한 역외적용 한계를 극복하고자 한다. 미국의 Foreign Intelligence Surveillance Act 제702조(이하 FISA 702)[36]는 미국 정보기관이 국가안보 위협에 대한 해외정보를 수집하고 분석할 수 있도록 하는 중요한 정보수집 권한을 규정하고 있으며, 이에 근거하여 광범위한 "전자통신서비스제공자(electronic communication service provider)"에게 정보를 요청할 수 있다. 앞서 언급한 CLOUD Act도 "미국의 통신서비스제공자들이 보유 또는 관리하고 있는 통신내용, 트래픽 데이터, 가입자 정보 등에 대해 미국 정부기관이 실제 데이터가 저장된 위치에 관계없이 제공 요청을 할 수 있도록 규정"하고 있다.

4-2. '위험 제로(zero risk)'와 소버린 클라우드(sovereign cloud)

1) '위험 기반'에서 '위험 제로'로

EU-미국 간 프라이버시 실드(Privacy Shield)를 무효로 하는 2020년 7월의 CJEU의 Schrems Ⅱ 결정 이후, EU의 DPA는 GDPR 제5장과 관련하여 "위험 제로(zero risk)" 이론을 발전시켜 왔다. 2020년 11월 11일, EDPB는 슈렘스 Ⅱ 이후 매우 중요한 지침인 "유럽 필수 보장(EEG) 권고사항"을 발표했다.[37] 이에 의하면 데이터를 이전하는 데이터 컨트롤러에게 EU 법률에서 의무화한 것과 본질적으로 동일한 안전장치를 법률 시스템에 포함하지 않는 외국의 정부기관이 유럽 개인정보에 액세스할 수 있는 모든 위험을 '제거'하도록 요구한 것이다.

2) EU국가의 '위험 제로 접근방식'의 집행

2-1) 개요

---

36) FISA 702는 미국 정보 기관이 국가 안보 위협에 대한 해외 정보 정보를 수집하고 분석할 수 있도록 하는 중요한 정보 수집 권한을 규정한 조문이다.

37) EDPB on November 11, 2020 entitled: "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures" (EEG Recommendations). The objective of these Recommendations is to provide data exporters with a guide, based on the two European Courts' jurisprudence, in order to determine whether foreign countries surveillance laws meet the European human rights requirements and could therefore be considered as offering an "essentially equivalent protection".

이러한 '위험 제로' 요구 결과, 많은 비유럽 기업들은 유럽에 데이터를 국지화하는 소위 '주권적' 해결책(sovereign solutions)을 시행하기로 하였다. 즉 미국의 여러 주요 클라우드 제공업체와 다른 외국 기업들은 EEA에서 데이터를 국지화하는 '소버린 클라우드' 솔루션을 제공하기 시작한 것이다. 다양한 솔루션의 세부 사항과 방식은 다르지만, 모두 "①유럽의 데이터 국지화, ②강력한 데이터 암호화 및 제어 기능을 갖춘 기술적 조치,③ 제3국 정부의 EU 개인정보 요청에 대해 합법적으로 이의를 제기하겠다는 계약상의 약속 이행" 등 최소 이 세 가지 요소를 기반으로 한다. 마이크로소프트의 '유럽 데이터 바운더리',[38] 아마존 웹 서비스의 '디지털 주권'서약과[39] 유럽 소버린 클라우드,[40] 구글의 '디지털 주권' 솔루션,[41] 오라클의 'EU 소버린 클라우드,[42] 틱톡의 '프로젝트 클로버'.[43] 등이 그 예다. 이러한 노력에도 불구하고 몇몇 유럽 DPA 및 기타 정부 당국은 외국 정부의 역외 접근 위험이 없어야 함을 지속적으로 요구하고 있으며, 때로는 외국 정부로부터 유럽 내 데이터 제공 요청을 받는 것 자체가 GDPR 48조[44] 위반이라고 여기기도 한다(T. Christakis, 2019). 더불어 유럽의 DPA는 유럽에 저장된 데이터에 대한 역외 접근의 위험을 강조하면서 이러한 해결책만으로는 불충분하다고 판단하는 경우가 많다.

2-2) 프랑스

프랑스 DPA인 CNIL(Commission nationale de l'informatique et des libertés)은 미국정부가 유럽 데이터에 불법적으로 접근할 위험이 제로에 가까워져야 한다는 점을 고려할 때

---

38) 9 참조 https://www.microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb; **https://blogs.microsoft.com/eupolicy/2024/01/11/microsoft-cloud-european-data-boundary (2024.4.30. 최종확인)**

39) https://press.aboutamazon.com/2023/10/amazon-web-services-to-launch-aws-european-sovereign-cloud (2024.4.30. 최종확인)

40) 51
https://press.aboutamazon.com/2023/10/amazon-web-services-to-launch-aws-european-sovereign-cloud (2024.4.30. 최종확인)

41) https://cloud.google.com/blog/products/identity-security/announcing-google-clouds-new-digital-sovereignty-explorer?hl=en (2024.4.30. 최종확인)

42) https://www.oracle.com/cloud/eu-sovereign-cloud/ (2024.4.30. 최종확인)

43) https://newsroom.tiktok.com/en-ie/project-clover-ireland (2024.4.30. 최종확인)

44) Article 48 GDPR. Transfers or disclosures not authorised by Union law(유럽연합 법률로 승인되지 않은 정보의 이전 또는 제공 : 컨트롤러 또는 처리자에게 개인정보 이전 또는 공개를 요구하는 제3국의 법원 또는 재판소의 판결 및 행정 당국의 결정은 이 장에 따른 다른 이전 근거를 침해하지 않고 요청하는 제3국과 유럽연합 또는 회원국 간에 발효 중인 상호법률지원조약 등의 국제 협약에 근거하는 경우에만 어떤 방식으로든 인정되거나 집행될 수 있다.)

