

미국의 데이터안보 대응과 시사점:

틱톡 규제를 중심으로



박주희 | 국가보안기술연구소 선임연구원

I. 서론

1. 미국의 틱톡 규제 배경
1. 중국 디지털산업의 성장
2. 틱톡에 관한 데이터안보 우려 제기

II. 미국의 틱톡 규제 정책

1. 대미 투자 제한
2. 서비스 이용 금지와 강제 매각
3. 개인정보 수반 거래 금지 또는 제한

III. 한국에 주는 시사점

1. 개인정보보호법의 역할과 한계
2. 외국인 투자 국가안보위해 심사 요건 개선
3. 공통 가치 기반 디지털경제 협력 모색

IV. 결론

논문 요약

국가 간 데이터 무역, 즉 디지털무역의 확산은 국경을 넘어 타국으로 이전된 데이터를 취급하는 상업적 주체를 매개로 일국 정부가 그 데이터에 접근하는 체계를 국가안보 차원에서 검토할 필요성을 부각시키고 있다. 특히 중국의 디지털산업 성장이 가시화되면서 미국은 지난 몇 년간 디지털서비스 제공자를 통해 중국 당국이 서비스 이용자 데이터에 접근하는 것에 대한 안보 우려를 제기하고 있다. 미국이 이러한 데이터안보 위협을 인식하고 적극적으로 대응한 대표적 사례가 바로 틱톡에 대한 규제이다. 틱톡 관련 데이터안보 문제는 미중 패권경쟁의 맥락에서 주로 평가되어 왔기 때문에 이들 양국에만 국한되는 쟁점으로 인식되는 경향이 있다. 그러나 디지털무역이 점차 활발해지고, 우리 일상에서 다양한 해외 디지털서비스를 이용하고 있는 현실에서, 이 문제를 이들 두 국가에만 국한된 안보 문제로 인식해서는 아니된다. 오히려 이는 초국경 데이터 이동이 초래하는 데이터안보의 보편적 논제로서, 디지털시대 국가들이 직면한 신형안보 이슈로 이해되어야 한다. 이에 본 연구는 미국의 틱톡 규제를 중심으로 제기되는 데이터안보 우려를 이해하고, 미국의 틱톡 대응 사례에 비추어 한국의 데이터 안보 현황을 진단하며, 향후 한국이 추구할 데이터안보 전략 방향에 대한 정책적 함의를 도출하고자 한다.

주제어 데이터안보, 틱톡, 개인정보보호, 인공지능, 미중경쟁, 디지털무역, 데이터 국경간 이전

I. 서론

미국 내 틱톡 매각 시한인 2025년 9월 17일을 이틀 앞두고 스콧 베센트 미국 재무장관은 중국과 틱톡 매각에 관한 윤곽에 합의를 이루었다고 밝혔다(BBC 2025/9/16). 트럼프 행정부 1기에서부터 제기되어 온 미국 내 틱톡 이용에 관한 여러 가지 우려가 미국 기업의 틱톡 지배 구조를 강화하여 일부 해소될 수 있을 것으로 기대되고 있다. 아마존, 애플, 알파벳, 메타, 마이크로소프트, 엔비디아, 테슬라 등 세계적으로 영향력 있는 테크 기업을 보유한 미국에서 중국 베이징에 본사를 둔 바이트댄스가 소유하고 있는 틱톡의 대중적 인기는 미국의 국가안보에 관한 인식에 변화를 초래하였다. 중국이 미국 내 개인의 데이터에 접근하는 양태는 더 이상 해킹 등을 통한 데이터 탈취에 국한되지 않고, 바이트댄스와 같은 상업적 주체를 통해 미국 이용자 데이터 접근이 가능해졌다는 점에 미국이 심각한 안보 우려를 제기하기 시작한 것이다. 이 우려는 데이터안보라는 개념의 틀에서 지난 약 5년간 문제로 지속 제기되며 신홍안보 이슈로 자리 잡게 되었다.¹⁾ 특히, 디지털무역을 통한 데이터의 국경 간 이전 그리고 이전된 데이터를 취급하는 상업적 주체를 통해 일국 정부가 그 데이터에 접근하는 방식을 국가안보 차원에서 검토할 필요성을 부각시켰다. 이에 본 연구는 미국의 틱톡 규제를 중심으로 제기되는 데이터안보 우려를 이

1) 데이터는 그동안 디지털무역과 같이 경제적 관점 그리고 데이터 프라이버시와 같은 개인의 권리 관점에서 다뤄져왔다. 그러나 빅데이터 및 인공지능 기술 발전으로 데이터 문제는 점차 국가 안보 현안으로 인식되고 있으며 오늘날 데이터안보라는 신홍안보 관점에서 다뤄지고 있다(김상배 2020, 7).

해하고 미국의 대응에 비추어 우리의 데이터안보 현황을 평가하고 몇 가지 시사점을 도출하고자 한다. 제2장에서는 먼저 미중 경쟁 맥락에서 데이터안보 우려가 제기되는 지점을 탐색해보고, 우리의 데이터안보 현황 점검의 필요성을 환기한다. 제3장에서는 데이터안보 관점에서 미국이 틱톡 규제를 위해 도입한 조치를 세 가지로 나누어 설명한다. 제4장에서는 우리의 법제도적, 지정학적 현실에 비추어 데이터안보 대응 현황을 평가하고 시사점을 도출하며, 제5장에서 결론을 제시한다.

II. 미국의 틱톡 규제 배경

1. 중국 디지털산업의 성장

지난 몇 해간 뚜렷하게 목도되는 중국의 기술적 산업적 성장 중심에는 데이터가 있다. 2013년 전국인민대표대회에서 시진핑 국가주석이 공식 취임한 이래로 중국은 경제 발전을 이루고 기술 역량을 갖추기 위한 핵심 요소로 데이터를 강조해 왔다. 2016년 국무원에서는 제13차 국가 전략적 신흥산업 발전계획(十三五国家战略性新兴产业发展规划)을 발표하며,²⁾ 디지털 기반을 구축하고 데이터를 활용하며 디지털

2) 2016년 11월 29일 중국 국무원(国务院)은 제13차 국가 전략적 신흥산업 발전계획(十三五国家战略性新兴产业发展规划)을 발표한다.

거버넌스를 정비하여 디지털경제를 국가 신성장 동력의 핵심으로 추진할 것임을 밝혔다. 그 이후로도 지속적으로 중국은 디지털 기반 경제 성장을 추진하며 2025년 초 딥시크 충격에 이르기까지 전 세계의 예상을 뛰어넘는 빠른 속도로 성장하였다. 하버드대학교 케네디 스쿨 벨퍼센터는 향후 10년간 미국의 인공지능 분야 우위를 위협할 국가 중 하나로 중국을 꼽았다(Belfer Center 2025, 6). 중국은 데이터와 인적 자본 분야에서 타국에 앞서 있으며, 딥시크 R1모델과 알리바바의 Qwen3 모델은 현재 미국이 유지하고 있는 인공지능 분야 우위가 예상보다 더 취약할 수 있음을 보여주는 일례라고 평가하였다(Belfer Center 2025, 6).

이와 같이 디지털 분야에서 뚜렷해지는 중국의 성장으로 인해, 중국이 사이버공간에서 미국에 초래하는 안보 위협에 관한 인식에서 미국 내 변화가 목도되고 있다. 오바마 행정부 시기만 해도 미국은 사이버공간을 통하여 지식재산을 탈취하여 중국 산업 경쟁력 강화를 모색하는 이른바 ‘경제 첩보(economic espionage)’ 행위를 중국이 사이버공간을 통해 행하는 주된 위협 행위로 인식하였다(The U.S. DOD 2015, 9). 그러나 점차 중국의 기술적 산업적 성장이 가시화되면서, 미국은 중국이 지식재산 탈취를 넘어 미국의 이익을 직접적으로 위협하고, 신흥기술을 지배할 역량을 갖춘 가장 발전한 전략적 경쟁자가 되었다고 평가하게 되었다(The White House 2023, 3). 특히 중국의 디지털서비스가 글로벌 시장에서 경쟁력을 얻으면서, 사이버공간을 통한 데이터 탈취 없이도 중국은 디지털서비스를 제공하는 상업적 주체를 통하여 당해 제품 이용자의 정보에 접근하는 것이 가능해졌다. 물론 해킹을 통한 데이터 탈취는 여전히 안보에 위협을 끼치나, 최근 부각되는 데이터 접근 방식은 디지털서비스를 제공하는 상업적 주체를

통한 이용자 정보의 접근이 된 것이다. 바로 이것이 미중 경쟁 맥락에서 데이터안보 우려가 제기되는 지점이다. 점차 중국의 디지털서비스가 글로벌 시장에서 경쟁력을 갖게 되면서 중국 당국이 중국의 국가정보법(国家情报法) 등에 기반하여 상용 디지털서비스 제공자를 통해 데이터에 접근하는 것이 미국에게 큰 안보 위협으로 부상하고 있는 것이다. 미국이 이와 같은 위협을 인식하고 적극적으로 대응한 사례가 바로 틱톡에 대한 규제이다.

2. 틱톡에 관한 데이터안보 우려 제기

미국은 트럼프 행정부 1기에서부터 틱톡에 관하여 국가안보 관점 여러 가지 우려를 제기해 왔다. 백도어 설치를 통한 악의적 사이버활동, 틱톡을 통한 허위조작정보 확산 등 영향력 공작, 그리고 데이터안보에 관한 우려가 바로 틱톡에 대하여 제기되는 주요 우려였다(Lewis 2024). 이 중 데이터안보에 관한 우려는 틱톡을 소유한 바이트댄스가 틱톡을 이용하는 미국인의 개인정보를 처리하게 되고, 중국 당국이 바이트댄스를 통해 틱톡 이용자의 개인정보에 접근할 수 있다는 점에서 제기되고 있다. 이에 대응하기 위해 미국은 지난 몇 년간 틱톡을 대상으로 다양한 규제를 도입해왔다.

