생성형 AI 시대의 주요국 데이터 규제 동향

Data Regulatory Landscape of Major Countries in the Era of Generative AI

이지연 (J.Y. Lee, jiyeonlee@etri.re.kr) 통신정책연구실 박사후연수연구원

ABSTRACT

As the era of generative AI emerges, significant shifts are occurring in data governance and regulatory frameworks across major countries. Unlike previous AI technologies that focused primarily on automation and data analysis, generative AI introduces advanced capabilities, raising new concerns about data privacy, security, and ethical implications. In response, countries such as the United States, the European Union, China, and others are adapting their data regulatory policies to address the growing complexity and potential risks posed by generative AI. This study explores the evolving landscape of data regulation in key countries and examines how the generative AI revolution is reshaping regulatory approaches to ensure the safe, fair, and trustworthy development of AI technologies.

KEYWORDS 개인정보 보호, 데이터 거버넌스, 데이터 규제, 생성형 AI

Ⅰ. 서론

AI 기술의 발전, 특히 생성형 AI의 진보는 데이터 보호와 관련된 기회와 위험을 동시에 제기하고 있다[1]. 최근 생성형 AI 시스템은 텍스트와 음성은 물론 이미지, 영상 등 다양하고 방대한 데이터를 통합하여 처리할 수 있는 멀티모달(Multimodal) 기능을 갖추게 되었다[2]. 이러한 대형 멀티모달 모델(LMM: Large Multimodal Model)은 복잡한 데이터의 처리 및 인간과의 상호작용 능력이 향상되어 의료, 자율주행 등 산업에서의 응용 범위가 확대됨과 동시에, 생성형 AI 시스템이 데이터를 학습하고 생성하는 과정에서 개인정보를 포함한 민감 데이터를 사용할 가능성이 높아졌다[3]. 예를 들어, 민감 데이터가 정보 주체의 동의 없이 사용되거나, 편향이 있는 학습데이터로 인해 편향된 결과물이 생성되거나, 저작권이 있는 콘텐츠가 무단으로 복제되는 등의 위험 요소가 등장하였다[4].

생성형 AI 시스템의 성능과 신뢰성은 학습에 사용되는 데이터의 양과 질에 크게 의존하는 만큼, 데이터로부터 야기될 수 있는 위험에 대응하기 위한 글로벌 규제 체계의 필요성이 높아지고 있다[3]. 다

* DOI: https://doi.org/10.22648/ETRI.2024.J.390610
* 본 연구는 과학기술정보통신부 및 한국방송통신전파진흥원의 2024년도 ICT 기금사업(정보통신방송 해외진출지원)의 일환으로 수행하였음[24MF1100, ICT 통상 대응 지원].

자 차원에서는 G7 히로시마 AI 프로세스에 따른 'AI 개발자를 위한 자발적 행동 강령(Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI System)'을 수립하고, 생성형 AI의 주요 위험으로 개인정보 및 지식재산권 침해와 허위 정보 확산 등의 문제를 강조하였다[5,6]. 이처럼 AI 기술 발전에 따른 데이터 보호 및 개인정보 보호 문제는 개별 국가의 문제만이 아닌 국제적 조정과 협력이 필요한 도전과제이다.

본고에서는 우리나라를 포함하여 미국, 유럽연합 및 중국에 대한 생성형 AI 관련 데이터 규제 정책 변화와 대응 전략을 정성적으로 분석한다. 데이터의 개념은 법령이나 학자에 따라 다양하게 정의되고 있으나 본고에서는 생성형 AI의 맥락에서 데이터의 정의를 'AI 시스템이 학습 및 생성하는 모든 디지털 정보'로 확장하여 적용한다. 이를 바탕으로 각국의 데이터 규제 접근 방식을 비교하고 한국의 정책적 대응 방향에 대한 시사점을 제시하고자 한다.

II. 주요국 데이터 규제 동향

1. 미국

미국의 데이터 및 개인정보 보호 규제는 연방 차원의 포괄적 법률 대신 분야별 연방법과 주(州)별 법률로 구성되어 있다. 미국의 주(州)별 법률 체계는 일반적으로 분야별로 개별적 개인정보 보호 법률을 두고 있으나, 최근 캘리포니아주를 시작으로 포괄적 개인정보 보호법 제정 추세가 나타나고 있다. 캘리포니아주는 2018년 캘리포니아 소비자 개인정보 보호법(CCPA: California Consumer Privacy Act)을 제정하고, 2020년 캘리포니아 개인정보 권리법(CPRA: California Privacy Rights Act)으로 개정하였다. CPRA의 개정 내용으로는 민감 데이터 개념의 분리 및 관련 추가 의무 부과, 유럽연합 일반 개인정보 보호 규정(GDPR: General Data Protection Regulation)상 목적 제한, 정보 최소화 및 보관 제한 원칙 반영, 자동화된 의사결정에 대한 알 권리 및 거부권, 부정확한 정보에 대한 정정 청구권, 민감 정보 공유 및 사용 거부권 등을 포함한다[7].

트럼프 행정부는 2020년 10월 '신뢰할 수 있는 인공지능의 연방정부 사용 촉진 행정명령(Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government)'[8] 및 2021년 1월 '국가 AI 이니셔티브법(National Artificial Intelligence Initiative Act)' 제정[9]을 통해 AI 기술 활용 촉진과 미국의 기술적 우위 강화에 중점을 두었다. AI의 윤리, 법, 안전, 보안 등의 측면을 다루는 연구에 대한 지원과[10] AI 표준 및 위험관리 체계 개발을 포함시키는 한편[11], 전반적으로 규제보다는 기술 혁신과 데이터 활용 확대를 통한 경제 성장에 우선순위를 두는 정책 기조를 보였다.

