CENTER FOR FUTURE WARFARE STUDIES
INSTITUTE OF INTERNATIONAL STUDIES
SEOUL NATIONAL UNIVERSITY

서울대학교 국제문제연구소
미래전 연구센터
08826 서울시 관악구 관악로 1
서울대학교 종합교육연구동 220동 517호

Tel. 02-880-6311
Fax. 02-871-4115

Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전연구센터 워킹페이퍼 No.77(발간일: 2021.5.26.)

디지털 안보 규범외교의 미중경쟁과 한국:

데이터 규범경쟁의 쟁점과 시사점[1)]

유준구 국립외교원 연구교수

Ⅰ. 머리말

전 세계 주요국들이 4차 산업혁명의 주도권을 둘러싸고 디지털 패권 경쟁을 전개하는 가운데, 진영 간 디지털 안보 규범경쟁이 개별국가 및 다자협의체에서 가속화되고 있다. 일반적으로 사이버 안보가 ICT 네트워크, 컴퓨터 시스템, 디지털 구성요소인 정보 · 데이터 등 포괄적인 이슈를 다루고 있는 반면 디지털 안보의 경우 사이버 안보의 하위 부분인 온라인상 실재하는 정보 · 데이터 및 기술과 관련되어 있다. 디지털상의 정보 및 기술을 보호한다는 디지털 안보 논의에서 데이터의 중요성이 강조되고 있는 바, 각국은 데이터 문제를 국가안보 관점에서 접근하고 있다. 즉, 4차 산업혁명 시대 데이터는 인간, 자본 등 기존의 생산요소를 능가하는 석유와 같은 핵심 자원으로 부상하고 있는 바, 인터넷이 신경망 내지 혈관이라면 데이터는 혈액이라 할 수 있다. 현재 세계 데이터 시장은 2017년 1,508억 달러에서 2020년 2,100억 달러로 연간 11.9% 규모로 급속히 성장하고 있는 상황이다(IDC, 2017). 이에 따라 최근 수년간 한국을 포함한 주요국들이 인공지능(AI: Artificial Intelligence) 국가 전략 · 정책을 수립함과 동시에 디지털 뉴딜 및 데이터 뉴딜 정책을 수립하여 추진하고 있다. 개별국의 데이터 정책은 단순 산업경쟁력 강화 차원은 물론 '데이터의 안보화', 즉 국가안보 관점에서 설립 · 추진되고 있다. 이에 따라 미국, 중국, 유럽

* 이 글은 저자의 논문 2021년 『국가전략』 제27권 2호(2021)에 게재한 "국가안보 차원의 데이터 주권의 이중성과 시사점"을 편집하여 수록한 것임을 밝힙니다.

연합(EU: European Union), 일본 등은 자국의 데이터 관리체제 전반을 고려하면서 '데이터 안보'에 입각한 법 · 제도 정비에 박차를 가하고 있다. 또한, 주요국들은 국내적 체제 정비를 바탕으로 자국에 유리한 지역적 · 국제적 차원의 데이터 안보 구상을 제안하면서 지지를 확대 · 유도하고 있다. 이러한 데이터 안보 경쟁은 최근 화웨이를 둘러싼 미 · 중 기술패권 경쟁과 연계되어 가속 · 심화되고 있다.

4차 산업혁명과 관련한 기술패권 경쟁에서 표준화 및 규범 설정이 주요 쟁점인 것처럼 데이터 안보의 핵심적 쟁점 역시 데이터 관리체제에 있어 일종의 기준 및 규범을 마련하는 것이다. 표준 및 규범 설정 문제는 미중 간 전략적 경쟁이 심화되는 가운데, 4차 산업혁명 시대 국제 안보 · 경제 질서를 재편할 기술패권을 중심으로 미중 간 경쟁 분야의 융 · 복합화가 가속화되는 상황과 맞물려 더욱 중요해지고 있다. 즉, 미 · 서방과 중러 등 주요 기술강국들은 첨단기술이 국제안보에 미치는 융 · 복합 환경 하에서, 4차 산업혁명 플랫폼 기술인 데이터, 네트워크, 인공지능 기술의 활용을 통해 사이버, 우주, 자율무기시스템(AWS: Autonomous Weapons Systems)시스템 등 뉴프론티어 이슈를 선도해 나가기 위한 국가안보 전략 · 정책을 수립하고 있다. 특히, 데이터의 경우, 상기 핵심 플랫폼 기술 축적의 기초 자원이 될 수 있으며 신기술과 관련한 군사 · 경제안보의 필수적 자원이다. 따라서 각국은 데이터 개발 · 축적 · 활용에 사활적 경쟁을 하고 있으며 이를 위해 자국에 유리한 데이터 관리체제의 표준화 및 규범 설정을 위해 국내 법제도는 정비를 바탕으로 글로벌 · 지역적 차원의 데이터 관리체제 거버넌스 구축을 추진하고 있다.

데이터 관리체제의 경우 국가, 기업, 개인 등 모든 행위자의 이해가 걸려 있는 문제로 최근 데이터 관리체제에서 국가 · 기업 · 개인 간 첨예하게 대립되는 이슈는 데이터 주권 및 관할권을 누가 어떻게 행사하는 것인 바, 이는 데이터의 이전 · 유통과 '데이터 현지화(data localization)' 문제로 집약되고 있다. 즉, 국가는 안보 및 산업정책 차원에서 데이터의 배타적 주권을 강조하면서도 타국의 데이터 경쟁력 강화는 견제하려는 전략 · 정책을 강화하고 있다. 같은 맥락에서 플랫폼 기업들은 데이터의 자유로운 접근을 중시하면서도 데이터의 독점적 지위를 유지하려는 경향이 강하다. 반면, 개인의 경우 자신의 개인정보를 통제할 수 있는 정당한 권리를 주장하면서도 국가 및 기업에 의한 개인정보 활용을 통한 혜택 역시 공유 받기를 원하고 있다.

또한 데이터 주권 논의는 사이버안보는 물론 최근 신기술 안보 거버넌스 및 규범 논의 전반에서 핵심적 쟁점으로 부각되고 있는 주권문제와 연계되어 있다. 즉, 데이터, 사이버 및 신기술 개발 · 활용이 급속히 증대됨에 따라 신기술 활용으로 인한 국가안보 미치는 부정적 측면이 부각되고 있고 이를 규제하는 규범적 수단으로 주권이 강조되고 있다. 이는 현재 소수의 미국 정보기술(IT: Information Technology) 및 글로벌 플랫폼 기업이 전 세계 사용자들의 데이터를 독과점하는 구조에서 미 · 서방과 중 · 러 등 진영 간 대립은 물론 미국, 일본, EU 등 서방진영 내에서도 갈등이 증대되고 있다. 따라서 주요 디지털 강국들은 국가안보 차원에서 수립된 전략 · 정책들을 바탕으로, 데이터 안보 이니셔티브를 지역화 · 다자화하려는 시도를 강력히 추진할 것이다.