틱톡에 대한 데이터안보 우려, 즉, 중국 당국이 디지털서비스를 제공하는 상업적 주체를 통해 미국인의 개인정보에 접근하는 것은 크게 세 가지 점에서 미국의 국가안보에 위협이 되는 것으로 인식되고 있다. 첫째, 개인의 데이터 그 자체가 적성국에게 유용한 인텔리전스로 기능한다는 점이다. 대표적으로 연방정부 직원의 개인위치정보가 그러하다. 예컨대, 경호요원이 이용하는 피트니스 앱을 통

해 경호요원의 위치정보를 추적하여 기밀에 해당하는 대통령 등 고위 정치인의 위치가 추적될 수 있다(AP 2024/10/29). 또한, 개인의 민감정보를 적성국이 악용하는 경우 그 개인을 협박 내지는 강압하는데 이용할 수 있다(ODNI 2024, 13). 개인의 민감정보는 정보주체에게 사회적 차별을 야기하고 인권을 침해할 수 있어 한국, 유럽연합 등에서는 그 처리가 제한된다.³⁾ 정치인이나 유명 인사 등의 민감정보를 악용하는 경우 정보주체를 강압하여 입수하기 어려운 기밀 정보를 수집하거나, 이들의 정치적, 사회적 신망을 무너뜨려 타국의 정치 사회에 영향력을 행사할 수 있다(The Washington Post 2021/7/21; Hazelrig 2024, 1). 또한, 개인정보를 분석하여 특정 개인 맞춤형 영향력 공작도 가능하다. 비식별화되어 익명처리 또는 가명처리된 개인 정보라 하더라도, 인공지능 기술을 통해 또는 과거 악의적 사이버활동을 통해 수집한 정보와 결합되면, 식별이 가능해질 수 있고 그로써 개인에 관한 인사이트가 더욱 심화될 수 있다(E.O. 14083 Section 3(c)).

둘째, 데이터안보 문제는 인공지능 경쟁과도 긴밀히 관련되어 있다. 인공지능이 향후 글로벌 패권을 재편성할 수 있는 중요 기술로 주목받게 되면서, 인공지능 경쟁이 미중 경쟁 맥락에서 두드러지게 나

3) 우리 개인정보보호법상 민감정보란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로 '대통령령으로 정하는 정보'를 의미한다. 여기서 대통령이 정하는 정보에는 (i) 유전자 검사 등의 결과로 얻어진 유전정보, (ii) 형의 실효 등에 관한 법률 제2조 5호에 따른 범죄경력자료에 해당하는 정보, (iii) 개인의 신체적, 생리적, 행동적 특징에 관한 정보로 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보, (iv) 인종 또는 민족에 관한 정보가 있다. 개인정보보호법 제23조. 유럽연합 일반개인정보보호규칙(General Data Protection Regulation, GDPR)에서도 개인정보의 특별한 범주로서 이를 규정하고 있다. GDPR 제9조 참조.

타나고 있다. 미국은 중국이 인공지능 분야에서 신속한 발전을 이루었고, 인공지능 역량에 있어 주목할 만한 투자를 하고 있다고 평가한다. 또한, 중국이 단지 경제 성장만을 위해 인공지능 발전을 모색하는 것이 아니라, 자율무인시스템, 인지전 등 군사적 응용을 고려하여 인공지능 발전을 모색하고 있다고 평가하고 있다. 인공지능 경쟁의 승패는 어떤 국가가 대규모의 고품질 데이터셋을 확보하는지, 어떤 국가가 데이터 공유 체계를 잘 구축하는지에 달려있다. 미국은 중국이 인공지능에 있어 데이터가 가지는 가치를 잘 이해하고 있고 양질의 데이터를 활용할 수 있도록 적극적 조치를 취하고 있다고 평가한다(The Commission 2024, 170). 이와 관련하여 미국은 중국의 권위주의적 관행이 중국이 데이터를 수집하는 데 미국에 비해 비교우위를 갖게 한다고 보고있다(The Commission, 2024 198). 중국의 국가정보법(国家情报法), 반간첩법(反间谍法), 데이터안보법(数据安全法) 등을 통해 중국 정부는 데이터를 수집할 수 있는 광범위한 권한을 가지는데,⁴⁾ 이렇게 중국 정부 차원에서 수집한 데이터는 다시금 중국의 기업이 자신의 데이터셋을 강화하는 데 이용될 수 있다(The Commission 2024, 198). 요컨대, 중국 당국 차원의 광범위한 데이터 수집과 제공을 통해 다른 국가의 기업들에 비하여 중국 기업들이 데이터의 양적 확보가 가능하다는 것이다.

마지막으로 중국과의 생명공학기술 분야 경쟁이다. 중국은 상업영역이나 군사영역에 있어 생명공학기술 활용을 모색하고 있는데, 생

4) 예컨대, 2021년 중국에서 제정된 데이터안보법(数据安全法) 제35조에 따라,公安(公安)·국가안전(国安) 기관은 국가안보·형사수사 등 사유로 데이터를 열람 송부를 요구할 수 있는데, 그와 같은 요구를 받는 조직과 개인은 협조하여야 한다.

명공학기술 분야 중국의 역량은 인공지능 기술과 머신러닝을 통해 획기적 발전을 이룰 수 있다고 평가되고 있다. 인공지능과 생명공학 기술의 연계에서 역시 중요한 것은 양질의 데이터이다(The U.S. NCSC 2021, 2). 생명공학기술 분야에서 인공지능의 응용과 광범위한 개인정보 데이터셋, 특히 개인 유전체 정보에 관한 데이터셋이 합쳐지는 경우 특정 국가의 특정 민족이 어떠한 유전적 특징을 지니는지 파악할 수 있다. 적성국이 이를 무기화하는 경우 심각한 국가안보 위협이 될 수 있다(Reuters 2020/8/5).

사실 일국의 정부 당국이 자국의 법 집행이나 국가안보를 위하여 상업적 주체가 보유한 데이터에 접근하는 것은 그 국가의 정당한 권리로 평가될 필요도 있다. 그러나 미국이 제기하는 우려는 중국의 권위주의적 체제에서 기인한 데이터 접근 권한이다. 미국은 중국의 국가정보법, 반간첩법, 데이터안보법 등을 통해 허용되는 중국 당국의 데이터 수집 권한이 지나치게 광범위하여 민주주의 국가에서 정부의 데이터 접근 일반원칙으로 작동하고 있는 독립 감독기구, 개인 권리 침해에 관한 권리 구제제도, 투명성과 같은 장치들이 결여되어 있다고 평가한다. 따라서 데이터안보 문제는 상업적 주체가 보유한 데이터에 정부 당국이 접근하는 체제에 관한 권위주의 진영과 민주주의 진영 사이의 경쟁이 된다.

디지털무역이 점차 활발해 지면서, 이미 우리 일상에서 넷플릭스, 아마존, 알리, 테무 등 다양한 해외 서비스 제공자가 공급하는 상용 디지털서비스가 활발히 이용되고 있다. 디지털무역 원활화는 우리가 당사국인 디지털무역 협정을 기반으로 한다. 우리는 중국 등과 디지털무역 챕터를 포함하고 있는 역내포괄적경제동반자협정(Regional Comprehensive Economic Partnership)을 체결하여, 2022년 동 협정이

국내에서 발효한 상태이다.⁵⁾ 또한, 우리나라는 최초의 복수국간 디지털무역 협정인 디지털경제동반자협정(Digital Economic Partnership Agreement)에 가입하여 동 협정이 2024년 국내에서 발효한 상태이며,⁶⁾ 싱가포르와는 기존 자유무역협정을 일부를 개정하여 디지털동반자협정을 체결하였다. 뿐만아니라 디지털무역 규범을 최초로 담고 있는 포괄적 점진적 환태평양동반자협정(Comprehensive and Progressive Agreement for Trans-Pacific Partnership) 가입도 검토 중인 상황이다. 디지털무역 규범은 기본적으로 데이터의 원활한 국경 간 이동을 통해 경제적 성장과 혁신을 모색하는 것을 목표로 삼고 있다. 우리는 디지털무역 규범에 기반하여 글로벌 시장에서 우리의 디지털 산업 혁신과 경쟁력 강화를 추구해야 하지만, 반대로 우리가 해외 디지털서비스를 이용함으로써 타국으로 이전된 데이터에 관한 안보적 우려 역시 고려하여야 한다. 따라서 미중 경쟁 맥락에서 주목받고 있는 데이터안보 문제는 이들 둘 국가 관계에서만 발생하는 안보 문제로 인식되어서는 아니된다. 그보다 우리는 미국의 틱톡 규제의 배경이 무엇이고 미국이 어떠한 대응을 도입하고 있는지에 주목하여 우리의 데이터안보 대응 현황에 관하여 평가할 필요가 있다.

5) 2025년 11월 기준 RCEP 당사국은 브루나이, 캄보디아, 인도네시아, 라오스, 말레이시아, 미얀마, 필리핀, 싱가포르, 태국, 베트남, 한국, 중국, 일본, 호주, 뉴질랜드이다.

6) 2025년 11월 기준 DEPA 당사국은 뉴질랜드, 칠레, 싱가포르, 한국이다.

III. 미국의 틱톡 규제 정책

1. 대미 투자 제한

소셜네트워크서비스 틱톡을 운영하는 중국 기반 기업 바이트댄스가 당시 미국에서 대중적 인기를 얻고 있던 립싱크 플랫폼 뮤지컬리(Musically)를 인수하려 하자, 이에 관하여 2019년 당시 미국 상원의원 이던 마르코 루비오 의원이 국가안보 우려를 제기하며 미국 외국인 투자위원회(Committee on Foreign Investment in the United States, CFIUS)에 심리를 청구하는 서한을 보내면서 안보 우려에 기반한 미국의 틱톡 규제가 시작된다(Marco Rubio 2019). 미국에서는 방위생산물법(Defense Production Act of 1950)에 근거하여 대통령이 외국인의 대미 투자가 미국의 국가안보에 미치는 영향을 심사할 권한을 갖는다(방위생산물법 제721(b)(1)조). 대통령은 또한 대미 투자가 미국의 안보를 저해할 우려가 있는 경우 해당 투자를 중지하거나 금지할 권한을 갖는다(방위생산물법 제721(d)조). 대통령의 이와 같은 권한 행사는 CFIUS를 통해 이루어지는데, CFIUS는 대상 투자가 미국의 국가안보에 미치는 영향을 조사하고, 미국의 안보를 보호하기 위하여 해당 투자와 관련하여 필요한 조치를 취한다(방위생산물법 제721(b)(2)조). 당시 제기되었던 우려는 미국에 서비스를 제공하여 미국인의 개인정보를 취급하던 기업이 중국 기업에 매각되는 경우 미국인의 개인정보가 해당 투자를 통해 중국으로 넘어갈 수 있다는 것에 관한 우려였다. 외국인의 대미 투자 안보 영향을 심사할 권한에 기반하여 트럼프 대통령은 2020년 8월 14일 행정명령을 발표하여 바이트댄스의 뮤지컬리 인수 거래를

금지하고, 틱톡 운영과 관련하여 바이트댄스와 그 자회사가 보유한 미국 내 유무형 자산과 미국인 이용자 데이터를 행정명령 발표일로부터 90일 이내 완전히 처분하도록 명한다. 그러나 당시 틱톡 이용을 규제하는 행정명령 13942호 등 여러 행정명령 관련 소송으로 인해 이행되지 못한다.