데이터 국지화와 미국 CSP의 위에서 언급한 '소버린 클라우드' 솔루션만으로는 충분하지 않다는 입장을 취한바 있다. 2021년 5월 27일에 발표된 고등 교육 및 연구를 위한 미국 협업 도구 사용에 관한 의견서에서 CNIL은 다음과 같이 명시적으로 언급한 바 있다.

"데이터 이전 여부와 관계없이 미국 기업에 의해 미국 영토 밖에 저장한 데이터에는 미국 법률이 적용된다. 따라서 미국정부가 프랑스에 저장된 개인정보에 접근할 수 있는 위험이 있다. 이러한 접근은 국제 협약에 근거하지 않은 경우, GDPR 제48조를 위반에 따른 무단 공개에 해당한다. 이러한 맥락에서, CNIL은 미국 정부가 이 데이터에 불법적으로 액세스할 수 있는 위험을 제거해야 한다고 생각한다"[45]

더욱이 CNIL은 Microsoft의 프랑스 "건강 데이터 허브(French Health Data Hub)"의 데이터 호스팅과 관련해서 프랑스최고행정법원(French Supreme Administrative Court, Conseil d'Etat)에 계류된 사건에 개입한 바 있다. "건강 데이터 허브"는 2019년에 만들어진 프랑스의 공공 플랫폼으로, 연구 지원을 위해 건강 데이터를 공유하도록 만들어졌다. 해당 플랫폼은 2020년 4월 15일 Microsoft와 호스팅 계약을 체결했다. Microsoft가 서비스 요구 조건 및 인증 등 엄격한 요구 사항을 충족하는 유일한 서비스 제공업체였기 때문이다. 그러나 해당 데이터가 미국정부에 의해 접근될 위험이 있으므로 해당 계약을 무효화 하는 소송이 제기되었고 CNIL은 2020년 10월에 약정의 무효를 주장하는 입장에서 법원에 다음과 같은 의견서를 제출하였다.

"Microsoft는 FISA와 EO 12333[46]의 적용을 받아 EU에서 처리되고 저장된 데이터를 제공할 것을 요구하는 미국 정부기관에 종속될 수밖에 없다. 따라서 CNIL은 FISA 702 또는 EO 12333에 따라 미국 정부기관이 Microsoft에게 발하는 요청은 GDPR 제48조에 따라 EU 법을 위반한 불법 공개로 간주되어져야 한다."[47]

이는 CNIL이 미국 정부의 접근 요청은 GDPR 48조에서 금지하는 공개로 자동 간주되어야 한다는 입장을 고수하는 것이라고 볼 수 있다.

또 다른 사례로, 2021년 7월 23일 CNIL은 보건부에 서한을 보내 사용자가 Covid 인증서를 저장할수 있도록 하는 "TOUSANTICOVID" 앱이 GDPR을 준수하도록 필요한 조치를 취

---

45) CNIL calls for changes in the use of US collaborative tools for higher education and research, 27 May 2021. https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche.(2024.4.30. 최종확인)

46) Executive Order 12333 United States Intelligence Activities Avaibke at https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf (2024.8.27. 확인)

47) CNIL, Mémoire en Observations, Conseil d'Etat, Referé L, 521-2 CJA, 8 Oct. 2020, p. 9.

할 것을 요청한 바 있다. 이 서한에서 CNIL은 "유럽연합의 배타적 관할권에 속하는 회사"의 솔루션을 사용하기 위해 서비스 제공업체 변경을 고려할 것을 보건부에 요청했다.[48] 유사하게, CNIL은 2023년 9월 3일, 체육부(Ministry of Sports)에도 민감하지 않은 스포츠 데이터 처리를 위해서도 'EU 역외의 비유럽 법률'에 대하여도 강력한 데이터 보호를 보장할 수 있는 클라우드 컴퓨팅 솔루션을 사용할 것을 권고한 바 있다.[49]

그러나 결국 CNIL은 2024년 1월 31일 공익 단체인 '건강 정보 플랫폼'(Plateforme des données de santé, 이하 "GIP PDS")의 건강 데이터 처리를 위해 미국 클라우드 서비스 제공자인 Microsoft를 승인하는 것으로 마무리했다. 그 이유로 GIP PDS의 기술적 기능적 요구조건에 부합하는 호스팅 서비스를 제공할 수 있는 업체가, 즉 주권적 솔루션(sovereign solution)을 제공할 수 있는 다른 기업이 없기 때문이다. 프랑스 정보보안청(French National Agency for Information Systems Security, 이하 "ANSSI")에서 발행한 SecNumCloud 가이드라인(SNDS)에 명시된 대로 유럽 법률의 적용을 받고 적절한 수준의 보호를 제공하는 서비스 제공업체를 채택해야 한다. 그러나 이러한 기준을 충족하는 자국 호스팅 업체가 존재하지 않아 결국 해외업체(MS)를 이용할 수밖에 없었던 것이다. 그러나 궁극적으로 추후 자국기업으로의 이전을 위해 3년만 이러한 해외업체의 호스팅을 허용하였다.[50]

2-3) 독일

독일 역시 프랑스만큼은 아니나 비슷한 입장을 취한바 있다. 2022년 11월 25일, 독일 데이터 보호 회의(German Data Protection Conference, 이하 "DSK"라 한다)는 Microsoft 365에 대한 평가를 발표하면서 "Microsoft는 계약상 광범위한 공개를 할 수 있는 권리를 보유하며, 이러한 공개를 시행할 경우 GDPR 제48조에 명시된 요구 사항에 부합하지 않게 될 수 있다"[51]고 언급하였다. 독일 DPA는 이러한 문제에 대해 보다 신중한 접근 방식을 채택

48) EDPB, 2022 Coordinated Enforcement Action, Use of cloud-based services by the public sector, 17 January 2023, p. 25.