이러한 배경에서 본 논문은 국제안보 차원의 데이터 규범 논의의 동향, 쟁점, 그리고 전망과 시사점을 분석한다. 제2장에서 데이터 안보 및 규범 논의의 이중성을 국제안보 관점에서 분석한 바, 국가들이 데이터 주권을 강조하는 기저에는 분명히 데이터가 단순 정보가 아닌 국가 및 국제안보의 핵심 요소로 인식하고 있음을 고찰한다. 이를 바탕으로 제3장은 주요 디지털 강국의 데이터 주권에 대한 관점, 지향점 및 정책적 대응을 분석한다. 제4장에서는 향후 데이터 주권을 둘러싼 국가, 진영 간 대립의 전망과 시사점을 평가하고 결론에서 우리의 대응 방향을 제시해 본다.

Ⅱ. 데이터 안보 규범 논의의 현안과 쟁점

1. 데이터 안보 논의의 부상

데이터는 4차 산업혁명 시대 혁신성장을 주도하는 자산이자 글로벌 정치, 경제 전반에서 시스템 운영과 새로운 가치 창출을 위한 기반 역할을 수행한다. 데이터 활용이 모든 산업 발전의 매개체 내지 수단 역할을 수행하는 데이터 집약적인(Data-Intensive) 데이터 경제로 진입함에 따라 데이터가 단순 보조재가 아니라 노동, 자본과 같은 새로운 자원으로 간주되고 있다(Economist, 2017.5.). 즉, 초 연결된 개인, 조직, 기업, 정부의 모든 활동이 천문학적인 규모의 데이터를 생성하고, 인공지능을 통해 처리 · 분석되는 데이터 경제 시대에는 데이터 활용이 모든 사회경제 활동의 촉매 역할을 수행한다(정희영, 2020). 그럼에도 불구하고 신기술의 부정적 측면이 적지 않은 것처럼 데이터 역시 안보적 차원의 대응이 시급히 요구되고 있는 상황이다. 데이터가 정치안보에 미치는 파급력은 상당한 바, △빅데이터(Big data) 권력과 사생활 침해, △데이터 훼손 및 유출, △데이터 오용과 조작정보, △데이터의 군사적 활용, △기술패권 경쟁과 데이터 안보화 등 국가 · 지역 · 글로벌 차원의 데이터 안보 이슈가 대두되고 있다(김상배, 2020).

데이터의 정치 · 경제적 중요성이 높아짐에 따라 데이터 관리체제 전반에서 국가, 기업, 개인 간 '데이터 주권' 논의가 부상하고 있다. 국가 차원에서는 데이터의 훼손, 악용 등 국가안보 및 공공이익을 고려한 주권적 규제가 필요한 반면 데이터의 접근 및 원활한 흐름을 유도하여 경제혁신을 달성해야 하는 유인이 있다. 개인의 경우 자신의 개인정보를 통제할 수 있는 정당한 권리가 있으면서도 자신의 데이터가 효율적으로 개발되어 혜택을 얻기 위해서는 기업 간 원활한 데이터 이동 역시 필요하다. 기업의 입장에서는 데이터 수집 · 발굴에 사활적 이해가 걸려 있는 바, 기본적으로 데이터의 자유로운 접근을 강조하면서도 기업의 특성상 데이터에 대한 독점적 지위를 유지하려는 경향이 강하다.

데이터는 생산 주체에 따라 공공(public) 데이터와 사설(private)로 구분될 수 있고 현재 국내에서 상대적으로 중시되는 영역은 공공 데이터 개방을 통한 공공 데이터의 산업적인 활용이다

(정희영, 2020). 그러나 데이터의 실체적 내용(substance)을 고려하면 이러한 구분이 모호할 뿐만 아니라 향후 공공 데이터 보다 구글, 페이스북, 아마존 또는 국내 네이버나 카카오와 같은 IT 플랫폼 기업에서 생산되는 사설 데이터가 규모나 파급력이 클 것이다. 문제는 이러한 사설 데이터는 사실상 다수의 공공 혹은 개인정보로 구성됨에도 불구하고 데이터에 대한 관리 권한은 서비스 제공자들에 의해 독점되고 있는 현실이다. 실제 전 세계 사용자들의 데이터를 구글, 애플, 페이스북, 아마존 등 소위 GAFA가 독과점하는 구조로 글로벌 클라우드 시장 역시 아마존, MMS, 구글이 50% 이상을 점유하고 있다(Internet Report, 2019). 이러한 상황에서 '데이터 완전성'(data integrity) 훼손, 오남용, 기술경쟁으로 인한 부정적 영향 역시 증대하고 있다. 현재 전 세계 100개국 이상이 관련 법제를 수립한 상황에서 데이터 주권 논의는 개별 국가의 산업경쟁력 차원을 넘어서 포괄적·복합적인 국가 · 지역 · 글로벌 데이터 안보 담론으로 부상하고 있다.

2. 데이터 주권 논의의 이중성

데이터 주권 개념은 중의적 의미를 내포하는바, △데이터의 영역적 범위, △데이터 생산 · 제공자, △데이터의 실체적 주체 간 권리 · 의무의 충돌 · 조정 과정이 필연적이다. '당위적' 차원에서 데이터 주권은 독점적일 수 없으며 공유가능하며 개별 행위자 간 데이터 주권의 강조점이 다르다. 즉, 국가적 차원에서는 일국 내 데이터의 수집·저장 · 유통 · 활용 등에 있어 해당 국가가 배타적 주권을 행사하여 규제할 수 있다는 개념으로 원용된다. 반면, 개인의 입장에서는 정보주체로서 개인이 자신과 관련한 데이터에 대한 결정권을 가져야 한다는 정보 주체의 자기결정권 차원에서 데이터 주권 개념이 강조되고 있다(Taylor and Kukutai, 2016). 다만, 두 개념 모두 국가안보를 고려하면서 거대 IT 기업에 맞서 자국 데이터 산업을 보호 · 육성하고 민감 데이터의 해외 유출을 방지하기 위한 규제 명분으로 활용되고 있다(Maurer and Morgus, 2014). 국가안보 차원의 국가의 데이터 주권의 충돌 역시 이중적 측면을 고려해야 하는 바, 미국의 경우 국가가 기업에 대해서 데이터의 접근 및 제공을 강제할 수 있는지 여부에 대한 다수의 분쟁이 발생하고 있다(Woods, 2018). 특히, 미국 IT 기업이 외국에서 데이터 관련 영업활동을 하는 상황에서 미국 정부가 해당 기업에 대해 국가안보를 근거로 데이터에 대한 접근과 이전을 강제하는 경우, 미국 정부, 영업지 외국정부, 기업 간 데이터 주권과 관련한 복잡한 분쟁이 발생할 가능성이 있다(Thielman, 2015). 반면, 미국 IT 기업의 해외 영업 시 외국정부가 특정 데이터 및 정보의 이전 및 삭제를 제한 · 강제하는 분쟁 또한 다수 제기되고 있다(Woods, 2018).

