Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전연구센터 연구위원 워킹페이퍼 No.15.(발간일: 2025.2.3.)

데이터 국제규범과 데이터 주권

이효영 국립외교원 부교수

1. 서론

디지털 상품 및 서비스 거래의 급성장에도 불구하고 현재 디지털 통상을 규율하는 글로벌 차원의 다자적 규범은 부재한 상황이며, 이에 따라 새로운 통상 현안으로 부상하고 있는 국가 간 디지털 통상 관련 갈등이 원활하게 해결되지 못하고 있는 상황이다. 특히 데이터의 국경간 거래(cross-border data transfer)와 관련된 통상 현안들은 단순히 데이터의 자유로운 이동 및 원활화를 막는 디지털 장벽의 문제 뿐 아니라 디지털 경제에서의 경쟁 및 반독점 이슈와도 밀접한 연관이 있기 때문에 각국의 글로벌 데이터 산업 및 시장에서의 경쟁적 위치에 따라 국가들은 상이한 디지털 통상 정책을 추구하고 있다. 또한 대량의 빅데이터 또는 국가의 민감정보를 활용한 여론 · 정보 조작, 영향력 공작, 첩보 활동 등이 가능해지면서 데이터 안보(data security) 및 데이터 주권(data sovereignty)의 문제와도 연계되고 있다.

지난 몇 년간 WTO 차원에서 복수국간 다자규범 수립을 위한 협상이 진행되어 왔으나, 미국, EU 등 주요국이 추구하는 디지털 통상 정책의 차이로 인하여 타결이 쉽지 않은 상황이었다. 데이터의 자유로운 국경간 이동을 허용하는 디지털 통상 규범의 수립을 적극적으로 지지하는 미국과 달리 EU는 데이터를 포함한 개인정보의 강력한 보호를 지지하며 데이터의 국외이전에 대하여 유보적인 입장을 채택해 왔기 때문이다. 바이든 행정부 출범 후 미국과 EU는 디지털서비스세(digital services tax) 문제를 비롯한 양국간 디지털 통상 갈등을 해결하며 글로벌 차원의 디지털 통상 규범 수립을 위한 협력을 강화해나가는 모습을 보이기 시작하였다. 특히 미국과 EU는 중국의 첨단 기술 분야에서의 전략적인 부상을 견제하기 위

하여 서방국 중심으로 첨단기술 분야의 규범 리더십을 확보하기 위한 '통상기술위원회(Trade and Technology Council, TTC)'를 설립하기도 하였다.

그러나 최근 미국은 기존의 디지털 통상 정책 방향을 크게 선회하며 국경간 데이터 이전 허용에 대한 강력한 지지 입장을 공식적으로 철회한 상태이다. 그동안 WTO 내에서 복수국간 무역협정 형태로 추진해오던 전자상거래 JSI(Joint Statement Initiative) 협상에서 미국은 데이터의 국경간 이전 허용, 데이터 현지화 요건 부과 금지, 소스코드 공개요구 금지 등의 의무조항을 담은 디지털 통상 규범의 수립을 강력하게 지지해왔으나, 2023년 8월 발표된 WTO 전자상거래 JSI 통합문서에서는 세 가지 의무조항이 삭제되었다. 이후 2024년 7월 WTO 전자상거래 JSI 협정이 타결되었으나 미국은 이를 승인하지 않았다.

그동안 디지털 통상 관련 다자적 규범의 공백은 초기에는 미국 중심의 양자 및 소다자 형태의 디지털 통상 협정을 통해 메워져 왔다. 2017년에 체결된 '환태평양 동반자 협정(CPTPP)' 이후 미국-멕시코-캐나다 협정(USMCA)', 미-일 디지털무역협정(USJDTA)'이 체결되면서 한동안 미국 중심의 디지털 통상 협정이 주된 규범의 틀(template)을 제공하며 국경 간 데이터 거래의 자유화를 주도하였다. 무엇보다 초기 미국 주도의 디지털 통상 규범은 미국 디지털 플랫폼 기업의 해외 진출을 더욱 용이하게 만들기 위하여 초점이 맞추어져 있으며, 데이터 안보의 문제는 특별히 다루고 있지 않다. 이후 아시아태평양 지역의 국가들을 중심으로 싱가폴, 뉴질랜드, 칠레가 체결한 '디지털경제동반자협정(DEPA)', 싱가포르와 호주가 참여하고 있는 '디지털경제협정(DEA)', 아세안(ASEAN) 10국과 한 · 중 · 일 등이 참여한 '지역포괄적경제동반자(RCEP)' 협정이 체결되면서 기존 미국 주도의 규범 형식과는 상이한 새로운 형태의 디지털 통상 규범화 노력이 이루어졌다. 그러나 후자의 디지털 통상 규범에서도 공공정책 목적이나 국가안보 목적의 예외 조항 외에 데이터 안보 관련 규정을 특별하게 도입하고 있지 않다.

반면, EU는 데이터 주권을 보장하기 위한 디지털 통상 규제 노력을 주도해왔다고 할 수 있다. 프랑스, 이탈리아, 스페인 등 일부 EU 회원국들은 '디지털 서비스세(digital services tax)'의 도입을 추진하였으며, EU 차원에서는 '디지털 시장법(Digital Market Act)'와 '디지털 서비스법(Digital Services Act)'의 도입 등을 통한 디지털 플랫폼 서비스 기업에 대한 규제를 통해 EU 역내에서의 데이터 주권 강화를 위한 입법화 노력을 적극적으로 추진해왔다. 이는 겉으로는 EU 역내 디지털 경제에서의 '공정한 경쟁 환경(level playing field)'의 구축을 목표로 하고 있지만 사실상 미국 디지털 플랫폼 기업의 독주를 막고자 하는 규제 정책으로서 평가받고 있다. 이 외에도 EU의 '데이터법(Data Act)' 및 '데이터거버넌스법(Data Governance Act)'의 제정을 통해 EU 역내에서의 데이터 안보를 강화하기 위한 입법화 노력도 전개하고 있다.

최근 미국도 데이터 안보 및 데이터 주권 강화를 위한 입법화 노력을 추진한 바 있다. 미국은 자국의 국내 디지털 플랫폼 기업(소위 '빅테크(Big Tech)')을 규제하고자 한 바 있는데, 이의 여파로 미국이 주도한 '인도태평영경제협의체(IPEF)'의 디지털 통상 관련 협상과 및 WTO 복수국간 전자상거래 협상에서 미국은 데이터의 국경간 이전 자유화 정책과 관련하여 과거와 달리 유보적인 입장을 보이며 협상의 타결을 지연시켰다. 또한 최근 미 대선을 앞두고 바이든 대통령은 미국 정부기관의 데이터가 중국 등 우려대상국으로 유출되지 않도록 강력한 조치를 취하기 위한 행정명령도 발표한 바 있다. 이와 같이 데이터 안보 강화에 대한 정책적 수요가 확대되면서 미국과 EU 등 선진국 주도로 데이터 안보 관련 입법화 노력이 진행되고 있는데, 이러한 데이터 안보 규제 도입에 대한 정책적 시사점을 도출하고 우리의 대응방안을 고민해 볼 필요가 있다.

2. 데이터 관련 국제통상규범의 수립 현황

(1) 주요국의 데이터 관련 상이한 정책적 입장

미국 기업들이 세계 디지털 시장을 주도하고 있는 상황에서 미국은 국경을 넘나드는 디지털 상거래의 활성화를 위한 글로벌 통상환경의 구축에 가장 앞장서고 있다. 이에 따라 국경 간 데이터 이전을 제한하는 각국의 국내규제는 미국 디지털 기업의 국제시장 진입을 방해하는 디지털 통상 장벽으로 인식되고 있다. 미국 정부가 매년 발표하는 미 무역대표부(USTR)의 무역장벽보고서(National Trade Estimate Report on Foreign Trade Barriers, NTE 보고서)에서는 '디지털 통상장벽'이라는 별도의 항목을 마련하여 각국의 무역장벽 현황을 모니터링하고 있다. 또한 개인정보보호와 관련하여 미국은 디지털 통상에 대한 소비자의 신뢰를 확보하기 위하여 필요한 최소한의 법제도를 마련하도록 규정하고 있다. 디지털 통상 협정상의 규범에서도 참여국들의 개인정보보호 관련 법제도의 수준에 대해서는 특별하게 명시하고 있지 않다.