이후 2022년 10월, 생성형 AI 기술의 급격한 발전과 함께 바이든 행정부는 'AI 권리장전 청사진(Blueprint for an AI Bill of Rights)'을 발표하며[12], 데이터 사용의 투명성과 공정성을 보다 강조하였다. 데이터 프라이버시 원칙에 따르면, 시스템 설계자, 개발자 및 배포자는 데이터의 수집, 사용, 접근, 이전 및 삭제에 관한 정보 주체의 동의를 명확히 하여야 한다. 특히 건강, 고용, 교육, 형사 사법, 금융을 포함한 민감 영역의 데이터에 대해서는 추론을 제한하고 보호를 강화해야 한다. 민감 영역 데이터에 대해 추가적으로 권고되는 원칙은 표 1과 같다.

이와 같은 노력의 연장선에서, 바이든 행정부는 2023년 10월 '안전하고 신뢰할 수 있는 인공지능 개발 및 사용 행정명령 제14110호(Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence)'를 발표하였다[13]. AI가 엄청난 잠재력과 동시에 사기, 차별, 편견, 허위 정보, 일자

표 1 민감 데이터에 대한 강화된 보호 원칙

원칙	주요 내용
목적 외 사용 금지	민감 데이터는 해당 영역에서 반드시 필요한 경우에만 사용할 것
윤리적 검토	민감 데이터 또는 민감 데이터를 기반으로 하는 의사결정 프로세스의 사용은 사전 및 주기적 검토 및 모니터링을 거칠 것
데이터 품질	부정확한 데이터에 기반한 의사결정으로 인해 발생하는 부정적 결과를 피하기 위해 정기적 품질 검사 및 신속한 시정 조치를 실시할 것
파생 데이터 접근 제한	민감 데이터는 민감 정보 추론에 사용될 수 있으므로 파생 데이터를 판매, 공유 또는 공개하지 말 것
보고	민감 영역 관련 기술을 개발하는 기관과 민감 데이터를 수집, 사용, 저장 또는 공유하는 기관은 민감 데이터 유출을 초래한 모든 데이터 침해 사례, 윤리 검토 횟수, 유형 및 결과, 데이터 위험 평가 방법 및 완화 조치를 제공

출처 Reproduced from The White House, "Blueprint for an AI Bill of Rights," Office of Science and Technology Policy, Oct. 2022.

리 대체 및 국가 안보 위협과 같은 위험을 초래할 수 있다는 인식하에, 이러한 위험을 최소화하고 AI의 책임 있는 사용을 촉진하기 위한 노력이 필요하다고 여겨졌기 때문이다[14]. 제4조(AI 기술의 안전 및 보안의 보장)에 따르면 행정관리예산국장은 국무장관, 국방부장관, 법무부장관, 상무부장관과 협의하여 미국 국립표준기술연구소(NIST: National Institute of Standards and Technology) 원장, 국토안보부장관, 국가정보국장 및 적절하다고 판단하는 그 밖의 기관장을 통해 디지털 콘텐츠 라벨링 및 인증 지침을 마련하도록 하였다[15]. 제9조(개인정보 보호)에서는 AI가 개인에 관한 정보의 수집이나 이용을 촉진하는 것 및 개인에 관한 추론을 실시하는 것을 AI에 의한 악용 가능성이 있는 개인정보 위험으로 지적한다[16]. 이에 NIST가 AI 시스템에 사용되는 기술을 포함하여 개인정보 보호 기술의 효과를 평가할 수 있는 지침을 개발하도록 하고[17], 국립과학재단(NSF: National Science Foundation)은 개인정보 보호 강화 기술을 개발 및 연구협력네트워크(RCN: Research Coordination Network)에 자금을 지원하도록 하였다[18]. 제10조(연방정부의 AI 사용의 발전)에서는 AI 이용에 관하여 각 기관에 대해 생성형 AI의 생성물에 워터마크 및 기타 라벨을 지정하기 위한 합리적인 조치를 할 것과 생성형 AI에 대해 차별적이거나, 오해를 불러일으키거나, 선동적이거나, 안전하지 않거나, 기만적인 생성물에 대한 테스트 및 보호 조치, 아동 성학대 자료 제작의 방지 조치를 권고하고 있다[19].

국가 AI 이니셔티브법에 따른 미국 의회의 지시로[11] 미국 NIST는 2023년 1월 'AI 위험관리 프레임워크(AI RMF: AI Risk Management Framework)'를 개발하였다. AI RMF는 AI 시스템을 설계, 개발 및 도입하는 조직을 위한 자발적 활용 가이드 문서로, AI 시스템의 전 주기에 걸쳐 안전성과 신뢰성을 보장하기 위한 지침을 제공한다. AI RMF에 따르면 조직이 AI 시스템에 대해 가장 높게 판단한 위험을 기반으로 우선순위와 위험관리 프로세스를 지정할 수 있는데, AI 시스템이 개인정보 식별과 같은 민감한 또는 보호된 데이터로 구성된 대규모 데이터 세트를 학습하거나, 그 결과가 인간에게 직접적 또는 간접적 영향을 미칠 수 있는 경우 높은 우선순위로 간주한다[4].

2. 유럽연합

유럽연합은 2018년 5월 GDPR을 제정함으로써 개인정보 보호와 데이터 사용에 있어 체계적인 법적 프레임워크를 구축하였다. 데이터 처리와 관련된 조항은 표 2와 같다. GDPR 제5조(개인정보 처리 원칙)에서는 개인정보는 정보 주체에 대해 합법적이고, 공정하며, 투명하게 처리될 것과 구체적이고 명시적이며 적법한 목적을 위해 수집되어야 하고, 해당 목적과 양립되지 않는 방식으로 추가 처리되어서는 안 됨을 명시한다. 다만 공적 기록 보존, 과학적 및 역사적 연구, 통계적 목적의 개인정보 처리는