이후 바이든 대통령은 2022년 9월 15일 행정명령 14083호를 발표하여, 해외 적성국이 대미 투자를 통해 미국인의 개인정보 접근함으로써 발생할 수 있는 위험을 관리할 수 있는 근거를 구체화하였다. 동 행정명령을 통해 (방위생산물법 제721조에 따라) 외국인의 미국 기업 인수합병 심사에서 고려되는 안보 위해 요소에 민감 개인데이터 관련 안보 우려가 추가되었다.⁷⁾ 이에 따라 CFIUS는 미국인의 민감 개인데이터에 접근하거나 이를 저장하는 미국 기업에 대한 외국 투자가 미국 안보에 위해가 되는 외국인과 관련되는지 검토하여야 한다. 또한 그 외국인이 해당 투자를 통해 안보 위협을 초래할 수 있는 제3자와 관련되는지도 심사 대상에 포함된다. 구체적으로 살펴보면, CFIUS는 대상 투자를 심사할 때 다음 사항들을 고려해야 한다. 먼저, 미국인의 민감 개인데이터를 다루는 미국 기업에 대한 투자에서 해당 외국인 투자자가 미국 안보를 해칠 수 있는 행동을 취할 가능성이 있는지 검토한다(E.O. 14083 Section 3(c)(ii)). 다음으로, 투자 대상 기업이 보유한 민감 개인데이터가 개인 식별이나 추적에 악용되어 안보 위협이 될

7) 2018년 해외투자위험심사현대화법(Foreign Investment Risk Review Modernization Act of 2018, FIRMMA)에 따라 외국인의 미국 기업 인수합병 심사에서 고려되는 안보 위해 요소(방위생산물법 제721조상 요소)가 한 차례 구체화 된 바 있다. 방위생산물법 제721조(f)항에 따라, 대통령은 대미투자 안보 위해 요소 심사에서 고려할 요소를 정할 수 있는데, 행정명령 14083호를 통해 민감 개인데이터 관련 안보 위해가 심사시 고려할 요소로 추가된 것이다.

수 있는지(E.O. 14083 Section 3(c)(ii)(A)), 그리고 외국인이 미국 내 특정 개인이나 집단을 겨냥하는 데 활용할 수 있는 인구 데이터에 접근하게 되는지를 검토한다(E.O. 14083 Section 3(c)(ii)(B)). 아울러 CFIUS는 투자로 인해 미국인의 민감 개인정보가 안보 위협 행위를 할 수 있는 외국인에게 이전되는지, 그리고 그 외국인이 해당 데이터를 악용하려 하거나 악용 능력이 있는 제3자와 연결되어 있는지도 함께 검토하여야 한다(E.O. 14083 Section 3(c)(iii)). 행정명령 14083호를 통해 미국인의 개인정보를 처리하던 기업에 외국인이 투자하여 미국인의 개인정보가 해외 적성국으로 이전되어 발생할 수 있는 안보 위협을 관리할 수 있는 근거가 마련된 셈이다.

2. 서비스 이용 금지와 강제 매각

1) 정부 장비 이용 금지

틱톡 이용에 대한 미국 내 안보 우려가 확산하면서, 2022년 12월 바이든 대통령은 ‘정부 장비 틱톡 금지법(No TikTok on Government Devices Act)’이 포함된 회계연도 2023년도 통합세출법(Consolidated Appropriation Act)에 서명하여 연방 행정기관이 이용하는 장비에서 틱톡 이용을 금지하였다. 당시 국방부, 국무부, 국토안보부 등 일부 연방 행정기관은 이미 개별적으로 각 기관이 이용하는 장비에서 틱톡 이용을 금지하고 있었으나, 연방 행정기관 전체에 적용되는 일괄적인 금지 의무는 존재하지 않았다. 정부 장비 틱톡 금지법에 따라 관리예산국(Office of Management and Budget, OMB)에게 연방 행정기관이 이용하는 정보기술에서 대상 앱(즉, 틱톡 법인 및 바이트댄스 유한회사와 이 회사가 소유한 실체가 개발하거나 제공하는 모든 후속 앱 또는 서비스)을 제

거하도록 지침을 개발할 의무가 부여되었다(정부장비 틱톡 금지법 제102조).⁸⁾ 이 법에 근거하여 2023년 2월 27일 관리예산국은 정부 장비 틱톡 금지법 이행을 위한 각서를 발표한다(OMB 2023). 이 각서에 따라 동 각서 발표 30일 이내 예외가 승인된 경우를 제외하고, 행정기관은 그들이 소유하거나 운영하는 정보기술에서 대상 앱, 즉 틱톡을 제거하여야 하며, 정보기술에 틱톡을 설치하여선 아니되고, 틱톡으로 인터넷 트래픽을 차단하여야 한다(OMB 2023). 이 금지는 행정기관이 소유 또는 운영하는 정보기술뿐 아니라 연방 행정기관이 당해 정보기술 이용하도록 계약한 하도급자가 이용하는 정보기술에도 적용된다(OMB 2023).⁹⁾ 이로써 연방 행정기관 직원과 이들 하도급 업체 직원이 업무용으로 이용하는 컴퓨터, 서버, 스토리지, 휴대기기 등에서 틱톡 이용이 금지되었다. 이와 같은 정부 장비에서의 틱톡 이용 금지는 이후 전 세계로 확산한다. 이용 금지 근거와 범위는 다소 상이하나, 유사한 금지 제도는 유럽연합, 캐나다, 영국, 호주 등으로 확산한다.¹⁰⁾

8) 관리예산국(Office of Management and Budget, OMB)은 미국 대통령 직속 기구로 연방정보보안현대화법(Federal Information Security Modernization Act)에 따라 연방 사이버보안 정책을 개발하고 감독할 책임을 진다.

9) 여기서 여기서 행정기관(executive agencies)은 미국 연방법전(US Code) 제41부 제133조에 정의된 행정기관을 의미하며, 정보기술(information technology)은 미국 연방법전 제40부 제11101(6)조에 정의된 정보기술을 의미한다. 여기서 정보기술은 행정기관이 데이터를 자동으로 수집하고 저장하며 분석·평가·조작·관리·이동·통제·표시·전환·교환·송신·수신하는 데 사용하는 장비나 그와 연결된 시스템을 의미한다. 이 장비는 행정기관이 직접 사용하지 않더라도, 행정기관과의 계약에 따라 계약자가 서비스를 수행하거나 제품을 제공하는 과정에서 해당 장비를 사용해야 하거나, 또는 그 장비를 상당한 정도로 사용해야 하는 경우도 포함된다. 또한 정보기술에는 컴퓨터, 보조 장비(이미징 장비와 보안·감시를 위한 입력·출력·저장 장치 포함), 컴퓨터 중앙처리장치(CPU)에 의해 제어되는 주변 장비, 소프트웨어와 펌웨어 같은 프로그램 요소, 이들과 관련된 각종 서비스(지원 서비스 포함), 그리고 관련 자원들이 모두 포함된다.

10) 2023년 3월 영국은 “민감정보가 접근되는 방식” 관련 위험을 제기하며 정부 전자 기기에서

2) 미국 내 이용 전면 금지

(1) 행정명령 13942호

미국 내에서 틱톡 이용을 전면 금지하려는 조치는 트럼프 행정부 1기에서부터 시작된다. 그러나 미국 내 틱톡 이용 전면 금지에 대하여 표현의 자유 침해 등을 이유로 소송이 제기되면서 트럼프 행정부 1기에서는 제대로 이행되지는 못한다. 2020년 8월 6일, 트럼프 대통령은 행정명령 13942호를 발표하여 미국 내 틱톡 이용을 처음으로 금지하고자 하였다. 동 행정명령은 틱톡이 이용자의 위치정보 및 검색 내역 등 방대한 양의 정보를 자동으로 수집하고, 이렇게 수집된 미국 이용자의 개인정보 및 전유(專有) 정보에 중국 공산당이 접근하는 것이 가능하다는 우려를 배경으로 마련되었다. 상업적 주체를 통한 중국 공산당의 이와 같은 접근으로 중국이 미국 연방직원 및 하도급자의 위치를 추적하거나, 협박 목적으로 개인정보의 기록물을 구축하고, 산업 첩보를 수행할 수 있다는 점에서 미국 안보에 위협이 된다는 것이다(E.O. 13942 Preamble). 이에 행정명령 13942호에서는 미국 관할 내 모든 자가 행하는 거래 또는 미국 관할 내 모든 재산에 관한 거래 중, 바이트댄스 및 이들의 자회사와의 거래로 상무부가 본 행정명령에 따라 식별한 거래가 금지된다. 2020년 9월 상무부는 (i) 앱스토어를 통한 틱톡 앱, 구성 코드, 앱 업데이트 배포, (ii) 틱톡 모바일 앱 기

틱톡 이용을 금지하였으며 캐나다도 프라이버시 및 보안 우려를 제기하며 정부 기기에서 틱톡 이용을 금지한다. 2023년 2월과 3월 유럽연합 차원에서도 유사한 금지가 도입된다. 2023년 2월 유럽집행위원회는 직원이 이용하는 기기에서 틱톡 이용을 금지하였으며, 3월 유럽의회도 그와 같은 금지에 동참한다. 2023년 4월 호주도 보안 우려를 제기하며 정부 이용 기기에서 틱톡 이용을 금지한다.

능을 위한 인터넷 호스팅 서비스, (iii) 틱톡 모바일 앱 기능을 위한 콘텐츠 딜리버리 네트워크 서비스, (iv) 틱톡 모바일 앱 기능을 위한 인터넷 트래픽 연결 서비스, (v) 다른 소프트웨어에서 틱톡 기능 사용을 금지되는 거래로 식별하였다(The U.S. DOC 2020). 그러나 이후 틱톡 이용자 등에 의한 소송으로 가처분이 인용되어 시행되지 못하다가 바이든 대통령 행정명령 14034호에 의해 동 행정명령은 폐지된다.¹¹⁾

(2) 해외 적성국 통제 앱으로부터 미국인 보호에 관한 법

행정명령 13942에 따른 틱톡 이용 금지에 대하여 제기된 소송과, 틱톡이 미국 내에서도 대중적으로 인기 있는 앱이라는 점을 고려하여 미국은 대통령 권한, 즉 행정명령이 아닌 의회 입법을 통해 틱톡을 포함한 해외 적성국이 통제하는 앱 이용을 제한한다. 2024년 4월 24일 바이든 대통령은 ‘해외 적성국 통제 앱으로부터 미국인 보호에 관한 법(Protecting Americans from Foreign Adversary Controlled Applications Act, PAFAC법)’이 포함된 미국 국가안보 관련 패키지 법률(H.R. 815)에 서명하였다. 사실상 미국 내 틱톡 이용을 금지하는 법률이다. 미국 내에서 (i) 해외 적성국이 통제하는 앱을 유통·유지·업데이트하기 위한 서비스를 제공하거나, (ii) 그를 위해 인터넷 호스팅 서비스를 제공하여 해외 적성국이 통제하는 앱을 유통·유지·업데이트하는 것을 불법

11) 틱톡뿐만 아니라 바이든 대통령 재임 직전인 2021년 1월 5일 트럼프 대통령은 행정명령 13971호를 발표하여, 알리페이(Alipay) 등 중국 연결 소프트웨어 앱을 개발하거나 통제하는 자 또는 이들 자회사와의 거래를 금지하였는데, 이 행정명령 역시 바이든 대통령 행정명령 14034호에 의해 폐지된다. Executive Order 13971 of 5 January 2021 on Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies, January 5, 2021.

