경북대학교 법학연구원『법학논고』
제81집 (2023.04) 409~440면.
Kyungpook Natl. Univ. Law Journal
Vol.81 (APR 2023) pp.409~440.
http://doi.org/10.17248/knulaw..81.202304.409

유럽 AI 법안에 있어 데이터 위험관리*

- GDPR 제35조와의 관계를 중심으로 -

서 창 배**

〈국문초록〉

AI 시스템의 활성화를 통해서 사회의 변화가 가속화 되고 있는 현실에서 AI 시스템에 대한 적절한 규제도 논의되고 있다. 현재는 이러한 규제의 논의가 자발적 규제의 수준에 머물러 있는 것으로 보인다. 그러나 이러한 자발적 규제만으로는 당면한 현실에 대비할 수 없는 상황이며 이러한 배경에서 EU에서 최근인 2021년 4월에 공표한 AI 법안은 독특하면서도 앞서가는 단일 법령으로 중요한 의미를 가지고 있다.

이러한 입법의 노력은 향후 AI 시스템 산업의 주도권을 가지기 위한 시도로 볼 수 있으며 그 내용적인 측면에서 위험 수준을 기준으로 시스템의 규제의 방식을 달리 하고 있다는 점에서 큰 시사점을 가진다.

이러한 측면은 이미 GDPR을 통해서 마련된 개인 정보 보호 장치들과 유사한 부분을 많이 가지고 있으며 AI 시스템의 특성상 양 법률이 중복될 여지가 많은 것으로 보인다. 특히 GDPR 제35조에서 규정하고 있는 정보보호 영향평가(Data Protection Impact Assessment) 방식은 AI 법안이 마련하고 있는 적합성 평가(Conformity Assessment)와 실질적으로 비슷한 내용임에도 중복 적용될 여지가 많아 산업 경쟁력의 측면에서도 문제가 제기된다.

아직 AI 법안이 최종 통과된 것은 아니며 앞으로의 변화를 지켜봐야 하겠지만 양 법률의 규제의 대상이 될 AI 시스템 공급자의 입장에서는 GDPR 제35조의 예비 평가의 방식과 AI 법안에서 예정하고 있는 적합성 평가라는 자율 평가 방식을 주목할 필요가 있다. 이는 여전히 대응적인 입법을 하지 못하고 있으며 FTA 등을 통해 산업적으로 계속 접촉하게 되는 EU와의 인공지능 시스템 산업 기준들과의 정합성 문제가 중요한 우리에 있어서도 중요한 문제가 될 것이기 때문이다.

우리의 경우에도 이미 EU의 AI 법안과 유사한 '인공지능산업 육성 및 신뢰 기반 조성에 관한 법률안'이 최근에 국회 과학기술정보방송통신위원회(과방위)의 법안소위를 통과하였으며 당해 법안은 국회 과방위에 발의된 7개의 인공지능 관련 법안을 통합한 법안으로 인공지능의 육성과 규율을 다루고 있다. 그러나 당해 법안은 데이터 오용의 위험성에 큰 관심을 두고 있지 않으며 이러한 와중에 최근 우리 개인정보보호법 개정 내용이 자동화된 의사결정과 같은 상황에 관해 새로운

* 이 논문 또는 저서는 2021년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2021S1A5C2A02089229)

** 전북대학교 동북아법연구소 전임연구원, 법학박사 (libero21c@naver.com)

내용을 규정하고 있어 향후 입법화 과정에서 좀 더 유연화된 입법 방향과 동시에 이에 대한 논의가 필요할 것으로 보인다.

주제어 : 유럽 인공지능 시스템 법안, 유럽 일반정보보호규정, GDPR 제35조, 정보보호 영향평가, 적합성 평가

• 투고일 : 2023.04.07. / 심사일 : 2023.04.24. / 게재확정일 : 2023.04.24.

Ⅰ. 들어가며

인공지능(Artificial Intelligence)의 활용에 관한 기대감과 동시에 큰 걱정의 분위기가 점점 고조되고 있는 것 같다. 이러한 분위기는 특히 자율주행차나 전장에서 사용되는 무인 항공기와 같이 실제로 개발되어 사용되고 있는 여러 인공지능 기술들의 실용화를 직접 눈으로 목격하면서 일반 시민들의 입장에서도 현실성을 느끼는 것에 기인하는 것으로 보여진다. 이러한 배경에서 인공지능 기술에 대한 규제 방안을 정립하려는 노력은 현재도 급격한 발전속도를 보이는 AI 기술력의 위험성에 대한 염려와 세계적인 산업 경쟁력 확보라는 두 가지 방향 사이에서 일종의 균형을 잡으려는 시도로도 해석할 수 있다. 즉 현재 인공지능 기술의 발전을 독려하고 있는 편익과 장래의 경제성이라는 요소들은 세계 각국의 적극적인 투자와 규제 개선의 방식을 이끌어 가고 있으며 이는 결과적으로 국가간의 경쟁으로 이어져 특히 기술 및 표준 개발을 위한 노력으로 이어지고 있는 것이다.

이미 미국과 중국에 비해 경쟁력을 잃고 있다고 판단한 유럽연합(EU)의 경우 2018년 '유럽 인공지능 전략'을 마련한 뒤 이에 따라 인공지능 산업의 발전을 위해 체계적으로 규제 방안에 관해 준비를 해 왔으며 구체적으로, 2018년 인공지능에 관한 독립적인 고등전문가 그룹의 작업을 시작으로 그 뒤 윤리가이드를 통한 자율적 규제를 실시하였으며 2021년 4월에 유럽연합 집행위원회(European Commission)을 통해 「인공지능에 대한 조화규범의 제정 및 일부 연합제정법들의 개정을 위한 법안(Proposal for a Regulation laying down harmonized rules on articial intelligence (Articial Intelligence Act) and amending certain Union Legislative Acts)」[1]을 공표하였던 것이다. 당해 법안

1) 이하 AI 법안으로 표시하며 각 조항들의 구체적인 내용은 지면 관계상 따로 표시하지 않음.

의 내용은 모든 형태의 인공지능을 대상으로 EU 역내에 인공지능 시스템을 출시하거나 서비스를 제공하는 전 세계의 사업자들에게 위험기반접근(risk-based approach) 방식을 통해 엄격하게 규제하는 것으로 볼 수 있다.

EU는 이러한 인공지능에 관한 법률과 제도적 장치를 통하여 세계 인공지능 기술 개발과 시장의 영향력을 강화하겠다는 목표를 가지고 있으며 당해 법안을 통해 향후 여러 국가의 입법화 과정에서 중요한 표준이 될 수 있을 것이다. 또한, 동 법안의 규제 대상이 EU 역내에서 사용되는 인공지능 개발 관련자들이라는 점에서 당해 법안이 입법화 되는 경우 전 세계 인공지능 시스템 공급업체 및 이용자에게 상당한 영향력을 끼칠 것으로 보여 결과적으로 구속력 있는 국제규범으로서의 역할을 담당할 가능성이 높다.[2)]

EU는 당해 법안이 공표되지 전인 2018년에 이미 일반정보보호규정(General Data Protection Regualation, 이하 GDPR)을 제정하였으며 AI 법안은 GDPR을 기본으로 마련된 이유로 많은 유사성을 지니고 있다.

인공지능 기술의 발전은 결과적으로 많은 사람들의 개인 정보를 분석할 가능성이 높기 때문에 이러한 영역의 정보 처리 방식은 특정 인공지능 시스템을 글로벌 데이터 개인 정보 보호 규정에 큰 영향력을 끼치고 있는 EU의 GDPR의 영역 내에서 다루어질 가능성이 높다. GDPR이 위험 기반 접근 방식을 사용하여 인공지능 시스템 내에서 뿐만 아니라 일반적인 개인 정보 처리를 규제하지만 이와 중복되는 기능의 인공지능 시스템의 경우에는 GDPR의 원칙이 적용되어야 한다. 이러한 상황은 AI 법안과 GDPR이 중복되어 규제되는 상황을 발생시키며 그 결과 몇몇 규정들의 경우는 해당 사업자들에게 큰 혼란을 던져줄 여지가 있다.

특히 높은 위험성을 가진 인공지능 시스템을 대상으로 한 EU AI 법안과 GDPR의 규제 방식에 상당한 유사점을 가지고 있어 이에 대한 평가 방식 즉 적합성 평가(Conformity Assessment)와 정보보호 영향평가(Data Protection Impact Assessment)의 중복 적용의 문제가 발생할 여지가 크며 이러한 부분들에 대한 해결 방식에 관해 EU 차원에서도 논의가 진행중이다.

우리의 경우에는 여전히 인공지능 산업 전체를 규제하는 특정 법률이 마련되지 못한 상태이며 이러한 이유에서 제21대 국회에서는 인공지능 산업 전반을 다루는 많은 법률안들이 의원발의로 제안되어 소관상임위원회에 회부되는 등 법률제정절차를 거치고 있는 중이다. 그러나 각 법안들의 체계와 입법방식

2) 고학수 · 임용 · 박상철, “유럽연합 인공지능법안의 개요 및 대응방안”, 「DAIG」, 2021년 제2호, 22면.

에 대하여 여전히 정해진 것은 없는 상황이며 그 중에서도 시스템의 평가 및 다른 법제와의 조화 문제를 다루는 내용은 포함되지 않은 것으로 보인다.

AI 산업 정책과 관련한 여러 의원 발의 입법안이 검토되고 있으며 관련 법률 개정을 통해 개별적인 내용들은 입법화 되고 있으나 여전히 AI 산업 규제에 대한 정부 부처간의 기준 또한 정리하지 못한 우리의 상황[3]에서 EU의 이러한 규제 방식을 통해 향후 관련 규제의 방향을 정함에 있어 참고할 필요가 있다고 보여진다.