데이터 주권을 둘러싼 쟁점은 결국 초국경적 차원에서 국가, 기업, 개인 간 데이터 관리에 대한 권리로 집약될 수 있는 바, 국내적, 국제적 논의 역시 안보 및 경제적 이익을 고려한 데이터 관리 주체 간 균형을 달성하는 데 초점을 두고 있다. 이러한 경향은 데이터 주권이 강화하는 추세에서 새로운 데이터 활용과 이익 환원 · 공유 방식에 대한 논의와 연결된다. 즉, 최근 주요 데

이터 강국은 데이터 활용을 통해 발생하는 사회적 혜택을 공정하게 배분하여 개인의 데이터 제공 · 활용을 촉진할 수 있는 포괄적인 데이터 관리 체계를 구축하고 있는 상황이다. 다만, 개별 국가는 종합적 · 포괄적인 데이터 관리 체제 구축 시 자국의 국가안보 및 공공이익을 고려하여 데이터 주권의 쟁점과 구체적 이행 방안을 법제화하고 있다(NIA, 2018).

3. 데이터 주권 논의의 주요 쟁점

실질적 · 구체적으로 데이터 주권의 핵심적 쟁점은 데이터 및 개인 정보의 이전 · 유통의 제한 여부와 데이터의 자국 내 서버 저장 강제화 등 데이터 현지화(data localization) 이슈로 귀결된다. 데이터 이전 · 유통 문제는 데이터 수집 · 활용과 필연적으로 연계되는바, 데이터의 축적과 활용은 특정 국가가 자신의 경제적 · 사회적 · 군사적 역량을 측정하고 동원하는 기초 자산으로 활용될 수 있다는 인식에 기반한다. 같은 맥락에서 데이터의 자유로운 이동이 비록 사회전반에 혜택을 가져다주지만 민감 데이터의 유출, 데이터 왜곡 · 남용 등 국가안보에 부정적 영향을 끼친다는 관점에서 데이터의 자유로운 이동을 제한하는 입장이 상존한다. 미국이 자국 IT 기업들의 입장을 감안하여 데이터의 초국경적 이전 · 유통을 강조하는 반면 중국은 데이터를 일국적 재산으로 인식하고 데이터 안보 및 데이터 주권을 주장하면서 데이터 현지화 정책을 확대 · 강화하고 있다(NIA, 2018).

데이터 현지화와 관련 첨예한 쟁점은 데이터의 자국 내 서버 저장을 의무화하고 국가안보 등 필요시 국가가 서버에 대한 접근권을 기업에 요구할 수 있는지 여부이다. 미국 및 거대 IT 기업들은 이러한 현지화 요건이 데이터의 자유로운 이동을 제한하고 왜곡한다고 판단하는 반면 중국, 러시아, 인도 등 일부 신흥국들은 이러한 요건이 국가안보 등 “정당한 공공정책 목적”에 기초한다고 주장한다. 서버 접근의 경우 국가가 기업에 요구하는 것이 일반적이나 구글 등 거대 IT 기업들이 데이터의 자유로운 이전 · 유통을 강조하면서 영업지 국가 서버에 대한 접근권을 요구하는 사례도 있다(이승주, 2018). 데이터 현지화 이슈 역시 데이터의 이전 · 유통과 연계된 이슈인 바, 최근 디지털 무역 관련 WTO 및 FTA에서 핵심적 쟁점으로 논의되고 있다(이재민, 2020).

일반적으로 데이터 주권이 행사되는 경우는 국가주권의 형태로 국가가 타국가, 기업, 개인을 대상으로 행사하거나 데이터의 소유자 즉 개인이 자신의 개인정보를 소유 · 처리 및 이동 · 유통을 통제 · 관리하고 이를 국가가 보장하는 방식으로도 행사된다. 이러한 데이터 주권의 대표적인 사례는 EU이 제정한 일반개인정보 보호법(GDPR: General Data Protection Regulation)인바, GDPR은 개인에게 자신의 데이터 정보에 대한 광범위한 권한을 부여하고 있다. 예컨대, GDPR은 기존의 데이터 열람권이나 수정권 등과 함께 데이터 삭제권, 이동권, 프로파일링 거부권 등 포괄적인 데이터에 관리 권한을 규정하고 있다(Lucarini, 2020). 특히, GDPR에서 중시되는 개인정보 이동권과 관련하여 주목할 것은 제20조 제2항에서 제3자에게 제공할 수 있도록 하

는 데이터 결정권을 강화한 점이다. 이는 1995년'지침'(Directive)에는 규정되지 않은 바, 입법의 의도는 미국 거대 IT 기업과의 경쟁력 제고 차원에서 규정된 것으로 평가되고 있다(Kamleitner and Mitchell, 2019). 데이터 주권 논의에서 개인의 데이터 관리 권한을 강화하는 것은 궁극적으로 데이터 역시 자산이자 재산권의 일부로 인식하는 것이다. 이는 지적재산권의 관리체제 논의 시 국가, 기업, 권리소유자의 균형이 주된 쟁점인 것처럼 향후 국제적 차원의 포괄적인 데이터 관리체제 형성 논의에 중요한 시사점을 제공한다.

Ⅲ. 주요국 동향 및 정책

1. 미 · 일의 데이터 자유 이동 지지

미국은 자국 기업들이 이미 글로벌 시장을 확보한 선도국가라는 이점을 바탕으로 데이터의 자유로운 초국경 이동을 옹호하고 중 · 러 등의 데이터 현지화 조치에 명시적으로 반대하고 있다. 미국의 전통적인 데이터 주권에 대한 인식은 시장경제 질서 유지를 중시해 특별한 경우에만 법률을 제정하는 등, 업계의 '자율 규제'를 중시하고 미국 정부기관은 각종 가이드라인을 제공하여 지원한다. 오바마 정부에서는 빅데이터 산업 활성화 정책과 동시에 개인의 데이터 주권을 강화하기 위한 프라이버시 정책을 추진한바, 데이터 수집 · 이용 · 공개 과정에서 정보주체의 의사를 반영할 수 있도록 권고하는 내용의 소비자 프라이버시 권리장전(Consumer Privacy Bill of Right)을 통해 데이터 권리와 관련 산업의 발전을 도모하였다(Bischoff, 2018). 반면, 트럼프 정부에서는 전반적인 규제완화 정책의 일환으로 데이터 규제는 완화하고, 국가안보 관점의 사이버 보안을 강화하는 추세이다. 즉, 기존 데이터 보호 규정을 관련 산업의 성장과 혁신을 저해하는 장애물로 인식하고, 광대역통신망 프라이버시 보호규칙의 폐지 등 규제완화 조치를 시행하였다. 기존 연방통신위원회(FCC)의 광대역통신망 프라이버시 보호규칙에 따르면 인터넷서비스 제공자(ISP)가 사용자의 위치 · 금융 · 건강정도 등을 광고마케팅에 활용하려면 반드시 사용자의 동의를 구해야 했지만(Opt-in), 동 규칙의 폐지로 인터넷 서비스 제공자가 사용자 정보를 추적 · 수집해 제3자에게 판매를 할 수 있게 되었다(한국데이터진흥원, 2017).