으로 규정하였다(PAFAC법 제2(a)조). 여기서 ‘해외 적성국이 통제하는 앱’이라 함은 바이트댄스와 틱톡이 직간접적으로 운영하는 웹사이트, 데스크톱 앱, 모바일 앱, 또는 증강·몰입 기술 앱을 의미한다. 이 뿐 아니라, 해외 적성국이 통제하는 바이트댄스 자회사나 승계사, 또는 이들에 의해 직간접적으로 소유되거나 통제되는 실체가 직간접적으로 운영하는 경우의 것도 포함된다(PAFAC법 제2(g)(3)(A)조). 틱톡 이외에도 해외 적성국이 통제하는 대상 회사로서 대통령이 미국의 안보에 상당한 위협이 된다고 결정하는 경우 그들이 직간접적으로 운영하는 앱도 포함되게 된다(PAFAC법 제2(g)(3)(B)조). 사실상 미국 내 틱톡 이용을 전면적으로 금지한 것이다.

단, 이와 같은 금지가 발효하기 이전에 ‘적격 매각(qualified divestiture)’이 이루어지는 경우 이와 같은 금지는 적용되지 않는다(PAFAC법 제2(c)조). 이 법에 따른 금지는 본래 2025년 1월 19일 효력을 발휘하게 되었는데, 그때까지 틱톡 매각이 이루어지지 않으면, 미국 내 틱톡 이용이 금지되는 것이었다. 그러나 2024년 5월 7일 바이트댄스 유한회사와 틱톡 법인 등이 이 법이 1차 수정헌법을 위반한다고 주장하며 DC연방순회항소법원(US Court of Appeals for the D.C. Circuit)에 소를 제기하였다. 이 문제는 결국 연방대법원에서까지 다루어지게 되는데, 연방대법원은 2025년 1월 17일 이 법이 수정헌법에 위배되지 않는다는 취지의 판결을 내렸다.¹²⁾ 이후 트럼프 대통령은 네 차례 행정명령을 통해 PAFACA법 집행을 연기하고, 현재 2025년 12월 16일까지 틱톡 매각 시한이 설정되어 있는 상황이다(E.O. 14166; E.O. 14258; E.O.

12) TikTok Inc. v. Garland, Nos. 24-656 & 24-657 (U.S. Jan. 17, 2025)

14310; E.O. 14350). 또한, 최근 백악관은 틱톡 매각과 틱톡에 대한 미국 기업의 지배에 관한 협상 윤곽을 공개하기도 하였다(BBC 2025/9/21).

3. 개인정보 수반 거래 금지 또는 제한

미국은 개인데이터 수반 거래를 통해 중국, 러시아, 북한, 이란과 같은 적성국으로 미국인의 개인데이터가 흘러 들어가는 것을 차단하고자 이들 국가 및 이들 국가가 통제하는 실체와 개인데이터 수반 거래를 금지하거나 제한하는 규제를 도입하였다. 이하에서 다룰 행정명령 14117호와 ‘해외 적성국으로부터 미국인 데이터 보호에 관한 법(Protecting Americans’ Data from Foreign Adversaries Act, PADFA법)’에서 그와 같은 금지와 제한의 근거를 제공한다. 이들 규제는 틱톡 혹은 바이트댄스라는 특정 서비스나 특정 기업을 겨냥하기 보다, 적성국과 적성국이 통제하는 실체와의 개인데이터 거래를 포괄적으로 금지하거나 제한한다.

1) 행정명령 14117호

바이든 대통령이 2024년 2월 28일 발표한 행정명령 14117호는 지금까지 발행된 행정명령 중 해외 적성국이 미국인의 민감 개인데이터에 접근함으로써 나타나는 국가안보에 대한 위협을 가장 구체적으로 제한하고 있는 행정명령이다. 동 행정명령은 바이든 대통령 시기 발행되었으나, 제2기 트럼프 행정부에 들어서도 여전히 폐지되지 않고 유지되고 있다. 행정명령 14117호는 이른바 ‘우려국’의 미국인의 민감 개인데이터에 대한 접근이 미국 안보에 수용할 수 없는 위협을 초래하는 경우, 그러한 접근을 제한하는 것을 기본 방침으로 삼고 있

다. 이를 위해 동 행정명령은 미국인이 미국의 우려국 또는 우려국이 통제할 수 있는 주체와 민감 개인데이터를 수반하는 거래를 행하는 것을 금지하거나 제한한다.

구체적으로 살펴보면, 행정명령 14117호에 따라 금지되거나 제한되는 거래는 미국인과 우려국 또는 대상인 사이의 대량 민감 개인데이터 또는 정부 데이터를 수반하는 대상 거래이다. 행정명령 14117호에 따라 법무부가 금지되거나 제한되는 거래에 관한 주요 사항을 결정할 권한을 가지는데, 2024년 12월 법무부에서는 그와 같은 결정을 담은 최종규칙을 발표하였다(The U.S. DOJ 2024). 그에 따르면, ‘우려국’은 중국, 쿠바, 이란, 북한, 러시아, 베네수엘라를 의미한다. 또한 ‘대상인’은 우려국 등이 직간접적으로 50% 이상 소유하거나, 우려국의 법률에 따라 설립 또는 등록되거나, 우려국에 주 사업장이 있는 외국 법인, 우려국 영토 관할권 내 주로 거주하는 외국 개인 등을 의미한다. ‘민감 개인데이터’는 (i) 대상 개인 식별자, (ii) 위치 또는 관련 센서 데이터, (iii) 생체 식별자, (iv) 휴먼 오믹(human 'omic) 데이터,¹³⁾ (v) 개인 건강 데이터, (vi) 개인 금융 데이터를 의미한다.¹⁴⁾ ‘정부 데이터’는 민감 개인데이터 중에서도 (i) 연방정부 전현직 직원 또는 하도급

13) 휴먼 오믹(human 'omic) 데이터는 인간 유전체 데이터(human genomic data), 인간 후성 유전체 데이터(human epigenomic data), 인간 단백질체 데이터(human proteomic data), 인간 전사체 데이터(human transcriptomic data)를 의미한다. (The U.S. DOJ 2024, Section 202.224)

14) 단, 대중에게 합법적이고 일반적으로 이용될 수 있는 공공 기록물의 성격을 가진 데이터(법원 기록 또는 그 밖의 정부 기록), 국제긴급경제권법(International Emergency Economic Powers, IEEPA) 제203조(b)항(1)호 범위 내 있는 개인 통신, IEEPA 제203조(b)항(3)호 범위 내 있는 정보 또는 정보 자료(예: 출간물, 영화, 포스터 등)는 민감 개인데이터 범위에서 제외된다.

자 및 전직 고위 공무원 관련 민감 개인정보, (ii) 전술한 자를 식별하는 데 이용될 수 있는 데이터 관련 민감 개인정보, (iii) 특정 민감 지역 관련 민감 개인정보를 의미한다. ‘대상 거래’는 데이터 중개,¹⁵⁾ 재화 및 서비스 판매 계약,¹⁶⁾ 고용 계약,¹⁷⁾ 투자 계약이다.¹⁸⁾ 흥미로운 점은 규제 대상 거래에 수반되는 민감 개인정보 ‘규모’ 기준이 민감 개인정보 유형 별로 설정되어 있다는 점이다. 단, 정부 데이터 수반 거래는 그 규모와 관계없이 모두 규제 대상이다.¹⁹⁾ 우려 국 또는 대상인과의 민감 개인정보 수반 대상 거래 중 전면 금지되는 대상 거래는 데이터 중개와 대량의 휴먼 오믹 데이터 수반 대상

15) 동 행정명령에서 ‘데이터 중개’는 개인정보 제공자에서 개인정보 수령자로의 데이터 판매나, 접근 허가, 또는 이와 유사한 상업거래로, 수령자가 당해 수집되거나 처리되는 정보와 관련되거나 관련될 수 있는 개인으로부터 직접 그 데이터를 수집하거나 처리하지 않은 경우를 의미한다(The U.S. DOJ 2024, Section 202.214).

16) ‘판매 계약’은 어떠한 자가 대가나 그 외 보상을 받고 클라우드 컴퓨팅 서비스를 포함한 재화나 서비스를 다른 자에게 제공하는 모든 계약이나 약정을 의미하며, 고용 계약은 제외된다(The U.S. DOJ 2024, Section 202.258).

17) ‘고용 계약’은 독립 계약자가 아닌 자격으로 대가나 기타 보상을 받고 어떤 사람을 위해 직접 업무를 수행하거나 직무 기능을 수행하는 모든 계약이나 약정을 의미한다. 여기에는 이사회나 위원회에서의 고용, 임원급 약정이나 서비스, 그리고 운영 차원의 고용 서비스가 포함된다(The U.S. DOJ 2024, Section 202.217).

18) ‘투자 계약’은 어떤 자가 대가나 기타 보상을 지급하여, 미국 내 위치한 부동산 또는 미국 법인에 대한 직간접적 소유 지분이나 권리를 취득하는 계약이나 약정을 의미한다(The U.S. DOJ 2024, Section 202.228).

19) 규제 대상 민감 개인정보 유형별 규모는 다음과 같다. 100명 이상의 미국인에 관한 인간 유전체(genomic) 데이터, 1,000명 이상의 미국인에 관한 기타 세 가지 유형의 휴먼 오믹(omic) 데이터, 1,000명 이상의 미국인에 대한 생체 식별자(biometric identifiers), 1,000개 이상의 미국 기기(장치)에 대한 정밀 위치정보, 10,000명 이상의 미국인에 대한 개인 건강 데이터 및 개인 금융 데이터, 100,000명 이상의 미국인에 관한 대상 개인 식별자, 또는 위의 데이터 유형들이 포함된 데이터셋 중, 해당되는 범주를 가운데 가장 낮은 기준(threshold)을 충족하는 어떤 조합의 데이터.

