기본연구 | 24-02

인공지능 감시에 의한 권력의 확대와 그 규범적 대응방안 연구

문광진/허진주/전민경

2024. 10

정보통신정책연구원
KOREA INFORMATION SOCIETY DEVELOPMENT INSTITUTE

기본연구 | 24-02

인공지능 감시에 의한 권력의 확대와 그 규범적 대응방안 연구

문광진/허진주/전민경

2024. 10

KISDI 정보통신정책연구원
KOREA INFORMATION SOCIETY DEVELOPMENT INSTITUTE

서 언

최근 인공지능 기술이 빠른 성장을 보이면서, 우리 주변에서 인공지능을 활용한 감시 시스템도 점차 많이 활용되고 있습니다. 특히, 지난 2022년 10월 말 안타깝게 발생한 이태원 참사 이후, 정부는 재난안전관리 체계 전반을 개편하기 위해 지능형 CCTV 확충 및 관제센터 고도화를 포함하는 「국가 안전시스템 개편 종합대책」을 발표하기도 했습니다. 각종 대형·복합재난으로부터 국민을 안전하게 보호하기 위해 인공지능이라는 신기술의 활용 수요가 점차 늘어나고 있지만, 그로 인해 사생활의 비밀과 자유, 개인정보자기결정권, 표현의 자유 등 헌법에서 보장하는 국민의 기본권이 침해될 우려가 있는 것도 사실입니다.

감시라는 개념은 이와 같이 긍정적 의미와 부정적 의미를 동시에 내포하고 있습니다. 감시는 이러한 이중성을 바탕으로 피감시자의 신체를 억압하지 않고도 통제하고 순종하게 하면서 질서를 유지하는 권력의 메커니즘을 발휘하게 합니다. 인공지능이 권력에 관계되어 활용되는 만큼 그 규범적 대응이 매우 중요합니다.

이 연구는 정보통신정책연구원의 문광진 부연구위원이 총괄책임을 맡았으며, 영남대학교 양천수 교수, 전남대학교 홍석한 교수, 경상국립대학교 박성민 교수, 강원대학교 윤수정 교수, 한국전통문화대학교 장선미 강사, 고려대학교 김민규 연구교수, 숙명여자대학교 정애령 연구교수가 자문에 참여하여 귀중한 조언을 주셨습니다. 이 연구를 통해 진화하는 인공지능·디지털 환경 속에서 국민의 안전과 기본권을 동시에 보장할 수 있는 규범적 대응방안을 모색할 수 있기를 기대합니다.

2024년 10월

정보통신정책연구원

원장 직무대행 김 정 언

목 차

서 언 ····· 1

요약문 ····· 9

제 1 장 서 론 ····· 13

제 1 절 연구의 배경 ····· 13
제 2 절 연구의 목표 및 주요 내용 ····· 17

제 2 장 인공지능 감시와 권력 확대의 위험성 ····· 20

제 1 절 인공지능의 위험 일반 ····· 20
제 2 절 감시와 권력의 상관관계 ····· 24
1. M. Foucault의 이론과 감시 ····· 24
2. M. Foucault의 권력 개념에 있어 감시의 역할 ····· 33
3. 권력의 법학적 의미 ····· 43
4. 오늘날 인공지능과의 관계 ····· 46
제 3 절 인공지능 감시를 통한 권력의 확대 가능성 ····· 50
1. 의의 ····· 50
2. 인공지능 기반 감시 기술의 활용 ····· 50
3. 감시의 효과를 가지는 인공지능 기술 ····· 68
제 4 절 인공지능 감시 기술에 대한 규제 필요성 ····· 70
1. 인공지능 감시를 통한 기본권 침해 가능성 증대 ····· 70
2. 생체정보 및 생체인식정보 활용의 문제 ····· 80

3. 예측 치안을 위한 인공지능 활용의 문제점 ····· 83
4. 형사사법 분야에서의 인공지능 활용의 문제점 ····· 88
5. 인공지능 감시를 통한 노무관리의 문제 ····· 93
6. 소결 ····· 97

제 3 장 인공지능 감시에 대한 규제 동향 ····· 99

제 1 절 인공지능에 대한 규제 방식 검토 ····· 99
1. 의의 ····· 99
2. 자율규제에서 법적 규제로 ····· 99
3. 법적 규제 방식의 유형 ····· 101
제 2 절 국외의 규제 동향 ····· 109
1. 미국 ····· 109
2. 유럽연합 ····· 120
3. 영국 ····· 126
4. 중국 ····· 131
제 3 절 국내의 규제 동향 ····· 135
1. 개설 ····· 135
2. 직접적 규제 방식을 통한 규제 ····· 136
3. 간접적 규제 방식을 통한 규제 ····· 140
4. 간접적 규제 방식을 통한 규제 ····· 145

제 4 장 인공지능 감시 문제에 대한 규범적 대응방안 ····· 147

제 1 절 대응 원칙 ····· 147
1. 규범적 대응의 필요성과 원칙 ····· 147
2. 인공지능 활용 근거 규범의 구체화 ····· 149
3. 투명성 및 객관성 확보 방안 마련 ····· 151

4. 실효적인 감독 및 권리구제 제도 마련 ····· 153
제 2 절 독일 헌법재판소 결정의 시사점 ····· 155
1. 의의 ····· 155
2. 사실관계 ····· 155
3. 개인정보자기결정권의 제한 ····· 156
4. 제한의 정당성 심사 ····· 157
5. 개정된 「헤센주법」에 따른 데이터 분석을 위한 자동화된 앱 이용의 조건 ····· 170
제 3 절 프랑스 헌법재판소 결정의 시사점 ····· 175
1. 의의 ····· 175
2. 입법의 배경 및 과정 ····· 176
3. 법률 규정의 주요 내용 ····· 177
4. 헌법재판소의 결정 ····· 179

제 5 장 결 론 ····· 181

제 1 절 요 약 ····· 181
제 2 절 정책적 제언 ····· 183

참고문헌 ····· 187

Abstract ····· 213

표 목 차

〈표 3-1〉 15개 주의 보안카메라 규제 현황 ····· 113

그 림 목 차

[그림 2 - 1] 판옵티콘의 설계도 ····· 31

요 약 문

1. 제목

인공지능 감시에 의한 권력의 확대와 그 규범적 대응방안 연구

2. 연구 목적 및 필요성

인공지능 기술의 성장과 확산 속도가 점차 빠르게 진행되고 있다. 인공지능이 경제적·사회적 혁신을 창출할 것이라는 기대가 현실이 되고 있지만, 일자리 대체에 의한 고용 불안정의 문제, 기술적 한계 및 오용과 악용의 가능성으로 말미암아 안전과 신뢰에 대한 우려도 함께 나타나고 있다. 특히, 이러한 우려 속에는 인공지능 기술을 활용한 감시 시스템이 우리 사회 곳곳에서 점차 많이 활용되면서 발생하는 사생활 침해에 대한 불안감 또한 증폭되고 있다.

인공지능의 안전성 및 신뢰·윤리의 확보가 전 세계 시민의 공통적 관심사가 되면서 세계 각국과 국제기구 등은 인공지능에 대한 합리적인 규제 체계를 마련하기 위해 노력하고 있다. 특히, 인공지능 감시 기술은 범죄 예방과 질서 유지와 같이 공익적 차원에서 활용될 수 있으나, 그 이면에는 권력을 확대하는 도구로 활용될 수 있다는 측면에서 헌법이 보장하는 각종 기본권의 제한 내지 침해 가능성이 문제가 되고 또한 민주주의에 대한 위협이 될 수도 있다. 따라서 이 연구에서는 인공지능 기술을 활용한 감시와 그로 인한 권력 확대의 위험성에 관하여 검토하는 것을 시작으로, 인공지능 감시에 대한 국내외 규제 동향을 검토한 후 관련 문제에 대한 규범적 대응방안을 고찰하고자 한다.

정보통신기술이 등장하면서부터 개인에 관한 정보가 네트워크 공간에서 전송되

면서 자기 자신도 모르는 사이에 타인이나 공권력이 이를 활용할 수 있다는 불안감에 살아왔지만, 인공지능 기술이 발전을 거듭함에 따라 이러한 현상은 더욱 극심해질 것이다. 인공지능 기술이 과거에 사람이 처리하던 규모와는 비교할 수 없을 정도의 많은 양의 데이터를 빠른 속도로 처리하면서 특정한 결과를 예측하기 때문이다. 이러한 기술이 개인과 사회에 미칠 영향이 막대한 만큼, 그에 대응하기 위한 제도적 방안에 대한 검토는 매우 중요한 의미가 있다.

3. 연구의 구성 및 범위

이 연구는 총 5장으로 구성된다. 제1장에서는 이 연구의 배경과 목표 및 주요 내용을 서술한다. 제2장에서는 인공지능 기술을 활용한 감시 시스템과 권력 확대에 내재하는 위험성에 대하여 살펴보고자, 먼저 인공지능 일반의 위험을 간략하게 검토한다. 이후 인공지능의 위험을 인공지능 감시로 인한 위험으로 특정하고, 여기에 권력이라는 문제를 함께 다루기 위해 감시와 권력의 상관관계를 철학과 법학 이론을 통해서 살펴보며, 감시와 관련된 인공지능 활용 사례를 통해서 규제의 필요성을 확인한다. 제3장에서는 인공지능 감시에 대한 국내외의 규제 동향에 대해서 인공지능에 대한 규제 방식을 유형화하여 살펴본다. 제4장에서는 제2장과 제3장에서 진행한 연구를 바탕으로 인공지능 감시 문제에 대한 규범적 대응방안을 검토하기 위해서 대응의 원칙을 설정하고, 관련 시사점을 얻고자 독일과 프랑스의 헌법재판소 결정을 검토한다. 제5장에서는 앞의 논의를 요약하고 정책적 시사점을 확인한다.

4. 연구 내용 및 결과

감시는 이중성 성격을 가진다. 오늘날 공공의 안전과 사회의 질서유지라는 공익 목적을 달성하기 위해 감시가 이루어지고 있는데, 그 과정에서 비정상인을 보호하

는 차원에서는 긍정적 의미가 있고, 비정상인을 통제하고 배제한다는 차원에서는 부정적 의미가 있다. M. Foucault의 이론에 따르면, 비정상인인 범죄자를 감옥에 가두지 않더라도 감시라는 행위를 이용해 통제하고 순종하게 하면 질서는 유지되는 것인데, 이것이 바로 권력의 메커니즘이라고 할 수 있다. 오늘날 사회는 정보통신기술의 발달에 인공지능 기술이 더해져 사회 구성원이 전혀 인식하지 못하는 사이에도 감시라고 하는 메커니즘에 의해 설령 권력자가 의도하지 않았다고 하더라도 미세한 권력이 확대되는 현상 속에서 통제되어 가고 있다. 실제로 인공지능 기술 기반의 감시 시스템은 지능형 CCTV를 비롯하여 우리 주변의 곳곳에서 활용되고 있다.

이러한 기술의 활용은 개인정보자기결정권, 사생활의 비밀과 자유, 인간의 존엄과 가치, 일반적 행동의 자유, 평등권, 표현의 자유와 같은 헌법상 국민의 기본권을 침해할 우려가 있다. 이에 각국은 다양한 방식으로 인공지능 감시에 대한 규제를 마련하고 있다. 미국에서는 주로 개별적 규제 방식을 활용하여 주나 시 단위에서 보안카메라나 안면인식 기술의 활용을 규제하고 있는 반면에, 유럽연합은 GDPR을 통한 간접적 규제 방식이나 최근 제정한 「인공지능에 관한 명령(AI Act)」을 통한 직접적 규제 방식을 채택하고 있다. 우리나라는 인공지능 기술의 개발과 활용 전반에 적용되는 일반법률의 제정을 추진하고 있으나 현재까지는 진전되지 않고 있고, 인공지능 감시에 대해서 「개인정보 보호법」의 자동화된 결정에 대한 정보주체의 권리 보호 규정과 영상정보처리기기에 관한 규정을 통해 간접적 규제가 이루어지고 있다. 개별적 규제 역시 이루어지고는 있지만, 개별 영역에서 인공지능 기술의 활용이나 금지 또는 제한에 관련된 근거 법률은 존재하지 않는다.

인공지능 기술을 활용한 감시 시스템이 늘어나는 현재 상황에서 규범적 대응의 최우선 원칙으로서 고려해야 할 점은 인공지능 활용 근거 규범을 법치주의의 원칙 아래서 구체화하는 것이다. 특히, 국가와 국민의 관계에서는 인공지능 감시가 그 자체로 국민의 기본권에 대한 큰 영향을 미치는 영역이기 때문이다. 아울러 인공지능 감시에 있어서 적법절차를 준수하여 투명성과 객관적 확보 방안을 마련하고, 실효적인 감독과 권리구제를 위한 제도를 마련하는 것이 중요한 과제가 될 것

이다.

현재 논의되는 인공지능 관련 기본법 제정과 관련해서는 인공지능의 위험을 통제하기 위해 적절한 수준의 법적 규제의 도입을 고려해야 하고, 인공지능 기술의 지속가능성을 또한 고려해야 하며, 국제규범 체계 마련의 동향도 마찬가지로 고려해야 할 필요가 있을 것이다. 현재 국회에 계류 중인 대동소이한 여러 건의 법률안은 기술의 발전과 산업의 활성화 차원의 큰 틀에 기조를 두고 직접적 규제 요소라고 하여도 신뢰성·안전성 확보 차원에서의 자율규제 중심의 정책 지원이 주를 이루고 있다. 다만, 투명성 확보와 관련해서는 규제 수준을 조금 높여도 될 것이다. 인공지능 감시가 가지는 국민의 기본권 침해에 대한 위험성이나 민주주의 원리에 대한 위협은 개별적 규제 방식을 주로 채택하여 인공지능 활용의 구체적 법적 근거를 도입함으로써 해결이 가능할 것이다.

5. 기대효과

이 연구는 인공지능 기술의 발전과 사회적 확산이 빠르게 진행되는 현 상황에서, 현대 사회에서의 감시와 권력에 관한 다각적인 검토를 통한 이론적 토대를 마련하고 국민의 안전과 권리를 보장하기 위한 법이론 형성에 대한 기여를 기대한다. 아울러 정부는 디지털 심화 시대를 맞아 2023년 9월 25일 새로운 디지털 질서 정립의 기본 방향으로서 「디지털 권리장전」을 발표하였고, 본 권리장전 제19조는 “디지털 환경에서 개인의 프라이버시는 디지털 감시, 위치추적 등을 비롯한 불법적인 식별과 추적으로부터 보호되어야 한다”고 규정하였다. 이 연구가 구체적으로는 향후 진행되는 인공지능 관련 입법 마련 또는 개인정보 및 사생활 보호 관련 입법 개선의 기초자료로 활용될 수 있기를 기대하며, 특히 인공지능 기술을 활용한 개인 감시가 늘어날 수 있는 우려 속에서 국민의 기본권을 보호하기 위한 관련 정책 수립과 추진의 토대를 제공하기를 기대한다.

제1장 서 론

제1절 연구의 배경

최근 들어 인공지능 기술의 성장과 확산이 빠른 속도로 진행되고 있다. 국내에서 인공지능에 대한 대중적 인지도가 높아진 것은 2016년 3월 딥마인드(DeepMind)가 개발한 인공지능 기반의 바둑 프로그램인 알파고(AlphaGo)와 프로바둑기사 이세돌 9단 간의 바둑 대결에서 알파고가 4승 1패로 승리를 거둔 것이 계기가 되었다고 할 수 있다. 당시에는 인공지능이 향후 우리 경제·사회 전반의 변화를 불러올 것이라는 막연한 기대감이 나타났다. 그런데 그로부터 8년이 가까이 지난 2022년 11월에는 미국의 오픈AI(Open AI)가 초거대 인공지능 언어모델인 GPT-3.5 기반의 대화형 인공지능 서비스 챗지피티(ChatGPT)를 출시하였고, 그로부터 두 달 만에 사용자 수 1억 명을 기록하는 등 전 세계적인 주목을 받았다.[1] 이에 자극을 받은 글로벌 인공지능 기업이 경쟁적으로 대형언어모델(Large Language Model: LLM)이나 대형멀티모달모델(Large Mutimodal Model: LMM) 기반의 서비스를 선보이면서, 이제는 전 세계 누구라도 인공지능을 손쉽게 이용할 수 있게 되었다. 또한 산업의 전 영역에서 업무의 효율성과 생산성을 높이기 위해 인공지능을 적극적으로 활용하고 있고, 이에 따라 일하는 방식이 점차 변화하고 있다.

인공지능의 경제적·사회적 가치가 갈수록 높은 평가를 받고 또한 기술 수준이 곧 국가 경쟁력으로도 연결되자, 우리 정부는 국가 차원의 기술 발전 및 혁신 전

---

1) Reuters(2023. 2. 3.), “ChatGPT sets record for fastest-growing user base - analyst note”, https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01 (2024. 10. 3. 최종 방문).

략을 수립하기 시작하였다.[2] 대표적인 것이 2019년 12월 발표한 「인공지능 국가전략」인데, 본 전략은 "IT 강국을 넘어 AI 강국으로!"라는 비전 아래 인공지능 관련 인프라 확충, 기술경쟁력 확보, 인재 양성, 규제 개혁, 사업 및 공공분야에서의 활용, 사람 중심의 인공지능 구현 등의 세부 전략을 제시하였다.[3] 또한 최근에는 2024년 9월 26일 '국가인공지능위원회'[4] 출범식에서 "인공지능 3대 강국(AI G3) 도약을 견인할 국가 AI 혁신 비전"으로서의 「국가 AI 전략 정책방향」을 발표하기도 하였다.[5] 본 정책방향은 민관 협력을 통한 범국가적 '4대 AI 플래그십 프로젝트'를 추진하겠다고 밝히고 있는데, 첫 번째 프로젝트는 국가 인공지능 컴퓨팅 인프라의 대폭 확충이고, 두 번째 프로젝트는 민간부문에서의 인공지능 투자를 대폭 확대하는 것이고, 세 번째 프로젝트는 국가 전반의 인공지능 대전환을 추진하는 것이며, 네 번째 프로젝트는 인공지능 안전·안보·글로벌 리더십을 확보하는 것이다.

인공지능 기술의 발전이 과거에는 인간만이 담당하던 영역을 대체하는 등 인간 능력의 한계를 극복함으로써 경제적·사회적 혁신을 창출하고 궁극적으로는 삶의 질을 높일 것이라는 기대의 이면에 사회적 불안과 우려가 만연해 있다는 것도 사실이다. 인공지능의 일자리 대체에 의한 실업 발생과 고용의 불안정과 같은 문제는 현실화가 되고 있고, 기술의 한계와 오용이나 악용의 가능성으로 인하여 안전과 신뢰에 대한 우려도 나타나고 있다.

특히, 이러한 우려 속에는 인공지능 기술 기반의 감시 시스템이 우리 사회 곳곳에서 점차 많이 활용되면서 나타나는 불안감을 언급하지 않을 수 없다. 물론 오늘날과 같이 법치주의와 민주주의가 정착된 사회에서는 인공지능 감시 시스템을 활

---

2) 문광진(2024), "인공지능 규제 입법에 관한 일고찰", 《외법논집》 제48권 제3호, 한국외국어대학교 법학연구소, 80쪽.

3) 과학기술정보통신부 보도자료(2019. 12. 17.), "IT 강국을 넘어 AI 강국으로!": 범정부 역량을 결집하여 AI 시대 미래 비전과 전략을 담은 'AI 국가전략 발표'.

4) 국가인공지능위원회는 2024년 8월 6일 대통령령 제34787호로 제정 및 시행된 「국가인공지능위원회의 설치 및 운영에 관한 규정」에 따라 설치되었다.

5) 과학기술정보통신부 보도자료(2024. 9. 26.), "인공지능 3대 강국(AI G3) 도약을 위한 대한민국 AI 혁신의 청사진 제시".

용하는 목적이 대부분은 범죄를 예방하거나, 혹은 더 넓은 의미에서 질서를 유지하는 등의 공익적 차원이라고 할 수 있다. 그럼에도 불구하고 인공지능 감시 기술의 활용 자체만으로도 우리 헌법이 국민의 기본권으로 보호하고자 하는 사생활의 비밀과 자유와 개인정보자기결정권의 제한 내지 침해 가능성이 문제가 될 수 있다. 또한 단순히 기본권 관련 문제를 넘어서서 인공지능 감시 기술이 특정인이나 특정 집단을 탄압하기 위한 목적으로 활용되는 것에 대한 우려도 있다. 이는 권력자가 해당 기술을 활용하여 피권력자에 대한 자신의 권력을 더욱 공고하게 할 수도 있다는 문제와 연결되기도 한다. 다른 측면에서는 인공지능 기술의 활용이 감시를 목적으로 하지 않더라도, 그 활용 자체만으로써 감시에 준하는 효과가 발생하고 종국적으로는 권력자의 영향력이 높아지는 현상, 일종의 권력 확대 현상이 나타날 수도 있다. 즉, 인공지능 감시는 이를 의도하였건 하지 않았건, 국민의 기본권에 대한 영향은 물론 민주주의에 대한 영향까지도 미칠 수 있는 문제이다.

ChatGPT가 선풍적인 인기를 끌고 있던 2023년 3월 미국 비영리단체 '삶의 미래 연구소(Future of Life Institute: FLI)'는 인공지능 기술이 사회에 미칠 잠재적 위험을 우려하면서 당시 ChatGPT의 기반모델(Foundation Model)이었던 GPT-4의 성능을 능가하는 인공지능 시스템에 대해서는 최소 6개월 동안 개발을 중단하자는 공개서한을 발송하였다.[6] 본 공개서한에 테슬라의 CEO인 Elon Musk, 애플의 공동창업자 Steve Wozniak, 딥러닝 분야의 석학인 Yoshua Bengio, 베스트셀러 작가이자 역사학자인 Yuval Harari 등 1,000여 명이 공동으로 서명을 하면서 인공지능의 위험성이 전 세계적으로 알려지게 되었다. 인공지능을 활용함으로써 발생할 수 있는 위험 또는 부작용을 최소화 내지 관리하면서 인공지능이 미래의 우리 사회에 가져올 긍정적 변화를 수용하는 것이 오늘날의 중요한 과제가 되었다. 이러한 문제는 인공지능 기반의 감시 기술의 개발이나 활용과 관련하

6) Future of Life Institute(2023. 3. 23.), "Pause Giant AI Experiments: An Open Letter" https://futureoflife.org/wp-content/uploads/2023/05/FLI_Pause-Giant-AI-Experiments_An-Open-Letter.pdf (2024. 10. 3. 최종 방문).

여서도 마찬가지이다.

즉, 인공지능 기술의 개발과 활용 전반에 대해서는 물론이고, 감시와 관련된 분야에서도 정당하고 합리적인 규제가 작동할 수 있는 규범적 대응이 필요하다. 인공지능 기술 전반에 대해서는 우리나라를 비롯한 세계 각국이 꽤 몇 년 전부터 정책적 수단을 활용하여 인공지능의 윤리·신뢰성을 확보하고자 노력을 해왔다.[7] 이러한 노력에 더하여 법적 수단을 통해 인공지능에 대한 규제의 움직임도 있는데, 가장 많은 진전을 보이는 곳은 유럽연합이다. 유럽연합은 2024년 6월 13일 '인공지능에 관한 명령(AI Act)'을 제정하였고, 본 명령은 같은 해 8월 1일 발효되었다. 인공지능 감시 기술에 대해서는 미국의 경우 주와 시 단위에서 주 법률 또는 시 조례로 이를 규제하고 있고, 유럽연합의 경우 관련 지침을 제공하기도 한다. 그러나 우리나라의 경우 인공지능에 관한 일반법률의 도입이 제21대 국회에서 시도되었지만 2024년 5월 말 임기종료로 무산되었고, 제22대 국회가 출범하면서 다시 관련 법안이 제출되고 있다. 또한 인공지능 감시 기술에 대한 명확한 법적 근거도 마련되어 있지 않은 상황이다.

인공지능이 유발할 수 있는 위험에 대한 규범적 대응 노력은 개별 국가 단위에서 그치지 않고 국제협력의 차원에서도 계속해서 이어지고 있다.[8] 인공지능 감시 기술의 확산이 초래하는 인권 침해와 민주주의에 대한 위협에 관해서도 국내외를

---

7) 문광진(2024), 앞의 논문, 81쪽.

8) 2024년 5월 21일 서울에서는 대한민국, 유럽연합, 프랑스, 독일, 이탈리아, 미국, 호주, 캐나다, 영국, 일본, 싱가포르 등이 참여한 '인공지능 안전성 정상회의(AI Safety Summit)'가 개최되었다. 이 정상회의에서 각국 정상들은 인공지능의 안전·혁신·포용을 목표로 위험 기반 접근의 정책 및 거버넌스 체계를 지지하는 등 다양한 국제협력을 촉구하는 '안전하고 혁신적이며 포용적인 인공지능을 위한 서울 선언(Seoul Declaration for Safe, Innovative and Inclusive AI by Participants Attending the Leaders' Session of the AI Seoul Summit)'과 개방성·투명성·상호주의 기반의 인공지능 안전 과학을 증진하기 위한 국제협력의 중요성을 확인하고, 인공지능 연구, 평가, 개발 지침 마련 등을 위한 인공지능 안전연구소의 설립 노력을 격려하며, 인공지능 안전 과학의 진전을 가속화하기 위한 상호 간의 네트워크를 발전시키기로 약속하는 '인공지능 안전 과학에 대한 국제 협력을 위한 서울 의향서(Seoul Statement of Intent toward International Cooperation on AI Safety Science)'를 발표하였다.

막론하고 지속해서 관심 사항이 될 것임이 분명하다. 이에 우리 정부는 2023년 9월 25일 전 세계 앞에서 새로운 디지털 질서를 제시하기 위해 보편적 디지털 질서 규범으로서 「디지털 공동번영사회의 가치와 원칙에 관한 헌장」, 이른바 「디지털 권리장전」을 발표하였다. 「디지털 권리장전」은 5대 기본원칙으로 ① 자유와 권리보장, ② 공정한 접근과 기회의 균등, ③ 안전과 신뢰의 확보, ④ 디지털 혁신의 촉진, ⑤ 인류 후생의 증진을 제시하였고, 무엇보다도 제19조 (디지털 프라이버시의 보호)에서 "디지털 환경에서 개인의 프라이버시는 디지털 감시, 위치추적 등을 비롯한 불법적인 식별과 추적으로부터 보호되어야 한다"고 규정하였다. 본 권리장전 전문이 "디지털 모범국가를 지향하는 대한민국은 디지털 공동번영사회를 함께 이루어나갈 것을 세계 시민 앞에 제안하며, 인류가 함께 추구해야 할 가치와 원칙을 아래와 같이 선언한다"고 한 만큼, 인공지능 감시가 가져올 권력의 확대를 경계하고 이에 대한 규범 마련에도 국가 차원의 대응이 필요한 상황이다. 따라서 감시와 권력에 관한 개념 연구, 인공지능 기반 감시 기술의 활용 또는 감시의 효과를 가져오는 인공지능 기술의 활용에 관한 사례 연구, 인공지능 감시에 대한 규제 동향에 관한 연구 등을 통해서 이 분야의 규범적 대응 방향을 제시할 필요가 있다.

제2절 연구의 목표 및 주요 내용

이 연구의 목적은 인공지능 기술의 발전과 사회적 확산에 따라 인공지능 알고리즘과 빅데이터를 활용하여 개인을 프로파일링할 수 있는 환경이 갖추어지고, 그로 인하여 개인에 대한 감시와 통제 가능성에 대한 우려와 함께 권력이 확대되는 가능성 하에서 국민의 안전과 권리를 실질적으로 보장할 수 있는 규범적 대응방안을 제시하는 것이다. 안면인식기술을 비롯한 생체인식기술은 특정인을 식별하는 목적의 기술이어서 이를 개인을 감시하는 용도로 활용하게 되면, 사생활의 비밀과 자유와 개인정보자기결정권과 같은 헌법상 기본권의 침해 가능성이 있다. 또한 이

러한 기술을 공권력이 법집행을 목적으로 공공장소에서 개인을 실시간으로 감시하는 데 활용하게 되면 감시사회 또는 통제사회의 등장에 대한 우려가 제기될 수 있다. 개인에 대한 감시는 해당 개인의 자유를 직·간접적으로 위축시키는 일종의 권력으로 작용하는 것이고, 인공지능을 통해 개인을 감시할 수 있게 되면 인공지능 기술은 곧 권력의 도구가 되는 것이며, 인공지능에 의한 감시는 권력의 확대 또는 확장을 의미할 수 있게 되는 것이다.

따라서 이 연구에서는 인공지능 감시와 그로 인한 권력 확대의 위험성에 관하여 사례와 이론을 중심으로 살펴보고자 한다. 이어서 인공지능 감시에 대한 규제 동향에 관하여 검토하기로 한다. 이를 바탕으로 인공지능 감시 문제에 대해 규범적 대응방안을 제시할 것이다.

구체적으로 제2장에서는 인공지능 감시와 권력 확대에 내재하는 위험성에 대하여 살펴보기 위해서, 우선은 인공지능 일반의 위험에 관하여 간략하게 검토해 보기로 한다. 그러고 나서 인공지능의 위험을 인공지능 감시로 특정하고 또한 권력이라는 문제를 함께 다루고자, 감시와 권력의 상관관계를 조망하는 차원에서 두 개념에 관한 철학과 법학 분야의 이론을 검토한다. 이어서 인공지능 감시를 통한 권력의 확대 가능성을 살펴보고자 인공지능 기반 감시 기술의 활용 또는 감시의 효과를 가져오는 인공지능 기술의 활용에 관한 사례를 확인해 본다. 이를 통해서 인공지능 감시 기술 활용의 법제도적 이슈 내지 이러한 기술에 대한 규제의 필요성을 살펴본다. 제3장에서는 인공지능 감시에 대한 규제 동향을 분석하는데, 체계적인 분석과 대응방안 제시를 위해서 인공지능에 대한 규제 방식을 총 3가지 방식으로 구분하여 진행한다. 첫째로 인공지능에 대한 직접적 규제 방식에 관하여 검토하고, 둘째로 인공지능에 대한 간접적 규제 방식에 관하여 검토하며, 셋째로 인공지능에 대한 개별적 규제 방식에 관하여 검토한다. 제4장은 제2장과 제3장에서 진행한 연구를 바탕으로 인공지능 감시 문제에 대한 규범적 대응방안을 제시하기 위한 부분이다. 우선은 이에 앞서 대응의 원칙부터 간략하게 정하고 난 후, 앞서와 마찬가지로 인공지능에 대한 규제 방식의 유형화에 따라 직접적 대응방안,

간접적 대응방안, 개별적 대응방안을 제시한다. 제5장에서는 앞의 논의를 요약하고 종합적인 정책적 제언으로서 향후 입법 방향과 이에 필요한 정부의 노력에 관하여 제안한다.

제 2 장 인공지능 감시와 권력 확대의 위험성

제 1 절 인공지능의 위험 일반

인공지능 기술의 활용에 따라 발생할 수 있는 위험(risk)은 매우 다양하다. 이러한 위험은 사전배려의 원칙 아래 일정한 관리가 되면 기술의 편익이 극대화될 수 있는, 즉 적절한 규제가 필요한 영역이다. 이를 위해서는 위험이 발생하는 원인을 파악하는 것이 우선일 것인데, 그 원인은 인공지능의 작동 원리와 인공지능의 개발 과정의 특성과 밀접한 관련이 있다. 인공지능 시스템은 지도학습이나 비지도학습과 같은 방식을 통해 컴퓨터가 대량의 데이터를 학습하면서 스스로 일정한 패턴을 반복적으로 찾는 과정을 거쳐 개발된다. 이 과정에서 최적의 알고리즘이 생성되고 발전하는 것이다. 이렇게 개발된 인공지능이 특정한 명령을 받게 되면 인간의 개입이 없이 그에 상응하는 판단 또는 결정을 내리게 되는데, 이때 예측곤란성이나 자율성과 같은 특징을 가진다.[9] 또한 학습 과정에서 대량의 데이터가 활용되고, 그 작동에서도 프로파일링처럼 일정한 예측을 하고자 대량의 데이터 분석을 하기도 해서 개인정보나 사생활에 대한 침해의 위험 역시 존재한다.

한편, 인공지능 기술에 의한 인간 노동력 대체 우려가 계속해서 제기되면서 노동시장에 대한 위험이 언급되기도 한다. 인공지능 기술의 발전이 노동시장에 변화를 초래하는 것은 필연적인데, 우리나라의 경우 전체 취업자의 12%에 해당하는 약 341만 명이 인공지능 기술로 대체될 수 있다고 예측되었다.[10] 일자리 총량에 관해서는 세계경제포럼(World Economic Forum)이 2023년 실시한 조사에서,

---

9) 양종모(2016), “인공지능의 위험의 특성과 법적 규제방안”, 《홍익법학》 제17권 제4호, 홍익대학교 법학연구소, 544-545쪽.

10) 한지우·오삼일(2023), “AI와 노동시장 변화”, 《BOK 이슈노트》 제2023-30호, 한국은행, 5쪽.

향후 5년 동안 6,900만 개의 일자리가 새로 생겨나고 8,300만 개의 일자리가 사라질 것이라고 예상되었다.[11] 인공지능이 노동시장에 많은 변화를 가져오면서 개개인의 근로권이나 인간다운 생활을 할 권리에 대하여 영향을 미치는 것은 물론 인공지능의 위험 중 하나일 것이다. 다만, 이러한 사회적 문제는 인공지능이 직접 유발하는 위험이라고 볼 수는 없는데, 인공지능이 인간의 지능을 전자적인 방식으로 구현하여 결국에는 인간의 노동력을 대체하는 것이 목적이기 때문이다. 즉, 인공지능으로 인한 노동시장의 변화는 인공지능 기술의 개발과 활용에 대한 규제보다는 고용, 복지, 교육 등의 정책적 수단을 활용하여 사회안전망을 강화하는 방식으로 접근할 필요가 있다.[12]

인공지능 관련 규제는 인공지능의 기능 그 자체를 제한하기보다는 인공지능이 본래 달성하고자 하는 목적과 다르게 악용되거나 역기능 내지 부작용으로 발생할 수 있는 위험을 관리하는 방향으로 이루어져야 할 것이다. 궁극적으로는 인공지능에 대한 사회적 신뢰를 제고하여 기술 발전의 지속가능성이 담보되어야 할 것이다. 이를 위해서는 기술이 빠르게 성장하여 인간 전체 지능의 합을 뛰어넘는 초지능의 수준에 도달한 인공지능이 인류의 생존 자체에 대해 가하게 되는 위험, 이른바 '실존적 위험'을 우려하여 설계된 규제를 도입하여서는 아니 된다.[13] 이러한 태도는 우리 실정법에서도 확인할 수 있다. 현행 법률에서는 '규제'라는 개념이 「행정규제기본법」 제2조 제1항에 따른 '행정규제'에 해당할 것이다. 행정규제는 "국가나 지방자치단체가 특정한 행정 목적을 실현하기 위하여 국민(국내법을 적용받는 외국인을 포함한다)의 권리를 제한하거나 의무를 부과하는 것으로서 법령등이나 조례·규칙에 규정되는 사항"으로 정의되어 있는데, 여기에서의 국민에 대한 권리의 제한과 의무의 부과는 정당한 행정 목적의 달성을 위해 효과적이면서도 비

11) World Economic Forum(2023), Future of Jobs Report 2023: Insight Report, May 2023, p. 28.

12) 문광진(2024), 앞의 논문, 83쪽.

13) 이상욱(2020), "인공지능의 실존적 위험 - 비판적 검토 -", 《인간연구》 제40호, 가톨릭대학교 인간학연구소, 109-110쪽.

례적인 수단일 것을 요한다. 즉, 국민의 자유와 권리를 부당하게 침해하지 않아야 하는데, 이러한 연유로 '자율규제'가 규제 방법론의 하나로 주목받고 있으며, 특히 신기술의 등장에 따른 시장과 사회의 변화가 규제의 축소나 유연화 현상을 가져오기도 했다.[14)]

기술적인 측면에서는 인공지능 활용에 따라서 발생할 수 있는 위험 그 자체에 집중하기보다는, 그러한 위험을 완화하는 일종의 관리(risk management)를 통해 신뢰할 수 있는 인공지능(Trustworthy AI)을 구현하려는 시도가 이루어지고 있다. 미국에서는 2023년 국립표준기술연구소(National Institute of Standards and Technology: NIST)가 인공지능 시스템의 설계, 개발, 배포, 활용 등을 하는데 있어 관련 위험 관리에 필요한 지침으로서 '인공지능 위험 관리 프레임워크 1.0(AI Risk Management Framework 1.0)'을 발표하였는데, 여기에서는 신뢰할 수 있는 인공지능의 특성으로 유효성·신뢰성, 안전성, 보안성·복원성, 책무성·투명성, 설명가능성·해석가능성, 사생활보호성, 공정성 등이 제시되었다.[15)] 이러한 특징은 인공지능의 위험을 적절히 관리하기 위해 인공지능이 갖추어야 하는 요소를 의미하는 것으로서, 이를 통해 역으로 파악할 수 있는 점은 인공지능의 개발이나 활용이 초래할 수 있는 위험에는 안전에 대한 위협 문제, 편향성 및 차별가능성 문제, 프라이버시 침해 문제, 불투명성 및 탈진실성 문제 등이 거론된다는 것이다.[16)]

첫째, 안전에 대한 위협은 사회 전반에 폭넓게 활용될 수 있는 범용기술로서의 인공지능이 각종 제품이나 서비스에 적용되어 시장에 출시되면서,[17)] 이용자가 소비자로서 이를 활용하면서 기술의 오작동으로 생명이나 신체에 위험을 초래할 수

---

14) 선지원(2021), "규제 방법의 진화로서 자율규제의 실질화를 위한 연구", 《행정법연구》 제34호, 행정법이론실무학회, 101-102쪽.

15) National Institute of Standards and Technology(2023), Artificial Intelligence Risk Management Framework,, pp. 12-18.

16) 이러한 위험의 유형에 관하여는 문광진(2024), 앞의 논문, 84-92쪽 참조.

17) 최경진 편(2024), 『인공지능법』, 박영사, 36쪽.

있는 문제이다. 대표적인 사례로 자율주행자동차의 사고를 생각해볼 수 있다.[18)]

둘째, 편향성 및 차별가능성은 인공지능의 개발 과정에서 사람이나 사회의 각종 편견, 선입견, 고정관념 등을 포함하는 학습데이터가 활용되어 기존의 편견 등을 더욱 확대 재생산하는 편향적 인공지능 시스템이 탄생하고, 이러한 인공지능 시스템이 특정 개인이나 집단에 대한 차별적 결과를 산출하는 문제이다. 미국에서 아마존이 자체 개발·활용한 인공지능 채용 시스템이 성별 등을 이유로 입사지원자를 차별한 것이 논란이 되어 2018년 해당 시스템이 폐기된 것이 대표적인 예라고 할 수 있다.[19)]

셋째, 프라이버시 침해는 인공지능 시스템 개발 단계에서 막대한 데이터를 활용하면서 정보주체의 개인정보 관련 권리가 침해되거나, 인공지능 시스템을 직·간접적으로 감시의 목적이나 그와 유사한 효과가 발생하도록 활용하면서 개인의 사생활에 관한 권리를 제한 내지 침해하는 문제이다.

끝으로, 불투명성과 탈진실성은 인간이 인공지능의 기술적 원리, 학습데이터, 의사결정 과정 및 근거 등에 대해서 알기가 어렵고 전문가나 당해 개발자도 인공지능의 의사결정 근거 내지 인과관계를 명확하게 설명하지 못한다거나, 이용자의 의도 여부와 관계없이 거짓된 정보 및 콘텐츠가 생성될 수 있다는 문제이다. 전자의 예로는 인공지능 채용 시스템에 대한 투명성 관련 제소가 이어지고 있는 것을 들 수 있겠고,[20)] 후자의 예로는 딥페이크(deepfake) 기술을 활용한 허위조작정보

---

18) CNN Business(2016. 7. 1.), “Tesla's autopilot probed by government after crash kills driver”, https://money.cnn.com/2016/06/30/technology/tesla-autopilot-death/index.html (2024. 10. 3. 최종 방문) ; Reuters(2018. 3. 21.), “Homeless Arizona woman killed by Uber self-driving SUV was ‘like everyone’s aunt’” https://www.reuters.com/article/us-autos-selfdriving-uber-victim/homeless-arizona-woman-killed-by-uber-self-driving-suv-was-like-everyones-aunt-idUSKBN1GW36P (2024. 10. 3. 최종 방문).

19) Reuters(2018. 10. 11.), “Insight - Amazon scraps secret AI recruiting tool that showed bias against women”, https://www.reuters.com/article/idUSKCN1MK0AG (2024. 10. 3. 최종 방문).

가 개인의 권리에 대한 침해는 물론 경제적·사회적으로 악영향을 미치고 있다는 점을 들 수 있겠다.[21)]

이러한 위험을 적절하게 관리하는 것이 인공지능에 대한 규제의 목표라고 할 수 있을 것이다. 특히, 이 연구의 직접적인 대상이 되는 인공지능 기반 감시 기술의 활용은 프라이버시 침해에 관한 문제와 크게 관련이 있으며, 아래에서는 감시와 권력의 상관관계를 시작으로 하여 인공지능 감시가 가져올 수 있는 권력 확대의 위험성과 규제 필요성을 검토하고자 한다.

제 2 절 감시와 권력의 상관관계

1. M. Foucault의 이론과 감시

가. 감시의 의의

오늘날 우리 사회에서 감시는 일상적인 현상이 되어 있다. 우리는 일상생활 속 곳곳에서 CCTV와 같은 감시 카메라, 개인 블랙박스 카메라, 휴대폰 카메라 등을 통해 감시를 경험하고 있다. 이에 너무나도 익숙해져 때로는 감시가 곳곳에서 이루어진다는 점을 느끼지 못할 때도 있다. 자연스럽게 이에 대한 거부감도 줄어든다.

사실 이러한 감시 장치가 증가하면서 우리 일상생활에서의 안전이 보장되는 측

---

20) *Forbes*(2020. 2. 3.), "EPIC Asks Federal Trade Commission To Regulate Use Of Artificial Intelligence In Pre-Employment Screenings", https://www.forbes.com/sites/patriciagbarnes/2020/02/03/group-asks-federal-trade-commission-to-regulate-use-of-artificial-intelligence-in-pre-employment-screenings/?sh=5ed2028c2b54 (2024. 10. 3. 최종 방문); 수원지방법원 2022. 5. 26 선고 2020구합73847 판결; 광주지방법원 2022. 6. 16 선고 2020구단11377 판결.

21) CNN(2023. 5. 23.), "'Verified' Twitter accounts share fake image of 'explosion' near Pentagon, causing confusion", https://edition.cnn.com/2023/05/22/tech/twitter-fake-image-pentagon-explosion/index.html (2024. 10. 3. 최종 방문).

면도 있다. 그 때문에 CCTV의 설치를 늘려달라는 요청도 손쉽게 제기된다. 감시가 지닌 긍정적 측면이 강조된 덕분이다. 그렇지만 전통적으로는 오히려 감시의 부정적 측면이 주목받았다. 감시는 우리의 자유를 침해하는 것으로 기피 대상이 되고는 하였다. 즉, 감시는 이중적 의미를 내포하는데, 그 때문에 감시의 규범적 의미를 정확하게 분석하고 평가하는 것이 쉽지 않다.

'감시(監視)'의 사전적 의미는 "단속하기 위하여 주의 깊게 살핌"이다.[22] 즉, 감시는 통제가 목적으로 전제된 행위라고 보아도 무방할 것이다. 법령에서도 감시라는 용어가 많이 활용되고 있다. 법령의 제명에서 '감시'를 사용하는 경우는 단 1건이 존재하는데, 이는 2023년 10월 24일 제정되어 2024년 10월 25일 시행 예정인 「기후·기후변화 감시 및 예측 등에 관한 법률」이다. 동법 제1조가 "이 법은 기후·기후변화에 대한 과학적인 감시 및 예측 등에 필요한 사항을 정하여 기후변화로부터 생태계 및 기후체계를 보호하고 공공복리를 증진하는 데에 이바지함을 목적으로 한다"고 규정하는 것에 비추어 감시는 기후변화라고 하는 생태계에 대해 악영향을 미칠 수 있는 요소의 방지 목적을 갖는 행위로 보인다. 기타 법령에서도 마찬가지로 「가상자산 이용자 보호 등에 관한 법률」상의 '이상거래에 대한 감시', 「감염병의 예방 및 관리에 관한 법률」상 '감염병감시', 「자본시장과 금융투자업에 관한 법률」상 '시장감시' 등과 같이 주로 위법행위 또는 공공의 안녕이나 질서 훼손 행위에 대한 통제 목적의 활동에 상응하는 용어로 활용되고 있다. 감시에 대한 사전적 의미나 법률적 의미를 통해 살펴보아도, 결국 감시는 공익적 목적을 달성하기 위한 통제 행위라는 이중적 의미를 가지는 것으로 볼 수 있다.

감시에 대하여 학문적으로 가장 체계적이고 심도 있는 성과를 거둔 학자로는 인문·사회 분야를 통틀어 20세기 최고의 석학인 Michel Foucault(1926~1984)를 꼽을 수 있을 것이다. M. Foucault는 Jacques Derrida나 Gilles Deleuze와 더불어 포스트모더니즘(postmodernism)을 대표하는 프랑스 철학자로서 감시를 실

22) 국립국어원, 표준국어대사전, https://stdict.korean.go.kr/search/searchView.do (2024. 10. 3. 최종 방문).

증적 분석을 바탕으로 정교하고 설득력 있게 분석함으로써 이후 다양한 학문 영역을 탐구하는 많은 이에게 영향을 미쳤다. 또한 M. Foucault의 이론은 자신의 극적인 삶과 결부되면서 큰 울림을 주기도 하였다.[23] M. Foucault는 많은 영역에서 독창적인 사유를 전개하였는데, 감시로 대변되는 권력과 통치성에 대한 섬세한 분석과 비판은 인공지능을 활용한 지능형 감시가 점점 더 확대되는 오늘날의 상황에서 검토의 시의성이 높다고 말할 수 있다. 이에 아래에서는 감시에 관한 논의를 중심으로 하여 M. Foucault가 권력과 통치성을 어떻게 파악했는지를 본격적으로 살펴보기에 앞서, 그의 이론을 간략히 살펴보고자 한다.[24]

나. M. Foucault의 이론 개관

1) M. Foucault의 이론과 근대 사상

M. Foucault의 이론에서 가장 먼저 눈에 띄는 점은 근대성 또는 근대 사상에 대한 비판이라 할 수 있다. 마치 제1세대 프랑크푸르트학파가 그랬던 것처럼 M. Foucault 이론에서는 근대성을 향한 설득력 있는 비판이 전면에 등장한다.[25] 따라서 M. Foucault의 이론을 조감하려면 그가 비판 대상으로 삼았던 근대 사상의 특징을 개관할 필요가 있는데,[26] 그 특징 가운데 가장 먼저 언급할 만한 것으로는 주체 중심적 사고를 들 수 있다.[27] 그 점에서 근대 사상을 대변하는 근대 철학을 주체 중심 철학으로 지칭하기도 한다. 주체 중심적 사고는 주체와 객체를 개념적·

---

23) 이에 관하여는 慎改康之(2019), 『ミシェル·フーコー: 自己から脱け出すための哲學』, 岩波新書, 2-4쪽 참고.

24) M. Foucault를 간략하게 소개하는 경우로는 양운덕(2003), 『미셸 푸코』, 살림출판사 참고.

25) 그 점에서 프랑크푸르트학파 제1세대에 속하는 Theodor W. Adorno와 M. Foucault를 분석하는 연구로는 양운덕(1994), “계몽적 이성과 지배: 아도르노와 푸코의 이성비판”, 《철학연구》 제18권, 고려대학교 철학연구소, 116-147쪽 참고.

26) 근대 사상의 특징에 관하여는 양천수(2022), “현대사회의 구조변혁과 법규범의 대응방향”, 《인간연구》 제46호, 가톨릭대학교 인간연구소, 37-75쪽 참고.

27) 이에 관하여는 김원식(2002), “근대적 ‘주체’ 개념의 비판과 재구성: 주체의 자기 관계와 상호 주관성”, 《해석학연구》 제9집, 한국해석학회, 191-219쪽 참고.

실체적으로 구별한다. 이때 주체와 객체는 수평적 관계를 맺기보다는 수직적 관계를 형성한다. 이로 인해 객체, 가령 물건은 주체의 수단으로 취급된다. 반면 객체에 우월적 지위를 획득하는 주체는 이성을 갖춘 합리적이고 자율적인 존재로 상정된다. 여기서 자율적인 존재란 스스로 올바른 법칙을 찾아 이를 따를 수 있는 존재를 뜻한다.[28)]

이처럼 주체 중심적 사고는 이성 및 합리성과 밀접하게 연결된다. 이렇게 연결된 이성과 합리성은 긍정의 의미, 발전의 의미를 지닌다. 개별 주체를 포함하는 사회는 이성과 합리성에 힘입어 더욱 나은 사회로 발전할 수 있다는 것이다. 계몽주의와 공리주의가 이를 예증한다. 이성을 지닌 주체를 계몽하면 자유가 더욱 증진하고 이를 통해 사회 전체의 공리(utility)도 확장될 수 있다는 것이다.

이러한 이념은 자본주의로 제도화되어 나타난다. 자본주의에 따르면 시장은 자유와 평등이 보장되는 거래 공간이다. 이러한 시장에 참여하는 주체는 합리적인 경제적 존재로 전제된다. 이들이 시장에서 자유롭고 평등하게 활동하고 거래하면서 시장은 이른바 보이지 않는 손을 통해 공리를 극대화한다. 이에 힘입어 사회의 이익 역시 극대화된다. 이는 사회를 더욱 나은 사회로 발전시킨다.

근대 사상의 이념 아래 근대법의 역할도 다음과 같이 규정된다.[29)] 근대법은 이성을 지닌 합리적 주체를 정상인으로 설정한다. 이러한 정상인이 활동하는 공간을 사회로 규정하면서 사회의 자유를 최대한 보장하고자 한다. 이를 위해 정치권력에 관해 두 가지 장치가 마련된다. 민주주의와 법치주의가 그것이다. 민주주의를 통해 신이 부여한 절대권력이었던 주권은 왕 개인에서 국민 전체로 이양된다. 나아가 법치주의에 의해 국가권력은 합법적으로 제어된다. 국가권력이 자유로운 공간인 사회에 자의적으로 개입하는 것을 제한한다. 이에 바탕을 두어 자유가 최적화된 사회 질서가 형성된다. 근대법은 이러한 사회 질서를 보장하기 위해 일탈행위

---

28) 이는 Kant 철학에서 극명하게 나타난다. 이를 분석하는 경우로는 심재우(2020), 『열정으로서의 법철학』, 박영사, 175쪽 이하 참고.

29) 근대법에 관하여는 양천수(2009), “법의 근대성과 탈근대성: 하버마스와 투렌의 기획을 중심으로 하여”, 《법학연구》 제50권 제1호, 부산대학교 법학연구소, 161-191쪽 참고.

와 범죄를 규율한다. 이에 손해배상이나 형벌과 같은 제재를 부과한다. 이들 행위는, John Stuart Mill의 관점에서 말하면, 사회에 해악(harm)을 미치는 행위이기 때문이다.

2) 개인적 체험

M. Foucault는 위에서 살펴본 근대 사상, 즉 근대적 사고와 대결하면서 자신의 독창적인 이론을 구축하였다. 이는 M. Foucault 자신의 개인적 사정과도 관련이 없지 않은데, 그 자신이 사회적 소수자에 속했기 때문이다. 동성애자였던 M. Foucault는 이성애자를 정상인으로 설정한 근대적 사고에 거부감을 가졌다. 스스로 마약을 복용하기도 하고 학생운동을 지원하기도 하였다.[30] 이러한 개인적 상황이 이론과 결합하여 근대 사상에 대한 M. Foucault의 비판으로 이론화된 것이다.

3) 방법

물론 개인적 거부감을 설득력 있는 이론으로 승화하려면 이를 뒷받침할 수 있는 탄탄한 방법이 필요하다. M. Foucault의 이론이 성공을 거둔 이유는 바로 기초가 탄탄한 방법을 사용했기 때문이다. 심리학에서 출발했던 M. Foucault의 방법은 인간학을 거쳐 유명한 지식 고고학 및 계보학으로 발전하였다.[31] 쉽게 말해 M. Foucault는 역사적 분석 방법에 힘입어 방대한 문헌을 검토하고 이를 통해 담론의 역사적 계보를 분석하였다. 설득력 있는 비판이론을 정초하기 위해 치밀한 실증적인 방법을 사용한 것이다. 이를 토대로 하여 M. Foucault는 근대적 사고가 어떻게 권력을 은폐하고 활용하는지 드러내고 비판한다.

4) 주체 중심 사고 비판

M. Foucault는 근대 사상의 핵심인 주체 중심 철학을 비판한다.[32] 상호주관성

---

30) 愼改康之, 앞의 책, 2-4쪽 참고.

31) 愼改康之, 위의 책, 10쪽 이하 참고. 고고학적 방법을 보여주는 경우로는 Foucault, M.(2000), 『지식의 고고학』, 이정우 (역), 민음사 참고. 계보학적 방법에 관하여는 Foucault, M.(2023a), 『감시와 처벌: 감옥의 탄생』, 오생근(역), 나남 참고.

32) 이에 관하여는 양운덕(1997), “푸코의 권력계보학: 서구의 근대적 주체는 어떻게 만들

(Intersubjektivität)으로 근대 주체 철학의 긍정적 의미를 복원하고자 한 독일의 사회철학자 Jürgen Habermas와는 달리 M. Foucault는 주체를 권력, 즉 통치의 산물로 파악한다. 주체를 선험적 개념으로 파악한 Kant와는 달리 M. Foucault에게 있어서 주체는 권력작용으로 만들어진 개념에 해당하였다. 이는 권력작용에 바탕을 둔 동일성 역사의 산물이다.[33] 이때 동일성의 기준은 이성과 자율성을 갖춘 정상인이다. 따라서 광기에 시달리는 환자는 비정상인으로서 주체성을 인정받지 못한다. 이러한 M. Foucault의 주장에 의할 때 주체란 구성된 개념이다.[34] 이 점에서 주체는 선험적 사고가 아닌 구성주의적 사고와 연결된다.[35] M. Foucault에 따르면 주체 개념의 전제가 되는 구별 자체가 동일성을 지향하는 권력이 작용한 결과이다.

5) 계몽주의 비판

이의 연장선상에서 M. Foucault는 근대 계몽주의를 비판한다. 계몽주의는 이성에 힘입어 사회가 발전한다고 믿었다. 이때 사회가 발전한다는 것은 개별 주체의 자유가 확장된다는 것으로 이해할 수 있다. 사회 발전을 개인의 자유 확장으로 파악한 것이다. 자유가 확장된다는 것은 자유를 억압하는 권력이 축소 또는 적절하게 제한된다는 것을 뜻한다.

그러나 M. Foucault에 따르면 계몽주의는 권력을 미시화하여 은폐하는 과정에 불과하다. 계몽주의를 통해, 이에 연결된 합리화를 통해 절대권력은 미시 권력으로 전환되어 사회 곳곳에 침투되었을 뿐 권력이 사라진 것은 아니다. 이는 다음과

어지는가?", 《경제와사회》 제35권, 비판사회학회, 106-142쪽 참고.

33) 이에 관하여는 양운덕(1991), "탈구조주의 사회 이론의 기초", 《시대와 철학》 제3호, 한국철학사상연구회, 144-146쪽 참고.

34) 비판이론이 아닌 정보철학의 관점에서 주체를 구성 개념으로 파악하는 경우로는 박충식·김형주(2022), "구성주의적 정보 철학의 관점에서 본 근대와 그 이후의 주체 개념", 《인공지능인문학연구》 제12권, 인문콘텐츠연구소, 139-158쪽 참고.

35) 뇌과학의 성과를 반영하여 주체와 밀접하게 관련되는 자아의 실체성을 비판하는 경우로는 Berns. G.(2024), 『'나'라는 착각: 뇌는 어떻게 인간의 정체성을 발명하는가』, 홍우진(역), 흐름 출판 참고.

같이 설명할 수 있다.

앞에서 언급한 것처럼 민주주의와 법치주의가 안착하면서 정치권력이 지녔던 절대권력은 제한된다. 이는 사회 전체의 복잡성이 증가하고 기능적 분화가 진행되면서 더욱 심화한다.[36] 사회 전체가 다양한 기능 영역으로 분화되면서 정치권력의 힘은 점차 약화되었다. 반대로 사회의 다른 기능 영역, 가령 경제나 법, 교육, 학문, 의료 영역 등의 영향력은 강화되었다. 이로 인해 언뜻 보면 권력이 약해진 것처럼 보인다. 하지만 실제로 권력은 기능적으로 분화된 사회 각 영역에 침투하여 힘을 발휘한다. 예를 들어 경제 영역에서는 경제 권력으로, 교육 영역에서는 교육 권력으로, 학문 영역에서는 지식 권력으로 작용한다. 이게 가능한 이유는 권력이 바로 담론권력으로 전환되어 사회 각 영역에 침투하였기 때문이다. 담론은 사회 어느 한 영역에서만 이루어지는 게 아니라 사회가 있는 곳이면 어디에서든 이루어지기 때문이다.

6) 공리주의 비판

같은 맥락에서 Jeremy Bentham으로 대표되는 공리주의 역시 비판 대상이 된다. 이는 Bentham이 설계한 판옵티콘(Panopticon)에 대한 비판에서 확인된다. 최대 다수의 최대 행복을 추구하는 공리주의를 형벌이론으로 구체화한 일반예방이론에 따르면 판옵티콘이 상징화하는 감옥은 다음은 같은 의미가 있다. 한편으로 감옥은 범죄자를 공간적으로 격리함으로써 일반 시민의 안전을 보장한다. 다른 한편으로 감옥은 정상인의 규범에서 일탈한 범죄자를 재사회화함으로써 이들이 정상인으로 복귀하도록 돕는다. 그러나 M. Foucault에 따르면 이는 공리를 극대화한다는 명목 아래 범죄자로 표상되는 비정상인의 신체에 관한 규율권력을 강화할 뿐이다. 말하자면 M. Foucault에 따르면 공리주의란 권력의 또 다른 변화 형식에 불과한 것이다.

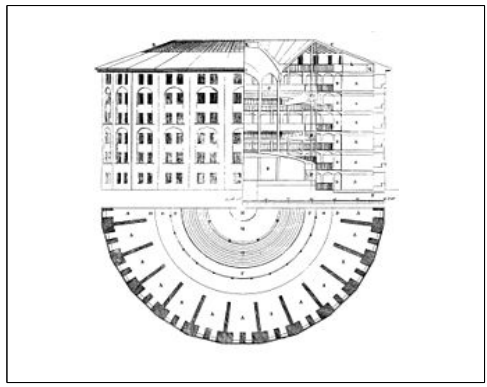
---

36) 사회의 기능적 분화에 관하여는 Kneer, G./Nassehi, A.(2008), 『니클라스 루만으로의 초대』, 정성훈(역), 갈무리, 149쪽 이하 참고.

다. M. Foucault에게 있어 감시의 의미

M. Foucault는 1975년에 출간한 자신의 저서 『감시와 처벌: 감옥의 탄생(*Surveiller et punir: Naissance de la prison*)』을 통해서 현대사회가 개인에 대한 감시가 일상이 된 구조이며, 사회적 감시는 인간을 통제하는 새로운 권력의 기제로 작용함을 밝히고 있다. 특히, M. Foucault는 형벌의 역사적 변천을 분석하면서 권력이 어떻게 변화하였는지를 관찰하였는데, 초기의 형벌은 범죄자의 사지를 찢어 죽이는 등 공개적으로 잔인하게 신체에 대한 고통을 가하는 이른바 신체형이 주를 이루었다.[37] 18세기 후반 프랑스 혁명을 거쳐서 19세기에 들어서는 이와 같은 신체형은 점차 줄어들어서 19세기 중반에는 많이 사라지게 되었고, 그 대신 감옥이라는 공간적 도구를 활용하여 범죄자를 통제하기 시작하였다.[38] 여기에서의 감옥은 단순히 죄수의 신체 자유를 제한하는 데만 의미가 있는 것이 아니라, 죄수를 효율적으로 감시할 수 있는 수단이 된다는 것에도 큰 의미가 있다. M. Foucault가 공리주의의 창시자인 철학자 Jeremy Bentham이 고안한 원형 감옥인 판옵티콘에 주목한 까닭이 이러한 지점과 맞닿아 있다.

[그림 2-1] 판옵티콘의 설계도



자료: Wikipedia 홈페이지[39]

37) Foucault, M.(2023a), 『감시와 처벌: 감옥의 탄생』, 오생근(역), 나남, 33쪽.
38) Foucault, M.(2023a), 위의 책, 45쪽 이하.

