이슈리포트 <정보인권> 2020-12 (통권 제10호)

경찰 등 법집행기관의 얼굴인식 감시기술 사용과 인권 문제

I. 서론 ····· 3
II. 얼굴인식 기술의 개념 ····· 9
III. 해외 현황 및 관련 법제도 ····· 13
IV. 국내 현황 및 관련 법제도 ····· 58
V. 결론 및 제언 ····· 82

사단법인 정보인권연구소 Institute for Digital Rights

서울시 서대문구 독립문로8길 23, 3층
전화 02)701-7687, 이메일 idr.sec@gmail.com
홈페이지 http://idr.jinbo.net

4.9통일평화재단 The April 9 Unification & Peace Foundation 이 보고서는 4.9통일평화재단의 지원으로 제작되었습니다.

이슈리포트 〈정보인권〉 2020-12 (통권 제10호)
경찰 등 법집행기관의 얼굴인식 감시기술 사용과 인권 문제

발행인 : 사단법인 정보인권연구소 (이사장 이호중)
발행일 : 2020년 12월 1일

♣ 일시후원/후원회원 신청은 홈페이지 http://idr.jinbo.net 참조

경찰 등 법집행기관의 얼굴인식 감시기술 사용과 인권 문제

사단법인 정보인권연구소[1)]

I. 서론

법집행(law enforcement)이란 법을 어긴 자를 찾아내고, 수사하고, 체포하고, 처벌하거나, 교정하여 법을 집행하는 과정이다. 법집행기관(Law enforcement agency)에는 법원이나 형집행기관, 세관이 포함되기도 하지만, 일반적으로는 일선에서 범죄를 저지 및 탐지하는 치안 및 감시 활동을 수행하거나, 범죄를 수사하거나 범죄자를 체포하는 업무를 수행하는 경찰을 의미한다.

세계 여러나라에서 경찰 등 법집행기관이 얼굴인식 기술의 도입을 추진하고 일부 사례에서는 CCTV 실시간 얼굴인식에 이르면서 인권침해 논란이 커지고 있다. 한국에서는 아직 대중적 논란이 크지는 않지만 최근 한국 경찰 역시 치안활동에 첨단과학기술을 결합한 '스마트치안'을 강조하면서, 지문, 유전정보 등 고전적 형태의 생체인식정보를 넘어 얼굴정보, 행동정보 등 새로운 형태의 생체정보를 활용하는 치안활동을 확대해 가고 있다.

경찰과 사실상 공동관제하고 있는 지방자치단체 CCTV는 최근 급격히 지능화하고 있다. 지난 2002년 서울 강남구가 방범용 CCTV 5대를 도입한 이후로 지방자치단체는 쓰레기투기 방지, 공원 등 시설물관리, 주차 관리, 재난 감

1) 필자: 김민, 이호중, 장여경, 조지훈

시, 학교 진입로 감시 등 여러 목적으로 CCTV 를 설치·운영해 왔다. 광역 및 기초 자치단체 통합관제센터는 치안과 관련된 방범용 외에도 여러 목적의 CCTV를 통합하여 관제하고 있는데 사실상 그 운영을 경찰청에서 파견 나온 경찰공무원에게 일임하고 있고 지방자치단체의 모든 CCTV가 방범용으로 운영되는 것과 마찬가지 상황이다[2].

최근 여기서 통합관제되는 지능형 CCTV는 상황만을 감시하는 아날로그식의 감시형 CCTV와 달리, CCTV 카메라에 촬영된 영상에서 특정 객체를 인식하고 이를 추적할 수 있다. 지능형 CCTV는 화소가 정밀하고 번호판 등 객체 인식과 추적은 물론 대상에 따라 주의 경보를 내보내거나, 공용주차장에 세금체납자의 차량이 들어서면 담당공무원 핸드폰으로 '알림' 문자를 자동으로 발송하는 등 자동화된 처리에 이르고 있다. 서울 성동구에선 범죄 예측을 할 수 있는 CCTV도 개발 중이다. CCTV로 폭력 행위나 배회와 같이 '수상한' 행동을 '자동으로 식별'하고, 더 나아가 범죄 징후로 예상되는 움직임이라고 '평가'를 내리며 그에 대응하는 경찰 출동 신고 등 후속조치에 이르는 '의사결정'까지 가능하다는 것이다. 많은 지능형 CCTV가 얼굴인식 기술의 탑재를 추진 중이다[3].

이미 경찰은 CCTV, 블랙박스 등 범죄현장에서 찍힌 용의자 사진과 구속된 9대 수법범죄자[4] 데이터베이스를 비교·검색하여, 용의자의 신원확인을 신속하게 지원하는 〈범죄예방 3D얼굴인식시스템〉을 개발 및 관리해 왔다. 이 시스템에는 2019년 현재 이미 198,330건의 얼굴인식정보가 포함되어 있다.

경찰은 이 시스템의 구축 및 개인정보 처리에 대한 법적 근거로 개인정보보호법 제15조 제1항 제3호, 형사소송법 제196조, 경찰관 직무집행법 제2조,

---

2) 최미경·최정민(2019), "CCTV 통합관제센터 운영실태 및 개선방안", 국회입법조사처 입법·정책보고서 제29호, p13.

3) AI와 결합한 CCTV…택시 성추행범 잡고 극단선택 막았다, 중앙일보(2020. 2. 26); 최정일(2020), "빅 데이터 분석을 기반으로 하는 첨단과학기법의 현황과 한계 - 범죄예방과 수사의 측면에서", 법학연구, 20(1), p60.

4) 9대 수법범죄 : 강도, 절도, 사기, 위·변조, 약취·유인, 공갈, 방화, 강간, 장물

과학수사 기본규칙 제18조를 들고 있다. 이 조항들은 경찰직무 및 수사에 대한 일반조항으로, 민감정보를 포함한 개인정보시스템의 구축·운용이나 얼굴인식정보 처리에 특별한 규정이 아니다.

경찰은 3D얼굴인식시스템을 계속 고도화할 계획으로, 2024년에는 실시간 CCTV 연계 얼굴인식을 목표로 하고 있으며, 인공지능을 이용하여 나이 등 대상자 특성에 대한 자동화된 식별도 추구하고 있다.

특히 경찰청과 과학기술정보통신부, 산업통상자원부는 공동으로 2018년부터 5개년에 걸쳐 '실종아동등 신원확인을 위한 복합인지기술개발사업'을 진행하고 있다. 이 사업은 실종자 개인/가족의 유전정보를 포함하는 개인정보(DNA, 지문, 신상정보, 실종당시 사진)와 다양한 치안 시·공간 정보를 복합분석하고 최적화된 형상을 추론함으로써, 시공간 및 시점의 동적 변화에 지능적으로 대응하여 고도화된 실종자(초동/장기) 신원분석을 목표로 하고 있다. 이를 위해 경찰 등 참여기관은 △ 유전정보, △ 얼굴정보, △ 행동정보, △ 시·공간정보 등을 수집하고 연계하여 인공지능(AI)기반으로 분석하는 'AI 기반 신원확인 핵심기술'을 개발할 계획이다[5]. 이 사업의 경우 일단 '실종아동수색'이라는 목적에 한정하여 개발되고 있으나, 일단 기술적 기반이 갖추어지면 그 활용이 향후 범죄 수사, 위험방지 등 다양한 경찰활동으로 확대될 가능성이 존재한다.

이처럼 경찰이 법집행 분야에 얼굴인식 기술을 도입하고 다른 정보와의 결합 등 그 적용을 확대해 가면 범죄예방 및 수사를 보다 효율적이고, 효과적으로 할 수 있을 것으로 기대받고 있다. 그러나 인권기반 접근의 관점에서는 수사기관이 얼굴인식 기술을 사용하는 데 대하여 문제의식을 가질 필요가 있다.

그 이유는 첫째, 국민의 기본권을 제한하는 법집행기관의 신기술 사용에 대하여 합헌적이고 합법적인 통제가 필요하기 때문이다.

---

5) 실종아동등 신원확인을 위한 복합인지기술개발사업 신규과제 선정계획 통합공고, 과학기술정보통신부·산업통상자원부·경찰청 통합공고(2018.03.08.); 복합인지기술로 실종아동 안전한 귀가 돕는다, 정책브리핑(2018. 11. 13)

박주희(2020: 430)[6]는 과학기술이나 정보통신기술의 발전에 편승하여 수사기관이 모든 첨단수사기법을 사용할 수 있도록 해서는 안 된다고 지적한다. 수사기법의 발전은 대부분 필연적으로 일반적 행동자유권, 통신의 비밀, 사생활 비밀과 자유, 개인정보자기결정권 등 기본권의 제한을 수반하기 때문이다. 그래서 신기술을 활용한 수사기법에 대해서는 발생할 위험성과 사회적·법적 영향을 미리 검토해야 하며, 기존의 적용가능한 법률 규정이 있더라도 그 규정이 변화된 기술 진화와 통신환경을 반영하지 못한다면 새로운 수사기법과 기본권 침해 간의 비교형량을 통해 다시 입법적인 대응을 논의해야 한다는 것이다.

특히 지능형 CCTV는 아날로그 감시형 CCTV에 비하여 그 기본권을 침해하는 정도가 더욱 크다. 기존의 CCTV가 정보주체의 권리에 간섭하는 경우는 관찰에 따른 사생활의 비밀과 자유의 침해와 더불어 행동, 위치, 사회관계 등 때로는 민감할 수 있는 개인정보를 수집, 이용 및 제공하는 데 따르는 문제였다. 그런데 자동차번호판 등 정보주체를 자동으로 식별하고 나아가 자동 추적 등의 기법으로 개인정보를 자동적으로 처리하는 경우는 좀더 침해가 커진다. 또한 개인정보를 다른 개인정보와 연계하여 개인에 대한 새로운 사실을 발견하고자 하거나 이동이나 위험도에 대한 분석이나 예측 등 개인을 평가하기 위하여 개인정보를 자동적으로 처리하는 '프로파일링'의 경우 그 침해성이 더욱 커진다. 이런 개인정보 처리가 벌금 부과 등 정보주체에게 법적 또는 유사하게 중대한 의사결정을 자동적으로 내리는 데 이른다면 이는 매우 중대한 기본권 제한에 해당한다.

유럽연합 개인정보 보호법(General Data Protection Regulation, GDPR)은 프로파일링 처리를 법적으로 제한하고 정보주체에게 이를 사전에 설명하거나 사후에 반대할 수 있는 권리를 보장하도록 규정하였다. 법적 또는 유사하게 중대한 의사결정을 자동화된 의사결정에 의해서만 내리는 것을 일반적으로 금

6) 박주희(2020), "수사목적의 개인정보 제공·이용에 대한 규범적 통제", 홍익법학 제21권 제2호.

지하고, 법률에 의해 예외적으로 실시하는 경우에도 정보주체의 권리와 자유 및 정당한 이익을 보호하기 위한 적절한 조치를 포함하도록 하였는데 이 조치에는 인간의 개입을 받을 권리를 포함한다. 민감정보 처리는 이 처리가 추구하는 목표에 비례하고 '상당한 공익적 목적'에 한정되는 법률에 근거해야 하며, 개인정보 보호권의 본질을 존중하고 개인정보주체의 기본적 권리 및 이익을 보호하기 위해 적절하고 구체적인 조치를 제공하는 경우에만 허용된다. 그러나 우리의 경우 프로파일링을 제한하거나 자동화된 의사결정을 제한하는 법률을 가지고 있지 않다.

더불어 CCTV 영상촬영 등 국가의 광범위한 감시에 있어서 특히 고려해 볼 부분은 '이중적 비례성 심사'에 대한 견해이다(박원규, 2019: 256). 즉 특정한 감시수단의 대상이 되는 사람의 기본권만을 기준으로 비례성 심사를 하는 것이 아니라, 그러한 감시수단의 사용으로 인하여 위축될 수 있는 국민 전체의 자유도 함께 고려되어야 한다는 것이다. 익명성이 보장되는 상황에서 공개된 장소를 다니는 것과, 누군가가 자신을 알아볼 수도 있다는 느낌을 받는 것은 개인의 행동의 자유에 큰 차이를 가져다줄 수 있기 때문이다. 특히 그러한 감시가 경찰에 의해 이루어진다면 더욱 그러하다.

둘째, 얼굴인식정보는 생체인식정보라는 점에서 더욱 엄격한 제한이 필요하다. 법집행기관이 얼굴인식 기술을 활용하면 육안 식별 등 전통적인 방식으로는 처리할 수 없는 방대한 양의 정보처리와 감시를 가능하게 한다. 얼굴인식정보를 다른 개인정보와 결합할 경우 자동으로 신원확인이 가능한 대량감시수단이 될 수 있으며, 특히 무차별 대중을 대상으로 하는 실시간 얼굴인식(live facial recognition)의 경우 그 침해성이 매우 크다.

생체인식정보는 사람의 고유한 신체적, 행동적 특징을 이용하여 개인을 나타내는 정보로서, 이러한 정보의 특수성은 다른 개인정보와는 달리 살아있는 동안 그 사람과 결합되어 있고, 이름이나 주소, 식별번호, 암호처럼 변경할 수 없다는 점에 있다. 생체인식기술은 개인이 가진 신체 특징이 태어나서 죽을 때까지 변하지 않는다는 점과 신체 일부가 일치하는 사람은 없다는 점에 착안한 기술인 것이다. 그렇다면 생체인식정보의 유출 시, 이에 대한 변경이 불가

능하여 지속적으로 정보가 악용될 수 있으므로 일반 개인정보보다 더욱 강화된 보호가 필요하다(김일환, 2019: 493)[7].

법집행기관의 입장에서 얼굴인식 기술이 매력적인 이유는 국가기관이 광범위하게 취득, 보관하는 데이터베이스상의 얼굴사진을 인식대상의 사진 또는 동영상과 대조하여 쉽게 신원확인을 할 수 있고, 홍채, 지문과 같은 생체인식정보와 달리 얼굴인식정보의 경우 수집 단계에서 원거리 촬영 등이 가능하기 때문에 정보주체의 협조가 필수적이지 않다는 점이다. 반면에 국가기관이 정보주체의 동의를 받지 않고서도 얼굴이미지를 광범위하게 수집할 수 있기 때문에 상시적 감시가 가능해진다는 점에서 침해성이 클 수 있다(이성기, 2018: 174)[8]. 또한 공공기관의 얼굴인식 기술 사용을 무제한적으로 허용한다면 공공장소 CCTV 뿐 아니라 페이스북, 인스타그램등 소셜네트워크에 개인이 자발적으로 공개한 사진과 영상 또한 무제한적으로 수집 및 분석될 우려가 있으며, 그 결과 국민에 대한 빈틈없는 감시가 이루어질 가능성이 존재한다. 경찰이 상시적으로 다양한 장소에 설치되어 있는 CCTV 영상에 대한 복합적인 분석을 수행할 경우 대상자의 이동경로를 확인하고 향후의 행동 또한 예측할 수 있기 때문에 개인정보 자기결정권과 일반적 행동의 자유에 대한 심각한 침해로도 이어질 수 있다. 이 경우 국민은 “감시받는다는 기분”을 가지게 되고, 공공장소에서 익명으로 다닐 수 있는 자유 또한 침해받게 된다. 그 결과 자유주의 국가에서의 핵심 가치인 개인의 인격발현에 심각한 장애를 야기할 수 있다. 더 나아가 집회 및 그 인근에서 촬영된 영상정보를 광범위하게 수집하고 영상에 촬영된 모든 사람들의 얼굴정보를 신원확인목적으로 저장·분석한다면 국민들이 집회참가를 주저하게 되는 위축효과 또한 발생시킬 수 있다. 즉 국가에 의한 광범위한 감시는 국민들의 모든 기본권 행사를 위축시킬 수 있는 것이다(박원규, 2019: 252)[9].

---

7) 김일환(2019), “생체인식정보의 보호와 이용에 관한 법제정비방안에 관한 연구”, 유럽헌법연구 제30호.

8) 이성기(2018), “생체인식정보와 감시: 수사기관의 얼굴 인식기술을 활용한 신원확인 행위의 법적 근거와 한계에 관한 연구”, 法과 政策硏究 第18輯第1號.

9) 박원규(2019), “경찰의 안면인식기술 사용에 관한 법적 검토”, 「입법과 정책」 제11권

Ⅱ. 얼굴인식 기술의 개념

1. 얼굴인식 기술의 개념과 작동방식

얼굴인식 기술이란 사람의 얼굴을 자동으로 식별하거나 대조 또는 분류하는 생체인식 기술이다. 카메라와 같은 영상정보처리기기를 통해 수집한 디지털 이미지에서 눈, 눈썹, 코, 입, 귀, 이마, 얼굴 윤곽 등 각 개인 얼굴의 고유한 부위를 분석하여 특징되는 데이터를 추출하고 사전에 등록된 데이터베이스의 다른 얼굴 특징점과 비교하여 인식을 수행한다. 2차원 또는 3차원 이미지를 이용하거나 열화상 이미지를 이용하는 방식이 있으며 특징점의 추출과 분석에서 정확도가 갈린다.

얼굴인식 기술은 일반적으로 1. 얼굴이미지 수집 및 검출, 2. 검출된 얼굴 보정 및 특징점 추출, 3. 비교 및 인식의 단계를 거친다. 과거 얼굴인식 기술의 얼굴 특징점 추출을 위한 방식은 실제 상황에서 적용 시 촬영된 얼굴의 각도, 조명 방향과 빛의 품질, 카메라의 성능 등 주변 환경의 변화에 의해 그 성능이 매우 저하된다는 단점이 있으나 최근 고도화된 컴퓨팅 성능과 심화된 인공지능 딥러닝 연구의 적용 등으로 정확도가 향상되고 있는 추세이다. 그러나 딥러닝 기반의 기술은 알고리즘 모델이 학습한 데이터셋의 구성에 따라 피부색, 젠더, 연령 등에 차별적 오류가 발생한다는 취약점이 지적되고 있다.

얼굴인식 기술은 비접촉으로 개인식별이 가능하고 다른 생체인식 기술과 다르게 정보주체의 인지 없이 대량으로 개인을 식별하거나 대조하는 등 생체인식을 수행할 수 있다. 생체인식 형판(biometric template) 추출 및 저장을 위한 얼굴 이미지 또한 정보주체의 동의 없이 쉽게 수집되고 처리될 수 있다. 이러한 생체인식정보 수집 및 처리의 용이성과 편의성이라는 특징으로 인해 얼굴인식 기술이 광범위하게 도입되고 있는 동시에, 과도한 개인정보 침해와 대량감시의 문제가 지속해서 제기된다. 그렇기에 얼굴인식 기술을 그 사용 목

제2호, 국회입법조사처.

적에 따라 구분해 살펴보는 것이 중요하며 이는 크게 검증, 식별, 분류로 나눠 살펴볼 수 있다[10].

① 검증(Verification)

인증은 흔히 본인 확인이라고 할 수 있으며 두 개의 얼굴인식 템플릿을 비교하는 1:1 매칭 방식으로 진행된다. 이러한 1:1 방식의 얼굴인식은 시스템에 입력된 두 얼굴 이미지가 동일한 인물인지 여부만을 판단하기에, 중앙화된 데이터베이스가 필수적이지 않다. 공항에서 출입국 검사를 위해 현장에서 스캔한 여권의 증명사진과 실제 얼굴을 촬영하여 비교하는 경우가 대표적인 얼굴 검증 기술의 사례이다.

② 식별(Identification)

식별은 특정 대상의 얼굴 이미지를 데이터베이스에 저장된 모든 N명의 얼굴인식 템플릿과 비교하여 일치 및 유사도 여부를 판단하는 1:다(多) 매칭 방식으로 진행된다. 식별을 위해 구성한 데이터베이스의 얼굴 이미지 또는 얼굴인식 템플릿의 수집과 처리의 과정에 있어 개인정보 침해 문제가 발생할 수 있다. 식별 용도의 얼굴인식은 주로 공공장소에 대한 대량 감시 목적으로 활용되는데, 실제 환경의 카메라를 통해 촬영된 얼굴 이미지의 품질, 빛, 복장, 거리, 얼굴 각도 등을 통제할 수 없기에 그 비교에 있어 거짓양성(false positve) 등 오류가 발생할 가능성이 크다. 또한 대조 식별의 과정에 있어 불특정 다수의 얼굴 이미지를 동의 없이 수집하고 저장 및 처리하며 개인정보 자기결정권을 제한하는 결과를 가져올 수 있다.

③ 분류(Categorisation)

얼굴 분석이라고도 불리우는 분류는 특정 대상의 얼굴 이미지를 통해 개인의 특성을 추출해내고 해당 특성에 따라 개인을 분류하는 것이다. 특정 인물

10) FRA(2019), "Facial recognition technology: fundamental rights considerations in the context of law enforcement".

의 신원을 확인하는 일반적 얼굴인식 기술과는 다르게, 이는 주로 성별, 나이, 출신 민족을 분류해내거나 감정 상태, 거짓 또는 진실 유무를 추론하는 것을 목표로 한다. 그러나 이러한 얼굴 분류 및 분석은 표면에 드러나는 몇몇 특징으로 사람의 감정이나 상태를 해석하고 판단할 수 있다는 믿음을 기반으로 하며 과학적 타당성에 대한 논란이 제기되고 있다. 그럼에도 불구하고 현재 인공지능 면접, 출입국 관리 등의 목적으로 이미 사용되고 있거나 이를 도입하기 위해 연구되고 있다.

2. 얼굴인식 기술의 성능 평가와 논란

얼굴인식 기술의 성능을 평가할 때에는 보통 거짓양성(False Positives)이라 불리우는 오인식률(또는 타인수락률, FAR: False Accept Rate)과 거짓음성(False Negative)이라 불리우는 오거부율(본인거부율, FRR: False Rejection Rate), 그리고 동일 오류율(ERR:Equal Error Rate) 등을 지표로 확률을 측정하여 분석하는 것이 일반적이다.

거짓양성이란 얼굴인식 시스템이 입력된 인물의 얼굴에 대해 데이터베이스의 특정 얼굴과 일치한 것으로 판단하여 결과를 내놓았지만, 실제로는 일치하지 않는 경우이다. 예를 들어, 경찰이 A의 얼굴을 입력하였으나 시스템은 B라고 판단하는 것이다. 이처럼 특정 용의자의 얼굴과 범죄자 데이터베이스의 얼굴을 대조하는 경우 거짓양성이 높을수록 무고한 사람이 용의자로 몰리거나 법적 조치를 당하는 일이 발생할 수 있으므로 가능한 한 오인식률이 적어야 한다. 그러나 거짓양성을 낮추기 위해 얼굴인식정보를 판단하는 임계값을 엄격하게 설정한다면, 그와 비례하여 입력된 A의 얼굴을 A라고 판단하지 않는 거짓음성의 발생이 많아질 것이다. 이러한 거짓양성과 거짓음성의 비율, 즉 오인식률과 오거부율이 서로 같아지는 비율을 동일 오류율이라고 하는데, 일반적으로 동일 오류율이 낮을수록 보다 정확한 성능이라고 말할 수 있다.

얼굴인식 기술은 어떤 시스템이냐, 어떤 상황에서 사용하냐에 따라 그 정확성이 천차만별이며 어떤 시스템도 모든 조건에서 완벽하게 정확하지 않다. 또한 인공지능 기술의 편향성 문제로, 동일한 알고리즘이더라도 피부색, 젠더 등

에 따라 심한 성능의 차이를 보여준 연구 결과가 잇달아 공개되며 알고리즘 자체에 내재된 차별 문제가 강하게 제기되고 있다. 마이크로 소프트, FACE++, IBM의 상업적 얼굴인식 알고리즘을 평가한 2018년 MIT 미디어 랩의 연구에 의하면 3사 모두 남성에 비해 여성에 대해, 밝은 피부색에 비해 어두운 피부색의 인물에 대해 더 높은 오인식률을 보였으며, 어두운 피부색 여성 대상의 경우 20.8~34.7%의 오인식률을 보였다[11]. 또한 2019년 미국표준기술연구소(NIST)의 연구에 따르면 1:1 방식의 검증 알고리즘의 경우 백인에 비해 서아프리카와 동아프리카, 미국 원주민, 아프리카계 미국인, 아시아계에 대해 10배에서 100배 정도의 거짓양성률을 보였고 여성과 노인 및 어린이에게도 차별적 경향을 보여준 것으로 드러났다[12].

11) Gender Shades: Intersectional Accuracy Disparities inCommercial Gender Classification 〈http://gendershades.org/overview.html〉

12) NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software 〈https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software〉

III. 해외 현황 및 관련 법제도

1. 미국

가. 현황

미국은 경찰과 연방수사국(FBI)을 비롯한 다양한 법 집행기관에서 범죄 예방과 수사, 출입국 통제 등의 목적으로 얼굴인식 기술을 사용하고 있다. 여러 기관에서 용의자 머그샷 데이터베이스 등을 기반으로 소셜미디어, CCTV 이미지의 얼굴을 비교하거나 스마트폰, 태블릿과 같은 모바일 기기를 활용해 직접 보행자나 운전자의 사진을 촬영하고 신원 확인을 시도해 왔다. 각 주와 시 그리고 법집행기관마다 사용하는 소프트웨어나 정책, 검색 가능한 얼굴정보에는 차이가 있지만, 전체 주 및 시, 법집행기관 중 25% 이상이 자신들의 데이터베이스 또는 타 기관의 데이터베이스를 통해 얼굴인식 검색 및 비교를 실행하고 있거나 그러한 시스템에 접근할 권한이 있을 것으로 추정하고 있다[13].