반면, EU는 개인정보 보호의 권리에 대하여 기본적인 인권에 해당한다는 입장이다. '개인정보보호지침(Data Protection Directive)'을 개정하여 2018년 이후 시행하고 있는 '일반개인정보보호규정(General Data Protection Regulation, GDPR)'을 통해 역내 회원국의 개인정보에 대한 보호수준 강화, 역외국에 대해서는 EU와 동등한 수준의 개인정보보호 법제도를 갖추지 않은 경우 시장접근을 제한하고 있다. 특히 EU 회원국 국민의 개인정보를 보관, 저장, 기록 및 처리함에 있어 역내외 기업들에게 동일하게 적용되는 규칙을 제정하여, 개인

정보보호 제도의 적합성(adequacy)이 인정된 역외국에게만 EU 회원국의 개인정보 국외 이전을 허용하고 있다. 이와 관련하여 미국과 체결한 양자간 개인정보 공유 협약인 '프라이버시 쉴드(Privacy Shield)' 협약은 미-EU 간 관계 악화에 따라 유럽재판소(ECJ)가 이에 대하여 무효화 판정을 내려 미국 디지털 기업의 EU 시장 진출이 매우 어려워지기도 하였다.

(2) 디지털 통상 협정에서의 데이터 관련 규범화 현황

데이터 관련 국제규범은 현재 다자적 차원에서 합의된 내용은 없으며, 대신 디지털 통상장벽의 완화를 통해 상업적 이익을 추구하거나 규범화를 주도하고자 하는 국가들을 중심으로 양자 FTA 및 지역무역협정(RTA)을 통해 다양한 형태와 수준으로 규범이 도입되고 있다. 디지털 통상 관련 규범화 노력의 시초인 2018년 3월 서명된 CPTPP 전자상거래(electronic commerce) 챕터의 도입을 계기로 미국 주도의 수준 높은 디지털 통상 규범의 틀(template)이 마련되었으며, 국경간 데이터 이전의 자유화, 데이터 저장설비의 현지화 요구 금지, 현지 진출 조건으로 소프트웨어의 소스코드 공개 요구 금지 등 데이터 관련 핵심 조항을 의무 규정의 형태로 처음 도입하였다. 2018년 11월 서명된 USMCA의 디지털무역(digital trade) 챕터는 CPTPP의 데이터 관련 의무 조항의 도입과 함께 예외 규정의 범위를 축소하여 국경간 데이터 거래의 자유화 수준이 더욱 높아진 것으로 평가된다.

이후 체결된 디지털 통상 협정인 미-일 디지털통상협정(DTA)은 FTA의 챕터 형태가 아닌 독립적인 협정으로 최초 도입된 사례이며, CPTPP와 USMCA에 도입되어 있는 주요 데이터 관련 의무 규정 외에도 소스코드 및 암호화 기술 관련 규정을 업그레이드 및 신규 도입하였다. 2020년 6월 서명된 DEPA, 2020년 8월 서명된 DEA도 별도의 독립적인 디지털 통상 협정으로, 싱가포르가 주도하고 있으며 새로운 형태의 협정 구조를 갖추고 있으나 데이터 관련 규범의 내용과 자유화 수준은 CPTPP와 유사한 수준인 것으로 평가되고 있다. 2020년 11월 서명된 소다자 지역무역협정인 RCEP은 전자상거래 챕터를 도입하고 있으며, 중국 외에도 개도국이 대부분인 아세안 회원국들이 주도하고 있는 지역무역협정의 성격상 상대적으로 폭넓은 예외 규정을 도입하고 있다. 특히 RCEP 전자상거래 챕터의 모든 규정은 분쟁해결절차의 적용을 받지 않는다고 명시하고 있어 모든 의무 규정의 구속력이 부재한 것이 특징이다.

디지털 통상 협정에서 도입하고 있는 데이터 관련 규범은 국경간 디지털 무역과 투자의 자유화를 확대하기 위한 규정으로 분류되고 있으며, 이에 해당하는 규정들은 (1) 국경간 데이터 이전의 자유화(cross-border transfer of data), (2) 데이터 설비의 현지화 요구 금지(location/localization of computing facilities), (3) 소프트웨어의 소스코드(source

code) 공개 요구 금지(강제적인 기술이전 방지 조항), (4) 인터넷 접근 및 이용의 자유화 (access to and use of the internet for electronic commerce), (5) 인터넷 서비스제공업체 (internet service provider, ISP)의 책임 면제 조항 등이다. 이와 같이 디지털 통상 협정에 도입되어 있는 데이터 관련 규정들은 디지털 상거래의 핵심 규정으로서 디지털통상장벽의 완화 목적을 갖고 있으므로 디지털 통상의 자유화 확대를 위한 중요한 규정인 것으로 간주되고 있다.

[표 1] 기체결 디지털통상협정에서의 데이터 관련 규범의 의무화 수준 비교

데이터 관련 디지털통상협정 규정	CPTPP	USMCA	USJDTA	DEPA	DEA
국경간 데이터 이전	의무	의무	의무	의무	의무
데이터 현지화 요구 금지	의무	의무	의무	의무	의무
소스코드 공개요구 금지	의무	의무	의무	–	의무
인터넷 접근 및 이용 자유화	협력	협력	–	협력	협력
ISP 책임 면제	–	의무	의무	–	–
정부의 정보 공개	–	협력	협력	협력	협력
암호화 기술 사용 ICT 제품	–	–	의무	의무	의무

위의 디지털 통상 협정에 도입되어 있는 데이터 관련 규정들은 데이터 주권 이슈와 직간접적인 연관이 있다고 할 수 있다. 특히 데이터 현지화 요구 금지 관련 조항(컴퓨팅 시설의 위치 관련 조항)은 대표적인 데이터 안보를 위한 조치인 데이터 현지화(data localization)에 대하여 명시하고 있다. 현재까지 체결된 디지털 통상 협정은 기본적으로 글로벌 IT 기업 등이 현지 투자에 대한 조건으로서 데이터 현지화 요구를 금지하고 있는데, 기본적인 금지 원칙과 함께 예외 조항을 함께 도입하고 있는 형태로 규범화되어 있다.

디지털 통상 협정에 도입되어 있는 국경 간 데이터 이전의 자유화 및 데이터 현지화 요구 금지 관련 의무 규정은 '정당한 공공정책 목적(legitimate public policy objective, LPPO)'을 위한 조치에 대하여 예외 적용을 인정하고 있다. 단, 정당한 공공정책 목적에 대한 예외 적용의 조건으로 해당 조치가 자의적이거나 부당한 차별의 수단으로 사용되지 않고 위장된 무역제한적 조치가 아니어야 함을 명시하고 있다. 또한 당사국이 데이터의 국경 간 이전을 제한하는 조치를 채택하는 경우 조치의 목적에 비례(proportional)하는 수준일 것을 요구하고 있다.

다만, 미국이 참여국인 디지털 통상 협정은 데이터 현지화 금지에 대한 LPPO 예외

조항을 인정하지 않고 있다. 특히 미국, 멕시코, 캐나다 간에 체결된 지역무역협정인 USMCA(디지털무역 챕터)와 미-일 디지털통상협정(DTA)의 경우에는 데이터의 국경간 이전 자유화에 대해서는 LPPO 예외 규정을 인정하고 있지만, 데이터 현지화 금지 의무에 대한 LPPO 예외는 인정하지 않는다. 즉, 미국이 참여하고 있는 디지털 통상 협정에서는 데이터의 현지화 금지에 대해서는 예외 적용을 인정하지 않음으로서 보다 높은 수준의 디지털 통상 자유화를 추구하고 있는 것으로 평가된다.