표 2 GDPR상 데이터 처리 관련 조항 및 주요 내용

구분	주요 내용
합법성, 공정성 및 투명성	개인정보는 정보 주체에 대해 적법하고, 공정하며, 투명하게 처리될 것
목적 제한	구체적이고 명시적이며 적법한 목적을 위해 수집될 것, 해당 목적과 양립되지 않는 방식으로 추가 처리되어서는 안 됨(공익 기록 보존, 과학적·역사적 연구, 통계적 목적 예외)
정보 최소화	개인정보는 처리 목적과 관련하여 적절하고 관련성이 있으며 필요한 범위로 제한될 것
정확성	정확하고, 필요한 경우 최신 정보일 것, 처리 목적과 관련하여 부정확한 개인정보는 지체 없이 삭제 또는 정정되도록 모든 적절한 조치가 시행될 것
보관 제한	처리 목적 달성에 필요한 기간 동안만 정보 주체를 식별할 수 있는 형태로 보관될 것(공익 기록 보존, 과학적·역사적 연구, 통계적 목적 예외)
무결성 및 기밀성	보호 조치는 개인정보가 무단으로 또는 불법적으로 처리되거나 우발적으로 소실, 파기, 손상되었을 경우 적절한 기술 및 관리적 조치를 사용할 것
정보 주체 권리	정보 주체는 프로파일링을 포함해 자동화된 처리만을 바탕으로 한 결정으로서 자신과 관련한 법적 영향 또는 이와 유사하게 중대한 영향을 미치는 결정의 대상이 되지 않을 권리를 가짐(계약 체결 또는 이행, 유럽연합 또는 회원국 법률이 허용하는 경우 예외)

출처 Reproduced from EU, "General Data Protection Regulation (Regulation (EU) 2016/679)," 2018. 5. Article 5, [20] and Article 22 [21].

본래의 목적과 양립되는 것으로 보지 않는다. 또한, 개인정보는 처리 목적과 관련하여 적절하고 관련성이 있어야 하며, 필요한 범위로 제한되어야 함을 명시하고 있다. 부정확한 정보는 지체 없이 수정 또는 삭제되도록 모든 적절한 조치를 해야 하며, 개인정보의 보관 기간은 처리 목적 달성에 필요한 기간으로 제한된다. 이와 함께 개인정보의 무결성 및 기밀성을 보장하기 위해 무단 또는 불법적인 처리, 우발적인 손실, 파기 및 손상을 방지하기 위한 기술적 및 관리적 조치가 시행되어야 한다[20].

GDPR상 AI 시스템에 대해 명시적으로 다룬 구체적 규정은 없지만, 제22조(프로파일링을 포함한 자동화된 개별 의사결정)에 따르면 정보 주체는 프로파일링(Profiling)을 포함하여 자동으로 처리된 정보만으로 결정이 내려지는 경우, 자신의 법적 권리나 이와 유사하게 중대한 영향을 받을 수 있는 결정의 대상이 되지 않을 권리를 가진다[21]. 법적 규율의 대상인 '자동화된 처리에만 기초한 결정(Decision Based Solely on Automated Processing)'에 활용되는 기술은 AI만을 염두에 둔 것은 아니나, AI가 인간의 개입 없이 인간에게 중대한 영향을 미칠만한 의사결정들을 내릴 수 있게 됨에 따라, 자동화된 의사결정에 의해 정보 주체가 불리한 영향을 받지 않도록 인간의 개입을 보장하고 개인의 권리를 보호하도록 하는 것이 동 조항의 목적이다.

2024년 8월 발효된 'AI 법(AI Act)'은 AI 기술에 대한 최초의 포괄적 규제 법안이다. 동 법안은 유럽연합 역내에 AI 제품이나 서비스를 출시하는 전 세계 모든 기업에 적용된다. AI 법에서는 AI 시스템의 위험성을 수용 불가(Unacceptable Risk), 고위험(High Risk), 제한된 위험(Limited Risk) 및 최소 위험(Minimal Risk)의 네 등급으로 분류하고, 위험 수준에 따라 차

표 3 유럽연합 AI 법상 정의된 고위험 AI 위험 요인과 적용되는 데이터 및 데이터 거버넌스 규제

위험 등급	유형	적용 규제
고위험	• 생체 인식(관련 유럽연합 법령 또는 국내법에 따라 사용이 허용된 경우에만) • 핵심기반시설 • 교육 및 직업 훈련 • 고용, 근로자 관리 및 자영업 • 법 집행(관련 유럽연합 법령 또는 국내법에 따라 사용이 허용된 범위에서) • 이민, 망명 및 국경 통제 관리(관련 유럽연합 법령 또는 국내법에 따라 사용이 허용된 범위에서) • 사법행정 및 민주적 절차	• 고위험 AI 시스템의 의도된 목적에 부합하는 방식으로 관리될 것 • 데이터가 인간의 기본권에 부정적 영향을 미치거나 유럽연합의 법령에 따라 금지된 차별을 초래할 위험이 있는 경우, 편향 가능성을 감지하고 방지 및 완화하기 위한 적절한 조치를 취할 것 • 고위험 AI 시스템이 사용하는 데이터 세트는 의도된 목적을 고려하여 관련성 있고, 충분히 대표성을 띠며, 오류가 없고 완전하여야 함

출처 Reproduced from EU, "The AI Act (Regulation (EU) 2024/1689)," Article 10., 2024. 8. [22].

등적인 규제를 적용하는 위험 기반 규제(Risk-Based Regulation) 방식을 취하고 있다. 특히, 유럽연합 AI 법안 제10조(데이터 및 데이터 거버넌스)에서는 고위험 AI 시스템의 데이터 관리에 대해 표 3과 같은 구체적인 요구사항을 제시하고 있다.

유럽연합의 AI 법에 의해 고위험으로 분류되는 AI 시스템은 일정 품질 기준을 충족하는 학습, 검증 및 시험 데이터 세트를 기반으로 개발되어야 한다. 이러한 데이터 세트는 데이터의 수집(Collection), 출처(Origin), 목적(Purpose), 라벨링(Labelling), 어노테이션(Annotation), 정제(Cleaning), 갱신(Updating), 보강(Enrichment), 집계(Aggregation) 등의 과정에서 AI 시스템의 의도된 목적에 부합하는 방식으로 관리되어야 한다. 또한, 데이터가 인간의 기본권에 부정적 영향을 미치거나 유럽연합의 법령에 따라 금지된 차별을 초래할 위험이 있는 경우, 편향 가능성을 감지하고 방지 및 완화하기 위한 적절한 조치를 하도록 한다. 이와 함께, 고위험 AI 시스템이 사용하는 데이터 세트는 의도된 목적을 고려하여 관련성이 있고, 충분히 대표성을 띠며, 오류가 없고 완전해야 한다[22].