데이터 이전에 관한 미국의 다자적 이니셔티브를 주도하고 있는 바, 2011년 APEC CBPR(Cross border Privacy Policy)은 회원국 간 개인정보 국외이전의 자율 인증제도로서 여러 미국 주도 통상협정에서 진화 · 발전되고 있다(Sullivan, 2019). 즉, 트럼프 행정부는 데이터 이전과 현지화 정책에 대한 미국의 기존 정책을 계승하여 미국 · 캐나다 · 멕시코 무역협정(USMCA: United States-Mexico-Canada Agreement) 및 미 · 일 디지털통상협정(2019.10.9. 체결, 2020.1.1. 발효)에서 데이터 이전 제한과 현지화 금지 조항을 규정하고 이후 인도 등 데이터 현

지화를 강제하는 국가를 대상으로 비자발급 축소까지 검토하였다(Business Standard, 2019.6.21.).

일본의 데이터 주권에 대한 기본 입장은 미국과 유사하며 특히, 2019년 G20 정상회의 시 '신뢰 가능한 데이터의 자유로운 이동(DFTA, Data Free Flow with Trust)'을 도모하는 국제규범 마련을 위한 '오사카트랙'을 제안하였다. 오사카 트랙에서는 △국제적 데이터 이전 · 유통 규칙의 표준화, △개인정보와 지적재산권의 보호, △사이버안보 강화, △미국 정보통신기술(ICT: Information and Communication Technology) 기업들에 대한 과세기준 마련 등이 논의되었다. 일본이 제안한 오사카 트랙은 중국의 디지털 보호주의와 데이터 현지화 정책을 겨냥한 미국 등 서방 진영의 대응의 일환이다(Carter, 2019). 현재 오사카트랙의 경우 한 · 미 · 일 · 중 · 러 · 유럽연합(EU) 등 24개국이 관련 성명에 서명하였고(인도는 거부) 현재 민관협의가 진행 중이다.

일본은 데이터 주권 확대 강화를 위해 개정 개인정보보호법(2017.5. 시행)에서 개인정보 정의를 명확히 하고 익명가공정보(특정 개인을 식별할 수 없도록 이름, 전화번호 주소 등 개인정보를 삭제하는 등 정부가 정하는 방식으로 가공한 개인 데이터) 제도를 도입하여 정보 주체의 동의 없는 수집을 제외한 데이터 활용과 제3자 매매가 가능하게 하여 데이터 이전 · 유통 시장을 활성화하고 있다. 다만, 개정 개인정보보호법에는 해외에 있는 제3자에게 자국민 개인 데이터 제공을 제한하고 EU의 GDPR과 같이 일본과 동일한 수준으로 개인정보가 보호되고 있다고 인정되는 국가와 제3자에게만 정보주체 동의 없이 개인 데이터 제공을 허용한다. 결국, 일본 역시 데이터의 자유로운 이전 · 유통을 강조하지만 이는 국내적 적용에 한정되고 데이터 주권을 고려하여 국외 이전에 대해서는 제한을 두고 있다.

2. 중 · 러의 국가 규제권 강조

중국은 데이터를 국가 발전의 기초 전략 자원으로 간주하고, 자국 영토 내 인터넷 사용에 대한 통제 · 규제 권리를 주장하며 국가의 데이터 주권을 강화하고 있다. 즉, 중국 정부는 국가안보를 이유로 '황금방패시스템'으로 자국민의 해외 사이트 접속을 차단하고, 외국 기업의 자국민 데이터 수집 · 처리를 엄격히 제한한다. 반면, 자국 기업의 데이터 활용은 적극 장려하여 데이터 산업 육성, 신기술 개발, 데이터 기반 프로젝트를 적극적으로 추진하고 있다. 데이터 주권 강화를 위한 법 · 제도 정비와 관련 중국은 분산되어 있던 네트워크 보호와 개인정보보호 관련 규정을 네트워크안전법(2017.6. 시행)으로 통합해 국가의 데이터 통제권을 강화하였다(ITWorld, 2019.3.13.). 동법에서는 사이버안보를 강조하고 주요 데이터의 중국 내 저장, 해외 전송 시 안전평가 등을 기업 의무로 규정한 바, 데이터의 이전과 데이터 현지화 정책을 강화하고 있다. 기본적으로 중국에서 수집 · 생성된 데이터는 중국 내에 저장해야 하고, 중국 정부가 요구할 경우 데이터 암호해독 정보 제공이 요구한다. 데이터 이전 제한과 현지화 정책 확대는 중국 기업 보호

와 육성 전략으로 추진되지만, 역으로 중국 기업의 글로벌 시장 진출에는 장애물로도 작용하기도 한다(Nussipov, 2020).

최근 왕이 중국 외교부장은 '글로벌 데이터 안보 구상'을 발표(2020.9.8.)하면서, 데이터 주권, 관할권, 거버넌스를 강조하면서 타국 동의 없는 타국 소재 데이터 취득 금지를 제안하였다(Wand Wenwen and Zhang Hui, 2020). 글로벌 데이터 안보 구상의 주요 내용은 △종합적 · 객관적 · 증거 기반의 데이터 안보 및 ICT 공급망 개방성 · 안전성 유지, △주요기반시설 데이터 훼손 · 탈취 및 국가안보를 저해하는 데이터 이용 금지, △대규모 감시 및 개인정보 불법 수집 반대, △기업의 주재국 법령 준수 권장 및 자국 기업의 해외 생산 · 취득 데이터의 자국 영토내 저장 요구 금지, △데이터 주권 · 관할권 · 거버넌스 존중, △법집행을 위한 해외 데이터 취득 필요시 사법공조 또는 양 · 다자 협정을 통해 요청, △데이터 불법 취득 및 시스템 통제 · 악용을 위한 ICT 공급자의 백도어 설치 금지, △ICT 기업들의 업그레이드 등 이용자 의존성 악용 방지 및 취약점 보고 의무 등이다(Tiezzi, 2020.9.10.). 중국의 의도는 데이터 안보 관련 국제규범 제정을 제안하여 국제적 지지를 유도하는 한편, 미국의 대중 압박정책에 대응인 것으로 평가된다. 실제, 동 구상 발표 시 왕이 부장은 특정국이 '클린 네트워크'라는 명목으로 타국 기업들을 약탈하기 위해 일방적 조치를 취하고 있다고 비난한 바 있다. 이는 또한 EU의 GDPR, 미국 주도 CBPR, 클린네트워크 등 지역 차원의 규범을 넘어 국제사회에 데이터 안보 관련 포괄적 규범 제정을 제안하여 주도권 확보를 위한 구상이다(CGTN, 2020.9.8). 특히, 중국은 중국보다 강도는 낮으나 데이터 이전을 제한하거나 데이터 현지화 정책을 추진하고 있는 러시아, 인도, 인도네시아, 브라질 등 주요 신흥국과 개도국의 지지를 유인하여 동 구상을 유엔 개방형 실무그룹(OEWG: Open Ended Working Group), G20, SCO(상하이협력기구) 등 다자논의체에서 문서화 작업을 시도할 가능성이 높다. 2021년 3월 최종 OEWG 회의에서도 중국은 데이터 안보 규정의 포함을 강력히 요구한 바, 최종보고서가 아닌 의장요약문에서 반영하는 방식으로 타협을 이루었다(A/AC.290/2021/CRP.2 & A/AC.290/2021/CRP.3).