(1) 연방수사국(FBI)

NGI-IPS 및 FACE

2010년 이후 연방수사국은 1999년부터 운영해왔던 기존의 지문 식별 시스템(Integrated Automated Fingerprint Identification System, IAFIS)을 차세대 인식 시스템(Next Generation Identification, NGI)으로 대체하기 시작하며 지문 정보 뿐만 아니라 얼굴인식정보를 포함한 다양한 종류의 생체인식정보 데이터베이스의 구축을 시작했다. NGI 구축을 위해 수백만 명의 개인으로부터 지문, 홍채, 흉터, 문신 등의 생체인식정보를 수집하였으며, 이에는 범죄를 사유로 수집된 생체인식정보 뿐만 아니라 신원조회, 면허 조회, 이민 등 비범죄 사유로 인해 수집된 생체인식정보 또한 포함되어 있다[14].

---

13) Georgetown Center on Privacy and Technology

14) https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi

이후 연방수사국은 전국적인 얼굴인식 기술의 활용을 위해 주(州)간 사진 시스템(Interstate Photo System, IPS)을 구축하였고 내부 부서로 얼굴인식 전담 부서인 '얼굴 분석과 비교 및 평가 부서'(Face Analysis, Comparison and Evaluation Service Unit, 이하 FACE)를 두었다. 연방수사국은 주간 사진 시스템을 통해 주 및 지방의 법 집행기관에게 얼굴 검색 등의 시스템을 제공하는데 이에는 용의자의 머그샷 등, 형사 절차에서 수집된 사진이 데이터베이스로 활용된다. FACE 부서는 이러한 주간 사진 시스템에 대한 접근 권한을 관리하며 각 주 및 기관과의 협약을 통해 기존 생체인식 데이터베이스를 넘어 최소 27개 주가 소유한 운전면허증 데이터베이스와 국무부의 비자, 여권 데이터베이스 등을 직접적으로 사용하거나 검색을 위한 열람 요청이 허용된다. FBI는 FACE를 통해 2011년 8월부터 2019년 4월까지 총 15만 3636장의 인물 식별 요청을 받아 데이터베이스에 검색한 것으로 알려져 있으며, 2019년 기준 검색 가능한 얼굴 사진의 총 수는 6억 4100만장이 넘고 대부분 비범죄 미국인과 외국인의 사진을 포함하고 있다. 미국 성인의 절반 정도가 최소 한 장 이상의 사진이 얼굴인식 검색이 가능한 데이터베이스에 포함되어 있는 셈이다[15].

(2) 경찰

미국 전역의 주 경찰서와 지방 경찰서가 자체적으로 얼굴인식 시스템을 구축하고 있으며 상당수는 FBI의 얼굴인식 시스템보다 더 고도화된 것으로 파악된다[16]. 미국의 가장 오래된 얼굴인식 시스템 중 하나인 플로리다의 피넬라스 카운티 보안관 사무소의 얼굴인식 시스템은 2001년 도입되었으며 242곳의 연방, 주 및 지방 기관에서 사용할 수 있고 링컨 시, 마리코파 카운티 등의 지방

15) "FACE RECOGNITION TECHNOLOGY DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains." source: EFF(2019), "Who Has Your Face" 〈https://www.eff.org/press/releases/are-your-identification-photos-face-recognition-database GAO〉

16) https://www.banfacialrecognition.com/map/; https://www.perpetuallineup.org/#map

경찰은 각각 주의 차량국과 협약을 맺어 수천만장의 운전면허 사진을 데이터베이스로 활용한다. 또한 시카고, 댈러스, 로스앤젤레스를 포함한 5개 이상의 경찰서는 공공장소를 대상으로 한 실시간 얼굴인식을 실행하거나 최소 실행 가능한 기술을 구매한 것이 확인되었다. 이러한 정보는 소수의 시스템을 제외하곤 공개되지 않았으며 오용에 대한 감사를 받지 않는 것으로 드러났다.

디트로이트 시는 일부 지역에 대해 실시간 얼굴인식 기술을 활용하고 있다. 이는 법 집행기관이 민간에서 설치한 CCTV까지 활용할 수 있게 만든 프로젝트 그린라이트와 함께 작동한다. 프로젝트 그린라이트 디트로이트는 시의 법 집행기관과 협약을 맺은 민간 사업자가 CCTV를 직접 구매하여 설치하고, 이를 통한 영상 피드를 디트로이트 경찰국이 실시간으로 관리하고 모니터링하는 정책으로 주유소, 패스트푸드점, 주류 판매점과 같은 심야 영업 사업장으로 시작해 교회, 호텔, 지역 마약치료 센터, 공공주택 및 학교까지 확장되었다. 디트로이트 시의 실시간 얼굴인식 시스템은 CCTV 뿐만 아니라 일반 카메라, 드론 영상, 바디캠 등 실시간으로 영상을 보낼 수 있는 모든 기기와 연동될 수 있으며, 그 데이터베이스로는 시가 보유한 50만 장의 머그샷과 함께 운전면허 사진을 포함한 미시간 주의 얼굴 사진 데이터베이스를 활용할 수 있는 권한이 있다.

샌디에고 정부 협의회(SANDAG)는 2012년부터, 태블릿 PC, 스마트폰 등 얼굴인식에 특화된 기기를 통해 직접 대상을 촬영하고 데이터베이스와 비교하여 신원을 확인할 수 있는 시스템 TACIDS(Tactical Identification System)을 운영해왔다. 해당 시스템은 샌디에고를 비롯한 각 시와 카운티의 기관이 서로 범죄와 관련한 정보 및 시스템을 실시간으로 공유하기 위한 시스템[17]의 일부로써, 경찰과 국토안보부, 이민관리국 등 지방기관과 연방기관을 합해 최소 66개 기관이 접근할 수 있으며, 이 중 28개 기관이 이를 활용하고 있는 것으로 밝혀졌다. TACIDS는 140만 장 이상의 머그샷 데이터베이스를 검색할 수 있으며, 운전면허 사진 검색이나 영상에서 나온 실시간 얼굴 인식은 허용하지

17) http://www.arjis.org/SitePages/Home.aspx

않고 있다.

그러나 2019년 10월 캘리포니아 주에서 경찰의 바디 캠 얼굴인식 기술 사용을 3년간 금지하는 조례가 통과되며 사용이 중지되었다[18].

(3) 출입국 관리

미국 국토안보부는 출입국 통제를 위해 생체인식정보를 포함하는 몇 개의 프로그램을 운영해 왔다. 미국 방문자 및 이민자 신분표시기술(The United States Visitor and Immigrant Status Indicator Technology, US-VISIT)은 미국을 방문하는 외국인의 개인 정보를 수집하고 국경에서의 여행자 통제를 위한 국토안보부의 프로그램으로, 지문과 디지털 사진을 포함한 생체인식정보를 수집한다. 처음에는 입국을 위해 비자가 필요한 방문자에게만 적용되었지만, 2004년 이후 미국 비자면제국의 여행자들에게도 적용되었으며 미국 시민이 아닌 모든 사람들을 대상으로 확대되었다.

2017년 이후 트럼프 행정부의 추진으로 JFK공항을 포함한 미국 주요 공항 27곳에서 국제선을 이용하는 모든 외국인을 대상으로 얼굴인식 시스템이 도입하여 사용되고 있다. 해당 얼굴인식 시스템은 1:다(多)와 1:1 방식 모두를 수행할 수 있으며, 젯블루(JetBlue)와 같은 민간 항공사가 수집하여 국토안보부 산하의 관세국경보호청(CBP)의 데이터베이스에 입력한 탑승객의 여권사진을 탑승 수속과정에서 촬영한 탑승객의 얼굴 사진과 비교하는 방식으로 이루어진다. 이는 이후 외국인 입국자의 출국 여부를 확인하는 등 불법 체류 및 테러용의자 수사 등의 목적으로 활용될 수 있다. 미국 시민권자는 얼굴인식정보 처리에 대한 동의를 철회할 수 있게 되었으나, 외국인의 경우 얼굴인식 기술을 도입하지 않은 항공사의 항공편을 이용하는 게 아닌 이상 동의를 거부할 수 없다. 또한 외국인의 경우 수집된 얼굴정보는 관세국경보호청의 시스템에 75년간 보관되는 것으로 알려져 있다[19].

---

18) https://www.eff.org/deeplinks/2019/10/victory-california-governor-signs-ab-1215; https://www.eff.org/deeplinks/2019/12/victory-san-diego-suspend-face-recognition-program-cuts-some-ice-access

2020년 9월, 미국 회계감사원(General Accounting Office, GAO)는 출입국 관리 과정에서의 얼굴인식 기술의 사용에 개인정보 침해 문제가 있다는 보고서를 통해 개인정보 처리에 대한 적절한 통지를 할 것, 얼굴인식 시스템을 사용하는 곳에서 통지가 가능하도록 할 것, 개인정보 보호를 위해 감사 계획을 개발하고 구현할 것 등의 권고 사항을 발표했다[20].

나. 관련 법 제도 및 비판

(1) 개요

현재 경찰과 연방수사국을 비롯한 법 집행기관의 얼굴인식 기술 사용을 규제하는 연방법은 존재하지 않는다. 법 집행기관이 얼굴 정보를 수집하고 보관하는 것은 연방법 제33장에 근거하고 있으며 이 규정은 신원확인, 범죄수사 등을 위해 필요한 정보를 제한없이 수집할 수 있으며 이를 다른 기관과 교환할 수 있게 한다. 수사기관이 직접 촬영하거나 CCTV 등을 통해 촬영된 공개된 장소의 경우, 객관적으로 기대 가능한 프라이버시가 인정되지 않아 정보주체의 동의가 필요하지 않으며 스스로 인터넷에 공개하거나 제출한 사진 또한 제공받을 수 있다. 또한 이렇게 수사기관이 얼굴 정보를 수집하고 보관하는 것에 대한 적법성이 인정되는 경우, 그 정보를 얼굴인식 데이터로 변환하여 데이터베이스를 운영하는 것에 대한 다른 법적 근거가 필요하지 않다[21].

그러나 얼굴인식 기술의 급격한 발달과 도입 확대, 인공지능의 편향성으로 인한 차별 문제가 대두되기 시작하며 규제의 흐름이 나타났다. 특히 미국의 경우 인종, 여성 등에 대한 높은 오인식 비율에 대한 연구 결과와 기존의 차별

---

19) The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show 〈https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for〉

20) CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues 〈https://www.gao.gov/products/GAO-20-568〉

21) 이성기(2018), 위의 글

적 법 집행으로 인한 과도한 통제로 시민들의 반발이 커지며 여러 주와 지방 차원에서 규제 법안을 마련하기 시작했다.

(2) 공공 영역에 관한 규제

2019년 5월, 캘리포니아 주 샌프란시스코 시에서 미국 최초로 시 법 집행기관의 얼굴인식 기술 사용을 금지하는 조례가 통과되었다. 해당 조례는 전반적인 감시 기술이 시민 모두의 프라이버시를 위협할 수 있지만 역사적으로 특정한 지역사회와 집단에게 더 큰 위협과 억압이 되는 등 그 차별적 법 집행 가능성에 대해 명시하고 있으며, 특히 얼굴인식 기술의 경우 시민권과 자유권에 대한 위험이 이익보다 훨씬 더 크다는 걸 근거로 하고 있다. 해당 조례는 경찰을 포함한 지방 기관의 얼굴인식 기술을 포함한 여러 감시 기술의 사용을 전면적으로 금지하며, 그외 타 도시 및 기관 소유의 감시 기술로부터 정보를 공유 받는 행위 또한 규제한다. 다만 지역 내 공항 등을 관할하는 연방 기관에는 규제의 범위가 미치지 않는다.

샌프란시스코 시를 시작으로 메사추세츠 주 섬머빌, 캘리포니아 주 오클랜드, 버클리 등 약 10곳의 도시가 유사한 얼굴인식 금지 조례를 통과시켰으며 각 주 또한 이를 이어 받아 캘리포니아 주, 뉴 햄프셔 주, 오레건 주에서는 경찰의 바디카메라 얼굴인식 기술 사용을 금지하는 법안이 통과되었다[22].

2020년 3월 워싱턴 주에서 얼굴인식을 규제하는 최초의 주 법률이 제정되었다. 해당 법안은 얼굴인식 기술의 활용을 위해 정부 부처와 조달 기업에 일정 정도의 투명성과 책임성을 부여하고 있다[23]. 워싱턴 주의 법은 얼굴인식 기술을 활용한 서비스를 개발, 조달, 사용하려는 기관에 대한 투명성과 일정한 의무를 부여하지만 법적 의무의 구체적 집행 및 강제수단을 두고 있지 않으며 '긴급 상황' 등을 사유로 실시간 얼굴인식 등을 허용하는 점 등에 있어 기존의 지방정부 차원의 규제에 비해 기술의 사용을 용인하는 약한 규제에 머물고 있

22) https://www.eff.org/aboutface/bans-bills-and-moratoria

23) 한국인터넷진흥원(2020), 인터넷 법제동향(2020년 4월)

다[24]. 얼굴인식 기술에 대한 금지를 요구해온 미국시민자유연명(ACLU)는 해당 법이 오히려 인종차별적인 얼굴인식 기술을 계속해서 사용할 수 있도록 허용하고 적절한 보호장치도 제공하지 못하고 있다고 비판하였다.

주 및 지방정부의 의무	얼굴인식을 활용한 서비스의 내용과 목적을 포함한 계획서, 의향서를 기술위원회에 제출해야 함
	얼굴인식 기술을 개발, 조달, 활용하기에 앞서 책무성(accountability) 보고서를 작성해야 함.
	책무성 보고서는 얼굴인식 기술을 활용하는 해당 서비스의 내용, 성능과 한계, 예상되는 혜택과 부작용, 정확도, 소수집단에 미치는 영향과 대응책 등에 관한 상세한 내용을 포함하며 웹사이트 포스팅 등을 통해 대중에게 정보가 공개되어야 함
	지속적인 감시나 실시간 얼굴인식 등의 활용을 위해서는 영장을 발부받아야 함(긴급 상황이나 실종자 탐색을 목적으로 법원의 명령을 받은 경우는 제외)
	인종, 민족, 국적, 출생지, 이민 상태, 나이, 장애, 성별, 성정체성, 성적 지향 또는 기타 법으로 보호되는 특성을 확인하기 위한 목적으로 얼굴인식 기술 활용은 금지됨
	얼굴인식 기술을 활용하는 수사관 및 검사들은 재판 전 피고인 측에 해당 사실을 고지해야 하며 얼굴인식 결과를 유일한 증거로 하여 형사사건의 혐의를 구성할 수 없고, 개인에게 법적 효과 또는 그와 유사한 중대한 효과를 낳는 결정과 관련된 경우 의미있는 인적 검토를 보장해야 함.
조달 기업의 의무	편견과 차별과 관련된 사항을 정부에 공개해야 함
	기관의 독립적이고 합리적인 테스트를 위해 API 또는 다른 기술적 기능을 제공해줘야 함.
	인종, 피부색, 성별, 나이 등 신체적인 특징 전반에 걸쳐 그 정확도와 불공정성에 대한 별도의 시험과 이를 줄이기 위한 계획과 실행을 요구로 함.

24) 이창민(2020), "안면인식정보 보호 및 안면인식기술 규제에 관한 미국법 연구", 법률신문 연구논단(2020. 9. 14.)
〈https://m.lawtimes.co.kr/Content/Info?serial=164179〉

이렇게 지방정부의 금지 조례가 이어지며 연방 차원의 얼굴인식 규제의 필요성 또한 대두되었다. 이는 얼굴인식이 가져오는 차별에 대한 연구들[25], 클리어뷰(Clearview AI) 사건, Black Lives Matter 운동을 필두로 한 급격한 경찰 개혁의 운동 등의 영향으로 논의가 활발해졌으며 현재 '얼굴인식의 윤리적 사용법(Ethical Use of Facial Recognition Act)', '국가 생체인식 정보보호법(National Biometric Information Privacy Act of 2020)' 등의 법안이 제안되었다.

(3) 민간 영역에 관한 규제

2008년 일리노이 주는 얼굴인식정보를 포함한 생체인식정보를 규율하는 미국 최초의 법인 일리노이 생체인식 개인정보 보호법(Biometric Information Privacy Act, BIPA)을 제정하였다. 해당 법은 얼굴인식정보를 열거된 생체인식 바이오메트릭 식별자(biometric identifier) 중 하나로 명시하여 일반 개인정보보다 강력하게 보호하고 있으며 그 내용은 다음과 같다[26].

- 바이오메트릭 식별자(biometric identifier) = "망막 또는 홍채 스캔, 지문, 성문, 손 또는 '얼굴 형상'(face geometry)의 스캔(scan)"이라고 한정적으로 열거하여 정의
- 바이오메트릭 정보(biometric information) 개인의 바이오메트릭 식별자에 기초한 정보로서 개인을 식별하는데 사용되는 정보(그것이 어떻게 수집, 전환, 보관, 공유되었는지 불문함)
- 바이오메트릭 식별자/정보를 보유한 민간 기업(private entity)은 서면 정책 공개, 보관기록대장, 파기 가이드라인을 수립해야 함
- 민간 기업은 사전에 당사자에게 바이오메트릭 식별자/정보를 수집 또는 보관할 것이라는 점과 그 구체적 목적과 사용기간을 고지하고 서면 동의를 받아야 함
- 위법 행위로 피해를 입은 사람은 위반 당사자를 상대로 주 또는 연방법원에 소송을 제기할 수 있는 권리를 가짐

---

25) "Gender Shades: Intersectional Accuracy Disparities inCommercial Gender Classification" 〈http://gendershades.org/overview.html〉

26) 이창민(2020), 위의 글

서면 동의와 고지, 소송에 대한 권리를 보장하고 있는 일리노이 생체인식 개인정보 보호법은 강력하지만 민간 기업을 규율하며 법 집행기관의 생체인식 기술 또는 정보 처리를 규율하고 있지 않다.

2020년 9월, 오레곤 주 포틀랜드 시는 미국 최초로 민간영역의 얼굴인식 기술 사용을 금지시키는 조례를 통과시켰다. 2021년부터 시행되는 해당 조례는, 얼굴인식 기술 사용을 금지함에 있어 성별과 인종에 대한 편향적 결과 및 소외 지역에 대한 과대한 감시와 그에 미치는 악영향을 근거로 들고 있으며 내용은 다음과 같다.

- ‘얼굴 인식 기술(Face Recognition Technologies)’을 개인의 얼굴 특징을 식별, 검증, 분류를 위해 또는 개인에 대한 정보를 추출하기 위해 얼굴인식 기술을 활용한 자동화된 또는 반자동화된 절차로 규정
- 민간 기업(private entities)은 공공시설에서 얼굴인식 기술을 사용하는 것이 금지되며 예외로 (1)연방법, 주법, 지방법을 준수하기 위한 목적 (2)사용자 개인이나 고용 관계에서 통신 기기 및 전자 기기에 접근하기 위한 사용자 인증 목적 (3)소셜미디어 어플리케이션의 자동화된 얼굴 감지를 둠

해당 조례는 민간 영역을 대상으로 한 내용이나, 포틀랜드 시는 경찰과 같은 공공 영역의 얼굴인식 기술 사용의 경우 샌프란시스코 조례와 같은 별도의 조례를 통해 규제하고 있다.

(4) 인권침해 논란

클리어뷰 AI (Clearview AI)

클리어뷰AI는 민간회사, 법 집행기관 및 개인에게 얼굴인식 서비스를 제공하는 미국 기업으로 페이스북, 유튜브, 인스타그램 등 소셜미디어를 비롯한 인터넷에서 공개적으로 접근 가능한 이미지를 자동으로 수집하여 얼굴 검색용 데이터베이스로 사용하는 얼굴인식 기업이다.

2020년 1월 뉴욕타임스의 보도[27]를 통해 알려진 이 기업은 사용자는 물론이고 소셜미디어 기업의 동의나 협조 없이 막대한 이미지를 스크랩하며 데이

터베이스로 활용했으며 최소 30억장 이상의 이미지에 접근 가능한 것으로 알려졌고 이는 미국 정부가 보유하고 검색할 수 있었던 얼굴정보의 수를 훌쩍 뛰어넘는다.

보도 이후 전자개인정보센터(EPIC)을 비롯한 40여곳의 시민단체가 미국 대통령 직속 프라이버시와 시민자유 감시위원회(Privacy and Civil Liberties Oversight Board)에 얼굴인식 기술 사용 중지를 요청하는 서한을 보내는 등 정부와 법 집행기관의 얼굴인식 기술 규제에 대한 전세계적 논쟁이 촉발되었다. 트위터, 페이스북, 구글 등의 소셜 미디어 기업 또한 자사 플랫폼을 통한 이미지 스크랩 중단을 요청하며 자사 정책에 반한다는 의사를 밝혔다.

클리어뷰AI는 또한 버몬트 주 소비자 보호법, 일리노이 주 생체인식 개인정보 보호법, 캘리포니아 주 소비자 개인정보 보호법, 뉴욕 주 개인정보 보호법 등 위반으로 주 정부와 시민단체로부터 소송을 제기당했다.

2020년 2월 유출된 고객 자료에 따르면 미국 이민세관집행국, 각 주와 지방 경찰 및 법무부 산하 기관을 포함해 27개국의 2,200단체가 실제로 계약 또는 시험 활용을 진행한 것으로 밝혀졌다[28]. 이후 유럽연합 개인정보보호이사회(EDPB)는 유럽연합의 법 집행기관이 클리어뷰AI 서비스를 이용하는 것은 유럽연합 개인정보 보호 규제의 틀에서 벗어난 불법 행위라고 해석하였고, 영국과 호주, 캐나다의 개인정보 보호 당국 또한 조사에 들어가 각 국가 기관의 클리어뷰AI 사용이 중지되었다.

차별적 기술과 집회 및 시위 얼굴인식 논란

미국 법 집행기관의 얼굴인식 기술 활용은 유색인종에 대한 차별적인 집행과 편향적인 기술적 결과로 인한 무고한 시민의 체포와 더불어, 집회 및 시위

27) The Secretive Company That Might End Privacy as We Know It <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>

28) Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>

에 참가한 시민의 신원을 확인하기 위해 사용되고 있어 그 논란이 크다.

2020년 1월, 디트로이트 시에서 얼굴인식 기술로 인해 무고한 시민이 체포되는 일이 발생했다. 이에 대해 디트로이트 경찰 측은 해당 얼굴인식 시스템의 오인식률이 96%에 달해 신뢰성에 문제가 있다고 밝혔다. 또한 70번의 사용 중 인종을 알 수 없었다는 2명을 제외한 68명의 대상자가 흑인이었으며 대조에 사용된 사진은 SNS나 CCTV를 통해 확보한 것으로 알려졌다[29].

워싱턴 DC에서 진행된 한 시위의 참가자는 SNS에 올라온 스마트폰 영상을 통해 신원이 식별되어 폭행 및 공무 집행 방해 혐의로 기소되었는데, 해당 재판 문서를 분석한 워싱턴 포스트에 따르면 해당 시위 참가자의 신원을 식별한 것은 수도권얼굴인식수사지휘시스템(National Capital Region Facial Recognition Investigative Leads System, NCRFRILS)으로 2019년 이후 1만 2000회 이상 사용되었으며, 140만 명이 데이터베이스에 포함되어 있고 14개 지방 및 연방 기관이 이에 대한 접근권을 가지고 있는 것으로 드러났다[30]. 하지만 해당 프로그램은 시험 단계에 있다는 이유로 개발 및 활용에 대한 정보가 공개된 적이 없으며 미국의 시민단체는 이러한 불투명한 운영이 수사기관이 얼굴인식 기술을 전국적으로 활용하는 전형적인 방법이라고 비판했다. 그 외에도 뉴욕, 마이애미 경찰이 클리어뷰AI를 활용해 시위 참가자의 신원을 식별하고 체포했다는 사실이 드러나기도 했다[31].

---

29) Wrongfully Accused by an Algorithm <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>

30) Facial recognition used to identify Lafayette Square protester accused of assault <https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html>

31) Miami Police Used Facial Recognition Technology in Protester's Arrest <https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/> ; NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment <https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment>

이러한 시민에 대한 탄압과 인공지능 기술이 내제한 편향성, 수사기관의 차별적 법 집행은 얼굴인식 기술에 대한 강력한 금지 요구를 불러왔고 이는 기술 개발 기업에도 영향을 미쳤다. 대표적으로 IBM은 의회에 보내는 공개적 서한을 통해 "대량 감시와 인종 프로파일링에 이용되며 인권과 자유를 침해하는 얼굴인식을 비롯한 모든 기술의 사용에 반대한다"는 입장과 함께 얼굴인식 및 분석 소프트웨어와 관련한 기술 제공을 중단하겠다고 밝혔으며 뒤를 이어 아마존과 마이크로소프트와 같은 기업 또한 임시적인 제공 중단 등 규제를 촉구하는 입장을 밝히기도 했다[32].

2. 영국

가. 현황

영국의 수도경찰청(Metropolitan Police Service)은 2009년부터 얼굴인식 기술을 사용하여 300백만장의 얼굴 이미지를 포함한 데이터베이스를 구성한 것으로 알려져 있다[33]. 또한 전국적으로는 2014년부터 경찰 국가데이터베이스(PND, Police National Database)를 기반으로 얼굴인식 기술을 사용해왔다. 경찰 국가데이터베이스는 혐의가 취하되거나 체포 후 법정에서 무죄 판결을 받은 사람을 비롯한 경찰의 유치장을 거친 사람 및 구류자(custody)의 얼굴 사진으로 구성되어 있고, 얼굴 사진 뿐만 아니라 문신이나 흉터 등 신체적 특징 또한 포함해 약 2천 3백만장의 사진이 저장되어 있고 이중 얼굴인식을 위해 검색 가능한 품질의 사진은 1천만장에 이르는 것으로 추정하고 있다[34].

