▣ 논 단

디지털 무역과 개인정보 보호:

공동 컨트롤러 개념의 필요성을 중심으로

법무부 국제법무지원과 공익법무관, 서울대학교 상법 박사과정 이 동 건

*논문접수 : 2025. 4. 18. *심사개시 : 2025. 4. 21. *게재확정 : 2025. 5. 2.

〈목 차〉

Ⅰ. 서론

디지털 무역은 급격히 변화하는 글로벌 경제 환경에서 중요한 경제 활동으로 자리 잡았다. 인터넷과 정보통신기술(Information and Communications Technology, ICT)의 발전이 무역을 물리적 제약으로부터 자유롭게 하는 동시에 그 개념의 외연을 확장한 것이다. 기술의 발전은 국가 간 물리적 제약을 넘어, 디지털 플랫폼을 통해 상품과 서비스의 교환이 이루어지는 새로운 형태의 무역을 만들어냈다. 또한, 무역의 개념은 이제 단순히 전통적인 상품과 서비스

의 거래를 넘어, 데이터, 소프트웨어, 그리고 다양한 디지털 상품과 서비스의 교환을 포함하게 되었다. 이러한 패러다임 시프트(paradigm shift)는 기업뿐만 아니라 개인에게도 다양한 기회를 제공하고 있으며, 국가 경제에도 중대한 영향을 미치는 현대 상업활동의 핵심 요소가 되었다. 지금부터 약 11년 전인 2014년에 이미 미국과 유럽연합(European Union, EU) 간 서비스 분야 무역의 30%는 온라인을 통해 이루어졌다.[1] 그러나 디지털 무역의 급성장과 함께 여러 법적, 규제적 문제들이 대두되고 있다.[2] 그 중에서도 최근 강조되고 있는 것이 개인정보 보호이다.

디지털 경제가 성장하면서, 개인정보 보호는 경제적 가치와 연결되는 중요한 자원으로 인식되고 있다. 기업들은 소비자 데이터와 거래 데이터를 인공지능(Artificial Intelligence, AI)에 학습시키고, 이를 활용해 서비스 품질을 개선하거나 소비자에게 맞춤형 광고를 제공하는 등의 방식으로 경쟁력을 높이고 있다. 한편, 각국은 개인정보의 중요성을 다시 새기며 이를 보호하기 위한 규제를 강화하고 있기도 하다. 우리나라 또한 헌법재판소가 2005년 개인정보자기결정권을 헌법상의 독자적인 기본권으로서 헌법에 명시되지 않은 기본권이라는 점을 확인하였고, 그 근거로 헌법에서 인간의 존엄과 가치 및 행복추구권을 규정한 제10조와 사생활의 비밀과 자유를 규정한 제17조를 들었다.[3] 개인정보자기결정권은 '정보 주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리'로 정의된다. 우리 입법자들은 개인정보자기결정권을 바탕으로 개인정보 보호법을 제정하였다. 하지만, 이러한 규제는 디지털 무역의 활성화에 제약을 가할 수 있다. 특히 데이터 활용을 지나치게 엄격하게 규제할 경우 세계무역기구(World Trade Organization, WTO) 회원국의 시장 개방 확대를 취지로 하는 우루과이 라운드(Uruguay Round, UR) 협정에 위반될 수 있다. 결국 혁신과 규제를 어떻게 조화시킬 것인지가 중요한 법적 과제가 된다.

실제로 개인정보 보호에 관한 국가별 법령의 차이가 디지털 무역에 큰 영향을 미치고 있다. 예를 들어, 2018년 5월 25일부터 시행된 유럽연합(EU)의 「일반정보보호규정(General Data Protection Regulation, GDPR)」[4]은 기업들이 글로벌 시장에서 데

1) Tourkochoriti Ioanna, "The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide Between U.S.-EU in Data Privacy Protection", University of Arkansas at Little Rock Law Review, Vol. 36, 161-162, 2014.

2) 김흥종, "디지털 무역 규범의 국제 논의와 한국의 대응" 통상법률, 2020년 4호, 3면, 2020.

3) 헌법재판소 2005. 5. 26. 선고 99헌마513 결정.

이터를 처리하고 거래하는 방식에 중대한 영향을 미쳤고, 결과적으로 많은 글로벌 기업들로 하여금 EU 회원국에서 제공하는 서비스의 회원가입 화면 등을 다른 나라에서의 화면과 다르게 설정하도록 하였다.

디지털화로 인해 디지털 서비스의 세계화가 진행되는 한편, 각국은 자국의 경제적 이익을 보호하기 위해 개인정보 보호를 위한 규제를 강화하고 있다. 이에 대해, 통상법적 차원에서 보면 현행 WTO 체제하에서 서비스 무역에 관한 일반 협정(General Agreement on Trade in Services, GATS) 제14조 예외의 인정을 엄격하게 하고 있어 개인정보 보호를 이유로 한 데이터 이전 제한이 인정되지 않을 가능성이 있다. 현재 세계 곳곳에서 디지털 무역과 개인정보 보호 간의 갈등이 발생하고 있으며, 이를 해결하기 위한 법적 접근이 중요한 시점에 있다.

개인정보의 활용과 보호 간 균형점을 찾고, 개인정보 유출 등 문제 발생 시 책임소재를 명확히 규정하는 일은 개인정보와 관련한 통상 갈등을 예방하기 위한 가장 좋은 해결책이 될 것이다. 그럼에도 WTO 통상 규범에서는 데이터 제한의 근거가 되는 개인정보 보호와 관련한 구체적인 규범이 부존재하는 것이 현재 상황이다. WTO 내에서는 개인정보 보호를 위해 데이터 국외 이전을 제한하고 빅테크 기업들을 규제해야 한다는 목소리와, 과도한 규제는 무역 장벽으로 작용한다는 목소리가 대립하고 있는 것으로 보인다. 미국은 WTO 전자상거래 협상(Joint Statement Initiative on Electronic Commerce at the World Trade Organization, WTO JSI)에 대한 지지 철회를 밝히기 전까지 개인정보를 포함한 정보의 자유로운 이전을 추구한 반면, EU는 GDPR과 같은 규제로 정보 주체의 개인정보를 보호하는 기조를 이어왔다.

본 논문의 목적은 디지털 무역과 개인정보 보호라는 두 가지 주요 이슈가 통상법적 관점에서 어떻게 상호작용을 하는지 분석하고, 혁신과 규제 사이에서 균형을 이루는 보편적인 글로벌 프라이버시 규범을 제시함에 있다. 특히, 보편적인 글로벌 프라이버시 규범으로 EU GDPR의 공동 컨트롤러 개념의 채용을 제시하고자 한다. 나아가 디지털 무역에서의 개인정보 보호 규제가 자유무역의 흐름을 방해하는 요소로 작용하는 경우, 이를 해결하기 위한 통상법적 접근 방안을 제시하고자 한다.

4) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Ⅱ. 디지털 무역의 개념과 발전

1. 디지털 무역의 정의와 특징

디지털 무역(digital trade)에 대한 확립된 정의는 없지만, 정보통신기술(ICT)을 기반으로 한 물품 및 서비스의 거래를 의미한다는 컨센서스(consensus)가 형성되고 있다.[5] 전통적인 무역이 물리적 상품의 이동을 중심으로 이루어졌다면, 디지털 무역은 데이터, 소프트웨어, 디지털 콘텐츠, 전자상거래 및 클라우드 컴퓨팅 서비스 등 무형의 자산과 관련된 거래가 주를 이룬다. 디지털 무역은 물리적인 국경을 넘는 거래로, 거래 당사자들이 실시간으로 상품과 서비스를 교환할 수 있게 한다.

디지털 무역의 주요 특징은 다음과 같다.

첫째, 시간과 장소의 제약이 없다. 디지털 무역은 주로 데이터 교환을 중심으로 이루어지기 때문에, 특정한 시간과 장소를 지정하여 물건의 거래가 이루어지는 전통적인 무역과 달리 언제 어디서나 이루어질 수 있다. 다만, 이러한 경우에도 결국 거래의 대상이 국경을 넘어 이동하는 것은 동일한바, 데이터의 국경 간 이동이 디지털 무역 규제의 핵심 요소가 된다.

둘째, 플랫폼 기반의 거래가 이루어진다. 디지털 무역은 다양한 온라인 플랫폼을 통해 이루어진다. 예를 들어, 우리가 흔히 이용하는 아마존, 알리바바, 이베이와 같은 전자상거래 플랫폼에서 이루어지는 거래가 디지털 무역의 대표적인 예시이다. 전통적인 무역이 성립하려면 거래 당사자들이 물품의 품질 및 상태를 확인하고 거래에 관한 의사를 표시할 물리적인 공간이 필요하였다. 다른 지역 또는 다른 국가의 사람끼리 무역을 하기 위해 접근성이 좋은 항구나 접경지역 등에 상인들이 몰리고는 하였다. 무역의 디지털화에 따라 플랫폼이 그 공간을 대체하였고, 물품의 우수성을 홍보하는 역할은 판매자 자신에게서 판매자가 사진과 영상으로 구성한 상세 페이지로 넘어가게 되었다. 결제조차 디지털화된 지금, 상인들은 예전처럼 손님을 붙잡고 상품을 구매하도록 열심히 설득한 다음 대금을 지불받을 때까지 긴장을 놓지 않는 노력을 할 필요가 없다. 상인이 자는 사이에도 상세 페이지가 세계 각지의 잠재 고객들에게 제품을 홍보하고, 고객들이 제품을 구매하고 결제 버튼을 누르면 주문 내역이 정리되어 다음날 아침 상인의 컴퓨터 화면에 나타난다. 디지털 무역은 몇백 년간 축적되어 온 무역 및 상업의 근본적인

5) González Javiel López and M. Jouanjean, “Digital Trade: Developing a Framework for Analysis”, OECD Trade Policy Papers, No. 205, OECD Publishing, 6, 2017.

전제들을 뒤엎어버린 것이다.

셋째, 소프트웨어 및 서비스의 거래가 이루어진다. 디지털 무역은 소프트웨어 라이센스, 클라우드 서비스, 디지털 콘텐츠와 같은 비물질적 자산을 포함한다. 기술의 발전은 무역의 방법만 변화시킨 것이 아니라 무역의 대상조차 변화시킨 것이다. 이는 무역의 개념의 외연을 확장한 것으로써, 디지털 무역은 물리적 상품을 거래하는 전통적인 무역과는 다른 차원의 무역이라고도 표현할 수 있을 것이다.

2. 디지털 무역의 글로벌 현황

디지털 무역은 최근 몇 년간 급격히 성장하였으며, 특히 팬데믹 이후 더욱 가속화되었다. 전 세계적으로 여러 국가가 디지털 경제의 중요성을 인식하고, 이를 위한 법적 및 정책적 기반을 마련하고 있다. WTO는 디지털 무역을 촉진하기 위한 여러 가지 정책을 추진 중이며, 많은 자유무역협정(Free Trade Agreement, FTA)에도 디지털 무역에 관한 규정이 포함되고 있다.

