경북대학교 법학연구원『법학논고』
제85집 (2024.04) 57~82면.
Kyungpook Natl. Univ. Law Journal
Vol.85 (Apr 2024) pp.57~82.
http://doi.org/10.17248/knulaw..85.202404.57

유럽 AI법에 따른 생체정보의 활용과 보호에 관한 고찰*

이 권 일**

〈국문초록〉

유럽에서는 생체인식정보 기술의 발달과 AI 기술의 발달, 그리고 이 두가지 기술이 결합되어서 나타나게 되는 기본권 침해상황을 심각하게 생각하여 이를 규제하기 위한 법제를 만들기 위해 노력해왔다. 특히 2021년 인공지능법안이 유럽연합 집행위원회에서 유럽연합 의회에 제안되었고, 3년 이상의 기간동안 이에 대해 유럽의 학계와 정치계, 시민사회와 각 회원국에서 뜨겁게 논의된 결과 지난 2024년 3월 유럽연합 의회에서 압도적 다수로 인공지능법이 통과되었고, 일부 조항은 6개월 후부터, 2026년부터는 전면 시행된다. 이는 소위 브뤼셀 효과로 인하여 GDPR과 같이 세계에 영향을 미치는 인공지능 규제법으로 기능할 것으로 보인다.

이번에 통과된 인공지능법의 가장 큰 특징 중의 하나는 AI 기술을 이용한 생체인식정보의 처리를 강하게 규제하고자 한다는 점이다. EU에서는 생체인식기술과 AI기술이 결합하였을 때 발생할 수 있는 대량감시와 추적의 가능성과 이로 인한 일반적 인격권, 사생활의 비밀, 개인정보자기결정권, 평등권 등의 기본권 침해적 상황이 심각할 수 있다는 점에 대한 분명한 인식으로 이를 강하게 규제하고자 한다. 특히 감정인식시스템, 생체 인식 분류 시스템, 실시간 원격 생체 인식 시스템, 사후 원격 생체 인식 시스템 등의 새로운 기술에 대해 개념정의를 하고자 노력하였고, 이를 바탕으로 AI 기술과 생체인식정보가 결합되어 사용되는 경우 이러한 AI 시스템의 실행을 금지하거나 고위험 AI 시스템으로 분류하여 강하게 제한하고자 한다.

앞으로 AI 기술과 생체인식기술을 더욱 발전할 것이고, 이러한 기술이 우리의 삶 속에 우리의 생활을 편리하게 하기 위하여 더 광범위하게 사용될 것이 예측된다. 또한 이러한 기술을 사용하는 시장도 엄청나게 확대될 것으로 예상되는데, 이는 AI법이 AI를 규제하기 위한 법이면서도 목적조항에 인공지능의 활용을 촉진하고 혁신을 지원하기 위한 법이라고 명문으로 규정한 것에서도 알 수 있다. 따라서 이러한 기술의 사용을 전면적으로 금지함으로서 우리의 기본권을 보장한다는 생각은 더 이상 유효할 수 없고, 이러한 기술의 사용으로 인한 부작용을 최소화하는 방안을 마련하고, 이러한 기술의 사용을 어떻게 제한하여야 할 것인지에 대한 논의를 하여야 한다. 이런 점에서 유럽의 AI법이 우리에게 주는 시사점은 분명히 있다. 이러한 기술의 사용은 더욱 확대될 것이고 확대되어야 하는데, 이러한 기술의 사용이 더 유연해질 수 있도록 법제를 개편하는 것과 아울러 개인의 기본권이 더

* 이 논문은 2023학년도 경북대학교 신임교원 정착연구비에 의하여 연구되었음.
** 경북대학교 법학전문대학원 교수

실효적으로 보장될 수 있는 조화로운 방법을 모색하여야 할 것이다.

주제어 : 인공지능법, 생체인식정보, 실시간 원격 생체 인식 시스템, 고위험 AI 시스템, 개인정보보호

• 투고일 : 2024.04.07. / 심사일 : 2024.04.23. / 게재확정일 : 2024.04.26.

Ⅰ. 들어가며

2021년 8월, 개인정보보호위원회(이하 개인정보위)는 제14회 전체회의를 개최해 이용자의 동의를 받지 않고 개인을 식별할 수 있는 안면인식 정보를 생성·이용한 페이스북에게 개인정보보호 법규 위반을 이유로 64억 4천만원의 과징금 부과 등 시정조치[1]를 의결했다.

같은 해 10월 법무부와 과학기술정보통신부에서 출입국 심사를 안면정보를 통해 할 목적으로 개발되는 인공지능을 학습시키기 위해 약 1억7천만건의 내·외국인 얼굴 사진을 민간개발업체에 넘겨 사회적 문제가 되었다.[2] 이 사건에 대해 개인정보위는 법무부가 출입국심사 고도화를 목적으로 인공지능 식별추적 시스템 개발을 위해 개인정보처리 위탁계약을 인공지능 개발업체와 체결한 것과 관련하여 업무상 처리범위에 포함되나 「개인정보 보호법(이하 개인정보보호법)」 제26조의 '개인정보 처리위탁'에 해당하므로 법무부가 위탁계약을 체결하면서 위탁사실과 수탁자를 홈페이지에 공개하지 않은 것은 개인정보보호법 제26조 제2항 위반되므로 이를 이유로 과태료 100만원을 부과하는 결정을 하였다.[3] 2023년 이 기술이 개발·적용되어 인천공항에서 7월 28일부터

---

1) 페이스북은 2018년 4월부터 2019년 9월까지 약 1년 5개월간 이용자의 동의 없이 얼굴인식 서식(템플릿)을 생성·수집하였으며, 이러한 위반행위에 대해 64억 4천만원의 과징금을 부과하였다. 동의 없는 얼굴정보 수집 등 위반 사항에 대해 시정명령을 내리고, 개인정보 추가 수집 시 법정 고지사항이 불명확하여 개인정보 처리실태가 미흡한 점은 개선하도록 권고하였다. (안건번호 제2020-007-008)

2) [단독] 정부, 출입국 얼굴사진 1억7천만건 AI업체에 넘겼다, 한겨레신문, 2021.10.21., https://www.hani.co.kr/arti/economy/it/1016022.html

3) 법무부가 출입국 심사과정에서 확보한 내·외국인의 얼굴 이미지 등의 정보를 과학기술정보통신부에 이관하고 과기부는 「인공지능 식별추적 시스템 구축 사업」을 위한 연구 목적으로 이러한 이미지 정보를 민간업체에 제공한 것으로 이에 개인정보위가 내·외국인 얼굴 사진 등을 이용한 인공지능 식별추적 시스템 구축 사업 관련 자료를 법무부·과학기술정보통신부에 요구하며 적법성 검토를 실시하였다. 또한 정보주체의 동의 없는 이용 및 제공으로 인권침해라며 대한변협과 시민단체가 성명서를 통해 날카롭게 비판하였으며, 2022년

여권과 항공권 제시없이 안면인식을 통해 출국할 수 있는 스마트패스 서비스가 개시되었다. 본인의 안면인식정보를 미리 등록하면 출국 시 얼굴을 인식하는 것만으로도 출국할 수 있게 된 것이다.

2022년 국가인권위원회는 국공립 어린이집 직원들의 출퇴근 시 안면인식기를 이용한 근태관리에 대해 그 외의 대체수단을 마련하지 않아 국공립 어린이집 교사들의 개인정보자기결정권을 과도하게 침해하는 것이라고 판단한 바 있다. 인권위원회는 안면인식 정보는 식별 가능한 개인정보에 해당하며, 살아 있는 동안 그 사람과 결합되어 있고, 이름이나 주소, 식별번호, 암호 등의 여타 개인정보와 달리 변경할 수 없는 생체정보로서, 신체 그 자체로부터 획득할 수 있는 강한 일신전속성을 가지는 유일식별자로, 이는 언제든 축적이 가능하고 데이터베이스 연결의 고리로 기능할 수 있으므로, 축적된 정보가 부당하게 활용되거나 유출될 경우 정보주체에게 미칠 수 있는 피해의 위험성이 결코 작지 않다고 판단하였다.[4)]

실제로 우리는 매일매일 스마트폰을 켜거나 노트북을 켤 때, 은행업무를 스마트폰으로 처리할 때 등 일상생활 속에서 본인의 지문이나 얼굴정보를 이용하는 편리함을 누리고 있다. 특히 모바일 기기 활용 증가와 생체정보를 활용한 개인식별의 편의성과 보안성 등 그 장점을 바탕으로 공공과 민간의 여러 영역에서 활용되어 왔고 최근 들어 기술이 발전하면서 다른 기술과 결합하여 그 활용영역이 더욱 확대되고 있다. 앞으로 이런 현상은 가속화될 것으로 예상되고, 시장의 상황분석도 글로벌 생체인식 시장이 2022년 429억 달러에서 2027년 829억 달러로 연평균 성장률이 14.1%에 달할 것으로 예상된다,[5)]

그러나 한편으로, 생체인식기술을 통한 생체인식정보의 처리는 정보주체인 개인의 사생활과 개인정보에 대한 침해가능성을 비롯하여 대량감시(mass surveillance)와 부당한 차별(discrimination)이라는 기본권 위협상황을 야기한다. 이러한 위협은 일반적인 개인정보의 처리에서 나타나는 위협과 또 다른 차이가 있다. 세계 각국은 개인의 자유와 권리가 침해될 위험성을 인식하고 생체인식기술의 광범위한 사용으로 인한 기본권 침해의 우려 상황에서 보다 강화된 보호체계를 마련하고자 노력하고 있다.

