Research Paper Informatization Policy Vol. 30, No.1 (2023), pp.089-108
https://doi.org/10.22693/NIAIP.2023.30.1.089

미·중 초국경 데이터 규제와 사이버안보 담론 비교:
아세안 개발원조 사례를 중심으로*

이 가 연**

요 약 과학기술혁신은 행위자들의 활동을 전통적인 물리적 영토에서 사이버 영역으로 확장했다. 데이터 기반의 플랫폼 서비스와 시장은 사이버 공간의 주권에 대한 담론뿐 아니라 초국경 협력과 사이버 안보에 대한 새로운 논의를 진전시킨다. 이러한 변화는 미국과 중국의 패권 경쟁에도 영향을 미치고 있다. 특히 천연가스나 심해자원과 같은 주요 자원 수송로에 위치한 개도국에 대한 원조 경쟁이 치열하다. 아세안은 미·중의 강대국이 충돌하는 지정학적인 군사·안보의 요지일 뿐만 아니라 6억 명에 이르는 인구는 데이터 자원으로 인해 디지털 경제의 발전 가능성이 크다. 이에 이 논문은 국제개발협력에서 자유주의와 권위주의 담론을 데이터 규제 및 사이버안보와 연계하고, 이를 통해 아세안 통합에 대한 함의를 도출하고자 한다. 본 연구는 글로벌 거버넌스의 측면에서 빅데이터와 관련한 국제정치적 사안들을 연계하는 융합 연구의 의의가 있다.

주제어 : 미·중 경쟁, 초국경 데이터 규제, 사이버안보, 아세안 개발 원조

Comparative Study of US-China Discourse on Cross-border Data Regulation and Cybersecurity:
Focusing on ASEAN Development Assistance Cases*

Kayeon Lee**

Abstract Science, technology and innovation (STI) has expanded the activity of actors from the traditional physical territory to the cyberspace. Data-driven platform services and markets advance new discussions on cross-border cooperation and cyber security, as well as discourse on sovereignty in cyberspace. These changes are also affecting the hegemony competition between the US and China. In particular, competition for aid to developing countries that are located along major resource transportation routes, such as natural gas and deep sea resources, is fierce. ASEAN is not only a geopolitical military and security point where the US and China powers collide, but its population of 600 million has great potential for the development of the digital economy due to its data resources. In this regard, this article aims to connect the discourse of liberalism and authoritarianism with data regulation and cybersecurity in international development cooperation, and derive implications for ASEAN integration through this. This study has significance as a convergence study that links international political issues related to big data in terms of global governance.

Keywords : US-China competition, cross-border data regulation, cybersecurity, ASEAN development assistance

Received Jan 17, 2023; Revised Feb 10, 2023; Accepted Feb 24, 2023

* This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2020S1A5B5A17090430).

** Reserch Professor, Center for East Asian Studies, Sungshin Women's University(lkayeon83@gmail.com, https://orcid.org/0000-0003-3141-8664).

I. 서론

과학기술혁신(Science, Technology, Innovation, STI)은 행위자들이 활동하고 행위 하는 공간을 사이버 영역으로 확장하였다. 이는 물리적 영토에 기반한 전통 안보뿐만 아니라 국제사회의 비전통 분야의 협력에도 영향을 미치고 있다. 특히 미·중 패권 경쟁과 다국적 플랫폼 기업의 출현은 초국경 데이터 이동과 관련한 새로운 문제에 직면하도록 하고 있다.

첫째, 디지털 불평등(Digital Divide)의 심화이다. 플랫폼 서비스는 사용자들의 행동 양식이나 선택을 통해 수집되는 데이터를 통해 새로운 부가가치를 만들 수 있다는 장점이 있다. 하지만 광범위한 데이터의 축적은 플랫폼 소유자와 사용자 간의 틈을 넓혀 경제적 불평등과 계급구조를 심화시킨다. 과학기술혁신은 저개발국의 개발과 경제 성장을 앞당길 수 있다는 점에서 지속가능개발목표(Sustainable Development Goals, SDGs)의 달성을 위한 중요한 수단으로 여겨지기도 한다. 2015년 7월 아디스아바바 제3차 개발재원총회에 참가한 국가들은 '국가의 지속가능개발전략의 필수 요소로 과학기술혁신 전략을 채택'하기로 약속했으며(IATT-STI, 2017), 이후 UN 기술촉진메커니즘(The UN Technology Facilitation Mechanism, TFM)'과 그 산하에 'SDGs를 위한 과학기술혁신에 관한 기관 간 협조체제(The Inter-agency Task Team on Science, Technology & Innovation for the SDGs, IATT)'가 설치되어 STI for SDGs를 지원하고 있다.

둘째, 사이버 공간에서의 주권과 개인정보보호 문제이다. 플랫폼 기업의 데이터 축적과 활용은 곧 사용자의 개인정보를 처리하는 것으로, 초국경 서비스를 제공할 시 자국민을 보호할 책임의 측면에서 주권의 영역과 충돌한다. 주권을 위임하는 거버넌스의 측면에서 각 국가는 데이터 주권 및 데이터 이동에 대해 어떻게 대처하고 있을까? 미국은 투명하고 개방적인 디지털 환경을 요구하며 공식적인 국제 공조를 요구하는 반면, 중국은 내정불간섭과 데이터 주권을 담론으로 내세우며 비공식적인 협력을 선호한다. 투명성과 개방성을 내세우는 자유주의적 담론과 주권과 내정불간섭을 내세우는 중국식 베이징 컨센서스는 실제 동아시아 거버넌스에서 어떻게 작동할까?

셋째, 데이터 규제는 사이버안보와도 밀접한 관계가 있다. 사이버 범죄로 인한 데이터 추적의 국제 공조가 필요한 경우 플랫폼 기업의 주소지, 해당 기업의 데이터 센터의 위치, 해당 플랫폼 서비스 이용자의 국적, 플랫폼 서비스 이용자들의 데이터 발생국 등이 복잡하게 얽혀 각국의 국내법과 개방성 사이에 충돌이 일어날 수 있다. 예를 들어 미국의 빅테크 기업의 본사가 캘리포니아에 위치하고, 데이터 센터는 아일랜드 더블린에 소재하며, 플랫폼 서비스 이용자의 국적은 싱가포르인이고, 플랫폼 서비스의 이용 장소는 태국이다. 만약 범죄와 연루된 데이터 열람과 정보 제출을 요구하고자 한다면 어느 국가의 법규를 따라야 할까? 사이버 범죄를 행한 이들은 가상화폐를 통해 자금 세탁을 함으로써 경제제재의 대상이 되기도 하며, 이들이 해외로 도피할 경우 국제 공조가 필요하다.

개발원조는 인프라와 거버넌스 구축을 통해 국경 간 협력과 지역통합을 촉진한다. 특히 과학기술의 발전에 따라 연계성(Connectivity)이 가치 창출의 핵심으로 부각 됨에 따라 글로벌 경제 패러다임에서 플랫폼 경제가 중요한 부분을 차지하게 되었다. 지역 차원에서 데이터 이동(Data Flow)과 관련한 새로운 법제를 마련하거나 프레임워크를 만드는 일련의 과정은 지역 협력과 통합에 중요한 영향을 미칠 수 있다. 초국경 데이터 규제는 주권을 보호하기도 하지만 무역장벽으로 작용해 무역과 협력을 저해하기도 한다. 동시에 데이터 이동은 자국민의 개인정보보호와 연계되기에 각국은 주권과 자국민의 권리를 보호하면서도 역내 협력을 통한 경제 발전을 도모해야 하는 과제에 직면해 있다.

이 논문은 데이터 규제 및 사이버안보를 국제개발협력에서 국제사회의 투명성과 책무성, 그리고 중국의 내정불간섭의 담론과 연계하여 정리하고 이것이 아세안 지역통합에 미치는 함의를 도출한다. 이를 위해 제2장

에서 국제사회와 중국의 개발원조 및 사이버 공간과 데이터 주권에 대한 규범적 입장을 정리하고, 제3장에서 미국과 중국의 플랫폼 기업에 대한 데이터 규제 및 사이버 안보 정책을 비교한다. 제4장에서는 데이터 거버넌스의 측면에서 아세안 통합 및 동아시아 거버넌스에 미치는 함의가 무엇인지 규명한다. 관련 연구는 한국이 동아시아 역내 협력 방안을 모색하고 데이터 관련 규제 및 전략을 수립하는데 참고자료로 활용될 수 있다.

Ⅱ. 개발원조와 지역통합

1. 레짐과 지속가능개발목표(SDGs)

국제개발레짐은 개발의 쟁점에 있어 행위자들의 기대가 수렴되는 명시적 혹은 묵시적인 규범, 규칙, 원칙 및 정책결정자를 의미한다(Krasner, 1983). 미국의 영향력은 미국 중심의 레짐에 참가하고 미국의 리더십을 따름으로 인해서 상대국이 받을 수 있는 편익을 통해 만들어졌다(Keohane, 2005). 그 편익은 자유로운 국제무역과 지불을 촉진하는 안정적인 국제통화체제, 개방적 상품시장, 그리고 안정적인 석유(에너지) 가격과 그 유통에 기반한다. 하지만 전 산업의 디지털화와 함께 행위자들의 활동 영역이 사이버 공간으로 확장하면서 그러한 편익이 제공되던 환경은 물리적 영토와 사이버 공간이 얽힌 복잡성(Complexity)을 띠게 되었다. 미국 달러와 미국이 주도해 세워진 제도를 중심으로 안정적으로 유지되던 국제통화체제는 화폐 및 지급결제의 디지털화와 함께 새로운 규칙과 제도의 필요성이 대두하였다. 개방적 상품시장 역시 데이터 이동과 규제에 대한 각국의 입장에 따라 이와 관련해 국내법을 제정하고 있다. 마지막으로 안정적인 에너지 가격과 그 유통은 환경문제로 인해 재생 에너지의 개발과 사용으로 전환하는 추세이지만 여전히 석유 및 천연가스 의존도가 높다. 특히 아세안은 에너지 수송로로서의 지정학적 가치를 지니기 때문에 물리적 공간과 사이버 공간에서의 협력과 경쟁이 지역 안보에 지대한 영향을 미치게 되었다.

SDGs는 유엔과 국제사회가 2030년까지 빈곤, 분쟁, 기후변화, 에너지, 주거·고용 등의 경제·사회 문제를 해결하기 위해 세운 목표이다. 다국적 플랫폼 기업의 출현과 함께 SDGs는 디지털 불평등이나 개인정보보호와 같은 플랫폼 경제로부터 야기되는 문제뿐 아니라, 개방성 및 투명성의 원칙, 재원의 다변화, 개인정보보호 등과 관련한 새로운 도전에 직면했다. 특히 초국적 연결시대에는 데이터의 보유·처리·유통과 관련해 특정 행위자가 과도한 권한을 가지면 독점이나 독재로 이어질 수 있다.