러시아도 자국민 데이터를 국가주권의 적용 대상으로 규정하는 법률을 제정한바, 푸틴 러시아 대통령은 2014년 12월 러시아는 러시아 국민의 개인 정보는 러시아 영토 서버에 저장하는 것을 의무화한 법안에 서명하였다. 동 법안은 당처 2016년 9월 1일자로 발효하는 것으로 예정되었지만 그 시기를 앞당겨 2015년 9월 1일자로 발효하였다(Gratchener, 2015). 또한 2019년 5월 푸틴 대통령은 러시아에서 수집된 데이터의 국외 이전 시 정부 검열을 거치도록 강제하는 개인정보보호법에 서명한 바, 러시아는 데이터 이전을 제한하고 데이터 현지화를 강화하는 정책을 강화하고 있다(Khayryuzov, 2020). 특히, 2019년 11월 「독립인터넷법」을 공포하여 러시아 통신회사 로스콤나드조르를 통해 해외 트래픽을 차단하여 순수하게 러시아의 독자적인 인터넷을 만들도록 규정하고 있다.

또한 러시아는 데이터 주권 강화를 위해 기존 유엔 및 SCO 등 지역 · 글로벌 협의체를 활

용하는 기존 전략을 지속적으로 추진하고 있는 바, 특히 미 · 서방과 대립 구도를 유지하는 맥락에서 중 · 러 협력을 강화하고 있다. 즉, 러시아 세르게이 라브로프(Sergey Lavrov) 장관은 러 · 중 외교장관회담(2020.9.11.)시 중국의 글로벌 데이터 안보 구상에 대한 원론적 차원의 지지를 표명하면서, 러시아는 OEWG 회의 러시아 제안서에서 데이터 주권 이슈를 포함하는 등 관련 국제규범 수립을 위해 중 · 러 간 협력을 강조하고 있다. 이와 관련 중 · 러는 2020년 제75차 유엔 총회 결의(A/C.1/75/L.8/Rev.1, 26 Oct. 2020)를 통해 데이터 주권을 OEWG 주된 의제로 다룰 것을 제안하여 통과하였다.

3. EU의 개인의 데이터 관리권 중시

유럽 시장에서 미국의 글로벌 IT 기업들의 데이터의 독점 경향이 강해지면서 EU는 경제안보 차원에서 데이터 주권을 강화하는 정책을 추진 중이다. 실제, 유럽 검색시장에서 구글의 경우 웹과 모바일을 합쳐 무려 91.5% 점유율을 차지하고 있는바, 글로벌 IT 대기업들의 국경 간 데이터 이동을 제한하는 데이터 주권 강화 필요성이 대두되고 있다(연합 인포맥스, 2018.4.24.). 한편, EU 역시 데이터를 경제성장과 혁신 경제의 핵심 자원으로 인식, 원활한 데이터 유통 · 활용 촉진과 함께 역내 데이터 거버넌스를 통합해 데이터 이동 장벽을 허물고 총체적인 데이터 역량 강화를 도모하고 있다. 즉, EU는 또한 EU 데이터 단일시장 구축전략 채택(2020.2.), 독일 · 프랑스의 EU 독자 클라우드 구축 프로젝트인 Gaia-X 추진(2019.10.) 등 데이터 주권 강화 차원에서 자생적 데이터 산업 육성에 노력을 기울이고 있다(European Commission, 2017).

이러한 배경에서 EU는 단순 정책 페이퍼(policy paper)나 지침(directive)보다 강력하고 EU 회원국 전체를 직접 구속하는 GDPR(2018.5. 시행)을 통해 개인의 데이터 주권을 강화하고 EU IT 기업의 경쟁력 강화를 추진하고 있다(Carla, 2020). GDPR은 EU 국가 간 자유로운 데이터 이동을 보장하지만 자국민 데이터의 해외서버 이전을 엄격하게 제한하고, 국외 이전 허용 조건과 절차를 규정화하여 데이터 주권을 강화하고 있다. 즉, GDPR는 엄격한 사생활 보호 기준을 충족시키는 EU의 '적정성 평가(adequacy decision)' 없이는 EU 시민으로부터 수집한 데이터를 역외로 이전할 수 없게 하고 전 세계 매출액의 4% 또는 최대 2,000만 유로에 달하는 거액의 과징금(administrative fines)을 부과하고 있다(GDPR 제83조 제6항). 이에 따라 현재 캐나다(사업단체), 아르헨티나, 이스라엘, 일본, 뉴질랜드, 스위스, 우루과이 등 12개국이 평가를 마쳤으며 한국은 현재 최종 평가 확정단계에 있다(European Commission, 2021). 또한 영국항공, 구글이 GDPR 위반으로 적발되어 거액의 과징금(administrative fines)이 부과되었으며 아마존, 애플, 넷플릭스, 유튜브도 위반 혐의로 조사받고 있다(보안뉴스, 2019.8.8.). 유럽이 전통적으로 사생활 보호를 중시하는 문화가 형성되었는 바, GDPR에서 명시한 데이터 이동권은 '시민주권' 내지 '시민안보' 차원의 접근으로 향후 데이터 주권의 핵심 요소로 부상할 전망이다(김상배, 2020).