Ⅱ. EU AI 법안의 구체적 내용

1. EU AI 법안의 의의

(1) EU AI 법안의 입법 과정

2021년 4월 21일 유럽집행위원회(European Commission)는 유럽의회(European Parliament)에 「인공지능에 대한 조화규범(AI 법)의 제정 및 일부 연합제정법들의 개정을 위한 법안(Proposal for a Regulation laying down harmonized rules on articial intelligence (Articial Intelligence Act) and amending certain Union Legislative Acts)」을 발의했으며 이를 통해 EU가 준비해 온 인공지능 백서[4]에 관한 수많은 토론의 결과물과 인공지능 윤리 원칙에 관해 유럽 의회가 제안해 온 내용들을 구체화 하였으며 특히 2020년 10월 21일 유럽 이사회가 제출한 제안서[5] 및 인공지능에 관한 고등전문가그룹의 제안서 내용[6]까지 모두 반영하여 입법화 과정을 거쳤던 것이다.

유럽연합 집행위원회(European Commission)는 AI 산업 규제라는 주제에 관해 윤리적인 방향과 법을 통한 규제의 방향이라는 두 가지 측면에 중점을 두고 있었으며 또한 이러한 두 가지 방향을 현실화 시키기 위해서 일반인의 이해와 신뢰를 바탕으로 실현하려는 의도를 가지고 구체적인 제도적 장치를 마

3) https://www.seoul.co.kr/news/newsView.php?id=20220113027013(2022년 11월 4일 방문)
4) European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 2020.
5) Council of the European Union, Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change, 11481/20, 2020.
6) HLEG, Ethics Guidelines for Trustworthy AI, 2019; HLEG, The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment, 2020.

련하려 노력하였던 것이다. 구체적으로, 인공지능 고등전문가그룹에 의한 '윤리 가이드라인(The Ehics Guidelines for Trustworthy Artificial Intelligence)'이 제정되고 개정되었으며 2019년 6월에는 제1차 유럽 인공지능 연합 총회에서 인공지능을 위한 평가목록(Assessment List for Trustworthy Artificial Intelligence)이 만들어지고 개정되었으며 그 결과 2020년 7월에는 기존 가이드라인에서 정하고 있는 7가지 요건[7]을 확인하기 위한 최종 상세안이 공표되었다. 또한 유럽연합 집행위원회는 이러한 과정에서 2020년 2월 인공지능의 활용을 위한 환경 조성의 방안으로 인공지능 알고리즘에 대한 법적 규제의 필요성을 배경으로 백서[8]를 발간하였으며 특히 당해 백서의 내용에 관해서 EU 회원국 및 시민들의 적극적인 참여를 이끌어 내기 위해서 설문조사 과정을 적극적으로 활용하였던 것이다.

이러한 배경에서 2020년 10월 EU 의회는 인공지능 관련 기술의 윤리 구축, 민사 책임 그리고 지적재산권에 관하여 각각의 보고서[9]를 채택하여 구체적인 원칙들을 제시했다. 또한 그 이 후 더 다양한 분야들 즉 인공지능의 활용 부분, 교육, 문화 및 시청각 부문에 대한 인공지능 등을 대상으로 한 규제 연구가 진행 되었으며 이러한 모든 보고서들의 내용을 감안하여 EU AI 법안이 제출되었던 것이다.

특히 당해 법안의 제정 배경에 대하여 미국과 중국의 방식과 다른 새로운 대안으로서의 입법화를 목표로 하는 것 보다는 현재 경쟁에서 우위를 차지하지 못하고 있는 EU의 산업적 상황을 개선시키려는 의도를 가진 보호 무역적 규제 체계로서의 의미가 강한 것으로 보여진다.[10]

---

7) '인적 기관 및 감독, 기술적 견고성 및 안전, 개인정보보호 및 데이터 거버넌스, 투명성, 다양성, 비차별성 및 공정성, 사회 및 사회적 웰빙, 책임'의 7가지 핵심 요구사항을 의미한다.

8) European Commission, WHITE PAPER On Artificial Intelligence – A European approach to excellence and trust, European Commission, 2020, 14-25면.

9) '인공지능, 로보틱스 및 관련 기술들의 윤리적 측면에 관한 구조 구축을 위한 제안 보고서(RE PORT with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies)','인공지능 민사 책임 체제를 위한 제안 보고서(REPORT with recommendations to the Commission on a civil liability regime for artificial intelligence)' 그리고 '인공지능 기술의 발전을 위한 지적재산권에 대한 보고서(REPORT on intellectual property rights for the development of artificial intelligence technologies)'의 3가지 보고서를 의미한다.

10) 고학수 · 임용 · 박상철, 앞의 글, 11면.

(2) 당해 법안의 주요 체계

당해 법안이 적용되는 대상인 인공지능 시스템의 범주는 구체적으로 첫째, 인간이 스스로 정의해 놓은 특정한 목적을 위한 용도인 경우 둘째, 기계학습, 논리·지식 기반 접근, 통계적 접근 등의 방식 중 하나 또는 복수의 기술 내지 기법을 활용하여 개발된 것인 경우 셋째, 해당 시스템들이 서로 작용할 수 있도록 해주는 일종의 소프트웨어들로 명시되어 있다(AI 법안 제3(1)조, 부속서 Ⅰ).

당해 법안이 구체적으로 제안하는 내용들은 대체적으로 신기술 개발을 저해하거나 비용을 증가시키지 않으면서도 인공지능과 관련된 위험과 문제를 해결하기 위한 균형감 있는 일종의 '위험 기반 규제 방식(risk-based regulatory approach)'을 제시하고 있다. 이러한 위험 기반 규제 방식의 특징은 인공지능 시스템이 EU 기본권을 해할 위험성의 정도를 기준으로 하여 그 규제의 강도를 나누어 정해 놓는 것으로 특히 고위험 인공지능 시스템을 대상으로만 강제적인 의무를 부과하면서 다른 인공지능 시스템에 관해서는 수정된 의무와 행동강령을 정해두는 식의 방식을 이용하고 있다. 특히 법안의 내용 중 고위험 인공지능 시스템이 가장 핵심적인 규제의 대상이 되며 이를 금지 시키지 않기 위해 다양한 요구사항을 상정해 놓고 이에 대한 사용을 허용하는 방식을 취하고 있는 것이다.[11]

이러한 배경에서 EU AI 법안은 특정 AI 시스템을 EU 내에서 출시(Placing on the market) 또는 서비스를 제공(Putting into service)하는 자(Providers) 혹은 EU 내에 위치한 인공지능 시스템의 영업 목적의 활용자(Users)를 당해 법안을 통한 규제의 대상으로 규정하고 있을뿐만 아니라(AI 법안 제2(1)(a)조, 제2(1)(b)조, 제3(4)조) EU 밖에 위치한 인공지능 시스템의 경우에도 그 시스템의 결과물이 EU 내에서 활용될 경우 해당 시스템의 제공자와 영업 목적의 활용자에게도 적용되도록 규정하고 있다(AI 법안 제2(1)(c)조, 제3(4)조).

규제 기관과 관련하여서도 회원국과 유럽연합 집행위원회의 대표들로 구성된 '유럽 인공지능위원회(European Artificial Intelligence Board)'를 설립하도록 하여 이를 통해 회원국 내 감독기구 및 유럽연합 집행위원회와 효율적으로 협력할 것을 정하고 있다. 또한 유럽연합 집행위원회에 조언과 전문지식을 제공하며 회원국 사이의 모범사례를 수집하고 공유하도록 정하고 있다(AI법안 제56조-제58조).

규제를 통한 산업의 위축과 위험성을 고려하여 특히 당해 법안은 기술 혁신

11) 김진우, "유럽연합 인공지능법안에 따른 고위험 인공지능 시스템 공급자 등의 의무", 「과학기술과 법」 제12권 제2호 2021.12, 119면.

의 필요성이 있는 소규모 기업과 스타트업을 지원하도록 여러 가지 장치를 마련하고 있으며 대표적으로 인공지능 규제 샌드박스 제도를 들 수 있다(AI 법안 제53조-제55조).

2. 위험[12] 기반 규제 방식(risk-based regulatory approach)의 구체적 내용

1) 수인불가 위험(Unacceptable Risk)의 경우

AI 법안은 EU 기본권 가치에 반하는 특정 목적을 지닌 AI 시스템에 대하여 그 사용을 원칙적으로 불허하는 태도를 보인다. 즉 잠재의식에 영향을 미치는 기술을 통해 사람들의 행동을 조작하려는 목적을 가진 AI 시스템의 경우, 특정 취약 계층에 대한 약취를 목적으로 한 AI 시스템의 경우, 셋째, 공공기관이 인공지능 기반 사회적 평점 시스템을 통해 자연인의 신뢰도를 평가 및 분류하려는 목적을 가진 경우, 넷째, 법집행을 위한 목적으로 공개적으로 '실시간' 원격 생체인식 시스템을 사용한 경우를 의미하며[13] 이러한 범주에 해당하는 경우에 당해 시스템의 사용을 금지시키는 것을 원칙으로 한다.

2) 높은 수준의 위험(High Risk)에 해당하는 경우

(1) 높은 수준의 위험(High Risk)을 가진 인공지능 시스템

높은 수준의 위험(High Risk)을 가진 인공지능 시스템을 허용하기 위한 요구 조건은 기본적으로 인공지능에 관한 고등전문가그룹(HLEG)의 권고 사항과 이를 바탕으로 한 인공지능에 대한 평가목록(Assessment List for Trustworthy Artificial Intelligence)을 통해 구체화 되었다.[14]

높은 수준의 위험을 가진 AI 시스템은 당해 법안 제6(1)조와 제6(2)조를 통해서 정해지며 그 기준을 두 가지 방식으로 나누어 규율하고 있다.

구체적으로, 우선 EU AI 법안의 부속서 II(Annex II)에 열거된 제품들을 대상으로 적합성 평가를 거쳐야 되는 제품이거나 그러한 제품의 안전장치(safety

---

12) AI 법안상의 위험의 의미는 단순한 위험(danger)이 아닌 불확실성(uncertaninty)을 포함하는 것으로 해석하여야 한다: 고학수 · 임용 · 박상철, 앞의 글, 20면.

13) 중국의 천망공정(Skynet Project)을 대표적인 예로 들 수 있으며 그 중에서도 범죄 피해자 표적 수색(중국의 사회신용체계와 같은 것을 의미), 임박한 위협방지 등의 특수한 경우에는 예외로 한다.