거래이다(The U.S. DOJ 2024, Section 202.301, 제202.302, 제202.303). 전면 금지되지는 않으나 제한되는 대상 거래는 판매 계약, 고용 계약, 투자 계약으로, 이들 거래 유형은 사이버인프라보안청(Cybersecurity and Infrastructure Agency, CISA)이 개발한 보안 요건을 충족하는 경우에만 제한적으로 거래가 허용된다.

틱톡을 운영하는 모회사 바이트댄스가 중국에 설립되어 있고, 중국이 동 행정명령에서 우려국으로 지정되어 있다. 이로써 행정명령 14117호는 틱톡 서비스 이용을 통해 미국인의 민감 개인데이터가 중국으로 이전되는 것을 규제하는 역할을 한다. 그러나 동 행정명령은 이보다 더 광범위하게 행정명령에서 미국의 우려국으로 지목된 국가로 미국인의 민감 개인데이터가 이전되는 것을 금지하거나 제한할 수 있는 근거를 제공한다. 특히 다음 세 가지 사항을 주목할 만 하다. 첫째, 일반 민감 개인데이터와 달리 전현직 공무원의 민감 개인데이터는 규모와 관계없이 규제 대상이 된다는 점이다. 이는 공무에 종사하는 자의 민감 개인데이터가 우려국에 흘러 들어가는 것을 특별히 규제하려는 미국의 노력을 시사한다.

둘째, 전면 금지되는 유형의 거래에 데이터 중개가 포함된다는 점이다. 미국에서는 데이터 중개업(data brokerage)이라는 개인정보 주체에게서 직접 개인정보를 수집하지 않고 개인정보를 사고파는 비즈니스가 활발히 이루어지고 있다. 데이터 중개자는 정보주체로부터 직접 개인정보를 수집하지 않고 모바일 앱, 온라인 서비스, 그리고 다른 데이터 중개자 등 다양한 출처로부터 개인정보를 수집한다(The U.S. House of Representative 2024). 미국 내 데이터 중개업의 성행은 연방법을 차원의 개인정보 보호에 관한 법률이 제정되어 있지 않고, 개별법 또는 주(州)법에서 파편적으로 개인정보 보호를 규율하고 있는 미국

의 특수한 법적 환경을 바탕으로 한다.²⁰⁾ 그러나 점차 미국은 데이터 중개업을 통해 중국으로 개인정보가 무분별하게 이전되는 것을 안보 위협으로 인식하고 이를 전면적으로 금지하기 시작한 것이다.

셋째, 대량 휴면 오믹 데이터 수반 대상 거래 역시 전면 금지되는 거래 유형에 포함되었다는 점이다. 휴면 오믹 데이터는 인간의 유전체, 후성유전체, 단백질체, 전사체에 관한 데이터를 의미한다(The U.S. DOJ 2024, Section 202.224). 사람의 유전체, 후성유전체, 단백질체, 전사체는 사람마다 고유하고 일생 동안 변하지 않는다. 특정 집단·민족·국가 단위의 휴면 오믹 데이터를 분석하여 이들을 대상으로 한 생물학적 공격 설계가 가능해진다는 점에서 우려국의 휴면 오믹 데이터 접근은 안보적 우려가 아닐 수 없다. 이와 같은 안보적 우려를 해소하고자 행정명령 14117호는 미국인의 휴면 오믹 데이터가 우려국으로 흘러가는 것을 차단하는 역할을 한다.

2) 해외 적성국으로부터 미국인 데이터 보호에 관한 법

데이터 중개를 통한 해외 적성국과의 미국인의 민감 개인정보 거래는 연방법률을 통해서도 금지된다. 2024년 4월 24일 바이든 대통령은 ‘해외 적성국으로부터 미국인 데이터 보호에 관한 법(Protecting Americans’ Data from Foreign Adversaries Act, PADFA법)’이 포함된 미국 국가안보 관련 패키지 법률(H.R. 815)에 서명하였다. 이 법에 따라,

20) 데이터 중개업에 관한 대표적 주(州)법은 2018년 제정된 버몬트주 데이터중개자법(Vermont Data Broker Act), 2019년 제정된 캘리포니아주 데이터중개자등록규정(Data Broker Registration Regulations), 2023년 제정된 오리건주 데이터중개자법(Oregon Data Broker Law) 등이 있다. 이들 데이터중개에 관한 주법은 데이터중개자에 대하여 등록의무 및 정보공개의무 등을 부과함으로써, 데이터 유통 과정의 투명성을 확보하고자 마련되었다.

데이터 중개자가²¹⁾ 해외 적성국 또는 해외 적성국이 통제하는 실체에 미국인의 민감 개인데이터를 판매, 허가, 대여, 거래, 이전, 배포, 공개, 접근제공, 또는 달리 이용 가능하게 하는 것이 불법으로 규정된다(PADFA 법 제2(a)조). 이와 같은 불법 행위는 연방무역위원회법상 불공정 또는 기만 행위 또는 관행으로 취급된다(PADFA법 제2(b)조). PADFA법에서 해외 적성국은 중국, 러시아, 북한, 이란을 의미한다.²²⁾ PADFA법에 따른 해외 적성국 대상 미국인의 개인데이터 중개업 제한은 행정명령 14117호 도입 배경과 마찬가지로 적성국의 소유·통제·관할 하에 있는 기업을 통해 적성국 정부가 그러한 기업이 제공하는 서비스를 이용하는 자의 정보에 접근할 수 있다는 우려를 배경으로 도입되었다.

IV. 한국에 주는 시사점

이상 미국의 틱톡 규제를 중심으로 미국의 데이터안보 정책을 검토하였다. 미국은 미국인의 개인정보가 상업적 주체를 통해 중국으로 이전되는 것을 제한하고자 행정부 및 입법부 권한을 활용하여 대미 투자 제한, 틱톡 이용 금지, 개인정보 수반 거래 금지 또는 제한과

21) PADFA법에서 “데이터 중개자”란, 미국 개인들로부터 직접 수집하지 않은 데이터를 대가를 받고 서비스 제공자로 활동하지 않는 다른 실체에게 판매, 라이선스 부여, 임대, 거래, 양도, 공개, 제공하거나 기타 방식으로 이용하도록 하는 실체를 의미한다. PADFA법, 제2(c)(3)조.

22) PADFA법에서 “해외 적성국”은 미국 연방법전 제10장 제4872(d)(2)조에 따른 국가를 의미하는데, 중국, 러시아, 북한, 이란이 포함된다. PADFA법 제2(c)(4)조.

같은 정책을 도입하였다. 미국과 한국의 지정학적 그리고 법제도적 상황은 다르기에, 미중 경쟁 맥락에서 미국이 실시하는 제도를 그대로 우리가 도입하여야 한다는 주장은 경계할 필요가 있다. 예컨대, 미국이 도입한 매각 조건부 틱톡 이용 전면 금지는 중국과 다양한 분야에서 협력을 유지하여야 하는 우리의 현실에서 채택하기 어렵다. 그러나 데이터안보 목적으로 미국이 도입한 대미 투자 제한과 개인정보 수반 거래 금지 또는 제한과 관련하여 평가할 때, 우리 국내 법제도 환경에서 개선할 부분이 발견된다.

1. 개인정보보호법의 역할과 한계

미국에는 연방법률 차원의 일반 개인정보보호법이 존재하지 않는다. 연방법률 차원에서는 분야별로 개인정보 보호에 관한 사항이 일부 규율될 뿐이다. 예컨대, 1974년 프라이버시법(Privacy Act)은 연방기관이 개인정보를 수집 및 이용하는 것을 규율하며, 건강보험 양도 및 책임법(Health Insurance Portability and Accountability Act, HIPAA)은 의료 서비스 제공자가 환자의 개인정보를 이용하는 기준에 대하여 규율한다. 또한, 일부 주에서는 해당 주의 거주민의 프라이버시를 보호하는 법률이 제정되어 있다. 캘리포니아주에서 시행 중인 캘리포니아 소비자 프라이버시법(California Consumer Privacy Act)이 대표적 사례이다. 동 법은 캘리포니아에 거주하는 소비자의 개인정보 처리에 관한 알권리, 삭제권, 정정권 등을 규정한다. 이처럼 미국은 연방법률 차원의 포괄적 개인정보 보호에 관한 법률이 존재하지 않아, 미국인은 이른바 데이터 수확(data harvesting)에 취약할 수 밖에 없는 환경을 가지고 있다고 평가된다(The U.S. House of Representative 2024).

이와 달리 개인정보보호법이 개인정보 보호에 관한 일반법으로 자리잡고 있는 우리나라에서는 해외 국가가 상업적 주체를 통해 한국에 거주하는 개인의 개인정보에 무분별하게 접근함으로써 초래되는 안보 위해가 어느 정도 제한된다. 특히 다음 세 가지 점에서 우리 개인정보보호법이 그러한 역할을 할 수 있다. 먼저, 우리 개인정보보호법은 개인정보의 수집, 이용, 제3자 제공, 목적 외 이용과 제공을 기본적으로 정보주체의 동의나 법률상 특별 규정이나 법령상 의무 준수를 위해 불가피한 경우 등에만 허용하고 있다. 또한, 민감정보와 고유식별정보는 기본적으로 처리가 금지되며(개인정보보호법 제23조 1항 및 동법 시행령 18조), 예외적으로 정보주체의 별도 동의가 있거나 법령에서 민감정보나 고유식별정보 처리를 요구하는 경우에만 처리가 허용된다(개인정보 보호법, 제23조 1항 및 제24조 1항). 이와 같은 개인정보 보호 규정으로 인해 미국과 달리 국내에서는 데이터 중개업이 성행할 수 없는 환경이다(김현경 2018, 258~259).

둘째, 개인정보의 국외 이전이 원칙적으로 제한된다. 개인정보처리는 예외적인 상황, 즉 (i) 정보주체의 별도 동의를 받거나, (ii) 법률, 조약 등에 국외 이전 관련 특별 규정이 있거나, (iii) 정보주체와의 계약 체결 및 이행을 위해 필요하거나, (iv) 개인정보보호위원회가 인정하는 인증을 받거나, (v) 개인정보가 이전되는 국가 또는 국제기구의 개인정보 보호 수준이 국내법상 보호 수준과 동등하다고 인정되는 경우에만 국외 이전이 가능하다. 특히 동등성 인정을 위해 개인정보보호위원회는 이전 대상국이 우리 개인정보보호법에서 정하는 개인정보보호원칙에 부합하고 정보주체의 권리를 충분히 보장하는 법령 등을 갖추고 있는지, 그와 같은 개인정보 보호체계를 집행할 독립 감독기관이 있는지, 피해 구제 절차가 실질적으로 보호되는지 등을 고

려한다. 따라서 개인정보가 이전된 국가 정부가 독립된 감독체계 없이 무분별하게 이전된 개인정보에 접근할 수 있는 체계를 유지하고 있는 국가라면 우리법상 동등성 평가 기준을 충족하지 못할 가능성이 높다.

