지식재산연구
Journal of Intellectual Property

지식재산연구 20권 4호, 2025년 12월, 147-163면
Journal of Intellectual Property Volume 20, Issue 4, December 2025, Pages 147-163.
https://doi.org/10.34122/jip.2025.20.4.147

Print ISSN 1975-5945
Online ISSN 2733-8487

RESEARCH ARTICLE

The EU AI Act Based on the Precautionary Principle and France's Response: Focused on the Protection of the Right to One's Image

Hee Jin Choe

Assistant Professor, Department of Arts and Cultural Management, College of Cultural Knowledge Convergence, Dongduk Women's University, Republic of Korea

Corresponding Author: Hee Jin Choe (paris8@dongduk.ac.kr)

ABSTRACT

This study aims to interpret how the right to one's image, as a fundamental right, is protected under the precautionary principle, which serves as the EU AI Act's normative philosophy. It also analyzes the specific administrative and legislative systems that France established before the Act's entry into force. The Act uses a risk-based approach that adjusts precautionary controls through outright prohibitions, human oversight, information provision, transparency, labeling obligations, and duties imposed on providers and deployers. Together, these measures protect the right to one's image. In response, France has adopted a dual CNIL–SREN track: CNIL provides guidance, supervises and sanctions, and enforces transparency and notice duties, while the SREN Act strengthens notice-and-action procedures for illegal content and criminalizes non-consensual deepfakes, improving online safety. Future research will compare national rules on the commercial exploitation of the right to one's image and examine post-mortem, digital and biometric, and minors'aspects.

KEYWORDS

EU AI Act, precautionary principle, right to one's image, French Data Protection Authority(CNIL), SREN law

Open Access

Received: September 21, 2025
Revised: September 25, 2025
Accepted: December 03, 2025
Published: December 30, 2025

Funding: The author received manuscript fees for this article from Korea Institute of Intellectual Property.

Conflict of interest: No potential conflict of interest relevant to this article was reported.

원저

'예방주의 원칙' 기반 EU AI 법과 프랑스의 대응: 초상권 보호를 중심으로

최희진

동덕여자대학교 문화지식융합대학 문화예술경영 전공 조교수

교신저자: 최희진 (paris8@dongduk.ac.kr)

차례

국문초록

이 연구는 EU AI 법(EU AI Act)이 규범 철학으로 준거하고 있는 '예방주의 원칙'을 통해 기본권의 영역인 초상권이 어떻게 보호되고 있는지를 해석하고, EU AI 법 발효에 이르는 과정에서 프랑스가 어떠한 행정 체계와 입법 체계를 마련하였는지 구체적으로 그 대응 방식을 분석하는 것이 목적이다. EU AI 법은 위험기반 접근을 통해 AI 활용 분야에서 예방주의적 통제 강도를 달리한다. EU AI 법은 전면 금지부터 인간 감독, 정보 제공, 투명성, 표시 의무, 개발자, 배포자에 대한 의무 규정 등을 통해 기본권 보호 차원에서 초상권을 보호하고 있다. 프랑스는 EU AI 법에 대응하여 'CNIL–SREN법' 이중 트랙을 마련하고 있다. CNIL은 AI 기술에 대한 가이드라인, 감독, 제재, 표시 의무와 같은 행정 집행 차원에서 역할을 담당하고, SREN법은 온라인 불법콘텐츠 이용자 신고 처리 및 신속 삭제 체계, 딥페이크 처벌로 안전한 디지털 환경을 강화한다. 향후 초상권 연구는 초상의 상업적 이용을 둘러싼 국가별 규율 수준, 사후 초상권, 디지털 초상권 그리고 미성년자 초상권에 관한 정책 연구로 이어질 것으로 전망된다.

주제어

EU AI Act, 예방주의 원칙, 초상권, 국가정보자유위원회, SREN법

1. 서론

인공지능 기술은 눈부신 속도로 발전하며 이 기술의 예측 불가능성에 대한 논의가 뜨겁다. 특히 딥러닝 기반 AI 기술로 사람의 얼굴 이미지 및 음성을 자동으로 생성하고 합성하는 현실은 기술 개발 및 사용에 대한 법적 규제와 시민 교육 차원에서 기술 활용에 대한 윤리 교육이 절실히 필요하다는 것을 인식시킨다. 최근 이페르트뤼카쥬(hypertrucage)[1], 즉 딥페이크(deepfake)로 인한 피해는 유명 연예인, 정치인 등 공인들에게 집중되었고 이들의 인격권 침해, 초상권[2] 침해는 일반 사용자들에게도 일상에 침투한 딥러닝 기반 AI 기술에 대한 경각심을 불러일으켰다.

프랑스 내 현실도 예외는 아니다. 2024년 2월 15일, 국제보도 전문채널 프랑스24(France 24) 자사 아나운서가 진행한 한 뉴스는 딥페이크 기술로 변조된 영상이 온라인상에 유포된 사실로 드러나며 큰 곤욕을 치러야 했다. 마크롱 대통령이 우크라이나 방문을 취소한 이유가 암살 위협 때문이었다는 것인데 이는 명백한 거짓이었다.[3] 작고한 프랑스 샹송 가수 달리다(Dalida)의 음성이 AI 음성 추출 서비스 플랫폼 잠마블(Jammable)[4]에서 권리자의 사전 이용 허락 없이 활용된 바 있는데, 달리다의 음성은 고인의 인격과 정체성을 이루는 음성을 인공지능이 저작물을 통해 학습한 것이었다. 2024년 영국 음악산업 협회(British Phonographic Industry)는 잠마블을 상대로 초상권과 저작권 침해에 대하여 법적 대응을 예고한 바 있다.

본 연구는 위험의 수준을 체계적으로 분류하여 설계된 세계 최초의 체계적·포괄적 인공지능 규제 EU AI 법의 도입 배경, 규범적 철학인 '예방주의 원칙'을 밝히고, 해당 원칙이 관류하는 EU AI 법체계 안에 초상권이 어떻게 보호되는지 분석하는 것이 목적이다. 아울러 EU AI 법 제정, 시행, 발효에 이르기까지 프랑스의 역할과 자국 내 법제, 정책적 대응을 교차 검토하며 그 내용을 밝히는 것이 목적이다. 국내 EU AI 법에 관한 선행 연구는 주로 위험 분류, 적합성 평가, 준수 실무 소개에 집중되어 온 데 비해, EU AI 법 안에 명시되지는 않았으나 규범의 기반이 되는 '예방주의 원칙'을 환기하는 연구, 특정 권리에 대한 보호 매커니즘을 밝히는 연구는 아직 진행되지 못한 것으로 보인다.

EU AI 법 이전 프랑스는 민법 제9조, 1992년부터 존재해 온 형법 제226-8조 등으로 초상권 침해를 처벌해 왔다.[5] 그러나 AI 기술이 하루가 다르게 발전하면서 이에 상응하는 기본권 보호 규제, AI 기술 개발자, 배포자, 사용자가 지켜야 할 규제가 부재한 것이 사실이며 미래에 발생할 수 있고 불확실한 기본권 침해는 기존 법률만으로 처벌하는 데 한계가 있다. 이에 본 연구는 EU AI 법의 입법 취지가 잘 드러나는 설명문, 적용 범위, 용어 정의를 통해 초상권이 어떻게 보호되는지를 검토하고자 한다. 이어 초상권과 직결되는 생체식별, 딥페이크, 고위험 AI 시스템 제공

1) '딥페이크'는 기술적 용어이고, '이페르트뤼카쥬'는 프랑스 및 유럽 법제에서 사용하고 있는 공식 법률용어이다. EU AI 법 제3조는 딥페이크를 "인공지능에 의해 조작되거나 생성된 이미지 또는 오디오, 비디오로서, 사람, 사물, 장소, 실체 또는 현존하는 사건과 유사성을 지니고, 사람이 이를 진짜이거나 사실인 것으로 오인되어 인식될 수 있는 것"으로 정의하고 있다.