판옵티콘의 중앙에는 여러 개의 큰 창문이 뚫려 있는 높은 감시탑이 위치하고, 감시탑의 바깥 둘레를 따라서 죄수들의 방이 자리 잡고 있다. 감시탑에서는 죄수들의 방 내부가 보이지만, 죄수들의 방에서는 감시탑이 보이지 않도록 설계되어 있다. 이러한 구조는 죄수에게는 감시자의 시선이 자신에게 향하는지 알 수가 없게 한다. 감시자 1인의 존재만으로도, 혹은 감시자가 존재하지 않더라도 죄수는 상시적으로 감시받는다는 심리적인 압박을 받게 될 것이다. 즉, 이러한 불가시성은 질서를 보장하게 하여, 수감자가 음모를 꾸미거나 탈옥을 꾸밀 수 없도록 통제하게 되는 것이다.[40]

그런데 M. Foucault는 이러한 판옵티콘의 메커니즘이 감옥의 설계에 그치는 것은 아니라고 한다. 죄수를 교화하기 위한 감옥에서뿐만 아니라 병원, 학교, 작업장 등에서 병자의 간호, 학생의 교육, 노동자의 감시에 이용할 수 있다고 한다.[41] 판옵티콘은 근대사회의 권력이 작동하는 하나의 전형에 불과하다. 감옥에 갇힌 죄수가 아니더라도 근대사회에서는 모든 인간이 판옵티콘과 같은 구조 속에서 감시받거나 혹은 감시를 받지는 않더라도 감시받는다는 느낌을 받게 되어 결국 감시자, 즉 그 사회의 권력자가 요구하는 바대로 자기 행동을 맞추어 가게 되는 것이다.[42]

M. Foucault가 판옵티콘을 통해 바라보았던 근대사회의 특성은 오늘날과 같은 디지털 사회에서도 마찬가지로 적용된다. 현대사회에서는 개인에 대한 감시가 인간을 통해서 순간적으로 이루어지거나 고작해서 수기로 기록되는 수준이 아니다. 수많은 CCTV가 불특정 다수를 촬영한 영상이 저장되고 있고, 자신이 컴퓨터를 통해서 접속하거나 작성한 내용은 기록되고 있으며, 자신도 모르게 행한 발언과 행동이 기록되어 전자자료로 남아 있게 된다. 개인에 대한 감시가 일상화된 현대

39) https://en.wikipedia.org/wiki/Panopticon (2024. 10. 3. 최종 방문).
40) Foucault, M.(2023a), 앞의 책, 368쪽.
41) Foucault, M.(2023a), 위의 책, 377쪽.
42) 한희진(2012), “미셸 푸코의 파놉티시즘에서 인식, 권력, 윤리의 관계”, 《의철학연구》 제13호, 한국의철학회, 77쪽.

사회는 '디지털 판옵티콘의 사회'로 명명될 수도 있을 것이다.[43] 사실 정보통신기술이 발달함에 따라 현대사회가 전자감시사회가 될 수 있다는 우려는 20세기 후반부터 이미 나타나고 있었다.[44] 1990년대 PC통신 시절에도 국가의 감시에 대한 문제 제기가 있었다.[45] 그런데 인공지능 기술은 이러한 과거의 정보통신기술이 불러일으켰던 우려의 수준을 훨씬 뛰어넘는다. 개개인과 관계되는 빅데이터를 비교할 수 없을 정도로 빠르게 처리하고, 또한 이를 통해서 알고리즘을 스스로 생성해 낼 수 있다. 결국 이러한 인공지능 알고리즘이 프로파일링하여 개인을 식별해 내기도 하지만, 앞서 살펴본 편향성 등의 위험이 나타나기도 한다.

근대 이후의 감시는 감시라는 목적과 관계없이 피감시자의 자율적인 행동을 위축시키는 효과를 가진다. M. Foucault에게 있어서 감시는 권력과 크게 연관이 되어 있다. 특히, 감시는 권력의 개념을 변화하게 하는 큰 원동력이 되었다.

2. M. Foucault의 권력 개념에 있어 감시의 역할

가. M. Foucault의 권력 이론 개관

M. Foucault에게 있어서 권력은 주로 권력관계라는 개념으로 나타난다. 이는 권력이 누구에게 있느냐의 문제라기보다는 권력이 행사되는 공간과 환경에 더욱 집중하는 것으로서, 권력에 관한 연구에서 사회조직의 역학 관계의 다양성을 중요하게 파악하는 것이다.[46] M. Foucault는 사회를 하나의 권력이 작동하는 단일체가 아니라고 보았고, 상이한 권력이 특수성을 유지하면서 병치, 연결, 결집, 위계

---

43) Foucault, M.(2023a), 앞의 책, 15쪽(이 부분은 옮긴이 서문에 해당함).

44) 김동윤(2006), "정보테크놀로지, 전자감시, 그리고 프라이버시 위기: 푸코와 루크스의 권력개념을 중심으로", 《사이버커뮤니케이션학보》 통권 제18호, 사이버커뮤니케이션학회, 45쪽.

45) 매일신문(1994. 5. 3.), "PC통신 표현의 자유 사생활 보호 "비밀보장을"", https://www.imaeil.com/page/view/1994050308531057886 (2024. 10. 3. 최종 방문).

46) 박병락(2009), "Foucault의 권력 개념과 학교교육", 《교육사상연구》 제23권 제3호, 한국교육사상연구회, 258쪽.

를 이루고 있다고 설명한다.[47] 흔히 권력은 권력자 또는 지배자가 피권력자 또는 피지배자에 대해 행하는 억압 정도로 이해되었고, 따라서 권력에 관한 탐구 역시 이러한 권력의 정당성을 확보하는 문제에 관심을 가졌다.[48] 그러나 M. Foucault는 권력의 소유에 관한 문제보다는 사회조직이나 사람 간의 관계에 집중하였다.

근대 이전의 형벌이 잔혹함을 보인 것은 당시의 주권자인 군주가 사법적 수단을 통해 무한한 권력을 명시하는 행위였던 것이다.[49] 즉, 이 시대의 권력은 개념적으로 주권권력에 해당하는 것인데, M. Foucault는 근대 이후의 권력관계는 이러한 주권권력에 비추어서는 설명할 수 없고, 특히 권력의 역동성을 국가 또는 정치구조보다는 사회 전체를 관통하는 미시적인 관계망에서 찾고자 하였다.[50] 형벌에 관하여도, 근대에 들어와서는 민주주의의 발전과 더불어 신체형보다는 죄수의 교정 필요성이 커지면서, 감옥이라는 감시 장치가 감시자와 피감시자의 관계를 형성하고 피감시자인 죄수를 효과적으로 순종하게 만드는 것이다. 즉, 감옥이란 당시 군대나 학교를 운영한 경험을 통해서 범법자를 법에 복종하는 인간으로 변화시키기 위해 고안된 장치였던 것이다.[51]

M. Foucault에게 있어서 권력의 속성이자, 권력의 지향점은 피권력자를 '순종하는 신체'로 만드는 것이다.[52] 신체 활동을 면밀하고 효율적으로 통제하는 방법을 '규율(discipline)'이라고 한다.[53] 즉, 과거의 주권권력 아래에서는 왕이라고 하는 주권자이자 권력자의 공포심이 신체를 순종하게 하는 규율이었다면, 근대에 들어와서는 '감시'라고 하는 메커니즘이 피권력자에 대한 규율인 것이다.

M. Foucault에게 있어서 권력에 대한 탐구는 주권권력에 대한 물음이 아니라

---

47) Foucault, M.(2023b), 『권력과 공간』, 이상길(역), 문학과지성사, 18쪽.
48) 김정경(2016), 미셸 푸코의 통치성 개념 연구, 석사학위 논문, 이화여자대학교, 12쪽.
49) Foucault, M.(2023a), 앞의 책, 107쪽.
50) 김용규(2018), "주권권력에서 생명권력으로 「성의 역사 1 - 앎의 의지」를 중심으로-", 《코기토》 제85호, 부산대학교 인문학연구소, 338쪽.
51) Foucault, M.(2023b), 앞의 책, 32쪽.
52) Foucault, M.(2023a), 앞의 책, 253쪽.
53) Foucault, M.(2023a), 위의 책, 254-255쪽.

사회와 개인, 조직과 개인, 개인과 개인이라고 하는 관계와 공간 속에서 드러나는 '규율권력(disciplinary power, pouvoir disciplinaire)'의 전개 과정이 대상이다. 여기에서 감시는 앞서 살펴본 판옵티콘의 사례에서와 같이 감옥 내에서 감시자가 피감시자를 감시하는 것을 넘어서서 사회 전체에 내재하고, 감시를 통한 보상과 처벌이 자연스러운 현상이 되었다. 물리적인 상벌이 없더라도, 실제 감시를 받는 여부와 관계없이 피감시자는 심리적으로 감시라는 메커니즘에 자신의 신체를 권력에 순종시킨다. 현대사회에서도 이러한 감시와 상벌의 메커니즘은 작동하고 있다. 이는 바로 감시를 통한 위계질서의 기술과 규범화를 통한 상벌제도의 기술이 결합된 '평가'이다.[54] 감시자는 피감시자를 평가라는 명목으로 감시하고, 그에 따르는 상벌을 제공한다. 그러나 상벌과는 관계없는 피감시자도 그러한 위계질서와 규범에 복종하는 결과가 나타나게 된다.

그런데 이러한 근대시대의 규율권력이 감시를 통해서 개인의 신체를 순종시키는 것이었지만, M. Foucault는 권력의 성격이 억압적이라기보다는 생산적인 것으로 보았다. 즉, 18세기 말부터 권력이 작동하는 메커니즘은 '신체로서의 개인'과는 구별되는 '종으로서의 인간', 즉 생명에 대한 관리 혹은 인구 전체를 조절하는 권력, 이른바 '생명권력(bio-power, bio-pouvoir)'에 해당한다는 설명이다.[55] 인구는 물질과 연결되어 생물학적으로 존재하는 개인들의 무리이고, 사람들은 자신들이 살아가는 환경 속에서 각종 사건과 상호작용하면서 살아가는데, 인구 조절 차원에서 이와 같은 환경에 개입하는 권력이 생명권력 내지 생명관리권력인 것이다.[56] 이러한 권력은 피권력자에 대한 억압, 금지, 통제와 같은 '죽이는 권력' 또는 '살게 내버려두는 권력'보다는 '살리는 권력' 또는 '죽게 내버려두는' 권력에 해당한다.[57] 다만, 생명권력은 규율권력을 배제하는 것이 아니라, 오히려 상호 효과적

54) Foucault, M.(2023a), 위의 책, 342쪽.
55) Foucault, M.(2023b), 앞의 책, 245쪽.
56) Foucault, M.(2023c), 『안전, 영토, 인구』, 심세광·전혜리·조성은(역), 난장, 18쪽 이하.
57) 은재호(2011), "규율과 통치: 조직연구에 있어서 Michel Foucault 권력론의 함의와 기여", 《한국조직학회보》 제8권 제2호, 한국조직학회, 18쪽.

으로 결합하거나 생명권력이 규율권력을 포섭하기까지도 한다.[58]

이러한 M. Foucault의 감시와 권력 개념은 오늘날과 같은 인공지능 시대 혹은 인공지능 감시 시대에서도 여전히 큰 의미가 있다. 국가와 개인과의 관계에 있어 인공지능의 활용은 개인에 대한 국가의 감시 효율성을 높이는 것은 물론이고, 국가가 원하는 방향으로 통제하는 데 활용하는 좋은 수단이 될 수 있다. 그것이 규율권력의 요소나 성격만을 고려한 활용은 아니라고 하더라도, 생명권력의 측면에서 사회와 그 사회를 구성하고 있는 개개인을 통치자가 원하는 방향으로 이끌 수 있는 도구가 되기 때문이다.

나. 감시의 대상

앞서 살펴본 바와 같이 M. Foucault가 저서 『감시와 처벌: 감옥의 탄생』을 통해 분석하는 감시는 부제가 시사하듯이 범죄자를 대상으로 한다. 범죄자가 공간적으로 격리된 감옥에서 탈출하지 못하도록 하는 것이 감시이다. 그 점에서 감시는, 인권법학의 관점에서 보면, 범죄자의 인권과 기본권을 제한하는 형사사법의 전형적인 통제 수단이다.[59] 이때 주목할 부분은 범죄자라는 인적 존재이자 감시 대상이다. 범죄자는 일반 시민과 구별된다. 근대적 사고의 기반이 되는 '정상과 비정상의 구별'을 활용하면 일반 시민이 정상인이라면 범죄자는 비정상인에 해당한다. 이렇게 보면 감시는 비정상인을 통제하기 위한 수단이라 볼 수 있다.

이러한 이분법에 따르면 M. Foucault는 그 자신이 비정상인의 범주에 속했고, 이에 범죄자를 대상으로 하는 감시라는 통제 수단에 관심을 기울인다. 감시가 어떠한 권력 메커니즘이 작용하는지 규명한 것이고, 근대사회에서 감시가 범죄자에만 한정되는 게 아니라는 점에 주목한 것이다. 감시는 범죄자뿐만 아니라 사회에서 넓은 의미의 비정상인까지 확대된다는 점을 규명한다. 예를 들어 병원에서 환자나 학교에서 학생 등에도 감시가 이루어진다. 환자, 그중에서도 광기에 시달리는 환자는 정상인이 아닌 비정상인이다. 학생 역시, Kant의 관점에서 보면 계몽

58) Foucault, M.(2023b), 위의 책, 246쪽.

59) 인권법학에 관하여는 양천수(2023), 『인권법이론』, 박영사 참고.

되어야 할 대상이기에, 정상인인 성인과 비교할 때 비정상인의 범주에 속한다. 그 점에서 감시는 단순히 범죄자에 한정되어 투입되는 형사사법 통제 수단에 그치는 게 아니다. 감시는 사회 전체에서 비정상인을 통제하는 수단, 더욱 정확하게 말하면 규율권력이 작용하는 매체에 해당한다.[60)]

다. 감시의 이중성

여기에서 간과해서는 안 되는 점은 감시가 이중적 성격을 지닌다는 것이다. 이는 감시가 규율권력이라는 점과 크게 관련이 있다. 이는 규율권력은 본질적으로 이중적이기 때문이다. 나아가 감시는 인지(cognition)에서 출발한다는 점을 의식할 필요가 있다. 감시는 인지의 일종이다. 인지는 외부 세계의 정보를 받아들이는 과정이다. 인지 과정이 있어야 판단 및 결정도 가능해진다. 예를 들어 사회복지 국가에서 선별적·맞춤형 복지를 실현하려면 이것이 필요한 사회적 약자에 관한 정보가 요청된다. 이러한 정보는 인지 과정을 통해 수집된다. 어떤 인식관심 또는 선이해에 바탕을 두는지에 따라 이 같은 인지는 어떤 경우에는 맞춤형 복지를 위한 정보 수집 활동으로, 또 어떤 경우에는 비정상인에 대한 감시 활동으로 구체화되어 작동한다. 이 점에서 감시는 이중적 성격을 갖게 된다. 비정상인을 '보호'한다는 측면에서는 긍정적 의미로, 비정상인을 '통제'하고 '배제'한다는 측면에서는 부정적 의미로 사용된다. 이는 규율권력 자체가 포섭(inclusion)과 배제(exclusion), 달리 말해 생산과 배제를 동시에 가진다는 점과 무관하지 않다.

이러한 이중성은 판옵티콘으로 상징화되는 감옥에서 이루어지는 수형 과정 자체에서도 확인된다. 감옥이 재사회화의 공간인지 아니면 통치를 위한 규율권력의 장치인지의 문제이다. 근대 형사사법체계에서 형성된 감옥은 범죄예방을 목적으로 하는 일반예방의 측면에서 범죄자를 가둔다. 동시에 감옥은 범죄자를 재사회하는 교육 공간으로 활용된다. 감시와 결합한 재사회화 프로그램을 통해 범죄자는 사회에 복귀할 수 있는 교육을 받는다. 이는 정상인인 일반 시민의 관점에서 보면

60) 이에 관한 분석으로는 정규영(2013), "미셸 푸코의 '규율 권력'과 근대 교육", 《교육사학연구》 제23권 제2호, 교육사학회, 157-201쪽 참고.

바람직한 일이다. 사회에서, 질서에서, 정상인에서 배제되었던 범죄자를 다시 사회 안으로 포섭하는 절차이기 때문이다. 그러나 범죄자의 시선에서 보면 이는 강제적으로 자신을 타자가 결정한 정상인의 길로 가게 하는 것일 뿐이다. 범죄자는 과연 누가 정상성과 비정상성을 결정할 수 있을지에 대한 문제를 제기할 것이다. 이 같은 시선에서 보면 재사회화 과정이란 자신을 억압하는 규율권력이 작동하는 과정일 뿐이다.[61]

바로 이 같은 이유에서 감시를 일도양단적으로 평가하기는 어렵다. 감시는 억압이지만 동시에 보호 장치이다. 예를 들어 의약품의 위험을 지속적으로 관리하기 위해서는 의약품이 시장에 출시된 이후에도 약물감시가 필요하다.[62] 그 점에서 한편으로는 감시가 가져다주는 유용성을 최대한 유지하면서도 다른 한편으로는 감시가 남용되는 것을 막을 수 있도록 감시의 한계선을 적절하게 설정하는 게 중요하다.

라. 권력의 변화

1) 의의

『감시와 처벌: 감옥의 탄생』에서 『성의 역사』로 이어지는 M. Foucault의 연구를 보면, 근대사회 이후 권력이 어떻게 변화되었는지에 관한 M. Foucault의 설득력 있는 통찰을 발견할 수 있다.[63]

---

61) 바로 이 점에서 재사회화 프로그램은 실제 수형 과정에서 성과를 거두지 못하게 되는 것이다.

62) 의약품 규제에 관하여는 양천수(2024), “유럽연합 의약품 법제 동향: 의약품 개혁 법안을 중심으로”, 《글로벌법제전략연구사업》 2024년 제1호, 한국법제연구원 참고.

63) ‘성의 역사’에 관한 국내 번역 문헌으로는 Foucault, M.(2007), 『성의 역사 1: 앎의 의지』, 이규현(역), 나남; Foucault, M.(2018), 『성의 역사 2: 쾌락의 활용』, 문경자·신은영(역), 나남; Foucault, M.(2004), 『성의 역사 3: 자기 배려』, 이혜숙·이영목(역), 나남; Foucault, M.(2019), 『성의 역사 4: 육체의 고백』, 오생근(역), 나남 참고. M. Foucault의 권력 이론에 관하여는 조광제(1991), “미셸 푸코의 권력론”, 《시대와 철학》 제2호, 한국철학사상연구회, 149쪽 이하; 고승규(1999), “『성의 역사』를 통해 본 푸코의 권력이론”, 《강원인문논총》 제7집, 강원대학교 인문과학연구소, 229-246쪽 참고.

2) 거대 권력에서 미시 권력으로

먼저 사회가 발전해 가면서 절대 왕정이 보여주었던 절대적인 거대 권력이 정교한 미시 권력으로 변화되었다는 점을 언급할 수 있다. 이는 사회의 합리화, 달리 말해 정치권력의 민주주의화 및 법치주의화와 관련을 맺는다. 절대 왕정이 주권이라는 이름으로 지녔던 절대권력은 민주주의가 국가의 구성 원리로 자리매김하면서 국민주권으로 변모하였다. 이에 따라 정치권력의 정당성 기초가 바뀌었다. 이를테면 과거에는 신이라는 초월적 존재가 정치권력의 정당성 기초가 되었다면 이제는 주권자인 국민의 의사가 정당성의 기초가 된다. 더불어 사회학자 Max Weber가 강조한 형식적 합리화를 대변하는 법치주의화에 힘입어 정치권력의 행사 자체에 대한 법적 통제가 점점 더 강화되었다. 이러한 변화에 발맞추어 절대 왕정이 가졌던 거대 권력은 적절하게 제어되는 것으로 보였다.

그러나 권력 자체가 사라진 것은 아니었다. 권력은 사회가 변화하면서 미시 권력으로 변모하였다. 이는 앞에서 언급한 사회의 기능적 분화와도 관련을 맺는다. 사회의 기능적 분화가 진행되면서 정치권력이 총체적으로 지녔던 권력 자체도 사회의 다양한 기능 영역으로 분할되었다. 동시에 권력은 사회 각 영역에서는 다른 그 무엇, 가령 사회학자 Niklas Luhmann식으로 말하면 매체(Medium)의 모습으로 변모하였다.[64] 이러한 과정을 거치면서 권력은 미세화되고 은폐되었다.

3) 물리적 권력에서 담론권력으로

이러한 변화는 권력이 물리적 권력에서 담론권력으로 바뀌는 것과 결합해서 이루어진다. 일반적으로 권력은 타자를 권력자의 의지에 복종시키는 힘을 뜻한다. 이러한 권력은 전근대 사회에서는 폭력이라는 물리적 힘과 결합되어 표현되었다. 예를 들어 절대권력은 형벌로 대표되는 물리적 힘과 결합하여 통치 대상자에게 발현되었다. 이 점에서 권력은 물리적 권력을 뜻하였다. 이를 보여주는 예가 바로 M. Foucault가 『감시와 처벌: 감옥의 탄생』에서 묘사하는 잔혹한 형벌 권력이다.

---

64) N. Luhmann의 매체 개념에 관하여는 Luhmann, N.(2014a), 『체계이론 입문』, 윤재왕(역), 새물결, 2014, 293쪽 이하 참고.

형벌 권력이나 경찰 권력 그리고 군대 권력은 절대권력을 표현하는 대표적인 장치였다.

하지만 민주주의와 법치주의가 안착하면서 권력은 물리적 권력의 방식으로, 달리 말해 형벌이나 경찰력, 군사력으로 행사되기보다는 자제되는 방식으로, 달리 말하면 상징적으로 표현되는 권력의 방식으로 행사되었다. 이때 활용되는 수단이 담론(discourse)이었다. 권력은 물리적 권력이 배후에 존재하는 담론에 투영되어 상징적으로 행사되었다. 말을 바꾸면 물리적 권력이 행사되는 가능성이 보장된 담론을 활용함으로써 권력은 원하는 목적을 달성하게 되었다. 예를 들어 일탈행위를 저지르는 행위자의 행위가 범죄가 될 수 있다는, 그래서 처벌될 수 있는 담론을 보여줌으로써 권력자는 실제로 형벌 권력을 행사하지 않으면서 행위자를 통치 질서에 복종시킬 수 있게 되었다. 이에 따라 담론 그 자체가 권력이 되는 담론권력이 형성되었다.

4) 영역 권력에서 사회 전체의 권력으로

이처럼 담론권력이 형성되면서 권력이 정치 공간에만 머무는 게 아니라 사회 전체로 확장될 수 있는 계기가 마련되었다. 말하자면 권력이 정치라는 특정한 영역에서만 작동하는 영역 권력에서 사회 전체의 권력으로 변모한 것이다. 이는 권력과 결합한 담론 혹은 이를 포함하는 소통(communication)이 사회의 모든 영역에서 이루어지기 때문이다.[65] 따라서 권력은 담론을 활용하여 사회 곳곳에 침투할 수 있게 되었다. 사회 각 영역을, 사회 모든 구성원을 더욱 미세하게 통제할 수 있게 되었다.

이러한 사고방식은 비판이론의 전통에서 볼 때도 독창적인 것이다. 왜냐하면 예를 들어 가장 대표적인 비판이론가라 할 수 있는 Karl Marx 역시 권력을 영역적으로 사고하였기 때문이다. Marx의 '토대·상부구조론'에 따르면 권력은 법과 마찬가지로 상부구조에 해당한다.[66] 사회 전체가 '토대·상부구조'로 구성된다고 볼

65) 이를테면 N. Luhmann에 따르면 사회는 소통으로 구성되고 존속하는 사회적 체계이다. 이에 관하여는 Luhmann, N.(2014b), 『사회의 사회』, 장춘익(역), 새물결 참고.

때 이는 권력이 상부구조라는 특정한 영역에 속해 작동한다는 점을 시사한다. 이를 반대로 추론하면 경제 영역을 반영하는 토대에는 권력이 작용하지 않는다는 점을 뜻한다. 이처럼 비판이론 전통에서도 권력은 영역적으로 파악되었다. 그 때문에 권력에 대한 저항 또는 혁명이 강조되었다. 이러한 점에서 볼 때 권력을 탈영역적으로 파악한 M. Foucault의 권력 이론에 독창적인 의미가 있다.

5) 자유 억압에서 생명권력으로

권력의 형태가 물리적 권력에서 담론권력으로 변모하면서 권력의 작용 방식도 변화하였다. 기존의 물리적 권력이 주로 권력 대상자인 주체의 자유를 제한하거나 억압하는 방식으로 작용하였다면 담론권력은 주체의 생명 및 신체를 규율하는 생명권력으로 작용한다.[67] 생명권력은 주체의 신체 및 생명을 관리하고 통제한다.

이때 주의해야 할 점은 생명권력은 신체나 생명에 해악을 가한다는 의미가 아니라 신체나 생명의 작동 방식을 통제한다는 의미로서, 즉 규율권력으로서 작용한다는 점이다. 신체나 생명에 해악을 가하는 작용 방식은 오히려 기존의 물리적 권력이 즐겨 사용하는 방식이었다. 형벌 권력이 이를 잘 예증한다. M. Foucault가 『감시와 처벌: 감옥의 탄생』에서 보여주듯이 절대권력은 권력의 존재 의미를 표현하기 위해 형벌 권력을 잔혹하게 사용하였다. 형벌이라는 이름으로 범죄자의 목숨을 빼앗거나 신체 절단과 같은 해악을 가하였다.

이에 반해 생명권력은 담론권력이라는 형식을 이용하여 생명과 신체의 작동 방식을 가령 국가가 원하는 방식으로 정교하게 조종한다. 예를 들어 복지국가라는 명분 아래 국가는 국민이라는 주체의 건강에 개입한다. 건강검진 의무 수검이라는 담론권력을 활용하여 국가가 원하는 방향으로 국민이 건강을 유지할 수 있게끔 통제한다.[68] 또한 국가는 저출생이라는 문제에 대처하기 위해 자녀 출산에 관한

---

66) 토대·상부구조론에 관하여는 Konstantinov, F. et al(1986), 『토대/상부구조론 입문: 사회구성체론의 새로운 이해』, 학민사 편집실(편역), 학민사 참고.

67) 생명권력에 관하여는 양운덕(2011), “생명(관리)권력과 생명정치”, 《진보평론》 제47호, 계간지 진보평론, 159-188쪽; 김현철(2016), “생명정치, 생명권력, 생명법”, 《법과사회》 제51호, 법과사회이론학회, 1-22쪽 참고.

담론을 변화시킨다. 자녀 출산이라는 재생산에 적극적으로 동참하는 게 국가 공동체의 미덕이라는 담론을 강화한다. 이를 통해 재생산이라는 생명의 작동 방식을 규율한다.

이러한 점에서 새로운 권력 형식인 생명권력은 생명이나 신체에 해악을 가하거나 자유를 제한하는 등의 억압적 방식으로 작용하기보다는 권력 대상자인 주체의 삶을 개선하거나 건강을 회복하거나 재생산에 이바지하게 하는 등의 생산적인 방식으로 작용한다. 물론 그렇다고 해서 권력의 또 다른 측면인 자유 제한과 통제가 사라지는 것은 아니다. 예를 들어 주체가 자신의 삶을 개선하기 위해서는 다른 선택지를 제한해야 한다. 건강을 회복하거나 증진하기 위해서는 이에 해가 되는 쾌락 추구 행위를 제한해야 한다. 이는 신체를 지닌 주체에게는 생산이자 통제가 된다. 재생산을 제고하려면 주체가 홀로 있을 자유를 제한하거나 교묘하게 통제해야 한다. 이를테면 가족 공동체를 구성하는 게 행복으로 향하는 길이라는 담론을 형성함으로써 주체가 가족 공동체를 구성하는 데 참여하게끔 해야 한다. 그 점에서 규율권력이라는 의미가 있는 생명권력은 이중적인 성격을 지닌다. 생산적인 성격과 통제적인 성격이 그것이다.

6) 타율 통제에서 자율 통제로

권력 대상자, 달리 말해 통치 대상자의 삶을 개선하거나 건강을 증진하는 등의 규율은 고도로 정교하게 이루어져야 하는 권력 행사이다.[69] 이는 통치 대상자의 내면에 개입하여 이를 바꾸는 권력 행사이기 때문이다. 범죄자의 재사회화를 목표로 하는 적극적 특별예방이론이나 법규범에 대한 일반 시민의 신뢰를 강화하고자 하는 적극적 일반예방이론이 실제로는 성공하기 어렵다는 점이 이를 보여준다.[70]

---

68) 이에 관한 분석으로는 홍은영(2014), “푸코와 우리 시대의 건강 담론: 의료화 현상과 관련하여”, 《철학연구》 제50집, 고려대학교 철학연구소, 187-228쪽 참고.

69) 규율권력은 생산성을 지닌다는 점에서 국가를 조종하는 통치의 수단이 된다. M. Foucault의 통치에 관하여는 M. Foucault et al(2014), 『푸코 효과: 통치성에 관한 연구』, 심성보 외(역), 난장 참고.

70) 일반예방이론이나 특별예방이론에 관하여는 Hassermer, W.(2011), 『범죄와 형벌:

따라서 통치 대상자의 생명에 개입하는 생명권력은 물리적 권력이 흔히 사용하는 타율적 통제보다는 자율적 통제를 선호하게 되는 것이다. 타율적 통제는 통제 대상자의 반발을 야기하지만 자율적 통제, 더욱 정확하게 말하면 자율적으로 보이는 통제는 대상자에게 상대적으로 쉽게 수용될 수 있기 때문이다.

자율적 통제를 구현하기 위해 생명권력은 담론권력과 결합한다. 사회에서 진행되는 담론을 특정한 방향으로 유도하고 규율함으로써 자율적 통제를 실현한다. 이른바 자기계발서를 활용하는 방식을 이러한 예로 언급할 수 있다. 지배적인 담론권력을 통제함으로써 지배적인 담론이 추구하는 방향으로 통제 대상자들이 마치 자율적으로 따라가도록 하는 것이다. 이른바 넛지(nudge)를 활용하는 통제도 자율적 통제를 지향하는 권력 행사 방식으로 볼 수 있다.[71]

3. 권력의 법학적 의미

가. 의의

M. Foucault에게 있어 권력은 관계성을 바탕으로 사회구조나 공간 속에서 다양하고 미세한 요소가 작동함으로써 질서를 생산해 내는 것을 의미한다. 반면 법학에서의 권력은 이보다는 단순하게 다루어지는 것으로 보인다. 여기에서의 권력이 법학에서는 흔히 공권력으로 이해되고 있는데, 공권력을 다루는 법학의 분야는 공법 분야이고, 공법 분야는 대표적으로 헌법과 행정법 분야로 나누어진다.

나. 헌법학에서의 권력

권력, 특히 국가권력의 구조와 작용을 직접 다루는 법 영역은 헌법인데, 우리 「대한민국헌법」은 '권력'이라는 용어를 단 한 차례만 사용하고 있다. 바로 "대한민국의 주권은 국민에게 있고, 모든 권력은 국민으로부터 나온다"고 규정한 제1조 제2항에서 언급된 '권력'이 그것이다. 이는 우리 헌법이 국민주권의 원리에 입각

올바른 형법을 위한 변론』, 배종대·윤재왕(역), 나남, 61쪽 이하 참고.

71) 넛지에 관하여는 Thaler, R., Sunstein, C.(2018), 『넛지: 똑똑한 선택을 이끄는 힘』, 안진환 (역), 리더스북 참고.

하여, 민주주의 원리를 수호하겠다는 이념을 담고 있기 때문이라고 해석할 수 있을 것이다. 헌법 문언에서 국가조직이 정당한 권력을 행사하는 것에 대해서는 주로 '권한'이라는 용어를 사용하고 있다. 즉, 권력은 오로지 국민주권의 표현일 뿐, 헌법제정권력자이자 주권자인 국민 전체를 대리하는 국가조직은 권력을 행사하는 것이 아니라 헌법이 부여한 권한을 수행하는 것일 뿐이라는 의미이다.

사실 국민주권의 원리는 국가의 최고 의사결정의 근원인 주권이 국민에게 귀속된다는 것을 의미하는 동시에, 국민만이 국가권력에 대한 정당성을 부여할 수 있다는 것을 의미한다.[72] 주권이란 국가의 의사를 전반적으로 또한 최종적으로 결정할 수 있는 최고의 권력이자 권위로서, 대외적 독립성과 대내적 최고성을 바탕으로, 시원성·항구성·단일불가분성·불가양성·자율성 등의 특징을 보인다.[73] 과거에는 대외적 독립성 측면에서의 국가주권에 대한 논의가 진행되기도 하였지만, 오늘날의 헌법학에서는 주권의 대내적 최고성의 측면, 즉 국가 내 주권으로서의 국민주권이 그 연구 대상이 되었다. 그래서 '국민(nation)주권론'과 '인민(peuple)주권론'의 대립 논의를 거쳐서, 국민주권의 원리를 현실적으로 구현하기 위한 방법론으로서 대의제 민주주의에 대하여 검토하고 있다. 결국에는 헌법학에서 탐구하고자 하는 '권력'은 국민의 전체 의사가 어떻게 민주적 정당성에 근거하여 국가의 의사로 형성되는지에 관한 문제라고 할 수 있다.[74]

다. 행정법학에서의 권력

법학에서 관계를 중심으로 하여 권력을 다루는 분야로는 행정법학이 있다. 물론 여기에서의 관계는 법률관계를 의미한다. 법률관계는 사람과 사람 간의 법적인 권리와 의무 관계를 의미하는데, 행정법에서는 일반적으로 국가나 지방자치단체 등의 공법인과 개인 간의 법률관계를 탐구한다. 이러한 법률관계를 행정상 법률관계라고 하지만, 행정상 법률관계라고 하더라도 한쪽의 당사자인 공법인이 사인(私

72) 한수웅(2022), 『헌법학』, 법문사, 113쪽.
73) 성낙인(2019), 『헌법학』, 법문사, 130-131쪽.
74) 한수웅, 앞의 책, 121쪽.

人)의 지위에서 상대방인 국민과 사법상 법률관계가 형성되면 행정법관계에서 제외되고, 공법상 법률관계만이 행정법관계로서의 법률관계가 된다.

즉, 일반적으로 공권력을 행사하는 당사자인 행정주체와 공권력 발동 대상이 되는 당사자인 국민 간의 공법상 법률관계인 행정법관계로 이해되고, 이러한 행정법관계는 권력관계와 관리관계로 구분된다.[75] 관리관계는 행정주체가 비권력적인 관리자의 지위에서 공행정을 수행함에 있어서 국민과 맺는 관계이다. 권력관계는 행정주체가 우월적 지위에서 행정객체인 국민에 대하여 일방적인 조치를 하는 관계인 데 반하여, 관리관계는 행정주체가 비권력적인 관리자의 지위에서 공행정을 수행하면서 국민과 맺는 관계이다. 사실 관리관계 행정주체가 국민과 대등한 지위를 갖는 비권력관계에 해당한다. 비권력관계는 다시 관리관계와 국고관계로 구별되는데, 관리관계는 공법관계에 속하고, 국고관계는 사법관계에 속한다. 따라서 관리관계를 비권력적 공법관계 또는 비권력적 공행정관계라고도 부른다. 대표적인 관리관계로서는 공법상 계약관계가 있다.

권력관계와 관리관계를 구별하는 이유는 양자 간 상호 성질의 차이가 있고, 그에 따라 적용되는 공법상의 원리가 다르기 때문이다. 권력관계의 경우에는 관리관계와 비교할 때, 행정주체는 법률에 따라 행정객체인 국민보다 우월한 지위를 인정받지만 보다 엄격한 법적 통제를 받게 된다. 또한 이들 법률관계에서 분쟁이 발생하게 되면 권력관계의 경우 항고소송에 의하고, 관리관계의 경우 원칙적으로 당사자소송에 의하게 된다. 다만, 권력관계와 관리관계의 구별이 명확하지 않다는 비판도 있는데, 이는 공법상 계약이 사실상은 대등한 계약이 아닌 종속적 계약에 해당하기 때문에 공법상 계약관계를 관리관계로만 볼 것이 아니라 권력관계로도 볼 수 있을 것이라는 반론이 제기된다.[76]

권력관계는 전통적으로 행정법학의 영역에서 가장 중요하게 다루어지는 법률관계이면서도. 이 연구에서의 주된 관심사인 권력을 전면으로 내세우고 있다. 그러

75) 김동희·최계영(2023), 『행정법I』, 박영사, 80쪽.

76) 강병연(2022), “행정상 법률관계에 대한 새로운 고찰”, 《법조》 제71권 제2호, 법조협회. 101쪽.

나 행정법상 권력관계는 국가나 지방자치단체 등의 행정주체가 공익의 보호라고 하는 행정 목적을 달성하기 위해서 법률을 통해 부여받은 우월적 지위를 활용하여 행정객체인 국민에게 일방적인 조치를 하는 관계를 의미하는 것이지, M. Foucault가 바라보는 것과 같이 특정한 질서를 생산하고자 사회의 공간이나 구조 속에서 사람을 통제하려고 하는 힘과는 거리가 있다. 행정법상 권력관계는 행정의 작용형식 또는 행위형식 중에서 행정행위나 권력적 사실행위 등이 이에 해당하는데, 행정청이 이러한 행정작용을 하는 경우 오히려 당해 행정청이 법률에 따라 절차적으로도 실체적으로도 엄격한 통제를 받게 된다. 이는 사적자치가 주요한 법원리로 작동하는 사법관계와 차이가 나는 점인데, 바로 법치행정의 원리가 작동하기 때문이다. 즉, 법률적합성 원칙이 적용되므로 행정주체의 행정작용이 법의 허용범위를 벗어나거나 법적 근거가 없다면 위법하게 되며, 정상적인 법률관계가 성립할 수 없게 된다. 또한 권력관계에서 행정주체에 우월적 지위가 인정된다고 하더라도, 행정주체인 국가나 지방자치단체 등이 자유롭게 명령만 하면 행정객체인 국민이 무조건 복종하는 관계를 의미하지 않는다. 행정주체에 부여된 일정한 특권은 과거의 절대 왕정이나 권위주의 국가에서 국가가 국민을 힘으로 지배하기 위해 인정되는 것이 아니라, 공익의 실현이라는 행정 목적의 달성을 위해 법 기술상 요구되는 특권일 뿐이다.

4. 오늘날 인공지능과의 관계

가. 현대사회와 감시

앞에서 언급한 것처럼 M. Foucault의 이론상 감시로 대변되는 규율권력은 이중적인 의미를 갖는다. 그 때문에 이에 일률적인 판단을 내리기는 어렵다. 이는 다음과 같은 국가 및 사회 패러다임 변화로 인해 더더욱 어렵다. 첫째, 현대국가가 사회적 약자에 대한 맞춤형 복지를 강조하는 복지국가로 변모한다는 점이다. 둘째, 현대사회가 안전을 중시하는 이른바 안전사회로 바뀌었다는 점이다.[77] 전자

77) 현대 안전사회의 법적 문제에 관하여는 양천수(2016), “현대 안전사회와 법적 통제:

에서는 사회적 약자를 보호하기 위한 감시 또는 정보 수집이 중요하다. 예를 들어 고독사를 예방하기 위해서는 고독사 위험이 높은 이들을 지속적으로 감시 혹은 인지할 필요가 있다. 이들에게는 감시가 보호라는 의미로 다가올 것이다. 후자에서는 범죄나 재난으로부터 안전을 보장하기 위한 감시가 중요한 역할을 한다. 이를 위해 오늘날에는 지능형 CCTV처럼 인공지능 기술을 적극적으로 활용하는 감시가 즐겨 사용된다. 그 때문에 이를 둘러싼 논란도 발생한다.

나. 지능형 감시에 관한 세 가지 관점

오늘날 안전을 보장하기 위해 빈번하게 활용되는 지능형 감시를 어떻게 평가할 것인가에는 크게 세 가지 관점을 언급할 수 있다. 공리주의 관점, 자율주의 관점, 비판이론 관점이 그것이다.

사회의 공리를 극대화하는 것을 정의로 파악하는 공리주의에 따르면 지능형 감시는 사회 전체의 안전을 최대한 보장하기 위한 조치이기에 긍정적으로 평가될 것이다. 특히 우리 사회의 경우 안전을 매우 강조하므로 지능형 감시의 긍정적 측면이 돋보일 것이다. 이에 반해 자율성을 인간의 존엄에 관한 근원적 요소로 이해하는 Kant식의 자율주의에 따르면 지능형 감시는 인간 존재의 자율성을 불신하고 인간 존재를 도구화하는 것이라는 이유에서 비판적으로 평가할 가능성이 높다. 마찬가지로 비판이론, 특히 M. Foucault의 권력 비판의 관점에 따르면 지능형 감시는 인간의 생명과 신체에 규율권력이 직접 개입하는 것이기에 비판적으로 보일 것이다.

감시의 이중성에 관해 이미 지적한 것처럼 이러한 세 가지 관점 모두 지능형 감시가 가진 양면성의 어느 한쪽만을 드러낸 것이다. 따라서 세 가지 관점 가운데 어느 한쪽만을 선택해 지능형 감시를 평가하는 것은 적절하지 않다. 오히려 중요한 것은 세 관점을 적절하게 조화시키는 구체적인 방안을 모색하는 것이다.

형사법을 예로 하여", 《안암법학》 제49호, 안암법학회, 81-127쪽 참고.

다. 안면인식 기술의 상반된 측면

지능형 감시를 일률적으로 평가하기 어렵다는 점은 이와 연계된 안면인식 기술이 상반된 측면을 가진다는 점에서도 확인된다. 후술하여 자세히 검토할 안면인식 기술은 민감한 기술이다. 안면인식이야말로 감시를 위한 출발점에 해당하기 때문이다. 통치자가 그 누군가를 감시하기 위해서는 모종의 인적 대상이 그 누군가인지를 특정(identification)할 수 있어야 한다. 그래야만 비로소 그 누군가에 대한 감시가 가능해진다. 이때 안면인식 기술은 그 누군가를 특정할 때 가장 유용한 기술이 된다. 그 때문에 유럽연합의 「인공지능에 관한 명령」은 안면인식 기술에 관한 강력한 규제를 도입하고 있다.

하지만 안면인식 기술은 디지털 포용(digital inclusion)이라는 맥락에서 사용될 수도 있다. 예를 들어 키오스크 등에서 안면인식 기술을 활용해 사회적 약자를 인지함으로써 이들이 좀 더 손쉽게 키오스크 등을 사용할 수 있도록 하는 것이다. 그 점에서 안면인식 기술은 고령자와 같은 사회적 약자가 디지털 세계에 더욱 쉽게 포용될 수 있도록 하는 긍정적 의미도 지닌다.

라. 보호와 통치의 이중성

좀 더 시야를 확장하면 안면인식이나 디지털 감시에 관한 문제가 이에만 한정되는 것은 아님을 알 수 있다. 이는 국가권력에 의해 이루어지는 시민 보호와 통치의 이중성에서 문제의 근원을 찾아볼 수 있다. 왜냐하면 권력을 행사하여 시민을 보호한다는 것은 시민을 위협하는 그 무엇을 제한하고 규율하는 통치의 모습을 동시에 갖기 때문이다. 보호와 통치는 동전의 양면에 해당한다.

마. 질서의 이중성

이러한 성격은 사회의 질서 자체에서도 발견할 수 있다. 사회가 존속하려면 사회에 질서가 필요하다. 질서가 있어야 사회는 지속적으로 존속할 수 있다. 이때 질서는 '구별(Unterscheidung)'에 기초를 둔다. 질서와 무질서를 구별함으로써 무엇이 질서에 속하고 무엇이 속하지 않는지 결정한다. 만약 이러한 구별이 이루어지지 않으면 질서 자체가 성립하지 않는다. 그런데 문제는 이러한 구별은 그 자

체가 규율이자 권력 행사인 통치라는 점이다. 질서를 구별하는 권력은 한편으로는 질서를 형성하는 생성적 권력이자 다른 한편으로는 무질서를 배제하는 제한적 권력이다. 이러한 질서 자체의 이중성이 보호에, 감시에, 안면인식에 투영되는 것이다.

라. 소결

사실 인공지능의 활용이 권력을 확대하는 데 기여를 한다거나, 혹은 영향을 미친다는 가설을 법적인 권력관계의 틀에서 파악하는 것은 곤란해 보인다. 법학이 다루고 있는 권력에서의 관계는 법률관계를 의미하는 것인 반면에, M. Foucault의 관계는 구조와 공간과 같은 환경적인 역학관계를 의미한다고 할 수 있다. 이미 정보통신기술이 발달하고 정보화 사회가 도래하면서 인터넷 등 네트워크 공간에서의 개인 활동 흔적이 공권력 또는 타인을 통해 확인할 수 있다는 불안감이 있었다. 이는 감시라는 메커니즘에 따라 개인이 규율되는 효과를 낳는 것이고, 결국 눈에 보이지는 않지만 권력자가 개입하거나 의도하는 바대로 개인이 스스로를 순종시켜 가는 단계라고 할 수 있다.

그런데 인공지능 기술이 발전하면서 이러한 현상은 더욱 극심해진다고 보아야 할 것이다. 과거의 정보화 사회에서는 내가 남긴 흔적으로 컴퓨터라는 장치를 이용하더라도 결국은 사람의 손과 판단을 거치게 되는데, 이제는 인공지능이 이러한 역할을 대신하게 됨으로써 불안감은 더욱 확장되기 때문이다. 일반적으로 감시라는 개념이 가치 중립적인 개념일 수는 있으나, 감시에 의한 권력 확대는 부정적인 측면으로 받아들여지기 쉽다. 다만, M. Foucault의 시각에서는 권력이라는 것이 단순히 억압적인 특성만을 가진다고 볼 수는 없는 점에서, 사회 전체와 그 사회를 구성하는 다양한 조직과 사람들 간의 미세한 구조 속에서 권력을 이해해 볼 필요도 있다. 인공지능 기술은 현재 매우 빠르게 발전하고 있고, 또한 사회적으로 사회 구성원이 체감하지 못하는 동안에도 빠르게 확산하고 있다. 그리고 인공지능은 정보주체가 인식하지 못하는 사이에 정보주체의 개인정보를 활용하여 사람 대신에 수많은 판단을 하고 있다. 과거에는 누군가가 자신을 보고 있을 것이라는 감시에 대한 우려가 있었다면, 현재에는 그 누군가에 사람이 아닌 인공지능까지 포함

되는 것이다. 인공지능 감시에 의한 권력의 확대는 권력자가 의도하지 않는 경우에도 발생할 수 있고, 심지어 감시의 목적이 아닌 경우에도 발생할 수 있다. 국가와 개인 관계와 같은 공적 관계에서의 감시 문제가 권력에 관계된 문제에서 더욱 중요하게 다루어지는 것은 물론이겠지만, M. Foucault가 권력관계를 국가 영역을 벗어나 사회 전체의 주제로 다루었듯이, 개인과 개인 간의 관계, 즉 사법관계에서도 충분히 논의될 수 있는 것이다.

제 3 절 인공지능 감시를 통한 권력의 확대 가능성

1. 의의

인공지능 기술은 현재 우리 사회의 다양한 영역에서 활용되고 있고, 향후 그 영역의 범위는 더욱 확대될 것임이 틀림없다. 감시라는 영역을 따로 설정할 수 있을지에 대한 검토는 차치하더라도, 인공지능을 이미 다양한 분야에서 감시 목적으로 활용하고 있다는 것은 분명 사실이다. 그뿐만 아니라 감시를 직접적인 목적으로는 하지 않더라도 인공지능을 활용하는 그 자체만으로 감시의 효과를 달성하고 있는 경우도 있다. 양자 모두 의도하지 않더라도 권력의 확대와 관계가 될 수 있다. 아래에서는 이 두 가지 유형의 기술 활용에 관하여 관련 사례를 중심으로 검토해 보고자 한다.

2. 인공지능 기반 감시 기술의 활용

가. 지능형 CCTV

1) 의의

인공지능 기술 기반의 감시 기술 중 대표적인 것이 바로 지능형 CCTV라고 할 수 있다. 지능형 CCTV는 인공지능 기반 영상 분석 기술을 도입한 지능형 관제 시스템을 말하며, 관제사의 수작업에 의존한 장시간의 영상 분석 상황 판단을 돕

고, 육안 관제의 한계를 극복하며, 인력 공백에 대한 대안적 기능을 한다.[78] 즉, 지능형 CCTV는 CCTV와 관제 시스템의 결합인데, CCTV 그 자체는 영상의 전송 또는 저장 등을 하는 단순한 기능에 불과하다. 실제로 인공지능 기술이 적용되는 영역은 영상분석을 통한 관제 시스템으로서, 이러한 시스템을 통해서 사람이나 사물 등을 감시하는 데 활용되는 것이다. 특정 사건이 발생하면 즉각적인 조치를 위해 관련 지역에 설치되어 있는 CCTV를 통해 전방위적으로 영상정보를 신속하게 수집하고 재난, 범죄, 테러 등 위험 상황에 효과적으로 대응할 수 있다. 이러한 관제 시스템에서 특정 영상만을 추출해 내는 시스템을 선별관제 시스템이라고 한다. 또한 지능형 CCTV에 특정인을 식별하는 기술을 접목하게 되면 그 감시의 효과가 더욱 커지는 것은 물론인데, 특히 여기에는 안면인식 기술이 크게 주목받고 있다.

2) CCTV

지능형 CCTV는 기술적으로는 CCTV와 지능형 관제 시스템이 결합되어 있는 시스템이다. 지능형 CCTV에서 인공지능 기술의 활용은 실제로는 관제 시스템과 관련되어 있다. 흔히 '폐쇄회로 텔레비전(Closed-circuit Television)'이라고 번역되는 CCTV는 사실 비디오카메라를 활용하여 영상정보를 수집하여 유·무선으로 전송하는 단순한 기기라고 할 수 있으며, 특정 목적을 위해 특정인들에게 제공되는 텔레비전일 뿐이다.[79]

법률상으로 CCTV의 정식 명칭은 '고정형 영상정보처리기기'이다. 「개인정보 보호법」 제2조 제7호는 고정형 영상정보처리기기를 "일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치"로 정의하고 있다. 과거의 「개인정보 보호법」은 영상정보처리기기의 설치와 운영에 관한 단일한 규정만을 두

78) 박상욱 외(2023), "공공안전 분야에서의 지능형 CCTV 기술 적용 동향", 《주간기술동향》 제2105호, 정보통신기획평가원, 16쪽.

79) 이강원·손호웅(2016), 『지형 공간정보체계 용어사전』, 구미서관, https://terms.naver.com/entry.naver?docId=3474031&cid=58439&categoryId=58439 (2024. 10. 3. 최종 방문).

고 있었으나, 지난 2023년 3월 14일 일부개정을 통하여 위의 '고정형 영상정보처리기기'에 적용되는 규정과 '이동형 영상정보처리기기'에 적용하기 위한 제25조의2의 규정을 구분하였다. 후자의 '이동형 영상정보처리기기'는 동법 제2조 제7호의2에 따라 "사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(据置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치"로 정의되어 있다. 양자의 명칭 차이만으로도 그 차이를 확인할 수 있지만, 법률상 정의를 통해서도 양자가 일정한 장소에 고정이 되어 있는지의 차이가 있을 뿐 영상정보를 수집하여 전송하는 기능적 측면에서는 동일하다고 할 수 있다.

한편, 동법 제25조가 이러한 고정형 영상정보처리기기의 설치와 운영에 대한 규제 내용을 규정하고 있는데, 여기에서는 그 설치와 운영을 허용하는 경우에 관해서만 확인하고자 한다. 동조 제1항이 공개된 장소에서의 고정형 영상정보처리기기의 설치·운영이 허용되는 경우를 제1호 내지 제6호로 한정하고 있는데, 이는 "1. 법령에서 구체적으로 허용하고 있는 경우", "2. 범죄의 예방 및 수사를 위하여 필요한 경우", "3. 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우", "4. 교통단속을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우", "5. 교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우", "6. 촬영된 영상정보를 저장하지 아니하는 경우로서 대통령령으로 정하는 경우"로 열거하고 있다. 다시 제6호가 대통령령으로 위임한 사항에 대해서 「개인정보 보호법 시행령」 제22조 제1항은 제1호와 제2호를 통해서 "출입자 수, 성별, 연령대 등 통계값 또는 통계적 특성값 산출을 위해 촬영된 영상정보를 일시적으로 처리하는 경우"와 "그 밖에 제1호에 준하는 경우로서 보호위원회의 심의·의결을 거친 경우"로 구체화하고 있다. 즉, 범죄의 예방과 수사, 시설의 안전·관리 및 화재 예방, 교통단속 등은 직접 감시를 목적으로 하는 경우일 것이고, 기타 법령이 감시를 목적으로 「개인정보 보호법」에서 규정하고 있지 않은 다른 감시를 목적으로 CCTV의 설치와 운영에 관한 근거 규정을 둘 수도 있

을 것이다.

3) 선별관제 시스템

지능형 CCTV는 기존의 CCTV 영상을 활용하여 지능형 선별관제 시스템을 구축하는 것인데, 여기에서의 선별관제는 "전체 카메라 영상이 아닌 영상 분석과 분배 기능을 적용하여 관제가 필요한 영상만 추출하여 관제요원이 육안으로 확인할 영상만 모니터에 표출해 관제량을 획기적으로 감소시켜 효율을 높이는 것"을 의미한다.[80] 즉, 지능형 CCTV에서 인공지능 기술의 역할은 영상을 분석하여 특정인이나 특정 행위, 특정 사물, 특정 사건 등을 추출 해내는 것이 핵심 기술이라고 할 수 있다.

구체적으로는 특정 범죄에 대해 행동양식 등의 역할 값을 정해주게 되면, 설정된 알고리즘에 따라 범죄혐의자의 발견뿐만 아니라 관련 정보를 경찰이나 지방자치단체에 신속하게 전송 또는 알림을 통하여 즉각적인 조치가 가능하게끔 한다. 인공지능 기반의 지능형 CCTV가 기존의 CCTV에 비하여 가지는 본질적인 차이점은 단순한 범죄 상황이나 치안 수요의 상황을 발견할 뿐만 아니라 인공지능 기술을 활용하여 더욱 신속하고 정밀한 결과를 도출할 수 있고, 이를 통해 적극적으로 범죄의 예방에 필요한 적극적인 조치가 가능하다는 점이다. 이런 기술력을 바탕으로 많은 지방자치단체가 사람들의 특정한 행동 패턴을 분석하여 범죄나 각종 사고의 징후를 조기에 발견하여 탐지하는 '지능형 선별관제시스템'을 구축하고 있다. 이 시스템에서는 인공지능 CCTV에 특정 복장을 한 사람이 의미 없는 서성거림을 지속하여 반복하는 경우 이를 범죄징후로 예측하고, 쓰레기 무단투기, 길거리 흡연, 소방차 통행로 무단주차 등의 행위가 포착되면 이를 선별관제 센터에 해당 사실이 즉시 전송되고 관제사는 필요하고 적절한 조치를 하게 된다.

세부적으로는 안면인식 기술이나 동작인식 기술 등의 인공지능 기술을 적용하면 특정인을 실시간으로 식별하여 범죄예방 및 수사, 실종자 수색, 재난 피해 방

80) 배재권(2020), "인공지능과 빅데이터 분석 기반 통합보안관제시스템 구축방안에 관한 연구", 《로고스경영연구》 제18권 제1호, 한국로고스경영학회, 160쪽.

지 등 공익적 목적으로 활용할 수 있다. 물론 일정한 수준에서는 불특정 다수 국민에 대한 사생활의 자유와 비밀의 제한이 필연적으로 수반될 것이다.

4) 안면인식 기술

안면인식 기술이란 사람의 얼굴정보를 활용하여 특정인을 인식하고 분석하는 인공지능 기술을 말한다.[81] 그 목적은 개인을 식별하거나 인증하기 위한 것이고, 때로는 사람의 얼굴정보를 특정한 기준에 따라 범주화하기 위한 것일 수도 있다. 이러한 목적을 위해서 얼굴이라고 하는 사람의 중요한 생체정보에서 추출하고 개인의 특징점을 디지털화함으로써 기존에 보유하고 있던 데이터베이스에서의 정보와 직접 비교하거나 대조하는 과정을 거쳐 특정인을 식별해 내는 것이다.[82]

안면인식을 포함한 글로벌 생체인식 시장이 2024년 472억 달러에서 2029년 845억 달러로 연평균 성장률이 12.3%에 달할 것으로 예상된다.[83] 안면인식 기술은 개인을 식별하여 본인임을 인증하는 보안시스템으로 널리 사용되고 있고, 비밀번호나 디지털 인증서를 사용하는 것보다 본인확인 절차가 간단하기에 그 인기가 좋다. 실제로 오늘날 우리는 매일 같이 안면인식 시스템을 이용해서 비밀번호를 직접 누르지 않고도 휴대폰 잠금을 풀고, 금융이나 SNS 등의 애플리케이션에 접속하고 있다. 현재까지는 그 활용도가 매우 높다고 말할 수는 없겠지만, 안면인식 도어록에 얼굴만을 비춤으로써 가정이나 직장에 출입하는 경우도 있다. 특히, 인공지능 기술을 활용하는 안면인식 시스템은 매우 고도화된 성능을 보이는데, 대규모의 얼굴정보를 학습한 알고리즘이 사람들의 외모를 분석하여 수많은 군중 속에

81) 김민규(2023), “안면인식기술의 경찰법적 활용에 관한 연구”, 박사학위 논문, 고려대학교 대학원, 17쪽.

82) 김민규(2023), 위의 박사학위 논문, 17쪽.

83) MarketsandMarkets(2024), “Biometric System Market by Authentication Type (Fingerprint, Iris, Face, Voice, Vein, Signature, Multi-factor), Offering (Sensor, Camera, Reader & Scanner, Software), Type (Contact, Contactless, Hybrid), Mobility, Deployment - Global Forecast to 2029”, https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html (2024. 10. 3. 최종 방문).

서도 특정인을 식별해 낼 수 있게 된다.

한편, 유럽연합의 개인정보보호위원회(European Data Protection Board)는 2022년 5월 12일「법 집행 분야 안면인식 기술 사용에 관한 가이드라인(Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement)」초안을 발표하였는데, 이 가이드라인에서는 안면인식 기술을 인공지능 기반 기술로서 사람을 자동으로 인식하기 위해 사용되는 시스템으로 정의하고 있다. 즉, 확률 기술과 생체인식 기술을 활용하여 일선 현장에서 수집한 얼굴정보를 기존에 보유한 사진, 영상 등의 정보와 서로 비교하여 특정인을 식별하는 기술이다.

5) 지능형 CCTV의 활용

인공지능 기반의 CCTV를 감시 목적으로 활용하게 되면 물론 범죄예방이나 질서유지와 같은 공익 보호에 기여할 수도 있지만, 필연적으로 국민의 사생활의 비밀과 자유에 대한 제한 내지 침해가 수반될 수밖에 없다. 또한 개인 식별 목적의 인공지능 기술이 단순히 고정형 영상정보처리기기를 통해서 활용되는 것이 아니라 드론, 바디캠 등과 같은 이동형 영상정보처리기기를 통해서 활용되는 경우라면 해당 기본권의 침해 가능성이 더욱 높아질 것이다.

사실 우리나라에서 방범용으로 CCTV라고 하는 고정형 영상정보처리기기가 설치된 역사는 그리 오래되지 않았다. 2002년 강력범죄가 빈발하자 서울특별시 강남구 논현동의 한 골목길에 5대의 CCTV가 최초로 설치된 것을 기점으로 하여 전국적으로 공공 CCTV가 크게 늘었다.[84] 불과 20여 년 만에 CCTV의 활용은 이미 보편화되어 있는 상황이다.

우리 정부는 지난 2022년 10월 29일 발생한 이태원 참사를 계기로 지능형 CCTV 확충 및 관제센터 고도화를 포함하는 재난안전관리체계 전반에 대한 개편을 추진하고 있다. 2023년 4월 발표한「국가 안전시스템 개편 종합대책」에 따르

84) 한민경 외(2018),『범죄예방 목적의 공공 CCTV 운영실태 및 개선방안 연구』, 한국형사정책연구원, 21쪽.

면, 국내 CCTV 53만 대 중 13만 대(24%)가 지능형 CCTV에 해당하는데, 향후 노후 CCTV를 우선 교체하고 지능형 관제 체계로 전환할 계획이다.[85] 또한 과학기술정보통신부가 2024년 4월 "CCTV 카메라를 이용하여 영상 기반 행동 등을 분석하고, 이상행위를 탐지하여 특정 상황(배회, 침입 등)을 자동으로 인식하고 처리하는 인공지능 기반 시스템"으로 정의되는 지능형 CCTV 솔루션에 대한 성능시험을 도입하여 군중밀집 등 인파사고 예방에 활용할 수 있도록 성능향상을 유도하겠다고 밝히기도 하였다.[86] 즉, 과거의 CCTV를 기반으로 인공지능 기술을 적용한 지능형 CCTV의 도입과 운영이 많이 늘어나고 있다.

