국가전략, 제26권 2호 2020년 여름호, 5~34.

데이터 안보와 디지털 패권경쟁:
신흥안보와 복합지정학의 시각*

김 상 배**

❖ 요 약 ❖

최근 세계 주요국들이 벌이는 디지털 패권경쟁의 과정에서 '데이터'의 중요성이 강조되고 있다. 특히 데이터 문제를 국가안보의 관점에서 이해하기에 이르렀다. 그러나 오늘날 데이터 안보는 전통 군사안보와는 다른 메커니즘을 통해서 안보문제가 된다. 빅데이터 시대의 도래가 그러한 차이를 낳았다. 빅데이터 권력의 확산은 사생활 침해와 개인정보 보호에 대한 논란을 야기했다. 사이버 공격의 증대는 데이터 유출에 대한 '안보화' 논란을 낳았으며 테러색출을 내세운 데이터 감시를 정당화하고 있다. 다국적 기업들의 초국적 데이터 유통은 데이터 주권의 수호라는 관점에서 견제 받고 있다. 이러한 가운데 데이터 안보는 강대국들의 동맹과 연대외교의 쟁점이 되었으며, 정보기관 네트워크나 군사 정찰위성을 통한 데이터 수집 활동의 중요성도 커졌다. 전통 군사안보 분야에서도 빅데이터 역량은 미래전 수행의 핵심요소가 되었다. 이러한 과정에서 논란이 되는 데이터는 그 자체가 국가안보와 직접적으로 관련된 '내용'의 것만이 아니라, 양적으로 늘어나고 질적으로 연계되는 메커니즘을 거치면서 디지털 패권경쟁의 지정학적 쟁점으로 창발(創發, emergence)하는 성격의 데이터이다. 이 글은 신흥안보(emerging security)와 복합지정학(complex geopolitics)의 시각을 원용하여 데이터 안보의 세계정치를 분석하고 그 국가전략적 함의를 살펴보았다.

핵심어: 데이터 안보, 안보화, 데이터 주권, 디지털 패권, 신흥안보, 복합지정학

Ⅰ. 머리말

첨단부문으로서 4차 산업혁명 분야의 주도권을 둘러싸고 세계 주요국들의 디지털 패권경쟁이 한창이다. 이러한 경쟁의 과정에서 최근 부쩍 '데이터'의 중요성이 강조되고 있다. 단순히 '정보를 다루는 기술(IT)'의 시대가 가고 이제는 '데이터를 다루는

DOI: 10.35390/sejong.26.2.202005.001
* 이 논문은 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2016S1A3A2924409)
** 서울대학교 정치외교학부 교수

기술(DT)'의 시대가 도래 했다고 한다. 반도체가 산업의 '쌀'이었다면 데이터는 산업의 '원유'라고 비유되기도 한다. 데이터는 단순한 기술과 경제의 논제를 넘어서 국제정치학의 관심사로도 자리 잡아가고 있다. 데이터 자원의 확보와 데이터 경제의 활성화는 국가전략을 논하는 데 빼놓을 수 없는 요소가 되었다(김상배, 2015). 권력, 독점, 패권, 민주주의 등의 개념을 데이터에 적용해 보려는 시도가 늘어나는 현상은 데이터가 정치적 지배와 저항의 쟁점이 되었음을 보여준다. 국제관계의 영역에서도 데이터 주권이나 외교, 또는 안보와 국방 등과 같은 개념들이 출현하고 있다. 그야말로 '데이터를 지배하는 자가 세계를 지배하는 세상'이 오고 있다(리즈후이, 2019).

최근 데이터가 국제정치학의 어젠다로 부상한 데는 단순한 산업경쟁력의 이슈를 넘어서 포괄적인 국가안보의 문제로 데이터를 각인시킨 일련의 사건들이 영향을 미쳤다. 2013년 스노든 사건 이후 미국의 도청과 감시에 대한 경각심이 늘어나고, 2015년을 전후하여 사이버 안보 분야의 미중갈등이 고조되었으며, 2018-19년에는 이른바 화웨이 사태가 터졌다. 여기서 논란이 된 것은 그 자체가 국가안보와 직접적으로 관련된 '내용'을 가진 데이터만은 아니었다. 스몰 데이터 시대였다면 '속성론'의 차원에서 이해된 '안보 데이터'가 쟁점이었겠지만, 빅데이터 시대의 관건은 데이터가 안보문제로 쟁점화되는 과정, 즉 '데이터 안보화'의 문제였다. 미시적 차원에서 보면 개인정보나 집단보안의 문제에 불과한 데이터일지라도, 큰 규모의 수집과 처리 및 분석의 과정을 거치고 여타 비(非)안보 이슈들과 연계되는 와중에 거시적 차원에서는 국가안보에 치명적인, 숨어있던 '패턴'이 드러날 수도 있다는 것이었다.

모든 데이터를 거시적 국가안보의 시각에서 봐야 한다는 것이 아니다. 그보다는 오히려 특정 데이터가 국가안보 차원에서 인식되는 메커니즘에 주목하자는 것이다. 사실 데이터는 전통안보와는 다른 과정을 통해서 안보문제가 된다. 특히 빅데이터 시대의 도래가 그러한 차이를 낳았다. 빅데이터 경제의 확산은 사생활 침해와 개인정보 보호에 대한 논란을 야기했다. 테러행위 색출과 사이버 보안을 위한 빅데이터 감시는 빅브라더의 출현과 인권 침해 논란을 불러일으켰다. 다국적 빅데이터 기업들의 세계 시장으로의 진출은 국가주권 수호의 차원에서 데이터의 초국적 유통을 대하게 만들었다. 전통 군사안보 분야의 빅데이터 역량은 미래전의 승패를 가르는 핵심요인으로 인식되고 있다. 이러한 과정에서 국가안보에 치명적인 데이터는 미리

정해져 있는 것이 아니라, 양적으로 늘어나고 질적으로 연계되는 메커니즘을 거치면서 국가안보의 이슈로 창발(創發, emergence)한다.

여태까지 데이터 안보는 국제정치학 분야의 큰 관심사는 아니었다. 데이터 관련 연구가 있더라도, 데이터 안보보다는 데이터 경제에 주목했다. 주로 국제정치경제학의 시각에서 본 디지털 무역규범에 대한 연구가 그 사례이다. 최근에는 데이터의 초국적 유통에 대응하는 국가전략에 대한 관심이 커지면서, 그 과정에서 발생하는 각국 법제도의 정치적 충돌에 대한 연구가 늘어나고 있다. 이러한 와중에 그나마 진행된 데이터 안보의 국제정치학적 연구는, 다소 미시적 관점에서 다국적 빅데이터 권력에 의한 사생활 침해의 가능성을 탐구하거나, 아니면 거시적 관점에서 국가안보 관련 내용을 지닌 데이터의 대외적 유출을 우려하는 경향이 있었다. 이 글은 이러한 두 가지 연구경향을 넘어서 데이터의 미시적 쟁점이 거시적 국가안보의 문제로 창발하는 과정에 주목하는 이론적 시각을 모색하고자 한다.

데이터 안보는 미시적 안전이나 보호의 문제가 '양질전화'와 '이슈연계'의 임계점을 넘어서 집단보안과 국가안보의 문제로 창발하는 신흥안보(emerging security)의 대표적 사례이다. 다시 말해, 거시적 국가안보와 무관하게 보이는 데이터라도 빅데이터 환경을 배경으로 하여, 그 양이 늘어나고 복잡한 이슈와 연계되면서 어느 지점에 이르면 숨어 있던 국가안보적 함의가 드러날 수 있다. 이러한 시각에서 보면 다국적 기업들이 수집하는 비(非)군사적인 성격의 민간 데이터일지라도, 경우에 따라서는 매우 중요한 군사안보의 논란을 야기할 수도 있다. 실제로 이와 관련하여 최근 일국 단위에서 데이터 주권과 국가안보를 수호하는 문제가 쟁점으로 부상하고 있다. 4차 산업혁명 시대를 맞이하여 민간 분야에서 활용하는 데이터가 정치외교뿐만 아니라 군사안보의 차원에서 본 지정학 문제를 야기할 가능성이 커졌기 때문이다.

최근 데이터 안보의 문제는 강대국들이 벌이는 디지털 패권경쟁의 외양을 하고 전개되고 있다. 데이터 안보가 국제정치학의 지정학적 현안으로 인식되고 있다. 여기서 주의할 점은 전통안보 문제를 주된 연구대상으로 삼는 현실주의적 고전지정학의 관점에서만 데이터 안보를 봐서는 안 된다는 것이다. 최근 벌어지는 데이터 안보 경쟁에는 자유주의 국제정치이론의 시각에서 본 민간 행위자들의 참여와 이들의 협력을 통해서 구축하려는 제도와 규범에 대한 논의도 중요한 축을 이루고 있다.

안보 담론이나 정체성을 통해서 현실을 재구성하려는 구성주의 국제정치이론의 문제제기도 빼놓을 수 없다. 최근 첨단부문으로서 4차 산업혁명 분야에서 데이터 안보를 놓고 벌이는 미국과 중국, 유럽의 디지털 패권경쟁은 이러한 복합적인 면모를 보여주고 있다. 이 글이 복합지정학의 시각을 제안하는 것은 바로 이러한 이유 때문이다.

이 글은 크게 네 부분으로 구성되었다. 제2장은 데이터 안보와 디지털 패권경쟁을 보는 분석틀로서 신흥안보와 복합지정학의 시각을 소개하였다. 제3장은 빅데이터 권력과 사생활 침해, 사이버 공격과 데이터 유출, 그리고 기술패권 경쟁과 데이터 안보화로 이어지는 데이터 안보의 양질전화 과정을 살펴보았다. 제4장은 데이터 안보가 국제정치경제 분야의 비(非)군사 이슈와 연계되는 과정을 초국적 데이터 유통에 대응하는, 다양한 데이터 주권담론을 중심으로 살펴보았다. 제5장은 데이터 안보 이슈가 디지털 패권경쟁으로 창발할 가능성을 사이버 동맹형성과 연대외교, 정보기관의 데이터 감시와 감청, 군사 정찰위성과 '데이터 국방' 등의 지정학적 쟁점들을 중심으로 검토하였다. 끝으로, 맺음말에서는 이 글의 주장을 종합·요약하고 한국이 추구할 데이터 안보전략의 방향을 간략히 짚어 보았다.