2) 안용교(1982)는 초상권을 인격권, 프라이버시권으로서의 초상권과 재산권으로서의 초상권을 구분한다. 한 인간은 자신의 초상을 인격권의 하나로서 갖는다. 따라서 그 개인의 동의 없는 무단 이용, 무단 촬영은 사생활 침해에 해당하며, 이를 거절할 권리를 가진다. 초상의 주인은 동시에 초상 이용에 대하여 재산적 이익을 가질 권리가 있는데, 이를 재산권으로서 초상권이라고 설명하고 있다. 안용교, "초상권의 개념과 의의", 「언론중재」, 제3호(1982), 1-2면.

3) France 24, 「FRANCE 24 journalist impersonated in new deepfake video」, Truth or Fake, 2024. 2. 15자.

4) Jammable, "AI Dalida Voice", Jammable, <https://www.jammable.com/custom-dalida>, 검색일: 2025. 8. 6.

5) 프랑스 상원 웹사이트에는 1992년 제정 형법 제226-8조가 과학기술 진보에 따라 수정된 과정을 알리는 글이 있다. Sénat, "Bicentenaire du Code pénal", Sénat, <https://www.senat.fr/colloques/actes_bicentenaire_code_penal/actes_bicentenaire_code_penal11.html>, 검색일: 2025. 8. 4.

자 및 배포자의 의무, 투명성 조항 등을 살펴보고 법 전반에 예방주의 원칙이 어떻게 실제로 적용되고 있는지 살펴보고자 한다. 이어 프랑스는 EU AI 법이 발효되는 과정에 어떠한 대응을 하였는지 살펴보고자 한다. 마지막으로 AI 기술이 일상에 들어온 현재 초상권 보호가 갖는 의미를 논해 보고자 한다.

2. EU AI 법 도입의 배경

2.1. 정치적 선언에서 입법까지

EU AI 법은 우르줄라 폰데어 라이엔(Ursula von der Leyen)이 유럽연합 집행위원장에 지명되어 출마하기 전 그가 내건 정치적 공약에서 시작되었다. 2019년 7월 16일 유럽연합 집행위원장 출마 전 그는 취임 100일 안에 인공지능에 대한 입법을 새롭게 제안하고 유럽연합을 디지털 시대의 표준으로 자리 잡도록 하겠다고 밝혔다.[6] 집행위원장의 "AI의 인간적·윤리적 함의에 대한 유럽 차원의 조율된 접근법 마련"[7]이라는 포부는 그 실현을 위한 첫걸음으로 2021년 4월 21일 AI에 대한 포괄적 규제안(Proposition de règlement)[8] 제출로 구체화되었다.

AI 법안은 기술 발전에 대한 단순한 대응이 아니라 신뢰할 수 있고 인권 친화적인 AI의 개발과 사용을 제도적으로 보장하는 데 목적이 있다. 목적은 제안서에 4가지로 구체적으로 기술되어 있다. 첫째, 유럽연합 시장에 출시되고 사용되는 AI 시스템 안전을 통해 기본권에 대한 현행 법률과 EU의 가치를 준수하도록 보장하는 것, 둘째, AI 분야 투자 및 혁신을 촉진하기 위해 법적 안정성을 보장하는 것. 셋째, AI 시스템에 적용되는 기본권 및 안전 관련 기존 법률의 거버넌스와 집행의 실효성을 강화하는 것, 넷째, 합법적이고, 안전하며 신뢰할 수 있는 AI 애플리케이션의 단일시장 개발을 촉진하고, 시장의 분열을 방지하는 것이다. 특히 첫째와 셋째 항목은 기본권 보호와 안전성 확보라는 규범적 가치가 중점적으로 강조하고 있다. 이 가운데 기본권 보호는 인격권, 초상권 보호와 직접 연결되는 핵심 내용이다.

2021년 8월 6일 EU의회 정책부는 생체인식 윤리 및 법 연구보고서[9]를 작성, 공공 의견 수렴을 종료하였다. 이어 2021년 11월 29일 EU 이사회 순환의장국이었던 슬로베니아는 AI 법에 대하여 회원국 간 의견 충돌을 조율하기 위해 첫 번째 중재안을 공식적으로 제출하였다. 이어 2022년 4월 20일에는 EU의회 상임위원회 내부시장 및 소비자보호위원회[10]와 시민 자유, 사법 및 내무 위원회[11]가 최초 협상 리더로서 참여하였고 각각의 위원회에 소속된 2명의 위원[12]이 함께 초안 보고서를 작성하고 발표하였다. 이 초안 보고서는 3항 AI 시스템의 정의, 9항 고위험 AI 시스템에 대한 위험 관리 시스템, 51항 등 일부 내용을 수정하여 공개되었다.[13]

---

6) Ursula von der Leyen, "Political Guidelines for the Next European Commission 2019-2024: A Union that Strives for More", Commission Européenne, 2019, p. 13.

7) Commision Européenne, "Proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle", Commision Européenne, <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0206>, 검색일: 2025. 8. 4.

8) 이 법안의 완전한 명칭은 "유럽의회와 유럽이사회의 인공지능(인공지능 법제)에 관한 조화된 규칙을 마련하고, 유럽연합의 일부 입법 행위를 개정하는 규정안(Proposition de Règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'union)"이다.

9) Christiane Wendehorst & Yannic Duller, "Biometric recognition and behavioural detection", European Parliament, 2021, pp. 1-101.

10) IMCO, 'la Commission du marché intérieur et de la protection des consommateurs'의 줄임말.

11) LIBE, 'la Commission des libertés civiles, de la justice et des affaires intérieures'의 줄임말.

12) 브란도 베이페이(Brando Benifei, IMCO 소속)와 드라고시 투도라케(Dragoş Tudorache, LIBE 소속).

13) 최초 법안 제안서 내 AI 시스템에 대한 정의인 "부속서 I에 열거된 하나 이상의 기법 또는 접근법을 기반으로 개발된 소프트웨어로서, 인간이 정의한 일련의 목적을 바탕으로 콘텐츠, 예측, 추천, 또는 상호작용하

초안 보고서는 이후 2023년 12월 9일 EU의회, 이사회, EU집행위원회 3자 간 협상이 종료되기 전까지 총 808번 내용이 수정되어 보완되었다.[14] 이러한 긴 합의안 도출을 위한 시간이 흐른 끝에 2024년 3월 13일 본회의에서 최종 법안이 통과되었다. 이어 5월 21일 이사회가 최종 승인하고 6월 13일 공식 서명을 완료하였으며, 7월 12일 세계 최초의 AI 법이 EU 관보에 게재되었다.

2.2. 규범적 기초: 예방주의 원칙(Le principe de précaution)

EU AI 법의 규범적 원리는 '예방주의 원칙'이다. 유럽의회는 2017년 결의에서 로봇, AI 기술의 상용화 전환과 실증 테스트가 예방주의 원칙에 따른 안전 평가 이후에만 허용되도록 집행위원회에 권고한 바 있으며,[15] 2020년 결의에서는 AI·로보틱스 규제의 핵심 원리로 예방주의 원칙을 제시하고 인간 중심, 권리 보호를 토대로 고위험 사용의 사전평가와 감독을 요구하도록 집행위원회에 재차 권고하였다.[16] 예방주의 원칙의 기원은 독일 혹은 스웨덴으로 보는 견해가 공존한다.[17] 1970년 독일 연방 정부는 공기, 소음, 진동 등 다양한 오염원으로 야기되는 피해를 사전에 방지하고자 하는 최초의 입법 초안을 마련하였으며, 이는 세대 간 책임과 생태적 윤리를 반영하려는 입장에서 추진되었다.[18] 해당 초안은 이후 입법 과정을 거쳐 1974년 정식 법률로 제정되었다.