3. 중국

중국은 '사이버보안법(网络安全法)', '데이터보안법(数据安全法)', '개인정보 보호법(个人信息保护法)' 등 이른바 데이터 3법을 통해 데이터를 규율해왔다. 2016년 11월 제정된 사이버보안법은 네트워크를 통해 처리되는 전자 데이터의 안전성을 보장하기 위해 데이터 분류, 백업, 암호화 등의 조치를 요구한다[23]. 2021년 6월 제정된 데이터보안법은 데이터를 일반, 중요 및 핵심 데이터로 분류하여 보호하며, 핵심 데이터는 국가 안보와 공공 이익에 연관된 만큼 엄격하게 규제된다[24]. 같은 해 8월 제정된 개인정보 보호법[25]은 생체, 건강, 금융 등 민감 정보의 보호를 강화하며, 정보 처리 시 정보 주체에 대한 고지 및 동의를 필수적으로 요구한다[26-28].

중국은 앞의 3법의 시행으로 인터넷 거버넌스 구축을 위한 기본적인 법체계를 마련하였으며, 이후 인터넷 정보 서비스의 발전에 따라 이를 기반으로 한 다음과 같은 규정들을 제정하였다. 2022년 3월 '인터넷 정보 서비스 알고리즘 추천 관리 규정(互联网信息服务算法推荐管理规定)'을 통해 알고리즘 추천 서비스 제공자가 데이터 보안 및 개인정보 보호 등 관리 시스템과 기술 조치를 수립하도록 하고, 가짜 뉴스 제작 및 인터넷 여론 형성 행위를 제한하는 등 국가 안보와 사회공공이익을 위협하는 행위를 금지하였다[29]. 2023년 1월에는 '인터넷 정보 서비스 딥페이크 관리 규정(互联网信息服务深度合成管理规定)'을 마련하여 딥페이크 기술이 적용된 인터넷 콘텐츠에는 해당 사실 적시 및 원본을 추적할 수 있는 디지털 표식을 삽입하도록 하고, 서비스 제공자에게 관리 감독의 책임을 부과하는 등 관리를 강화하였다[30].

그동안은 산발적인 법률을 통해 생성형 AI에 따른 위험에 대응해왔다면, 2023년 8월 '생성형 인공지능 서비스 관리 잠정 방법(生成式人工智能服务管理暂行办法)'[31]을 통해 생성형 AI에 특정된 보다 체계적인 규제를 갖추게 되었다. 제4조에 따르면 국가 안보 훼손 등 행정 법규에서 금지하는 콘텐츠를 생성해서는 안 되며, 훈련 데이터 선택에 있어 민족, 신앙, 국가 등에 대한 차별 방지를 위한 효과적 조치를 해야 한다[32]. 제7조에 따르면 생성형 AI 서비스 제공자는 데이터와 기본 모델의 출처가 합법적인지 확인해야 한다. 데이터가 지식재산권과 관련된 경우 이를 침해해서는 안 되며, 개인정보와 관련된 데이터 처리 활동을 수행할 때는 반드시 개인의 동의를 얻거나, 관련 법률 및 행정 규정에 따라야 한다. 또한, 훈련 데이터의 품질 보장을 위해 진실성, 정확성, 객관성, 다양성을 향상시킬 수 있는 효과적인 조

치를 해야 한다[33]. 제8조에서는 생성형 AI 기술의 연구 개발 과정에서 사용되는 데이터에 명확하고 구체적인 라벨링 규칙을 제정하고, 샘플링을 통해 라벨링 내용의 정확성을 검증할 의무를 명시하고 있다[34]. 제11조는 불필요한 개인정보의 수집을 금지하며, 사용자의 신원을 식별할 수 있는 정보의 불법적인 보관과 제3자에게의 제공을 금하고 있다[35].

2024년 9월 중국 국가 사이버보안 표준화 기술위원회(SAC: Standardization Administration of China)는 'AI 보안 거버넌스 프레임워크(人工智能安全治理框架) 1.0'을 공개하였다. 이는 2023년 10월 발표된 '글로벌 AI 거버넌스 이니셔티브'의 이행을 촉진하기 위한 목적으로 마련되었으며, AI 시스템의 생애주기에 따른 보안 위험을 분석하고, 주체별 의무를 명확히 규정하였다. 데이터 보안 위험과 관련하여 데이터의 불법 수집 및 사용, 부적절한 학습 콘텐츠, 데이터 유출 등을 경고하고, 이에 대해 지식재산권 보호 강화, 민감 및 고위험 영역에서의 엄격한 데이터 선별, 편향 데이터 필터링 등을 대응 조치로 제시하였다[36].

4. 한국

우리나라는 2019년 12월 발표한 '인공지능 국가전략'의 과제 중 하나로 2020년 12월 과학기술정보통신부와 정보통신정책연구원이 '사람이 중심이 되는 인공지능 윤리기준'을 마련하여 발표하였다. 10대 핵심 요건 중 데이터 관리와 관련된 기준으로 개인정보의 목적 외 사용을 금지하고 데이터 수집과 활용의 전 과정에서 데이터 편향성이 최소화되도록 데이터 품질과 위험을 관리할 것을 강조하였다[37]. 이는 구속력이 없는 도덕적 규범이자 자율 규범으로 향후 분야별 세부 규범이 유연하게 발전해나갈 수 있는 기반을 조성하였다.

하지만 기존 「개인정보 보호법」에는 AI 개발에 사용되는 공개 데이터를 규제할 수 있는 명확한 기준이 없었다는 점에서 2024년 3월 「개인정보 보호법」의 2차 개정 시 '자동화된 결정에 대한 정보 주체의 권리' 조항(제37조의2)이 신설되었다[38]. 이는 AI 기술을 적용한 자동화된 시스템으로 개인정보를 처리하여 이루어지는 결정이 정보 주체의 권리 또는 의무에 중대한 영향을 미치는 경우, 해당 결정에 대한 거부 및 설명 요구권을 보장하는 등 변화하는 데이터 환경에서의 국민의 권리를 강화하였다.