영국 전역의 경찰이 경찰 국가데이터베이스에 접근할 수 있지만, 각 지방별로 자체적으로 수집한 데이터베이스 및 감시 대상 목록 또는 유럽 형사 경찰 기구(Europol) 데이터베이스를 이용하는 등 그 사용에는 차이가 있다.

---

32) IBM CEO's Letter to Congress on Racial Justice Reform <https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/>

33) 2009년부터 얼굴인식 기술을 활용해왔음이 정보공개 청구에 의해 공개됨 <https://www.whatdotheyknow.com/request/details_of_the_facial_recognitio#incoming-667080>

34) Biometris Commissioner(2018), Biometris Commissioner Annual Report

나. 실시간 얼굴인식 인권침해 논란

영국 경찰은 CCTV 영상 또는 스틸 이미지를 통한 얼굴인식, 태블릿 등 모바일 기기를 활용한 얼굴인식을 넘어 실시간 얼굴인식(Live Facial Recognition) 기술을 적극적으로 도입했다. 런던, 카디프, 맨체스터를 포함한 11곳의 지방 경찰들은 2015년부터 공공장소, 대형 행사, 집회 및 시위 등에 대해 이를 시험하며 사용해온 것으로 알려졌다.

영국 경찰의 실시간 얼굴인식의 주된 사용 방식은 다음과 같다. 먼저 실시간 감시 대상 목록의 데이터베이스를 구성하고 이를 어디서 진행할 지 결정한다. 이후 상단에 카메라가 설치된 관제차량을 활용하는데, 해당 카메라를 통해 공공장소와 거리를 촬영하며 수집되는 영상 속 모든 사람의 얼굴을 실시간으로 추출하고 분석하여 감시 대상 목록과 비교하는 절차를 자동으로 거친다. 특정 인물과 감시 대상 목록 속 인물의 일치 여부가 시스템을 통해 감지되면 관제차량의 경찰관은 체포 등 개입 절차를 판단한다.

이렇듯 영상촬영기기를 통해 수집되는 이미지 속의 모든 얼굴을 실시간으로 그리고 자동으로 추출하고 분석하여 데이터베이스나 감시 대상 목록과 비교하기 때문에 그 불법적 요소가 확연히 드러나 큰 논란을 일으키게 되었다.

또한 그 결과는 높은 오인식률로 인한 무고한 시민에 대한 신원 검사로 이어졌는데, 시민단체 Big Brother Watch가 정보공개 등을 통해 발표한 자료에 의하면 경찰이 사용한 대부분의 실시간 얼굴인식 기술의 결과가 부정확했으며 평균적으로 95%의 매칭 결과가 무고한 사람들로 밝혀졌다[35].

특히 런던 수도경찰의 경우 2% 미만의 정확도를 보였으며 실시간 얼굴인식을 통해 식별한 인물 중 102명이 식별 결과와는 무관한 다른 사람인 것으로 드러났다. 식별 결과가 동일한 것으로 드러난 인물 중 한 사람은 감시 대상 목록에 잘못 들어간 사람이었으며, 나머지 한 사람은 지명수배범이 아닌 정신

35) Big Brother Watch(2018), "FACE OFF - The lawless growth of facial recognition in UK policing".

건강으로 인해 감시 대상 목록에 있던 사람이었다.

사우스 웨일즈 경찰(South Wales Police Service)의 경우 런던 수도경찰의 기록에 비해 조금은 더 나은 결과를 보였으나 이또한 인식률이 9%에 불과했다. 그럼에도 불구하고 경찰 당국은 잘못 식별된 2451명의 사람들의 얼굴 정보를 12개월 동안 데이터베이스에 보관해왔으며 지속해서 이를 사용해왔다.

다. 관련 법 제도 및 비판

법 집행기관의 얼굴인식 기술 사용을 규제하는 구체적 법은 존재하지 않으며, 마찬가지로 경찰이 얼굴인식 기술을 사용할 법적 근거 또한 뚜렷하지 않다. 경찰과 범죄 증거법(Police and Criminal Evidence Act 1984, PACE)의 64A조는 경찰에게 체포 후 구금된 사람의 얼굴 사진을 찍을 수 있는 권한을 뒷받침하고 있으며 보통법(Common Law)에 따라 범죄를 예방하고 수사할 광범위한 권한을 갖고 있지만, 개인정보 보호법(Data Protection Act 2018)에 따라 경찰이 생체인식정보를 처리할 때에는 법 집행의 목적에 있어 반드시 필요하고 비례적이어야 한다는 조건을 갖고 있다.

그럼에도 불구하고 2010년 이후 각 지방경찰이 고유의 시스템을 통해 경찰 국가데이터베이스에 사진을 업로드할 수 있는 시스템이 만들어졌으며 2014년 얼굴인식 검색 기능이 추가되었으나 이 과정에서 의회나 공공의 검토 또는 의견 수렴 과정 없이 이루어졌다.

2009년, 형사입건 후 불기소된 원고들에 의해 경찰이 체포 당시 촬영한 사진을 계속 보관하는 것은 불법이라며 해당 사진을 삭제하게 해 달라는 소송을 제기되었고, 2012년 고등법원은 수사기관의 체포된 피의자 얼굴사진 촬영 및 처리가 불법이라 판시하며 국가가 삭제를 위한 구체적 기준을 마련할 것을 주문하였다. 2017년 정부는 삭제 기준을 마련했지만 유죄 판결을 받지 않은 경우 자동 삭제되는 게 아니라 본인이 직접 삭제 신청을 해야 하는 점, 경찰이 삭제 신청을 거부할 수 있는 점 등을 포함해 문제가 개선되지 않았다. 이에 생체인식정보 감독관(Biometrics Commissioner) 폴 와이즈는 이러한 정부의 기준이 DNA나 지문 정보에 비해 얼굴인식정보에 대한 보호가 완화된 것으로

보이며 얼굴 사진은 이제 단순 보관 목적이 아니고 경찰에 의해 공공장소에서 정보주체가 알지 못하는 사이 검색되고 처리될 수 있다는 점에서 오히려 DNA나 지문 정보보다 더 침해의 정보가 크기에 훨씬 더 엄격한 기준이 필요하다고 주장했다[36].

2019년 영국 개인정보 보호 감독기관(Information Commissioner's Office, ICO)는 경찰의 실시간 얼굴인식 사용에 대해 필요성과 적정성에 대한 고려, 개인정보 보호 영향평가, 개인정보의 삭제 등에 관한 의견과 보고서를 내고 정부로 하여금 법적 구속력이 있는 규제안을 도입할 것을 촉구했다[37].

ICO의 보고서에 의하면 실시간 얼굴인식 기술은 식별, 인증, 검증 또는 분류 목적으로 개인의 얼굴을 포함하는 디지털 이미지의 실시간 자동화된 처리를 포함하며, 그 일치 여부와 결과값 및 일치하지 않는 사람의 생체인식 데이터가 단시간 내 삭제되는지와는 관계없이 GDPR과 개인정보 보호법에서 명시하는 민감정보 즉 생체인식정보 처리에 속한다. ICO는 현재와 추후의 얼굴인식 기술 사용이 ICO의 규제 우선순위라는 입장을 밝히며 다음과 같은 근거를 들었다.

- 수많은 사람의 일상생활 속에서 아무런 인지도 없이 영향을 미칠 수 있는 사생활 침해의 규모
- 대규모 감시를 가능하게 하는 얼굴인식 기술의 잠재력과 그것이 인권과 정보인권에 미치는 영향
- 개인이 잘못 식별되거나 체포되는 등 부당한 대우로 이어져 기술적 무결성과 정당성을 훼손시키는 기술적 편견과 부정확한 데이터
- 예상되는 법 집행과 공익 목적 달성에 있어 기술의 효과에 대한 불확실성
- 경찰과 기술에 대한 대중의 신뢰를 떨어뜨릴 수 있는 불법적 집행 가능성

---

36) 이성기(2018), 위의 글.

37) ICO(2019). "ICO investigation into how the police use facial recognition technology in public places" <https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-Report-20191031.pdf>

또한 개인정보 보호법이 실시간 얼굴인식의 전체 과정에 적용되며, 이는 생체인식정보의 처리를 수반하는 민감정보 처리이므로 개인정보 보호 영향평가(DPIA)를 진행하고 감시 대상 목록 구성과 데이터 보존 및 시스템 사용에 있어 비례성을 반드시 적용하고 고려하는 등 적법한 근거를 갖출 것을 권고했다.

자유보호법(Protection of Freedoms Act, PoFA)에 의해 감시카메라 감독기구(Surveillance Camera Commissioner)와 생체인식정보 감독기구 또한 경찰의 얼굴인식 기술 사용 규제와 관련이 있으나 생체인식정보 감독기구의 경우 DNA 및 지문의 수집과 사용 등에 국한되어 그 직접적 규제에 한계가 있다. 감시카메라 감독기구는 얼굴인식 기술이 인권과 공공의 신뢰를 침해하는 도구이며 법적 정당성 없이 사용되어서는 안 된다며 감시카메라 예규(Surveillance Camera Code of Practice)를 개정할 것을 밝혔다.

경찰의 실시간 얼굴인식에 최초의 위법 판결

2019년, 전 지방의원 에드 브리지스와 시민단체 Liberty는 사우스 웨일즈 경찰의 실시간 얼굴인식 사용에 대해 인권법(Human Rights Act), 개인정보 보호법, 평등법(Equality Act), 유럽인권조약(ECHR)의 위반으로 소송하였다[38]. 2019년 9월 고등법원은 실시간 얼굴인식 기술의 사용이 해당 공공장소를 지나간 모든 사람의 사생활권을 침해하지만 현재의 법 규제 절차는 적절하며 다만 정기적 검토가 필요할 것이라 판결했다. 이에 에드 브리지스와 Liberty는 다음과 같은 근거를 제시하며 항소를 제기했다.

2020년 8월 항소 법원은 현재의 법 규제 절차가 사람들의 사생활권을 보호하고 있지 않고 이는 위법하다고 보고 경찰 얼굴인식 기술 사용에 대한 최초의 불법 판결을 내렸다. 항소 법원은 사우스 웨일즈 경찰이 얼굴인식 기술이 가져오는 차별적 영향을 적절히 고려하지 못했고, 평등법에 따른 의무를 다하

38) LIBERTY WINS GROUND-BREAKING VICTORY AGAINST FACIAL RECOGNITION TECH <https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking -victory-against-facial-recognition-tech/>

지 못했으며, 사람들의 얼굴을 스캔함으로써 고유하고 민감한 개인정보를 처리하지만 개인정보 보호법에 따른 처리 요건과 절차를 지키지 못했다고 지적했다[39].

3. 유럽연합[40]

가. 현황

유럽 정보인권 시민단체 EDRi에 따르면 2019년 말까지 최소 15개 유럽 국가가 얼굴인식 등 침입적인 생체인식 기술을 실험하고 있다고 한다.

예를 들어 EU Horizon 2020 프로그램이 지원하는 SPIRIT 연구과제는 얼굴 추출과 매칭 등의 도구를 사용하고, 소셜미디어 데이터 상의 정보를 연계시켜 범죄 수사에 관련된 모든 출처에 대해 지속적으로 연관 검색을 생성하는 내용으로 알려졌다. 헬레닉 경찰(그리스), 웨스트미들랜드 경찰(영국), 테임즈밸리 경찰·치안 위원장(영국), 세르비아 내무부(세르비아), 슈치트노 경찰아카데미(폴란드) 등 5개 법집행기관이 참여하고 있으며 2020년과 2021년 시범사업이 계획되어 있다. 또 Horizon 2020 프로그램은 헝가리, 그리스, 라트비아 국경들에 대해 iBorderCtrl이라 불리는 일련의 연구과제에도 자금을 지원했는데 여기에는 유럽연합에 입국하려는 사람들의 거짓말 등 속임수를 예측하기 위해 생체인식정보의 자동화된 분석을 사용하는 프로젝트가 포함되어 있었다. 시민사회는 속임수 예측용 '거짓말 탐지기' 실험은 힘의 역학관계가 불평등하고 일반적으로 소외된 개인들을 대상으로 감시 기술이 사용된다는 점에서 우

39) UK Court of Appeal Finds Automated Facial Recognition Technology Unlawful in Bridges v South Wales Police <https://www.huntonprivacyblog.com/2020/08/12/uk-court-of-appeal-finds-automated-facial-recognition-technology-unlawful-in-bridges-v-south-wales-police/>

40) 이 장의 내용은 다음 자료를 참고하였음. FRA(2019), "Facial recognition technology: fundamental rights considerations in the context of law enforcement" <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>; EDRi(2020), "EDRi paper: Ban Biometric Mass Surveillance" <https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf>.

려를 표하고 있다.

최근 코로나19 감염병의 지구적 유행에 대처하기 위해 얼굴인식 기술을 사용하는 경우도 있다. 폴란드의 경우 격리조치 대상자에게 의무적으로 얼굴인식 기반 애플리케이션을 사용하도록 하였다. 무작위적인 알람이 울린 후 격리대상이 20분 안에 애플리케이션에 얼굴인식을 하지 못하면 경찰이 격리장소로 출동한다. 프라이버시 인터내셔널의 보고에 따르면 격리대상은 휴대전화번호를 식별자로 하여 국가 데이터베이스 시스템에서 관리되는데 격리 애플리케이션이 설치될 때 참조용 얼굴 이미지가 수집된다. 그 후 알람 시점마다 격리대상의 얼굴이 일치하는지, 격리장소에 소재하는지를 파악하기 위해 애플리케이션에서 얼굴인식정보와 위치정보를 체크하고 국가 시스템이 이를 제공받는다[41].

유럽연합 기본권청(FRA)은 2019년 말까지 취합된 법집행기관의 도입 사례를 아래와 같이 소개하였다.

헝가리는 'Szitakoto'(dragonfly) 프로젝트에서 부다페스트 등 전국적으로 3만5천대 CCTV에 얼굴인식, 차량인식 기능을 장착하였다. 체코는 프라하 국제공항 얼굴인식 카메라를 100대에서 145대로 확대하는 계획을 승인하였다. 스웨덴에서는 개인정보 보호 감독기관이 범죄용의자 식별 목적으로 경찰의 얼굴인식 기술 사용을 승인하였다. 이는 CCTV 영상에서 추출한 범죄용의자 얼굴 이미지를 4만장 이상의 감시 대상 목록과 대조한다. 오스트리아도 2019년 얼굴인식 기술을 CCTV 등에 포착된 미지의 범죄자 식별을 위해 도입을 검토중이고 네덜란드에서는 이 기술을 테스트중이다. 유럽연합 차원의 IT 시스템에서는 난민, 이민, 국가보안 목적으로 광범위하게 적용하는 것을 추진 중이다. 특히 영국, 독일, 프랑스에서는 법집행을 위해 공공장소 CCTV에서 실시간 얼굴인식 기술을 적용하는 문제를 두고 사회적 논란이 크다.

---

41) Privacy International(2020), "Poland: App helps police monitor home quarantine", <https://privacyinternational.org/examples/3473/poland-app-helps-police-monitor-home-quarantine>.

우선 영국은 거리 CCTV에서 실제 감시 대상 목록(watchlist)을 대상으로 실시간 얼굴인식 기술을 테스트 중인 유일한 유럽연합 회원국이다. 사우스웨일즈경찰은 2017. 6. 최초로 UEFA 챔피온리그 카디프에 참가한 31만명을 대상으로 실시하는 등 일반대중 스포츠 및 음악 행사 때 실시간 얼굴인식 기술을 몇 차례 사용하였다. 사용된 감시 대상 목록은 행사별로 400명에서 1,200명에 달하며, △이미 중대범죄를 저지른 사람들 목록 △공공안전에 중대한 위협을 끼칠 것으로 간주되는 사람들 목록 △즉각 위협적이지는 않지만 경찰이 주의하는 사람들 목록 △시스템 성능을 테스트하기 위한 경찰관 얼굴이미지 데이터베이스 등 다양한 유형의 감시 대상 목록이 사용되었다. 이 첫 사례는 유럽사법재판소(카디프분소)에 회부되었으나 2019년 사법재판소는 현행 법체제가 자의적이지 않은 얼굴인식 기술 사용을 보장하기에 적절하며 인권법 및 개인정보 보호 관련 법률들의 요건을 준수했다고 판결하였다. 런던 경찰도 2016년에서 2019년 사이에 10건의 실시간 얼굴인식 테스트를 실시하였다. 이때 사용된 목록은 △체포영장발부 미체포자 △폭력범죄 가능자 △경찰에게 공공안전 위협을 유발할 수 있는 자로 알려진 자 △테스트용 경찰관 이미지였다.

다만 최근인 2020년 8월 11일 영국 법원은 경찰이 일반 대중을 상대로 안면인식 기술을 사용하는 것은 인권과 개인정보 보호법 위반으로 위법하다는 판결을 내렸다. 특히 경찰이 너무 많은 재량권을 갖고 있고, 기술 사용에 있어 명백한 지침 역시 갖고 있지 않다는 점이 문제로 지적되었다[42].

독일에서는 함부르크 경찰이 얼굴인식 기술을 2017년 G20 행사 시기에 기차, 버스, 지하철에서 사용하였다. 함부르크 개인정보 보호위원회는 G20 얼굴인식 기술 사용에 대한 보고서를 발간하고 이 기술이 개인정보 보호법을 준수하지 않았다고 지적하였다. 특히 법적 근거 부재가 문제되었다. 베를린 경찰은 2017년 및 2018년에 기차역에서 3종의 실시간 얼굴인식 기술 성능테스트를 실시하였다. 얼굴인식 기술을 사용해야 할 정당성은 실종자를 검색하기 위해

42) 영국 "경찰이 안면인식 기술 사용 위법"…세계에 어떤 영향?, 한겨레(2020. 8. 12).

모든 베를린 CCTV 영상을 검사하는 것이 불가능하다는 데서 찾았다. 테스트는 300명의 자원자로만 구성된 감시 대상 목록을 대상으로 하였다. 목록에 없는 사람은 얼굴인식이 이루어지고 있다고 표시된 기차역의 특정 구역을 지나가거나 지나가지 않을지 선택할 수 있었다. 경찰은 테러관련자, 성범죄자, 장기 탈옥범, 실종아동 등 향후 실제로 감시 대상 목록에 누구를 포함하고 어느 경우에 적용할지는 입법의 문제라고 밝혔다. 출입국 관리에서는 실시간 얼굴인식 기술 도입을 고려중이다. 프랑스 니스경찰은 2018년 축제에서 성능 테스트를 시행하였다. 감시 대상 목록은 자원자로 구성하였고, 축제 참여자들은 실시간 얼굴인식 구역을 지나갈지 여부를 선택할 수 있었다. 프랑스 경찰은 얼굴인식 기술을 범죄수사 목적으로 사용해 왔으나, 법적 기반 미비로 실시간 감시는 아직 공식적으로 도입하지 않았다.

한편 유럽은 회원국 경찰이 공동으로 이용하는 유럽 차원의 얼굴인식 데이터베이스 네트워크를 계획 중이다[43]. 2020년 2월 22일 폭로된 유럽연합 내부 문서에 따르면, 오스트리아를 비롯한 유럽 10개 국가 경찰은 각국 경찰의 얼굴인식 데이터베이스에 상호접속을 허용하는 법안을 추진하고 있다. 이 데이터베이스는 FBI 등 미국의 유사 데이터베이스에 연동될 가능성이 있어 대서양을 횡단하여 대규모 생체인식 통합이 이루어질 것이라는 우려를 낳고 있다. 이 계획은 유럽연합 전역의 DNA, 지문, 차량등록 데이터베이스를 연동하여 상호검색하는 플럼 시스템에 대한 확장 제안이다. 미국과 유럽 대다수 국가들 사이에는 비자 웨이버 프로그램이라는 이름으로 유사한 시스템이 이미 사용중이고, 미국과 유럽 기관들 간에는 쌍방의 지문 및 DNA 데이터베이스에 대한 접속을 허용하는 쌍무협정이 체결되어 있기도 하다. 2019년 4월, 본래 개별적이었던 5개 시스템의 데이터가 통합되어 3억 명에 달하는 비유럽연합 국가 시민의 지문, 얼굴 이미지 및 기타 개인정보가 보관된 데이터베이스가 구축되었다. 10개 경찰 기관은 이와 같은 방식으로 얼굴인식 데이터베이스를 통

43) "LEAKED REPORTS SHOW EU POLICE ARE PLANNING A PAN-EUROPEAN NETWORK OF FACIAL RECOGNITION DATABASES", The Intercept(2020. 2. 22) 〈https://theintercept.com/2020/02/21/eu-facial-recognition-database/〉

합하는 데에는 반대하였다고 한다. 그러나 얼굴인식 데이터베이스의 연동 및 상호검색은 실질적으로 통합과 같은 효과를 낳을 것으로 보인다.

유럽에서 얼굴인식 기술이 사회적으로 많은 관심과 비판을 받은 사례로는 마르세유 암페어 고등학교 얼굴인식 사건을 들 수 있다. 2019년 7월 프로방스 알프코트다쥐르(PACA) 지역 당국은 프랑스 개인정보 보호 감독기관 CNIL에 대해 마르세유 암페어 고등학교 출입 관리를 위해 얼굴인식 시스템 사용을 허가해줄 것을 요청했다. 이 시스템은 1년 간의 '시범사업' 목적으로 도입되었고 해당 지역의 다른 학교에서도 실시되고 있었으며, 학생과 학부모의 동의에 근거하여 실시된다고 하였다. 이 시스템의 도입 취지는 학교 보안 요원의 업무를 원활히 하여 신분 도용 사실을 적발하고 비인가자의 학교 접근을 방지하기 위한 것으로서 학생 및 교직원의 보안을 강화하고 학생들이 학교 구내에 진입하는 데 걸리는 시간을 단축할 것으로 기대되었다. 그러나 프랑스 개인정보 보호 감독기관 CNIL과 마르세유 지방법원은 이 시스템이 위법하다고 판단하였다. 시스템이 표방하고 있는 출입통제 목적 그 자체는 공공기관의 정당한 목표라고 할 수 있지만, 명찰을 사용하는 등 덜 침해적인 대안이 있을 경우 학교 얼굴인식 시스템이 필요적이지 않다는 것이 CNIL의 지적이다. 나아가, 단지 학교 출입을 목적으로 대규모로 미성년자를 대상으로 얼굴인식을 사용하는 것은 침해적 데이터 감시 프로그램으로서 불균형적이라고 보았다. 특히 유럽연합 개인정보 보호법(GDPR)에 따르면 동의 및 데이터 최소화에 대한 법적 요건이 존재한다. CNIL 뿐 아니라 마르세유 지방법원은 암페어 얼굴인식 시범사업이 이 두 가지 기준을 크게 위반하였다고 판단했다. 특히 공공기관과 학생 사이의 권력 역학 관계로 인해 근본적으로 정당한 동의를 얻지 못했다고 보았다. 또한 유럽연합법 전반에 걸쳐 아동청소년에 대하여 강화된 보호가 적용되고 생체인식정보는 GDPR상 매우 민감한 정보이기 때문에 미성년자 생체인식정보는 최고 수준의 보호가 필요한데 비해 암페어는 이를 충족시키지 못했다고 지적했다.

인권 침해 논란

현재 얼굴인식정보 처리 기술은 유색인종, 특히 유색인종 여성에 대해 편향

적이며, 이들을 식별할 때 급격하게 높은 오류율(거짓 양성 또는 거짓 음성)을 드러내 왔다. 얼굴인식 기술이 주로 백인 남성의 얼굴 이미지를 학습해 왔기 때문에 성별 및 민족적 집단에 따라 식별 오류 문제가 계속 나타나는 것이다.

특히 시민단체는 이런 현상이 식별 오류를 넘어 성별, 연령, 민족(인종), 장애 등에 따른 집단별로 차별적 효과를 낳을 수 있다는 점을 우려하고 있다. 이미 사회적으로 취약하고 과도하게 감시받고 있는 특정 집단에 대한 차별을 체계화할 수 있다는 것이다. 누군가를 "의심스럽다"거나 "위험한" 존재로 분류할 때 기존에 과잉 치안의 대상이 되어 온 집단은 생체인식 기술을 이용한 감시에 더 시달릴 위험성이 크다. 생체인식 시스템을 훈련하는 데 사용되는 입력 데이터가 중립적이 아니라, 그것들을 생성한 사회의 편향과 구조적 차별을 반영하고 내포했기 때문이다. 극단적으로는 얼굴인식 기술이 합법적인 반대활동을 하는 시민들(사회단체 활동가 등)이나 LGBTQ+ 성소수자들, 불안정한 체류자격의 이민자 및 외국인, 주거가 불안정한 주민이나 가난한 지역 등 소외 집단을 특정하고 체계적으로 분류하는 데 이용될 수도 있다.

이처럼 얼굴인식 기술이 도입되었을 경우 영향을 받는 인권으로 차별받지 않을 권리가 취약한 것으로 지적된다. 또 얼굴 이미지가 수집되고 처리되는 사람의 취약한 지위로 인해 정보주체 권리 행사가 어려울 수 밖에 없으며 효과적인 구제 및 공정한 재판을 받을 권리 행사에도 제한을 초래한다. 그밖에도 인간존엄성, 아동 및 노인의 권리, 장애인의 권리, 의사표현 및 집회결사의 자유, 좋은 행정의 권리(the right to good administration) 등이 영향을 받는다.

특히 기본권청은 프라이버시권 문제를 집중적으로 살펴보았다. 유럽 사법재판소[44] 및 인권재판소[45]는 일찌기 얼굴 이미지를 개인정보로 인정하였다. 얼굴 이미지는 개인의 고유한 특성을 나타내며 한 사람을 다른 사람과 구별할

44) CJEU, C-291/12, M. Schwarz v. Stadt Bochum, 17 October 2013, paras. 22, 48-49.

45) ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 56.

수 있게 한다. 따라서 유럽 인권재판소는 얼굴 이미지를 보호받을 권리가 개인의 발전에 핵심적인 요소라고 설시하였다[46]. 인권재판소는 "프라이버시에 대한 합리적 기대"라는 기준을 통해 프라이버시권이 공적 상황에서 타인과 교류도 포함하는 개념이라고 설명하고 있으며, 공공장소라 하여도 사람들은 감시에 종속되지 않고 프라이버시에 대한 기대를 가질 수 있다고 보았다. 유엔 특보 역시 옥외집회에 참가한다고 해서 프라이버시 침해가 일어날수 없다는 의미는 아니라고 보았다[47]. 프라이버시는 기본권 향유의 주춧돌이자 자유민주주의와 다양성이 보장되는 사회의 핵심적 가치이기 때문에 얼굴 등 대량 개인정보 처리는 우리 사회 민주주의 기능에 영향을 미칠수도 있다. 또한 얼굴 이미지의 생체인식 처리, 동영상의 보관, '감시 대상 목록' 데이터와 대조, 얼굴 이미지를 감시 대상 목록에 추가하는 과정은 프라이버시권 및 개인정보 보호권을 제한한다.

한편 얼굴인식 기술의 민간 행위자에 대한 의존도가 크다는 점도 문제로 지적되고 있다. 개인정보 보호 및 지적재산권 문제로 개발에 필요한 얼굴 이미지 데이터베이스를 확보하는 것이 쉬운 문제가 아니다. 이 때문에 얼굴인식소프트웨어 개발은 거대 IT기업에 유리한 측면이 있다. 또 영국 개인정보 보호 감독기관 ICO는 공공정책 목적에서조차 대부분의 생체인식 기술이 공적 행위자와 민간 행위자의 결합을 통해 개발·배치되는 문제를 지적한 바 있다[48]. 문제는 민간 행위자들이 공공 당국 및 법집행기관이 사용하는 기술에 대해 과도한 권력을 쥐고 있음에도 그에 부합하는 책임감이 거의 또는 전혀 없는 상태라는 점이다. 공공기관이 도입한 얼굴인식 기술임에도 민간의 영업 비밀이라

46) ECtHR, Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence, Strasbourg, Council of Europe, 31 August 2019, para. 138.

47) UN Human Rights Committee(2019), draft General Comment No. 37 [Article 21: right of peaceful assembly], draft prepared by the Rapporteur, Christof Heyns, July 2019, para. 69.

48) ICO(2019), "Statement on Live Facial Recognition Technology in King's Cross" 〈https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/〉

는 이유로 국민 앞에 공개되지 못하고, 심지어 클리어뷰AI의 사례(미국 사례 참조)에서처럼 민간기업이 경찰 등 국가기관의 국민 감시에 협업하면서 부당한 이득을 취하기도 한다. 생체인식 대량감시 시스템 개발에 민간 행위자들이 불투명하게 개입하는 것은 이들이 국민에 대한 부당한 권력을 발휘하고 국가 권력에도 영향을 미치게 된다는 의미이다. EDRi는 생체인식 처리를 공공적으로는 도입하는 행위자라면 공공, 민간 또는 양측의 협업을 불문하고 공적 투명성과 책임성을 제고할 필요가 분명히 있다고 지적한다. 정보공개의 권리, 절차적 권리 및 기타 모든 기본권과 자유를 보장해야 하고, 그에 대한 입증 부담은 기술을 개발하고 배치하는 행위자들이 져야 한다는 것이다.

특히 EDRi에 따르면, 공공장소에 얼굴인식 기술을 배치하는 것은 대량감시(mass surveillance)라는 점에서 큰 문제이다. 대량 감시란 "특정 개인에 대해 '특정적인(targeted)' 방식으로 수행되지 않는 모든 감시(유럽평의회)"로 정의되거나, "'사전적인 혐의 없이' 시작되는 무작위적인 사용(기본권청)"이라고 설명된다[49]. 대량감시는 대중에게 전반적으로 영향을 미치면서도, 합리적 혐의 없이, 무슨 일이 벌어지고 있는지 당사자들이 인지할 충분한 기회 없이, 동의권을 부여하지 않고, 옵트인하거나 옵트아웃을 할 수 있는 진정한 선택의 자유도 주지 않고, 무차별적으로 감시하는 활동이라는 점에서 문제이다. 이는 사람들이 공공장소에서 익명의 권리를 잃는 것을 의미한다. 독일 헌법재판소는 1983년 인구조사에 대한 결정에서 익명의 권리에 대하여 다음과 같이 설시한 바 있다. "매번 특이한 행동이 기록되고 그 후에 항상 기록되고, 사용되거나, 전달될지도 모르겠다고 생각하는 사람은 이런 방식으로 주목받지 않으려고 노력할 것이다. 예를 들어, 집회 또는 시민 행동에 대한 참여가 공식적으로 기록되고, 그로 인해 위험이 발생할 수 있다고 가정하는 사람은 관련 기본권

49) Council of Europe(2018), "Factsheet on Mass Surveillance" <https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e>; FRA(2018), "Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union Volume II"<https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-summary_en.pdf>.

을 행사하지 않기로 결정할 수 있다. 이것은 개인의 개인적 발전 기회를 제한할 뿐만 아니라 공공선 또한 제한할 것이다. 왜냐하면 자기결정권은 시민의 역량과 연대에 바탕을 둔 자유민주주의 사회의 필수 전제조건이기 때문이다." 즉, 대량감시의 편재성과 침해성은 사회적이고 공적이고 정치적인 삶에 대한 모든 사람들의 참여를 제한하고, 인구조사 사건에서 언급된 바와 같이, 끊임없이 감시당하는 두려움으로 인해 행동을 조정할 필요 없이 자율적인 삶을 살아야 할 사람들의 능력에 영향을 미친다. 이는 사람들이 자신의 정치적, 시민적 권리를 행사하는 것을 방해한다. 대량감시를 통해 수집된 정보를 분석하여, 주목할 필요가 있는 사람을 '식별'하기 위하여 군중이나 집단 속의 개인 누군가의 프로필을 만드는 데 얼굴인식 기술이 사용된다면, 인권 침해 위험성이 더욱 높아진다. 얼굴인식 등 생체인식 처리 시스템은 개인별로 소급하여 식별하는 것이 가능하다는 점에서 일반 사진이나 CCTV 와도 다르다. 이 기술은 기존의 감시 인프라, 검색 가능한 데이터베이스, 다른 공공기관의 데이터 및 공공장소 생체인식 처리를 통해 점점 더 많은 데이터가 연결될 때 그 기능적 효용성이 증대된다. 공공기관이 보유하고 있는 방대한 양의 데이터와 갈수록 민간 행위자들이 많이 보유하게 된 건강, 범죄 기록 및 기타 많은 다른 개인적인 사항들이 상호결합될 수 있다. 심지어 메타데이터 및 익명화, 가명화 또는 비개인정보조차 공공 및 민간 출처의 방대한 데이터들과 결합되면, 민감정보이고 개인정보이자 식별 가능한 정보를 추론하는 데 사용될 수 있다. 이렇게 지속적으로 증가하는 감시 네트워크로 인해 당사자는 적절한 동의나 옵트아웃할 수 있는 기회가 없이 합법적인 익명상태로 돌아갈 수 없으며, 모든 생활, 사회관계 및 행동에 대한 '영구적 기록'을 생성하게 된다.

EDRi는 일단 이런 시스템의 인프라가 갖춰지면, 기본권을 침해하는 기능확대가 계속될 수 있다고 지적한다. 공공장소에서 무작위적 생체인식 처리가 일반화되고 사람을 계속 식별하고 추적할 수 있게 되면, 거리의 개인이 실제 개인들과 연결되면서 사람들의 상호 작용과 매우 내밀한 삶까지 묘사할 수 있게 된다. 사람들은 어떻게, 왜 이런 일이 일어나는지, 또 이런 일들이 자신의 삶에 어떤 영향을 미칠지 알지 못한 채로 끊임없이 점수화되고, 분류되고, 평

가받게 된다. 이는 사회신용점수나 행동 조작과 같은 극단적인 용도로 이어질 수 있으며, 궁극적으로 이 기술에 기반한 사회 통제에 이를 수도 있다.

나. 관련 법제도 및 비판

(1) 기본권 관련 법

기본권청은 현재 유럽연합 회원국 공공기관이 추진 중인 얼굴인식 기술의 도입 및 시범사업이 주로 정확성(이미지 품질 및 에러율) 문제에 주목하고 있을 뿐, 보다 일반적인 기본권 영향에 대해서는 평가하고 있지 않다는 점을 지적하였다. 실시간 얼굴인식 기술은 설령 정확성 측면에서 완벽하다 하더라도, 당사자에게 알리거나 동의를 구하지 않고 사람들을 얼굴인식에 종속시킴으로 인해 취약하고 잠정적으로 모욕적인 지위에 처하게 한다는 점이 문제이다.

즉, 얼굴인식 기술의 사용은 무엇보다 일반적인 인간존엄성의 권리에 관한 문제이다. 얼굴 이미지 처리는 다양한 방식으로 인간 존엄성에 영향을 미칠 수 있다. 사람들은 얼굴인식 감시 하에 있는 공공장소에 출입하는 것에 불편함을 느낄 수 있다. 사회생활을 취소하거나 감시중인 주요장소를 방문하지 않게 되고, 기차역을 피하거나 문화사회스포츠행사 참석을 줄이는 등 감시로 인해 행동을 바꿀 수 있다. 얼굴인식 기술이 적용되는 정도에 따라 사람들은 삶 속에서 감시 기술을 의식하게 되는데 이 의식은 개인이 존엄한 삶을 영위할 역량에 영향을 미칠 정도로 매우 중대할 수 있다.

법집행기관이 대규모 공공행사 등에 얼굴인식 기술을 적용하였다가 일치하는 사람을 발견하면, 많은 사람들에 대해 검문검색을 실시하게 될 것이다. 이때 잘못된 매치된 사람들이 잘못 검문된다면 경찰 인력에 대해 문제제기가 이어질 것이고, 그에 대응하는 부적절한 경찰 행위가 증가하면 검문받는 사람의 존엄성이 침해될 수 있다.

따라서 얼굴 이미지를 비롯한 생체인식정보는 인간 존엄성을 존중하는 방식으로 처리되어야 한다. 그러나 현재 생체인식 기술의 배치에 있어 이러한 법적 기준이 충족되고 있지 않다는 것이 유럽연합 기본권청의 우려이다.

유럽연합의 헌법에 해당하는 유럽 기본권헌장(제52조제1항)에서 기본권 제한은 △법률로 규정해야 하고 △유럽연합이 인정하는 공공복리 목적에 진정으로 부합하거나 타인의 권리 및 자유를 보호하기 위하여 진정으로 필요한 경우에 한하여야 하고 △권리의 본질을 존중하고 △비례적이어야 한다. 유럽사법재판소에 따르면 이 요건들은 '모두' 충족되어야 하고, 그 가운데 '본질 존중'이란 부분적으로 제한될 수 있지만 완전히 무시되어서는 안 된다는 의미이다. 그 이후에 필요성과 비례성을 심사하게 된다. 범죄 예방 및 공공안전 등 '공공복리'는 그 자체로 기본권 간섭을 정당화할 수 없으며 덜 침해적인 다른 수단으로 충족될 수 없는지 살펴봐야 한다. 유럽연합 개인정보 보호 감독관(ESPS)는 필요성과 비례성이 "개인정보 처리를 수반하는 모든 조치 계획이 반드시 준수해야 하는 핵심적인 이중 요건"이라고 강조한다. 이런 기본권 심사는 기술이 사용되는 방식에도 적용될 수 있다. 달성하려는 목적의 정당성, 얼굴 이미지를 수집하는 방식(CCTV인지 바디캠인지 휴대전화 앱인지 등 등)으로부터 수반하는 에러율에 이르기까지 모든 요소를 고려해서 필요성과 비례성을 평가해야 한다. 기술이 침해적일수록 평가가 더 엄격해야 한다. 이때 목적 정당성은 공항 국경 검문소(1:1 대조)인지 감시 대상 목록에서 얼굴을 대조하는 범죄 수사용인지(1:다 대조)에 따라 다를 것이다. 후자에서는 수사중인 범죄의 심각성도 중요할 것이다.

EDPS는 당사자에게 불리하게 사용될 수 있는 민간 기업의 이익 또는 국가 감시 목적으로 사람들의 얼굴을 상품화하고 대상화하는 것은 그 자체로 존엄성을 침해한다고 설명한다[50]. 사람들의 신체적 특성을 추적하는 내밀하고 침해적인 성격과 결합하여, 특히 공공장소에서 무작위적인 생체인식 처리는 본질적으로 존엄성을 침해하는 관행이 된다.

시민단체 EDRi는 공공장소에서 민감정보인 생체인식정보를 무차별적으로 수집하고 추가적으로 이용하며 대규모 또는 심지어 전체 인구집단의 (정치적,

50) Wojciech Wiewiorowski(2019), "Facial recognition: A solution in search of a problem?" 〈https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en〉.

예술적 또는 사회적 활동을 포함하여 오프라인 또는 온라인에서 이루어지는) 활동에 대해 대량으로 감시하는 행위는 의심할 여지 없이 프라이버시권, 의사 표현 및 집회의 자유의 '본질'에 위배될 것이고, 따라서 유럽연합법과 양립할 수 없다고 보았다. 특히 실시간 얼굴인식 기술은 공공장소에서 얼굴 이미지에 대한 생체인식정보의 처리를 수반하며 개인의 신원을 파악하고 그 이미지들을 잠정적으로 보관하려는 목적으로 수행된다. 이때 얼굴 이미지의 최초 생체인식 처리 및 연쇄적인 동영상의 보관은 물론 이 데이터를 '감시 대상 목록'과 대조 및 목록에 추가하는 행위는 사생활권 및 개인정보 보호에 대한 권리를 간섭하게 된다. 이러한 기본권의 간섭은 엄격한 필요성 및 비례성 심사 요건을 충족해야 하며 명확한 법적 근거 및 정당한 목적을 필요로 한다. 정보의 민감성 및 정보가 사용되는 방식 또한 고려해야 한다.

개인정보에 대한 권리는 유럽연합 인권법인 기본권헌장 제8조에서는 규정하고 있으며 자세한 규범은 개인정보 관련 법에서 다루고 있다. 또 얼굴인식 기술의 사용은 개인정보에 대한 권리와 다소 독자적으로 사생활권도 문제가 된다. 사생활권은 기본권헌장 제7조 및 인권조약 제8조에 규정되어 있다. 이때 사생활권은 공적 상황에서 타인과 교류도 포함하는 개념이다. 유럽인권재판소는 '프라이버시에 대한 합리적 기대'라는 개념을 사용하여 사람들이 공공장소에서 감시에 종속되지 않고 프라이버시에 대한 기대를 가질 수 있다고 보았다. 따라서 옥외집회에 참가한다고 해서 프라이버시 침해가 일어날수 없다는 의미는 아니다.

(2) 개인정보 보호 관련 법

GDPR 및 경찰디렉티브 규범 일반

유럽연합 개인정보 보호 관련 법에서 얼굴인식정보는 민감정보로서 특별히 보호되고 있다. 개인정보 보호 관련 법은 개인정보 처리에 일반적으로 적용되는 개인정보 보호법(GDPR)과 법집행 목적에 적용되는 일명 '경찰디렉티브'[51]로 나누어 볼 수 있다. 경찰디렉티브는 법집행기관에 적용되는데 유럽법상 법집행기관은 범죄 예방, 수사, 탐지 및 공소제기, 형의 집행을 소관하는

기관을 의미한다[52]. GDPR 및 경찰디렉티브는 공통적으로 특수한 범주의 개인정보의 경우 특별히 민감하기 때문에 원칙적으로 그 처리를 제한하고 예외적인 처리에 대하여도 강화된 보호를 하도록 규정하고 있다(special categories of personal data, 이하 '민감정보').

자연인을 고유하게 식별하기 위한 목적으로 생체인식정보(biometrics data)를 처리하는 것과 나아가 인종, 민족, 성적 지향, 성별 정체성, 종교 또는 건강상태와 같이 특성을 식별하거나 예측할 수 있는 관찰은 민감정보에 포함된다. 생체인식정보는 자연인의 물리적, 생리적 또는 행동적 특성과 관련한 특정한 기술적 처리의 결과로 얻어진 개인정보들이다. 그중 물리적/생리적 특성은 얼굴 특성, 지문, 망막, 홍채 등 신체적인 특성이며 얼굴 이미지가 이에 속한다. 행동적 특성은 습관, 행동, 성격 특성, 중독 등에 깊이 배어있어 개인을 고유하게 식별할수 있는 서명 필체, 보행 및 동작 방식 등이다.

GDPR

제4조 정의

(14) '생체인식정보'는 얼굴 이미지나 지문정보 등, 자연인의 고유식별을 허용하거나 이를 확인하는, 자연인의 물리적, 생리적 또는 행동적 특성과 관련한 특정한 기술적 처리의 결과로 얻어진 개인정보를 의미한다.

(전문51) 사진 처리의 경우, 사진은 자연인의 고유 식별 또는 증명을 가능하게 하는 특정 기술 수단을 통해 처리될 경우에만 생체 정보로 정의되기 때문에, 특수 범주 개인정보 처리로 일괄 간주해서는 안 된다.

51) Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 일명 'police directive'.

52) The term 'law enforcement authorities' refers to Member State agencies and encompass "competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security". Source: Law Enforcement Directive, Article 1 (1).

사람을 식별하거나 본인을 확인하기 위한 목적으로 얼굴 이미지를 기술적으로 처리한 결과 얻어진 얼굴인식정보는 생체인식정보로서 민감정보에 속한다. 다만 얼굴인식 기능이 없는 사진은 민감정보가 아니라 일반 개인정보에 속한다.

유럽인권재판소는 얼굴 이미지가 개인의 고유한 특성을 나타내며 한 사람을 다른 사람과 구별할 수 있고 나아가 얼굴 이미지를 보호받을 권리는 개인의 발전에 핵심적인 요소라고 보았다. 얼굴 이미지는 고유하고, 쉽게 변경하거나 은닉할 수 없는 개인정보이다. 수집도 쉽다. 얼굴 이미지는 지문이나 DNA 등 다른 생체인식 식별자에 비해 공공장소에서 수집되고 감시되는 것을 통상 피하기 어렵다. 온라인이든 오프라인이든 공개된 장소에서 생체인식 기반으로 무작위적으로 사람을 식별하는 것은 민감정보에 대한 무차별적인 수집, 처리 또는 저장에 해당한다.

GDPR에 의하면 원칙적으로 민감정보의 처리는 금지되는데, 다만 특정 상황에서 명시적으로 허용되는 경우는 예외로 한다(제9조제2항). 이 예외에는 정보 주체가 하나 이상의 구체적 목적을 위한 개인정보 처리에 명시적으로 동의한 경우이거나(a), 정보 주체가 물리적인 이유나 법적인 이유로 동의를 제공할 수 없는 상황에서 정보 주체나 다른 자연인의 필수적 이익을 보호하는 데 처리가 필요한 경우(c), 처리가 정보 주체가 명백히 일반에 공개한 개인정보와 관련된 경우(e), 또는 상당한 공익을 이유로 처리가 필요한 경우이되, 추구하는 목적에 비례하고 정보 보호에 대한 권리의 본질을 존중하며 정보 주체의 기본권과 이익을 보호하기 위한 적절하고 구체적인 조치를 규정하는 유럽연합이나 회원국 법률을 바탕으로 하는 경우(g) 등이 있다. 통상 공공기관이 배치하는 얼굴인식 기술의 경우 (g)호에 근거하여 처리가 이루어진다. 유럽연합 회원국은 유전 정보, 생체인식정보 또는 건강 관련 정보의 처리와 관련하여서는 제한을 포함하는 추가 조건을 유지하거나 도입할 수 있다(제9조제4항).

경찰디렉티브에서 민감정보를 처리할 수 있는 경우는 ① 반드시 필요한 경우에 한하여(shall be allowed only where strictly necessary), ② 정보주체의

권리와 자유를 위한 적절한 보호조치를 취하는 한편, ③ 유럽연합이나 회원국 법률에서 허가하는 경우이거나(a), 정보주체나 다른 자연인의 필수적 이익을 보호하기 위한 경우(b), 또는 그 처리가 정보 주체가 명백히 일반에 공개한 개인정보와 관련된 경우(c)로 제한되며 ① 내지 ③의 요건이 모두 충족되어야 한다(제10조)[53].

유럽 개인정보 보호 관련 법에서 민감정보의 처리가 예외적으로 허용되는 경우에도 일반 개인정보 처리 원칙을 준수해야 한다. 프랑스 마르세유 암페어 학교에 대한 판례가 보여주듯이, 현재 유럽에서 공공장소에 배치된 생체인식 처리는 GDPR 제5조의 개인정보 처리 원칙을 준수하지 않았다는 결정을 받았다. 이 규범은 합법성·공정성·투명성 원칙, 구체적이고 명확하고 정당한 목적에서 수집되어야 한다는 목적 제한 원칙, 목적에 필요한 한도에서 개인정보를 수집해야 한다는 의미의 데이터 최소화 원칙, 충분하게 정확하지 않은 개인정보의 이용을 금지하는 정확성 원칙 등 데이터 품질 요건, 그리고 이러한 요건을 충족한다는 개인정보 처리자의 입증 부담 등 책임성에 대한 원칙 등이다.

경찰디렉티브의 개인정보 처리 원칙 또한 법집행 목적이라도 개인정보를 "적법하고 공정하게" 처리해야 하는 등 GDPR의 개인정보 처리원칙과 거의 유사하다[54]. 다만 경찰디렉티브는 진행중인 수사의 방해 및 왜곡를 방지하고 공공안전 및 국가안전보장을 위한 목적을 위해 정보주체의 일부 권리를 제한한다.

---

53) GDPR(제9조)와 경찰디렉티브(제10조) 모두 민감정보의 처리를 유사하게 보호하고 있지만 경찰디렉티브가 다소 허용적이라고 평가받고 있음(Article 10 of the Law Enforcement Directive lays down similar, albeit a bit more permissive conditions).

54) GDPR(제5조)과 경찰디렉티브(제4조)의 개인정보 처리 원칙(Principles relating to processing of personal data) 규정 모두 (a)~(f)까지 6개 항목을 두고 있으며 그 내용도 유사함. 다만 GDPR의 합법성·공정성·투명성의 원칙이 경찰디렉티브에서 합법성·공정성의 원칙으로(a) 축소되었으며, GDPR에 규정된 추가 처리를 경찰디렉티브는 인정하지 않는 반면(b) '목적에 필요한 경우에 … 한정된(…limited to what is necessary in relation to the purposes)' 처리 대신 '목적에 … 과도하지 않은(…not excessive in relation to the purpose)' 처리(c)를 규정하는 등 세밀한 차이가 있음.

EDRi는 이러한 법적 규범을 종합하여 법집행기관 등 공공기관에서 생체인식 기술을 사용하려면 대량감시가 아닌 경우에 한해 다음 4단계의 요건을 모두 충족해야 한다고 보았다.

첫째, 인권법은 기본권을 제한하는 조치의 경우 반드시 필요하고 추구하는 목표에 비례적인 경우로 한정한다(기본권헌장 제52조).

둘째, 생체인식 처리는 합법성 또는 "법률에 따르는" 요건을 충족해야 한다. 이것은 모든 생체인식 처리의 허가 및 배치는 법률에 명시적으로 규정되어야 하며 정당한 목적을 달성하기 위해 반드시 필요한 것으로 입증된 경우에 한정되어야 한다는 의미이다. 그 법률은 대중이 접근할 수 있어야 하며, 사람들이 그 적용과 침해 정도를 예측할 수 있도록 충분히 명확하고 정밀해야 한다. 특히 수사 대상에 속하지 않는 자의 생체인식을 처리하는 경우에는 법률이 수집된 개인정보의 보존, 접근, 규모 및 파기에 관해 명확하게 규정할 필요가 있다.

셋째, 이러한 침해적인 권력의 남용을 막기 위하여 법집행기관의 생체인식 처리 사용은 보호조치를 갖추어야 한다. 이러한 보호조치에는 최소 감시 대상 목록 수록 기준에 대한 투명성을 포함하며, 이 기술의 배치를 정당화할 만한 심각한 범죄나 위협에 연루되었다는 개별적이고 합리적인 혐의의 확인을 포함한다. 사전적인 개인정보 보호 영향 평가(경찰디렉티브 전문58) 뿐만 아니라 관련 감독 당국과 사전 협의(전문 28)도 포함되며, 개인들에게는 적절하게 생체인식정보 처리에 대해 고지하고 정정, 열람, 삭제 등 권리를 행사하고 처리 업무에 대해 법원이나 규제기관에 이의를 제기할 기회를 부여하는 것도 포함된다. 또한 법적 구제 등 권리를 보장하기 위한 독립적인 사법적/행정적 심사도 포함한다. 생체인식정보가 수집되었으나 당해 사건과 무관한 개인들에게는 최소 사후에 고지하고 정보 수집이 부당하거나 불법적으로 처리/제공/보관된 경우 구제받을 수 있도록 보장할 필요가 있다. 생체인식정보의 수집 및 성공률에 관하여 시기적절하고 신뢰할 수 있는 통계가 공개되면 국민은 이 공권력이 오남용되고 있지 않다고 신뢰할 수 있을 것이다.