프랑스에서 예방주의 원칙은 1990년대 후반 과학기술의 불확실성과 사회적 불안이 고조되면서 공적 담론의 핵심 주제로 등장하였다. 1995년에 제정된 바르니에 법(Loi Barnier)[19]은 '예방'(prévention)이 아닌 '예방주의'(précaution) 원칙에 근거한 법률이다. 프랑수와 에왈드(François Ewald)는 예방과 다른 '예방주의'를 구분한다. 아래는 '예방주의'의 핵심적 의미를 담고 있는 부분이다. '예방'이 인과관계가 명확하고 피해(결과) 내용이 파악될 때 사전에 방지하는 조치라면, '예방주의'는 현재 인간 지식의 수준에서 원인과 사이의 불확실성, 현저한 시간 지연, 장기적 결과, 결과의 비가역성이 존재할 때 위험을 앞질러 개입하는 규범 원리이다. 아래 내용은 예방주의 개념을 설명하는 부분이다:

> 예방주의 가설이 안전 문제에 도입한 새로운 차원 가운데 하나는 시간의 요소이다. 예방주의의 불확실성은 주로 원인과 유해한 결과의 발현 사이에 존재하는 시차, 즉 두 지점 사이의 현저한 지연에서 비롯된다. 예방주의 가설은 시간의 확장에 대한 자각, 그리고 인간 행위의 인과성 속에서 지속성을 새롭게 고려하는 것과 맞물려 있다. 이는 사고 가설(l'hypothèse de l'accident)에서는 상정되지 않는 상황으로, 사고는 본래 원인과 결과의 동시성이나 근접성으로 특징지어지기 때문이다.[…] 예방의 태도가 지식의 진실성을 보장하는 앎과의 관계를

는 환경에 영향을 미치는 결정과 같은 산출물을 생성할 수 있는 시스템을 말한다."에서 '인간이 정의한 일련의 목적을 바탕으로'가 삭제되었다. 미래에 AI가 AI에게 목적을 위임하는 기술의 진화까지 고려한 것으로 파악된다.

14) Parlement Européen, "Rapport sur la proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle (Législation sur l'IA) - Amendements 808-808, doc. A-9-2023-0188-AM-808-808, 14 juin 2023", Parlement Européen, <https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_FR.pdf>, 검색일: 2025. 7. 22.

15) European Parliament, Resolution of 16 February 2017 on Civil Law Rules on Robotics, 2015/2103(INL), Official Journal of the European Union, C 252/244.

16) Framework of ethical aspects of artificial intelligence, robotics and related technologiesEuropean Parliament resolution of 20 October 2020 with recommendations to the Commission on a frameworkof ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), Official Journal of the European Union, C 404/67.

17) La commission mondiale d'éthique des connaissances scientifiques et des technologies, "Le principe de précaution", l'ONU, 2005. p. 9.

18) Id., pp. 9-10.

19) Loi n° 95-101 du 2 février 1995, Loi relative au renforcement de la protection de l'environnement.

> 전제로 하지만, 예방주의의 가설은 가장 교묘하게 기만하는 악령(데카르트가 말한 malin génie)마저도 늘 곁에 두어야 할 동반자로 삼도록 요구한다.[20]

예방주의 원칙은 EU AI 법 설명문 26이 명시하고 있는 '위험기반' 접근으로 위험의 강도와 범위에 따라 금지, AI 시스템에 대한 요건, 운영자들의 의무과 시스템의 투명성 의무로 제도 속에서 구체적 적용되고 있다.[21] 예를 들어 딥페이크는 합성물임을 알 수 있게 하는 표시 의무 같은 투명성 의무를 통해 위험을 방지하는 '제한적 위험'으로 분류된다. 이것은 정보 제공으로 위험이 완화 관리될 수 있고 책임 추적 가능성이 확보된다고 보기 때문이다. 반면, 생체식별의 경우, 법 집행을 목적으로 공개적으로 접근 가능한 공간에서 실시간 원격 생체식별 시스템은 원칙적으로 금지 대상이다. 이 시스템은 만약 금지 대상이 되지 않을 경우, 감시, 추적 등 기본권 침해를 가져오며 그 피해는 심각하다고 판단되기 때문이다. 같은 맥락에서 감정인식에 사용되는 AI 시스템은 '고위험'으로 분류되는데, 이러한 기술은 전 생애주기 위험관리, 고품질 데이터 및 데이터 거버넌스, 활동기록, 상세 문서화, 명확한 사용자 정보 제공, 인적 감독, 정확성, 견고성, 보안성 기준 등 엄격한 기준을 통과해야 한다.[22] 다음 장에서는 예방주의 원칙이 어떻게 기본권의 영역인 초상권 보호와 관련되어 규범의 기초 원리로 적용되고 있는지 알아보기 위해 설명문, 적용 범위, 용어 정의의 개념적 층위와 구체적 의무 조항을 중심으로 검토하고자 한다.

3. EU AI 법의 초상권 보호 해석

EU AI 법은 총 180개의 설명 각서, 총 113개의 설명문, 13개의 부속서로 구성되어 있다. 제1장부터 제13장까지로 구성된 이 법은 제1장 법령의 기본적이고 포괄적 규정을 담은 총칙, 제2장 금지된 AI 관행, 제3장 고위험 AI 시스템, 제4장 특정 AI 시스템 제공자와 배포자의 투명성 의무, 제5장은 범용 AI 모델, 제6장 혁신 지원을 위한 조치, 제7장 거버넌스, 제8장 고위험 AI 시스템을 위한 EU 데이터베이스, 9장 출시 후 모니터링, 정보공유와 시장감독, 제10장 행동 강령 및 지침, 제11장 권한 위임 및 위원회 절차, 제12장 벌칙 그리고 제13장 최종규정으로 구분되어 있다.

3.1. 설명문, 제2조(적용 범위), 제3조(용어 정의)

초상권은 유럽연합 기본권 헌장 제7조(사생활과 가족생활의 존중)[23] 및 제8조(개인정보 보호), 프랑스 민법 제9조를 통해 기본권의 한 부분으로서 보호되고 있다.[24] 초상권은 개인의 얼

---

20) François Ewald, "Philosophie de la précaution", *L'année sociologique*, Vol.46 No.2(1996), pp. 401-402.

21) U AI 법 설명문(26): "AI 시스템에 대해 비례적이고 효과적인 구속 규정의 체계를 도입하기 위해서는, 명확히 정의된 위험기반 접근을 따라야 한다. 이러한 접근은 AI 시스템이 야기할 수 있는 위험의 강도와 범위에 맞추어 규정의 유형과 내용을 조정해야 한다. 따라서 용납할 수 없는 일부 AI 관행을 금지하고, 고위험 AI 시스템과 관련된 요건 및 해당 운영자들의 의무를 정하며, 아울러 특정 AI 시스템에 대해서는 투명성 의무를 부과할 필요가 있다."

22) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (Texte présentant de l'intérêt pour l'EEE), article 9.

23) "Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications", "Toute personne a droit la protection des données à caractère personnel la concernant": Charte des droits fondamentaux de l'Union européenne, article 7 & 8.

24) "Chacun a droit au respect de sa vie privée": Code civil français, article 9.

굴·신체 이미지 및 생체정보(생체식별자 포함)를 당사자의 동의나 적법한 근거 없이 수집, 이용, 전달, 영리적 활용하는 행위로부터 보호하는 자기결정권으로, 인격권의 한 유형이다. EU AI 법은 설명문, 적용 범위, 용어 정의 및 규범 체계를 통해 AI 기술의 위험에 따른 규제를 달리 적용하고 있다. 우선 설명문에서는 AI의 개발과 사용이 산업과 사회 다방면에 유익한 결과를 가져올 수 있음을 명시한다(설명문 4). 그러나 AI의 개발과 사용은 구체적 적용, 사용, 기술 개발 수준에 관한 상황에 따라 EU 법률이 보호하는 공익과 기본권에 위험 및 피해를 초래할 수 있다고 명시한다(설명문 5).