특히 생체인식기술과 AI 기술의 결합으로 이러한 위협상황은 더 심각해진

1월에는 감사원에 공익감사를 청구하기도 하였다. (안건번호2022-007-046호)

4) 국가인권위원회 2022. 9. 16. 22진정0139800

5) MarketsandMarkets, Biometric System Market, 2022. https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html

다. 이러한 상황에 대처하고자 하는 대표적인 움직임으로 EU에서의 AI법 제정을 들 수 있다. AI 법률안은 유럽집행위원회(European Commission)에서 2021년 4월 유럽이사회(European Council)와 유럽의회(European Parliament (EP))에 제출되었고 2024년 3월 14일 오랜 논의 끝에 유럽의회에서 통과되었다. EU는 인공지능기술의 발달에 따라 지능정보사회로 변화되는 과정 중에 AI기술의 활용을 촉진하고 이 기술의 특정한 사용과 관련된 위험을 관리하기 위해 이를 법제화하기 위해 노력했는데 AI 법률은 이러한 노력의 산물이라고 하겠다. 이 글은 AI법 중 AI 시스템에서 생체정보기술이 사용되는 경우 적용되는 법률의 내용을 중심으로 생체정보기술과 AI 기술의 결합으로 인해 발생하는 문제에 대한 AI법의 대응과 이러한 규정이 우리에게 주는 시사점에 대해 살펴보고자 한다.

Ⅱ. 생체정보에 대한 규율

1. 우리의 경우

인간의 신체가 가지는 유일하고 고유한 정보는 생체정보, 생체인식정보, 바이오메트릭스(Biometrics), 바이오 정보, 바이오 인식정보, 바이오메트릭 데이터(Biometric data) 등 다양한 용어가 사용되고 이에 대한 정의도 다양하다.

한국인터넷진흥원(KISA)의 2005년 '생체정보 보호 가이드라인'에서는 생체정보를 "지문 · 얼굴 · 홍채 · 정맥 · 음성 · 서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보"라고 정의하였다. 방송통신위원회가 발표한 2017년 '바이오정보 보호 가이드라인'에서는 "지문, 홍채, 음성, 필적 등 개인의 신체적 · 행동적 특성에 관한 정보로서 개인을 인증 또는 식별하기 위하여 기술적으로 처리되는 개인정보"를 바이오정보라고 정의하였다. 행정안전부는 2011년에 제정[6]하여 2021년 폐지된[7] '개인정보의 안정성 확보조치 기준'[8]에서 "바이오정보"를 "지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보"라고 정의하고 있다.

---

6) 행정안전부고시 제2011-43호
7) 행정안전부고시 제2021-72호
8) 행정안전부고시 제2019-47호.

개인정보보호위원회는 2020년 ‘개인정보의 기술적·관리적 보호조치 기준’[9]에서 “지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보”를 바이오정보라고 정의하였다가 2021년 ‘개인정보의 기술적·관리적 보호조치 기준’[10]에서 이를 수정하여 “지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보”를 생체정보로, “생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보”를 생체인식정보로 나누어 정의하였다. 개인정보보호위원회가 발간한 개인정보의 기술적 관리적 보호조치 기준 해설서에 의하면 생체정보는 신체적 특징, 생리적 특징과 행동적 특징을 기반으로 생성된 정보로 신체적 특징으로는 홍채·망막의 혈관 모양, 손바닥·손가락의 정맥 모양, 장문, 귓바퀴의 모양 등이 있고, 생리적 특징에는 뇌파, 심전도, 유전정보 등이 포함되며, 행동적 특징으로는 음성, 필적, 걸음걸이, 자판입력 간격·속도 등을 예로 들고 있다. 또한 열람·보관 등을 목적으로 수집하는 일반적인 얼굴 사진, 음성파일 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보가 ‘특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 기술적으로 처리’되지 않는다면 생체정보가 아닌 일반적인 개인정보에 해당하는 것으로 설명하고 있다.[11] ‘개인정보의 기술적·관리적 보호조치 기준’은 2023년 9월 폐지되었다.[12]

2021년 개인정보보호위원회는 ‘생체정보 보호 가이드라인’을 통해 생체정보를 조금 더 세부적으로 정의하고자 하였다. 이에 의하면 개인정보는 그 자체만으로 특정 개인을 알아볼 수 있거나 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보, 생체정보는 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보, 생체인식정보는 생체정보 중 특정 개인을 인증·식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보로 정의하고, 생체인식정보를 다시 생체인식 특징정보와 생체인식 원본

9) 개인정보보호위원회고시 제2020-5호
10) 개인정보보호위원회고시 제2021-3호
11) 개인정보의 기술적·관리적 보호조치 기준 해설서, 2022.10.
12) 개인정보보호위원회고시 제2023-7호, 「개인정보 보호법 시행령」의 제48조의2(개인정보의 안전성 확보 조치에 관한 특례)가 삭제됨에 따라 제48조의2 제3항에 따른 「(개인정보보호위원회) 개인정보의 기술적관리적 보호조치 기준」 고시를 폐지

정보로 나누어 생체인식 특징정보를 생체인식정보 중 입력장치 등을 통해 수집·입력된, 특징정보 생성에 이용되는 정보로, 생체인식 원본정보는 원본정보로부터 특징점을 추출하는 등의 일정한 기술적 수단을 통해 생성되는 정보로 보다 세밀하게 정의하고 있다.

현행 법령에서 생체정보 또는 생체인식정보를 정확하게 정의하고 있지는 않다. 개인정보보호에 대한 기본법이라고 할 수 있는 개인정보 보호법은 제23조에서 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보를 민감정보로 분류한 후, 개인정보 보호법 시행령 제18조 제3호에서 "개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보"를 민감정보의 범위에 포함하고 있다. 다만 동법 시행령 제18조 제3호는 서술적으로 민감정보를 기술만 하고 있을 뿐 이것이 생체정보인지 생체인식정보인지에 대한 용어를 사용하고 있지는 않아 생체정보에 대한 내용을 두고는 있지만 생체정보 또는 생체인식정보를 정의하고 있는 규정은 아니다.

이외 개별법에서 생체정보 또는 바이오정보를 정의하고 있는 규정이 있다. 먼저 출입국관리법 제2조 제15호는 '"생체정보"란 이 법에 따른 업무에서 본인 일치 여부 확인 등에 활용되는 사람의 지문·얼굴·홍채 및 손바닥 정맥 등의 개인정보를 말한다.'라고 규정하여 생체정보를 정의하고 있다. 항공보안법 제14조의2는 생체정보를 이용할 수 있는 규정을 두면서 따로 정의규정은 두지 않고 '관계 행정기관이 보유하고 있는 얼굴·지문·홍채 및 손바닥 정맥 등 개인을 식별할 수 있는 신체적 특징에 관한 개인정보(이하 "생체정보"라 한다)를 이용할 수 있다.'라고 하여 생체정보의 개념을 사용하고 있다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제9조의2 제1항 제1호는 '바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다.'라고 하여 바이오정보에 대한 규정을 두고 있다. 전자금융거래법 제2조 제10호 라목에서는 접근매체의 한 유형으로 "생체정보"라는 용어를 사용하고 있으나 이에 대한 정의규정은 없으며, 구 전자서명법 제2조 제13호에서 개인정보의 한 유형으로 "생체특성 등에 관한 정보"라는 개념을 사용하였으나 2020년 법을 개정하면서 이 조항이 삭제되었다.

여러 문헌에서도 생체 프라이버시[13], 생체인식기술[14]이라는 용어를 사용하

13) 이창범, 생체 프라이버시 보호원칙에 관한 연구, 인터넷법률 제31호, 2005.
14) 정연덕, 생체인식여권(bio passport)의 활용과 문제점, 인터넷법률 제24호, 2004.07.

기도 하고, 생체정보[15], 생체인식정보[16], 바이오정보[17]라는 용어를 사용하는 등 개념 정의도 다양하고 용어의 사용도 다양함을 알 수 있다.

2. EU의 경우

EU의 GDPR(유럽 개인정보보호 일반법, General Data Protection Regulation[18])의 경우 제4조 제14호에서 "biometric data"(생체인식정보)를 정의하고 있다. 이에 의하면 생체인식정보는 얼굴 사진이나 지문정보와 같이 특정 기술 처리로 얻어진 자연인의 신체적, 생리적, 행태적(physical, physiological or behavioural) 특성과 관련된 정보로서, 자연인을 고유하게 식별할 수 있도록 해주거나 확인해주는 것이라고 정의된다. GDPR은 이러한 생체인식정보를 제9조의 특정범주 개인정보(special categories of personal data)에 해당하는 것으로 규율하여 원칙적으로 이러한 정보의 처리는 금지되고 법률규정 상 예외적인 경우에만 허용되는 것으로 규율하고 있다. GDPR에서 생체인식정보에 대해 규정하는 외에 생체인식정보의 활용과 보호를 위한 다른 특별법이나 법규정을 두고 있지는 않았다.