14) The final report of HLEG on 31 January 2018: https://finance.ec.europa.eu/system/files/2018-01/180131-sustainable-finance-final-report_en.pdf.

component)로의 이용을 위해 마련된 인공지능 시스템을(당해 제품과의 독립성 여부와 상관없이) 하나의 유형으로 정하고 있다(AI 법안 제6(2)조). 즉 부속서 II에 열거된 제품을 예시하자면, 기계, 완구, 레저 · 개인용 선박, 승강기, 폭발성 기체 장치와 보호시스템, 전파기기, 고압기기, 케이블카, 개인보호장구, 기체 연료 연소장치, 의료기기, 실험실용 진단기기, 자동차, 민항기, 2륜차 · 3륜차 · 해상장비, 철도시스템 등을 들 수 있다.

이에 반해 부속서 Ⅲ(Annex Ⅲ)는 특정 목적이라는 기준을 통해서 높은 수준의 인공지능 시스템을 분류한다(제6(2)조). 즉 자연인의 생체인증 · 범주화(biometric identification and categorization of natural persons), 중요 인프라의 관리 · 운영(management and operation of critical infrastructure), 교육 · 직업훈련(education and vocational training), 채용 · 인사관리 · 자영기회(employment, workers management and access to self-employment), 필수적 공공 · 민간서비스 혜택의 접근 · 향유(access to and enjoyment of essential private/public services and benefits), 법집행(law enforcement), 이민 · 난민 · 출입국관리(migration, asylum and border control management), 사법과 민주적 절차의 집행(administration of justice and democratic process) 이라는 8가지 목적과 관련된 AI 시스템 의미한다.

특히 부속서 Ⅲ(Annex Ⅲ)에 대하여 AI 법안은 특정의 요건을 전제로 집행위원회가 그 구체적인 적용 범위를 정정 할 수 있도록 정하고 있으며(AI 법안 제7(1)조) 이 경우 이미 발생한 피해 및 기본권 위협 가능성 여부 또는 사용자들 사이의 불평등성 여부 등을 고려토록 정하고 있다(AI 법안 제7(2)조).

(2) 위험관리체계

높은 수준의 위험(High Risk)을 가진 인공지능 시스템의 경우 시스템 공급자, 제조업자뿐만 아니라 유통업체, 수입업체, 사용자 기타 제3자에게도 일정한 법적 의무를 부과하고 있다.

AI 법안 제16조부터 제29조까지 정하고 있는 구체적인 의무들은 '법안에 따라 요구사항들을 충족시킬 의무, 품질 관리 시스템(규정준수를 위한 전략, 시스템 디자인 · 테스트 · 데이터 관리 관련 절차 및 방법, 위험관리 시스템, 사후(post-market) 모니터링, 책임 체계 등) 구축 의무, 기술 문서 작성 의무, 통제하에 있을 때 고위험 인공지능 시스템에서 자동으로 생성된 로그 기록의 보관 의무, 고위험 인공지능 시스템의 시장 출시나 서비스 전 관련 적합성 평가 절차 수행의 의무, 등록 의무(제품 출시나 서비스 전 EU 데이터베이스에 인공지

능 시스템 등록) 준수 의무, 요구사항에 위배되는 상황 발생 시 필요한 시정조치를 수행할 의무, 인공지능 시스템이 사용되거나 서비스되고 있는 회원국 관할 당국 또는 인증기관이 의무 미준수사항 및 수행한 시정조치를 통지할 의무, 규정준수를 알 수 있도록 고위험 인공지능 시스템에 CE 마크를 부착할 의무, 국가 관할 기관 요청 시 고위험 인공지능 시스템의 요구사항 준수를 입증해야 할 의무'를 의미한다.

또한 높은 수준의 위험(High Risk)을 가진 인공지능 시스템이 시장에 출시되거나 해당 제품들과 함께 서비스되는 경우, 제품 제조업체는 인공지능 시스템 공급자와 동일한 의무를 지니며 수입업체, 유통업체에게는 요구사항 준수 확인, 위험 감지 시 통지, 요구사항 준수에 위협이 되지 않는 보관·운송, 정보 제공 및 협조의 의무 등이 부과된다.

이 이외에도 예외적으로 고위험 인공지능 시스템 사용자[15]에게도 제공된 사용지침을 이용할 의무, 시스템 목적에 맞는 인풋 데이터를 활용해야 할 의무, 시스템 모니터링 의무, 위험인지 시 통보 및 사용금지의 의무, 기록보관 및 데이터 보호를 위한 영향평가 수행을 위해 제공된 정보의 활용 등의 의무가 부과된다.

정리하자면, 높은 위험성을 가진 인공지능 시스템은 몇 가지의 요건들 즉 데이터 거버넌스, 투명성, 통제성, 정확성, 견고성, 보안성 등의 요건들을 갖추어야 하며 이를 보증하기 위한 위험 관리 시스템, 기술문서, 문서 보존 등의 시스템을 마련하여야 출시 및 사용할 수 있다.

(3) 허가 요건으로서의 적합성 평가(Conformity Assessment)제도

① 적합성 평가 제도

기술한 기본적인 허가 조건을 제외하고도 높은 수준의 위험(High Risk)을 가진 인공지능 시스템을 공급 또는 출시하기 위해서 가장 중요한 것은 AI 법안 제43조에 따른 적합성 평가 절차를 적용해야 한다는 점이다(AI 법안 제19조). 즉 당해 법안에 따른 모든 의무자들 중에서 특히 공급자의 경우에는 높은

15) 당해 법안에서 이 경우 정하고 있는 '사용자'의 범주는 자체 권한 하에서 인공지능 시스템을 사용하는 자연인 또는 법인, 공공기관, 에이전시, 또는 기타 기관을 포함하는 의미(단, 개인적으로 non-professional 활동을 위해 인공지능 시스템을 사용하는 경우는 제외)이다. 또한 고위험 인공지능 시스템에 부과되는 의무들의 경우에 만일 당해 결과물이 EU 내에서 사용된다면 EU 외 제3국에 존재하는 서비스 제공자, 사용자에게도 적용된다.

수준의 위험을 가진 인공지능 시스템에 관해 가장 광범위한 의무들을 부담하며 그 중에서도 부속서 Ⅳ에 따른 내부통제 또는 부속서 Ⅷ에 따른 인증기관에 의한 통제를 통한 고위험 시스템의 허용 요건은 차치하고서라도 CE 표식[16]을 포함한 적합성 평가 과정을 거쳐야 한다.

AI 법안은 적합성 평가 기관(conformity assessment bodies)은 각 회원국들에 설치된 통보기관(notifying authorities)을 통해 인증기관으로 지정되어 감독을 받도록 규정하고 있으며(AI 법안 제30조, 제31조) 이들 기관을 통해 높은 수준의 위험성을 가진 인공지능 시스템의 적합성이 검증되도록 정하고 있다(AI 법안 제33(1)조).

② 적합성 평가의 방식

인공지능 시스템 제공자는 원격 생체정보기반 식별의 시스템의 경우와 핵심기반시설의 관리·운영 시스템의 경우에는 우선 EU 통합기준을 준수했음을 입증하는 것을 전제로 자율 적합성 평가(conformity assessment based on internal control) 혹은 제3의 인증기관의 품질관리시스템 및 기술 문서에 기한 적합성 평가만을 요구한다. 이에 반해 EU 통합기준을 미적용 또는 부분 적용하거나 통합기준이 없는 경우에는 제3의 인증기관의 적합성 평가를 통과해야만 한다(AI 법안 제43(1)조).

특히 자율 적합성 평가(conformity assessment based on internal control)는 품질관리시스템, 기술 문서상의 정보, 시스템의 설계개발 과정 및 출시 후 관리자의 모니터링을 통해 당해 법안의 내용을 충실히 준수했음을 스스로 밝히는 방식으로 이루어지며(부속서 VI) 이 과정에서 인증기관은 적합성 평가 통과에 대한 확인서(certificate)를 발급하는 방식으로 평가 결과를 확인해 준다(AI 법안 제44조).

③ 인증기관(notified bodies) 및 시장감시기관(market surveillance authority)의 의무

AI 법안은 높은 수준의 위험성을 가진 인공지능 시스템의 적합성을 검증할

16) CE 표식(CE Marking)은 프랑스어 Conformité Européenne의 약어로 유럽공동체인 EC를 의미한다. CE 마크는 유럽 연합 국가와 유럽 경제 지역 모두에서 시장에 출시 된 제품에 대한 필수 준수 표시로서 이를 제품에 부착한다는 것은 제조자가 해당 제품이 EU 이사회에서 제정한 규정(Regulations) 또는 지침(Directives)의 필수 요구사항(Essential Requirements)에 따라 적합성 평가를 하였으며 이를 만족한다는 것을 의미한다: https://www.ceisaret.com/ko/ce-isareti-ne-anlama-gelir/

인증기관(notified bodies)과 적합성평가기관(conformity assessment bodies)에 대한 선임과 감독에 관해 각 회원국들이 설치한 통보기관(notifying authorities)에 권한을 부여하고 있다(AI 법안 제30조, 제31조).

그 결과 인증 기관(notified bodies)은 통보 기관(notifying authorities)에게 법안에서 정해 놓은 정보들 즉 부속서 VII의 요구사항에 따라 발급된 유럽연합 기술 문서 평가 인증서, 동 인증서의 추록, 품질 관리 시스템 승인, 부속서 VII의 요구사항에 따라 발급된 유럽연합 기술 문서 평가 인증서 등을 제공해야 한다(AI 법안 제46(1)조) 또한 각 인증 기관은 다른 인증 기관의 요청에 따라 당해 인증기관이 거부하거나 취소한 품질 관리 시스템 등에 관한 정보를 제공해야 한다(AI 법안 제46(2)조). 특히 각 인증 기관은 유사한 품목에 대한 적합성 평가 활동을 수행하는 다른 인증 기관에게도 적합성 평가 결과에 관한 정보를 제공해야 한다(AI 법안 제46(3)조).