〈표 1〉 주요국 디지털 주권 강화법안

중국	- 네트워크안전법/사이버보안법(17.6): ▲중국 내에서 수집한 데이터의 중국 서버 저장 의무화, ▲데이터 해외 이전시 중국 정부의 안전평가 의무화
러시아	- 개인정보보호법(19.5): ▲러시아인의 개인정보는 현지 DB에 관리, ▲DB 위치는 당국에 신고
EU	- 일반개인정보보호규정(GDPR)(18.5): ▲데이터 관련 개인의 이동권 · 삭제권 법제화, ▲EU 역내에서 데이터의 자유 이동 보장, ▲EU 시민의 데이터 해외 이전 제한(적정성 평가 통과시만 가능)
미국	- 소비자 프라이버시 권리장전(12.2): 개인정보에 대한 소비자의 통제권 강화
일본	- 개인정보보호법 개정(17.5): '익명으로 가공한 정보' 개념 도입을 통해 사생활 보호 수준 강화

출처: 필자 작성

Ⅳ. 향후 전망과 시사점

1. 미 · 중 경쟁의 새로운 전선으로 부상

미 · 중 무역 분쟁 및 화웨이 갈등의 이면에는 데이터 안보 이슈가 밀접히 연계되어 있는 바, 향후 미중 경쟁이 디지털 패권 경쟁에서 데이터 패권 경쟁으로 진화 · 확대될 가능성이 높다. 즉, 미 · 중은 자국의 데이터 수집 등 총체적인 데이터 확대를 추구하는 동시에 자국에서 생산된 데이터가 외국 정부기업에 반출되어 자국의 경쟁력과 국가안보를 위협받는 것에 적극적으로 대응할 것이다. 특히, 미국은 데이터가 인공지능, 빅데이터, 양자컴퓨팅 등 미래산업에서 경쟁력 확보의 원천이라는 점을 인식, 기술경쟁에서 빠른 속도로 도전해오고 있는 중국을 적극 견제할 것이다. 실제, 미국은 중국보다 정부 R&D가 뒤쳐져가고 있는 상황을 감안하여 데이터 등 신기술 분야에서 중국을 견제하는 구체적인 신기술 안보 전략을 민관협력을 기조하에 재정비하고 있다(Analytic Exchange Program, 2018).

데이터의 '자산화' 맥락에서 데이터 이전 및 데이터 현지화 이슈는 이중성이 있는 동전의 양면과 같은 문제로, 실질적으로는 자국 · 자국기업의 데이터 확보는 강화하면서 타국 · 타국기업의 데이터 이전 · 유치는 제한하는 방향으로 정책이 추진될 것임을 유의해야 한다. 미 · 중은 자국

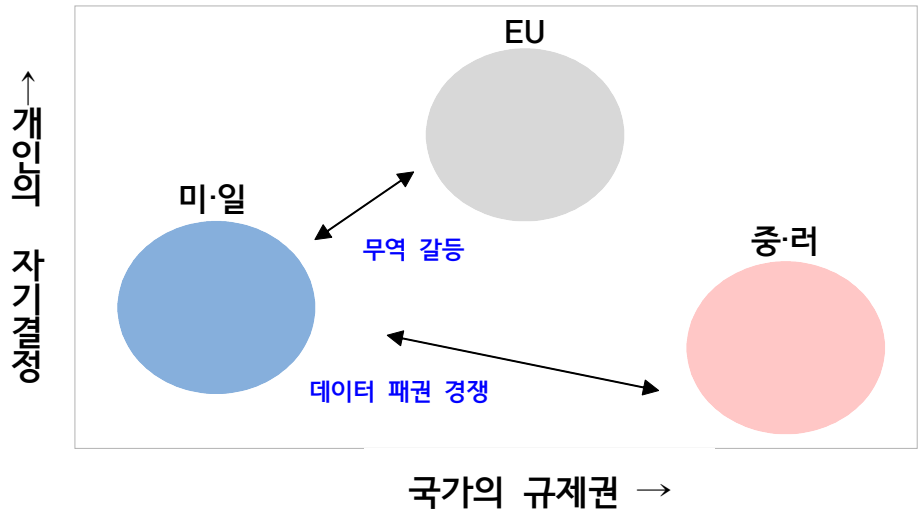
이익에 부합하는 디지털 거버넌스 구축 및 규범 수립을 추진하여 미 · 중 간 주도권 경쟁이 심화될 것이다. 다만, 보호주의를 강력히 추진 중인 트럼프 행정부의 정책이 데이터에 대한 자유로운 이동을 주장하는 미국의 일관된 입장과 상치된다는 지적이 제기되는 바, 바이든 신정부 출범 시 상기 이슈 관련 정책적 조정이 주목되는 바, 특히 데이터 활용이전에 있어 개인정보보호를 강화하는 연방법을 강화할 가능성이 있다(Atkinson, 2020). 한편, 일본이 오사카트랙을 제안한 바와 같이 일본이 미국 대신 주도적 역할을 하거나 유사입장그룹 및 'Five Eyes' 등 우호그룹을 통해 이슈를 주도할 도할 가능성도 상존한다(박세진, 2019.8.30.). 중국 및 러시아의 대응 역시 데이터 안보, 데이터 주권 이슈를 중 · 러 공조하에 SCO, OEWG 지역 · 다자협의체에서 규범화 시도를 강화할 것으로 전망된다.

2. 서방 진영 간 마찰 가능성 상존

GDPR 등 EU의 공세적 미국 IT 기업 규제에 대해 미국은 무역장벽으로 인식하고 있는 바, 향후 양측의 갈등 심화 요인으로 작용할 가능성이 있다(Shapiro, 2020). 실제 데이터 주권 확보를 명분으로 미국 IT 기업을 겨냥한 △과징금 부과, △디지털세 추진, △반독점법 적용 등에 대해 미국은 강력하게 반발하며 관세보복을 검토하고 있다. 미국과 EU는 GDPR 발효 이전부터 이미 스노든 사건을 계기로 EU · 미국 간 데이터 전송에 관한 프라이버시 실드(Privacy Shield) 협정을 체결하여(2016.8.) 데이터 전송 문제를 일시적으로 봉합하였다. 그러나 이후 유럽사법재판소(ECJ: European Court of Justice)의 프라이버시 쉴드 무력화 판결(2020.7.)로 인해 아일랜드 데이터보호위원회는 페이스북에 EU 이용자의 개인 정보를 미국으로 전송하는 것을 금지하는 명령을 내린바 있다(Case-311/18, 16 July 2020). 동 판결로 인해 EU내 개인정보의 미국 이전을 위해서는 미국과 EU 간 새로운 적정성 평가 협상을 진행해야 한다(Steinberg, 2020). 영국 또한 Brexit 이전 적정성 평가 협상이 완료되지 않은 관계로 미국, 영국, EU 등 서방 국가 간 데이터 안보에 대한 공조에 일정한 제한이 있을 것으로 전망된다(Burges Salman LLP, 2020).

미국과 EU 간 데이터 주권을 둘러싼 마찰은 데이터 주권을 바라보는 사회문화적 차이에서 비롯하기도 하지만 그 이면에는 데이터의 정치경제적 안보 가치의 중요성에 기인한다. 이는 클린 네트워크 및 신기술 패권 경쟁의 경우 EU의 포지션이 기후변화, 보건, 인권 등 다른 신안보 분야의 경쟁 구도와 차이가 있음을 시사한다. 즉, 5G의 안보적 위험성을 지적하면서 중국 화웨이 부품 · 기술을 제한하기 위해 미국이 제안한 '클린 네트워크'나 '프라하 제안'(Prague Proposals) 프로세스에 대해 EU는 원칙적 공감대를 표명하면서도 EU의 공동 정책을 강조하고 독자적인 5G 사이버안보 툴박스(EU 5G cybersecurity Toolbox)를 강화하는 입장은 이러한 현실을 반영한 것으로 평가된다(Oertel, 2020).