그러다 AI 기술의 발달과 생체인식정보 기술의 발달, 이 두 기술의 결합으로 인하여 생활의 편리함과 공권력 행사에서의 편리함은 물론 이를 통한 심각한 기본권 침해문제의 발생이 우려되자 이를 규제하기 위한 논의와 노력이 수년간 있었고, 이러한 노력의 결과 EU의 인공지능(AI)법이 유럽의회를 통과하기에 이르렀다. EU의 AI법은 특별히 인공지능을 활용한 생체인식정보의 수집

---

15) 전명근, 문기영. 생체정보 이용과 프라이버시 보호. 정보보호학회지 제15권 제6호, 2005; 박정훈, 김행문, 생체정보 프라이버시의 쟁점 및 정책 시사점 - 전자여권 사례를 중심으로 -, 정보화정책 제15권 제3호, 2008, 85-86쪽; 이유미, 민수홍, 형사사법기관의 생체정보 수집에 대한 동의에 영향을 미치는 요인, 한국범죄학 제10권1호, 2016.

16) 이성기, 생체인식정보와 감시: 수사기관의 얼굴 인식기술을 활용한 신원확인 행위의 법적 근거와 한계에 관한 연구, 법과 정책연구 제18집 제1호, 2018.

17) 정승일, 바이오 정보 보호에 관한 최근 주요이슈 및 법규 개선방안. 한국기술혁신학회 학술대회, 2016. 05; 정부금, 권헌영, 박혜숙, 임종인, 바이오정보 활용 서비스 현황 및 GDPR 사례를 통한 바이오정보보호 법제 개선방안. 한국통신학회논문지, 제43호 제1권, 2018; 정일영. 혁신기술과 바이오정보의 규제 이슈 - 안면인식기술, 유전체 분석 정보, 커넥티드 카를 중심으로. 한국기술혁신학회 학술대회, 2019.11.

18) REGULATION (EU) 2016/…OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 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(General Data Protection Regulation).

과 처리의 제한, 금지를 규율하고 있다는 점이 특징이다.

AI법은 제3조 정의에서 특별히 생체인식시스템에 대하여 정의하고 있다. 제34호에서는 '생체 인식 정보(biometric data)'를 얼굴 이미지나 지문 데이터와 같이 자연인의 신체적, 생리적 또는 행동적 특징(physical, physiological or behavioural characteristics)과 관련된 특정 기술적 처리의 결과물인 개인 정보라고 정의하여 GDPR의 정의와 약간 차이를 두고 있다. 2021년 유럽집행위원회의 법제안서[19]에서는 GDPR에서의 정의와 동일하게 생체인식정보를 정의한 것에 비하여 달라진 부분인데 GDPR 규정의 후단부가 삭제되었다. 이는 뒤의 제35호와 36호에 생체인식정보의 인식과 인증을 따로 호를 달리하여 정의하기 때문인 것으로 이해된다. 제35호에서는 생체인식식별(biometric identification)에 대한 정의규정을 두고 있는데, 자연인의 신원 확인을 목적으로 해당 개인의 생체 정보와 데이터베이스에 저장된 개인의 생체 정보를 비교하여 인간의 신체적, 생리적, 행동적 또는 심리적(psychological) 특징을 자동으로 식별하는 것을 의미하는 것으로 정의하고 있다. 이는 2021년 유럽집행위원회의 법제안서에는 없던 규정으로 의회에서 논의 중 새로 추가된 규정이다. 특히 생체인식정보의 정의에는 포함되지 않았던 심리적 특징이라는 요소가 포함된 것이 특이한 점이라 하겠다. 이는 뒤에 규정되는 감정인식시스템과 연결하여 이해할 수 있을 것이다. 또한 제36호에서는 생체인증(biometric verification)에 대해 따로 정의하고 있는데, 자연인의 생체인식정보를 이전에 제공된 생체인식정보와의 비교를 통하여 신원식별 확인(authentication)을 포함하는 자동화된 일대일 인증(one-to-one verification)을 의미하는 것으로 정의하고 있다. 그리고 제38호에서는 민감한 운영 데이터(sensitive operational data)를 형사 범죄의 예방, 탐지, 수사 또는 기소 활동과 관련된 운영 데이터로서 공개될 경우 형사 절차의 무결성을 위태롭게 할 수 있는 데이터로 정의하고 있다. 이 규정도 집행위원회의 제안안에서는 없던 규정을 추가한 것으로 법집행 활동과 관련되어 사용되는 개념이다.

생체인식정보의 개념과 관련된 정의와 함께 이렇게 정의된 생체인식정보가 사용되는 각종 인공지능 시스템에 대한 정의도 그 위험성의 유형과 단계에 따라 달리 정의하고 있다. 먼저 감정 인식 시스템(emotion recognition system)

19) 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, 21.4.2021

은 생체인식정보를 기반으로 자연인의 감정이나 의도를 식별하거나 추론하기 위한 목적을 위한 인공지능 시스템을 의미하는 것으로 정의한다(제39호), 생체인식 분류 시스템(biometric categorisation system)은 제안안에서는 '자연인의 생체인식정보를 토대로 성별, 연령, 머리와 눈동자 색, 문신, 민족, 성적지향 또는 정치적 지향 등의 특정 범주에 할당(assigning)하기 위한 인공지능 시스템'이라고 정의되었으나 법에서는 '다른 상업적 서비스에 부수적이고 객관적·기술적 이유로 엄격하게 필요한 경우를 제외하고, 생체인식정보를 기반으로 자연인을 특정 범주에 할당하기 위한 목적의 인공지능 시스템'을 의미하는 것으로 수정되었다(제40호). 즉 분류를 위한 구체적 기준을 삭제하고, 분류를 함에도 불구하고 예외적으로 생체 인식 분류 시스템에 포함되지 않은 영역을 추가하였다. 원격 생체 인식 시스템(remote biometric identification system)은 일반적으로 개인의 생체인식정보와 참조 데이터베이스에 포함된 생체인식정보의 비교를 통해 원거리에서 자연인의 적극적인 개입 없이 자연인을 식별하기 위한 목적의 인공지능 시스템을 의미(제41호)하는데, 이는 실시간 인식시스템과 사후 인식시스템으로 구분된다. 실시간 원격 생체 인식 시스템(real-time remote biometric identification system)은 생체인식정보의 수집(capturing), 비교(comparison), 식별(identification)이 모두 상당한 지연 없이 이루어지는 원격 생체 인식 시스템으로, 즉각적인 식별뿐만 아니라 우회 방지를 위한 제한된 짧은 지연도 포함하는 것으로 이해된다.(제42호), 사후 원격 생체 인식 시스템(post remote biometric identification system)은 실시간 원격 생체 인식 시스템을 제외한 여타의 원격 생체 인식 시스템을 의미한다.(제43호) 인공지능법은 특히 실시간 원격 생체 인식 시스템은 금지되는 것으로, 사람의 원격 생체 인식에 사용되는 다른 모든 AI 시스템은 고위험으로 간주하여 문서화 및 설계에 따른 인적 감독 요구 사항을 포함한 사전 제삼자 적합성 평가의 대상으로 규정하고 있다. 이에 대해서는 뒤에 자세하게 설명한다.

Ⅲ. AI기술과 생체정보기술이 결합된 기술 사용의 허용여부

1. 중국의 사례

AI 기술과 생체정보기술의 결합이 가장 발전해있으며 가장 많이 활용되고

있는 중국의 경우 원래 목적인 개인을 인증하거나 식별하고자 하는 목적을 넘어 국가가 국민을 추적하고 감시하는 수단으로 사용되는 경우가 많다. 특히 경찰의 치안유지를 위한 목적으로 생체인식정보(안면인식이나 발걸음 정보 등)를 CCTV 기술에 접목하여, 국민을 감시하고 추적하며 더 나아가 사회신용시스템(CCTV 분석을 통하여 개인의 특성과 행동을 데이터화해 점수를 매기는)[20]을 위한 수단으로 이러한 기술을 활용하고 있다. 중국의 경우, 국민 안전과 치안을 위해서라는 이유로 CCTV의 설치를 늘리고 CCTV를 통한 식별기술을 개발해 왔다. 중국에 설치된 안면인식 카메라는 2017년 1억7,600만 대에서 2020년 6억2,600만 대로 단기간에 급증한 것으로 파악된다.[21] 양적인 증가뿐만이 아니라 식별기술도 정부주도로 빠르게 발전하였는데, 안면인식기술의 경우 중국은 정부의 지원과 주도에 의해 현재 거의 세계 최고수준에 이르렀다. 예를 들어 중국에서는 휴대폰을 신규 등록하면 얼굴 스캔을 의무화하게 하여 모든 국민의 안면정보를 국가가 수집하여 축적할 수 있게 하고, 이 정보를 바탕으로 생체인식정보 기술을 개발하였다.[22]

하지만 이러한 기술의 사용은 국민을 쉽게 감시할 수 있는 거대 감시국가를 탄생시켰다. 이 기술은 특히 소수민족 탄압 또는 반정부 인사를 감시하기 위한 도구로 사용되고 있다는 의혹이 있다. 신장위구르 자치구에서는 소수민족인 위구르족을 식별하는 기술을 도입하여 위구르족의 생활을 감시하는 도구로 악용되고 있다는 것이다.[23] 또한 2019년 홍콩의 민주화 시위와 관련하여 중국 당국은 복면금지법을 시행했는데, 이는 안면인식기술로 시위참가자를 식별하여 검거할 수 있음을 간접적으로 인정하는 것이라 하겠다. 복면으로 안면인식이 어려워지자 중국은 발걸음 인식기술을 개발하여 안면인식기술과 발걸음 인식기술을 결합하여 국민을 식별하고자 시도하고 있다.[24]

---

20) 이는 AI법에서 금지하는 소셜 스코어링 기술이라고 하겠다.