(3) 국제통상 규범에서의 데이터 주권 관련 규범화 현황

일반적으로 국제통상규범에서는 관세 및 비관세장벽의 완화 등 무역자유화의 기본 원칙을 준수하는 것이 의무이지만 정당한 공공정책 목적 등을 수호하기 위한 정부의 규제 권한(regulatory autonomy)을 인정하고 있다. 일례로 WTO 규범상 GATT 제20조의 일반예외(general exceptions) 조항은 천연자원의 보호, 환경의 보전, 공공질서 및 공중도덕의 유지 등 공공정책 목적을 위해 필요한 경우 WTO 회원국들이 무역제한적인 조치를 채택할 수 있도록 예외 조항으로서 허용하고 있다. 단, 이들 규제 조치는 자의적이거나 정당하지 않은 차별적 조치여서는 아니되며 무역을 제한하기 위한 위장된 조치여서는 안된다.

GATT 제21조의 안보예외(security exceptions) 조항은 WTO 회원국들이 자국의 필수적인 국가안보 이익을 필요하다고 간주하는 경우 무역제한적인 조치를 도입할 수 있도록 허용하고 있다. 일반예외 조항과 달리 안보예외 조항은 무역제한적 조치에 대한 자의적 및 정당하지 않은 차별 및 위장된 무역제한 조치로서 적용되면 안된다는 두문(chapeau) 조항이 부재한데, 이에 따라 안보 필요성에 따른 규제 조치에 대한 회원국의 재량을 더 인정해주고 있는 것으로 평가되고 있다. 그러나 안보예외 조항은 기본적으로 (1) 핵물질과 관련된 조치, (2) 군사적 무기 및 군사시설에 공급되는 물품과 관련된 조치, (3) 전쟁 또는 국제관계에 있어서의 긴급 상황에서 취해지는 조치에 한해서만 적용될 수 있는 예외 조항이므로 적용 대상이 넓지 않다.

이외에도 국가들의 기술 규제 조치에 대한 WTO 규범인 TBT 협정 (Technology Barriers to Trade, 기술무역장벽에 대한 협정)에서는 '정당한 목적(legitimate objective)'을 달성하기 위해 도입되는 기술 규제 조치는 수출제품의 품질 보장, 인간 · 동물 · 식물의 건강 및 생명의 보호, 기만적인 행위의 방지를 위해 필요한 경우 허용되고 있는데, 일반예외 조항과 유사하게 자의적이거나 정당하지 않은 차별적 조치 또는 무역을 제한하기 위한 위장된 조치로서 적용되지 않을 것을 명시하고 있다. 그러나 기본적으로는 WTO 회원국들이 정당한 목적의 공공정책을 이행하기 위해 필요한 기술 규제 조치를 도입하도록 허용하고 있으며,

대신 필요 이상으로 무역제한적이어서는 안되며(비례성 원칙), '정당한 목적'에는 국가안보의 필요성, 기만적 행위의 방지, 인간 · 동물 · 식물의 건강 및 생명의 보호, 환경의 보호 등이 해당된다고 명시하고 있다.

이와 같이 현행 국제규범에서는 국가안보의 목적을 포함한 정당한 공공정책 목적을 위한 정부의 규제 권한에 대하여 전반적으로 인정되고 있다고 할 수 있다. 그러나 데이터 주권 및 데이터 안보와 관련하여 정당한 정책 목적으로서 직접적으로 언급되어 있지 않아 예외조항으로서 허용 여부를 불확실하다 할 수 있다. 단, GATT 제21조 (a)항에 "자국의 안전보장상 중대한 이익에 반한다고 인정하는 정보의 제공(provision of data)을 요구하는 것"을 허용하지 않는다고 명시되어 있어, 직간접적으로 데이터 안보와 관련된 조항으로 해석될 여지가 있다. 그러나 현재까지 동 조항을 원용한 WTO 분쟁 판정 사례가 존재하지 않기 때문에 해당 조항이 데이터 안보에 적용될 수 있도록 해석될 수 있는지 여부는 매우 불확실하다.

(4) IPEF 디지털 통상 협상 현황

이 외에도 2022년 5월 공식출범한 '인도태평양경제협의체(IPEF)'의 4개 협상 분야 중 무역 분야(Pillar 1)는 디지털 통상 규범을 내용으로 다루고 있으며, 데이터 관련 주요 규정도 IPEF 규범 협상의 대상이다. 최근 미국은 그동안 디지털 통상규범 협상에서 줄곧 주장해왔던 국경 간 데이터 이전의 자유화 및 데이터 현지화 요구 금지 등 디지털 통상 정책의 추진 방향이 변화하게 되면서 기존의 입장을 철회하였다. 이에 따라 IPEF의 공급망 안정화, 청정경제, 공정경쟁 등 3개 필라에서는 모두 합의를 타결하였으나 디지털 통상이 포함되어 있는 필라1 협상에 대해서만 합의를 도출하지 못한 상황이다.

이는 최근 미국의 소위 '빅테크(Big Tech) 규제' 정책 방향에 의한 것으로 파악된다. 미국 바이든 행정부는 미국의 디지털 플랫폼 기업의 독점행위 규제를 위하여 일련의 입법적 조치를 추구한 바 있는데, 결국 미국 국내 업계의 반대와 미-중 기술패권 경쟁 상황에서의 우위 상실 우려로 인하여 입법화 추진 노력이 거의 모두 무산되었다. 그러나 기존의 미국의 국경 간 데이터 이전 자유화에 대한 미국의 통상 정책 기조는 선회한 것으로 보여지며, 비록 국내 입법화 노력은 무산되었지만 국제 규범 논의에서는 여파가 남아있는 상황인 것으로 평가된다.

3. 데이터 안보 및 데이터 주권 관련 주요국의 최근 규범화 동향

(1) EU의 '디지털시장법(Digital Market Act)'

'디지털시장법(DMA)'은 디지털 서비스를 이용하는 모든 이용자의 권리가 보호되는 안전한 디지털 공간을 창출하고, EU 단일시장과 글로벌 시장에서의 혁신, 성장, 경쟁을 촉진하기 위한 공정한 경쟁의 장을 확립하는 것을 목표로 하고 있다. 2022년 4월 유럽 의회에 의해 법의 주요 내용이 합의되어 2024년 이후 이행될 예정이다. EU는 유럽 디지털 시장에서 활동하는 극소수의 독과점 플랫폼 사업자들이 상거래 조건을 일방적으로 결정하고 플랫폼 이용자 간의 교류를 통제하는 '게이터키퍼(gatekeeper)' 역할을 하고 있는 문제를 해결하고자 하였는데, 기존의 경쟁법으로는 플랫폼 서비스에 의존하고 있는 이용자들에게 부과되고 있는 불공정한 행위를 효과적으로 통제할 수 없다고 판단하고 동 문제를 해소하기 위하여 입안하였다. 특히 EU 역내 디지털 시장에서 시장지배력을 이미 보유했거나 시장지배력 보유가 예상되는 거대 플랫폼 기업에 대한 사전규제 방식을 도입하고자 하였다.

'디지털시장법(DMA)'의 규제 대상은 대규모 디지털 플랫폼을 통해 사업이용자(business user)와 최종사용자(end user) 간 '게이터키퍼' 역할을 하고 있는 '견고하고 영속적인 지위를 누리는' 플랫폼 사업자이며, 법은 이들 '핵심 플랫폼 서비스(core platform service, CPS)' 사업자들의 경합성(contestability)을 제한하는 불공정 관행을 통제하기 위하여 일련의 의무사항을 규정하고 있다. 특히, 개인정보의 결합 금지, 사업이용자의 판매자율권 허용, 사업이용자의 홍보 · 거래 자율권 및 소비자의 자율접근권 허용, 사업이용자의 이의제기 허용, 게이트키퍼의 본인확인서비스(identification services) 강요 금지, 광고서비스 제공 조건의 투명성 등을 의무화하고 있다. 또한 '게이터키퍼' 기업에 대하여 독점적 지위를 이용하여 확보한 데이터의 유리한 활용, 플랫폼을 통해 사전설치된 응용프로그램 사용 강제, 상품 및 서비스에 대한 노출순서(랭킹) 우대, 서비스 전환의 제한, 보조 서비스의 상호운용성 제한, 광고 효과의 무료 측정 수단 점유, 이용자 및 소비자의 데이터 이동권 제한 등을 금지하고 있다. 이와 같은 의무사항이 준수되지 않을 경우 EU 집행위원회는 위반행위에 대한 직권조사 등을 통해 매출액 10%에 해당하는 금액의 수준으로 과징금을 부여하는 등 처벌이 가능하도록 하였다.