이러한 과정과 더불어 시장 감시 기관(market surveillance authority)의 경우에는 AI 법안 제43조 즉 적합성 평가에 대한 예외를 허용할 수 있다. 즉 공공안전 또는 개인의 생명과 건강의 보호, 환경의 보호, 주요 산업 및 인프라 자산의 보호 등을 근거로 관련 회원국의 영토 내에서 특정 높은 위험을 가진 인공지능 시스템을 출시하거나 서비스를 개시하는 것을 예외적으로 허가해 줄 수 있으며 그 기간은 필요한 적합성 평가 절차가 수행되는 제한된 기간으로 한정되고 그러한 절차가 완료되는 즉시 종료되도록 정해져 있다(AI 법안 제47(1)조).

(4) EU 자기적합성 선언 및 CE 적합성 마크

인공지능 시스템 제공자는 각 인공지능 시스템을 대상으로 EU 적합성 선언서를 작성한 뒤 인공지능 시스템이 출시되거나 서비스 개시된 후 10년간 보관해야 한다. 관련 국가의 담당 기관에서 요청이 있는 경우에 인공지능 시스템 제공자는 EU 적합성 선언서 사본을 제공해야 한다(제48(1)조).

EU 적합성 선언의 내용과 관련해서 AI 법안은 특정 고위험(High Risk) 인공지능 시스템이 본 편 제2장에 명시된 요구사항을 준수하고 있다는 점과 부속서 V에 명시된 정보 모두 포함되어 있음이 표시되어야 한다(제48(2)조, 제48(3)조). 또한 고위험 인공지능 시스템과 관련하여 EU 적합성 선언을 요구하는 다른 EU 법령과의 조화를 고려하여 하나의 EU 적합성 선언을 작성해야 하며 이에는 관련된 모든 유럽연합 조화 법령의 식별에 필요한 모든 정보가 포함되어야 한다(제48(3)조).

CE 표식(마크)은 고위험 인공지능 시스템을 대상으로 가독성과 지속성을 갖

춘 형태로 직접 부착되어야 하나 이러한 방식이 현실적으로 어려운 경우 포장이나 첨부 문서를 통해 부착하는 것도 허용된다(제49(1)조).

3) 제한적 위험(Limited Risk)을 보유한 인공지능 시스템

(1) 세 가지 유형

AI 법안은 제한적 위험(Limited Risk)을 보유한 인공지능 시스템을 세 가지 유형으로 특정하여 규정한다. 구체적으로, 우선 인간과의 상호작용이 예정된 인공지능 시스템(AI systems intended to interact with natural persons)으로 대화형 인공지능 시스템(AI 법안 제52(1)조) 둘째, 인간의 뇌파 혹은 DNA 등과 같은 정보를 이용하는 감정인식 시스템(emotion recognition system) 및 생체정보 기반 범주화 시스템(biometric categorization system)(AI 법안 제52(2)조) 그리고 셋째, 실존하는 사람 · 대상 · 장소 또는 다른 주체 · 사건에 가깝고 진정 · 진실된 것처럼 보이게 하는 화상 · 시각 · 청각 콘텐츠를 생성 · 조작하는 인공지능 시스템(AI system that generates or manipulates image, audio or video content thatappreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful)(AI 법안 제52(3)조)의 세 가지로 유형 짓고 이들에 대해 투명성 의무를 부과하고 있다.[17]

(2) 투명성 의무에 관하여

기술한 세 가지 유형의 제한적 위험(Limited Risk)을 보유한 인공지능 시스템의 경우 제공자나 활용자에게는 고지 의무 혹은 공개 의무를 부과한다. 구체적으로, 시스템 설계 · 개발의 단계에서 시스템 제공자는 자연인과 상호 작용하는 인공지능 시스템이 해당하는 자에게 인공지능 시스템과 상호 작용하고 있다는 것을 미리 알려야 하며 감정 인식 시스템 또는 생체 인식 분류 시스템의 경우는 당해 시스템에 노출되는 사람들에게 이를 미리 고지해야 한다(AI 법안 제52(1)조, 제52(2)조).

특히 딥 페이크 인공지능 시스템 즉 기존의 사람, 물체, 장소, 기타 실체 또는 사건처럼 보이도록 영상 등이 조작된 경우 당해 시스템의 사용자는 해당 콘텐츠의 인위성 여부를 공개하여야 한다(AI 법안 제52(3)조).

17) AI 법안 해석에 따르면 투명성 의무는 높은 위험성을 가진 인공지능 시스템의 경우에도 부과될 여지가 있다: 고학수 · 임용 · 박상철, 앞의 글, 20면.

(4) 최저의 위험성(Minimal Risk)을 가진 인공지능 시스템

기술한 위험성을 띠지 않는 인공지능 시스템에 관해 AI 법안은 특별한 규제를 정하고 있지 않으며 EU 집행위원회와 회원국이 특정 인공지능 시스템에 적절한 행동지침을 자발적으로 준수할 것을 장려할 수 있도록 정하고 있을 뿐이다(AI 법안 제69조).

3. 그 이외의 규제 사항

1) 규제 샌드박스

위험성을 근거로 특정 인공지능 시스템에 관한 여러 규제 방안을 마련하고 있는 AI 법안은 산업에 대한 지나친 규제라는 우려에 완화책을 마련해 두고 있으며[18] 소상공인과 스타트업을 지원하기 위한 인공지능 규제 샌드박스 및 기타 수단을 사용할 수 있도록 허용하고 있는 점을 예로 들 수 있다(AI 법안 제53조-제55조).

구체적으로, 우선, 하나 이상의 회원권 관할 기관 또는 유럽 데이터 보호 감독관에 의해 특정된 인공지능 시스템 규제 샌드박스란 혁신적인 AI 시스템의 출시를 전·후로 하여 제한된 기간 동안 검증할 수 있는 자유로운 환경을 제공하는 방식을 의미하며(AI 법안 제53(1)조) 이러한 과정에서 건강과 안전 및 기본권에 대한 중대한 위험이 확인되면 완화 조치 및 일시 정지 조치가 이루어지도록 정하고 있다(AI 법안 제53(3)조).

두 번째로, 제3자에게 피해가 발생한 경우 해당 유럽 연합 및 회원국 법에 따라 책임을 부담해야 하며(AI 법안 제53(4)조) 또한 인공지능 규제 샌드박스를 설립한 회원국의 관할 기관은 유럽 인공지능 위원회의 프레임워크 내에서 활동을 조율하고 협력해야 한다. 이에 더하여 당해 기관은 샌드박스의 결과가 포함된 연례 보고서를 위원회와 유럽연합 집행위원회에 제출할 의무를 부담하며 이에는 모범 사례 및 샌드박스 내에서 감독을 받는 기타 EU 법의 적용에 대한 권고사항이 포함되어야 한다(AI 법안 제53(5)조).

세 번째로, 공익 목적의 특정 인공지능 시스템의 경우에는 이를 위한 개인 데이터 처리와 보관 방식 등에 관해 여러 가지 규칙을 미리 정해 놓고 있다

18) EU AI 법안 (EUROPEAN COMMISSION (2021.4.21), Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS), p. 4.

(AI 법안 제54조).

마지막으로, 특히 소규모 제공자 및 사용자를 위하여 당해 법안은 이들이 자격 요건을 갖춘 경우 인공지능 규제 샌드박스에 우선적으로 접근할 수 있도록 정하고 있으며 제43조에 따른 적합성 평가의 수수료를 책정하는 과정에서도 이들의 규모와 시장 규모에 비례하도록 수수료를 경감토록 정하고 있다(AI 법안 제55조).

2) 기밀유지와 벌칙 관련 조항

당해 법안의 내용을 실제로 적용함에 있어 국가 관할 기관과 인증 기관에게 획득한 정보들 즉 지적재산권이나 영업비밀 등에 관해 비밀유지 의무를 부과하고 있으며 이에 더하여 공공의 이해 관계 그리고 사법 또는 행정 절차의 무결성 등을 보호할 의무를 부과하고 있다(AI 법안 제70(1)조).

AI 법안은 당해 법안의 내용을 따르지 않는 인공지능 시스템의 사용 등에 관하여 높은 수위의 벌칙을 정하고 있다. 즉 수인불가 위험성을 가진 인공지능 시스템 관련 내용(AI 법안 제5조)을 위반한 경우 및 고위험 인공지능 시스템의 데이터와 데이터 거버넌스 요건(AI 법안 제10조)을 위반한 경우 3천만 유로의 과징금을 부과하고 있으며 특히 그 대상이 기업인 경우에는 직전사업연도 전세계 총매출액 6% 중 높은 액수 이하의 과징금을 부과하고 있다(AI 법안 제71(3)조). 또한 그 이외의 법안 내용 위반의 경우에도 2천만 유로를 부과하면서 이 경우에도 그 대상이 기업인 경우에는 직전 사업연도 전세계 총매출액 4% 중 높은 액수 이하의 과징금을 부과하고 있다(AI 법안 제71(3)조)).

이러한 처벌 규정의 적용과 관련하여 각 회원국에게 당해 벌칙 규정들의 효율성을 보장할 의무를 부과하고 있으며 특히 각 개별 사례를 처리함에 있어 법 위반과 그 결과의 성격과 중대성 및 지속기간, 누범 여부 및 행위자의 규모와 시장 점유율 등을 고려토록 정하고 있다(AI 법안 제71(6)조).

Ⅲ. GDPR의 AI에 대한 영향력 행사

1. GDPR의 의의

EU 일반 개인정보 보호법(GDPR, General Data Protection Regulation)은

EU 회원국에 직접 적용되는 개인정보 보호법이며 2016년 제정되어 2018년부터 시행되었다. GDPR이 보호하려는 개인정보란 식별되었거나 식별 가능한 정보주체와 관련된 모든 개인 정보들 뿐만 아니라 암호화 정보, 생체 정보, 온라인 식별 정보나 위치 정보도 포함하는 개념이다.

GDPR은 총 11장으로 나누어 개별적인 99개 조항으로 구성되어 있으며 특히 정보주체의 권리와 이를 침해한 기업의 책임을 강화시키는 내용들이 주를 이룬다. 특히 GDPR은 EU 내 사업장을 운영하는 기업뿐만 아니라 전자상거래 등을 통해 해외에서 EU 주민의 개인정보를 처리하는 기업에도 적용될 수 있을 뿐만 아니라 당해 규정 위반 시 막대한 과징금 부과[19]를 규정하고 있다.