특히, 아시아 태평양 지역에서는 디지털 무역의 성장이 두드러진다. 동남아시아 국가연합(Association of Southeast Asian Nations, ASEAN), 역내포괄적경제동반자협정(Regional Comprehensive Economic Partnership, RCEP) 등 지역적 협정은 디지털 무역의 규제를 포함한 협정을 강화하고 있으며, 이는 글로벌 디지털 무역의 기반이 되고 있다. ASEAN은 2023년 9월 3일 회원국 간 디지털 무역을 더욱 활성화하기 위한 「ASEAN 디지털 경제 프레임워크 협정(ASEAN Digial Economy Framework Agreement, DEFA)」협상을 개시하였으며, 2025년까지 이를 타결하는 것을 목표로 하고 있다.[6] 현재 베트남 등 디지털 인프라 구축에 많은 노력을 투입하고 있는 ASEAN 회원국은 기술 격차, 사이버 보안 및 규제 공백 등의 난관을 맞닥뜨리고 있다.[7] DEFA는 ASEAN 회원국 간 기술 격차를 해소하고 디지털화를 촉진함으로써 위와 같은 상황의 타개책이 될 수 있을 것이다.

우리나라도 다양한 디지털 협정에 가입하여 디지털 무역의 영역을 확대하고자 하고 있다. 먼저, 우리나라는 2022년 11월 21일 「한-싱가포르 디지털 동반자협정(Korea-Singapore Digital Partnership Agreement, KSDPA)」에 정식 서명하였고, 협정문 내 발효 규정에 따라 교환일로부터 30일 이후인 1월 14일에 위 협정이 발효되었다. KSDPA

6) https://asean.org/asean-launches-worlds-first-regionwide-digital-economy-framework-agreement/.

7) Zulianto Mukhamad, “ASEAN Digital Economy Framework Agreement (DEFA): Opportunities and Challenges for Vietnam”, Asia Pacific Journal of Public Policy, 10(01), 61, 2024.

의 분야별 조항을 표로 정리하면 다음과 같다.[8)]

<표 1> KSDPA 분야별 주요 조항 정리

분야	주요 조항
전자상거래 원활화	전자적전송 무관세
	전자인증·전자서명
	전자송장
	전자지급
	종이서류 없는 무역
디지털 비즈니스 활성화	디지털제품 비차별대우
	국경간 정보이전 원활화
	컴퓨터설비 현지화 요구 금지
	소스코드 공개 요구 금지
	인공지능·핀테크·디지털경제 표준 협력 등
온라인 소비자보호	개인정보 보호
	온라인소비자 보호
	스팸 메시지 규제
	사이버 보안

나아가 우리나라는 2021년 10월부터 「디지털경제동반자협정(Digital Trade Economy Partnership Agreement, DEPA)」 가입 절차를 개시한 후 2년간 총 6차례의 협상을 거쳐 2024년 5월 3일 DEPA 1호 추가 가입국이 되었다. 총 16개의 모듈과 1개의 부속서, 1개의 개정의정서로 구성된 DEPA 협정문은 디지털 경제와 기술 진보를 위한 관련 규범 및 협력을 지속적으로 진화시킬 필요성과 포용적 무역의 가치를 확인하는 내용을 담고 있다.[9)]

한편, EU는 회원국 간 디지털 무역을 활성화해 혁신적인 비즈니스 모델을 갖춘 유럽 기업이 자국 시장에만 머무르는 것이 아니라 EU 전체를 서비스 대상으로 하여 성장할 수 있도록 EU 회원국 간 무역 환경의 통일성을 꾀했다. 2015년 5월 발표된 EU의 디지털 단일시장 전략(Digital Single Market strategy, DSM strategy)은 EU 내부의 디지털 무역 환경을 촉진하기 위해 다양한 법적 틀을 마련하고자 한 시도였다.[10)]

EU는 위 전략을 바탕으로 회원국 사이의 디지털 장벽을 허물어 '디지털 단일시장'을 구축함으로써 연합 차원에서 글로벌 경쟁력을 갖추겠다는 목표를 세웠다.[11)] DSM 전략의 3대 과제 및 이를 달성하기 위한 16개 세부 의제를 정리하면 다음과 같다.[12)]

8) 산업통상자원부 2023. 1. 13. 보도자료 "1. 14일 「한-싱가포르 디지털동반자협정」 발효 – 양국 간 디지털 교역 확대 및 디지털 기술·비즈니스 협력 강화 기대 -".

9) 관계부처 합동, "디지털경제동반자협정(DEPA) 상세 설명자료", 2-41면, 2024.

10) 김정곤, 나승권, 장종문, 이성희, "EU 디지털 단일시장 전략의 주요 내용과 시사점", 오늘의 세계경제, Vol. 15, 3면, 대외경제정책연구원, 2015.

11) EUROPEAN COMMISSION, "A digital Single Market for Europe: commission sets out 16 initiatives to make it happen", 2015.

12) 김선호, "EU 디지털 단일시장 전략 분석", 2015년 1권 7호, 한국언론진흥재단 연구센터, 5면, 2015.

<표 2> 'EU 디지털 단일시장 전략' 3대 과제 요약

3대 과제	16개 세부의제
국경을 초월한 상품 및 서비스 접근을 위한 장벽 제거	EU 국가 간 전자상거래/배송
	지역적 차단조치 (geo-blocking) 해소
	저작권 보호를 받는 콘텐츠에 대한 접근
	온라인 상품 거래에 대한 부가가치세
디지털 네트워크 및 콘텐츠 서비스 발전을 위한 조건과 환경 조성	통신 단일시장
	시청각 미디어 서비스
	온라인 플랫폼/ 중계 서비스
	개인정보 보호/ 사이버 보안
디지털 경제 성장 잠재력 극대화	데이터 기반 경제
	호환성 및 표준화
	디지털 기술, 전문가 육성 및 교육
	전자정부

DSM 전략의 실행에 의해 EU 회원국 간 무역에 찾아온 변화는 다음과 같다.

첫째, EU는 국경을 초월한 상품 및 서비스 접근을 위한 장벽 제거라는 목적을 달성하고자 다양한 입법적 시도를 하였다. 대표적으로는 EU 회원국 간 로밍 금지와 부당한 지역적 차단 조치에 관한 규정이 있다.

2017년 6월 발효된 후[13] 2022년 전면 개정(recast)된 「유럽연합 로밍 규정(Roam-Like-At Home Regulation, R LAH)」[14]은 이동통신사업자로 하여금 A회원국에서 가입한 EU 소비자가 B 회원국에서 단기 로밍 서비스 이용 시 로밍 비용을 부과하지 못하도록 하였다.

다음으로, EU는 2018년 2월 「부당한 지역적 차단 조치 규정(Geo-Blocking Regulation)」[15]을 제정하여 EU 기업들로 하여금 EU 소비자들의 국적이나 거주지 등을 이유로 가격을 다르게 청구하거나 물품이나 서비스에 대한 접근 가부를 차별하는 것을 금지하였다. 예를 들어, 이전에는 독일 국민이 프랑스에 소재한 기업의 물품을 구매할 경우, 프랑스 국민에게 제공되는 가격보다 더 비싸게 물품을 구매해야 하였으나, 「부당한 지역적 차단 조치 규정」시행 이후에는 위와 같은 행동이 금지된다.

둘째, EU는 디지털 네트워크 및 콘텐츠 서비스 발전을 위한 조건과 환경 조성을 위해 개인정보 보호와 시장 질서 구축 관련 규정들을 제정하였다. 먼저, EU는 디지털 네트워크 및 콘텐츠 서비스 발전 과정

13) 2017년 당시 규정은 Regulation (EU) 2015/2102 참조.

14) Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union(recast).

15) Regulation (EU) 2018/302 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market.

에서 EU 시민의 프라이버시가 부당하게 침해되는 것을 방지하기 위한 수단으로 GDPR과 「개인정보 보호 및 전자 통신 지침(ePrivacy Directive)」[16]을 내세웠다.[17] ePrivacy Directive는 실무상 'EU 쿠키법'[18] 또는 'EU 쿠키지침'[19]이라고 불리는 EU 지침으로서 정보통신 분야에서 쿠키 사용(제25조)과 이메일 마케팅 방법(제40조) 등을 규제한다.

GDPR은 ePrivacy Directive를 보완하고 일부 요구사항을 강화하지만 기본적으로 병렬적으로 적용되는 구조이다. 이는 GDPR 제95조에서도 명시적으로 규정되어 있다.

Article 9. Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

한편, EU는 2023년 8월 25일에는 건전한 시장 질서 구축을 위해 디지털서비스법(Digital Services Act, DSA)을, 2024년 3월 7일 디지털시장법(Digital Markets Act, DMA)을 시행하였다. DSA는 온라인 플랫폼에 불법 콘텐츠를 규제할 의무를 부과하는 것을 주요 골자로 하고 있으며, DMA는 불공정거래를 방지하는 것을 핵심 내용으로 하고 있다. 특히 DMA는 EU DMA는 온라인 플랫폼이 급속도로 발전하면서 발생하는 반경쟁적 문제들을 해소하는 데 기여할 수 있을 것이라고 평가받고 있다.[20]

셋째, EU는 디지털 경제 성장 잠재력 극대화를 위해 EU는 온라인 콘텐츠 서비스의 이식성(portability)을 보장하였다. 2018년 1월부터 EU 소비자들은 회원국에서 TV 시리즈나 영화를 온라인에서 시청하고자 구매한 경우, 다른 회원국에서 이에 접속할 때 추가 비용을 내거나 접속이 금지

16) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.

17) EU-Commission, "A Digital Single Market Strategy for Europe" COM 192 final, 13, 2015.

18) https://www.cloudflare.com/ko-kr/learning/privacy/what-is-eprivacy-directive/.

19) https://www.lexology.com/library/detail.aspx?g=77cae731-0a1e-4049-97eb-c3b61f51b020.

20) 최요섭, "A Critical Review of the EU's Digital Markets Act - Possible Impacts on the Digital Economy -", 중앙대학교 법학연구원, 法學論文集, 45(1), 제251면, 2021.

되지 않는다.[21]

EU의 DSM 전략은 EU 내 불필요한 경쟁을 해소하고 상호 협력체제를 구축함으로써 경제적 이익을 창출하고자 하였다. 최근 연구에 따르면, 2017년「유럽연합 로밍 규정」발효로 인해 증가한 소비자들의 이익이 이동통신사업자들의 손실보다 크고, 매년 약 10억 유로의 경제적 잉여(total welfare surplus)를 창출한 것으로 분석된다.[22]

디지털 무역의 성장에 따라, 국제적으로 데이터 보호와 관련된 규제가 중요한 이슈로 떠오르고 있으며, 각국은 자국의 경제적 이익을 보호하기 위해 데이터 주권을 강화하고 있다. 그러나 이와 같은 규제 강화는 다른 국가와의 무역에서 중요한 법적 갈등을 유발하고 있다.

3. 디지털 무역에 대한 법적 접근

디지털 무역의 급성장에 따라, 이에 대응하기 위한 법적 규제가 필요하다. 기존의 무역 규범은 디지털 무역의 특성을 충분히 반영하지 못하고 있으며, 각국은 디지털 무역에 대한 규제를 자국의 이익을 우선으로 설정하고 있다. WTO는 디지털 무역과 관련된 논의를 촉진하기 위해 여러 차례 회의를 개최했으나, 국제적으로 통일된 규정은 아직 미비한 상태이다.