설명문 7은 직접 '공중 보건, 안전 및 기본권'을 언급하면서 이를 수호하기 위해 고위험 AI 시스템에 대한 공통 규칙을 마련해야 함을 설명하고 있다.[25] 얼굴, 사진, 음성 등 개인의 초상권은 사생활 보호에 해당하며, 이 사생활 보호는 모든 개인의 배타적 기본권의 핵심 요소이다.[26]

설명문 16, 17, 18은 각각 '생체분류', '원격 생체식별 시스템', '감정인식 시스템'을 설명하고, 기본권 침해가 아닌 경우와 침해 가능성을 구분하고 있다. 기본권 침해 대상이 아닌 경우는 AI 기술이 서비스 안에 보조 기능으로 사용되는 경우이다. 설명문 17은 원격 생체식별 시스템을 "특정 기술·절차·생체 데이터의 유형과 무관하게, 개인의 적극적 참여 없이 일반적으로 원격에서 그 개인의 생체정보를 참조 데이터베이스와 비교하여 자연인을 식별하도록 설계된 인공지능 시스템"[27]으로 규정한다. 원격 생체식별 시스템이란 '실시간' 및 '실시간에 가까운' 시스템 모두를 포함한다고 밝히고 있으며, 더불어 정보 수집과 분석이 사후에 일어나는 '사후적' 원격 생체식별 시스템까지 설명하고 있다. 설명문 17은 '실시간', '실시간에 가까운', 그리고 '사후적' 원격 생체식별 시스템 모두 원칙적으로 기본권을 침해하는 시스템으로 파악하고 있음을 알 수 있다(반면 개인이 특정 서비스에 접근하기 위해 실행하는 '인증'의 경우는 사생활 침해의 심각성이 낮다고 파악한다).[28]

설명문 18은 '감정인식 시스템'을 사람의 안면 인식을 통해 감정이나 의도를 파악하는 AI 시스템으로 정의한다. 감정인식 시스템은 EU AI 법 부속서 3(Annex Ⅲ)에서 명시한 기본권에 중대한 위해와 관련된 '고위험'에 해당한다. 고위험 AI 기술은 예방주의 원칙이 금지 대상 다음으로 강도 높게 적용되는 기술로서, 사전 규제, 사용상의 의무 등이 철저히 적용된다. 설명문 28은 인공지능을 활용한 조작, 착취의 오용 가능성을 경고하면서 기본권 침해 가능성을 명시하고 있다고 해석된다.

설명문 134는 실존 인물의 얼굴, 목소리, 행동을 정교하게 모방하여 제작된 딥페이크 콘텐츠에 대한 규제, 그 예외 사항에 관한 내용이다. 이 기술은 실존 인물의 얼굴, 목소리, 행동을 동의 없이 모방하여 진실인 것처럼 변형, 조작하는 것이기에 콘텐츠에 대한 정보를 의무적으로 공개해야 한다. 이때 정보 공개 의무는 해당 콘텐츠가 AI 기술로 만들어졌거나 실제가 아닌 조작된

25) EU AI 법 설명문(7): "건강, 안전 및 기본권과 관련된 공익 보호 수준의 일관성과 고도화를 보장하기 위해, 고위험 인공지능 시스템에 대해 공통 규칙을 수립하는 것이 타당하다."

26) "모든 사람은, 그의 지위, 출신, 재산, 현재 또는 장래의 직무와 관계없이, 자신의 사생활 존중을 받을 권리를 가진다.[…]더 나아가, 사생활을 침해하는 내용을 설명하기 위해 인물의 사진을 게재하는 것은 필연적으로 그 인물의 초상권을 침해하는 것이다.", Cour de cassation, Première chambre civile, 27 février 2007, n° 06-10393.

27) EU AI 법 설명문(7).

28) EU AI 법 설명문(7): "실시간(real-time)' 시스템의 경우, 생체정보의 포착, 비교, 그리고 식별이 모두 즉시, 거의 즉시, 또는 어쨌든 유의미한 지연 없이 이루어진다. 이와 관련하여, 경미한 지연의 가능성을 고려하더라도, 본 규정이 정한 '실시간' 사용 규정을 회피하지 못하도록 하는 것이 필요하다. 실시간 시스템은 카메라나 유사 기능을 가진 장치 때문에 생성되는 '라이브 영상'이나 '약간의 지연이 있는 영상'(예: 비디오 시퀀스)의 사용에 기반한다. 반대로, '사후적' 시스템의 경우에는, 생체정보가 우선적으로 수집된 뒤 일정한 시간적 지연이 지난 후에야 비교 및 식별이 이루어진다. 여기에는 CCTV나 개인 장치 때문에 사전에 생성된 이미지나 비디오 시퀀스와 같은 자료가 포함되며, 해당 자료는 이후에 해당 자연인에 대한 시스템 적용 과정에서 사용된다."

것임을 밝히는 것으로 한정되며, 콘텐츠의 감상, 활용, 창작의 자유를 방해해서는 안 된다고 규정하고 있다. 비윤리적인 딥페이크 기술 사용에 대한 규제가 표현의 자유 문제와 충돌할 수 있기 때문이다.[29]

EU AI 법 제2조는 적용 범위이다. 규제 대상은 공급자(제조사), 배포자(사람 혹은 조직), 수입자 및 유통업자, 공급자의 대리인 등이다. 예를 들어 한국 기업 A가 딥페이크 생성 AI 서비스를 제공하여 프랑스 사용자가 이 서비스를 이용해 유명인의 얼굴 이미지를 생성하여 소셜미디어(SNS)에 게시하면, 이 경우 한국 기업 A는 EU AI 법 규제 적용 대상이 된다. 제2조 7항은 EU AI 법이 기존 EU 정보보호에 관한 일반 규정(le règlement (UE) 2016/679),[30] EU 기관, 기구 자체의 데이터 보호 규정(le règlement (UE) (2815/1725)[31], 전자통신 분야에서 개인정보 보호 지침(la directive 2002/58/CE)[32], 경찰, 검찰, 사법 당국이 처리하는 개인정보 보호를 규율하는 지침(UE) 2016/680)[33]에 영향을 미치지 않음을 명시하고 있다. 즉, EU AI 법은 기존 법을 대체하거나 우선하는 특별법이 아니라 그러한 법률에 추가되는 규제이다.

제3조는 용어 정의 부분이다. 적용 범위에 이어 제3조의 '생체정보', '생체인식', '딥페이크', '생체식별', '실시간 생체인식 시스템'은 기본권 침해와 직접 연관되는 기술이다. 우선 제34항은 '생체정보'를 "특정한 기술적 처리 과정에서 생성된 개인정보로서 개인의 얼굴 이미지 또는 지문 정보 같은 자연인의 신체적, 생리적 또는 행동적 특징과 관련된 정보"[34]로 규정한다. 생체

29) EU AI 법 설명문(134): "[…]인공지능 시스템을 활용하여 사람, 사물, 장소, 단체 또는 실제 사건과 상당히 유사하게 보이는 이미지나 음성·영상 콘텐츠를 생성하거나 조작하는(소위 '이페르트뤼카쥬') 배포자는, 해당 콘텐츠가 인공지능에 의해 생성되거나 조작되었음을 명확하고 식별할 수 있게 표시하여 인공지능 산출물임을 명시하고 그 인위적 기원을 밝혀야 한다. 이러한 투명성 의무의 준수는 해당 인공지능 시스템의 사용이나 그것이 산출하는 결과물이 헌장(기본권 헌장)이 보장하는 표현의 자유 및 예술·과학의 자유를 침해한다고 해석되어서는 안 된다.[…]공익적 정보 전달을 목적으로 게시되는 AI 생성 텍스트에 대해서도 유사한 표시 의무가 필요하며, 단, 해당 콘텐츠가 사람에 의한 검토나 편집을 거쳤고, 실질적으로 출판에 대한 책임 주체가 명확한 경우에는 이 의무에서 제외될 수 있다."