넷째, 당국은 처리된 개인정보의 보안과 무결성을 보장할 의무를 지게 된

다. 기본적으로 생체인식 기술의 사용은 매우 민감한 정보의 처리를 포함함에도, 통상 취약성이 있거나 제3자 무단접근을 방지하는 보안조치가 적절하지 못한 장비를 사용하는 문제가 있다. 유럽연합법에 따르면 무작위 생체인식 처리가 아니라 일반적인 인식, 식별 또는 기타 처리를 위해 생체인식 기술을 사용하는 경우에도 예외적으로 엄격한 통제를 받아야 하는 것이다.

GDPR 및 경찰디렉티브와 실시간 얼굴인식 기술

기본권청은 GDPR과 경잘디렉티브 관련 규정의 개인정보 처리 원칙을 실시간 얼굴인식정보에 세밀하게 적용해 보고 다음과 같은 점에서 문제가 될 수 있다고 지적하였다.

(적법성, 공정성, 투명성 원칙)

실시간 얼굴인식 기술의 경우 공공장소에서 사람들의 인지나 동의 없이 얼굴 이미지를 수집하기 때문에 투명성과 명확한 정보 제공 원칙이 중요한 문제가 된다. GDPR에 따르면 '공정한' 개인정보 처리는 얼굴 이미지를 수집당하는 주체에게 적절한 정보 제공을 포함하는 의미이며(GDPR 제5조제1항), 경찰디렉티브 또한 같은 요건을 두고 있다(경찰디렉티브 전문26). 개인정보처리자는 "정보주체에게 간결하고 투명하며 이해하기 쉽고 접근이 용이한 형태로 명확하고 평이한 표현을 사용하여 개인정보 처리와 관련된" 정보를 제공하는 적절한 조치를 취해야 한다. 개인정보처리자 연락처, 처리 목적, 보관 기간, 열람/정정/삭제 청구권, 개인정보 보호 감독기관 진정권에 대해서도 고지해야 한다(GDPR 제13조 내지 제14조, 경찰디렉티브 제13조)[55]. 공공장소 실시간 얼굴인식의 경우 정보주체에게 설명에 기반한 사전적인 동의나 옵트아웃 절차 없이 이루어지기 때문에 이 의무가 매우 중요하다. 만약 정보 고지, 사전 동의 없이 이루어지는 얼굴인식 처리에 동반하여 열람권도 제한된다면 대단히 강력한 정당성이 있어야 한다. 유럽정보보호이사회(EDPB)는 대중이 감시 구역에

55) 다만 경찰디렉티브는 수사중인 사안에 대한 방해 및 편견을 방지하거나 공공안전 및 국가안보를 보장하기 위하여 일부 정보주체 청구에 대한 답변 의무의 예외를 인정하고 있음.

들어가기 전 CCTV의 존재 여부를 인지할 수 있도록 고지하는 것이 회원국의 의무라고 명시한 바 있다. 기본권청은 얼굴인식정보의 처리가 일반적인 사진 촬영이나 CCTV 영상 수집 보다 침해 수준이 더욱 크다고 보았다. 얼굴에서 생체인식 특성을 추출하는 처리는 얼굴 정보를 이후 다른 방식으로 처리하거나 결합하는 것을 가능케 하며, 특히 데이터베이스내에서 얼굴인식정보를 처리하는 것은 (실제 감시 대상 목록과 대조하는지 여부와 무관하게) 단독으로 얼굴 이미지를 인식하는 것과 또 다른 침해 효과를 낳는다. 함부르크 개인정보 보호위원회는 얼굴인식 기술이 완전히 새로운 방식의 침해라고 보았으며 처음에 법집행 목적과 개인정보 자기결정권 간의 균형이 법적으로 명확했더라도 이후 후자의 손해가 훨씬 더 큰 방향으로 상황이 변할 수 있다고 경고하였다. 따라서 이 위원회는 얼굴인식 기술에 대해 독립적이고 구체적인 규제가 필요하다고 권고하였다.

(목적 제한 원칙)

GDPR(제5조제1항제b호)과 경찰디렉티브(제4조제1항wpb호)는 모두 개인정보를 특정한 목적으로만 처리해야 한다는 목적 제한 원칙을 규정하고 있으며, 기본권청은 특히 법집행을 위한 개인정보 처리의 구체적인 목적을 법률적으로 명시하는 것이 요구된다고 보았다(It requires that personal data are processed only for specified purposes, which must be explicitly defined by law). 목적 제한 원칙은 얼굴인식정보의 무기한 저장을 금지한다. 얼굴인식정보는 처음 예상했던 목적 외로 오남용될 위험성이 있으며, 특히 각국 경찰기관이 유럽 차원의 대규모 데이터베이스를 상호운용할 수 있는 상황에서 얼굴인식정보가 불법적인 식별에 사용될 우려가 있다.

(데이터 최소화, 정확성, 보관 제한, 정보 보안 및 책무성 원칙)

GDPR(제32조) 및 경찰디렉티브(제29조)에 따르면 회원국은 개인정보에 대한 비인가 제공, 접근을 방지하는 조치를 취해야 한다. 얼굴인식 시스템이 장래 다른 IT 시스템에 연동될 경우 목적 제한 원칙이 특히 문제에 처할 것이고 정보 유출도 문제가 될 것이다. GDPR 및 경찰디렉티브에서 요구하는 개

인정보 보호 중심 설계(dada protection by design)는 정보주체 권리를 보호하는 조치를 내장해야 한다는 뜻이다. 얼굴인식 기술을 도입하려면 시작 시점에서부터 개인정보를 보호하기 위해 완전히 갖추어진 분석, 계획 및 절차가 마련되어 있어야 한다. 그밖에 GDPR 및 경찰디렉티브에 따르면 얼굴인식 기술을 사용하기 위해서는 개인정보 보호 영향평가도 실시해야 하는데, 여기에는 법적 허용 여부에 대한 평가 및 개인정보 보호 감독기관에 대한 사전 질의도 포함된다[56].

(보론 : 자동화된 의사결정에 인간 개입 원칙)

GDPR(제22조) 및 경찰디렉티브(제11조)는 자동화된 의사결정을 일반적으로 금지하고 있는데 이는 "프로파일링을 포함해 자동화된 처리만을 바탕으로 한 결정으로서 자신과 관련한 법적 영향 또는 이와 유사하게 중대한 영향을 미치는 결정의 대상이 되지 않는다"는 의미이다. 다만 유럽연합법 또는 국내법에서 승인했을 경우에는 이 금지의 예외가 가능한데 이 경우 정보주체의 권리와 자유를 위한 적절한 보호조치가 수반되어야 하고 이 조치에는 인간의 개입을 받을 권리를 포함한다[57]. 자동화된 의사결정에 얼굴인식정보처럼 민감정보에 대한 처리가 포함되는 것은 정보 주체가 하나 이상의 구체적 목적을 위한 개인정보 처리에 명시적으로 동의한 경우이거나(GDPR 제9조제2항제a호), 상당한 공익을 이유로 처리가 필요한 경우이되, 추구하는 목적에 비례하고 정보 보호에 대한 권리의 본질을 존중하며 정보 주체의 기본권과 이익을 보호하기 위한 적절하고 구체적인 조치를 규정하는 유럽연합법나 회원국 법률을 바탕으로 하는 경우(제g호)에만 가능하며, 정보 주체의 권리 및 자유와 정당한 이익을 보호하기 위한 적절한 조치가 수반되어야 한다. 다만 기본권청은

56) 앞서 독일과 프랑스의 실시간 얼굴인식 기술 시범사업에서 경찰은 개인정보 보호 감독기관의 사전 자문 또는 협업을 거쳐 실시하였음. 영국 사우스웨일즈 및 런던시 경찰은 영향평가를 실시하고 그 결과를 공개하였음. 그러나 EDRi를 비롯한 인권단체들은 이들 실시간 얼굴인식 기술을 위법이라고 비판하였음.

57) GDPR 제22조에서는 인간의 개입을 받을 권리 외에 자신의 견해를 표현할 권리, 결정에 이의를 제기할 권리도 함께 명시하고 있으나 경찰디렉티브 제11조에는 전자의 경우만 명시하고 있음.

'자동화된' 의사결정의 개념이 다소 규정하기 어렵기 때문에 추가적인 연구와 토론이 필요하다고 보았다. 예를 들어 '인간의 개입'이 시스템의 결과물에 단순히 결재하는 정도를 의미한다면 이는 사실상 의사결정을 완전히 자동화하는 것이다. 다른 한편으로 연구에 따르면 인간은 주로 알고리즘 결과가 자신의 고정관념과 일치하지 않을때 이를 배제하는 경향이 있는데 이 경우 인간의 개입이 오히려 사회적 약자 집단에게 불리한 영향을 미칠 수 있다.

대량감시로서 얼굴인식 기술

유럽 시민단체 EDRi의 경우 무작위 얼굴인식 기술의 배치가 '대량감시'라는 점에 주목하고 있다. 대량감시에 대한 금지는 최근 유럽 판례 전반에 걸쳐 발견되며, 합리적인 의심이 결핍된 감시를 특징으로 한다. 특히 유럽인권재판소는, 생체인식정보의 "전방위적이고 무차별적인" 보유는 프라이버시권에 대한 "불균형적 간섭"에 해당한다고 판시했다[58]. 사법재판소는 이들 조치가 "당사자들의 마음 속에 사생활이 지속적인 감시 대상이라는 느낌을 불러일으키는 것 같다"(37문)는 점에 주목했다. 이는 범죄 혐의나 공공장소에서 공공질서에 대한 위험과 관련이 없는 개인의 모든 행동양식에 대해 이루어지는 대량감시가 위법인 이유이다. 슈렘스 1차 사건에서 재판소는 다음과 같이 판결했다[59]. "공공기관으로 하여금 전자 통신의 내용에 일반적으로 접근할 수 있도록 허용하는 법률은 사생활을 존중하는 기본권의 본질을 훼손하는 것으로 간주되어야 한다. 이는 기본권헌장 제7항에서 보장된 바와 같다 … (94문)."

유럽연합법 하에서는 대량감시가 금지되어 있다. 우선 GDPR의 개인정보 개인정보 보호를 상기해볼 때 대량의 정보 수집 및 처리에는 높은 법적 한계가 있을 수 밖에 없다. 나아가 경찰디렉티브는 법집행 목적으로 민감정보의 처리를 허용하는 경우 반드시 법적 근거를 두도록 하면서 이와 병행하여 '반드시 필요한' 경우로 한정하였으며, 제29조 작업반의 설명에 따르면 이는 법집행기관이 민감정보를 처리하기 위해서는 "정확하고 특히 확실한 정당성을

58) ECtHR, S. and Marper v the United Kingdom (2008).

59) Case C-362/14, Schrems v Data Protection Commissioner (2015) E.C.R. 627.

확보해야" 한다는 의미이다.

한편 경찰디렉티브는 추가적으로 유죄가 확정된 자나 용의자(용의자인 경우 법집행기관은 "그들이 범죄행위를 저질렀거나 그런 일이 임박했다고 믿을 수 있는 중대한 근거가 있어야 한다")의 취급에 대해 유죄로 판결받지 않았거나 범죄 용의자가 아닌 사람과 구분하여 명시하고 있다(제6조제a항). 이러한 구분으로 인해 ("중대한 근거"를 충족하는 혐의에 의한) 진짜 용의자에 대한 정당하고 합법적인 특정 대상 감시인 경우와, 일반 대중에 대한 무작위적인 감시 간에 차이가 있을 수 밖에 없다. 그러나 무작위적인 보행자 통행은 공공장소의 고유한 특징인 만큼 대상특정이 어렵다. 따라서 공공장소에서 얼굴인식 장치의 설치는 금지되어야 한다는 것이 EDRi의 주장이다. 감시받는 인구 대다수가 범죄 또는 공공질서에 대한 위협과 아무런 관련이 없다는 사실에도 불구하고 이런 조치들이 이루어지기 때문에, 대량감시로 이어지는 생체인식정보의 처리는 불법이라는 것이다. EDRi는 대량감시가 겉으로 명시된 목적과 무관하게 실체적으로 불법적일 수 밖에 없으며, 그러한 대량감시 효과가 의도적인 것인지 또는 의도하지 않은 것인지 역시 관계가 없다고 비판한다.

EDRi는 입법적인 해결 역시 불가능하다고 본다. 대량감시는 사생활에 대한 부당한 제한을 가하며 생체인식정보를 사용할 때는 훨씬 더 침해적이어서 그 사용이 본질적으로 불균형적이기 때문이다. 기본권헌장, 인권조약, GDPR 및 경찰디렉티브를 종합해 볼 때 공공장소에서 정당한 공공정책 목표를 달성하기 위한 수단이라 하더라도 무작위적인 생체인식 처리는 필요적이거나 비례적이라고 볼 수 없다. 이것이 민감정보에 미치는 위험의 규모와 정보주체의 권리와 자유에 가하는 제한들이 결코 최소침해적 선택이 아니라는 의미에서 그렇다. 이 기술의 사용은 불법적인 대량감시를 위한 여건을 조성하고 바로 그 목적에서 인간 존엄성을 근본적으로 침해한다.

데이터에 굶주려서 대량감시를 가능하게 하거나 기여하는 얼굴 및 기타 생체인식 처리는 근본적으로 인간 존엄성, 민주 사회, 기본권 및 자유, 개인정보 보호, 절차적 권리, 법치주의의 본질과 상충한다. 대량 생체인식 처리에서 권력 불균형, 차별, 인종차별, 불평등, 권위주의적 사회통제 증가의 위험은 이러

한 기술의 사용이 가상적으로 가져오는 어떤 '편익'에 비해 너무 높다. EDRi는 유럽연합이 기본권의 본질을 믿는다면 공공장소 대량감시로 이어지는 생체인식 처리를 금지할 수밖에 없다며, 결론적으로 공공장소에서 대량감시로 이어질 수 있는 생체인식 처리를 도입하는 모든 입법 계획을 중단할 것을 유럽 각국에 촉구하였다. 더불어 얼굴인식 기술은 명확하고 예측 가능한 법률로서 해당 문제와 상황에 비례적으로 특정인의 식별 검사만 허용해야 하고, 그 남용에 대해 효과적인 구제책을 규정해야 한다고 덧붙였다.

(3) 차별

유럽법에서 차별이란 "인식된 또는 실제적인 개인적 특성에 기반하여 한 사람이 현재, 과거 또는 미래의 비슷한 상황에 처한 다른 사람보다 덜 호의적인 대우를 받는 것"을 의미한다. 다른 취급은 정당한(legitimate) 목적이 있을 경우 가능하고 목적 달성에 이 수단이 필요하고 비례적일 때 정당하다(justified). 그 경계는 상황에 따라 사례별로 다양하다. 알고리즘 자체에 내장된 (의도적/비의도적) 편향성에 의해 알고리즘 기반 의사결정에서 차별 문제가 발생할 수 있다. 알고리즘의 편향성은 얼굴인식에 사용되는 알고리즘 설계, 테스트, 실행 시에는 물론, 매치후 경찰관이 어떤 조치를 취할지 결정할 때에도 다방면으로 영향을 미칠수 있다. 알고리즘에 내재된 편향성은 수학적으로나 프로그램 솔루션으로 제거하기 어렵다. 미국 연구에서는 연령, 성별, 출신국가 등 표현형 / 소프트웨어에 따라 에러율이 달라졌다.

차별의 주요 요인은 알고리즘 및 소프트웨어 개발시 사용되는 데이터 품질의 문제이다. 논리적으로는 더 많은 이미지가 주입될수록 정확성이 향성된다. 그러나 정확성은 얼굴 이미지의 양으로만 결정되지 않으며 품질에서도 결정되는 문제이다. 우선은 데이터 품질 향상을 위해서는 다양한 인구 집단을 반영한 대표성이 요구된다. 지금까지는 서구 백인 남성으로 과잉대표된 얼굴 인식이 문제였다. 또 머리색, 피부색 등 표현형 특질은 얼굴인식 시스템의 생체인식 매치 결과에도 영향을 미칠 수 있다. 빛반사, 광도 부족이 피부색 오인으로 이어질 수 있다.

장애 또한 문제가 된다. 장애 유형은 다양한데 얼굴인식이 장애에 미치는 영향과 관련한 고려가 이루어지고 있지 못하다. 장애, 사고나 마비 후 성형, 안면 기형에 대한 정확한 인식 여부도 불확실하다. 얼굴인식 기술의 도입 후 특정 민족 집단이 더 많이 검문되면 얼굴인식 기술의 차별 문제가 사회 통합에 역효과를 야기할 것이다. 경찰관 및 출입국관리자에 대한 신뢰 문제에도 중대한 영향을 미칠 수 있다.

(4) 표현의 자유 및 집회결사의 자유

표현 및 정보에 대한 자유는 민주사회의 초석으로 유럽에서 헌법적으로 보장되어 있다. 따라서 그 제한은 과도해서는 안 되며 법률에 명시되어야 하고, 민주사회에서 필요하고 명시적으로 서술된 정당한 목적(국가 보안, 공공 안전, 범죄 예방 등)에 의해서만 가능하다. 집회시위의 권리 제한도 마찬가지이다.

공공장소에서 CCTV로 수집된 얼굴 이미지를 처리하는 기술을 적용하는 것은 의사표현의 자유를 침해할 수 있다. 의사표현의 자유의 핵심이 집단적인 익명의 자유를 포함하고 있기 때문이다. 2018년 독일 법원은 집회에서 촬영된 사진을 소셜미디어를 통해 출판한 사건에서 이 일이 집회의 자유에 미치는 부정적인 영향을 미친 점을 고려하여 불법이라고 판시한 바 있다. 공공 장소에서 얼굴인식 기술에 의해 감시된다는 사실을 아는 사람들에게는 위축적 효과가 야기되며 개인들로 하여금 자신의 행동을 변경하게끔 유도할 수 있다. 의사 표현을 아예 하지 않을 수도 있는데 이 또한 표현의 자유 침해에 해당한다는 것이 2019년 유엔 의사표현의자유 특별보고관의 입장이다.

특히 평화 집회의 자유는 사람들이 강력하지만 평화적인 방식으로 집합적으로 사회 형성에 참여할 수 있도록 보장하는 것이다. 집회의 자유는 사람들이 타인과 연대를 경험하는 동안 익명권을 행사할 수 있도록 보호한다. 그러나 평화집회에 대해 얼굴인식 기술을 사용하는 것은 사람들의 집회 참여 의욕을 저하시킨다. 폭력 집회에 대해서만 적용해도 여전히 이 기술은 폭력적인 참여자들 뿐 아니라 이들과 평화적으로 공존하는 참여자들에게 영향을 미친다. 얼굴인식 기술의 도입은 부정적인 결과에 대한 공포 때문에 합법적인 집

회 및 결사의 자유 행사를 주저하는 개인들에게 위축적 효과를 낳는다. 특정한 개인이나 단체와 교류하거나 특정 행사나 집회에 참여하는 것을 주저하게 할 수 있다. 이런 위축적 효과는 참여 민주주의의 효과적인 작동에도 명백히 영향을 미친다. 시민사회는 집회 현장의 얼굴인식 기술이 저항 행동 의사에 부정적인 영향을 미치는 국가 감시라고 보고 우려를 표해 왔다. 따라서 유럽법에 따라 집회에 얼굴인식 기술을 도입하기 위해서는 다른 공공장소에 대한 경우보다 더 엄격한 법적 요건 등 필요성 및 비례성 심사 기준을 충족해야 할 것이다.

(5) 양질의 행정에 대한 권리

유럽 기본권헌장은 양질의 행정에 대한 권리(Right to good administration)를 보장하고 있다. 이는 크게 기록접근권과 이유제시권으로 구성된다. 기록접근권은 개인이 결정이 내려진 근거 및 그 사유에 대해 쉽게 이해할 수 있도록 돕고 의견제시권을 행사할 때 반론을 제기할 수 있는 기반을 제공하며, 이유제시권은 의사결정 과정을 보다 투명하게 하여 관련자가 조치나 공권력 작용이 취해진 사유를 알 수 있게 한다.

> 유럽 기본권헌장 제41조 양질의 행정에 대한 권리
>
> 1. 모든 사람은 유럽연합의 기관, 기구, 사무소 및 조직에 의하여 합리적인 기간 내에 공평하고 공정하게 자신의 업무가 처리될 수 있는 권리를 갖는다.
> 2. 이 권리는 다음 다음 각 호의 권리를 포함한다.
> (a) 자신에게 불리한 개별적 조치가 취해지기 전에 의견을 진술할 수 있는 모든 사람의 권리
> (b) 비밀유지와 직업 및 영업비밀의 적법한 이익을 존중하면서 자신의 기록에 접근할 수 있는 모든 사람의 권리
> (c) 결정의 이유를 명시하여야 하는 행정기관의 의무
> 3. 모든 사람은 유럽연합의 기관 또는 그 직원이 직무를 수행함에 있어서 야기한 손해에 대하여 회원국의 법률에 공통된 일반원칙에 따라 보상을 청구할 권리를 갖는다.
> 4. 모든 사람은 유럽연합관련조약의 언어 중 하나로 유럽연합의 기관에 질의할 수 있고, 해당 기관은 동일한 언어로 답변하여야 한다.

기록에 대한 접근권을 행사하려면 사람들이 자신의 기록이 거기 존재한다는 사실을 알아야 하지만, 얼굴인식의 경우 사람들은 자신의 얼굴이 수집, 보관되고 대조를 위해 데이터베이스에서 처리되는 것을 잘 모른다는 문제가 있다.

이 권리 행사의 구체적인 내용은 GDPR 및 경찰디렉티브상 정보주체의 권리 및 구제의 권리와 연결될 수 있다. 개인정보 처리의 목적이 범죄 예방·수사·탐지 및 기소, 형의 집행, 공공안전 보호에 있을 경우 적용되는 경찰디렉티브는 △ 공적/법적 신문, 수사 및 절차에 대한 방해 행위 방지, △ 범죄행위 예방, 탐지, 수사 및 기소 및 형의 집행시 편견 방지 △ 공공안전 보호 △ 국가안전 보장 △ 타인의 권리와 자유 보호를 위한 경우 정보주체의 권리 행사를 제한한다. 이는 범죄수사의 밀행성에 따른 예외라고 이해할 수 있다. 따라서 법집행 목적의 개인정보 처리에 대한 효과적인 권리 행사를 보장하기 위해서는 독립적인 책무성 메카니즘이 중요하다. 법집행 목적 개인정보 처리에 대한 기관 내외부 감독 기능을 함께 활용하고 얼굴인식 기술의 사용 이전, 사용중, 사용후 각 단계에서 감독을 활성화하는 것이 개인의 권리를 보호하는 데 도움이 될 것이다.

(6) 효과적인 구제를 받을 권리

유럽 기본권헌장은 효과적인 구제 및 공정한 재판을 받을 권리를 규정하고 있다(제47조).

효과적인 구제를 받을 수 있는 권리는 얼굴인식에 따른 경찰 검문처럼 오로지 또는 중대하게 얼굴인식 기술에 의해 이루어진 의사결정에도 적용된다. 이때 효과적인 구제를 받을 권리는 사람이 자신의 얼굴 이미지가 처리된다는 사실을 알 수 있어야 한다는 것이다. 유럽사법재판소는 어떤 조치로 인해 권리와 자유가 침해된 사람들이 구제받을 권리를 행사하기 위해서는 고지가 필수적이라고 보았다. 2016년 유럽사법재판소는 비밀 감시의 경우 그 고지가 수사를 위협하지 않게 된 즉시 각국 법집행기관이 해당 조치로 영향을 받는 모든 사람들에게 고지해야 한다고 판결했다(Tele2 판결).

얼굴인식 기술로 개인정보를 처리하는 경우도 이 원칙에서 예외가 없다. 법집행기관이 '감시 대상 목록'을 방대한 사람들에게 적용하는 경우 역시 이에 해당할 것이다. 사람들은 자신의 얼굴 이미지가 어째서 '감시 대상 목록'에 포함되었는지 문제제기하고 싶을 수도 있고, 어째서 이렇게 불투명한 방식으로, 자신의 동의 없이 이루어지는지 문제제기하고 싶을 수도 있고, 자신들에게 부정적인 결과(불법적인 검문검색 혹은 연행)를 낳는 거짓 양성을 시정할 방법을 찾거나 손해(항공편을 놓치거나 입국이 거부되거나 사업상 회의를 놓치는 등)에 대한 배상을 요구하고자 할 수도 있다. 다만 행정 처분은 법원의 재판으로 이어지기 전까지는 재판받을 권리에 적용되지 않는다.

다. 권고 및 시사점

법집행 목적으로 사용되는 얼굴인식 기술이 기본권에 미치는 영향을 검토한 후 유럽 기본권청은 다음과 같이 권고하였다.

- 명확하고 충분히 구체적인 법제도를 통해 얼굴인식 기술의 도입과 사용을 규제해야 한다. 얼굴 이미지의 처리가 필요하고 비례적인지에 대한 판단 기준은 이 기술이 사용되는 목적과, 얼굴 이미지가 자동처리 대상이 된 개인들을 장래 부정적인 결과로부터 보호할 수 있는 보호장치의 수준에 달려 있다. 하나 이상의 기본권에 대하여 불가침의 본질적 핵심을 훼손하는 등 매우 높은 수준으로 침해하는 얼굴인식 형태는 불법이다.
- 두 개의 얼굴 이미지를 비교하여 동일한 사람에게 해당되는지를 확인할 때는 본인확인 목적으로 얼굴 이미지를 처리해야 하고, 얼굴이미지를 데이터베이스나 감시 대상 목록에서 검색할 때는 식별 목적으로 처리해야 하며, 이 두 가지 구분을 명확히 해야 한다. 두 번째의 경우에는 기본권 침해 위험이 더 높기 때문에 필요성과 비례성 심사가 더 엄격해야 한다.
- 공공장소에 배치된 CCTV에서 얼굴 이미지를 추출하는 이른바 '실시간 얼굴인식 기술'은 특히 문제적이다. 이런 방식의 사용은 인구집단내 여러 감정을 촉발하고 국가 대 개인 간 심각한 권력 불균형에 대한 우려를 불러온다. 이런 우려는 심각하게 받아들일 필요가 있다. 개인들이 자신의 얼굴 이미지가 감시 대상 목록에서 검색중이라는 사실을 인지하지 못할 가능성이 있고 통제된 환경(공항이나 경

찰서 등)에서 찍은 얼굴 이미지에 비해 오류율이 높다는 점을 고려할 때, 실시간 얼굴인식 기술의 사용은 예외적인 경우로 국한되어야 한다. 이는 테러리즘 및 중대범죄에 대응하거나, 실종자 및 범죄 피해자 발견 용도로 엄격히 제한되어야 한다.