미·중 간 패권 경쟁이 치열한 가운데 국가와 시장의 역할에 대한 다른 관점 및 담론은 이러한 초국경 데이터 이동에 대한 규제와 나아가 지역 안보에도 중요한 의의가 있다. 인권에 대한 담론은 미국의 자유주의 가치가 내재한 사례이다. 1990년대 냉전의 종식 후에도 소말리아, 코소보 등 국가에서 대량학살이 일어나자 '유엔개발권선언(Declaration on the Right to Development)에서 개발의 궁극적 목표로 설정한 '완전한 인권의 실현'을 위해 국제사회가 개입해야 한다는 주장이 늘어났다(Lee, 2020). 이는 민주주의, 인권, 그리고 반부패를 지향하는 세부 목표를 담고 있는 SDGs의 16번 목표에서도 확인할 수 있다. 반면에 중국은 인권과 관련한 국제사회의 개입을 내정간섭이라며 반발하고 있다.

플랫폼이나 인공지능과 같은 새로운 행위자의 등장과 함께 대두하는 국제사회의 논의는 투명성·책무성·내정불간섭과 관련한 담론과 사이버안보 및 데이터 주권과 관련한 논의로 나누어 생각해볼 수 있다. 첫째, 투명성·책무성·내정불간섭에 대한 담론이다. 국제사회의 개발원조는 수원국과 공여국의 협력을 위한 투명성과 개발로 인해 발생하는 결과에 대한 책무성이 강조된다. 반면에 중국은 비공식적 협상과 '무조건성, 내정불간섭' 원칙을 통한 투명성이 낮은 협력을 한다. 이러한 중국식 개발원조는 수원국에 책무성을 전가하고 수원국의 부패를 심화시킬 수 있으며(Choi & Hwang, 2022) 국제사회에서 수원국의 거버넌스 개혁을 위해 해왔던 노력을 무력화한다고 비판받고 있다(Ky, 2012; Cheng,

2019; Hong, 2021; Choi & Hwang, 2022).

2019년 중국의 공적개발원조(Official Development Assistance, ODA) 규모는 세계 공여 순위에서 6위에 있다. 중국의 대외원조는 OECD에서 규정하는 공적개발원조와는 성격이 다르다. 중국은 개발원조 기관을 통한 금융지원을 하지 않고, 최고 25%의 무상증여를 포함하지 않으며, 투자의 성격이 강하다. 중국은 자국의 국제개발협력과 일대일로(BRI)를 연계하고 있으며, 이는 거버넌스가 취약한 독재 정권에게 자금을 확보하고 돈세탁의 수단으로 이용되기도 한다.

공적개발원조(ODA)는 지난 10년간 꾸준히 성장해왔지만, 인도주의적 지출과 난민에 대한 지출이 증가함에 따라 개발원조를 위한 재정확보(Financing) 및 투명성의 문제가 대두하였다. 아디스 어젠다(Addis Agenda)는 공공-민간 파트너십을 포함한 혼합 금융의 적절하고 효과적인 사용의 중요성을 인정하고 있다.[1] 2017년 10월에는 OECD 개발원조위원회(Development Assistance Committee, DAC) 혼합 금융 원칙이 승인되었고, 2017년에 개발금융기관(Development Finance Institution, DFI) 워킹 그룹이 향상된 혼합 양허 금융 원칙을 합의하였다. 이러한 혼합 금융은 민간 부문의 과잉 보조금으로 이어질 수 있기 때문에 아디스 어젠다는 SDGs의 달성에 있어 명확한 책임 메커니즘과 투명성을 요구한다. 또한 부채의 지속가능성에 대한 혼합 금융의 역할을 모니터링하고(United Nations 2017) 자금이 어디로 전달되는지 더 정확하게 측정하기 위해 통합국가재정프레임워크(Integrated National Financing Frameworks)의 구축을 권고하고 있다.

둘째, 사이버안보 및 데이터 주권과 관련한 논의이다. 빅데이터는 다양한 방식으로 SDGs의 의제 달성에 기여할 수 있는 요소로 부상하고 있다. 하지만 이러한 데이터는 자칫하면 무분별한 개인정보 수집으로 인한 인권침해나 범죄 행위로 이어질 수 있다. 개방성은 빅테크와 같은 사적 행위자의 데이터 독점으로, 비공식성은 특정 국가권력의 데이터 독점과 정치적 독재로 이어질 수 있다는 위협이 존재한다. 이에 2014년 유엔 통계위원회에 설립된 유엔 글로벌 워킹그룹(Global Working Comittee, GWC)은 2018년 개인정보보호 기술테스크팀을 구성해 플랫폼에서 데이터 암호화에 대한 원칙, 정책 및 공개 표준을 개발하고 있다. 하지만 문제는 국경을 넘나드는 다국적 기업의 경우 그 본사와 데이터의 소재지, 서비스 이용국, 이용자의 국적 등의 복합적인 요인으로 인해 테러, 사이버 범죄 등을 위한 공조가 필요한 경우 정보와 데이터와 관련한 문제가 복잡성을 띠게 되었다.

2. 지역통합과 안보

Balassa는 지역 경제 통합의 이론으로 자유무역지대(Free Trade Area), 관세동맹(Customs Union), 공동시장(Common Market), 경제동맹(Economic Union), 정치·경제적 통합(Economic & Political Union)의 다섯 단계를 거친다는 단계적 분석을 발전시켰다(Balassa, 1961). 지역통합은 제도적 틀 내에서 발생하기 때문에(Keohane & Nye 1975: 368) 초국경 데이터 규제는 지역 단위의 프레임워크를 수립함으로써 상호의존을 강화한다는 측면에서 지역통합을 촉진할 수 있다.

통합은 종국에는 안보와 연결된다. 패권안정이론(Hegemonic Stability Theory)은 패권(Hegemon)이 공공재(Public Goods)를 공급함으로써 시장의 개방성을 유지한다고 주장한다. 제2차 세계대전 후 고정환율의 시대는 미국이 세계 안보와 글로벌 통화체제의

1) 2017년 세계은행, 지역개발은행, 기타 다자간 및 정부간 기관을 포함한 다자개발은행(MDB)의 총 대출은 630억 달러에 이르렀는데, 그 중에서 225억 달러는 양허성이었다. 특히 아시아인프라투자은행(AIIB)와 신개발은행(NDB)이 MDB에 합류하였다. AIIB의 대출 약정액은 2018년 9월 기준 33억 달러였으며, NDB는 2017년 18억 달러 상당의 신규 대출을 승인했다. World Bank Group(WBG) 주주들은 MDB에서 납입 자본을 확충하는 것을 고려하고 있다. 특히 2018년 4월에는 IBRD 75억 달러, IFC 55억 달러로 구성된 130억 달러의 유상자본 증자를 승인했다. 이렇게 승인된 자금은 IDA의 양허성 자원과 혼합될 것이다.

유지에 필요한 비용의 많은 부분을 감당함으로써 작동하였다. 전후 경제를 관리하게 위해 창설된 국제통화기금(IMF)과 세계은행(World Bank), 그리고 관세 및 무역에 관한 일반협정(GATT)는 케인즈주의 색채의 내재적 자유주의(Embedded Liberalism)의 기반하에 탄생하였다. 브레튼우즈 체제하의 고정환율제 시기에는 대다수 국가가 직접적인 자본통제를 통해 외환시장의 동요를 회피하였다. 국내 정책을 통해 세계시장에의 접근을 점진적으로 조절하거나 지역 경제 통합을 활용해 세계 경제로부터 보호 조치를 취할 수도 있었다(Park, 2003). 하지만 1973년 고정환율제가 변동환율제로 대체되고 1990년대 세계화가 진전되면서 각국은 세계 경제에서 유통되는 통화량과 통화에 대한 투기에 취약해졌다.

1990년대 이후 지역주의는 '개방적 지역주의'의 성격을 띠게 되었는데, 이는 곧 수출 혹은 외자 유치를 통해 세계시장과의 적극적 통합을 추진함을 의미했다(Katzenstein, 2005; Archara, 2007; Archara, 2014). 이러한 지역 경제 통합은 다자간 지역투자무역협정(Regional Trade Agreement, RTA)에 참여하는 국가들이 지역 시장(Regional Market)을 형성하는 것에서 확인할 수 있다. 특히 남반구 개발도상국들은 외자 유치와 선진수출시장에 대한 협상력을 높이기 위해 활발한 지역 경제 통합의 움직임을 보였다(Krapohl, 2017).

미·중간 패권 경쟁이 심화함에 따라 자원이 풍부한 개도국에 대한 원조 경쟁 역시 치열하다. 아세안은 동아시아 경제위기를 계기로 역외 무역 비중이 확대되었으며, TPP와 RCEP에 모두 참여하고 있다. 동남아시아 지역은 주요 자원의 수송로이자 심해 자원을 가진 지정학적인 군사·안보의 요지이다. 뿐만 아니라 6억 명에 이르는 인구는 데이터 자원으로 인해 디지털 경제의 발전 가능성이 많다. 국경간 데이터 흐름의 촉진은 지역 거버넌스에 일부 주권을 위임한다는 점에서 데이터 기반 경제와 지역 통합에 영향을 미칠 수 있다.

3. 사이버 공간과 데이터 주권

국가는 일정한 영토와 조직된 정치 형태인 정부를 통해 대내외적 자주권을 행사하는 정치적 실체이다. 베버는 국가를 "일정한 영토 내에서 단독 및 합법적으로 물리력을 사용할 수 있는데 성공한 인간의 집단"이라고 정의하였고(Weber, 1919), 주권은 영토, 독립, 평등과 같은 국제법적 개념들과 불간섭이나 무력 사용 금지 등의 국제법 원칙과 함께 설명된다(Park, 2020).

과학기술의 발전과 함께 사이버 공간에 대한 주권의 적용에 대한 논의 역시 활발하게 이루어지고 있다. 데이터 주권(Data Sovereignty)의 개념은 데이터 이동을 촉진해 관련 산업을 활성화하는 동시에 국경 간 정보 이동 제한이나 데이터 국지화 정책을 통해 개인정보보호의 필요성이 대두하면서 부상하였다(Krüger, 2016; National Information Society Agency, 2018; Jeong, 2019). 국제 안보와 관련해 유엔정부전문가그룹(UNGGE)은 2013년 제3차 UNGGE 보고서에서 "국가 주권과 주권에서 나오는 국제규범 및 원칙들이 자국의 영토 내 정보통신기술과 관련된 행위의 수행에 적용된다."라고 적시하고 있다.