감시 목적의 지능형 CCTV는 무엇보다도 불특정 다수를 대상으로 이상 행동이나 범죄징후를 예측하는 데 활용된다.[87] 이상 행동을 예측하기 위해서는 실시간으로 발생하는 배회, 침입, 유기, 쓰러짐, 싸움, 방화, 마케팅, 실종자, 익수자, 화재 등을 탐지하는 것이 필요하고, 범죄징후를 예측하기 위해서는 과거 범죄 이력에 따라 현재 또는 미래에 범죄가 발생할 것인지를 추측하는 것이 필요하다.

주요 사례를 살펴보면, 우선 서울특별시 성동구의 경우 특정한 행동 패턴을 분석하여 범죄나 각종 사고의 징후를 조기에 발견하여 탐지하는 '지능형 선별관제시스템'을 구축하고 있다.[88] 이 시스템에서는 인공지능 CCTV에 대하여 특정 복장을 한 사람이 의미 없는 서성거림을 오랜시간 반복하게 되면 이를 범죄징후로 예측하고, 또한 쓰레기 무단투기, 길거리 흡연, 소방차 통행로 무단주차 등의 행위가 포착되는 경우 해당 화면을 즉시 선별관제센터로 즉시 전송되고 관제사는 필요한 적절한 조치를 하게 된다.

또한 코로나19 팬데믹 상황에서는 얼굴정보를 활용하여 확진자를 식별하고 자

85) 관계부처 합동(2023. 4.), "국가 안전시스템 개편 종합대책", 18쪽.
86) 과학기술정보통신부 보도자료(2024. 4. 3.), "지능형 CCTV 솔루션 성능시험으로 국민안전 강화한다!"
87) 박상욱 외, 앞의 보고서, 17쪽.
88) 경향신문(2021. 1. 26.), "성동구, 범죄징후 CCTV로 잡아낸다 … '지능형 선별관제시스템' 구축", https://www.khan.co.kr/local/Seoul/article/202101261457001 (2024. 10. 3. 최종 방문).

동추적 할 수 있는 지능형 CCTV 구축에 관한 보도가 나오기도 하였다.[89] 「개인정보 보호법」이 생체인식정보로서의 얼굴정보를 민감정보로 보고 있고, 따라서 개인의 동의를 받거나 법적 근거가 있어야만 수집이 가능할 것이다. 그러나 이 사건에서 해당 시스템을 구축하기로 발표한 경기도 부천시는 과학기술정보통신부의 공공분야 지능정보화 사업의 일환으로 추진되는 이 사업에서 역학조사를 위한 안면인식정보 수집이 「감염병의 예방 및 관리에 관한 법률」에 저촉되지 않는다고 밝힌 바 있다.

또한 최근 들어서는 이러한 지능형 CCTV가 차세대 통합관제 시스템의 적용으로 더욱 고도화된 것으로 보인다. 경기도 고양시의 경우 인공지능 기반의 차세대 통합관제 시스템이 지리정보시스템과의 연계를 통해 이상 상황이 발생한 장소를 지도에서 정확하게 파악할 수 있게 함으로써, 집중 관제가 필요한 지역, 시간대, 대상 등을 더욱 효율적으로 관제할 수 있게 하였다.[90] 경기도 안산시에서는 차세대 통합관제 시스템이 적용된 지능형 CCTV를 활용하여 충무훈련을 진행하였으며, 해당 기술은 실시간 관제와 용의자 추적 및 검거 훈련 등을 위해서 활용되고 있다.[91]

다만, 국내에서는 현재까지 정부기관이 공공장소에서 실시간으로 개인을 식별하기 위해서 불특정 다수에 대하여 안면인식 기술을 적용한 지능형 CCTV는 활용하지는 않는 것으로 파악되고 있다. 2023년 1월 12월 국가인권위원회가 국무총리를 대상으로 실시간 원격 안면인식 기술에 대한 인권침해 위험성을 방지하기 위한 입법이 마련되기 전까지, 중앙행정기관 등 공공기관이 공공장소에서 이러한 기술의 도입과 활용을 하지 않도록 권고하였는데, 이에 대하여 국무조정실이 반복해

89) 뉴스1(2021. 2. 25.), "'CCTV 활용 안면인식·동선분석'으로 코로나 감염경로 파악한다", https://www.news1.kr/articles/?4223239(2024. 10. 3. 최종 방문).

90) 연합뉴스(2024. 8. 14.), "고양시, 전국 최초 차세대 인공지능(AI) 통합관제시스템(AMS) 구축" https://www.yna.co.kr/view/RPR20240814000400353 (2024. 10. 3. 최종 방문).

91) 소방방재신문(2024. 6. 20.), "안산시 충무훈련서 인텔리빅스 AI 관제시스템 활용", https://fpn119.co.kr/218338 (2024. 10. 3. 최종 방문).

서 관련 사례도 없고 개별 법령의 근거 없는 도입 계획도 없음을 밝혔기 때문이다.[92] 오히려 지능형 CCTV를 실시간으로 개인을 식별하는 데 활용하는 것은 국외 사례에서 확인할 수 있다. 2020년 1월 미국 디트로이트 경찰국은 CCTV에 포착된 절도범의 모습과 유사하다는 안면인식 인공지능의 결과를 바탕으로 한 흑인 남성을 체포하였으나, 그는 30시간 후 용의자가 아니라는 사실이 밝혀져서 석방되었다.[93] 이 사건에서 당사자가 부정확한 기술을 신뢰한 공권력에 의해 자신의 신체의 자유를 부당하게 침해받았다. 또한 당사자를 포함한 경찰이 활용한 CCTV를 통해 영상이 촬영되고 촬영된 영상이 인공지능 알고리즘에 의해 분석이 된 모든 정보주체는 각자의 사생활의 자유와 비밀과 개인정보자기결정권이 침해된 것으로 볼 여지가 있다.

안면인식 기술을 적용한 지능형 CCTV는 전 세계적으로 중국에서 많이 활용되는 것으로 알려져 있다. 중국은 2015년부터 '톈왕(天網)' 프로젝트를 진행하는 등 국가적 차원에서 인공지능 기술을 접목한 지능형 CCTV를 운용해 오고 있는데, 중국 정부가 해당 프로젝트를 범죄예방 등 국민 보호 목적이라고 밝히고 있으나 사생활 침해와 관련된 논란이 많다.[94] 중국 공안은 '톈왕'을 이용하여 7명을 살해하고 도주하였던 범죄수배자를 20년 만에 검거하기도 하였는데, 해당 수배자는 도피 과정에서 성형 수술 등으로 얼굴을 위장하고 가짜 신분증을 이용하는 등의 도피 행각을 벌였으나 안면인식 기술을 이용한 CCTV에 의하여 검거되었다. 또한 중국에서는 '톈왕' 이외에도 인공지능 기반 CCTV를 주민 통제가 어려운 농촌 지

92) 국가인권위원회 보도자료(2024. 2. 22.), "실시간 원격 얼굴인식 기술 도입·활용 중지 조치 권고, 국무총리 수용".

93) ABC News(2020. 6. 26.), "Black man wrongfully arrested because of incorrect facial recognition", https://abcnews.go.com/US/black-man-wrongfully-arrested-incorrect-facial-recognition/story?id=71425751 (2024. 10. 3. 최종 방문).

94) 아시아경제(2024. 4. 19.), "AI 안면인식 기술 시대 … 선진국선 '빅브라더' 우려 [CCTV 감시사회]②", https://www.asiae.co.kr/article/2024041815510255760(2024. 10. 3. 최종 방문).

역 등에 설치하는 '쉐량공정(雪亮工程)' 프로젝트가 2016년 하반기부터 진행되고 있는데, 이는 실제로는 주민을 통제·관리하기 위한 시스템을 구축하는 것인데 실제로 쓰촨(四川)성에서 '쉐량공정'이 도입된 지역의 범죄 발생 건수는 50%가 줄어들고 범죄검거율은 50%가 높아진 것으로 확인되었다.[95]

나. 인공지능 기반 전자감시 시스템

전자감시 시스템이란 주로 일정한 조건으로 석방 또는 가석방된 범죄자가 지정된 시간에 지정된 장소에 있는지를 확인하고자 해당 범죄자의 손목이나 발목 등에 전자감응 장치를 부착하고 유·무선 장비를 활용하여 원격 감시하는 시스템을 말한다.[96] 그 법적 근거로는 「전자장치 부착 등에 관한 법률」이 있는데, 동법 제5조에서 검사가 성폭력범죄, 미성년자 대상 유괴범죄, 살인범죄, 강도범죄, 스토킹범죄 등을 다시 범할 위험성이 있다고 인정되는 사람에 대하여 전자장치를 부착하도록 하는 명령을 법원에 청구할 수 있는 요건을 정하고 있다. 또한 동법 제16조3은 위치추적 관제센터의 설치·운영 등에 관한 규정을 두고 있다. 이때 고정형 이동장치를 활용할 수 있다.

다만, 국내에서는 이 분야 인공지능 기술의 활용이 현재까지는 초기적인 단계이기는 하지만, 이미 활용이 시작된 상황이고 향후 더욱 고도화될 것으로 전망된다. 법무부는 2021년부터 빅데이터와 인공지능 기술을 활용한 이른바 전자감독서비스를 도입 및 운영하고 있다고 밝힌 바 있다.[97] 인공지능 관제 및 인공지능 보호관

---

95) 서울신문(2018. 7. 8.), "[김규환 기자의 차이나 스코프] 사방에 깔린 '매의 눈' … 빅브러더 키우는 대륙", https://www.seoul.co.kr/news/plan/china_scope/2018/07/09/20180709016001 (2024. 10. 3. 최종 방문).

96) 김혜정(2000), 『전자감시제도의 도입 및 운영을 위한 예비연구』, 한국형사정책연구원, 29쪽.

97) 법무부 보도자료(2021. 6. 28.), "인공지능(AI) 기반의 전자감독서비스 구축", https://www.moj.go.kr/moj/221/subview.do?enc=Zm5jdDF8QEB8JTJGYmJzJTJGbW9qJTJGMTgyJTJGNTQ5MjQ4JTJGYXJ0Y2xWaWV3LmRvJTNG(2024. 10. 3. 최종 방문).

찰서비스, 빅데이터 분석플랫폼 구축 등이 그 주요 내용으로, 점차 증가하는 전자감독제도의 집행과 이로 인한 전담 인력의 업무 과중 문제를 해소하고 전자감독 업무의 효율적 운영을 지원하기 위한 목적이다. 여기에서의 인공지능 관제서비스는 각 경보별로 처리에 필요한 맞춤 정보를 제공하고, 단순경보 등은 자동으로 처리하는 등 단순반복 업무량을 감소시켜 관제직원으로 하여금 위험경보와 고위험 대상자에 더욱 관제를 집중할 수 있게 한다. 또한 2021년 6월 법무부는 인공지능 관제의 수준은 위험성이 낮은 단순경보 위주로 하여 전체 발생경보 중 약 23.6% 상황을 처리할 수 있는 단계로, 앞으로 사람에 의한 경보처리 결과를 인공지능 모델에 재학습시키는 등 성능을 개선하여 처리 가능 대상을 확대할 예정이라고 밝혔다. 인공지능 보호관찰서비스는 전자감독 대상자의 개인 데이터와 공간 및 지리정보를 분석하여 대상자에 대한 특징과 동향, 평가 등의 데이터를 종합적으로 제공하는 것이다. 이를 통해 선제적 감독 역량이 강화된다. 또한 빅데이터 분석플랫폼을 통해 관련 기능을 체계적이고 능률적으로 수행할 수 있으며, 해당 플랫폼에는 전자감독 대상자의 판결문 등의 관련 정보와 외부의 공공데이터 등을 연계하여 운영하고 있다.

한편, 2024년 2월에는 법무부와 과학기술정보통신부가 '재범 징후 선제적 감지 및 대응력 강화 사업' 신규 과제를 공모하였는데, 이 과제는 '강력 범죄 재범 예측·대응 신기술' 개발과 'AI 기반 전자 감독 통합 시스템' 개발의 두 부분으로 구성되어 있다.[98] 전자의 경우 전자감독 대상자의 개인별 범죄 유형, 일상 모델을 기반으로 대상자 맞춤형 일탈을 탐지하고 재범위험도를 분석하기 위한 인공지능 기술을 개발하는 것이 그 목적이고, 후자의 경우 인공지능 기반 재범 예방 R&D를 위해 산발적이고 정형화되지 않은 개인별 전자감독 데이터를 자동으로 정형화할 수 있는 인공지능 기술개발 및 이를 관리하기 위한 통합 DB를 구축하는 것이 그

98) 세계일보(2024. 3. 3.), "법무부, 인공지능(AI) 기반 전자 감독 기술·시스템 개발 본격 추진", https://www.segye.com/newsView/20240303503884 (2024. 10. 3. 최종 방문).

목적이다.[99]

다. 인공지능 기반 부정수급 등 탐지 시스템

인공지능 기술이 불특정 다수를 감시하기 위해서 개인의 영상정보만을 분석하는 것은 아니다. 개인의 경제활동이나 일상생활 등을 감시하기 위한 목적의 인공지능 기술도 존재한다. 국내에서는 사회서비스 바우처와 같은 사회보장급여의 부정수급 탐지를 위해 한국사회보장정보원이 운영하는 '부정수급 탐지시스템,'[100] 각종 국고보조금의 부정수급을 탐지하기 위해 한국재정정보원이 운영하는 '부정징후 탐지시스템'[101], 건강보험 부당청구를 탐지하기 위해 건강보험심사평가원이 운영하는 '부당청구감지시스템'[102] 등에서 감시 목적으로 인공지능 기술을 활용하고 있다. 이들 시스템에 적용되는 인공지능은 불특정 다수 국민의 경제활동이나 일상생활에 관계되는 개인정보 또는 위치정보 등을 분석하여 이상 징후를 파악하는 것이 목적인데, 지능형 CCTV와 마찬가지로 사생활의 비밀과 자유와 개인정보자기결정권의 침해 문제가 제기될 수 있다.

우선, 한국사회보장정보원이 운영하는 '부정수급 탐지시스템'은 'AI 기반의 공공재정 FDS(부정수급 탐지시스템 또는 이상결제탐지시스템) 신속 대응·탐지체계' 아래 빅데이터 분석 및 인공지능 부정모형을 바탕으로 사회서비스 바우처의 부정의심 결제와 부정 고위험군 점검대상자 선별 등의 역할을 수행하고 있다. 예를 들어 사망자가 바우처를 이용하거나 결제 장소나 시간이 이상한 의심 사례 등이 발

99) 과학기술정보통신부 사업공고(2024. 2. 28.), "2024년도 재범징후 선제적 감지 및 대응력 강화사업 신규과제 공모".

100) 한국사회보장정보원(2022. 7. 22), "한국사회보장정보원, 'AI 기반의 공공재정 FDS 신속 대응·탐지체계 구축'으로 우수행정 정책사례 우수상", http://www.ssis.or.kr/lay1/bbs/S1T101C486/B/101/view.do?article_seq=124162&cpage=1&rows=10&condition=&keyword= (2024. 10. 3. 최종 방문).

101) 대한민국 정책브리핑(2023. 2. 14), "국고보조금 시스템 개선으로 부정수급 적발률 지속 높여가", 기획재정부, https://www.korea.kr/multi/visualNewsView.do?newsId=148911651&sectIds=&cateId=&pageIndex=1&repCode_C=#visualNews (2024. 10. 3. 최종 방문).

102) 보건복지부(2022. 1. 28.), "2022년도 국가정보화 시행계획".

생하면 인공지능이 즉시 모니터링 대상으로 선별하는 것이다.[103)]

한국재정정보원의 '부정징후 탐지시스템'의 경우, 과거에 적발한 바 있는 부정수급 사업 관련 통계분석을 바탕으로 공통 속성을 발견하여 모니터링 대상 사업이 얼마나 유사한지 점수화하는 방식으로 위험도가 높은 사업을 추출해서 수급자인 보조사업자의 정보를 수집한다. 이를 바탕으로 가족 간의 거래, 출국 내지 사망자 수급, 세금계산서 취소 등의 패턴을 생성한 후 이에 대한 지급 건을 탐지해내고 있다. 2023년에는 2018년 이 시스템이 처음으로 가동된 이후로 493건, 700억 원의 부정수급을 적발했는데, 휴·폐업 기간 보조금 지급, 보조금 사용금지 업종 거래 등의 집행 오·남용과 가족 거래 순으로 적발 유형이 나타났다.[104)]

그런데 네덜란드에서는 정부가 사회보장, 조세, 노동 등 다양한 영역에서 발생하는 부정을 탐지하고자 자동화 시스템 SyRI(System Risk Indication)를 활용해 왔는데, 2020년 2월 헤이그 지방법원(The District Court of the Hague)이 사생활 관련 권리를 규정하는 「유럽인권협약(European Convention on Human Rights: ECHR)」 제8조 제2항을 위반하였다는 이유로 정부의 SyRI 활용이 위법이라고 결정하기도 하였다.[105)]

라. 민간에서의 활용: 인공지능 기반 노무관리

1) 의의

이러한 감시 목적의 인공지능 기술이 비단 국가나 지방자치단체 등 공법인에 의해서만 활용되는 것은 아니다. 민간에서도 인공지능 감시 기술을 적극적으로 활용

---

103) 머니투데이(2020. 4. 13.), "'돌아가신 분이 왜 바우처를' … 이런 부정수급 AI가 잡는다", https://news.mt.co.kr/mtview.php?no=2020041311103819755 (2024. 10. 3. 최종 방문).

104) 서울신문(2024. 2. 27.), "[공직자의 창] 국고보조금 누수, AI 탐지모델로 잡아낸다", https://www.seoul.co.kr/news/editOpinion/opinion/government-official-story/2024/02/27/20240227025004 (2024. 10. 3. 최종 방문).

105) 네덜란드의 'SyRI 사건'에 관하여는 홍석한(2023), "지능정보사회에서 사회보장 영역의 정보화와 기본권 보호 - 네덜란드 SyrI 판결에 대한 분석과 평가 -", 《헌법학연구》 제29권 제3호, 한국헌법학회, 134쪽 이하 참조.

하고 있다. 물론 사인과 사인 간의 법률관계를 국가와 국민과의 법률관계와 동일한 선상에서 규율할 수는 없을 것이다. 왜냐하면 앞서 살펴본 바와 같이, 행정법상 권력관계에 대해서는 법치행정의 원리가 적용되어 행정주체가 국민의 기본권 보호의 차원에서 법적 근거를 두고 각종 권한을 행사하는 반면, 사인 간의 법률행위에는 원칙적으로는 사적자치의 원리가 적용되기 때문이다. 그러나 사인과 사인 간의 관계라고 하더라도 일반적으로 불평등한 법률관계로 취급됨으로써 법적으로는 사적자치가 제약받는 대표적인 법률관계가 노사관계일 것이다. 그래서 노동법이 이에 개입하여 사업장에 대한 강력한 규제를 도입하고 있는 것인데, 이에 민간에서 인공지능 감시 기술을 어떻게 활용하고 있는지를 살펴보는 문제에서, 아래에서는 노무관리 분야에서의 활용에 대해서 살펴보고자 한다.

2) 인공지능 기반 노무관리의 도입과 확산

인공지능의 발전이 노동 관련 분야에서도 변화를 불러오고 있는데, 대표적으로 '인공지능 기반 노무관리(AI-based worker management: AIWM)'가 일터에 확산되고 있다. 'AIWM'은 "데이터를 수집하는 노무관리 시스템을 통칭하는 포괄적인 용어"로, "작업 공간, 작업자, 작업자가 수행하는 업무, 업무에 사용하는(디지털) 도구에 대한 데이터를 실시간으로 수집한 다음, 이를 인공지능 기반 모델에 입력하여 자동 또는 반자동으로 의사결정을 내리거나 작업자 관리 관련 질문에 대한 정보를 의사결정자에게 제공하는 시스템"을 말한다.[106]

인간 감독자에 크게 의존하는 이전의 노무관리 형태와 달리 AIWM은 다양한 출처를 통하여 근로자의 행동에 대한 실시간 데이터를 수집하여 정보를 제공하고 인공지능을 기반으로 자동 또는 반자동 의사결정을 지원하는 관리 시스템을 통해 노무를 관리한다.[107] 'AIWM' 활용은 채용 단계, 근로관계 성립 이후의 노무관리,

---

106) Christenko, A., Jankauskaittė, V., Paliokaittė, A., Van den Broek, K. R., Jarvis, M.(2022), Artificial intelligence for worker management: an overview, European Agency for Safety and Health at Work. p. 12.

107) 현재 활용되는 인공지능은 알고리즘을 사용하기 때문에 '알고리즘 노무관리(algorithmic management)'라는 표현이 AIWM을 포괄하는 노무관리를 지칭하는 데

근로관계 종료에 이르는 전반에서 활용할 수 있다. 해고 결정에는 인간의 개입이 필요하도록 규제가 설계되고 있지만 최종적으로 인간이 개입하기 전 단계까지의 정보처리 및 활용은 인공지능에 의해서도 가능하다. 전형적 근로관계가 아니라 근로자가 아닌 지위에서 노무를 제공하는 경우에도 노무제공자의 선정 및 선정 이후 노무관리에서 유사한 AIWM 활용이 이루어질 수 있다. 또한 알고리즘 노무관리가 노무관리의 기본적 형태인 '디지털 노동 플랫폼(digital labor platform)'은 플랫폼이 아닌 일터에 확대 활용될 수 있는 '알고리즘 노무관리(algorithmic management)'를 보여준다.

3) 인공지능 기반 노무관리의 활용 현황

인공지능 기술을 활용한 노무관리는 ① 노무관리에 적용되는 알고리즘에 근로자 및/또는 업무 프로세스에 대한 데이터 공급, ② 알고리즘을 통한 이러한 데이터의 처리 및 정교화, ③ 이러한 데이터 처리에 기반한 결정을 통해 근로자에게 가해지는 조정과 통제로 구현된다.

부문별 특성에 따라 알고리즘 노무관리의 구현은 경제 전반에 걸쳐 각기 다른 속도로 발전하고 있다. 호텔부터 식품 체인에 이르는 소매업, 음식 및 숙박업, 은행, 컨설팅, 콜센터, 저널리즘과 같은 다른 서비스 산업에서도 알고리즘에 의한 근무 교대 배정과 조정 및 감독, 알고리즘을 활용한 업무 모니터링, 평가 시스템 등의 알고리즘 노무관리가 진행되고 있다.[108)]

이러한 알고리즘 노무관리는 데이터 기반 노무관리(data-driven management)와 상당 부분 중첩된다. 데이터 기반 관리는 궁극적으로는 서로 연관되어 있는 다

사용된다. 알고리즘 노무관리는 "조직 내 노동력 투입을 조정하기 위해 컴퓨터 프로그래밍 절차를 사용"하는 것을 말한다. 직접 인용 부분은 Baiocco, S. et al.(2022), The Algorithmic Management of work and its implications in different contexts, ILO. 또한 인공지능은 일반적으로 자신의 기능을 개선하기 위해 스스로 편집할 수 있는 기능을 가진 여러 알고리즘이 함께 작동하는 조합을 지칭하는 용어로 정의할 수 있다. 이러한 이유로 여기에서의 논의 또한 AIWM을 포괄하는 개념어로 '알고리즘 노무관리(algorithmic management)'라는 용어를 사용한다.

108) Baiocco, S., Enrique, F., Rani, U. & Pesole, A.(2022), op. cit., p. 17.

양한 유형과 계층의 기술을 상호 연결하고 결합하는 데 의존한다. 데이터 기반 관리를 구현할 때 이러한 기술은 종종 함께 채택되어 조직 내에서 데이터를 사용하여 운영을 조정하거나 구체적으로 작업할 수 있도록 한다.[109] 데이터 기반 노무관리를 지원하는 기술인 사물인터넷(Internet of things: IoT), 인공지능, 데이터 분석, 웨어러블 디바이스(Wearable devices), 고객 관계 관리(Customer Relationship Management: CRM) 및 전사적 자원 관리(Enterprise Resource Planning: ERP)와 같은 관리 소프트웨어 애플리케이션을 비롯한 기타 관리 기술들이 결합되어 구현되는 데이터 기반 관리가 노무관리 영역에서 인공지능을 활용하는 경우 알고리즘 노무관리 내지 AIWM을 구현하게 된다.

이러한 노무관리 활용이 가시적으로 드러나는 것은 웨어러블 기기 활용이다. 따라서 현재 알고리즘 노무관리 관련 사례로 많은 연구의 대상이 되고 있는 것이 아마존 물류창고 사례이다. 아마존 창고에서 물류를 처리하는 직원이 착용한 웨어러블 기기를 통해 직원의 움직임을 지속적으로 모니터링하여 노무관리를 위한 데이터를 수집하고 해당 데이터에 기반하여 직원의 작업장 배치와 해당 직원의 업무 관련 프로파일링하고 피드백이 발송되는 근거 자료를 생성한다.

이러한 노무관리는 다양한 사업장에 맞춰 변형되어 활용할 수 있다. 예를 들어 유니클로나 세븐일레븐 등에서 활용되는 소프트웨어 애플리케이션인 Percolata는 하루 중 15분마다 매출을 극대화하기 위해 최적의 근무자 조합을 보장하는 것을 목표로 하며, 이를 달성하기 위해 시스템은 수요 예측을 기반으로 업무를 할당한다. 이러한 예측을 생성하는 데 사용되는 변수에는 일기 예보, 온라인 트래픽, 공휴일, 매장 내 프로모션 및 이전 판매뿐만 아니라 매장 내 센서로 캡처한 실시간 고객 흐름과 개인별 판매 데이터가 포함된다. 또한 판매 생산성에 따라 직원들의 순위를 매기고 판매 생산성이 가장 높은 시간대 및 팀 조합을 프로파일링한다.[110] 알고리즘은 단순히 교대 근무조에 직원을 매칭하는 것을 넘어, 기존에 관리

109) Urzì, B. C., Curtarelli, M., Riso, S., Baiocco, S.(2022), How digital technology is reshaping the art of management, European Commission. p. 10.

110) Patrick Brione(2020), My boss the algorithm: Research An ethical look at

자가 수행하던 일상적인 업무 배분의 상당 부분을 대체할 수 있다. 지멘스 제조 공장에서 사용 중인 Preactor 소프트웨어는 실시간으로 생산 주문을 계획하며 생산 공정의 각 단계를 정확히 어떤 순서로 수행해야 하는지 알려준다.[111] 화이트칼라 업무에서도 알고리즘에 의한 업무 배분이 활용된다. 다국적 마케팅 회사인 Publicis는 이미 계정 관리자, 코더, 그래픽 디자이너, 카피라이터 등 8만 명의 직원을 조직하고 할당하는 데 알고리즘을 사용하기 시작했다. 새로운 프로젝트나 고객 프레젠테이션이 있을 때마다 알고리즘은 최상의 결과를 위해 적합한 인재 조합을 추천하며, 이 회사는 프로젝트가 시작되거나 완료될 때마다 알고리즘의 추천에 따라 정기적으로 인력을 교체한다.[112] 예를 들어, 캐나다의 대형 의료 컨설팅 회사인 클릭 헬스(Klick Health)는 Genome이라는 수동 데이터 수집 시스템과 머신 러닝 도구를 사용한다. Genome은 다양한 작업을 완료하는 데 걸리는 평균 시간을 계산하고 프로젝트가 궤도를 벗어난 것으로 보이면 팀 리더에게 알려준다. 또한 이 시스템은 프로젝트 리더에게 시급하고 중요한 작업을 알려준다. 이 회사는 또한 작업자의 생산성이 마음의 상태(state of mind)라는 점을 인식하고 있으며, 직원이 최고의 성과를 내는 순간을 의미하는 'flow time'을 측정하는 방법을 찾고 직원의 활동을 추적하여 흐름과 생산성에 영향을 줄 수 있는 방해 요소를 표시하고 줄이는 데 도움이 되는 RescueTime이라는 데이터 도구를 사용한다.[113]

이처럼 알고리즘 노무관리를 통해 작업자에게 작업을 자동으로 할당하고, 인력을 배치하고, 작업자가 작업을 완료하는 데 필요한 경로와 시간을 안내하는 데 사용된다. 다만 현재 이러한 시스템이 인공지능에 기반하여 완전히 자율적으로 작업자를 감독하는 모델은 현재 찾기 어려우며, 이는 후술하는 바와 같이 해당 노무관

---

algorithms in the workplace, Acas, p. 10.

111) Ibid., p. 11.

112) Walsh, M.(2019). When Algorithms Make Managers Worse. *Harvard Business Review*, https://hbr.org/2019/05/when-algorithms-make-managers-worse (2024. 10. 3. 최종 방문).

113) Schweyer, A.(2018). Predictive Analytics and Artificial Intelligence in People Management, McLean: Incentive Research Foundation, p. 9.

리 영역에서의 알고리즘 활용에 대한 규제와 관련이 있다.

4) 디지털 노동 플랫폼의 인공지능 활용

디지털 노동 플랫폼은 알고리즘을 사용하여 노동의 수요와 공급을 매개하고 플랫폼을 통해 제공되는 노무 또한 알고리즘을 통해 관리한다. 디지털 노동 플랫폼의 알고리즘의 역할은 노동자에 대해 실시간 의사결정을 내리고, 계획하고, 작업을 할당하는 것에 한정되지 않는다. 노동자를 프로파일링하고, 그에 따라 노동자의 행동과 성과를 예측하고, 심지어 감정을 '인식'하기도 한다.[114]

대표적 디지털 노동플랫폼인 Uber는 라이더용 애플리케이션을 통해 성과 평가(별점 및 보상), GPS를 통한 운전 스타일 모니터링, 작업 할당(분류 및 매칭), 변동임금제 및 Q&A 시스템과 챗봇 지원이라는 다섯 가지 알고리즘을 통한 라이더 통제를 구현한다.[115] 플랫폼 노동은 '알고리즘에 의한 노무관리', 즉 노동자가 사용하는 플랫폼 업체의 애플리케이션에서 사용되는 알고리즘의 설계와 구현이 플랫폼과 플랫폼 노동자 사이의 종속관계를 결정하는 데 결정적 요인이 된다.[116] 즉, 대체로 고용계약을 맺지 않고 노무를 중개하는 디지털 노동플랫폼과 플랫폼 노무제공자 사이의 근로자 지위 관련 분쟁이 발생하는 경우, 알고리즘 노무관리를 통한 노무제공자 통제의 정도는 근로자 지위 인정을 위한 '종속성' 충족 여부 판단에 결정적 역할을 한다.[117]

---

114) Ponce del Castillo, A. & Naranjo, D.(2022), "Regulating algorithmic management: An assessment of the EC's draft Directive on improving working conditions in platform work", ETUI Policy Brief, The European Trade Union Institute, p. 2.

115) Mcdaid, E., Andon, P., Free, C.(2023), "Algorithmic management and the politics of demand: Control and resistance at Uber," *Accounting, Organizations and Society*, Volume 109.

116) 장선미(2023), "플랫폼 경제에 관한 헌법적 접근 - 플랫폼 노동의 보호와 플랫폼 사업의 규율 -", 《헌법재판연구》 제10권 제2호, 헌법재판연구원, 11쪽.

117) 예를 들어 프랑스 파기원은 2022년 Uber 드라이버의 종속성을 인정하면서, 해당 운전자가 자영업자 등록을 했으나 종속관계에 있는 근로자라고 판단했다. 이 사건의 종속관계 판단에서 Uber의 경로 추천 알고리즘을 따르지 않는 경우 Uber에 의한

3. 감시의 효과를 가지는 인공지능 기술

감시 자체가 목적은 아니지만 개인정보를 대량으로 처리하면서 개발 또는 운영되는 인공지능의 경우에는 그 고유의 목적과는 다르게 간접적으로 감시의 효과로 나타날 수 있고, 이로 인하여 개인의 프라이버시나 자유로운 인격의 발현에 영향을 미칠 수도 있을 것이다. 예를 들면, 우선 공공의 영역에서는 한국사회보장정보원이 운영하는 '복지 사각지대 발굴시스템'[118]과 '맞춤형급여안내(복지멤버십)'[119] 서비스를 들 수 있다. 전자는 단전, 단수 등 45종의 위기정보를 활용하여 사회보장급여 수급 자격이 있으나 신청을 하지 못하는 위기가구를 발굴하기 위한 인공지능 시스템이고, 후자는 개인이나 가구의 연령, 가족관계, 경제상황 등의 정보를 활용하여 혜택을 받을 수 있는 복지서비스를 추천해주는 시스템이다. 민간의 영역에서는 개인정보나 위치정보를 처리하는 과정을 거치는 인공지능이 개인을 프로파일링하여 상품, 서비스, 콘텐츠 등을 추천해주는 경우나 플랫폼 종사자의 개인정보, 위치정보 등을 활용하여 배차, 배달 등 일감배정을 하는 인공지능 알고리즘 등이 그 예이다. 아래에서는 한국사회보장정보원의 '복지 사각지대 발굴시스템'에 대해서 간략하게 살펴보고자 한다.

2014년 2월 발생한 이른바 '송파 세 모녀 사건'을 계기로 복지 전달체계에 대한 문제가 본격적으로 제기되었다. 국회에서 복지 사각지대 해소가 사회보장의 주요 과제로 등장하였고, 2014년 12월 9일「국민기초생활 보장법」개정안,「긴급복지지원법」개정안, 그리고「사회보장급여의 이용·제공 및 수급권자 발굴에 관한 법률(이하에서는 "사회보장급여법"이라 한다)」이 통과되었다. 특히, '사회보장급여

가격 조정, Uber 애플리케이션의 작동방식, 세 번의 운행요청 거부 후 일시적 접속 차단, 취소율에 따른 계정 접근 차단 등이 종속관계 인정 근거가 되었다. 이상 Cour de cassation, civile, Chambre sociale, du 4 mars 2020, n° 19-13.316.

118) 보건복지부 보도자료(2024. 3. 24.), "45종 위기정보 활용해 2024년 2차 복지 사각지대 발굴 시행".

119) 보건복지부 보도자료(2024. 1. 21.), "나를 위한 89가지 복지서비스, 복지멤버십이 알려드려요".

법'이 제정됨으로써 복지 사각지대 발굴을 위해 다양한 종류의 정보를 수집 및 처리할 수 있고 다른 기관과 공유할 수 있는 근거가 마련되었다. 그러나 정부는 2010년부터 활용해 오던 사회보장정보시스템의 처리능력이 한계에 도달했다고 판단하여 2019년부터 이를 전면 재구축하는 차세대 사회보장정보시스템 개발에 착수하였다. 이에 차세대 사회보장정보시스템은 2021년 9월 1차 개통에 이어 2022년 9월 2차 개통되었다.[120] 그리고 2024년부터는 기존의 복지 사각지대, 사각지대 발굴 위기정보를 기존 34종에서 39종, 39종에서 44종, 44종에서 45종까지로 확대하여 연락이 두절된 위기가구의 소재를 파악하고 있다.[121]

이를 위해서 한국사회보장정보원의 내외부 연계 시스템이 수집하는 데이터에 머신러닝 알고리즘을 적용하여 위험확률을 계산한 후, 이를 바탕으로 복지서비스가 필요한 대상자를 추출하는 것이다.[122] 다시금 필터링과 알고리즘 활용을 반복하여 복지 사각지대를 발굴함으로써 복지 담당 공무원이 복지 지원 대상자를 쉽게 파악할 수 있게 하는 것이다.

이러한 인공지능 기술은 실제 직접적으로는 감시를 목적으로 하는 데 활용되는 것이 아니다. 그럼에도 대다수 국민의 개인정보를 활용함으로써 감시와 유사한 효과를 발생시킨다고 할 수 있다.

---

120) 보건복지부 보도자료(2022. 9. 5.), "차세대 사회보장정보시스템 개통(2차)".

121) 보건복지부 보도자료(2024. 3. 24.), "45종 위기정보 활용해 2024년 2차 복지 사각지대 발굴 시행".

122) 홍석한(2023), "사회보장 영역에서 인공지능 활용에 대한 헌법적 고찰", 《법학논고》 제80집, 경북대학교 법학연구원, 45쪽.

제 4 절 인공지능 감시 기술에 대한 규제 필요성

1. 인공지능 감시를 통한 기본권 침해 가능성 증대

가. 개인정보자기결정권 및 사생활의 비밀과 자유 침해 가능성

현대사회에서 개인은 매일 같이 엄청난 양의 데이터를 생성해 낸다. 자신에 관한 데이터를 비공개로 유지하기는 사실상 불가능하다. 무엇보다 인터넷의 도입과 함께 개인의 비밀 영역은 상당 부분 사라졌다. 개인에 관한 데이터를 획득하여 다양한 이익을 얻는 데 활용하기가 그만큼 수월해진 것이다. 컴퓨터 사용자의 저장장치에 배치된 '쿠키(cookie)'는 인터넷에서 사용자의 움직임을 추적하고 해당 정보를 서버에 전달한다. 이에 서버에는 사용자가 검색한 단어, 각 페이지에서 소비한 시간, 장치의 유형, 자주 구매한 쇼핑 물품, 그리고 이름과 아이디(ID), 주소, 전화번호, 신용카드 번호 등 중요한 정보가 담겨 있다. 인터넷 업체는 쿠키를 사용하여 다양한 통계를 낼 수 있고 웹사이트 운영자는 정밀 타겟팅(targeting)을 통해 맞춤형 홍보 등 정보를 제공할 수 있다. 소셜 미디어와 기타 무료로 제공되는 온라인 서비스의 비즈니스 모델은 사용자에 관한 데이터와 콘텐츠를 얼마나 많이 이용하여 수익을 창출할 수 있는지에 따라 성공이 좌우된다.[123)]

계속해서 늘어나는 공적 과제를 신속하고 효율적으로 처리하도록 압박을 받는 국가도 마찬가지이다. 데이터는 개인과 조직이 더 정확하고 효과적인 의사결정을 내리는 데 필수적인 자원이며, 기업뿐만 아니라 국가의 경쟁력에도 직접 영향을 미치는 경제적 자산이다. 기업이나 국가 모두 데이터를 활용하여 문제를 해결하거나 새로운 제품과 서비스를 개발하고 경쟁에서 우위를 점할 수 있다. 국가도 개인

---

123) 제품의 생산보다는 데이터의 추출로 가동되는 정보사회의 생태계에서 모든 움직임은 개인에 대한 감시를 수반하며, 데이터의 판매와 공유로 감시가 더 견고해지는 "감시자본주의"의 구축이다. Manheim, K., Kaplan, L.(2019), "Artificial Intelligence: Risks to Privacy and Democracy," *Yale Journal of Law & Technology* Vol. 21, p. 124.

에 관한 데이터를 최대한 활용하여 분석과 예측을 수행할 때 비로소 신속성과 효율성의 요청을 충족할 수 있다.

데이터의 중요성은 인공지능과 관련하여 더욱 두드러진다. 인공지능의 본질적인 힘은 기계가 데이터에 접근할 수 있다는 데 있으며,[124] 인공지능의 성패는 얼마나 좋은 품질의 데이터를 얼마나 많이 확보하는지에 따라 결정된다. 이에 인공지능을 활용하려는 기관은 더 나은 예측을 하는 모델을 만들기 위해 더 많은 데이터를 수집할 수 있도록 항상 규범적, 윤리적 경계를 넓히고자 하며, 데이터를 공유하거나 여러 데이터베이스를 연계하는 시스템을 구축하고자 한다. 국가와 기업은 최고의 알고리즘이 아니라 최고의 데이터 접근성을 확보하고자 한다. 이에 새로운 작업을 수행하기 위한 알고리즘을 개발하기 위해서는 가능한 한 많은 데이터를 수집해야 하므로 그만큼 감시의 위험은 확대된다. 개인정보를 보호하기 위한 수단이 적용될 수 있으나 언제나 모든 정보를 성공적으로 보호할 수 있는 것은 아니다.

개인이 생성하는 데이터는 곧 자기 자신을 알리는 것이며, 인공지능의 필수 재료가 된다. 이에 인공지능을 이용한 감시 위험의 증대는 개인정보자기결정권을 비롯하여 주거의 비밀, 사생활의 비밀, 통신의 비밀과 같이 개인의 사사로운 영역을 보호하기 위한 기본권 보장에 결정적인 악영향을 미칠 수 있다.[125] 인공지능 활용의 목적을 충분히 달성하기 위해서는 포괄적인 정보의 수집과 정보 시스템의 연계, 다양한 데이터 출처를 통합하여 프로파일링과 종합적인 분석을 해야 하기 때문이다. 이에 따라 공적 과제의 원활한 수행이라는 공익을 위하여 개인정보자기결정권을 제한해야 할[126] 필요성이 커진다. 또한 국가가 사생활 영역을 들여다보는

---

124) Manheim, K., Kaplan, L.(2019), op. cit., p. 122.

125) 이준일(2022), “인공지능과 헌법 - 인공지능의 위험에 대한 헌법적 권리 차원의 대응 -”, 《헌법학연구》 제28권 제2호, 한국헌법학회, 357-358쪽.

126) “개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리로서, 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 보장된다. 이와 같이 개인정보의 공개와 이용에 관하여 정보주체 스스로가 결정할 권리인 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체,

것에 대한 보호 및 국가가 사생활의 자유로운 형성을 방해하거나 금지하는 것에 대한 보호를 제공하는 사생활의 비밀과 자유,[127] 사생활 영역 가운데 헌법이 개인 간의 의사소통을 특별히 보호하고자 별개의 조항을 두고 있는 통신의 자유[128]를 제한할 수 있는 범위도 확대하도록 한다.

특히 인공지능 시스템은 정확하고 정교한 대규모의 데이터 관리를 수행함으로써 빅데이터에 기반한 대규모 정밀 감시를 가능하게 한다. 기술의 발달과 함께 유전정보나 신체적, 생리적, 행동적 특징에 관한 정보와 같은 민감 정보를[129] 수집, 처리, 활용할 수 있는 역량도 강화된다. 또한 인공지능은 수집된 데이터에서 개인을 식별할 수 있는 정보를 제거하는 익명화를 쉽게 무력화할 수 있다.[130] 대량의 데이터에서 패턴을 식별하여 연관성을 분석하고, 공개된 다른 데이터와 쉽게 결합함으로써 익명화된 데이터를 재식별화할 수 있다. 데이터의 특정한 속성을 매우 세밀하게 분류하거나 기계 학습 기법을 적용함으로써 익명화된 데이터에서도 유용한 정보나 개인 식별 가능성을 쉽게 발견할 수 있다. 개인정보자기결정권과 사생활 침해의 위험은 훨씬 더 커질 수밖에 없는 것이다. 민감정보까지 포함하는 이러한 시스템이 사이버 공격에 노출될 때 발생할 수 있는 피해의 규모와 정도의 심각성까지 고려한다면 그 위험성은 배가된다.[131] 나아가 이러한 위험은 국가에 의

신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보이다. 또한, 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다(헌재 2022. 11. 24. 2021헌마130).” 헌재 2024. 1. 25. 2020헌마65, 공보 328, 217, 221.

127) 헌재 2014. 6. 26. 2012헌마331, 판례집 26-1하, 609, 617.

128) 헌재 2001. 3. 21. 2000헌바25, 판례집 13-1, 652, 658.

129) 인공지능 기술의 발달에 따른 생체인식정보의 활용 확대와 관련한 새로운 기본권 침해 위험에 대해서는 이권일(2020), “생체인식정보의 보호와 활용에 대한 헌법적 고찰 - 개인정보보호법 시행령 개정령안에 대한 분석을 겸하여-”, ≪법학연구≫ 제61권 제2호, 부산대학교 법학연구소, 11-17쪽.

130) Lubarsky, B.(2017), Re-Identification of “Anonymized” Data, *Georgetown Law Technology Review* Vol. 1, pp. 208-212.

131) 김민우·김일환(2021), “지능정보사회에서 민감정보의 보호와 이용을 위한 법제 정비

한 직접적인 침해뿐만 아니라 사인에 의한 기본권 침해 가능성 증가에 대응하여 국가가 기본권보호의무를 이행해야 한다는 측면[132]에서도 매우 중요한 문제가 된다.

나. 인간의 존엄과 가치 및 일반적 행동의 자유 침해 가능성

국가는 인공지능을 활용하여 감시 체제를 구축하면서 개인에 관한 규범적 판단과 평가, 그에 따른 집행을 자동화할 수 있다. 인공지능에 의한 감시, 자동화된 규제와 법 집행을 확대하면 그만큼 개인이 자율적인 의지를 발휘할 수 있는 조건이 점차 열악해지고 진정한 의미에서 스스로 결정을 내릴 기회를 박탈할 수 있다. 이는 인간의 존엄과 가치에 기초한 개인의 자율성을 억압하고, 자기결정권과 일반적 행동의 자유를 실질적으로 억압하는 결과를 초래한다.

헌법 제10조에 따라 모든 국민은 그의 존엄한 인격권을 바탕으로 자율적으로 자신의 생활 영역을 형성해 나갈 수 있는 권리를 가진다.[133] 인간의 존엄성에 의하여 일반적 인격권이 보장되고 이로부터 인간이 자신의 생활 영역에서 인격의 발현과 삶의 방식에 관한 근본적인 결정을 자율적으로 내릴 수 있는 자기결정권이 파생된다.[134] 특히 행복추구권의 구체적인 표현으로서 일반적 행동자유권은 가치 있는 행동만을 보호영역으로 하지 않는다.[135] 반면 인공지능을 활용한 법 집행의 자동화와 감시는 국가 후견주의를 강화하여 헌법의 인간상인 자기결정권을 지닌 창의적이고 성숙한 개체로서 국민[136]이 자아실현을 할 기회를 근원적으로 박탈할 수 있다.

민간 기업은 근로자의 노동 과정에 업무용 애플리케이션을 활용하도록 하고, 알고리즘을 활용한 작업 시간 관리 프로그램을 도입함으로써 노동에 대한 철저한

방안 연구", 《서울법학》 제29권 제2호, 서울시립대학교 법학연구소, 83쪽.

132) 이상학(2023), "생체적 안면인식의 법적 문제", 《유럽헌법연구》 제42호, 유럽헌법학회, 388-393쪽.

133) 헌재 1997. 3. 27. 95헌가14등, 판례집 9-1, 193, 204.

134) 헌재 2019. 4. 11. 2017헌바127, 판례집 31-1, 404, 416.

135) 헌재 2003. 10. 30. 2002헌마518, 판례집 15-2하, 185, 200.

136) 헌재 1998. 5. 28. 96헌가5, 판례집 10-1, 541, 555.

데이터 감시를 할 수 있게 되었다. 이는 시간 활용에 관한 근로자의 자율성을 파편화하고 근로자를 알고리즘에 예속된 부품으로 전락시키는 문제를 불러온다.[137] 국가도 마찬가지여서 국민을 대상으로 한 정책과 규율의 집행 과정을 고도로 자동화하고, 이를 준수하도록 엄격한 감시 체제를 운영한다면 국가 전체에 걸쳐 자율성을 파괴하고 개인을 국가에 종속시키는 상황을 초래할 것이다.

인공지능을 이용함으로써 다양하고 방대한 데이터를 바탕으로 개인에 대해 정밀한 감시를 할 수 있다는 것은 곧 평가와 분석을 통해 개인을 조정하는 힘이 더 커질 수 있음을 의미한다. 국가는 개인의 패턴을 인식하고 이를 분석과 예측에 활용하여 이를 기반으로 다시 정교한 감시를 시행할 수 있고 나아가 개인의 생각과 행동을 조정할 수도 있다. 개인에 대한 조정은 기본적으로 감시 가능성을 인식한 개인이 소극적, 방어적으로 판단하고 행동하도록 함으로써 자연스럽게 발생한다. 개인은 실시간으로 자신의 발언과 행동이 감시당할 수 있다는 데 대한 두려움 또는 언제라도 분석과 평가의 대상이 될 수 있다는 우려로 인하여 사전에 주의를 기울인다. 강제적인 규범이나 직접적인 감시 아니라 감시의 가능성만으로도 조정을 받는다.

국가는 개인이 접근할 수 있는 정보를 통제하는 은밀한 활동을 통해서도 조정을 할 수 있다. 인공지능을 이용해 개인이 접근할 수 있는 정보를 손쉽게 필터링함으로써 일정한 정보를 습득하거나 습득하지 못하도록 하는 것이다. 이로써 겉으로는 드러나지 않지만 국가가 의사결정에 개입하거나 의도하는 바에 따라 개인을 순응시키는 수준으로까지 나아갈 수 있다. 이러한 의견 형성의 조정은 인공지능 알고리즘이 사회적 미디어와 인터넷에서 일반적으로 콘텐츠를 필터링하거나 검열하도록 하여 집단적으로 할 수도 있고, 개인이 맞춤형 정보에 갇히도록 함으로써 특정인을 타겟팅하는 방식으로 할 수도 있다. 과거 정보사회에서는 개인의 흔적이 컴퓨터를 통해 처리되더라도 이를 활용하려면 결국 인간의 수작업과 판단을 거쳐야

137) 김영선(2020), “플랫폼 자본주의 시대의 노동자상”, 《도시연구》 제18호, 인천연구원, 122-127쪽.

했다. 그러나 인공지능이 규모와 정밀성 측면에서 전혀 다른 차원으로 인간의 역할을 대신한다. 이에 실질적으로 자유롭게 결정하고 행동하고자 하는 개인의 판단을 효과적으로 교란하고 조정할 수 있는 능력이 극적으로 확대된다.

민간 기업에서 이러한 조정은 소비자가 구매할 가능성이 높은 제품이나 서비스를 예측하여 이에 맞춤형 광고를 하는 방식으로 이루어진다.[138] 광고기업은 사람들의 생각과 행동에 영향을 미치는 데 전문적이다. 이들은 인공지능을 이용하여 온라인 활동을 하는 이용자를 감시하고, 광고주가 원하는 맞춤형 이용자를 찾아내 특정한 상황에 맞는 특정한 사용자를 대상으로 광고를 자유롭게 조정할 수 있다.[139] 이러한 민간 기업의 인공지능 이용 조정 메커니즘은 국민의 생각과 행동을 조정하려는 의지를 가진 국가도 마찬가지로 활용할 수 있다. 더욱이 국가는 행정과 형사사법 등을 위한 목적으로 막대한 양의 개인정보와 공공정보, 정보수집 및 분석기기를 보유하고 있다. 개인의 신념, 활동, 움직임을 깊고 정밀하게 통찰할 수 있으므로 기업과 협업하거나 그 시스템을 차용하여 더 은밀하고 세세하게 국민을 조정할 수 있다.

다. 불합리한 차별에 따른 평등권 침해 가능성

일반적으로는 인공지능이 인간보다 더 객관적이고 정확한 판단을 할 수 있을 것으로 받아들여지지만 항상 그런 것은 아니다. 인공지능은 편향성과 오류 가능성이라는 결정적인 한계를 내포한다. 이에 인공지능을 활용한 감시, 그에 따라 도출된 편향적이거나 오류가 있는 결론에 기초하여 개인에 대해 평가하고, 의사결정을 한다면 불합리한 차별로 인한 평등권 침해로 연결될 수 있다.

인공지능은 데이터를 재료로 작동하는 만큼 인공지능 모델은 훈련 데이터의 질

---

138) Aziz Z. Huq(2020), “Constitutional Rights in the Machine-Learning State”, *Cornell Law Review* Vol. 105, p. 1877.

139) 맞춤형 광고를 통해 온라인 이용자는 스스로 감시의 대상으로서 상품화되고 있다는 지적으로 김영욱(2018), “디지털 노동 착취와 감시의 상품화 - 온라인 맞춤형 광고에 대한 커뮤니케이션 정치경제학 해석 -”, 《언론과 사회》 제26권 제1호, 사단법인 언론과 사회, 61-65쪽.

과 양에 따라 성능이 달라진다. 데이터가 불완전하거나 부족하면 모델의 예측이 부정확해질 수 있다. 데이터가 특정 집단이나 특성에 치우쳐 있으면 편향된 결정을 내리고, 상대적으로 데이터가 부족한 집단에 대해서는 예측의 정확성이 떨어질 수밖에 없다. 또한 알고리즘 개발자가 의도적 또는 무의식적으로 편향적으로 설계할 수도 있는 등 인공지능 알고리즘이 문제를 해결하기 위해 설계된 방식이 항상 최적이 아닐 수 있다. 특히 인공지능은 데이터의 상관관계를 식별한 다음 통계기법을 적용하여 결론을 도출하나 이 상관관계가 항상 인과관계를 나타내는 것은 아니므로[140] 결론의 신뢰도는 크게 달라질 수 있다. 모델이 훈련 데이터에만 지나치게 맞춰져 학습하면 새로운 데이터는 일반화하여 적응하지 못하고 이 때문에 오류가 발생할 수도 있다. 이밖에 시간에 따라 데이터의 특성이 변할 수 있으므로 모델이 훈련된 이후에 사회적, 경제적 변화가 크다면 인공지능의 예측이 비현실적이거나 부정확할 수도 있고, 인공지능은 스스로 학습하고 진화하기 때문에 동일한 조건에서 서로 다른 결과를 낳을 수도 있다.

최근에는 LLM에 의존하는 생성형 인공지능 도구가 부정확하거나 오해의 소지가 있는 결과를 도출하는 '할루시네이션(AI hallucinations)', 즉 '환각' 문제가 주목받고 있기도 하다.[141] 미국 플로리다주에서는 '환각'으로 만들어진 가짜 판례를 인용한 서면을 법원에 제출한 변호사가 법원으로부터 정직 처분을 받기도 하였고,[142] 캐나다 브리티시컬럼비아주에서도 챗지피티(ChatGPT)가 생성한 가짜 판례를 인용한 변호사가 주 대법원으로부터 손해배상책임을 인정받기도 하였다.[143] 이는 리걸테크(legaltech) 관련 사례이지만 '환각'이 공적 영역에서도 심각한 문

140) Bayamlioğlu, E., Leenes, R.(2018), "Data-driven decision-making and the 'Rule of Law'", *Tilburg Law School Research Paper*, pp. 35-38.

141) 케임브리지 사전(Cambridge Dictionary)은 2023년 '올해의 단어'로 "hallucinate"을 선정하고 인공지능과 관련한 정의를 추가하였다. 케임브리지 사전 홈페이지 참조(https://dictionary.cambridge.org/editorial/woty).

142) 법률신문(2024. 8. 6.), "美법원, 'AI 가짜 판례' 인용 변호사에 정직 1년", https://www.lawtimes.co.kr/news/197090 (2024. 10. 3. 최종 방문).

143) Zhang v Chen, 2024 BCSC 285.

제를 불러올 수 있음을 보여준다. 법적인 정당성과 합리성이 강하게 요구되는 공권력 작용의 관점에서도 인공지능이 매우 강력하지만 아직은 완벽하지 않은 도구임을 다시 일깨우는 현상이다.

이러한 편향성과 오류로 인하여 인공지능이 도출한 결과의 정확성과 신뢰성이 부족한 경우가 다수 발생할 수 있다.[144] 그럼에도 그 결과를 그대로 받아들이고 이를 통해 개인을 평가하고 그에 기초하여 결정하는 것은 그 자체로 불합리한 차별을 불러오고,[145] 기존의 차별을 영속화할 수 있다. 정당한 이유 없이 특정한 개인이나 집단에 대해 감시를 강화하도록 할 수 있을 뿐만 아니라, 이러한 감시의 강화는 위법행위를 감지할 가능성을 더 높이므로 부당한 감시 대상이 된 개인과 집단에 대한 차별적 처우를 영속시킬 수 있는 것이다.[146] 과거 범죄 경력이 있는 개인이나 집단을 감시하는 경우라도 낙인효과를 유발하고, 집중적인 감시에 따른 범죄 탐지율 상승 및 그에 따른 감시의 재강화나 처벌의 확대로 이어질 수 있다.[147]

라. 표현의 자유 및 알 권리 침해 가능성

헌법 제21조 제1항에서 규정하고 있는 언론ㆍ출판의 자유는 자유로운 인격 발현의 수단임과 동시에 합리적이고 건설적인 의사 형성 및 진리 발견의 수단이며, 민주주의 국가의 존립과 발전에 필수 불가결한 기본권이다.[148] 그러나 감시는 표현의 자유 행사를 직간접적으로 억압하는 전형적인 기제이다. 무엇보다 감시는 개인이 자기검열을 하도록 유도한다. 감시를 의식한 개인은 자유롭게 발언하거나 행

---

144) Aziz Z. Huq(2020), op. cit., pp. 1889-1890.

145) 노현숙(2022), “범죄예측의 쟁점과 함의”, 《경희법학》 제57권 제1호, 경희법학연구소, 15쪽, 21쪽.

146) 송태은(2021), “인공지능 기술을 이용한 국가의 사회감시 체계 현황과 주요 쟁점”, 국립외교원 외교안보연구소, 20쪽.

147) 예를 들어, 알고리즘의 편향성으로 인해 고위공직자보다 하위공직자의 부패 범죄가 잘 적발되고 그러한 데이터가 축적된다면 이를 학습한 인공지능 시스템이 하위공직자에 편중하여 감시함으로써 하위공직자에게만 집중된 부패 범죄의 적발과 처벌이 이루어질 수 있다. 김병수(2022), “부패범죄에 AI 범죄예측 시스템 적용의 문제점과 개선방안”, 《한국부패학회보》 제27권 제2호, 한국부패학회, 131쪽.

148) 헌재 2011. 12. 29. 2007헌마1001등, 판례집 23-2하, 739, 756.

동하기 어렵고 특히 사회적으로 민감한 주제에 대한 의견을 밝히거나 비판적인 행동을 꺼리게 된다. 의견의 다양성을 줄이고 비판적 사고를 억제하여 공론의 질을 낮추며, 정치적 반대나 사회적 저항 운동을 위축시킬 수 있다.

국가는 인공지능을 활용하여 극단적으로 정밀한 감시 체제를 형성할 수 있고 그만큼 표현의 자유에 대한 침해 가능성은 커진다. 이는 집회·시위 현장에서 참가자의 사진을 찍거나 영상을 촬영하는 행위는 심리적 부담을 주어 여론 형성 및 민주적 토론 절차에 영향을 미치고 집회의 자유를 전체적으로 위축시키는 결과를 가져올 수 있다고 판시한 헌법재판소 결정[149]을 통해서도 확인할 수 있다. 인간이 카메라를 이용하여 촬영하는 것을 넘어 곳곳에 실시간 안면인식이 가능한 지능형 CCTV가 설치되어 정보를 수집할 수 있도록 한다면 표현의 자유 실현에 미치는 그 위해는 훨씬 더 커질 것으로 예상할 수 있다.

앞서 은밀한 조정을 통한 자기결정권 침해 가능성에서 살펴본 바와 마찬가지로 비록 표현행위를 하는 주체는 스스로 선택한 의사결정에 따라 표현하는 것으로 인식할 수 있지만 사실은 정교한 조작 기술에 의해 유도된 의사결정에 불과한 경우가 많을 수 있다. 많은 정보를 토대로 하여 대중을 특정한 방향으로 유도하고 효율적으로 통제할 수 있는 '빅 넛징(Big Nudging)'이 가능한 것이다.[150] 또한 앞서 언급한 바와 같이 인공지능은 비식별 조치를 쉽게 무력화할 수 있다. 표현의 자유는 자신의 신원을 누구에게도 밝히지 아니한 채 익명 또는 가명으로 자신의 사상이나 견해를 표명하고 전파할 익명 표현의 자유를 포함하며,[151] 이는 표현의 자유 실현과 민주주의 발전에 중요한 의미가 있다.[152] 따라서 이러한 재식별 가능

149) 헌재 2018. 8. 30. 2014헌마843, 판례집 30-2, 404, 412.

150) 빅 넛지는 현대적 형태의 후견주의로서 국가는 개인의 생활에 깊은 관심을 갖고 옳다고 생각하는 바에 따르도록 한다. 데이터로 무장한 "현명한 왕(wise king)"인 인공지능을 통해 원하는 경제적, 사회적 결과를 만들어낼 수 있다. Helbing, D. et al.(2019), "Will Democracy Survive Big Data and Artificial Intelligence?," in: Helbing, D. ed., *Towards Digital Enlightenment: Essays on the Dark and Light Sides of the Digital Revolution*, Spinger, p. 76.

151) 헌재 2022. 12. 22. 2019헌마654, 판례집 34-2, 753, 758.

성은 개인정보자기결정권뿐만 아니라 표현의 자유를 크게 위축시킬 수 있다.