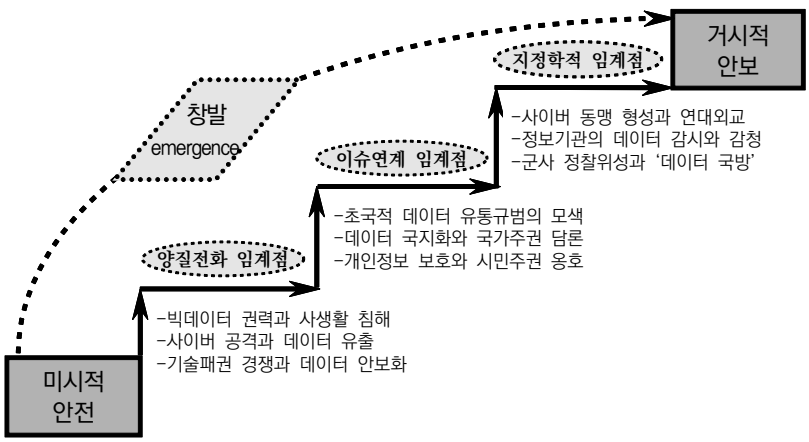
Ⅱ. 신흥안보와 복합지정학의 시각

4차 산업혁명 시대의 디지털 패권경쟁에서 데이터 변수가 차지하는 비중이 커지면서 데이터 자체가 야기하는 안보위협에 대한 우려도 커지고 있다. 〈그림-1〉에서 보는 바와 같이, 미시적 차원에서 시작된 데이터 관련 위협이 창발의 메커니즘을 따라서 양적으로 늘어나고 질적으로 복잡해지면서 민간 행위자뿐만 아니라 국가 행위자들 간의 이해갈등과 물리적 충돌을 예견케 하는 지정학적 이슈로 발전할 가능성이 있다. 이런 점에서 데이터 안보는 미시적 안전(安全, safety)의 문제가 집단 차원의 보안(保安) 문제를 거쳐서 거시적 안보(安保, security) 문제가 되는 신흥안보의 대표적 사례라고 할 수 있다(김상배, 2018a, p.40).

첫째, 데이터 안보 문제는 양적증대가 질적변화를 야기하는 '양질전화(量質轉化)'의 과정을 거쳐서 발생한다. 국가안보를 논할 정도는 아니고 사생활 침해 정도의

위협이지만, 그 양이 점차로 늘어나면서 거시적 안보와 연관될 가능성이 있다. 초국적 빅데이터 서비스는 개인정보를 도용하고 사생활을 침해할 가능성을 항시 갖고 있으며, 의도적인 사이버 공격을 통해서 개인정보와 지적재산이 절취되고 국가기밀을 담은 데이터가 유출될 수도 있다. 아직은 수면 아래 있는 문제이지만 '안보화'의 과정을 거쳐서 국가안보 문제로 쟁점화되는 일이 종종 벌어진다.

〈그림-1〉 신흥안보로서 데이터 안보의 창발



출처: 김상배(2018a) p. 40에서 응용

둘째, 데이터 안보 문제는 다양한 '이슈연계'의 메커니즘을 따라서 복잡화되는 성격을 갖는다. 다국적 기업들의 데이터 비즈니스는 초국적 데이터 유통규범의 형성을 모색하는데, 이 과정에서 여타 국제정치경제 이슈들과 복잡하게 얽히면서 그 데이터 안보적 면모가 확대된다. 특히 최근 데이터 안보 관련 이슈연계의 메커니즘은 빅데이터의 국경 간 이동과 이에 대한 국가적 통제 문제와 연계되는 양상을 보이고 있다. 특히 이는 데이터 주권의 옹호 논리와 연관되고 있다. 또한 초국적 데이터 비즈니스와 국내외 제도 및 규범 형성의 정치경제적 문제가 사회문화적 이슈와 연계되면서 개인정보 보호에 대한 시민주권 논의도 부상하였다.

끝으로, 데이터 안보의 문제가 지정학적 성격을 지닌 국가 간 갈등을 야기할 가능성이 높아지고 있다. 이는 역으로 기존의 지정학적 안보 문제가 데이터 안보 문제의

창발을 촉진하는 과정으로도 나타난다. 최근 테러행위 색출을 위한 인터넷 대량 감시를 둘러싸고 국가 간 갈등이 표출되었으며, 데이터 안보의 이슈가 동맹외교 및 연대외교의 추진과도 긴밀히 연결되었다. 또한 전통 군사안보 분야에서도 빅데이터 역량이 미래전 수행의 핵심이슈로 인식되고 있다. 이러한 지정학적 동학은 데이터 안보와 관련된 세계 주요국들이 벌이는 디지털 패권경쟁의 핵심적 현안으로 자리 잡아가고 있다.

이러한 관점에서 보면 신흥안보로서 데이터 안보는 전통안보의 지정학적 문제들로 비화될 가능성을 내포하고 있다. 특히 국가 간 분쟁과 동맹, 그리고 전쟁과 같이 '지정학적 임계점'에 다다르는 종류의 갈등을 내포하고 있는 데이터 안보의 위협은 고전지정학적 연구의 관심사가 아닐 수 없다. 고전지정학은 물질적 자원권력의 분포와 이에 대한 지리적 접근성이라는 시각에서 국가 행위자들이 주로 전통안보 분야에서 벌이는 경쟁에 주목해 왔다. 이는 국제정치의 역사에서 패권국과 도전국이 벌이는 지정학적 권력경쟁과 여기서 파생되는 세력전이의 과정에 주목하는 현실주의 국제정치이론의 논의와 통한다(Mead, 2014).

그러나 데이터 안보의 세계정치를 단순히 전통적인 고전지정학의 시각에서만 규정할 수는 없다. 데이터 안보는 지정학적 공간에 고착된 일국적 시각을 넘어서 다양한 이해당사자들이 국제적 해법을 모색하기 위해서 협력하는 비(非)지정학적 문제와도 만나기 때문이다. 최근 데이터 안보 문제는 통상, 금융, 산업, 외교 등과 같은 비(非)안보 영역에서 '이슈연계의 임계점'을 넘나들며, 데이터 주권에 대한 국제정치경제학적 논의를 유발하고 있다. 이러한 시각은 국가영토의 경계를 넘어서는 '상호의존'을 강조하고 글로벌 거버넌스의 모색을 중시하는 자유주의 국제정치이론의 시각과 맥이 닿는다(Ikenberry, 2014).

데이터 안보의 세계정치는 구성주의 국제정치이론의 시각에서 이해된 비판지정학의 성격도 지닌다. 데이터 안보의 위협이 '양질전화 임계점'의 문턱에 접근하는 과정에서 국제안보 연구의 코펜하겐 학파에서 말하는 '안보화'가 중요한 변수로 작동한다. 사실 사생활 침해나 개인정보 보호 또는 데이터의 대외적 유출 정도에서 시작된 데이터 안보의 문제가 국가안보 문제로 비화되는 과정에는 객관적으로 '실재하는 위험' 만큼이나 위험을 주관적으로 '구성하는 과정'이 중요하게 작동한다. 최근 벌어지는 디지털 패권경쟁의 이면에는 이러한 데이터 안보화의 비판지정학적 논리

가 강하게 작동하고 있다(Hansen and Nissenbaum, 2009).

한편, 데이터 안보 게임은 기존에 근대 국제정치가 벌어졌던 지리적 공간이라는 경계를 넘어서는 탈지리적 공간과도 겹치면서 발생하고 있음을 잊지 말아야 한다. 무엇보다도 데이터 안보가 쟁점이 되는 사이버 공간은 기본적으로 지리적 공간을 초월하여 구성되고 작동하는 성격을 지니고 있다. 이러한 사이버 공간은 기본적으로 기술과 정보 및 데이터와 커뮤니케이션 활동이 만들어내는 탈(脫)지정학의 공간이다. 이런 점에서 데이터 안보 게임은, 전통안보의 공간처럼 영토적 공간에만 고정되어 발생하는 것이 아니라, 훨씬 더 유동적인 복합 네트워크 공간을 배경으로 작동한다(Castells, 2000).

이러한 시각을 종합해서 보면, 데이터 안보의 세계정치는 고전지정학뿐만 아니라 다양한 이론적 시각을 원용해서 봐야 하는 복합지정학(complex geopolitics)의 게임이다(김상배, 2018a, pp. 66-86). 탈지정학적 공간으로서 사이버 공간의 부상은 데이터 안보의 중요성을 크게 높여 놓았다. 이러한 과정에서 보이지 않는 데이터 안보위협을 경고하는 안보화의 세계정치도 확대되고 있다. 또한 초국적 데이터 이동의 확산은 국제협력의 거버넌스와 국제규범의 형성을 모색케 한다. 최근 벌어지고 있는 세계 주요국들의 디지털 패권경쟁은 이러한 데이터 안보의 복합지정학을 극명하게 보여주는 사례이다.

Ⅲ. 데이터 안보화, 양질전화의 과정

1. 빅데이터 권력과 사생활 침해

4차 산업혁명 시대에는 과거와 비교할 수 없을 정도로 거대한 규모의 데이터가 생성된다. 이렇게 생성된 데이터는 빅데이터 기술을 통해 수집·처리·분석되어 자신도 모르는 사이에 기업 마케팅이나 공공정책에 활용되기도 한다. 그런데 문제는 이렇게 수많은 사용자들의 경제활동의 동향과 정치적 성향을 포함한 개인정보가 사적 권력으로서 민간 기업들에게 집중되면서 사생활 침해 논란이 커지고 있다는 사실이다. 특히 구글(G), 아마존(A), 페이스북(F), 애플(A), 즉 GAFA로 대변되는

미국의 다국적 기업들의 빅데이터 권력이 커지는 현상에 대한 우려가 늘어나고 있다(Jørgensen and Desai, 2017).

구글은 과도한 개인정보 수집이 사생활을 침해한다는 논란에 휩싸여 왔다. 2016년 3월 구글은 '스트리트 뷰' 서비스를 준비하면서 보안조치 없이 이메일과 비밀번호를 수집했다는 혐의로 벌금을 물었다. 2017년에도 안드로이드폰 사용자들의 위치정보를 무단으로 수집했다는 사실이 밝혀지면서 곤욕을 치렀다(민재용, 2019-08-30). 아마존은 고객들의 물품 구매와 관련된 정보를 수집하여 자회사나 제휴회사들과 공유한다는 이유로 조사를 받았다. 아마존의 택배용 소형 드론이 남의 집을 엿본다든가 타인의 동의 없는 무단 촬영을 하여 사생활을 침해했다며 그 운용에 대한 가이드라인을 만들라는 행정명령을 받기도 했다(이상은, 2019-02-07).