30) 유럽의회와 유럽이사회의 2016년 4월 27일자 규정(EU) 2016/679-개인정보 처리와 관련하여 자연인의 보호 및 해당 데이터의 자유로운 이동에 관한 규정, 그리고 지침 95/46/EC(정보보호에 관한 지침)를 폐지하는 규정(정보보호에 관한 일반 규정(GDPR)(RÈGLEMENT (UE)2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

31) 유럽의회와 유럽이사회의 2018년 10월 23일자 규정-유럽연합 기관, 기구, 조직들에 의한 개인정보 처리에 관하여 자연인의 보호와 해당 정보들의 자유로운 이동에 관한 규정, 그리고 유럽공동체 규정 제45/2001과 제1247/2002/ 결정을 폐지하는 규정(RÈGLEMENT (UE)2018/1725 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE).

32) 유럽의회와 유럽이사회의 2002년 7월 12일자 2002/58/EC지침-전자통신 분야에서 사생활의 보호와 개인정보 처리에 관한 지침(사생활 및 전자통신 지침)(DIRECTIVE 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

33) 유럽의회와 유럽이사회의 2016년 4월 27일자 지침(EU)2016/680—형사범죄의 예방 및 탐지, 수사 및 기소, 형사 제재의 집행을 목적으로 관할 당국이 수행하는 개인정보 처리와 관련하여 자연인의 보호와 해당 정보의 자유로운 이동에 관한 지침, 그리고 이사회 기본결정 2008/977/JAI를 폐지하는 지침(DIRECTIVE (UE)2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil).

34) EU AI 법 제3조 제34항: "«données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, telles que des images faciales ou des données dactyloscopiques;".

정보는 고도의 AI 기술을 통해 채집되어 인식되며, 이때 얼굴 이미지나 지문 정보는 사전 동의 없이 부지불식 간에 다른 목적으로 수집 활용될 수 있는 기본권 침해의 핵심을 이룬다. 제35항은 '생체인식'을 "한 개인의 신체적·생리적·행동적 또는 심리적 특성을 데이터베이스에 저장된 다른 개인의 생체정보와 비교를 통해 알아보는 자동화된 인식"[35]으로 규정한다. 생체인식은 다수의 생체정보와 비교하는 과정을 반드시 거치므로 그 자체로 기본권 침해, 초상권 침해를 내포한다. 따라서 생체인식 과정은 대상자가 반드시 이를 인지할 수 투명한 절차가 있어야 한다.

설명문 17에 이어 제41항, 제42항은 각각 '원격 생체식별 시스템', '실시간 원격 생체식별 시스템'을 다시 정의하고 있다. 원격 생체식별 시스템은 "특정 자연인을 능동적 참여 없이, 일반적으로 원격에서 식별하기 위하여 그 사람의 생체정보를 데이터베이스에 수록된 다른 생체정보와 비교하는 데 사용되는 인공지능 시스템"[36]을 가리킨다. '실시간 원격 생체식별 시스템'은 예방주의 원칙이 가장 강하게 적용된 분야로, 전면 금지 기술이다. 공공장소에서의 실시간 생체식별 장치는 감시, 추적 기능으로 변질되어 활용될 소지가 있으며, 그 피해는 돌이킬 수 없을 만큼 중대하기 때문이다.

설명문 134에 이어 제60항은 딥페이크를 다시 정의한다. 딥페이크는 "AI에 의해 생성되거나 조작된 이미지, 오디오 또는 비디오 콘텐츠로서, 기존의 인물·사물·장소·실체 또는 사건과 유사성을 띠며, 개인이 이를 진실하거나 사실적인 것으로 오인할 수 있는 것"[37]을 가리킨다. 요컨대, EU AI 법은 설명문, 적용 범위, 용어 정의라는 다중 층위를 마련하여 기본권 침해와 직결되는 개념군을 정밀하게 한정하고 있다. 이러한 법률의 구조는 권리 보호를 위한 해석 시 이견을 줄이고 명확한 집행 가능성을 높이는 효과가 있다. 다음 절에는 기본권 보호와 관련된 전면 금지 대상, 고위험 AI 시스템 개발자, 배포자에 대한 의무 체계를 구체적으로 살펴보고자 한다.

3.2. 금지된 행위, 고위험 AI 시스템 개발자, 배포자에 대한 의무 규정

제5조는 '인공지능 분야의 금지된 행위들'을 열거하고 있다. 제5조는 인간의 존엄, 자유와 민주주의, 사생활과 개인정보 보호, 차별 금지와 평등 등 EU 핵심가치, 기본권을 구조적으로 침해하는 사용을 원천적으로 차단하는 규정으로, EU AI 법이 근거하는 예방주의 규범 철학이 가장 강하게 구현된 부분이다. 구체적으로 인터넷, CCTV 등에서의 비선별적 얼굴 이미지 스크래핑을 통한 안면 인식 데이터베이스 생성, 확대, 직장, 교육환경에서의 감정인식, 생체정보를 이용하여 민감한 특성을 추론, 분류하는 생체범주화, 개인에게 사회적 점수를 부여하는 사회적 신용평가가 이에 해당한다.

제5조 제1항의 (e)는 인터넷 또는 영상감시(예를 들어 CCTV)로부터 얼굴 이미지를 비선별적으로 수집하여 안면인식 데이터베이스를 생성, 확대하는 AI 시스템을 시장에 출시하고 이러한 특정 목적을 위해 가동하거나 사용하는 것을 금지한다. 현대 사회에서 인터넷을 이용하지

35) EU AI 법 제3조 제35항: "«identification biométrique», la reconnaissance automatisée de caractéristiques physiques, physiologiques, comportementales". ou psychologiques humaines aux fins d'établir l'identité d'une personne physique en comparant ses données biométriques à des données biométriques de personnes stockées dans une base de données; ".

36) EU AI 법 제3조 제41항: "«système d'identification biométrique à distance», un système d'IA destiné à identifier des personnes physiques sans leur participation active, généralement à distance, en comparant les données biométriques d'une personne avec celles qui figurent dans une base de données;".

37) EU AI 법 제3조 제60항: "«hypertrucage», une image ou un contenu audio ou vidéo généré ou manipulé par l'IA, présentant une ressemblance avec des personnes, des objets, des lieux, des entités ou événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques;".

않거나, CCTV 시스템이 없는 공간을 찾기란 거의 불가능하다. 무차별 스크래핑은 인과의 불확실성, 발현 시점의 시간 지연, 원자료 유출로 인해 심각한 인권 침해가 분명히 예측된다는 점에서 가장 강력한 예방주의 원칙이 적용되었음을 확인할 수 있다. 다시 말해 비선별적으로 얼굴 이미지를 수집하여 데이터베이스를 생성, 확대하는 AI 시스템은 피해 발생 시점의 불확실성, 시간 지연, 돌이킬 수 없는 위험을 고려하여 금지 대상에 속함을 알 수 있다. 또, 공중이 접근 가능한 장소에서 '실시간 원격 생체식별 시스템'은 특정한 목적을 제외하고 금지된다(가령 법 집행 목적). 이는 제5조 제1항의 (h)의 규정으로, 실시간 원격 생체식별 시스템은 익명의 대중을 감시하는 데 활용될 가능성이 예견되며 그 피해는 중대하기 때문이다.