인공지능에 의한 감시의 확대는 표현의 자유와 표리관계에 있는 알 권리 보장에 대해서도 부정적인 영향을 미치기 쉽다. 알 권리는 일반적으로 정보에 접근하고 수집, 처리함에 있어서 국가권력의 방해를 받지 아니한다는 자유권적 측면과 적극적으로 정보를 공개할 것을 청구할 수 있는 청구권적 측면을 모두 포함한다. 특히 지능정보기술이 발달할수록 정보에 접근하고 정보를 요구할 수 있는 알 권리는 일상생활에 매우 중요한 기본권이다. 이에 헌법재판소는 알 권리의 핵심은 국민이 정부에 대해 일반적 정보공개를 구할 권리이며, 이러한 알 권리의 실현은 법률이 제정되어 있지 않다고 하더라도 헌법 제21조에 의해 직접 보장될 수 있다고 한다.[153]

그러나 앞서 언급한 바와 같이 인공지능은 기술적으로 블랙박스 특성을 가질 뿐만 아니라 제도적, 정책적 측면에서도 관련 정보를 비공개로 유지해야 할 필요가 인정된다. 법 집행 기관은 감시를 위한 시스템에 관한 정보를 공개하지 않는 데 따른 이익을 중요하게 생각한다.[154] 이러한 인공지능의 기술적, 제도적, 정책적 불투명성은 헌법상 기본권인 알 권리를 보장함으로써 감시 위험의 증대를 방지하는 것은 물론 당사자가 사후적으로 사법절차를 통해 감시의 정당성과 합법성을 다투는 데에도 불리한 영향을 미칠 수 있다.

---

152) "익명으로 이루어지는 표현은 외부의 명시적·묵시적 압력에 굴복하지 아니하고 자신의 생각과 사상을 자유롭게 표출하고 전파하여 국가권력이나 사회의 다수의견에 대한 비판을 가능하게 하며, 이를 통해 정치적·사회적 약자의 의사도 국가의 정책결정에 반영될 가능성을 열어 준다는 점에서 표현의 자유의 내용에서 빼놓을 수 없는 것이다. 그리고 인터넷 공간에서 이루어지는 익명표현은 인터넷이 가지는 정보전달의 신속성 및 상호성과 결합하여 계층·지위·나이·성 등으로부터 자유로운 여론을 형성함으로써 국민 의사를 평등하게 반영하여 민주주의를 더욱 발전시킬 수 있다." 헌재 2022. 12. 22. 2019헌마654, 판례집 34-2, 753, 754-755.(재판관 4인의 반대의견)

153) 헌재 1991. 5. 13. 90헌마133, 판례집 3, 234, 245-246.

154) Slobogin, C., Brayne, S.(2023), "Surveillance Technologies and Constitutional Law," *Annual Review of Criminology*, Vanderbilt Law School Faculty Publications, p. 220.

2. 생체정보 및 생체인식정보 활용의 문제

가. 의의

인공지능 기술을 활용한 감시는 궁극적으로 개인의 행동이나 특징을 통해서 특정인을 인식하거나 식별하기 위한 목적을 갖는다고 볼 수 있다. 개개인이 누구인지를 가려내기 위해서는 얼굴정보와 같은 생체정보 내지 생체인식정보를 인공지능에 대량으로 학습시키고, 이를 다른 정보와 결합하여 프라이버시 침해를 고도화하면서, 특히 미래 행동을 예측하는 프로파일링을 통해 사람을 선별·분류하는 감시체계가 구축될 수 있다.[155] 이를 위해서는 인공지능 알고리즘 모델 학습 단계에서도, 또한 결과물 산출을 위한 알고리즘 구동 단계에서도, 무엇보다 생체정보와 생체인식정보가 필요하다. 그리고 앞서 살펴본 인공지능 감시가 가지는 기본권 침해의 문제는 이러한 생체정보와 생체인식정보가 대량으로 활용된다는 측면에서 더욱 증폭된다.

나. 생체정보 및 생체인식정보의 개념과 특성

그런데 생체정보와 생체인식정보의 개념은 구분된다. 우선, 전자는 "지문, 얼굴, 홍채, 정맥, 음성, 유전자정보, 필적, 제스처, 걸음걸이 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징(연령, 성별, 감정 등)을 알아보기 위하여 일정한 기술적 수단을 통해 처리되는 정보"를 말한다.[156] 생체정보는 그 자체가 개인을 나타내기 때문에 생체정보의 보호는 매우 중요하다. 생체인식 기술은 이러한 생체정보를 측정한 후 이를 데이터베이스와 비교함으로써 그 개인을 자동적으로 인증·식별[157]하는 기술을 말한다. 생체정보

---

155) 송기복(2024), "AI 안면인식 기술의 활용과 범죄수사의 문제점", 《경찰법 연구》 제22권 제1호, 한국경찰법학회, 218쪽 이하.

156) 개인정보보호위원회(2021), "생체정보 보호 가이드라인", 3쪽.

157) '인증'이란 이용 권한이 있는 특정 개인임을 확인하기 위하여 이용자가 입력한 생체정보를 기기 등에 저장된 정보와 대조하여 본인 여부를 확인하는 것을 의미하며, '식별'은 개인의 생체정보를 데이터베이스에 저장된 다수의 생체정보와 대조하여 여러 사람 중 특정 개인을 구분하여 확인하는 것을 의미한다(개인정보보호위원회(2021),

가 제대로 보호되고 또 안전하게 활용되기 위해서는 명확한 개념 정의와 생체정보의 활용과 제한에 대한 명확한 규정이 필요하다. 이를 위해서는 생체정보와 생체인식정보를 구분하여 정의할 필요가 있다.

개인정보보호위원회는 "생체정보 보호가이드라인"에서 '생체인식정보'를 "생체정보 중 특정 개인을 인증·식별한 목적으로 처리되는 정보로, 특정 개인을 인증·식별할 목적으로 처리되는 정보"로 정의하고 있다. 따라서 생체정보는 특정 개인을 인증·식별하기 위한 목적으로 처리되는 '생체인식정보'와 인증·식별 목적이 아닌, 개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 처리되는 '일반적인 생체정보'로 구성된다. 또한 생체인식정보는 개인을 인증 또는 식별 목적으로 입력장치 등을 통해 수집·입력되는 '생체인식 원본정보'와 이로부터 특징점을 추출하는 등의 일정한 기술적 수단을 통해 생성되는 '생체인식 특징정보'로 구분된다.

「개인정보 보호법」상 보호되는 '개인정보'는 살아 있는 개인에 관한 정보여야 한다. 즉, 이를 세분화하면, ① 해당 대상이 '정보'여야 하고, ② 그러한 정보가 '개인에 관한' 것이어야 하며, ③ 그러한 개인이 '살아 있는' 사람이어야만 한다. 개인의 신체적, 생리적, 행동적 특징에 관한 정보, 즉 생체정보를 원본 정보라 할 때, 생체인식정보는 가공된 정보인 셈이다. 이 중 생체인식정보는 다음과 같은 특징을 갖는다. 첫째, 유일성·불변성이다. 생체인식정보는 그 자체로 개인을 유일하게 식별할 수 있고 변경이 불가능한 특성으로 인해 한번 유출되면 그 피해를 복구하기 어렵다. 다시 말해, 생체인식정보 활용 서비스를 도입하는 경우, 서비스 활용 목적에 필요한 최소한의 정보만을 적법하게 수집하는 것이 필요하다. 둘째, 민감정보의 추출 가능성이다. 원본 정보로부터 인종이나 건강정보 등 인증 및 식별 목적과 무관한 민감정보가 추출될 수 있다. 셋째, 위·변조 가능성이다. 즉, 정보주체가 인식하지 못하는 사이에 이러한 정보가 수집될 수 있다. 앞서 언급한 사례에서 알 수 있듯이 실리콘 인공지문이나 캡처된 얼굴·홍채 사진 등 위·변조된 생체인식정보를 이용한 해킹 사례가 지속적으로 발생하고 있다. 최근에는 카메라 기

위의 가이드라인, 3쪽).

능의 향상과 분석기능의 발달로 인하여 사진 속 손가락 V로부터 손쉽게 지문정보를 취득할 수도 있다.

나. 생체인식정보의 보호 필요성

생체인식기술은 개인이 가진 신체 특징은 태어나서 죽을 때까지 변하지 않는다는 점과 신체 일부가 일치하는 사람은 없다는 점에 착안한 기술이다. 그렇다면 생체인식정보는 일반적인 개인정보와는 달리 정보 그 자체가 개인을 나타낼 수 있는 정보이다. 다시 말해, 생체인식정보는 다른 어떤 정보보다 정보 주체에 대하여 강력한 불가분성 및 일신전속성을 가지므로 생체인식정보만으로 바로 그 정보 주체를 특정할 수 있기 때문에, 생체인식정보의 유출은 해당 정보 주체에 대한 특정으로 이어질 수 있다. 그 결과 생체인식의 직접 결과물인 신원확인 정보뿐만 아니라, 그로부터 간접적으로 알 수 있는 개개인의 현재 건강 상태나 과거 병력(病歷), 심지어 자기 자신조차 제대로 알지 못했던 유전자 정보까지 드러날 수 있다. 특히 유전자 정보는 미래에 사용 가능성을 예측하기 힘들 정도로 확대될 수 있다는 데 큰 위험성을 가진다.[158] 또한 주민등록번호나 휴대전화 번호 등 다른 개인정보는 유출이 확인되는 경우, 비록 번거로운 절차를 거치기는 하나 해당 정보의 폐기 또는 변경을 통해 추가적인 피해를 방지할 수 있는 반면에, 생체인식정보는 특유의 불변성으로 인해 한번 유출되면 피해를 원천적으로 차단하기는 어렵다. 아울러 지문이나 홍채 패턴 등과 같은 생체인식정보는 전자화되어 기기에 저장되는데, 기기를 절취하는 등의 방식으로 생체인식정보가 유출되는 경우 추가 범죄에 노출될 가능성도 매우 높다. 이러한 이유 등으로 생체인식정보를 수집, 저장하고 활용할 때 일반적인 개인정보보다는 더욱 강화된 보호가 필요하다고 할 수 있다.

특히, 이러한 생체인식정보가 인공지능 기술과 결합됨으로써 기본권 침해 가능성이 매우 증폭된다. 앞서 인공지능을 활용한 감시의 기본권 침해 가능성에 관하

158) 김일환(2019), “생체인식정보의 보호와 이용에 관한 법제정비방안에 관한 연구”, 《유럽헌법연구》 제30호, 유럽헌법학회, 512-513쪽 참조.

여 상세하게 검토하였는데, 무엇보다도 감시를 위한 인공지능 기술을 개발하고 활용하는 과정에서 생체인식정보가 대량으로 활용된다는 측면에서 개인정보자기결정권, 사생활의 비밀과 자유 혹은 인격권 등의 침해 가능성을 다시 언급할 수 있겠다. 아울러 국가가 국민의 정보를 수집하는 것 자체를 국가의 감시로 볼 수 있으며, 국가가 나를 지켜보고 있다는 것이 민주주의에 대한 심각한 위험을 초래할 수 있다. 즉, 국가에 의한 감시의 위험성은 기본권 침해 상황 넘어 국가 존립까지도 뒤흔들 수 있다.

3. 예측 치안을 위한 인공지능 활용의 문제점

가. 예측 치안을 위한 인공지능 기술의 활용

경찰활동의 패러다임이 전통적인 사후 대응적 범죄수사로부터 사회 각 기능과의 참여와 공유를 통하여 범죄를 사전에 억제하고, 예방하는 선도적 활동으로 진화하면서 예측 치안 내지 예측적 경찰활동(predictive policing)의 중요도가 증대하고 있다.[159] 발생 가능성이 있는 잠재적인 범죄행위를 예방하기 위한 목적으로 인공지능 및 빅데이터 등 지능정보기술에 기반한 예측분석 결과가 예측 치안 분야에서 적극적으로 활용되고 있다.[160]

예측 치안 알고리즘의 기본적 가정은 범죄가 무작위로 발생하는 것이 아니라, 특정 장소, 사람과 관련되어 발생한다는 것이다. 범죄패턴을 분석하면 범죄는 특정 시기에 특정 피해자와 취약한 공간이 만들어내는 환경적 요인의 산물이며, 범죄자들은 적은 노력과 위험으로 높은 보상을 제공하는 대상을 선택한다는 사실이 드러난다. 즉, 범죄는 무작위로 발생하는 것이 아니라, 동기를 가진 잠재적 범죄자, 적절한 대상, 범죄를 방지할 수 있는 장치의 부재와 같은 시공간적 요소의 결

159) 윤상연·신상화(2018), “범죄 예측의 현재와 미래 - 한국형 범죄예측 시스템 개선·도입에 대한 제언 -”, 《한국공안행정학회보》 제27권 제3호, 한국공안행정학회, 246쪽.

160) 정채연(2023), “예측적 치안과 형사정책”, 《영남법학》 제57호, 영남대학교 법학연구소, 67쪽.

합으로 발생한다.[161] 데이터를 분석한 결과, 특정 범죄자가 범죄를 범할 가능성이나 특정 지역의 범죄 발생 가능성이 크다는 패턴을 발견하게 되면, 해당 장소를 순찰하거나 해당 범죄자를 감시하여 범죄를 효율적으로 예방하는 것이다.[162]

예측적 치안의 가장 일반화된 방식이라 볼 수 있는 지리 공간적 범죄예측은 1960년대부터 미국과 유럽을 중심으로 발전해 왔고, 2000년대 후반 들어 인공지능의 발전에 힘입어 상용화가 본격적으로 가능해지게 되었다.[163] 우리나라에서도 스마트 경찰활동을 표방하면서 범죄 예측 시스템을 도입하고자 하는 노력을 기울이며, 2009년 범죄 다발지역 및 수사 대상자를 분석하고 예측하는 지리적 프로파일링 시스템을 시작으로, 2019년부터 경찰청은 범죄분포 이해도구(Crime Layout Understanding Engine: CLUE)와 2021년 예측적 범죄위험분석 시스템(Predictive Crime Rick Analysis System: Pre-CAS)을[164] 시범운영하고 있다. Pre-CAS는 치안. 공공데이터를 통합한 빅데이터를 최신 알고리즘을 적용한 인공지능으로 분석하여 지역별 범죄 위험도와 범죄발생 건수를 예측하고 효과적인 순찰 경로를 안내하는 시스템이다.[165] 「경찰관 직무집행법」 제8조의2는 "경찰관은 범죄·재난·공공갈등 등 공공안녕에 대한 위험의 예방과 대응을 위한 정보의 수집·작성·배포와 이에 수반되는 사실의 확인을 할 수 있다"고 규정하고 "정보의 구체적인 범위와 처리 기준, 정보의 수집·작성·배포에 수반되는 사실의 확인 절차와

161) 양종모(2021), "법 분야 위험의 예측을 위한 인공지능 알고리즘과 관련된 법적 쟁점", 《IT와 법연구》 제22집, 경북대학교 IT와 법연구소, 385쪽.

162) 안경옥(2023), "빅데이터를 활용한 범죄예측의 문제점과 개선방향", 《비교형사법연구》 제24권 제4호, 한국비교형사법학회, 67쪽.

163) Degeling, M., Berendt, B.(2018). "What Is Wrong about Robocops as Consultants? A Technology-Centric Gritique of Predictive Policing", *AI&Society*, Vol. 33, p. 348, 정채연(2023), 앞의 논문, 69쪽에서 재인용.

164) Pre-CAS는 기존의 범죄발생 통계 중심의 단편적 분석에서 벗어나, 범죄통계·112 신고 등 치안데이터와 인구, 주요업종 건물유형 등의 공공데이터를 융합, 분석한다는 장점이 있다.

165) 경찰청(2021), "범죄 위험도 예측·분석 시스템 PRE-CAS(Predictive Crime Risk Analysis System 통합매뉴얼", 2쪽.

한계는 대통령령으로 정한다"고 되어 있다. 이에 따라 2021년 3월 23일에 시행된「경찰관의 정보수집 및 처리 등에 관한 규정은 "정보활동의 기본원칙을 정하고, 국민의 자유와 권리를 보호하는 것을 원칙으로 필요최소한의 범위에 그칠 것"을 규정한다. 또한 경찰관이 수집·작성·배포할 수 있는 정보의 구체적인 범위규정을 두고 있는데, "범죄의 예방과 대응에 필요한 정보·재난·안전사고 등으로부터 국민안전을 확보하기 위한 정보, 국민의 생명·신체·재산의 보호와 공공안녕에 대한 위험의 예방과 대응을 위한 정책에 관한 정보 등"이다.[166] 수사와 구별하여 예측 치안활동을 위한 정보처리의 범위를 따로 정하고 있지 않으며, 법령에 경찰관은 비교적 넓은 범위의 범죄 예방과 대응에 필요한 정보를 수집 및 처리할 수 있도록 근거가 마련되어 있다.

나. 예측 치안의 위험성

2019년 법무부가 도입한 '범죄징후 예측시스템'은 특정 범죄 유형은 유사한 범죄 패턴을 반복한다는 점에 착안하여 전자발찌 비부착자에게 이상징후가 발견되면 이를 보호관찰관에게 고지하도록 하는 시스템이다.[167] 또한 경찰이 과학기술로 치안서비스를 개선하기 위해 추진하는 '폴리스랩 2.0사업'의 경우 금융·통신사로부터 받은 비정형화된 수사자료를 인공지능 기술을 사용하여 분석하는 '차세대 지능형 수사자료 분석 솔루션'을 개발하는 계획을 다루고 있다.[168] 그러나 특정 개인의 범죄위험도를 예측하는 것은 개인의 범죄성향에 대한 추상적 수준의 평가에 머무를 뿐 그 정확도를 담보할 수 없으며, 따라서 일반 국민을 대상으로 범죄예측 시스템을 구축하는 것은 사실상 불가능한 것으로 판단한다. 기본권 침해의 소지가 없는 지역 기반의 예측 기술은 손쉽게 사용하고 효율성을 높일 수 있겠으나 인적

166)「경찰관의 정보수집 및 처리 등에 관한 규정」제3조.

167) 강미영·정혜진(2022), "인공지능 기반의 CCTV에 의한 범죄예측 시스템 도입에 따른 법적 과제와 활용방안",《강원법학》제66권, 강원대학교 비교법학연구소, 202쪽.

168) 정보통신신문(2022. 7. 26.), "경찰, ICT·과학기술 융합 "더욱 든든한 치안 구현"", https://www.koit.co.kr/news/articleView.html?idxno=100518(2024. 10. 3. 최종 방문).

기반 예측의 경우는 사생활 및 인격권 침해의 소지가 있어 그 사용이 엄격한 요건하에 제한되어야 할 것이다. 아직 범죄가 실현되기 전의 시점이자 범죄를 저지르지 않은 상태에서 개인에 대한 기본권 제한이 정당화될 수는 없을 것이며, 사실상 감시에 해당한다고 할 수 있는 예측 시스템의 경우 더욱 그러하다. 다만 범죄 이력이 있는 자를 대상으로 제한적으로 도입될 가능성은 고려해 볼 수 있다.[169]

예측적 치안 프로그램이 가장 활발하게 사용되는 미국에서도 예측 결과의 비일관성과 사회적 차별문제를 비롯한 부작용 및 역효과를 고려하여 범죄 예측에 대한 재검토가 이루어지는 것으로 보인다. 예컨대 2020년에는 캘리포니아주 산타크루즈 경찰서가, 2021년에는 로스앤젤레스 경찰서가 예측적 경찰활동 소프트웨어 사용을 중단하기로 잠정 결정했다는 점을 유의미하게 바라볼 필요가 있다.[170]

예측적 치안과 관련하여, 근대 형법은 범죄실행의 사후대응에 기초한 시스템을 채택하고 있으므로 아직 저질러지지도 않은 범죄에 대한 산술적 예측으로 인해 시민의 기본권이 침해되어서는 안 된다는 형사사법의 법치국가적 관점을 재확인하고 있다.[171] 범죄예측과 관련하여서는 우리나라에서 활용하고 있는 범죄예측시스템이 선제적인 재범방지활동을 하며 비용 면 등에서 장점이 있기 때문에 종래의 전자감독제도와는 차원이 다르다는 점은 부인할 수 없다. 문제는 수집하는 개인정보에는 위치정보 이외에 생활정보나 인적 정보 등이 포함되며, 생활패턴을 실시간으로 분석하므로 개인의 사생활 영역을 심각하게 침해할 수 있다는 것이다.[172] 범죄에 대한 사전적 예측이라는 이익과 개인의 사생활 보호에 대한 이익이 충돌되므로 이러한 시스템의 적절성 여부가 문제가 된다고 하겠다.[173] 기본권 제약을

169) 정채연(2023), 앞의 논문, 81쪽.

170) 오경석·조미지(2023), “인공지능 경찰활동 도입 쟁점에 관한 연구”, 《경찰학연구》 제23권 제1호, 경찰대학, 47쪽.

171) 정소영(2022), “형사사법에서의 인공지능 사용에 대한 유럽의회 결의안: ‘인공지능에 의한 결정’ 금지에 관하여”, 《형사정책》 제34권 제2호, 한국형사정책학회, 140쪽.

172) 박민지·서정범(2020), “전자감독제도의 예방적 경찰활동으로서의 함의 - 범죄징후 예측시스템의 허용성을 중심으로 -” 《고려법학》 제99호, 고려대학교 법학연구원, 140쪽.

헌법적으로 정당화할 수 있는 공익과의 면밀한 형량은 결국 좁은 의미의 비례성 심사, 즉 법익의 균형성 판단으로 이어진다. 데이터 수집과 활용으로 인한 개인정보자기결정권 및 사생활, 인격권에 대한 제약이 얼마나 중한지, 반대로 이를 감수하면서 예방할 수 있는 범죄의 중대성을 살펴보아야 한다. 문제는 예측 치안 알고리즘의 사용 과정에서 어떤 문제가 발생하였을 때 경찰이 책임을 회피할 가능성이 높다. 흔히 경찰은 예측 치안 알고리즘의 단순한 구매. 사용자이며 치안 알고리즘으로 인한 문제는 오로지 개발자의 책임이라고 생각하기 쉽다. 그러나 경찰은 단순한 사용자가 아니라 예측 치안 알고리즘의 훈련에 사용되는 주요 데이터의 생산자라는 점이 간과되어서는 아니된다.[174]

또한 경찰이 기록한 범죄자료는 경찰이 경찰활동을 하는 과정에서 수집한 데이터로 구성되는데 이 데이터가 발생한 모든 범죄에 대한 온전한 설명이 될 수는 없다. 경찰은 가용자원의 제약으로 인해 발생한 모든 범죄를 적발할 수 없고 어느 정도 누락은 불가피하다.[175] 그러다 보니 경찰이 작성한 범죄자료는 어느 정도까지는 특정 경찰 부서 또는 개별 경찰관이 어떤 지역사회와 개인을 직무 집행의 대상으로 삼아야 하는지와 같은 선택을 반영할 수밖에 없는데, 경찰의 이러한 선택적 의사결정이 범죄현실의 인식이나 범죄통계형성에 결정적 역할을 한다.[176]

유럽연합 역시 형사사법 분야에서 인공지능을 기반으로 자동화된 의사결정 시스템을 활용을 지양하도록 권고하는 입장이다. 2021년 10월 발표한 「형사사법에서의 인공지능 사용에 대한 결의안」을 보면, 형사사법적 결정이 인공지능기술에 의해 이루어져서는 안 된다는 기본방침을 설정하고, 형사사법 영역에서 인공지능의 자동화된 의사결정이 갖는 역기능에 대해 심각한 우려를 표방하며 인공지능의

173) 안경옥(2023), 앞의 논문, 73쪽.

174) 양종모(2021), 앞의 논문, 387쪽.

175) Elizabeth E. Joh(2014). Elizabeth E. Joh, Policing By Numbers: Big Data And The Fourth Amendment, *89 Wash. L. Rev. 35*, pp. 289-290, 양종모(2021), 앞의 논문, 387쪽에서 재인용.

176) 양종모(2021), 앞의 논문, 387쪽.

공리적 효용으로 인해 기본권 보호의무를 해태하여서는 아니 된다는 분명한 입장을 취하고 있다.[177)]

4. 형사사법 분야에서의 인공지능 활용의 문제점

가. 인공지능기반의 음성인식활용조서 도입 논의

최근 형사사법 절차에 리걸테크의 도입 논의가 활발해지면서 형사전자소송의 가능성을 모색하는 다양한 시도가 이루어지고 있으며, 그 일환으로 「형사사법절차에서의 전자문서 이용 등에 관한 법률(이하 "형사절차전자문서법"이라 한다)」이 2021년 제정되어 2025년 6월 시행이 예고되어 있다. 「형사절차전자문서법」은 형사사법업무를 처리하는 기관의 형사사법업무와 관련된 절차를 전자화하는 데 의의가 있는데, 이를 위해 형사사법업무를 처리하는 기관은 원칙적으로 관련 문서를 전자문서로 작성하거나(제10조), 전자화문서로 시스템에 등재할 것을 규정하고 있다(제11조). 형사전자소송의 시행을 앞두고 있는 상황에서 그 성패를 좌우할 만한 사유로는 개인정보보호 및 범죄피해자의 2차 피해 방지 등 정보접근성 문제 이외에 우리 법조계의 보수적이고 경직된 법문화도 거론되고 있다.[178)] 즉, 디지털 심화 시대로의 전환기에 즈음하여 디지털기기의 사용에 익숙한 사람들이 늘고 있지만 여전히 변화에 익숙하지 않은 사람들은 존재하고, 모니터에 현출된 전자문서보다는 종이문서를 읽고 정리하는 것에 익숙한 업무 습관도 단시일에 개선될 여지는 없다. 실제 「형사절차전자문서법」이 시행되더라도 종이문서에 익숙한 사람들에게는 전자문서의 출력을 선호할 가능성이 있다.

그런데 실무의 관행이 형사절차의 전자화와 부합하지 않을 수도 있다. 예를 들면 피의자신문조서의 경우에는 피의자를 수차례 소환하여 신문하는 과정에서 조서의 증감 또는 수정보완이 일상이라는 점에서 그 전체 과정을 전자화하는 것이

177) 정소영(2022), 앞의 논문, 139-140쪽.

178) 박성민(2023), "리걸테크의 도입과 형사전자소송의 가능성과 한계", 《형사소송 이론과 실무》 제15권 제2호, 한국형사소송법학회, 283쪽 이하.

쉽지 않다. 2024년 6월 제정안이 발의된「형사사법절차에서의 전자문서 이용 등에 관한 법률 시행령안(이하 “시행령안”이라 한다)」제16조 제2항은 “형사소송법에 따른 조서내용의 증감변경 및 이의제기 내용에 대하여는 컴퓨터 등 정보처리장치를 이용하여 기재하고 전자서명(실지명의를 확인할 수 있음을 요하지 아니한다)을 할 수 있다”고 규정하고 있다. 해당 규정은 마치 피신조서의 증감변경 시 그 내용 기재까지 임의로 할 수 있는 것처럼 이해할 수 있지만, 증감변경 시 내용 기재는 의무[179]라고 보아야 하며, 형식적 진정성립에 있어 기존 규정과의 관계에서 후단의 전자서명의 임의성을 규정한 것으로 이해하는 것이 적절할 것으로 판단된다. 문제는 제3항의 규정인데, 제3항은 제2항에도 불구하고 피의자가 종이문서에 기재할 것을 요구하는 경우에는 조서를 출력하여 종이문서로 작성하고 이를 전자화할 것을 요구하고 있다. 시행령안 제16조는 이와 같은 절차를 참고인진술조서의 경우에도 준용하므로 실제 조서작성에 있어 일선 실무관의 업무 부담은 경감되는 것이 아니라 오히려 가중될 수 있다.

이에 따라 최근 법무부는 조서작성에 있어 실무자들의 부담을 경감시키기 위해 인공지능기반의 음성인식활용조서의 도입을 검토하고 있다고 한다.[180] 해당 시스템은 조사자와 피조사자의 음성을 인공지능이 자동으로 전자문서로 변환해 주는 시스템인데, 피의자 또는 참고인에 대한 조사 시간을 획기적으로 단축하고 조사과정에서 피의자 및 피해자에 대한 인권 보호 기능도 강화할 수 있을 것이다. 조사자 및 피조사자의 음성을 문자로 자동 변환하면, 종래 조서 작성 과정에서 조서의 작성내용을 두 번 세 번 확인하면서 피의자를 압박하거나 성범죄 피해자에 대해서도 피해사실을 확인하면서 고통을 가중하는 것과 같은 소위 2차 피해도 방지할 수 있을 것으로 기대된다. 특히 최근 원격화상진술제도의 도입 및 영상녹화물

179) 피의자신문조서의 내용에 증감 변경이 있는 경우에 이를 기재하지 않는 것은 조서 성립의 진정이 부정될 수 있는 중요한 절차적 하자라고 할 수 있다.

180) GTT KOREA(2022. 4. 6.), “음성인식 기술로 자동으로 조서 작성한다”, https://www.gttkorea.com/news/articleView.html?idxno=586 (2024. 10. 3. 최종 방문).

의 본증사용 여부 검토 등 디지털 증거활용의 변화를 모색하는 목소리가 커지고 있는 상황에서 인공지능기반 음성인식활용조서의 도입은 형사전자소송의 안착에 중요한 변곡점이 될 수 있다. 이처럼 인공지능 음성인식의 정확도가 증가하고 있다는 점에서 이와 같은 제도의 도입은 고무적이지만, 조서작성 후 피의자의 확인과정을 감안하면 시스템의 고도화가 전제되지 않으면 업무부담의 감경효과를 장담하기 어려울 수 있다는 점은 여전히 문제로 남는다.

나. 영상녹화물의 본증사용과 증명력 판단

구「성폭력범죄의 처벌등에 관한 특례법」(2012. 12. 18. 법률 제11556호로 전부개정된 것) 제30조 제1항은 19세 미만자 또는 장애인인 성폭력 피해자의 진술과정을 영상녹화하게 하고 그 영상녹화물에 대해서는 예외적으로 본증사용을 인정하고 있었지만, 헌법재판소는 해당 규정의 19세 미만의 성폭력 피해자 부분에 대해 과잉금지원칙위반을 이유로 위헌결정한 바 있다.[181] 이에 따라 해당 성폭력 피해자의 영상녹화물을 본증으로 사용하려면 해당 피해자가 법정에서 진술에 의한 성립의 진정을 인정해야 하거나 법정에서 피고인 측의 반대신문을 받아야 하는 부담이 추가되었다. 헌법재판소 결정 이후 논의는 피해자의 2차 피해 방지에 집중되었고 헌법재판소도 공판 전 증거보전절차의 적극적 활용, 심리비공개 등 다양한 방안을 제시하였으며 그중에는 비디오 등 중계장치에 의한 증인신문도 있다. 소위 전자적 원격진술이 그것인데, 기술적으로는 신문과정에 약간의 시간 차를 둠으로써 피해자와 피고인과의 접촉점을 제한하거나 신문과정에서 질문자의 음성을 피해자에게 친숙한 음성으로 변환하는 등의 음성변조기술을 도입할 수도 있으며, 인공지능의 자연어처리기술을 통해 신문과정에서의 욕설 및 공격적인 표현을 구분하여 사전에 차단하는 등의 방법도 고려할 수 있다.

이미 2020년부터 성폭력 피해자나 아동학대 피해자를 지원하는 해바라기 센터 및 성범죄 피해자를 조사하는 경찰청은 셀바스 AI의 'AI 음성인식 기반 성폭력 피

181) 헌재 2021. 12. 23. 2018헌바524, 판례집 33-2, 760.

해 조서 작성 시스템'[182]을 사용하여 피해자의 진술부담을 최소화하는 작업을 하고 있다. 이를 고도화하는 작업도 순차적으로 진행되어 피해자를 통해 제출받은 전화 녹취 음성파일을 조서 작성 시스템에 업로드하여 바로 인식할 수 있는 기능 등을 추가하거나,[183] 2023년부터는 모든 대화 내용의 기록 및 앞서 확인한 음성정보의 조서화 등의 기능을 지원한다고 한다.[184]

이처럼 인공지능 기반의 음성인식조서 활용 방안이 고도화되면서 이에 덧붙여 해당 영상녹화물의 본증사용 여부도 전향적으로 검토해 볼 수 있다. 조서에 드러난 사실 이외에 영상녹화물은 피해자 등 진술자의 진술 당시의 모습을 생생히 볼 수 있다는 점에서 요증 사실 판단에 중요한 근거가 될 수 있다. 영상녹화물의 본증사용을 제한하는 것은 우리 「형사소송법」이 왜곡이나 조작의 가능성이 있는 증거물의 진정성을 인정하지 않으려는 취지에 기인한 것이지만, 최근에는 조사 과정을 영상녹화한 경우 영상녹화물의 본증사용을 인정해야 한다는 주장도 있다.[185] 조작가능성이나 왜곡의 가능성이 기술적으로 보완 가능한 영역이라면 영상녹화물의 본증사용을 주저할 이유는 없다. 특히 형사전자소송과정에서 신문조서의 작성

182) 셀비 노트(Selvy Note)를 기반으로 한 AI 조서 작성 솔루션으로 수사 과정에서 이루어지는 음성 진술을 자동으로 텍스트 변환하여 기록 및 저장하고, 이를 데이터베이스화한다. 이를 통해 조사관들의 업무 부담 감소뿐 아니라 피해 진술 부담 최소화에도 큰 도움을 주고 있어 호평을 받고 있다고 한다. 뉴스핌(2021. 7. 21.), "셀바스 AI, 'AI 음성인식 기반 성폭력 피해 조서 작성 시스템' 경찰서·해바라기센터 확대 적용", https://www.newspim.com/news/view/20220804000126 (2024. 10. 3. 최종 방문).

183) 뉴스핌(2021. 7. 21.), 앞의 기사 참조.

184) 인공지능신문(2023. 9. 4.), "셀바스AI, 경찰청 'AI 음성인식 피해조사 시스템' 고도화…완성도 높은 조사 및 양질의 수사 지원 목표", https://www.aitimes.kr/news/articleView.html?idxno=28846(2024. 10. 3. 최종 방문).

185) 경향신문(2024. 8. 11.), "피의자 신문 영상, 증거 채택을", https://m.khan.co.kr/opinion/column/article/202408112110015?fbclid=IwY2xjawEmf9pleHRuA2FlbQIxMQABHRXW6cteRmQw1fCJK_zH7xdfMbJPaMaC-8GDLKOXtw6kWWMo8rNIH5tqJg_aem_k2wxhbp3xnZzQJOPC1BQHA&sfnsn=mo#c2b (2024. 10. 3. 최종 방문) 참조.

및 변경이나 전자문서화 과정이 오히려 수사기관의 업무효율성을 저하시킬 수 있다는 점, 조서의 형식적 진정성립요건에 대한 검증과 전자문서와의 부조화[186] 등의 지적이 있다는 점에서 영상녹화물의 본증사용에 대한 사고전환 및 개정에 대한 환경이 변화되고 있는 것만은 분명하다.

피해자 진술 시 음성녹화 또는 영상녹화물의 경우 그 진술의 신빙성을 판단할 수 있는 다양한 요소가 내재되어 있다는 점에서 인공지능 기술을 통해 그 진술의 신빙성을 판단할 수 있다는 입장도 있다. 아동 또는 장애인 피해자 진술의 신빙성 판단에 인공지능 알고리즘을 활용하는 방안을 도입하자는 입장[187]이 그것이다. 지적장애 또는 아동 성범죄의 경우 피해자 진술은 그 증거의 가치에도 불구하고 진술의 신빙성 판단에 어려움이 있는 만큼, 법원을 기속할 수 없는 전문가 감정서에 의존하는 것보다 인공지능 기술을 활용하여 그 진술의 신빙성을 확인하고 증명력을 제고하고자 하는 것이 골자이다.[188]

이와 관련해서는 인공지능이 과거 사례의 성폭력 사건을 학습하는 과정에서 피해자 유발주의 또는 피해자 저항 가능성이라는 판단기제를 학습함으로써 성인지 감수성이 결여된 학습 결과를 도출할 가능성이 있다. 법리적인 관점에서는 증거의 신빙성이라는 증명력 판단을 판사가 아닌 인공지능이 한다는 점에서 「형사소송법」 제308조 자유 심증주의 원리는 후퇴하고, 종국적으로 인공지능 판사가 도입되는 결과[189]에 직면하게 될 것이다.[190] 물론 현재로서는 증거의 증명력 판단 이전에

186) 이에 따라 디지털전자문서의 전문증거예외인정을 위한 별도의 규정 마련을 요구하는 입장으로는 김윤섭·박상용(2015), “형사증거법상 디지털 증거의 증거능력 - 증거능력의 선결요건 및 전문법칙의 예외요건을 중심으로 -”, 《형사정책연구》 제26권 제2호, 한국형사정책연구원, 209쪽.

187) 손지영(2021), “AI와 형사사법 리걸테크 시스템”, 《제도와 경제》 제15권 제4호, 한국제도경제학회, 156쪽 이하.

188) 손지영(2021), 앞의 논문, 156쪽.

189) 유럽의회는 이미 ‘형사사법에서의 인공지능 사용에 관한 결의안’을 통해 형사사법의 결정에서 인공지능 사용을 금지해야 한다는 결론을 내린 바 있다.

190) 인공지능 기술을 진술의 신빙성 판단에 이용하는 데 있어 비판적 입장으로는 박성민(2023), 앞의 논문, 301쪽 이하.

과학적 증거의 증거능력 인정 및 본증사용 여부와 관련된 기술적 문제가 선제적으로 해결되어야 할 것이다. 즉, 전자적 원격진술 방법을 조사방법으로 도입하고 그 영상녹화물의 본증사용이 인정된다는 전제하에 그 진술의 신빙성 논의가 시작될 수 있을 것이다.

5. 인공지능 감시를 통한 노무관리의 문제

알고리즘 노무관리나 AIWM은 앞서 언급한 노무제공자의 개인정보보호뿐만 아니라 노동감시의 문제를 제기한다. 국가인권위원회는 "사용자가 각종 정보통신기술을 활용하여 사업장 내외에서 근로자의 작업과정은 물론 일상생활에 이르기까지 각종 정보를 수집·저장·전송·가공· 분석하는 모든 행위"를 사업장의 전자감시로 정의한다.[191] 알고리즘 노무관리나 AIWM을 통한 노무관리에 노무제공자와 관련한 광범위한 데이터 처리와 분석 및 알고리즘을 통한 예측과 의사결정을 통한 더 정교한 상시 노동감시가 포함될 수 있다. 즉, CCTV 등 영상시스템, RFID 카드 등 IC칩 카드, 지문, 홍채 등 생체정보를 수집하는 인식기와 위치추적시스템(GPS), 개인용 컴퓨터 및 전화 열람·감청, 다수 사업장에서 구축되는 업무(생산) 통합관리시스템(ERP 등) 등 다양한 전자감시기술이 알고리즘 내지 인공지능과 결합하여 직원채용, 업무 할당, 시장예측과 직장 내 의사결정 지원 등 노동의 전 과정에서 기술적으로 강력한 노동통제를 수행할 수 있게 되었다.[192]

이러한 노동감시는 플랫폼 노동에서 매 순간 이루어진다. 주문의 수락 여부, 수락 이후 해당 노무 제공이 완료되기까지 걸리는 시간, 배달이나 운송의 경우 경로 이동에 대한 위치 추적, 주문 거절 횟수나 고객 평가 별점의 저장을 통한 성과 관리와 계정 이용 제한 등 노무제공의 개시 여부 결정부터 해당 디지털 노동 플랫폼 이용을 종료하는 순간까지 노동감시는 노동을 위해 필수적으로 이용해야 하는 애

191) 국가인권위원회 결정(2007. 11. 12.), "사업장 전자감시에서 근로자의 인권보호를 위한 법령·제도 개선권고", 6쪽.

192) 이율경(2024), "노동관계에서 알고리즘에 관한 법적 쟁점", 《노동법연구》 제56호, 서울대노동법연구회. 240쪽.

플리케이션을 통해 계속 수행된다.

기술 발전으로 감시수단이 첨단화되면서 노동관계에서 감시의 범위와 폭이 확대되어 전자감시는 시간적 및 공간적 범위가 계속해서 확장되고 있고, 감시의 강도도 높아지고 있으며, 신체뿐 아니라 다양한 정보를 활용하여 작업자의 정신 영역에 대한 감시까지 기술적으로 가능해지고 있다.[193] 이러한 노동감시는 해당 감시를 통한 노무제공자의 사생활 침해 위험을 내포한다. 따라서 알고리즘 노무관리나 AIWM은 사용자의 노무지휘권과 근로자 사생활의 자유 사이의 권리 충돌을 야기하며, 이는 결국 알고리즘 노무관리나 AIWM을 통한 노동감시의 허용 가능성과 허용 한계의 문제를 제기한다.

근로자의 안전과 건강에 대한 AIWM의 위험성으로 AIWM이 설정한 생산성 달성을 위하여 부여되는 업무 강도, 업무 통제 및 자율성 상실, 근로자의 비인간화, 근로자의 데이터화, 근로자 차별 및 개인정보 및 민감데이터 사용, 성과 모니터링, 작업자 평가 시스템, 위험하고 안전하지 않은 작업자의 행동경향, 반복적인 움직임이나 어색한 자세 및 인체공학적 문제, 외로움과 사회적 고립, 알고리즘 노무관리에 대한 저항, 투명성 및 신뢰 부족, 권력 비대칭, AIWM의 오작동과 그 영향, 작업자가 노출되는 전자기장 수준 증가 등 기타 위험이 제시된다.[194]

AIWM의 대상이 되는 작업자에게 작업자가 최소한의 휴식 시간 없이 일하도록 지시하고, 특정 절차에 소요되는 시간을 최소화하며, 빠른 속도로 일하도록 강요하는 AIWM 시스템을 구현할 수 있다. AIWM으로 인한 업무 강화의 예로 작업 속도를 높이기 위해 지시를 수행하고 완료하는 시간뿐만 아니라 작업자의 이동, 실수, 휴식 시간을 추적하는 데 AIWM을 활용하는 것을 들 수 있다. 이는 노동감시와도 연결된 문제이다.

---

193) 강현철 외(2013), “정보통신기기에 의한 노동인권 침해 실태조사”, 국가인권위원회. 8쪽.

194) Reinhold, K., Järvis, M., Christenko, A., Jankauskaitė, V., Paliokaitė A. & Riedmann, A.(2022). *Artificial intelligence for worker management: implications for occupational safety and health*, European Agency for Safety and Health at Work. pp. 8-14.

이러한 시스템은 사무직에서도 활용되고 있다. 예를 들어, 영국에 본사를 둔 금융회사인 Barclays는 런던 소재 본사에서 추적 소프트웨어를 사용하여 직원들이 책상에 머무는 시간을 기록하고 화장실 휴식 시간을 모니터링하여 알고리즘에 의해 휴식 시간이 너무 길어 업무 강도가 높아진다고 판단되면 근로자에게 알려준다.[195] 이 시스템은 또한 목표에 미달하는 직원에게 제안을 하기도 한다. 2017년에 이미 Barclays는 열과 동작을 감지하는 센서를 사용하여 직원들이 책상에서 보내는 시간을 기록하는 OccupEye라는 추적 장치를 사용한 것에 대해 비판을 받았다. 당시 Barclays는 성명서를 통해 이는 직원의 생산성을 모니터링하려는 것이 아니라 사무실 공간 사용량을 평가하고 에너지 효율성을 개선하려는 의도였다고 해명했다.

이러한 알고리즘 노무관리는 노무제공자의 건강과 안전을 위협할 수 있다. 특히 플랫폼 노동 분야의 산업재해 발생 건수는 알고리즘 노무관리를 기본적 노무관리 방식으로 채택하고 있는 플랫폼 노동에서의 노무관리가 근로자의 위험을 방지하고 건강을 증진하는 방식으로 수행되고 있지 않다는 것을 보여준다. 2023년 윤건영 의원이 공개한 산업재해 승인 1위 기업이 '배달의민족' 물류서비스를 전담하는 '우아한청년들'이었다. 2023년 1월부터 8월까지 우아한청년들의 산업재해(사고·질병) 신청 건수는 1,312건, 승인 건수는 1,273건이었다. 라이더 사망사고로 유족이 산재를 신청해 승인된 사례는 5건이었다. 우아한청년들에 이은 산업재해 승인 2위는 HD현대중공업(521건), 3위는 대우건설(467건)이었으며 2위와 비교하여 우아한형제들의 승인 건수는 2배 이상이었다. 알고리즘 노무관리가 활용되는 쿠팡과 물류 자회사들의 같은 기간 산재 승인 건수도 높은 순위를 기록했다. 쿠팡주식회사는 2023년 올해 1~8월 322건(공동 7위), 같은 기간 쿠팡의 물류 자회사인 쿠팡풀필먼트서비스 대구센터는 322건, 쿠팡로지스틱스서비스유한회사는 262건의 산재 승인 건수를 기록했다.[196] 이를 통해 알 수 있는 것은 알고리즘 노무관

195) Eurofound(2020), *Employee monitoring and surveillance: The challenges of digitalisation,* Publications Office of the European Union. p. 32.

196) 윤건영 의원의 공개 자료는 경향신문(2023. 10. 3.), "올해 산재 승인 1위는 '배달의

리가 노무제공자의 건강한 노무제공이 아닌 생산성 향상을 목적으로 하고 있고, 이를 위해 채택하는 다양한 정책들, 예를 들어 최저임금이 적용되지 않는 상황에서 시간대별로 달라지는 배달수수료로 인해 라이더들은 장시간 노동과 배달 건수를 늘리기 위한 속도경쟁을 하게 되고 상대적으로 배달수수료가 높은 공휴일이나 좋지 않은 기상 환경에서의 노무제공, 장시간 노무제공을 하게 되는데 이는 결국 과로로 이어져 사망에 이르기도 한다.

알고리즘 노무관리와 AIWM 등에 대한 규제에서 중요하게 논의되는 문제가 노무제공자의 개인정보 보호이다. 인공지능을 활용한 노무관리는 개별 근로자에 대한 데이터 수집을 토대로 이루어지고, 해당 데이터는 대체로 수집과 활용에 동의가 필요한 개인정보이기 때문에 노무제공자의 개인정보에 관한 권리를 침해할 소지가 있다. 따라서 「개인정보보호법」 영역에서 노무제공자의 정보권을 중심으로 각국에서 법적 분쟁이 발생하고 있다. 이러한 분쟁은 알고리즘 노무관리가 고도화된 플랫폼 노무제공자의 개인정보를 중심으로 발생하여 왔다. 특히, 우리나라에서는 개인정보자기결정권이 헌법상 기본권이기 때문에 개인정보의 헌법적 보장과도 연결된다.

디지털 플랫폼 노동의 경우 알고리즘에 의한 노무관리가 필수적으로 활용되며 이러한 노무관리에서 수집되고 활용되는 데이터 중 상당수가 헌법상 개인정보자기결정권의 대상인 개인정보이다. 현재의 기술은 위치 추적과 동선 파악과 같은 수행에 대한 통제뿐만 아니라 해당 노동자에 대한 프로파일링, 감정 인지, 건강상태 등 개인의 인격 및 내밀한 정보에 대한 수집도 가능한 정도로 발전하였다. 이러한 기술은 노동을 매개하는 디지털 노동 플랫폼의 노무제공자에 대해 활용된다. 따라서 이러한 기술이 어떤 방식으로 구현되고 있고 무슨 정보를 어느 정도로 수집하고 있는지에 대해 정보의 공개를 요구하고, 자신의 데이터에 접근, 수정, 삭제, 처리 및 이동 제한을 포함한 자신과 관련된 데이터 전반에 대한 기본권의

민족' … 달라지는 산재 지도",
https://www.khan.co.kr/national/labor/article/202310031216001(2024. 10. 3. 최종 방문).

보장이 플랫폼 노동자에 대한 헌법적 보호 및 「개인정보보호법」 영역에서 핵심적인 부분을 차지한다.[197] 또한 이러한 노무관리의 확대에 따라 개인정보보호 관련 법제상 데이터 주체의 권리 내용, 데이터 주체의 동의와 예외적 동의 면제 등 권리의 범위 및 행사, 제3자의 정당한 이익 등과 관련하여 실무상 구체적 가이드라인의 요구가 확대되고 있다.

6. 소결

기술이 빠른 속도로 발전을 거듭한다고 하여도, 기술 그 자체로는 가치중립적이다. 따라서 기술의 활용으로 인한 효과도 언제나 긍정적 또는 부정적, 하나의 방향으로만 나타나지는 않는다. 인공지능 기술에 대해서도 마찬가지이다. 장미빛 미래를 그리는 것도, 지나친 회의론으로 기우는 것 모두 경계해야 할 것이다. 과학기술의 혁신을 통해 국민경제의 발전을 이룩하는 것은 국가의 헌법적 의무에 해당하지만, 기술 자체에 대해서 충분한 이해를 바탕으로 그 효과와 부작용에 대한 철저한 분석을 거쳐서 부정적 영향을 최소한 후에 기술을 활용함으로써 긍정적 효과를 극대화해야 할 것이다. 감시와 관련된 분야에서는 더욱 신중해야 할 것이다. 인공지능 기술을 감시에 활용하게 되면 효율성이라는 긍정적 효과를 얻을 수 있다. 인공지능이 인간과 유사한 지적 능력을 발휘하여 본래 감시를 담당하였던 인력의 업무 부담을 크게 감소시키는 것은 물론이고, 피로의 누적, 질병, 휴가 등의 문제는 전혀 발생시키지 않는다는 장점이 있다. 또한 정교화된 기술이 인간보다 더 신속하고 정확한 예측을 가능하게 한다는 것도 큰 장점일 것이다.

그러나 이러한 긍정적 효과에는 일정한 대가가 따르는데, 감시를 목적으로 인공지능 기술을 활용하게 되면 방대한 개인정보의 수집 및 이용이 뒤따르는 만큼, 무엇보다도 사생활에 관한 비밀과 자유의 침해 내지 제한의 문제가 두드러진다. 알고리즘이 산출하는 결과의 정확성을 담보하기 위해서는 최대한의 데이터를 입력하여 학습과 추론이 이루어지도록 해야 하는데, 이로써 사생활의 비밀과 자유의

197) 장선미(2023), 앞의 논문, 25-26쪽.

침해 위험성이 높아진다. 이러한 위험성을 줄이기 위해서는 활용하는 정보의 종류를 한정시키거나 일정한 조건 아래에서 분석이 가능하도록 해야 하는데, 이러한 제한은 알고리즘의 산출 결과의 정확성을 보장하지 않는다. 물론 이러한 위험성이 비단 인공지능 기술에 대해서만 제기되는 문제라고 할 수는 없다. 그러나 과거의 정보통신기술과는 다르게 인공지능은 대규모의 데이터세트를 학습하여 스스로 최적의 알고리즘을 구축하고 폭넓은 추론, 분석, 예측 등을 수행한다. 또한 쉽고 빠르게 필터링과 프로파일링을 하여 정보를 선택적으로 획득하고 배포하는 능력이 탁월하다. 따라서 개인의 공적 영역뿐만 아니라 사적 생활영역에 대해 미칠 수 있는 영향력 역시 그 범위와 정도가 크게 증폭된다.

아울러 인공지능의 활용에서 발생하는 일반적 위험이 발생하는 것은 물론이고, 인간의 고유성과 관련된 문제도 발생할 수 있다. 법적으로는 인간의 존엄성 내지 자율성에 대한 경시의 가능성이다. 감시 그 자체가 목적이 아니더라도 인공지능을 활용함으로써 감시 효과가 발생하면서 파생되는 표현의 자유 등 기타 기본권의 침해 문제가 발생할 수도 있다. 무엇보다도 법치주의와 민주주의 원리의 훼손 가능성이 크다. 이는 바로 인공지능 감시에 의한 권력의 확대와 관련된 문제이다. M. Foucault가 지적하고 있듯이 근대 이후의 사회는 실제 감시라는 행위가 없더라도 다각적인 감시로 인하여 권력적인 관계가 작동하고 있다. 인공지능 기술이 여기에 개입되면 그 효과는 더욱 극대화될 수밖에 없다.

제 3 장 인공지능 감시에 대한 규제 동향

제 1 절 인공지능에 대한 규제 방식 검토

1. 의의

인공지능 기술을 활용한 감시에 대한 규제 동향을 살펴보기에 앞서 인공지능 자체에 대한 규제가 어떠한 방식으로 이루어지고 있는지부터 살펴볼 필요가 있다. 왜냐하면 인공지능에 대한 규제는 매우 다각적인 차원에서 이루어지고 있기 때문이다. 인공지능 기술의 개발과 활용에 대한 포괄적인 규제가 결국 인공지능 기술을 적용한 감시 행위의 규제로 작용하게 되고, 인공지능 감시만을 대상으로 하는 특정한 규제도 존재하기 때문이다. 또한 일정한 행정목적을 달성하기 위한 수단으로써의 규제가 단순히 법제도의 틀 안에서만 이루어지는 것이 아니고, 규제의 방식도 시시각각 변화하고 다양한 유형을 보이고 있다. 이에 먼저 인공지능에 대한 규제 방식과 양상을 폭넓게 검토한 이후, 인공지능 감시에 대한 각국의 규제 동향을 지능형 CCTV와 관련하여 인공지능 규제 방식의 시각에서 살펴보고자 한다.

2. 자율규제에서 법적 규제로

그동안 인공지능의 위험에 대한 관리 차원에서의 규제가 주로 자율규제의 방식으로 진행되어 왔다. 인공지능 분야에서는 인공지능의 개발과 활용에 적용할 수 있는 준칙 등 연성규범을 도입하여 인공지능 윤리를 확보하는 방식이 크게 활용된다. 꽤 수년 전부터 각국이나 국제기구에서는 인공지능 윤리를 확보하기 위한 준칙과 이를 실천하기 위한 가이드라인을 발표하고 있고, 인공지능 기술을 개발하고 활용하는 기업도 내부에서 자체적으로 활용하기 위한 준칙 등을 발표하고 있

다.[198] 인공지능 기술이 현재 성장하고 있는 신기술이라는 점에서 법적 규제를 선제적으로 도입하는 것을 최대한 늦추어 기술의 잠재적인 가능성을 훼손하지 않으면서도, 인공지능 관련 사업자가 기술의 위험을 최대한 관리할 수 있는 여지를 마련하는 것이 바로 이러한 자율규제의 장점이라고 하겠다.

또한 인공지능 윤리 확보의 목적에서 연성규범을 활용하는 방식의 자율규제는 규범적 차원에서 법적 규제보다 적응적 관점, 수용적 관점, 관할적 관점에서 유리한 점이 있다.[199] 먼저, 적응적 관점에서 인공지능 기술이 고도의 전문적 영역으로서 빠르게 발전하고 있어 경성규범으로 규제하는 것보다 연성규범을 활용하는 것이 유연한 대처가 가능하다. 둘째, 수용적 관점에서 연성규범이 경성규범보다 규제의 대상이 되는 상대방의 자유를 과도하게 제한하지 않아 협상의 여지가 많고 규제 도입에 대한 저항이 줄어들게 된다. 셋째, 관할적 관점에서 연성규범은 경성규범보다 공공이나 민간, 지역과 국경을 넘나들면서 적용될 수 있어 인공지능과 같은 전 세계적 관심사에 대한 효과적인 규제 방법이 될 수 있다는 장점도 있다.

국내에서는 2020년 12월 정부가 '사람이 중심이 되는 「인공지능(AI) 윤리기준」'을 발표하였고,[200] 유럽연합에서는 2019년 4월 유럽 집행위원회(European Commission)가 「신뢰할 수 있는 인공지능 윤리 가이드라인(Ethics Guidelines for Trustworthy AI)」을 발표한 바 있다.[201] 미국은 백악관 과학기술정책실이 2022년 10월 「인공지능 권리장전을 위한 청사진(Blueprint for an AI Bill of Right)」을 발표하였다.[202] 그런데 우리나라는 제20대 국회에서부터 현재 제22대

198) 관련된 자세한 사항에 대하여는 문광진(2024), 앞의 논문, 95쪽 이하 참조.

199) Bensamoun, A., Loiseau, G.(Sous la direction de)(2019), *Droit de l'intelligence artificielle*, LGDJ, pp. 28-29.

200) 과학기술정보통신부 보도자료(2020. 12. 22.), "과기정통부, 사람이 중심이 되는 「인공지능(AI) 윤리기준」 마련".

201) European Commission(2019. 4. 8.), "Ethics guidelines for trustworthy AI", https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (2024. 10. 3. 최종 방문).

202) Office of Science and Technology Policy(2022). Blueprint for an AI Bill of Right: Making Automated Systems Works for the American People, The

국회에 이르기까지 인공지능에 관한 기본법을 제정하기 위한 노력이 계속되고 있고, 유럽연합에서는 최근 들어 「인공지능에 관한 명령」이 제정되기도 하였다. 미국은 행정명령을 통하여 인공지능에 대한 연방 차원의 강력한 규제를 도입하기도 하였다. 이와 같이 각국은 인공지능에 대한 규제와 관련하여, 초기에는 인공지능 윤리를 확보하기 위한 자율규제를 시작하였으나, 최근에 와서는 법적 규제를 본격적으로 도입하였거나 도입하려고 준비하는 상황이다.

다만, 우리나라에서는 현재까지 인공지능에 적용되는 일반법률이 마련되어 있지 않은 상황이고, 따라서 인공지능 윤리를 확보하여 인공지능의 안전성과 신뢰성을 갖추겠다고 하는 자율규제의 목표가 여전히 유효하다고 하겠다.[203] 또한 법적 규제가 본격적으로 시작되더라도 인공지능의 위험도에 따라 사업자에 대해 차등화된 수준의 의무가 부과될 것이고, 그렇다면 많은 영역에서는 여전히 자율규제가 유의미하게 적용될 것이기 때문이다.

3. 법적 규제 방식의 유형

가. 의의

인공지능에 대한 법적 규제의 방식은 일률적이지 않다. 인공지능이 기반기술이자 범용기술에 해당하다 보니 인공지능의 위험을 관리하기 위해서 적용되는 규제 방식도 다양한 유형을 띨 수밖에 없다. 이러한 법적 규제 유형을 법률 적용 방식의 차원에서 나누어 보면, 첫째로는 직접적 규제 방식, 둘째로는 간접적 규제 방식, 셋째로는 개별적 규제 방식으로 분류될 수 있다.[204] 먼저, 직접적 규제 방식이란 인공지능에 관한 일반법률이 제정되고, 이러한 일반법률이 인공지능 기술 전반을 직접적으로 규율 내지 규제하는 것을 말한다. 둘째, 간접적 규제 방식이란 인공지능을 직접 규율하는 것이 아니라 다른 분야를 전반적으로 규율하는 법률이

White House, https://www.whitehouse.gov/ostp/ai-bill-of-rights (2024. 10. 3. 최종 방문).

203) 문광진(2024), 앞의 논문, 101쪽.

204) 문광진(2024), 위의 논문, 101쪽.

인공지능 기술의 개발과 활용에 대해서 규제의 효과를 가져오는 경우를 의미한다. 셋째, 개별적 규제 방식이란 개별 영역을 규율하기 위한 각각의 법률이 해당 영역에서 인공지능 활용을 규제하게 되는 것을 말한다. 아래에서는 각각의 유형에 대해서 국내와 유럽연합 및 미국의 입법을 중심으로 검토하고 한다.

나. 직접적 규제 방식

국내에서는 몇 년 전부터 인공지능에 관한 기본법 제정 논의가 진행되고 있다. 의원발의로 다수의 법률제정안이 계속해서 제출되고 있는데, 제20대 국회에서는 「인공지능 기술개발 및 산업 진흥에 관한 법률안(이상민의원 등 11인)」 등이 제출되었으나, 2020년 5월 임기종료로 모두 폐기되었다. 제21대 국회에서는 더욱 많은 법률제정안이 발의되었는데, 이들 법안은 주로 인공지능 기술의 발전과 산업의 진흥에 관한 내용을 다수로 하고 규제적 요소를 일부 포함하고 있었다. 2023년 2월 14일 국회 과학기술정보방송통신위원회 정보통신방송법안심사소위원회는 당시에 제출된 7건의 법률안[205]을 통합·조정하여 「인공지능산업 육성 및 신뢰 기반 조성 등에 관한 법률안」을 위원회 대안으로 통과시켰다.[206] 이 위원회 대안 역시 다수 규정이 인공지능 기술의 성장을 촉진하고 관련 산업의 진흥을 위한 정책을 추진하는 근거에 관한 내용이었지만, 일부 규정은 인공지능의 윤리·신뢰성 확보를 위해 개발과 활용에서의 자율규제를 촉진하는 내용과 고위험영역 인공지능 사업자에 대한 의무 부과와 관련된 내용을 두었다. 다만, 2024년 5월 29일 제21대 국회가 임기종료되면서 해당 법률안은 자동 폐기되었다. 제22대 국회가 출발하고

205) 해당 7건의 법안은 「인공지능 연구개발 및 산업 진흥, 윤리적 책임 등에 관한 법률안(이상민의원 등 11인)」, 「인공지능산업 육성에 관한 법률안(양향자의원 등 23인)」, 「인공지능 기술 기본법안(민형배의원 등 10인)」, 「인공지능교육진흥법안(안민석의원 등 10인)」, 「인공지능 육성 및 신뢰 기반 조성 등에 관한 법률안(정필모의원 등 23인)」, 「인공지능에 관한 법률안(이용빈의원 등 31인)」, 「알고리즘 및 인공지능에 관한 법률안(윤영찬의원 등 12인)」, 「인공지능산업 육성 및 신뢰 확보에 관한 법률안(윤두현의원 등 12인)」이다.