(2) EU의 '데이터거버넌스법(Data Governance Act)'

EU 집행위원회는 2020년 11월 유럽 전역의 데이터거버넌스에 관한 공통된 규칙 및 관행을 수립하여 데이터 가용성을 높이기 위한 '데이터거버넌스법(안)'을 발표하였으며 2021년 11월 법이 발효되었다. 이는 EU 디지털 단일시장 강화를 목표로 하는 '유럽 데이터 전략(European Strategy for Data)'(2020년 2월 발표)의 일환으로 EU 회원국에게 직접적인 구속력을 부여하는 규정(regulation)의 형식으로 추진되었다. 기본적으로 EU 역내에서의 데이터 공유에 대한 신뢰 증가를 기반으로 새로운 유럽 내 데이터 거버넌스 방식을 구축하고 사회와 경제에 이익이 되도록 데이터 공유를 위한 안전한 환경을 조성하는 것을 목표로 하고 있다.

'데이터거버넌스법'의 주요 내용은 (1) 공공기관이 보유한 데이터를 자연인 또는 법인이 기존 생산 · 수집 목적이 아닌 상업적 · 비상업적 목적으로 활용할 수 있는 법적 근거를 마련하였으며, (2) 상업적 기밀성, 통계적 기밀성, 영업비밀, 개인정보보호 등에 의해 보호되는 유형의 공공데이터에 대해서 재사용을 허용하여 공공데이터 활용의 폭을 넓혔다. 또한 (3) 데이터 중개자가 제공하는 데이터 공유 서비스(data sharing service)의 신뢰성을 확보하기 위한 요건을 규정하여 EU 차원의 규제 프레임워크를 구축함으로서 사업자의 신뢰도를 높이고 데이터 공유 서비스를 활성화하고자 하였다. (4) 정보 주체의 자발적인 데이터 제공 행위를 확대하고 이를 통해 EU 역내 국경을 초월한 데이터 풀을 만드는 것을 목적으로 '데이터 이타주의(data altruism)' 실현에 대한 내용을 규정였다. 이를 위해 EU에서 승인되어야 하는 '데이터 이타주의 조직'은 공익적 목적 달성, 비영리 기반의 운영 등을 요건으로 하고 있다.

EU의 데이터거버넌스법의 내용 관련하여 구체성이 부족한 것으로 평가되는 측면도 있으나, 데이터의 재사용 및 데이터 공유 서비스의 신뢰 요건 등에 관한 내용은 국내 데이터 거버넌스 정책의 벤치마크로 활용 가능하다. '데이터 이타주의'와 관련된 내용은 국내외 법령에서 생소한 분야이나 방대한 양의 데이터 수집을 촉진하기 위한 방안으로서 고려 가능한 것으로 평가된다.

(3) EU의 '데이터법(Data Act)'

EU '데이터법'은 '데이터거버넌스법'에 이어 EU를 오늘날의 데이터 중심 사회를 주도할 수 있도록 역량 확보를 목표로 하는 '유럽 데이터 전략'의 일환으로 추진된 주요 입법 이니셔티브 중 하나이다. EU 집행위원회는 2022년 2월 데이터법의 초안을 발표하였으며 현

재 유럽의회 및 유럽이사회에서 잠정적 합의를 도출한 상태이다. EU 역내 데이터 단일 시장을 형성하고 데이터 공유를 활성화하기 위한 주체별 접근 및 공유 조건을 규정하고 있다.

데이터법의 목적은 사물인터넷(IoT) 기기에서 생성되는 산업 데이터에 대하여 기존 데이터 시장 약자(개인, 중소기업)의 접근성을 강화해 공유를 활성화하며 데이터 공유의 안정성과 합법성을 확보하기 위한 보안규정을 강조하고 있다. 데이터법의 적용대상은 IoT 제품 제조사 및 서비스 업체와 클라우드 서비스 업체로, 기존 산업 데이터를 보유 및 제공할 수 있는 기업들이며, 중소기업은 공유 의무에서 제외된다. 데이터법은 데이터 접근 주체별로 사용자, 중소기업, 정부 기관으로 구분하여 데이터 접근 조건을 규정하고 있으며, 데이터 공유의 플랫폼을 제공하는 클라우드 서비스 업체에 대한 의무 규정들을 담고 있다.

데이터 접근 주체별로 (1) 사용자에 대해서는 IoT 제품을 사용하고 산업 데이터의 생산에 기여하는 개인사용자의 접근 권한을 강화하고 있다. 반면, 중소기업 대상으로 시장에서 지배력을 행사하는 '게이트키퍼(gatekeeper)' 기업은 이와 같은 무상 제공 대상에서 제외된다. (2) 중소기업 관련해서는 서비스 개발이나 혁신을 위해 IoT 제품 제조사의 산업 데이터에 접근하는 경우 공정하고 수평적인 계약을 체결할 수 있도록 중소기업을 보호하고자 하며, 특히 산업데이터를 보유 및 독점적으로 활용하고 있는 대기업에 대하여 불공정 계약이 성립되지 않도록 방지하고자 한다. (3) 산업 데이터에 대하여 정부는 재난이나 국가 비상사태 발생시 기업에게 데이터를 요청할 수 있으며, 공공 이익을 위한 목적이나 피해 복구를 위한 데이터 활용을 위해서 기업에 데이터를 요청할 수 있다. 기업은 데이터를 무상으로 제공할 의무가 있으며, 정부는 기업에게 데이터 제공 비용을 보상해야 한다. (4) 데이터 공유를 위해 필수적인 역할을 하는 클라우드 서비스 업체 관련하여 데이터법은 산업 데이터에 대한 불법적인 접근을 방지하기 위하여 클라우드 업체의 보안에 관한 의무를 부과하고 있다. 소비자의 자유로운 선택권을 보장하기 위하여 클라우드 서비스는 사용자의 데이터 이동 및 전환을 보장해야 하며, 소비자의 서비스 이용 종료시 데이터 전환에 필요한 비용을 사용자에게 청구할 수 있으나 즉각적인 전환이 가능하도록 클라우드 기술 표준을 마련해야 하며 법 발효 후 3년 이후부터 무상이동을 보장해야 한다.

(4) 미국의 데이터 안보 행정명령

미국 바이든 대통령은 2024년 2월 미국 데이터가 특정국가로 거래되는 것을 제한하는 '우려국에 의한 민감한 대량의 미국인 데이터 및 미국 정부 관련 데이터의 접근금지(Preventing Access to Americans' Bulk Sensitive Data and United States Governmet-Related Data by Countries of Concern)'에 관한 행정명령(EO 14117)을 발령

하였다. 이를 통해 '우려국가'와의 데이터 거래로 인하여 심각한 개인정보 침해, 방첩활동 방해, 군사 및 정보기관에 대한 다량의 이메일 발송 등 국가안보 우려에 대응하고 미국의 데이터 안보를 강화하기 위한 강력한 조치를 추진하고자 하였다.

행정명령은 데이터 중개, 제3자 공급업체 계약, 고용 계약, 투자 계약 및 기타 계약이 대량의 미국인 민감 데이터에 대한 직접적이고 자유로운 접근을 제공하여 국가안보를 심각하게 위협하고 있는 상황에서 미국 법무부 장관으로 하여금 미국인의 데이터가 '우려국가'로 대규모로 이전되는 것을 방지할 수 있도록 권한을 부여하고 있다. 또한 연방 부처 및 기관으로 하여금 민감한 개인 데이터를 '우려국가'(중국, 북한, 러시아, 쿠바, 이란 등)로 전송하는 것을 억제하기 위하여 새로운 규칙의 제정을 포함하여 필요한 조치를 강구하도록 지시하고 있다.