탈린 매뉴얼 2.0에서는 "국가 주권의 원칙이 사이버 공간에 적용된다."라고 적시한바, 곧 국가의 주권 영토에 자리한 물리적 기반시설, 사람 및 사이버 활동에 대해 주권적 권한을 가지고 있다는 것이다(Schmitt, 2013). 조화순(2015)은 데이터 주권은 "국가 이익의 차원에서 자국 내에서 유통되는 정보에 대해 외부로부터 간섭을 받지 않는 궁극적 결정권 및 통제의 제반 권리"라고 정의하고 있다. 하지만 다국적 기업의 소재 위치, 데이터 서버의 위치, 서비스 제공 위치, 사용자의 국적 등이 복잡하게 얽히며 데이터 주권의 논의 역시 한층 더 복잡성을 띠게 되었다. 예를 들어 개인정보 제공 내역 요청 등의 법적 보호는 국내법에 기반하지만, 전 세계에 이용자를 가진 구글 서비스 약관은 "독점적으로 미국 캘리포니아주 법률에 따르는 것을 동의"하도록 하고 있다. 즉, 등록된 회사의 소재지에 기반한 생산 및 유통되

는 데이터에 대해 국내법을 적용하고 배타적 권리를 행사하는 데 한계를 보여주는 것이다(Cho, 2015: Jeong, 2019 재인용).

사이버 공간의 주권에 대한 규범적 입장은 국가마다 다르다. 데이터 주권과 관련해 각국은 개인정보보호 문제에 어떤 입장과 대응을 보이고 있을까? 유럽은 개인정보보호가 사회문화적 가치를 담고 있다고 인식하는 반면, 미국은 개인정보를 재산권적 가치로 인식하고 자발적 흐름을 선도하는 경향이 강하다(Jeong, 2019). 미국과 유럽은 2000년 세이퍼 하버 협정을 통해 고지 원칙(Notice), 선택 원칙(Choice), 제삼자에의 정보이전원칙(Onward Transfer), 보안(Security), 정보의 완결성 원칙(Data Integrity), 접근(Access), 집행(Enforcement)의 7대 원칙을 규정하였다. 하지만 미국 정보당국이 자국 빅테크 기업의 서버에 설치된 별도의 프로그램을 통해 이용자를 감시한다는 것이 밝혀지자 해당 협약은 무효로 선언되었다. 이후 EU 역외에 있는 기업이라도 그 서비스가 유럽 시민에 적용된다면 유럽 정보보호 규칙을 따르도록 하고 있다(GDPR Art. 3 Abs. 2.; Jeong, 2019).

미국의 경우 오바마 행정부 시기에는 사이버 공간에 대해 기존의 물리적 영토에 기반한 전통적 주권 관념을 내재한 법을 적용할 것을 주장했으나(Koh, 2012; Park, 2020) 트럼프 행정부 시기에는 타국의 동의 없이도 타국에서 이용되는 사이버 기반시설에 대한 사이버 오퍼레이션이 가능하다는 태도로 변화했다(Watts & Richard, 2018; Park, 2020). 중국은 데이터 주권을 내세워 영토를 경계로 분리된 네트워크를 원칙으로 하는 강력한 국지화 정책을 취하고 있다. 이를 뒷받침하기 위해 제정된 『네트워크안전법』은 중국에서 생산된 데이터를 중국 영토 내에 저장하는 것을 강제할 뿐 아니라 기업에는 체제에 반하는 콘텐츠 검열을 의무화하고 국민에는 해외 사이트 접속을 차단하고 있다(National Information Society Agency, 2018). 이러한 조치는 무역기술장벽(Technical Barriers to Trade, TBT)으로 작용한다.

유럽 시장에서 미국의 글로벌 테크 기업의 독점이 강화하면서 유럽 국가들은 데이터 보호를 위해 자국민 데이터의 국외 이전을 위한 조건과 절차를 강화하고 해외 서버 이전을 제한하였다(Jeong, 2019). 러시아도 국민의 개인정보는 국내에 있는 데이터 서버로 관리해야 하며(Chander & Le, 2015) 캐나다 역시 캐나다 영토에서 생산된 데이터를 캐나다에 있는 서버에 저장하도록 하고 있다. 이는 캐나다 데이터가 2001년 테러리즘 저지와 회피를 위해 제정된 『애국자법(The Patriot Act of 2001)』의 대상이 되지 않기 위함이다(Government of Canada Information Technology Strategic Plan 2016-2020).

데이터 주권은 국가의 데이터 통제를 강화함으로써 감시 및 검열을 정당화할 수 있다는 한계도 있다(Kim, 2017). 중국은 2019년 10월 중국 우젠에서 개최된 제6차 세계인터넷대회에서 '사이버 공간에서의 주권: 이론과 관행'을 통해 독립권, 평등권, 관할권, 자위권이 포함됨을 명시하였다(Park, 2020). 중국은 이를 통해 서구의 개방형 인터넷과 다른 인터넷 및 그 콘텐츠에 대한 검열과 통제에 대한 근거를 마련하고 있다. 국경 간 결제는 사이버보안 위협의 표적이 되기 쉬우며 규모가 작은 기업일수록 이에 더 취약하다. 사기 및 사이버 위험의 증가에 따라 국가 간의 분쟁을 방지하기 위해 사이버보안과 관련한 민관 파트너십을 구축하거나 상호 법률 지원을 위한 조약을 세우는 등 새로운 형태의 거버넌스의 필요성이 증가하고 있다. 정보가 돈이자 권력인 디지털 시대에 개인정보의 국외 이전은 국제무역의 한 형태로 볼 수 있으나 이와 관련한 적절한 규범과 법체계가 마련되지 않아 국가 간 협력을 저해하고 갈등의 요인이 되고 있다.

Ⅲ. 미국과 중국의 초국경 데이터 규제 비교

시장은 전통적인 영토와 국가의 경계를 넘나들도록 하며 1990년대 냉전의 해체로 급속도로 확산하였다. 미국의 시장은 자유주의 이념을 기반으로 민간 행위자

들, 즉 기업 친화적인 환경이 조성해 있는 반면에 중국은 생산 수단을 국가가 통제하는 사회주의 체제를 유지하고 있다.

전 산업의 디지털화는 다양한 행위자들이 전통적 영토의 경계를 넘어서는 것을 촉진한다. 각국은 주권과 자국의 산업을 보호하기 위해 각종 규제를 통해 중상주의적 정책을 펼치기도 한다. 이러한 플랫폼 결제 서비스 제공이나 보안 감독 등과 관련된 규제는 무역기술장벽(TBT)으로 작용할 수도 있고, 오히려 자유로운 데이터 이동과 협력을 촉진할 수도 있다.

데이터의 수집, 처리, 조회는 사이버안보에도 중요한 역할을 한다. 글로벌 빅테크 기업의 본사가 위치한 미국은 역외 데이터 접근에 대한 법률적 근거를 마련하기 위해 클라우드 액트(The CLOUD Act)를 제정하였다. 이는 외국 정부와 개인정보보호에 대한 상호 존중을 기반으로 하여 국제 협정을 체결하는 기반이 되고 있다. 반면 중국은 『데이터안전법』의 제정을 통해 데이터 이동을 장려하는 것 같으면서도 국익에 반하는 행위를 규제하는 근거를 마련하고 있다.

1. 미국의 초국경 데이터 규제

미국 중심의 자유주의적 관념은 인터넷과 데이터 이동과 관련한 문제에서도 드러난다. 인터넷은 누구나 편견 없이 진입해 자신의 신념을 표현할 수 있는 인간 행위의 자유를 보장해야 하며, 데이터 소유권에 대한 법적 규제를 통해 그 이동을 자유롭게 해야 한다는 태도를 견지한다(Barlow, 1996; Lee, 2020). 이러한 표현의 자유는 미국의 수정헌법 1조에 명시되어 있으며, '사상의 자유시장론(Marketplace of Ideas)'과 Abrams vs. United States(1919) 판결에서 비롯되었다(Chang, et al., 2021; Choi, 2022).

1) 미국의 사이버안보와 정보보호

미국은 사이버 공간의 보호를 국가안보의 현안 중 하나로 여겨왔다(Hyeon, 2009). 산업스파이 활동으로 인한 피해뿐만 아니라 금융서비스나 전력시설 등 물리적 사회기반시설이 사이버 공격에 노출되는 경우 세계 시장에서 미국의 경쟁력과 주도권이 위협을 받을 수 있기 때문이다(Hyeon, 2009). 미국은 1980년대부터 정보보호정책과 관련한 법률을 제정하였는데 사이버안보와 관련한 법은 1980년 제정된 『프라이버시보호법(Privacy Protection Act)』과 1986년 제정된 『전자통신프라이버시법(Electronic Communications Privacy Act)』, 그리고 1987년 『컴퓨터보안법(Computer Security Act of 1987)』이 대표적이다.

9·11사태 이후 사이버보안에 대한 인식이 더욱 강화하면서 부시 대통령은 2001년 『애국자법(The Patriot Act of 2001)』을 제정하였다. 이는 미국 재무부 비밀검찰국에 테러리스트 공격 등 전자 범죄에 대한 예방, 탐지, 조사하기 위한 네트워크를 개발할 수 있는 권한을 부여한 것이었다. 미국국가안전보장국(National Security Agency, NSA)은 『애국자법』 215조를 토대로 미국 시민 수백만 명의 통신기록을 한꺼번에 수집해 5년간 보관하는 권한을 행사할 수 있었다. 『애국자법』은 2013년에 에드워드 스노든(Edward Joseph Snowden)의 폭로사건 이후 인권침해 논란이 불거지자 2015년 6월 『미국자유법(The USA Freedom Act)』으로 대체됐다. 이로써 시민의 통신기록은 원칙적으로 통신회사만 보유하고, 정보기관은 개별 통신기록에 대해서만 법원 영장을 발부받아 접근할 수 있게 되었다(Cho, 2015).

클라우드 컴퓨팅(Cloud Computing) 서비스의 보편화와 함께 데이터가 실제 저장된 위치를 알지 못하는 경우가 있다(Song, 2018). 즉, 데이터가 여러 지역의 서버에 분산되어 저장해 있어 테러리즘 등의 범죄에 대응할 시 데이터에 대한 접근이 제한적인 경우가 발생하는 것이다. 범죄자들의 다국적 기업의 서비스 이용이 증가하면서 각국 경찰이 데이터 소재국과 공조하기보다 글로벌 통신서비스 제공자에 대한 직접 데이터 요청이 급증하고 있다. 이러한 행위의 적법성은 국제법상 영토 주권의 침해 및 개인정보보호와 연계되어 사안에 따라 다르게 나타난다.

2013년 미국 연방정부가 마이크로소프트를 상대로 마약 밀매 사건과 관련된 이메일 계정 정보 제출을 요청하였으나, 데이터가 아일랜드 더블린의 데이터 센터에 저장되어 있다는 이유로 거절한 사건이 발생한다(Song, 2018). 이와 관련해 2016년 7월 미국 제2 순회 항소법원은 더블린에 소재한 데이터 센터에서 집행된 영장에 대한 행위가 미국 밖에서 일어났으므로 법률의 불법적인 역외 적용이라고 판시하였다(Stored Communications Act 2703; Song, 2018). 이 사건 이후 역외 데이터 접근에 대한 법률적 근거를 마련하기 위해 미국은 2018년 종합세출법안(Omnibus Appropriations Bill)을 통과시켰다(H.R.4943 — 115th Congress (2017-2018); Song, 2018). 이 법안은 합법적 해외 데이터 활용을 명확히 하는 CLOUD Act(Clarifying Lawful Overseas Use of Data Act)를 포함하고 있다.