49) CNIL, Deliberation No. 2023-084 of 7 September 2023 on a draft decree relating to the organisation and operation of the national platform for combating competition manipulation, section D.

50) Deliberation no. 2023-146 of 21 December 2023 authorising the "Plateforme des données de santé" public interest grouping to implement automated processing of personal data for the purpose of creating a data warehouse in the field of health, called "EMC2". (Request for authorisation no. 2229962v1), published on 31 January 2024. 이에 대하여 프랑스 국내 클라우드 공급업체들은 "기술적으로 Microsoft에 필적하는 서비스를 제공할 수 있는 유럽 클라우드 업체가 없다는 CNIL의 평가에 공식적으로 이의를 제기"하고 "프랑스의 디지털 주권의 이름으로 CNIL의 결정을 재고해 줄 것을 엄숙히 요청"하는 온라인 청원 운동을 시작했다.

51) https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf (2024.8.30. 최종확인)

했지만, 하급심에서 더 엄격한 판결을 내린 사례도 있다. 일례로 2021년 12월 1일 비스바덴 행정법원(Wiesbaden Administrative Court)은 "데이터가 실제로 EU 역외로 이전되는지 여부와 관계없이 기업은 미국 기반 쿠키 관리 제공업체를 사용하여 데이터를 수집할 수 없다"는 최초의 판결을 내린 바 있다. 즉 법원은 "실제로 데이터 '국외 이전'이 발생했는지 여부는 평가하지 않은 것이다. 이 결정[52]은 데이터 수신자가 비EU 당국의 공식적인 요청을 받는다면 데이터가 EU 역외로 이전하지 않더라도 '이전'이 발생한다고 가정한 것이다. 법원은 "데이터가 Akamai 서버에서 처리되기 때문에 제3국으로의 데이터 이전이 발생한다"고 판단했는데, 이는 단순히 "미국 기업인 Akamai Technologies Inc.가 클라우드 법(CLOUD Act)의 적용을 받기 때문"이라고 판단한 것이다.

바덴-뷔르템베르크주 공공조달청(Baden-Württemberg Chamber of Public Procurement)도 2022년 7월 13일에 비슷한 입장을 채택한 바 있다. 바덴-뷔르템베르크주 공공조달청은 장기 요양 시설의 관리시스템 공급을 위한 입찰을 진행하였고 AWS의 유럽 자회사와 독일 스타트업인 "PM"이 입찰했다. AWS가 재입찰에 선정되었으나 바덴-뷔르템베르크주 공공조달청은 2022년 7월 결정에서 "실제 제3국에서 개인정보에 접근 했는지 여부와 관계없이 제3국에서 접근할 수 있는 플랫폼에 개인정보가 저장되 있는 경우에도 국가 간 이전으로 추정해야 한다"고 하면서 AWS와의 계약체결을 무효화 했다. 즉 개인정보에 실제 접근하였는지 여부는 상관없이 개인정보에 접근할 가능성만으로 GDPR의 "이전(transfer)"에 해당된다고 본 것이다.

따라서 미국 법률의 적용을 받는 기업을 이용하는 것만으로도 데이터 국외 "이전"으로 간주한 것이다. 그러나 바덴-뷔르템베르크주 DPA는 이 결정이 "법적으로 의심스럽다"고 판단하여 부정적 태도를 취하였고,[53] 결국 2022년 9월 7일에 카를스루에 항소법원(Karlsruhe Court of Appeal)에서 이 결정이 뒤집혔다.

4-3. '위험 제로 접근방식'의 한계

앞서 검토한 바와 유럽 전역의 DPA는 국경 간 데이터 이동에 대하여 '위험 제로' 접근 방식을 추진하고 있는 것으로 보인다. 특히 CSP가 외국 기업인 경우 외국 정부의 유럽 개인정보 접근에 대하여 '위험 제로' 접근 방식을 추진하고자 하는 것으로 보인다. 그러나 EDPB는 "EEA 주권 요건을 준수하는 클라우드 솔루션"이 무엇을 의미하는지 명확히 설명하지 못하고

52) https://rewis.io/urteile/urteil/2tj-01-12-2021-6-i-73821wi/ (2024.8.27.최종확인)
53) https://www.baden-wuerttemberg.datenschutz.de/stellungnahme-zum-beschluss-der-vergabekammer-bw/ (2024.8.27.최종확인)

있으며 '디지털 주권'과 '주권 요건'이라는 용어는 법적 관점에서 매우 모호한 용어이고 불투명하며 혼란을 초래할 수 있다(Christakis, 2020). 어쨌든 EDPB는 "EEA에 데이터를 저장하는 비(非)EU CSP를 사용할 때 외국 정부기관이 유럽 개인정보에 접근할 위험"이 있다는 가정에 근거하여 "EEA 주권 클라우드 솔루션 준수(compliant EEA–sovereign cloud solutions)"를 제안하고 있는 것으로 보인다. 그러나 EU에 본사를 둔 CSP를 통해 데이터를 저장하는 경우에도 마찬가지로 외국 정부의 접근 위험이 모두 제거되는 것은 아니다.

1) 데이터 국지화의 문제점

1–1) 국가안보와 프라이버시 비친화적

데이터 국지화 정책은 스노든 사태에 대한 반응으로 미국과 같은 외국의 정보기관의 감시로부터 자유와 안전을 확보하려는 시도의 일환으로 본격화 되었다. 즉 외국의 감시에 대한 우려, 데이터 보안 등의 관점에서 제안된 것이다. 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(김현경.2017). 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(Chander & Le, 2014). 또한 악성소프트웨어(malware)의 사용은 데이터를 국지화로 막을 수 있는 성질의 문제가 아니다.