- 공공장소에 배치된 CCTV에서 얼굴 이미지를 추출할 때, 얼굴인식의 필요성 및 비례성 심사는 카메라가 어디에 배치되는지도 고려해야 한다. 스포츠 및 문화 행사인 경우와 사람들이 자신의 기본권을 행사하는 경우 간에는 차이가 있다. 집회에 대해 얼굴인식 기술을 적용하는 것은 사람들로 하여금 부정적인 결과에 대한 우려로 합법적인 집회결사의 자유 행사를 꺼리게 하는 위축적 효과를 초래할 수 있다. 집회 참여자들에게 얼굴인식 기술을 적용하는 것이 필요적이고 비례적인 상황을 상정하는 것은 어렵다.
- 얼굴인식 기술 알고리즘은 결정적인 결과를 제공하는 것이 아니라, 두 사람이 동일인에 속할 가능성만을 보여줄 뿐이다. 따라서 법집행 상황에서 보면, 사람들을 잘못 표시할 일정한 오차범위가 있다. 이 기술을 도입할 때는, 사람들을 잘못 표시할 위험율을 최소한도로 유지해야 한다. 기술 적용 결과로 검문받는 사람들에 대하여는 존엄성을 존중하는 방식으로 대해야 한다.
- 공공기관은 일반적으로 기술을 조달하고 배치하는 데 민간 기업에 의존한다. 산업계와 과학연구계는 개인정보 보호 등 기본권 보장을 증진하는 기술 솔루션을 개발하는 데 중요한 역할을 담당할 수 있다. 그러나 이를 위해서는 기술 규격 및 계약 상으로 기본권에 대한 고려사항이 포함될 필요가 있다. 유럽연합 공공조달 지침(2014/24/EU)은 회원국들이 제품이나 서비스를 구입시 사회적으로 책임 있는 공공 조달이 이루어지도록 책무를 강화했다. 2014년 지침의 취지에 따라 유럽연합과 그 회원국들은 얼굴인식 기술을 조달하거나 혁신적인 연구를 의뢰할 때 유사한 접근법을 사용할 수 있다. 기본권, 특히 개인정보 보호 및 차별금지 요건을 모든 기술 규격의 중심에 둔다면, 업계가 이에 대해 마땅한 주의를 기울이게 될 것이다. 그밖에 설계시 기본권 준수를 보장하기 위해 기술 개발팀에 개인정보 보호 전문가와 인권 전문가를 참여시키는 구속력 있는 요건 마련도 가능하다. 나아가 기술 규격은 성별, 민족 및 연령에 대한 오인식률과 역효과를 최소화하기 위해 고품질 표준을 참조할 수 있을 것이다.
- 얼굴인식 기술이 어떤 상황에 도입되는지와 무관하게 기본권 영향평가는 기본권

을 준수하는 기술 응용을 위한 필수적인 도구다. 이러한 영향평가는 본 문서에 열거된 권리 등 영향을 받는 모든 권리를 종합적으로 평가할 필요가 있다. 공공기관들이 이러한 영향평가를 수행할 수 있으려면, 기술이 기본권에 미치는 영향을 평가하는 데 필요한 모든 정보를 기업으로부터 제공받을 필요가 있다. 영업비밀이나 기밀 유지 원리가 이러한 노력을 방해해서는 안 된다.

- 끊임없이 발전하는 기술에 비추어 볼 때, 기본권 침해를 예측하기가 쉽지 않다. 따라서 얼굴인식 기술 발달에 대해 독립적인 감독 기구의 면밀한 감시가 필수적이다. 유럽 기본권헌장 제8조 제3항은 독립된 기관의 개인정보 처리 감독을 요구하고 있다. 얼굴인식 기술의 영향을 받는 사람들의 기본권 침해를 방지하고 이들의 기본권을 효과적으로 옹호하려면 감독 당국이 충분한 권한과 자원, 전문지식을 갖춰야 한다.

4. 중국

중국 정부는 전국적인 영상 감시 네트워크 시스템을 추구하고 있으며, 이에는 얼굴인식 기술과 더불어 모든 영상을 당국이 감시하고 비교할 수 있는 데이터베이스 등 인공지능을 활용한 다양한 감시 기술이 포함되어 있다.

현재 중국 전역에는 공공과 민간을 합하여 약 2억 대 이상의 CCTV가 설치되어 있는 것으로 추정되는데, 이중 최소 2천만대 이상이 2005년부터 시작된 공공의 안전과 재난 방지 목적의 감시 시스템 '톈왕(天網, Skynet)'의 운영을 위해 활용되고 있다. 톈왕 시스템을 위해 설치된 CCTV는 최근 얼굴인식을 포함해 성별, 연령대, 복장 등 다양한 특성을 도출해내는 기능을 갖췄으며 약 2년 간 2,000명 이상의 범죄자를 체포했다고 관영 언론을 통해 보도된 바 있다. 이러한 광범위한 감시 체계는 2016년 중국판 스마트시티 사업인 '쉐량(雪亮, Sharp Eye)' 시스템으로 확장되는데, 중국 정부는 이를 통해 2020년까지 중국 공공영역과 주요 산업지역의 100%를 모두 감시하는 것을 목표로 하고 있다. 쉐량은 톈왕 시스템과 마찬가지로 데이터 마이닝, 얼굴인식, 번호판 인식, 행동 인식, 지능형 경고 시스템 등 각종 인공지능 기술을 활용하고 있으며 이는 국가적 차원의 인공지능 산업, 특히 감시 목적 기술의 인공지능에 대한 막대한 투자와 지원과 함께 진행되었다[60].

강력한 국가적 감시 체계의 추구는 중국 당국이 반체제, 반정부 인사를 식별하고 탄압하는 데 얼굴인식 기술을 악용해 왔다는 지적으로 이어진다. 실제로 휴먼라이츠워치(HRW)에 의하면 중국 정부가 위구르족과 신장 지역 무슬림의 통제와 탄압을 위해 얼굴 인식 정보를 비롯한 생체인식정보를 수집하고 민족에 따른 분류를 진행하는 등 다양한 인공지능 기술을 활용하고 있음이 밝혀지기도 했다[61]. 2019년 여름 홍콩에서 일어난 대규모 시위에서도 중국 정부의 얼굴인식 기술 활용에 대한 우려 때문에 공공장소의 CCTV와 스마트 가로등을 파손하거나 직접적으로 가리는 행위가 시위 전략의 일부로 등장했다.

중국은 감시와 통제 뿐만 아니라 일반 행정 분야와 민간 분야에도 얼굴인식 기술이 빠르게 도입되었다. 특히 텐센트 같은 민간 기업은 중국 정부와 함께 얼굴인식으로 본인인증을 거쳐 발급받는 디지털 모바일 신분증, 얼굴인식을 통한 결제 등을 구축하는 등 정부의 신분증 데이터베이스에 등록된 얼굴 사진이 민간 기업을 통해서도 적극적으로 활용되고 있다.

최근에는 이러한 방대한 양의 얼굴인식 기술 활용이 생체인식정보의 유출과 오용으로 인한 국민의 피해로 돌아오고 있다. 민간 기술 업체와 앱 운영사 등의 얼굴 정보 유출 뿐만 아니라, 남의 얼굴 정보를 도용하여 결제를 진행하거나 현금을 인출하는 등 관련한 범죄가 갈수록 심각해지는 양상을 보인다. 중국 과기일보의 설문조사에 따르면 응답자의 64.4%가 얼굴인식 기술이 남용되고 있다고 답했으며, 응답자 30% 이상이 얼굴 정보 유출과 남용으로 인한 사생활 침해 또는 재산 피해를 경험했다고 하는 등 생체인식정보에 대한 강력한 보호 필요성을 보여주고 있다[62].

---

60) 과학기술&ICT 정책기술 동향(2019. 8. 2); China Public Video Surveillance Guide: From Skynet to Sharp Eyes 〈https://ipvm.com/reports/sharpeyes〉

61) How Mass Surveillance Worksin Xinjiang, China 〈https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang〉

62) 중국인 64% "中얼굴인식 기술 남용"…'빅브라더' 우려, 한국경제(2020. 10 .20).

Ⅳ. 국내 현황 및 관련 법제도

1. 국내 얼굴인식 기술 사용 현황 및 계획

가. 경찰청

(1) 경찰 3D 얼굴인식 시스템

경찰청은 '3D 얼굴인식 및 3D 얼굴영상 변환 시스템 개발 사업'을 진행하며 얼굴인식 기술을 통해 CCTV, 블랙박스 등으로 범죄현장에서 촬영된 용의자의 신원을 식별하는 시스템을 구축하기 시작했다.

먼저 경찰은 기존에 존재하던 구속피의자에 대한 사진 자료를 3D 사진으로 변환해 데이터베이스로 구축하는 것을 목표로 했다. 기존 경찰이 보유한 정면과 측면 얼굴 사진을 대상으로 하는 경우 CCTV 등 실제 환경에서 추출해낸 용의자의 다양한 얼굴 각도에 대해 얼굴인식의 성능이 현저히 떨어지는 관계로 기존의 사진을 고도화시킨 것이다.

기존 사진의 고도화 이후 서울, 인천, 경기 지역 15개 경찰서에 자체적인 3D 영상 촬영 시스템을 보급해 구속피의자에 대한 3D 촬영을 시작했으며 이는 2017년 전국 경찰서에 보급되었다. 2019년 기준 해당 시스템의 데이터베이스에는 198,330건의 얼굴인식 정보가 포함되어 있다.

〈표1〉 범죄별 DB 구축 현황(9대 수법범죄)

구분	강도	절도	사기	위·변조	약취유인	계
DB(건)	18,777	77,068	49,439	8,911	963	
구분	공갈	방화	강간	장물	기타	198,330
DB(건)	6,368	3,121	29,421	1,707	2,555	

*자료 : 2019년 정기국회 국정감사 자료(정인화 의원, 이하 같음)

경찰청은 해당 개발 사업을 시작한 2014년 이후 오인식율 개선, 검색 후보군 검출, 저조도 인식 개선 등 고도화 작업을 거쳐왔으며 이후 사업 계획에 따르면 2024년 CCTV를 통한 실시간 얼굴인식을 목표로 하고 있다.

〈표2〉 경찰 인공지능 알고리즘 및 자동화된 의사결정 도입 현황

구분	3D얼굴인식시스템 알고리즘 개발 내용
'14	○ 3D얼굴인식 및 3D 얼굴영상 변환 시스템 개발 ❖ 2D → 3D 변환 시스템 개발(KIST) ❖ 얼굴인식시스템 개발(1:N) - 정면 얼굴, 좌우 90도 이내(오인식율 10% 이내) 등
'15	○ '15년 3D 얼굴인식시스템 고도화 ❖ 얼굴인식시스템 개발(1:N) - 정면 얼굴, 좌우 90도 이내(오인식율 5% 이내) 등 ❖ 나이 인식 시스템 개발(±7세) ○ 운용 서버 구축 ❖ 매칭 서버 2개, 스토리지 서버 1개 설치, DB 구축, 검색 후보군 검출 가능
'16	○ '16년 3D얼굴인식시스템 고도화 ❖ 얼굴인식시스템 개발(1:N) - 정면 얼굴, 좌우 90도 이내(오인식율 3% 이내) ❖ 저조도(200Lux 이상) 정면 얼굴인식 개발
'17	○ '17년 3D얼굴인식시스템 고도화 ❖ CCTV 상단 30도 이내, 좌우 45도 이내 얼굴인식 성능 개발 (Kface DB 기준* 오인식율 3.96% 이내) * Kface DB 기준 도입 : 한국인 얼굴로 구성된 데이터베이스('17년 구축) ❖ 저조도(100Lux 이상) 정면 얼굴인식 개발 (Kface DB 기준 오인식율 1.3% 이내)
'18	○ '18년 3D얼굴인식시스템 고도화 ❖ CCTV 하단 15도 이내, 좌우 45도 이내 얼굴인식 성능 개발 (Kface DB 기준 오인식율 3.4% 이내) ❖ 부분 가림 얼굴인식(정면) 개발(눈과 눈썹이 가려진 부분 얼굴인식 개발)
'19	○ '19년 3D얼굴인식시스템 고도화 ❖ 저조도(40lux 이상) 상단 30°에서 하단 15°이내 정면 얼굴인식 개발 (Kface DB 기준 오인식율 10% 이내) ❖ 특징점 위치 추출의 정확도 향상을 위한 성능 고도화 등

〈표3〉 범죄예방 3D얼굴인식시스템 연차별('20년~'24년) 고도화 사업 계획

년도	요구예산	얼굴인식 성능 고도화 사업 내용(예정)
'20	2억	○ 어두운(저조도 40Lux이상) 범죄현장에서 찍힌 용의자 얼굴인식 개발(CCTV 각도 : 상단 30도 &좌우 45도 이내) ※ 일반조도 : 300 ~ 500Lux
'21	2억	○ 어두운(저조도 40Lux이상) 범죄현장에서 찍힌 용의자 얼굴인식 개발(CCTV 각도 : 하단 15도 &좌우 45도 이내)
'22	2억	○ 마스크 착용 등 얼굴 사진이 일부 가릴 경우 얼굴인식(정면) 개발 등
'23	2억	○ 범죄현장 동영상 속 얼굴 사진 인식 등
'24	2억	○ 실시간 CCTV 연계 얼굴인식 등

현재 경찰 등 수사기관이 3D 얼굴인식 데이터베이스 또는 얼굴인식 데이터베이스를 구축하고 자동으로 비교하며 대조할 수 있는 시스템을 운영하도록 허용하는 직접적인 법적 근거는 없다. 통상 수사기관에 의한 개인정보 수집은 경찰법 3조, 경찰관직무집행법 2조상 '치안정보의 수십, 작성 및 배포' 조항에 의해 정당화되는데, 얼굴인식 기술을 비롯한 인공지능 기술의 도입으로 인한 잠재적인 침해 가능성을 고려할 때 그 근거가 충분한지 의문이다. 2018년 말 기준 공공기관의 공개된 장소에 지속적으로 설치된 CCTV는 100만대를 돌파했고, 민간에서 설치한 CCTV를 포함하면 2014년 기준 8백만 대가 전국에 설치된 것으로 파악된다. 이러한 환경에서 CCTV 등 영상정보처리기기를 통해 수집된 영상이 뚜렷한 활용 기준과 보호장치 없이 얼굴인식 기술과 결합된다면 정보주체는 동의와 인지 없이 신원 확인을 당하는 등 정보주체의 권리가 무차별적으로 침해되는 결과를 가져올 것이다.

특히 정부에 비판적인 집회의 주최자나 노동쟁의 행위자 등까지 그 채취와 보관 대상으로 하였던 디엔에이신원확인정보 데이터베이스의 경우와 경찰이 2011년 유성기업 파업 노동자를 대상으로 3D 영상 채증 및 비교 시험을 했던 사례 등을 보면 생체인식정보의 수집과 저장 대상, 보관 및 폐기 등에 대한 논의와 평가가 시급하다 할 수 있다.

(2) CCTV 통합관제센터

대다수의 지방자치단체는 범죄예방, 교통, 불법주정차 관리 등 각기 다른 목적으로 설치·운영하고 있던 CCTV를 효율적이고 체계적으로 관리·운영한다는 명목으로 CCTV를 통합하여 관제·관리하는 CCTV통합관제센터를 설치했다. CCTV통합관제센터에는 대부분 평균 2인 이상의 경찰이 파견되어 관제요원의 관제 업무를 지휘·감독하고 있으며, 이들은 관할 경찰관서와 업무협약서 등을 체결하여 현장출동 지휘, 사건사고 관련 영상자료 열람 및 반출 등 개인정보처리자의 역할 또한 수행하고 있는 것으로 드러났다. 국가인권위원회는 개인정보를 당초 수집의 목적을 넘어 다른 목적으로 이용하거나 특히 범죄 수사 등을 위해 경찰에 제공하는 것을 들어 법률적 근거가 없는 CCTV통합관제센터 운영이 인권침해라고 결정하였다. 2019년 국회 입법조사처가 지적하였듯이, CCTV통합관제센터 영상정보의 실질적인 이용자가 경찰임에도 경찰은 CCTV 영상정보에 대한 개인정보처리자가 아니며 일상적인 관제를 통해 영상정보를 제공받을 수 있는 법적 근거 또한 없다[63].

CCTV통합관제센터는 심각한 기본권 침해와 법적 근거 부재, 개인정보 보호 원칙과의 충돌 등 해결되지 못한 문제가 있음에도 불구하고 각 지자체 별로 그 확대와 활용이 무분별하게 증가하고 있는 추세이다. 특히 기존의 CCTV를 다양한 생체 및 객체 인식 기술을 도입한 지능형 CCTV로 교체하는 스마트 선별 관제시스템, 사물인터넷 활용과 경찰 등 기관과 실시간으로 연계하는 스마트시티 통합 플랫폼 시스템이 대표적이다. 이미 전국 수십 곳의 CCTV통합관제센터에서 CCTV를 통해 지나가는 시민의 성별과 나이대, 입고 있는 옷의 색깔과 종류 등을 식별하고 영상의 특정인을 재식별하는 시스템을 도입했거나 추진하고 있다. 최근 스마트 선별 관제시스템을 도입한 경기도 부천시의 경우 코로나19 대응을 위해 확진자의 얼굴 사진과 CCTV 영상 속 시민들의 얼굴을 대조해 같은 사람을 찾아내고 동선을 파악하는 '확진자 동선 추적 시스템'을 개발하고 있다고 밝히기도 했다[64].

---

63) 최미경·최정민(2019), 위의 글.

나. 기타 기관

(1) 법무부의 외국인 출입국 관리

2010년 9월, 법무부 출입국외국인정책본부는 G20 정상회의를 앞두고 전국 22개 공항·항만에 지문인식기와 얼굴인식기를 설치하여 외국인의 지문과 얼굴 정보를 확인하는 입국심사 강화조치를 시행했다. 해당 강화조치는 최종적으로 국내에 입국하는 모든 입국 외국인, 등록 외국인, 범법 외국인의 지문과 얼굴 정보를 등록하고 확인하는 시스템 구축으로 이어졌으며 사전적인 출입국관리법 개정을 통해 국내 입국 외국인의 생체정보 제공이 의무화되었다.

수집된 외국인의 생체정보는 입국 심사 외 경찰 등 국내 기관의 수사 용도에도 쓰이고 있다. 2013년 법무부는 특정인의 얼굴과 지문을 입국 과정에서 수집된 외국인의 생체정보 데이터베이스와 비교·분석하는 '바이오정보전문분석시스템(Biometrics Analysis System for Experts, BASE)' 프로그램을 개발해 운영하고 있는데, 해당 프로그램은 경찰 등 수사기관이 특정해내지 못한 외국인 용의자의 신원을 식별해내는 등 수사를 지원하고 있다[65]. 언론 보도에 의하면 현재 국내 체류 외국인들의 입국심사 당시 사진 1억 5000만 장이 데이터베이스에 저장되어 있는 것으로 추정되며 2015년부터 2019년 6월까지 총 8435건의 분석 의뢰를 받아 2089건의 신원을 식별해냈다고 한다[66].

2019년 과학기술정보통신부와 법무부는 자동화된 출입국관리를 포함해 공항 내 위험인물에 대해 얼굴 인식 및 이상 행동을 자동으로 식별하고 추적하는 '인공지능 식별·추적 시스템' 사업을 시작했는데 이에 법무부가 기존 확보해둔 출입국 관련 데이터(인공지능 알고리즘 학습에 적합한 안면 데이터 200만 장 이상)를 다수의 AI기업에게 데이터 가공, 학습 및 실증 작업 수행을 위해 제공되고 있는 것으로 추정된다[67].

---

64) 부천시, AI 활용 '확진자 동선 추적 시스템' 개발 추진, KBS News(2020. 11. 9).
65) 바이오정보 분석으로 위험인물 입국 막는다, 법무부 보도자료(2018. 1. 23).
66) 콧수염-뿔테안경으로 가려도…1초만에 "얼굴 일치도 78%", 동아일보(2019. 12. 14).

(2) 성동구청 열화상 카메라

코로나 19라는 공중보건 위기상황을 맞아 개인정보 수집 및 처리를 기반으로 하는 다양한 방역 대책이 도입되기 시작했다. 2020년 5월, 서울시 성동구청은 코로나19 예방을 위한 체온 측정을 명목으로 얼굴인식 기술을 활용한 열화상 카메라를 구매하여 청사와 도서관 입구 등에 배치하였는데, 해당 체온계의 경우 태블릿형으로 카메라 앞에 선 출입자의 얼굴을 인식하여 자동으로 체온을 체크하고 방문 시간 및 얼굴 사진을 저장하는 것으로 보도되었다. 이러한 얼굴인식 열화상 카메라는 성동구청 뿐만 아니라 다양한 지자체의 관공서, 기업, 숙박시설 등의 입구에 배치되었으며 각기 사용하는 제품은 다르지만 비슷한 얼굴인식 기능을 탑재하고 있는 현황이다.

진보네트워크센터의 공개 질의에 대한 답변에 의하면 해당 체온계는 25,000명의 얼굴 사진을 자동으로 저장하며, 얼굴인식 라이브러리를 가져와 관리하는 등의 기능이 존재하는 것으로 밝혀졌다. 구청 측은 얼굴 사진을 포함한 개인정보를 처리하는 기기를 운영함에도 개인정보 보호법에 따른 정보주체의 동의를 받지 않았으며 그 근거로 개인정보 보호법 제58조조제1조제3항을 들며 개인정보 보호법 적용 제외 대상이라고 주장했다. 그러나 해당 예외규정은 정보주체의 권리와 개인정보 보호에 관한 규정을 일괄적으로 배제하기에 '긴급히 필요한 경우로서 일시적으로 처리'되어야 하는 상황에 극히 제한적으로 적용되어야 하는 조항이다.

이후 개인정보 보호위원회는 비공개 실태조사를 통해 주요시설의 열화상 카메라 일부가 개인의 얼굴이 포함된 영상정보를 불필요하게 저장·관리·전송하고 있는 것으로 확인되었다고 밝히며 개인정보의 과다수집 및 오남용 방지, 사생활 침해 예방을 위해 개인정보의 저장·관리·전송을 원칙적으로 금지하고 열화상 카메라 운영에 있어 개인정보 보호법을 준수해야 한다는 내용의 운영수칙을 발표했다[68].

---

67) 인공지능(AI)을 활용한 차세대 출입국관리시스템 개발 본격화, 법무부 보도자료(2020. 07. 23).

(3) 공공기관에 도입된 AI면접과 얼굴 분석 (Categorisation)

2018년부터 채용 절차에 인공지능 시스템이 본격적으로 활용되기 시작했다. 약 20여곳에 달하는 공공기관 또한 이를 도입했는데, 일명 AI면접이라 불리우는 해당 인공지능 시스템은 게임 수행과 함께 화상 면접을 진행하며 구직자의 표정, 감정, 안구 움직임 등의 얼굴 정보와 목소리 톤, 크기, 속도, 음색 등의 음성정보를 추출하여 매력도, 의사표현, 감정 전달력 등 외형적인 특성을 분석하고 분류하는 것으로 알려져 있다[69].

이와 같이 인공지능을 활용한 채용 과정은 자동화된 의사결정으로 인한 차별 가능성, 불투명성과 개인정보 자기결정권 침해 등의 문제가 있지만, 그중에서도 생체인식정보를 활용해 개인을 특성을 분석하고 평가할 수 있다고 주장하는 기술이 취업 과정에 영향을 미치는 방식으로 사용되는 것은 과학적 타당성에 대한 비판이 제기될 수 있다.

뉴욕대 인공지능 연구센터인 AI Now Institute는 미세한 얼굴 표정, 목소리 톤 등을 분석하는 감정인식 기술이 인종학, 골상학 및 유사 과학 등에 기반하고 있어 공공과 민간 영역에서의 개발과 도입을 즉각 유예할 것을 권고했다[70]. 또한 식별과 검증 목적의 얼굴인식 기술과 마찬가지로 분류를 위한 얼굴인식 기술 또한 인공지능이 가질 수 있는 편향적 결과를 가져올 수 있어 대표적인 상용 감정인식 소프트웨어의 경우 백인 남성의 얼굴에 비해 흑인 남성의 얼굴을 보다 화난 얼굴, 경멸하는 얼굴로 인식하는 등, 피부색에 따라 다른 감정인식 값을 보여주는 것으로 드러났다[71].

---

68) 코로나19 관련 열화상카메라 운영 시 동의없이 개인 얼굴영상 저장 금지, 개인정보보호위원회(2020. 11. 05).

69) 투명성·공정성·신뢰성…AI면접 믿을 만할까?, 한겨레21(제1335호)

70) AI Now Institute, New York University (2020), Submission to the European Commission on "White Paper on AI - A European Approach"

71) Rhue(2018), Racial Influence on Automated Perceptions of Emotions 〈https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765〉

2. 국내 관련 법제도 및 비판

이하에서는 법집행기관의 얼굴인식과 관련한 우리나라 법규범 현황을 검토한다. 다만, 출입국 등의 절차에서 여권에 내장된 얼굴인식정보를 1:1로 처리하여 본인을 인증하는 경우는 분석에서 제외하고, 데이터베이스를 이용하여 1:다(多) 또는 다(多):다(多) 방식으로 다수인을 대조하는 얼굴인식정보 처리에 대하여 살펴본다.