디지털 무역에서 가장 큰 법적 이슈 중 하나는 데이터의 국경 간 이동에 관한 규제이다. 일부 국가들은 자국의 데이터를 자국 내에 보관하도록 요구하는 데이터 로컬라이제이션(data localization) 정책을 채택하고 있다. 최대한 많은 양의 고품질 데이터를 수집하여 AI에 학습시킴으로써 서비스의 개선을 꾀하고자 하는 디지털 서비스 기업들 입장에서 데이터 로컬라이제이션 정책은 일종의 무역 장벽으로 작용할 수 있다. 디지털 무역장벽은 국가 간 디지털 무역에서 장애가 될 수 있는 정책적 규제나 기술적 장벽을 뜻한다.

디지털 무역의 법적 틀을 마련하는 데 있어, 국제 협정은 중요한 역할을 할 수 있다. 그러나 각국의 규제 차이가 존재하기 때문에, 이를 해결하기 위한 다자간 협정 등 새로운 국제법적 규범이 필요하다.

21) Like Andrine, Leo Peeters, “The end of geo-blocking, and the portability of digital services in the European Union”. Seeds of Law, 2018.

22) Canzian Giulia, Gianluca Mazzarella, Louis Ronchail, Frank Verboven & Stefano Verzillo, “Evaluating the impact of price caps - evidence from the European roam-like-at-home regulation”, SSRN Electronic Journal, 16-19, 2021.

Ⅲ. 개인정보 보호의 글로벌 규제 현황

1. 개인정보 보호의 필요성과 국제적 요구

디지털 무역의 확장과 더불어 개인정보 보호의 중요성은 날로 커지고 있다. 디지털 기술이 발전하면서 기업과 정부는 점점 더 많은 개인정보를 수집하고 활용하고 있다. 특히, 전자상거래와 같은 디지털 플랫폼에서 사용자 데이터는 맞춤형 광고나 서비스 개선 등을 위한 중요한 자원으로 간주된다. 그러나 이러한 데이터가 기업에 의해 악용될 수 있다는 우려와 함께, 개인의 프라이버시를 보호해야 한다는 국제적 요구가 제기되었다.[23]

개인정보 보호는 단순히 개인의 권리를 보호하는 차원에서 그치지 않고, 신뢰 구축, 데이터 경제의 지속 가능성 및 국제적으로 인정받는 규범의 형성이라는 측면에서도 중요한 문제이다. 개인정보 보호가 제대로 이루어지지 않으면, 디지털 무역에서의 거래 참여자 간의 신뢰가 감소하고, 이는 전체적인 디지털 경제 발전에 걸림돌이 될 수 있다. 이에 따라 여러 나라가 개인정보 보호법을 제정하고 개인정보 보호를 강화하는 방향으로 나아가고 있다.

2. 주요 국가 및 지역의 개인정보 보호 법제

개인정보 보호 법제는 각국의 법적, 사회적, 경제적 배경에 따라 다른 모습을 띠고 있다. 그러나 최근 몇 년간 범지구적으로 개인정보 보호의 법적 틀이 강화되었으며, 그 중 대표적인 규제가 EU의 GDPR과 미국의 캘리포니아 주 프라이버시 권리법(California Privacy Right Act, CPRA)이다.[24]

2018년 5월 25일 시행된 EU GDPR은 세계에서 가장 포괄적이고 강력한 개인정보 보호법으로 평가된다.[25] 유럽의회(European Parliament) 역사상 가장 많은 로비가 이루어진 법안이라는 기록을 세웠다는 그 파급력을 엿볼 수 있다.[26] 다만, 이에 대해 GDPR의 개인정보 보호 수준이 일반적인 소비자 보호 수준을 넘어서는 과도한 규제로서, EU 시장에서 경쟁력을 확보한 미국 빅테크 기업 등에 상대적으로 큰 부담을

23) https://news.un.org/en/story/2013/12/458232.

24) CPRA는 2018년 제정된 캘리포니아 주 소비자 개인정보보호법(California Consumer Privacy Act, CCPA)의 개정 법률로서, 본래 EU의 GDPR과 대응되던 미국의 법률은 CCPA였다.

25) https://www.consilium.europa.eu/en/policies/data-protection-regulation/

26) European Commission, “LIBE Committee Vote Backs New EU Data Protection Rules.”, 2013.

초래할 것이라는 비판도 있다.[27] 전문가들은 GDPR이 EU 회원국뿐만 아니라 EU 외에 소재한 국가 및 기업의 개인정보 활용 관련 관행에도 변화를 촉구할 것으로 예상하기도 한다.[28] 실제로 언론에서도 GDPR이 EU의 개인정보 보호 기준을 전 세계에 수출하고 있다고 평가하며 이를 '브뤼셀 효과'라고 명명하고는 한다.[29]

GDPR의 입법 연혁은 다음과 같다. EU는 1995년 10월 「개인정보의 처리와 개인정보의 자유로운 유통에 관련된 개인정보 지침」(Directive 95/46/EC)[30]를 채택하였다. 그러나 지침이라는 법형식의 특성으로 인해 EU 회원국에게 이행을 강제할 수 없다는 한계가 있었다. 이에 따라 EU 각 회원국의 개인정보 관련 규율이 통일되지 않음으로 인한 문제들이 발생하였으며, 개인정보의 처리에 있어서 모호한 법적 불확실성이 항상 남아있었다. EU 내에서 구속적인 규범체계의 확립을 요구하는 목소리가 높아짐에 따라 EU 전역에 통일적으로 적용될 개인정보 보호법의 제정을 위한 움직임이 개시되었다. EU 집행위원회(European Commission)는 2009년 7월부터 회원국들의 의견을 수렴하는 절차에 돌입하여, 2012년 1월 25일 GDPR의 초안을 공표하였으며, EU 입법기관인 유럽의회와 EU 이사회(Council of the European Union)에 위 초안이 제출되었다. 이후 2016년 4월 8일 EU 이사회의 최종 법안 채택과 2016년 5월 4일 유럽의회의 최종법안 채택을 거쳐 2016년 5월 4일 EU 공보에 공포된 후 2016년 5월 2일 발효되어, 2년의 유예기간이 지난 2018년 5월 25일부터 시행된 것이다.

GDPR의 발효에 따라, 기존의 Directive 95/46/EC는 GDPR로 대체되었다. Directive 95/46/EC와 GDPR의 가장 핵심적인 차이는 EU 법체계상 Directive와 Regulation의 차이에 있다. EU 법체계에 따르면, Directive는 회원국에서 직접적으로 적용되지 않는다.[31] 다만 각 회원국은 Directive에 따라 입법할 의무를 갖게 되므로, 위 지침이 명령하는 바를 참고하여 국가별로 개별 입법을 진행하게 된다. 한편 Regulation의 경우, 발효 즉시 법적 효력을 가지며, 회원국의 개별 국내법에 우선하여 적용된다.

27) https://www.verdict.co.uk/has-five-years-of-gdpr-stifled-tech-innovation/?utm_source=chatgpt.com&cf-view.

28) 오태현, 강민지, "EU 개인정보보호법(GDPR) 발효: 평가 및 대응방안", 오늘의 세계경제 Vol. 18 No. 19, 대외경제정책연구원, 14면, 2018.

29) https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/.

30) Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

31) Directive는 회원국에 대해서 곧바로 적용되기는 하나, 회원국 내에서 법률로서의 효력이 없다.

따라서 각 회원국이 지침을 참고하여 개별적인 개인정보 보호법 입법을 진행했던 기존 Directive 95/46/EC와는 달리, GDPR은 그 자체가 각 회원국의 국내법에 우선하여 적용되는 법률로서의 효력을 갖는다.[32]

GDPR은 EU 내에서 개인정보 처리와 관련된 모든 활동에 적용된다. 또한, GDPR은 데이터 주체의 권리를 강화하고, 기업에게 더 높은 수준의 투명성과 책임을 요구한다. 나아가 GDPR은 데이터의 국경 간 이동에 대한 명확한 규정을 두고 있으며, EU 외부 국가에도 영향력을 미친다. GDPR의 특징 중 하나는 EU와 거래를 하는 국가들로 하여금 GDPR에 따라 데이터를 처리하게끔 한 것이다.

미국의 대표적인 개인정보보호법인 CPRA를 설명하기에 앞서, CPRA가 계승한 「캘리포니아 소비자 개인정보 보호법」(California Consumer Privacy Act, CCPA)을 설명하고자 한다. 2020년 1월 1일에 시행된 미국의 CCPA는 캘리포니아주 내 소비자의 개인정보 권리를 강화하는 데 중점을 두고 있다. 또한 캘리포니아주 내 소재한 기업이 아니라 하더라도 ① 연간 수익이 2,500만 달러 이상이고, ② 5만 명 이상의 소비자(또는 가구/기기)의 개인정보를 수집하며, ③ 연간 매출의 50% 이상을 개인정보 판매로부터 얻는 경우에는 CCPA 적용 대상이 된다. CCPA는 개인정보를 수집하는 기업에 대해 소비자에게 어떤 정보를 수집하는지 투명하게 고지하도록 요구하며, 소비자는 자신이 제공한 개인정보에 대해 통제할 수 있는 권리를 갖는다. CCPA는 특히 데이터 접근권, 삭제권 등을 강화하여 소비자 보호를 강조하고 있다.

CCPA는 EU의 GDPR 제정에 영향을 받아 만들어진 법률이고, CPRA는 CCPA를 계승한 법률이므로, 결과적으로 CPRA도 GDPR에 지대한 영향을 받은 법률이라고 평가할 수 있을 것이다. 그러나 CPRA는 접근 방식과 적용 범위에 있어 GDPR과 차이가 있다. 첫 번째로 GDPR과 CPRA는 보호하고자 하는 정보 주체의 범위에서 차이가 있다. GDPR은 EU 시민을 정보 주체로 하는 반면, CPRA는 기본적으로 캘리포니아 주 법인 만큼 캘리포니아 주민을 정보 주체로 하고 있다. 두 번째로 GDPR과 CPRA는 적용 대상에서 차이가 있다. GDPR의 경우, 정보 주체인 EU 시민의 개인정보를 처리하는 모든 기업, 기관 및 개인을 적용 대상으로 하고 있다. 이와 달리 CPRA는 특정 기준을 충족하는 기업만을 적용 대상으로 하고 있다. 세 번째 차이점

32) 김인석 외, “국제적 상호운용성 강화 및 지능정보화 시대에 부응한 발전방안 연구”, 개인정보보호위원회 연구보고서, 고려대 산학협력단, 5면, 2016; 함인선, 위의 논문, 411면 등 참조.