21) 인구 14억명 다 알아보는 중국 '안면인식 빅브러더'...정말 없앨까?, 한국일보, 2023.10.23., https://www.hankookilbo.com/News/Read/A2023101820100001841

22) 중국, 스마트폰 사용자 얼굴 정보 등록 의무화, 한겨레, 2019.12.01., http://www.hani.co.kr/arti/international/china/919120.html#csidx61d89052b5fce0eb9e4f3c684115cbc; 안면인식기술 수준은 14억 인구 중 한 사람을 식별하는데 소요되는 시간이 대략 3초, 인식 정확도는 약 99%를 웃돌아 쌍둥이도 구분할 수 있을 정도라고 한다. [지구촌 돋보기] 중국 안면인식기술 어디까지?, KBS 뉴스, 2023.08.29., https://news.kbs.co.kr/news/pc/view/view.do?ncd=7759867

23) 인구 14억명 다 알아보는 중국 '안면인식 빅브러더'...정말 없앨까?, 한국일보, 2023.10.23., https://www.hankookilbo.com/News/Read/A2023101820100001841

24) 이에 대해 자세한 내용은 김형섭, 황선영, AI기술의 부패방지와 인권 침해의 논의 - 홍콩 사례(복면금지법)를 중심으로 -, 한국부패학회보 제25권 제2호, 2020 참고; "14억 인구,

중국에서 이러한 기술의 무분별한 사용에 대해 비판이 크게 일어나자 중국 사이버공간관리국은 '안면 인식 기술 적용 안전관리 규정'을 발표하여 AI 기술을 통한 생체인식정보의 처리를 제한하고자 하고 있다. 이 규정의 주요한 내용의 예를 들면 우선 민간 영역에서 안면인식 기술을 사용하려면 특정한 목적과 충분한 필요성이 있어야 하며, 엄격한 보호 조치가 취해진 경우에만 사용이 가능하도록 규정하고 있다. 또한 안면인식 기술을 대체할 수 있는 기타 비생물학적 특정 식별 기술 방안이 존재하는 경우, 반드시 비생물학적 특정 식별 기술 방안을 먼저 고려할 것을 명령하는 규정도 두고 있다. 사생활이 침해될 수 있는 장소인 호텔 객실이나 목욕탕, 탈의실, 화장실 등에서는 영상 수집 및 개인 신원을 식별할 수 있는 장비의 설치를 제한하고, 공공장소에 안면인식기술을 사용하는 기기를 설치하는 경우 이를 고지하는 안내판을 설치할 것 등도 규정하고 있다.[25] 하지만 이러한 기술이 실제 적용되는지, 민간영역이 아닌 공적인 목적으로 사용되는 경우에는 어떠한 제한과 조건이 있는지는 불명확하다.

2. EU의 사례[26]

EU 차원에서의 공권력에 의한 AI 기술과 생체정보 결합기술이 사용되는 것은 원칙적으로 금지되어 있고 예외적으로 허용되어 있다. GDPR은 생체정보를 특정범주의 개인정보(민감정보)로 분류하기 때문에 본인의 동의가 필요하고, 동의를 정당화하는 사유가 필요하다. AI 법률에서도 공권력에 의한 이러한 기술의 사용은 예외적인 경우에만 허용되는 것으로 규정하는데, 이에 대해서는 뒤의 AI법률에서의 규율에서 살펴보기로 하고 우선 민간영역에서의 이러한 기술의 사용에 대한 사례에 대해 살펴본다.

(1) 네덜란드 슈퍼마켓 사례[27]

먼저 네덜란드의 한 슈퍼마켓에서 이러한 기술을 사용하여 매장출입을 금지

CCTV 6억대로 감시"…中, 걸음걸이까지 데이터화, 한국경제, 2020.06.25., https://www.hankyung.com/article/2020062412541g

25) 더 자세한 사항은 이상우, 중국의 안면인식 기술 입법동향과 시사점 - 안면인식 기술응용 안전관리규정 의견수렴안을 중심으로 -, 법학연구 제26집 제4호, 2023 참고

26) 이 부분은 '이인호 외, 생체정보 보호 강화를 위한 법·제도 개선방안 연구, 한국인터넷진흥원, 2022' 연구보고서에서 필자가 집필한 부분을 수정·보완한 것이다.

27) https://www.edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_en; 이인호 외, 생체정보 보호 강화를 위한 법·제도 개선방안 연구, 한국인터넷진흥원, 2022, 37쪽

하는 사례이다. 슈퍼마켓 출입구에 카메라를 설치하고, 이 카메라로 매장에 출입하는 사람들의 안면을 스캔하여 미리 설정한 데이터베이스와의 비교를 통하여 출입이 금지된 자의 출입을 통제하였다. 금지되지 않은 자의 안면정보는 바로 삭제조치를 하였다. 이러한 기술을 통하여 고객과 직원의 보호는 물론 소매치기 방지를 위한 것이라고 슈퍼마켓은 주장하였다. 이러한 기술의 사용에 대해 네덜란드 데이터 보호청(DPA)은 2021년 슈퍼마켓에 대해 공식적인 경고와 함께 이러한 기술 사용을 금지하였다.

보호청은 '안면인식은 우리 모두를 걸어 다니는 바코드(walking bar codes)로 만든다. 안면인식 기술을 사용하는 매장, 경기장(stadium), 축구장(arena)에 출입 시마다 정보주체의 동의 없이 얼굴이 스캔된다. 검색 엔진에 얼굴을 입력하면 사용자의 얼굴이 이름 및 기타 개인 데이터와 연결될 가능성이 있다. 이는 예를 들어 소셜 미디어 프로필과 얼굴을 교차 확인하는 방식으로 이루어질 수 있다. 이 기술은 해당 정보를 어떻게 처리할지 결정할 수 있는데 범죄혐의가 있는 경우, 고객으로서 관심이 있는 경우, 고객의 구매행위를 모니터링하고 프로필을 생성할 가치가 있는 경우 이러한 처리가 수행될 수 있다. 만약 안면인식 기술이 탑재된 카메라를 어느 곳에서나 사용할 수 있다면, 모든 것을 그리고 우리 모두를 지속적으로 감시할 수 있을 것이다.'라고 설명하면서 지속적인 감시의 우려를 표명하였다.

이 사례에서 안면인식 카메라는 생체인식 정보를 사용하여 사람을 식별(identify)한다. 보안 목적을 위한 안면인식기술의 사용은 GDPR에 의하면 두 가지 예외상황에서만 허용될 수 있는데, 바로 동의와 공익적 목적이다. 첫 번째 동의의 경우 정보주체가 자신의 개인정보 처리에 대해 명시적으로 동의한 경우만 허용된다. 이 사례에서 슈퍼마켓 주인은 고객에게 안내를 통해 매장에서 안면인식 기술을 사용한다는 경고를 했다고 주장했지만, 이를 고객의 명시적인 동의로 간주할 수는 없다고 판단하였다. 즉 침묵이 곧 승인(동의)이라는 가정은 여기서 인정되지 않는다. 단순히 슈퍼마켓에 출입하는 것만으로는 동의한 것으로 간주될 수는 없다는 것이다. 다른 예외사유는 인증(authentication)이나 보안(security) 목적으로 안면인식 기술의 사용이 필요한 경우라 하더라도 상당한(substantial) 공익과 관련된 경우에만 기술의 사용이 가능하다는 것이다. 이 사례에서 슈퍼마켓은 이 예외사유에 해당한다고 주장하였지만, DPA는 인정하지 않았다. DPA는 원자력 발전소의 출입을 통제하기 위한 정도가 이 예외사유에 해당할 수 있지 도난을 방지하기 위한 목적은 이 예외에 해당하지 않는다고 설명하였다.

(2) 덴마크 축구장 사례[28]

덴마크의 경우 위와 다르게 판단한 사례가 있다. 덴마크의 축구단인 Brøndby IF는 2019년 7월부터 자신들의 경기장에 자동화된 안면인식(automated facial recognition, AFR) 기술을 도입할 예정이라고 발표했다. 이는 클럽의 자체규정을 위반하여 Brøndby IF의 축구 경기 관람이 금지된 사람을 식별하기 위해 사용될 예정이었다. 자동화된 안면인식 기술 시스템은 카메라를 설치하여 경기장 입구의 공개된 장소를 스캔하여 출입금지목록에 등록된 사람이 출입구에 도달하기 전에 다른 관중으로부터 선별(picked out)될 수 있도록 하는 것이다.

경기장에 자동화된 안면인식 기술을 도입하기 위해서는 데이터 보호법의 요건인 덴마크 데이터 보호청(Danish Data Protection Authority (DPA))의 사전 승인이 필요한데, Brøndby IF는 덴마크에서 자동화된 안면인식 기술 사용을 승인 받은 최초의 기업이 되었다.