가. 법집행과 얼굴인식정보

얼굴인식정보는 특별한 보호가 필요한 민감정보에 해당한다. 우리 개인정보 보호법은 사회적 차별을 야기하거나 현저히 인권을 침해할 우려가 있는 민감한 개인정보를 일반 개인정보보다 엄격히 보호하고 있다(법 제23조 및 동법 시행령 제18조).

2020. 8. 5. 개정 개인정보 보호법 시행령 제18조는 민감정보의 범위에 "개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보"를 신설하였다. 이는 유럽연합 GDPR에서 생체인식정보(biometric data)를 "얼굴 이미지나 지문정보와 같이 특정한 기술적 처리로 얻어진 자연인의 신체적, 생리적, 행동적 특징에 관한 개인정보로서, 자연인을 고유하게 식별할 수 있도록 하거나 확인해주는 것을 의미"한다고 정의한 것과 유사하다. GDPR은 생체인식정보를 그 민감성에 의해 특정 범주(special categories)의 개인정보로 분류하고 그 처리를 일반 개인정보보다 제한한다. 얼굴인식정보는 대표적인 생체인식정보에 속하는데 우리 개인정보 보호법령도 생체인식정보를 민감정보에 포함하여 규율하기 시작한 것이다. 일반 개인정보 보다 제한적으로 처리되는 민감정보의 경우 정보주체에게 별도로 동의를 받은 경우이거나 법령에서 민감정보의 처리를 요구하거나 허용하는 경우를 제외하고 그 처리가 금지되며 이를 위반할 경우 형사처벌을 받는다. 따라서 원칙적으로 법집행기관 역시 얼굴인식정보를 특별히 보호해야 하며 이를 사용하기 위해서는 그 처리를 명시적으로 요구하거나 허용하는 법령적 근거에 기반하는 것이 올바르다.

문제는 공공기관이 “범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우” 얼굴인식정보를 민감정보에서 제외하도록 한 현행 개인정보 보호법령이다. 얼굴인식정보를 포함한 생체인식정보를 민감정보로 분류하여 일반 개인정보 보다 한층 더 보호하는 것은 유럽연합 GDPR을 비롯하여 전세계가 유사하다. 국내 개인정보 보호법령은 법에서 열거한 민감정보 외에도 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 시행령인 대통령령에 위임하여 민감정보로 정하도록 하고 있는데 유전정보, 범죄경력에 관한 정보, 생체인식정보, 인종이나 민족에 관한 정보 등이 그것이다. 그런데 시행령에서 규정한 민감정보의 경우 법 제18조 제2항 제5호부터 제9호까지의 규정에 따라 공공기관이 처리하는 경우 민감정보에서 “제외한다”고 규정되어 있다(동법 시행령 제18조). 본래는 민감정보에 속했던 생체인식정보가 수사기관등이 범죄 수사등에 필요로 하는 경우(법 제18조제2항제7호) 민감정보가 아닌 것으로 간주되게 되는 것이다.

또 현행 개인정보 보호법상 생체인식정보의 처리를 실무에서 소극적으로 해석할 우려도 있다. 2020. 10. 개인정보 보호법령 및 지침·고시 해설(안)에 따르면 얼굴인식을 통해 연령/성별을 ‘추정’하여 유형에 맞는 광고를 내보내는 경우에는 민감정보를 처리하는 것으로 판단하지 않는다고 보았다(개인정보 보호위원회, 2020: 159)[72]. 이런 경우는 특정 개인을 식별하지 않고 단지 연령이나 성별 등 추정된 특성에 따라 대상을 ‘분류’하는 것이기 때문에 “특정 개인을 알아볼 목적으로” 처리하는 경우로 한정된 생체인식정보에 해당하지 않는다고 보았기 때문으로 보인다. 개인정보 보호법의 주무기관인 개인정보 보호위원회는 발열 여부를 분류하는 코로나19 열화상 얼굴인식 카메라가 민감정보를 처리하지 않는다고 보고 일반 개인정보 수집·이용에 대한 법 제15조를 적용하였고, 얼굴영상을 저장하는 경우에 정보주체의 동의를 받도록 하였다[73]. 또 서울 성동구의 체온측정 얼굴인식 카메라에 대한 질의에서는 얼굴인

72) 개인정보 보호위원회가 사전 공개 및 의견수렴 중인 해설서(안)을 기준으로 함. “개인정보 보호법 해설서(안) 사전 공개 및 의견수렴” 공지사항(2020. 10. 6) 참조.

73) 코로나19 관련 열화상카메라 운영 시 동의없이 개인 얼굴영상 저장 금지, 개인정보

식 카메라가 얼굴영상을 저장하지 않고 일시적으로 판단하는 경우 법 제15조 제1항 제3호에 해당하는 공공기관 소관 업무의 수행을 위하여 불가피한 경우에 해당하여 동의 없는 처리가 가능하다고 보았다. 지방자치단체장은 「감염병의 예방 및 관리에 관한 법률」 제49조 제1항 제7호에 따라 감염병 예방에 필요한 시설의 설치를 명할 수 있고 이 경우 동법 시행령 제32조의3에 따라 개인정보가 포함된 자료를 처리할 수 있다는 것이다(개인정보 보호위원회 2020. 10. 28. 결정 성동구의 영상정보 처리 관련 법령해석에 관한 건).

그러나 특정 개인을 식별하는 데 이르지 않는 분류라 하여 이를 일반적으로 생체인식정보에서 제외하는 것은 매우 부당하다. 영국 개인정보 보호 감독기관(ICO)는 경찰의 실시간 얼굴인식 사용에 대해 검토한 2019년 보고서에서 개인을 식별, 인증, 검증 뿐 아니라 '분류'하기 위한 목적으로(for the purposes of identification, authentication or verification, or categorisation of individuals) 얼굴인식정보를 처리하는 경우에 대하여 모두 동일한 규정을 적용하여 분석하였다[74]. 유럽연합 기본권청(FRA) 또한 1:1 개인 인증(verification, one-to-one comparison), 1:다(多) 개인 식별(identification, one-to-many comparison) 뿐 아니라 특성별 분류(categorisation, matching general characteristics) 역시 얼굴인식 처리의 여러 사용 목적(different purposes) 중 하나로 보았을 뿐 생체인식정보가 아닌 것으로 간주하지는 않았다[75]. 얼굴인식정보가 민감정보인 생체인식정보로서 특별히 보호받는다고 하면, 얼굴 영상을 저장하지 않는 일시적인 처리라는 이유로 이를 생체인식정보에서 제외할 수 없다. ICO는 얼굴인식 처리는 그 일치 여부 및 일치하지 않는 사람의 정보가 단시간 내 삭제되는지와는 관계없이 생체인식정보 처리에 속한

보호위원회 보도자료(2020. 11. 5).

74) ICO(2019). "ICO investigation into how the police use facial recognition technology in public places"〈https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf〉

75) FRA(2019). "Facial recognition technology: fundamental rights considerations in the context of law enforcement" 〈https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law〉

다고 보았으며(ICO, 2019: 2)[76], 실시간 얼굴인식의 전체 과정에 개인정보 보호법이 적용된다고 설명하였다.

경찰이 대상자를 분류하기 위해 얼굴인식정보를 처리할 수 있는 경우는 매우 다양하다. 발열자와 그렇지 않은 사람을 분류하듯이, 집회의 참가자와 비참가자를 분류하거나 나이 또는 성별에 따라 사람을 분류하거나, 거짓말과 참말을 분류할 수도 있다. 경찰이 얼굴인식정보의 처리를 통하여 사람을 분류한 결과에 따라 검문검색, 통행제한, 출입거부 등 차별적이고 강제적인 조치가 취해지거나 때로 물리적 충돌이나 연행 등 인권침해가 이어질 수도 있다. 이런 경우가 인증이나 식별 등 얼굴인식정보의 다른 처리에 비하여 그 침해 정도가 덜하다고 보기 어렵다.

한편, 그 분류 대상 범주가 장애 등 건강 상태, 인종이나 민족 등 개인의 민감한 속성에 대한 것이라면 이는 그 자체가 민감정보의 처리로서 원칙적으로 제한되어야 한다. 미국 워싱턴 주 얼굴인식 규제법{S.B. 6280 (Wash. 2020)}에서는 인종, 민족, 국적, 출생지, 이민 상태, 나이, 장애, 성별, 성정체성, 성적 지향 또는 기타 법으로 보호되는 특성을 확인하기 위한 목적으로 얼굴인식 기술의 활용을 금지하였다.

결론적으로, 개인정보 보호법의 제정 취지에서 민감정보를 원칙적으로 보호하도록 한 만큼 공공기관이 법집행 목적으로 민감정보를 처리하는 경우 이를 민감정보에서 제외하도록 한 규정은 삭제하는 것이 바람직하다. 특히 이러한 제외를 법률에 근거하지 않고 시행령 단서 규정으로만 규정하고 있는 점은 위임입법의 한계를 일탈한 것이다. 법집행기관이 명시적인 법적 근거 없이 인증, 식별은 물론 분류 목적으로 얼굴인식정보를 처리하는 것은 모두 금지되어야 한다. 특히 민감한 속성을 분류하기 위하여 얼굴인식정보를 처리하는 것 또한 민감정보 처리로서 제한되어야 한다.

---

76) "Sensitive processing occurs irrespective of whether that image yields a match to a person on a watchlist or the biometric data of unmatched persons is subsequently deleted within a short space of time."

나. 경찰의 직무와 개인정보 처리

만약 얼굴인식정보가 민감정보가 아니라면 일반 개인정보에 해당한다. 수사기관 등 법집행기관은 개인정보 보호법 제15조 제1항 제2호에 따라 '법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우' 또는 동조 동항 제3호에 따라 '공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우' 일반 개인정보를 수집 및 이용할 수 있다. 그런데 우리 헌법재판소의 결정례 및 대법원의 판례에서는 경찰의 개인정보 처리 근거에 대한 허용폭을 매우 크게 보고 있다.

2005년 헌법재판소는 경찰청장이 지문정보를 보관하는 행위에 대하여 구체적인 법률에 근거하지 않아도 "공공기관은 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보화일을 보유할 수 있다."고만 규정하고 있는 (구)공공기관의개인정보보호에관한법률 제5조, 제10조 제2항 제6호에 근거한 것으로 충분하고, 그 밖에 주민등록법 제17조의8 제2항 본문, 제17조의10 제1항, "치안정보의 수집, 작성 및 배포"에 대한 경찰법 제3조 및 경찰관직무집행법 제2조에도 근거하고 있다고 보았다(헌재 2005. 5. 26. 결정 99헌마513, 2004헌마190병합). 재판관 송인준, 재판관 주선회, 재판관 전효숙은 반대의견에서 경찰법 제3조가 경찰청은 치안에 관한 사무를 관장한다는 경찰의 조직법이며 경찰관직무집행법 제2조는 경찰관의 일반적인 직무집행의 범위를 규정한 것에 불과하므로, 경찰청장이 구체적인 법률에 근거를 두지 않고 지문원지를 수집·보관하는 행위는 정보이용의 주체, 목적과 범위 등을 구체적으로 특정하여 규율하여야 할 개인정보자기결정권의 본질에 반한다고 지적하였으나 소수에 그쳤다. 대법원도 헌재 결정과 유사한 취지의 판결을 하였다. 2009년 무혐의 처분을 받은 피의자의 사건정보를 경찰이 구체적인 법률에 근거를 두지 않고 경찰범죄정보관리시스템이나 법무부 형사사법정보시스템에 기록·보관한 행위에 대하여 제기된 손해배상 청구소송에서, 대법원은 (구)공공기관의개인정보보호에관한법률 제5조가 공공기관이 소관업무를 수행하기 위해 필요한 범위 안에서 개인정보파일을 보유할 수 있도록 허용하고 있고, 치안정보의 수집, 작성

및 배포를 규정한 경찰법 제3조, 경찰관직무집행법 제2조 등에 근거하여 위 개인정보의 기록·보관이 위법하지 않다고 보았다(대법원 2012.10.25. 선고 2012다12641 판결).

경찰은 현재까지도 이러한 결정례 및 판례에 근거하여 상당히 많은 국민의 개인정보를 특별한 법적 규율 없이 수집 및 이용하고 있다. 그러나 2011년 제정 시행된 개인정보 보호법은 (구)공공기관의개인정보보호에관한법률과 달리 공공기관의 경우에도 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 '불가피한 경우' 또는 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 '불가피한 경우'에 한하여 개인정보의 수집·이용을 허용하고 있다(개인정보 보호법 제15조 제1항 제2호 및 제3호).

경찰이 방대한 양의 개인정보 처리가 필요한 불가피성을 입증하지 않은 채 특별한 요건이나 절차적 제한도 없이 계속하여 이를 처리하고 향후 프로파일링 분석 및 자동화된 의사결정에까지 이른다면 위법일 뿐 아니라 국민의 개인정보 자기결정권에 대한 부당한 제한이 아니라 할 수 없다. 실제로 개인정보보호위원회는 2019년 5월 서울특별시 민생사법경찰단의 인공지능 수사관이 피내사자 또는 피의자를 특정하지 않고 온라인에 공개된 전국 불특정 다수의 게시물을 광범위하게 감시·분석하는 것은 개인정보 보호법 제15조에 위반된다고 보았다(개인정보 보호위원회 2019. 5. 13. 결정 제2019-09-130호).

법집행기관의 얼굴인식 기술 사용에 앞서 현행 법규범에서 범죄 수사 등을 이유로 개인정보 처리에 대하여 광범위한 예외를 인정하고 있는 규정과 관행의 문제를 해결할 필요가 있다. 경찰의 개인정보 처리는 관련된 사람에게 중대한 영향을 미치기 때문에 이 분야 개인정보 처리에 대한 보호 규율을 상세하게 규정하는 것이 필수적으로 요구된다(FRA, 2018: 277)[77]. 유럽연합은 2016년 GDPR과 함께 〈형사 법집행 목적의 개인정보 보호에 대한 디렉티브(일명 '경찰디렉티브')[78]〉를 제정하여 회원국이 일부 예외를 제외하고 법집행

77) FRA and Council of Europe(2018). "Handbook on European data protection law : 2018 edition".

분야에도 원칙적으로 개인정보 보호 원칙을 적용하도록 하였다. 경찰디렉티브는 GDPR에 비해 일부 규정이 완화되어 있지만 경찰 등 법집행기관에 대해서도 원칙적으로 개인정보 보호 원칙 및 독립적인 감독을 적용하도록 하였다는 점에서 개인정보 보호 감독을 강화하였다. 유럽평의회의는 여기서 더 나아가 개인정보 처리 관련 규범에서 경찰 및 형사사법을 포함한 모든 분야를 망라하여 동일한 원칙의 적용을 요구하고 있다. 유럽평의회는 1987년 '경찰 권고(police recommendation)'를 채택하여 회원국들에게 〈개인정보 보호 협약(일명 '108호 협약')〉[79]의 원칙을 경찰의 개인정보 처리에도 적용할 것을 권장하였다. 2018년 유럽평의회는 108호 협약을 개정하여 현대화하면서 〈경찰 분야에서의 개인정보 사용에 관한 실질적 지침〉을 채택하여 경찰 권고를 보완하였다. 이 지침은 '19. 외부통제(External control)' 원칙에서 하나 이상의 독립적이고 효과적인 감독기관을 두도록 의무화하였다. 이때 부처 또는 경찰 자체 내에 설립된 감독기관은 명확히 배제하였다는 점이 눈에 띈다[80].

범죄수사를 비롯하여 법집행기관들의 개인정보 처리 및 민감정보의 처리에 많은 예외를 두고 있는 우리 개인정보 보호 관련 법령의 경우 시급한 개선이 필요하다. 유럽연합 〈경찰 지침〉 및 유럽평의회 〈경찰 분야에서의 개인정보 사용에 관한 실질적 지침〉 등 국제규범에 부합하는 방향으로 경찰 등 법집행기관에 대해서도 원칙적으로 개인정보 보호 원칙 및 독립적인 감독을 적용하도록 입법적 조치가 이루어져야 하며 이 기관이 경찰의 얼굴인식 기술 활용에 대해서도 사전적이고 사후적으로 감독해야 한다.

---

78) DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

79) CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108].

80) "The supervisory authority set up within a ministry or the police itself does not fulfil this obligation."

다. 경찰의 얼굴인식정보 처리

(1) 얼굴인식 데이터베이스의 구축 및 운용

현재 경찰이 데이터베이스로 보유하고 있는 얼굴정보는 주민등록증과 운전면허증의 얼굴이미지, 또 범죄수법원지와 우범자관찰 기록상의 얼굴이미지를 들 수 있다. 이처럼 경찰이 범죄 예방 및 수사 목적으로 보유 중인 얼굴이미지에 대한 인식의 효용성을 높이기 위하여 얼굴인식정보로 변환하여 데이터베이스를 구축하는 행위는 과잉금지 원칙에 위배될 가능성이 높다.

우선 경찰청은 전국민의 주민등록증 발급 과정에서 채취된 지문정보와 얼굴정보를 전산화하여 보유하고 있다. 그러나 주민등록법은 주민등록발급 신청서를 통해 이들 신체정보를 채취할 수 있는 근거만 담고 있으며 그 시행규칙에서 해당 발급신청서상의 정보들을 경찰청에 송부하는 규정을 두었을 뿐이다. 즉 '채취(행위)'에 대한 간접적인 수권규정을 두고 있지만, 지문 및 사진 자체를 개인정보 차원에서 규율하고 있는 법률은 존재하지 않는다. 헌법재판소는 주민등록증제도 취지에 날인된 지문의 범죄수사목적상 이용도 포함된다고 밝혔지만, 한편으론 지문정보의 수집·보관·활용에 있어서 그 목적과 대상, 범위, 기한 등의 요건을 구체적으로 규정하는 입법개선의 노력도 필요하다며 법률유보의 흠결을 인정하기도 했다(헌재 2015. 5. 28. 결정 2011헌마731).

나아가 경찰이 이를 얼굴인식정보로 변환하는 것은 전 국민을 대상으로 한다는 점에서 법적 근거가 미약할 뿐만 아니라 과잉금지의 원칙에도 위반된다. 얼굴이미지를 전자적으로 인식할 수 있는 얼굴인식정보는 CCTV 등 다른 정보와 결합하여 자동적으로 대량의 얼굴검색을 가능하게 하는 새로운 감시수단으로 사용될 가능성이 높다(박주희, 2020: 441). 특히 이성기(2018: 187)는 헌재결정의 다수의견이 지문정보수 집의 위헌성 판단에 있어서 다른 개인정보를 통합하는 '연결자(key data)'로 사용되거나 새로운 감시수단으로 사용됨으로써 새로운 개인정보의 침해가능성이 있는지 여부를 검토하였다는 점을 주목하였다(헌재 2015. 5. 28. 결정 2011헌마731). 얼굴인식정보는 CCTV등 다른 정보와 결합하여 자동적으로 대량의 얼굴검색을 가능하게 하는 새로운 감시수

단으로 사용될 가능성이 높다는 점, 범죄수사의 목적을 위해서라면 별도의 법률이나 형사소송법상 근거 규정에 따라 재범의 가능성이 있는 범죄자를 중심으로 운영하는 것이 더 효과적이고 통제가 가능하다는 점에서 경찰이 주민등록신청서상의 얼굴이미지를 이용하여 얼굴인식 데이터를 처리하는 것은 위법, 위헌의 가능성이 크다는 것이다.

한편 경찰이 운영하고 있는 범죄수법원지와 우범자관찰 기록상의 얼굴이미지의 경우 그 자체로 명확한 법적 근거가 없어 해당 얼굴이미지를 변환한 얼굴인식 데이터베이스를 운영하는 것도 위법하다.

이성기(2018: 192)는 수사기관이 사용하는 얼굴인식정보와 관련하여 별도의 법률을 제정하여 그 보호 및 관리·감독에 대한 명확한 절차를 두고 보관기간 및 삭제 시기 등에 대하여 구체적인 제한 규정을 두는 것이 바람직하다고 제언하였다. 특히 얼굴인식정보의 데이터베이스를 운용하기 위해서는 그 기본권 제한 목적의 정당성, 수단의 적합성, 피해의 최소성, 법익의 균형성이 갖추어진 법률에 의하여야 위법, 위헌성을 개선할 수 있을 것이다. 경찰이 얼굴인식정보 데이터베이스를 구축·운용하고 분석하는 것은 국가에 의한 전면적인 감시 가능성을 내포하고 있기 때문에 일반적인 상황에 비해 목적구속의 원칙을 더욱 엄격하게 적용하여야 하며, 더 나아가 목적변경 자체를 금지할 필요성도 있다(박원규, 2019: 259). 다만 어떠한 법률이라도 전 국민을 대상으로 하는 얼굴인식정보 데이터베이스를 구축·운영하는 것은 과잉금지원칙 위반을 벗어나기 어려울 것이다.

재범의 가능성이 있는 범죄경력자를 대상으로 얼굴인식정보 데이터베이스를 운영하는 경우 그 구체적인 수집 및 이용의 목적, 대상 범죄 및 수집의 범위, 수집 및 이용의 방법과 절차, 보관 및 파기 등을 법률에서 구체적으로 규정해야 할 것이다. 다만 현행 「디엔에이신원확인정보의 이용 및 보호에 관한 법률」에 대한 인권침해 논란에서 볼 수 있듯이, 재범 위험성이 있는 대상의 요건에 대한 규정 미비나 보관 및 삭제 기간이 미흡한 것은 중대한 기본권 침해이므로 구체적으로 규정해야 한다. 특히 디엔에이법의 경우 그 대상 범죄에 집단주거침입죄, 퇴거불응죄 등을 포함함으로 인해 철거민, 노동조합원, 노점

상 등 생존권을 요구하며 농성 등 옥내외 집회나 시위에 참가하였다가 유죄판결을 받은 경우 때로는 그 실형 선고 여부와 무관하게 디엔에이신원확인정보가 채취 보관되어 논란을 빚은바 있다. 집회 및 시위에 관한 법률 위반 및 일반도로교통방해죄를 얼굴인식정보 데이터베이스의 포함 대상에 포함할 경우 이를 이용하여 불특정 다수 집회참가자에 대한 실시간 감시가 상시적으로 가능해 지고 이는 국민의 집회 시위의 권리를 본질적으로 침해할 우려가 있기 때문에 그 대상에서 제외하는 것이 바람직하다.

또 얼굴인식정보를 다른 정보와 연계하여 프로파일링에 사용하고 자동화된 의사결정에 이를 때에는 그 제한 및 정보주체의 보호에 대하여 구체적으로 법률에 규정해야 한다.

(2) 사후 얼굴인식을 통한 신원확인

만약 경찰이 합법, 합헌적인 얼굴인식정보 데이터베이스를 보유하고 있다면 그 이후 이를 이용하여 신원확인 등 얼굴인식 처리를 할 때 다시 그 구체적인 목적의 정당성 및 대상의 규모, 그 침해성의 측면에서 차등적으로 검토할 필요가 있다. 민감정보인 얼굴인식정보 데이터베이스가 일단 구축되었다는 이유로 제한 없이 사용한다면 과잉금지원칙에 위배될 수 밖에 없기 때문이다. 경찰의 얼굴인식정보의 처리는 시점별로 사후적인 신원확인과 특히 논란이 많은 실시간 신원확인으로 나누어서 검토할 수 있다.

우선 사후적인 신원확인으로는 범죄현장에서 확인된 CCTV 얼굴정보를 보유 중인 얼굴인식 데이터베이스와 대조하여 미지의 신원을 확인하는 경우를 생각해볼 수 있다. 이성기(2018: 188)는 이 경우를 임의수사로 볼 수 있기에 별도의 영장은 불요하다고 보았다.

그러나 경찰의 지문인식정보 수집 및 이용에 대한 두 차례의 헌법적 판단에서 그 목적과 대상, 범위, 기한 등의 요건을 법률에 구체적으로 규정하여 규율할 것을 요구하는 의견이 커져 왔음을 주목할 필요가 있다(헌재 2005. 5. 26. 결정 99헌마513, 2004헌마190병합; 헌재 2015. 5. 28. 결정 2011헌마731).

비록 특정한 범죄 용의자를 사후에 식별하기 위한 목적이라고는 하지만 민감정보인 생체인식정보를 처리하는 만큼 법률에서 구체적으로 제한할 필요가 있다. 이 법률은 경찰이 입수한 얼굴이미지를 얼굴인식기술을 이용하여 얼굴인식정보 데이터베이스와 대조하여 처리하는 유형과 단계별로 그 목적, 대상, 방법, 절차 및 기한을 구체적으로 규율해야 할 것이다. 범죄현장에서 확인된 CCTV 얼굴이미지 식별이나 피체포자의 신원확인 목적으로 보유 중인 얼굴인식 데이터베이스와 대조하는 경우, 그 얼굴정보 수집부터 얼굴인식 처리, 결과 보관 및 파기에 이르기까지 단계별로 규율할 수 있어야 한다. 이창민(2020)은 얼굴인식 기술에 대한 규제프레임으로서 (i) 얼굴인식 기술의 도입에 대한 기관간 견제와 감시 제도 마련 (ii) 개인정보영향평가 실시 의무화 (iii) 얼굴인식 기술의 성능과 한계에 대한 투명한 공개 의무화 (iv) 얼굴인식기술의 오류, 편향성에 대한 테스트 의무화 (v) 얼굴인식기술을 적용한 결과에 대한 인적검토 보장 등을 제안하였다[81]. 즉, 법집행기관이 민감정보인 얼굴인식정보를 처리하는 것은 국민에게 법적 또는 상당한 영향을 미치는 결정으로 이어질 수 있고 고위험 자동화된 처리인 만큼 독립적인 외부 감독체계를 갖추고 사전적인 영향평가를 비롯해 정기적인 점검을 수행할 수 있도록 해야 한다.