특히 행정명령은 미 법무부로 하여금 '고도로 민감한 데이터의 거래'는 전면 금지하고 있는데, 그 밖의 데이터에 대해서는 '우려국가'의 접근을 차단하기 위해서 미리 규정된 특정 보안요건을 준수하는 것을 조건으로 제한적인 거래를 진행할 수 있도록 하고 있다. 특히 데이터의 중개 거래, 대량의 인간 게놈 데이터 또는 인간 게놈 데이터를 도출할 수 있는 인간 생체 표본의 전송과 관련된 거래 등에 대하여 거래를 전면적으로 금지하고자 한다. 반면, 공급업체의 계약(기술 서비스 계약 및 클라우드 서비스 계약 포함), 고용 계약, 투자 계약 등에 대해서는 특정 요건의 충족을 조건으로 제한적 거래를 허용하고 있다.

(5) 미국의 '합법적 해외 데이터 활용의 명확화를 위한 법(CLOUD Act)'

미국 트럼프 행정부 하에서 2018년 3월 발효된 미국 CLOUD Act는 미국 사법당국으로 하여금 자국의 IT 기업들이 해외 서버에 저장하고 있는 데이터를 열람할 수 있도록 법적 근거를 마련하고 있다. 과거 미국 수사기관들은 테러 · 마약 관련 범죄의 수사 과정에서 자국 IT 기업에 이메일 계정 등 통신 자료를 요청하였으나 해외에 저장되어 있는 정보의 제출을 거부한 사례가 있으며, 동 사건에 대한 법적 소송(미국 정부 vs. 마이크로소프트) 결과 미국 법원은 영장 대상의 내용이 미국 역외의 데이터센터에 저장되어 있으므로 영장의 집행은 불법적인 역외적용(extraterritoriality)에 해당된다고 판시한 바 있다. 이에 따라 그동안 미국 정부는 해외에 저장된 데이터에 대한 접근성 부재로 인해 테러 · 마약 · 밀매 등 범죄의 조사가 어렵다는 입장이었는데, 최근 클라우드 서비스와 같은 대규모 데이터 시스템을 활용한 범죄의 증가에 대응하여 동 법의 제정을 통해 효과적으로 대응하게 될 수 있게 되었다.

미국 CLOUD Act의 주요 내용은 (1) 역외적용의 명시적 근거 마련, (2) 서비스제공

업체의 영장 각하신청 제도 신설, (3) 외국 정부와의 행정협정 체결을 통한 정보제공 절차 마련 등이다. CLOUD Act 제2713조는 "서비스제공자는 해당 통신, 기록 또는 기타 정보가 미국 내 또는 미국 밖에 저장되어 있는지 여부와 관계없이 해당 제공자가 보유, 보관 또는 통제하고 있는 유선 또는 전자통신의 내용 및 기타 기록 또는 고객 또는 가입자의 정보를 보존, 백업 또는 공개할 법적 의무를 준수해야 한다"고 규정하여 법률의 역외적용에 대한 명시적 근거를 마련하였다. 또한 미국 정부에 의해 발부된 영장의 집행이 외국의 법률(데이터 현지화 요건 등)을 위반한 소지가 있는 경우, 대상자가 미국인이 아닌 경우 서비스제공자가 영장 각하 또는 변경 청구를 할 수 있도록 장치를 마련하여 서비스제공자가 우려하는 외국 법률과의 충돌 문제를 사전에 예방하고자 하였다. 또한 초국경적 정보 제공 요청을 위한 미국과 외국 정부 간의 행정협정(executive agreement)에 대한 규정을 마련하여 미국의 전자통신 서비스 제공자가 법률을 위반하지 않고 행정협정에 따라 외국 정부의 정보제공 요청에 응할 수 있도록 법적 근거를 마련하였다.

(6) 평가 및 시사점

EU는 일련의 데이터 관리에 관한 법률 제정을 통해 그동안 EU 회원국들의 개별적인 제도의 도입으로 인해 파편화되어 있는 데이터 거버넌스 체계를 정비하여 EU 단일시장으로서의 디지털 경쟁력 성장을 추구하고 있는 것으로 평가된다. 특히 EU '데이터거버넌스법'은 글로벌 디지털 시장 및 데이터 산업에서 미국 IT 기업들의 독점적인 시장지배력이 확대되고 있는 상황에서 EU 회원국들의 데이터 안보를 강화하기 위한 정책 수단으로서 EU 역내에서의 데이터 공유를 활성화하기 위한 비즈니스 환경을 구축하고자 하는 것으로 보여진다. 이러한 측면에서 EU의 데이터 안보 정책은 단순히 '개인정보의 보호 강화'를 통한 역내 데이터의 보호 보다는 역내에서의 '데이터 공유의 확대'를 통해 현재 주요국에 비해 열위에 있는 EU의 디지털 경쟁력을 제고시키고자 하는 것으로 평가된다.

EU '데이터법'도 미국의 거대 IT 기업의 글로벌 데이터 산업에서의 시장지배력 및 데이터의 독점을 견제하기 위한 데이터 안보 정책수단인 것으로 평가된다. 특히 미국의 거대 IT 기업을 의미하는 '게이트키퍼(gatekeeper)'에 대한 데이터 공유 의무 규정은 이들 기업에 대한 규제를 통해 유럽 기업들이 데이터 및 클라우드 서비스 시장에서 경쟁력을 확보할 수 있도록 여지를 마련하기 위한 것으로 평가되고 있다. 또한 클라우드 서비스 제공업체들에 대하여 외국의 역외적용 법률로부터 EU 소비자 데이터를 보호하기 휘한 의무규정을 도입하고 있는데, 이는 미국으로의 데이터 이전을 규제하고 EU 역내에서의 데이터 저장을 유도하는 데이터 현지화 조치의 효과를 갖고 있는 것으로 평가된다.

미국의 데이터 안보 관련 행정명령은 데이터에 대한 지배력을 강화하여 미-중 간 디지털 경쟁에서의 우월적 지위를 확보하고 국가안보를 더욱 강화하고자 하는 미국 정부의 노력을 나타내고 있다. 특히 미국은 통합적인 개인정보 보호에 대한 국내 규범이 부재한 상황에서 우선적으로 '우려국가'에 대한 미국인 정보의 대량 이전 및 유출을 방지하고자 한 것으로 평가된다. 미국의 민감 데이터가 '우려국가'로 이전될 경우 미국에 대한 방첩 활동, 영향 공작을 비롯하여 미국을 대상으로 한 무력공격 및 사이버 공격 등에 악용될 수 있으므로 이를 강력하게 제한하고자 하는 것이다. 무엇보다 '우려국가'에 의한 빅데이터의 접근을 제한하여 기술 발전 노력을 지연시키고, 빅데이터의 입수를 통한 영향력 공작 및 첩보 활동을 무력화하고 여론과 정보조작 행위를 견제하는 전략적 목적을 갖고 있는 것으로 평가된다.

또한 미국의 해외 데이터 활용을 위한 CLOUD Act는 자국민의 데이터에 대한 국외 이전을 제한하기보다는 국외에 있는 자국민의 데이터에 보다 신속하고 용이하게 접근할 수 있도록 법적 근거를 마련하였다는 점에서 '공공이익'의 보호 강화를 위한 데이터 안보 조치를 도입한 것으로 평가할 수 있다. 특히 상대국의 데이터 현지화 조치로 인하여 해당국에 설치되어 있는 미국 IT 기업의 데이터 서버에 대한 접근권이 부재한 국가안보 리스크를 해결하고자 한 것으로 보이며, 결국 동 법의 제정을 통해 무역상대국들의 데이터 현지화 조치를 무력화시키는 효과가 있는 것으로 평가된다.