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 국지화 요건에 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(Anupam Chander & Uyên P. Lê, 2015). 또한 특정 지역에 거주하는 이용자들의 정보를 그 지역에 중앙집중화한다면 특정 국가국민들의 감시를 더 용이하게 집중할 수 있도록 해주므로 외국의 첩보부담을 줄여주는 결과를 초래할 수도 있다(이를 "Jackpot" 문제라 한다).

이러한 국가안보와 유사한 사유로 데이터 국지화는 개인정보/프라이버시 보호에도 그다지 친화적 정책이라고 보기 어렵다(Daniel Castro, 2013) 데이터 국지화 서버는 여러 지역에 있는 여러 서버에 데이터를 분산시킬 기회를 감소시킨다. 이러한 경우 위에서 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(Patrick S. Ryan et al 2013). 샤딩(sharding)은 전 세계의 서버에서 데이터베이스 테이블의 행을 개별적으로 보관하는 프로세스로, 데이터를 작동하기에 충분한 각각의 파티션을 만들지만, 개개인을 재식별하기에 충분하지는 않다. 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(Dharmakumar, 2013).

1–2) 반(反)경제적 효과

한편 데이터 국지하는 경제적 효과 측면에서도 그다지 긍정적이라고 볼 수 없다. 데이터 국지화 조치는 종종 자국 지역경제 활성화를 위한 동기유발이 될 수 있다. 그러나 데이터 국지화는 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(Mari, 2013). 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(Anupam Chander & Uyên P. Lê, 2015). 데이터 센터는 최고 수준의 보안을 유지하는 경우 비용이 많이 든다. 브라질은 서반구에서 데이터센터를 구축하는데 가장 비싼 국가라는 연구도 있다. 브라질에 데이터 센터를 짓는데는 평균 6천 9백 억 달러가 들지만, 칠레와 미국에서는 1천 2백 5십만 달러와 4천 3백만 달러의 비용이 든다. 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(FROST & SULLIVAN, 2012).

한편 운영비용의 4분의 3이 에너지 비용이므로 인건비 비중이 높지 않으며 결국 데이터 센터의 고용효과는 미비하다(DINES, 2011). 2013년 데이터 센터 위험도 지수에 따르면, 호주, 러시아, 중국, 인도네시아, 인도 및 브라질은 데이터 센터를 운영하는 데 있어 가장 위험한 국가에 해당된다.[54]

데이터 국지화에 따른 경제적 비용뿐만 아니라 그 잠재적 이익 역시 정부가 예측한 것보다는 훨씬 제한적이다. 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(FROST & SULLIVAN,2012). 따라서 모순되게도 데이터 국지화 규율의 수혜자는 오히려 서버와 장비를 공급하는 외국의 글로벌 업체인 경우가 많다.[55] 브라질의 경우에도 오히려 수입산이 서버장비시장을 지배하고 있기 때문에 내국의 장비업체는 이러한 데이터국지화 규정으로부터 혜택을 받지 못한다고 한다.[56] 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(Anupam Chander & Uyên P. Lê, 2015).

1-3) 정보의 자유 억제

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 공식적

54) CUSHMAN & WAKEFIELD, DATA CENTRE RISK INDEX (2013), http://www.cushmanwakefield.com/~/media/global-reports/data-centre-risk-index-2013.pdf, at 7. 본 연구는 30개 국가를 대상으로 성공적인 데이터 센터 운영에 영향을 미치는 위험요인에 대한 분석을 기반으로 하고 있다.

55) 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).

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

인 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.[57] 그러나 인권운동가들은 외설정보 등을 이유로 한 정부의 추적감시행위는 정부의 진정한 의도를 감추기 위한 것이며, 결국 반대의견을 억누르고 국제적 소통을 막기 위한 것이라고 한다.[58] 언론은 이란인들이 허가된 웹사이트만 방문하도록 허용하는 것은 정권에 의한 책략이라고 비판한다.[59] 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.[60]

아마도 데이터 국지화의 가장 큰 위험은 독재국가들이 정보에 대한 통제를 확장하는 것이다. 자유주의 국가들이 독재체계에 의한 정보의 통제를 비판할 때, 독재국가는 자유주의 국가들 역시 데이터 국지화룰 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(Anupam Chander & Uyên P. Lê, 2015). 데이터가 외부로 나가는 것을 차단하고 들어오는 데이터를 걸러내는 기능으로 무장한 데이터 국지화는 감시 및 검열을 위한 인프라를 제공함으로써 정부의 데이터 통제권을 더욱 결집, 강화 시킬 수 있다(Anupam Chander & Uyên P. Lê, 2015).

2) 해외 정부의 접근 가능성 : 직접 접근(“Direct” Access)

정부가 민간 부문이 보유한 데이터에 접근하는 첫 번째 주요 형태는 데이터에 대한 직접 접근이다. OECD에 의하면 직접 접근은 정보기관이 기업등 민간에게 데이터 제공을 요청하지 않고 민간 행위자가 보유한 데이터를 얻기 위해 직접 노력하는 상황을 말하며, 실제로 거의 모든 경우에 민간 행위자는 정부가 데이터에 접근하려는 사실을 알지 못한다. 예를 들어 신호 정보 및 감청, 은밀한 첩보 활동 또는 해킹을 통해 이러한 작업을 수행할 수 있다

57) 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.
58) Jillian C. York, Is Iran’ Halal Internet Possible?, ALJAZEERA (Oct. 2, 2012, 08:18),
59) Government Blocks Google and Gmail, While Promoting National Internet, REPS. WITHOUT BORDERS (Sept. 24, 2012).
60) VN Digital Content Firms Find Home Disadvantage, VIỆT NAM NEWS (Sept. 22, 2008), http://vietnamnews.vn/economy/business-beat/180617/vn-digital-content-firms-find-home-disadvantage.html(베트남에서 서비스되고 있는 Yahoo!’ 서버는 싱가포르에 있다.