206) 이 위원회 대안이 법안심사소위에서 통과된 이후에도 「인공지능책임법안(황희의원 등 14인)」과 「인공지능 책임 및 규제법안(안철수의원 등 10인)」이 발의되었다.

는 이와 유사한 법률이 다수 발의되고 있다. 개원 5개월이 채 되지 않아서 이미 10건의 법률제정안이 발의되었는데, 이는 ①「인공지능 산업 육성 및 신뢰 확보에 관한 법률안(안철수의원 등 12인)」, ②「인공지능 발전과 신뢰 기반 조성 등에 관한 법률안(정점식의원 등 108인)」, ③「인공지능산업 육성 및 신뢰 확보에 관한 법률안(조인철의원 등 19인)」, ④「인공지능산업 육성 및 신뢰 확보에 관한 법률안(김성원의원 등 11인)」, ⑤「인공지능기술 기본법안(민형배의원 등 13인)」, ⑥「인공지능 개발 및 이용 등에 관한 법률안(권칠승의원 등 15인)」, ⑦「인공지능 기본법안(한민수의원 등 10인)」, ⑧「인공지능책임법안(황희의원 등 10인)」, ⑨「인공지능 발전 진흥과 사회적 책임에 관한 법률안(배준영의원 등 10인)」, ⑩「인공지능의 발전과 안전성 확보 등에 관한 법률안(이훈기의원 등 14인)」이다. 이 중에서 여당의 당론으로 채택되어 발의된「인공지능 발전과 신뢰 기반 조성 등에 관한 법률안(정점식의원 등 108인)」은 우선허용·사후규제 원칙을 삭제하고 생성 AI 표시 의무를 추가하는 등의 수정이 이루어졌고,「인공지능 개발 및 이용 등에 관한 법률안(권칠승의원 등 15인)」은 '금지된 인공지능'의 개념을 정의하고 이를 개발하거나 이용하는 자에 대하여 5년 이하의 징역 또는 5천만 원 이하의 벌금을 예정하고 있는 등 타 법안에 비하여 강력한 규제 수단을 도입하고 있다는 특징이 있다.

인공지능에 대한 직접적인 법적 규제에 가장 빠른 진척을 보인 곳은 바로 유럽연합이다. 유럽연합은 2024년 6월 13일「인공지능에 관한 명령(AI Act)」[207]을 제정하였고, 이 명령은 같은 해 8월 1일에 발효되었다. 물론 총 13장 113개 조항 모두가 동명령 발효 이후 각각 6개월부터 36개월까지의 경과기간을 가진다.[208] 입법 과정을 더 자세히 살펴보면, 먼저 유럽집행위원회가 2020년 2월 인공지능에 대한 정의를 내리고, 인공지능의 각종 이점과 기술의 발전 필요성을 강조하면서도

207) 정식 명칭은 "Regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts".

208) 심소연(2024), "규제중심의 유럽연합 인공지능법(EU AI Act)", 《최신 외국입법정보》, 제242호, 국회도서관, 2-3쪽.

잠재적 위험을 파악하고자 「인공지능 백서(White Paper on AI)」를 발표했다. 이 백서에서는 인공지능의 신뢰성과 안전성 확보 차원에서 다양한 정책과제를 제시하였는데, 여기에 인공지능의 위험 관리를 위해 인공지능의 위험도에 따른 법적 규제의 필요성을 밝혔다. 2021년 4월 유럽집행위원회가 이를 반영하여 인공지능 시스템에 의한 위험을 '수용불가의 위험(unacceptable risk)', '고위험(high risk)', '저위험(low risk)', '최소위험(minimal risk)'으로 구분하면서 각각의 위험 수준에 따른 규제 방식을 채택한 「인공지능에 관한 명령안」을 발의하였다. 2022년 말 챗지피티(ChatGPT)가 등장하면서 초거대·생성형 인공지능에 대한 규제 수요가 증가하자, 2023년 유럽의회가 '범용 인공지능 모델(general-purpose AI model)'에 대한 규제를 신설하는 등 수정하였다.[209] 2023년 12월 집행위원회, 의회, 이사회는 동명령안의 구체적인 내용에 대하여 최종 합의를 하였고, 2024년 3월 13일 유럽의회에서 찬성 523표, 반대 46표로 통과되었다.[210] 이어서 같은 해 5월 21일 27개 회원국 장관이 참여하는 유럽이사회에 의해 승인되었다.

미국에서는 2020년 '국가 인공지능 이니셔티브법(National AI Initiative Act of 2020)'이 제정되는 등 인공지능 관련 연방법률이 제정된 바는 있었으나, 인공지능에 대한 직접적 규제 법률이 마련된 적은 없다. 다만, 현재까지 통과되지 않았지만, 발의는 꾸준히 되고 있다. 대표적인 것이 '알고리즘 책임법안'인데, 우선 2019년 4월 상원의원 Ron Wyden과 Cory Booker, 하원의원 Yvette Clarke가 고위험의 자동화된 의사결정 시스템(high-risk automated decision system)에

---

209) 2021년 유럽집행위원회가 발의한 「인공지능에 관한 명령안」과 2023년 유럽의회 수정안의 자세한 비교에 관하여는 김중권(2024), "EU의회의 인공지능법안의 주요 내용에 관한 소고 - EU집행이사회의 인공지능법안과 비교해서 -", 《공법연구》 제52집 제3호, 한국공법학회, 260쪽 이하 참조.

210) *Le Figaro*(2024. 3. 13.), Les eurodéputés adoptent une loi encadrant l'intelligence artificielle, une législation unique au monde, https://www.lefigaro.fr/secteur/high-tech/les-eurodeputes-adoptent-une-loi-encadrant-l-intelligence-artificielle-une-legislation-unique-au-monde-20240313#:~:text=L'AI%20Act%20interdit%20certains,la%20lutte%20contre%20le%20terrorisme (2024. 10. 3. 최종 방문).

대한 영향평가의 실시를 주된 내용을 하는 '알고리즘 책임법(Algorithmic Accountability Act of 2019)안'을 상원(S.1108)과 하원(H.R.2231)에 각각 발의하였다. 2022년 3월에는 이들 의원들이 기존 법안을 대폭으로 수정·보완을 거쳐 같은 제목(Algorithmic Accountability Act of 2022)의 법안을 다시 각각 상원(S.3572)과 하원(H.R.6580)에 제출하였다. 제117대 연방의회의 회기가 종료되어 법안이 자동 폐기가 되자, 2023년 9월에는 같은 내용의 법안(Algorithmic Accountability Act of 2023)을 또다시 각각 상원(S.2892)과 하원(H.R.5628)에 제출한 바 있다.

한편, 최근에는 대통령 주도로 인공지능에 대한 규제적 성격의 행정명령(Executive Order)을 발표하였다. 이는 2023년 10월 바이든 대통령의 '안전하고 신뢰할 수 있는 인공지능의 개발 및 사용에 관한 행정명령(Executive Order(14110) on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence)'인데,[211] 연방정부의 주도로 범부처 차원의 인공지능의 개발과 활용에 대한 규제 지침을 담고 있다. 세부적으로는 ① 안전 및 보안, ② 혁신 및 경쟁, ③ 근로자 지원, ④ 형평 및 시민의 권리 보호, ⑤ 소비자 보호, ⑥ 개인정보 보호, ⑦ 연방기관의 인공지능 사용 지침, ⑧ 글로벌 리더십이라고 하는 8가지 핵심 원칙을 제시하고, 소관기관에 구체적인 조치를 하도록 지침을 담고 있다. 이 중에서 민간 기업 등에 대하여 향후 법적 규제로 연결될 수 있는 사항을 살펴보면, 첫째 '이중 용도 기반모델(dual-use foundation model)' 개발 기업이 국립표준기술연구소가 제공하는 기준에 따른 레드팀 테스트를 실시하고 해당 결과를 연방정부에 모델 훈련에 관한 정보와 함께 제공하도록 하였고, 둘째, 잠재적으로 악의적 사이버활동에 사용될 우려가 있는 인공지능 모델을 훈련하기 위해 미국 IaaS

211) *Federal Register*(2023. 11. 1), Executive Order 14110 of October 30, 2023: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence (2024. 10. 3. 최종 방문).

(Infrastructure as a Service) 업체와 거래하는 사업자는 상무부 장관에게 보고서를 제출하도록 하고, 셋째, 인공지능이 생성한 콘텐츠에 대한 워터마크 표시를 비롯한 위험 완화 지침 마련, 넷째, 형사사법, 교육, 의료, 복지, 채용, 주택 등의 분야에서의 인공지능 활용에 필요한 지침 개발 등이 있다.

다. 간접적 규제 방식

간접적 규제 방식에 의한 인공지능 규제는 인공지능을 직접적으로 규제하는 것은 아니지만 인공지능 기술의 개발이나 활용의 기반이 되거나 혹은 영향을 미치는 분야가 법적 규제의 대상이 됨으로써, 그 규제의 효과에 따라서 인공지능 기술의 개발과 활용 전반에 미치게 되는 것이다. 간접적 규제가 이루어지는 대표적인 분야가 개인정보의 보호와 관련된 영역이다. 오늘날 인공지능의 성능을 좌우하는 것은 무엇보다도 데이터의 양과 질이 중요한 요소로 작용한다. 양질의 학습데이터를 대량으로 확보하는 것이 고성능 인공지능 시스템을 개발하기 위한 전제 조건이 되는데, 많은 경우 인공지능 개발을 위해 활용되는 학습데이터에는 개인정보가 포함되어 있거나, 혹은 개인정보 그 자체를 학습데이터로 요구한다. 개인정보가 학습데이터로 활용되지 않는 인공지능도 있지만 주로 대량의 개인정보를 학습데이터로 활용하여 알고리즘 모델을 구축한 인공지능이 상업적으로 또는 공공적으로 높은 가치를 가지게 될 것이다.

인공지능을 개발하고자 이러한 학습데이터를 활용하기 위해서는 「개인정보 보호법」, 「신용정보법」, 「위치정보의 보호 및 이용 등에 관한 법률(이하 “위치정보법”이라 한다)」 등이 규정하는 개인정보, 신용정보, 위치정보 등의 수집과 활용을 위한 원칙, 즉 ‘동의’라고 하는 까다로운 요건을 충족하거나 그에 준하는 법적 근거가 있어야 한다. 이러한 간접적인 방식의 법적 규제는 정보주체의 권리 보호 차원에서 개인정보를 보호하기 위한 규제이지만, 간접적으로는 인공지능에 대한 규제로 작용하게 된다.

한편, 개인정보 보호뿐만이 아니라, 지식재산권 보호 관련 규제도 인공지능 기술 개발과 활용에서는 간접적 규제로 작용할 수 있다. 특히, 최근 생성형 인공지

능 개발 경쟁으로 저작권 침해 문제가 크게 이슈가 되고 있는데, 인공지능 모델 학습 과정에서 웹 크롤링 등을 하면서 타인의 저작물을 이용허락 없이 학습데이터로 활용하는 경우가 많아 논란이 발생하고 있다. 현행 「저작권법」이 저작자의 권리와 이에 인접하는 권리를 보호하고자 원칙적으로 타인의 저작물의 이용에 대한 규제를 두고 있어 인공지능의 개발에 대해서도 간접적으로는 규제로 작동하는 것이다.

또한 인공지능 기술도 기본적으로는 제품과 서비스에 융합 내지 결합되어 네트워크를 통해서 데이터를 주고받는 정보통신기술이라는 점에서, 관련 사업자에게는 안정적 네트워크 환경과 서비스 제공 유지의 의무가 부여된다. 대표적으로 「정보통신망법」 제45조가 규정하는 정보통신망의 안정성 확보와 제45조의2가 규정하는 정보보호 사전점검 등의 의무가 있다. 또한 학습데이터나 인공지능 시스템이 처리하는 데이터세트를 클라우드에 보관한다면 데이터 센터에 대한 규제가 적용될 수도 있다. 물론 이 경우는 해당 사업자에 대한 규제보다는 데이터 센터를 운영·관리하는 집적정보통신시설 사업자에 대한 규제[212]로 작용할 것이다. 그러나 결과적으로는 인공지능 개발과 활용에 대하여도 간접적으로는 영향을 미친다. 한편, 초거대·생성형 인공지능의 개발과 활용 과정에서 막대한 전력이 소비되는데,[213] 환경이나 에너지 관련 규제 역시 한편에서는 인공지능에 대해서 간접적인 규제가 될 수도 있을 것이다.

라. 개별적 규제 방식

개별적 규제 방식으로 인공지능을 규제한다는 것은 특정 영역에서 인공지능 기

212) 2022년 10월 판교 화재 사건 이후로 디지털 안전 3법(정보통신망법, 전기통신사업법, 방송통신발전기본법) 및 시행령 개정으로 관련 규제가 신설되었다.

213) *Le Figaro*(2024. 3. 22.), “On émet soixante fois plus de carbone en opérant une requête sur ChatGPT que sur Google”, https://www.lefigaro.fr/secteur/high-tech/on-emet-soixante-fois-plus-de-carbone-en-operant-une-requete-sur-chatgpt-que-sur-google-20240322 (2024. 10. 3. 최종 방문).

술의 활용을 제한적으로 규제함을 의미한다. 대표적인 사례를 살펴보면, 자율주행자동차의 영역에서, 「도로교통법」 제50조의2가 완전 자율주행시스템이 갖추어지지 않은 자율주행자동차에 대해서 운전자로 하여금 즉각적인 대응을 하도록 규정하거나, 「자동차관리법」 제27조가 시험·연구 목적으로 자율주행자동차를 임시운행하는 경우 국토교통부 장관으로부터 허가를 받도록 규정하고 있다는 점을 들 수 있다. 도로나 자동차와 관련된 개별 영역에서의 입법이 인공지능 기반의 자율주행자동차의 운행에 대한 법적 규제를 도입하고 있는 것이다.

개별적 규제 방식은 공적 영역에서 더욱 활발하게 이루어지고 있다. 먼저, 공직선거운동에서 딥페이크 활용은 「공직선거법」이 최근 엄격한 규제를 도입하였는데, 제22대 국회의원 선거를 앞두고 2023년 12월 28일 일부개정을 통해서 신설된 동법 제82조8은 제1항에서 선거일 전 90일부터 선거일까지 선거운동 목적으로 인공지능 생성 음향, 이미지, 영상 등을 제작·편집·유포·상영·게시하는 행위를 전면 금지하도록 규정하였다. 아울러 동조 제2항이 이 기간을 제외하고는 해당 음향, 이미지, 영상 등이 인공지능을 활용하여 생성되었다는 사실을 표시하는 조건 아래 허용하였다.

그리고 행정 분야에서는 2021년 제정된 「행정기본법」이 제20조를 통해 인공지능 기술을 활용한 처분의 법적 근거를 두고는 있지만, 이는 단순히 그 법적 근거를 마련한 것에 그치는 것이 아니라, 인간의 개입 없이 인공지능에 의한 처분에 대해서 법률유보의 원칙 적용 및 재량행위를 위한 활용의 금지라고 하는 규제적 요소를 도입한 것이다. 반면에 2022년 일부개정으로 신설된 「전자정부법」 제18조의2는 인공지능 등의 기술을 활용한 전자정부서비스 제공과 관련 지원에 관한 근거만을 규정하고 있다. 다만, 행정안전부고시로 마련된 「지능형 전자정부서비스 도입 및 관리지침」이 행정기관등의 장에게 의사결정과정에 사전고지 의무를 준수하고 서비스 이용 거부 및 이의제기, 설명요구 권리를 보장하기 위한 노력 의무, 인공지능 활용이 갖는 역기능 방지 및 사람 중심의 인공지능 구현의 노력 의무, 보안 대책 수립 의무를 부과하고 있다.

제 2 절 국외의 규제 동향

1. 미국

가. 개관

미국의 지능형 CCTV 관련 규제는 주로 개인정보 보호와 프라이버시 보호 그리고 공공의 안전 간의 균형을 맞추는 데 중점을 두고 있다. 미국 수정헌법 제4조는 "개인에 대한 불합리한 수색 및 압수로부터의 보호"를 규정하고 있는데,[214] 이런 원칙은 이른바 CCTV와 같은 감시기술에 대해서도 동일하게 적용되는 것으로 보고 있다.[215] 이에 연방법률으로서의 「전자정보통신 개인정보보호법(Electronic Communications Privacy Act of 1986: ECPA)」, 「저장통신법(Stored Communications Act: SCA)」 등에서 전자통신 기기를 이용한 비디오 녹화 등의 규정을 찾아볼 수 있지만, 이러한 법률들이 지능형 CCTV를 직접 규율·규제하기 위한 법률은 아니기 때문에 아직까지는 미국에서는 연방 차원의 지능형 CCTV 규제 법률은 존재하지 않는다고 할 수 있다.

반면 안면인식 기술과 같이 특정 인공지능 기술을 직접 활용하기 위한 법적 근거는 개별 주의 법률 혹은 도시의 조례에서 그 구체적인 내용을 확인할 수 있다.[216] 특히, 인공지능에 기반한 새로운 기술들이 복합적으로 등장하는 상황에서[217]

---

214) senate.gov, Constitution of the United States, https://www.senate.gov/about/origins-foundations/senate-and-constitution/constitution.htm (2024. 10. 3. 최종 방문).

215) Gary C. Robb(1980), "Police Use of CCTV Surveillance: Constitutional Implications and Proposed Regulations", *University of Michigan Journal of Law Reform*, Vol. 13, 1980, p. 575, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2144&context=mjlr (2024. 10. 3. 최종 방문).

216) Pimloc(2024), CCTV signage requirements in the US, https://www.securiredact.ai/articles/cctv-signage-requirements-in-the-us (2024. 10. 3. 최종 방문).

217) PELCO(2024), Top CCTV Camera Technology Trends for 2024, https://www.pelco.com/blog/cctv-and-video-security-camera-trends (2024.

관련 규제는 '프라이버시 보호'와 '기술의 발전'을 중심으로 점진적으로 확립되는 추세이다.

나. 지능형 CCTV에 대한 규제

1) 연방의 규제 법규

① 의의

현재까지 연방 차원에서 지능형 CCTV를 규제하는 법률은 존재하지 않는다. 하지만 인공지능이나 자동화된 의사 결정 시스템을 규제하기 위한 일반적인 내용의 법률과 법안 또한 지능형 CCTV와 같은 새로운 형태의 감시 시스템에도 영향을 미친다. 예를 들어, 연방상원의 「알고리즘 책임법안(Algorithmic Accountability Act of 2022: S.3572)」은 기업이 인공지능 기술을 사용할 때 책임성과 투명성을 보장하도록 요구하고 있는데, 이러한 원칙들이 인공지능을 이용한 지능형 CCTV에도 동일하게 적용될 수 있다. 이에 연방 차원의 지능형 CCTV 관련 규제를 담는 법률은 다음과 같은 것들이 있다.

② 미국 수정헌법 제4조(Fourth Amendment, 1791)

수정헌법 제4조는 불합리한 수색 및 압수로부터 시민의 보호받을 권리를 명시하고 있다. 다만, 이러한 보호는 전자기기 등을 활용하는 경우에도 확대되어 적용된다.[218] 지능형 CCTV와 관련하여, 사적 공간에서의 감시가 수정헌법 제4조에 저촉될 수 있는데, 특히 인공지능을 이용한 안면인식 기술이 포함된 CCTV의 사용에 대한 법적 논란은 개인정보 보호에 대한 우려와 맞물려 있다. 예를 들어 지능형 CCTV로 수집한 영상이나 데이터를 이용한 수색이 정당한지 여부를 판단하는 경우 법원은 수정헌법의 이 조항에 근거해 판단한다.[219]

---

10. 3. 최종 방문).

218) Pimloc(2024), op. cit.

219) Monica Gonzalez(2022), Challenges when dealing with video surveillance footage as evidence in court, https://www.security101.com/blog/challenges-when-dealing-with-video-surveillance-footage-as-evidence-in-court (2024. 10. 3. 최종 방문).

③ 「프라이버시법(Privacy Act, 1974)」

「프라이버시법」은 연방정부가 수집한 개인정보를 보호하기 위한 법률로, 이 법은 연방기관이 수집하는 개인 데이터의 사용과 공개를 제한하고, 개인의 동의 없이 수집된 정보가 사용되지 않도록 보장한다. 지능형 CCTV를 활용하여 수집된 데이터 또한 기본적으로 이 법의 규제를 받게 된다.[220]

④ 「비디오 프라이버시 보호법(Video Privacy Protection Act: VPPA, 1988)」

VPPA는 원래 비디오 대여 기록에 대한 프라이버시 보호를 위해 제정된 법률로 디지털화된 비디오 감시 기록을 포함하여 모든 형태의 비디오 데이터를 보호하는 것으로 확대 해석될 수 있다. 본래 이 법은 비디오 대여업의 감소에 따라 그 적용이 크게 줄었으나, 최근 비디오 서비스를 제공하는 모바일 애플리케이션, 웹사이트 기업을 대상으로 최근 개인정보 위반 소송이 증가하는 추세이다.[221] 지능형 CCTV로 수집된 비디오 데이터가 개인의 식별정보를 포함하는 경우, VPPA에 의해 해당 데이터가 보호받을 수 있다.[222]

⑤ 「안면인식과 바이오 기술 제한법안(Facial Recognition and Biometric Technology Moratorium Act, 2023)」

이 법안은 2023년 3월 연방상원에서 발의(S.681)되어 현재 계류 상태로,[223] 이

---

220) iapp, AI surveillance camera company allegedly violated US state laws(2024. 2. 28.), https://iapp.org/news/b/ai-surveillance-camera-company-allegedly-violates-us-state-laws (2024. 10. 3. 최종 방문).

221) Amy Gordon(2023. 10. 2.), The Return of the Video Privacy Protection Act(VPPA), https://www.mindingyourbusinesslitigation.com/2023/10/the-return-of-the-vppa/ (2024. 10. 3. 최종 방문).

222) Amy Gordon(2023. 10. 2.), op. cit.

223) ED MARKEY(2023. 3. 7.), MARKEY, MERKLEY, JAYAPAL LEAD COLLEAGUES ON LEGISLATION TO BAN GOVERNMENT USE OF FACIAL RECOGNITION AND OTHER BIOMETRIC TECHNOLOGY, https://www.markey.senate.gov/news/press-releases/markey-merkley-jaya

법안은 연방 차원에서 안면인식 기술을 비롯한 생체인식 기술의 사용을 일시적으로 금지한다. 지능형 CCTV 시스템이 안면인식 기능을 갖추고 있는 경우, 이 법안에 의해 연방 차원에서 사용을 중단할 수 있도록 하고 있다.[224] 법안의 주요 내용으로는 연방기관이 안면인식 기술을 사용하는 것을 금지하거나 제한하고, 해당 기술이 시민의 권리와 프라이버시를 침해할 수 있는 위험성에 대해 조사할 것을 요구한다.[225] 다만, 이 법안은 지난 2021년에도 연방하원에서 유사하게 발의(H.R.3907)되었으나,[226] 제117대 국회의 회기 만료로 자동 폐기된 바 있다. 하지만 미국 내에서도 지속적으로 안면인식 기술의 금지에 관한 법률이 발의되고 있다는 점은 연방 차원에서 인공지능을 포함한 감시 기술의 사용을 규제하고자 하는 적극적인 취지를 엿볼 수 있다.

2) 개별 주 및 도시의 규제 법규

① 의의

미국에서 보안 카메라에 대한 구체적인 법률을 가진 주는 15개 정도에 불과하지만, 일부 카운티와 도시는 조례 등의 법률을 제정해 개별적으로 활용에 대한 근거를 마련하고 있다. 개별 주에서의 보안카메라 관련 주요 규제 내용은 아래와 같다.

---

pal-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-and-other-biometric-technology (2024. 10. 3. 최종 방문).

224) CONGRESS.GOV, S.681 - Facial Recognition and Biometric Technology Moratorium Act of 2023, https://www.congress.gov/bill/118th-congress/senate-bill/681 (2024. 10. 3. 최종 방문).

225) CONGRESS.GOV, ibid.

226) CONGRESS.GOV, H.R.3907 - Facial Recognition and Biometric Technology Moratorium Act of 2021, https://www.congress.gov/bill/118th-congress/house-bill/3907/text (2024. 10. 3. 최종 방문)

〈표 3-1〉 15개 주의 보안카메라 규제 현황

해당 주	주요 규제 내용
조지아	카메라가 잘 보이는 곳에 설치되는 한 공공 및 사적 환경에서 비디오 감시 카메라를 사용하는 것이 허용
플로리다, 앨라배마, 미네소타	비공개 설정에서 숨겨진 비디오 감시를 허용
테네시, 미시간, 유타	공공장소에 보안 카메라를 설치하는 데는 허가가 필요하지 않지만, 사생활로 간주되는 장소에 카메라를 숨기는 경우에는 동의 필요
하와이	보안 카메라를 설치하려면 감시 대상자의 동의 필요
뉴햄프셔, 메인, 캔자스, 사우스다코타, 델라웨어	'합리적인 개인정보 보호 기대' 원칙을 적용하고 숨겨진 카메라 감시를 사용하려면 동의가 필요
캘리포니아	다른 주들보다 조금 더 구체적이지만, 캘리포니아주에서는 누구든지 기밀로 간주되는 통신 내용을 영상으로 녹화하는 것이 불법
아칸소	주법은 사적 공간에서 개인을 녹음할 때 동의 요구

자료: 연구진 정리

② 「캘리포니아주 소비자보호법(California Consumer Privacy Act: CCPA, 2018)」

CCPA는 캘리포니아주에서 시행되는 법률 중에서 개인정보 보호를 가장 강력하게 규정한 법률로 알려져 있으며, 미국에서의 개인정보에 관한 내용을 소개할 때 자주 제시된다. 특히 내용적 측면에서 유럽 「일반데이터보호명령(GDPR)」에서 정보주체의 프라이버시 보호 규정을 상당 부분 반영함으로써, 미국판 GDPR로 불리기도 한다.[227] 캘리포니아주에서 이 법의 제정 이후 유사한 취지의 법률이 버지니아, 네바다 등에서도 통과되었으며, 다른 주들 또한 이러한 흐름을 이어갈 예정이다.[228] 특히 CCTV 데이터를 포함한 개인정보의 수집, 사용, 판매에 대해 엄격한 규정을 적용한다.[229] 이에 따라 캘리포니아주 내에서 지능형 CCTV가 수집하는 영

227) NAVER, 미국 캘리포니아 소비자 프라이버시 보호법(CCPA) 준수 가이드, 3쪽, https://privacy.naver.com/download/NAVER_CCPA_Guideline.pdf (2024. 10. 3. 최종 방문).

228) Seena, The CCPA Explained, https://www.secureredact.ai/datapolicies/the-ccpa-explained (2024. 10. 3. 최종 방문).

상 데이터가 개인 식별 정보를 포함할 경우, 이는 CCPA의 규제대상이 된다. 이 법률에서는 개인정보, 소비자, 사업, 집합소비자정보, 생체정보, 수집, 비식별 등의 다양한 개념에 관하여 정의하고 있으며(§1798.140), 개인정보에 관한 알 권리, 접근권, 삭제권, 거부권, 서비스평등권리 등을 규정하고 있다.[230]

또한 CCPA에 이어 2023년 1월부터 시행된 「캘리포니아주 프라이버시 권리법(The California Privacy Rights Act of 2020: CPRA)」은 CCPA를 보완한 법률로, 더욱 강화된 소비자 권리보호와 기업의 의무 강화 등을 규정하고 있다.[231] 이 외에도 개인정보보호 원칙의 추가, 민감 데이터의 정의, 처리제한 등에 관한 훨씬 강화된 규정을 볼 수 있다.[232]

③ 「버지니아 소비자 데이터 보호법(Consumer Data Protection Act: VCDPA)」

버지니아주 역시 2023년 1월 소비자의 개인 데이터를 보호하는 법률을 제정했다. 다만 동법에서 명확히 지능형 CCTV가 수집하는 영상 데이터 등에 관하여 규정하고 있지는 않으나, 동법에서는 지문, 음성, 눈, 망막, 홍채 또는 특정 개인을 식별하는 데 사용되는 기타 고유한 생물학적 패턴이나 특성과 같은 개인의 생물학적 특성을 자동으로 측정하여 생성된 '생체인식데이터'에 대해 규정하고 있으며, 물리적 또는 디지털 사진, 비디오 또는 오디오 녹음 또는 그로부터 생성된 데이터라고 규정하고 있는바,[233] 지능형 CCTV를 통해 수집·가공되는 정보도 이 법의 적용대상이라 할 수 있다. 이 법률에 따라 기업은 수집한 데이터를 보호하고,

---

229) Seena, ibid.

230) 김성천(2018), "미국 캘리포니아주 소비자프라이버시법(CCPA)의 주요내용과 시사점", 《소비자정책동향》 제93호, 한국소비자원, 6쪽 이하.

231) Consumer Privacy Act, California Privacy Rights Act, 2020(CPRA), https://www.consumerprivacyact.com/california-privacy-act-2020-cpra/ (2024. 10. 3. 최종 방문).

232) 한국인터넷진흥원(2020), "미국 캘리포니아주 프라이버시 권리법 제정 배경 및 주요 내용", 415쪽 이하.

233) LIS, Chapter 53. Consumer Data Protection Act, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/ (2024. 10. 3. 최종 방문).

개인이 자신의 데이터를 제어할 수 있도록 데이터 관리자 책임, 투명성 등의 조치를 취해야 한다(§ 59.1-578).

④ 「생체정보 프라이버시법(Biometric Information Privacy Act: BIPA, 2008)」

BIPA는 일리노이주에서 제정된 생체정보 보호법으로, 생체정보를 수집, 저장, 처리하는 경우 사전 동의를 필수적으로 요구한다.[234] 지능형 CCTV가 안면인식과 같은 생체정보인식 기술을 사용하는 경우, BIPA의 엄격한 규제가 적용될 수 있기 때문에 생체정보를 수집하려면 개인의 명시적인 동의가 필요하고, 수집된 생체정보는 저장 기간이 제한되며, 특정 목적 외에는 사용을 금지한다. 또한 법 위반 시에는 벌금과 소송을 통한 보상 청구가 가능하다.

다만, 최근의 법 개정 동향을 살펴보면, 기업이 근로자와 소비자로부터 지문 및 기타 생체인식 데이터를 부적절하게 수집하고 사용할 경우, 받을 수 있는 처벌을 크게 완화하는 법안에 주지사가 서명하는 등 일부 규제 완화의 움직임도 있다.[235]

⑤ 샌프란시스코 「안면인식금지 조례」

2019년 샌프란시스코시는 미국 최초로 안면인식 기술을 금지하였다.[236] 이후 약 20개의 다른 도시가 이 조례를 따르게 되었다. 그 이유는 여전히 안면인식 기술은 유색인종 등에 대한 정확도가 떨어져 편향적인 기술로 분류할 수 있으며, 개인의 프라이버시를 충분하게 보호하기 위한 기술적 정확도가 신뢰할 수 없다는 점

---

234) ACLU Illinois, BIOMETRIC INFORMATION PRIVACY ACT (BIPA), https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa (2024. 10. 3. 최종 방문).

235) Reuters(2024. 8. 6.), “Illinois governor approves business-friendly overhaul of biometric privacy law”, https://www.reuters.com/legal/government/illinois-governor-approves-business-friendly-overhaul-biometric-privacy-law-2024-08-05/ (2024. 10. 3. 최종 방문).

236) CNN(2019. 5. 14.), “San Francisco just banned facial-recognition technology”, https://www.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html (2024. 10. 3. 최종 방문).

을 제시하였다.[237] 이에 따라 샌프란시스코에서는 조례에 따라 시의 기관은 자동 번호판 판독기 및 카메라가 장착된 드론과 같은 다른 종류의 감시 기술을 구매하기 전에 시의 승인을 받아야 한다.[238]

다. 안면인식 기술의 규제

지능형 CCTV는 다양한 인공지능 기술과의 접목이 가능한데, 그중에서도 많이 사용되는 기술 중에 하나가 안면인식 기술이다. 미국에서는 샌프란시스코의 사례와 같이 지방자치단체 단계에서 안면인식 기술에 대한 규제가 빠르게 증가하는 추세이다. 다만 경찰 등 사법기관에서 안면인식 기술의 사용은 각 주마다 상이한 특색을 지니고 있다. 예를 들어, 캘리포니아, 오리건, 매사추세츠 등 여러 주는 시민의 프라이버시 보호와 관련된 우려로 인해 경찰 및 공공기관에서 안면인식 기술 사용을 금지하거나 제한하고 있고,[239] 샌프란시스코, 오클랜드 등 도시에서 안면인식 기술을 포함한 지능형 감시 시스템의 공공 사용을 금지하는 지방조례를 통과시킨 사례는 앞서 살핀 바와 같다.[240]

그 이유는 우선 안면인식 기술 자체의 정확성 문제를 꼽을 수 있다. 인공지능

---

237) WIRED(2024. 3. 6.), “5 Years After San Francisco Banned Face Recognition, Voters Ask for More Surveillance”, https://www.wired.com/story/san-francisco-banned-face-recognition-voters-ask-for-more-surveillance/ (2024. 10. 3. 최종 방문).

238) Vox(2019. 3. 15.), “San Francisco’s facial recognition technology ban, explained”, https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained (2024. 10. 3. 최종 방문).

239) innovation&tech today, “13 Cities Where Police Are Banned From Using Facial Recognition Tech”, https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/ (2024. 10. 3. 최종 방문).

240) VICE(2019. 7. 17.), “Oakland Becomes Third U.S. City to Ban Facial Recognition”, https://www.vice.com/en/article/oakland-becomes-third-us-city-to-ban-facial-recognition-xz/ (2024. 10. 3. 최종 방문).

기반 안면인식 기술은 흑인을 오인식하여 불법으로 체포하는 사례가 발생하는 등 인종적, 성별 편향 문제가 지적되면서,[241] 이를 사용하는 지능형 CCTV의 신뢰성에 대한 논란과 문제 제기가 지속적으로 발생하고 있다. 이에 따라 여러 법안들에서는 해당 기술에 대한 정확성 검토 및 인증을 보다 엄밀히 요구하고 있다.[242]

라. 경찰 및 공공 감시 시스템

지능형 CCTV는 공공안전을 위해, 특히 경찰 및 정부기관에서 적극적인 활용을 모색하고 있다.[243] 경찰의 지능형 CCTV 사용 규제는 경찰이나 공공기관에서 지능형 CCTV를 사용하는 경우, 이를 어떻게 관리하고 사용하는지에 대한 투명성을 요구하는 법안들이 증가하고 있다.[244] 많은 주에서 경찰이 지능형 CCTV를 사용할 때 데이터 사용 정책을 공개하고, 공공이 이에 대해 의견을 제시할 수 있는 기회를 제공하도록 하고 있다.

또한 경찰이 지능형 CCTV 데이터를 수집한 후 보관하는 기간과 방법에 대한 규제도 강화되고 있으며, 불필요한 장기 보관이나 불법적인 데이터 공유를 방지하기 위한 장치가 마련되고 있고, 데이터의 보관 기간은 수집 목적에 맞게 제한해야

---

241) Scientific American(2023. 5. 18.), “Police Facial Recognition Technology Can’t Tell Black People Apart”, https://www.scientificamerican.com/article/police-facial-recognition-technology-cant-tell-black-people-apart/ (2024. 10. 3. 최종 방문).

242) *Guardian*(2019. 3. 30.), “San Francisco was right to ban facial recognition. Surveillance is a real danger”, https://www.theguardian.com/commentisfree/2019/may/30/san-francisco-ban-facial-recognition-surveillance (2024. 10. 3. 최종 방문).

243) *AMNESTY INTERNATIONAL*(2022. 2. 15.), “USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research”, https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/ (2024. 10. 3. 최종 방문).

244) Tate(2023. 7. 20.), “The movement to limit face recognition tech might finally get a win”, *MIT Technology Review*, https://www.technologyreview.com/2023/07/20/1076539/face-recognition-massachusetts-test-police/ (2024. 10. 3. 최종 방문).

하며, 영상 데이터 보관 및 사용을 제한해야 하는 등의 투명성을 위한 조치를 마련하도록 하고 있다.[245)]

마. 기업의 책임성 강화

지능형 CCTV를 상업적으로 사용하는 기업에 대한 규제도 증가하고 있다. 먼저, 데이터의 투명성에 관한 요구이다. 기업은 지능형 CCTV가 수집하는 데이터에 대해 투명성을 높이고, 데이터 수집 목적 및 활용 방법을 공개해야 한다. 또한 소비자가 자신의 데이터 사용 여부에 대해 알 권리를 보장하고, 필요시 이를 삭제할 수 있도록 해야 한다.[246)]

인공지능의 편향성 문제로 기업이 사용하는 인공지능 기반 CCTV 시스템이 특정 인종, 성별, 연령에 대해 편향된 결과를 도출하지 않도록 인공지능의 학습데이터 및 알고리즘을 평가하고 개선하기 위한 설명가능성 등을 요구하는 규제들이 늘어나고 있다.[247)]

바. 향후 지능형 CCTV 기술에 대한 규제

미국에서 지능형 CCTV와 같은 감시 기술에 대한 규제는 점점 더 강화될 것으

---

245) *BIOMETRIC*(2024. 3. 1.), "US AI Advisory wants more disclosure on facial recognition use by federal law enforcement", https://www.biometricupdate.com/202405/us-ai-advisory-wants-more-disclosure-on-facial-recognition-use-by-federal-law-enforcement(2024. 10. 3. 최종방문).

246) Hafiz(2022. 12. 21.), "Facial Recognition Technology and Privacy Concerns", ISACA, https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-51/facial-recognition-technology-and-privacy-concerns(2024. 10. 3. 최종 방문).

247) Rita(2024. 5. 28.), *4 - Transparency of Facial Recognition Technology and Trade Secrets, Cambridge Core*, CAMBRIDGE UNIVERSITY PRESS, https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/transparency-of-facial-recognition-technology-and-trade-secrets/580AE16FF598DC4735FFF0CD06E389F5(2024. 10. 3. 최종 방문).

로 예상되며, 미국 정부는 인공지능 기반 감시 기술의 발전을 지원하면서도, 시민의 권리를 보호하기 위한 정책을 강화하고 있다.[248] 대표적으로 2020년 연방하원에서 「미국 인공지능 이니셔티브법안」을 발표함으로써,[249] 인공지능 기술의 발전을 촉진하고, 지능형 CCTV와 같은 기술이 공공안전과 경제적 성과에 기여할 수 있도록 정책을 수립한 바 있다. 그러나 동시에 개인정보 보호를 위한 기술적, 법적 장치 마련도 강조하고 있으며 다른 여러 법률들을 통해 이러한 인공지능 기술의 활용과 개인정보보호는 지속적으로 추진되고 있다.

또한 국토안보부(DHS)는 공공안전을 위해 지능형 감시 시스템의 사용을 권장하면서도, 프라이버시 및 데이터 보호에 대한 가이드라인을 제공한다.[250] 이 가이드라인은 CCTV를 포함한 인공지능 기반 기술이 시민의 권리를 침해하지 않도록 관리 방안을 제시하고 있다.

앞으로 인공지능 기술이 더욱 발전함에 따라, 개인 프라이버시 침해 가능성에 대한 우려 역시 커지고 있어 향후 연방 차원에서도 포괄적인 프라이버시 보호 법안이 마련될 것으로 예상된다. 특히 지능형 CCTV와 관련해서는 앞서 살펴본 「안면인식기술 제한법」이 연방 차원에서 최종적으로 입법이 될 것인지 그 경과를 면밀히 살펴볼 필요가 있다.

---

248) 김경숙·홍건식(2023), “바이든 행정부의 첫 인공지능(AI) 행정명령과 시사점”, 《이슈브리프》 480호, 국가안보전략연구원, 3쪽 이하.

249) 다만 동법안은 제116대 의회의 회기 만료로 폐기된 이후 재상정되지는 않았다. CONGRESS.GOV, H.R.6216 - “National Artificial Intelligence Initiative Act of 2020”, https://www.congress.gov/bill/116th-congress/house-bill/6216 (2024. 10. 3. 최종 방문)

250) DHS, DHS CCTV Systems(2012. 7. 18.), https://www.dhs.gov/sites/default/files/2023-10/privacy-pia-dhs042-cctvappendixupdate-october2023.pdf (2024. 10. 3. 최종 방문).

2. 유럽연합

가. 개관

유럽연합의 지능형 CCTV 규제 동향은 기술 발전에 맞춰 개인정보 보호와 공공안전 사이의 균형을 맞추는 데 초점을 맞추고 있다. 다만, 현재 시점을 입법 동향의 기준으로 평가한다면 인공지능에 대한 규제에 초점이 맞추어진 것으로 보인다. 지능형 CCTV는 실시간 모니터링, 행동 분석, 안면인식 등 고급 기능을 통해 안전을 강화할 수 있지만, 개인정보 침해와 같은 문제를 야기할 우려가 있기 때문에 이에 대한 규제는 점차 강화되고 있다. 더욱이 2024년 「인공지능에 관한 명령(AI Act)」을 제정하여 안면인식 등 생체정보를 수집, 활용을 매우 제한적인 범위 내에서만 허용하는(제5조) 등 지능형 CCTV의 활용에 관하여는 매우 엄격하게 다루고 있다.

나. 인공지능에 관한 명령

1) 일반 내용

① 금지되는 인공지능 시스템

유럽연합의 「인공지능에 관한 명령」은 수용불가의 위험에 해당하는 인공지능 시스템의 유형을 ① 사람의 의식이나 결정 능력을 조작하거나 손상하여 피해를 주는 인공지능 시스템, ② 사람이나 특정 집단의 취약점을 이용하여 피해를 주는 인공지능 시스템, ③ 사회적 점수를 부여하여 개인이나 집단을 차별하는 인공지능 시스템, ④ 프로파일링이나 성격 특성 평가만으로 범죄 가능성을 예측하는 인공지능 시스템, ⑤ 인터넷이나 CCTV 영상에서 이미지 스크래핑하여 얼굴인식 데이터베이스를 생성 및 확장하는 인공지능 시스템, ⑥ 사업장이나 교육기관에서 개인의 감정을 추론하는 인공지능 시스템, ⑦ 생체정보를 통해 민감정보를 추론하여 개인을 분류하는 인공지능 시스템, ⑧ 공공장소에서 법 집행 목적인 실시간 원격 생체인식 인공지능 시스템(단, 납치, 인신매매, 성 착취 등 피해자 및 실종자 수색, 테러공격 위협 방지, 중대범죄 용의자 식별 등에는 활용 가능)으로 나열하고 있으며, 이러한 인공지능 시스템의 제공 또는 배포 자체를 원천적으로 금지하고 있다.

이를 위반하면 최대 3,500만 유로 또는 직전 회계연도 전 세계 매출액의 7% 중 더 높은 금액의 과징금이 부과될 수 있다.

② 고위험 인공지능 시스템

고위험 인공지능 시스템은 허용되지 않는 위험까지는 내포하고 있지 않지만, ① 원격 생체인식, ② 중요 인프라, ③ 교육 및 직업훈련, ④ 고용, 인사 및 자영업 접근, ⑤ 필수적 민간·공공서비스 접근, ⑥ 법 집행, ⑦ 이민 및 국경관리, ⑧ 사법행정 및 민주적 절차 영역에서 활용되는 인공지능 시스템을 의미하는데, 이러한 시스템의 제공자에게는 품질관리시스템 구축, 로그기록 보관, 적합성 평가 수행 및 표시, 관련 정보 제공 등의 의무가 부과되고, 배포자에게는 안전확보 조치, 모니터링 수행, 위험 대응, 사업장 근로자에 대한 사전 고지 등의 의무가 부과된다. 이를 위반하면 최대 1,500만 유로 또는 직전 회계연도 전 세계 매출액의 3% 중 더 높은 금액의 과징금이 부과될 수 있다.

③ 기타

저위험 인공지능 시스템은 인간과의 상호작용을 하지만 수용불가 위험이나 고위험 인공지능 시스템에 속하지 않는 시스템을 말하는데, 이때에는 투명성 확보 의무가 부과되며, 나머지 최소위험 인공지능 시스템에 대해서는 규제가 적용되지 않는다. 다만, 2023년도에 새롭게 추가된 것이 범용 인공지능 모델에 대한 규제인데, 해당 모델 제공자에게는 학습과 테스트에 관한 기술 문서 작성, 학습에 활용한 콘텐츠에 관한 정보 제공, 지식재산권법 준수 방침 마련, 해당 모델을 자신의 인공지능 시스템에 통합하려는 제공자에 대한 정보 제공 등의 의무가 부과된다.

2) 인공지능 감시 기술에 대한 규제

① 고위험 인공지능 시스템에 대한 관리

기본적으로 공공장소 등에서 안면인식 기술 등을 활용한 ‘실시간 원격 생체인식’ 기술은 엄격히 금지된다(제5조). 하지만 특별히 허용된 조건에서는 지능형 CCTV를 활용해 공공장소 등에서 실시간 원격 식별 시스템을 허용한다(동조 제1

항(h)). 이에 고위험 기술을 사용해 사람을 식별하거나 행동을 예측하는 경우, 이러한 시스템은 반드시 사용 전에 승인 절차를 거쳐야 한다. 아울러 특별히 허용된 조건이라 함은 실종자 혹은 범인의 수색 등을 말하며, 안면인식 기술을 활용하는 경우 개별 회원국에서의 사법적 또는 행정적 승인을 사전 혹은 사후에 받아야 한다.[251]

② 투명성 강화

제50조는 특정 인공지능 시스템 제공자 및 배포자의 투명성 의무를 규정하고 있다. 지능형 CCTV 운영자가 인공지능 기술을 사용하는 경우, 그에 대한 정보를 투명하게 제공할 것을 요구하며, 특정 프로그램의 경우는 개발단계에서부터 사용자가 인공지능 시스템과 상호 작용 중임을 알 수 있도록 고지할 의무를 부과하고 있다(제50조 제1항). 이에 CCTV 시스템의 설치 목적, 수집되는 데이터 종류, 데이터 처리 방법 또한 명확하게 공개해야 한다.

다. 「일반데이터보호명령」

1) 의의

2016년에 제정되고 2018년에 시행된 「일반데이터보호명령(General Data Protection Regulation: GDPR)」은 유럽의 「개인정보 보호법」으로 불리며, 개인정보에 관하여는 유럽연합 내에서 매우 중요한 법적 지위와 위상을 차지하고 있다. 특히, 디지털 플랫폼 기업에서 인공지능을 활용한 개인정보의 수집 및 활용의 빈도가 점차 높아짐에 따라 GDPR의 영향력도 지속적으로 확대되고 있다. 유럽연합은 GDPR을 통해 지능형 CCTV를 포함한 모든 감시 기술에 대한 규제를 강화하고 있다. GDPR이 도입된 이후 개인정보 보호의 중요성이 크게 부각되면서 지능형 CCTV 시스템이 수집하는 데이터에 대한 통제도 엄격해졌다. 이와 관련한 GDPR의 주요 내용은 다음과 같다.

---

251) 법제처 법제동향(2024. 5. 9.), “유럽의회, 「AI법」 가결”, https://world.moleg.go.kr/web/dta/lgslTrendReadPage.do?A=A&searchType=all&searchPageRowCnt=10&CTS_SEQ=52117&AST_SEQ=96&ETC=1(2024. 10. 3. 최종 방문).

2) 책임성 원칙의 강조

지능형 CCTV의 활용에서 중요한 점은 데이터 수집 및 처리는 목적 달성을 위한 최소한의 데이터로만 제한되어야 한다. 이 원칙에 따라 생체정보 등의 민감한 개인정보를 수집하는 지능형 CCTV는 지나치게 광범위한 데이터 수집을 피하고, 불필요한 감시나 개인정보의 수집을 방지해야 한다. 특히 정보주체는 처리의 적법성, 공정성, 투명성, 목적 제한, 개인정보 최소화, 정확성, 무결성 및 기밀성 등의 원칙을 엄격히 준수해야 한다.[252)]

3) 정보 주체의 권리 강화

정보 주체는 지능형 CCTV가 수집한 자신의 개인정보에 대해 열람권(제15조), 정정권(제16조), 삭제권(제17조) 등의 권리를 갖는다.[253)] 이는 개인정보 보호 규정을 철저히 준수할 수 있도록 하는 중요한 기제가 되어, 정보를 수집하는 기관과 기업에서는 개인정보 처리에 앞서 이 명령이 요구하는 기준에 따라 정보주체의 권리를 보호하기 위한 일련의 방법과 절차를 준수해야 한다.

4) 개인정보 처리를 위한 적법성 준수

수집된 데이터는 합법적이고 투명한 방법으로만 처리해야 하며, 특정 목적을 위해 수집한 정보는 그 목적 외의 용도로는 사용할 수 없다. 이러한 적법성을 확보하기 위해 중요한 것은 먼저 개인 동의, 계약의 이행, 법률의 준수 및 중대 이익의 보호 등이 있다.[254)] 단순한 감시를 넘어 개인을 식별할 수 있는 기술을 사용한다면 명시적 동의를 받아야 한다.

---

252) 이진규(2018), “EU GDPR 주요 내용의 검토”, 《KISO 저널》 제30호, 한국인터넷자율정책기구.

253) 네이버, EU GDPR이란, https://privacy.naver.com/global_support?menu=global_support_eu_gdpr_understand (2024. 10. 3. 최종 방문)

254) 이진규(2018), 앞의 글.

5) 데이터 보호 책임자 임명

기업이나 공공기관이 지능형 CCTV를 사용하는 경우, 데이터 보호 책임자(Data Protection Officer: DPO)를 임명하여 데이터를 안전하게 관리해야 한다(제37조). 공공기관이나 단체가 개인정보를 처리하는 경우나, 핵심 활동이 정보주체에 대한 대규모의 장기적이고 체계적인 모니터링을 요구하는 등 법정 지정 요건에 해당하면 DPO를 지정해야 한다.[255)]

6) 금전적 제재

GDPR의 개인정보 처리의 핵심 원칙을 준수하지 않는 경우 기업은 전 세계 연간 매출의 4% 또는 최대 2,000만 유로에 해당하는 과징금을 부과할 수 있다. 일반적인 위반에 해당하는 경우 1,000만 유로 또는 직전 회계연도 매출액의 2%를 금전적 제재로 부과할 수 있다.[256)]

7) 인공지능에 관한 명령의 도입과 영향

유럽연합은 지능형 CCTV에 포함된 인공지능 기술에 대해 인공지능에 관한 명령을 통해 보다 구체적으로 규제하고 있다. 특히, 인공지능에 관한 명령은 인공지능 시스템이 제공하는 위험 수준에 따라 서로 다른 규제를 적용하며, 얼굴인식 및 행동 예측과 같은 고위험 인공지능 기술은 특별히 엄격한 감독을 받는다.

라. 회원국에서의 규제

유럽연합의 개별 회원국은 공통의 GDPR 및 「인공지능에 관한 명령」의 원칙을 바탕으로 자체적인 지능형 CCTV 규제를 마련하고 있으며, 국가별로 감시 기술에 대한 규제는 다소 상이하다.[257)]

---

255) IGLOO(2019. 7. 31.), “국내 기업 및 조직에 대한 GDPR의 적용과 DPO의 이해”, https://www.igloo.co.kr/security-information/%EA%B5%AD%EB%82%B4-%EA%B8%B0%EC%97%85-%EB%B0%8F-%EC%A1%B0%EC%A7%81%EC%97%90-%EB%8C%80%ED%95%9C-gdpr%EC%9D%98-%EC%A0%81%EC%9A%A9%EA%B3%BC-dpo%EC%9D%98-%EC%9D%B4%ED%95%B4/ (2024. 10. 3. 최종 방문).

256) 이진규(2018), 앞의 글.

257) 특히, 인공지능에 관한 명령은 ‘Regulation’으로 제정되어, 법의 제정과 동시에 개

일부 국가들의 예를 살펴보면, 먼저 독일은 개인정보 보호에 매우 민감한 국가로 알려져 있으며, 공공장소에서의 지능형 CCTV 설치와 사용에 대한 규제가 특히 엄격하다.[258] 이에 CCTV 시스템이 설치되기 전에 지역 당국의 승인을 받아야 하며, 설치된 CCTV는 개인정보 보호 감독 기관의 정기적인 감사를 받는다. 특히 인공지능에 관한 명령의 제정 이후 안면인식 기술을 사용하는 CCTV에 대해서는 매우 높은 수준의 규제를 적용하고 있다.[259]

프랑스에서는 CCTV 설치 전 주민들에게 사전에 고지하고, CCTV 사용의 목적과 범위를 명확히 해야 한다.[260] 특히, 공공장소에서의 CCTV 사용은 공공의 안전을 위한 경우에만 허용되며, 위반 시 강력한 제재를 받는다.[261]

마. 향후 전망

유럽연합은 지능형 CCTV가 공공의 안전을 위해 필요할지라도 시민의 프라이버시와 기본권을 침해할 가능성이 있음을 인지하고 있으며, 특히 최근 몇 년 사이 「인공지능에 관한 명령」에 앞서 「디지털 서비스에 관한 명령(DSA: 2023년)」, 「

별 회원국에서도 별도의 입법이 없어도 법적 효력을 발휘하나, 안면인식 기술의 구체적인 활용 등에 대해서는 개별 회원국 자율로 운영된다.

258) Lexology(2020. 12. 22.), “Germany: Detailed guidance concerning data processing by CCTV”, https://www.lexology.com/library/detail.aspx?g=48ea93f6-3cb7-42e5-92c7-3d4d5bff4398 (2024. 10. 3. 최종 방문).

259) BIOMETRIC(2024. 3. 8.), “Police in Germany using live facial recognition”, https://www.biometricupdate.com/202405/police-in-germany-using-live-facial-recognition (2024. 10. 3. 최종 방문).

260) veesion(2024, 2. 20.), “Video surveillance: how to store data and what regulations apply to businesses in France?”, https://veesion.io/en/video-surveillance-how-to-store-data-and-what-regulations-apply-to-businesses-in-france/ (2024. 10. 3. 최종 방문).

261) The Connexion(2024. 3. 22.), “Home security cameras: what are the rules in France?”, https://www.connexionfrance.com/practical/home-security-cameras-what-are-the-rules-in-france/635684 (2024. 10. 3. 최종 방문).

디지털 시장에 관한 명령(DMA: 2024년)」 등의 디지털 사회에서 필요한 새로운 규제체계를 지속적으로 도입하고 있다. 이에 앞으로 「인공지능에 관한 명령」과 GDPR을 기반으로 한 규제는 더욱 정교해지고, 특히 인공지능 기반 예측 시스템에 대한 감독이 강화될 것으로 예상된다.

지능형 CCTV의 사용이 전 세계적으로 확대됨에 따라, 유럽연합은 국제 사회와 협력하여 개인정보 보호 및 감시 기술의 규제를 글로벌 차원에서 조정할 필요성을 인식하고 있다.[262] 또한 다소 규제적 성격이 강한 「인공지능에 관한 명령」의 제정 등은 미국 등과의 기술력 격차를 법규제 프레임을 통한 격차 해소의 목적으로 보는 시각도 있다.[263] 미국, 중국 등과의 규제 격차를 줄이기 위한 논의가 활발히 이루어질 것으로 예상된다.[264]

3. 영국

가. 개관

영국의 지능형 CCTV 규제는 유럽연합의 GDPR에 영향을 받은 「데이터 보호법(Data Protection Act 2018: DPA)」을 통해 독자적인 개인정보 보호 규제를 적용한다.[265] 특히, 정보보호위원회(Information Commissioner's Office: ICO)를 통해 지능형 CCTV 시스템의 사용에 대한 감독과 규제를 강화하고 있으며, 시민

---

262) Meltzer, J., Tielemans, A.(2022). “The European Union AI Act: Next steps and issues for building international cooperation in AI”, Global Economy and Development Policy Brief May 2022, Brookings Institution.

263) 윤정현·조은정(2024), “EU ‘인공지능 규제법(AI Act)’ 통과의 의미와 시사점”, 《이슈 브리프》 제527호, 국가안보전략연구원, 3쪽 이하.

264) Renew Europe(2023. 7. 12.), INTERNATIONAL COOPERATION IS KEY FOR THE DEVELOPMENT OF GENERATIVE AI, https://www.reneweuropegroup.eu/news/2023-07-12/international-cooperation-is-key-for-the-development-of-generative-ai (2024. 10. 3. 최종 방문).

265) CCTV information(2020. 1. 27.), THE DATA PROTECTION ACT AND CCTV, ”, https://www.cctv-information.co.uk/article/the-data-protection-act-and-cctv/ (2024. 10. 3. 최종 방문).

의 프라이버시 보호를 중요한 원칙으로 삼고 있다.

나. DPA와 GDPR의 조화

영국은 비록 유럽연합에서 탈퇴했지만, DPA는 유럽연합의 GDPR과 매우 유사한 내용을 포함하고 있으며, 지능형 CCTV와 같은 감시 시스템에도 이를 적용한다. DPA는 개인정보 보호와 관련된 주요 원칙을 유지하면서 브렉시트 이후 유럽 GDPR을 영국 현지화하여 데이터 보호에 관한 규제 체계를 구축하고 있다. 주요 내용을 간략히 살펴보면 먼저, 개인정보 처리 원칙으로 CCTV 시스템이 수집하는 모든 데이터는 합법적이고 투명하게 처리되어야 하며, 수집된 데이터는 명확한 목적에 맞게 사용되어야 한다. 또한 불필요한 데이터 수집과 처리 활동은 금지된다.[266]

그리고 명확한 동의를 요구하는데, 지능형 CCTV를 통해 개인정보를 수집하는 경우, 정보주체의 명확한 동의를 얻어야 한다. 예외적으로 공공안전과 같은 특수한 목적의 경우 별도의 동의 절차 없이도 CCTV 설치가 가능하나, 이러한 경우에도 데이터 최소화 원칙을 준수해야 한다.[267]

다. 감독기관(ICO)의 역할

ICO는 정보 보호와 관련된 법적 규정을 감독하는 독립 기관의 역할을 수행한다. 이 기관에서는 '사전 평가(Privacy Impact Assessment: PIA)'의 시행을 통해 시민의 프라이버시를 침해할 가능성을 평가한다.[268] 특히, 안면인식과 같은 민

---

266) University of BATH, Data Protection Act, https://www.bath.ac.uk/legal-information/data-protection-act/ (2024. 10. 3. 최종 방문).

267) Information Commissioner's Office(2022a), Video surveillance(including guidance for organisations using CCTV), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/ (2024. 10. 3. 최종 방문).

268) Information Commissioner's Office(2014), Conducting privacy impact assessments code of practice, p. 5, https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf (2024. 10. 3. 최종

감한 기술을 사용하는 지능형 CCTV는 PIA를 통해 개인정보 침해 가능성을 면밀히 분석하고,[269] 이를 줄이기 위한 조치를 사전에 취해야 하며 CCTV에 관하여는 별도의 가이드라인 통해 보다 엄격히 관리한다.[270] 또한 '책임자 지정'으로 지능형 CCTV를 운영하는 조직은 데이터 보호 책임자를 지정하여 ICO와의 의사소통을 책임지며,[271] CCTV 운영이 DPA와 GDPR을 준수하는지 확인해야 한다.[272]

또한 정기적인 감사 및 모니터링을 통해 ICO는 지능형 CCTV의 운영 실태를 정기적으로 감사하고, 법적 요구 사항을 준수하지 않는 운영자에게는 벌금과 같은 제재를 부과한다.[273] 이는 공공장소에서의 감시 활동에 대한 책임성을 높이기 위한 조치에 해당한다.

라. 안면인식 등 지능형 CCTV의 활용에 대한 규제

영국은 공공 및 민간 부문에서 사용하는 안면인식 기술을 포함한 지능형 CCTV

방문).

269) Information Commissioner's Office(2022b), What are our responsibilities in terms of accountability?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/what-are-our-responsibilities-in-terms-of-accountability/ (2024. 10. 3. 최종 방문).

270) Information Commissioner's Office(2014), op. cit., p. 21.

271) Information Commissioner's Office(2022c), Data protection officers, https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/accountability-and-governance/data-protection-officers/ (2024. 10. 3. 최종 방문).

272) Information Commissioner's Office(2022d), How can we comply with the data protection principles when using surveillance systems?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/how-can-we-comply-with-the-data-protection-principles-when-using-surveillance-systems/ (2024. 10. 3. 최종 방문).

273) Information Commissioner's Office(2022e), Penalties, https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/penalties/ (2024. 10. 3. 최종 방문).