은 정보 주체로부터 '동의'를 받는 방식과 관련하여, 어떤 방식이 적법한 동의에 해당하는지에 관한 기준이다. GDPR은 정보 주체로부터 사전에 동의를 받는 옵트인(opt-in) 중심 동의 기준을 설정한 반면, CPRA는 정보 주체가 사후에 거부 의사를 표시하여야 비로소 정보처리를 멈추는 옵트아웃(opt-out) 중심 동의 기준을 설정하였다. 다만, CPRA도 16세 미만의 정보 주체로부터 동의를 받는 경우에는 옵트인 동의를 받도록 하고 있다. 마지막으로 CPRA는 정보주체의 권리로 열람, 삭제, 정정 등을 보장하고 있는데, GDPR은 여기서 더 나아가 이의제기권(right to object), 처리 제한권(right to restrict processing), 동의 철회권(right to withdraw consent) 등 더 폭넓은 권리를 정보 주체에게 보장하고 있다.

2011년 9월 30일 시행되어 현재까지 지속적으로 개정되어 오고 있는 한국의 개인정보 보호법은 개인정보 처리와 관련된 법적 기준을 명확히 하고 있으며, 정보 주체의 권리 보호에 중점을 둔다. 우리 개인정보 보호법은 제정 과정에서부터 GDPR의 전신인 Directive 95/46/EC를 주요 참고 자료로 활용하였으며,[33] 현재도 GDPR의 영향을 받아 개인정보 보호에 대한 법적 틀을 강화하고 있다.

우리 개인정보 보호법은 대한민국 내 모든 정보 주체를 대상으로 하고, 개인정보를 처리하는 모든 기업 및 기관에 적용된다. 이용자로부터 개인정보 처리 관련 동의를 받고자 할 경우 GDPR과 같이 사전동의(옵트인)를 받도록 하는 방식을 채택하고 있으며[34], 나아가 당해 개인정보가 민감정보에 해당할 경우에는 정보 주체로부터 명시적인 동의를 받도록 하고 있다.[35] 또한 GDPR과 유사하게 정보 주체에게 자신의 개인정보와 관련하여 열람권, 정정권, 삭제권, 처리 정지권, 동의 철회권 등을 보장한다.

제35조(개인정보의 열람)

① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

제36조(개인정보의 정정·삭제)

① 제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되

33) 최경진, "EU GDPR의 분석 및 시사점", 네이버 프라이버시 백서, 40면, 2016.

34) 개인정보 보호법 제15조 제1항 제1호.

35) 개인정보 보호법 제23조 제1항 제1호.

어 있는 경우에는 그 삭제를 요구할 수 없다.

제37조(개인정보의 처리정지 등)

① 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구하거나 개인정보 처리에 대한 동의를 철회할 수 있다. 이 경우 공공기관에 대해서는 제32조에 따라 등록 대상이 되는 개인정보 파일 중 자신의 개인정보에 대한 처리의 정지를 요구하거나 개인정보 처리에 대한 동의를 철회할 수 있다.

디지털 무역에 개인정보 보호법과 GDPR의 가장 큰 차이는 개인정보 보호법상 개인정보 처리자와 GDPR의 컨트롤러(controller)·프로세서(processor)의 개념적 차이에 있으며, 이에 대해서는 후술한다.

3. 개인정보 보호와 디지털 무역 간의 갈등

디지털 무역의 주요 특성 중 하나는 데이터 국경 간 이동이다. 그러나 개인정보 보호 규제는 각국의 법체계에 따라 상이하기 때문에, 국제적으로 통일된 규제 체계가 부족한 상황이다. 유엔무역개발회의(UNCTAD)도 2016년 보고서에서 지역 간 개인정보 보호 법체계의 차이로 인해 상호운용성(interoperability)에 문제가 발생할 수 있다고 평가한 바 있다.[36] 이는 기업 운영뿐만 아니라 소비자 보호에도 부정적인 영향을 미칠 것이다. EU 회원국 등 일부 국가들은 자국민의 데이터를 자국 내에서 보관하도록 요구하는 반면, 다른 국가들은 데이터의 자유로운 이동을 주장한다. EU의 GDPR은 외국 기업으로 하여금 EU 시민의 데이터를 수집했을 경우, 그 데이터를 EU 외 서버에 저장하는 것이 아니라, EU 내에 위치한 서버에 저장하도록 하는 데이터 로컬라이제이션(data localization)을 요구한다. 물론 GDPR에 명시적으로 데이터 로컬라이제이션을 요구하는 규정은 없지만, 데이터의 역외 이전을 엄격하게 규제함으로써 사실상의 데이터 로컬라이제이션(de facto data localization)을 요구하고 있다는 것이 실무상 널리 받아들여지고 있다.[37] 이처럼 데이터에 국경 개념을 도입하는 구조는 다른 국가들과 데이터를 공유하고자 하는 유인을 감소시킴으로써 자유로운 데이터 흐름을 제한할 수 있다. 이는 더 나아가 법적 갈등으로 이어질 수도 있

36) United Nations Conference on Trade and Development, “Data Protection Regulations and International Data Flows: Implications for Trade and Development”, United Nations, 32, 2016.

37) https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities.

을 것이다. 이에 대해서는 다음 목차에서 자세히 설명하고자 한다.

Ⅳ. 디지털 무역과 개인정보 보호의 충돌

1. 데이터 국경 간 이동 문제

디지털 무역에서 데이터는 핵심적인 역할을 한다. 정보는 물리적인 국경을 넘어 자유롭게 이동하며, 이는 전 세계적인 상호작용과 경제적 발전을 촉진하는 요소로 작용한다. 그러나 데이터 국경 간 이동은 각국의 개인정보 보호 법령에 의해 제한될 수 있다. 특히 GDPR이 데이터 국외 이전 관련 규정을 두어 데이터의 역외 이전을 엄격하게 규제하고, 중국이 자국의 데이터는 반드시 중국 내부에서 처리하도록 요구하는 정책을 채택함에 따라 데이터의 국경 간 이동이 디지털 무역에서 중요한 법적 논점으로 떠오르고 있다. 이러한 규제는 빅테크와 같은 다국적 디지털 서비스 기업이 EU 회원국 또는 중국 내에서 디지털 서비스를 제공하는 데 중대한 제약으로 작용한다.

2. 프라이버시 관련 책임 문제

디지털 무역 과정에서 개인정보 관련 문제가 발생 시 누가 책임을 지는지도 짚고 넘어가야 할 것이다.

한국 개인정보 보호법상 '개인정보처리자'는 GDPR의 컨트롤러와 개념상 차이가 있다. 개인정보처리자란 업무를 목적으로 개인정보 파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.[38] 현재 우리 개인정보 보호법은 GDPR의 공동 컨트롤러에 해당하는 '공동개인정보처리자' 개념을 인정하고 있지 않다.

공동 개인정보처리자 개념을 인정하고 있지 않은 현행 개인정보 보호법으로 인해 복수의 주체가 개인정보 처리 과정에 관여하는 경우, 그 주체 중 하나만이 개인정보처리자가 되고, 다른 주체 또는 주체들은 '개인정보의 처리를 위탁받은 자' 또는 '개인정보를 제공받은 제3자'의 지위를 갖게 된다. 이는 현행 개인정보 보호법 관련 실무에서 드러난다. 실무상 제3자 제공과 같은 형식으로 동의를 받는 방식이 가장 널리 사용되고 있는데, 제3자 제공의 경우 정보 주체에 대하여 양자가 공동으로 책임

38) 개인정보 보호법 제2조 제5호.

을 지는 경우는 없게 되고 제공자 또는 제공받은 자 중 일방이 그 책임을 부담하게 되며, 위탁 처리의 경우 누구의 목적을 위하여 업무를 처리하였는지 여부에 따라 정보주체에 대하여 책임지는자가 결정된다.[39]

개인정보 보호법상 '제공'이란 개인정보처리자가 보유하고 있는 정보 주체의 개인정보에 대한 지배권 및 관리권을 제3자에게 이전한다는 의미로 새길 수 있다.[40] 표준 개인정보보호지침(개인정보보호위원회 고시 제2025-4호, 시행 2025. 4. 11.)도 제7조 제1항에서 개인정보의 "제공"은 개인정보의 저장 매체나 개인정보가 담긴 출력물 책자 등을 물리적으로 이전하거나 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제3자의 접근권한 부여, 개인정보처리자와 제3자의 개인정보 공유 등 개인정보의 이전 또는 공동 이용 상태를 초래하는 모든 행위를 말한다고 명시하고 있다.[41]

한편 개인정보 보호법상 '처리위탁'이란 개인정보처리자가 자신의 업무를 수행하기 위해 다른 사람(수탁자)에게 개인정보의 처리 업무를 맡기는 것을 의미한다. 개인정보 보호법은 제26조에서 개인정보 처리 업무 위탁에 따른 개인정보의 처리 제한에 관해 규정하고 있다.

제26조(업무위탁에 따른 개인정보의 처리 제한)

③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.

④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.

⑥ 수탁자는 위탁받은 개인정보의 처리 업무를 제3자에게 다시 위탁하려는 경우에는 위탁자의 동의를 받아야

39) 강태욱, "개인정보의 제3자 제공을 둘러싼 몇 가지 쟁점에 대하여", 네이버 프라이버시 백서, 56면, 2023.

40) 이창범, "개인정보 제3자 제공 및 처리위탁 규제의 법적 과제", 개인정보보호의 법과 정책, 박영사, 258면, 2016.

41) 표준개인정보보호지침 제7조 제1항.

한다.

⑦ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.

개인정보 보호법은 복수의 주체가 개인정보 처리 과정에 개입된 경우, 개인정보의 '처리위탁'과 개인정보의 '제3자 제공' 중 하나로 포섭하여 규율하고 있다. 다만, 이에 대하여 복수의 기관이 개인정보 처리에 관여하는 형태의 경우의 수는 수없이 다양하게 나올 수 있는데, 이들을 현행 개인정보 보호법상 처리위탁과 제3자 제공이라는 두 유형만 가지고 이분법적으로 규율하는 체계는 이제 한계를 맞고 있다는 지적이 존재한다.[42]

개인정보의 '처리위탁'과 '제3자 제공'은 법률효과에서 큰 차이를 보이는데, 처리위탁의 경우 개인정보에 대한 지배·관리권 및 책임이 여전히 위탁자에게 존재하고, 위탁자는 수탁자를 관리·감독하여야 하며, 정보 주체의 동의를 받지 않는 대신 수탁자를 고지 또는 공개하면 되는 한편, 제3자 제공의 경우 개인정보에 대한 지배·관리권 책임이 그 수령자에게로 이전되어, 제공자가 수령자를 관리·감독하지 않고, 수령자는 자신의 책임하에 그 개인정보를 처리하며, 원칙적으로 정보 주체의 동의를 받을 필요가 있다.[43] 이때 어떠한 행위가 개인정보의 제공인지 아니면 처리위탁인지는 개인정보의 취득 목적과 방법, 대가 수수 여부, 수탁자에 대한 실질적인 관리·감독 여부, 정보 주체 또는 이용자의 개인정보 보호 필요성에 미치는 영향 및 이러한 개인정보를 이용할 필요가 있는 자가 실질적으로 누구인지 등을 종합하여 판단하여야 한다는 종합적 판단설이 우리 대법원의 입장이다.[44]

정리하면, 기업 A와 기업 B가 같은 개인정보 처리 과정에 관여하는 경우, 우리 개인정보 보호법은 먼저 기업 A와 기업 B 중 누가 개인정보 처리자인지를 먼저 검토한 다음, 개인정보 처리자가 아니라고 판단된 기업을 대상으로 그 기업이 개인정보의 처리를 위탁받은 자인지 혹은 개인정보 처리자로부터 개인정보를 제공받은 제3자인지를 판단하게 되는 것이다.