(Christakis et al., 2021). 두 번째 형태는 “강제 접근”이다. 이는 법률에 근거하여 국가안보 또는 범죄 수사를 이유로 정부기관이 자국 기업이 보유한 데이터에 대한 접근을 요청하고, 대상 기업은 이러한 요청에 따라 해당 데이터를 제공 혹은 접근하게 할 의무를 지는 모든 상황을 의미한다.[61] 이 경우 정부 당국은 자체적인 기술적 수단을 통해 데이터에 접근하는 것이 아니라 개인정보를 보유한 기업에 대하여 협조 의무를 요구하는 것이다.

미국은 EO 12333에 따라 미국 정보기관이 자체 기술 자원을 사용하여 미국 외의 외국인으로부터 직접 데이터를 수집 할 수 있도록 허용하고 있다.[62] 여기에는 미국으로 전송 중인 통신을 가로채거나 유럽을 포함한 외국 영토에 있는 데이터에 직접 액세스하는 것이 모두 포함될 수 있다. FISA 702와 달리 EO 12333은 대량 데이터 수집도 허용한다. 반면, EO 12333은 해당 데이터를 보유한 기업이나 단체로 하여금 데이터 제공을 의무화하는 법적 근거로는 사용할 수 없다. 즉 '강제 접근(compelled access)'의 법적 근거가 아니다.

유럽 기업이 외국 정부의 '직접 액세스' 위험으로부터 자국민의 개인정보를 보호하려면 당연히 미국뿐만 아니라 모든 국가(악의적인 외국 행위자 및 러시아 같은 국가의 '프록시' 포함)가 제기하는 위험을 고려해야 한다. 따라서 소위 '주권적' 솔루션을 선택한다고 해서 외국 정부의 '직접 액세스'에 대한 보호가 제공될 것이라고 볼 수는 없다.

한편 미국 CSP는 "미국인"으로 간주되므로 미국인을 "불합리한 수색 및 압수로부터" 보호하는 수정헌법 제4조를 포함하여 미국 헌법이 제공하는 모든 보호 혜택을 받을 수 있다. 수정헌법 제4조의 목적은 미국 정부의 자의적인 행동으로부터 미국 국민을 보호하는 것이며 미국 영토 밖의 외국인에 대한 연방 정부의 행동을 제한하는 것은 아니다. 또한 미국 국적자 여부와 무관하게 일부 미국 법집행기관은 미국 영토내 데이터보다 미국 영토 외부에 저장된 데이터에 대해 더 광범위한 접근을 허용한다. 오히려 미국 내에서 접근이 이루어지는 경우, 미국 법 집행기관 및 국가안보 기관은 범죄 수사를 위한 상당한 이유가 인정된 경우 영장 발부 또는 해외정보감시법원(Foreign Intelligence Surveillance Court)의 판사의 감독하에 이루어지는 FISA 702의 절차 등의 경우에만 데이터에 대한 접근이 가능하다.

즉 'EEA 주권 클라우드 솔루션'이 외국 정부가 유럽 개인정보에 ‘직접 접근'할 위험을 모두 제거해 주는 것은 아니며, 미국 이외의 CSP는 오히려 미국 정부 당국의 '직접 접근' 시도에 미국 업체보다 더 취약할 수 있다.

---

61) 물론 해당 기업은 관할권의 존재, 데이터의 소유, 보관 및 통제권의 존재 또는 법률의 충돌 가능성 등 다양한 법적 근거를 이유로 이러한 요청에 이의를 제기할 수 있다.

62) EO 12333의 자세한 내용은 Intelligence Community Legal Reference Book, Winter 2020, p. 693 https://www.dni.gov/files/documents/OGC/IC%20Legal%20Reference%20Book%202020.pdf (2024.8.18.)

3) 미국의 인적 관할 확장

FISA 702와 CLOUD Act는 정보수집 요청을 미국 영토 내에 저장된 데이터로만 제한하지 않는다. 따라서 핵심 쟁점은 유럽 데이터 컨트롤러가 CNIL과 같은 DPA가 제안한 대로 유럽 경제 지역(EEA)의 CSP를 사용하는 경우 "FISA 702 또는 CLOUD Act에 근거한 데이터 제공요청에 응할 필요가 없는가"라는 점이다.

그러나 데이터를 처리하는 기업의 국적은 FISA 702 또는 CLOUD Act 명령을 준수해야 하는지 여부와 무관하다. 미국 법원의 인적 관할권이 적용되는 모든 기업은 FISA 702 또는 CLOUD Act에 따른 미국 명령이 적용될 수 있다. 그리고 미국 경제와 관련이 있는(관련성이 적다 하더라도) 모든 회사는 미국 관할권의 적용을 받을 수 있다.

미국은 미국의 인적 관할권을 상당히 광범위하게 해석하고 있다. 미국 법무부는 "미국 관할권은 미국 기업, 미국에 본사를 둔 회사 또는 미국인에 의해 소유된 회사로 제한되지 않는다. 미국 영토에서 서비스를 제공하는 회사가 미국 관할권의 적용을 받는지 여부는 해당 법인이 관할권 행사를 근본적으로 공정하게 만들기에 충분한 미국과의 접촉이 있는지 여부에 대한 사실에 따라 달라질 수 있다. 해당 기업이 미국에서 활동을 수행하는 특권을 의도적으로 활용하거나 의도적으로 미국으로 활동을 지시할수록 미국 법원이 해당 회사가 미국 관할권의 적용을 받는다고 판단할 가능성이 높아지게 된다" 며 미국 관할권의 범위가 미국 기업만으로 제한되지 않는다는 점을 분명히 밝힌 바 있다.[63]