이와 같이 데이터 안보를 강화하기 위한 일련의 법제도적 노력은 미국이 디지털 통상 정책방향으로서 강하게 지지해왔던 '데이터의 자유로운 국경간 이전'에 대한 기존의 입장이 변하고 있음을 시사한다. 미국은 그동안 디지털 통상 관련 체결된 다양한 무역협정을 통해 '국경간 데이터의 자유로운 이전'을 지지해왔으나, 최근 WTO 전자상거래 관련 규범 협상에서 기존의 입장을 철회하여 미국의 디지털 정책 방향이 변하고 있음을 나타낸다. 미국은 2023년 WTO 전자상거래 JSI 협상에서 '국경간 데이터의 자유로운 이전', '데이터 서버의 현지화(localisation) 요구 금지', '소스코드 공개요구 금지' 등을 의무화하는 내용의 디지털 통상 규범을 담은 제안서를 철회한 바 있다. 대신 미국 정부는 최근 G7 정상회의에서 채택된 '신뢰에 기반한 데이터의 자유로운 이전(Data Free Flow with Trust, DFFT)' 원칙에 대한 지지를 표명하였는데, 이는 기존의 '조건 없는' 데이터 이전의 자유화에서 변화된 입장인 '신뢰'를 기반으로 한 데이터 이전을 강조하고 있다.

이에 따라 미국은 안보적 우려를 제기하지 않는 신뢰할 수 있는 국가와는 '데이터의 자유로운 국경간 이전'이라는 근본적인 원칙을 준수하되, 안보적 우려가 있는 국가에 대해서는 데이터의 이동과 유출을 제한하는 방식으로 '분절화'된 접근방식을 취하고 있는 것으로 평가된다. 반면, 데이터 현지화 조치에 대한 금지 원칙은 계속 고수하고 있는 것으로 보이는데, 미국의 CLOUD Act는 자국의 역외 데이터에 대한 접근권을 보장하도록 국내규범을 역

외적용하도록 하여 무역상대국의 데이터 현지화 조치를 무력화시키는 효과를 추구하고 있다고 볼 수 있다.

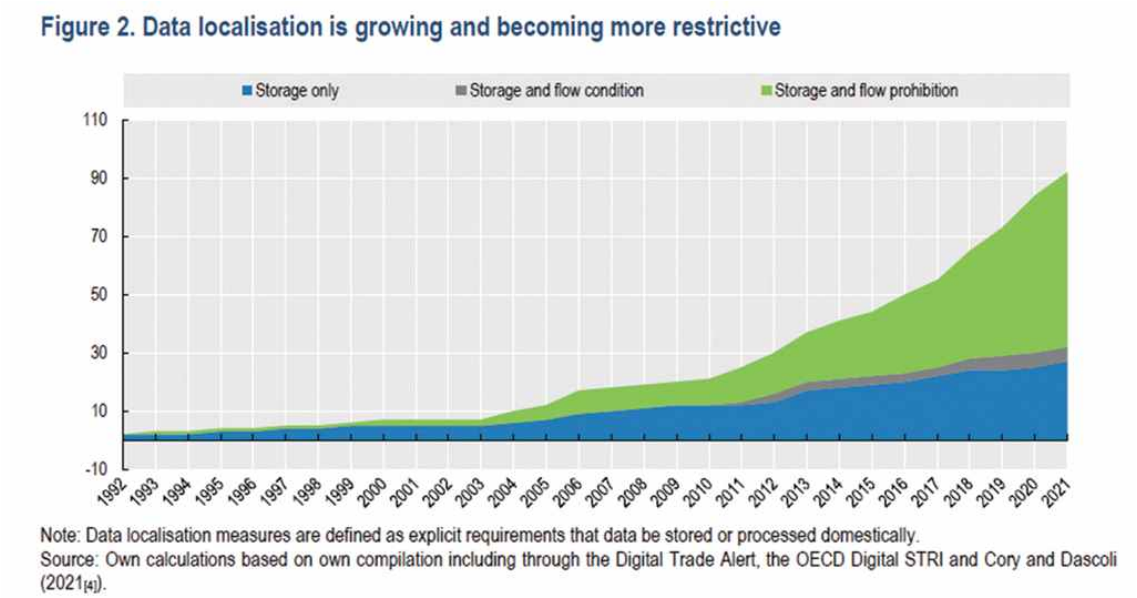
4. 데이터 주권 관련 주요 통상 현안

(1) 데이터 현지화 조치를 통한 데이터 주권 강화

데이터 안보의 강화를 법제도는 데이터 주권 이슈와 긴밀하게 연계되어 있으며, 이는 자국민의 개인정보에 대한 국경간 이전을 제한하는 '데이터 현지화(data localisation)' 조치의 형태로 주로 나타난다. 이와 같이 데이터 현지화 조치는 대표적인 데이터 주권 및 데이터 안보 강화를 위한 정책 수단으로서 자국민의 데이터가 역외로 이전 및 역외에서 저장·처리될 경우 해당 데이터에 대한 통제권을 상실하게 된다는 우려에서 비롯된다. 이에 따라 데이터 현지화 조치는 정부당국이 자국민의 개인정보를 보호하기 위한 목적 및 규제 목적으로 필요한 데이터에 대한 접근권을 보안하기 위해 도입되고 있으며, 국가안보의 관점에서 민감한 데이터에 대한 보호 수단으로서 신뢰할 수 없는 국가로부터 데이터 접근권을 제한하기 위해 도입되기도 한다. 또한 데이터 현지화 조치는 자국의 관할권 밖에서 보관되고 있는 자국민 데이터에 대한 외국정부의 접근권을 제한하여 외국정부의 개입으로부터 자유로워지기 위한 목적도 추구하고 있으며, 기술 발전의 속도로부터 뒤처지지 않기 위해 데이터 현지화 조치를 통해 대량의 데이터를 다루는 외국 기업에 대하여 국내 시장에서의 활동과 경쟁력을 제한하고자 하는 목적도 추구하고 있다.

[그림 1]에서 나타나는 것과 같이, 국가별 데이터 현지화 조치는 지속적으로 증가하고 있는 추세이다. 2017년 35개국에서 67건의 데이터 이전 제한 조치가 도입되었다면 2020년에는 62개국에서 144건의 데이터 이전 제한 조치가 도입된 것으로 집계된다. 특히 최근 5년간 데이터 현지화 조치의 도입 건수가 크게 늘어난 것으로 나타나며, 2021년 기준으로 도입된 데이터 현지화 조치 중 70%는 가장 강력한 형태의 데이터 현지화 조치(데이터의 국외이전 금지 및 현지 저장 요구)인 것으로 나타난다. OECD 자료에 따르면 선진국의 비중이 높은 OECD 회원국의 경우 데이터의 현지 저장만 요구하는 데이터 현지화 조치를 가장 많이 도입하고 있는 반면, 개도국의 비중이 높은 OECD 비회원국들은 데이터의 현지 저장과 함께 데이터의 국외 이전 금지를 의무화하는 가장 강력한 형태의 데이터 현지화 조치를 많이 도입하고 있는 것으로 나타난다.

[그림 1] 데이터 현지화 조치 도입 동향(1992–2021)



자료: OECD(2022)

데이터 현지화 조치는 크게 세 가지 형태로 구분되는데, (1) 데이터의 국외이전 및 외국에서의 데이터 저장과 처리를 허용하면서 데이터의 복사본에 대한 국내 저장을 요구하는 경우, (2) 자국 내에 복사본을 저장할 경우 데이터의 국외이전을 허용하는 조건부 조치이면서 데이터의 국외이전 및 데이터 접근에 대한 명시적인 요건을 부과하는 경우, (3) 자국 내에서 생산된 데이터의 국외이전을 금지하고 국내에서의 저장 및 처리를 요구하는 경우(가장 강력한 형태)이다. 데이터의 국외이전을 허용하면서 국내저장을 요구하는 경우는 주로 회계 정보 등 기업 데이터 또는 정보통신 데이터가 이에 해당되며, 일례로 자국 회계법에 따라 회계정보는 자국 내에서 7년간 저장되어야 할 것을 규정하고 있다. 자국내 데이터 복사본을 저장할 경우 데이터의 국외이전을 허용하는 조건부 조치는 주로 보건 의료 데이터에 해당되며, 사용자의 필요에 따라 역외 데이터에 대한 접근권을 보장하도록 하고 있다. 마지막으로 데이터의 국외이전을 금지하고 국내저장 및 처리를 의무화하는 현지화 조치는 금융, 정보통신, 결재 관련 정보 등 다양한 데이터에 해당되며, 일례로 전자적 시스템을 통한 거래에 활용되는 모든 데이터를 국내에서 관리,처리 및 저장할 것을 요구하는 조치 등이다.