CLOUD Act는 글로벌 빅테크 기업과 같이 미국의 통신서비스 제공자들이 관리 및 보유하는 가입자 정보, 트래픽 데이터, 통신 내용 등에 대해 정부 기관이 데이터가 저장된 위치와 무관하게 제공 요청을 할 수 있도록 명시하고 있다. 이 법률(Act)은 『저장통신법(Stored Communications Act)』[2]에 미국과 외국 정부 간의 행정 협정(Executive Agreement)에 대한 근거를 마련함으로써 초국경적 정보 제공에 관한 규정을 명시하였다는 것에 주목할 필요가 있다(CLOUD Act § 105(a) (18 U.S.C. § 2523 신설). 만약 외국 정부의 국내법과 그 실행이 프라이버시 및 자유권을 보장하는 등의 요건을 충족하면 미국과 행정 협정을 체결할 수 있도록 한 것이다. 이 행정 협정은 미국과 다른 국가들이 상호 정보를 공유하고 해외에 저장된 데이터에 접근할 수 있도록 한다. 또한 CLOUD Act는 미국 정부에 의한 영장의 집행이 외국의 국내법을 위반할 소지가 있는 경우 서비스 제공자가 영장에 대한 각하나 변경 청구를 함으로써 외국의 국내법과의 충돌을 예방하고자 하였다(Song, 2018). 구글, 메타(페이스북), 마이크로소프트 등 미국에 본사를 둔 빅테크 기업은 대다수 전자 통신을 자사의 서버에 보유하고 있기 때문에 CLOUD Act의 통과에 따라 더 많은 국가가 미국과의 행정 협정을 시도할 수 있다.

2) 미국의 암호화폐와 사이버 안보

미국의 자유에 대한 관념은 민간 화폐 발행과 그 사용에서도 확인할 수 있다. 가상화폐(Virtual Currency) 중에서도 블록체인(Blockchain)을 이용한 암호화폐(Cryptocurrency) 산업은 2008년 비트코인(Bitcoin)이 처음 등장한 후 급속히 성장했다. 이는 분산원장기술(Distributed Ledger Technology)을 통해 중앙통제 시스템이 부재한 사적 화폐의 발행과 그 이용으로 이어졌다. 하지만 이러한 가상화폐는 테러리스트를 비롯한 범죄자들의 자금 세탁 등 불법적 용도로 사용될 수 있다는 우려를 낳았으며 실제로 그러한 사례가 발견되고 있다. 특히 2001년 미국 애국자 법의 통과와 함께 도입된 금융제재로 인해 어려워졌던 자금 세탁 및 제재 회피가 비트코인을 포함한 암호화폐들로 인해 다시 쉬워졌다(Todd Jacquez, 2016).

미국은 행정명령 제13694호(2015) 및 제13757호(2016)를 통해 랜섬웨어 공격 등 사이버 범죄 행위를 저지른 자의 자산을 동결하고 있다. 하지만 랜섬웨어 공격 시 범죄자들이 주로 암호화폐를 사용하므로 가상화폐와 관련된 경제제재로 분류된다(Kim, 2021). 미국 해외자산통제국(Office of Foreign Assets Control, OFAC)은 2021년 10월 〈가상화폐산업에 대한 제재 준수 관련 지침(Sanctions Compliance Guidance for the Virtual Currency Industry)〉를 발표하여 기존의 OFAC 제재 준수 프레임워크 및 경제제재 가이드라인이 가상화폐 기업에도 적용됨을 적시하였다.

가상화폐와 관련한 사이버 범죄 사례는 2015년 이

2) 『저장통신법(Stored Communications Act)』은 1986년 전자통신 프라이버시법(Electronic Communications Privacy Act)의 Title 2에 '제3자 인터넷 제공자(ISPs)에 의해 저장된 유선 및 전자 통신과 거래 내역의 자발적 강제적 공개'를 명시한 법안이다. 『저장통신법』은 정부가 서비스제공자에게 미국 관할권 외에 저장된 데이터의 제출을 요구할 수 있는지 등에 대한 명시적 규정이 없었으며 CLOUD Act는 이러한 『저장통신법』의 개정과 함께 제정되었다.

란인 위주의 범죄자들이 Samsam이라는 랜섬웨어를 만들어 전 세계 200여 개 기관에 파일 잠금 악성코드를 유포하고 피해자로부터 암호화폐로 대가를 받은 사건이 있다. 이때 OFAC는 두 명의 이란인 남성을 제재 대상에 추가함으로써 이들과의 거래를 금지하고 자산을 동결시켰다. 해당 사건에 관련된 또 다른 두 명의 이란인 남성은 현재 도피 중이며, 미국의 연방수사국(Federal Bureau of Investigation, FBI)뿐만 아니라 캐나다 경찰청, 영국의 국가범죄청 등의 여러 정부 부처의 공조가 이루어지고 있다.

3) 반독점법안 패키지

미국은 2018년 기관 간 우선순위로 '데이터의 전략적 자산화'를 목표로 정하였고(OMB, 2020; Yoon and Kwon, 2021), 같은 해 『캘리포니아주 소비자프라이시법(California Consumer Privacy Act of 2018: CCPA)』이 제정되어 소비자가 언제든지 본인의 개인정보 처리 혹은 판매를 중단하도록 했다(Yoon and Kwon, 2021). 이는 데이터를 사적 재산으로 바라보고 그 재산권의 주체를 분명히 하여 행사하도록 한 자유 관념이 드러난 사례이다.

2021년 6월 미국 하원에서 발의되어 법제사법위원회를 통과한 반독점법안 패키지의 5개 법률은 월간 활성 사용자 5,000만 명 이상, 시총 6,000억 달러 이상인 GAFA(Google, Amazon, Facebook, Apple)의 지배력에 대한 규제안이다(Maeil Economy, 2021). 그중에서 데이터 이동(Data Flow)와 관련된 법률은 『서비스 전환 활성화를 통한 경쟁과 호환성 증진법(Augmenting Compatibility & Competition by Enabling Service Switching Act)』이 있다. 이 법률은 사용자가 데이터를 다른 플랫폼으로 쉽게 이동하도록 데이터 이동(Data Flow)과 상호운용성(Interoperability)을 보장한다. 예를 들어 페이스북 사용자가 자신의 데이터를 타사 플랫폼으로 쉽게 이동할 수 없어 생기는 네트워크 효과는 시장 경쟁에 해롭기 때문이다. 이는 유럽의 데이터 보호 법안인 GDPR에도 명시되어 있다.

이 외 4개 법률은 공정한 시장 경쟁을 추구하는 자유 관념이 내재한 것으로 볼 수 있다. 즉, 글로벌 빅테크 기업 등이 과도한 데이터 축적과 활용을 통해 시장 경쟁을 저해하는 것을 방지하기 위한 것이다. 첫째, 『미국 온라인 시장 선택과 혁신 법률(American Choice & Innovation Online Act)』은 플랫폼이 자사 상품에 유리하게 검색 결과를 왜곡하거나 플랫폼 운영을 통해 얻게 된 비공개 데이터를 통해 자사 상품을 우대하는 등의 차별적 행위를 규제한다. 둘째, 플랫폼 독점 종식 법률(Ending Platform Monopolies Act)은 타 업체에 불리할 수 있는 플랫폼의 이중 역할(Dual Role)로 인한 이해 상충을 일으키는 사업을 금지하는 것이다. 셋째, 『플랫폼 경쟁과 기회 법률(Platform Competition & Opportunity Act)』은 빅테크가 다른 사업자를 인수·합병함으로써 시장 혁신과 경쟁을 제한하고 시장지배력을 강화하는 것을 견제하는 법률이다. 넷째, 『M&A 수수료 현실화 법안(Merger Filing Fee Modernization Act)』은 M&A시 경쟁 당국에 내야 하는 수수료를 인상하는 법률이다.

이러한 반독점법안은 공정한 시장 경쟁을 촉진하려는 의도를 가지고 제정되었지만, 기업들은 자사에 유리한 세제 혜택을 찾아 국경을 넘나드는 경향이 있다. 이는 곧 각국의 국내법 역시 행위자의 초국경적 활동에 영향을 미치기 때문에 공정한 시장 경쟁과 관련한 자유 관념을 확산하고자 하는 유인이 될 수 있다.

2. 중국의 초국경 데이터 규제

중국은 강력한 중앙 집중형 권력을 통해 자원을 배분하는 정치 체제를 유지해 왔으며, 이러한 권위주의적 특징은 인터넷과 데이터 관련 정책에서도 드러난다. 중국의 권위주의 인터넷은 중국식 개발원조를 통해 이를 확산하려는 노력으로 이어진다. 디지털 실크로드를 통한 정보통신 인프라 건설, 생체 정보 인식, 감시 체계 구축 계약, 그리고 관료들에 대한 기술이전 세미나의 개최 등이 그 사례이다.

1)『데이터안전법』

중국은 2015년『국가안전법(中华人民共和国国家安全法)』을 국가안보의 기본법으로 입법함으로써 사이버 안보를 국가안보의 영역에 포함했다. 전국인민대표대회 상무위원회는 데이터 보안과 관련된 입법을 추진하여 2020년 7월 3일『데이터안전법(초안)数据安全法』이 공개되었고, 2021년 6월 10일 전인대 상무위원회 제29차 회의에서 최종안이 최종 통과되었다. 이『데이터안전법(数据安全法)』은『네트워크안전법(中华人民共和国网络安全法)』 및『개인정보보호법(中华人民共和国个人信息保护法)』과 함께『국가안전법』을 지원하고 있다(Lee, 2021).

『데이터안전법』 제1장 제7조와 제11조는 "국경 간 데이터 이동을 촉진함"을 명시함으로써 자국의 글로벌 빅테크 기업의 데이터 수집 및 이동에 대한 법적 근거를 마련하고 있다. 하지만 규제 목록을 만들어 수출 규제를 하고 있고, 중국 역외에서의 데이터 처리나 중국 내 저장한 데이터 제공을 불허할 수 있는 법적 근거 역시 마련하고 있다. 제1장 제2조에서 "중국 역외에서의 데이터 처리 활동이 중국 국가안전·공공이익 또는 공민·조직의 합법적인 권익에 손해를 끼치면, 이 법에 의거 해 법적 책임을 묻는다."라고 했으며, 제3장 제25조 "국가는... (중략) 규제 목록에 속하는 데이터에 대해 법에 의거 해 수출 규제를 시행한다."라고 명시한 것이 그것이다. 이는 곧 중국의 국가 이익에 부합하는 데이터 이동은 허용하고, 부합하지 않는 데이터 이동은 불허하고자 하는 중국의 의도를 엿볼 수 있다. 특히 제4조 제36조에서 "중국 당국의 승인 없이 중국 내 조직이나 개인이 외국의 사법이나 법 집행 기관에 중국 내 저장한 데이터를 제공할 수 없다."라고 명시하고 있다(Lee, 2021). 이를 통해 중국 영토 내 관할 구역에 대한 강력한 주권을 주장하고 있고, 데이터 이동과 관련해 국가가 강력하게 주도하고 그 권한을 가짐(내정)을 확인할 수 있는 대목이다.