제26조는 고위험 AI 시스템의 배포, 사용 단계에서 예방주의 원칙이 적용되도록 설계된 규정이다. 핵심은 권한을 가진 인간 감독에 의해, 구체화되고 있는 부분이다. 핵심 내용은 배포자가 고위험 AI 시스템을 지침 대로, 사람의 감독 아래, 기록, 보고, 투명성을 갖추어 사용하고, 위험 징후가 있으면 즉시 중단, 통지해야 한다는 사실이다. '고위험 AI 시스템'은 앞선 제6조의 제2항에서 언급한 부속서 3의 규정에 따라, 원격 생체식별 시스템, 고용, 노동, 인사관리 등 특정 사용 영역에서 활용되는 AI 시스템을 가리킨다. 제26조의 1항에 따라 고위험 AI 시스템 배포자는 해당 시스템에 첨부된 사용 지침을 준수하고 적절한 기술적, 조직적인 보완책을 마련해야 할 의무를 진다. 예를 들어 고위험 AI 시스템이 생체식별, 얼굴 인식, 감정인식의 기능을 포함한다면, 해당 시스템 배포자는 이 조항에 따라 사용 목적과 범위를 명확히 하고 개인정보 침해가 발생하지 않도록 관리와 책임을 다해야 한다.

제26조 제2항은 고위험 AI 시스템 배포자가 충분한 전문성과 권한을 갖춘 사람이 시스템을 통제할 수 있도록 요구하고 있다. 즉, 고위험 AI 시스템에 대한 감독은 고도로 지능화된 AI 기술로 이루어지는 것이 아니라 인간에 의해 이루어져야 한다. 요컨대 2항은 기본권 침해와 관련한 경우 인간 감독자의 전문성, 개입 권한의 수준을 높여 사전 차단 능력을 강화하는 법의 취지가 반영된 것으로 해석된다. 제4항은 고위험 AI 시스템 배포자는 다양한 인종, 성별, 연령을 반영하는 대표성 있는 학습 데이터를 확보할 의무를 지닌다. AI 시스템이 특정 집단에 편중된 데이터를 활용할 경우, 얼굴 오인식, 차별적 분류의 가능성을 높이고 불명예스러운 맥락에서 얼굴 이미지가 노출될 가능성이 크고 이것은 기본권 침해와 관련된다. 데이터 편향은 양상이 불확실하지만 피해는 크고 돌이킬 수 없다는 점에서 이러한 위험은 설계 단계가 아닌 배포, 사용 단계에서도 관리 되도록 하고 있다. 이어 제6항은 고위험 AI 시스템 배포자의 로그 보관 의무를 규정한다. 배포자는 자신의 관리 범위 내에서 시스템이 자동 생성하는 로그를 의도된 목적에 비례하여 최소 6개월 이상 보관해야 한다. 제7항은 직장에서 고위험 AI 시스템을 가동, 사용하기 이전에, 배포자는 근로자 대표 및 관련 근로자에게 사전 고지 의무를 부과한다. 특히 고위험 AI 시스템이 근로자의 얼굴 인식, 감정 추정 등 비윤리적 목적으로 활용되어서는 안 되므로 당사자들의 참여적 감시가 이루어지도록 하고 있다. 요컨대, 6항, 7항의 추적 가능성, 절차적 투명성은 배포, 사용 단계에서 예방주의 원칙을 내재화하고 있는 것으로 해석된다.

제50조는 특정 AI 시스템 제공자 및 배포자에 대한 의무이다. '특정 AI 시스템'이란 고위험 AI 시스템으로 분류되지는 않지만 "별도의 투명성 의무가 있는 시스템"이며, 이러한 시스템에 대한 별도의 특별한 의무를 간과할 경우, 예상치 못한 위험이 야기될 수 있는 시스템을 말한다. 특정 AI 시스템은 첫째, 인간과 직접 상호작용하는 AI 시스템, 둘째, 합성 콘텐츠(오디오, 이미지, 비디오, 텍스트) 생성 AI 시스템, 셋째, 감정인식 또는 생체분류 AI 시스템, 마지막으로 딥페이크에 해당하는 이미지, 음성 또는 영상 콘텐츠를 생성하거나 조작하는 AI 시스템이다. 요컨대, 특정 AI 시스템 제공자는 AI와의 상호작용 및 합성·조작 사실을 식별할 수 있게 명시하고 관련 정보를 충분히 공개하며, 특정 AI 시스템 배포자는 관련자에게 사전 고지와 식별 표시를 이행하

여 추적, 검증 가능성을 확보하여, 제한 위험 영역에서도 사전 예방적 통제가 이루어지도록 해야 한다.

4. 프랑스의 EU AI 법 대응: 'CNIL-SREN법' 이중 트랙

프랑스는 EU AI 법에 대응하여 행정 집행체계, 입법 체계가 병렬로 작동하는 이중 트랙을 마련하였다. 앞서 검토한 대로 EU AI 법은 예방주의 원칙 철학에 따라 위험의 수준을 고려하여 해당 조치를 요구하고 있다. 프랑스는 이에 상응하여 CNIL의 감독과 제재, SREN법 기반의 온라인 침해 대응 체계를 결합함으로써 기본권의 하나로서의 초상권을 다층적으로 보호하고 있다.

4.1. 국가정보자유위원회(CNIL)의 역할

국가정보자유위원회(Commission Nationale de l'Informatique et des Libertés, 이하 CNIL)는 1978년에 제정된 '정보기술, 파일 및 자유에 관한 법'[38]에 근거하여, 정보기술의 발전이 시민의 자유와 기본권을 침해하지 않도록 감시하고 규제하는 독립 행정기관이다. 2018년 5월 25일부터 발효된 EU 정보보호에 관한 일반 규정이 유럽연합 회원국 전체에 적용되면서 프랑스는 이에 대응하여 1978년 제정된 정보기술, 파일 및 자유에 관한 법을 개정하였다. 그러한 배경에서 실질적으로 시민의 개인정보 보호, 기업 및 공공기관이 준수해야 할 지침을 제공해 온 기관이 바로 CNIL이다.

2023년 1월 CNIL은 AI 및 혁신 기술 발전에 대응하여 'AI 서비스'(service de l'intelligence artificielle, 이하 SIA)를 신설하였다.[39] 목적은 EU AI 법 발효에 따른 AI 시스템 관리 감독 강화, 사생활 침해 위험에 대한 이해 강화 및 시민 차원 확산이다. SIA의 주요 임무는 크게 4가지이다. 첫째, 시민을 대상으로 한 AI 시스템의 작동 방식과 초상권 침해 기술에 대한 이해 확산, 둘째, 초상권 침해와 직결되는 고위험 AI 시스템이 처리하는 생체정보(얼굴, 음성 등)에 대한 법적·제도적 능력을 강화, 셋째, EU AI 법의 국내 시행 준비 넷째, AI 생태계를 구성하는 산업계, 연구기관, 시민 사회와의 협력 및 연대 강화이다.

CNIL은 2015년 무렵부터 디지털 혁신연구소 LINC(Laboratoire d'innovation Numérique de la CNIL, 이하 LINC)[40]를 운영해오며 시민들이 접근할 수 있는 자료들을 발간, 제공해 왔다. LINC의 운영은 AI 기술 문화 관련 정보를 시민 사회에 확산시키는 데 크게 이바지하였다.

중요한 사실은 CNIL이 EU AI 법이 제정되는 과정에 보이지 않지만 큰 영향을 미쳤다는 점이다. CNIL은 2019년 개인정보 처리와 관련하여 당사자의 권리와 자유에 위험이 발생할 것을 우려하여 모든 기업과 공공기관을 대상으로 RGPD법 제25조, '정보기술, 파일 및 자유에 관한 법', EU 기본권 헌장 제8조(가족과 사생활 존중)[41]에 근거하여 '개인정보 영향평가'[42]를 문서로 만들었다. 그리고 이를 관련 주체들에게 알리며 책임 있게 운영하도록 감독하였다는 사실이

38) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
39) CNIL, "Création d'un service de l'intelligence artificielle : la CNIL lance ses travaux sur les bases de données", CNIL, <https://www.cnil.fr/fr/creation-dun-service-de-lintelligence-artificielle-la-cnil-et-lancement-des-travaux-sur-les-bases-de>, 검색일: 2025. 7. 31.
40) LINC, "ChatGPT: un beau parleur bien entraîné", CNIL, <https://linc.cnil.fr/dossier-intelligence-artificielle>, 검색일: 2025. 8. 3.
41) Charte des droits fondamentaux de l'Union européenne, article 8: "Toute personne a droit à la protection des données à caractère personnel la concernant".
42) Data Protection Impact Assessment, 즉 l'AIPD.