42) 전승재, "개인정보 처리위탁, 제3자 제공, 공동처리자", 정보법학, 26(3), 195면, 2022.

43) 전승재, 전게논문(주 42), 195면.

44) 대법원 2017. 4. 7. 선고 2016도13263 판결.

3. WTO와 개인정보 보호: 자유무역과 개인정보 보호의 균형 문제

개인정보 보호 규제는 디지털 무역 장벽으로 작용할 수 있다. 미국 무역대표부는 미국시간 2025년 3월 31일 「2025년 국가별 무역장벽 보고서(National Trade Estimate Report on Foreign Trade Barriers, NTE)」에서 데이터 국외 이전에 대한 규제를 이유로 한국의 개인정보 보호법이 미국 기업들에게 무역장벽으로 작용한다고 발표하였다.[45]

특히, 데이터 보호법이 각국의 법적 요구사항에 따라 다르게 적용되기 때문에, 기업들은 다양한 국가의 규제에 맞춰 서비스를 제공해야 한다. 특히 전 세계에서 이용하는 서비스를 제공하는 글로벌 기업들은 각국의 개인정보 보호법을 준수하기 위해 상당히 많은 자원을 투자해야 한다. 예를 들어, 구글과 메타 같은 빅테크 기업들은 다른 국가에 비해 상대적으로 개인정보 규제가 엄격한 GDPR 적용 국가들에 서비스를 제공할 때, 별도의 회원가입 화면을 구축하여 5가지의 세부 옵션을 선택하게 끔 함으로써 EU 외 국가와는 다른 회원가입 화면을 표시하고 있다.

세계무역기구(WTO)는 글로벌 무역의 규범을 제정하는 기구로서, 1998년부터 「세계전자상거래선언(Declaration on Global Electronic Commerce)」과 「전자상거래 작업프로그램(Work Programme on Electronic Commerce)」 등을 통해 디지털 무역에 대한 규제와 정책을 논의하고 있다.[46] 그러나 개인정보 보호와 자유무역 간의 균형 문제는 WTO 내에서도 해결되지 않은 주요 쟁점이다. 디지털 무역의 활성화를 위해 데이터의 자유로운 이동을 촉진하는 것이 중요한 반면, 개인정보 보호의 강화는 이를 저해할 수 있기 때문이다. WTO는 이 두 가지 목표를 어떻게 조화시킬 수 있을지에 대한 논의를 계속해야 한다.

Ⅴ. 통상법적 해결 방안

1. WTO의 디지털 무역 규범과 개인정보 보호

WTO는 디지털 무역에 대한 규범을 제정하기 위한 논의를 진행해 왔다. 개인정보 보호가 디지털 경제 및 무역 발전에서

45) United State Trade Representative, “2025 National Trade Estimate Report on Foreign Trade Barries of the President of the Unites States on the Trade Agreements Program, United States Trade Representative”, p. 252.

46) WTO, “Work Programme on Electronic Commerce”, WT/L/274, 1, para. 1.3., 1998.

소비자의 신뢰 향상에 기여한다는 측면 때문에 포괄적·점진적 환태평양 경제 동반자 협정(Comprehensive and Progressive Trans-Pacific Partnership, CPTPP), 미국-멕시코-캐나다 협정(United States-Mexico-Canada Agreement, USMCA), RCEP, 디지털 동반자 협정(Digital Partnership Agreement, DPA), DEPA 등은 전자상거래 및 디지털 무역 이용자의 개인정보 보호를 규정하는 법체계를 채택하거나 유지할 것을 의무화하고, 개인정보 보호를 위한 법체계를 개발할 때, 관련 국제기구의 원칙 및 지침을 고려할 것 또한 의무화하고 있다.[47]

CPTPP는 미국의 탈퇴로 동력을 잃었던 환태평양동반자협정(Trans-Pacific Parntership, TPP)이 일본 주도의 협상을 통해 재구성된 협정이다[48]. CPTPP는 국경 간 데이터 흐름에 관한 규정을 도입한 첫 주요 협정으로서, 14.11조와 14.13조에서 상업적 목적의 국경 간 데이터 이전을 제한하는 것과 데이터 로컬라이제이션을 금지하였다. 이는 CPTPP 등 무역협정의 기본적인 취지인 자유무역과 경제 통합을 잘 드러낸다.

Article 14.11 Cross-Border Transfer of Information by Electronic Means

2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

Article 14.13 Location of Computing Facilities

2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

WTO의 디지털 무역 관련 규정 또한 디지털 상품 및 서비스의 자유로운 교환을 촉진하는 방향으로 나아가고 있다. 그러나, 앞서 언급한 바와 같이, 현재 WTO는 디지털 무역에서의 데이터 보호 혹은 프라이버시 관련 규정이 미비하다. WTO는 디지털 무역에 대한 다자간 협정을 통해 각국의 개인정보 보호 규제를 통합하는 방안을 모색해야 한다. 이때 핵심은 디지털 무역에서 개인정보 보호와 자유무역 간의 균형점을 찾아 혁신을 저해하지 않는 선에서의 규제가 이루어지도록 하는 것일 것이다.

47) 김현수, "디지털 전환 시대의 농업", 세계농업 2024 겨울호, 62면, 2024.

48) 이요셉, "CPTPP 타결 의미와 시사점", KITA 통상 리포트 2018 VOL.06, 3, 2024.

2. 다자간 협정 및 글로벌 법적 규범의 필요성: 공동 컨트롤러 개념의 도입

디지털 무역에서 개인정보 보호와 자유무역 간의 균형점을 찾기 위해 가장 중요한 것은 책임 소재의 분배라고 생각된다. 플랫폼, 웹사이트, 앱과 같은 디지털 서비스는 물리적 한계로부터 자유롭다는 특성으로 인해 언제든 해외 이용자를 유치할 수 있다. 그 과정에서 디지털 서비스 사업자는 국외 사업장을 구축하기도 하고, 국외 소재 기업에 운영·관리 외주를 맡기기도 한다. 더 나아가서는 각기 다른 나라에 소재한 기업들끼리 협력하여 디지털 서비스를 구축하거나 기존 서비스를 확장하는 경우도 나타나고 있다. 그 예시로 구글(Google)의 맞춤형 광고 서비스가 있다. 구글은 전 세계를 상대로 검색엔진, 이메일 서비스, 모바일 기기 운영체제(Operation System, OS) 등을 제공하는 글로벌 플랫폼 기업으로서, 세계 각국의 이용자들이 구글의 서비스를 이용하고 있다. 구글은 웹사이트 운영자, 유튜브(YouTube) 채널 보유자, 모바일 앱 개발자 등 다양한 디지털 사업자를 대상으로 그들이 소유한 웹사이트, 유튜브 채널, 또는 앱에 구글 광고를 게재하고 그 광고 수익을 디지털 사업자와 나누는 사업을 하고 있다.[49] 동시에, 구글은 모든 온라인·오프라인 사업자를 대상으로 앞서 언급한 디지털 사업자들이 제공한 웹사이트, 유튜브 채널, 앱을 디지털 광고판으로 삼아 원하는 광고를 게재할 수 있도록 하는 서비스를 제공하고 있다.[50] 이 과정에서 구글은 자신의 이용자가 제공한 개인정보를 바탕으로 이용자의 관심사를 분석 후 이용자가 관심을 가질만한 광고를 선별하여 제공하는 맞춤형 광고를 활용하기도 한다. 한마디로 구글은 디지털 세상에서 광고판 보유자와 광고주를 매칭하는 브로커 역할을 하고 있는 것이다. 이때 디지털 사업자들과 온라인·오프라인 사업자들의 소재지에는 제한이 없다.

위에서 언급한 구글의 비즈니스 모델을 디지털 무역 관점에서 살펴보기 위해 구체적인 사례를 예시로 들어보고자 한다.[51] 경기도 수원에 소재한 음원 제작 기업은 구글을 통해 '광고용 음원 제작 외주를 맡을 수 있다'는 내용의 광고를 게재해달라고 요청한다. 구글은 자사 서비스 이용자 중 '음원 제작' 또는 '광고용 음원 제작업

49) 구글은 웹의 경우 Google Adsense, 앱의 경우 Google Admob이라는 서비스를 통해 디지털 사업자들과 광고 수익을 나눠 갖고 있다.

50) 구글은 Google Ads(前 Google AdWords)를 통해 광고 서비스를 제공하고 있다.

51) 예시는 필자의 경험을 바탕으로 작성되었다.

체' 등의 키워드를 검색한 이용자나 이전에 위와 같은 키워드로 검색하였던 이용자에게 위 광고를 송출한다. 음원 제작 기업은 영어로 광고를 제작 후 영미권 국가 이용자들에게 광고를 송출해달라고 요청할 수도 있다. 이 기업이 광고의 효과로 영미권 국가 클라이언트로부터 의뢰를 수주하였다면 남은 건 음원을 제작하여 MP3, FLAC, 또는 WAV 형태로 변환 후 이메일을 통해 클라이언트에게 음원을 보내준 다음, 몇 번의 수정을 거쳐 대금을 수령하면 된다.

위 사례는 디지털 무역에서 자유 무역이 보장될 경우 어떤 통상적 이익이 발생하는지를 잘 드러낸다. 음원 제작 기업의 사례에서 볼 수 있듯이 디지털 서비스의 높은 자유도는 곧 다양하고 창의적인 디지털 비즈니스 모델들의 등장으로 이어진다. 그러나 그와 동시에 각기 다른 나라에 소재한 복수의 디지털 서비스 사업자가 개입된 비즈니스 모델들에 대한 법률관계는 나날이 복잡다기해지고 있다. 무역에서 가장 빈번하게 발생하는 문제가 물품의 하자에 대한 책임이 누구에게 귀속되느냐인 것처럼, 디지털 무역에서도 데이터 관련 문제 발생 시 그에 대한 책임이 누구에게 귀속되는지가 주요 문제가 될 것이다.

GDPR의 경우 데이터 관련 책임이 누구에게 귀속되는지에 관한 문제를 해결하기 위해 '컨트롤러' 및 '공동 컨트롤러(joint controller)'의 개념을 차용하였다. '컨트롤러'의 정의는 '개인정보 처리의 목적과 수단을 결정하는 자'이다. 그리고 두 명 이상의 컨트롤러가 공동으로 개인정보 처리의 목적과 수단을 결정하는 경우 공동 컨트롤러에 해당하게 된다.[52] GDPR은 공동 컨트롤러에 해당하는 각 컨트롤러들로 하여금 각자의 개인정보 처리 관련 책임 범위를 합의하도록 하고 있다. GDPR에 따르면, 이렇게 컨트롤러 간 합의된 개인정보 처리 책임 범위는 개인정보 수집·이용 관련 고지 등을 통해 정보 주체들에게 제공되어야 한다.