이후 2024년 5월 정부는 정부 합동으로 '새로운 디지털 질서 정립 추진계획'을 발표하였다. 동 계획은 2023년 9월 발표한 '디지털 권리장전'의 5대 원칙(자유, 공정, 안전, 혁신, 연대)을 바탕으로 한 20대 정책과제를 포함하고 있다. AI 및 데이터와 관련된 핵심 과제로는 '딥페이크를 활용한 가짜뉴스 대응'을 위한 AI 생성물의 워터마크 표시 의무화와 'AI 개발 · 활용 관련 저작권 제도 정비'를 위한 AI 학습 저작물에 대한 적정 이용 대가 산정방안 연구 등이 있으며, '디지털 재난, 사이버 위협, 범죄 대응'을 위한 피싱, 디지털 성범죄 등 민생 사이버 범죄 대응체계 정비 등의 내용을 포함한다[39,40].

이와 같은 배경 속에서, 개인정보보호위원회는 2024년 7월 'AI 개발 · 서비스를 위한 공개된 개인정보 처리 안내서'를 마련하였다. 공개 데이터는 인터넷상 누구나 합법적으로 접근할 수 있는 데이터로, 챗GPT 등 생성형 AI를 개발하기 위한 학습데이터의 핵심 원료로 사용된다. 이러한 공개 데이터에는 주소, 고유식별번호, 신용카드번호 등 여러 개인정보가 포함될 수 있어 정보 주체의 권리가 침해될 위험이 크다. AI 학습은 전통적인 개인정보 처리와 규모, 방식, 목적 등이 상이하여 적법 근거가 불명확한 측면이 있다. 이에 개인정보보호위원회에서는 AI 개발을 위해 공개된 개인정보가 수집 및 이용될

표 4 제22대 국회 발의 11개 AI 법률안 주요 내용

법률안	생성형 AI	고위험 AI		금지된 AI
	고지 및 표시	확인 제도	사전 고지	개발·이용 제한
인공지능 산업 육성 및 신뢰 확보에 관한 법률안 (안철수 의원 대표발의, 2024.5.31.)	●	●	●	×
인공지능 발전과 신뢰 기반 조성 등에 관한 법률안 (정점식 의원 대표발의, 2024.6.17.)	●	●	●	×
인공지능산업 육성 및 신뢰 확보에 관한 법률안 (조인철 의원 대표발의, 2024.6.19.)	●	●	●	×
인공지능산업 육성 및 신뢰 확보에 관한 법률안 (김성원 의원 대표발의, 2024.6.19.)	×	●	●	×
인공지능기술 기본법안 (민형배 의원 대표발의, 2024.6.28.)	●	●	●	×
인공지능 개발 및 이용 등에 관한 법률안 (권칠승 의원 대표발의, 2024.7.4.)	×	●	●	●
인공지능 기본법안 (한민수 의원 대표발의, 2024.8.22.)	●	●	●	×
인공지능책임법안 (황희 의원 대표발의, 2024.8.27.)	×	×	●	×
인공지능 발전 진흥과 사회적 책임에 관한 법률안 (배준영 의원 대표발의, 2024.8.28.)	●	●	●	×
인공지능의 발전과 안전성 확보 등에 관한 법률안 (이훈기 의원 대표발의, 2024.9.12.)	●	●	●	×
인공지능산업 진흥 및 신뢰 확보 등에 관한 특별법안 (김우영 의원 대표발의, 2024.9.24.)	×	●	●	×

출처 국민참여입법센터, https://opinion.lawmaking.go.kr/ 2024. 10. 8. 접속 [44].

수 있는 「개인정보 보호법」상 근거로 정당한 이익(제15조 제1항 제6호) 적용의 요건을 구체화하였다. 정당한 이익 조항의 충족 요건은 목적의 정당성, 처리의 필요성 및 구체적 이익 형량으로 구분되며, 기업은 이를 통해 개인정보 처리의 적법성을 주장할 수 있다. 기업은 공개된 개인정보 처리를 통해 개발하려는 AI의 개발 목적과 용도를 구체화하여야 하며, 해당 정보 처리의 필요성이 인정되어야 한다. 또한, 개인정보처리자의 정당한 이익이 정보 주체의 권리에 명백히 우선하는지를 평가하여야 하는데, 이때 기업은 안내서에 제시된 안전성 확보조치 방안을 도입하여 개인정보 침해 위험을 낮출 수 있다. 예를 들어, 적법한 수집 출처 검증, 개인정보 유출 방지 조치, 미세조정(Fine-tuning)을 통한 안전장치 도입 등의 기술적 조치를 포함한다[41-43].

우리나라에는 아직 AI에 관한 기본법이 없지만, 2020년부터 AI 기본법 제정을 위한 노력이 계속되어왔다. 현재 제22대 국회에는 표 4와 같이 11건(2024. 10. 8. 기준)의 AI 관련 법률안이 발의되어 있다[44].

데이터 보호 및 개인정보 보호 측면에서는 모든 법률안에서 고위험 AI를 '사람의 생명, 신체의 안전 및 기본권의 보호에 중대한 영향을 미칠 우려가 있는 영역에서 활용되는 인공지능'으로 별도 정의하고, 관련 사업자의 책무를 명시하고 있다. 사전 고지 의무만을 포함하는 1건의 법률안을 제외하고는 AI 시스템이 고위험 영역에 해당하는지 여부를 사업자가 확인하고 이를 이용자에게 사전 고지할 의무를 공통적으로 규정하고 있다. 7건의 법률안은 생성