다.[43] 이어 2021년 6월 18일 CNIL은 EU 내 동급 기관들, 유럽 정보보호 위원회[44]와 함께 AI 법안에 대한 의견서를 채택하여 미래의 AI 법 제정에 영향을 미쳤다.[45] 더 나아가 2022년 LINC를 통해 발간한 'AI 시스템 보안 보고서'[46]는 2023년 SIA 신설 이전 CNIL이 EU AI 규제 입법 과정에 실질적 영향을 미쳤음을 시사한다. 종합하자면 프랑스가 유럽연합 내 강력한 입법 제안국가라는 사실과 함께 이루어진 CNIL의 중요한 활동들은 EU AI 법이 마련되는 과정에 영향을 미쳤다. 또한, CNIL은 SREN법, 즉 '디지털 공간의 규제와 보안에 관한 법률'[47] 제정에 체계화된 지식을 제공하며 법 제정에 직, 간접적 영향을 미쳤다.

4.2. 초상권 보호 관련 입법: SREN법

2024년 5월, CNIL은 공식 인터넷 홈페이지를 통해 "디지털 공간 규제 및 보안 법률, 일명 'SREN법'이 CNIL에게 새로운 임무를 맡김으로써 인터넷 사용자들을 보호하는 역할을 강화하다"[48]라고 밝혔다. SREN법은 프랑스 정부 초안 마련, 2024년 4월 10일 국회에서 최종 채택, 5월 21일 법률로서 공포, 최종적으로 5월 22일 관보에 게재되어 공식적으로 효력이 발생하였다. SREN법은 국회에 통과되기까지 일부 국회의원들이 인터넷상에서 과도하게 표현의 자유, 정보 접근권을 제한한다는 의견을 내며 합의점에 이르는 데 진통을 겪은 디지털 공간의 안전 규제법이다. SREN법은 2022년 EU의 플랫폼 책임 강화, 불법콘텐츠 대응, 알고리즘 투명성, 딥페이크에 대응하기 위해 개정한 일명, '디지털 서비스법'[49]에 대응하여 프랑스가 국내 차원에서 관련 범죄를 예방하기 위해 마련한 법이다.

SREN법은 총 5개 절로 구성된다. 그중 인터넷상 미성년자 보호와 연령 인증(제1조부터 6조까지), 디지털 환경에서 시민 보호(제7조부터 25조까지), 데이터 경제에서 신뢰 및 경쟁과 신뢰 강화(제26조부터 39조까지) 등이 그 주요 내용이다. 핵심 조항은 제7조부터 제25조에 이르는 디지털 환경에서 시민 보호 내용이다.

구체적으로 살펴보면 제15조는 개인의 초상권을 침해한 자를 처벌하는 형법 226-8조를 수정한 조항이다. 제15조는 형법 제226-8조를 수정하여 개인의 초상권 침해 행위를 처벌하는 조항으로, "형법 제226조-8은 다음과 같이 개정한다. 1항은 다음과 같이 수정한다. a) "게시하다"라는 단어는 "대중 또는 제3자에게 알리는 행위"로 대체한다."[50]를 명시하고 있다. 또, "b) 다음과 같이 작성된 문장이 추가된다: 알고리즘으로 생성된 시각적 또는 청각적 콘텐츠로서 어떤

43) CNIL, "Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD)", CNIL, <https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd>, 검색일: 2025. 8. 3.

44) le Comité européen de la protection des données(CEPD).

45) CNIL, "Intelligence artificielle : l'avis de la CNIL et de ses homologues sur le futur règlement européen", CNIL, <https://www.cnil.fr/fr/intelligence-artificielle-lavis-de-la-cnil-et-de-ses-homologues-sur-le-futur-reglement-europeen>, 검색일, 2025. 8. 2.

46) LINC, "Dossier Sécurité des systèmes d'IA", CNIL, <https://linc.cnil.fr/sites/linc/files/atoms/files/linc_cnil_dossier-securite-systemes-ia.pdf>, 2022, 검색일, 2025. 8. 3.

47) LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

48) CNIL, "La loi visant à sécuriser et réguler l'espace numérique(SREN) renforce la protection des internautes en confiant de nouvelles missions à la CNIL", CNIL, <https://www.cnil.fr/fr/sren-loi-securiser-reguler-lespace-numerique-nouvelles-missions-cnil>, 검색일, 2025. 8. 3.

49) 2022년 10월 19일 유럽이사회와 유럽의회에 의해 제정된 디지털 서비스 단일시장에 관한 2000/31/EC 지침을 개정한 2022/2065 EU 규제(Règlement (UE)2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive2000/31/CE).

50) "L'article 226-8 du code pénal est ainsi modifié : 1° Le premier alinéa est ainsi modifié : a) Le mot : « publier » est remplacé par les mots : « porter à la connaissance du public ou d'un tiers »;", LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

방식으로든 그 이미지나 음성이 특정 인물의 것임을 나타내고, 해당 인물의 동의 없이 공개되며, 그것이 알고리즘 생성물임이 명백히 드러나지 않거나 명시적으로 표시되지 않은 경우, 이 역시 현 항에서 언급된 범죄와 동일하게 간주하며 동일한 형벌이 부과된다."를 명시하고, 2항은 "동일 1항 뒤에 다음과 같은 단락을 삽입한다. "본 조에 규정된 범죄가 온라인 대중 통신 서비스를 통해 이뤄졌을 경우, 형벌은 징역 2년 및 벌금 4만 5천 유로로 가중된다."의 문단이 삽입된다"를 명시하고 있다.[51] 요컨대 SREN법 제15조는 프랑스가 디지털 환경에서 시민의 기본권, 초상권 침해를 강력하게 처벌하려는 의지를 반영한다.

SREN법은 사후 규율을 통해 불법콘텐츠 사용자 신고, 접수 후 플랫폼의 신속한 즉시 삭제 의무, 미이행 시 형사 처벌 및 과징금의 연쇄를 확립하고 있다. 즉, 개인정보와 초상권 침해 감독기관인 CNIL과 '디지털과 시청각 규제청'[52]을 통한 플랫폼 감시, 시정 명령, 접속 차단 명령 등 행정적 집행수단을 강화하였다. 한편 SREN법, EU AI 법은 각각 2024년 5월 21일, 2024년 7월 12일에 관보 게재로 효력이 확정되었으며, 입법적 경로가 상이하고 직접적인 입법 연계는 존재하지 않는 것으로 파악지만, 그렇더라도 두 규범은 기본권, 인격권 보호를 통한 초상권 보호, 딥페이크 기술에 대한 오인 위험 차단이라는 공통 목표에 수렴한다. EU AI 법이 위험기반 접근을 통해 예방주의적 통제 강도가 달리 적용되었다면, 프랑스는 이에 대응하여 SREN법과 CNIL의 이중의 트랙, 추가로 디지털과 시청각 규제청의 행정 집행수단을 결합하여 집행 가능한 수단을 배치한 것으로 볼 수 있다. 결과적으로 프랑스는 동일한 위험에 대하여 다중적 규제 체계를 마련하였다고 평가할 만하다.