셋째, 우리 개인정보보호법은 역외적용된다. 즉, 우리 개인정보보호법은 특정한 경우 해외 사업자에게도 적용된다. 국내에 설립되지 않은 해외 사업자라 하더라도 (i) 한국 정보주체를 대상으로 재화나 서비스를 제공하는 경우, (ii) 해외 사업자의 개인정보처리자가 한국 정보주체에 영향을 미치는 경우, (iii) 한국 영토 내에 해외 사업자의 사업장이 존재하는 경우 개인정보보호법의 적용 대상이 된다(개인정보보호위원회 2024, 9). 이 경우 해외 사업자는 개인정보보호법상 모든 규정을 준수하여야 한다(개인정보보호위원회 2024, 17). 따라서 정보주체가 해외 사업자에게 자신의 개인정보를 직접 제공하는 경우라 하더라도 상기 적용 대상이 되는 해외 사업자는 우리 개인정보보호법상 개인정보 수집, 이용, 제3자 제공, 목적 외 이용과 제공, 국외이전에 관한 요건을 준수하여야 한다. 예컨대, 2024년 7월 개인정보보호위원회는 해외 사업자인 알리익스프레스에 개인정보 국외 이전(제공) 관련 규정 위반을 이유로 과징금 및 과태료를 부과하였다(개인정보보호위원회 보도자료 2024/7/25). 마찬가지로 해외 사업자 태무에 대해서도 국외 이전(처리 위탁), 주민등록번호 처리에 관한 우리 개인정보보호법상 규정을 위반하여 과징금이 부과된 바 있다(개인정보보호위원회 보도자료 2025/5/15). 또한, 딥시크에 관하여 개인정보보호위원회는 2025년 2월 15일 개인정보 처리방침상 미비한 부분을 일부 확인하여, 국내 앱 마켓 다운로드를 잠정 중단하였다(개인정보보호위원회 보도자료 2025/2/17). 이와 같은 조치들은 모두 국내 개인정보보호법이 해외 사

업자에게 적용되어 제재가 가해진 사례이다.

이처럼 미국의 경우와 달리 우리나라에서는 개인정보보호법이 어느 정도는 해외 국가가 상업적 주체를 통해 한국에 거주하는 개인의 개인정보에 접근함으로써 나타나는 안보 위협을 제한하는 역할을 할 수 있다. 그러나 그 한계에 대한 평가도 필요하다. 우리 개인정보보호법은 개인정보 처리에 관한 개인의 자유와 권리를 보호하기 위하여 마련된 법률이며(개인정보보호법 제1조), 국가안보를 위해 마련된 법률은 아니기 때문이다. 먼저, 안보 우려가 제기되는 국가로 국내 정보주체의 개인정보 이전을 우리 개인정보보호법에 근거하여 원천 차단하기는 어렵다. 우리 개인정보보호법에서는 개인정보 국외이전을 기본적으로 제한하고 있긴 하나 정보주체의 별도 동의를 근거 또는 정보주체와의 계약 체결 및 이행을 위해 개인정보처리자는 그 정보주체의 개인정보를 국외 이전이 가능하다. 개인정보 국외 이전 시 개인정보처리자에게 안정성 확보 조치 의무가 부과되어 있으나(개인정보보호법 시행령 제29조의10) 이 의무가 이전된 개인정보에 대한 해외 당국의 접근을 제한하기 위한 근거 조항으로 기능하기에는 한계가 있다. 또한 정보주체가 해외에서 제공하는 서비스를 이용하기 위해 직접 개인정보를 제공하는 경우도 있다.²³⁾ 이 경우 개인정보보호법이 역외적용되나, 정보주체가 직접 해외 사업자에 제공한 개인정보의 취급에 관하여 중국법과 우리법의 충돌이 발생할 수 있고, 우리 개인정보보

23) 이 경우 우리 개인정보보호법상 개인정보 국외 이전 규정의 대상이 되지 않는다. 우리 개인정보보호법상 개인정보 국외 이전 제한에 관한 조항은 개인정보처리자의 의무로 규정되어 있어, 정보주체가 직접 개인정보를 해외 사업자에 제공하는 경우는 이 규정의 대상이 되지 않기 때문이다. 물론 그럼에도 우리 개인정보보호법의 역외적용으로 해외 사업자에게 우리 개인정보보호법이 적용될 수 있다.

호법의 실질적 집행이 어려울 수 있다.

우리는 개인정보보호법 체계 내에서 데이터안보 문제를 적절히 다룰 수 있도록 노력을 기울일 필요가 있다. 주지한 바와 같이 개인정보보호법은 국가안보 목적으로 마련된 법률이 아니다. 그러나 우리가 데이터안보 문제를 지나치게 안보적 관점에서만 접근하는 것은 국가간 관계에서 부정적 영향을 초래할 수 있기 때문에, 개인정보보호와 프라이버시 보호 차원에서 접근하여 해결하려는 전략이 필요하다. 본 연구에서 주목하는 데이터안보 문제의 핵심은 개인정보가 상업주체를 통해 해외로 이전되는 것 그 자체가 아니라 이전되는 개인정보에 대한 이전국 정부 당국의 무분별한 데이터 접근 체계이다. 이는 국가안보 문제이기도 하나 정보주체의 개인정보에 관한 권리와 프라이버시권 보호와 직결되는 문제이기도 하다. 먼저 개인정보보호위원회 차원에서 중국 당국에 우리 국민 개인정보 보호에 관한 우리법 기준을 설명하고 준수를 적극 요구할 필요가 있다. 최근 개인정보보호위원회가 중국과 소통 창구를 마련하고 우리법 준수를 요청하는 등 노력을 기울이고 있는데 이는 바람직한 움직임이라 평가할 수 있다.²⁴⁾

둘째, 국가안보 관점에서 전현직 공무원 개인정보의 특별한 보호 필요성에 관한 평가도 필요하다. 미국의 행정명령 14117호에서는 개인정보 중 전현직 연방정부 직원의 개인정보 이전을 수반하는 대상

24) 2025년 5월 개인정보보호위원회는 중국과 첫 소통 창구를 마련하고 6월 중국 정부에 우리 국민 개인정보 관리 및 보호를 당부한 바 있다. 개인정보보호위원회 보도자료, “개인정보위, 중국 정부와 개인정보 보호 협력 논의” 2025년 6월 13일; 개인정보보호위원회 보도자료, “개인정보위, 중국과 첫 소통창구 열었다.”, 2025년 5월 28일.

거래는 그 규모와 관계없이 규제하고 있다. 전현직 연방정부 직원은 미국 정부 시설, 운영 등에 관한 내부 지식을 가지고 있기 때문에, 이들의 개인정보는 적성국이 악용하기에 유익한 표적이 되기 때문이다(The U.S. DOJ 2024, 1662). 우리나라의 국가공무원법 및 그 시행령 국가공무원 복무규정에 따라 전현직 공무원은 직무상 알게 된 비밀, 정책 수립 또는 사업 집행 관련 사항, 개인 신상이나 재산에 관한 사항을 누설하는 것이 금지된다. 그러나 전현직 공무원이 직무상 알게 된 정보가 아닌 이들의 개인정보 자체는 개인정보보호법에서 규정되는 수준을 넘어 특별한 보호를 향유하고 있지 못하다. 미국 보안요원이 사적으로 이용하는 상용 앱을 통해 보안요원이 수행하고 있던 고위급 정치인의 위치가 추적될 수 있다는 점이 문제된 바 있다는 점을 주지할 필요가 있다. 전현직 공무원이 사적으로 이용하는 상용 디지털 서비스를 통해 공무원의 개인정보가 해외로 이전될 경우 발생할 수 있는 안보 위해에 대한 평가도 필요한 것이다.

다만 개인정보보호법상 처리가 제한되는 특별 범주의 개인정보로 공무원의 개인정보 처리에 관한 특별 규정을 마련하는 것은 무리가 있다. 먼저 미국 행정명령 14117호에 따른 민감 개인데이터 수반 거래 금지 혹은 제안 의무의 대상이 되는 자는 ‘미국인(U.S. persons)’이다. 우리 개인정보보호법에서는 개인정보처리자의 의무를 중심으로 규정이 마련되어 있어 미국의 규제와 의무 수범 주체에서부터 차이가 있다. 뿐만아니라 서두에서 밝힌 바와 같이, 일반인의 개인정보보호 수준을 넘어 요구되는 공무원의 개인정보의 특별한 보호의 필요는 국가안보 보호를 위해 제기되는 사항으로 개인정보보호법의 목적과 부합하지 않는다. 또한, 특정 국가로 국가 공무원의 개인정보가 이전되는 것을 규제하기 위하여 ‘법률’ 수준의 규정을 마련하는 것도 국

가 간 관계에 부정적 영향을 미칠 우려가 있다. 앞서 주장한 바와 같이 협력이 필요한 국가를 대상으로 안보 문제를 노골적으로 제기하기보다, 개인정보나 프라이버시 보호 관점에서 데이터안보 우려를 해소하는 것이 기본 방침이 되어야 한다. 이를 종합하여 고려할 때 공무원이 준수하여야 할 행동지침의 수준으로 먼저 접근할 필요가 있다. 우려가 제기되는 국가가 통제하는 민간 주체가 제공하는 디지털 서비스를 공적 목적뿐 아니라 사적으로 사용하는 경우 초래될 수 있는 안보적 우려를 공무원 사회에 환기시키고, 문제된 서비스 이용을 삼가도록 권고할 필요가 있다.

2. 외국인 투자 국가안보위해 심사 요건 개선

외국인투자 촉진법에 따라 우리나라에서도 외국인의 투자가 국가의 안전과 공공질서의 유지에 지장을 주는 경우 그 투자는 제한된다(외국인투자 촉진법 제4조 2항). 동법 시행령에 따라 산업통상자원부장관(이하, 산업부 장관)이 외국인투자위원회 심의를 거쳐 외국인 투자가 국가안보위해에 해당하는 것으로 결정한 경우, 그 투자는 제한된다. 산업부 장관은 그와 같은 결정에서 다음 여섯 가지를 고려한다(외국인투자 촉진법 시행령 제5조 1항 2호 및 제5조의2 3항). 즉, 외국인이 이미 설립된 기업의 주식 등을 취득하여 해당 기업의 경영상 지배권을 실질적으로 취득하려 할 때, 산업부 장관이 그와 같은 외국인 투자가 (i) 방위사업법에 따라 방위산업물자 생산에 지장을 초래할 우려가 있는지, (ii) 대외무역법에 따른 수출허가 대상 물품 등이나 기술로, 군사목적으로 전용될 가능성이 높은지, (iii) 국가정보원법에 따라 국가기밀로 취급되는 계약 등의 내용이 공개될 우려가 있는지, (iv) 국제평화와 안

전유지를 위한 국제연합 등의 국제적 노력에 심각하고 중대한 지장을 초래할 우려가 있는 지, (v) 산업기술보호법에 따라 국가핵심기술 유출 가능성이 높은지, 또는 (vi) 국가첨단전략산업법에 따라 국가첨단전략기술 유출 가능성이 높은지를 결정하여 제한할 수 있다. 그러나 미국 방위생산물법상 외국인 투자의 안보 위해 심사에서처럼 외국인 투자로 인해 개인정보가 이전되어 발생할 수 있는 안보 위해는 고려되고 있지 않다.