형 AI에 대한 고지 및 표시 의무를 추가로 포함하고 있으며, 이는 생성형 AI를 이용하여 제품 또는 서비스를 제공하려는 자는 해당 제품 또는 서비스가 생성형 AI에 기반하여 운용된다는 사실을 이용자에게 사전에 고지하고, 해당 제품 또는 서비스의 결과물이 생성형 AI에 의해 생성되었다는 사실을 표시해야 한다는 의무이다. '인공지능 개발 및 이용 등에 관한 법률안'에서는 금지된 AI의 개발 및 이용을 제한하고 있으며, '인공지능책임법안'에서는 고위험 AI의 개발 및 이용을 별도의 장으로 구성하여 고위험 AI 개발사업자 및 이용사업자의 책무와 이용자의 권리를 구분하여 명시하고 있다는 특징이 있다. '인공지능의 발전과 안전성 확보 등에 관한 법률안'에서는 AI 관련 사업자가 AI 제품 또는 서비스를 제공하기 전 국민의 기본권에 미치는 영향을 평가하기 위해 노력하도록 하고, 국가기관 등은 고위험 AI를 이용한 제품 또는 서비스를 제공받으려는 경우 영향 평가를 실시한 제품 또는 서비스를 우선적으로 고려하도록 하였다. '인공지능산업 진흥 및 신뢰 확보 등에 관한 특별법안'에서는 고위험 범용 AI를 별도 정의하고 이와 관련한 사업자의 추가 의무를 명시하였다는 점에서 다른 법률안들과 차이가 있다.

Ⅲ. 주요국 데이터 규제 비교

주요국별 규제 접근 방식을 비교 정리하면 표 5와 같다. 미국은 법적 구속력이 발생하는 법률보다는 AI 권리장전 청사진과 같은 큰 틀을 제시하고, 행정명령을 통해 안전하고 신뢰할 수 있는 AI 개발 및 활용 촉진에 대한 연방정부와 기업의 책임을 강화하고 있다. AI의 위험성을 관리하기 위한 장치인 AI RMF는 AI 시스템의 위험도를 평가하고 우선순위를 지정해 사전 예방하는 규제 방식이나, 그 실행은 기업에 자율적으로 맡겨진다. 개인정보 보호법의 경우, 미국은 일반법을 두어 규율하는 유럽연합, 중국, 한국과는 달리 연방 차원에서 포괄적인 법률이 없고, 개별 주(州)가 독자적인 법을 시행하고 있다.

반면, 유럽연합은 AI 법과 GDPR을 통해 생성형 AI에 대한 포괄적인 법적 규제를 시행하는 국가이다. 특히 AI 시스템을 수용 불가, 고위험, 제한된 위험 및 최소 위험으로 구분하여, 고위험 AI 시스템에 대한 사전 규제와 감독을 강화하고 있다. 개인정보 보호와 AI 기술의 투명성을 핵심 원칙으로 삼으며, 생성형 AI가 야기할 수 있는 윤리적 문제나 편향성을 고려하여, AI 시스템이 학습 및 생성하는 데이터에 대한 책임을 명확히 부여하고 있다. 이는 생성형 AI가 가져올 위험성을 사전에 평가하고 이를 통제하는 강력한 법적 규제 체계를 구축하였다는 점에서 다른 국가들과 차별화된다.

중국은 데이터 및 개인정보 보호에 관하여 사이버보안법, 데이터보안법 및 개인정보 보호법을 기반으로 데이터 3법 체계를 구축하고 있다. 이에 더해 인터넷 정보 서비스 알고리즘 추천 관리 규정 및 인터넷 정보 서비스 딥페이크 관리 규정을 통해 생성형 AI에 따른 새로운 이슈들에 포괄적이기보다는 단편적으로 신속하게 대응해왔다. 이후 마련된 생성형 인공지능 서비스 관리 잠정 방법은 생성형 AI에 특정된 최초 규제로, 생성형 AI 기술의 유형 및 중요성 등급에 따른 차등 관리를 원칙으로 한다. 또한, 최근 중국이 AI 보안 거버넌스 프레임워크를 발표하여 AI 보안 위험을 분석하고 이에 주체별로 적극적으로 대응하려는 움직임을 보인다는 점은 주목할 만하다.

한국은 아직 생성형 AI에 대한 구체적인 법적 기준이 명확히 확립되지 않았으나, 범용성을 가진 AI 윤리기준을 일반 원칙으로 하여 이후 각 영역별 세부 규범이 유연하게 발전해나갈 수 있는 기반을 조성하였다. 이는 윤리 담론을 형성하는 도덕적 규범

표 5 주요국의 생성형 AI 시스템 학습 및 생성 데이터 규제 비교

구분		미국	EU	중국	한국
주요내용	학습데이터	• 데이터 수집, 사용, 접근, 이전 및 삭제에 관한 개인의 동의 필요 • 건강, 고용, 교육, 형사 사법, 금융 등 민감 영역에 대한 추론 제한 및 보호 강화	• 시스템의 의도된 목적을 고려한 관련성, 대표성, 무결성 및 완전성 보장 • 개인의 건강, 안전, 기본권에 부정적 영향을 미치거나 유럽연합 법령에 따라 금지된 차별을 초래하는 데이터 세트상의 편향 가능성 감지 및 완화를 위한 조치 시행 • 개인정보의 경우 구체적·명시적이며 정당한 목적으로 수집(공적 기록 보존, 역사·과학연구, 통계 목적 예외) • 개인정보의 수집·보관 최소화 • 개인정보 처리의 정확성, 무결성 및 기밀성 보장	• 합법적 출처가 있는 데이터 사용 • 개인정보의 경우 개인의 동의를 얻거나 법률 및 행정 법규에 규정된 그 밖의 상황에 부합 • 학습데이터의 품질 향상을 위한 효과적 조치 시행(진실성, 정확성, 객관성, 다양성) • 명확하고 구체적인 라벨링 규칙 제정·검증 및 담당자 교육 • 지식재산권 침해 금지 • 사이버보안법, 데이터보안법, 개인정보 보호법 준수 • 학습데이터 선택 시 민족, 신앙, 국가 등에 대한 차별 방지	• 데이터의 목적 외 사용 금지 • 데이터 수집 및 활용의 전 과정에서 편향성이 최소화되도록 데이터 품질·위험 관리 • 공개 데이터 세트 수집 사실, 주요 출처 및 처리 목적 공개 • 개인 식별자 삭제 또는 비식별화 조치를 통한 개인정보 유·노출 방지 • 미세조정을 통한 추가 안전장치 마련 권장
	생성데이터	• AI 생성물 인증, 출처, 라벨링, 음란 콘텐츠 생성 방지 관련 관행 보고 • 콘텐츠 인증 및 라벨링 지침 개발 • 차별적 생성물에 대한 테스트 및 보호 조치 시행 • 아동성학대 자료 제작 방지 조치 시행 • 생성형 AI 출력에 워터마크 등 라벨 표시	• AI 생성물이 기계 판독 가능한 형식으로 표시되고 인위적으로 생성 또는 조작되었음을 공개	• 가짜 뉴스 제작 및 인터넷 여론 형성 행위 제한 • 국가 안보 및 사회공공이익을 위협하는 콘텐츠 생성 금지 • 딥페이크 적용 콘텐츠에 해당 사실 적시 및 원본 추적용 디지털 표식 삽입, 서비스 제공자에게 관리 감독 책임 부과	-
관련근거	AI	• 국가 AI 이니셔티브법 • AI 권리장전 청사진 • 행정명령 제14110호 • AI RMF	• AI 법	• 인터넷 정보 서비스 알고리즘 추천 관리 규정 • 인터넷 정보 서비스 딥페이크 관리 규정 • 생성형 AI 서비스 관리 잠정 방법 • AI 보안 거버넌스 프레임워크	• AI 윤리기준 • AI 개발·서비스를 위한 공개된 개인정보 처리 안내서
	데이터	• 주(州)별 법률	• GDPR	• 사이버보안법 • 데이터보안법 • 개인정보 보호법	• 개인정보 보호법