GDPR은 기존의 지침(Directive)의 형식을 가졌던 규제들과 달리 법규(Regulation)라는 법 형식으로 제정되어 법적 구속력을 가지며 모든 EU 회원국 들에게 직접 적용되는(GDPR 제99조) 통일된 개인정보보호로서의 특징을 가지고 있다.

2. GDPR의 기본 원칙

GDPR은 개인정보를 처리하는 경우 7가지 원칙을 모두 준수하도록 규정하고 있으며 그 구체적 내용은 합법성 · 공정성 · 투명성 원칙, 목적 제한의 원칙, 개인정보 최소처리 원칙, 정확성의 원칙, 보유기간 제한의 원칙, 무결성과 기밀성의 원칙, 책임성의 원칙을 의미한다(GDPR 제5조).

구체적으로 개인정보 처리의 합법성 · 공정성 · 투명성 원칙에 관하여 개인정보 처리는 GDPR에서 허용한 요건들 중 하나 이상에 해당해야 합법적인 것으로 인정된다(GDPR 제6조). 즉 정보 주체가 하나 이상의 특정한 목적을 위하여 본인의 개인정보 처리에 동의한 경우, 정보 주체가 계약 당사자로 있는 계약의 이행을 위하여 또는 계약 체결 전 정보주체의 요청에 따라 조치를 취하기 위하여 처리가 필요한 경우, 컨트롤러에 적용되는 법적 의무를 준수하는 데 처리가 필요한 경우, 정보 주체 또는 제3자의 생명에 관한 이익을 보호하기 위한 경우, 공익을 위하거나 콘트롤러의 권한에 따라 이루어진 업무 처리를 위한 경우, 컨트롤러 또는 제3자의 정당한 이익 목적을 위해 처리가 필요한 경우를 의미한다. 그러나 이러한 경우에도 개인정보가 보호되어야 할 정보 주체의 이익 또는 기본적 권리와 자유가 우선되는 경우에는 예외로 한다.

---

19) 전 세계 매출액의 2% 혹은 1천만 유로(약 125억원) 중 높은 금액을 기준으로 과징금을 책정하며, 중요한 위반 사항인 경우 전 세계 매출액의 4% 혹은 2천만 유로(약 250억원) 중 높은 금액을 과징금으로 부과한다.

3. GDPR과 AI 법안의 관계

실제로 GDPR과 AI 법안과의 중복 적용 여부가 문제가 되는 것은 높은 위험성을 보유한 AI 시스템의 경우 즉 GDPR에서 규제하는 고위험 정보 처리 작업의 경우에 있어서이다.

AI 법안 초안에 대한 설명에서 유럽 위원회는 GDPR이 AI 법의 영향을 받지 않을 것을 선언하고 있어[20] 원칙적으로 양 규정은 중복하여 적용될 수 있다. 즉 고위험 AI 시스템을 개발하기 위해 개인 데이터를 사용하는 경우 공급자는 AI 법의 데이터 처리 요구 사항 및 GDPR의 개인 데이터 처리를 위한 요구 사항을 준수해야 한다.

그러나 유럽 위원회가 AI 법안을 정당화하기 위해 사용하는 두 가지 법적 근거 중 하나는 EU가 개인 데이터 처리와 관련하여 개인 보호와 관련된 규칙을 제정하도록 의무화하는 유럽 연합 기능에 관한 조약(TFEU) 제16조이다. 이를 근거로 적어도 어느 정도는 AI 법의 규칙이 GDPR에 따라 데이터 주체에게 제공되는 보호를 보완할 것임을 의미한다고 볼 수 있다. 실제로 2021년 AI 법에 대한 공동 의견에서 유럽 데이터 보호 감독관(EDPS)과 유럽 데이터 보호 위원회(EDPB)는 AI 시스템이 AI 법에 따라 CE 마크 제품으로 유럽 시장에 진입할 수 있도록 하기 위한 전제 조건으로 GDPR 준수를 제안한 바가 있다.

사실 2021년 4월 공표된 AI 법안은 현재에도 제정 작업 중에 있으며 그 구체적인 내용이 GDPR과 유사성을 띠는 것도 사실이며 GDPR 집행상의 문제점을 반복하지 않으려 여러 가지 거버넌스 조항을 2022년 4월에 수정안을 통해 보완하였다.[21] 이러한 과정들은 향후 완성된 AI 법안이 AI 관련 사업자들에게 추가적인 과제를 부과할 가능성이 높다고 볼 수 있으며 그 구체적인 내용은 GDPR 상의 엄격한 데이터 보호 요구 사항과도 밀접한 관련성이 있다고 보여진다.

---

20) EU AI 법안 (EUROPEAN COMMISSION (2021.4.21), Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS), p. 4.

21) 정소영, “유럽연합 인공지능법안의 거버넌스 분석 - 유럽인공지능위원회와 회원국 감독기관의 역할과 기능을 중심으로 -”, 「연세법학」제39호(2022. 7), 33면.

Ⅳ. GDPR과 AI 법안의 실제 적용의 문제

1. AI 환경에서의 GDPR 적용의 문제

최근의 AI 기술의 급격한 발전은 완전 자동화된 시스템을 통한 개인 정보 처리의 양이 크게 증가하는 현상이 생기고 있으며 이러한 결과물에 의존한 의사결정의 횟수도 크게 늘어나고 있다.

EU GDPR 역시 이러한 상황에 대비하여 자동화된 알고리즘에 의한 개인정보 처리와 그에 따른 결정의 결과 인간 존엄을 해할 위험성이 있다는 인식을 전제로 이를 방지할 정보 주체의 권리를 보호하는 방향의 내용 즉 원칙적 금지와 예외적 허용의 방식을 정하고 있다.

AI를 통해 처리되는 개인정보가 포함된 데이터의 법 적용 범위는 원칙적으로 GDPR의 내용에 속하게 되지만 실제로 그 기준이 잘 마련된 것은 아니다. GDPR이 정하고 있는 개인정보의 구체적인 정의를 살펴보면, 식별된 혹은 식별가능한 정보주체와 관련된 모든 정보를 의미하며 이들의 이름, 식별번호, 위치정보, 온라인 식별자와 같은 식별자를 참조하여 식별될 수 있거나 또는 생리적, 유전적 정보를 통해서 특정 가능해지는 정보주체의 모든 정보를 의미한다(GDPR 제4조). 그러나 최근 ChatGPT로 대표되는 인공지능 시스템을 통해서 다루어지는 다양한 데이터들은 AI의 성능에 따라 여러 데이터의 관련성을 찾을 수 있는 가능성을 향상될 수 있으며 이는 곧 비개인정보화 시킨 정보를 다시 식별 가능하게 만드는 데이터 패턴을 인식하는 방식을 사용하기 때문에 개인정보보호법상의 내용을 직접 적용하기에 는 그 기준을 더욱 불명확하게 만들 가능성이 있다.

이러한 배경에서 개인 민감정보 및 이와 관련된 내용을 최대한 보호하려는 목적을 가진 GDPR의 내용과 그 내용을 최대한 해제시켜 원하는 결과를 이끌어 내려는 인공지능 알고리즘의 기능과의 차이는 결과적으로 GDPR과 AI 법안의 적용 범위와 관련해서도 중복되는 내용을 발생시킨다.

개인정보보호와 관련하여 AI 법안과 중복 및 충돌이 예상되는 GDPR의 구체적인 내용으로 제22조와 제25조 및 제35조를 들 수 있으나 그 중에서도 GDPR 제35조에 따른 정보보호 영향평가제도(Data Protection Impact Assessment)와의 중복 적용 문제는 아직 이에 관한 규율을 정하지 못하고 있는 우리나라의 입장에서는 중요한 참고사항이 될 것으로 보인다. 또한 그 구체적인 내용은

유럽과의 주요 교역 상대국인 우리나라 산업계에도 큰 영향을 끼칠 것으로 예상된다.

2. GDPR 제35조와 AI 법안 내용과의 충돌

1) GDPR 제35조의 정보보호 영향평가(Data Protection Impact Assessment)

GDPR은 제35조에서 특히 새로운 기술을 사용하는 처리에 있어 자연인의 권리와 자유에 대한 높은 위험을 초래할 가능성이 있는 경우에 한해 정보보호 영향평가(Data Protection Impact Assessment)를 거치도록 명시하고 있다(GDPR 제35조 제1항)[22].

AI 법안과 마찬가지로 이러한 부분은 EU GDPR의 방식 또한 정보처리자의 의무를 데이터 처리와 관련된 위험 노출과의 연관성을 근거로 데이터 보호에 대한 위험 기반 접근 방식을 강화하고 있는 것으로 해석할 수 있다. 즉 GDPR의 제35조 제1항은 처리 작업이'중대한 위험'을 초래할 가능성이 있는 경우에만 개인정보보호 영향평가 요구사항을 적용하도록 정하고 있으므로 그 위험의 정도에 대한 고려가 필요하다고 해석된다.

2) 정보보호 영향평가의 요건과 구체적 방식

GDPR은 정보보호 영향평가와 관련하여 당해 정보처리자에게 당해 데이터 처리에 대한 예비 평가를 수행하도록 정하고 있으며 이를 위해 GDPR 제35조 제3항[23]은 그 구체적인 조건들을 명시하고 있다. 구체적으로, 우선, 자동화된

---

22) Article 35 Data protection impact assessment 1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

23) Article 35 Data protection impact assessment 3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

처리를 통해서 개인에 관한 프라이버시 측면을 체계적이고 광범위하게 평가하는 시스템으로 당해 평가를 통한 결정 내용이 특정 개인에게 법적 효력을 미치게 하거나 이와 유사하게 개인에게 중대한 영향을 미치는 경우를 들 수 있으며 둘째로, 제9조 제1항에 규정된 특별 범주의 개인정보 즉 인종 또는 민족, 정치적 견해, 종교적 또는 철학적 신념, 노동조합의 가입여부를 나타내는 개인정보의 처리와 유전자 정보, 자연인을 고유하게 식별할 목적의 생체정보, 건강정보, 성생활 또는 성적 취향에 관한 정보에 대한 대규모 처리나 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보에 대한 처리의 경우를 들 수 있다. 그리고 셋째로, 공개적으로 접근 가능한 장소에 대한 대규모의 체계적 모니터링의 경우를 들 수 있다.