시스템에 대해 특별한 규제를 적용한다. 영국 GDPR에 따라, 제6조에 따른 합법적 근거와 제9조의 조건을 충족하지 않는 한, 개인을 고유하게 식별하는 목적으로 생체 인식 데이터를 처리하는 것은 금지된다.[274] 특히 공공장소에서의 안면인식 기술을 활용한 지능형 CCTV 사용은 엄격하게 제한되며, ICO는 이러한 기술이 프라이버시를 심각하게 침해할 우려가 크기 때문에 얼굴 인식 CCTV는 범죄예방이나 공공안전을 위한 목적 외에는 사용이 불가하며, 그 목적이 명확하게 정의되어야 한다.[275]

또한 법적 근거 확보를 위해 안면인식 기술을 사용하는 CCTV 시스템은 법률에 따라 사용 목적을 명확히 해야 하며, 해당 목적이 공공의 이익에 부합하는지에 대한 법적 근거를 마련해야 한다. 무차별적인 감시는 법적으로 금지되며, 특정 범죄 용의자 식별과 같은 특수한 목적에 대해서만 제한적으로 허용된다.[276] 그리고 시민의 권리 보호를 위해 얼굴 인식 CCTV로 수집한 데이터에서는 시민의 권리 보호가 우선되어야 하며, 개인은 자신의 데이터가 어떻게 처리되고 있는지에 대해 접근할 권리가 있다. 시민들이 자신의 얼굴 인식 데이터 삭제를 요구할 경우(EU GDPR 제17조), 이를 즉시 처리해야 하며, 삭제되지 않을 경우 ICO에 문제를 제기할 수 있다.

---

274) Information Commissioner's Office(2022f), Additional considerations for technologies other than CCTV, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/?q=fine#frt (2024. 10. 3. 최종 방문).

275) Information Commissioner's Office(2023). Special category data, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/#scd4 (2024. 10. 3. 최종 방문).

276) Information Commissioner's Office(2022g), What does this guidance address?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/what-does-this-guidance-address/ (2024. 10. 3. 최종 방문).

마. 지능형 CCTV의 실시간 데이터 처리 규제

감시카메라를 통한 감시에 관하여는 DPA와 영국 GDPR 외에도 실무적으로 2013년 제정되고, 2021년 전면 개정된 「감시 카메라 행동 지침」에 따른다.[277]

'실시간 분석 및 행동 예측'을 통해 영국에서 지능형 CCTV가 실시간으로 데이터를 분석하거나 행동을 예측하는 기능을 제공하는 경우, ICO는 해당 기술이 데이터 보호 규정을 엄격히 준수하도록 감독한다. 특히 실시간 데이터를 분석하는 시스템이 특정 개인을 식별할 수 있는 경우, 그 데이터를 저장하거나 제3자와 공유하는 행위는 엄격히 금지된다.[278] 만약 경찰 등의 법집행기관에서 실시간 안면인식 기술을 활용하고자 하는 경우, 카메라의 배치 시기와 장소 결정의 기준을 명시하고, 합법적 경찰활동 목적으로만 활용해야 하며, 실시간 안면인식시스템을 통해 감시 목록에 있는 사람에 대한 경고를 생성하지 않는 모든 생체인식 데이터는 즉시 삭제되도록 보장해야 하는 등의 요건을 수행해야 한다(「감시카메라 운영지침 기준」 12 참조). 이를 위해 CCTV 시스템 운영자는 데이터 처리의 목적과 그 필요성을 명확히 제시해야 한다.[279]

바. 지능형 CCTV에 대한 법적 제재

ICO는 지능형 CCTV가 데이터 보호 법규를 위반할 경우 강력한 법적 제재를 가할 수 있다. 특히 개인정보를 부당하게 수집하거나 사용하는 경우, 해당 운영자는 막대한 벌금을 부과받을 수 있으며, 공공기관이나 사기업 모두 규제 대상에 포함된다. 금전적 제재로 ICO는 데이터 보호 위반 사항에 대해 최대 1,750만 파운드 또는 연매출의 4%에 해당하는 벌금을 부과할 수 있다.[280] 이러한 제재수단을

277) GOV.UK, Amended Surveillance Camera Code of Practice(accessible version), https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version (2024. 10. 3. 최종 방문).

278) Information Commissioner's Office(2022d), ibid.

279) Information Commissioner's Office(2022d), ibid.

280) Information Commissioner's Office(2022h), "Enforcement of this code",

마련함으로써 개인정보 보호 규정 준수를 더욱 강화하기 위한 조치가 가능하다. 또한 지능형 CCTV 운영자가 개인정보 보호에 대한 책임을 다하지 못할 경우, ICO는 법적 조치를 취하며 필요시 감시 시스템의 운영 중지를 명령하는 등의 법적 책임을 명확히 하고 있다.[281)]

사. 향후 규제 전망

영국은 지능형 CCTV와 관련된 규제를 지속적으로 강화하고 있으며, 특히 인공지능 기반의 감시 기술이 발전함에 따라 새로운 법적 프레임워크를 마련하고 있다. 인공지능과 데이터 보호에 대한 국제적인 협력이 중요한 이슈로 떠오르고 있으며, ICO는 이러한 변화를 반영하여 규제를 강화할 계획이다. 특히, '인공지능에 관한 명령과의 조율'을 위해 현재 영국은 유럽연합에서 탈퇴한 상태이지만, 유럽연합의 「인공지능에 관한 명령」과 유사한 규제 체계를 도입하여 인공지능 기반 감시 기술에 대한 규제를 강화할 것으로 예상된다.[282)] 그리고 '윤리적 감시 기술의 사용'을 위해 영국 정부는 인공지능 기반 감시 기술의 윤리적 사용을 강조하며, 감시 시스템이 공정하고 비차별적으로 사용될 수 있도록 새로운 법적 규제를 도입할 가능성이 크다.

4. 중국

가. 개관

중국은 세계에서 가장 발전된 지능형 CCTV 인프라를 구축하고 있으며, 이를 통해 광범위한 사회적 감시와 공공안전 강화를 목표로 하고 있다. 중국의 CCTV

---

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/enforcement-of-this-code/ (2024. 10. 3. 최종 방문).

281) Information Commissioner's Office(2022h), ibid.

282) European Parliament(2024), The United Kingdom and artificial intelligence, https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762285/EPRS_ATA(2024)762285_EN.pdf (2024. 10. 3. 최종 방문).

시스템은 주로 인공지능, 빅데이터, 얼굴인식 기술 등을 활용해 효율적인 감시와 데이터 분석이 가능하다. 앞에서 언급하였듯이, '톈왕(天網)'이나 '쉐량공정(雪亮工程)'과 같은 프로젝트를 통해 전국적으로 약 4억 대의 CCTV 카메라를 설치하고, 이를 통해 도시와 농촌 구역을 포괄적으로 감시하고 있다.[283] 이러한 프로젝트는 국가의 치안 및 공공안전을 강화하는 데 중점을 두고 있으며, 전국적인 감시 네트워크 구축을 목표로 하고 있다.[284] 중국에서 지능형 CCTV는 인공지능 기술을 적용해 사람의 행동을 분석하고, 범죄 예측과 교통 관리, 범죄 예방 등 다양한 목적으로 사용되며,[285] 인공지능 기반 CCTV 시스템은 실시간으로 영상을 분석하고, 이상 행동을 탐지하며, 특정 인물이나 차량을 추적할 수 있다.[286]

다만, 중국의 지능형 CCTV 규제는 서구 국가들, 특히 유럽연합과는 매우 다른 접근 방식을 취하고 있으며, 개인의 프라이버시보다는 국가 안전 및 사회 통제를 중시하는 정책을 바탕으로 운영되고 있다. 하지만 최근 「공공장소 영상정보 시스템 관리에 관한 규정」 초안이 공개되는 등 점차 법적 근거 등을 마련하기 위한 노력을 기울이고 있다.[287]

---

283) 채널A(2022. 7. 10.), "[세계를 보다]AI로 충성도 검사…中 디지털 감시 '첩첩'", https://www.ichannela.com/news/main/news_detailPage.do?publishId=0000000304856(2024. 10. 3. 최종 방문).

284) Medium(2021. 3. 3.), "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space", https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015 (2024. 10. 3. 최종 방문).

285) 매일경제(2019. 11. 1.), "[김대기 특파원의 차이나 프리즘] 최첨단 달리는 中 감시 시스템, 공안이 휴대폰으로 얼굴 찍자 '개인정보' 줄줄 … 무단 횡단하면 대형 스크린에 얼굴·신분 노출", https://www.mk.co.kr/news/world/9047851 (2024. 10. 3. 최종 방문).

286) Reuters(2021. 11. 30.), "EXCLUSIVE Chinese province targets journalists, foreign students with planned new surveillance system", https://www.reuters.com/technology/exclusive-chinese-province-targets-journalists-foreign-students-with-planned-new-2021-11-29/ (2024. 10. 3. 최종 방문).

287) China Law Translate(2024. 4. 9.), "Regulations on the Management of Video

나. 중국의 법적 프레임워크

1) 의의

중국은 지능형 CCTV와 관련된 구체적인 법률을 갖추고 있지 않지만, 광범위한 규제를 개인정보 보호보다는 공공안전 및 국가 안보에 중점을 두고 있다. 일반적으로 중국에서 데이터와 인공지능 등의 문제에 있어서 주요 법률로 꼽히는 것이 「네트워크 안전법」, 「데이터 안전법」, 「개인정보 보호법」 등의 법률이다.[288] 개별 법률의 주요 내용은 다음과 같다.

2) 「네트워크 안전법」 및 「데이터 안전법」

2017년에 제정된 「네트워크 안전법(中华人民共和国网络安全法)」은 정보와 데이터의 수집 및 보호를 위한 광범위한 지침을 제공하며, 특히 공공안전과 관련된 데이터 수집 및 처리에 있어 국가의 권한을 확대하고 있다. 지능형 CCTV가 수집하는 데이터는 주로 공공안전을 목적으로 처리되며, 이를 통해 국가기관은 범죄 예방과 사회 통제를 강화할 수 있다.[289]

또한 2021년에 제정된 「데이터 안전법(数据安全法)」은 중국 내에서의 데이터 처리 활동을 비롯하여 보안에 대한 관리, 감독에 관한 규정을 두고 있으며(제2조), 데이터와 보안의 개념, 데이터 처리 활동에 대한 권리와 의무(제8조, 제12조 등), 데이터 보안 제도(제24조) 등이 규정되어 있다.[290]

Imaging Information Systems in Public Spaces(Draft for Solicitation of Public Comments)", https://www.chinalawtranslate.com/en/cctv-regs/ (2024. 10. 3. 최종 방문).

288) 이상우(2023), "중국의 안면인식 기술 입법동향과 시사점 - 안면인식 기술응용 안전관리규정 의견수렴안을 중심으로 -", 《법학연구》 제26집 제4호, 인하대학교 법학연구원, 198쪽.

289) 보안뉴스(2017. 4. 14.), "中 2017년 6월 사이버보안법 전면 시행", https://m.boannews.com/html/detail.html?idx=65149(2024. 10. 3. 최종 방문).

290) 허욱·원중재(2021), "중국 데이터 보안법 제정과 시사점", 법무법인 세종, https://www.shinkim.com/kor/media/newsletter/1559 (2024. 10. 3. 최종 방문).

3)「국가 안전법」

2015년에 제정된 「국가 안전법(中华人民共和国国家安全法)」은 국가의 안보와 관련된 다양한 활동을 규제하고 국가 안전을 보호하기 위한 포괄적인 법적 근거를 제공하는 법률로 국가의 정치적, 경제적, 군사적, 문화적, 사회적 안보를 유지하기 위한 법적 프레임워크를 설정하고 있다. 동법 제51조 등을 통해 "국가는 정보의 수집, 분석 및 사용을 위한 통일되고 중앙 집중적이며 효율적인 시스템을 구축"하도록 하고 있으며, 제53조의 규정을 통해 "지능정보 작업을 수행하려면 현대 과학기술 수단을 충분히 활용하여 지능정보의 식별, 심사, 종합, 연구 및 분석을 강화해야 한다"고 규정하고 있다. 이를 통해 CCTV와 같은 감시 시스템도 국가 안보를 위해 정당화된다.[291)]

라)「개인정보 보호법」

2021년 제정된 중국의 「개인정보 보호법(个人信息保护法)」은 데이터 처리에 대한 규제를 마련했지만, 공공안전과 국가 안보가 우선하는 경우 CCTV를 통한 개인정보 수집과 분석이 허용된다. 이에 관하여는 제26조에서 공공장소에 이미지 수집 및 개인 식별을 위한 장치를 설치할 수 있으며, 수집된 개인영상 및 식별정보는 공공의 안전을 유지하기 위한 목적으로만 사용할 것을 규정하고 있다.[292)]

다. 안면인식 기술 규제

중국은 지능형 CCTV에 안면인식 기술 등의 인공지능 기술을 광범위하게 도입하고 있으며, 이를 통해 시민들의 신원을 실시간으로 식별하고 추적할 수 있는 시스템을 구축하였다. 이러한 기술은 특히 공공장소, 기차역, 공항, 학교 등에서 주로 사용되는데, 안면인식 기술은 국가 안보, 범죄 예방, 공공안전을 목적으로 합

---

291) 央视网(2015. 7. 2.), 「中华人民共和国国家安全法」, http://news.cntv.cn/2015/07/02/ARTI1435799475468828.shtml (2024. 10. 3. 최종 방문).

292) 中华人民共和国中央人民政府(2021. 8. 20.), 「中华人民共和国个人信息保护法」, https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm (2024. 10. 3. 최종 방문).

법적으로 사용되며, 개인정보 보호와 같은 우려보다 안전과 질서를 우선시한다.[293] 중국에서는 익히 알려진 바와 같이 안면인식 기술이 매우 보편화되어 있으며, 대부분의 공공장소에서 이를 통해 시민들을 실시간으로 감시하고 있다.

이에 안면인식 기술의 사용이 지나치게 확대되면서 프라이버시 침해와 인권 문제에 대한 국제적인 비판이 제기되고 있으나 중국 정부는 여전히 이러한 인공지능 기술이 사회 안정을 위한 필수적인 도구로 활용하고 있다.

제 3 절 국내의 규제 동향

1. 개설

앞서 국외에서의 인공지능 감시 기술에 대한 규제 동향을 살펴보았다. 인공지능 기술의 개발과 활용에 대한 법적 규제는 직접적 규제 방식, 간접적 규제 방식, 개별적 규제 방식이라는 세 가지 규제 유형에 따라 이루어질 수 있다. 물론 이러한 규제 방식은 각국에서 혼합되어 인공지능 감시 기술에 대하여 영향을 미치게 되지만, 국가별로 두드러지는 방식이 나타날 수도 있다. 미국의 경우에는 주로 연방보다는 주나 시 단위에서 규제 입법이 많이 진행되어 있기는 하나, 2023년 「안면인식과 바이오 기술 제한법안」이 제출된 만큼, 연방에서도 개별적 규제 방식이 나타나고 있다. 물론 주나 시의 경우에는 보안카메라나 안면인식 기술이라고 하는 개별 영역에서의 인공지능 규제, 즉 개별적 방식의 규제가 많이 부과되고 있다. 반면, 유럽연합은 기존의 GDPR이 유럽연합 내에서의 개인정보에 대한 강력한 보호 조치를 도입하고 있었기 때문에 자연스럽게 인공지능에 대해서도 간접적 규제가 적용되었지만, 최근에는 「인공지능에 관한 명령」이라고 하는 인공지능의 개발

293) QUARTZ(2024. 2. 21.), “China wants more control of its mass surveillance system”, https://qz.com/china-mass-surveillance-system-control-1851273607 (2024. 10. 3. 최종 방문).

과 활용의 전반을 관통하는 법제를 도입함으로써 인공지능에 대한 직접적 규제 방식을 채택하였다. 여기에는 인공지능 감시 기술이 원칙적으로 금지되는 경우도 있다.

우리나라의 경우 현재까지는 인공지능에 관한 기본법, 즉 인공지능 기술의 개발과 활용에 적용하기 위한 일반법률이 마련되지 않았다. 즉, 직접적 규제 방식은 지금까지 이루어지고 있지 않다. 그런데 「개인정보 보호법」을 비롯한 간접적 규제 방식을 통해서는 인공지능에 대한 법적 규제가 비교적 강하게 이루어지고 있을 뿐 아니라, 감시에 관련된 규제 내용도 찾아볼 수가 있다. 개별적 규제 방식의 경우에는 개별 영역에서 일정 정도 인공지능 감시가 제한될 수는 있겠으나 국가나 지방자치단체의 활동 등과 관련하여 인공지능 활용 그 자체에 대한 근거 규정을 두는 경우를 찾기는 어려운 상황이다.

아래에서는 이와 같은 인공지능 감시 기술에 대한 국내의 규제 동향에 대해서 인공지능에 대한 규제 유형을 중심으로 살펴보고자 한다.

2. 직접적 규제 방식을 통한 규제

가. 입법 추진의 주된 내용

앞서 언급하였듯이 제20대 국회에서부터 제22대 국회에 이르기까지 인공지능에 관한 기본법 제정 논의가 계속되고 있다. 의원 발의로 관련 법률제정안이 대략 20여 건 제출되었는데, 실제 상임위 법안심사소위의 문턱이라도 넘은 것은 비록 제21대 국회 임기종료로 폐기되기는 하였지만, 위원회 대안으로 마련된 「인공지능산업 육성 및 신뢰 기반 조성 등에 관한 법률안」이 유일하다. 그리고 제22대 국회에서 발의된 법률안들의 경우에도 위의 법률안과 큰 틀에서는 구성과 내용이 매우 유사한 것이 사실이다. 주지하였다시피 이러한 법률안들의 주된 목적은 인공지능 기술의 개발과 관련 산업을 활성화하기 위해서 정책적 지원 근거를 마련하는 것이다. 이에 대해서 부수적인 목적이라고 하기보다는 일종의 산업 진흥의 전제 조건이 되는 것이 바로 인공지능의 안전성과 윤리·신뢰성의 확보이

다.[294] 이를 위해 법안은 세 가지 방식을 채택하고 있는데, 첫째, 인공지능 안전성·윤리·신뢰성 확보 정책의 추진의 근거를 마련하는 것이고, 둘째, 인공지능 안전성·윤리·신뢰성 확보에 필요한 자율규제를 촉진하는 것이며, 셋째는 인공지능 기술의 개발과 활용을 직접 규제하기 위해 법적 의무를 부과하는 것이다.

나. 정책 추진 및 자율규제 촉진 내용

정책 추진과 관련하여서는, 「인공지능산업 육성 및 신뢰 기반 조성 등에 관한 법률안」 제23조에서 인공지능 윤리원칙을 제정·공표하는 정부의 권한을 규정하고, 제24조에서는 인공지능이 국민 생활에 미치는 잠재적 위험의 최소화와 안전한 인공지능의 이용을 위한 신뢰 기반 조성을 위한 시책 마련 의무를 규정하고 있다.

자율규제 촉진의 경우, 제25조가 '민간 자율의 인공지능 신뢰성 검·인증 활동'[295]을 지원하는 사업 추진의 근거와 이러한 검·인증을 받고자 하는 중소기업에 대한 행정적·재정적 지원의 근거를 두고 있다. 정부 차원에서의 검·인증 활동 지원 사업에는 인공지능 제품 또는 인공지능 기반 제품 또는 서비스의 개발에 관한 가이드라인 보급, 관련 연구 및 장비와 시스템 구축·운영 지원, 전문인력의 양성 지원 등이 포함된다. 그리고 제29조는 인공지능 윤리원칙을 준수하기 위한 목적에 인공지능 관련 기관, 사업자, 단체 등은 민간자율인공지능윤리위원회를 설치할 수 있고, 각종 관련 업무를 자율적으로 수행함을 규정하고 있다. 이러한 위원회의 구성·운영 등에 필요한 사항은 설치 기관 등이 자율적으로 정하지만, 그 구성이 하나의 성(性)으로만 할 수 없고, 사회적·윤리적 타당성 평가가 가능한 전문가와 외부인을 포함하도록 정하고 있다. 그리고 과학기술정보통신부 장관이 해당 위원

294) 문광진(2024), 앞의 논문, p. 137.

295) 과학기술정보통신부는 이미 민간 자율의 '인공지능신뢰성 인증' 제도를 지원하고 있다. 이 제도는 한국정보통신기술협회가 2023년부터 운영을 해오고 있는데, 인공지능 신뢰성 인증을 부여하기 위해서 인공지능 기술을 활용한 제품·서비스의 위험요인을 분석하고, 위험에 기반하여 신뢰성 확보를 위한 사업자의 요구사항 준수 여부를 평가하는데, 평가의 기준으로는 '인공지능신뢰성 단체표준'을 활용하고 있다. 자세한 사항에 관하여는 과학기술정보통신부 보도자료(2024. 2. 6.), "국내 1·2호 '민간자율 인공지능 신뢰성 인증' 부여".

회를 공정하고 중립적으로 구성하고 운영하도록 표준 지침 등을 마련하고 보급에 대한 권한을 규정하고 있다.

다. 사업자에 대한 규제 내용

동법안 제27조 제1항은 고위험영역 인공지능을 이용하여 제품 또는 서비스를 제공하려는 자에게 해당 제품 또는 서비스가 고위험영역 인공지능에 기반하여 운용된다는 사실을 이용자에게 사전에 고지하도록 하고, 제2항은 이러한 고지가 해당 제품 또는 서비스를 제공하는 자의 인터넷 홈페이지에 게시되거나 해당 제품 또는 서비스의 설명서에 포함시키는 등 이용자가 쉽게 알 수 있는 방법으로 제공하도록 규정하고 있다. 또한 제28조는 제1항에서 고위험영역 인공지능 개발자와 관련 제품·서비스 제공자에게 인공지능의 신뢰성·안전성 확보 조치를 사전적으로 하도록 의무로 부과하고 있다. 이어서 제2항은 과학기술정보통신부 장관이 관련 조치의 내용을 정하여 법안 제6조에 따른 인공지능위원회의 심의·의결을 거쳐 고시하고, 관련 사업자에게 해당 고시의 준수를 권고할 수 있도록 하였다. 제3항에서는 제2항의 고시가 ① 위험관리방안의 수립·운영에 관한 사항, ② 신뢰성 확보 조치 내용을 인할 수 있는 문서의 작성과 보관에 관한 사항, ③ 기술적으로 가능한 범위 내에서 인공지능이 도출한 최종결과, 인공지능의 최종결과 도출에 활용된 주요 기준, 인공지능의 개발·활용에 사용된 학습용 데이터의 개요 등에 대한 설명 방안, ④ 이용자 보호 방안, ⑤ 고위험영역 인공지능에 대한 사람의 관리·감독에 관한 사항, ⑥ 기타 고위험영역 인공지능의 신뢰성과 안전성 확보를 위해 필요한 사항을 포함하도록 하였다.

라. 검토

「인공지능산업 육성 및 신뢰 기반 조성 등에 관한 법률안」의 자율규제를 촉진하는 부분의 경우, 입법자는 법률을 제정하고 정부는 법률을 집행함으로써 자율규제의 구체적 틀을 형성하고, 이러한 틀 속에서 민간이 자율규제를 수행한다는 측면에 비추어 공동규제 또는 규제된 자율규제의 방식으로 볼 수 있을 것이다.[296] 정부와 민간이 협력적으로 규제 목적을 달성하도록 설계되어 있는 것이다. 또한 의

무의 부과와 관련된 부분의 경우에도, 관련 사업자 등에게 투명성 고지와 신뢰성·안전성 확보에 관한 의무를 부과하고 있지만, 이에 따르는 벌칙은 마련되어 있지 않다. 즉, 이러한 의무규정은 '훈시규정'에 불과한데, 후자의 사업자가 신뢰성·안전성 확보 의무를 위반에 대해서는 고시의 위반이 있더라도 규제 당국은 권고 수준의 권한을 행사할 수 있을 뿐인데, 문제는 이러한 의무를 부과하는 대상이 고위험영역 인공지능 관련 사업자라는 것이다.

'고위험영역 인공지능'은 법안 제2조 제3항에서 사람의 생명, 신체의 안전 및 기본권의 보호에 중대한 영향을 미칠 우려가 있는 영역에서 활용되는 인공지능으로서, ①「에너지법」 제2조제1호에 따른 에너지,「먹는물관리법」 제3조제1호에 따른 먹는물 등의 공급을 위하여 사용되는 인공지능, ②「보건의료기본법」 제3조제1호에 따른 보건의료의 제공 및 이용체계 등에 사용되는 인공지능, ③「의료기기법」 제2조제1항에 따른 의료기기에 사용되는 인공지능, ④「원자력시설 등의 방호 및 방사능 방재 대책법」 제2조제1항 제1호 및 제2호에 따른 핵물질과 원자력시설의 안전한 관리 및 운영을 위하여 사용되는 인공지능, ⑤ 범죄 수사나 체포 업무에 있어 생체정보(얼굴·지문·홍채 및 손바닥 정맥 등 개인을 식별할 수 있는 신체적·생리적·행동적 특징에 관한 개인정보를 말한다)를 분석·활용하는 데 사용되는 인공지능, ⑥ 채용, 대출 심사 등 개인의 권리·의무 관계에 중대한 영향을 미치는 판단 또는 평가 목적의 인공지능, ⑦「교통안전법」 제2조제1호부터 제3호까지에 따른 교통수단, 교통시설, 교통체계의 주요한 작동 및 운영에 사용되는 인공지능, ⑧ 국가, 지방자치단체,「공공기관의 운영에 관한 법률」에 따른 공공기관 등이 사용하는 인공지능으로서 국민에게 영향을 미치는 의사결정을 위하여 사용되는 인공지능, ⑨ 그 밖에 국민의 안전·건강 및 기본권 보호에 중대한 영향을 미치는 인공지능으로서 대통령령으로 정하는 인공지능으로 규정되어 있다. 즉, 고위험영역 인공지능은 중대한 위험성을 가지는 영역에서 활용되는 인공지능을 의미하는데, 그 구분은 항상 주관적일 수밖에 없다. 이에 법안 제26조는 관련 사업

296) 문광진(2024), 앞의 논문, 102쪽.

자가 과학기술정보통신부 장관에 대하여 해당 인공지능이 고위험영역 인공지능에 해당하는지의 여부를 확인 요청할 수 있도록 하고 있다. 이러한 규정이 규제 샌드박스 제도의 '신속확인'과 유사하지만, '훈시규정'에 불과한 사안을 이행하고자 이러한 절차를 속행할 사업자가 얼마나 있을지는 의문이다.[297]

또한 '고위험영역 인공지능'의 범주에 "범죄 수사나 체포 업무에 있어 생체정보를 분석·활용하는 데 사용되는 인공지능"이 포함된 것을 확인할 수 있다. 또한 국가, 지방자치단체, 공공기관 등이 사용하는 인공지능 중 국민에게 영향을 미치는 의사결정을 위하여 사용되는 인공지능도 여기에 포함된다. 공권력이 형사사법 절차에 활용하기 위한 인공지능은 물론이고, 공공의 영역에서 광범위하게 감시 목적으로 활용하는 인공지능이 이 법률안에 따르면 모두 고위험 인공지능에 포함될 것이다. 앞서 인공지능을 활용한 감시가 과거의 정보통신기술을 활용한 감시행위보다 국민의 기본권을 훨씬 더 침해할 가능성이 높다는 것을 확인하였고, 그로 인해 침해될 수 있는 국민의 기본권이 비단 개인정보자기결정권과 사생활의 비밀과 자유에 그치지 않는다는 것도 확인하였다. 기본권 침해를 넘어서서 우리 사회의 중요 가치인 민주주의 원리의 훼손까지도 우려된다는 것도 물론이다. 그럼에도 이러한 영역의 인공지능 기술의 개발이나 활용에서 관련 사업자나 배포자 등에게 단순히 인공지능 기반 운용 사실의 고지 의무 정도를 부과하고 또한 훈시규정 수준의 신뢰성·안전성 확보 의무만을 부과하는 것은 국민의 기본권 보호의 차원에서는 미흡한 수준의 규제로 보인다.

3. 간접적 규제 방식을 통한 규제

가. 의의

인공지능을 직접 규제하지는 않지만 인공지능 기술의 개발과 활용에 큰 영향을 미치는 규제 수단을 꼽자면 무엇보다도 개인정보에 대한 규제일 것이다. 앞서 확

297) 문광진(2024), 앞의 논문, 103쪽.

인하였듯이 인공지능 기술을 개발하거나 이미 개발한 인공지능 시스템을 구동하는 데 필요한 개인정보를 확보하기 위해서는 개인정보 관계 법령이 규정하고 있는 일정한 절차를 충족하여야 한다. 대표적인 것이 정보주체의 '동의'를 받는 절차이다. 그런데 오히려 공권력의 인공지능 개발과 활용에 있어서는 '동의'보다는 법률의 규정을 통해 개인정보를 수집 및 이용하는 경우도 많다. 물론 이러한 부분은 헌법상 기본권인 개인정보자기결정권의 범위 내에서는 입법재량에 해당하는 영역일 것이다.

한편, 「개인정보 보호법」은 인공지능에 관련된 특수한 규정을 두고 있고, 감시와 관련해서도 특별한 규정을 두고 있다. 아래에서 이에 대해서 살펴보기로 한다.

나. 자동화된 결정에 대한 정보주체의 권리

2023년 「개인정보 보호법」 일부개정을 통하여 자동화된 결정에 대한 정보주체의 권리를 규정한 동법 제37조의2[298]가 마련되었다. 이 규정은 사실 유럽연합의 GDPR 제22조의 영향을 받은 것인데, 제22조 제1항이 정보주체에 대하여 자동

298) 「개인정보 보호법」 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 "자동화된 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 제15조제1항제1호·제2호 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 재처리·설명 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 거부·설명 등을 요구하는 절차 및 방법, 거부·설명 등의 요구에 따른 필요한 조치, 자동화된 결정의 기준·절차 및 개인정보가 처리되는 방식의 공개 등에 필요한 사항은 대통령령으로 정한다.

화된 결정의 적용을 받지 않을 권리, 즉 거부권을 인정하고 있고, 제2항이 이러한 권리가 인정되지 않는 예외 사유로서 계약의 체결이나 이행에 필요한 경우, 유럽연합이나 회원국 법에 따라 허용되는 경우, 정보주체의 명시적 동의가 있는 경우를 규정하였다. 동조 제3항은 이러한 예외 사유에 해당하는 경우에 정보주체가 인적 개입을 요구하거나, 의견진술을 할 수 있거나, 이의제기를 할 수 있도록 규정하고 있다.

우리「개인정보 보호법」제37조의2 역시 정보주체의 개인정보에 대한 권리를 보호하는 차원에서 인공지능 기술이 적용된 시스템을 포함하는 개념인 자동화된 결정에 대해서 설명요구권, 의견제출 및 검토 요구권, 거부권 등을 규정하고 있다. 보다 자세히 살펴보면, 동조는 사람의 개입이 전혀 없이 자동화된 시스템이 개인정보를 처리하여 중대한 결정을 하면 해당 결정의 상대방인 정보주체가 거부권을 행사할 수 있고, 일반적인 인공지능 활용에 대해서는 설명요구권을 행사할 수 있도록 하고 있다. 또한 인공지능을 활용하는 개인정보처리자의 투명성 의무로서 자동화된 결정의 기준 및 절차, 처리되는 방식 등을 홈페이지 등에 미리 공개하도록 하는 사전 공개의 의무를 부과하고 있다. 언뜻 보기에는 인공지능에 대한 직접적 규제로 파악될 수도 있으나, 이는 정보주체의 개인정보자기결정권을 실질적으로 보호하기 위한 규정으로서, 삭제권, 거부권, 열람권 등 개인정보자기결정권을 구성하고 있는 세부 권리와 맞닿아 있다. 직접적 규제와 간접적 규제의 중간 지점을 형성하고 있는 부분이라고 할 수 있겠다. 다만, 인공지능을 활용한 감시가 점차 확대되어 가는 현실에서 이와 같이 개개인에게 권리를 부여하는 형태만으로 국민의 기본권 보호가 어느 정도 실효성 있게 달성될 것인지에 대해서는 의문이다.「개인정보 보호법」이 2011년 통합 제정된 이래로 공공의 영역과 민간의 영역에 공동으로 적용되는 법규범인데, 개인과 개인 간의 법률관계를 규율하기 위한 법기술 방식과 국가와 국민 간의 법률관계를 규율하기 위한 법기술 방식이 동일해야 하는 것인가에 대해서도 마찬가지로 의문이다.

다. 감시에 대한 규제 내용

「개인정보 보호법」은 제25조[299]에서 고정형 영상정보처리기기의 설치와 운영에

---

299) 「개인정보 보호법」 제25조(고정형 영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치·운영하여서는 아니 된다.
1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
4. 교통단속을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
5. 교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
6. 촬영된 영상정보를 저장하지 아니하는 경우로서 대통령령으로 정하는 경우

② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 고정형 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

③ 제1항 각 호에 따라 고정형 영상정보처리기기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 고정형 영상정보처리기기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

④ 제1항 각 호에 따라 고정형 영상정보처리기기를 설치·운영하는 자(이하 "고정형 영상정보처리기기운영자"라 한다)는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다. 다만, 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, 「통합방위법」 제2조제13호에 따른 국가중요시설, 그 밖에 대통령령으로 정하는 시설의 경우에는 그러하지 아니하다.
1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 연락처
4. 그 밖에 대통령령으로 정하는 사항

⑤ 고정형영상정보처리기기운영자는 고정형 영상정보처리기기의 설치 목적과 다른 목적으로 고정형 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

⑥ 고정형영상정보처리기기운영자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다.

관련된 규정을 두고 있고, 제25조의2[300]에서 이동형 영상정보처리기기의 운영에 관한 규정을 두고 있다. 이들 규정은 개인에 대한 감시를 규제하는 입법 규정이라고도 할 수 있는데, 영상정보처리기기의 설치와 운영에 대해서 적용되는 규제의 내용이 지능형 CCTV에 적용되는 인공지능 기술에 대해서도 간접적으로 영향을 미칠 수 있기 때문이다.

그런데 이 두 규정은 영상정보처리기기를 설치하거나 운영하는 데 적용하는 것으로서, 그 기본적인 목적은 해당 기기로부터 정보주체의 권리, 즉 개인정보자기결정권과 사생활의 비밀과 자유와 같은 프라이버시에 관한 권리를 침해할 수 있

---

⑦ 고정형영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 고정형 영상정보처리기기 운영·관리 방침을 마련하여야 한다. 다만, 제30조에 따른 개인정보처리방침을 정할 때 고정형 영상정보처리기기 운영·관리에 관한 사항을 포함시킨 경우에는 고정형 영상정보처리기기 운영·관리 방침을 마련하지 아니할 수 있다.

⑧ 고정형영상정보처리기기운영자는 고정형 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 고정형 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.

300) 「개인정보 보호법」 제25조의2(이동형 영상정보처리기기의 운영 제한) ① 업무를 목적으로 이동형 영상정보처리기기를 운영하려는 자는 다음 각 호의 경우를 제외하고는 공개된 장소에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상(개인정보에 해당하는 경우로 한정한다. 이하 같다)을 촬영하여서는 아니 된다.

1. 제15조제1항 각 호의 어느 하나에 해당하는 경우
2. 촬영 사실을 명확히 표시하여 정보주체가 촬영 사실을 알 수 있도록 하였음에도 불구하고 촬영 거부 의사를 밝히지 아니한 경우. 이 경우 정보주체의 권리를 부당하게 침해할 우려가 없고 합리적인 범위를 초과하지 아니하는 경우로 한정한다.
3. 그 밖에 제1호 및 제2호에 준하는 경우로서 대통령령으로 정하는 경우

② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실, 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있는 곳에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하여서는 아니 된다. 다만, 인명의 구조·구급 등을 위하여 필요한 경우로서 대통령령으로 정하는 경우에는 그러하지 아니하다.

③ 제1항 각 호에 해당하여 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우에는 불빛, 소리, 안내판 등 대통령령으로 정하는 바에 따라 촬영 사실을 표시하고 알려야 한다.

④ 제1항부터 제3항까지에서 규정한 사항 외에 이동형 영상정보처리기기의 운영에 관하여는 제25조제6항부터 제8항까지의 규정을 준용한다.

는 정보가 수집되고 전송되는 것을 방지하는 것이다. 따라서 이러한 기기가 설치나 운영될 수 있는 요건을 세밀하게 규정하는 것에 집중하고 있고, 또한 설치나 운영이 금지되는 장소를 정하거나, 설치나 운영이 되는 경우라고 하더라도 정보주체의 권리가 최소한으로 제한될 수 있도록 하는 규정을 두고 있다. 즉, 인공지능 기술의 적용에 관한 사항은 입법 당시에도 전혀 고려하고 있지 않고, 동법 시행령은 물론 고정형 영상정보처리기기와 이동형 영상정보처리기기에 관하여 상세하게 세부적인 규정을 두고 있는 개인정보보호위원회고시 형식의 「표준 개인정보 보호지침」 역시 인공지능 기술의 활용과 관련된 내용은 두고 있지 않다.

4. 간접적 규제 방식을 통한 규제

우리나라에서도 앞서 각종 사례를 통해서 살펴본 바와 같이, 감시와 관련된 인공지능 기술이 매우 폭넓게 활용되고 있음을 알 수 있다. 그런데 이러한 인공지능 기술을 활용한 감시행위가 허용이 되는지, 아니면 전면적으로 금지되거나 혹은 일정한 요건 아래 제한이 되는지 등에 관한 법률 규정이 마련되어 있지 않다.

복지 사각지대 발굴을 위해 인공지능 기술이 적극적으로 활용되고 있으나, 「사회보장급여법」 제23조는 수급권자의 선정 및 급여관리 등에 관한 업무를 효율적으로 수행할 수 있도록 사회보장정보시스템을 이용해서 자료 또는 정보를 처리할 수 있도록 규정하고 있고, 또한 동법 제12조가 사회보장급여 지원대상자 발굴을 위해 단전, 단수, 단가스, 신용정보 중 연체정보, 임대료 체납정보, 관리비 체납정보 등을 비롯한 수많은 정보를 처리할 수 있도록 근거를 두고 있다. 그럼에도 불구하고 인공지능 기술을 활용할 수 있는지에 대해서는 규정하고 있지는 않다.

지능형 CCTV는 현재 수많은 지방자치단체가 활용하고 있지만, 「개인정보 보호법」이 고정형 또는 이동식 영상정보처리기기의 설치와 운영에 관한 규정만 두고 있을 뿐, 지능형 선별관제 시스템과의 융합적 활용에 관한 근거를 두고 있지 않다.[301] 범죄 예방이나 공공안전의 확보 목적으로 지능형 CCTV를 운영하면서 인공

301) 미국의 경우 주나 시 단위에서 감시 목적의 안면인식 기술 사용을 규제하는 경우가

지능 기반의 선별관제 알고리즘을 적용하게 되면 단순히 정보주체의 개인정보가 수집되는 정도의 개인정보자기결정권이 제한되는 수준을 넘어서서, 인공지능의 평가가 바탕이 되는 프로파일링이 이루어져도 정보주체는 자신의 정보처리를 알 수 없는 등 기본권 침해의 범위가 더욱 증대될 수 있다.[302] 그럼에도 불구하고 인공지능의 활용과 관련해서는 우리나라 입법자는 항상 침묵으로 일관하고 있다.

이러한 문제는 안전과 관계되는 법률 규정에서 그 문제점이 더욱 드러난다. 인공지능 기반의 지능형 CCTV는 선별관제 시스템을 통해서 재난 상황에 대비하고 실종자를 수색하고 있다. 그러나 「재난 및 안전관리 기본법」 제74조의3이 고정형 영상정보처리기기를 통해 수집한 정보를 재난 예방·대비·대응 목적으로 활용하는 근거를 규정하고는 있으나, 선별관제라고 하는 인공지능 기술을 활용하기 위한 근거는 어디에도 마련되어 있지 않다. 「실종아동 등의 보호 및 지원에 관한 법률」도 제8조의2에서 실종아동 등에 대한 신속한 신고 및 발견 체계를 갖추기 위한 정보시스템을 구축 및 운영하도록 규정하고 있고, 제9조의2에서 경찰관서의 장이 고정형 영상정보처리기기를 통하여 수집된 정보의 제공을 요청할 수 있도록 규정하고 있다. 그럼에도 불구하고 선별관제 시스템에 적용되는 인공지능 기술의 활용에 관한 언급은 찾을 수 없다. 이러한 입법적 태도는 문제가 있다.

있는데, 예를 들어 워싱턴주는 2020년 3월 「안면인식 기술 규제에 관한 법률」을 제정하여 주와 주의 소속기관이 계속적 감시, 실시간 식별, 지속적 추적 등을 목적으로 하는 안면인식 시스템의 사용을 금지하였다(S. B. 6280(Wash-, 2020)).

302) 김민규(2023), 앞의 박사학위 논문, 52쪽.

제 4 장 인공지능 감시 문제에 대한 규범적 대응방안

제 1 절 대응 원칙

1. 규범적 대응의 필요성과 원칙

인공지능 기술은 빠르게 발전하고 있으며, 구성원들이 인지하지 못하는 사이에도 급속하게 확산하고 있다. 인공지능이 개인에 대해 많은 결정을 내리면서 인간에 의한 감시가 아니라 기계에 의한 감시까지 우려해야 할 상황이 되었다. 이러한 감시의 확대는 인공지능을 활용하는 주체와 그 대상자 사이에 정보의 불균형을 초래한다. 인공지능의 불투명성 때문에 더 심해지는 정보의 불균형은 그만큼 권력의 불균형도 극단화한다. 이는 감시와 권력의 불균형을 직접적으로 의도하는지와 관계없이 발생하는 현상으로서 비단 국가와 개인 사이만이 아니라 사인 상호 간의 관계에서도 마찬가지로 나타난다.

헌법은 개인이 스스로 선택한 인생관·사회관을 바탕으로 사회공동체 안에서 각자의 생활을 자신의 책임 아래 스스로 결정하고 형성하는 성숙한 민주시민을 전제로 한다.[303] 자신의 생활을 스스로 결정하고 그에 대한 책임과 위험도 본인이 지도록 하는 것이 헌법의 정신에 부합한다. 국가는 인공지능을 활용함으로써 개인에 대한 포괄적인 정보의 수집과 일상적인 감시, 사전 예방적 대응과 자동 결정 및 집행 체제를 굳힐 수 있다. 이는 국가에 의한 후견주의를 넘어 은밀하면서도 강력한 억압을 정착시켜 헌법이 지향하는 바람직한 인간상, 민주주의의 모습과 근본적으로 상충하는 사회로 향하게 할 수 있다.

모든 과학기술은 궁극적으로 인간의 전체적인 삶을 풍요롭게 하는 데 사용되어야 한다. 인간을 대체할 능력을 갖추고 모든 영역에서 막대한 파급효과를 미칠 것

303) 헌재 2000. 4. 27. 98헌가16등, 판례집 12-1, 427, 461.

으로 여겨지는 인공지능 기술이라면 인간 중심적 개발 및 활용의 필요성은 더욱 강조될 수밖에 없다. 국가의 인공지능 활용은 기계에 의한 인간의 '객체화' 또는 '수단화'를 초래할 위험이 있으므로[304] 인간이 단순히 기계에 의한 예측, 판단, 조정의 대상으로 전락하여 자율성을 구속당하는 상황을 철저하게 경계해야 하는 것이다.[305]

인공지능 활용이 초래할 수 있는 감시 체제의 고도화를 경계하기 위해서는 기본적으로 개인정보와 사생활에 대한 보호를 강조해야 한다. 그러나 이는 자칫 인공지능이 활용할 수 있는 데이터를 양적·질적으로 부족하게 만들고, 결국 그 효용을 낮출 수 있다는 점에서 문제가 된다. 인공지능이 가져올 수 있는 업무 처리의 효율성과 신속성, 객관성과 정확성의 이익을 포기할 수는 없으며, 이를 위한 자원으로서 개인정보의 활용은 필수적이다. 이로써 개인은 무료 혹은 저렴한 비용으로 편리한 서비스를 누리고 거래 비용을 줄일 수 있다. 또한 인공지능을 적용한 감시 시스템은 공권력 작용의 남용과 부패를 방지하기 위한 목적으로도 기능할 수 있으므로 국가권력 행사에 대한 민주적 통제의 관점에서 유용한 수단이다.[306] 국가 차원에서도 사회적 안전과 여러 위기에 대한 대응의 첨단화, 국제 관계에서 경제와 안보의 우위를 확보하기 위한 경쟁력 확보의 가치를 가볍게 여길 수는 없다. 인공지능을 비롯한 지능정보기술의 진보는 국가가 계속해서 증대하는 공적 과제를 신속하고 효율적으로 수행할 수 있도록 하고, 인류가 직면한 다양한 위기를 완화, 해소하는 데 매우 중요한 역할을 할 수 있다. 이러한 장점은 대량의 데이터를

---

304) 김일환(2020), "지능정보사회에서 헌법의 역할과 기능", 《성균관법학》 제32권 제3호, 성균관대학교 법학연구원, 78쪽.

305) Ad Hoc Committee on Artificial Intelligence(CAHAI)(2020), Feasibility Study, Council of Europe, p. 27.

306) 인공지능을 활용한 감사시스템의 구축과 규범적 대응방안에 대해서는 백국흠·김일환(2018), "지능정보사회에서 AI감사에 관한 법적 쟁점 고찰", 《미국헌법연구》 제29권 제2호, 미국헌법학회, 45-72쪽, 반부패 도구로 활용할 수 있는 이른바 AI-ACT의 가능성 및 그 위험성에 대한 검토와 대안에 대하여는 조한상(2022), "인공지능 기반 반부패 도구(AI-ACT)의 헌법원리 적합성에 관한 고찰", 《한국부패학회보》 제27권 제1호, 한국부패학회, 5-30쪽.

처리함으로써 개인과 사회에 대한 평가와 분석, 예측과 조정이 가능할 때 비로소 달성될 수 있다. 따라서 국가가 인공지능 기술의 활용 범위를 확대할수록 감시 체제의 구축 가능성이 커지는 것은 어쩌면 자연스러운 흐름이다.

결국, 인공지능 활용에 따른 다양한 이점을 최대한 누릴 수 있도록 하되 사생활의 이익, 민주주의 및 법치주의의 가치와 조화할 수 있도록 신중한 균형을 모색해야 한다.[307] 국가가 감시를 수행하는 것은 단순히 통제만을 목적으로 하는 것이 아니라 사회의 안전과 질서를 유지하고 국민을 보호하려는 것이기도 하다.[308] 핵심은 보호와 통제를 위한 인공지능 활용의 확대가 지나친 가부장주의 또는 국가 후견주의로 전이되거나 국민에 대한 직접 감시 체제 구축을 정당화하지 않도록 하는 것이다. 인공지능의 고유한 특성을 염두에 두면서 그 활용이 법치주의가 요구하는 한계를 준수하고 민주적인 통제의 범위 내에서 이루어지도록 관련 규범을 정비할 필요가 있다. 자의적인 기술 활용, 의도적인 감시 체제 구축을 방어하는 가운데 인공지능이 권력 행사를 통제하고 국민의 자유와 권리를 신장할 수 있는 대표적인 기제로 작용하도록 하려는 노력이 중요하다.

2. 인공지능 활용 근거 규범의 구체화

무엇보다 국가가 구체적인 법적 근거에 따라 인공지능을 활용하도록 하여 법치주의의 가치를 실현해야 한다. 인공지능을 활용한 공권력 작용에 대한 기존의 법제를 전반적으로 검토하여 인공지능 환경에 맞도록 수정하는 한편 인공지능의 고유한 특징 및 위험에 부합하는 규범 체계를 새롭게 정립해야 한다.

---

307) 선지원(2022), “인공지능 생애주기의 관점에서 본 규제와 거버넌스”, 《연세법학》 제39권, 연세법학회, 18-23쪽; 이권일(2023), “지능정보사회에서 개인정보자기결정권이 보호하고자 하는 헌법적 가치”, 《공법연구》 제51권 제3호, 한국공법학회, 229-231쪽; 정애령(2022), “지능정보사회 개인정보자기결정권을 보완하는 데이터 활용과 개인정보보호”, 《공법학연구》 제23권 제1호, 한국비교공법학회, 34-35쪽.

308) Fontes, C., et al.(2022), “AI-powered public surveillance systems: why we (might) need them and how we want them”, *Technology in Society* Vol. 71, p. 2.

인공지능을 이용한 감시의 위험은 주로 행정기관에 의하여 발생한다. 이에 행정의 법률적합성, 즉 법률우위의 원칙과 법률유보의 원칙을 통해 행정부를 통제하는 법치주의[309]를 강조하는 것이 감시에 따른 위험을 경계하는 데 주효할 수 있다. 법치주의는 행정작용에 국회가 제정한 형식적 법률의 근거가 요청된다는 법률유보를 핵심으로 한다.[310] 「행정기본법」도 제8조 법치행정의 원칙에서 "행정작용은 법률에 위반되어서는 아니 되며, 국민의 권리를 제한하거나 의무를 부과하는 경우와 그 밖에 국민생활에 중요한 영향을 미치는 경우에는 법률에 근거하여야 한다"고 하여 '국민생활에 중요한 영향을 미치는 행정작용'은 법률에 근거하도록 명시하였다. 이때 요구되는 법률의 근거는 직무의 범위를 규정한 조직규범으로는 부족하고 그 행정권 발동의 근거가 되는 작용규범이어야 하며,[311] 행정작용이 법률에 근거하고 있는지는 해당 행정작용의 특성 및 그로 인한 기본권 제한의 정도를 고려하여 판단한다.[312]

인공지능 활용은 그 자체로 국민 생활에 매우 큰 영향을 미친다. 단순히 행정권이 목적 달성을 위해 선택할 수 있는 하나의 권한 행사 방법의 하나로만 치부하기 어렵다. 인공지능을 활용한 공권력 작용의 특성 및 그로 인한 감시의 효과와 기본권 침해 가능성을 고려한다면 원칙적으로 권한 행사 자체뿐만 아니라 인공지능이라는 특정한 방법을 활용한 권한 행사가 법률에 근거해야 비로소 법률유보 원칙을 준수한 것으로 평가할 수 있다. 또한 이미 데이터를 수집하기 위한 정보통신기기의 활용이 법률에 의해 규율되고 있는 경우라도 인공지능을 통해 데이터를 처리하는 시스템을 적용하기 위해서는 별도의 법률상 근거가 필요하다고 해야 한다.[313]

---

309) 헌재 2004. 10. 28. 99헌바91, 판례집 16-2하, 104, 118.

310) 헌재 2024. 5. 30. 2023헌마820등, 공보 332, 1021, 1027.

311) 김동희·최계영(2021), 『행정법Ⅰ』, 박영사, 37쪽; 박균성(2017), 『행정법론(상)』, 박영사, 24쪽; 이영무(2024), 『행정법총론』, 정독, 13쪽; 대법원 2005. 2. 17. 선고 2003두14765 판결.

312) 헌재 2005. 5. 26. 99헌마513등, 판례집 17-1, 668, 687; 헌재 2023. 3. 23. 2019헌마1399, 판례집 35-1상, 800, 812.

313) 예컨대, 현행 「개인정보 보호법」 제2조는 "고정형 영상정보처리기기"(제7호), "이동

물론 정보의 수집을 위한 인공지능 활용의 목적과 수준, 그로 인한 감시와 기본권 침해의 위험에 따라서 법률로 정해야 할 사항 또는 법률에 근거해야 하는 사항은 달라질 수 있다. 이는 일률적으로 획정하기보다는 구체적 사례에서 관련된 이익이나 가치의 중요성, 기본권 침해의 정도와 방법 등을 고려하여 개별적으로 결정해야 할 것이다. 다만, 적어도 인공지능 활용이 의도적이든 비의도적이든 개인에 대한 감시의 위험을 직접 내포하는 때에는 그 활용의 목적을 특정하고, 조건과 범위, 통제와 감독을 분명히 규율하는 구체적인 법적 근거를 갖추도록 해야 한다.[314)]

3. 투명성 및 객관성 확보 방안 마련

국가가 필요한 범위 내에서 인공지능을 활용한 감시를 하는 경우 그러한 공권력 작용이 적법절차를 준수하도록 해야 한다. 이는 관련 규범이 가능한 한 감시 활동의 투명성과 객관성, 정확성을 확보할 수 있는 장치를 포함하도록 함으로써 실현할 수 있다. 이에 무엇보다 감시 대상자에게 본인이 인공지능에 의한 분석과 평가의 대상이 된다는 사실을 통지해야 한다. 알 권리는 청구인에게 이해관계가 있고

형 영상정보처리기기"(제7의2호)를 정의하고 있으며, 각각 제25조와 제25조의2에 의하여 규율하고 있다. 그러나 일반적인 영상정보처리기기와 인공지능이 적용된 CCTV나 네트워크 카메라 또는 착용형, 휴대형, 부착·거치형 장치는 기술적 측면이나 기능적 측면에서 서로 다르고, 기본권 보호에 미치는 위험성에도 차이가 크므로 더 직접적인 별도의 활용 근거를 마련할 필요가 있다. 인공지능 CCTV와 일반 CCTV의 구분에 대해서는 김민규(2023), 앞의 논문, 133-137쪽.

314) 이와 관련하여 「행정기본법」 제20조는 "행정청은 법률로 정하는 바에 따라 완전히 자동화된 시스템(인공지능 기술을 적용한 시스템을 포함)으로 처분을 할 수 있다. 다만, 처분에 재량이 있는 경우는 그러하지 아니하다."라고 하여 법률에 근거한 자동적 처분을 원칙적으로 허용하고 있다. 이에 따라 「수입식품안전관리 특별법」 제20조의2는 제1항에서 국민건강에 미치는 위해발생의 우려가 낮고 반복적으로 수입되는 수입식품등의 수입신고는 수입식품통합정보시스템에 의하여 완전히 자동화된 방식으로 수리할 수 있도록 규정하고, 제2항에서 자동화된 방식으로 수리하는 수입신고의 대상 및 절차 등에 관한 세부적인 사항을 총리령으로 정하도록 위임하고 있다. 특정 인공지능 시스템의 활용 근거와 범위, 절차 등을 법령으로 규율한다는 점에서 고무적이다.

타인의 기본권을 침해하지 않으면서 동시에 공익 실현에 장애가 되지 않는다면 최대한 널리 인정해야 하고, 적어도 직접적인 이해관계가 있는 자에 대하여는 특단의 사정이 없는 한 관련된 정보를 의무적으로 공개할 것을 요구한다.[315] 따라서 이해관계가 있는 당사자라면 원칙적으로 인공지능에 적용된 알고리즘과 관련한 정보에도 접근할 수 있어야 한다.[316]

인공지능 활용 감시의 투명성 확보는 단순히 관련 정보에 대한 형식적인 접근 가능성 보장에 그쳐서는 안 된다. 컴퓨터에서 사용하는 프로그램 작성 언어 또는 기계어가 아니라 자연어를 통해 이해하기 쉬운 방식으로 정보를 제공하도록 해야 한다. 인공지능 활용의 내용과 이유, 결정이 이루어진 과정 등을 명확한 언어로 공개할 때 감시 활동의 절차적인 적법성을 인정할 수 있고, 이는 당사자가 감시 및 그로 인한 피해에 대하여 책임을 묻고 이의제기와 사법절차를 통해 권리구제를 도모하기 위해서도 필수적이다.[317]

인공지능 활용으로 인하여 감시 체제가 구축될 위험은 그 자체로 중대한 문제이다. 하지만 더 심각한 문제점은 사실과 다른 정보나 부적절한 지표에 기초하여 인공지능 시스템이 분석과 예측을 진행하고, 이에 따라 평가나 단속, 감찰이 부당하게 이루어질 수 있다는 점이다. 앞서 살펴본 것처럼 인공지능은 데이터를 정교하게 분석하여 결과를 도출하는 만큼 대표성, 진실성, 최신성 등 훈련 데이터의 품질에 따라 예측 결과의 편향성과 그로 인한 부당한 차별 문제가 발생하기 쉽다.[318]

---

315) 헌재 1991. 5. 13. 90헌마133, 판례집 3, 234, 246-247.

316) 유럽연합의 「인공지능에 관한 명령」은 제13조에서 투명성 및 이용자에 대한 정보 제공을 규정하면서 고위험 인공지능 시스템(High-risk AI systems)은 사용자가 시스템의 결과물을 해석하고 적절하게 사용할 수 있을 만큼 그 작동이 충분히 투명하게 설계 및 개발되어야 한다고 명시하고(제1항), 사용자와 관련이 있고 접근 가능하며 이해할 수 있는 정보를 간결성, 완전성, 정확성, 명확성을 갖추어 제공하도록 하면서(제2항) 이에 포함되어야 할 정보를 구체적으로 나열하고 있다(제3항).

317) Burgess, P.(2024), AI and the RULE OF LAW: The Necessary Evolution of a Concept, Hart Publishing, p. 163.

318) 인공지능 활용에 따른 차별의 위험과 차별받지 않을 권리의 실현을 위한 방안에 대해서는 이준일(2022), 앞의 논문, 367-369쪽.

따라서 감시가 꼭 필요한 범위에서 객관성과 정확성을 갖추어 그 목적을 달성할 수 있도록 하는 것이 매우 중요하다. 이를 위해서는 처음부터 달성하려는 목적과 밀접한 연관성을 갖는 지표를 설정하고 그에 적합한 데이터의 유형과 범위를 합리적인 범위에서 선택해야 한다. 또한 훈련 데이터의 품질을 확보하고 다양성을 극대화하는 방안,[319] 차별 방지 알고리즘을 적용하는 방안[320]이 필요하며, 오류를 탐지, 조정, 해결할 수 있는 장치나 제도를 반영해야 한다.

이러한 조건이 갖추어져야만 인공지능을 편향성 같은 인간의 한계를 극복하고 사회적 발전을 추진하는 동력으로 활용할 수 있다. 인공지능의 객관성과 정확성은 그 활용을 통한 감시 및 감시에 따른 조치의 공정성과 합리성을 신뢰하기 위한 전제 조건이라는 점에서 특별히 강조되어야 한다.[321] 물론 지나치게 정확성에만 초점을 두면 그만큼 데이터의 수집과 처리의 범위를 확장할 수 있어 감시의 위험을 더 확대할 수 있으므로 양자의 조화를 이루도록 하는 수준을 면밀하게 설정해야 한다.

4. 실효적인 감독 및 권리구제 제도 마련

인공지능 기반 감시 시스템이 정해진 목적을 위하여 허용된 범위 내에서 사용되도록 감독하고, 특정한 상황에서 감시의 필요성과 이를 통해 달성하고자 하는 공

---

319) 편견과 차별 문제를 해결하기 위해 인공지능 시스템의 구축 및 개발, 배포 단계를 포함하여 인공지능 프로세스의 모든 단계에서 다양성을 극대화해야 할 필요성에 대해서는 Evans, L.(2020). Artificial Intelligence and Public Standards: A Review by the Committee on Standards in Public Life, The Committee on Standards in Public Life, p. 59.

320) 직장에서의 알고리즘 차별 문제와 관련하여 알고리즘과 빅데이터의 중립성이 허구임을 강조하면서, 개인을 그가 속한 집단과 관련한 고정관념을 기반으로 판단하지 않는 반고정관념에 초점을 둠으로써 비차별을 넘어 적극적인 차별 방지 알고리즘으로 나아가야 한다는 주장에 대해서는 Stephanie Bornstein(2018), "Antidiscriminatory Algorithms", *Alabama Law Review* Vol. 70 No. 2, pp. 519-572.

321) 「행정절차법」은 투명성과 함께 행정의 공정성 및 신뢰성 확보를 목적으로 명시한다(제1조).

익이 그에 따른 비용 및 기본권 침해의 위험성보다 더 큰지를 공정하게 평가할 수 있는 체제를 갖추어야 한다.[322] 인공지능을 활용하기에 앞서 사전에 적합성 및 위험성을 평가하고, 인공지능을 활용하는 전 단계에 걸쳐 감독이 가능하도록 국가기관 내외부에 체계적인 거버넌스를 구축해야 한다.

법치주의의 실현이라는 관점에서 국가기관이 수행하는 업무를 객관적으로 평가, 감독하는 것은 일반적으로도 중요한 과제이다. 다만, 인공지능 활용에 따라 감시의 위험이 증대하는 문제에 대해서는 개인에게 주관적인 권리를 부여하여 개별적으로 대응하도록 하는 방식은 실효성을 기대하기 어렵다는 점에서 그 중요성이 더해진다. 국가가 인공지능을 활용하여 개인을 감시하고 그 결과에 기초하여 불이익한 결정을 함으로써 권리침해가 발생할 수 있음에도 불투명성 때문에 당사자는 그 배경과 이유를 쉽게 이해하지 못하고, 개별적으로 권리구제를 도모하는 데 어려움을 겪을 수 있다. 국가와 개인 사이의 정보와 자원의 불균형으로 인해 개인이 실효적으로 대처하기 쉽지 않은 것이다.