(2) 공공 클라우드 보안 기준

대량의 데이터 및 빅데이터를 다루는 클라우드 컴퓨팅 분야에서 데이터의 저장 및 처리에 대한 문제는 매우 중요하며 자유로운 국경간 데이터 이전이 허용되는 환경에서 가장 효율적인 서비스가 제공될 수 있을 것이다. 클라우드 컴퓨팅은 데이터를 인터넷 상에 저장해두고 인터넷에 접속만 하면 언제 어디서든 다양한 IT 서비스를 활용할 수 있도록 하는 서비스이며, 인공지능과 빅데이터 처리를 위한 기본 인프라로 부상하였다. 이에 따라 데이터의 자유로운 국외 이전을 제한하는 데이터 현지화 조치는 클라우드 컴퓨팅 서비스 시장의 성장에 부정적인 영향을 줄 것으로 우려되고 있다.

한편, 정부당국 및 공공기관의 입장에서는 클라우드 서비스의 활용을 위해 자국 밖에 저장되어 있는 자국민의 데이터에 대하여 외국정부가 접근할 수 있다는 것 자체가 리스크 요인이며 국가안보의 사안으로 간주되고 있다. 외국 클라우드 서비스 사업자들의 데이터 센터에 정보를 저장할 경우 해당 정부의 열람 대상이 될 수 있다는 점이 우려되며, 외국의 클라우드 서버에서 개인정보가 유출될 경우 구제받기 힘들다는 점도 우려의 대상이 되고 있다. 특히 미국의 CLOUD Act에 근거해 안보 위험이 존재한다고 판단할 경우 미국 정부가 역외에 있는 자국기업의 클라우드 서버에 저장된 데이터에 접근할 수 있게 되는 우려가 현실화될 수 있는 상황이다.

이와 같은 국가 데이터의 유출 관련 국가안보 리스크에 대응하기 위해 우리나라는 공공기관 클라우드 보안 정책의 일환으로 '공공기관 클라우드 보안 인증 제도(Cloud Security Assistance Program, CSAP)'을 채택하고 있다. 공공기관 클라우드 보안정책은 정부 및 공공기관의 클라우드 서비스 도입을 위해 준수되어야 하는 보안 기준을 마련하고 있는데, 과학기술정보통신부의 CSAP 인증 제도를 활용하여 CSAP을 통과한 클라우드 서비스는 공공기관 클라우드 보안 기준을 만족한 것으로 간주하여 국가기관으로의 도입을 허용하고 있다.

이와 관련하여 최근 몇 년간 미국은 우리나라의 클라우드 보안 인증 제도인 CSAP에 대하여 글로벌 클라우드 서비스 제공 기업들에 대한 디지털 무역장벽이라고 문제를 제기해왔다. 2021년 이후 미국무역대표부(USTR) 무역장벽보고서(NTE Report on Foreign Trade Barriers)를 통해 한국의 CSAP 제도를 지적해왔으며, 우리의 CSAP 보안 기준으로 인하여 미국 클라우드 서비스 제공업체들이 한국의 공공 클라우드 시장에 진출하지 못하고 있다고 주장하고 있다. 특히 우리나라의 CSAP 보안 기준을 충족하려면 미국 클라우드 서비스 제공업체들이 한국 시장 진출을 위한 고유한 클라우드 서비스 제품을 만들어야 하기 때문에 부담이 되며, 이로 인하여 한국의 중앙 및 지방정부부처, 공공기관 및 교육기관으로의

서비스 제공을 위한 공공조달 시장으로부터 배제되어 왔다는 것이다. 무엇보다 CSAP 보안 기준 중 데이터 현지화, 안정성이 검증된 정보보호 제품 사용, 정부에서 인증한 암호화 알고리즘 사용, 물리적 망 분리 등의 요건들이 글로벌 표준에 부합하지 않는 과도한 차별적인 무역장벽이라 주장한다.

사실 우리나라의 공공기관 클라우드 보안 정책은 국가정보원에서 관리하고 있는 국가 공공기관에 대한 '클라우드 보안 기준'을 충족하도록 하고 있으며, 현재 이를 충족하고 있는 과기부의 CSAP 인증제도를 국가기관에 대한 클라우드 서비스 보안기준으로 도입하고 있다. 미국은 우리나라의 공공기관 클라우드 서비스 시장에 진출하기 위해 우리의 '공공기관 클라우드 보안 정책'보다 공략하기 쉬운 'CSAP 보안 기준'을 공격하고 있는 것으로 파악된다.

미국의 지속적인 보안기준 완화 요구에 대하여 우리의 '공공기관 클라우드 보안 정책'에 따라 국가안보를 위한 최소한의 보안 조건이라고 설명하고 해당 보안 기준이 미국 기업만을 대상으로 부과되는 차별적인 보안 기준이 아니며 국내외 기업에게 동일하게 적용되는 보안 기준이라는 입장을 제시해왔다. 미국 외에 프랑스, 독일 등 주요국들도 자국의 국가안보 목적을 위해 동일한 또는 유사한 클라우드 보안기준을 도입하고 있는 상황이다. 미국 또한 'FedRAMP (Federal Risk and Authorization Management Program)' 보안 인증 제도를 2012년부터 도입하여 보안 문제와 시스템 취약성을 검증해 기준을 충족할 경우 공공기관 및 민간 모든 영역에서 클라우드 서비스를 도입하고 있다.

작년 우리 정부는 CSAP을 개정하여 정보 보안등급을 3등급으로 구분하여 물리적 망 분리 조건을 완화하였다. '상'과 '중' 등급으로 분류되는 보안등급이 높은 공공 데이터에 대해서는 물리적 망 분리 조건을 지속 적용하고, 보안등급이 낮은 '하' 등급으로 분류되는 데이터에 대해서는 논리적인 망 분리를 허용하여, 알고리즘을 통해 민간 및 공공 데이터를 구분하도록 하였다. 이 외에도 개정된 제도에 따라 백업 시스템에 대한 현지화 요건을 부과하고 클라우드 서버 관리 인력도 현지화하도록 요구하고 있다. 또한 안보, 외교, 금융 관련 데이터에 대해서는 계속 현지화 요건이 적용되도록 하였으며, 공공기관 데이터의 저장위치를 공공기관이 지정할 수 있도록 새로운 의무규정도 신설하였다. 그러나 미국 클라우드 서비스 기업들은 '중' 등급의 보안등급까지 보안 기준을 완화할 것을 요구하면서 한국시장에 대한 진출 장벽을 낮추기 위해 계속 압박을 가하고 있는 것으로 파악된다.

(3) 지도 정보 등 위치기반데이터의 국외반출 제한

최근 미국의 디지털 플랫폼 서비스 업체(애플)가 우리나라 정부를 대상으로 국내 정

밀 지도(5000대1 축적) 데이터의 해외 반출 허가를 요청하였으나, 이에 대하여 정부가 반출 불가 방침을 통보하여 지도 데이터의 국외 반출 관련 한–미 간 통상 현안이 재점화될 것으로 예상되고 있다. 한국 정부는 국가안보에 영향을 줄 수 있다는 이유로 지도 반출 요구를 불허하였으며, 현행법 상 국토교통부 장관의 허가 없이는 2만5000대1 축적보다 세밀한 지도의 국외 반출이 불가능한 상황이다. 이와 관련하여 미 무역대표부(USTR)의 2023년 국별 무역장벽보고서(NTE)는 한국의 지도 정보 국외반출 제한을 디지털 무역장벽으로서 명시하고 있다.