2) 중국의 디지털 화폐

중국은 자국의 금융 시스템이 채무자 중심이며 서구의 금융 시스템은 채권자 중심의 약탈적 시스템이라며 비판한다. 하지만 중국의 금융 시스템은 권위주의 정부에 의해 강력하게 통제되어 자원이 중앙에 집중되는 시스템이라는 비판 역시 존재한다. 중국과 같은 사회주의 정부는 부채를 상환할 수 없을 때 강제 폐쇄, 파산, 자산 및 일자리의 손실 없이 산업을 지속해서 운영할 수 있다. 중국 정부가 최종 채권자이기 때문에 계획된 부채 상환, 세금, 임대료 및 공과금에 대한 계획을 수정할 수 있기 때문이다.

중국 정부 당국은 빅테크를 규제하고 중앙은행이 모든 데이터를 독점적으로 소유, 접근 및 사용할 수 있다. 중국의 몇몇 학자는 중국의 강력한 중앙 정부가 부를 창출한 후 '재분배' 과정인 효과적인 재정 이전을 통해 빈부 격차를 완화할 수 있다고 주장한다. 블록체인과 스마트 계약으로 강화된 디지털 화폐(Digital Currency Electronic Payment, DCEP)는 이러한 재분배 역할을 더욱 잘 수행할 수 있다는 것이다(Long, 2020).

2018년 1월 1일부터 중국인민은행(PBoC)은 비 예금 기관 부문이 보유한 머니마켓펀드(Money Market Fund, MMF)를 광범위한 RMB M2 통계에 포함시켰다. 앤트파이낸셜이나 텐센트를 필두로 한 디지털 금융 서비스의 확장은 상업 은행의 소매 예금을 감소시켰고 독점적 시장지배력에 대한 위협이 되었다. 데이터 권리에 대한 독점, 기존 금융 기관과의 압도적 교섭력 차이, 그리고 다른 시장 참여자의 배제로 인한 문제가 인식되자 중국 정부는 이와 관련한『데이터안전법』의 제정을 통해 독점과 관련한 규정을 마련하고 있다.

시진핑 중국 국가주석은 2021년 3월 15일 제9차 중앙재경위원회에서 데이터 재산권 제도(数据产权制度)를 구축할 것을 지시하였다. 이는 플랫폼 기업의 데이터에 대한 안전과 보호의 책임을 강화하고자 한 것이다. 이러한 조치는 플랫폼 기업의 데이터 독점에 대응하기 위한 원칙이 수립된『개인정보보호법』에서도 확인할 수 있다.『개인정보보호법』의 제6조에서는 개인정보의 수집을 "목적 실현에 필요한 최소한의 범위"로 한정하고 있으며, 제45조에서는 특정 플랫폼만이 데이터를 독점

하는 것을 방지하고 있다(Lee, 2021). 제21조 제1항에서는 국가가 데이터를 등급별 유형별로 보호하는 제도를 마련할 것을 규정하고, 유관부서가 중요데이터 보호를 총괄 및 조율한다고 명시하였다(Lee, 2021). 이는 곧 정부 권한의 강화와 통제와 검열에 대한 정당성이 확보됨을 의미한다. 이처럼 중국은 데이터 이동과 규제에 대한 법적 근거를 마련해놓고 있지만, "중국 당국의 승인 없이" 혹은 "국가안전 등의 권익에 손해를 끼치면" 등의 구문이 자의적으로 해석될 수 있다.

3) 부패와 자금 투명성

에이드데이터(AidData)에 의하면 중국 ODA는 지원 금액과 분야가 불투명해 그 규모를 알기 어렵다. 특히 중국의 원조는 내정불간섭의 원칙으로 인해 거버넌스 개선을 요구하지 않는다. 이는 곧 권위주의 국가가 투명성이나 책무성에 대한 부담을 지지 않으며, 권력의 사유화와 부패와 연계될 가능성을 보여준다. 중국이 주도하는 남남협력이 전통 개발협력의 재원을 보완하는 측면에서 긍정적으로 평가되지만, 중국의 구속성(Tied), 무조건성의 특징을 가진 이러한 원조가 오랜 기간 수혜국의 거버넌스 개선을 위해 해왔던 노력을 무력화할 수 있다(Ky, 2012; Cheng, 2019; Hong, 2021). 또한 영국 Publish What You Fund에 의하면 중국의 원조 투명성 지수(Aid Transparency Index)는 매우 취약한(Very Poor) 국가로 분류된다(Aid Transparency Index; Choi & Hwang, 2022).

중국과 동남아시아의 권위주의 정권과의 협력이 부패로 이어지는 사례도 있다. 권위주의 정권 간의 비공식적 협력은 비공식 무역장벽으로 작용함으로써 공정한 시장 경쟁을 통한 개도국의 건전한 성장과 발전을 저해할 수 있다. 말레이시아는 나집이 총리로 있던 2016년 중국의 통신건설사인 CCCC(China Communications Construction Company)와의 계약을 하면서 말레이시아 동부와 서부 해안의 육상다리를 잇는 말레이시아 동해안 철도(The East Coast Rail Link, ECRL) 사업이 시작되었다. 이전까지는 중국이 말라카해협을 통과하기 위해서는 싱가포르 항구를 경유해야 했다(Choi & Hwang, 2022). ECRL 사업은 중국의 쿤밍에서 말레이시아로 이어지는 남북 경제회랑을 건설함으로써 새로운 육상 교역로가 개척된다는 의의가 있었다. 하지만 이 사업은 CCCC와 나집 정부의 입찰 계약 과정에서 타당성 검토에 불과 2 개월이 소요되는 등 서둘러 낙찰되었고, 나집 정부는 선지급된 공사대금을 1MDB 자금난 해소에 사용하고자 했다. 중국 국영 은행인 중국공상은행(ICBC, Industrial & Commercial Bank of China)이 중국의 대출과 그 자금의 세탁 과정에 깊이 관여한 정황이 포착되었다(Choi & Hwang, 2022). 부패 권력은 결국 2018년 나집 정부의 몰락으로 이어졌으며 말레이시아 금융 거버넌스의 취약점을 여실히 드러냈다.

Ⅳ. 아세안 통합에의 함의

아세안은 1967년 인도네시아, 말레이시아, 싱가폴, 태국, 필리핀의 해양국을 중심으로 출범하였고, 1990년대 대륙국인 CLMV(캄보디아, 라오스, 미얀마, 베트남) 국가가 합류하면서 외연이 확대되었다. 아세안은 미국과 중국 사이에서 헤징(Hedging) 전략과 아세안 중심성(ASEAN Centrality)을 원칙으로 내세우고 있어, 이들이 경제 공동체에서 안보 공동체로 진화할 것인지에 많은 학자가 관심을 보인다.

국경 간 데이터의 흐름은 아세안의 디지털 경제를 뒷받침한다. 즉, 상호운용 가능한(Interoperable) 데이터 거버넌스의 시스템은 아세안의 디지털 경제와 생태계의 강화에 중요하다. 아세안은 2010년 아세안 정상회의에서 아세안연계성마스터플랜(Master Plan on ASEAN Connectivity, MPAC)을 통해 연계성 증진과 역내 통합에 관한 논의를 본격화했고, 2016년 아세안 정상회의에서는 디지털 분야를 주요 전략적 추진 분야로 설정한 아세안연계성마스터플랜 2025(MPAC 2025)를 채택했다(The ASEAN Secretariat 2016). 이처럼 디지털 협력은 역내 연계성과 통합에 중요한 부분을 차지하고 있다.

1. 아세안과 미·중 경쟁

1) 미국과의 협력

데이터 프라이버시를 위한 규제 프레임워크는 아시아 및 전 세계 국경 간 데이터 흐름을 촉진하는 데 중요한 역할을 한다(GSMA, 2018). 규제를 통한 데이터의 안전한 공유는 기업이 상업과 경제발전을 도모할 수 있도록 하기도 한다. 투명성과 개방성을 담론으로 내세우는 미국은 아세안에서도 자유로운 데이터의 흐름을 기반으로 협력을 하고 있다. 미국의 US-ABC(US-ASEAN Business Council)은 ASEAN이 데이터 기반 경제를 육성하도록 돕고 있으며, ASEAN 디지털 데이터 거버넌스 프레임워크(ASEAN Framework on Digital Data Governance)를 통해 정책 및 규제의 접근 방식을 조정할 것을 강조하고 있다. 또 개인정보보호 및 개인정보의 국경을 넘나드는 흐름에 대한 OECD 가이드라인, APEC 개인정보보호 프레임워크 및 『일반개인정보보호법(General Data Protection Regulation, GDPR)』과의 사례와 일치시킬 것을 권고한다. 미국은 특히 다자적 관여 수단의 협력적 제도와 메커니즘을 위해 지역 기구인 ASEAN의 중요성을 강조하고 있으며, APEC과 ASEAN의 협력을 통해 투명성·개방성·공정성 등의 자유 관념을 확산시키고자 한다.

미국은 APEC CBPR(Cross Border Privacy Rule)의 다자간 데이터 전송 프레임워크와 같은 기존의 양자와 다자 프레임워크의 활용을 권고하고 있다. 또한, 지역적 데이터 전송을 촉진하는 메커니즘뿐만 아니라 양자 간 데이터 전송, 비 개인 데이터의 자유로운 이동 등에 대한 지침을 발표하도록 권고하고 있다(US-ASEAN Business Council). 이로써 기업이 국경 너머에서 활동할 때 개인 데이터의 정보보호를 위해 확립된 원칙과 메커니즘을 사용할 수 있도록 하는 것이다.

일부 아세안 회원국은 데이터 보호법을 제정함으로써 이러한 메커니즘을 받아들이는 듯 보인다. 예를 들어 싱가포르는 『개인데이터보호법 2012(PDPA: Personal Data Protection Act 2012)』의 제정을 통해 데이터가 '비교 가능한 보호 표준'을 제공하는 한 영토 외부로의 데이터 전송을 허용하고 있다(US-ASEAN Business Council).

자유주의 질서는 국내 및 해외 결제 서비스 및 서비스 공급자를 동일하게 대우하는 WTO 기본원칙을 강화할 것을 주장하고 있다. 이론적으로 서비스거래에 관한 일반협정(GATS)은 국가가 시장 접근에 대한 합의를 한 경우 데이터 현지화 요구 사항을 금지하고 있다. 그런데도 데이터 현지화는 확산하고 있다. 이러한 추세를 뒤집고 국경 간 지급 마찰을 줄이기 위해 향후 세계무역기구(World Trade Organization, WTO) 및 지역 무역 협정에서 데이터 현지화 요구 사항을 금지하는 특정 약속이 필요하다는 논의가 진행되고 있다. 예를 들면 미국-멕시코-캐나다(United States-Mexico-Canada Agreement, USMCA) 무역 협정은 데이터의 자유로운 흐름에 대한 명시적이고 상세한 보호를 제공하고 금융서비스 장에서 데이터 현지화에 대해 금지하고 있다(Article 17.18.).