물론, 이 경우에도 국내 개인정보보호법이 어느 정도 역할을 할 수 있다. 기존 국내 개인정보처리자가 수집한 개인정보를 영업양도 등을 통해 국외 양수자에게 직접 개인정보를 이전하는 경우, 개인정보 국외이전에 해당하여 앞서 다룬 개인정보보호법 제28조의 8에 따른 제한을 받는다. 또한 개인정보보호법 제27조에서 영업양도 등에 따른 개인정보 이전 제한에 관한 규정도 적용될 수 있다(개인정보보호위원회 2025, 193). 그러나 영업양도 등에 따른 개인정보 이전 제한 규정은 개인정보처리자 및 영업양수자의 고지 의무를 중심으로 규정되어 있어, 외국인의 대한 투자를 통한 안보 위해를 차단하는데 한계가 있다. 또한, 앞서 주지한 바와 같이 이와 같은 규정은 본질적으로 개인정보보호법상 개인의 자유와 권리를 보호하기 위해 마련된 규정이지 안보 목적으로 고려된 규정들은 아니므로 외국인의 투자를 통해 국내 정보주체가 해외로 넘어가 발생할 수 있는 안보 위해를 제한하는데 한계가 있다.

따라서 외국인투자 촉진법상 국가안보위해 심사시 고려 요소에 외국인의 대한 투자를 통해 우리 국민과 거주민의 개인정보가 국외 이전되어 발생할 수 있는 안보 위해를 추가할 필요가 있다. 외국인투자 촉진법 시행령 제5조 1항 2호에 우리 개인정보보호법에 따른 개인정

보에 해외 국가 접근하여 발생할 수 있는 안보적 우려를 추가하여 외국인 투자 국가안보위해 심사에서 이와 같은 우려를 심사할 법적 근거를 마련할 필요가 있다. 다만 제한하고자 하는 개인정보 유형, 규모 등 최종 결정 권한은 외국인투자위원회 심의를 거쳐 심사의 유연성과 전문성을 제고하도록 할 필요가 있다. 외국인투자위원회 위원에 국가정보원이 지명하는 차장이 포함되기 때문에(외국인투자 촉진법 제 27조 2항), 안보 관점 평가가 가능할 것으로 보이나, 개인정보 보호에 전문화된 위원은 현행 외국인투자위원회 위원에 포함되어 있지 않다. 따라서 외국인투자위원회 구성에 관한 조항에 개인정보 보호에 전문화된 위원이 보충될 필요가 있다.

3. 공통 가치 기반 디지털경제 협력 모색

데이터안보 문제는 국가안보 관점에서만 단편적으로 평가되는 경우 해결될 수 없다. 데이터에 경제, 사회, 정치적으로 아주 다양한 이익이 결부되어 있기 때문이다. 예컨대, 디지털 개인정보는 정보주체의 기본권 보호 차원에서 보호되며, 영업기밀과 같은 기업의 전유 정보 역시 지식재산으로 보호된다. 또한, 군사기밀 등 기밀 정보는 국가 안보를 위해 보호된다. 한편, 국가는 정보활동을 위해 또는 범죄 수사 등 법 집행을 위해 데이터에 접근하기도 한다. 또한 디지털경제 활성화를 위하여 데이터 원활한 이전과 활용도 강조되고 있다. 데이터의 보호와 활용이 다양한 이익과 결부되어 강조되는 탓에 양자는 충돌의 관계에 있기도 하다. 글로벌 차원에서 본다면, 자연인이나 법인의 권리 보호를 위한 것이든 안보를 위한 것이든 일국이 데이터 보호를 위해 기본적으로 취하는 조치는 데이터가 국경을 넘어 타국으로 이

동하는 것을 제한하는 것이다. 그러나 국가는 디지털경제 발전을 통한 경제 성장과 혁신을 위해 데이터의 자유로운 국경 간 이전을 보장해야 하기도 한다.²⁵⁾ 국가의 데이터안보 전략은 위와 같은 다양한 이익을 고려하여 마련되어야 한다.

흥미로운 점은 데이터를 둘러싼 다양한 이익이 상호 간 고정불변의 관계에 있는 것은 아니라는 점이다. 여전히 데이터 기반 신기술이 발전하고 있기 때문이다. 대표적으로 자국 데이터 기반 산업의 글로벌 확장을 위해 데이터의 자유로운 국경 간 이전을 강조해왔던 미국의 입장 변화가 그를 보여준다. 미국의 데이터의 자유로운 국경 간 이전의 강조는 특히 미국, 멕시코, 캐나다 사이의 기존 자유무역협정인 북미자유무역협정(North American Free Trade Agreement)을 개정한 미국-멕시코-캐나다 자유무역협정(US-Mexico-Canada Agreement) 디지털 무역 챕터에 반영되어 있다. 아울러 세계무역기구(World Trade Organization, WTO) 차원에서 추진되던 디지털무역 협상 초반 논의에서도 이러한 입장은 유지되었다. 그러나 2023년 10월 미국 무역대표부는 “충분한 정책 권한” 확보를 위해 이와 같은 기존 입장을 철회하였고, 2024년 WTO 디지털무역 협정문 채택에 참여하지 않았다. 데이터를 둘러싼 국가의 정책 권한을 폭넓게 확보하기 위해 미국이 기존의 데이터 자유방임주의적 입장을 철회한 것이다(박주희 2024, 61; 이효영 2024, 8).

25) 국경 간 데이터 이전의 자유가 이와 같이 경제적 혜택에 기여하더라도, 국가는 다양한 이유로 국경 간 데이터 이전을 제한하는데, OECD는 국경 간 데이터 이전 제한 근거로 (i) 프라이버시 및 개인정보 보호, (ii) 지식재산권 보호, (iii) (법집행 등) 규제, (iv) 국가안보, (v) 사이버보안, (vi) 디지털산업 정책을 꼽았다. OECD, “Fostering Cross-border Data Flows with Trust,” OECD Digital Economy Papers, No. 343, December 2022, p. 13.

또한, 인공지능의 부상은 개인정보보호와 국가안보 사이의 관계를 변화시켰다고 하여도 과언이 아니다. 사실 개인정보보호를 통한 정보주체의 자유와 권리의 추구와 국가안보는 대책의 관계에 있는 것으로 인식되곤 하였다. 우리 개인정보보호법과 유럽연합의 일반개인정보보호규칙에서는 정보주체의 개인정보보호에 관한 권리를 국가안보를 이유로 제한할 수 있도록 허용하는 규정을 두었다는 점이 이를 증명한다(개인정보보호법 제58조 2항; GDPR 제23조). 그러나 앞서 다른 데이터안보 우려로 인해 개인정보의 보호가 결국 국가안보에도 기여할 수 있다는 점 역시도 최근 강조되고 있다. 이로 인해 연방법 차원의 개인정보보호법이 없는 미국에서조차도 개인정보보호에 관한 연방법률 제정의 필요성이 제기되기도 하였다(Duffy and Fendorf 2024).

데이터안보와 관련하여 특히 디지털경제 이익과의 조화를 모색할 필요가 있다. 최근 미국과 중국에서 목격되는 인공지능 발전에 자극 받은 여러 국가에서 인공지능 기반 성장을 적극 추진하고 있다. 인공지능 기반 성장을 위해서는 국내에서 그리고 국제적으로 데이터 이전과 활용이 원활히 이루어져야 한다. 그러나 앞서 주지한 바와 같이 데이터안보에 관한 우려는 데이터의 국경 간 이전을 제한하는 동인이 된다. 따라서 글로벌 차원의 협력과 노력 없이는 데이터안보와 디지털경제의 절충 지점을 모색하기 어렵다. 글로벌 환경에서 다자주의, 법치주의 등이 위기에 직면한 상황이기는 하나, 우리에게 다른 대안이 있는 것은 아니다. 우리는 오늘날 제기되는 데이터안보 문제의 지점을 주목하고 국가안보와 디지털경제 사이의 절충을 모색하기 위해 글로벌 차원의 노력을 기울여야 한다.

그러나 이와 같은 글로벌 차원의 노력을 실행하기 위해서는 필연적으로 민주주의 진영과 권위주의 진영 중 양자택일 선택의 상황에

직면할 수 밖에 없다. 주지한 바와 같이 틱톡 규제를 통해 부각되는 데이터안보 문제의 핵심은 해외 정부 당국이 상용 디지털서비스 제공자를 통해 해당 디지털서비스 이용자 정보에 접근하는 것에 관한 우려이다. 일국은 한편 자국에서 사업을 영위하는 상업적 주체가 보유한 데이터에 법 집행이나 안보를 위해 접근할 정당한 권한을 갖는다. 문제는 그와 같은 정부 당국의 접근 체계에 있어 민주주의 진영과 권위주의 진영 사이에 상당한 차이가 존재한다는 점이다. 민주주의 진영은 민간 주체 보유 데이터에 정부가 접근하는 것에 관하여 일정 수준의 공통된 원칙을 공유하고 있다. 그 원칙은 대표적으로 경제협력개발기구(OECD) 차원에서 마련된 ‘민간 주체 보유 개인정보 정부 접근에 관한 선언’에 언급된 주요 원칙에 반영되어 있다(OECD 2022). 동 선언에는 민간 주체가 보유한 개인정보에 국가의 정부 당국이 접근하는 체계에 관한 원칙으로 (i) 법적 근거, (ii) 목적의 정당성 (iii) 승인, (iv) 데이터 취급, (v) 투명성, (vi) 감독, (vii) 구제라는 일곱 가지 원칙을 담고 있다.²⁶⁾ 이들 원칙은 인권, 민주주의, 법치 등을 고려하여 마련되었다. 그러나 권위주의 진영은 이와 같은 원칙의 준수가 어렵다. 예컨대, ‘목적의 정당성’ 원칙은 정부 기관의 데이터 접근이 정당한 목적(예: 안보)에 비해 과도하지 않은 방식으로 수행되며, 필요성, 비례성, 합리성 그리고 정부 기관의 데이터 접근의 오남용 위험으로부터 보호를 위한 그 외 기준에 따를 것을 요구한다. 중국의 국가정보

26) 호주, 오스트리아, 벨기에, 캐나다, 칠레, 콜롬비아, 코스타리카, 체코, 덴마크, 에스토니아, 핀란드, 프랑스, 독일, 그리스, 헝가리, 아이슬란드, 아일랜드, 이스라엘, 이탈리아, 일본, 한국, 라트비아, 리투아니아, 룩셈부르크, 멕시코, 네덜란드, 뉴질랜드, 노르웨이, 폴란드, 포르투갈, 슬로바키아, 슬로베니아, 스페인, 스웨덴, 스위스, 튀르키예, 영국, 미국, 그리고 유럽연합이 이 선언에 참여하였다.