〈그림 1〉 디지털 주권을 둘러싼 진영 간 갈등 구도



출처: 필자 작성

3. 자유무역과 국가안보의 충돌 · 조정

데이터 이전과 현지화 관련 법적 구속력 있는 국제법은 통상분야에서 확인할 수 있는 바, 기존 디지털 교역 분야 관련 통상 협정에서 데이터 주권 관련 개인정보 데이터 해외이전과 서버 현지화 요건 금지를 규정하고 있다. 즉, △세계무역기구(WTO) 차원의 다자 간 논의, △자유무역협정(FTA) 포함 항목으로서 양자적 · 지역적 논의, △디지털 교역 문제만을 다루는 별도의 협정 체결 논의에서 상기 이슈를 규정하고 있다. 이와 관련 최근 체결 · 발효되었거나 진행 중인 △CPTPP(Comprehensive and Progressive Agreement for Trans-Pacific Partnership, 2018.12.30. 발효), △USMCA (United States-Mexico-Canada Agreement, 2020.7.1. 발효), 미 · 일 디지털 통상협정(US-Japan Digital Trade Agreement, 2020.1.1. 발효), △DEPA(Digital Economy Partnership Agreement; 싱가포르, 칠레, 뉴질랜드 3국간 체결 절차 진행 중) 등에서 두 이슈에 대한 원칙과 예외 요건을 규정하고 있다.

상기 통상협정상 데이터 주권 이슈는 통상협정의 국가안보 예외에 포함되는 정보 관련 조항이 개인정보 및 데이터에도 직접적으로 적용된다는 것을 시사한다. 즉, 데이터 이전의 제한 및 데이터 현지화 금지가 상기 통상협정에서 원칙으로 규정되고 있으나, 관세무역일반협정(GATT: General Agreement on Tariffs and Trade) 및 제반 통상협정상의 일반적 예외와 국가안보 예외 규정은 그대로 적용됨은 물론 '정당한 공공정책 목표(LPPO: Legitimate Public Policy

Objective)'를 위하여도 규제할 수 있다는 규정을 추가하고 있다. EU의 GDPR도 전문에서 GDPR이 국가안보 사항에는 적용되지 않는다는 점을 전문에 규정함은 물론 별도의 국가안보 예외조항이 도입되어 있는 바, 개인의 데이터 주권을 적극적으로 강조하는 EU도 보호의 예외로 국가안보를 들고 있다는 사실은 시사하는 바가 크다. 이는 향후 구체적 예외와 협정 전체 예외의 관계를 명확히 해야 함은 물론 국가안보 예외조항의 문언을 구체화하는 등 통상협정의 전반적 정비가 필요한 상황이다(이재민, 2020). 더욱이 국가안보 예외의 경우 비교적 포괄적으로 용인하는 것이 관행인 바, 따라서 향후 국가 간 이견 조율과 이해관계의 균형 달성이 필요하며 같은 맥락에서 국가안보 예외 역시 일정한 충돌 · 조정과정이 있을 것으로 예상된다(Bolkan, Daria & Bahri, Amrita, 2020).

2차 대전 후 형성된 자유무역레짐과 국가안보에 기한 무역규제레짐은 각 레짐의 출범 후 수십 년에 걸쳐 독자적으로 영역을 확대해왔지만 최근 레짐 간 갈등이 표면화되고 있다. 특히, 신기술 안보 분야가 부상하면서 국가안보와 자유무역간의 갈등을 가속화하고 있는 상황이다. 더욱이 데이터 주권 갈등의 경우 그 양상이 미 · 중 간 진영 갈등은 물론 미 · EU, 한 · 일 간 진영 내 갈등 역시 증폭되고 있어 데이터 주권을 둘러싼 핵심 쟁점의 갈등 구도는 복잡하게 전개될 것으로 예상된다(Prazers, 2020).

Ⅴ. 맺음말

현재 데이터 주권 논의는 디지털 기술 패권 경쟁의 핵심 현안으로 부상하고 있는 가운데 주요 디지털 강국들은 데이터 주권을 단순 산업경쟁력 차원이 아닌 포괄적인 국가안보 맥락에서 조망하고 있다. 또한 디지털 주권 경쟁은 기존 지정학적 미 · 중 경쟁은 물론 기술 선진국 사이에서도 갈등 이슈로 전개될 가능성이 크기 때문에 실리와 명분을 조화시킨 한국의 입장을 사전에 선제적으로 정립할 필요가 있다. 정부의 데이터 뉴딜 정책 등 데이터의 산업 경쟁력 강화라는 실리적 목적과 개인정보 · 데이터 보호 간 실용적 균형 모색을 통한 일관된 정책적 입장을 유지할 필요가 있다. 데이터 주권의 과도한 강조는 지양하면서 EU 사례를 참조, 시민주권의 강화 등 민주주의 원칙의 강화라는 기조를 유지할 필요가 있다. 또한 미국의 CBPR 및 클린 네트워크, 중국의 글로벌 안보 구상, 일본의 오사카트랙 등 각 구상과 관련 주도국이 적극적 · 공세적으로 지지 요청을 제안할 것인 바, 각 구상의 주요 쟁점들에 대한 대응 논리 및 입장 정립이 필요하다.

세계 5위 데이터 생산국(Tufts University Gross Data Product, 2020)으로서 한국의 국익에 부합하는 디지털 규범이 형성될 수 있도록 각종 규범형성 논의에 주도적으로 참여하는 것이 필요하다. 적극적인 규범형성 논의에 참여하기 위해서는 각 쟁점별 규범 · 정책 · 기술 관련 부처 및 전문가 간 조율이 중요한 바, 워킹그룹 형태라도 부처 간, 전문가그룹 간 관련 협의체를 외교

부 주도로 조직하여 운영하는 것이 필요하다. 실제 사이버, 우주, LAWS 등 UN 및 다자협의체의 신안보 관련 규범 형성 논의에서는 규범 · 정책 · 기술 전문가 간 하위 실무 그룹(Sub-WG)를 조직하여 이슈 간 분절적인 논의를 방지하려는 경향이 지배적이다. 기존 사이버안보 협의체에 상기 워킹그룹 협의체를 통합하여 운영하는 것도 검토할 필요가 있다.