페이스북은 2016년 미 대선 당시, 영국 데이터분석 업체 케임브리지 애널리티카(CA)가 페이스북 이용자 수천만 명의 정보를 트럼프 대선 캠프로 넘겨주어 선거운동에 활용토록 지원한 사실이 폭로되면서 곤욕을 치렀다. 게다가 2018년 세 차례의 개인정보 유출 사건이 드러나며 주가는 고점 대비 38% 하락했고 가입자의 이탈도 가속되었다. 애플의 개인정보 침해 가능성도 논란거리였다. 2010-11년에는 이용자들의 동의 없이 위치정보를 수집했다고 여러 차례 손해배상이 청구되었으며, 2014년 6월에는 위치서비스 기능을 꺼도 위치정보가 수집되는 버그가 발생했다. 애플이 iOS에 사용자를 모니터링할 수 있는 백도어를 숨겨놓았다는 주장이 제기되어 파문이 일기도 했다(변재현·지민구, 2018-03-20).

GAFA의 사생활 침해 사건은 빅데이터 비즈니스 모델 전반을 재검토하고 이들을 규제해야 한다는 논란을 불러 일으켰다. 사실 검색엔진, 전자상거래 시스템, 소셜 네트워크 서비스(SNS) 등 각종 플랫폼을 소유하고 있는 빅데이터 기업들은 이용자의 검색내역, 위치정보, 상품구매내역, 콘텐츠 선호도 등을 축적해 맞춤형 광고와 상품추천에 사용하거나 제3의 기업에 판매해왔다. 이러한 빅데이터 비즈니스 모델은 사생활 침해의 가능성이 있을 뿐만 아니라 편견이 담긴 예측 분석을 통해서 개인에게 차별을 가할 수 있는데, 이러한 차별이 인공지능을 기반으로 '자동화'될 경우 그 차별 여부조차도 알아내기 어려워 질 수 있다.

최근 급부상한 중국의 BAT 기업들, 즉 바이두(B), 알리바바(A), 텐센트(T)도 상황은 마찬가지이다. 예를 들어, 알리바바는 전자상거래와 알리페이 결제서비스를 제공

하는 과정에서 소비 패턴을 실시간으로 해석하고 다음 행보를 예측해 새로운 서비스를 창출해낸다. 여태까지는 주로 개인의 소비생활에 영향을 미치던 빅데이터 분석이 유통, 의료, 제조 등 전통산업 영역으로도 침투하고 있다. 중국 최대 차량 공유업체 디디추싱도 승객 개개인의 움직임에 대한 정보를 보유하는 데이터 기업이다. 디디추싱은 고객인 운전자와 승객에게 편리함을 선사한다는 명목으로 수집한 데이터를 다방면으로 활용하고 있다(리즈후이, 2019).

그런데 중국은 서구 국가들보다 느슨한 개인정보 보호체계를 갖고 있다. 사생활 보호보다 빅데이터를 활용한 경제 활성화에 더 적극적이다. 이러한 상황에서 중국 기업들이 제공하는 신용평가 서비스가 개인정보를 침해할 가능성은 더 크다. 안면인식 기술을 도입한 생체 데이터의 수집은 더 심각한 개인정보 침해를 야기할 수 있다(강혜란. 2019-02-18). 게다가 이러한 중국의 상황은 정치적 감시와 검열, 통제와도 연결된다. 예를 들어, 2019년 12월 1일 발효된 중국의 정보보안등급보호 규정(MLPS) 2.0은 5단계의 보안등급 중에서 낮은 등급인 3-5등급을 받으면 연 1회 이상 중국 공안의 감사를 받아야 한다고 규정했다.

2. 사이버 공격과 데이터 유출

사이버 공격을 통한 데이터 안보위협도 큰 논란거리이다. 사이버 공격은 물리층의 파괴나 시스템의 교란 등을 노리기도 하지만, 정보·데이터 자원이나 지적재산의 절취를 노리고 감행되기도 한다. 이는 보통 '사이버 간첩'(cyber espionage)으로 개념화된다(김상배, 2019a, p.125). 이러한 사이버 간첩 활동의 사례로는 1999년 미 공군 네트워크에 대해서 러시아가 감행했던 문라이트 메이즈 작전, 2003년 미군과 미 정부 컴퓨터 시스템에 대해 중국이 감행한 타이탄 레인 작전, 2008년 미 국방부의 비밀 네트워크에 대한 악성코드 침입 사건, 2009년 토론토 대학의 고스트넷에 대해서 중국 해커로 추정되는 세력의 침투사건 등이 있다.

2012년 미국이 이란에 침투시킨 악성코드인 플레임(Flame)은 데이터 자원을 노린 사이버 공격의 대표적인 사례이다. 이란도 2012년에 샤문(Shamoon)이라는 악성코드를 사용하여 사우디의 석유회사 아람코의 전체 컴퓨터 4분의 3에 해당하는 약 3만대의 컴퓨터 데이터를 지워버리는 사이버 공격을 감행하기도 했다. 한편

2014년 3월 러시아가 크림 반도를 점령하는 과정에서 우크라이나에 대해서 감행한 사이버 공격은 물리적 파괴가 아니라 정보·데이터의 절도와 조작을 위주로 하는 사이버 스파이 활동의 형태로 진행되었다.

미국 내 시스템에 대한 침투나 정보·데이터 자산의 탈취를 노린 중국 해커들의 공격도 논란거리였다. 2013년 2월 미국의 사이버 보안업체인 맨디언트가 내놓은 보고서에 의하면 중국군 61398부대는 2006년부터 미국과 서구 국가들의 공공 및 민간기관을 대상으로 수백 테라바이트의 정보를 유출했으며, 그 중 81퍼센트가 미국 기업이나 공공기관을 대상으로 한 것으로 밝혀졌다. 이들 공격은 정보통신과 항공우주 분야뿐만 아니라 과학연구와 컨설팅 분야에 집중되었으며, 주로 지적재산과 중요 데이터의 절취를 목표로 했다는 것이었다.

데이터 안보의 관점에서 더 큰 문제가 된 것은, 2015년 6월 중국 해커들이 미 연방인사관리처(OPM)를 해킹하여 미 상하원 의원과 FBI 요원들의 장기누적 인사정보가 유출된 사건이었다. 2016년 12월에는 중국군이 지원하는 해커조직이 미 연방예금보험공사(FDIC)를 해킹한 사건도 발생했다. 2018년 1-2월에는 중국 해커들이 미 해군 수중전센터와 계약한 업체의 컴퓨터를 해킹하여, 2020년까지 운용하는 초음속 대함 미사일과 수중전에 대한 세부 정보계획을 포함한 614GB 가량의 매우 민감한 데이터를 절취한 것으로 알려져서 논란을 빚었다.

2010년대 후반으로 넘어 오면서 데이터 절취를 노린 사이버 공격은 금전적 이득을 노린 사이버 범죄와 결합되는 양상을 보였다. 2014년 11월 소니 해킹을 감행했던 북한은 2016년 2월에는 방글라데시 중앙은행의 SWIFT 시스템을 해킹했다. 이후에도 국제사회의 대북제재가 한층 강화되면서 돈줄이 막힌 북한이 7천여 명으로 구성된 해커 부대를 앞세운 대대적인 외화벌이 작전에 나섰고, 2017년 12월에는 국내 비트코인 거래소 유빗을 해킹해 파산시켰다. 또한 북한은 한국의 국방망과 국내 방위산업체들을 해킹해 해군 이지스함과 잠수함, 공군 F-15 전투기의 취약점을 파악할 수 있는 설계도면과 이와 관련된 데이터를 훔쳐갔다고 알려졌다.

2017년 5월 들어 데이터 안보를 위협했던 해킹 사건은 라자루스로 알려진 해커 집단의 워너크라이 랜섬웨어 공격이었다. 이는 전세계 150여 개국 30만 대 이상의 컴퓨터를 감염시켜 큰 피해를 입혔다. 미국 사이버 보안업체인 파이어아이는 2018년 2월 발표한 보고서를 통해서 이를 북한의 소행으로 지목하였다. 특히 북핵 경제

제재에 발목이 잡힌 북한 정권이 돈줄을 찾기 위해 사이버 공격을 확대한 것으로 해석했다. 북한이 국가기밀 데이터를 훔치는 기존의 행태를 넘어서 악성코드의 유포를 통해서 불법적인 금전취득을 노리고 있다는 것이었다.

3. 기술패권 경쟁과 데이터 안보화

데이터 안보위협은 안보화 과정을 통해서 주관적으로 구성되기도 했다. 특히 중국과 기술패권 경쟁을 벌이는 미국의 견제가 데이터 안보화의 외양을 하고 나타났다. 2010년대 후반에 걸쳐서 미국은 화웨이 통신장비 제품의 사이버 보안 문제를 내세워 수입통제를 포함한 다방면의 압박을 가했다. 미국이 우려한 바는 화웨이 제품의 백도어를 통해 유출될 데이터가 야기할 국가안보의 문제였다. 특히 미국은 화웨이라는 기업의 뒤에 중국 정부가 있다고 의심했다. 이러한 상황에서 화웨이가 5G 이동통신망을 장악할 경우 이는 미국의 핵심적인 국가정보를 모두 중국 정부에게 내주는 꼴이 될 것이라는 우려가 제기되었다(김상배, 2019a).

화웨이 다음으로 표적이 된 것은 민간 드론 시장을 석권한 중국 업체 DJI였다. 미국 국토안보부(DHS) 사이버안보·기간시설 안보국(CISA)은 2019년 5월 중국의 드론이 민감한 항공 정보를 중국 본국으로 보내고, 중국 정부가 이를 들여다본다고 폭로하였다. 이를 두고 CISA는 국가기관의 정보에 대한 '잠재적 위협'이라고 경고하였다. CISA가 특정 드론을 거론한 것은 아니었지만, 사실상 중국의 DJI를 염두에 둔 발표였다. CISA는 자국 소비자들에게 중국산 드론을 구입할 경우 신중해야 하며 인터넷 장비를 분리해야 한다는 방침까지 내놨다. 화웨이에 대해서 제기되었던 데이터 안보화를 연상케 하는 조치였다.