2) 중국과의 협력

중국은 정치적 폐쇄성으로 인해 "만리방화벽(Great Firewall)"을 통해 인터넷 콘텐츠를 필터링하고 민감한 정치적 발언에 대한 모니터링을 강화하고 있다. 2018년에는 『사이버보안법(网络安全法)』의 제정을 통해 인터넷 정책의 중앙집권화와 사용자 실명 등록을 의무화했다(Lee, 2020). 중국은 아세안과의 협력에 있어 부패 정권에 대한 '내정불간섭'원칙을 내세우면서도 일대일로와 디지털 실크로드 및 디지털 표준과 기술 협력을 추진함으로써 영향력을 확대하고 중국식 시스템의 확산을 도모하고 있다. 이러한 권위주의 모델은 결국 정부가 관리하는 중앙집권식 데이터 통제로 이어질 우려가 있다.

중국은 아세안과의 협력에 있어 부패 정권에 대한 '내정불간섭'원칙을 내세우면서도 인프라를 중심으로 투자를 하고 있다. 중국은 일대일로를 통해 중국의 낙후된 서부 지역 개발을 촉진할 수 있어 아세안과의 협력에 특히 공을 들이고 있다. 1992년부터 아시아개발은

행(Asian Development Bank, ADB)을 중심으로 라오스, 태국, 캄보디아, 미얀마, 베트남, 중국 윈난성과 광시장족 자치구의 메콩강 유역권(Greater Mekong Subregion) 경제협력 프로그램이 대표적이다. GMS 프로그램은 메콩강 지역의 도시개발, 농업, 에너지, 환경, 관광, 무역, 정보통신기술 등 다양한 범위에 걸쳐 폭넓은 협력을 추진하고 있다.

2015년에는 란창-메콩(LMCM) 협력을 통해 연결성, 생산성, 국경을 초월한 경제협력, 수자원 및 농업, 빈곤 감소 등 5개 분야에서 협력을 추진하고 있다. 란창-메콩 5개년 행동계획(2018-2022)은 중국의 일대일로와 아세안 공동체와의 협력을 통해 지역통합을 구축하고 UN의 2030 지속가능개발목표를 위한 노력의 하나로 볼 수 있다. 이처럼 중국은 동남아시아 지역에서 지리적 이점과 막대한 자본을 이용해 5G와 인프라 시설물 건설을 통해 영향력을 확대하고 있다.

아세안 국가에서도 역시 구글, 페이스북, 알리바바 등의 글로벌 빅테크 그룹의 점유율이 높으며 이는 곧 네트워크 효과로 인해 큰 플랫폼의 계속된 선호로 이어진다. Google은 모든 아세안 회원국에서 검색 시장의 90% 이상을 점유하고 있다(Edit Chart Data). 구글의 크롬 브라우저는 모든 AMS(Application Management Services)에서 50% 이상의 시장 점유율을 보유하고 있으며 인도네시아, 말레이시아, 미얀마, 필리핀에서는 75% 이상을 차지한다(Browser Market Share Worldwide). 전자상거래 플랫폼은 태국, 말레이시아, 필리핀 등에서 중국의 알리바바(Alibaba Group)가 소유한 라자다(Lazada)가 가장 영향력이 높다(Southeast Asia Digital, Social & Mobile, 2019).

2. 데이터 프레임워크

아세안은 2018년 아세안 디지털 데이터 거버넌스 프레임워크(ASEAN Framework on Digital Data Governance)를 발표하였다. 이는 데이터 분류 프레임워크, 국경간 데이터 흐름을 위한 메커니즘, 디지털 혁신 포럼, 그리고 데이터 보호 및 개인정보보호 포럼 결성에 대한 이니셔티브의 수립을 요청하였다. 이러한 이니셔티브의 일환으로 2021년에 싱가포르 주도로 제1회 아세안 디지털 장관 회의가 개최되었으며, 아세안 데이터 관리 프레임워크(ASEAN Data Management Framework, DMF)와 아세안 국경 간 데이터 이전 모델계약조항(ASEAN Model Contractual Clauses for Cross Border Data Flows, MCC)을 채택하였다(Korea Internet & Security Agency, 2021).

데이터관리프레임워크(DMF)의 목표는 첫째, 데이터 유출 및 침해를 감소하고 기업간, 기업내, 아세안 회원국간 데이터 이전을 촉진한다. 둘째, 데이터 관리 지원을 위한 공통의 언어를 마련하고 데이터 사용 시 투명성, 신뢰 및 책임성을 부여함으로써 안전한 국경 간 데이터 이전을 지원한다. 셋째, 위기 기반 데이터 관리 방법론을 통해 데이터 생애 주기별 데이터 보호를 위한 비용을 발굴하고자 한다.

국경간 데이터 이전 모델 계약 조항(MCC)는 국경을 초월한 개인정보 전송과 이전에 대한 계약 조건을 제시함으로써 아세안 기업들이 지역내·외의 파트너들과 협력할 수 있는 토대를 마련하고, 개인정보 전송 매커니즘을 통해 안전한 국경간 데이터 이전을 실현하기 위함이다. 이 조항은 아세안 개인정보보호 프레임워크(ASEAN Framework on Personal Data Protection) (2016)의 원칙에 따라 데이터 주체의 데이터를 보호하기 위해 제정되었다(ASEAN, 2021).[3] 데이터 전송 당사자는 상업계약 시 주요 데이터 보호 의무에 대한 계약 조항에 동의해야 한다. 이러한 보호 조치는 아세안 디지털 생태계에서의 상호 신뢰를 증진해 초국경 데이터 이동을 촉진한다는 의의가 있다.

3) 아세안 개인정보보호 프레임워크(2016)의 기본원칙은 (1) 아세안 회원국(ASEAN member states)의 법률에 따른 데이터 수집, 사용, 공개 및 전송 보장; (2) 데이터 수집, 통지, 목적, 정확성, 보안보호장치, 접근 및 수정, 이전, 보존 및 책임과 관련된 기본 데이터 보호 조항; (3) 데이터 수입자가 개인 데이터 손실, 무단 사용, 복사, 수정, 공개, 파괴 혹은 접근을 인지할 경우 즉시 또는 당사자가 지정한 시간 내에 통지하는 것을 포함한다.

아세안 회원국들은 이러한 이니셔티브를 지지하는 입장이지만 캄보디아의 경우 국내에 데이터 보호에 특화된 법과 담당 규제 당국이 부재하다는 한계가 있다. 필리핀은 자국법과 상충되는 조항에 대해 자국법을 우선하는 방침을 보이고 있으며, DMF/MCC를 공식적으로 채택하기 전에는 비구속적·자발적 가이던스로 활용한다는 입장이다. 태국 역시 개인정보보호 관련 기관이 설치되지 않아 초국경 데이터 이동과 관련한 원칙이나 DMF/MCC를 실행할 추진체가 부재하다는 한계가 있다(Korea Internet & Security Agency, 2021).

아세안 이외에 지역 및 글로벌 차원에서 구축된 개인정보보호 프레임워크는 개인 데이터 보호에 관한 ASEAN 프레임워크(2016), APEC 프라이버시 프레임워크(2004, 2015), OECD 개인정보보호 프레임워크(1980, 2013), 개인정보 자동 처리에 관한 개인보호협약(1981), 마드리드 결의안(2009), 유럽연합 일반데이터보호규정(2016), EU-미국 프라이버시 쉴드(2016)가 있다.

OECD, ASEAN 및 APEC 프레임워크의 기본 목표는 모두 정보 흐름에 대한 불필요한 장벽을 피하고 해당 지역의 지속적인 무역 및 경제 성장을 보장하는 것이다. 이 프레임워크들은 국내 규칙의 대체가 아닌 회원국에 해당 조항의 자발적 이행을 촉구한다. OECD의 가이드라인은 개인정보보호 및 개인정보의 국경 간 이동에 관해 충분한 보호 장치가 있고 다른 국가도 유사한 지침을 준수하는 경우 국가가 데이터 이동을 제한하지 않도록 권장하고 있다. APEC 역시 정부는 개인정보 및 보안을 보호하면서 국경 간 데이터 이동에 불합리한 장애물이 없도록 권장한다(GSMA, 2018). ASEAN 프레임워크의 목표는 명시적으로 다루고 있지는 않지만 '지역과 글로벌 무역의 성장 및 정보이동에 이바지할 수 있도록 ASEAN에서 개인 데이터 보호를 강화하고 참여자 간의 협력을 촉진'하도록 하고 있다(GSMA, 2018). 즉, ASEAN 프레임워크의 참여자들은 개인정보를 국내 법률 및 규정을 통해 보호하고 참여 국가 간의 자유로운

〈표 1〉 데이터 프레임워크 비교
〈Table 1〉 Comparison of data privacy frameworks

	OECD	Convention 108	Madrid Resolution	APEC	ASEAN	EU GDPR
Objective	Economic	Fundamental Rights	Fundamental Rights	Economic	Economic	Fundamental Rights
Application scope by jurisdiction	Territorial - subject to national law	Territorial - subject to national law	Territorial - subject to national law	Territorial - subject to national law	Territorial - subject to national law	Extra-territorial - not subject to national law
Accountability provisions	Principle	None (in original agreement)	Principle + voluntary mechanism	Principle + voluntary mechanism	Principle	Principle + voluntary mechanisms + legal requirements
Default position on data flow	Promotes data flow	Restrictive (outside the group); promotes data flow (within the group)	N/A	Promotes data flow	Promotes data flow	Restrictive (outside the group); promotes data flow (within the group)

source: GSMA 2018

정보의 흐름을 촉진하기 위해 노력한다는 것이다.

ASEAN은 본래 경제적 목적으로 구성된 만큼 기능적인 목적이 강했다. 하지만 최근에는 아세안 중심성(ASEAN Centrality)을 통해 강대국 사이에서 균형 전략을 취하는 등 경제와 안보의 이슈가 복합적으로 얽히고 있다. 그런데도 관할권 적용 범위, 책임 조항, 데이터 이동의 측면에서 APEC의 기본 성격과 유사하다.

3. 무역 협정과 데이터 규제

지역 및 양자 무역 협정은 국가가 지급 서비스에 대한 시장장벽과 국경 간 마찰을 더욱 줄이도록 한다. 아세안은 포괄적·점진적 환태평양경제동반자협정(Comprehensive & Progressive agreement for Trans-Pacific Partnership, CPTPP)와 역내포괄적경제동반자협정(Regional Comprehensive Economic Partnership Agreement, RCEP)에 모두 참여하고 있다. CPTPP는 지급 서비스와 관련해 이론상 데이터 저장고와 처리 시설을 각 국가에 위치하도록 하는 규제적 요구를 제한하는 특별 조항을 annex에 첨부하고 있다(WEF, 2020). 하지만 국가들이 현지 요건을 통해 해외 지급 제공자를 차별하고 현지 디지털 지급 서비스 제공자에 대한 우호적 조치를 제공할 수 있다는 점에서 한계가 있다(WEF, 2020).