덴마크 데이터 보호청이 자동화된 안면인식 기술 사용을 허용한 이유는 GDPR의 상당한 공익을 인정하였기 때문이다. GDPR에 의하면 개인을 고유하게 식별하기 위한 생체인식 정보는 제9조의 특수한 범주의 정보(민감정보)에 속하기 때문에 생체인식정보의 처리를 위해서는 정보주체의 명시적 동의가 필요하다. 다만 여기서의 동의는 자발적 동의를 의미하므로 정보주체의 동의가 이 사례에서의 자동화된 안면인식 기술이 허용되는 법적 근거가 될 수 없다. GDPR 제9조 제2항 (g)는 '유럽연합 또는 회원국 법률에 근거하여 상당한 공익상의 이유로 처리가 필요하고, 추구하는 목적에 비례해야 하며, 데이터 보호권의 본질을 존중하고, 정보 주체의 기본권과 이익을 보호하기 위한 적절하고 구체적인 조치를 제공해야 하는 경우' 민감정보를 처리할 수 있도록 규정하고 있으므로 이 조항에 해당한다면 자동화된 안면인식 기술의 사용이 허용될 수 있을 것이다. 덴마크 데이터 보호청은 이 사례에서 자동화된 안면인식 기술을 통해 사적 금지목록을 집행하는 것이 상당한 공익(substantial public interest) 상의 이유로 필요하고, 이러한 처리가 추구하고자 하는 목적에 비례한다고 결정했다. 보호청은 상당한 공익이 무엇인지에 대한 정확한 정의는 없으므로, 이러한 기술이 수동 검사(manual checks)에 비해 금지 목록을 더 효과적으로 시행할 수 있다는 점과 자동화된 처리를 통해 출입구의 대기열을 줄일 수 있다는 점, 이를 통해 인내심이 부족한 축구팬들의 대중 불안의 위험을 저하시킬 수 있다는 점이 공익이라고 판단하였다.

---

28) https://edri.org/our-work/danish-dpa-approves-automated-facial-recognition/

이에 대해서 반대하는 견해도 있는데, 자동화된 안면인식 기술은 수많은 군중들을 생체인식(안면정보)으로 식별하고, 사전에 작성된 감시목록과의 일치 여부를 기준으로 자동으로 분류할 수 있으므로 가장 침습적인(invasive) 감시기술의 하나라 할 수 있다는 점이다. 또한 이 기술은 특정한 소수 민족에 대해 더 높은 오류발생률을 보이는 시스템의 편향성이 있는 신뢰하기 어렵고 부정확한 기술이라는 점이다. 실제 경기당 평균 14000명이 출입하는데, 금지된 자들은 50명에 불과하여 이를 위해 14000명의 생체인식정보가 처리되어야 하는지에 대한 최소한의 공익을 위한 실질적인 이유가 있는지, 긴급한 공공 보안에 대한 필요성이 있는지, 이 기술 사용에 대한 비례성 심사가 제대로 되었는지에 대한 비판이 있다. 이러한 기준이라면 다른 민간기업들의 이 기술사용 신청이 많아질 것이고, 이러한 기술의 사용이 광범위하게 허용될 수 있을 것이라는 우려도 크다는 점도 반대하는 자들의 의견이다.

(3) 독일 베를린의 Südkreuz역 사례[29]

독일에서는 생체인식 기술의 사용에 대한 시범프로젝트(Pilotprojekt)가 진행되었다. 2017년 베를린에 있는 Südkreuz역에 연방경찰의 “안전한 베를린 Südkreuz역” 프로젝트를 위해 생체인식기술이 포함된 CCTV가 설치되었다. 이 프로젝트는 안면인식기술이 CCTV에 찍힌 사람을 어느 정도로 인식하고 경찰에 신고할 수 있는가를 테스트하기 위한 것이었다. 이를 위해 베를린 Südkreuz역에 정기적으로 출입하는 275명의 자원봉사자의 이미지를 포함한 데이터베이스를 구축하여 대조하였다.

생체인식카메라의 사용을 가능하게 하는 법적 근거에 대해서 독일 연방의회에서도 논의된 바가 있는데, 이를 허용할 법적 근거를 찾기가 현행법상 어렵다는 지적에 대해 연방경찰법 제27조[30]와 프로젝트 자원봉사자의 자발적인 동의로 인하여 프로젝트가 허용될 수 있다고 판단하였다.[31]

지금까지의 독일에서의 CCTV에 관한 논의는 개인정보자기결정권에 대한 중대한 위협이 될 수 있으므로 특별한 근거를 필요로 한다는 것이었다. CCTV에 촬영되는 모든 사람들의 안면정보가 이미 데이터베이스에 수록된 개인의 안면정보와 지속적으로 대조되므로 이는 기본권에 대한 추가적인 제한을 수반

29) S. Schindler, Noch einmal: Pilotprojekt zur intelligenten Videoüberwachung am Bahnhof Berlin Südkreuz, ZD-Aktuell 2017, 05799
30) 자동 사진촬영기록장치에 관한 조항(Selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte)
31) BT-Drs. 18/13350, S. 10

하고, 따라서 이를 정당화하는 특별한 법적 근거가 필요하게 된다. 현행 법령상으로는 전통적인 CCTV를 통한 감시만 허용될 뿐 CCTV를 통한 안면정보의 대조(생체정보의 결합)는 허용되지 않는다. CCTV를 통한 감시와 안면인식과 같은 생체정보기술의 결합은 기본권에 대한 중대한 위협이 되기 때문에, 이러한 기술의 사용을 위해서는 독립적이고 구체적인 법적 근거가 필요하다. 즉 새로운 기술을 사용한 감시를 경찰의 임무 수행에 적용하려면, 이러한 기술의 사용으로 인한 기본권에 대한 제한(침해)를 정당화할 수 있는 구체적 법적 근거가 있어야 한다는 것이 이 프로젝트에 대해 반대하는 견해의 주장이다.

(4) 소결

유럽의 사례에 나타난 AI기술과 생체인식정보 기술의 결합을 사용할 것인지, 허용할 것인지는 먼저 공적인 영역과 사적인 영역에서의 사용이 구별되고, 공적 영역에서의 사용의 겨우 특별하고 구체적인 법적 근거가 있어야 하는지, 아니면 GDPR등의 일반적인 법규정으로도 가능한지의 문제가 발생하고, 민간영역에서는 정보주체의 동의를 어떻게 해석할 것인지가 문제가 된다고 하겠다. 그리고 공통적으로 이러한 기술의 사용의 공익적 필요성과 비례성 심사가 필요한데, 공익의 기준과 심사의 강도를 어느 정도로 할 것인지에 대해 다양한 견해가 있음을 알 수 있다.

Ⅳ. 생체인식과 AI의 결합으로 인한 기본권 침해상황과 이에 대한 AI법의 대응

생체인식정보를 사용할 수 있는 기술이 계속 개발되고 있고, 우리의 삶에 많이 사용되고 있다. 이러한 기술이 인공지능기술과 결합되면서 새로운 차원의 기본권 침해 상황이 발생하게 되고 이를 허용할지에 대해 각 국마다 그 대응방법이 다양함을 살펴보았다. 이러한 상황에서 유럽연합 차원에서는 인공지능법에 이러한 내용을 규율함으로서 세계적인 스탠다드를 구축하고자 하고 있다. 인공지능법에 나타난 생체인식기술과 인공지능기술의 결합허용 여부를 살펴본다.

1. 생체인식정보와 인공지능기술의 결합으로 인한 기본권 침해

생체인식정보 기술과 인공지능기술의 결합으로 인한 기본권 침해의 전형적인 모습은 개인정보자기결정권의 침해일 것이고, 더 나아가 사생활의 비밀이나 일반적 인격권 등이 침해될 수 있을 것이다. 우리의 경우 개인정보보호법 제23조에 '그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보'를 민감정보로 분류하고, 개인정보보호법 시행령 제18조에 '개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보'를 대통령령이 정하는 민감정보에 포함시키고 있으므로 생체인식정보를 사용하는 모든 처리는 민감정보의 처리에 해당하게 된다. 즉 생체인식정보는 개인정보인 민감정보에 해당하고 이의 처리는 일단 개인정보자기결정권에 대한 제한이 되는 것이다. EU의 GDPR도 앞서 설명한 바와 같이 생체인식정보를 개인정보로 분류하고 특별히 제9조의 특정범주의 개인정보(민감정보)로 분류하고 있으므로 생체인식정보의 처리는 개인정보자기결정권을 제한할 가능성이 매우 높다고 볼 수 있겠다. 따라서 생체인식정보와 인공지능기술이 결합된 기술을 사용하기 위해서는 정보주체의 명시적인 동의나 상당할 정도의 공익이 필요하다고 하겠다.