또한 미국 정부는 2017년부터 하이크비전, 다후아 등과 같은 중국 CCTV업체들이 수집하는 데이터가 중국 정부로 유출될 수 있다는 의혹을 제기하였다. 특히 하이크비전은 CCTV 제작기술에서 세계적으로 앞서 갈 뿐만 아니라 안면인식이나 사람들의 버릇과 신체특성 등을 고려해 특정 인물을 식별하는 기술로 유명하다. 중국 정부는 이러한 기술을 감시도구로 활용해서 소수민족이나 반체제 세력을 통제하는 데 적극 활용하고 있다. CCTV업체인 하이크비전에 대한 압박은 천안문 사태 30주년을 맞이한 중국의 인권 문제를 겨냥했다는 해석을 낳았으며, 이는 2019년 하반기

뜨거운 쟁점이 되었던 홍콩 시위 사태와도 무관치 않다(He, 2018).

2018년 1월 미국 재무부 산하 미국외국인투자위원회(CFIUS)는 알리바바 계열 앤트파이낸셜이 미국 최대 송금서비스 업체 머니그램을 인수하는 것을 제지했다. 금융 서비스와 관련된 데이터 안보상의 우려가 크다는 이유로 CFIUS가 승인하지 않은 것이다. 결국 2018년 5월 앤트파이낸셜은 알리페이 결제 서비스와의 상승효과를 노리고 추진하던 머니그램 인수를 포기했다. 마찬가지로 2019년 5월 중국 게임회사 쿤룬은, 2018년에 인수했던 미국의 소셜 미디어 그라인더를 2020년 6월까지 매각하겠다고 발표했다. CFIUS는 800여만 명의 미국인이 사용하는, 세계 최대의 성(性)소수자 커뮤니티인 그라인더의 데이터가 중국으로 넘어가면 안보위협이 될 수 있다며 매각 명령을 내렸기 때문이었다(강동철·오로라, 2019-05-18).

2019년 말에 새로이 데이터 안보의 쟁점으로 부상한 중국의 앱 서비스는 15초짜리 짧은 동영상을 공유하는 틱톡이었다. 중국의 스타트업인 바이트댄스의 틱톡은 전세계 5억 명 이상의 사용자를 자랑하며, 미국에서만도 가입자가 2천 5백만 명에 달한다. 미국 정부는 2019년 2월 틱톡에 대해 아동 개인정보 불법 수집혐의로 과징금을 부과한 바 있다. 또한 미 상원의원들도 틱톡의 국가안보 위험여부를 조사해달라고 공식 요청했다. CFIUS는 바이트댄스가 미국의 뮤직앱인 뮤지컬.리(musical.ly)를 인수한 데 대한 조사를 실시하였다. 미 육군과 해군도 사이버 안보에 위협이 될 수 있다며 소속 장병들의 틱톡 사용을 금지하였다(Vigdor, 2020).

이상에서 언급한 데이터 안보화와 동전의 양면과도 같은 관계에 있는 것이 사이버 루머와 가짜뉴스(fake news)의 유포이다. 최근 미국이나 서방 진영 국가들의 선거과정에서 수행된 러시아발 가짜뉴스 공격은 인터넷과 소셜 미디어 상에서 여론을 왜곡하고 사회분열을 부추기며 서구 민주주의 체제의 정상적인 작동을 방해하는 효과를 빚어냈다. 이러한 문제들은 이른바 데이터 민족주의와 결합되며 사이버 공간에서의 국가 간 역사·문화 갈등으로 비화될 가능성이 있다. 한국에서 제기되었던 구글 지도의 동해 표기 오류 문제나 구글의 1:5000 지도 반출 사건 등은 데이터 안보 문제가 민족주의적 정서와 결합된 사례였다(이승주, 2018).

Ⅳ. 데이터 주권논란, 이슈연계의 메커니즘

1. 초국적 데이터 유통규범의 모색

미국은 화웨이에 대해서는 안보를 빌미로 한 보호주의의 칼날을 휘둘렀지만, 자국 빅데이터 기업들의 데이터 비즈니스에서는 자유로운 이동을 보장하자는 입장이다. 국경 간 자유로운 데이터 이전이 보장되는 가운데 개인정보 유출이나 왜곡, 남용 등의 문제가 발생할 경우에만 해당 기업이 책임지면 된다는 것이다. 주로 의료, 금융, 정보통신 분야 등의 특정 데이터를 중점적으로 보호하고 있으며, 국가적 차원의 정책보다는 해당 주(州) 또는 기업의 법 테두리 안에서 대응하고 있다. 이러한 미국의 입장은 초국적 유통을 통해 글로벌 차원에서 데이터의 가치를 극대화하려는 미국 다국적 기업들의 이해관계를 대변한다(김상배, 2018b, pp. 31-36).

이러한 미국의 입장은, WTO에서의 서비스 무역에 대한 논의가 부진한 가운데, 지역무역협정 차원에서 진행되었던 다자간서비스협정(Trade in Services Agreement, 이하 TISA)에서 그대로 드러났다. TISA에서 논의되는 '정보의 국경 간 이동 보장' 조항이 관철될 경우, 빅데이터 분석에 필요한 다량의 데이터의 수집, 축적, 관리 및 유통을 제한하는 정부의 조치는 불허된다. 또한 데이터의 수집과 축적을 위해 필요한 데이터센터를 자국 내 둘 것을 요구하거나 데이터의 이전과 관련하여 통상 차원에서 정당화할 수 없는 요건을 부여할 수 없게 된다(강하연, 2013).

트럼프 대통령이 TPP의 탈퇴를 선언하면서 미국이 주도하던 디지털 무역협상이 소강상태를 맞고 있는 가운데, 데이터 무역에 대한 논의는 CPTPP와 USMCA에서 이루어졌다. 미국을 제외한 TPP 11개국이 체결하여 2018년 12월 발효된 CPTPP는 무역협정 중 최초로 국경 간 자유로운 데이터 이동, 서버 국지화 금지, 개인정보 보호 등의 내용을 포함하였다. 2018년 미국, 캐나다, 멕시코가 기존의 NAFTA를 개정하여 체결한 USMCA는 기본적으로 CPTPP를 기초로 하되 새로운 규범을 포함했다. 개인정보 보호, 국경 간 자유로운 데이터 이동 및 서버의 설치, 인터액티브 컴퓨터 서비스 등에 대한 규정을 담고 있다(박지영·김선경. 2019).

미국과 일본도 2018년 중후반부터 개인정보 보호와 빅데이터 국제유통 규칙 마련을 위한 논의를 진행시켜 왔다(배준호, 2018-10-29). 2018년 7월 미국은 자유로

운 디지털 무역을 촉진하기 위해 TPP를 대체할 틀을 미국과 일본이 주도해 만들자고 제안했다. 사실상 트럼프 대통령이 탈퇴했던 TPP의 데이터 버전으로 볼 수 있는 구상을 제시한 것이었다. 이러한 '데이터 TPP'의 바탕에는 2011년 비준된 APEC의 '국경간 프라이버시 규칙(Cross-Border Privacy Rules, CBPR)'이 있었다. CBPR은 기업의 개인정보 보호를 평가하고 인증하는 체계이며 회원국들 간 데이터 이전 활성화와 안전한 개인정보 이전을 위해 지켜야 할 일련의 원칙을 제시했다. 현재 한국과 미국, 일본, 캐나다 등 8개국만 참여하고 있지만 미국은 이를 베트남, 대만, 남미 국가들까지 확대하려 한다(박지영·김선경. 2019).

2019년 6월 오사카 G20 정상회의는 미중 기술패권 경쟁의 무게 중심이 '화웨이 라운드'에서 '데이터 라운드'로 옮겨갈 조짐을 보여줬다. G20에서 일본이 제안한 오사카 트랙은 중국의 디지털 보호주의와 데이터 국지화 정책을 겨냥한 미국 등 서방 진영의 속내를 담고 있었다. 오사카 트랙에서는 국제적 데이터 유통 규칙의 표준화뿐만 아니라 개인정보와 지적재산권 보호 및 사이버 보안의 강화, 그리고 미국의 인터넷 기업들에 대한 과세기준 마련 등이 논의되었다. G20 차원에서 제기된 이러한 문제들은 양자 및 다자 그리고 지역 차원의 협상과정에서 유사한 구도로 재현 및 확장될 것으로 전망된다.

오사카 G20 정상회의에서 미중 정상은 데이터 주권으로 설전을 벌였다. 트럼프 대통령이 중국의 데이터 통제를 겨냥해 "국가를 넘는 데이터 유통 등을 제한하는 (중국의) 움직임은 무역을 방해하고, 프라이버시나 지적재산을 침해하는 것이어서 반대한다"고 말했다. 이에 대해 시진핑 주석은 "각국의 자주적인 관리권을 존중하고 데이터의 질서있는 안전이용을 확보해야 한다"고 반박했다. 또한 시 주석은 불법적인 데이터 수집 가능성 등을 이유로 중국 화웨이에 대해 제재를 가하고 있는 미국 정부를 향해 "공평, 공정하고 차별 없는 시장 환경을 만들어야 한다"고 역공을 펴기도 했다(민재용, 2019-08-30).

2. 데이터 국지화와 국가주권 담론

미국이 자국의 빅데이터 기업들의 이익을 내세워 데이터의 초국적 유통을 옹호하고 있는 가운데, 최근 각국은 데이터를 일국적 재산으로서 이해하고 데이터 안보의

시각에서 접근하는 행보를 보이고 있다. 특히 데이터 주권의 개념을 내세워 자국 기업과 국민의 데이터를 보호하고 데이터 유통 활성화 및 그 활용역량을 증대시키고자 노력하고 있다. 데이터 현지 보관, 해외반출금지 등으로 대변되는 '데이터 국지화(Data Localization)' 정책을 확대해 국가의 사이버 보안뿐만 아니라 국민의 개인정보 보호를 달성하겠다는 것이다. 이렇게 원칙적으로 데이터의 초국적 이동을 제한하는 입장을 추구하는 대표적인 국가는 중국이다(Liu, 2019).