2012년 ASEAN을 중심으로 시작된 RCEP는 15개 아시아·태평양 국가가 참여하고 있다. 2020년 11월 15일에 서명된 RCEP의 목표(Joint Leaders' Statement on the Regional Comprehensive Economic Partnership)는 'ASEAN+1' 자유무역협정(FTA)의 기존 네트워크를 통일된 협정으로 조화시켜 지역에 대한 단일하고 응집력 있는 무역 규칙 세트를 만드는 것이다. 이러한 통일된 협정은 지역 통합을 촉진하는 요소가 될 수 있다. RCEP에는 "서비스, 투자, 전자 상거래, 통신 및 지적 재산권과 같은 21세기 무역 문제에 관한 규제 조항"이 있다(Wilson, 2020). 이는 해외 서비스 공급자에 대한 시장 접근을 확대하고, 국내와 해외 공급자를 동등하게 대우하며(내국민 대우), 해외 공급자를 최소한 비 RCEP 국가의 공급자와 같이 대우한다(최혜국 또는 MFN)는 내용을 포함하고 있다(RCEP Outcomes at a Glance).

RCEP 국가들은 또한 이동 전화 번호의 이동성을 허용하기로 약속했으며(특정 AMS 면제 포함), 국제 전화 접속에 대한 합리적인 국제 모바일 로밍 요금과 합리적이고 비차별적인 대우를 촉진하기 위해 협력하기로 합의했다. 또, 제12장에서는 전자상거래와 관련한 활동 일부로 국경을 넘어 데이터를 전송하는 ASEAN 기업을 지원하고 데이터 현지화(저장) 요구 사항을 포함하여 정부가 제한을 부과할 수 있는 범위를 제한하고 있다(ASEAN Digital Masterplan 2025). ASEAN은 RCEP를 통해 해외 기업을 유치하되 역내 중소기업(SME)을 글로벌 및 지역 공급망에 더 많이 포함하려 한다(Malvenda, 2019). 이는 ASEAN이 집단을 이룸으로써 편익을 증대시키는 것을 보여준다.

4. SWIFT와 CIPS 참여

아세안은 유럽에 있는 국제은행간 통신협정인 SWIFT(Society for Worldwide Interbank Financial Telecommunication)와 중국이 구축한 CIPS(Crossborder Interbank Payment System)에 모두 참여하고 있다. 2006년 CIA와 미국의 정부 기관이 SWIFT의 거래 데이터에 접근하는 테러리스트 금융 추적 프로그램(The Terrorist Finance Tracking Program)을 운영 중임이 밝혀졌는데(Brand, 2010), 이러한 미국 정부와 SWIFT의 거래는 2006년 벨기에 및 유럽의 개인정보보호법 위반이라는 판결을 받았다(LA times). 이후 유럽연합은 유럽 내 SWIFT 거래정보를 일부 미국으로 이전하는 것을 협상하였으나 결국 유럽 의회의 반대로 무산되었다(European Parliament Resolution of 17 September 2009 on the SWIFT Agreement).

미국이 SWIFT를 제재의 수단으로 삼은 사례는 이뿐이 아니다. 미국 상원 은행 위원회는 2012년 2월

SWIFT가 이란 은행과의 관계를 종료하라는 압력을 가하기도 하였다(Gladstone, 2012). 영국은 2014년 8월에는 러시아가 우크라이나에 대한 군사 개입을 감행하자 러시아의 SWIFT 사용을 차단하기 위해 유럽연합에 압력을 가하기도 하였다(Hutton, 2014).

중국의 국경 간 은행 간 지불시스템(CIPS)의 주요 목적은 국내 및 국경 간 위안화 거래를 청산 및 결제함으로써 위안화의 국제 사용을 장려하는 것이지만, SWIFT 지불시스템에 대한 대안이 되기도 한다. CIPS는 SWIFT와 비교해 그 규모가 현저히 작지만, 2021년 약 80조 위안(12조 6,800억 달러)을 처리하는 등 그 성장 속도가 가파르다(Reuters, 2022). CIPS는 2015년부터 운영이 시작되어 일본의 30개 은행, 러시아의 23개 은행, 중국의 일대일로 프로젝트를 통해 위안화 자금을 받는 아프리카 국가의 31개 은행이 참여한다. 2022년 2월 기준 1,304개의 직간접 사용자가 있으며 2020년 CIPS의 사용률은 아세안 국가가 8%를 차지했다(Mckinsey & Company, 2021).

아시아의 주요 디지털 은행은 유럽이나 미국에서 볼 수 있는 수직적 접근 방식의 모델과 달리 컨소시엄 비즈니스 모델로 운영된다. 아시아의 디지털 뱅킹 라이센스는 특히 비은행 기업이 은행 시장에 접근할 수 있도록 한다(The Asian Banker). 말레이시아도 최대 5개의 디지털 라이센스를 제공하는 프레임워크 초안을 발표했고, 필리핀 역시 당국의 최초 디지털 은행인 Tonik Digital Bank에 라이센스를 발급했다. 2019년 싱가포르의 라이센스를 발급받기 위한 지원자의 대다수는 컨소시엄이었으며, 2020년 최종적으로 라이센스를 부여받은 4개 중 2개가 컨소시엄이었다. 이러한 컨소시엄 모델의 보급은 부분적으로 규제로 주도된다. 다른 지역의 디지털 은행은 스타트업인 경우가 많지만, 아시아 디지털 뱅킹은 주로 기존 회사와 컨소시엄에 의해 주도되고 있다. 이는 규모의 측면에서 상당한 이점을 제공한다. 컨소시엄은 참가자 간의 조정이 필요하다는 점에서 복잡성이 증가하지만, 빠르게 확장할 수 있는 장점을 가지고 있다(Mckinsey & Company, 2021).

V. 결론 및 함의

본 논문은 미·중 패권경쟁 속 자유주의와 권위주의의 담론을 데이터 규제 및 사이버 안보와 연계하고, 동아시아 거버넌스에 대한 함의를 위해 아세안 개발협력 사례를 살펴보았다. 데이터가 한 곳에 집중되는 것은 인공지능을 활용한 개발 자원과 권력이 집중되는 것을 의미한다. 자유주의의 개방성의 담론은 자칫하면 사적 행위자의 데이터 독점으로, 권위주의의 내정불간섭과 비공식적 협력은 자금의 출처와 사용의 불투명성을 초래하여 국가권력의 데이터 독점과 부패로 이어질 수 있다는 맹점이 존재한다. 이에 미국과 중국은 그러한 문제를 보완하기 위해 『반독점법』이나 『데이터안전법』을 제정하였다.

행위자들의 활동 영역이 사이버 공간으로 확장되면서 데이터 규제는 점점 더 경제의 영역을 넘어 안보의 영역으로까지 이어지고 있다. 테러리스트의 자금이 가상화폐를 통한 자금 세탁과 연계되거나 범죄자의 데이터 및 정보와 관련해 국가와 기업의 초국경적 협력이 필요하다. 미국은 CLOUD Act 제정을 통해 국가 간 행정 협정을 할 수 있는 규명을 명시하였고, 중국은 『데이터안전법』의 제정을 통해 '영토 내' 관할에 대한 강력한 주권을 주장하며 데이터 이동과 규제에 대한 법적 근거를 마련하였다. 하지만 중국의 데이터 규제에 대한 구문들은 상황에 따라 자의적으로 해석될 수 있다는 한계가 있다.

미·중 간의 경쟁이 심화함에 따라 중간국들은 선택을 강요받는 현실 속에서 아세안은 집단을 이루어 미국과 중국 사이에서 회피(Hedging) 전략을 취하고 있다. 아세안은 CPTPP와 RCEP 모두에 참여하고 있으며, 미국과 중국 모두와 데이터 거버넌스 및 인프라와 관련된 협력을 하고 있다. 이러한 아세안 중심성(ASEAN Centrality)을 내세운 회피전략은 아세안 집단적 공조를 통해 강대국에 맞서고 내부적 결속을 다지도록 한다. 아세안은 아세안 디지털 데이터 거버넌스 프레임워크를 통해 데이터 관리 프레임워크(DMF)와 국경간 데이터 이전 모델계약조항(MCC)을 채택하고 역내 효과

적인 데이터 거버넌스를 위한 협력을 하고 있다. 아세안 회원국들은 이러한 이니셔티브를 지지하는 입장이지만 국내에 데이터 보호에 특화된 법과 담당 규제 당국이 부재하거나 자국법과 상충되는 조항에 대해 자국법을 우선하는 방침을 보이고 있다.

초국경 데이터 규제는 국가 영토를 넘나드는 플랫폼 서비스의 경쟁력 측면에서뿐만 아니라 개인정보보호와 국가안보, 금융, 지역통합 등 다양한 이슈가 얽혀있는 사안이 되었다. 이에 따라 한국 역시 관련한 학제 간뿐만 아니라 민과 관이 협력해 초국경 데이터 규제를 연구함으로써 자국민의 권리를 보호하면서도 경쟁력을 향상하는 방안을 고민할 필요가 있다.

■ References

Acharya, A. (2014). "ASEAN Dilemma: Courting Washington without Hurting Beijing." *Asia Pacific Bulletin,* 133, East-West Center.

Brand, C. (2005). "Belgian PM: Data Transfer Broke Rules," *The Washington Post,* September 28.

Chander, A. & Le, U. (2015). "Data Nationalism." *Emory Law Journal, 64*(3), 701.

Chang, W., Gil, J., Kim, J., Min, H. & Choi, J. (2021). "Political Participation and Decision-Making in an Era of Digital Transformation and Innovations in Legislature and Party Politics." *Broadcast and Communications Policy Studies,* 2021-0-00008, 38-58.

{장우영·길정아·김정연·민희·최재동 (2021). 정치적 의사결정 및 정치참여 방식의 디지털 전환과 의회 정당정치의 혁신. 〈방송통신정책연구 2021-0-00008〉, 38-58.}

Cho, H. (2015). *Information Sovereignty in the Network Era and the Role of the State (Presentation). National Assembly Research Service,* paper presented at National Research Foundation Joint Academic Forum, Big Data, Personal Information Protection and Establishment of Information Sovereignty.

{조화순 (2015). 네트워크시대 정보주권과 국가의 역할 (발표문). 국회입법조사처, 한국연구재단 공동학술포럼, 빅데이터와 개인정보보호와 정보주권 확립방안, 2015. 11. 5, 18.}

Choi, J. (2022). "The Politics of Internet Content Regulation in the U.S.: A Case Study on Communications Decency Act Section 230 Reform with New Institutionalist Approach." *Information Policy, 29*(3), 48-60.

{최재동 (2022). 미국 인터넷 내용규제의 정치: 신제도주의로 본 연방통신품위법 230조 개정 논의. 〈정보화정책〉, 29권 3호, 48-60.}

Choi, K & Hwang, Y. (2022). "China's 'ODA-like' and Political Corruption: Focusing on the Case of ECRL in Malaysia." *The Southeast Asian review, 32*(4), 119-158.