2007년 미국의 구글이 국내 지도 데이터의 국외 반출을 시도한 바 있는데, 이에 대하여 우리 정부는 구글이 운영중인 위성사진 서비스에 5000대1 축적의 지도를 결합하면 국가 주요기관의 위치가 노출되므로 이를 국가안보 위험을 이유로 반대한 바 있다. 디지털 전략 자산인 디지털 지도는 길 안내 뿐 아니라 자율주행 · 증강현실(AR) · 가상현실(VR) · 디지털트윈 등 신사업 확장을 위한 핵심 데이터 자원이므로 해당 데이터를 반출하게 될 경우 특정 디지털 기업의 데이터 독점 현상은 더욱 심화될 것으로 우려되고 있다.

동 문제는 디지털 통상 관련 국제규범에서 금지하고 있는 '데이터 현지화' 이슈와 직접적으로 연계되어 있으므로 논란의 여지가 많을 것으로 보인다. 국가안보의 사안으로서 지도 정보에 대하여 데이터 서버의 현지화 요구 및 규제의 필요성도 존재하지만 데이터 관련 국제규범화의 추세를 고려하여 데이터 현지화 관련 정책적 입장을 정립할 필요가 있다.

5. 시사점 및 고려사항

(1) 각국의 국익에 기반한 데이터 주권 정책 추진

미국과 EU 등 주요국이 최근 도입하고 있는 데이터 주권 및 데이터 안보 관련 조치는 각국의 글로벌 데이터 산업에서의 경쟁력 및 글로벌 시장에서의 위치에 따라 다른 목적 및 형태로 전개되고 있는 것을 확인할 수 있다. 미국의 경우 전세계적으로 증가하고 있는 데이터 현지화 조치에 대응하기 위하여 자국 기업이 보유하고 있는 역외 데이터에 대한 접근권을 확보하고 자국의 데이터 산업 경쟁력을 유지할 수 있도록 국내 규제권한의 역외적용(extraterritoriality)을 허용하기 위한 제도를 도입하고 있다. EU의 경우에는 미국 거대 IT 기업의 데이터 산업에서의 경쟁력 확대를 견제하기 위하여 유럽 내에서의 '데이터 단일시장' 구축 및 데이터 공유 활성화를 통한 디지털 산업의 성장을 지원하고 유럽 기업의 데이터 시장 진입 및 경쟁력 확보를 위한 여지를 마련하고자 하고 있다.

미국은 그동안 경제적 이익의 확대 차원에서 '국경간 데이터 이전의 자유화'를 위한 국제통상규범을 수립하기 위한 노력을 전개해 왔지만, 미-중 기술패권 경쟁이 심화되고 있는 상황에서 이제는 '국가안보'의 논리를 활용하여 자국의 데이터 안보 및 데이터 주권 강화를 추구하고 있는 것으로 평가된다. 그동안 WeChat, TikTok 등 중국 플랫폼 서비스의 미국 시장으로부터의 퇴출 사례에서 볼 수 있듯이, 미국은 데이터 시장의 확대를 위하여 데이터 서비스 기업들의 외국인 투자를 환경하던 입장에서 자국민 데이터의 유출 방지 및 국가안보 강화의 필요성에 따라 데이터의 국경간 거래를 부분적으로 통제하는 방향으로 변화하고 있다. 이와 같이 미국의 데이터 안보 강화 노력은 '우려국가'를 대상으로 전개되고 있으며, 앞으로 신뢰할 수 있는 국가들과의 공조 및 연대로 확대될 가능성도 있다 하겠다. 또한 미국이 추구하는 데이터 안보 정책의 효과 제고를 위하여 유사입장국 간 유사한 제도 도입의 필요성을 강조할 수도 있다 하겠다.

우리나라도 데이터 안보의 관점에서 '데이터의 국경간 이전 자유화'의 기본 원칙 하에서 국가안보의 필요에 따라 '우려대상국'에 대한 데이터 유출의 위험에 대하여 안보 · 경제 · 사회적 인식을 제고하고, 필요시 이에 대한 적절한 대응을 할 수 있도록 국내법적 근거를 마련할 필요가 있다. 한국이 기체결한 외국과의 디지털 통상 협정에서는 데이터의 국경간 이전 및 데이터 현지화 금지 조치 관련하여 정당한 공공정책 목적 및 국가안보의 필요에 의해 제한할 수 있는 여지

를 마련하고 있다. 우리나라의 경우 성장 잠재력이 높은 데이터 산업의 손실을 유발하지 않으면서 우리의 특수한 국가안보적 위협 상황을 고려한 데이터 안보 정책의 수립을 위한 국내 제도의 재점검이 필요할 것으로 보인다.

(2) 데이터 현지화 조치의 확산에 대한 미국의 새로운 접근방식 대응

주요국의 데이터 안보 강화를 위한 정책수단으로서 데이터 현지화 조치의 활용은 지속되고 있으며, 이러한 데이터 현지화 조치에 대한 대응 및 접근방식이 변하고 있는 것으로 보인다. 미국은 그동안 디지털 통상 관련 국제규범의 수립을 통해 무역상대국들의 데이터 현지화 조치의 도입을 금지하고자 하였으나, 이는 지역적 차원에서의 통상규범 수립을 위한 노력에 그치고 있어 한계가 있는 것으로 드러난다. 이에 따라 미국은 주요 무역상대국의 데이터 현지화 조치를 무력화하는 방식으로 자국 기업의 데이터에 대한 접근권을 확보하는 형태로 접근방식의 변화를 보이고 있다.

미국의 CLOUD Act 입법 사례에서 볼 수 있듯이, 미 정부기관이 국가안보 등의 이유로 데이터가 저장된 위치와 관계없이 정보의 이전을 요청할 수 있게 됨으로써 자국의 역

외 데이터 접근에 대한 법적 근거를 마련하게 되었다. 무역상대국의 데이터 국내 저장에 대한 규제 강화를 통한 접근방식(기존의 데이터 현지화 금지 조치)보다는 자국의 역외 데이터 접근권에 대한 권한 강화를 통한 접근방식(새로운 데이터 현지화 금지 조치)을 채택하고 있는 것으로 평가된다. 미국은 CLOUD 법에서 보장하고 있는 역외 데이터에 대한 접근 권한을 통해 무역상대국의 데이터 현지화 조치를 효과적으로 상쇄할 수 있는 방안으로 활용할 가능성도 있다.

앞서 살펴본 바와 같이 우리나라의 공공데이터에 대한 데이터 안보 정책인 공공기관 클라우드 보안 정책에 대하여 미국은 디지털무역장벽으로서 간주하고 있으며, 기타 국가지리정보의 국외반출 금지 조치에 대해서도 데이터 현지화 조치로서 통상 문제를 제기할 가능성이 있다. 현재 미국과 EU 등 주요국에서 추진하고 있는 데이터 안보 강화를 위한 정책을 참고하여 우리의 근본적인 디지털 경쟁력 강화를 위하여 국제적인 기준에 부합하는 보안 정책 등 접근방식을 고민하고 정책을 마련할 필요가 있겠다.

[참고자료]

김경훈 외(2021), “EU 데이터거버넌스 법안(Data Governance Act) 주요 내용 및 시사점”, KISDI Premium Report 21-01, 정보통신정책연구원.

손한별(2021), “미국과 중국의 정보우세 경쟁: 디지털 시대의 ‘데이터 안보’를 중심으로”, 전략연구 제84호.

송영진(2018), “미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점”, 형사정책연구 29(2).

오일석(2024), “데이터에 대한 지배력과 국가안보”, 이슈브리프 526호, 국가안보전략원.

Broadbent, Meredith(2023), “The EU Data Act: The Long Arm of European Tech Regulation Continues”, Center for Strategic and International Studies (CSIS).

Fahey, Elaine(2023), “Does the EU’s Digital Sovereignty Promote Localisation in its Model Digital Trade Clauses?”, European Papers Vol. 8 No.2.

Nigel, Cory, LUke Dascoli(2021), “How Barriers to Cross-Border Data Flows are Spreading Globally, What they Cost, and How to Address Them”, Information Technology and Innovation Foundation (ITIF).

OECD(2022), A Preliminary Mapping of Data Localisation Measures, OECD Trade Policy Paper No. 262.

Wu, Emily(2021), “Sovereignty and Data Localization”, Belfer Center for Science and International Affairs, Harvard Kennedy School.