스노든 사건 이후 미국의 데이터 감시에 대한 위기감은 중국이 이러한 입장을 강화하는 데 작용했다. 중국에서 활동하는 모든 기업들은 중국에서 수집된 데이터를 반드시 역내에 보관해야 하며, 데이터를 역외로 이전하기 위해서는 중국 당국의 허가를 받고, 중국의 규정에 따라 안전평가 절차를 거쳐야 한다는 것이다. 또한 중국 정부의 요구가 있을 경우 데이터 암호 해독 정보를 제공해야 하며, 거부 시에는 기업에게 영업정지와 벌금을 부과한다는 것이다. 이러한 중국의 행보는, 공익을 해치는 데이터를 검열·통제하고, 자국 내에서 수집한 데이터의 국외 유출을 규제하는 것은 국가주권이라는 관념에 입각해 있다(김상배, 2018b, pp. 36-41).

2017년 6월 시행된, 중국의 〈인터넷안전법〉은 이러한 내용을 담고 있다. 〈인터넷안전법〉에서는 데이터 국지화와 인터넷 안전검사 관련 조항이 쟁점인데, 상위 등급에 있는 '핵심 정보인프라 운영자'로 지정되면, 데이터 서버를 중국에 둬야만 하고, 중국 정부가 지정하는 네트워크 장비와 서비스만을 사용해야 한다. 그리고 중국 정부는 안전 수준에 대해 지속적으로 점검하고 모니터링할 수 있다. 〈인터넷안전법〉은 표면적으로는 개인정보 보호와 국가와 국민의 안전을 목표로 내세웠지만, 실상은 자국 산업의 보호와 인터넷 콘텐츠의 통제와 검열 강화를 노리는 것으로 평가된다.

실제로 〈인터넷안전법〉은 미국의 다국적 기업에 대한 압박을 가했다. 2017년 11월 아마존웹서비스(AWS)는 중국사업부 자산을 매각했으며, 2018년 초에는 마이크로소프트와 아마존도 자사 데이터를 각기 베이징과 닝샤의 데이터센터로 옮겼다. 또한 〈인터넷안전법〉 시행 직후 애플은 중국 내 사용자들의 개인정보와 관리권을 모두 중국 구이저우 지방정부에 넘겼으며, 2018년 2월에는 제2의 데이터센터를 중국 네이멍 자치구에 건설할 계획을 발표하기도 했다. 한편 중국은 2020년 1월 1일부터 외국인 투자법을 개정해 외국 기업이나 외국인 투자기업의 특별대우를 폐지하고 중국 기업과 동일하게 다루기로 했다.

러시아도 자국민 데이터를 국가주권의 범위로 규정하는 법률을 연이어 제정하고 있다. 푸틴 러시아 대통령은 2019년 5월 러시아에서 발생한 데이터를 해외로 가지고 나갈 경우 정부 검열을 거치도록 강제하는 법안에 서명했다. 해외 기업의 무차별적인 데이터 수집과 국외 반출을 금지한 것이다. 이러한 연속선상에서 2019년 11월에는 〈독립인터넷법〉을 발표했다. 〈독립인터넷법〉은 러시아의 통신회사 로스콤나드조르에 외부와의 트래픽을 차단하여 순수하게 러시아만의 인터넷을 만들도록 규정하였다. 많은 인권 활동가들과 사이버 전문가들은 러시아의 인터넷에 일종의 '디지털 철의 장막'을 드리우게 되어 인터넷에 대한 검열 및 감독에 새로운 국면을 열 것이라고 우려했다(유세진, 2019-11-03).

기타 국가들의 데이터 주권 행보에도 주목해야 한다. 베트남도 2018년 데이터 국외 반출을 금지하는 법안을 발효했다. 호주 정부는 2018년 말 해외에 있는 자국민의 데이터를 볼 수 있도록 규정한 법안을 통과시켰다. 해외 기업이 해외에 보관한 호주 국적민의 데이터라도, 호주 정부가 제공을 요청할 근거를 만든 것이다. 한국에서도 국내 기업들의 클라우드 사업이 지지부진한 상황에서 미국 클라우드 기업들에 대한 지나친 의존으로 인해서 국내에서 생산되는 수많은 데이터가 해외로 빠져나갈 가능성이 우려되고 있다. 네이버는 국내에서 유일하게 시설, 운용, 솔루션 개발까지 자체적으로 총괄하는 데이터센터를 강원도 춘천에 구축한 데 이어, 두 번째 데이터센터를 세종시에 대규모로 구축할 계획을 밝혔다.

3. 개인정보 보호와 시민주권 옹호

이렇듯 데이터의 초국적 유통규범을 모색하는 움직임과 이에 대응하여 자국 데이터 시장을 지키려는 데이터 국가주권의 움직임이 경합하는 가운데, 최근 유럽연합의 행보가 주목을 끌고 있다. 역사적으로 세이프하버 협정 체결과 그 무효화 및 프라이버시 실드 도입 등의 행보를 밟아온 유럽연합은, 2018년 5월에는 GDPR(General Data Protection Regulation)을 시행하기에 이르렀다. 이 과정에서 데이터 국외 이전 및 국지화의 문제 이외에도 데이터의 효과적 활용 및 개인정보 보호 문제, 소유권 개념이 아닌 방식으로 개인의 데이터 권리를 인정하는 문제, 그리고 구글세의 부과 문제 등이 쟁점으로 거론되었다(Farrell and Newman, 2018).

이러한 유럽연합의 행보는 개인의 권리를 바탕으로 하여 국민(nation)의 차원에서 행사되는 주권의 개념을 엿보게 한다. 이러한 주권 개념은 민권(民權)의 개념으로 통하며, 좀 더 구체적으로 말하면, 개체적 '시민'의 권리에 근거를 두는 집합적 '국민'의 권리라는 의미에서 일종의 '시민주권'이다. 이를 데이터 분야에 적용하면, 개인의 집합으로서 국민의 민감한 정보를 담은 데이터나 개별 사용자로서 국민들의 개인정보를 보호하는 권리 개념으로 나타난다. 이는 국가를 구성하는 개인의 권리를 집합적으로 이해하는 주권 개념으로서 앞서 소개한 국가주권으로서 데이터 주권에 대한 논의와는 구별된다(김상배, 2018b, pp. 41-47).

이러한 시민주권론을 엿볼 수 있는 대표적인 사례가 바로 GDPR이다. GDPR은 그 규정 위반 시 전 세계 매출액의 4% 또는 최대 2,000만 유로(한화 약 268억 원) 규모의 과징금이 부과되는데, 유럽연합 회원국은 물론 유럽연합에 역내 사업장을 두거나 온라인 서비스로 재화나 서비스를 제공하는 모든 글로벌 기업들에 해당한다. 실제로 영국항공은 2018년 50만 명의 개인정보 유출 사고로 GDPR 적용을 받아 거액의 벌금을 물었다. 구글도 2019년 1월 프랑스의 정보처리자유국가위원회(CNIL)로부터 GDPR 위반으로 벌금을 부과받았다. 유럽 민간단체인 NOYB는 아마존과 애플이 GDPR을 위반했다고 주장했고, 넷플릭스, 유튜브에 대해서도 같은 혐의로 조사가 진행되었다(최연진, 2019-11-13).

GDPR은 기존의 데이터 열람권이나 수정권 등과 함께 데이터 삭제권(즉, 잊힐 권리), 데이터 이동권, 프로파일링 거부권 등을 규정하고 있다. 다시 말해, 사용자가 기업이 보유한 자신의 개인 데이터를 삭제하거나 다운로드할 수 있어야 함은 물론 자신의 데이터를 자신이 지정한 제3자에게 제공할 수 있도록 하는 데이터 결정권을 강화했다. 또한 가명정보 활용을 법적으로 규정함으로써, 데이터 활용과 관련 서비스에 대한 사용자의 신뢰를 제고하였다. 해외 서버로 건너간 자신의 데이터가 침해될 경우 언제든 소송을 제기할 수 있음은 물론이다(구태언. 2019-11-04).

특히 국경 간 데이터 이전에 대한 규제와 관련하여, GDPR은 역외로 데이터를 이전할 경우 유럽연합과 동등한 수준의 개인정보 보호의 체계를 갖추었다는 사실을 증명하는 '적정성 평가'(adequacy or equivalence decision)를 통과해야만 데이터의 자유로운 이전이 가능하도록 했다. 그러나 데이터 보호 수준이 기준에 부합하지 않더라도 데이터 주체의 동의가 있거나 계약을 이행해야 할 경우, 또는 법적

협력이 필요한 경우에는 데이터 이전이 가능하게 되어 있다. 국가 차원에서 데이터를 보호하는 권리 개념의 근거를 찾는 것이 아니라. 개인 차원에서 그 권리의 근거를 찾고 이를 유럽연합이 보장하는 법제도를 제공하는 모델이다.

이러한 맥락에서 유럽의 개별국가들은 개인정보의 보호를 저해하지 않는 범위 내에서 개인정보를 활용할 기회를 높여나갔다. 영국과 프랑스의 경우, 개인정보 이동권을 통해 보호와 활용의 균형을 도모하는 시범사업을 시행했다. 영국의 마이데이터(MiData)와 프랑스의 셀프데이터(SelfData)는 개인정보를 주체인 본인에게 돌려주고, 본인 스스로 판단 하에 개인정보의 활용여부 및 방법을 제공하는 사업을 시행했다. 영국의 마이데이터는 자신의 거래내역을 다운로드 받을 수 있도록 한 제도이다. 셀프데이터는 개인의 목표를 달성하기 위해 개인 자신의 통제 하에서 개인정보를 생산해 사용 및 공개하는 것을 의미한다(구태언. 2019-11-04).

한국도 2018년 6월 각 분야에 개인중심의 데이터 유통체계인 마이데이터 사업을 의료·금융·에너지·유통·학술연구 등의 분야에서 도입하여 시범사업을 추진한 바 있다. 이를 통해 과기정통부는 본인정보 활용에 따른 혜택을 체감해 개인중심의 데이터 유통체계를 확립하겠다고 했다. 그러던 중 2020년 1월 9일 데이터 3법(개인정보 보호법·정보통신망법·신용정보법 개정안)이 통과되었다. 가명정보 활용 근거를 명시하고, 법 집행 체계를 일원화하는 게 골자다. 가명정보는 통계작성, 과학적 연구, 공익적 기록 보존 등을 위해 정보주체의 동의 없이 적절한 안전조치 하에 이용할 수 있다. 이러한 행보는 한국이 GDPR의 '적정성 평가'를 통과하는 데 긍정적인 영향을 미칠 것으로 예견된다.