그러나 이러한 규정상의 내용들이 모든 경우를 포섭할 수 없어 GDPR은 감독 당국을 통해 개인정보보호 영향평가가 필요한 처리 작업 목록(Blacklist)과 이러한 요구 사항에서 면제되는 작업(Whitelist)을 구분하여 미리 공표할 수 있도록 하고 있다. 구체적으로, GDPR은 감독 당국이 정보보호 영향평가의 요건이 적용되는 처리 작업의 종류의 목록을 작성 및 공개하도록 정하고 있으며 감독기관은 제68조에 규정된 유럽 데이터보호 이사회에 해당 목록을 통보하도록 정하고 있다(GDPR 제56조 제4항)[24]. 이에 더하여 GDPR은 감독 당국에게 개인정보보호 영향평가가 요구되지 않는 처리 작업의 종류의 목록 또한 작성하여 공개할 수 있으며 이러한 경우 감독기관은 유럽 데이터보호 이사회에 해당 목록을 통보토록 정하고 있어(GDPR 제56조 제5항) 결과적으로 허용되지 않는 작업 목록(Blacklist)의 경우와 달리 허용된 작업 목록(Whitelist)에 있어서는 그 목록 작성과 공개를 강제하지 않는 태도를 보여준다.

3) GDPR에 따라 평가가 면제되는 작업 목록

허용된 작업 목록(Whitelist)은 허용되지 않는 작업 목록(Blacklist)과 달리 강제적인 성격을 가진 것은 아니지만 특정 작업 처리의 위험성의 정도 그 중에서도 고위험에 해당하는지의 여부는 예비 평가시 발생할 수 있는 소모적인 과정을 피할 수 있게 해준다는 측면에서 중요성을 가진다.

(c) a systematic monitoring of a publicly accessible area on a large scale.

24) Article 35 Data protection impact assessment 4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

이와 별도로 GDPR 제35조 제10항은 데이터 처리가 개인정보보호 영향평가에서 면제될 가능성이 있는지 여부를 평가할 때도 필수적인 조건이 된다. 구체적으로, 유럽연합 또는 회원국 법률 내에 법적 근거를 두고 제6조(1)의 (c)호 또는 (e)호에 따른 처리 즉 정보처리자의 법적 의무를 준수하기 위해 개인정보 처리가 필요한 경우 혹은 공익을 위하거나 정보처리자의 법적 권한을 행사하여 이루어지는 업무 수행에 필요하여 이루어진 처리의 경우에는 당해 법률이 특정 처리 작업이나 일련의 관련 작업을 규제하고 개인정보보호 영향평가가 이미 그 법적 근거를 통해 일반적 영향평가의 일환으로 시행된 경우에는 당해 작업 처리에 관해서는 제1항에서 제7항까지의 내용은 적용되지 않도록 예외를 두고 있으면서도 다른 한편으로는 이러한 예외 규정에도 불구하고 그 판단은 회원국에 일임하는 태도를 취하고 있다(GDPR 제35조 제10항)[25].

이러한 배경에서 결국 회원국의 필요성에 따라 일정한 요건 하에 개인정보보호 영향평가를 생략할 수 있도록 정하고 있으나 일반적으로는 특정 정보 처리 작업이 허용된 작업 목록(Whitelist)에 속하는지 아니면 허용되지 않는 작업 목록(Blacklist)에 속하는지 명확하지 않은 경우가 대부분일 것이므로 개인정보보호 영향평가를 수행하게 될 것으로 보여진다.

이에 관해 제29조 정보 보호 작업반(ARTICLE 29 DATA PROTECTION WORKING PARTY)의 의견서에는 GDPR 제35조 제3항 적용을 위한 상세한 기준을 제시하고 있으며 구체적으로 ①'개인 정보 프로파일의 생성 또는 이용을 위한 업무 성과, 경제 상황, 건강, 개인적 선호도 또는 관심, 신뢰성 또는 행동, 위치 또는 이동 등과 관련된 측면'에 대한 프로파일링 및 예측을 통한 평가 ② 법적 영향 또는 이와 유사한 상당한 영향을 미치는 자동화된 결정 ③ 네트워크를 통해 수집된 정보와 같은 공개된 접근 가능 지역에서의 체계적인 감시 ④ 일상기록 애플리케이션과 같은 민감한 개인적인 정보 ⑤ 정보 주체의 숫자, 처리되는 정보의 양, 정보 처리 활동의 지리적 범위 등으로 특정되는 대량 처리되는 정보 ⑥ 합리적인 목적을 넘어선 방식으로 서로 다른 목적을 위해 수행된 두 가지 이상의 정보 처리 작업을 통한 정보의 조합 ⑦ 정보 주체

25) 10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

와 정보 관리자 사이에서 확대된 힘의 불균형에 기인한 취약한 정보 주체와 관련된 정보 ⑧ 지문 인식과 안면 인식을 결합한 방식과 같은 새로운 기술적 또는 조직적 솔루션의 혁신적인 적용 ⑨ 은행이 대출 제공 여부를 위해 신용 조회를 하는 것과 같이 정보 처리 자체가 정보 주체의 서비스 이용을 막는 결과를 가져오는 경우를 예로 들 고 있다.

그리고 이러한 전제에서 당해 권고안은 대부분의 경우 두 가지 기준에 해당하는 정보 처리 작업에 관해서 정보처리자에게 정보보호 영향평가를 수행하도록 제안하고 있으며 특히 해당되는 기준이 많을수록 강제될 가능성도 높은 것으로 간주하여야 한다고 제안하고 있다.[26] 또한 이러한 경우 감독 기관에게도 GDPR 제35조 제4항의 의무 즉 목록 공개의무와 이사회 통지의무를 다시 환기시키고 있다.

그러나 GDPR과 당해 권고안에 있어서도 나타나는 추상적인 표현들 특히 그 중에서도'고위험'과 같은 불명확한 개념은 결국 특정 작업목록의 성격을 판단할 감독기관의 권한에 의존하게 될 것으로 보인다. 왜냐하면 이는 결국 자율규제 방법을 일정 부분 채용하더라도 감독 기관에게 그 최종 판단을 맡기겠다는 의미로 해석 될 수 있기 때문이며 이러한 이유에서 이미 몇몇 국가들[27]은 해당목록을 미리 공표하고 있어 앞으로는 그 수가 더욱 늘어날 것으로 보인다.

3. 고위험 인공지능 시스템에 있어서의 문제점

AI 법안과 GDPR은 고위험을 보유한 시스템 혹은 정보 처리 작업에 있어적합성 평가(Conformity Assessment) 절차와 정보보호 영향평가(Data Protection Impact Assessment) 절차를 각각 수행하도록 되어있으나 양 평가 방식의 적용에 있어서는 분명히 차이가 존재한다. 즉 정보보호 영향평가(Data Protection Impact Assessment)의 경우에는'자연인의 권리와 자유에 미치는 위험'을 그 적용 대상으로 고려하게 되나 이에 반해 적합성 평가(Conformity Assessment)의 과정은'고위험 시스템에 부과된 특정 요건 충족 여부'를 평가한다는 측면에

---

26) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017 As last Revised and Adopted on 4 October 201, pp. 8-11.

27) 2019년까지 업데이트 된 내용에 의하면, 오스트리아, 벨기에, 불가리아, 크로아티아, 체코, 프랑스, 독일, 핀란드 등 EU 회원국 36개국이 블랙리스트 혹은 화이트리스트를 전부 혹은 일부를 이미 공표하였다: https://iapp.org/resources/article/eu-member-state-dpia-hitelists-and- lacklists/ (22.12.30.방문)

서 차별된다.

이러한 차이에도 불구하고, 양자의 구체적인 내용을 자세히 검토하면, AI 법안의 고위험 시스템에 대한 요구사항의 상당부분이 GDPR의 합법성, 공정성, 목적 제한 및 정확성이라는 원칙들과 유사한 특징을 띠고 있음을 발견하게 된다. 즉 높은 위험(High Risk)을 가진 인공지능 시스템에 대한 AI 법안상의 규제 요건들이 개인정보 처리와 관련해서는 사실상 GDPR상의 요건들과 중복되며 이러한 경우 원칙적으로 양자 모두 적용되어야 한다.

정보보호 영향평가(Data Protection Impact Assessment)는 기술한 바와 같이 GDPR에 따른 법적 의무로서 정보처리 작업을 담당하는 주체가 개인 데이터 보호에 미치는 영향에 대한 검증을 거치는 절차이며 특히 당해 정보처리 작업이 개인의 권리와 자유에 높은 위험을 초래할 가능성이 있는 경우 이를 사전에 방지하기 위한 제도이다.

이러한 GDPR에 따른 정보처리자는 데이터 처리 작업의 목적과 수단을 결정 내리는 자로서 법률을 준수하고 특히 필요한 경우 정보보호 영향평가(Data Protection Impact Assessment)를 수행할 책임을 부담하지만 AI 법안상의 적합성 평가(Conformity Assessment)의 경우 주로 높은 위험(High Risk)을 가진 인공지능 시스템의 공급자(제조업자, 유통업자 혹은 수입업자)에 의해서 수행된다.