최근 데이터 안보 및 데이터 주권 이슈는 국가 간 동맹 · 파트너십의 지정학적 안보 차원으로 발전하고 있는 바, 사이버 · 디지털 외교라는 관점에서 접근, 양자 · 지역 · 글로벌 연대외교를 강화할 필요가 있다. 미국과 영국이 주도하는 Five Eyes나 EU의 사이버외교(Cyber Diplomacy)의 경우 외교기제로서 상기 이슈를 적극적으로 활용하고 있다. 데이터 안보 이슈에 대한 연대외교를 전개하기 위해서는 이슈에 대한 한국의 법제도, 규범, 전략 · 정책, 기본 입장 등을 담은 정책문서를 만들어 적극적인 아웃리치 활동을 전개할 필요가 있다. 사이버 · 디지털 외교의 경우 해당 의제의 포괄적 · 융합적 성격을 고려하여 현재 부처에 산재해 있는 관련 조직 · 부서를 확대조정 할 필요가 있다. 정부 조직 정비 이전에라도 관련 부서에 실무가가 참여하는 TF를 구성하여 정기적인 대응 협의를 통해 중장기적인 정책 · 전략을 추진할 필요가 있다.

데이터의 정치 · 경제적 중요성은 급속히 증대될 것인 바, 한국의 실익과 연계된 데이터 주권 강화를 도모하기 위해서는 관련 법제도 정비, 인프라 구축, 인식제고 등 국내적 차원의 역량 강화가 시급하다. 이와 관련 데이터의 보호와 자유로운 이전 · 유통 간의 적절한 균형이 필요한 바, 이는 데이터 주권의 실효적 행사를 위한 데이터의 적정 관리체제 구축에 좌우된다. 이를 위해서는 정부 · 기업 · 개인 등 데이터 주권의 이해관계자 간 데이터 안보에 대한 인식제고를 통해 데이터 활용과 이익 환원 방식에 대한 사회적 합의 도출이 필요하다.

[참고문헌]

강혜린. 2019.8.8. "GDPR 규정 위반! 과징금 폭탄 맞은 글로벌 기업들," 보안뉴스.

김상배. 2020. "데이터 안보와 디지털 패권경쟁," 『국가전략』. 92, pp. 1-33.

박세진. 2019.2.4. "중 경제 미 중심 새 정보동맹 '파이브 아이즈+3' 출범," 『연합뉴스』.

신은실. 2018.4.24. "구글은 어떻게 검색시장 점유율 90%를 장악하게 됐나." 『연합인포맥스』.

이승주. 2018. "사이버 산업과 경제-안보 연계: 구글 vs. 한국 사례," 이승주 편. 『사이버 공간의 국제정치경제』. pp. 223-247.

이재민. 2020. "디지털 교역 시대의 아날로그 규범: '개인정보'의 국경간 이전과 국가안보 예외," 『국제법학회논총』. 65(2). pp. 227-262.

정희영. 2020. "데이터기반 사회에서 데이터 주권 이슈와 대응기술 동향," 정보통신기획평가원, 기획시리즈. pp. 1-12.

한국데이터진흥원. 2017. 『데이터산업백서』. pp. 1-327.

ITWorld. 2019. "중국의 새 사이버보안법과 CISO의 대응방안."

NIA. 2018. "데이터 주권 부상과 데이터 활용 패러다임의 전환," IT & Future Strategy. pp. 1-28.

Analytic Exchange Program. 2018. "Emerging Technology and National Security," Public-Private Analytic Program. pp. 1-33.

Atkinson, "Trump vs. Biden: Comparing the Candidates' Positions on Technology and Innovation," ITIF, pp. 1-41.

Bischoff, Paul. 2018. "What is the Consumer Privacy Bill of Rights? and How it Evolved?", Comparitech, pp. 1-17.

Bolkan, Daria & Bahri, Amrita. 2020. "The First WTO's Ruling on National Security Exceptions: Balancing Interests or Opening Pandora's Box?," World Trade Review 19(10), pp. 123-136.

Burges Salmon LLP. 2020. "UK-US data sharing risk to UK's GD
PR adequacy decision application," Lexiology.

Business Standard. 2019. "No H-1B visa caps for data localization: US Date Department."

Carla Hobbs(ed.). 2020. "Europe's digital sovereignty: From rulemaker to superpower

in the age of US-China rivalry," European Council on Foreign Relations, pp. 1-89.

Carter, William. 2019. "Resolved: Japan Could Lead Global Efforts on Data Governance," Debating Japan 2(6), pp. 1-8.

CGTN. 2020.9.8. "Wang Yi: China proposes global data security initiative."

Gratchner, Amanda. 2015. "The New Russian Data Protection Law: Five Important Things To Know," Risk & Compliance Matters. pp. 1-6.

Economist. May 2017. "The worlds's most valuable resource," pp. 14-17.

European Commission. 2017. "Supporting the Emergence of Data Markets and the Data Economy," European Data Infrastructure ICT-13.

IDC. 2017. "World Semiannual Big Data and analytics Spending Guide."

Internet Society Global Internet Report. 2019. "Consolidation in the Internet Economy."

Kamleitner, Bernadette and Mitchell, Vince. 2019. "Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringement," Journal of Public Policy & Marketing. 38(4), pp. 433-450.

Khayryuzov, Vyacheslav. 2020. The Privacy, Data Protection and Cybersecurity Law Review(Russia).

Lucarini, Francesca. 2020. "The differences between the California Consumer Privacy Act and the GDPR," EU GDPR Blog.

Maurer, Tim and Morgus, Robert. 2014. "Technical Sovereignty: Missing the Point?", pp. 1-40.

Nussipov, Adil. 2019. "How China Governs Data," Center for Media, Data and Society, pp. 1-6.

Oertel, Janka. Carla(ed) 2020. "China: Trust, 5G, and the Coronavirus Factors," European Council on Foreign Relations, pp. 22-29.

Prazeres, Tatiana Lecerda. 2020. "Trade and National Security: Rising Risks for the WTO," World Trade Review, 19(1), pp. 137-148.

Shapiro, Jeremy. Carla(ed) 2020. "Europe's Digital sovereignty," European Council on Foreign Relations, pp. 7-22.

Steingberg, Mario. 2020.7.20. "ECJ Invalidates Privacy shield: What This Ruling Means for Website Operators," Raidboxes.

Sullivan, Clare. 2019. "EU GDPR or APECT CBPR? A comparative analysis of the approach of the EU and APEC to cross border data ransfers and protection of personal data in the IoT era," Computer Law & Security Review. 35(4), pp. 380-397.

Taylor, John and Kukutai, Tahu. 2016. "Alexander. 2014. "NAPCI: Solving the Asian Paradox," NATO. (2014.10.28.)

Thielman, Sam. 2015. "Nationality in the cloud: US clashes with Microsoft over seizing date from abroad," The Guardian.

Tiezzi, Shannon. 2020.9.10. "China's Bid to Write the Global Rules on Data Security," The Diplomat.

UNGA Report. 2021.3.10. A/AC.290/2021/CRP.2 & A/AC.290/2021/CRP.3

Wand Wenwen and Zhang Hui. 2020. "China launches global data security initiative, respects data sovereignty," Global Times.

Woods, Andrew Keane. 2018. "Litigating Data sovereignty", The Yale Law Journal 128, pp. 328-406.

A/AC.290/2021/CRP.2 & A/AC.290/2021/CRP.3