특히 얼굴인식기술의 기반이 되는 인공지능 기술의 투명성과 공정성에 대한 논란이 세계적으로 계속 일고 있다. 세계 여러 나라에서 공공기관이 국민을 상대로 한 의사결정의 기반으로 사용하는 인공지능 알고리즘이 특정 인종, 성별, 빈곤 지역을 차별하는 문제를 드러내어 논란이 되어 왔다[82]. 인공지능 기술은 그 학습 과정에서 데이터 및 알고리즘의 편향성 문제를 극복하지 못하는 한계를 가지고 있는 것이다. 미국 위스콘신주 대법원은 2016년 피고인의 재범 위험성을 평가할 때 참고하는 콤파스(COMPAS) 알고리즘의 평가지수가 법원 결정의 유일한 요소가 되었다면 위법이지만, 보조적인 수단으로 사용

81) 이창민(2020), 위의 글

82) 민주주의를 위협하는 안면인식 기술, 가디언 사설(2019. 6. 9), 번역: NewsPeppermint <https://newspeppermint.com/2019/06/11/the-guardian-view-on-facial-recognition-a-danger-to-democracy/>

되는 경우 적법절차 위반이 아니라고 판결하였다. 그러나 언론사 프로퍼블리카에서 2013년부터 2014년까지 콤파스 알고리즘에 의해 법원의 결정이 이루어진 피고인 1200명의 기록을 검증한 결과, 재범률이 높은 것으로 예측되었지만 실제로 2년간 범죄를 저지르지 않은 경우가 흑인의 경우 45%, 백인의 경우는 23.5%이었던 반면, 재범률이 낮은 것으로 예측되었지만 실제로 2년간 범죄를 저지른 경우가 백인이 48%로 흑인 28%보다 훨씬 높았던 것으로 드러나 논란을 빚었다[83]. 또 영국 시험감독청(Ofqual)은 2020년 코로나19로 대학수학능력시험에 해당하는 A레벨 시험을 취소하는 대신 인공지능 알고리즘을 통해 학생 성적을 부여하였으나 부유한 지역 학생이 높은 점수를 받은 반면 가난한 지역 학생은 상대적으로 차별을 받은 것으로 나타나 논란을 빚었다[84]. 공공기관은 아니지만 거대IT기업인 아마존은 인공지능을 이용한 채용시스템을 활용하였다가 여성을 차별하는 알고리즘이 발견되어 2015년도에 해당 시스템을 폐기한 바 있다[85].

따라서 경찰의 얼굴인식기술의 성능과 그 오류, 편향성 등 한계에 대한 테스트 및 관련 정보는 국민 앞에 투명하게 공개해야 한다. 이때 민간의 영업비밀등으로 국민 앞에 공개될수 없어 투명성을 보장하지 못하고 결과를 설명할 수 없어 그 적법성을 검증할수 없는 시스템은 도입될수 없다. 2017년 5월 미국 휴스턴 지방법원은 민간회사 인공지능 비밀 알고리즘에 기반해서 공립학교 교사의 해고를 결정한 사건에서 “공공기관이 매우 중요한 노동 관련 의사결정을 할 때 민간회사의 비밀 알고리즘에 기반한다면, 이는 최소한의 적법절차를 준수하기 어렵다. 따라서 적법절차와 영업비밀을 모두 지키기 위한 적절한 해결책은 비밀 알고리즘의 공공 도입을 중단하는 것”이라고 설시한 바 있다[86].

---

83) 프로퍼블리카 관련 보도 〈https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing〉

84) 가디언 관련 보도 〈https://www.theguardian.com/education/2020/aug/13/who-won-and-who-lost-when-a-levels-meet-the-algorithm〉; 한겨레21 관련 보도 〈http://h21.hani.co.kr/arti/culture/culture_general/49206.html〉

85) 국가생명윤리정책원 요약소개 참조 〈http://www.nibp.kr/xe/news2/123168〉

86) HOUSTON FED. OF TEACHERS v. HOUSTON INDEPENDENT

또 2020년 2월 네덜란드 헤이그 지방법원은 인공지능 알고리즘으로 부정수급 소지가 있는 사람들을 발견하는 사회복지 위험발견시스템(SyRI)이 프라이버시 침해 보호조치가 충분치 않고 그 작동 원리에 대한 "투명성이 중대하게 결여되어 있다"며 사용 중단을 명령한 바 있다[87].

얼굴인식정보 처리의 대상이 되는 사람은 그 판단의 이유에 대하여 설명을 요구할 수 있고 이의를 제기할 수 있으며, 인적인 검토를 보장받아야 한다. 어떤 경우에는 그 사용이 제한되어야 한다. 미국 워싱턴 주 얼굴인식 규제법{S.B. 6280 (Wash. 2020)}에서는 얼굴인식 기술을 활용하는 수사관 및 검사들은 재판 전 피고인 측에 해당 사실을 고지해야 하며 얼굴인식 결과를 유일한 증거로 하여 형사사건의 혐의를 구성할 수 없고, 개인에게 법적 효과 또는 그와 유사한 중대한 효과를 낳는 결정과 관련된 경우 의미있는 인적 검토를 보장해야 한다. 후자는 유럽연합 GDPR에서 자동화된 의사결정을 제한하는 규정과 유사하다.

한편, 집회참가자 일반의 채증자료에 대한 판독의 경우 그 대상이 매우 많아 사실상 다(多):다(多) 얼굴인식이 이루어지게 된다. 이 경우 사후라 하더라도 그 대상의 규모가 크고 국민의 집회 시위의 권리를 크게 위축시킬 우려가 있다는 점에서 침해성이 더욱 커진다. 만약 국가가 집회 후 참가자에 대하여 늘 얼굴인식을 할 수 있다면, 국민은 자신의 인적상황, 집회에 참석했다는 사실 및 참석한 집회에 관한 정보가 국가에 의해 늘 확보되고 관리되며 향후 불이익으로 이어질 수 있다는 가능성에 대해 두려움을 느끼게 될 것이다. 이러한 두려움은 집회참가를 통해 국가권력이 추구하는 정책 등에 대하여 이견을 제시하고자 하는 개인의 집회의 자유를 위축시킬 수 있다. 민주주의가 원활하게 작동하기 위해서는 투표 이외에도 국민들이 정치적 의사형성에 참여할 수

〈https://www.leagle.com/decision/infdco20170530802#〉.

87) 가디언 관련 보도 〈https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance- system-violates-human-rights-dutch-court-rules〉; 유엔 빈곤과 인권에 관한 특별보고관 보도자료 〈https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25152 &LangID=E〉; 공익소송단 〈https://pilpnjcm.nl/en/landslide-victory-in-syri-case-dutch-court-bans-risk-profiling/〉

있는 기회가 폭넓게 보장되어야 하는데, 위와 같은 위축효과는 개인의 공민으로서의 삶을 제약하게 될 것이다(헌재 2018. 8. 30. 결정 2014헌마843 재판관 이진성, 재판관 김이수, 재판관 강일원, 재판관 이선애, 재판관 유남석의 반대의견).

2020. 11. 9.자로 개정되어 2021. 1. 1.부터 시행되는 「집회등 채증활동규칙(경찰청예규 제571호)」은 경찰이 채증자료에서 집회 또는 시위 등의 참가자를 특정하기 위한 방식에 있어 채증자료 외 촬영자료를 일반적으로 활용할 수 있도록 하였다. 다만 기록이나 연구등 범죄수사 외의 목적으로 촬영한 자료나 교통정보 수집·분석 및 제공용으로 설치·운영 중인 영상정보처리기기에 의해 촬영된 자료의 사용을 금지할 뿐이다(동규칙 제13조). 이 경우 경찰이 보유한 얼굴이미지나 얼굴인식 데이터베이스가 집회 또는 시위 등의 참가자 특정을 위하여 사용될 가능성이 있다. 채증활동규칙은 경찰 경비부서가 집회 또는 시위 등 현장에서 사진, 영상녹화물 또는 녹음물 등 채증자료를 방대하게 수집한 후 채증판독프로그램을 통하여 관리하도록 하였으나 그 수집 요건에서 불법행위에 대한 증거자료를 확보할 필요성과 긴급성으로 제한하지 않았고 무엇보다 법률에 구체적인 근거를 두고 있지 않다는 점에서 기본권을 크게 제한하고 있다. 경찰은 방대한 집회 채증자료를 판독하여 수많은 참가자의 신원을 특정 후 소환해 왔는데 그 구체적인 방법은 정확히 알려져 있지 않다. 운전면허증 전산시스템 상의 사진을 대조 등 이용하는 사실이 알려져 목적외 이용 논란이 일기도 하였다. 다만 경찰은 '육안'으로 식별한다는 입장을 지금까지 고수해 왔는데, 인권단체들은 집회에서 생산되는 채증자료의 규모가 막대한 점을 들어 경찰이 불법적인 얼굴인식기술을 사용하는 것은 아닌지 의심해 왔다[88]. 만약 민감정보인 얼굴인식기술을 이용해 집회참가자 일반에 대한 방대한 양의 채증자료가 자동으로 판독된다면 과잉금지 원칙에 위배될 가능성이 높다. 따라서 명시적인 불법 행위자에 대하여 사후에 요건과 절차를 갖추어 판독할 필요가 있다.

88) 사진 한장으로 신원파악 - 경찰 '족집게 기술' 쓰나, 한겨레(2011. 7. 19).

(3) 실시간 얼굴인식을 통한 신원확인

얼굴인식기술을 이용한 실시간 신원확인으로는 우선 특정인의 신원을 실시간으로 확인하기 위하여 데이터베이스에서 1:다(多) 방식으로 대조하는 경우가 있다.

예를 들어 경찰관이 치안 활동 중에 마주친 사람의 신원 또는 수배 여부를 조회하는 경우를 들 수 있다. 이성기(2018: 188~189)는 경찰관이 운전면허증 또는 주민등록증상의 위변조 등의 여부를 확인하기 위해 데이터베이스에 단말기로 접속하여 검색하는 행위는 도로교통법 등에 의해 허용될 것이라고 보았다. 그러나 검문검색 중에 정보주체가 동의하거나 영장이 없는데 직접 사진촬영을 하는 경우 불법적이므로 허용되지 않을 것으로 보았다. 공공장소라고 하더라도 범죄혐의가 있고 긴급을 요하여 증거확보의 필요성이 있는 부득이한 경우에만 수사기관의 사진촬영을 허용하는 것이 대법원 판례의 기준이기 때문에 검문검색의 일환으로 사진촬영을 하는 것은 위법하다는 것이다. 다만, 특정인을 범죄혐의로 검거한 후 피체포자가 신원확인을 거부하는 경우 체포에 수반한 검증이 허용되므로 얼굴을 촬영하여 데이터베이스상에서 신원확인을 하는 것은 형사소송법상 허용된다고 보았다.

그러나 헌법상 기본권인 진술거부권을 행사하고 있는 피체포자에 대하여 얼굴인식을 통한 신원확인이 일반적으로 허용될 경우 헌법상 기본권의 본질적 측면을 제한할 우려가 있다. 특히 얼굴인식의 경우 대상자의 협조 없이 은밀히 이루어질 수 있기 때문에 이를 원칙적으로 금지할 필요가 있다. 종래에는 강제처분의 판단 기준을 물리적 강제력 또는 법적 의무 부과 여부에 두었는데, 오늘날에는 중요 권리나 이익에 대한 침해 여부를 중요한 판단 기준으로 하고 있다는 지적도 있다. 사진촬영의 경우 수사 대상자에게 어떠한 물리적 강제력이나 법적 의무가 부과되지 되지 않고 수사 대상자도 모르게 순간적인 방법으로 사진촬영이 이루어졌다 하더라도, 이로 인해 수사 대상자의 권리 또는 이익이 침해되었거나 형사절차상 중대한 결과가 초래되었다고 인정된다면 강제처분으로 보아야 한다는 것이다. 따라서 범죄수사방법으로 드론등을 이용

하여 사진 또는 동영상을 촬영하는 것은 강제수사로 볼 수 있다는 견해이다(최정일, 2020: 70)[89]. 촬영 뿐 아니라 강제적인 얼굴인식 역시 마찬가지 관점에서 그 침해성을 판단할 수 있을 것이라고 생각한다. 경찰은 피체포자가 신원확인을 거부하는 경우 신체검증영장을 법원으로부터 발부받아 강제적으로 지문을 채취한 후 지문정보 데이터베이스와 대조하여 신원을 확인하기도 한다[90]. 그러나 지문, 나아가 얼굴인식과 같이 민감한 생체인식을 통하여 강제적으로 신원을 확인하기 위하여 신체검증영장을 발부하는 경우에는 그 요건과 절차에 대하여 법률적으로 세밀하게 규정할 필요가 있다.

얼굴인식 처리를 이용하여 특정인을 실시간으로 지속적으로 추적하고 감시하는 것 역시 기본권 침해가 큰 만큼 법률에서 제한할 필요가 있다. 영국 ICO는 경찰의 실시간 얼굴인식에 대하여는 개인정보 보호 영향평가를 반드시 실시하고 대조용 감시 대상 목록(watchlist)의 구성과 정보의 보존 및 시스템의 사용에 있어 비례성을 엄격하게 적용하고 고려하는 법적 근거를 갖출 것을 권고했다. 미국 워싱턴 주 얼굴인식 규제법{S.B. 6280 (Wash. 2020)}는 계속적 감시(ongoing surveillance), 실시간 또는 준실시간 식별(identification) 또는 지속적 추적(persistent tracking)을 위한 얼굴인식 처리를 금지하고 있다. 다만 영장이 있는 경우, 긴급한 사태인 경우 또는 법원이 실종자 또는 사망자의 위치확인 또는 식별만을 목적으로 하는 서비스의 사용을 인가한 경우는 예외이다. 다만 '긴급한 사태'라는 매우 광범위한 사유를 포함시키고 있는 점 등이 비판을 받고 있다(이창민, 2020).

현행법상으로는 도주 중인 특정 범죄용의자를 검거하기 위하여 공공장소에 설치된 영상처리정보기기의 얼굴정보를 '실시간'으로 데이터베이스 상에 수록된 얼굴인식정보와 자동대조하는 것이 허용될 수 없다. 실시간 검색을 위해서는 모든 공공장소의 영상정보와 수사기관간의 데이터베이스를 실시간으로 연동하여 정보의 공유 및 처리가 가능해야 하는데 이는 이종 목적의 데이터베이

89) 최정일(2020). "빅 데이터 분석을 기반으로 하는 첨단과학기법의 현황과 한계 - 범죄예방과 수사의 측면에서", 법학연구, 20(1).

90) 18살 소녀 지문날인 거부하며 '자해', 한겨레(2006. 7. 12).

스를 사실상 통합하는 것으로서 별도의 법적 근거가 없는 한 허용되기 힘들고, 실시간 감시의 기본권 침해가 심각하기 때문이다. 중요 지명수배자의 검거와 같은 목적이 있다고 해도 그 범위를 구체적으로 특정함이 없이 모든 공공장소의 CCTV를 실시간 연동하여 자동으로 검색하는 것은 수사상 비례의 원칙에 반한다는 것이다.

다만 이성기(2018: 189)는 특정 범죄용의자를 특정하여 그 도주로 부위 등을 한정하여 인근 CCTV정보를 데이터베이스와 연동하여 검색하는 것은 영장을 발부받거나 영상정보처리기기 운영자의 동의를 받아 임의제출받는 경우 가능하다고 보았다. 박원규(2019: 254)는 제한적인 상황, 즉 생명, 중대한 상해 등 고차원적인 법익에 대한 위험이 존재하고, 더불어 경찰이 빠른 시간 내에 대상자의 신원이나 위치를 확인할 필요성, 즉 긴급성이 인정된다면 엄격한 요건과 절차 하에 허용해야 한다고 보았다. 물론 이때에도 비례의 원칙 관점에서 이러한 수단을 사용하는 것이 꼭 필요한 것인지에 대한 검토가 필요하다(박원규, 2019: 258). 일상적인 상황에서는 국가에 의해 감시당하지 않고 익명으로 다닐 수 있는 자유가 우월하며, 경찰의 얼굴인식기술 사용을 광범위하게 허용한다면 일반 국민을 잠재적 범죄자 혹은 법규 위반자로 취급하는 것이나 다름없기 때문이다. 따라서 경찰의 얼굴인식기술 사용을 허용한다 하더라도, 사용범위를 장소적·시간적으로 제한하고 긴급한 필요가 있는 경우에 한하여 허용할 필요가 있다.

따라서 실동아동등의 수색, 중대범죄자의 도주 등 긴급한 경우가 발생하여 그 대상자의 신원이나 위치를 확인해야 할 구체적인 필요성이 소명되었고 아동이나 치매노인의 실종 등 그 대상이 위험성에 처해 있을 가능성이 상당하거나 무기소지 등으로 추가범행의 위험성이 있는 등 제한적 요건을 충족하는 경우에 한하여, 특정한 범위로 제한하여 법원의 영장 발부 등의 절차를 거치는 방식으로 경찰의 실시간 얼굴인식정보의 처리를 허용할 것인지에 대한 입법적 고민이 필요하다. 공공장소 보행자 등 불특정다수의 신원을 실시간으로 확인하기 위하여 다(多):다(多) 방식으로 얼굴인식을 처리하는 것은 비례의 원칙을 중대하게 위반하기 때문에 어떠한 경우에도 금지되어야 한다.

V. 결론 및 제언

1. 법집행 목적 얼굴인식정보 보호의 측면

공공기관이 법집행 목적으로 민감정보를 처리하는 경우 이를 민감정보에서 제외하도록 한 시행령 단서 규정은 삭제해야 한다. 법집행기관이 명시적인 법적 근거 없이 인증, 식별은 물론 분류 목적으로 얼굴인식정보를 처리하는 것은 모두 금지되어야 한다. 특히 장애 등 건강 상태, 인종이나 민족 등 개인의 민감한 속성을 분류하기 위하여 얼굴인식정보를 처리하는 것 또한 민감정보 처리로서 제한되어야 한다.

2. 경찰의 직무와 개인정보 처리 규범의 측면

범죄수사를 비롯하여 법집행기관들의 개인정보 처리 및 민감정보의 처리에 많은 예외를 두고 있는 우리 개인정보 보호 관련 법령의 경우 시급한 개선이 필요하다. 유럽연합 〈경찰 지침〉 및 유럽평의회 〈경찰 분야에서의 개인정보 사용에 관한 실질적 지침〉 등 국제규범에 부합하는 방향으로 경찰 등 법집행기관에 대해서도 원칙적으로 개인정보 보호 원칙 및 독립적인 감독을 적용하도록 입법적 조치가 이루어져야 하며 이 기관이 경찰의 얼굴인식 기술 활용에 대해서도 사전적이고 사후적으로 감독해야 한다.

3. 얼굴인식 데이터베이스의 구축 및 운용의 측면

경찰이 얼굴인식정보의 데이터베이스를 운용하기 위해서는 그 기본권 제한 목적의 정당성, 수단의 적합성, 피해의 최소성, 법익의 균형성이 갖추어진 법률에 의하여야 위법, 위헌성을 개선할 수 있을 것이다. 다만 어떠한 법률이라도 전 국민을 대상으로 하는 얼굴인식정보 데이터베이스를 구축·운영한다면 과잉금지원칙 위반을 벗어나기 어려울 것이다.

재범의 가능성이 있는 범죄경력자를 대상으로 얼굴인식정보 데이터베이스를 운영하는 경우 그 구체적인 수집 및 이용의 목적, 대상 범죄 및 수집의 범

위, 수집 및 이용의 방법과 절차, 보관 및 파기 등을 법률에서 구체적으로 규정해야 할 것이다.

다만 현행 「디엔에이신원확인정보의 이용 및 보호에 관한 법률」에 대한 인권침해 논란에서 볼 수 있듯이, 재범 위험성이 있는 대상의 요건에 대한 규정 미비나 보관 및 삭제 기간이 미흡한 것은 중대한 기본권 침해이므로 구체적으로 규정해야 한다. 특히 디엔에이법의 경우 그 대상 범죄에 집단주거침입죄, 퇴거불응죄 등을 포함함으로 인해 철거민, 노동조합원, 노점상 등 생존권을 요구하며 농성이나 집회시위에 참여하였다가 유죄판결을 받은 경우 때로는 그 실형 선고 여부와 무관하게 디엔에이신원확인정보가 채취 보관되어 논란을 빚은바 있다. 집회 및 시위에 관한 법률 위반 및 일반도로교통방해죄를 얼굴인식정보 데이터베이스의 포함 대상에 포함할 경우 이를 이용하여 불특정 다수 집회참가자에 대한 실시간 감시가 상시적으로 가능해 지고 이는 국민의 집회 시위의 권리를 본질적으로 침해할 우려가 있기 때문에 그 대상에서 제외하는 것이 바람직하다.

또 얼굴인식정보를 다른 정보와 연계하여 프로파일링에 사용하고 자동화된 의사결정에 이를 때에는 그 제한 및 정보주체의 보호에 대하여 구체적으로 법률에 규정해야 한다.

4. 얼굴인식정보 처리의 측면

가. 사후 얼굴인식을 통한 신원확인

특정한 범죄 용의자를 사후에 식별하기 위한 목적으로 민감정보인 생체인식정보를 처리하는 경우 법률에서 구체적으로 제한할 필요가 있다.

이 법률은 경찰이 입수한 얼굴이미지를 얼굴인식기술을 이용하여 얼굴인식정보 데이터베이스와 대조하여 처리하는 유형과 단계별로 그 목적, 대상, 방법, 절차 및 기한을 구체적으로 규율해야 할 것이다. 범죄현장에서 확인된 CCTV 얼굴이미지 식별이나 피체포자의 신원확인 목적으로 보유 중인 얼굴인식 데이터베이스와 대조하는 경우, 그 얼굴정보 수집부터 얼굴인식 처리, 결과

보관 및 파기에 이르기까지 단계별로 규율할 수 있어야 한다.

이때 독립적인 외부 감독체계를 갖추고 사전적인 영향평가를 비롯해 정기적인 점검을 수행할 수 있도록 해야 한다. 또한 경찰의 얼굴인식기술의 성능과 그 오류, 편향성 등 한계에 대한 테스트 및 관련 정보는 국민 앞에 투명하게 공개해야 한다. 이때 민간의 영업비밀등으로 국민 앞에 공개될수 없어 투명성을 보장하지 못하고 결과를 설명할수 없어 그 적법성을 검증할수 없는 시스템은 도입될수 없다. 얼굴인식정보 처리의 대상이 되는 사람은 그 판단의 이유에 대하여 설명을 요구할 수 있고 이의를 제기할 수 있으며, 인적인 검토를 보장받아야 한다. 얼굴인식 결과를 유일한 증거로 하여 형사사건의 혐의를 구성할 수 없는 등 어떤 경우에는 그 사용이 제한되어야 한다.

만약 민감정보인 얼굴인식기술을 이용해 집회참가자 일반에 대한 방대한 양의 채증자료가 자동으로 판독된다면 과잉금지 원칙에 위배될 가능성이 높으므로 이는 원칙적으로 금지되어야 한다. 명시적인 불법 행위자에 대하여 사후에 요건과 절차를 갖추어 판독할 필요가 있다.

나. 실시간 얼굴인식을 통한 신원확인

경찰관이 치안 활동 중에 마주친 특정인의 신원 또는 수배 여부를 데이터베이스에서 1:다(多) 방식으로 조회하는 경우는 도로교통법 등에 의해 허용될 수 있다. 그러나 검문검색 중에 정보주체가 동의하거나 영장이 없는데 직접 사진촬영을 하는 것은 허용되지 않는다.

헌법상 기본권인 진술거부권을 행사하고 있는 피체포자에 대하여 얼굴인식을 통한 신원확인이 일반적으로 허용될 경우 헌법상 기본권의 본질적 측면을 제한할 우려가 있다. 특히 얼굴인식의 경우 대상자의 협조 없이 은밀히 이루어질 수 있기 때문에 이를 원칙적으로 금지할 필요가 있다. 얼굴인식과 같이 민감한 생체인식을 통하여 강제적으로 신원을 확인하기 위하여 신체검증영장을 발부하는 경우에는 그 요건과 절차에 대하여 법률적으로 제한할 필요가 있다.

실동아동등의 수색, 중대범죄자의 도주 등 긴급한 경우가 발생하여 그 대상자의 신원이나 위치를 확인해야 할 구체적인 필요성이 소명되었고 아동이나 치매노인의 실종 등 그 대상이 위험성에 처해 있을 가능성이 상당하거나 무기소지 등으로 추가범행의 위험성이 있는 등 제한적 요건을 충족하는 경우에 한하여, 특정한 범위로 제한하여 법원의 영장 발부 등의 절차를 거치는 방식으로 경찰의 실시간 얼굴인식정보의 처리를 허용할 것인지에 대한 입법적 고민이 필요하다.

공공장소 보행자 등 불특정다수의 신원을 실시간으로 확인하기 위하여 다(多):다(多) 방식으로 얼굴인식을 처리하는 것은 비례의 원칙을 중대하게 위반하기 때문에 어떠한 경우에도 금지되어야 한다.

5. 이상과 같이 국민을 보호하기 위한 법적 근거가 갖추어지기 전에는 법집행기관의 얼굴인식정보 처리는 중단되어야 한다. □