특정인이 개인정보를 처리하는 인공지능 시스템과 관련하여 AI 법안상의 '공급자'이자 동시에 GDPR상의 '정보처리자'의 지위를 가지는 경우에는 두 가지 절차 즉 AI 법안상의 적합성 평가(Conformity Assessment)와 GDPR상의 정보보호 영향평가(Data Protection Impact Assessment)를 모두 수행해야 한다. 그러나 실제로는 AI 법안상의 '사용자'가 이러한 GDPR의 정보처리자의 지위를 가지는 경우가 빈번할 것이며 이러한 경우 당해 사용자에게 모든 책임이 전가될 것이다. 이러한 상황은 AI 시스템 '공급자'가 수행하는 적합성 평가(Conformity Assessment)의 과정을 통해서 당해 '사용자'가 GDPR 상의 정보보호 영향평가(Data Protection Impact Assessment)의 결과에 따라 어떤 조치를 취해야 하는 지를 명백히 제시하게 될 것이다. 또한 시스템의 초기에 적합성 평가(Conformity Assessment)를 수행해야 하는'공급자'의 지위를 고려한다면 이들이 비록 특정 시스템에 있어 GDPR에 따른 '정보처리자'의 지위를 가지지 않더라도 이들에게도 일정 부분 책임을 전가할 필요가 있다고 보여진다.[28]

---

28) EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence

특히 정보보호 영향평가(Data Protection Impact Assessment)의 과정에 앞서 행해지는 '예비 평가(사전 적합성 평가)'의 과정에는 허용된 작업 목록(Whitelist)과 허용되지 않는 작업 목록(Blacklist)이 이용된다. 특히 이러한 목록에는'프로파일링 및 행동 분석을 포함한 평가' 또는 '자동화된 의사결정을 포함하거나 이러한 의사 결정에 크게 기여하는 처리'와 같은 인공지능 시스템과 관련된 처지 작업이 포함될 수 있다. 이러한 과정에서 당해 목록이 높은 위험도(High Risk)를 지닌 것으로 판단되면 AI 법안상의 적합성 평가(Conformity Assessment)를 수행하게 되나 불필요한 중복 작업이나 모순된 결과를 피하기 위한 방안이 필요할 것이다.

V. 우리나라의 데이터 관련 법제 현황

1. 데이터 기본법의 제정과 문제점

이미 데이터를 기반으로한 거대 온라인 플랫폼 기업의 발전과 경쟁을 통해 일상 생활이 큰 영향을 받고 있지만 우리나라의 경우 공공데이터에 대한 여러 규제들과 달리 민간 데이터의 경우 법적 근거가 제대로 마련되어 있지 않은 상황이다.[29] 이러한 상황은 특히 기업의 입장에서는 데이터 활용의 측면에서 제약이 많아 산업 전반의 효율성의 측면에서 큰 어려움이 예상되어 이러한 상황을 타개할 입법적 장치의 필요성이 제기된다.

우리나라의 경우 2020년 12월 조승래 의원이 대표 발의한 '데이터 산업진흥 및 이용촉진에 관한 기본법(이하 데이터산업진흥법)'이 2021년 9월 국회 본회의에서 의결ㆍ통과 되었으며 그 이 후 동법 시행령과 시행규칙이 제정되어 2022년 4월 20일부터 시행되었다. 당해 법률은 총8장 48개 조문으로 구성되어 있으며 특히 그 주된 내용이 데이터산업을 위한 국가의 기본계획 수립과 관련된 내용과 데이터 산업의 촉진을 위한 기반 조성과 분쟁조정 등을 규정하고 있어 사실상 데이터산업 진흥법으로서의 지위를 가지고 있다.

그러나 동 법은 다른 법률들과의 관계에 관하여 정하고 있으며 이에 따라 데이터 생산, 거래 및 활용 촉진에 관하여 다른 법률에 특별한 규정이 있는 경

(Artificial Intelligence Act) 18 June 2021, p. 19.

29) 인하대학교 법학연구소 AIㆍ데이터법 센터, 「데이터법」, 2022. 8., 세창출판사, 424면.

우에는 해당 법률이 적용되며 또한 개인정보, 저작권 및 공공데이터에 관해서도 각 개별법률인‘개인정보 보호법’,‘저작권법’,‘공공데이터의 제공 및 이용 활성화에 관한 법률’이 적용됨을 규정하고 있다(데이터산업진흥법 제7조).

이러한 배경에서 데이터 보호와 관련한 내용은 이미 시행되고 있는 데이터 3법(「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」)을 통해 규율되고 있으며 그 중에서도 개인정보보호법이 중요한 법원으로 역할을 담당한다.

2. 국내법상 정보보호평가와 인공지능의 문제

개인정보보호와 관련하여 국내법도 개인정보 영향평가를 수행하도록 정해져 있으며 이는 공공기관의 개인정보 침해 예방을 위해 마련되어 있는 것이나(개인정보 보호법 제33조 제1항)[30] 개인정보 침해사고를 미연에 방지하려는 민간 또한 이를 수행할 수 있다. 만일 개인정보 침해가 발생한 경우 이러한 절차를 거쳤다는 사실은 법정에서 책임 입증을 위해서 활용될 수 있으며[31] 고유식별정보의 내부망 암호화 예외 처리 등의 상황에 맞는 유연한 취급이 가능해진다.

특히 최근인 2023년 3월 14일‘개인정보 보호법’제2차 전면 개정안이 국회를 통과하였으며 그 대표적인 내용으로 자동화된 의사결정에 대한 대응권 도입과 개인정보 국외이전 요건 다양화를 들 수 있다. 그 중에서 자동화된 의사결정에 대한 배제 등의 권리 도입을 시도하려는 구체적인 의미는 정보주체에게 법적 효력이 미치거나, 생명ㆍ신체 ㆍ정신ㆍ재산에 중대한 영향을 미치는 경우, 정보주체가 해당 의사결정에 대한 거부, 이의제기, 설명 요구를 할 수 있는 권리를 신설함과 동시에 이러한 경우 개인정보처리자에게 당해 의사결정을 배제하거나 재처리하거나 설명을 해야 할 의무를 부담시키는 것을 의미한다[32].

---

30) 제33조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 “영향평가”라 한다)를 하고 그 결과를 보호위원회에 제출하여야 한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4., 2023. 3. 14.>

31) 이는 개인정보 보호법 제74조에서 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리 하지 않았음을 입증하는 경우 면책되도록 정하고 있기 때문이다.

32) 제37조의2(자동화된 결정에 대한 정보주체의 권리 등) ① 정보주체는 완전히 자동화된 시스템(인공지능 기술을 적용한 시스템을 포함한다)으로 개인정보를 처리하여 이루어지는 결정(「행정기본법」 제20조에 따른 행정청의 자동적 처분은 제외하며, 이하 이 조에서 “자

3. 인공지능 관련 입법 현황

우리나라에서 인공지능을 규율하는 태도는 자율주행자동차나 드론과 같은 특정 상품을 전문적으로 다루는 방식과 인공지능 정책을 다루는 방식으로 크게 나눌 수 있으며 특히 전자의 경우로 2019. 4. 30. 제정된 「자율주행자동차 상용화 촉진 및 지원에 관한 법률」과 「드론 활용의 촉진 및 기반조성에 관한 법률」을 예로 들 수 있다. 이를 제외한 인공지능 산업 정책과 관련한 직접적인 입법[33]은 이루지지 못한 상황이며 이러한 입법안들의 내용 또한 개인정보 보호법과의 관련성 그것도 특히 자율적인 평가와 관련한 내용을 포함하지 못하고 있는 것으로 보인다.[34]

이와 관련하여 2023년 2월 14일 지난달 14일 국회 과학기술정보방송통신위원회(과방위)의 법안소위에서 통과된 '인공지능산업 육성 및 신뢰 기반 조성에 관한 법률안'은 국회 과방위에 발의된 7개의 인공지능 관련 법안을 통합한 법안이다. 특히 당해 법안은 인공지능의 육성을 목표로 하면서도 그 과정에서의 윤리적 원칙 등을 규정해 인공지능을 신뢰할 수 있는 기반을 마련하려는 목적으로 가지고 있는 것으로 알려져 있으며 그 구체적인 내용은 2021년 발의된 '알고리즘 및 인공지능 법률안'내용이 반영되어 기술발전을 위해 우선 허용, 사

동화된 결정"이라 한다)이 자신의 권리 또는 의무에 중대한 영향을 미치는 경우에는 해당 개인정보처리자에 대하여 해당 결정을 거부할 수 있는 권리를 가진다. 다만, 자동화된 결정이 제15조제1항제1호ㆍ제2호 및 제4호에 따라 이루어지는 경우에는 그러하지 아니하다.
② 정보주체는 개인정보처리자가 자동화된 결정을 한 경우에는 그 결정에 대하여 설명 등을 요구할 수 있다.
③ 개인정보처리자는 제1항 또는 제2항에 따라 정보주체가 자동화된 결정을 거부하거나 이에 대한 설명 등을 요구한 경우에는 정당한 사유가 없는 한 자동화된 결정을 적용하지 아니하거나 인적 개입에 의한 재처리ㆍ설명 등 필요한 조치를 하여야 한다.
④ 개인정보처리자는 자동화된 결정의 기준과 절차, 개인정보가 처리되는 방식 등을 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.
⑤ 제1항부터 제4항까지에서 규정한 사항 외에 자동화된 결정의 거부ㆍ설명 등을 요구하는 절차 및 방법, 거부ㆍ설명 등의 요구에 따른 필요한 조치, 자동화된 결정의 기준ㆍ절차 및 개인정보가 처리되는 방식의 공개 등에 필요한 사항은 대통령령으로 정한다.
[본조신설 2023. 3. 14.] [시행일: 2024. 3. 15.] 제37조의2

33) 인공지능교육진흥법안(조해진 의원 등 12인 2022. 8. 24.), 알고리즘 및 인공지능에 관한 법률안(윤영찬 의원 등 12인 2021. 11. 24.), 인공지능에 관한 법률안(이용빈 의원 등 31인 2021. 7. 19.) 인공지능 육성 및 신뢰 기반 조성 등에 관한 법률안(정필모 의원 등 23인 2021. 7. 1) 외 5건의 의원안이 현재 국회에 계류 중이다.

34) 자동화된 결정에 대한 정보주체의 권리에 관해 새롭게 신설한 내용이 정부에 의해 2021년 9월 개인정보 보호법 일부개정법률안으로 발의된 바 있으나 이는 자율 평가 방식과는 결이 다른 내용이다.