에 그치나, 최근 개인정보 보호 개정을 통해 자동화된 결정에 대한 정보 주체의 권리를 강화하는 등 단계적으로 규제 체계를 확립해나가고 있는 것으로 보인다.

종합적으로, 각국의 데이터 규제 접근 방식에서 공통적으로 확인할 수 있는 점은, 생성형 AI 시스템에 활용되는 데이터는 개인정보 및 데이터 관련 법과 긴밀하게 연계하여 규제하고 있다는 것이다. 포괄적 법적 체계를 마련한 유럽연합을 제외한 국가들은, 생성형 AI 기술의 발전과 함께 나타나는 위험들에 대해 행정명령, 규정 · 방법, 지침 · 규범 등 각국의 상황에 맞는 규제 형태로 대응하는 것을 볼 수 있다. AI 시스템의 학습데이터는 수집 과정에서 적법한 목적을 가질 것을 기본으로 하며, 개인정보를 포함한 민감 영역에 해당하는 데이터의 경우 정보주체의 권리를 보호하기 위한 조치를 강화하였다. AI 생성물에 대해서는 미국이 생성형 AI의 출력에 대한 라벨링을 권고하고, NIST와 같은 기관을 통해

관련 지침을 개발하도록 하였다. 유럽연합과 중국은 AI에 의해 제작된 콘텐츠의 경우 이를 명시하도록 요구하고 있는 반면, 한국은 AI 생성물에 관한 지침이 아직 마련되지 않았다.

Ⅳ. 결론

AI 기술이 대규모 언어모델(LLM: Large Language Model)을 기반으로 한 생성형 AI로 발전하면서, AI가 가져오는 편익에 대한 기대가 높아짐과 동시에 데이터 보호 관련 문제가 더욱 중요해졌다. 이러한 기대와 우려 사이에서 주요국은 앞서 살펴본 바와 같이 생성형 AI 시스템의 데이터 학습 및 생성 과정에서 발생할 수 있는 위험을 방지하기 위한 규제들을 마련하고 있다.

지침 또는 규범의 형태로 생성형 AI 시대의 데이터 규제에 접근해온 우리나라는 다른 분석 대상 국가들의 규제 접근 방식과 내용을 객관적으로 비교 및 평가하여, 추진 중인 AI 법안에 대한 논의를 이끌어갈 필요가 있다. 미국, 유럽연합 및 중국은 모두 AI 시스템이 지닌 위험의 정도에 따라 규제 수단과 강도를 차별화하여 불필요한 규제 대상은 제외하고 혁신의 공간을 남겨두고 있음을 확인할 수 있었다. 생성형 AI의 규제와 발전 간 균형은 핵심 쟁점 중 하나인 만큼 보안과 혁신 촉진을 동등하게 중시하고, 서비스 제공자에게 지나친 의무를 부과하여 연구개발 의지를 약화시킬 가능성이 있지는 않은지 규제 내용을 면밀히 검토할 필요가 있다.

또한, 딥페이크로 인한 피해 사례가 속출하기 시작함에 따라, 생성형 AI 콘텐츠가 AI가 생성한 것임을 명시하여 개인정보 및 지식재산권 침해 등을 예방할 필요가 있다. 현재 유럽연합과 중국은 AI 생성물 라벨링을 의무화하고, 미국은 이를 권고하고 있는 상황이다. 반면, 우리나라의 경우 딥페이크를 악용한 범죄행위에 대해서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「형법」 및 「성폭력범죄의 처벌 등에 관한 특례법」에 의해 처벌하고 있으나, 딥페이크를 방지하기 위한 AI 생성물에 관한 직접적인 규제 내용은 마련되어 있지 않다. 이에 우리나라도 AI 생성물에 대한 적절한 식별 체계를 마련하여 생성형 AI의 오남용을 막기 위한 최소한의 안전장치를 마련할 필요가 있다.

마지막으로, 생성형 AI로 인한 위험은 글로벌 차원에서 공동의 도전과제로 인식됨에 따라, 이에 대응하기 위해서는 각국의 데이터 규제에 대한 상호 연계와 협력이 요구된다. 한국은 데이터 거버넌스의 강화와 더불어 국제적인 규제 동향을 적극 반영하면서도, 자체적인 데이터 관리 기준을 정교화하여 데이터 안전성과 공정성 및 윤리적 사용을 보장하는 방향으로 나아갈 필요가 있다. 이를 통해 생성형 AI 시대에서 기술 혁신을 뒷받침하는 동시에, 사회적 책임을 다하는 균형 잡힌 데이터 규제 체계를 마련할 수 있을 것이다.