V. 데이터 안보의 (복합)지정학의 차원

1. 사이버 동맹 형성과 연대외교

최근 데이터 안보 이슈는 국가 간 동맹이라는 지정학적 차원으로 발전했다. 이는 화웨이 사태가 이른바 '파이브 아이즈'(Five Eyes)로 알려진, 미국, 영국, 캐나다, 호주, 뉴질랜드 등 5개국의 상호 정보동맹과 연계되면서 나타났다. 2018년 초부터

미국은 파이브 아이즈 국가들에 화웨이 장비를 도입하지 말라고 요청했다. 영국의 BT그룹은 화웨이 제품을 5G 사업에서 배제하려는 움직임을 보였다. 캐나다는 중국과의 무역마찰을 무릅쓰고 화웨이 부회장인 멍완저우를 체포했다. 호주와 뉴질랜드는 5G 사업에 중국 업체가 참가하지 못하도록 했다. 일본도 정부 차원의 통신장비 입찰에서 화웨이를 배제하기로 결정했다. 독일과 프랑스도 미국의 화웨이 견제 전선에 동참하였다. 이러한 행보를 보고 기존의 파이브 아이즈에 일본, 독일, 프랑스 등 3개국이 합류한 '파이브 아이즈+3'의 출현이 거론되기도 했다(박세진, 2019).

그런데 2019년 2월말을 넘어서면서 미국의 압박에 동참했던 영국과 뉴질랜드 등 파이브 아이즈 국가들이 '사이버 동맹전선'에서 이탈하는 조짐을 보였다. 이들 국가들의 입장이 변화한 이유는, 화웨이를 배제한 채 자체 기술로 5G 네트워크를 구축하는 것이 현실적으로 어려운 상황이 작용했기 때문으로 해석되었다. 이후 트럼프 대통령은 화웨이에 대한 유화적 제스처를 취하는 동시에 강경책도 병행하는 양면전술을 채택했다. 결국 화웨이 제재의 '사이버 동맹전선'이 흔들리는 조짐을 보이자, 트럼프 대통령은 2019년 5월 화웨이 통신장비의 국내 도입 금지뿐만 아니라 5G 네트워크 구축에 필요한 핵심 부품을 제공해 온 미국 기업들의 화웨이에 대한 수출을 금지하는 행정명령을 내리기에까지 이르렀다(우은식, 2019).

사이버 안보를 내세운 미국의 동맹결속 전략은 미국의 인도·태평양 전략에서도 나타났다. 2019년 4월에는 미국을 위협하는 북한과 중국의 사이버 공격에 대응하기 위한 국제협력체 신설을 골자로 하는 〈인도·태평양 국가 사이버 리그(CLIPS)〉 법안이 상원에서 발의됐다. 이 법안에 따르면, CLIPS에는 인도·태평양 지역의 미국 동맹국과 파트너 국가들이 참여한다(이조은, 2019). 한편 미 국방부는 2019년 6월 공개한 '인도·태평양 전략보고서'에서 중국의 일대일로(一帶一路) 전략에 맞서 인도·태평양 전략을 강화하였으며, 화웨이 사태를 재래전뿐만 아니라 정치, 경제 등 비군사적 요소와 사이버전, 심리전 등이 혼합되어 전개되는 새로운 개념의 전쟁, 즉 '하이브리드 전쟁'의 개념으로 규정하기도 했다(정충신, 2019).

이러한 미국의 화웨이 견제에도 불구하고 중국 정부는 일대일로 추진 차원에서 해외 통신 인프라 확충을 가속화했다. 2018년 4월 시진핑 중국 국가주석은 일대일로 건설을 계기로 관련 국가들, 특히 개도국에 인터넷 기반시설을 건설하고 디지털 경제와 사이버 보안 등 다방면에서 협력을 강화하여 '21세기 디지털 실크로드'를

건설해야 한다고 선언했다. 미국의 사이버 동맹외교에 대항하는 일종의 연대외교의 모색으로 해석될 수 있다. 이러한 맥락에서 2019년 후반 동남아 국가들이 화웨이를 선호하는 조치를 취한 행보를 이해할 수 있다. 화웨이와 중국 정부는 서방국가들에 대한 우호적 공세도 진행했는데, 이러한 행보에 힘입어 유럽의 이동통신사들은 화웨이 장비를 선택하는 추세인 것으로 평가된다.

이러한 전개는 한미관계에도 영향을 미쳤다. 실제로 화웨이 사태는 단순한 기술 선택의 문제가 아닌 동맹외교의 문제로 한국에 다가왔다. 2019년 6월 주한 미국대사가 직접 나서 한국이 화웨이에 대한 제재에 동참할 것을 공개적으로 요구하기도 했다. 이와 마찬가지로 데이터의 초국적 이동 문제도 향후 한미관계를 긴장시킬 가능성이 제기되었다. 2016년 한국 정부는 국가안보를 이유로, 구글이 요청한 1:5000 축적의 국내 지도 데이터의 해외 반출 요청을 거부하기도 했다. 2018년 10월에는 국회에서 구글·아마존 등 미국 IT기업들에게 국내에 데이터센터용 서버를 설치할 의무를 지우는 법안이 발의되자, 주한 미국대사가 클라우드의 장점을 가로막는 데이터 현지화 조치를 피해줄 것을 요구하기도 했다.

2. 정보기관의 데이터 감시와 감청

지정학적 차원에서 본 데이터 안보 문제는 국가안보 차원에서 이루어지는 정보기관의 데이터 수집 활동을 통해서 오래전부터 제기되어 왔다. 최근 논란이 된 것은 미 국가안보국(NSA)의 암호해독과 정보수집 활동이다(Petit, 2020). 앞서 살펴본 바와 같이 미국은 민간 차원의 데이터 유통과 관련해서는 자유로운 유통을 옹호하면서 국가안보를 내세워 데이터 국지화를 주장하는 중국을 비판하지만, 지정학적 임계점을 넘는 대목에 오면 사생활 보호보다는 국가안보를 우선에 두고 데이터 수집과 감청 활동을 합리화한다. 이러한 미국의 태도를 보여주는 대표적인 사례로는, 1998년 유럽의회에서 그 존재가 처음 폭로되면서 파문을 일으켰던, 미국 NSA의 에셜론 프로젝트를 들 수 있다.

에셜론은 미국이 중심이 되어 이른바 영국, 캐나다, 호주, 뉴질랜드 등 파이브 아이즈 국가들이 운영하는 전 세계의 통신감청 협력체제이다. 에셜론은 1960년대 냉전시대에 소련과 동구권의 군사 및 외교 통신을 감청하기 위해 만들어졌으며,

소련 붕괴 이후에는 테러모의나 마약거래, 기타 국가안보 관련 통신을 감청해왔다고 알려져 있다. 이러한 활동을 통해서 확보된 각종 데이터는 NSA가 20억 달러를 들여서 건설한 미국 내 유타 데이터센터에 저장된다. 유타 데이터센터는 NSA의 도청위성과 해외 감청기지, 미국 전역의 이동통신 시설 내 비밀 모니터링 룸 등으로부터 데이터를 수집해서 저장하는 민간 기업이 보유한 데이터센터를 제외하고는 미국 내 최대 규모인 것으로 알려져 있다(박희준, 2013-06-15).

2013년 6월 전직 NSA 직원인 에드워드 스노든은 NSA가 프리즘(PRISM)이라는 프로그램을 통해서 장기간에 걸쳐 각종 데이터를 감청해 왔다고 폭로했다. NSA와 연방수사국(FBI)이 인터넷·정보통신 업체들의 서버에 접속해서 인터넷 검색기록을 비롯한 파일전송 기록, 오디오, 동영상, 사진, 이메일, 채팅 정보까지 수집했다는 것이었다. 미국 정부는 정보 수집 사실을 인정했지만 이는 테러 방지 등의 국가안보 목적으로만 사용했다고 해명했다. 프리즘은 미국 법률에 따라 합법적으로 운영됐으며 국가안보를 위해서는 사생활에 대한 침해가 불가피하다는 것이었다(강영연, 2013-06-14). 테러 방지와 사생활 침해 간의 논쟁은 2016년 미국 FBI와 애플 간의 분쟁에서도 등장했다. FBI는 당시 총기 난사 사건의 범인이 소지한 아이폰의 화면보호 암호해제를 애플에 요청했지만 애플은 개인정보 보호를 이유로 이를 거부했다.

이러한 맥락에서 미국이 9.11테러 이후 만든 이른바 〈애국자법〉에 주목할 필요가 있다. 〈애국자법〉은 FBI가 법원의 영장 없이도, 또한 대상을 명시하거나 근거를 제시할 필요도 없이 통신기록과 거래내역을 볼 수 있게 했다. 미국의 정보기관들은 〈애국자법〉을 근거로 하여 정보수집에 제한을 받지 않고 불특정 다수의 개인정보를 수집했으며, 민간 기업들은 정보기관으로부터 특정인에 대한 정보를 요구받으면 무조건 제공해야 했다. 게다가 신원조회 사실을 본인에게 통보하지 않아도 됐기 때문에 인권침해 논란이 크게 벌어지기도 했다. 결국 이러한 애국자법은 2015년에 폐지되어 〈자유법〉으로 대체되었다.

이러한 미국의 입장은 최근 테러 색출 차원에서 국경을 넘어 확장되었다. 2018년 3월 미국은 〈클라우드법(CLOUD Act)〉, 즉 〈해외 데이터 이용 합법화 법률〉을 발표했다. 골자는 미국 정부가 테러·범죄 수사와 같은 합당한 이유가 있을 때 해외에 저장된 미국 기업의 데이터를 들여다볼 권한을 갖는다는 것이다. 미국 법원의 압수

수색 영장을 발부받지 못해도 감청이 가능하며, 데이터가 어디에 저장돼 있든지 간에 필요한 개인정보 관련 데이터의 수집이 가능하다. 예컨대 중국 베이징에 있는 MS의 데이터센터에 저장된 중국인 데이터를 미국 정부가 볼 수 있도록 한 것이다. 미중 양국이 데이터의 법적 관할권을 두고 정면충돌할 가능성이 있는데, 특히 앞서 살펴본 중국 〈인터넷안전법〉과의 충돌 가능성이 있다(Gimelstein, 2019).