미국 정부는 "1. 미국 법인, 2. 미국에 사무소가 있는 외국 법인(예: 지사), 3. 인적 관할권 요건을 충족할 만큼 미국과의 접촉이 충분한 미국 내 외국 법인"에 대하여 인적 관할권을 가진다. 미국 법원은 외국 법인의 인적 관할 여부를 결정할 때 해당 법인이 미국에 위치한 사람이나 기업에 서비스 또는 제품을 판매하는지, 미국에서 마케팅 및 광고를 하는지, 미국 서비스 제공업체와 협력하는지 등 다양한 요소를 분석한다. 또한 온라인으로 서비스를 제공하는 외국 법인의 경우 미국 법원은 해당 외국 법인이 미국에서 액세스할 수 있는 대화형 웹사이트를 보유하고 있는지, 미국 IP주소를 차단하고 있는지, 미국 기반 서버를 사용하고 있는지 여부도 분석한다. 일반적으로, 이러한 요소들 중 어느 것도 인적 관할권의 존재 여부를 결정하는 요소는 아니지만, 외국 법인이 미국에서 사업을 수행한 사실을 바탕으로 인적 관할권이 존재하는지 평가하기 위해 함께 고려된다(Greenberg Traurig LLP, 2022).

일례로 Plixer Int'l, Inc. v. Scrutinizer GmbH,[64] 사건에서 2018년 미국 제1순회 항소법

63) US Dep't of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act", White Paper, April 2019 available at www.justice.gov/CLOUDAct ("US CLOUD Act White Paper") p. 17.

64) Plixer Int'l, Inc. v. Scrutinizer GmbH, 905 F.3d 1 (1st Cir. 2018).;

원은 미국과 물리적 연고가 없지만 전 세계 기업이 웹사이트를 이용할 수 있도록 한 독일 CSP에 대하여 인적 관할권을 행사할 수 있는 최소한의 미국과의 접촉이 있었다고 판시하였다. 해당 독일 회사는 미국에 소송 서비스를 위한 사무실, 전화번호, 대리인이 없었고, 미국에서 광고를 하지 않았으며, 유로화로만 결제를 받았고, 계약서에 독일 법원에서 판결을 내리는 독일법만이 분쟁에 적용된다고 명시했으며, 직원들이 업무상 미국으로 출장을 가지 않았다. 그러나 독일 회사의 웹사이트는 영어로 게시되었고, 미국 사용자를 차단하기 위해 웹사이트에 대한 액세스를 제한하려고 시도하지 않았으며, "자사 서비스가 미국 사용자를 위한 것이 아니라는 면책 조항을 게시하는 낮은 수준의 기술적인 조치도 취하지 않은바, 이러한 점이 인적 관할을 인정하는데 고려되었다(Greenberg Traurig LLP, 2022). 즉 법원은 이러한 요소를 고려할 때 독일 회사가 "인적 관할권의 행사를 합리적으로 예상할 수 있다"고 판결했다.[65]

결국 미국의 인적 관할의 대상이 되는 사업자는 미국에 자회사를 둔 외국기업이나, 미국 시장을 대상으로 활동하는 기업까지 폭넓게 포함된다. 미국 이외의 회사가 미국 시장을 대상으로 해외에서 디지털 서비스를 제공하는 경우 즉 미국 사이트에서 광고하는 경우 미국 당국은 이를 '미국 내'로 간주할 수 있다.[66] 그렇게 볼 때 주요 유럽 클라우드 제공업체(SAP, OVH, 3DS Outscale 등)는 대부분 미국에 진출해 있으므로 미국 CSP와 마찬가지로 미국 법률의 적용을 받을 가능성이 높다.

4) 소버린 클라우드(EEA-sovereign) 업체의 이의 제기의 실효성

앞서 언급하였듯이 EU 법인이 전적으로 미국 영토밖에 위치하더라도 미국이 EU 법인에 대하여 관할권을 주장하는 것이 합당할 정도로 미국과 충분한 접촉이 있고 영장에 따라 요청된 데이터를 소유, 보관 또는 통제하고 있다면 여전히 CLOUD Act의 적용을 받을 수 있다(Christakis, 2017). 물론 미국 당국으로부터 이러한 데이터 제공(생성) 명령을 받은 유럽 CSP는 미국의 인적 관할권에 속하지 않거나 유럽 법률이 유럽 개인정보를 외국 정부에 공개하는 것을 금지하고 있다며 미국 법원에 이의를 제기할 것이다. 미국 기업도 (관할권을 이유로 한 것은 아니지만) 이러한 미국 정부 또는 법원의 명령에 이의를 제기할 수 있으며 실제 몇몇 미국 CSP는 유럽 데이터 컨트롤러와 계약을 통해 EU 또는 회원국 법률과 상충되는 요청에 대해 체계적으로 이의를 제기하기로 약속한 바 있다(소버린 클라우드의 내용임).

---

https://casetext.com/case/plixer-intl-inc-v-gmbh-3 (2024년 8월 27일 확인)

65) Plixer Int'l, Inc. v. Scrutinizer GmbH, 905 F.3d 1 (1st Cir. 2018).; https://casetext.com/case/plixer-intl-inc-v-gmbh-3 (2024년 8월 27일 확인)

66) https://casetext.com/case/plixer-intl-inc-v-gmbh-3 9페이지

그러나 엄격히 이러한 이의제기가 성공할 것을 보장할 수 없기 때문에 미국 CSP의 이러한 약속은 미국 정부의 데이터 접근에 대한 해결책이 될 수 없다. 이는 유럽 기업이 CLOUD Act에 근거하여 미국 법원으로부터 받은 명령에 대해 이의를 제기하려는 경우에도 동일하게 적용된다. 유럽 기업은 강력한 주장을 펼칠 수 있지만 성공할 것이라는 보장은 없다. 인적 관할권에 관한 기존 판례에 의하면 미국 경제와 관련이 있는 어떠한 유럽 기업도 미국 법률을 준수해야 하며 따라서 '위험 제로'라는 것을 입증할 수 없다.