그리고 생체정보라는 것은 정보주체의 신체적 특성, 즉 인체 자체가 가지는 특성이기 때문에 이를 수집하거나 처리하는 것은 사생활 또는 일반적 인격권에 대한 침해가 될 수 있다.[32] 하지만 생체정보가 공공장소에서 수집된 경우 이를 사생활의 비밀의 보호영역으로 포섭하는 것이 애매할 수 있으므로 이 경우에는 사생활의 비밀에 대한 침해보다 일반적 인격권 또는 개인정보자기결정권에 대한 침해문제가 될 수 있다. 그리고 일반적 인격권(das allgemeine Persönlichkeitsrecht)의 중요한 내용인 인격의 자유로운 발현권(das Recht auf freie Entfaltung der Persönlichkeit)은 자신의 삶을 타자의 간섭없이 스스로 결정하고 영위해나갈 수 있는 권리로서 자신의 인격(개성)을 스스로 결정할 수 있는 영역인 사생활의 영역의 보호는 물론, 외부세계와 교류하여 인격을 형성하고 발전시킬 수 있는 자유를 포함하는 개념으로 보아야 한다.[33] 누군가가 나의 생활과 행동을 지켜보고 있다면, 혹은 지켜보고 있다는 느낌을 가진다는 것만으로도, 더 나아가 공권력에 의해 나의 생활이 수집되고 처리되어 분석된

32) 이상경, 생체인식정보의 활용과 개인정보보호에 관한 비교법적 고찰 - 미국의 법제를 중심으로 -, 서울법학 제26권 제3호, 2018, 113쪽
33) 한수웅, 헌법학, 법문사, 제12판, 2022, 567쪽

다면 또는 분석될 수 있다는 위험만으로도 인간은 자신의 삶을 자유롭게 영위하지 못하게 되고, 의식적으로 조심하고 다르게 행동하게 될 것이다.[34] CCTV만으로도 이러한 위험이 높은데, 개인을 식별할 수 있는 생체인식정보 기술이 결합되는 경우 개인을 식별하여 추적할 수 있게 되므로 이러한 위험은 훨씬 높아지게 될 것이고, 일반적 인격권에 대한 심각한 위협이 될 수 있음은 명확하다고 하겠다.[35]

특히 생체인식기술과 인공지능기술이 결합되는 경우 무엇보다 대량감시(mass surveillance) 및 추적이 쉽게 가능해 질 수 있다. 이러한 감시를 통해 개인은 그 자체가 목적으로 대우받는 인격체가 아니라 국가권력의 대상 또는 수단으로 전락하게 되며, 위축효과(Chilling Effect)가 발생할 가능성이 굉장히 높아진다. 이러한 기술의 사용은 범죄 예방이나 용의자의 검거 등 수사나 치안유지 등 경찰행정 분야에서 획기적인 전환점이 될 수 있다. 예를 들어 범죄자를 추적하여 검거할 확률이 상당히 높아질 것이고, 예방적 치안활동도 가능할 것이다. 행정의 영역에서는 코로나 사태에서의 경우 이러한 기술이 사용되었다면 국가가 확진자의 동선 파악을 훨씬 효율적으로 할 수 있었을 것이라고 쉽게 예측할 수 있을 것이다. 하지만 이를 역으로 생각해보면, 평상시에도 우리 일상의 삶이 국가기관에 의해 녹화되고 분석된다면, 특히 발달된 식별기술을 통해 누구인지 특정되어 각 개인에 관한 정보가 공권력에 의해 자세하게 저장되고 분석되어 감시와 추적이 쉽게 가능하다면, 우리는 헌법에 보장된 자유로운 삶을 영위할 수 있을 것인가에 대해 심각하게 고민하게 될 것이다. 공·사 구분 없이 설치된 수많은 CCTV를 통하면 정보주체가 인지할 수 없는 상태에서 정보주체의 정확한 동선이 파악될 수 있으며, 나아가 개인이 스스로 공개한 SNS상의 사진들 역시 어렵지 않게 수집하여 대조군인 데이터베이스로 활용될 수 있다. 생체정보는 개인의 고유한 정보들을 포함하고 있으므로 그 처리의 오·남용은 곧 개인에 대한 감시와 추적으로 이어질 수 있다. 민주주의에서 가장 중요한 요소 중 하나가 자유롭게 행동하고 표현할 수 있는 것인데, 국가권력이 모든 곳에서 개인을 특정하여 감시, 추적할 수 있다고 한다면 이러한 자유로운 행동과 표현은 불가능해질 것이고, 이것은 기본권에 대한 굉장한 침해가 되며 민주주의에도 굉장한 위협이 될 것이다.

그리고 AI기술이 결합된 생체인식정보는 인식(recognition), 인증(authentication).

---

34) 이권일, 생체인식정보의 보호와 활용에 대한 헌법적 고찰, 법학연구 제61권 제2호, 2020, 15쪽

35) 생체인식정보의 처리를 통한 기본권 침해에 대한 더 자세한 사항은 이권일, 위의 논문 참조

식별(identification), 검증(verification) 목적으로도 사용될 수 있지만 범주화의 목적으로도 사용될 수 있다. 범주화(categorization)는 개인을 식별하고자 하는 목적이 아니라 개인을 미리 분류되어 있는 분류체계에 그 사람의 특징에 따라 분류를 하는 것이기에 개인을 식별하거나 개인정보에 대한 처리가 없을 수도 있어서 개인정보자기결정권이나 사생활의 비밀에 대한 제한에 해당하지 않을 수도 있다. 하지만 다른 관점에서 기본권에 굉장히 위협적일 수 있다. 왜냐하면 부당한 차별(discrimination)의 위험성 때문이다. 우리나라에서는 그 위험이 덜할 수 있는데, 피부색과 출신에 따른 인종적 차별이 심한 나라의 경우 이러한 차별의 위험성은 굉장히 높다고 하겠다. 우리의 경우도 노인과 청년 등 나이에 따른 차별이나 성별에 의한 차별이 발생할 수 있는 등 부당한 차별의 위험이 없는 것은 아니다. 특히 생체인식기술이 완전하지 않은 경우, 0.1%나 0.01%의 오류에 불과하다고 하더라도 국민 전체의 0.1% 또는 0.01%가 되면 실제로는 많은 수가 될 수 있기 때문에 잘못 분류되어 범주화된다면 치명적인 위협이 될 수도 있다.

2. EU 인공지능법의 대응

EU 인공지능법은 내부시장의 기능을 개선하고 인간 중심의 신뢰할 수 있는 인공지능의 활용을 촉진하며, 유럽연합 내 인공지능 시스템(AI 시스템)의 유해한 영향으로부터 건강, 안전, 기본권 헌장에 명시된 기본권(민주주의, 법치주의, 환경 보호 등을 포함하는)을 높은 수준으로 보호하고 또한 혁신을 지원하는 것을 목적으로 한다.(AI 법 제1조) 이 조문은 이사회의 AI 법률안에서는 제안이유(Erwägung)에서만 설명되었고, 실제 조문에는 없었으나 의회의 최종 결의안에서는 제1조에 명문으로 규정하는 것으로 변경되었다.

인공지능법은 인공지능을 위험에 기반하여(risk-based approach) 분류하고 규제의 강도를 달리하고자 한다. AI 시스템에 비례적이고 효과적인 구속력 있는 규범을 도입하려면 명확하게 정의된 위험 기반 접근 방식을 따라야 한다. 이러한 접근 방식은 AI 시스템이 생성할 수 있는 위험의 강도와 범위에 맞게 규범의 유형과 내용을 조정해야 하는데, 크게 허용되지 않는 AI(unacceptable AI), 고위험 AI(high-risk AI), 일반(보통)의 AI로 분류된다. 허용되지 않는 AI는 실행이 금지되고 예외적인 경우에만 허용된다. 고위험 AI는 시스템 사용에 대한 요건과 관련 운영자의 의무가 상세히 규제되며, 일반 AI의 경우 시스템에 대한 투명성 의무가 있다.

이 법은 AI 시스템을 '배포 후 적응성을 발휘할 수 있으며 명시적 또는 묵시적 목적을 위하여 수신한 입력으로부터 물리적이거나 가상적인 환경에 영향을 미칠 수 있는 예측, 콘텐츠, 권고나 결정과 같은 산출물을 생성해내는 방법을 추론할 수 있도록 다양한 수준의 자율성(autonomy)을 가지고 작동하도록 설계된 기계 기반 시스템'으로 정의하고 있다. 자율성이란 개념은 인간의 개입으로부터 어느 정도 독립적으로 가동하고 인간의 개입 없이도 작동할 수 있는 기능을 갖추고 있음을 의미한다. 또한 배포 후의 적응성(adaptiveness)이란 것은 사용중에도 시스템의 변경이 가능한 자가학습(self-learning) 능력을 의미한다.[36] 또한 이 법에서는 위험(risk)을 피해 발생 확률과 피해의 심각성을 결합한 것이라고 정의한다.

인공지능 기술과 결합되는 생체인식정보는 자연인의 인증, 식별, 분류, 감정인식(recognition of emotions)의 목적으로 사용될 수 가능성이 있다.

이 법에서 말하는 생체인식인증(biometric identification)은 개인의 동의 여부와 관계없이 해당 개인의 생체인식정보를 참조 데이터베이스에 저장된 개인의 생체인식정보와 비교하여 개인의 신원을 확인할 목적으로 얼굴, 눈 움직임, 체형, 음성, 운율, 걸음걸이, 자세, 심박수, 혈압, 냄새, 키 입력 특성 등 신체적, 생리적, 행동적 인간의 특징을 자동으로 인식하는 것으로 정의할 수 있다. 다만 본인임을 확인하여 서비스에 엑세스하기 위한 목적, 기기의 잠금해제를 위한 목적, 구내보안을 위한 엑세스 목적으로만 이러한 기술이 사용되는 것은 이 법의 적용에서 제외된다.