{최기룡·황인원 (2022). 중국 'ODA-like'와 정치적 부패-말레이시아 동부해안철도(ECRL) 사례를 중심으로. 〈동남아시아연구〉, 32권 4호, 119-158.}

Gladstone, R. (2012). "Iran Praises Nuclear Talks with Team from U.N.," *The New York Times,* January 13.

GSMA. (2018). *Regional Privacy Frameworks and Cross-Border Data Flows. How ASEAN and APEC can Protect Data and Drive Innovation.* London: GSMA.

GSMA. (2019). *Operationalising the ASEAN Framework on Digital Data Governance- A Regulatory Pilot Space for Cross-Border Data Flows-.* London: GSMA.

Cho, C. (2015). "Instead of extending the Patriot Act, the Freedom Act…," *Hankook Ilbo,* June 3.

{조철환 (2015). 결국 애국법 연장 대신 자유법… 美정보기관 무제한 도·감청 금지. 〈한국일보〉, 6월 3일.}

Hong, M. (2021). "China's Southern Railway Expansion is not All Good News for Laos." *Hankyoreh.* December 21. https://english.hani.co.kr/arti/english_edition/e_international/1023847.html

Hutton, R. (2014). "U.K. Wants EU to Block Russia From SWIFT Banking Network," *Bloomberg News.* August 29.

Hyeon, D. "The Current Situation and Prospect on the US Cyber Risk Management and Relevant

Legislation." *Dankook Law Review, 33*(1), 3-39.
{현대호 (2009). 미국의 사이버위기 관련 법제의 현황과 전망. 〈법학논총〉, 33권 1호, 3-39.}
Ikenberry, G. John.2001. After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order After Major Wars. Princeton: Princeton University Press.
Jacquez, T. (2016). "Cryptocurrency the new money laundering problem for banking, law enforcement, and the legal system." Master's Thesis, Science in Cybersecurity, Utica College.
Jeong, A. (2019). "Review of requirements for transborder flow of personal information." *Public Law Journal, 20*(2), 209-244.
{정애령 (2019). 개인정보 국외이전 허용요건의 검토.〈공법학연구〉, 20권 2호, 209-244.}
Katzenstein, P. (2005). *A World of Regions: Asia and Europe in the American Imperium.* Ithaca and London: Cornell University Press.
Keohane, R. O., & Nye, J. S. (1975). "International Integration and Interdependence." In F. Greenstein & N. Polsby (Eds.), *Handbook of political science,* 363 - 414.
Keohane, R. (2005). *After Hegemony: Cooperation and Discord in the World Political Economy.* Princeton Classic Editions.
Kim, K. (2021). "U.S. Economic Sanctions on Virtual Currency - Focusing on Recent Cases." *Financial Law 14*(2), 265-300.
{김규진(2021). 미국의 가상화폐(virtual currency) 관련 경제제재 - 최신 사례를 중심으로 -. 은행법연구 14권 2호. 265-300.}
Krapohl, S. (2017). *Regional Integration in the global South: External Influence on Economic Cooperation in ASEAN, MECOSUR and SADC.* Palgrave Macmillan.
Kim, H. (2017). "A Study on the Legal Issues of Data Attributes and Localization Norms." *Public land law review,* 78, 1-48.
{김현경 (2017). 데이터 속성과 국지화 규범의 법적 쟁점에 대한 고찰. 〈토지공법연구〉, 78집, p. 1-48.}
Koh, H. (2012). Remarks at USCYREBERCOM Inter-Agency Legal Conference.
Korea Internet & Security Agency. (2021). *2021 Privacy Report.* Naju: Korea Internet & Security Agency.
{한국인터넷진흥원. (2021). 〈개인정보보호 해외동향분석〉, 나주: 한국인터넷진흥원.}
Krüger, P. (2016). "Datensouveränität und Digitalisierung." *ZRP*, 190.
Ky, S., Lee, C. & Stauvermann, P. (2012). "A Comparative Study on Characteristics of ODA of China-Japan-Korea to Cambodia." *Journal of East Asian Economic Integration, 16*(4), 333-361.
LA Times. (2006). "Belgian Panel Finds SWIFT Deal With U.S. Violates EU Privacy Law," September 29. https://www.latimes.com/archives/la-xpm-2006-sep-29-fg-swift29-story.html
Lee, K. (2020). "Global Digital Standards Cooperation and Data Governance: Human Rights and Development in the Digital Age." *International Area Studies Review(IASR), 24*(3), 177-199.
{이가연 (2020). 글로벌 디지털 표준협력과 데이터 거버넌스: 자유주의적 인권과 개발협력 담론을 중심으로. 〈국제지역연구〉, 24권 3호, 177-199.}
Lee, S. (2021). "The Main Contents and Implication of China's Data Security Law: Focused on the Key System for Data Security." *China Knowledge Network,* 17, 451-501.
{이상우 (2021). 중국 데이터 안전법의 주요내용과 시사점: 데이터 안전보호를 위한 중점 제도를 중심으로. 〈중국지식네트워크〉, 17권, 451-501.}
Long, B. (2020). "On the eight major challenges of digital currency" *Journal of Translation from Foreign Literature of Economics,* 4, 60-100.
{龙白滔 (2020). 论数字货币八大冲, 经济资料译丛4期. 60-100.}
Lor, J. J. (2019). "A Study of Intra-ASEAN Trade: An analysis of its indicators, determinants and implications." Master's Thesis, Seoul National University.
Mckinsey & Company. (2021). *Joining the next generation of digital banks in Asia.*
Maeil Economy (2021). "Google, Apple, Amazon, Facebook split... U.S. House of Representatives Proposes Strong Antitrust Law." June 13.
{매일경제 (2021). 구글·애플·아마존·페북 쪼개지나…美하원, 초강력 반독점법 발의. https://www.mk.co.kr/

news/world/view/2021/06/570688/} 6월 13일.
Malvenda, M. (2019). *The RCEP: Impacting ASEAN's Supply Chains and Business Environment.* December 27.
National Information Society Agency (2018). "The Rise of Data Sovereignty and the Transformation of Data Utilization Paradigm." *IT&Future Strategy,* 5, 1.
{한국정보화진흥원 (2018). 데이터 주권 부상과 데이터 활용 패러다임의 전환. 〈IT&Future Strategy〉, 5호, 1.}
OMB(Office of Management and Budget). "Federal Data Strategy." https://strategy.data.gov/background/#how-were-the-principles-created
Park, J. (2020). "The Normative Status of the Principle of Sovereignty and Cybersecurity." *The Studies of International Affairs, 20*(1), 79-114.
{박주희 (2020). 사이버 공간에 적용되는 주권의 규범적 성격과 사이버안보.〈국가안보와 전략〉, 20권 1호, 79-114.}
Reuters. (2022). "Factbox: What is China's onshore yuan clearing and settlement system CIPS?" Feb 28. https://www.reuters.com/markets/europe/what-is-chinas-onshore-yuan-clearing-settlement-system-cips-2022-02-28/#:~:text=WHAT%20IS%20CIPS%3F,banks%20in%20offshore%20yuan%20hubs.
Song, Y. (2018). "Passage of the CLOUD Act and Its Implications for Law Enforcement Access to Extraterritorial Data." *Korean criminological review, 29*(2), 149-172.
{송영진 (2018). 미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점. 〈형사정책연구〉, 29권 2호, 149-172.}
Schmitt, M. (2013). (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare.* Cambridge University Press.
The ASEAN Secretariat. (2016). *MASTER PLAN ON ASEAN CONNECTIVITY 2025.*
The Asian Banker. (2020). *Are central banks issuing digital banking licences to counter the threat of fintechs and big techs? Rise of digital banking licences special report,* 3. Singapore: The Asian Banker.
WEF. (2020). *Connecting Digital Economies: Policy Recommendations for Cross-Border Payments.* Geneva: WEF.
Watts, S. and Richard, T. (2018). "Baseline Territorial Sovereignty and Cyberspace." *Lewis & Clark Law Review, 22*(803), 861.
Weber, M. (1919). *Politics as a Vocation.* Seoul: Moonye Publishing.
{막스 베버. (2017). 〈직업으로서의 정치〉, 문예출판사.}
World Economic Forum. (2018). "Addressing E-Payment Challenges in Global E-Commerce." *White Paper.* http://www3.weforum.org/docs/WEF_Addressing_E-Payment_Challenges_in_Global_E-Commerce_clean.pdf
Wilson, J. (2020). "RCEP will redraw the economic and strategic map of the Indo-Pacific," 21 https://www.aspistrategist.org.au/rcep-will-redraw-the-economic-and-strategic-map-of-the-indo-pacific/
Yang, Y. & Lee, H. (2021). Introduction of Platform Antitrust Act in the US and its Implications. *KDI Focus.*
{양용현·이화령 (2021). 미국의 플랫폼 반독점법안 도입과 시사점. 〈KDI Focus〉.}
Yi, C. (2021). "A Study on Legal Issues of Data Portability and the Direction of Legislative Policy." *Information Policy, 28*(4), 54-75.
{이창범 (2021). 개인정보 이동권의 법적 이슈와 입법 정책 방향. 〈정보화정책〉, 28권 4호, 54-75.}
Yoon, S. & Kwon, H. (2021). "Analysis of the Global Data Law & Policy and its Implications: Focusing on the cases of the United States, the United Kingdom, and the European Union." *Informatization Policy, 28*(2), 98-113.
{윤상필·권헌영 (2021). 국내외 데이터법·정책 분석 및 시사점: 미국, 영국, EU의 사례를 중심으로. 〈정보화정책〉, 28권 2호, 98-113.}
Unpublished: "Articles 17.17 and 17.18 of the USMCA trade agreement." https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/17-Financial-Services.pdf
Unpublished: "ASEAN Digital Masterplan 2025." (2021).https://asean.org/book/asean-digital-masterplan-2025/
Unpublished: Browser Market Share Worldwide July 2021 - July 2022, https://gs.statcounter.com/browser-market-share/

Unpublished: Cheng, C. (2019). "The Logic Behind China's Foreign Aid Agency." Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/05/21/logic-behind-china-s-foreign-aid-agency-pub-79154

Unpublished: Edit Chart Data. (2021-22). Search Engine Market Share Worldwide July 2021 - July 2022. https://gs.statcounter.com/search-engine-market-share.

Unpublished: Government of Canada. Information Technology Strategic Plan 2016-2020. https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/information-technology-strategy.html

Unpublished: H.R.4943 — 115th Congress (2017-2018). https://www.congress.gov/bill/115th-congress/house-bill/4943

Unpublished: Southeast Asia digital, social and mobile 2019, https://aseanup.com/.

Unpublished: Stored Communications Act 2703(2nd Circuit). (2016). In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., Case No. 14-2985

Unpublished: WTO, GATS, in subparagraph 5(a)(xv) of the Annex on Financial Services. https://www.wto.org/english/tratop_e/serv_e/10-anfin_e.htm