법(国家情报法), 반간첩법(反间谍法), 데이터안보법(数据安全法)에 따른 중국 당국의 데이터 접근이 국가안전 보호, 간첩활동 방지, 데이터안보 확보라는 목적의 정당성이 인정된다할 수 있겠으나, 필요·비례성에 관한 구체적 요건이 부재하다. 또한 ‘감독’ 요건은 정부 접근이 이와 같은 법적 체계를 준수하도록 보장하기 위한 효과적이고 공정한 독립 감독 체계를 유지할 것을 요구한다. 그러나 상기 중국 법률에 따른 감독 체계는 행정부 내부 통제 위주로 작동하여, ‘독립된’ 감독 체계라 하기 어렵다. 이처럼 데이터안보와 디지털경제 이익과의 조화는 민간 주체 보유 데이터에 대한 정부 접근 원칙에서 우리와 공통된 접근법을 취하는 국가와의 연대를 통해 가능하다. 민주주의, 법치, 인권 등 가치를 공유하고 있는 국가와 민간 주체 보유 데이터 접근에 관한 글로벌 신뢰를 제고하는 것이 데이터안보와 디지털경제 사이의 절충을 모색할 수 있는 최선의 방법이 될 것이다.

V. 결론

이상 본 연구는 미국의 틱톡 규제를 중심으로 제기되는 데이터안보 우려의 배경을 짚어보고 미국의 대응에 비추어 우리의 데이터안보 현황을 평가해 보았다. 미국은 틱톡 규제를 위해 대미 투자 제한, 틱톡 이용 금지, 개인정보 수반 거래 금지 또는 제한과 같은 조치를 도입하였다. 이와 같은 조치는 궁극적으로 중국이 디지털서비스를 제공하는 자국의 상업적 주체를 통해 그 서비스를 이용하는 미국인의 개인정보에 접근하는 것을 제한하기 위하여 마련되었다. 이와 같은 미국의 틱톡 규제 조치는 우리에게 다음 세 가지 주요 시사점을

제공한다. 먼저, 연방법률 차원의 일반 개인정보보호법이 존재하지 않는 미국의 경우와 달리 한국에서는 개인정보보호법이 개인정보 보호에 관한 일반법으로 기능하고 있어 해외 국가가 상업적 주체를 통해 한국에 거주하는 개인의 개인정보에 무분별하게 접근함으로써 초래되는 안보 위험이 어느 정도 제한된다. 다만 개인정보보호법은 개인의 자유와 권리를 보호하기 위하여 마련된 법률이지 국가안보 혹은 데이터안보를 위해 마련된 법률은 아니기에, 개인정보보호법이 우리나라의 데이터안보에 있어 수행하는 역할의 한계를 평가하고 미비점을 개선할 필요가 있다. 둘째, 외국인의 대한 투자를 통해 개인정보가 해외로 이전되어 나타나는 안보 위험이 투자 심사에서 고려될 수 있도록 우리나라의 외국인투자 촉진법상 외국인 투자 국가안보위해 심사 고려 요소를 검토할 필요가 있다. 셋째, 우리의 데이터안보 전략은 데이터와 관련한 다양한 이익, 특히 디지털경제 측면을 고려하여 수립되어야 한다. 디지털경제 성장은 데이터의 원활한 국경 간 이전을 통해 실현되므로, 이전된 데이터에 대한 정부 접근에 대하여 공동의 가치에 기반하여 유사한 접근법을 가지는 국가와의 연대를 통해 데이터 관련 안보 우려 해소와 함께 디지털 혁신과 경제 성장을 모색하여야 한다.

〈참고문헌〉

- 개인정보보호위원회, 2024, 해외사업자 개인정보 보호법 적용 안내서.
- 개인정보보호위원회, 2025, 개인정보 처리 통합 안내서.
- 개인정보보호위원회 보도자료, 2024, 알리익스프레스에 개인정보 보호법 위반으로
19억 7,800만원 과징금 부과 (7월 25일).
- 개인정보보호위원회 보도자료, 2025, ‘답시크 앱’ 국내 서비스, 잠정 중단 후 개선 보완
키로 (2월 17일).
- 개인정보보호위원회 보도자료, 2025, 국외이전 규정 등 개인정보 보호법 위반한 테무
에 13억 6,900만 원 과징금 부과 (5월 15일).
- 김상배, 2020, “데이터 안보와 디지털 패권경쟁: 신흥안보와 복합지정학의 시각,” 『국가전략』 제26권 2호, 5-34.
- 김현경, 2018, “미국 ‘데이터 브로커’ 제도의 국내법적 함의,” 『경제규제와 법』 제11권 제2호, 248-268.
- 박주희, 2024, “인공지능 시대 국가안보 목적 개인정보 이전 제한의 디지털경제 규범
쟁점 검토,” 『국제법학회논총』 제69권 4호, 35-75.
- 이효영, 2024, “데이터안보와 국제통상: 현안과 시사점,” 국립외교원 주요국제문제분석
석 (7월 3일).
- Belfer Center for Science and International Affairs (Belfer Center), 2025,
Critical and Emerging Technologies Index.
- Corbet, Sylvie, 2024, “Fitness app Strava gives away location of Biden, Trump
and other leaders, French newspaper says,” AP (October 29).
- Duffy Kat and Fendorf Kyle, 2024, “In the Age of AI, Personal Data Security Is
National Security”, Council on Foreign Relations (April 1).
- Executive Order 13942 of 6 August 2020 on Addressing the Threat Posed by
TikTok and Taking Additional Steps to Address the National
Emergency with Respect to the Information and Communications

- Technology and Services Supply Chain, August 6, 2020.
- Executive Order 13971 of 5 January 2021 on Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies, January 5, 2021.
- Executive Order 14083 of September 15, 2022 on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States, September 15, 2022.
- Executive Order 14166 of January 20, 2025 on Application of Protecting Americans from Foreign Adversary Controlled Applications Act to TikTok, January 20, 2025.
- Executive Order 14258 of April 4, 2025 on Extending the TikTok Enforcement Delay, April 4, 2025.
- Executive Order 14310 of June 19, 2025 on Further Extending the TikTok Enforcement Delay, June 19, 2025.
- Executive Order 14350 of September 16, 2025 on Further Extending the TikTok Enforcement Delay, September 16, 2025.
- Hazelrig, Kirsten, 2024, "Surveillance technologies are imbedded into the fabric of modern life—the Intelligence Community must respond, MITRE.
- Iati, Marisa and Boorstein, Michelle, 2021, "Case of high-ranking cleric allegedly tracked on Grindr app poses Rorschach test for Catholics," The Washington Post (July 21).
- Lewis, James A., 2024, "TikTok and National Security", CSIS (March 13).
- Needham, Kirsty, 2020, "Special Report: COVID opens new doors for China's gene giant," Reuters (August 5).
- OECD, 2022, "Fostering Cross-border Data Flows with Trust," OECD Digital Economy Papers, No. 343.
- OECD, 2022, Declaration on Government Access to Personal Data Held by

Private Sector Entities.

Rawnsley, Jessica and Jamali, Lily, 2025, “US says ‘framework’ for TikTok ownership deal agreed with China,” BBC (September 16).

Rubio, Marco, 2019, Letter to Secretary Steve Mnuchin, (9 October).

The U.S.–China Economic and Security Review Commission (The Commission), 2024, Report to Congress (November).

The U.S. Department of Commerce (The U.S. DOC), 2020, Identification of Prohibited Transactions to implement Executive Order 13942 and address the threat posed by TikTok and the National Emergency with respect to the information and communications technology and services supply chain (September 24).

The U.S. Department of Defense (The U.S. DOD), 2015, The Department of Defense Cyber Strategy.

The U.S. Department of Justice (The U.S. DOJ), 2024, Final Rule to Address Urgent National Security Risks Posed by Access to U.S. Sensitive Personal and Government-related Data from Countries of Concern and Covered Persons (December 27).

The U.S. House of Representative (The Committee on Energy and Commerce), 2024, Report on Protecting Americans’ Data from Foreign Adversaries Act of 2024 (March 11).

The U.S. National Counterintelligence and Security Center (The U.S. NCSC), 2021, China’s Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security (February).

The Office of the Director of National Intelligence (ODNI), 2024, National Counterintelligence Strategy.

The Office of Management and Budget (OMB), 2023, Memorandum for the Heads of Executive Departments and Agencies, “No TikTok on

Government Devices” Implementation Guidance, M-23-13, (February 27).

The White House, 2023, National Cybersecurity Strategy (March).

Wright, George, 2025, “White House outlines TikTok deal that would give US control of algorithm,” BBC (September 21).

U.S. Regulatory Response to TikTok and its Implications for Data Security of South Korea

Joohui Park | National Security Research Institute

The proliferation of cross-border data flows, namely digital trade, accentuates the necessity of examining the mechanisms through which national governments access such data via commercial entities handling transferred data, from the perspective of national security. Particularly as China's digital industry growth has materialized, the United States has raised security concerns regarding Chinese authorities' access to user data through Chinese digital service providers. A quintessential case exemplifying American recognition of and proactive response to such data security threats is the regulation of TikTok. The data security matter surrounding TikTok has predominantly been evaluated within the context of Sino-American hegemonic competition. However, as digital trade intensifies progressively and diverse overseas digital services permeate our quotidian life, this issue should not be reductively understood merely as a dimension of bilateral hegemonic rivalry between the United States and China. Rather, it must be apprehended as a universal agenda of data security engendered by transnational data flows—an emerging security issue confronting diverse nation-states. Accordingly, this study endeavors to elucidate the data security concerns articulated centering on American regulation of TikTok, diagnose the current state of South Korea's data security in light of the U.S. response, and derive policy implications regarding the direction of data security strategy that South Korea should pursue henceforth.

Keyword Data Security, TikTok, Personal Data Protection, Artificial Intelligence, US-China Competition, Digital Trade, Cross-Border Data Flow