인공지능을 활용한 감시가 특정한 개인이나 집단의 권리, 의무에 직접 영향을 미칠 때는 문제 제기에 따른 분쟁 가능성과 후속 조치를 어느 정도 기대할 수 있다. 그러나 그러한 감시와 그에 따른 평가와 결정이 이루어지고 있는지를 일일이 통지하지 않고 당사자가 알기 어려운 경우, 특정한 개인이나 집단의 이해관계와 직접 연관이 없는 경우에는 이의제기와 분쟁을 통한 적법성 평가와 수정을 기대하기 어렵다. 개인에게 주관적인 권리를 부여하는 방식으로 인공지능을 활용한 공권력 작용을 통제하려는 시도는 한계가 있는 것이다. 이러한 측면에서도 인공지능을 활용한 감시에 대해서는 이를 중립적이고 객관적으로 평가, 감독할 수 있는 절차의 중요성이 더 특별하다.

---

322) Fontes, C. et al.(2022), op. cit., p. 10.

제 2 절 독일 헌법재판소 결정의 시사점

1. 의의

예측 치안 활동과 관련하여, 개인정보를 포함하는 데이터를 무작위로 수집하고 활용하는 정보처리는 개인정보자기결정권에 대한 제약으로 볼 수 있고, 이에 대한 헌법적 정당성 평가는 자유권 제한의 한계를 준수하였는지의 여부를 기본적인 법률유보 원칙 및 과잉금지원칙 등의 심사도구로 판단하면 될 것이다. 그러나 인공지능 기술을 활용하는 경우 이미 집적된 데이터라고 하더라도 이에 대한 분석 및 평가는 새롭고 가치 있는 사실과 정보를 만들어내고, 개인의 삶에 대한 감시가 가능해질 수 있는 위험성 등을 고려한다면 구체적 심사를 진행하는 데 있어 범죄의 예방 내지 안전의 확보 대(對) 데이터의 활용을 통한 자유의 제약 정도를 형량하는 과정이 쉽지 않다.

정당한 목적 아래 수집한 데이터를 인공지능 기술을 이용하여 새롭게 분석하고 평가하는 행위를 어떻게 바라볼지, 이는 어떠한 요건하에 가능할지, 독일의 헤센주의「공공안전 및 질서법」제25a조의 위헌성 판단 및 개정된 법률을 통해 시사점을 도출할 수 있다.

2. 사실관계

헤센주 법률과 함부르크주 법률의 두 조항은, 이전에 연결되지 않았던 데이터들을 자동화된 데이터베이스와 분석 플랫폼에 연결될 수 있도록 하고, 검색기능을 사용하여 기존 수집된 데이터에 체계적으로 접근할 수 있도록 하는 법적 근거를 마련해주는 것으로 양자의 내용은 거의 유사하다. 이 조항들은 경찰이 개별 사건에서「형사소송법」제100a조 제2항에서 언급된 중대한 범죄행위를 예방하거나(제1문) 특정한 법익에 대한 위협을 방지하기 위하여(제2문) 데이터 분석 또는 평가의 일환으로 자동화된 애플리케이션을 통해 저장된 개인 관련 데이터를 추가 처리할 수 있도록 권한을 부여하고 있다. 자동화된 프로그램은 개인이나 개인들의

모임, 기관, 사물 및 사건 간의 특별한 연관성 또는 관계를 설정하고 중요하지 않은 정보나 지식은 걸러내고 새로 생성된 지식을 알려진 사실관계에 편입시키는 등 저장된 데이터를 통계적으로 분석하거나 평가할 수 있다. 헤센주에서는 hessenDATA 분석 플랫폼을 통해 "「헤센주 공공안전 및 질서법(HSOG, 이하 헤센주 공공안전법)」 제25a조의 권한"이 매년 수천 번 이상 활용되고 있다. 반면 함부르크주 「경찰 데이터 처리에 관한 법률」 제49조는 아직까지 적용되지 않은 상태에서 독일 연방헌법재판소의 결정을 받게 되었다.

특히 청구인(German Society for Civil Rights: GFF) 측은 범행이 저질러지기도 전에 용의자의 프로필을 생성하는 해당 소프트웨어가 예측적 경찰활동에 활용됨으로 인해 법 집행에서의 오류 및 차별의 위험이 커진다는 점을 주장하였다. 또한 헤센주와 함부르크주가 경찰 등 법집행기관의 데이터 수집 출처나 분석 기법 활용 근거 등을 사전에 명확히 제공하지 않았다는 점을 지적하면서, 해당 범죄예측 시스템의 법적 정당성이 충분하지 않다고 주장하였다. 이에 해당 주들은 범죄예측 소프트웨어가 범죄예방 관련 정책의 일환으로 도입된 것이며, 기존에 수집된 데이터를 처리한 것에 불과하다 대응하였다.[323]

3. 개인정보자기결정권의 제한

수집된 데이터를 새로운 목적에 이용하기 위한 수권은 기본권에 대한 새로운 침해에 해당한다.[324] 그렇다면 이미 집적된 데이터를 새롭게 분석하고 평가할 수 있는 애플리케이션에 연결하는 것을 새로운 정보처리로 볼 것인가, 즉 새로운 기본권에 대한 제한으로 볼 것인가를 먼저 판단해야 할 것이다.

독일연방헌법재판소는 저장된 데이터가 데이터 분석 및 데이터 평가를 위한 자동화된 애플리케이션을 통해 처리되는 경우, 이 과정에서 개인 관련 데이터가 사용되는 모든 사람의 개인정보자기결정권을 제약하는 것으로 확인하였다. 헤센주

323) 정채연(2023), 앞의 논문, 85쪽.

324) BVerfG, Urt. 20.04.2016 – 1 BvR 966/09, Rn. 285.

「공공안전법」 제25a조 또는 함부르크주 「경찰법」 제49조을 통해 입법자는 저장된 데이터의 자동화된 분석을 통해 이전에 수집된 데이터를 원래의 목적을 넘어 추가로 사용할 수 있도록 승인하는 것이다. 이는 기본권에 대한 새로운 침해에 해당하며 목적 제한의 원칙에 따라 헌법상 구체적으로 정당화되어야 한다.[325)]

4. 제한의 정당성 심사

가. 법률유보의 원칙

해당 판결은 독일 헤센주 및 함부르크주 경찰데이터 처리에 관한 법률에 대한 위헌성 판단으로, 저장된 데이터를 분석 또는 평가할 수 있는 자동화된 애플리케이션의 사용을 규정하고 있다. 따라서 헤센주와 함부르크주 경찰활동을 위한 형식적 법적 근거는 마련되어 있다. 다만 법률의 구체적 내용이 명확성 원칙 내지 과잉금지원칙을 준수하였는지 여부에 따라 본 대상 법률에 위헌성을 판단할 수 있을 것이다.

개인정보의 수집이나 저장이 구체적인 법규정에 근거하지 않거나, 처리 목적을 위한 적절한 연결점을 법규정이 제공하지 않고 당사자 또한 동의 등을 제공하지 않는다면, 그러한 개인정보처리의 위법성 여부를 검토해야 한다.[326)] 법률의 일반적·추상적 성격상 미리 방법과 목적 및 범위에 대한 명확하고 구체적인 규정이 불가능하다는 점과, 예측 치안활동은 아직 실현되지 않은 위험을 방어하기 위한 것으로 아주 개별적이고 구체적인 목적과 방법을 규정하기 어려운 측면이 있다. 이에 따라 원칙적으로 입법자는 이러한 규율의 과제를 입법자 자신과 행정 간에 배분할 수 있다. 그러나 입법자는 법률유보를 유지하면서 특별히, 데이터의 유형과 범위를 제한하고 데이터 처리방법을 제한하기 위해 전반적으로 충분한 규율이 이루어지도록 보장해야 한다. 입법자가 스스로 직접 일률적으로 규정할 수 없는 부분을 규정하기 위해, 위임명령을 고려해 볼 수 있다.[327)]

---

325) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 50.

326) 김일환(2020), 앞의 논문, 129쪽.

입법자는 특수한 기술적 특성과 침해를 완화하기 위하여 필요한 규정을 신속하게 추가해야 하는데, 보다 심층적인 법적 표준화가 실행 가능하지 않은 한 행정부가 조직 및 기술적 세부 사항을 더 자세히 규제할 수 있도록 승인할 수 있다. 그러나 그것은 규제요건과 행정기관의 규제 권한 및 의무와 함께 데이터의 종류와 범위, 처리 방법 등에 대하여 충분하고 명확하며 투명하게 제한되도록 보장해야 한다.[328] 나아가 허용된 데이터 처리를 제한하는 조치가 이미 일반적 또는 「경찰 데이터 보호법」의 규정에서 비롯되는 경우, 데이터 분석 또는 평가 권한에 대한 적용 가능성은 당국과 시민 모두에게 충분히 명확해야 하며, 특히 데이터 분석 또는 평가 권한의 실제 설계를 위해 어떤 결과가 뒤따르는지 충분히 명확해야 한다.[329]

나. 과잉금지원칙 위반 여부

1) 목적과 수단의 비례관계 판단

자동화된 데이터 분석 또는 평가에는 헌법적 정당화가 요구된다. 원칙적으로 헌법적으로 정당화는 가능하지만, 특별히 비례성 원칙의 위반 여부가 중요하며 그 요건은 해당 권한의 구체적 범위에 따라 달라진다. 심판대상조항은 정보기술의 발전에 따라, 감지되지 않은 채로 남아 있던 경찰 데이터에서 중대하고도 임박한 범죄의 징후를 발견하여 중대한 범죄예방의 실효성을 증대시키는 정당한 목적을 추구한다(목적의 정당성). 경찰은 특히 테러리스트 및 극단주의의 폭력, 조직적이고 중대한 범죄에서 디지털 미디어와 통신수단의 이용이 증가함에 따라 품질과 형식이 점점 더 이질적인 데이터 스트림(Datenaufkommen)에 직면하고 있다고 설명한다. 경찰 데이터에 포함되어 있는 정보에서 기존 검색능력으로는 시간적 제한 아래 중대한 정보를 확보하기 어렵다는 점에서 자동화된 데이터 분석 앱의 사용은 성공적 경찰 작용에 있어 중요한 의미를 가지며, 이는 범죄예방이라는 목적을 실현하는 적절한 수단이다(수단의 적합성). 또한 자동화된 데이터 분석 또는 평가

327) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20= NJW 2023, 1196, 1196.

328) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 112.

329) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 114.

는 다른 덜 침해적 수단으로 범죄예방 관련 정보를 생성하는 데 동일한 효과를 생성할 수 없기 때문에 필요하고도 침해최소적 조치라고 볼 수 있다(피해의 최소성).

2) 법익의 균형성 판단: 좁은 의미의 비례성 심사

① (수집목적에 따른) 기본권 제한의 중대성 판단

자동화된 데이터 분석 또는 데이터 평가의 기본권 제한의 중대성은 일차적으로 이전의 데이터 수집으로 인한 제한의 비중에 따라 결정된다. 이와 관련하여 「연방범죄수사청법은(Bundeskriminalamtsgesetz)」에 대한 결정[330]에서 이미 설시한 바와 같이, 목적구속의 원칙[331] 및 목적변경금지의 원칙[332]이 적용된다. 국가기관이 수집한 데이터의 계속적 이용과 이전에 관한 요청들은 목적구속의 원칙과 목적변경금지의 원칙에 따라야 한다.[333]

---

330) 독일 「연방수사청법」의 테러방지 권한에 대해 연방헌법재판소는 위험방지를 위한 데이터의 교부와 이전이 만일 구체적 수사의 계기와 무관하게 이루어지거나 테러범죄의 일반적 예방을 위해 허용된다고 한다면, 헌법에 위반된다고 판단한 바 있다.

331) 헌법상 기본권 제약에 요구되는 규범명확성의 원칙은 개인정보보호 영역에서 실현되는 구체적 표현을 목적구속의 원칙으로 볼 수 있다. 규범명확성 원칙을 실현하는 법률규정이란 개인정보의 처리 및 이용목적을 정확하게 표현하는 것이므로, 구체적이지 않거나 계속해서 구체화될 수 없는 목적을 위한 개인정보의 준비행위는 금지된다. OECD의 가이드라인에서 제시하는 개인정보처리 8대 원칙 중 하나인 목적구체성 원칙은 “개인정보의 수집목적은 늦어도 수집할 당시에 특정되어 있어야 한다. 그 후의 이용은 수집목적의 실현 또는 수집목적과 양립하는 것이어야 하고 수집의 목적이 변경될 때마다 그 목적을 구체화하여야 한다”고 규정하고 있다. 구체적인 목적확정 및 원래 수집된 개인정보의 범위 내에 있도록 개인정보처리를 유지시키는 목적구속원칙이 모든 합법적 정보처리과정을 위하여 중요한 기준으로 작용한다. 김일환(2014), “개인정보보호법상 목적구속원칙의 의의와 내용에 관한 연구”, 《미국헌법연구》 제25권 제3호, 미국헌법학회 참조.

332) 애초에 정해진 목적과 다른 이용은 목적변경금지의 원칙(Zweckänderung)에 따라 단지 법률에 명시적 규정이 있을 경우 또는 당사자의 동의에 의해서만 허용된다는 것을 말한다. 입법자는 데이터의 목적변경을 개별 사안에서 비견될 만한 비중의 범죄규명을 위한, 또는 적어도 비견될 만한 비중의 법익에 대한 위험의 방지를 위한 구체적 단초가 존재할 경우 허용할 수 있을 것이다.

333) BVerfG, Urteil 20.04.2016 - 1 BvR 966/09, Rn. 276.

입법자는 원래 목적 범위 내에서 (데이터를 수집한 목적에 부합하는 경우), 당초 데이터 수집을 하게 한 특정한 조사나 수사를 넘어서는 추가적인 사용을 허용할 수 있다. 수집된 데이터를 새로운 목적에 이용하기 위한 수권은 기본권에 대한 새로운 침해에 해당한다.[334] 목적과는 다른 정보 이용 및 처리는 매우 제한된 범위 내에서만 인정되는 법률상 근거가 필요한 새로운 기본권 제한에 해당한다. 결국 이는 목적구속의 원칙을 보장하기 위하여 국가기관 간 정보 전달과 이용에 관한 엄격한 대비책이 필요하다는 것을 뜻한다.[335] 서로 다른 목적의 결합을 통하여 개인정보의 연결을 허용하는 법률규정은 해당 정보주체의 권리보호를 불확실한 쪽으로 이끌 수 있다.[336] 목적구속원칙은 원칙적으로 처음에 수집하거나 저장한 목적으로만 개인정보의 처리를 요구하므로 해당 개인정보들은 분리해서 저장해야 한다. 결국 목적구속의 원칙은 원래 수집 목적을 벗어나는 다기능적 정보 이용의 배제를 뜻한다.[337]

② 데이터의 추가처리: 증가한 제약의 위험성, 추가되는 헌법적 정당화 요건

본 사건에서 문제된 앱을 이용하여 자동화된 데이터 분석 또는 평가를 통해 일단 수집·저장된 데이터의 추가 처리는 그 자체로 원래 수집이 가지는 제약의 정도(Eingriffsgewicht)를 넘어서 부담적 효과를 가질 수 있으므로, 자동화된 데이터 분석 또는 평가는 고유한 제약의 비중을 가진다. 이러한 점에서 좁은 의미의 비례성 원칙에 따른 추가적 정당화 요건의 필요성이 도출된다.

i. 추가적 제약의 위험성

자동화된 데이터 분석 또는 평가는 새로운 지식의 생성을 목적으로 한다. 이와 관련된 경찰 당국은 기존의 거의 모든 정보통신기술을 사용하여 기존에 활용 가능한 데이터로부터 광범위한 지식을 확보할 수 있으며, 데이터 평가를 통해 새로

334) BVerfG, Urteil 20.04.2016 - 1 BvR 966/09, Rn. 285.
335) BVerfGE 65, 1, 46.
336) 김일환(2014), 앞의 논문, 121쪽.
337) Friedrich v. Zezschwitz(2003), Konzept der normativen Zweckbegrenzung, Alexander Roßnagel(Hrsg.), Handbuch Datenschutzrecht, C. H. Beck, S. 221.

운 상관관계를 추론해 낼 수도 있다. 사실 경찰이 이전에 확보한 정보를 가지고 또는 다른 정보와의 결합을 통하여 추가 수사를 위한 출발점으로 삼아 추적이나 수사의 단서로 활용하는 것은 드문 일이 아니다. 다만, 인공지능 기술을 이용한 자동화된 데이터의 분석 및 평가는 복잡한 대량의 정보를 처리할 수 있기 때문에, 한 단계 더 나아가는 것으로 평가한다. 기존 데이터를 연결하고 사용하는 분석 기술 및 방법에 따라 다른 방법으로는 접근할 수 없었을 새로운 개인 관련 정보를 획득할 수 있다. 따라서 이러한 해당 처분은 데이터에 포함된 정보를 이전보다 더 집중적으로 강도 높게 추출할 수 있게 된다. 이러한 처분은 데이터에 이미 포함되어 있기는 하지만, 연결고리가 부족해서 드러나지 않았던 개인에 관한 정보를 드러낼 뿐만 아니라, 적절히 활용하면 완전한 프로파일링에 근접할 수 있다. 소프트웨어가 해당 인물을 둘러싼 관계들과 연결고리들에 관한 데이터와 알고리즘에 의해 산출된 가정까지 포함해 개인에 대한 그림을 완성할 수 있는 새로운 가능성이 생겨날 수 있기 때문이다. 그렇다면 목적 구속의 원칙은 그 자체로 제약의 비중을 충분히 고려하지 못할 수 있다.

자동화된 애플리케이션을 사용하면 관계와 상관성 등을 식별하기 위한 복잡한 알고리즘을 적용하는 것 외에도 예측 치안이라는 의미에서 스스로 추가적인 진술(Aussage)을 확보할 수 있다. 이는 특히 검증하기 어려울 수 있는 개인에 대한 광범위한 정보와 가정을 생성할 수 있다. 왜냐하면 복잡한 알고리즘 시스템이 기계 학습 과정에서 원래의 인간 프로그래밍과 점점 더 분리될 수 있고, 기계 학습 과정과 프로그램 적용 결과를 추적하기 점점 더 어려워질 수 있기 때문이다. 이는 동시에 이 애플리케이션에 대한 국가의 통제권이 상실될 위험이 있다. 일반적으로 개인정보자기결정권에 대한 제약의 정도는 주로 데이터의 유형, 범위 및 예상 가능한 활용 그리고 오용의 위험에 따라 결정된다. 또한 승인된 데이터 분석 또는 평가의 방법도 제약의 강도에 영향을 미친다. 복잡한 형태의 데이터 교차확인기법(Datenabgleich, data cross-checking)[338]을 사용함으로써, 특별히 (기본권에

338) 데이터 교차확인은 시스템이 수집하거나 처리한 데이터의 정확성 및 일관성을 보장하기 위한 중요한 단계, 잘못된 데이터로 인한 잘못된 결정을 방지하고 시스템의 신

대한) 제약이 가중될 수 있다. 전체적으로 볼 때, 자동화된 데이터 분석 또는 평가의 방법은 그로부터 얻을 수 있는 개인에 대한 정보가 광범위하고 깊을수록, 오류취약성(Fehleranfälligkeit)과 차별취약성(Diskriminierungsanfälligkeit)이 높을수록, 소프트웨어에 의해 생성되는 링크를 역추적하기가 더 어려울수록 제약의 강도가 더 커진다.[339]

사적 행위자나 다른 국가의 소프트웨어를 사용하는 경우, 제3자가 탐지되지 않은 조작이나 눈에 띄지 않게 데이터에 액세스할 위험도 있다. 또 다른 구체적인 과제는 차별적인 알고리즘의 개발과 사용을 방지하는 것이다. 따라서 자가 학습 시스템은 제한된 추적 가능성에도 불구하고 충분한 수준의 보호를 보장하는 특별한 절차적 예방 조치하에서만 경찰 업무에 사용될 수 있다.[340]

ii. 추가되는 헌법적 정당화 요건: 예) 구체화된 위험

법률적 프레임워크에 따라 제약의 강도가 완전히 달라질 수 있기 때문에, 자동화된 데이터 분석 또는 평가를 헌법적으로 정당화하기 위한 요건들은 다양하다. 입법자는 데이터의 종류와 범위, 평가방법의 한계에 관한 규정을 통해 제약의 강도를 조정할 수 있으며, 이는 기본권 제약의 전제에 관한 헌법적 요건에 각각 상응한다. 각 제약의 비중에 해당하는 좁은 의미의 비례성 명령의 요건은 해당 처분으로 보호하고자 하는 법익, 그리고 해당 처분의 발동 요건인 제약의 임계치(Eingriffsschwelle)에 따라 달라진다. 자동화된 애플리케이션이 정보주체의 개인정보자기결정권에 중대한 제약을 초래하는 경우, 그러한 제약은 일반적으로 높은 강도의 제약에 해당하는 비밀 감시 조치에 적용되는 엄격한 요건을 충족시키는 경우에만 정당화된다. 이러한 방법의 사용은 예를 들어 개인의 생명, 신체 또는 자유와 같은 특히 중요한 법익을 보호하기 위해서만 허용된다. 여기서 헌법적으로 요구되는 제약의 한계는 충분히 구체화된 위험(충분히 식별할 수 있는 위험,

---

뢰성을 높이는 데 도움이 된다.

339) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20 .Rn. 90.

340) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20 .Rn. 100.

hinreichend konkretisierte Gefahr)이다.[341] 충분히 구체화된 위험은 최소한 보호되는 법익에 대하여 구체적인 위험[342]이 발생했다는 실질적 증거가 있어야 한다는 것을 의미한다. 이러한 점에서 일반적 경험원칙만으로는 충분하지 않다. 오히려 개별 사건에서 보호하고자 하는 법익을 침해하는 사건이 일어날 것이라는 예측을 뒷받침할 만한 특정 사실이 확인되어야 한다. 이러한 의미에서 충분히 구체화된 위험은 피해로 이어지는 인과적 과정을 아직 충분한 확률로 예측할 수 없는 경우, 특정 사실이 이미 개별 사건에서 최우선적인 법적 이익에 대한 임박한 위험을 나타내는 경우 이미 존재할 수 있다. 이러한 사실들은 한편으로는 적어도 그 나름대로 사건의 성격이 구체적이고 시간적으로 예측 가능하다는 결론을 도출할 수 있어야 하며, 다른 한편으로는 적어도 감시 조치가 그들에 대해 구체적으로 사용될 수 있고 대부분 그들에게만 국한될 수 있을 정도로 신원이 알려진 특정인이 관련되어 있다는 결론을 도출할 수 있어야 한다.[343] 특히 중요한 법익에 대한 최소한의 구체화된 위험의 한계 기준이 면제되기 위해서는, 허용된 분석 및 평가의 가능성이 실질적으로 매우 좁게 제한되고 규범적으로 명확하고 충분한 확실성을 가지고 있어서 조치에 따른 제약의 비중이 현저히 감소되는 경우이어야만 한다.

---

341) BVerfGE 141, 220 = NJW 2016, 1781, Rn. 112.

342) 구체적 위험에서 위험이란 어떠한 상태나 행위가 그의 객관적으로 예상될 수 있는 진행이 저지되지 않는다면 경찰상 보호법익을 손상할 개연성이 있는 경우를 말한다. 즉, 위험은 가정적인 사건진행에 따르면 공공의 안녕과 질서의 관념에 포함되는 규범, 권리, 법익이 외부로부터의 영향으로 훼손되는 것을 의미하는 손상이 발생되는 경우에 성립된다. 결국 위험에 있어서는 법익손상과 손상발생의 개연성이라는 두 가지 요소가 중요한 의미를 갖는다(Gusy, Polizeirecht, 6. Aufl. Rn. 194.).

343) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 106.
물론 객관적으로 위험이 존재하지 않음에도 불구하고 경찰권이 행사된다면 위법이 되겠지만, 손해발생의 개연성 판단은 불확실 아래서의 행위이고 그 성질상 예측과는 다른 결과가 발생할 수 있는 가능성을 포함하고 있기 때문에 경찰개입이 되지 않아도 손해는 발생하지 않았다는 사실이 나중에 판명된다고 해도 그것으로 경찰개입이 반드시 위법이라 할 수는 없다. 구체적 위험을 예방할 목적, 즉 구체적 위험이 발생하기 이전인 ① 위험의 사전대비(Gefahrenvorsorge)단계에서 정보수집, ② 구체적 위험단계에서의 정보수집으로 구분될 수 있다. 경찰이 수집한 정보를 다른 정보와의 연결고리를 통해서 새로운 가치가 창출한다면 새로운 기본권 제약으로 보고 있다.

반면에 덜 심각한 개입은 구체적인 위험이 있는 경우, 예를 들어 적어도 상당히 중요한 범죄를 예방하는 것과 같이 최소한 상당히 중요한 법적 이익을 보호하는 역할을 하는 경우 이미 정당화될 수 있다. 반대로, 구체적인 위험에 미치지 못하는 침해 기준은 해당 조치가 고위험, 매우 중요하거나 특히 가장 중요한 법적 이익을 보호하는 데 도움이 될 경우 충분하다.(자세한 내용은 BVerfGE 155, 119, 150항 = NJW 2020, 2699 참조). 침해적 조치의 경우 구체적인 위험(konkretisierte Gefahr)과 특히 중요한 법적 이익의 보호(der Schutz besonders gewichtiger Rechtsgüter)가 함께 있어야 하지만, 덜 침해적인 조치의 경우 법적 허가기준(Ermächtigungsnorm)이 구체적인 위험 또는 특히 중요한 법적 이익의 보호를 전제로 하는 경우 충분하다. 이는 특히 입법자가 사용 가능한 데이터의 종류와 범위 및 처리방법에 대한 보다 엄격한 규제를 통해 데이터 분석 또는 평가의 침입적 비중을 줄이고자 할 경우 고려된다.[344)]

③ 증가한 위험에 따른 추가적, 헌법적 정당화 요건 심사

위에서 제시한 일반적 기준에 따르면, 헤센주「공공안전법」제25a조 제1항 제1문 및「함부르크 경찰법(HmbpolDVG)」제49조 제1항 제1문에 따라 부여된 데이터 분석 및 평가의 권한들은 데이터와 방법을 넓게 규정하고 있어, 그 구체적 제약의 비중이 잠재적으로 매우 높고, 따라서 헌법적으로 이러한 규정은 제약에 관한 엄격한 조건을 충족해야 한다.[345)] 심판대상 법률규정에 따른 권한들은 법적으로 무제한의 데이터세트를 처리 방법에 대한 제한도 없이 가능하게 허용하고 있다. 이를 통해 경찰로 하여금 단 한 번의 클릭으로 개인, 집단, 군중의 포괄적인 프로필을 생성할 수 있도록 허용하며, 무고한 수많은 사람들이 이런저런 상황에서 남기게 되는 많은 데이터에 대한 자동화된 평가를 받게 되고, 경찰의 잘못된 단서로 활용되면 추가적 경찰활동에 내맡겨지게 된다. 그러므로 이러한 조치가 허용되

344) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 107.
345) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20. Rn. 108.

려면, 특히 중요한 법익에 대한 구체화된 위험요건이 적용되어야 한다.

i. 데이터의 유형과 범위 제한 여부

포함될 수 있는 데이터의 유형과 범위가 법에 의해 축소되고 자동화된 분석 또는 평가의 가능한 방법이 처음부터 제한되어 있어 권한에 기반한 조치가 비록 더 복잡하고 더 느리지만, 자동화된 애플리케이션 없이도 현실적으로 얻을 수 있거나, 처음부터 승인이 개인정보를 생성하지 않고 위험하거나 취약한 장소를 식별하는 것만을 목표로 하는 경우, 목적 제한 원칙을 준수하는 것만으로도 자동화된 애플리케이션에서 데이터의 추가 처리를 정당화할 수 있다.[346] 입법자가 특정 위험에 직면하기 전에 이 애플리케이션을 사용하여 자동화된 데이터 분석 또는 평가할 수 있도록 허용하되 기본권 제약의 강도 줄이기를 원하는 경우, 자동 데이터 분석 또는 평가에 사용할 수 있는 데이터의 유형과 범위에 대한 기본 지침을 스스로 결정해야 한다. 특히, 어떤 데이터세트가 포함될 수 있고 어느 정도까지 자동화할 수 있는지를 법 자체에서 규제해야 한다. 입법자가 사용 가능한 데이터 집합을 구체적으로 나열하지 않는 경우, 법률에 따라 추상적이고 일반적인 방식으로 규제하고 공개해야 한다. (자동으로) 포함될 수 있는 데이터의 범위는 헌법상 엄격하게 정의되어 있지 않다. 그러나 사용할 수 있는 데이터세트가 크고 많을수록 간섭의 강도는 커지며, 제한의 사유와 보호하고자 하는 법적 이익에 대한 요건도 그에 상응하여 높아져야 한다.[347] 헌법상 목적구속성 원칙은 주거 감시 또는 온라인 수색에서 얻은 데이터가 범죄를 예방하기 위한 목적으로 데이터 분석 또는 평가에 포함되지 않도록 법률 자체에서 규제해야 함을 의미한다.[348]

그러나 두 조항 모두 자동화된 데이터 분석 또는 평가에 데이터의 유형과 데이터의 범위 및 사용량을 거의 제한하지 않는다. 일반 목적구속성 조항으로 「헤센주법」 제25a조에 의한 자동화된 데이터 분석이 가능한 데이터의 종류에 사건경과정

346) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20. Rn. 125.
347) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20. Rn. 116.
348) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 118.

보가 명확히 제외되지 않는다.[349] 전반적으로 데이터의 범위가 목적구속성에 관한 일반 규정에 의해 명확하게 제한되지 않아 데이터 분석이나 평가에 대한 헌법적 침해의 심각성이 중대하게 제한될 수 있다.[350] 대규모 데이터세트의 자동화된 분석 또는 평가에서도 일부가 자동화된 방식으로 포함되는 경우, 데이터의 양과 부분적으로 자동화된 통합으로 인해 개별 날짜의 목적을 식별하고 확인하기 어렵기 때문에 목적구속성 원칙이 현실적인 이유로 쉽게 그 제한 효과를 발휘할 수 없다.[351] 사건경과정보(Daten von Vorgangsbearbeitung)의 포함은 데이터 분석의 양에 크게 기여한다. '사건(Vorgang)'은 경찰 활동과 관련하여 특정 사람, 사물 또는 기타 경찰 조치의 대상에 대해 보관되는 모든 문서를 포함한다. 사건 처리 시스템에서 경찰은 개별 사건의 특정 경찰 업무 및 사건 처리에 필요한 데이터를 기록한다. 특히 도로 교통 사고와 관련된 내용을 포함하여 혐의, 수사 보고서 및 메모가 기록된다. 또한 이 시스템에는 신고를 하거나 정보를 제공한 사람, 목격자, 사고 관련자, 형사소송법상 용의자나 피고인이 아닌 사람 또는 경찰법상 책임이 있는 사람에 대한 데이터도 포함되어 있다. 헤센주에서는 이 데이터가 분석 플랫폼에 자동으로 통합된다.[352] 해당 조항들은 일정한 사람들이 범죄를 저지를 수 있다는 가정을 불러일으키거나, 범죄혐의가 있는 사람과 이와 특별한 연관성이 있는 사람의 데이터와 그렇지 않은 사람의 데이터를 구분하지 않는다. 결과적으로 해당 조항은 경찰수사의 대상과 전혀 관련없는 사람들의 데이터까지 광범위하게 포함할 수 있도록 허용하고 있다.[353]

ii. 데이터 분석 및 평가를 위한 방법 제한 여부

입법자가 특정 위험에 앞서 자동화된 데이터 분석 또는 평가의 침입 강도를 낮추기 위해 이를 활용하고자 한다면, 자동화된 데이터 분석 또는 평가 방법에 대한

349) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 133.
350) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 137.
351) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 138.
352) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 134.
353) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 125.

제한적 요건을 설정하고 그 기본적인 특징을 법률 자체에 규정해야 한다.[354] 자가 학습 시스템의 사용은 법률에 의해 명시적으로 배제되어야 하며, 입법자는 자동화의 정도를 제한하기 위한 근본적인 조치를 취해야 한다. 경찰 당국이 데이터 분석 또는 평가를 자동화된 형태의 단순한 데이터 매칭을 넘어서는 방식으로 구성하는 것만으로는 충분하지 않으며, 특히 매칭 결과를 다른 데이터세트와 연결하기 위해 반복되는 매칭 단계가 자동으로 수행되지 않도록 하는 것만으로는 충분하지 않다. 오히려 매칭 옵션에 대한 제한을 법 자체에 명시해야 할 것이다.[355]

해당 조항은 자동화된 데이터 분석 및 평가를 위한 매우 광범위한 방법의 사용을 허용하고 있다. 데이터 집합을 데이터 분석 또는 평가에 자동으로 통합하는 문제도 특별히 규정되어 있지 않다.[356] 입법자는 데이터 분석 및 평가의 방법에 제한을 두지 않으므로, 인공지능 사용을 포함한 데이터 마이닝도 허용한다. 더구나 여기에는 개방형 검색 역시 포함된다.

데이터 분석 또는 평가는 다량의 데이터에서 단순히 통계적 이상 징후만을 발견하는 것을 목적으로 할 수 있으며, 이를 통해 다른 자동화된 애플리케이션의 도움을 받아 추가 결론을 도출할 수도 있다. 이러한 검색결과에서 핵심은 기계적 평가인데, 여기에서 예측 치안(predictive policing)은 결국 개인의 위험 가능성을 예측하는 것까지 포함한다. 따라서 이는 데이터 분석 또는 평가를 통해 다른 방법으로는 획득할 수 없는 새로운 개인 관련 데이터를 생성할 수 있음을 의미한다. 이렇게 새로운 지식을 얻을 수 있는 잠재적 가능성의 범위가 넓음에도 불구하고 그러한 (데이터 분석 또는 평가를) 사용에 대한 기본권 제약을 정당화할 수 있는 규율이 수반되어 있지 않다.[357] 이로부터, 자동화된 분석을 허용하기 위한 구체적 위험 또는 구체화된 위험이 있는 상황이 이미 존재한다는 점을 추론할 수는 없고 제약의 근거를 한정적으로 구체화했다고 하기에는 부족하다.

---

354) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 120.
355) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 121.
356) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 128.
357) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 140.

심판대상 조항들은「형사소송법」제100a조 제2항에서 명시된 범죄행위를 예방하기 위한 목적으로 데이터 분석 또는 평가를 허용하는 한, 그 (기본권) 제약의 비중(제한의 중대성)에 비추어 볼 때, 제약의 근거가 광범위하여 비례성을 상실하였으며 따라서 위헌이다.

iii. 실무상 개별사건에 대한 검토

두 심판대상 조항은 개별사건마다 정당화 근거가 있어야 한다는 추가적 기준이 있지만, 여기에 구체화된 실질적 규정을 담고 있지 않으므로 헌법상 요구되는 제한의 정당화 기준에는 미치지 못한다.[358] 물론 구두변론에서 헤센주 경찰의 실무에서는 '개별사건'에 대한 검토가 요건으로 인식되고 또 적용되는, 다소 엄격한 요건(Konzept)이 제시된 바 있었다. 이에 따르면, 데이터 분석은 일관되게 이미 저질러진 범죄행위와 연결되어 있거나, 적어도 사실관계를 통해 범죄행위가 이미 저질러졌다는 혐의와 연결된 경우 이루어지며, 미래에 대한 예측도 이에 근거하여 이루어진다. 이러한 콘셉트 아래 자동화된 데이터 분석을 수행하려면 다음과 같은 두 가지 조건이 필요하다. 첫째,「형사소송법」제100a조 제2항에 명시된 범죄행위 중 하나가 과거에 저질러졌다는 것, 둘째, 이러한 정황을 근거로 향후 유사한 범죄행위가 추가로 발생할 것으로 예상할 수 있어야 한다는 것이 그것이다.[359]

헤센주 실무에서 적용되는 구체화된 제도설계와 관계없이, 대상 법률조항은 최소한 처음부터 구체화된 위험과 그러한 위험을 방지하는 데 적합한 데이터를 식별하는 것을 목표로 하지 않았기 때문에, 이미 헌법적 요건을 충족하지 못한다. 심판대상 조항에 따라 분석되는 데이터 종류와 방법을 광범위하게 허용하는 문제를 개선하기 위해 실제 적용한다고 언급한 위의 요건들의 명확한 규정이 필요할 것이다.

iv. 적절한 통제장치의 존재 여부

비례의 원칙은 투명성, 개별 법적 보호 및 감독 통제에 대한 요구사항도 제기한

358) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 157.
359) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 159.

다. 특히, 적절한 통제조직을 구성하는 것은 매우 중요하다. 개인정보를 보호하기 위한 목적구속성의 원칙 역시 제한의 효과는 조직적, 기술적 예방 조치를 통해서만 달성할 수 있으며, 헌법적으로 허용 가능한 방식으로 기본권 침해의 위험성을 줄이려면 구체적으로 자세히 규제되어야 한다.[360] 목적구속성을 보장하는 기술적·조직적 안전장치는 예를 들어 다양한 처리 목적에 따른 데이터세트의 기술적 분리 또는 데이터세트에 대한 접근 권한의 목적별 분배로 구성될 수 있다.[361] 예를 들어 단계적 통제개념에 따라 독립적인 데이터 보호책임자와 공식적인 데이터 보호책임자로 나눌 수 있으며, 무작위 샘플링 절차로 규제할 수도 있다. 효과적인 통제를 위해서는 특정 범죄예방을 위해서 자동화된 데이터 분석 앱을 사용하여 특정 데이터세트를 분석하는 이유에 대하여 공식화된 설명을 제공하는 것이 필수적이다. 보다 복잡한 형태의 자동화된 데이터 분석을 허용하는 소프트웨어를 사용할 경우, 이와 관련된 특정 오류 발생에 대한 예방책도 필요하며, 사용되는 소프트웨어의 개발을 위한 모니터링에 관한 법적 규정을 포함할 수 있다.[362]

그러나 심판대상 법률에는 이에 대한 어떠한 조항도 포함되어 있지 않다. 관련 조직 및 기술적 예방 조치에 대한 표준화도 없다.[363] 헤센주「공공안전법」제20 IV조 및「일반데이터보호명령」과 함부르크「경찰데이터법」제56조는 목적구속성 원칙을 준수하기 위한 조직적 및 기술적 예방 조치를 의무화하고 있다. 그러나 이는 자동화된 데이터 분석 또는 평가를 위한 데이터 액세스를 충분히 명확하고 구체적인 방식으로 제한하지는 않았기 때문에, 데이터의 자동화된 분석이 가능한 앱의 사용을 위해서는 더 자세히 규제되어야 할 것이다.[364] 또한 헤센주 정부는 특별한 역할과 권리 개념에 따라 데이터 분석 플랫폼에 대한 접근 권한을 다양한 수준

360) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 139.
361) BeckOK Polizei- und Ordnungsrecht Hessen/Bäuerle HSOG 제20조 Rn. 105.
362) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 109.
363) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 130.
364) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 140.

으로 분류해서 허용한다고 반복해서 언급했으나, 이러한 개념은 원칙적으로 목적 제한의 기술적 및 조직적 보호에 적합할 수 있지만 이 역시 표준화되지 않았고, 공개적으로 접근할 수 있는 방식으로 추상적인 일반 법규정으로 문서화하지 않았다.[365]

또한 현재 무제한적 데이터 평가기술이 (아직) 사용할 수 없다는 점을 근거로, 문제되는 권한들이 헌법적으로 적절히 제한되고 있다고 할 수도 없다. 향후 기술 발전의 결과로 (데이터 평가) 기능의 확대가 이루어질 수 있다 하더라도, 헌법적 요건은 원칙적으로 이미 법적으로 형성된 (기본권) 제약의 가능성에 근거한다.[366]

다. 소결

독일연방헌법재판소는「헤센주 공공안전 및 질서법(HSOG)」제25a조 제1항 제1문 및「함부르크주 경찰 데이터 처리에 관한 법률」제49조 제1항 제1문이 헌법에 위반된다고 결정했다. 해당 조항은 경찰이 데이터 분석 또는 데이터 평가의 일환으로 자동화된 애플리케이션을 통해 저장된 개인 관련 데이터를 추가 처리할 수 있는 권한을 부여한다. 이 조항들은 권리의 제약을 정당화할 수 있는 충분한 제한의 한계(ausreichende Eingiffsschwelle)를 마련하지 않았기 때문에, 좁은 의미의 비례성 원칙의 요건을 충족하지 않는다. 해당 조항은 개인정보자기결정권으로 표현되는「독일 기본법」제1조 제1항 및 제2조 제1항의 일반적 인격권을 침해한다. 다만「헤센주 공공안전 및 질서법」제25a조 제1항 제1문은 새로운 규정으로 개정될 때까지 계속 적용되지만 늦어도 2023년 9월 30일까지만 잠정적으로 적용된다. 단, 해당 조항의 잠정적용을 위해서는 영향을 받은 기본권을 보호하기 위한 일정한 제한적 기준을 부과할 필요가 있다.

5. 개정된「헤센주법」에 따른 데이터 분석을 위한 자동화된 앱 이용의 조건

가.「헤센주 공공안전 및 질서법」제25조 개정

2023년 7월 12일「헤센주 공공안전법」은 독일연방헌법재판소의 결정에 따라

365) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 140.
366) BVerfG Urt. 16.02.2023.-1BvR1547/19, 1BvR2634/20, Rn. 149.

자동화된 데이터 분석 애플리케이션을 사용할 수 있는 상황과 사용 가능한 데이터의 유형을 구체적으로 언급하는 등, 기본권 침해를 최소화하는 방안으로 개정하였다.

먼저 동법 제25조 제1항에서 데이터 분석을 위한 자동화된 애플리케이션은 경찰 당국이 가능한 한 신뢰할 수 있는 사실적 근거하여 아래의 구체적 규정에 따라 업무를 수행하고 평가, 예측 및 결정을 내릴 수 있도록 설계된 기술적 도구임을 명시하고,[367] 항상 구체적이고 목표 지향적 검색 기준에 따라 수행되며[368] 수동으로 작동하고 사람이 정의한 분석 및 처리 단계의 순서 및 규칙에 따라 실행됨을 명시하고 있다.[369] 또한 방법상 제한으로 인터넷 서비스에 대한 직접 연결은 제외됨을 밝힌다.[370]

나. 자동화된 데이터 분석도구의 사용 가능한 상황과 데이터 유형

1) 데이터 분석을 위한 자동화된 애플리케이션 사용 가능한 상황

① 구체적 위험에 대한 방어

경찰 당국은 연방 또는 주의 존립 또는 안전, 사람의 생명, 신체 또는 자유 또는 공익을 위해 보존이 요구되는 중요한 가치 있는 사물에 대한 위험방지를 위해 필요한 경우, 그와 동등한 환경피해가 예상되어 이러한 위험에 대한 방어가 필요한 경우, 데이터 분석을 위해 자동화된 애플리케이션을 통해 저장된 개인 데이터를 추가로 처리할 수 있다.[371]

② 구체화된 위험의 방어

경찰 당국은 사실에 입각한 증거가 상당히 중요한 범죄 발생이 예측 가능한 기간 내 그 성격상 구체적인 방식으로 저질러질 것이라는 가정을 정당화하는 경우,

367) 「헤센주 공공안전법」 제25조 제1항 제3문.
368) 「헤센주 공공안전법」 제25조 제1항 제4문.
369) 「헤센주 공공안전법」 제25조 제1항 제5문.
370) 「헤센주 공공안전법」 제25조 제1항 제6문.
371) 「헤센주 공공안전법」 제25조 제2항 제1문 제1호.

그리고 이것이 이러한 범죄를 예방하기 위해 필요한 경우 데이터 분석을 위해 자동화된 애플리케이션을 통해 저장된 개인 데이터를 추가로 처리할 수 있다.[372)]

③ 범죄의 예방조치

경찰 당국은 법익침해의 증거가 매우 중대하고 심각한 범죄가 저질러질 것이라는 가정을 정당화하고 그러한 범죄를 예방하기 위해 추가 처리가 필요한 경우 데이터 분석을 위해 자동화된 애플리케이션을 통해 저장된 개인 데이터를 추가로 처리할 수 있다.[373)]

2) 자동화된 데이터 분석 애플리케이션으로 사용 가능한 데이터의 유형

자동화된 데이터 분석 애플리케이션을 사용하여 사건처리 데이터, 경찰 정보시스템 데이터, 교통 데이터, 통신데이터, 증거 데이터 및 경찰 정보교환의 데이터(각 데이터 종류에 대한 특성)를 결합할 수 있다. 별도로 관리되는 국가의 등록부에 있는 심문 목적의 자료기록과 인터넷에서 발췌하여 개별적으로 저장한 데이터 기록도 포함될 수 있다. 데이터 분석을 위하여 자동화된 앱을 사용하는 요건 중, 앞에서 언급한 제2항 제1문 제3호의 범죄의 예방을 위한 조치를 수행할 때 통신데이터는 포함되어서는 안 된다.[374)]

다. 자동화된 데이터 분석 도구 사용의 원칙

1) 개인정보 분류와 표지에 대한 구상

자동화된 데이터 분석을 사용할 때에는 동법 제20조 제1항[375)] 및 제2항[376)]에 규

372) 「헤센주 공공안전법」 제25조 제2항 제1문 제2호.

373) 「헤센주 공공안전법」 제25조 제2항 제1문 제3호.

374) 「헤센주 공공안전법」 제25조 제2항 제2문.

375) 제20조 제1항 보안 및 경찰 당국은 각각의 데이터 수집 규정을 고려하여 자체적으로 수집한 개인 데이터를 추가로 처리할 수 있다.
1. 동일한 업무 수행을 위해 그리고
2. 동일한 법적 이익 또는 기타 권리의 보호 또는 동일한 형사 범죄 또는 행정 범죄의 예방을 위해.
제1항은 추가 처리를 위해 저장 목적을 고려해야 한다는 조건하에 이전에 수집되지

정된 정보처리의 원칙이 적용된다.[377] 이는 공표된 행정 규칙을 통해 보장되어야 하며,[378] 이러한 규정에는 기능 및 권리 개념과 개인정보의 분류와 표지에 대한 구상이 포함되어야 한다.[379] 기능과 권리 개념은 현상의 영역에 따라 객관적으로 제한된 접근 권한을 목적에 따라 분배하는 것을 규제한다. 이러한 구상의 기준은 보호해야 할 법익의 중요성과 경찰개입의 긴급성 정도이다. 더 많은 처리 권한이 부여된 사람은 더 적은 양의 데이터에 접근할 수 있고, 더 적은 처리 권한이 부여된 사람은 더 많은 양의 데이터에 접근할 수 있다는 원칙에 따라 설계되어야 한다. 그것은 최소한 각각의 현상 영역, 가중치와 상호 관계를 기술하고 각 권한 범위와 관련하여 승인된 사람의 법적 지위, 기능 및 특정 요건을 정의해야 한다.[380]

개인정보의 분류 및 표지 구상은 인과관계 및 기본권과의 관련성을 기준으로 자동화된 분석에 어떤 개인정보가 포함될 수 있는지를 규제한다. 개인정보 분류와 표지에 대한 구상의 기준은 분석의 영향을 받는 사람과 각 현상 영역(인과관계)의 사실적 연관성이다. 인과적 맥락이 중요할수록 자동화된 데이터 분석은 더 복잡하게 행해질 수 있고, 인과적 맥락이 덜 중요할수록 더 단순해야 한다는 원칙을 따른다. 그 출발점은 유죄 판결을 받은 사람, 피고인, 피의자 및 기타 원인 제공자와

않은 개인 데이터에도 동일하게 적용된다. 제15조 제4항 또는 제15c항에 따른 조치에서 얻은 개인 데이터를 추가로 처리하려면 해당 조항의 의미 내에서 위험 또는 위험상황이 존재해야 한다.

376) 제20조 제2항 보안 및 경찰 당국은 업무를 수행하기 위해 각 데이터 수집 규정을 고려하여 다음과 같은 경우 수집된 목적 이외의 목적으로 개인 데이터를 추가로 처리할 수 있다.
1. 최소한 a) 비교적 심각한 형사범죄 또는 행정 규제 위반을 방지하거나 또는 b) 그에 준하는 중대한 법적 이익 또는 기타 권리가 보호되는 경우라야 한다.
2. 개별 사건에 대한 구체적인 조사 접근 방식이 있는 경우
a) 그러한 형사 범죄 또는 행정 규제 위반을 방지하기 위해 또는
b) 예측 가능한 기간 내에 발생할 수 있는 위험을 방지하기 위해 최소한 그에 준하는 중대한 법적 이익 또는 기타 권리에 대한 임박한 위험을 피하기 위한 경우.

377)「헤센주 공공안전법」제25조 제3항 제1문.

378)「헤센주 공공안전법」제25조 제3항 제2문.

379)「헤센주 공공안전법」제25조 제3항 제3문.

380)「헤센주 공공안전법」제25조

그 접촉자 및 관련 없는 사람을 구분하는 것이다. 범죄에 연루되지 않은 사람을 보호하기 위해 그들의 개인 사건처리정보(Vorgangsdaten)는 자동화된 데이터 분석에 포함되지 않는다.[381] 자세한 사항은 행정 법규에 의해 규제되며, 특히 교신데이터(Verkehrsdaten)의 경우 분석 플랫폼에 2년의 정기 저장 기간을 제공해야 한다.[382] 데이터 분석을 위해 자동화된 애플리케이션에는 주거에 대한 감시 및 온라인 검색을 통해 얻은 개인 데이터가 포함되지 않아야 한다.

2) 제한 강도의 감소 목표

데이터 분석을 위해 자동화된 애플리케이션을 사용할 수 있는 상황에서의 보호법익과 제한의 임계치(Eingriffsschwelle)에 따른 다양한 상황들을 고려하여 분석 중인 데이터의 양을 줄이고, 각 경우에 사용되는 분석 방법의 적절성을 보장하며, 무고한 사람에 대한 최대한의 보호(제한 강도의 기능적 감소)라는 최우선 목표에 기반해야 한다.[383]

앞서 언급한 개인정보 분류와 표지의 구상 기준은 개인정보 수집 시 개인정보자기결정권에 대한 제한의 심각성(기본권과의 관련성)에 따라 개인 데이터를 분류하는 것이다. 기본권에 대한 심각한 침해로 인한 데이터의 제한적 활용성을 고려한 추상적 규정을 만들어야 하며, 이러한 규정이 실제로 효력을 발휘할 수 있도록 기술적·조직적 예방조치를 취해야 한다.

---

381) 경찰의 개별 데이터베이스 내에는 다양한 형태의 저장소가 있다. 연방 주의 데이터베이스에서는 일반적으로 모든 경찰 활동(예: 신원 확인 또는 불만 사항)에 대한 항목이 기록되는 사건경과데이터(Vorgangsdaten)와 범죄 조사가 저장되는 이른바 형사 경찰 수집과 같은 특수 파일이 구분된다. Polizeidatenbanken, “Datenbanken der Polizei”, https://www.polizeidatenbanken.de/polizei-datenbanken/datenbanken-der-polizei/ (2024. 10. 3. 최종 방문).

382) 「헤센주 공공안전법」 제25조 제3항.

383) 「헤센주 공공안전법」 제25조 제3항 제4문.

라. 조직적·절차적 통제장치

1) 자동화된 애플리케이션에 대한 접근규제

데이터 분석을 위해 자동화된 애플리케이션에 대한 접근이 규제된다. 앱에 대한 접근 사실은 지속적으로 기록되며, 데이터 분석을 위해 자동화된 애플리케이션의 사용에 대하여서 각 사용자에게 설명의무를 부과한다. 자동화된 데이터 분석에 대한 애플리케이션 사용의 정당성은 자기보증 및 후속 통제의 목적으로 사용된다. 접근 제어의 세부 사항과 정당화에 필요한 내용은 행정법규로 규정해야 하며, 정보보호책임자에게 무작위 점검을 수행할 권한을 부여한다.[384)]

2) 정보보호 조직

데이터 분석을 위해 자동화된 애플리케이션의 설정 및 중대한 변경은 기관의 장 또는 기관의 장으로부터 권한을 위임받은 직원이 행한다. 헤센주 데이터보호 및 정보 자유위원회는 설립 또는 중대한 변경에 앞서 헤센주 데이터 보호 및 정보 자유 위원회 위원과 협의해야 하며, 임박한 위험이 발생할 경우 그 이후에 협의해야 한다. 그 이외의 헤센주 데이터 보호 및 정보 자유 위원회의 의무와 권한은 영향을 받지 않는다.[385)]

제 3 절 프랑스 헌법재판소 결정의 시사점

1. 의의

프랑스는 2023년 5월 2024년 파리 올림픽과 패럴림픽 개최를 앞두고 테러행위 등으로부터 안전을 확보하기 위한 목적에서 인공지능 기반 감시카메라의 사용을 실험적으로 허용하는 입법을 도입하였다. 또한 본 법률의 제정 과정에서 좌파정당 소속 하원의원들이 관련 규정에 대한 사전적 위헌법률심판을 헌법재판소에 청구

384) 「헤센주 공공안전법」 제25조 제4항.
385) 「헤센주 공공안전법」 제25조 제5항.

하였고, 헌법재판소는 이에 대하여 조건부 합헌 결정(일종의 한정합헌결정)을 한 바 있다. 현재 국내에서 지능형 CCTV가 광범위하게 사용되고 있고 앞으로 더욱 그럴 예정이지만, 국민의 기본권 제한 가능성에도 불구하고 그 활용의 법적 근거가 불충분한 상황에서 헌법재판소의 결정을 통해 합헌성을 인정받은 프랑스의 관련 입법이 시사하는 바가 적지 않다. 이에 아래에서는 프랑스의 해당 입법 및 헌법재판소 결정 등과 관련된 내용을 살펴보기로 한다.

2. 입법의 배경 및 과정

2017년 7월 31일 2024년 하계 올림픽과 패럴림픽이 프랑스 파리에서 개최되는 것으로 결정되어 2024년 7월 26일부터 8월 11일까지는 올림픽이 개최되었고, 8월 28일부터 9월 8일까지 패럴림픽이 개최되었다. 특히 올림픽의 경우 프랑스 파리에서 개최되는 세 번째 올림픽이자, 1924년 하계 올림픽 이후 100년 만에 개최되었다. 그런데 프랑스에서는 2015년 1월 7일 Charlie Hebdo 총격 테러 사건을 시작으로, 특히 파리를 중심으로 대형 테러 사건이 다수 발생한 바 있다. 또한 파리 올림픽 조직위원회는 2024년 파리 올림픽을 친환경 올림픽으로 개최하기로 하면서, 개막식을 주경기장이 아닌 센강과 그 주변에서 진행하기도 하였다.

이러한 배경에서 올림픽 개최 기간 중의 안전에 대한 우려가 커지면서 CCTV나 드론 영상 촬영 장치 등을 통해 수집한 영상을 인공지능 알고리즘으로 처리하여 안전상의 위험에 대응할 필요성이 커지게 되었다. 이에 「2024년 올림픽과 패럴림픽 및 기타 규정에 관한 2023년 5월 19일 제2023-380호 법률」이 제정되었고,[386] 동법률 제10조가 테러행위 또는 사람의 안전에 대한 중대한 침해의 위험에 노출된 스포츠, 레크리에이션 또는 문화 행사의 안전을 보장하기 위한 목적에서만 해당 행사가 개최되는 장소와 그 주변 장소 등에서 CCTV나 드론 등을 활용한 영상에 대하여 인공지능 알고리즘 처리를 허용하는 규정을 두었다.

386) LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions.

이 법률의 제정은 우선, 2022년 12월 22일 정부가 해당 법률안을 발의하였고, 2023년에 들어와서 상원과 국민의회에서 심사를 거치면서 본격적으로 시작되었다. 그 과정에서 시민단체 등에서 사생활에 관한 권리와 표현의 자유에 대한 침해 가능성을 우려하기도 하였다.[387] 그러나 2023년 4월 17일 좌파정당 소속 국민의회의원들이 관련 규정에 대하여 프랑스 제5공화국 헌법 제61조 제2항이 규정하고 있는 사전적 위헌법률심판을 헌법재판소에 청구하였다. 이에 대하여 헌법재판소는 같은 해 5월 17일 해당 규정이 일정한 해석상 한계 내에서 합헌임을 선언하는 조건부 합헌 결정, 우리나라의 한정합헌과 유사한 결정을 하였다. 이에 본 규정이 포함된 「2024년 올림픽과 패럴림픽 및 기타 규정에 관한 2023년 5월 19일 제2023-380호 법률」이 해당 일에 유효하게 제정되었고, 5월 20일 관보에 게재됨으로써 익일인 5월 21일 발효되었다.[388]

3. 법률 규정의 주요 내용

프랑스에서 「2024년 올림픽과 패럴림픽 및 기타 규정에 관한 2023년 5월 19일 제2023-380호 법률」이 제정되기 이전에도 비디오감시(vidéosurveillance)와 관련된 법률 규정은 존재하였다. 「대내안전법전(Code de la sécurité intérieur)」 제L.252-1조가 비디오보호 시스템의 설치, 즉 고정형 영상정보처리기기에 관한 규정을 두고 있었고, 또한 동법전 제L.242-1조 이하에서는 비행체(드론)에 설치된 카메라의 사용에 관한 규정을 두고 있었다. 「2024년 올림픽과 패럴림픽 및 기타 규정에 관한 2023년 5월 19일 제2023-380호 법률」 제10조는 이러한 CCTV와 드론을 활용한 비디오감시 또는 감시카메라를 통해 수집한 영상정보에 대하여

387) Amnesty(2024. 4. 14), "JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème", https://www.amnesty.fr/liberte-d-expression/actualites/pourquoi-la-video surveillance-algorithmique-pose-probleme-cameras-technologies (2024. 10. 3. 최종 방문).

388) C. C., Décision n° 2023-850 DC du 17 mai 2023.

인공지능 알고리즘을 활용하여 선별관제 시스템 구축의 법적 근거를 마련한 것이다.

동법률 제10조는 이러한 알고리즘 비디오감시의 법적 근거를 영구적으로 규정한 것은 아니며, 법률 시행일로부터 2025년 3월 31일까지 시기를 정하는 실험법률의 형식을 취하였다. 이는 법률의 효력 측면에서 우리나라의 한시법과 유사하다고 하겠다. 이 기간은 올림픽과 패럴림픽 기간을 목표로 한 것은 맞지만, 그 기간이 1년이 넘는 기간이며, 그동안 프랑스에서는 2023년 9월 8일부터 10월 28일까지 럭비 월드컵이 개최되기도 하였다.

실험법률이 적용되는 2023년 5월 21일부터 2025년 3월 31일까지는 테러행위 또는 사람의 안전에 대한 중대한 침해의 위험에 노출된 스포츠, 레크리에이션 또는 문화 행사의 안전을 보장하기 위한 목적에서만 해당 행사가 개최되는 장소와 그 주변 장소 등에서 CCTV나 드론 등을 활용한 영상에 대하여 인공지능 알고리즘 처리가 허용되게 되었다. 감시 대상은 행사 주최 장소와 그 주변, 대중교통의 차량 내부와 통행지, 이들 차량에 제공되는 도로이다. 해당 영상에 대한 알고리즘 처리의 목적은 실시간으로 위험을 사전에 감지하여 국가 경찰, 국가 헌병대, 소방구조대, 지방경찰, 철도공사 및 파리지역대중교통공사 내부안전담당조직이 적절한 조치를 하도록 하는 것이 유일하다.

기타 이러한 영상을 알고리즘 처리하는 것에 대해서는 적절한 수단을 이용해서 사전에 대중에게 알리도록 하고 있다. 그리고 생체인식 시스템을 활용하지는 못하도록 하고 있으며, 안면인식 기술의 활용도 금지하고, 다른 개인정보와의 결합 등도 허용되지 않는다. 따라서 허용되는 선별관제 시스템은 무기, 차량 등의 물체 출현, 금지 구역 내에 출입하는 사람, 과도하게 밀집되어 있거나 무질서 또는 반항적인 움직임을 드러내는 군중의 이동 등이다.

이러한 알고리즘 비디오감시의 활용은 데빠흐트멍 단위에서는 국가의 대표, 즉 préfet의 허가가 필요하고, 파리에서는 경시청장의 허가가 필요하다. 다만, 이러한 허가는 알고리즘 처리가 추구하는 목적에 비례하는 경우에만 가능하다. 또한 허가 내용에는 데이터 관리자 및 그 구현과 관련된 서비스, 관련 스포츠 및 레크리에이션 또는 문화 행사와 그 목적과 관련된 처리를 실행하는 이유와 목적 범위

내에서 처리 실행에 관련된 지리적 관할의 경계, 정보주체의 권리에 대해 고지하는 방법, 허가 기간 등이 포함되어야 한다. 이때 허가 기간은 1개월을 초과할 수 없으나 갱신이 가능하다. 이후 préfet나 파리 경시청장은 영상정보 처리와 관련된 보고를 매주 받고, 국가정보자유위원회(Commission nationale de l'informatique et des libertés: la CNIL)에 대한 보고서 제출 등의 의무가 부여되며, 허가의 철회 권한도 가진다.