Article 26. Joint Controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the in-

52) GDPR 제26조 제1항.

formation referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

GDPR은 책임 범위의 분배와 관련하여 컨트롤러 간 계약까지 요구하지는 않지만, 잠재적 분쟁을 예방하는 차원에서 서면으로 계약을 체결하는 것이 바람직할 것이다.

공동 컨트롤러의 개념을 가장 명확히 나타내는 것은 "Facebook '좋아요' 버튼" 사건(Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (Case C-40/17))이다. 이 사건의 요지는 다음과 같다.

온라인 의류소매업체인 Fashion ID가 자사 웹사이트에 소셜 네트워크 서비스(Social Network Service, SNS)인 Facebook의 소셜 플러그인(Social Plug-in) 중 하나인 '좋아요' 버튼을 설치하였다.[53] 이용자가 Fashion ID 웹사이트에 방문할 경우, Facebook은 그 '좋아요' 버튼을 도관으로 하여 Fashion ID 이용자의 개인정보를 수집하였다.[54] 수집행위는 ① 이용자가 Facebook의 회원인지 여부, ② Facebook '좋아요' 버튼을 클릭하였는지 여부를 불문하고 이루어졌다. 또한, 위 수집 행위는 이용자가 자신의 개인정보가 수집된다는 사실을 인지하지 못한 상태에서 이루어졌다.[55] 이와 관련하여 Fashion ID 웹사이트에서 이용자의 개인정보가 수집되어 Facebook으로 전달될 수 있다는 점을 정보 주체에게 고지할 의무가 Fashion ID와 Facebook 중 누구에게 있는지가 문제 되었다.

53) Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (Case C-40/17), 25번 문단.

54) 앞의 판결(주53), 27번 문단.

55) 앞의 판결(주53), 76번 문단.

이에 대해 소비자 보호 공익 단체인 Verbraucherzentrale NRW가 독일 뒤셀도르프트 지방법원에 Fashion ID를 상대로 위와 같은 개인정보 수집 행위를 중단할 것을 청구하는 소를 제기하였고, 2016. 3. 9. 뒤셀도르프 지방법원은 Fashion ID에게 컨트롤러로서의 지위를 인정하며 Verbraucherzentrale NRW의 청구를 일부 인용하였다.[56] 위 결정에 대해 Fashion ID는 독일 뒤셀도르프 고등법원에 항소하였고, EU에서 Facebook 서비스를 제공하는 Facebook Ireland가 Fashion ID를 위하여 항소심에 보조 참가한 것이 "Facebook '좋아요' 버튼" 사건이다.[57]

"Facebook '좋아요' 버튼" 사건에서 Fashion ID는 자사 웹사이트에서 ① 방문자의 브라우저에 의하여 전송된 정보, ② Facebook의 당해 정보사용 여부, ③ (Facebook이 당해 정보를 사용한다면) Facebook의 당해 정보사용 방법에 대해 아무런 영향력도 가지지 못하므로, 뒤셀도르프 지방법원이 Fashion ID를 Directive 95/46 제2조 (d)의 컨트롤러로 판단하는 것은 타당하지 않다고 주장하였다.[58]

Fashion ID의 주장에 대해 재판부는 다음과 같이 답변하였다. 'Directive 95/46의 입법취지, 즉 개인정보 처리에 대한 자연인의 기본적인 권리와 자유, 특히 개인정보 보호에 대한 높은 수준의 보호를 보장하기 위해, Directive의 제2조 (d)는 개인정보 처리의 목적과 수단을 결정하는 자를 '컨트롤러'로 규정하며, 자연인뿐만 아니라 법인, 공공 단체, 기관 또는 기타 단체도 컨트롤러에 해당할 수 있도록 넓게 정의하고 있다. 기존 판례들도 제2조 (d)의 목적이 컨트롤러의 정의를 폭넓게 규정하여 정보 주체의 효과적이고 완전한 보호를 보장하는 것이라고 판시하였다.[59] 또한, Directive 95/46의 제2조 (d)에 명시된 것과 같이, 컨트롤러라는 개념은 개인정보 처리의 목적 및 수단을 '자체적으로 또는 공동으로' 결정하는 주체와 연관되므로, 이 개념은 반드시 단일 주체에만 국한되는 것이 아니며, 각 주체는 정보처리 과정의 각 단계에 따라서 개별적으로 규정될 수 있으며, 당해 모든 주체가 당해 정보보호 규정의 규율을 받게 된다.[60] 자연인 또는 법인이 자신의 목적을 위해 개인정보 처리에 영향을 주고, 그 결과 간접적으로 개인정

56) 앞의 판결(주53), 30번 문단.

57) 앞의 판결(주53), 31번 문단.

58) 앞의 판결(주53), 34번 문단.

59) 2014년 5월 13일 판결 Google Spain 및 Google, C_131/12, EU:C:2014:317, 34번 문단 및 2018년 6월 5일 판결 Wirtschaftsakademie Schleswig-Holstein, C_210/16, EU:C:2018:388, 28번 문단.

보 처리의 목적 및 수단을 결정하게 되는 경우에도 컨트롤러로 간주될 수 있다.[61] 개인정보 처리 과정에 개입한 주체의 공동책임 여부는 개인정보에 액세스할 권한이 없다 하더라도 인정될 수 있다.[62] 결국 Directive 95/46 제2조 (d)의 목적은 컨트롤러 개념을 넓게 정의하여 정보 주체에 대한 효과적이고 포괄적인 보호를 보장하는 것이므로, 개인정보 처리 과정에서 공동책임을 지는 주체들이라고 하여 반드시 그 책임의 범주 및 내용이 동일한 것은 아니다. 위 주체들은 개인정보 처리의 각 과정에서 서로 다른 정도로 관여할 수 있다는 점을 고려하여, 각 주체의 책임 수준은 개별 사안에서의 제반상황을 종합적으로 고려하여 평가되어야 한다.[63] 결론적으로 자연인 또는 법인은 그가 공동으로라도 개인정보 처리의 목적과 수단을 결정하는 경우에 한하여 컨트롤러가 될 수 있다. Fashion ID는 자사 웹사이트에 Facebook의 '좋아요' 버튼을 설치하여 Facebook으로 하여금 자사 웹사이트 이용자의 개인정보를 수집할 수 있도록 허용한 것으로 보이고, 또한 이러한 수집은 방문자가 Facebook의 회원인지 여부, Facebook '좋아요' 버튼을 클릭하였는지 여부, 또는 이러한 정보수집 과정을 알았는지 여부 등과 무관하게 이루어진다. 이러한 점을 고려할 때, 결국 Fashion ID가 Facebook Ireland와 공동으로 결정할 수 있는 개인정보 처리 작업은 웹사이트 방문자의 개인정보 전송 과정에서의 정보수집 및 공개에 한정된다. Fashion ID가 Facebook Ireland로 개인정보가 전송된 이후에 진행되는 개인정보 처리 과정의 목적과 수단을 결정하는 것은 일응 불가능해보이는바, Fashion ID는 위 처리 과정의 범주에서는 컨트롤러로 여겨질 수 없다.[64] 결론적으로 재판부는 Fashion ID가 자사 웹사이트에 Facebook의 소셜 플러그인인 '좋아요' 버튼을 설치하여 해당 웹사이트 이용자의 개인정보를 Facebook으로 전송하는 경우, Directive 95/46의 제2조 (h) 및 제7조 (a)가 규정하는 '개인 정보 처리에 관한 동의'는 Fashion ID가 목적과 수단을 결정하는 개인정보 처리 작업 또는 일련의 작업들에 대해서만 받아야 하고, 제10조가

60) 2018년 6월 5일 판결, Wirtschaftsakademie Schleswig-Holstein, C_210/16, EU:C:2018:388, 29번 문단 및 2018년 7월 10일 판결, Jehovan todistajat, C_25/17, EU:C:2018:551, 65번 문단 참고.

61) 2018년 7월 10일 판결, Jehovan todistajat, C_25/17, EU:C:2018:551, 68번 문단.

62) 2018년 6월 5일 판결, Wirtschaftsakademie Schleswig-Holstein, C_210/16, EU:C:2018:388, 38번 문단 및 2018년 7월 10일 판결, Jehovan todistajat, C_25/17, EU:C:2018:551, 69번 문단.

63) 앞의 판결(주61) 66번 문단.

64) 앞의 판결(주53), 76번 문단.

규정하는 이용자에게 개인정보 처리 사실을 통지할 의무도 Fashion ID가 실제로 목적과 수단을 결정하는 개인정보 처리 작업 또는 일련의 작업들에 대해서만 존재한다고 해석되어야 한다.[65]

정리하면, GDPR에 따를 때 개인정보 처리의 목적과 수단을 결정하는 자는 모두 컨트롤러에 해당하고, 여러 주체가 공동 컨트롤러가 될 수도 있으며, 개인정보 처리의 각 단계별로 컨트롤러 해당 여부에 대한 판단이 달라질 수 있다.

디지털 무역에서 개인정보 보호와 자유무역 간의 균형을 맞추는 것은 매우 중요한 문제이다. 이를 해결하기 위해서는 상호인정 및 상호규제를 통해 각국의 법적 요구사항을 일정 부분 조율할 필요가 있다. 예를 들어, 각국은 기본적인 개인정보 보호 원칙을 공유하고, 이를 바탕으로 디지털 무역에서의 데이터 이동을 자유롭게 할 수 있을 것이다. 이때 각국이 컨센서스를 이루어 공통적으로 차용할 개념 중 하나로 GDPR의 공동 컨트롤러 개념이 포함되어야 한다고 생각한다. 공동 컨트롤러 개념을 도입함으로써 개인정보 처리 관련 책임을 지는 기업들이 늘어날 것이고, 각 기업은 개인정보의 올바른 활용이 이루어질 수 있도록 각자의 비즈니스 모델을 수정해야 할 것으로 예상된다. 다만, 절대다수의 개인정보 보호 법령이 정보 주체의 명시적인 동의만 있다면 기업을 규제로부터 자유롭게 하고 있는바, 결국 공동 컨트롤러 개념을 도입하였을 때 기업들에게 예상되는 변화는 '그동안 받지 않았던 개인정보 활용에 관한 동의를 받는 것'에 불과할 것이다. 반면에 개인들은 그동안 동의 없이 개인정보가 처리됨으로 인해 침해당한 개인정보 자기결정권을 다시 보장받을 수 있게 된다. 결국 공동 컨트롤러 개념의 도입만으로 기업 및 무역환경에 과도한 부담을 지울 것으로 생각되지는 않는바, 적어도 공동 컨트롤러의 개념은 개인정보 보호를 위한 글로벌 컨센서스에 포함되어야 한다고 생각한다.

3. 기타 디지털 무역 글로벌 컨센서스에 도입되어야 할 데이터·프라이버시 보호수단

현대 사회에서 가장 각광받는 기술은 단언컨대 AI일 것이다. AI 모델은 더 많은 데이터를 처리할수록 더 뛰어난 성능을 보인다.[66] 이에 따라 최근 AI 기술은 알고리즘 및 프로그램 개발 중심에서 대규모 학습데이터를 활용한 기술개발 방식으로 전환되고 있다.[67] 실제로 우리나라 기업들도

65) 앞의 판결(주53), 106번 문단.