용어해설

AI 시스템 AI를 사용하여 전체적 또는 부분적으로 작동하는 데이터시스템, 소프트웨어, 하드웨어, 애플리케이션, 도구 또는 공익시설

멀티모달 텍스트, 이미지, 음성, 영상 등 다양한 데이터 양식을 함께 처리하는 것

데이터 거버넌스 데이터의 가용성, 품질 및 보안을 증진하는 일련의 프로세스, 정책 및 표준

프로파일링 자연인의 개인적인 특정 측면을 평가하기 위하여 행해지는 모든 형태의 자동화된 개인정보 처리

고위험 AI 개인 또는 사회의 안전, 기본 권리 및 자유에 대해 높은 위험을 초래할 수 있는 AI 시스템

대규모 언어모델 대규모 데이터 세트에서 얻은 지식을 기반으로 자연어 및 기타 유형의 콘텐츠를 인식하고 요약, 번역, 예측 및 생성할 수 있는 딥러닝 알고리즘

약어 정리

CCPA California Consumer Privacy Act

CPRA	California Privacy Rights Act
GDPR	General Data Protection Regulation
LLM	Large Language Models
LMM	Large Multimodal Model
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
RCN	Research Coordination Network
RMF	Risk Management Framework
SAC	Standardization Administration of China

참고문헌

[1] OECD, "AI, data governance and privacy: Synergies and areas of international co-operation," OECD Artificial Intelligence Papers, No. 22, 2024. https://doi.org/10.1787/2476b1a4-en

[2] Google, "Gemini: A Family of Highly Capable Multimodal Models," arXiv preprint, 2023. https://doi.org/10.48550/arXiv.2312.11805

[3] CEDPO AI Working Group, "Generative AI: The Data Protection Implicatikons," CEDPO, 2023.

[4] C. Autio et al., "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile," NIST, 2024. https://doi.org/10.6028/NIST.AI.600-1

[5] G7 Hiroshima Summit, "Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI System," 2023.

[6] OECD, "G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI," 2023. https://doi.org/10.1787/bf3c0c60-en

[7] CPRA, California Privacy Protection Agency, 2024.

[8] The White House, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," Executive Order No. 13960, Dec. 8, 2020.

[9] National Artificial Intelligence Initiative Act of 2020.

[10] National Artificial Intelligence Initiative Act of 2020, Article 5103.

[11] National Artificial Intelligence Initiative Act of 2020, Article 5301.

[12] The White House, "Blueprint for an AI Bill of Rights," Office of Science and Technology Policy, 2022.

[13] The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Executive Order No. 14110, Oct. 30, 2023.

[14] The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Executive Order No. 14110, Article 1, Oct. 30, 2023.

[15] The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Executive Order No. 14110, Article 4.5(c), Oct. 30, 2023.

[16] The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Executive Order No. 14110, Article 9(a), Oct. 30, 2023.

[17] The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Executive Order No. 14110, Article 9(b), Oct. 30, 2023.

[18] The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Executive Order No. 14110, Article 9(c), Oct. 30, 2023.

[19] The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Executive Order No. 14110, Article 10.1(b)(viii), Oct. 30, 2023.

[20] EU, "General Data Protection Regulation (Regulation (EU) 2016/679)," Article 5.

[21] EU, "General Data Protection Regulation (Regulation (EU) 2016/679)," Article 22.

[22] EU, "The AI Act (Regulation (EU) 2024/1689)," Article 10.

[23] 全国人民代表大会常务委员会, 中华人民共和国网络安全法, 2016. 11. 7.

[24] 全国人大常委会, 中华人民共和国数据安全法, 2021. 6. 10.

[25] 全国人民代表大会常务委员会, 中华人民共和国个人信息保护法, 2021. 8. 20.

[26] 全国人民代表大会常务委员会, 中华人民共和国个人信息保护法, 第十七条.

[27] 全国人民代表大会常务委员会, 中华人民共和国个人信息保护法, 第二十九条.

[28] 全国人民代表大会常务委员会, 中华人民共和国个人信息保护法, 第三十条.

[29] 国家互联网信息办公室, 互联网信息服务算法推荐管理规定, 2022. 1. 4.

[30] 国家互联网信息办公室, 互联网信息服务深度合成管理规, 2023. 8. 15.

[31] 国家互联网信息办公室, 生成式人工智能服务管理暫行办法, 2023. 7. 13.

[32] 国家互联网信息办公室, 生成式人工智能服务管理暫行办法,

第四条.

[33] 国家互联网信息办公室, 生成式人工智能服务管理暂行办法, 第七条.

[34] 国家互联网信息办公室, 生成式人工智能服务管理暂行办法, 第八条.

[35] 国家互联网信息办公室, 生成式人工智能服务管理暂行办法, 第十一条.

[36] 全国网络安全标准化技术委员会, 人工智能安全治理框架, 2024. 9. 19.

[37] 과학기술정보통신부 보도자료, "인공지능(AI) 윤리기준 마련," 2020. 12. 23.

[38] 개인정보 보호법(법률 제19234호), 제37조 제2항.

[39] 대한민국정부, "새로운 디지털 질서 정립 추진계획," 2024. 5. 14.

[40] 과학기술정보통신부 보도자료, "대한민국이 새로운 디지털 질서 정립의 추진계획을 공개합니다," 2024. 5. 21.

[41] 개인정보보호위원회, "인공지능(AI) 개발·서비스를 위한 공개된 개인정보 처리 안내서," 2024. 7.

[42] 개인정보보호위원회 보도자료, "인공지능(AI) 개발·서비스에 이용되는 '공개 데이터' 처리 기준 제시," 2024. 7. 17.

[43] 개인정보보호위원회, "인공지능 시대 안전한 개인정보 활용 정책방향," 2023. 8.

[44] 국민참여입법센터. https://opinion.lawmaking.go.kr/ 접속일: 2024. 10. 8.