인공지능법 제5조는 금지되는 AI 시스템의 실행이 규정되어 있는데, 제1항 제e호에서 인터넷이나 CCTV 영상에서 표적화되지 않은 얼굴 이미지를 스크랩하여 안면인식정보를 생성하거나 확장하는 AI 시스템을 시장에 출시하거나 이러한 목적을 위해 서비스를 제공하거나, 이러한 시스템을 사용하는 것은 금지되는 것으로 규정하고 있다. 또한 의료 또는 안전상의 이유로 인공지능 시스템을 도입하거나 시장에 출시하려는 경우를 제외하고, 직장 및 교육 기관의 영역에서 자연인의 감정을 추론하기 위해 인공지능 시스템을 시장에 출시하거나 이러한 특정 목적을 위해 서비스를 제공하거나 인공지능 시스템을 사용하는 행위, 생체인식정보를 기반으로 자연인을 개별적으로 분류하여 인종, 정치적 의견, 노동조합 가입 여부, 종교적 또는 철학적 신념, 성생활 또는 성적 취향을 추론하거나 유추하는 생체 분류 시스템(biometric categorisation systems)을

36) 제안이유 12

시장에 출시하거나 이러한 특정 목적을 위해 서비스하거나 이러한 시스템을 사용하는 행위는 금지된다.(동조 동항 제f, g호) 다만 생체 분류 시스템의 경우 생체인식정보를 기반으로 법적으로 취득한 생채인식정보세트(biometric datasets)의 라벨링이나 필터링, 법 집행 영역에서 생체인식정보를 분류하는 행위는 금지되지 않는다.

공적인 영역에서 법 집행 목적으로 공개적으로 접근 가능한 공간에서 '실시간(real-time)' 원격 생체 인식 시스템을 사용하는 것은 원칙적으로 금지된다. 여기서 '공개적으로 접근 가능한 공간(publicly accessible space)'이란 특정한 접근 조건이 적용되는지 여부와 잠재적 수용인원 제한 여부에 관계없이 불특정 다수의 자연인이 접근할 수 있는 공공 또는 사적 소유의 물리적 장소를 의미하는 것으로 정의하고 있다.(법 제3조 제44호) 다만 공개적으로 접근 가능한 공간에서의 실시간 원격 생체 인식 시스템의 사용은 3가지의 예외적인 경우에 사용이 가능하다. 첫째로 납치, 인신매매 또는 성적 착취의 피해자에 대한 표적 수색(targeted search) 및 실종자 수색을 위한 경우, 둘째로 자연인의 생명 또는 신체적 안전에 대한 구체적·실질적·임박한 위협(specific, substantial and imminent threat) 또는 테러 공격의 실질적이고 현존하는 또는 실질적이고 예측 가능한(genuine and present or genuine and foreseeable) 위협의 방지를 위한 경우, 마지막으로 부속서 II(Annex II)에 언급된 범죄에 대한 수사, 기소 또는 형사 처벌을 수행하거나 해당 회원국에서 최대 4년의 구금형으로 처벌할 수 있는 범죄를 저지른 것으로 의심되는 사람의 위치 추적(localisation) 또는 신원 확인(identification)을 목적으로 하는 경우에만 이 시스템의 사용이 예외적으로 허용된다. 이 시스템의 사용이 허용되는 경우라 하더라도 구체적으로 표적 대상의 신원을 확인하기 위해 위에 명시된 목적으로만 배치되어야 하고, 배치되는 경우에도 사용 가능성을 야기하는 상황의 특성, 특히 시스템을 사용하지 않을 경우 발생할 수 있는 피해의 심각성, 가능성 및 규모와 시스템 사용으로 인해 모든 관련자의 권리와 자유에 미치는 결과, 특히 그 결과의 심각성, 가능성 및 규모가 고려되어어야 한다(비례성 심사). 또한 이 시스템의 사용과 관련하여 시간적, 지리적, 개인적 제한(temporal, geographic and personal limitations)과 관련하여 필요하고 비례적인(necessary and proportionate) 안전장치와 조건이 준수되어야 한다.

그뿐만 아니라 공개적으로 접근 가능한 공간에서 이 시스템을 법 집행 목적으로 사용할 수 있기 위해서는 회원국의 국내법으로 세부 규정을 정하여 구속력을 가지는 사법기관이나 독립행정기관에 의한 사전허가를 받을 것을 규정하

고 있다. 단 이 경우에도 적절한 절차에 따라 정당화되는 긴급 상황의 경우, 늦어도 24시간 이내에 부당한 지체 없이 승인을 요청하는 경우에는 승인 없이 시스템 사용을 시작할 수 있는 예외규정을 두고 있다. 다만 사후 승인이 거부되면 시스템의 사용은 즉시 중단되어야 하고 모든 데이터와 해당 사용의 결과 및 산출물은 즉시 폐기 및 삭제되어야 한다. 사법기관이나 독립행정기관은 법에 명시된 목적을 달성하기 위해 필요하고 비례성을 충족한다고 판단한 경우 승인할 수 있으며, 승인할 때에도 지리적, 인적 범위와 기간을 엄격하게 제한하여야 한다. 만약 이러한 조건에 따라 이 시스템의 사용이 허용되어 실행되는 경우 실시간 원격 생체 인식 시스템을 사용할 때마다 관련 시장 감시 기관 및 국가의 정보보호기관에 통지해야 한다.

이러한 내용을 종합해볼 때 공개적으로 접근 가능한 공간에서의 법 집행 목적으로 실시간 원격 생체 인식 시스템을 사용하는 것은 아주 예외적인 경우에만, 매우 복잡한 조건을 부과하여 실행될 수 있도록 법이 규정하고 있음을 알 수 있다. 더 나아가 인공지능법은 각 회원국이 이와 관련된, 그리고 실행에 필요한 세부적이고 구체적인 사항을 국내법에 따로 규정하도록 명령하고 있다. 이때 각 회원국은 원격 생체 인식 시스템의 사용에 대해 EU 인공지능법보다 더 제한적인 내용의 법률을 제정하는 것이 허용된다.

그리고 실시간 원격 생체 인식 시스템, 감정 인식 시스템(emotion recognition system), 생체 인식 분류 시스템(biometric categorisation system) 이외의 원격 생체인식 시스템, 즉 사후(post) 원격 생체 인식 시스템은 금지되는 AI 시스템이 아닌 고위험 AI 시스템으로 분류한다. 자연인의 원격 생체 인식 식별을 위한 AI 시스템의 기술적 부정확성은 편향된 결과를 초래하고 차별적 효과를 수반할 수 있다. 편향된 결과와 차별적 효과의 위험은 특히 연령, 민족, 인종, 성별 또는 장애와 관련이 있으므로 원격 생체 인식 시스템은 이러한 위험성을 고려하여 고위험군(high-risk)으로 분류되는 것이다.[37]

고위험 AI 시스템은 금지되는 것은 아니지만 의도된 목적과 인공지능 및 인공지능 관련 기술에 대해 일반적으로 인정되는 최신 기술을 고려하여 법에 명시된 요건을 완전히 준수할 책임이 있다. 인공지능법은 제8조 이하에 이러한 요건에 대해 상세하게 규정하고 있다. 고위험 AI 시스템은 위험관리 시스템을 수립하고 구현하며 문서화 및 유지ㆍ관리해야 한다. 이를 통해 고위험 AI 시스템의 실행으로 발생할 수 있는 위험을 보다 효과적으로 제거하거나 최소화

37) 제안이유 54

해야 하고 위험을 제거할 수 없는 경우 이를 완화하기 위한 적절한 조치와 통제조치를 취해야 한다. 고위험 AI 시스템은 가장 적절하고 목표에 맞는 위험관리 조치를 식별하기 위해 테스트를 받아야 한다. 이 테스트는 시장에 출시되기 전 그리고 출시된 후에도 언제든지 수행되어야 한다. 이러한 여러 제한들을 시행하기 위해 제공자(provider)와 배포자(deployer)에게 의무를 부과하고 있다. 즉 사후 원격 생체 인식 시스템은 실시간 원격 생체 인식 시스템보다 기본권 침해가 덜 할 수 있기 때문에 금지되는 것이 아니라 고위험군으로 분류되어 사용은 가능하지만 고강도의 상세한 규제를 받는 것으로 법이 규정하고 있음을 알 수 있다.

V. 나가며

유럽에서는 생체인식정보 기술의 발달과 AI 기술의 발달, 그리고 이 두가지 기술이 결합되어서 나타나게 되는 기본권 침해상황을 심각하게 생각하여 이를 규제하기 위한 법제를 만들기 위해 노력해왔다. 특히 2021년 인공지능법안이 유럽연합 집행위원회에서 유럽연합 의회에 제안되었고, 3년 이상의 기간동안 이에 대해 유럽의 학계와 정치계, 시민사회와 각 회원국에서 뜨겁게 논의된 결과 지난 2024년 3월 유럽연합 의회에서 압도적 다수로 인공지능법이 통과되었고, 일부 조항은 6개월 후부터, 2026년부터는 전면 시행된다. 이는 소위 브뤼셀 효과로 인하여 GDPR과 같이 세계에 영향을 미치는 인공지능 규제법으로 기능할 것으로 보인다.