5. 결론 및 시사점

EU AI 법은 예방주의 원칙에 따라 위험을 수위별로 층화하고 각 수위에 상응하는 금지, 의무, 투명성 요건을 배치함으로써 기본권 침해를 선제적으로 억제하도록 설계된 정교한 규제 체계이다. '예방주의 원칙'은 이미 그 개념을 살펴본 대로 위험의 발생 시점과 경로가 불확실하고, 잠복적, 장기적, 비가역적 피해가 예상되는 경우, 결과가 확정되지 않았더라도 사전적 억제 조치를 정당화하는 규범 철학이다. 이는 인과관계가 확인된 위험을 관리하는 '예방'과 달리, 기술 발전 과정에서 발생할 수 있는 거의 모든 예측 불가능한 피해 전반을 포괄적으로 고려하는 규범 철학이다.

EU AI 법 전반을 검토한 결과, 기본권으로서의 초상권은 설명문, 적용 범위, 용어 정의 등 규범의 개념 층위와 금지, 의무 투명성, 감독 등 구체적 준수 체계를 통해 복합적으로 보호되고 있다. 특히 실시간 생체식별 시스템, 안면 인식, 딥페이크 등 기본권이 침해 우려가 큰 AI 기술 남용, 오용 지점에 대해 신중하고 엄격한 태도를 보인다. EU AI 법은 AI 기술의 상업적, 기술적 가능성을 전면적으로 억제하기보다, 기본권 침해 위험의 고저에 따라 적용 영역을 세분화하고 그에 맞춘 위험관리에 초점을 두는 적극적 규범적 모델이다. 이러한 모델은 EU 회원국 간 AI 기술에 대한 세부 규제 수위는 상이하더라도 기본권 보호를 최우선으로 하는 공동 원칙에 대하여 내부 합의가 이루어질 수 있기 때문에 가능하다고 해석된다.

프랑스는 EU AI 법의 규범적 요구에 대응하여 'CNIL-SREN법' 이중 트랙으로 규제 체계를

51) "Après le même premier alinéa, il est inséré un alinéa ainsi rédigé :
« Ces peines sont portées à deux ans d'emprisonnement et à 45 000 euros d'amende lorsque les délits prévus au présent article ont été réalisés en utilisant un service de communication au public en ligne. »;", LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

52) Autorité de régulation de la communication audiovisuelle et numérique(ARCOM).

마련하고 있다. CNIL은 가이드라인, 감독, 조사, 제재를 통해 표시 의무 준수, 생체정보 처리의 적법성, 설명 가능성을 점검하며, 2019년 개인정보 영향평가 지침, 2021년 공동 의견서, 2022년 LINC의 'AI 시스템 보안 보고서' 제시, 2023년 AI 서비스(SIA) 신설 등으로 제도 역량을 확충하였다. SREN법은 이용자 신고, 플랫폼의 신속 삭제, 불이행 시 형사·행정 제재라는 사후 규율과 딥페이크 기술 활용 콘텐츠에 대한 표시 의무 등 플랫폼 책임을 강화하여 EU 차원의 좌표를 국내에서 집행 가능한 설계로 연결한다. EU AI 법과 SREN법은 입법 경로의 직접 연계는 확인되지 않지만 동일한 위험을 행정 집행, 플랫폼 규율이라는 서로 다른 층위에서 동시 규제함으로써 기능적 정합성을 구현하고 있다.

초상권 보호는 앞으로 살아갈 인공지능 시대에 인간의 존엄, 인격적 자율, 사적 영역을 지키는 핵심적 방어선이다. 소셜미디어를 경유한 데이터 검색, 저장, 복제가 일상화된 환경에서 개인의 음성과 얼굴 이미지는 한 개인이 인지할 수 없는 상황에서 변형, 가공되어 잠복적으로 축적된 뒤 비윤리적 방식으로 유통될 수 있다. 따라서 현재 시점에서 국내 AI 법 입법자들은 AI 기술이 가져올 유토피아적 효익에 상응하여 기본권 보호의 중대성을 인식하고, 이를 제도화하여 그 취지가 시민 사회로 확산될 수 있도록 힘써야 할 것이다. 요컨대, EU AI 법과 프랑스의 대응이 시사하는 바는 AI 기술 발전은 인간의 감독 아래 이루어져야 한다는 점이다. 프랑스의 이중 트랙은 EU AI 법의 연장선에서 사전적 감독, 법 사후적 집행을 중층적으로 결합함으로써 기본권의 영역인 초상권 침해 위험을 현실적으로 억제하는 모델로 평가할 수 있다. 향후 초상권 연구는 개인 초상에 대한 상업적 이용을 둘러싼 국가별 규율 수준, 개인의 사후 초상권, 디지털 초상권, 미성년자 초상권 침해에 대한 처벌 및 정책 등 국가별 판례 비교로 확장될 수 있을 것이다.

참고문헌

학술지(국내)

안용교, "초상권의 개념과 의의", 「언론중재」, 제3호(1982).

학술지(서양)

François Ewald, "Philosophie de la précaution", *L'année sociologique*, Vol.46 No. 2(1996).

판례

Cour de cassation, Première chambre civile, 27 février 2007, n° 06-10393.

신문기사

France 24, 「FRANCE 24 journalist impersonated in new deepfake video」, Truth or Fake, 2024. 2. 15자.

Tom Whittaker, 「EU Artificial Intelligence Act: one year on and further proposed amendments from the Committees on the Internal Market and Civil Liberties」, Burges Salmon, 2022. 4. 25자.

인터넷 자료

CNIL, "Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD)", CNIL, <https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd>, 검색일: 2025. 8. 3.

CNIL, "Création d'un service de l'intelligence artificielle : la CNIL lance ses travaux sur les bases de données", CNIL, <https://www.cnil.fr/fr/creation-dun-service-de-lintelligence-artificielle-la-cnil-et-lancement-des-travaux-sur-les-bases-de>, 검색일: 2025. 7. 31.

CNIL, "Intelligence artificielle : l'avis de la CNIL et de ses homologues sur le futur règlement européen", CNIL, <https://www.cnil.fr/fr/intelligence-artificielle-lavis-de-la-cnil-et-de-ses-homologues-sur-le-futur-reglement-europeen>, 검색일, 2025. 8. 2.

CNIL, "La loi visant à sécuriser et réguler l'espace numérique(SREN) renforce la protection des internautes en confiant de nouvelles missions à la CNIL", CNIL, <https://www.cnil.fr/fr/sren-loi-securiser-reguler-lespace-numerique-nouvelles-missions-cnil>, 검색일, 2025. 8. 3.

Commision Européenne, "Proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle", Commision Européenne, <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0206>, 검색일: 2025. 8. 4.

Jammable, "AI Dalida Voice", Jammable, <https://www.jammable.com/custom-dalida>, 검색일: 2025. 8. 6.

LINC, "ChatGPT: un beau parleur bien entraîné", CNIL, <https://linc.cnil.fr/dossier-intelligence-artificielle>, 검색일: 2025. 8. 3.

LINC, "Dossier Sécurité des systèmes d'IA", CNIL, <https://linc.cnil.fr/sites/linc/files/atoms/files/linc_cnil_dossier-securite-systemes-ia.pdf>, 2022, 검색일: 2025. 8. 3.

Parlement Européen, "Rapport sur la proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle (Législation sur l'IA) – Amendements 808-808, doc. A-9-2023-0188-AM-808-808, 14 juin 2023", Parlement Européen, <https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_FR.pdf>, 검색일: 2025. 7. 22.

Sénat, "Bicentenaire du Code pénal", Sénat, <https://www.senat.fr/colloques/actes_bicentenaire_code_penal/actes_bicentenaire_code_penal11.html>, 검색일: 2025. 8. 4.

연구보고서

Christiane Wendehorst & Yannic Duller, "Biometric recognition and behavioural detection", European Parliament, 2021.

La commission mondiale d'éthique des connaissances scientifiques et des technologies, "Le principe de précaution", l'ONU, 2005.

Ursula von der Leyen, "Political Guidelines for the Next European Commission 2019-2024: A Union that Strives for More", Commission européenne, 2019.