일례로 미국의 캐나다 내 금융 데이터의 제출 요청을 다룬 노바 스코샤 은행 사건(Bank of Nova Scotia case)[67]에서 캐나다 은행은 미국의 인적 관할에 대해 이의를 제기하였지만 성공하지 못했다. 마크 리치(Marc Rich) 사건[68]에서 스위스 회사는 미국 법원의 인적 관할에 속하지 않으며 스위스 법이 요구한 자료 제출을 금지한다는 이유로 소환장을 기각해 달라고 신청했지만 미국 법원은 이러한 기각 신청을 기각하고 마크 리치에게 문서 제출을 거부한 책임을 물은바 있다.

이러한 태도는 역으로 유럽도 마찬가지다. 새로 채택된 “EU 전자 증거법(EU e-Evidence Regulation)”은 데이터가 저장된 위치에 관계없이 비유럽 업체에도 동일하게 적용된다.[69] 이 법은 CLOUD Act와 거의 동일한 내용이며, '데이터의 위치에 관계없이 (regardless of the location of the data)' 유럽의 데이터 생성(제공) 요청에 적극적으로 대응해야 할 의무를 규정하고 있다. 물론 EU 전자 증거법에 근거하여 데이터 제공 요청을 받은 미국 기업은 법 충돌 상황에 직면하게 된다. 미국의 저장통신법(Stored Communications Act)과의 충돌 등이다. 그러나 이는 미국의 CLOUD Act에 의해 데이터 제공 명령을 받은 유럽/미국 기업 역시 GDPR 제48조 위반의 가능성으로 인해 유사한 ’법 충돌‘ 상황에 직면하게 된다. 법률의 상충(충돌)이 존재한다고 해서 해당 국가의 법원이 결정을 보류하거나 중단할 것이라는 보장은 없다. 즉 이러한 위험은 회사의 국적에 관계 없이 동일하게 존재한다고 볼 수 있다.

미국 정부는 데이터 명령이 이행되도록 상당한 수단을 동원할 수 있다. 일부 유럽 제공업체는 미국 정부의 명령이 있더라도 미국 법률을 준수하지 않겠다고 했지만, 이러한 행위(해당 기업이 미국 관할권에 속하고 해당 데이터를 저장·보유·통제하고 있다고 간주되는 경우)

---

67) Grand Jury Proceedings (Bank of Nova Scotia), 740 F.2d 817 (11th Cir. 1984), cert. denied, 469 U.S. 1106 (1985)

68) Marc Rich & Co., A.G., 707 F.2d 663 (2d Cir. 1983), cert denied, 463 U.S. 1215 (1983).

69) Article 1(1) of the e-Evidence Regulation, which emphasises that the obligation to produce data exists “regardless of the location of the data” (Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, [2023] OJ L191/118, 12 July 2023 Art. 5(6). (Regulation (EU) 2023/1543).

에 대하여 미국 법원은 특별 벌금과 민형사상 불이행 제재를 포함한 광범위한 구제책을 마련할 수 있는 권한을 가지고 있다. 일례로 미국 법원은 EEA 클라우드 제공업체에게 유럽에 저장된 요청 받은 데이터를 제공하거나 지연일마다 10만 달러의 벌금을 지불하라는 금지 명령을 내릴 수 있다.[70] EEA CSP가 이를 따르지 않을 경우 미국 내 자산을 압류하거나 미국 시장에서 배제될 위험, 심지어 소속 직원에 대한 형사 소송의 위험까지 감수하게 될 수 있다. 미국 시장과 그 시장에서 얻는 모든 경제적 이익을 포기할 의사가 없다면 미국 법의 적용을 받는 대부분 기업은 규정 준수를 거부하기 어려울 것이다. 적어도 당분간은 이러한 문제에 대해 '위험 제로'는 불가할 것이다.

5. 마무리

세계 모든 국가는 서로 고유한 법체계와 문화를 가지고 있으며 이를 형성해 온 정치 · 사회 · 경제적 배경이 각각 다르다. 따라서 전 세계적으로 통일된 데이터 규범을 만든다는 것은 현실적으로 거의 불가능한 일이다. 데이터의 역외 이동과 관련된 정책은 각 국가가 처한 정치적 · 경제적 상황에 따라 다를 수밖에 없다. 특히 개인정보는 여타 데이터와 달리 인공지능 등 데이터 경제의 기반이 되는 기술과 서비스에 있어서도 핵심일뿐더러 자국민의 기본권과 관련되므로 더욱 신중을 기할 수밖에 없다.

정치경제학적으로 자국 플랫폼을 가지지 못하고 인공지능 핵심기술의 선두를 미국에 빼앗긴 유럽 입장에서 '주권'을 이유로 개인정보의 역외 이전을 엄격히 제한하는 것은 그럴만하다고 볼 수 있다. 중국이나 러시아 역시 자국의 정치체계와 경제적 상황에 비추어 볼 때 개인정보를 비롯한 데이터 역외 이전의 금지를 원칙으로 하는 것 역시 그럴 수 있다고 본다. 연혁적으로 데이터의 자유로운 거래와 이용을 허용하고 이를 기반으로 데이터 경제를 확장해온 미국 역시 현재의 자유로운 거래와 활용 중심의 데이터 규범이 납들할 만 하다. 하지만 인터넷 공간에서 데이터 규범의 국제적 합의의 실패는 국가 간에 논쟁과 갈등을 일으킬 수 있다. 그렇다면 이러한 상황에서 우리의 입지를 어떻게 가져가야 하는가? 단순히 선진국 벤치마킹을 통해 해결할 문제가 아니다. 데이터 주권에 대한 감정적 호소에 기반하여 유럽식 '위험 제로– 데이터 국지화' 방식을 채택하기에는 미래지향적 데이터 경제를 지탱할 만큼 데이터가 양적/질적으로 만족스러운 상태라고 보기 어렵다. 집안 침대 밑에 숨겨둔 돈처럼, 내 집에 보관해 둔다고 해서 데이터가 마냥 안전한 것만도 아니다. 데이터가 그 집안, 그 나라