인공지능 도입·운용 과정에서의 어려움으로 데이터 부족을 주된 이유로 제시한다.[68] 이처럼 데이터의 중요성이 강조됨에 따라 현재 공공·민간을 불문하고 다양한 분야에서 데이터가 실시간으로 생성되고 있다. 이에 따라 최근 몇 년간 세계 각국에서 인공지능 학습데이터를 통합 및 관리하는 통합적인 체계 설정 및 인공지능 생태계 구축을 위한 국가 차원에서의 노력에 관한 연구가 이루어져 왔다.[69] 호주의 경우 2023년 「데이터와 디지털 정부 전략(Data and Digital Government Strategy)」을 공개하였으며, FAIR(Findable, Accessible, Interpretable, and Reusable)와 CARE(Collective benefit, Authority to control, Responsibility and Ethics) 데이터 원칙을 공개하였다.[70] 칠레는 2022년 누구나 국가가 자금을 지원한 연구 데이터에 대한 접근할 수 있도록 데이터를 개방하는 정책을 개시하였다.[71] 우리 정부도 순차적으로 분야별 공공데이터를 개방하는 등 인공지능에 학습시킬 데이터셋의 양적 성장을 위해 노력하고 있으며[72], 공공데이터의 체계적이고 통합적인 관리를 위해 공공데이터포털을 운영하고 있다.[73]

본고는 여기서 더 나아가, 데이터가 단순히 국내에만 머무르지 않고 범지구적으로 전송 및 공유되고 있다는 점에 착안하여, 인공지능 시대의 데이터 활용에 있어 국경을 초월한 협력과 규범 정립이 필수적임을 강조하고자 한다. 인공지능의 학습 및 활용에 필요한 데이터는 점차 글로벌하게 수집·가공·이동되고 있는바, 이에 따라 국가 간 데이터 이전과 관련된 법적·제도적 조율이 중요해질 것이다. 그러나 현재까지는 각국이 자국의 개인정보 보호와 산업 보호를 이유로 데이터 주권을 강조하는

66) Sahlgren Magnus, Alessandro Lenci, “The Effects of Data Size and Frequency Range on Distributional Semantic Models”, Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing, Association for Computational Linguistics, 977–978, 2016.

67) 이용, 최명석, 김성찬, 이건우, 장래영, 이승우, 이상환, “인공지능 학습 데이터 공유·활용 현황과 서비스 구축 방향”, KISTI 이슈브리프, 2면, 2022.

68) 인공지능 전문가 좌담 “인공지능 시대, 어떻게 활용할 것인가” 세션 2 : 인공지능 기술과 활동 영역: 국내 AI 적용 사례 참조.

69) Castle David, Vanessa Mcbride, Dureen Samandar Eweis 외, “Preparing National Research Ecosystems for AI – second edition”, International Science Council, 2025.

70) 상게 논문, 18.

71) 상게 논문, 41.

72) https://www.korea.kr/news/policyNewsView.do?newsId=148941452&pWise=sub&pWiseSub=C2.

73) https://www.yna.co.kr/view/AKR20250218143600530.

경향이 강해, 국제적 데이터 이동을 둘러싼 규제 환경은 상이하고 단편적이다. 다양한 무역 협정들이 각국 정부의 데이터 규제를 제한할 가능성을 열어두고는 있지만[74], 아직 국경 간 데이터 흐름을 방해할 수 있는 각국 정부의 데이터 규제를 예방하지는 못하고 있다.[75] 이러한 상황은 디지털 무역의 예측 가능성과 안정성을 저해할 뿐 아니라, 인공지능 기술의 국제 공동 연구와 상호운용성을 어렵게 만들고 있다. 따라서 국가 간 인공지능 관련 데이터 시책이 디지털 무역 규범의 핵심 요소로 포함되어야 하며, 이를 위한 글로벌 컨센서스가 시급하다. 국제사회는 데이터의 자유로운 이동과 함께 개인정보 보호, 데이터 윤리, 신뢰성 확보 등의 원칙을 조화롭게 담아낼 수 있는 새로운 국제적 기준을 논의하고 마련해 나가야 할 시점이다.

Ⅵ. 결론

디지털 무역과 개인정보 보호를 조화롭게 다루기 위해서는 글로벌 차원의 협력과 법적 규범 설정이 필요하다. 각국의 법적 요구사항을 상호 존중하고, 데이터 보호와 자유무역 간의 균형을 맞추는 새로운 국제법적 틀이 필요하다. 새 국제법적 틀을 만들어 나가는 과정에서 필연적으로 비교법적 분석이 수반되어야 할 것인데, 본고는 EU GDPR이 채용한 컨트롤러 및 공동 컨트롤러의 개념이 포함되어야 한다고 주장하고자 한다. 현대사회에서 디지털 무역은 시간과 장소를 불문하고 네트워크를 통해 실시간으로 이루어지고 있다. 특히 플랫폼 사업자의 경우 자국 국민들만을 이용자로 모집하는 것이 아니라 국경을 넘어 다양한 국적의 이용자들을 용이하게 모집할 수 있게 되었다. 이러한 과정에서 플랫폼 사업자들은 다른 나라의 기업과 협력하거나, 다른 나라의 기업 서비스를 매개로 하는 경우가 빈번해졌다. 이로 인해 개인정보 수집 및 처리에 관여하는 당사자가 점점 늘어나고 있는 상황이다. EU GDPR이 공동 컨트롤러 개념을 도입하고, 개인정보 처리의 각 단계별로 컨트롤러 간 책임을 개별적으로 판단하게 하는 것도 이러한 현대사회 및 정보통신기술의 발전 양상을 고려한 것으로 생각된다.

결국, 현재 디지털 서비스 제공 기업들의 관행 등을 고려하면, 개인정보를 처리하는

74) Leblond Patrick, “Uploading CPTPP and USMCA Provisions to the WTO’s Digital Trade Negotiations Poses Challenges for National Data Regulation: Example from Canada”, Big Data and Global Trade Law, Cambridge University Press, 301-315, 2021.

75) Cory Nigel, Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them”, Information Technology & Innovation Foundation, 27-57, 2021.

모든 주체들에게 공정하게 책임을 귀속하기 위해서는 공동 컨트롤러의 개념을 도입하여 규제할 필요성이 있을 것이다. 우리나라의 상황에 대입하여 보더라도, 공동 컨트롤러 개념의 도입을 통해 '기업이 그동안 받지 않고 있던 개인정보 활용 혹은 처리 관련 동의를 받고 이에 맞춰 비즈니스 모델을 수정해야 하는' 번거로움보다 '침해당하고 있었던 헌법상 기본권인 개인정보자기결정권의 회복'이라는 공익이 더 크다고 판단된다. 또한 기업 입장에서도, 현존하는 규제 중 가장 엄격하는 규제에 맞춰 비즈니스 모델을 구성하고 서비스를 개선하는 것이 가장 효율적일 것이다.

디지털 무역과 개인정보 보호 간의 갈등을 해결하기 위한 연구는 계속되어야 한다. 향후 데이터와 프라이버시에 관련한 글로벌 디지털 무역 컨센서스가 정립되는 것은 피할 수 없을 것이기 때문이다. 특히 AI와 빅데이터가 기업의 전략과 서비스 품질 개선에 필수요소가 된 현 상황에서, 사용할 수 있는 데이터의 양과 질은 곧 기업의 경쟁력과 직결될 것이다. 규제 공백으로 인한 문제를 예방하기 위해서라도 디지털 무역과 프라이버시 간 균형점 도출에 더 많은 관심이 필요한 시점이다.

과도한 규제는 혁신을 저해하고, 과도한 자유는 공공의 위협으로 다가올 수 있다. 특히, 세계화가 더욱 가속화되고 있는 점을 고려할 때, A국이 상대적으로 엄격한 규제정책을 펼친다면 A국 기업들의 글로벌 경쟁력이 감소할 수 있고, 최악의 경우에는 다른 국가로 소재지를 이전할 수도 있다. 그럼에도 불구하고 글로벌 디지털 무역 컨센서스를 조성 과정에서 프라이버시에 대한 보장이 소홀해져서는 아니 될 것이다. 특히 우리나라의 경우 개인정보 자기 결정권은 헌법에 명시되지 않은 기본권이라는 지위에 있는바, 이를 더욱 두텁게 보장할 필요가 있다.

글로벌 컨센서스 정립 과정에서 한 가지 더 고려되어야 할 점은 데이터의 문제는 곧 독점의 문제로 이어질 수 있다는 것이다. AI 모델은 더 많은 데이터를 처리할수록 더 뛰어난 성능을 보인다. 많은 고품질 데이터를 수집한 기업은 그 데이터를 AI에게 학습시켜 더 발전된 서비스를 제공할 것이다. 이용자들은 자신의 수요를 충족시키는 많은 유사 서비스들 중 가장 높은 퀄리티의 서비스를 이용할 것이고, 이는 곧 그 기업으로 하여금 더 많은 이용자들의 이용 행태 분석을 바탕으로 서비스를 거듭 발전하게 한다. 경쟁에서 밀려나 이용자 수가 적은 기업들은 정보의 양이 부족하여 품질 개선에 애로사항을 겪을 것이고, 결국 선두기업과의 격차가 더욱 벌어지게 될 것을 예상할 수 있다.

최근 AI의 발전으로 정보통신기술의 발전이 더욱 가속화되었다. 어느새 Cursor AI 등의 AI툴을 활용하여 프로그래밍 언어에 문외한인 사람도 손쉽게 웹사이트나 앱을 만들 수 있게 되었다. 이전에는 코드 작성 시 시간복잡도(time complexity)나 데이터 효율성(data efficiency) 등의 요소를 얼마나 세밀하게 고려하였는지가 개발자의 실력을 판가름하는 요소가 되었으나, 이제는 프롬프트를 통해 텍스트 형태로 명령을 입력하여 위와 같은 요소들을 용이하게 챙길 수 있다. 이는 곧 정보통신기술의 상향평준화로 이어질 가능성이 높다. AI의 성능은 학습된 데이터의 양과 질에 의존하는 만큼, AI의 발전은 필연적으로 데이터의 중요성을 더욱 강조하게 된다. AI와 함께 정보통신기술이 이전보다 더 빠른 속도로 발전할 것이 명명백백하게 예상되는 상황에서 데이터 및 프라이버시 문제들을 해결하기 위한 다자간 협정 등 새로운 국제법적 규범과 같은 컨센서스는 언제 만들어져도 시기상조가 아닌바, 국가 간 긴밀한 협력을 통해 조속한 보편적 국제규범이 확립할 것이 요구된다. 그 과정에서 GDPR의 공동 컨트롤러 개념을 차용한다면, 자신의 정보가 각기 다른 국가에 소재한 여러 기업들 사이에서 여러 절차를 거쳐 처리된다 하더라도, 각 단계별로 귀책사유가 있는 개인정보 처리자를 대상으로 문제를 제기하여 완전하고 실질적인 권리 보호를 실현할 수 있을 것이다.