한편, 선별관제를 통한 감지의 품질 향상을 위한 영상 샘플에 대해서 최대 12개월까지 인공지능 학습데이터로 활용할 수 있는 근거도 마련하고 있다. 그러나 이러한 영상은 실험기간이 종료되면 폐기하도록 규정되어 있다. la CNIL은 이러한 실험 시행 조건에 대해서 3개월마다 통보를 받도록 하고, 정부는 2024년 12월 31일까지 실험 시행에 대한 평가보고서를 의회에 제출하여야 한다. 의회의 검토를 거친 평가보고서는 공개되도록 되어 있다.

4. 헌법재판소의 결정

좌파정당 소속 국민의회의원들이 관련 규정에 대한 사전적 위헌법률심판을 청구한 이유는 올림픽 및 패럴림픽 기간에 비하여 실험법률에 따라 알고리즘 비디오감시를 허용하는 기간이 너무 길다는 점, 알고리즘 처리의 대상인 사건이 정의되지 못한 점, 왕래의 자유·시위할 권리·표현의 자유·사생활을 존중받을 권리 등이 침해된다는 점, 알고리즘을 활용한 영상의 처리가 차별을 배제하지 못하고 인간의 안전과 존엄을 침해한다는 점 등이었다.

헌법재판소는 이들의 주장을 기각하고 해당 규정을 합헌으로 선언하였다. 다만, CCTV나 드론으로 수집한 영상을 알고리즘 처리하는 데 대한 허가와 관련하여 préfet나 파리 경시청장이 "허가를 정당화하는 요건이 더 이상 충족되지 않음을 확인하는 경우에는 해당 허가를 언제든지 중단하거나 종료할 수 있다"라고 규정하고 있기 때문에, 이러한 규정은 사생활을 존중받을 권리를 침해하지 않고서는 해당 허가를 정당화하는 요건이 더 이상 충족되지 않는 경우에 préfet에게 허가

를 즉시 중단할 의무가 있다는 것 외의 해석은 가능하지 않다고 하였다. 해당 규정에 대한 해석상의 한계 내에서 합헌성을 인정한 일종의 한정합헌결정으로 볼 수 있으며, 그 취지는 허가 요건이 불충분할 때는 préfet가 반드시 해당 허가를 철회할 수 있도록 하는 기속의무를 부과한 것이다.

제5장 결 론

제1절 요 약

국가는 감시를 통해서 국민을 안전하게 보호하고 사회 질서를 유지할 수 있다. 그러나 필요한 수준을 넘어 광범위하게 개인에 관한 데이터를 수집하고 처리하면서 전반적이고 체계적인 감시 체제를 구축하는 것은 분명히 경계해야 한다. 이는 감시가 가지는 이중적 의미와 관계된 것으로서, M. Foucault는 감시를 통한 권력과 통치를 언급하였다. 정보사회의 도래와 함께 본격적으로 문제가 된 감시 체제의 구축과 기본권 침해의 위험은 최근 국가가 인공지능을 활용하여 개인의 일상적인 활동을 적나라하게 추적하고, 정교하고 정확한 분석과 평가를 할 수 있게 되면서 획기적인 변화를 맞이하였다.

국가는 매우 다양하고 점점 복잡해지는 공적 과제를 효율적이고 신속하게 해결하기 위해서 인공지능을 비롯한 지능정보기술을 활용해야 한다. 앞으로도 국가가 국민의 일상생활과 활동을 규율하기 위하여 법 집행에 인공지능을 활용하는 비중은 점점 커지고 그 수준도 높아질 것이다. 국민에 대한 국가의 감시 역량이 극대화하면서 권력의 불균형으로 이어지고 다양한 기본권 침해 가능성이 크게 증가할 수 있는 조건이다.

인공지능을 이용한 감시는 가장 직접적으로 개인정보자기결정권을 비롯하여 주거의 비밀, 사생활의 비밀, 통신의 비밀과 같이 개인의 사사로운 영역을 보호하기 위한 기본권 보장에 결정적인 악영향을 미칠 수 있다. 또한 국가 후견주의를 강화하여 국민이 자유롭게 자아를 실현할 기회를 박탈하며, 은밀하고 세세하게 국민을 조정함으로써 인간의 존엄과 가치, 일반적 행동의 자유를 실질적으로 침해할 수 있다. 편향성과 오류를 내포한 인공지능의 한계에도 불구하고 인공지능을 활용한 감시를 지속하면서 그에 따라 도출된 결론에 기초하여 개인을 평가하고 의사결정

을 한다면 공적 과제 수행이 정확성과 객관성을 상실하여 불합리한 차별을 강화할 수 있다. 이 밖에도 시간적, 공간적 제약이 없이 이루어지는 광범위하고 정밀한 인공지능 감시는 자기검열과 위축 효과를 야기함으로써 표현의 자유를 침해하고 민주주의 발전을 저해할 수 있다. 특히 인공지능을 활용한 감시는 익명성 보장을 어렵게 하고, 감시 활동에 대한 알 권리 보장도 쉽지 않다는 점에서 더욱 그러하다.

국가가 계속해서 증대하는 공적 과제를 신속하고 효율적으로 수행하기 위해서는 인공지능을 활용하여 대량의 데이터를 처리함으로써 개인과 사회에 대한 평가와 분석, 예측과 조정을 할 수 있어야 한다. 이 과정에서 감시 체제 구축 가능성이 커지는 것은 자연스러운 흐름이다. 중요한 것은 인공지능 활용에 따른 다양한 이점을 최대한으로 누릴 수 있도록 하되 사생활의 이익, 민주주의 및 법치주의의 가치와 조화할 수 있도록 신중한 균형을 모색하는 것이다. 인공지능의 고유한 특성을 염두에 두면서 그 활용이 법치주의가 요구하는 한계를 준수하고 민주적인 통제의 범위 내에서 이루어지도록 관련 규범을 정비해야 한다.

이를 위해서는 인공지능 활용의 구체적인 법적 근거를 마련해야 한다. 인공지능을 활용한 공권력 작용에 대한 기존의 법제를 전반적으로 검토하여 인공지능 환경에 맞도록 수정하는 한편 인공지능의 고유한 특징 및 위험에 부합하는 규범 체계를 새롭게 정립하는 것이다. 또한 국가가 필요한 범위 내에서 인공지능을 활용하여 감시하는 경우 그러한 활동이 투명성과 객관성, 정확성을 확보할 수 있는 장치를 포함하도록 해야 한다. 감시 대상자에게 인공지능 활용 감시에 관한 정보를 제공하고, 정보에 대한 실질적 접근 가능성을 보장해야 하며, 인공지능의 편향성과 차별 위험을 방지하기 위해 데이터의 품질을 보장하기 위한 장치나 제도를 반영해야 한다. 나아가 인공지능을 활용하기에 앞서 사전에 적합성 및 위험성을 평가하고, 인공지능을 활용하는 전 단계에 걸쳐 감독할 수 있도록 국가기관 내외부에 체계적인 거버넌스를 구축해야 한다. 국가의 인공지능 활용 감시를 중립적이고 객관적으로 평가, 감독할 수 있는 제도를 마련하는 한편, 사전에 당사자가 인공지능 활용 감시 및 그에 따른 결정에 참여할 수 있는 절차를 보장하고 부당한 감시

와 결정에 대해서는 간편하고 쉽게 권리구제를 도모할 수 있도록 해야 한다.

인공지능 기반 감시 시스템은 개인의 위치, 행동, 이력, 통신 등에 대해 방대한 데이터를 수집하고 분석함으로써 사생활 영역에 대한 보호를 심각하게 침해할 수 있다. 감시 체제의 투명성과 공정성, 보안성이 갖춰지지 않는다면 이러한 위험은 더 분명하다. 인공지능이 우리 사회의 안전과 지속 가능한 발전을 뒷받침하는 핵심적인 기술로서 더 높은 단계로 나아가려면 기술이 기본권과 민주주의, 법치주의와 같은 헌법의 가치를 준수하는 가운데 활용될 것이라는 신뢰를 확보해야 한다. 인공지능이 가진 많은 이점은 방대하고 정밀한 감시 체제 구축에 따른 기본권 침해 가능성을 최소화하기 위한 규범적 노력을 전제로 할 때 비로소 빛을 발할 수 있을 것이다.

제2절 정책적 제언

인공지능 감시 역시 인공지능이 기반이 되는 것이므로 우선은 인공지능 자체에 대한 안전성, 윤리·신뢰성 확보 차원의 적정한 규제가 도입되어야 할 것이다. 그리고 그것이 입법을 통한 규제라고 할 때에는 몇 가지 고려 사항이 있다. 첫째로 인공지능 기술의 성장 가능성을 고려해야 한다. 인공지능은 분명 인간의 한계를 극복함으로써 경제적·사회적 혁신에 기여하고 삶의 질을 개선하기 위한 기술이라는 점이다. 실존적 위험에 대한 규제는 기술과 산업의 성장을 저해할 수 있다. 실제 현실에서의 위험을 통제하기 위한 법적 규제가 도입되어야 하기 때문이다. 둘째로 인공지능 기술의 지속 가능성을 고려해야 한다. 이는 기술 개발의 선순환 구조를 확립하는 것인데, 단순한 안전 등에 대한 위협만이 아니라 차별 발생이나 프라이버시 침해와 같은 부작용이 발생하면 이용자를 포함하여 사회적인 신뢰가 떨어지게 되고, 그러면 인공지능 기술 발전의 동력이 저하될 수밖에 없다. 따라서 인공지능의 부작용 내지 역기능을 차단하거나 완화하기 위한 규제가 필요하다. 이 두 가지 사항을 종합하면, 현재 유럽연합이나 미국에서 도입하였거나 도입을 준비

하는 법적 규제 사례와 마찬가지로 인공지능이 유발하는 위험 수준에 비례하는 규제가 필요하다는 것이다. 셋째로 유럽연합과 미국의 예를 살펴본 것과 같이 국제규범 동향을 고려해야 하고, 또한 국내의 산업 생태계와 거버넌스 차원의 고려가 필요하다.

그런데 2019년 법무부가 출입국심사 고도화를 위해 인공지능(AI) 식별추적 시스템 개발사업을 추진하였고, 이 과정에서 사업 참여기업이 법무부가 「출입국관리법」에 따라 수집한 내국인 5,760만 건 및 외국인 1억 2,000만 건의 개인정보에 접근하여 출입국관리 고도화를 위한 인공지능 알고리즘을 학습시킨 사실이 확인되었다.[389] 개인정보위원회는 동 사안에 대한 「개인정보 보호법」 위반 여부를 판단하기 위하여, 첫째, 인공지능 식별추적시스템 개발을 위해 활용된 얼굴정보 등이 민감정보에 해당하는지, 둘째, 출입국 심사를 위한 인공지능 학습에 얼굴정보를 이용한 것이 목적범위 내 이용인지, 셋째, 이와 같은 이용이 개인정보 처리위탁에 해당하는지, 넷째, 개인정보 처리위탁 사실을 공개하지 않은 것이 「개인정보보호법」 위반인지 여부 등을 논의하였다. 조사결과 개인정보위원회는 해당 정보는 생체정보로서 민감정보이며 「개인정보 보호법」 제23조에 따라 정보주체의 동의 또는 명시적 법적 근거가 필요한데 「출입국관리법」이 그 법적 근거가 된다는 점,[390] 법무부가 보유한 정보를 동 사업의 인공지능 학습에 활용한 것은 「출입국관리법」의 목적범위 내에 해당된다는 점[391]은 인정하였지만, 해당 사업은 개인

389) 개인정보보호위원회 보도자료(2022. 4. 27.), “개인정보위, 출입국관리 인공지능 식별추적시스템 구축사업 개인정보보호법 위반 여부 조사결과 발표”.

390) 개인정보위원회는 「개인정보보호법」 제23조 제1항 제2호는 “법령에서 민감정보의 처리를 요구하거나 허용하는 경우” 민감정보 처리가 허용된다고 규정하고 있는데, 이는 법령에서 민감정보의 종류를 열거하고 그 처리를 요구하는 경우를 의미한다고 전제한 후 현행 「출입국관리법」은 얼굴이미지를 생체정보로 규정하면서 그 활용에 관하여 규정하고 있는데(제3조, 제6조, 제12조의2), 본인 확인을 위해서는 홍채, 얼굴, 지문 이미지 등으로부터 특징점을 추출한 정보의 처리가 필수적이라는 점에서 「출입국관리법」이 생체정보와 같은 민감정보의 처리를 허용하는 것으로 해석함이 타당하다고 판단하였다. 이로써 개인정보위원회는 출입국관리법」의 법적 근거성을 긍정하였다.

정보처리위탁에 해당되는 데도 법무부가 위탁계약을 체결하면서 위탁사실과 수탁자를 홈페이지에 공개하지 않은 데 대해 「개인정보보호법」 제26조 제2항 위반으로 과태료처분하였다.[392] 흥미로운 점은 해당 사업의 경우 안면인식정보 활용 이외에 CCTV를 활용한 출입국심사장 이상행동 인공지능 식별추적사업도 병행하였는데, 이를 위해 CCTV 영상정보 내 특정 개인에 대한 특징점을 추출하는 행위가 민감정보의 처리에 해당하지만 실제 이용하지 않았다는 점에서 그 위법 여부를 판단하지는 않았다. 다만, 개인정보위원회는 '폐쇄회로텔레비전 영상정보를 이용한 인공지능 이상행동 탐지 솔루션' 개발을 재추진하기 위해서는 정보주체의 사전동의(예: 개인정보 이용 동의를 받은 연기자의 연출 데이터 활용 등)를 받거나, 이를 허용하는 법적 근거를 마련하거나, 다른 정보와 결합하더라도 개인을 식별할 수 없도록 비식별화하여 추진할 필요가 있다고 판단하였다.[393] 걸음걸이 등 행동적 특성을 가진 생체정보가 법보행분석을 통해 개인식별이 가능하다는 점에서 비식별화를 위한 기술적·제도적 통제책은 필수적이라 할 것이다. 그러나 그 이전에 인공지능 기술의 개발과 활용의 근거가 아무리 안전한 국경관리가 될 수 있다고 하더라도 「출입국관리법」 제1조의 목적 조항을 법치주의 원칙을 달성하기 위한 구체적인 근거 조항으로 삼는 것은 무리가 있다고 하겠다.

앞서 살펴본 고려 사항과 위의 사례를 종합하면, 현재 국회에 계류 중인 대동소이한 여러 건의 법률안은 대부분 큰 틀에서는 합의가 가능할 것이다. 기술의 발전과 산업의 활성화를 기조에 두고, 신뢰성·안전성 확보 차원에서 자율규제 중심의 정책 지원이 그것이다. 다만, 관련 사업자에 대한 투명성 의무는 지금보다 엄격하게 부과하여 자율규제의 실효성을 높여야 할 것이다. 고위험영역을 추상적으로 열거하고 해당 영역에서 활용되는 인공지능이라고 하여 모두 같은 규제를 적용하는

391) 해당 사업은 「출입국관리법」상 정보화기기를 통한 출입국 심사·고도화를 통해 법의 목적인 '안전한 국경관리'를 달성코자 하는 것으로 당초 개인정보 수집·이용 목적범위에 포함된다고 판단하였다.(개인정보보호위원회(2022), 앞의 보도자료 참조)

392) 개인정보보호위원회(2022), 앞의 보도자료 참조.

393) 개인정보보호위원회(2022), 앞의 보도자료 참조.

것은 정당하지 않다. 다만, 투명성 확보와 관련하여서는 규제 수준을 조금 높여도 될 것이다. 인공지능 감시가 가지는 국민의 기본권 침해에 대한 위험성이나 민주주의 원리에 대한 위협은 개별적 규제 방식을 주로 채택하여 인공지능 활용의 구체적 법적 근거를 도입함으로써 해결이 가능할 것이다.

참 고 문 헌

[국내 문헌]

강현철 외(2013), 『정보통신기기에 의한 노동인권 침해 실태조사』, 국가인권위원회.
김동희·최계영(2021), 『행정법I』, 박영사.
_____(2023), 『행정법I』, 박영사.
김혜정(2000), 『전자감시제도의 도입 및 운영을 위한 예비연구』, 한국형사정책연구원.
미셸 푸코(2000), 『지식의 고고학』, 이정우 (역), 민음사.
_____(2004), 『성의 역사 3: 자기 배려』, 이혜숙·이영목 (역), 나남.
_____(2007), 『성의 역사 1: 앎의 의지』, 이규현(역), 나남.
_____(2018), 『성의 역사 2: 쾌락의 활용』, 문경자·신은영(역), 나남.
_____(2019), 『성의 역사 4: 육체의 고백』, 오생근(역), 나남.
_____(2023a), 『감시와 처벌: 감옥의 탄생』, 오생근(역), 나남.
_____(2023b), 『권력과 공간』, 이상길(역), 문학과지성사.
_____(2023c), 『안전, 영토, 인구』, 심세광·전혜리·조성은(역), 난장.
미셸 푸코 외(2014), 『푸코 효과: 통치성에 관한 연구』, 심성보 외(역), 난장.
빈프리트 하세머(2011), 『범죄와 형벌: 올바른 형법을 위한 변론』, 배종대·윤재왕 (역), 나남.
박균성(2017), 『행정법론(상)』, 박영사.
성낙인(2019), 『헌법학』, 법문사.
송태은(2021), 『인공지능 기술을 이용한 국가의 사회감시 체계 현황과 주요 쟁점』, 국립외교원 외교안보연구소.
심재우(2020), 『열정으로서의 법철학』, 박영사.
양천수(2023), 『인권법이론』, 박영사.

이영무(2024), 『행정법총론』, 정독.

한민경 외(2018), 『범죄예방 목적의 공공 CCTV 운영실태 및 개선방안 연구』, 한국형사정책연구원.

한수웅(2022), 『헌법학』, 법문사.

Berns. G.(2024), 『'나'라는 착각: 뇌는 어떻게 인간의 정체성을 발명하는가』, 홍우진(역), 흐름.

Konstantinov, F. et al(1986),, 『토대/상부구조론 입문: 사회구성체론의 새로운 이해』, 학민사 편집실(편역), 학민사.

Luhmann, N.(2014a), 『체계이론 입문』, 윤재왕(역), 새물결.

Luhmann, N.(2014b), 『사회의 사회』, 장춘익(역), 새물결.

Thaler, R./Sunstein, C.(2018), 『넛지: 똑똑한 선택을 이끄는 힘』, 안진환(역), 리더스북.

강미영·정혜진(2022), "인공지능 기반의 CCTV에 의한 범죄예측 시스템 도입에 따른 법적 과제와 활용방안", 《강원법학》 제66권, 강원대학교 비교법학연구소.

강병연(2022), "행정상 법률관계에 대한 새로운 고찰", 《법조》 제71권 제2호, 법조협회.

고승규(1999), "『성의 역사』를 통해 본 푸코의 권력이론", 《강원인문논총》 제7집, 강원대학교 인문과학연구소.

김경숙·홍건식(2023), "바이든 행정부의 첫 인공지능(AI) 행정명령과 시사점", 《이슈브리프》 480호, 국가안보전략연구원.

김동윤(2006), "정보테크놀로지, 전자감시, 그리고 프라이버시 위기: 푸코와 루크스의 권력개념을 중심으로", 《사이버커뮤니케이션학보》 통권 제18호, 사이버커뮤니케이션학회.

김민규(2023), "안면인식기술의 경찰법적 활용에 관한 연구", 박사학위 논문, 고려대학교 대학원.

김민우·김일환(2021), "지능정보사회에서 민감정보의 보호와 이용을 위한 법제 정

비방안 연구”, 《서울법학》 제29권 제2호, 서울시립대학교 법학연구소.
김병수(2022), “부패범죄에 AI 범죄예측 시스템 적용의 문제점과 개선방안”, 《한국부패학회보》 제27권 제2호, 한국부패학회.
김성천(2018), “미국 캘리포니아주 소비자프라이버시법(CCPA)의 주요 내용과 시사점”, 《소비자정책동향》 제93호, 한국소비자원.
김영선(2020), “플랫폼 자본주의 시대의 노동자상”, 《도시연구》 제18호, 인천연구원.
김영욱(2018), “디지털 노동 착취와 감시의 상품화: 온라인 맞춤형 광고에 대한 커뮤니케이션 정치경제학 해석”, 《언론과 사회》 제26권 제1호, 사단법인 언론과 사회.
김윤섭·박상용(2015), “형사증거법상 디지털 증거의 증거능력: 증거능력의 선결요건 및 전문법칙의 예외요건을 중심으로”, 《형사정책연구》 제26권 제2호, 한국형사정책연구원.
김원식(2002), “근대적 ‘주체’ 개념의 비판과 재구성: 주체의 자기 관계와 상호 주관성”, 《해석학연구》 제9집, 한국해석학회.
김용규(2018), “주권권력에서 생명권력으로: 「성의 역사 1 - 앎의 의지」를 중심으로”, 《코기토》 제85호, 부산대학교 인문학연구소.
김일환(2020), “지능정보사회에서 헌법의 역할과 기능”, 《성균관법학》 제32권 제3호, 성균관대학교 법학연구원.
_____(2019), “생체인식정보의 보호와 이용에 관한 법제정비방안에 관한 연구”, 《유럽헌법연구》 제30호, 유럽헌법학회.
_____(2014), “개인정보보호법상 목적구속원칙의 의의와 내용에 관한 연구”, 《미국헌법연구》 제25권 제3호, 미국헌법학회.
김정경(2016), “미셸 푸코의 통치성 개념 연구”, 석사학위 논문, 이화여자대학교.
김중권(2024), “EU의회의 인공지능법안의 주요 내용에 관한 소고: EU집행이사회의 인공지능법안과 비교해서”, 《공법연구》 제52집 제3호, 한국공법학회.
김현철(2016), “생명정치, 생명권력, 생명법”, 《법과사회》 제51호, 법과사회이론학회.
노현숙(2022), “범죄예측의 쟁점과 함의”, 《경희법학》 제57권 제1호, 경희법학연구소.

문광진(2024), “인공지능 규제 입법에 관한 일고찰”, 《외법논집》 제48권 제3호, 한국외국어대학교 법학연구소.

박민지·서정범(2020), “전자감독제도의 예방적 경찰활동으로서의 함의 - 범죄징후 예측시스템의 허용성을 중심으로 -”《고려법학》 제99호, 고려대학교 법학연구원.

박병락(2009), “Foucault의 권력 개념과 학교교육”, 《교육사상연구》 제23권 제3호, 한국교육사상연구회.

박상욱 외(2023), “공공안전 분야에서의 지능형 CCTV 기술 적용 동향”, 《주간기술동향》 제2105호, 정보통신기획평가원.

박성민(2023), “리걸테크의 도입과 형사전자소송의 가능성과 한계”, 《형사소송이론과 실무》 제15권 제2호, 한국형사소송법학회.

박충식·김형주(2022), “구성주의적 정보 철학의 관점에서 본 근대와 그 이후의 주체 개념”, 《인공지능인문학연구》 제12권, 인문콘텐츠연구소.

배재권(2020), “인공지능과 빅데이터 분석 기반 통합보안관제시스템 구축방안에 관한 연구”, 《로고스경영연구》 제18권 제1호, 한국로고스경영학회.

백국흠·김일환(2018), “지능정보사회에서 AI 감사에 관한 법적 쟁점 고찰”, 《미국헌법연구》 제29권 제2호, 미국헌법학회.

선지원(2022), “인공지능 생애주기의 관점에서 본 규제와 거버넌스”, 《연세법학》 제39권, 연세법학회.

_____(2021), “규제 방법의 진화로서 자율규제의 실질화를 위한 연구”, 《행정법연구》 제34호, 행정법이론실무학회.

손지영(2021), “AI와 형사사법 리걸테크 시스템”, 《제도와 경제》 제15권 제4호, 한국제도경제학회.

송기복(2024), “AI 안면인식 기술의 활용과 범죄수사의 문제점”, 《경찰법 연구》 제22권 제1호, 한국경찰법학회.

심소연(2024), “규제중심의 유럽연합 인공지능법(EU AI Act)”, 《최신 외국입법정

보》, 제242호, 국회도서관.

안경옥(2023), “빅데이터를 활용한 범죄예측의 문제점과 개선방향”, 《비교형사법연구》 제24권 제4호, 한국비교형사법학회.

양운덕(1991), “탈구조주의 사회 이론의 기초”, 《시대와 철학》 제3호, 한국철학사상연구회.

_____(1994), “계몽적 이성과 지배: 아도르노와 푸코의 이성 비판”, 《철학연구》 제18권, 고려대학교 철학연구소.

_____(1997), “푸코의 권력계보학: 서구의 근대적 주체는 어떻게 만들어지는가?”, 《경제와사회》 제35권, 비판사회학회.

_____(2011), “생명(관리)권력과 생명정치”, 《진보평론》 제47호, 계간지 진보평론.

양종모(2021), “법 분야 위험의 예측을 위한 인공지능 알고리즘과 관련된 법적 쟁점”, 《IT와 법연구》 제22집, 경북대학교 IT와 법연구소.

_____(2016), “인공지능의 위험의 특성과 법적 규제방안”, 《홍익법학》 제17권 제4호, 홍익대학교 법학연구소.

양천수(2016), “현대 안전사회와 법적 통제: 형사법을 예로 하여”, 《안암법학》 제49호, 안암법학회.

_____(2009), “법의 근대성과 탈근대성: 하버마스와 투렌의 기획을 중심으로 하여”, 《법학연구》 제50권 제1호, 부산대학교 법학연구소.

_____(2022), “현대사회의 구조변혁과 법규범의 대응 방향”, 《인간연구》 제46호, 가톨릭대학교 인간연구소.

_____(2024), “유럽연합 의약품 법제 동향: 의약품 개혁 법안을 중심으로”, 《글로벌법제전략연구사업》 2024년 제1호, 한국법제연구원.

오경석·조미지(2023), “인공지능 경찰활동 도입 쟁점에 관한 연구”, 《경찰학연구》 제23권 제1호, 경찰대학.

윤상연·신상화(2018), “범죄 예측의 현재와 미래: 한국형 범죄예측 시스템 개선·도입에 대한 제언”, 《한국공안행정학회보》 제27권 제3호, 한국공안행정학회.

윤정현·조은정(2024), “EU ‘인공지능 규제법(AI Act)’ 통과의 의미와 시사점”, 《이슈 브리프》 제527호, 국가안보전략연구원.

은재호(2011), “규율과 통치: 조직연구에 있어서 Michel Foucault 권력론의 함의와 기여”, 《한국조직학회보》 제8권 제2호, 한국조직학회.

이광석(2014), “포스트-판옵티콘 시대 감시 연구: 연구 동향과 새로운 영역”, 《ICT 인문사회융합동향》 Vol. 4, 정보통신정책연구원.

이권일(2023), “지능정보사회에서 개인정보자기결정권이 보호하고자 하는 헌법적 가치”, 《공법연구》 제51권 제3호, 한국공법학회.

_____(2020), “생체인식정보의 보호와 활용에 대한 헌법적 고찰: 개인정보보호법 시행령 개정령안에 대한 분석을 겸하여”, 《법학연구》 제61권 제2호, 부산대학교 법학연구소.

이상우(2023), “중국의 안면인식 기술 입법동향과 시사점: 안면인식 기술응용 안전관리규정 의견수렴안을 중심으로”, 《법학연구》 제26집 제4호, 인하대학교 법학연구원.

이상욱(2020), “인공지능의 실존적 위험: 비판적 검토”, 《인간연구》 제40호, 가톨릭대학교 인간학연구소.

이상학(2023), “생체적 안면인식의 법적 문제”, 《유럽헌법연구》 제42호, 유럽헌법학회.

이율경(2024), “노동관계에서 알고리즘에 관한 법적 쟁점”, 《노동법연구》 제56호, 서울대학교노동법연구회.

이준일(2022), “인공지능과 헌법: 인공지능의 위험에 대한 헌법적 권리 차원의 대응”, 《헌법학연구》 제28권 제2호, 한국헌법학회.

이진규(2018), “EU GDPR 주요 내용의 검토”, 《KISO 저널》 제30호, 한국인터넷자율정책기구.

장선미(2023), “플랫폼 경제에 관한 헌법적 접근: 플랫폼 노동의 보호와 플랫폼 사업의 규율”, 《헌법재판연구》 제10권 제2호, 헌법재판연구원.

정규영(2013), “미셸 푸코의 ‘규율 권력’과 근대 교육”, 《교육사학연구》 제23권 제2

호, 교육사학회.
정소영(2022), “형사사법에서의 인공지능 사용에 대한 유럽의회 결의안; ‘인공지능에 의한 결정’ 금지에 관하여”, 《형사정책》 제34권 제2호, 한국형사정책학회.
정애령(2022), “지능정보사회 개인정보자기결정권을 보완하는 데이터 활용과 개인정보보호”, 《공법학연구》 제23권 제1호, 한국비교공법학회.
정채연(2023), “예측적 치안과 형사정책”, 《영남법학》 제57호, 영남대학교 법학연구소.
조광제(1991), “미셸 푸코의 권력론”, 《시대와 철학》 제2호, 한국철학사상연구회.
조한상(2022), “인공지능 기반 반부패 도구(AI-ACT)의 헌법원리 적합성에 관한 고찰”, 《한국부패학회보》 제27권 제1호, 한국부패학회.
한국인터넷진흥원(2020), “미국 캘리포니아주 프라이버시 권리법 제정 배경 및 주요 내용”, 2020 최종보고서.
한지우·오삼일(2023), “AI와 노동시장 변화”, 《BOK 이슈노트》 제2023-30호, 한국은행.
한희진(2012), “미셸 푸코의 파놉티시즘에서 인식, 권력, 윤리의 관계”, 《의철학연구》 제13호, 한국의철학회.
허욱·원중재(2021), “중국 데이터 보안법 제정과 시사점”, 법무법인 세종.
홍석한(2023), “사회보장 영역에서 인공지능 활용에 대한 헌법적 고찰”, 《법학논고》 제80집, 경북대학교 법학연구원.
_____(2023), “지능정보사회에서 사회보장 영역의 정보화와 기본권 보호: 네덜란드 SyrI 판결에 대한 분석과 평가”, 《헌법학연구》 제29권 제3호, 한국헌법학회.
홍은영(2014), “푸코와 우리 시대의 건강 담론: 의료화 현상과 관련하여”, 《철학연구》 제50집, 고려대학교 철학연구소.

개인정보보호위원회(2021), “생체정보 보호 가이드라인”.
개인정보보호위원회 보도자료(2022. 4. 27.), “개인정보위, 출입국관리 인공지능 식별추적시스템 구축사업 개인정보보호법 위반 여부 조사결과 발표”.

경찰청(2021), “범죄 위험도 예측. 분석 시스템 PRE-CAS(Predictive Crime Risk Analysis System 통합메뉴얼”.

국가인권위원회 결정(2007. 11. 12.), “사업장 전자감시에서 근로자의 인권보호를 위한 법령·제도 개선권고”.

국가인권위원회 보도자료(2024. 2. 22.), “실시간 원격 얼굴인식 기술 도입·활용 중지 조치 권고, 국무총리 수용”.

과학기술정보통신부 사업공고(2024. 2. 28.), “2024년도 재범징후 선제적 감지 및 대응력 강화사업 신규과제 공모”.

과학기술정보통신부 보도자료(2019. 12. 17.), ““IT 강국을 넘어 AI 강국으로!”: 범정부 역량을 결집하여 AI 시대 미래 비전과 전략을 담은 ‘AI 국가전략 발표’”.

_____(2020. 12. 22.), “과기정통부, 사람이 중심이 되는「인공지능(AI) 윤리기준」마련”.

_____(2022. 2. 24.), “인공지능의 윤리적 개발·활용을 촉진하는 논의의 장 마련”.

_____(2024. 2. 6.), “인공지능의 윤리적 개발·활용을 촉진하는 논의의 장 마련”.

_____(2024. 9. 26.), “국내 1·2호 ‘민간자율 인공지능 신뢰성 인증’ 부여”.

관계부처 합동(2023. 4.), “국가 안전시스템 개편 종합대책”.

대한민국 정책브리핑(2023. 2. 14), “국고보조금 시스템 개선으로 부정수급 적발률 지속 높여가”, 기획재정부, https://www.korea.kr/multi/visualNewsView.do?newsId=148911651&sectIds=&cateId=&pageIndex=1&repCode_C=#visualNews(2024. 10. 3. 최종 방문).

법무부 보도자료(2021. 6. 28.), “인공지능(AI) 기반의 전자감독서비스 구축”, https://www.moj.go.kr/moj/221/subview.do?enc=Zm5jdDF8QEB8JTJGYmJzJTJGbW9qJTJGMTgyJTJGNTQ5MjQ4JTJGYXJ0Y2xWaWV3LmR

vJTNG(2024. 10. 3. 최종 방문).

법제처 법제동향(2024. 5. 9.), “유럽의회, 「AI법」 가결”, https://world.moleg.go.kr/web/dta/lgslTrendReadPage.do?A=A&searchType=all&searchPageRowCnt=10&CTS_SEQ=52117&AST_SEQ=96&ETC=1(2024. 10. 3. 최종 방문).

보건복지부 보도자료(2024. 3. 24.), “45종 위기정보 활용해 2024년 2차 복지 사각지대 발굴 시행”.

_____(2024. 1. 21.), “나를 위한 89가지 복지서비스, 복지멤버십이 알려드려요”.

_____(2022. 9. 5.), “차세대 사회보장정보시스템 개통(2차)”.

보건복지부(2022. 1. 28.), 『2022년도 국가정보화 시행계획』.

경향신문(2024. 8. 11.), “피의자 신문 영상, 증거 채택을”, https://m.khan.co.kr/opinion/column/article/202408112110015?fbclid=IwY2xjawEmf9pleHRuA2FlbQIxMQABHRXW6cteRmQw1fCJK_zH7xdfMbJPaMaC-8GDLKOXtw6kWWMo8rNIH5tqJg_aem_k2wxhbp3xnZzQJOPC1BQHA&sfnsn=mo#c2b (2024. 10. 3. 최종 방문).

_____(2023. 10. 3.), “올해 산재 승인 1위는 ‘배달의민족’…달라지는 산재 지도”, https://www.khan.co.kr/national/labor/article/202310031216001(2024. 10. 3. 최종 방문).

_____(2021. 1. 26.), “성동구, 범죄징후 CCTV로 잡아낸다 … ‘지능형 선별관제 시스템’ 구축”, https://www.khan.co.kr/local/Seoul/article/202101261457001 (2024. 10. 3. 최종 방문).

네이버, EU GDPR이란, https://privacy.naver.com/global_support?menu=global_support_eu_gdpr_understand (2024. 10. 3. 최종 방문).

뉴스1(2021. 2. 25.), “‘CCTV 활용 안면인식·동선분석’으로 코로나 감염경로 파악한다”, https://www.news1.kr/articles/?4223239(2024. 10. 3. 최종 방문).

뉴스핌(2022. 8. 4.), “셀바스 AI, ‘AI 음성인식 기반 성폭력 피해 조서 작성 시스템’ 경찰서·해바라기센터 확대 적용”, https://www.newspim.com/news/view/20220804000126(2024. 10. 3. 최종 방문).

머니투데이(2020. 4. 13.), “‘돌아가신분이 왜 바우처를’...이런 부정수급 AI가 잡는다”, https://news.mt.co.kr/mtview.php?no=2020041311103819755(2024. 10. 3. 최종 방문).

매일경제(2019. 11. 1.), “[김대기 특파원의 차이나 프리즘] 최첨단 달리는 中 감시 시스템, 공안이 휴대폰으로 얼굴 찍자 ‘개인정보’ 줄줄 … 무단 횡단하면 대형 스크린에 얼굴·신분 노출”, https://www.mk.co.kr/news/world/9047851(2024. 9. 10 최종 방문).

매일신문(1994. 5. 3.), “PC통신 표현의 자유 사생활 보호 “비밀보장을””, https://www.imaeil.com/page/view/1994050308531057886(2024. 10. 3. 최종 방문).

법률신문(2024. 8. 6.), “美법원, ‘AI 가짜 판례’ 인용 변호사에 정직 1년”, https://www.lawtimes.co.kr/news/197090(2024. 10. 3. 최종 방문).

보안뉴스(2017. 4. 14.), “中 2017년 6월 사이버보안법 전면 시행”, https://m.boannews.com/html/detail.html?idx=65149(2024. 10. 3. 최종 방문).

서울신문(2024. 2. 27.), “[공직자의 창] 국고보조금 누수, AI 탐지모델로 잡아낸다”, https://www.seoul.co.kr/news/editOpinion/opinion/government-official-story/2024/02/27/20240227025004(2024. 10. 3. 최종 방문).

_____(2018. 7. 8.), “[김규환 기자의 차이나 스코프] 사방에 깔린 ‘매의 눈’… 빅브러더 키우는 대륙”,

https://www.seoul.co.kr/news/plan/china_scope/2018/07/09/20180709016001(2024. 10. 3. 최종 방문).

세계일보(2024. 3. 3.), “법무부, 인공지능(AI) 기반 전자 감독 기술·시스템 개발 본격 추진”, https://www.segye.com/newsView/20240303503884(2024. 10. 3. 최종 방문).

소방방재신문(2024. 6. 20.), “안산시 충무훈련서 인텔리빅스 AI 관제시스템 활용”, https://fpn119.co.kr/218338 (2024. 10. 3. 최종 방문).

아시아경제(2024. 4. 19.), “AI 안면인식 기술 시대 … 선진국선 ‘빅브라더’ 우려 [CCTV 감시사회]②”, https://www.asiae.co.kr/article/2024041815510255760(2024. 10. 3. 최종 방문).

연합뉴스(2024. 8. 14.), “고양시, 전국 최초 차세대 인공지능(AI) 통합관제시스템(AMS) 구축”, https://www.yna.co.kr/view/RPR20240814000400353(2024. 10. 3. 최종 방문).

이강원·손호웅(2016), 『지형 공간정보체계 용어사전』, 구미서관, https://terms.naver.com/entry.naver?docId=3474031&cid=58439&categoryId=58439 (2024. 10. 3. 최종 방문).

인공지능신문(2023. 9. 4.), “셀바스AI, 경찰청 ‘AI 음성인식 피해조사 시스템’ 고도화…완성도 높은 조사 및 양질의 수사 지원 목표”, https://www.aitimes.kr/news/articleView.html?idxno=28846(2024. 9. 13. 최종 방문).

정보통신신문(2022. 7. 26.), “경찰, ICT. 과학기술 융합 “더욱 든든한 치안구현””, https://www.koit.co.kr/news/articleView.html?idxno=100518(2024. 10. 3. 최종 방문).

채널A(2022. 7. 10.), “[세계를 보다]AI로 충성도 검사 … 中 디지털 감시 ‘첩첩’”, https://www.ichannela.com/news/main/news_detailPage.do?publishI

d=000000304856(2024. 10. 3. 최종 방문).

한국사회보장정보원(2022. 7. 22.), “한국사회보장정보원, 'AI 기반의 공공재정 FDS 신속 대응·탐지체계 구축'으로 우수행정 정책사례 우수상”, http://www.ssis.or.kr/lay1/bbs/S1T101C486/B/101/view.do?article_seq=124162&cpage=1&rows=10&condition=&keyword=(2024. 10. 3. 최종 방문).

GTT KOREA(2022. 4. 6.), “음성인식 기술로 자동으로 조서 작성한다”, https://www.gttkorea.com/news/articleView.html?idxno=586(2024. 10. 03. 최종 방문).

IGLOO(2019. 7. 31.), “국내 기업 및 조직에 대한 GDPR의 적용과 DPO의 이해”, https://www.igloo.co.kr/security-information/%EA%B5%AD%EB%82%B4-%EA%B8%B0%EC%97%85-%EB%B0%8F-%EC%A1%B0%EC%A7%81%EC%97%90-%EB%8C%80%ED%95%9C-gdpr%EC%9D%98-%EC%A0%81%EC%9A%A9%EA%B3%BC-dpo%EC%9D%98-%EC%9D%B4%ED%95%B4/(2024. 10. 3. 최종 방문).

[해외문헌]

Bensamoun, A., Loiseau, G.(Sous la direction de)(2019). Droit de l’intelligence artificielle, LGDJ.

Burgess, P.(2024). AI and the RULE OF LAW: The Necessary Evolution of a Concept, Hart Publishing.

Aziz Z. Huq(2020). “Constitutional Rights in the Machine-Learning State”. Cornell Law Review Vol. 105.

Ad Hoc Committee on Artificial Intelligence(CAHAI)(2020). “Feasibility Study”. Council of Europe.

Christenko, A., Jankauskaittė, V., Paliokaittė, A., Van den Broek, K. R.,

Jarvis, M.(2022). “Artificial intelligence for worker management: an overview”. European Agency for Safety and Health at Work.

Baiocco. S, Enrique. F, Rani. U, Pesole. A.(2022). “The Algorithmic Management of work and its implications in different contexts”. International Labour Organization.

Lubarsky, B.(2017). “Re-Identification of ‘Anonymized’ Data”. Georgetown Law Technology Review Vol. 1, Georgetown Law.

Slobogin, C., Brayne, S.(2023). “Surveillance Technologies and Constitutional Law”. Annual Review of Criminology, Vanderbilt Law School Faculty Publications.

Helbing, D. et al.(2019). “Will Democracy Survive Big Data and Artificial Intelligence?”, in: Helbing, D. ed., Towards Digital Enlightenment: Essays on the Dark and Light Sides of the Digital Revolution. Spinger.

Eurofound(2020). Employee monitoring and surveillance: The challenges of digitalisation. Publications Office of the European Union.

Bayamlioğlu, E., Leenes, R.(2018). “Data-driven decision-making and the ‘Rule of Law’”, Tilburg Law School Research Paper.

Degeling, M., Berendt, B.(2018). “What Is Wrong about Robocops as Consultants? A Technology-Centric Gritique of Predictive Policing”, AI&Society, Vol. 33.

European Commission(2019). “Ethics guidelines for trustworthy AI”.

European Parliament(2024). “The United Kingdom and artificial intelligence”.

Fontes, C. et al.(2022). “AI-powered public surveillance systems: why we (might) need them and how we want them”. Technology in Society. Vol. 71.

Friedrich v. Zezschwitz(2003). “Konzept der normativen Zweckbegrenzung”.

Alexander Roßnagel(Hrsg.). Handbuch Datenschutzrecht, C. H. Beck.

Gary C. Robb(1980). "Police Use of CCTV Surveillance: Constitutional Implications and Proposed Regulations". University of Michigan Journal of Law Reform. Vol. 13.

Meltzer, J., Tielemans, A.(2022). "The European Union AI Act: Next steps and issues for building international cooperation in AI". Global Economy and Development Policy Brief May 2022, Brookings Institution.

Manheim, K., Kaplan, L.(2019). "Artificial Intelligence: Risks to Privacy and Democracy". Yale Journal of Law & Technology. Vol. 21, Yale University.

Evans, L.(2020). "Artificial Intelligence and Public Standards: A Review by the Committee on Standards in Public Life". The Committee on Standards in Public Life.

Mcdaid. E., Andon. P, Free. C.(2023). "Algorithmic management and the politics of demand: Control and resistance at Uber". Accounting, Organizations and Society. Volume 109.

National Institute of Standards and Technology(2023). "Artificial Intelligence Risk Management Framework".

Patrick Brione(2020). "My boss the algorithm: Research An ethical look at algorithms in the workplace". Acas.

Ponce del Castillo. A. & Naranjo. D.(2022). "Regulating algorithmic management: An assessment of the EC's draft Directive on improving working conditions in platform work". ETUI Policy Brief, The European Trade Union Institute.

Reinhold, K., Järvis, M., Christenko, A., Jankauskaitė, V., Paliokaitė A. & Riedmann, A.(2022). "Artificial intelligence for worker management:

implications for occupational safety and health". European Agency for Safety and Health at Work.

Baiocco, S. et al.(2022). "The Algorithmic Management of work and its implications in different contexts". International Labour Organization.

Schweyer, A.(2018). "Predictive Analytics and Artificial Intelligence in People Management". McLean: Incentive Research Foundation.

Stephanie Bornstein(2018). "Antidiscriminatory Algorithms". Alabama Law Review. Vol. 70 No. 2.

Urzì, B. C., Curtarelli, M., Riso, S., Baiocco, S.(2022). "How digital technology is reshaping the art of management". European Commission.

World Economic Forum(2023). "Future of Jobs Report 2023: Insight Report".

Amy Gordon(2023. 10. 2.). "The Return of the Video Privacy Protection Act(VPPA)", https://www.mindingyourbusinesslitigation.com/2023/10/the-return-of-the-vppa/(2024. 10. 3. 최종 방문).

ABC News(2020. 6. 26.). "Black man wrongfully arrested because of incorrect facial recognition", https://abcnews.go.com/US/black-man-wrongfully-arrested-incorrect-facial-recognition/story?id=71425751(2024. 10. 3. 최종 방문).

ACLU Illinois. "BIOMETRIC INFORMATION PRIVACY ACT (BIPA)", https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa(2024. 10. 3. 최종 방문).

Amnesty(2024. 4. 14). "JO 2024 : Pourquoi la vidéosurveillance algorithmique pose problème", https://www.amnesty.fr/liberte-d-expression/actualites/pourquoi-l

a-videosurveillance-algorithmique-pose-probleme-cameras-technologies(2024. 10. 3. 최종 방문).

AMNESTY INTERNATIONAL(2022. 2. 15.). “USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research”, https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/(2024. 10. 3. 최종 방문).

BIOMETRIC(2024. 3. 1.). “US AI Advisory wants more disclosure on facial recognition use by federal law enforcement”, https://www.biometricupdate.com/202405/us-ai-advisory-wants-more-disclosure-on-facial-recognition-use-by-federal-law-enforcement(2024. 10. 3. 최종방문).

BIOMETRIC(2024. 3. 8.). “Police in Germany using live facial recognition”, https://www.biometricupdate.com/202405/police-in-germany-using-live-facial-recognition(2024. 10. 3. 최종 방문).

CCTV information. “THE DATA PROTECTION ACT AND CCTV(2020. 1. 27.)”, https://www.cctv-information.co.uk/article/the-data-protection-act-and-cctv/(2024. 10. 3. 최종 방문).

China Law Translate(2024. 4. 9.). “Regulations on the Management of Video Imaging Information Systems in Public Spaces (Draft for Solicitation of Public Comments)”, https://www.chinalawtranslate.com/en/cctv-regs/(2024. 10. 3. 최종 방문).

CNN(2019. 5. 14.). “San Francisco just banned facial-recognition technology”, https://www.cnn.com/2019/05/14/tech/san-francisco-facial-recog

nition-ban/index.html(2024. 10. 3. 최종 방문).

CNN(2023. 5. 23.). "'Verified' Twitter accounts share fake image of 'explosion' near Pentagon, causing confusion", https://edition.cnn.com/2023/05/22/tech/twitter-fake-image-pentagon-explosion/index.html(2024. 10. 3. 최종 방문).

CNN Business(2016. 7. 1.). "Tesla's autopilot probed by government after crash kills driver", https://money.cnn.com/2016/06/30/technology/tesla-autopilot-death/index.html(2024. 10. 3. 최종 방문).

CONGRESS.GOV, "S.681 - Facial Recognition and Biometric Technology Moratorium Act of 2023", https://www.congress.gov/bill/118th-congress/senate-bill/681(2024. 10. 3. 최종 방문).

CONGRESS.GOV, "H.R.3907 - Facial Recognition and Biometric Technology Moratorium Act of 2021", https://www.congress.gov/bill/118th-congress/house-bill/3907/text (2024. 10. 3. 최종 방문).

CONGRESS.GOV, H.R.6216 - "National Artificial Intelligence Initiative Act of 2020" https://www.congress.gov/bill/116th-congress/house-bill/6216 (2024. 10. 3. 최종 방문).

Consumer Privacy Act, California Privacy Rights Act, 2020 (CPRA), https://www.consumerprivacyact.com/california-privacy-act-2020-cpra/ (2024. 10. 3. 최종 방문).

DHS, DHS CCTV Systems(2012. 7. 18.), https://www.dhs.gov/sites/default/files/2023-10/privacy-pia-dhs042-cctvappendixupdate-october2023.pdf (2024. 10. 3. 최종 방문).

ED MARKEY(2023. 3. 7.). “MARKEY, MERKLEY, JAYAPAL LEAD COLLEAGUES ON LEGISLATION TO BAN GOVERNMENT USE OF FACIAL RECOGNITION AND OTHER BIOMETRIC TECHNOLOGY”, https://www.markey.senate.gov/news/press-releases/markey-merkley-jayapal-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-and-other-biometric-technology (2024. 10. 3. 최종 방문).

Federal Register(2023. 11. 1.). “Executive Order 14110 of October 30, 2023: Safe, Secure, and Trustworthy Development and Use of Artificial”, Intelligence,https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence(2024. 10. 3. 최종 방문).

Forbes(2020. 2. 3.). “EPIC Asks Federal Trade Commission To Regulate Use Of Artificial Intelligence In Pre-Employment Screenings”, https://www.forbes.com/sites/patriciagbarnes/2020/02/03/group-asks-federal-trade-commission-to-regulate-use-of-artificial-intelligence-in-pre-employment-screenings/?sh=5ed2028c2b54(2024. 10. 3. 최종 방문).

Future of Life Institute(2023. 3. 23.). “Pause Giant AI Experiments: An Open Letter”, https://futureoflife.org/wp-content/uploads/2023/05/FLI_Pause-Giant-AI-Experiments_An-Open-Letter.pdf(2024. 10. 3. 최종 방문).

GOV.UK. “Amended Surveillance Camera Code of Practice(accessible version)”, https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-ac

cessible-version(2024. 10. 3. 최종 방문).

Guardian(2019. 3. 30.). “San Francisco was right to ban facial recognition. Surveillance is a real danger”, https://www.theguardian.com/commentisfree/2019/may/30/san-francisco-ban-facial-recognition-surveillance(2024. 10. 3. 최종 방문).

Hafiz(2022. 12. 21.). “Facial Recognition Technology and Privacy Concerns, ISACA”, https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-51/facial-recognition-technology-and-privacy-concerns(2024. 10. 3. 최종 방문).

iapp, “AI surveillance camera company allegedly violated US state laws(2024. 2. 28.)”, https://iapp.org/news/b/ai-surveillance-camera-company-allegedly-violates-us-state-laws(2024. 10. 3. 최종 방문).

Information Commissioner’s Office(2023). “Special category data”, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/#scd4(2024. 10. 3. 최종 방문).

_____(2022a). “Video surveillance(including guidance for organisations using CCTV)”, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/(2024. 10. 3. 최종 방문).

_____(2022b). “What are our responsibilities in terms of accountability?”, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-inc

luding-cctv/what-are-our-responsibilities-in-terms-of-accountability/(2024. 10. 3. 최종 방문).

Information Commissioner's Office(2022c). "Data protection officers", https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/accountability-and-governance/data-protection-officers/(2024. 10. 3. 최종 방문).

_____(2022d). "How can we comply with the data protection principles when using surveillance systems?", https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/how-can-we-comply-with-the-data-protection-principles-when-using-surveillance-systems/(2024. 10. 3. 최종 방문).

_____(2022e). "Penalties", https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/penalties/(2024. 10. 3. 최종 방문).

_____(2022f). "Additional considerations for technologies other than CCTV", https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/?q=fine#frt(2024. 10. 3. 최종 방문).

_____(2022g). "What does this guidance address?", https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/what-does-this-guidance-address/(2024. 10. 3. 최종 방문).

_____(2022h). "Enforcement of this code",

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/enforcement-of-this-code/(2024. 10. 3. 최종 방문).

Information Commissioner's Office(2014). "Conducting privacy impact assessments code of practice", https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf(2024. 10. 3. 최종 방문).

innovation&tech today, "13 Cities Where Police Are Banned From Using Facial Recognition Tech", https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/(2024. 10. 3. 최종 방문).

Le Figaro(2024. 3. 22.). "On émet soixante fois plus de carbone en opérant une requête sur ChatGPT que sur Google", https://www.lefigaro.fr/secteur/high-tech/on-emet-soixante-fois-plus-de-carbone-en-operant-une-requete-sur-chatgpt-que-sur-google-20240322(2024. 10. 3. 최종 방문).

_____(2024. 3. 13.). "Les eurodéputés adoptent une loi encadrant l'intelligence artificielle, une législation unique au monde", https://www.lefigaro.fr/secteur/high-tech/les-eurodeputes-adoptent-une-loi-encadrant-l-intelligence-artificielle-une-legislation-unique-au-monde-20240313#:~:text=L'AI%20Act%20interdit%20certains,la%20lutte%20contre%20le%20terrorisme(2024. 10. 3. 최종 방문).

Lexology(2020. 12. 22.). "Germany: Detailed guidance concerning data processing by CCTV", https://www.lexology.com/library/detail.aspx?g=48ea93f6-3cb7-42e5-92c7-3d4d5bff4398(2024. 10. 3. 최종 방문).

LIS, Chapter 53. “Consumer Data Protection Act”, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/ (2024. 10. 3. 최종 방문).

MarketsandMarkets(2024). “Biometric System Market by Authentication Type (Fingerprint, Iris, Face, Voice, Vein, Signature, Multi-factor). Offering (Sensor, Camera, Reader & Scanner, Software). Type (Contact, Contactless, Hybrid). Mobility, Deployment - Global Forecast to 2029”, https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html (2024. 10. 3. 최종 방문)

Medium(2021. 3. 3.). “China’s ‘Sharp Eyes’ Program Aims to Surveil 100% of Public Space”, https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015(2024. 10. 3. 최종 방문).

Monica Gonzalez(2022). “Challenges when dealing with video surveillance footage as evidence in court”, https://www.security101.com/blog/challenges-when-dealing-with-video-surveillance-footage-as-evidence-in-court(2024. 10. 3. 최종 방문).

Office of Science and Technology Policy(2022). “Blueprint for an AI Bill of Right: Making Automated Systems Works for the American People”. The White House. https://www.whitehouse.gov/ostp/ai-bill-of-rights(2024. 10. 3. 최종 방문).

PELCO(2024). “Top CCTV Camera Technology Trends for 2024”, https://www.pelco.com/blog/cctv-and-video-security-camera-trends(2024.09.10. 최종 방문).

Pimloc(2024). “CCTV signage requirements in the US”, https://www.secureredact.ai/articles/cctv-signage-requirements-in-

the-us(2024. 10. 3. 최종 방문).

Polizeidatenbanken, “Datenbanken der Polizei”, https://www.polizeidatenbanken.de/polizei-datenbanken/datenbanken-der-polizei/(2024. 10. 3. 최종 방문).

QUARTZ(2024. 2. 21.). “China wants more control of its mass surveillance system”, https://qz.com/china-mass-surveillance-system-control-1851273607(2024. 10. 3. 최종 방문).

Renew Europe(2023. 7. 12.). “INTERNATIONAL COOPERATION IS KEY FOR THE DEVELOPMENT OF GENERATIVE AI”, https://www.reneweuropegroup.eu/news/2023-07-12/international-cooperation-is-key-for-the-development-of-generative-ai(2024. 10. 3. 최종 방문).

Reuters(2023. 2. 3.). “ChatGPT sets record for fastest-growing user base - analyst note”, https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01(2024. 10. 3. 최종 방문).

_____(2018. 3. 21.). “Homeless Arizona woman killed by Uber self-driving SUV was ‘like everyone’s aunt’”, https://www.reuters.com/article/us-autos-selfdriving-uber-victim/homeless-arizona-woman-killed-by-uber-self-driving-suv-was-like-everyones-aunt-idUSKBN1GW36P(2024. 10. 3. 최종 방문).

_____(2024. 8. 6.). “Illinois governor approves business-friendly overhaul of biometric privacy law”, https://www.reuters.com/legal/government/illinois-governor-approves-business-friendly-overhaul-biometric-privacy-law-2024-08-05/(2024. 10. 3. 최종 방문).

Reuters(2018. 10. 11.). “Insight - Amazon scraps secret AI recruiting tool that showed bias against women”, https://www.reuters.com/article/idUSKCN1MK0AG(2024. 10. 3. 최종 방문).

_____(2021. 11. 30.). “EXCLUSIVE Chinese province targets journalists, foreign students with planned new surveillance system”, https://www.reuters.com/technology/exclusive-chinese-province-targets-journalists-foreign-students-with-planned-new-2021-11-29/(2024. 10. 3. 최종 방문).

Rita(2024. 5. 28.). 4 - Transparency of Facial Recognition Technology and Trade Secrets. Cambridge Core, CAMBRIDGE UNIVERSITY PRESS, https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/transparency-of-facial-recognition-technology-and-trade-secrets/580AE16FF598DC4735FFF0CD06E389F5(2024. 10. 3. 최종 방문).

ScienceDirect. “Stored Communications Act”, https://www.sciencedirect.com/topics/computer-science/stored-communications-act(2024. 10. 3. 최종 방문).

Scientific American(2023. 5. 18.). “Police Facial Recognition Technology Can’t Tell Black People Apart”, https://www.scientificamerican.com/article/police-facial-recognition-technology-cant-tell-black-people-apart/(2024. 10. 3. 최종 방문).

Seena, The CCPA Explained, https://www.secureredact.ai/datapolicies/the-ccpa-explained(2024. 10. 3. 최종 방문).

senate.gov. “Constitution of the United States”,

https://www.senate.gov/about/origins-foundations/senate-and-constitution/constitution.htm(2024. 10. 3. 최종 방문).

Tate(2023. 7. 20.). “The movement to limit face recognition tech might finally get a win”, MIT Technology Review, https://www.technologyreview.com/2023/07/20/1076539/face-recognition-massachusetts-test-police/(2024. 10. 3. 최종 방문).

The Connexion(2024. 3. 22.). “Home security cameras: what are the rules in France?”, https://www.connexionfrance.com/practical/home-security-cameras-what-are-the-rules-in-france/635684(2024. 10. 3. 최종 방문).

University of BATH, “Data Protection Act”, https://www.bath.ac.uk/legal-information/data-protection-act/(2024. 10. 3. 최종 방문).

VICE(2019. 7. 17.). “Oakland Becomes Third U.S. City to Ban Facial Recognition”, https://www.vice.com/en/article/oakland-becomes-third-us-city-to-ban-facial-recognition-xz/(2024. 10. 3. 최종 방문).

veesion(2024, 2. 20.). “Video surveillance: how to store data and what regulations apply to businesses in France?”, https://veesion.io/en/video-surveillance-how-to-store-data-and-what-regulations-apply-to-businesses-in-france/(2024. 10. 3. 최종 방문).

Vox(2019. 3. 15.). “San Francisco’s facial recognition technology ban, explained”, https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained(2024. 10. 3. 최종 방문).

Walsh, M.(2019. 5. 8.). “When Algorithms Make Managers Worse. Harvard Business Review”,

https://hbr.org/2019/05/when-algorithms-make-managers-worse(2024. 10. 3. 최종 방문).

WIRED(2024. 3. 6.). “5 Years After San Francisco Banned Face Recognition, Voters Ask for More Surveillance”, https://www.wired.com/story/san-francisco-banned-face-recognition-voters-ask-for-more-surveillance/(2024. 10. 3. 최종 방문).

慎改康之(2019).『ミシェル·フーコー: 自己から脱け出すための哲學』, 岩波新書.

中华人民共和国中央人民政府(2021. 8. 20.). “中华人民共和国个人信息保护法”, https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm(2024. 10. 3. 최종 방문).

央视网(2015. 7. 2.). “中华人民共和国国家安全法”, http://news.cntv.cn/2015/07/02/ARTI1435799475468828.shtml(2024. 10. 3. 최종 방문).

Abstract

Kwangjin MOON

■ Title

The Expansion of Power through AI Surveillance and the Normative Response

■ Purpose of Research

AI surveillance technology can be employed as a tool to expand power, raising concerns about the potential infringement of fundamental rights and posing a threat to democracy. This study aims to explore the risks associated with surveillance facilitated by AI technology and the consequent expansion of power. It begins by examining domestic and international regulatory trends concerning AI surveillance and subsequently considers normative approaches to addressing these issues.

■ Main Outcomes of Research and Policy Implications

Several similar bills currently pending in the National Assembly may potentially reach an agreement in the broader framework. However,

regarding the assurance of transparency, this study suggests to increase the level of regulation. It adresses the risks posed by AI surveillance, such as the infringement on citizens' fundamental rights and threats to democratic principles, by primarily adopting an individual regulatory approach and introducing specific legal foundations for the utilization of AI.

● 저 자 소 개 ●

문 광 진

- Université Paris 1 Panthéon-Sorbonne 공법학 박사
- 현 정보통신정책연구원 부연구위원

허 진 주

- 숙명여자대학교 법학 석사
- 전 정보통신정책연구원 연구원

전 민 경

- 서울과학기술대학교 AI공공정책전공 석사 수료
- 현 정보통신정책연구원 연구원

기본연구 24-02

인공지능 감시에 의한 권력의 확대와 그 규범적 대응방안 연구

2024년 10월 일 인쇄
2024년 10월 일 발행

발행인 김 정 언
발행처 정 보 통 신 정 책 연 구 원
충청북도 진천군 덕산읍 정통로 18
TEL: 043-531-4114 FAX: 043-535-4695～6
인 쇄 인 성 문 화
ISBN 979-11-7000-390-8 93320

〈비매품〉