2019년 11월 미 상원은 〈국가안보와 개인정보보호법〉을 발의했다. 미국인들의 민감한 정보가 미국을 위협하는 국가들로 전송되거나, 그런 국가들의 영토 내에서 저장하지 못하도록 하는 내용을 담고 있다. 기업들이 필요할 경우에만 사용자의 개인정보를 수집하되, 법안에 명시된 국가 혹은 국가안보에 해를 끼칠 수 있는 국가로의 데이터 전송을 금지했다. 이 법안에 명시된 '우려되는 국가'는 중국과 러시아였는데, 이 두 나라에만 국한되지 않고 '미국의 국가안보에 위협이 되는 모든 나라'로 확대될 가능성이 있었다. 게다가 개인정보의 경우라면 적국이 아니더라도, 미국 영토 외에 저장하는 것 자체를 전부 금지하였다(문가용, 2019-11-22).

3. 군사 정찰위성과 '데이터 국방'

군사안보 분야에 오면 데이터 안보 이슈는 그 자체가 지정학적 이슈가 된다. 특히 빅데이터 시대의 도래는 데이터의 수집·처리·분석 역량을 군사작전과 전쟁수행의 핵심요소로 인식케 하고 있다. 과거에 비해 양도 많아지고 질도 높아진 민간 부문의 데이터와 이를 수집·처리·분석하는 시스템이 군사안보 부문에 미치는 영향도 커졌다. 일반 사용자들이 생성하는 개인정보나 다국적 기업들이 수집한 빅데이터는 군사안보에 있어서도 중요한 자원이 된다. 최근 4차 산업혁명 시대를 맞이하여 민간 주도 우주개발 사업이 늘어나는 가운데, 민간 부문에서 취득된 데이터가 군사안보 분야에서도 유용하게 사용되고 있는 현상은 그 사례 중의 하나이다.

이와 관련하여 주목 받는 것이 위성항법시스템(GPS: Global Positioning System)이다. 위성항법시스템은 4차 산업혁명 시대의 사회 기간시설을 지원하고, 개인의 편익을 증진하는 국가의 주요 인프라로 부상하고 있다. 또한 위성항법시스템은 항법, 측지, 긴급구조 등 공공부문 뿐만 아니라 스마트폰 등과 같은 국민 개개인의 생활 속까지 그 활용 영역을 급속히 확대하고 있다. 게다가 최근 현대전이 인공위

성의 위성항법장치를 이용한 우주전의 형태를 띠고 있다는 점에서 그 데이터 (군사) 안보적 함의가 크다. 이러한 추세에 부응하여 미국과 유럽 국가들뿐만 아니라 러시아, 중국, 일본 및 인도 등의 국가도 독자적인 위성항법시스템을 구축했거나 또는 구축하기 위한 준비를 펼치고 있다.

군사 분야에서 정찰위성이나 정찰기를 활용한 군사 정보·데이터의 수집은 전략적 우위를 창출하는 핵심역량이다. 예를 들어, 미군은 정찰위성이나 무인정찰 드론 등을 활용하여 북한의 대륙간탄도미사일(ICBM) 이동발사 차량을 정확하게 추적·파악하고 있는 것으로 알려져 있다(Lieber and Press, 2017). 최근 논란이 되었던 지소미아(GSOMIA)에 의거하여, 일본은 북핵·미사일 기술 관련 정보를 제공해 왔는데, 일본의 위성은 하루에 3-4차례 한반도 상공을 지나가는 미국의 정찰위성이 커버하지 못하는 사각 시간을 일부 보완한다. 2019년 12월에는 미국이 북한의 추가 시험과 도발 동향 징후를 파악하기 위해서 한반도 상공에서 운용하는 특수정찰기가 하루 동안 3대나, 그것도 위치발신 장치를 켠 상태로 비행하며 대북 감시활동을 벌인 것으로 드러나 논란이 되기도 했다(최평천, 2019).

이러한 상황에서 북한도 인공위성 개발이라는 명분을 내세워 미사일 개발에 적극 나서고 있다. 적어도 대외적으로는 최첨단 위성 발사와 달 착륙을 목표로 한 우주개발 계획을 내세우고 있다. 우주개발 계획을 통해서 지구관측 위성의 추가발사와 북한 최초 정지궤도 통신위성의 발사를 추진하고 있다. ICBM의 발사가 아니라 인공위성 발사이더라도 이를 통해서 북한이 정찰위성을 얻게 되면 김정은 위원장은 평양에 앉아서 한국에 전개되는 전략자산과 표적, 이동상황을 모두 다 볼 수 있다. 한반도를 하루에 2-3차례 통과하면서 괌과 일본의 항공모함 이동까지 볼 수 있고 미국까지도 감시가 가능하다. 북한으로서는 한반도 전역을 탐지할 수 있는 전략자산이 생기는 셈이다(김주영, 2019-12-09).

최근 정찰용 드론도 데이터 안보와 관련된 쟁점이다. 2017년 6월 9일 강원도 전방지역에서 북한군의 정찰용 드론으로 추정되는 비행체가 발견되어 큰 이슈가 되었다. 북한의 정찰용 드론이 추락한 것은 2013-2014년에도 백령도, 파주, 삼척 지역에서 3차례에 걸쳐 있었다. 그 당시 발견된 정찰용 드론은 비행거리와 내부 기술수준이 낮아 비웃는 사람들도 많았다. 그러나 2017년에 발견된 드론은 비행거리를 대폭 개량한 것으로 한국 측 방공망의 허점을 뚫고, 내륙 전략시설을 정찰할

수 있는 능력을 보여줘 적지 않은 당혹감을 안겨 주었다. 군사적 위협의 가능성 여부 논란을 떠나 남측의 방공망을 뚫고 내륙 깊숙이 정찰용 드론이 활보하고 다닌다는 사실은 충분히 우려할만한 상황이다(최창영. 2017-07-20).

4차 산업혁명의 진전과 함께 군사 분야에서도 빅데이터의 중요성이 인식되면서 이른바 '데이터 국방'이 모색되고 있다. 특히 인공지능 기술의 발달로 인해 더 강력해진 데이터 처리 능력은 점점 더 군사안보를 위해 필요한 핵심으로 자리 잡을 것이다. 이러한 과정에서 전장 센서로부터 데이터를 수집하고, 더 많은 처리능력으로 보강한 알고리즘으로 데이터를 처리하고, 결과적으로 적보다 빠르게 침투하는 것이 핵심이 된다. 모든 전장 정보를 데이터화시켜 클라우드 서버에 저장·분석하여, 이를 필요한 부대에 제공하는 이른바 '지능형 데이터 통합체계'의 구축과 활용이 모색되고 있다. 이를 바탕으로 각종 정보와 데이터를 분석하고, 실시간으로 인간 지휘관의 지휘결심체계를 지원할 것으로 기대되고 있다(김상배, 2019b).

데이터의 도입은 첨단 방위산업에도 큰 영향을 미치고 있다. 무기체계의 스마트화와 디지털 플랫폼의 구축을 바탕으로 한 제품-서비스 융합을 통해서 가치를 창출하는 변화가 군수 분야에서 발생하고 있다. 제품 자체의 가치창출 이외에도 유지·보수·관리 등과 같은 서비스가 새로운 가치를 창출하는 영역이 새로이 자리 잡고 있다. 기존 재래식 무기체계의 엔진계통에 센서를 부착하여 축적된 데이터를 분석함으로써 고장 여부를 사전에 진단하고 예방하며, 부품을 적기에 조달하는 '스마트 군수 서비스'의 비전이 제기되고 있다. 이러한 디지털 공급사슬에 대한 투자는 시장 접근성의 속도를 빠르게 하고 생산비용을 절감하며 협업혁신을 촉진하는 데 기여함으로써 방위산업 분야에서 시스템 변화를 야기할 것으로 기대된다(김상배, 2020).

Ⅵ. 맺음말

데이터가 기술과 산업, 그리고 경제와 사회의 이슈를 넘어서 국가안보의 이슈로 부상하고 있다. 이것은 국가안보와 관련된 내용을 직접적으로 담은 데이터가 중요해졌다는 의미만은 아니다. 빅데이터 시대에는 민간 영역의 개인정보 침해나 사이버 공격을 통한 데이터 유출도 안보의 문제가 될 수 있다. 스몰데이터 시대의 속성론적

마인드로 보면 이 자체로서 국가안보를 논하기에는 무색하지만, 빅데이터의 과정론적 마인드로 보면 이러한 미시적 데이터가 양적으로 늘어나고 이슈연계되면서 거시적 차원에서 지정학적 함의를 지닌 국가안보의 패턴을 드러낼 수 있다. 이 글은 신흥안보의 시각을 원용하여 이러한 창발의 메커니즘을 살펴보았다.

최근 이러한 데이터 안보를 둘러싼 디지털 패권경쟁은 '지정학의 부활'을 방불케 한다. 그러나 전통적인 (고전)지정학의 시각으로만 봐서는 안 된다. 데이터 안보 논의의 근간은, 탈지정학적 사이버 공간을 배경으로 활동하는 다국적 기업들의 사생활 침해 가능성에서 발견된다. 또한 데이터 안보는 지리적 경계를 넘어서는 데이터의 유통과 이를 데이터 주권의 논리를 내세워 규제하는 비(非)지정학적 국제정치경제의 이슈이다. 게다가 이러한 과정은 최근 비판지정학의 시각에서 파악되는 '데이터 안보화'와 연결되고 있다. 그야말로 데이터 안보는 탈지정학, 비지정학, 비판지정학 현상이 고전지정학적 현상과 중첩되는 복합지정학의 논제이다.

이러한 데이터 안보의 복합지정학에 한국은 어떻게 대응해야 할까? 세계 주요국들을 중심으로 벌어지는 데이터 안보의 디지털 패권경쟁 속에서 중견국으로서 한국이 모색할 데이터 전략의 방향은 어디일까? 포괄적으로 보면 미래 국력의 핵심요소로서 데이터 자원의 중요성을 인식하고 이를 확보하는 역량의 개발과 관련정책의 추진, 법제도 환경의 정비, 국제규범 형성에의 참여 등이 필요하다. 그러나 데이터가 단순한 경제의 이슈를 넘어서 안보의 쟁점이 되고 있다는 사실을 고려할 때 좀 더 정교한 데이터 안보전략의 개발이 필요할 것이다. 이러한 맥락에서 이 글에서 제기한 분석틀에 기대어 새로운 발상의 필요성을 지적해 보고자 한다.