70) 유사한 예로 2014년 미국 정부는 야후가 국가안보국에 사용자 데이터를 넘기지 않으면 하루에 25만 달러의 벌금을 부과하겠다고 한 바 있다 https://www.theguardian.com/world/2014/sep/11/yahoo-nsa-lawsuit-documents-fine-user-data-refusal (2024.8.27. 최종확인)

안에 보관되어 있다고 할지라고 범죄자들은 결국 불법적인 접근을 시도한다. 데이터에 대한 국지화 규범을 포함한 유럽의 “위험 제로 접근 방식”은 경제적 파급효과, 데이터 협력 필요성, 실효성 등에 비추어 볼 때 신중한 검토가 필요하다. 우리가 개인정보의 역외이전에 대한 유럽식 상호적정성 모델을 채택한 것은 국내 경제 상황에서 유럽 시장의 비중을 무시할 수 없었기 때문이다. 즉 경제의 대외의존성이 상당한 우리 입장에서는 통상 국가별로 유연한 방식을 채택하면서 자국 이익을 고수할 수 있는 전략적 묘안을 찾아야 할 것이다.

〈참고문헌〉

김민호, 개인정보의 의미, 성균관법학 제28권 제4호, 2016, 13-14쪽.

김현경, '데이터 주권'과 '개인정보 국외이전' 규범 합리화 방안 연구, 성균관법학 제31권 제4호(2019.12), 623-624쪽.

김현경, 데이터 속성과 국지화 규범의 법적 쟁점에 대한 고찰, 토지공법연구 제78집 (2017.5), 244-254쪽.

김현수, 미국에서의 온라인 다크패턴 규율과 시사점, IT와 법연구 제26권, 2023, 48쪽.

김현수, 소비자보호와 정보주체의 권리 실현 집행체계- 미국 FTC의 사례를 중심으로 -, 개인정보보호법학회 학술제미나 자료집, 2024.3.29

박선욱, 미국과 EU의 개인정보보호에 관한 법제 비교분석. 동아법학(83),2019, 269-309쪽.

오태현, "EU 개인정보보호법 발효: 평가 및 대응방안", 오늘의 시계경제, 대외경제정책연구원 2018.5., 11-12쪽.

이인호외, 개인정보감독기구 및 권리구제방안에 관한 연구, 한국전산원, 2014, 49쪽.

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/ 2024. 9.10. 확인

Chander, Anupam and Le, Uyen P., Lê, Data Nationalism, 64 EMORY L.J. 677(2015) at 716-717.

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

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.

European Commission, Communication from the Commission to the European Parliament and the Council, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation', 24 June 2020, COM(2020) 264 final, at 17

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). p. 10.

Greenberg Traurig LLP, Application of the CLOUD Act to EU Entities, Report for the Dutch Ministry of Justice and Security NCSC, July 26, 2022, p. 3.

Herbert J. Spiro, "Privacy in Comparative Perspectives", in: Privacy Nomos XIII (J. Roland Pennock & John W. Chapman eds., 1971), p. 122.

Joel R. Reidenberg, "A New Legal Paradigm? Resolving Conflicting International Data Privacy Rules in Cyberspace", 52 Stan. L. Rev. 1315, 1342 (May, 2000).

Millard and Kamarinou, 'Article 27', in: Kuner, Bygrave, and Docksey (eds), The EU General Data Protection Regulation: A Commentary (OUP 2020), 589-598, at 590.

Yves Poullet, "Data Protection Between Property and Liberties: A Civil Law Approach", in: Amongst Friends in Computers and Law (H.W.K. Kaspersen & A. Oskamp eds., 1990), pp. 170-175.

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

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

Priscilla M. Regan, A Design for Public Trustee and Privacy Protection Regulation, 44 Seton Hall Legis. J. 487, 505 (2020)

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. 2024. 9.10. 확인

Rohin Dharmakumar, India' Internet Privacy Woes, FORBES INDIA (Aug. 26, 2013), http://forbesindia.com/article/checkin/indias-internet-privacywoes/35971/1#ixzz2r0zriZTF. 2024. 9.10. 확인.

Ryngaert and Taylor, 'The GDPR as Global Data Protection Regulation?', 114 AJIL Unbound 5 (2020), at 7-8.

Theodore Christakis, "Data, Extra-territoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence – Legal Opinion on the Microsoft Ireland Case (US Supreme Court)" (November 29, 2017). The White Book: USA v.

Microsoft: What Impact, CEIS & The Chertoff Group White Paper (2017), p.3 Available here: https://ssrn.com/abstract=3081958

Theodore Christakis, "Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?" in Randal Milch, Sebastian Benthall, Alexander Potcovaru (eds), "Cybersecurity and Privacy in a Globalized World – Building Common Approaches", (New York University School of Law, e-book, 2019), at 60-76. Available here: https://ssrn.com/abstract=3397047.

Theodore Christakis, "European Digital Sovereignty: Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy, MIAI/Grenoble Data Institute e-book, December 2020

T. Christakis, K. Propp, P. Swire, "Towards OECD Principles for Government Access to Data: Can Democracies Show the Way?", LAWFARE, 20 December 2021. (available here: https://www.lawfaremedia.org/article/towards-oecd-principles-government-access-data).