참 고 문 헌

1. 국내문헌

강태욱, “개인정보의 제3자 제공을 둘러싼 몇 가지 쟁점에 대하여”, 네이버 프라이버시 백서, 2023

김선호, “EU 디지털 단일시장 전략 분석”, 2015년 1권 7호, 한국언론진흥재단 연구센터, 2015

김인석 외, “국제적 상호운용성 강화 및 지능정보화 시대에 부응한 발전방안 연구”, 개인정보보호위원회 연구보고서, 고려대 산학협력단, 2016; 함인선, 위의 논문 등

김정곤, 나승권, 장종문, 이성희, “EU 디지털 단일시장 전략의 주요 내용과 시사점”, 오늘의 세계경제, Vol. 15, 대외경제정책연구원, 2015

김현수, “디지털 전환 시대의 농업”, 세계농업 2024 겨울호, 2024

김홍종, “디지털 무역 규범의 국제 논의와 한국의 대응” 통상법률, 2020년 4호, 2020

오태현, 강민지, “EU 개인정보보호법(GDPR) 발효: 평가 및 대응방안”, 오늘의 세계경제 Vol. 18 No. 19, 대외경제정책연구원, 2018

이요셉, “CPTPP 타결 의미와 시사점”, KITA 통상 리포트 2018 VOL.06, 2024

이용, 최명석, 김성찬, 이건우, 장래영, 이승우, 이상환, “인공지능 학습 데이터 공유·활용 현황과 서비스 구축 방향”, KISTI 이슈브리프, 2022

이창범, “개인정보 제3자 제공 및 처리위탁 규제의 법적 과제”, 개인정보보호의 법과 정책, 박영사 2016

전승재, “개인정보 처리위탁, 제3자 제공, 공동처리자”, 정보법학, 26(3) 2022

최경진, “EU GDPR의 분석 및 시사점”, 네이버 프라이버시 백서, 2016

최요섭, “A Critical Review of the EU’s Digital Markets Act - Possible Impacts on the Digital Economy -”, 중앙대학교 법학연구원, 法學論文集, 45(1), 2021

2. 외국문헌

Canzian Giulia, Gianluca Mazzarella, Louis Ronchail, Frank Verboven & Stefano Verzillo, “Evaluating the impact of price caps - evidence from the European roam-like-at-home regulation”, SSRN Electronic Journal, 2021

Castle David, Vanessa Mcbride, Dureen Samandar Eweis 외, “Preparing National Research Ecosystems for AI – second edition”, International Science Council, 2025

Cory Nigel, Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them”, Information Technology & Innovation Foundation, 2021

González Javiel López and M. Jouanjean, “Digital Trade: Developing a Framework for Analysis”, OECD Trade Policy Papers, No. 205, OECD Publishing, 6, 2017

Leblond Patrick, “Uploading CPTPP and USMCA Provisions to the WTO’s Digital Trade Negotiations Poses Challenges for National Data Regulation: Example from Canada”, Big Data and Global Trade Law, Cambridge University Press, 2021

Like Andrine, Leo Peeters, “‘The end of geo-blocking, and the portability of digital services in the European Union”. Seeds of Law, 2018

Sahlgren Magnus, Alessandro Lenci, “The Effects of Data Size and Frequency Range on Distributional Semantic Models”, Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing, Association for Computational Linguistics, 2016

Tourkochoriti Ioanna, “The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide Between U.S.-EU in Data Privacy Protection”, University of Arkansas at Little Rock Law Review, Vol. 36, 2014

Zulianto Mukhamad, “ASEAN Digital Economy Framework Agreement(DEFA): Opportunities and Challenges for Vietnam”, Asia Pacific Journal of Public Policy, 10(01), 2024

3. 기타문헌

헌법재판소 2005. 5. 26. 선고 99헌마513 결정

https://asean.org/asean-launches-worlds-first-regionwide-digital-economy-framework-agreement/

산업통상자원부 2023. 1. 13. 보도자료 “1. 14일「한-싱가포르 디지털동반자협정」발효 - 양국 간 디지털 교역 확대 및 디지털 기술·비즈니스 협력 강화 기대 -”

관계부처 합동, “디지털경제동반자협정(DEPA) 상세 설명자료”, 2-41면, 2024

EUROPEAN COMMISSION, “A digital Single Market for Europe : commission sets out 16 initiatives to make it happen”, 2015

EU-Commission, “A Digital Single Market Strategy for Europe” COM 192 final, 13, 2015

https://www.cloudflare.com/ko-kr/learning/privacy/what-is-eprivacy-directive/

https://www.lexology.com/library/detail.aspx?g=77cae731-0a1e-4049-97eb-c3b61f51b020

https://news.un.org/en/story/2013/12/458232

https://www.consilium.europa.eu/en/policies/data-protection-regulation/

European Commission, “LIBE Committee Vote Backs New EU Data Protection Rules.”, 2013

https://www.verdict.co.uk/has-five-years-of-gdpr-stifled-tech-innovation/?utm_source=chatgpt.com&cf-view

https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/

United Nations Conference on Trade and Development, “Data Protection Regulations and International Data Flows: Implications for Trade and Development”, United Nations, 32, 2016

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities

United State Trade Representative, “2025 National Trade Estimate Report on Foreign Trade Barries of the President of the Unites States on the Trade Agreements Program, United States Trade Representative”, 252

WTO, “Work Programme on Electronic Commerce”, WT/L/274, 1, para. 1.3., 1998

Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (Case C-40/17)

2014년 5월 13일 판결 Google Spain 및 Google, C_131/12, EU:C:2014:317

2018년 6월 5일 판결 Wirtschaftsakademie Schleswig-Holstein, C_210/16, EU:C:2018:388

2018년 7월 10일 판결, Jehovan todistajat, C_25/17, EU:C:2018:551

인공지능 전문가 좌담 “인공지능 시대, 어떻게 활용할 것인가” 세션 2 : 인공지능 기술과 활동 영역: 국내 AI 적용 사례 참조

https://www.korea.kr/news/policyNewsView.do?newsId=148941452&pWise=sub&pWiseSub=C2

https://www.yna.co.kr/view/AKR20250218143600530

[국문초록]

디지털 무역과 개인정보 보호:
공동 컨트롤러 개념의 필요성을 중심으로

이동건

디지털 무역은 정보통신기술의 발달과 함께 기존의 무역 개념을 넘어서는 새로운 상거래 형태로 자리매김하고 있으며, 데이터 및 개인정보의 이동이 중심이 되는 무형의 자산 거래가 전 세계적으로 확대되고 있다. 이와 같은 디지털 무역의 성장 이면에는 국가 간 개인정보 보호 수준의 상이로 인한 법적 충돌 가능성이 상존하며, 이는 무역의 자유와 개인의 프라이버시 보호라는 두 법익 간의 균형이라는 중대한 법적 과제를 야기한다.

본 논문은 이러한 문제의식에 기반하여 디지털 무역과 개인정보 보호 간의 갈등을 통상법적 관점에서 분석하고, 그 해결방안을 모색하는 데 목적이 있다. 이를 위해 유럽연합의 GDPR, 미국 캘리포니아주의 CPRA, 한국의 개인정보 보호법을 비교·검토하여, 각국 규제체계의 차이점이 디지털 무역에 미치는 법적 영향을 고찰한다. 특히 데이터의 국경 간 이동 제한, 개인정보 유출 시 책임소재의 불명확성, 그리고 WTO 체제 내 자유무역 원칙과 프라이버시 보호 규범 간의 긴장 관계를 중심으로 분석을 전개한다.

이 과정에서 본 논문은 GDPR상 공동 컨트롤러(joint controller) 개념을 주목하며, 다수의 기업 또는 기관이 개인정보 처리의 목적과 수단을 공동으로 결정하는 현실을 반영하는 법적 틀로서 공동 컨트롤러 모델이 갖는 의의를 조명한다. 반면, 한국의 개인정보 보호법은 처리위탁과 제3자 제공이라는 이분법적 구조만을 인정함으로써 다국적 디지털 서비스 환경에서 발생하는 복잡한 법률관계를 충분히 포섭하지 못하고 있다. 이에 본 연구는 공동 컨트롤러 개념의 국내 도입 필요성과 가능성을 고찰하고, 정보주체 권리 보장과 글로벌 법제 간 상호운용성 제고라는 측면에서 그 법적·정책적 함의를 제시한다.

결론적으로 본 논문은 디지털 무역의 지속 가능성과 개인정보 보호의 조화를 위해, 보다 정교하고 현실적인 책임 분배 체계로서 공동 컨트롤러 모델의 법제화가 요구된다고 주장한다. 이는 WTO를 포함한 국제무역질서 내에서 개인정보 보호 규범의 통일성과 일관성을 확보하는 데 기여할 수 있으며, 글로벌 디지털 경제에서의 신뢰 기반 구축과 분쟁 예

방을 위한 중요한 초석이 될 것이다.

주요어: 디지털 무역, 개인정보 보호, 공동 컨트롤러, WTO, GDPR,
통상법, 데이터 국경 간 이동, 통상 규범 충돌, 데이터 로컬라이제이션,
프라이버시

[Abstract]

Digital Trade and the Protection of Personal Data:
Focusing on the Necessity of 'Joint Controller'

Donggun Lee

Digital trade has emerged as a transformative force in the global economy, transcending traditional boundaries of commerce and reshaping the way goods, services, and data are exchanged across borders. As this shift accelerates, personal data has become a critical asset in the digital economy, leading to complex legal challenges surrounding its protection and regulation. Among these, the tension between the free flow of data—essential for digital trade—and stringent privacy regulations imposed by individual jurisdictions has become increasingly pronounced.

This paper explores the legal and institutional conflicts between digital trade and personal data protection from an international trade law perspective. Through a comparative analysis of the European Union's General Data Protection Regulation (GDPR), the United States' California Privacy Rights Act (CPRA), and the Republic of Korea's Personal Information Protection Act (PIPA), the study identifies fundamental differences in regulatory approaches that hinder cross-border data flows and create legal uncertainty for multinational businesses.

A central argument of this research is that the GDPR's "joint controller" concept offers a viable legal framework for allocating responsibility in transnational data processing activities. In contrast, Korea's binary regulatory model—dividing all data processing relationships into either consignment (outsourcing) or third-party provision—is no longer adequate to capture the complexity of contemporary digital services involving multiple stakeholders across jurisdictions. By examining landmark cases such as Fashion ID v. Verbraucherzentrale NRW, the paper illustrates how joint controllership can serve as a regulatory solution that promotes both accountability and interoperability.

The paper concludes by advocating for the adoption of the joint controller model within Korean data protection law and encourages the development of multilateral norms within the

WTO or other international frameworks. Such legal innovation is essential for reconciling the dual imperatives of protecting personal data and facilitating the growth of a robust, inclusive global digital economy.

Key words: Digital Trade, Personal Data Protection, Joint Controller, WTO, GDPR, Trade Law, Cross-Border Data Flows, Regulatory Conflict, Data Localization, Privacy