이번에 통과된 인공지능법의 가장 큰 특징 중의 하나는 AI 기술을 이용한 생체인식정보의 처리를 강하게 규제하고자 한다는 점이다. EU에서는 생체인식기술과 AI기술이 결합하였을 때 발생할 수 있는 대량감시와 추적의 가능성과 이로 인한 일반적 인격권, 사생활의 비밀, 개인정보자기결정권, 평등권 등의 기본권 침해적 상황이 심각할 수 있다는 점에 대한 분명한 인식으로 이를 강하게 규제하고자 한다. 특히 감정인식시스템, 생체 인식 분류 시스템, 실시간 원격 생체 인식 시스템, 사후 원격 생체 인식 시스템 등의 새로운 기술에 대해 개념정의를 하고자 노력하였고, 이를 바탕으로 AI 기술과 생체인식정보가 결합되어 사용되는 경우 이러한 AI 시스템의 실행을 금지하거나 고위험 AI 시스템으로 분류하여 강하게 제한하고자 한다. 실시간 원격 생체 인식 시스템은

원칙적으로 사용이 금지되고 극히 예외적인 경우 법집행의 목적으로 공개적으로 접근 가능한 공간에서의 사용이 허용되는데 이 또한 사법기관 등의 사전허가를 받도록 규제하고 있다. 사후 원격 생체 인식 시스템은 고위험 AI 시스템으로 분류하여 법에서 규정하고 있는 상세한 규제를 모두 준수해야 하는 고강도 규제를 받도록 규정하고 있다.

사적 영역에서의 생체인식기술이 사용되는 AI 시스템의 사용은 명시적인 동의를 어떻게 해석할 것인지(예를 들어 안내판을 설치했음에도 불구하고 출입한 경우 동의로 볼 것인지, SNS에 사용자의 얼굴 사진을 스스로 업로드한 것이 생체인식기술로 처리될 수 있음에 동의를 한 것으로 볼 것인지)의 문제가 발생하며, 공익에 의한 필요성과 비례성 심사가 이루어져야 하는데 명확한 기준 설정이 어려움을 살펴보았다.

우리의 경우 AI 관련한 특별법도 생체정보와 관련한 특별법도 아직 제정되지 않는 상황이다. 생체인식정보의 경우 개인정보보호법 시행령에 그 내용만에 민감정보에 속하는 것으로만 규정되어 있을 뿐 아직 이를 규율할 법제가 마련되어 있지 않다. EU에서도 생체인식정보의 사용에 대해 다른 특별법없이 GDPR 규정으로 해결해 왔으나 이제 AI법이 제정됨에 따라 이와 관련한 사항은 AI법의 규제를 받게 되었다.

앞으로 AI 기술과 생체인식기술을 더욱 발전할 것이고, 이러한 기술이 우리의 삶 속에 우리의 생활을 편리하게 하기 위하여 더 광범위하게 사용될 것이 예측된다. 또한 이러한 기술을 사용하는 시장도 엄청나게 확대될 것으로 예상되는데, 이는 AI법이 AI를 규제하기 위한 법이면서도 목적조항에 인공지능의 활용을 촉진하고 혁신을 지원하기 위한 법이라고 명문으로 규정한 것에서도 알 수 있다. 따라서 이러한 기술의 사용을 전면적으로 금지함으로서 우리의 기본권을 보장한다는 생각은 더 이상 유효할 수 없고, 이러한 기술의 사용으로 인한 부작용을 최소화하는 방안을 마련하고, 이러한 기술의 사용을 어떻게 제한하여야 할 것인지에 대한 논의를 하여야 한다. 이런 점에서 유럽의 AI법이 우리에게 주는 시사점은 분명히 있다. 이러한 기술의 사용은 더욱 확대될 것이고 확대되어야 하는데, 이러한 기술의 사용이 더 유연해질 수 있도록 법제를 개편하는 것과 아울러 개인의 기본권이 더 실효적으로 보장될 수 있는 조화로운 방법을 모색하여야 할 것이다.

[참고문헌]

장영수, 헌법학, 홍문사, 제11판, 2019
한수웅, 헌법학, 법문사, 제12판, 2022
이인호 외, 생체정보 보호 강화를 위한 법·제도 개선방안 연구, 한국인터넷진흥원, 2022

김형섭, 황선영, AI기술의 부패방지와 인권 침해의 논의 - 홍콩 사례(복면금지법)를 중심으로 -, 한국부패학회보 제25권 제2호, 2020
박정훈, 김행문, 생체정보 프라이버시의 쟁점 및 정책 시사점 - 전자여권 사례를 중심으로 -, 정보화정책 제15권 제3호, 2008
이권일, 일반에게 공개된 개인정보의 보호와 활용, 법학논고, 제68집, 2020
_____, 헌법상 보호되는 프라이버시 개념의 변화에 관한 소고 – 독일 연방헌법재판소 판례 분석을 중심으로 –, 세계헌법연구 제25권 제1호, 2019
_____, 생체인식정보의 보호와 활용에 대한 헌법적 고찰, 법학연구 제61권 제2호, 2020
이상경, 생체인식정보의 활용과 개인정보보호에 관한 비교법적 고찰 – 미국의 법제를 중심으로 -, 서울법학 제26권 제3호, 2018
이성기, 생체인식정보와 감시: 수사기관의 얼굴 인식기술을 활용한 신원확인 행위의 법적 근거와 한계에 관한 연구, 법과 정책연구 제18집 제1호, 2018
이유미, 민수홍, 형사사법기관의 생체정보 수집에 대한 동의에 영향을 미치는 요인, 한국범죄학 제10권1호, 2016
이창범, 생체 프라이버시 보호원칙에 관한 연구, 인터넷법률 제31호, 2005
전명근, 문기영. 생체정보 이용과 프라이버시 보호. 정보보호학회지 제15권 제6호, 2005
정부금, 권헌영, 박혜숙, 임종인, 바이오정보 활용 서비스 현황 및 GDPR 사례를 통한 바이오정보보호 법제 개선방안. 한국통신학회논문지, 제43호 제1권, 2018
정승일, 바이오 정보 보호에 관한 최근 주요이슈 및 법규 개선방안. 한국기술혁신학회 학술대회, 2016. 05
정연덕, 생체인식여권(bio passport)의 활용과 문제점, 인터넷법률 제24호, 2004.07.
정일영. 혁신기술과 바이오정보의 규제 이슈 -안면인식기술, 유전체 분석 정보, 커넥티드 카를 중심으로. 한국기술혁신학회 학술대회, 2019.11.
S. Schindler, Noch einmal: Pilotprojekt zur intelligenten Videouberwachung am Bahnhof Berlin Sudkreuz, ZD-Aktuell 2017, 05799

[Abstract]

Study on the use and protection of biometric data under EU AI Act*

Kwom Il LEE**

In Europe, the development of biometric data technology and the development of AI technology, and the violation of fundamental rights caused by the combination of these two technologies, have been seriously considered, and efforts have been made to create legislation to regulate them. In particular, the Artificial Intelligence Act was proposed to the European Parliament by the European Commission in 2021, and after more than three years of heated discussions in European academia, politics, civil society, and member states, the Artificial Intelligence Act was passed by the European Parliament with an overwhelming majority in March 2024, and some provisions will be implemented in six months, and all provisions will be implemented in 2026. Due to the so-called Brussels effect, it is expected to function as an AI regulatory law with global impact like the GDPR.

One of the most significant features of the AI Act is that it seeks to strongly regulate the processing of biometric data using AI technology. The EU clearly recognizes the potential for mass surveillance and tracking that can arise from the combination of biometrics and AI technologies, and the potential for serious violations of fundamental rights such as the personality right, the right to privacy, the right to self-determination of personal information, and the right to equality. In particular, the Act endeavors to conceptualize new technologies such as emotion recognition systems, biometric categorisation systems, remote biometric identification systems, real-time remote biometric identification systems, and post remote biometric identification systems, and based on this, it seeks to prohibit the practices of such AI systems or classify them as

* This research was supported by Kyungpook National University Research Fund, 2023
** Assistant Professor, Kyungpook National University Law School

high-risk AI systems and strongly restrict them when AI technology and biometric data are used in combination.

It is expected that AI technology and biometrics will be further developed in the future, and that these technologies will be used more widely in our lives to make our lives easier. The market for the use of these technologies is also expected to expand tremendously, which is evident from the fact that the AI Act is intended to regulate AI, but the purpose clause clearly states that it is intended to promote the utilization of AI and support innovation. Therefore, the idea of ensuring our fundamental rights by prohibiting the use of these technologies outright is no longer valid, and we need to discuss how to minimize the adverse effects of these technologies and how to limit their use. In this regard, the implications of European AI law are clear. The use of these technologies will and should be expanded, and we need to find a harmonized way to ensure that the fundamental rights of individuals are better protected, while also reforming the legal framework to make it more flexible.

Keywords : AI Act, biometric data, real-time remote biometric identification systems, high-risk AI systems, information privacy protection