첫째, 데이터 안보의 양질전화 과정을 고려한 국가전략이 필요하다. 미시적 차원의 개인정보 보호를 거시적 차원의 데이터 국가안보와 연결해서 보는 입체적 발상이 필요하다. GAFA나 BAT로 대변되는 빅데이터 기업들의 권력은 민간 영역에만 국한된 것이 아니라 이제 국가안보의 쟁점을 야기할 정도로 커졌다. 아울러 데이터 유출을 노리는 직접적인 해킹위협에 대응하는 전략뿐만 아니라 사이버 보안제품의 도입이 야기할 데이터 안보위협의 가능성을 인식해야 한다. 그렇지만 이러한 대응이 지나친 안보화로 흐르지 않도록 경계해야 함은 물론이다.

둘째, 데이터 안보의 이슈연계 메커니즘을 고려한 국가전략이 필요하다. 데이터의 초국적 유통에 대응하는 새로운 데이터 주권의 발상이 필요하다. 이러한 주권발

상에는 개인 차원의 권리보호를 근간으로 하고, 데이터의 가치를 극대화하려는 기업의 목적을 인정하면서도, 데이터의 공공성을 보장하는 취지가 모두 반영되어야 한다. 데이터 권리주체로 국가를 내세우기보다는, 개별적 개인이자 집합적 국민의 권리를 근간으로 하면서, 데이터 기업의 활동을 활성화시키는 가운데, 공익에 봉사하는 국가의 역할을 정립하는 복합적인 주권 개념이 필요하다.

끝으로, 데이터 안보의 (복합)지정학적 차원을 고려한 국가전략이 필요하다. 데이터 안보가 강대국들의 동맹과 연대외교의 아이템으로 부상하고 있음을 인식할 필요가 있다. 이러한 변화는 한국과 같은 중견국에게는 중개외교의 기회이자 도전이 되고 있음도 깨달아야 한다. 아울러 데이터 안보의 지정학적 경쟁에 대응하는 차원에서 정보기관에서도 빅데이터 분석역량을 길러야 할 것이며, 군에서도 사이버 공간과 우주공간을 중심으로 재편되고 있는 군사작전에 효율적으로 대응하는 데이터 기반 국방 운영체계를 구축해야 한다.

요컨대, 오늘날 데이터 문제가 안보 문제를 매개로 국가전략의 논제가 되고 있음을 인식해야 한다. 그러나 데이터 안보 문제는 전통안보와 그 성격이 매우 다르다. 신흥안보의 창발이라는 안보 패러다임의 변화 속에서 봐야 하는 문제이다. 이러한 인식을 반영한 '국가데이터전략계획'(NDSP)이 필요하다. 이를 바탕으로 향후 데이터 안보의 국가전략을 추진해갈 구체적인 실천방안들이 마련되어야 할 것이다. 그 실천방안은, 전통안보의 대책과 같은 획일적 구도가 아니라, 데이터 안보와 관련된 다양한 가치들을 포괄하는 구도에 담겨야 할 것이다.

투 고 일: 2020. 04. 09.
심사완료일: 2020. 05. 22.
게 재 일: 2020. 05. 30.

참고문헌

강동철·오로라. 2019-05-18. "中 '데이터 국외 반출 금지' 美 '해외 미국기업 데이터도 다 관리'."『조선일보』.

강영연. 2013-06-14. "빅데이터가 부른 '빅 브러더 시대'…국가 안보 vs 사생활 침해."『한국경제』.

강하연. 2013. "ICT교역의 글로벌 거버넌스." 서울대학교 국제문제연구소 편.『커뮤니케이션 세계정치』. 기획특집 〈세계정치〉 33(2). 사회평론, pp. 73-109.

강혜란. 2019-02-18. "13억 인구 빅데이터가 무기… 중국 AI, 미국에 1.4년차 추격."『중앙일보』.

구태언. 2019-11-04. "'데이터 주권' 상실, 왜 치명적인가."『디지털타임스』.

김상배. 2015. "빅데이터의 국가전략: 21세기 신흥권력 경쟁의 개념적 성찰."『국가전략』. 21(3), pp. 5-35.

_____. 2018a.『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』. 파주: 한울엠플러스.

_____. 2018b. "초국적 데이터 유통과 정보주권: 국가주권 변환의 프레임 경쟁." 이승주 편.『사이버 공간의 국제정치경제』. 사회평론, pp. 17-51.

_____. 2019a. "화웨이 사태와 미중 기술패권 경쟁: 선도부문과 사이버 안보의 복합지정학."『국제·지역연구』. 28(3), pp. 125-156.

_____. 2019b. "미래전의 진화와 국제정치의 변환: 자율무기체계의 복합지정학."『국방연구』. 62(3), pp. 93-118.

_____. 2020. "4차 산업혁명과 첨단 방위산업 경쟁: 신흥권력론으로 본 세계정치의 변환."『국제정치논총』. 60(2), pp. 1-46.

김주영. 2019-12-09. "北, 중대한 시험은… '백두산 엔진 결합한 정찰위성 가능성 높아'."『파이낸셜뉴스』.

리즈후이. 2019.『데이터를 지배하는 자가 세계를 지배한다』. 남양주: 더봄.

문가용. 2019-11-22. "미국, '영토 외에서 개인정보 저장할 수 없다'는 법 발의."『보안뉴스』.

민재용. 2019-08-30. "데이터에 주권은 없다? 중·일·EU는 자국민 정보 보호 안전장치."『한국일보』.

박세진. 2019-02-04. "'中 견제' 美 중심 새 정보동맹 '파이브 아이즈+3' 출범."『연합뉴스』,

박지영·김선경. 2019. “디지털 무역 경쟁과 데이터 보호주의.” 아산정책연구원, 6월 11일.

박희준. 2013-06-15. “미국 국가안보국(NSA)이 개인정보를 수집하는 유타센터 초미의 관심사.”『아시아경제』.

배준호. 2018-10-29. “‘디지털 패권경쟁’ 본격화… 미국, ‘데이터 TPP’로 대중 포위망 구축 노려.”『이투데이』.

변재현·지민구. 2018-03-20. “페북 사태로 본 ‘빅데이터 독점의 민낯’, 理想사회는 커녕, 異常사회 부르나.”『서울경제』.

우은식. 2019-03-08. “美, ‘反화웨이 동맹’ 흔들리자 통신부품 수출금지 추진.”『뉴시스』.

유세진. 2019-11-03. “러시아 새 독립인터넷법 발효…‘디지털 철의 장막’ 우려.”『뉴시스』.

이상은. 2019-02-07. “페이스북·아마존 '데이터 독점'에 칼 뽑은 EU.”『한국경제』.

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

이조은. 2019-04-09. “미 상원, 인도태평양 사이버 연합체 ‘클립스’ 설립 법안 발의…‘북한 범죄 지속 가능성’.” Voice of America.

정충신. 2019-06-07. “기술·자원·무역 ‘모든 것을 무기로’… 美·中, 이미 ‘3차 대전’.”『문화일보』.

최연진. 2019-11-13. “EU ‘보이지 않는 무역장벽’ GDPR에 돌아서는 한국 기업들.”『한국일보』.

최창영. 2017-07-20. “대한민국 군사용 드론 vs. 북한 군사용 드론.”『아나드론스타팅』.

최평천. 2019-12-11. “‘첩보 위성급’ 美글로벌호크 한반도 비행… 15㎞ 상공서 감시.”『연합뉴스』.

Castells, Manuel. 2000. *The Rise of the Network Society*. 2nd edition. Oxford: Blackwell.

Farrell, Henry and Abraham L. Newman. 2018. “Linkage Politics and Complex Governance in Transatlantic Surveillance.” *World Politics*, 70(4), pp. 515-554.

Gimelstein, Shelli. 2019. “Storm on the Horizon: How the U.S. Cloud Act may interact with Foreign Access to Evidence and Data Localization Laws.” *Data Catalyst Report*. January.

Hansen, Lene and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly*, 53(4), pp. 1155-1175.

He, Laura. 2018. "China's two Largest Surveillance Camera Makers take a Beating from US Ban." *South China Morning Post*. August 3.

Ikenberry, G John. 2014. "The Illusion of Geopolitics: The Enduring Power of the Liberal Order." *Foreign Affairs*, 93(3), pp. 80-90.

Jørgensen, Rikke Frank and Tariq Desai. 2017. "Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google." *Nordic Journal of Human Rights*. 35(2), pp. 106-126.

Lieber, Keir A. and Daryl G. Press. 2017. "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence." *International Security*, 41(4), pp. 9-49.

Liu, Jinhe. 2019. "China's Data Localization." *Chinese Journal of Communication*. DOI: 10.1080/17544750.2019.1649289

Mead, Walter Russell. 2014. "The Return of Geopolitics: The Revenge of the Revisionist Powers." *Foreign Affairs*, 93(3), pp. 69-79.

Petit, Patrick. 2020. "'Everywhere Surveillance': Global Surveillance Regimes as Techno-Securitization." *Science as Culture*. 29(1), pp. 30-56.

Vigdor, Neil. 2020. "U.S. Military Branches Block Access to TikTok App Amid Pentagon Warning." *New York Times*. January 4.

Data Security and Digital Hegemony Competition: From the Perspectives of Emerging Security and Complex Geopolitics

Sangbae Kim

The importance of “data” has recently been emphasized in the process of digital hegemonic competition among major world powers. In particular, data is understood as a critical issue for national security. The emerging mechanism of today’s data security, however, is different from that of traditional military security. The advent of the big data era has led to such differences. The spread of big data power has caused controversy over privacy protection. Increased cyber attacks have sparked controversy over “securitization” of data leaks, and are justifying the surveillance of data featuring terrorist searches. Transnational data flows by multinational companies are being checked in terms of protecting data sovereignty. In the midst of this, data security has become an issue of alliance and coalition diplomacy among major powers, and the importance of data collection activities through intelligence networks and military reconnaissance satellites has also increased. Even in the traditional military areas, big data capabilities have become a key element in deploying future warfare. In this process, the controversial data itself is not the one containing “contents” directly related to national security. Rather, it is the one that is transformed through its unique quantitative and qualitative mechanisms, and further emerged as a geopolitical issue in the digital hegemonic competition. This paper adopts the perspective of emerging security and complex geopolitics to analyze the world politics of data security and explores its national strategic implications.

Keywords: Data Security, Securitization, Data Sovereignty, Digital Hegemony, Emerging Security, Complex Geopolitics