후규제 원칙을 따르며 인간의 생명과 안전과 직결된 부분을‘고위험 영역 인공지능’으로 정하여 사용 사실 고지의무와 설명 의무 등을 정하고 있다.[35]

그러나 당해 법안이 표명하는 선 허용과 후 규제의 원칙에 대한 위험성에 대한 비판이 제기되고 있으며 특히 인권과 관련한 유럽 AI 법안에 관한 비판과 마찬가지로 다양한 논쟁을 불러일으킬 것으로 예상되어 실제 입법화 과정에는 난항이 예상된다. 이에 더하여 무엇보다도 당해 법안 또한 정보처리과정에서의 개인정보보호의 문제를 주의 깊게 다루고 있지 않아 향후 개인정보보호법과의 중복 적용 여부가 문제가 될 것으로 보인다.

Ⅵ. EU의 인공지능 시스템 데이터 위험관리 체계와 우리 법제에의 시사점(결론)

EU AI 법안이 위험 수준에 맞춰 허용 요건과 규제 방식을 달리하는 방식을 택하고 있어 합리적인 규제라는 평가도 있는 반면에 아직 세상에 출시되지도 않은 인공지능 시스템을 사전에 규율하려는 태도 그리고 모호하고 추상적인 개념들을 이유로 많은 우려를 낳고 있는 것도 사실이다. 특히 특정 인공지능 시스템과 결합된 개별 제품들을 고려치 않는 규제 방식, 규제 담당 기관에 따른 결정에 의존해 기술중립적이지 못하다는 점 그리고 복잡하고 높은 수준의 기술의 결과를 설명하고 위험성을 평가 받아야 한다는 부분들은 결과적으로 산업 시장진입장벽으로 작용을 할 가능성이 높다.

특히 기술한 바와 같이 EU AI 법안이 일정부분 GDPR과 중복되는 지점에서(특히 고위험 인공지능 시스템과 관련하여) 각 법률에 따른 평가 즉 적합성 평가(Conformity Assessment)와 정보보호 영향평가(Data Protection Impact Assessment)를 모두 수행해야 할 가능성이 있다는 점은 불필요한 규제의 중복으로 결과적으로 산업발전을 저해할 가능성이 높아 보인다.

당해 법안이 우리에게 중요한 이유 중 하나는 바로 우리 산업계의 세계화의 흐름과 밀접한 관련이 있기 때문이다. 즉 인공지능 시스템에 대한 우리 나라의 규제 방식 또한 영토 기반의 접근방식에서 벗어나 세계적 흐름을 적절히 반영해야 하며 FTA 등을 통해 산업적으로 계속 접촉하게 되는 EU와의 인공지능 시스템 산업 기준들과의 정합성 문제는 우리에 있어서도 중요한 문제가 될 것

35) https://www.ekoreanews.co.kr/news/articleView.html?idxno=65909(23. 3. 29. 방문)

이다.

이러한 관점에서 EU AI 법안이 유럽 연합이 계약을 체결한, 제3국의 법률에 따라 설립된 적합성 평가 기관은 본 규정에 따른 인증기관의 활동을 수행할 권한을 부여받을 수 있다(제39조)고 규정하고 있는 점 그리고 이와 병행하여 EU GDPR이 의도한 데이터 처리에 대한 예비 평가를 위하여 현실적인 이유에서 감독 당국이 정보보호 영향평가(Data Protection Impact Assessment)가 필요한 처리 작업 목록(블랙리스트)과 이러한 요구 사항에서 면제되는 작업(화이트리스트)을 미리 게시할 수 있도록 정하고 있는 점(GDPR 제35조 제4항 및 제5항 참조)은 우리에게도 시사하는 바가 크다. 왜냐하면, 국외가 아닌 국내 인정기관이나 우리나라 정부에 의한 평가의 범위가 넓어질수록 경제적인 이득을 차치하고서라도 산업 비밀의 해외 유출 가능성을 줄일 수 있는 등의 여러 가지 산업 정책적 장점을 얻을 수 있기 때문이다. 또한 현재 제출된 AI 법안에 관하여 EU 공동 입법자인 유럽 의회와 EU 이사회를 통한 검토가 진행 중으로 알려져 있으며 이미 잘 정립된 적합성 평가(Conformity Assessment)의 틀을 깨진 않는 선에서 상대적으로 더 전문성을 갖춘 인공지능 시스템 공급자에 의한 자율적인 방식으로 평가의 방식이 발전해 나갈 것으로 기대된다.

우리나라의 경우에도 EU의 AI 법안과 유사한 '인공지능산업 육성 및 신뢰기반 조성에 관한 법률안'이 최근인 2023년 2월 14일에 국회 과학기술정보방송통신위원회(과방위)의 법안소위를 통과하였으며 당해 법안은 국회 과방위에 발의된 7개의 인공지능 관련 법안을 통합한 법안으로 인공지능의 육성과 규율을 다루고 있다. 그러나 당해 법안은 산업적 활용도 개선에 중점을 두고 있어 인공지능을 통해 야기될 수 있는 여러 문제들 특히 그 중에서도 데이터 오용의 위험성에 큰 관심을 두고 있지 않으며 이러한 와중에 최근 우리 개인정보보호법 개정 내용이 자동화된 의사결정과 같은 상황에 관해 새로운 내용을 규정하고 있어 향후 입법화된다면 충돌되는 부분이 발생할 것이 예상되는 상황에서도 이에 대한 논의는 여전히 부족한 것으로 보인다.

현재의 입법 방향에서 좀더 고려해야 할 부분이 있다면, 산업 정책적인 측면에서 AI 시스템에 대한 엄격한 규제의 틀을 마련하는 방식은 오히려 경쟁력의 측면에서 우리에게 불리할 수도 있다는 점이 충분히 고려되어야 한다는 점이다. 그래서 오히려 인터넷을 통해 국경을 넘나들면서 작업을 수행하는 인공지능의 작동 메커니즘의 특성상 규율의 방식 또한 산업정책적인 관점에서 비관료적이고 혁신 친화적인 방식의 적절한 수준을 유지하여야 할 것이며 그 구체적인 방식으로 KC 인증 시스템과 같이 이미 산업계에서 널리 사용되어 온

기존의 평가 방식들을 활용한 AI 시스템 규제 방식을 포함하여 글로벌화된 규제 방식과의 정합성을 고려한 비규제적이며 유연한 방식을 고민해 볼 필요가 있을 것이다.

EU GDPR의 개인정보 영향평가 제도와 AI 법안에 따른 인공지능에 대한 적합성 평가가 사실상 같은 내용으로 구성되어 있다는 점은 EU와 빈번한 무역을 하고 있는 우리 산업계의 입장에서도 데이터 산업의 진흥을 위해서도 개인정보 예비평가제도와 기존의 산업 인증제도를 통한 EU의 기준과의 정합성을 개선시키는 방식을 현실적인 방안으로 고려할 수 있을 것이다.

이에 더하여 EU AI 법안이 만들어져 온 과정에서 볼 수 있듯이 정보를 공개하며 설문 조사 등을 통해 산업계와 일반 시민들을 대상으로 소통을 계속 시도해 온 점은 현재 여러 가지 입법 방향을 모색하고 있는 우리에게 시사하는 바가 적지 않다고 생각된다.

[참고문헌]

김진우, 유럽연합 인공지능법안에 따른 고위험 인공지능 시스템 공급자 등의 의무, 과학기술과 법 제12권 제2호(2021. 12.)

고학수 · 임용 · 박상철, 유럽연합 인공지능법안의 개요 및 대응방안, DAIG 2021년 제2호

박노형 외 8인 저, EU 개인정보보호법 - GDPR을 중심으로 - , 박영사, 2017.

박혜성 · 김법연 · 권헌영, 인공지능 규제에 관한 연구 - 유럽연합의 입법안을 중심으로-, 사단법인 한국공법학회공법연구 제49집 제3호 2021년 2월

이경선, EU 인공지능 규제안의 주요 내용과 시사점, 정보통신정책연구원, 2021. 05, No. 1

인하대학교 법학연구소 AI · 데이터법 센터,「데이터법」, 2022. 8., 세창출판사

정소영, 유럽연합 인공지능법안의 거버넌스 분석 - 유럽인공지능위원회와 회원국 감독기관의 역할과 기능을 중심으로 -, 연세법학 제39호(2022. 7)

COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the Proposal for a Regulation of the European Parliament and of the Council LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS {COM(2021) 206 final} - {SEC(2021) 167 final} - {SWD(2021) 85 final}

Council of the European Union, Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change, 11481/20, 2020

EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence(Artificial Intelligence Act) 18 June 2021

European Commission, WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust, European Commission, 2020

EUROPEAN COMMISSION (2021.4.21), Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN

UNION LEGISLATIVE ACTS
HLEG, Ethics Guidelines for Trustworthy AI, 2019
HLEG, The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment, 2020

[Abstract]

Data Risk Management on EU AI Regulation*
- Issue with GDPR Art. 35 -

Changbae Seo**

Since changes in community approach due to the use of artificial intelligence, study on AI-System Regulations affecting community are from now on being held. And more while these AI-System Regulation are now seen as some guidelines, which are not forcely, will have no meaning.

In this circumstance, EU has announcen a unique ominus Regulation Plan in 2021. The EU AI Act, which was introduced by the European Commission in April 2021, is still being on a held about a year. At this time when both expections and tensions broght about by GDPR habe become musch moderated, there is an atmosphere of waiting and seeing to what extent the EU's attempt to be a rule-maker or pioneer in AI Business around the world.

For AI Act has the European Commission adopted many articles that resemble GDPR. On the other hand, both Regulation can be used separatelly on some points with simmilar way.

In our case, the 'Artificial Intelligence Industry Fostering and Trust Foundation', similar to the EU's AI bill, has recently passed the subcommittee of the National Assembly's Science and Technology Information Broadcasting and Communications Committee (overdefense), and the bill has been passed by the National Assembly overdefence. However, the bill does not pay much attention to the risk of misuse of data, and in the midst of this, the recent revision of our Personal Information Protection Act stipulates new content regarding situations such as automated decision-making, so the direction of more flexible legislation in the future legislative process. At the same time, it seems necessary to discuss this.

---

* This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea(NRF-2021S1A5C2A02089229)

** Researcher of Institute for North-East Asian Law, Dr. jur.

Keywords : EU AI Regulation, EU GDPR, GDPR Art. 35,
Data Protection Impact Assessment, Conformity Assessment