경북대학교 법학연구원『법학논고』
제85집 (2024.04) 121~142면.
Kyungpook Natl. Univ. Law Journal
Vol.85 (Apr 2024) pp.121~142.
http://doi.org/10.17248/knulaw..85.202404.121

인공지능을 이용한 범죄예방에 관한 헌법적 연구
- 안면인식기술(FRT)에 대한 규범적 통제를 중심으로 -

주 민 호* · 정 태 옥**

〈국문초록〉

본 논문은 범죄예방단계에서 안면인식기술의 사용에 대한 법적 타당성을 논증하였다. 이를 위하여 비교법적 관점에서 유럽인권법원의 GLUKHIN v. RUSSIA 결정에서 원용된 유럽수준의 안면인식기술의 이용에 대한 가이드라인을 확인하고, 범죄예방단계에서 안면인식기술의 사용 여부에 대한 기준을 제시하였다.

안면인식기술은 정보의 보호밀도가 높은 민감정보로서 원칙적 이용이 금지된다, 기술의 특성상 정보주체가 인식하지 못할 뿐만 아니라 정보주체에 대하여 지속적인 추적이 가능하므로, 기본권의 침해 가능성이 높다. 그러나 예외적으로 공익적 목적이 있는 경우에만 그 이용이 가능하므로, 범죄예방단계에서의 이용은 법집행기관이 범죄의 위험성이 고도로 높은 경우에 한하여 제한적으로 가능하므로, 이에 대한 구체적인 규범적 통제가 필요하다.

현행법상 범죄예방단계에서 안면인식기술의 이용은 전문 행정기관이라 할 수 있는 개인정보보호위원회의 통제에 따르게 되어 있으므로 이에 대한 절차와 요건에 대한 명확성이 요구된다.

주제어 : 범죄예방, 안면인식, GDPR, 개인정보보호, 유럽인권법원

• 투고일 : 2024.04.02. / 심사일 : 2024.04.23. / 게재확정일 : 2024.04.23.

Ⅰ. 서론

범죄예방을 위하여 안면인식기술을 탑재한 영상정보 처리기기의 이용하는 것은 인격권을 중심으로 하는 기본권 보장체계와 긴밀한 관련성을 가질 뿐만 아니라, 기본권에 대한 기존의 해석을 변경시킬 수도 있는 중요한 쟁점들을 포함하고 있다. 국가안전보장, 질서유지와 같은 정당한 목적성을 가진 치안 행정이라 하더라도, 만약 국가기관이 범죄예방 차원에서 구체적 위험의 발생과 밀

* 제1저자, 경북대학교 법학연구원 전임 연구원
** 교신저자, 경북대학교 데이터사이언스대학원 교수

접하지 않은 치안 행정의 일환으로, 안면인식기술을 탑재한 CCTV를 운영할 수 있다고 한다면, 결국 CCTV를 이용하여 수집한 정보를 바탕으로 불특정 다수인의 얼굴정보를 분석할 수 있으며, 또한 수집된 정보를 다른 정보 및 다른 기관과 연계될 가능성을 인정하게 되는 것이다. AI기술의 급격한 발전에 따라서 전통적 방식의 처리수준에 비하여 방대한 양의 정보처리가 가능해짐으로써, 우선적으로 기본권 차원에서 개인정보보호와 관련된 문제가 직접적으로 문제가 된다. 뿐만 아니라, 무엇보다 이와 관련한 개인 정보 감시 체계 시스템에 대한 위험은 일반인의 기본권 행사의 위축 효과를 초래하고, 이와 더불어 인간의 존엄성, 사생활의 비밀과 자유, 평등권, 표현의 자유, 집회·시위의 자유, 일반적 행동의 자유권, 적법절차의 원리 등 주요 기본권과 원리들이 망라적으로 영향을 받게 된다.

사건 현장에서의 이미지와 주민등록증 혹은 운전면허증의 사진을 비교하는 특정인의 신원을 확인하는 전통적 방식은 소관 공무원이 일일이 하나의 이미지와 다른 이미지를 대조하여 특정인을 인식하는 정보 처리 형태이지만, 데이터 처리의 엄청난 속도를 가진 인공지능은 다수의 이미지를 동시에 대조하는 정보처리를 가능하게 만들었다. 이에 더하여 효과적인 영상 정보 수집·이용이용이한 정보처리기기인 CCTV의 광범위한 설치 환경과 결합된 고도의 안면인식 시스템을 통하여 시민들의 모든 행위 태양을 감시의 대상으로 전락시키는 빅브라더 사회의 출현에 대한 위험을 예고하고 있으므로,[1] 이는 우리 헌법이 예정한 일반적 인격권 보호대상으로 인간의 독자적인 개인성[2]에 대한 중대한 침해 가능성을 포함하고 있다.

따라서 예방단계에서 안면인식기술의 활용에 대해서는 엄밀하게 위험성과 비례하여, 그 운영 시간, 구체적 이용 목적, 정보처리의 적법성·투명성·공정성 등의 정보처리의 일반원칙이 준수되어야 할 규범적 통제를 수반할 필요성

1) 캘리포니아 주, 법 AB-1215는 법집행기관이 카메라에 의해 수집된 데이터와 관련하여 생체인식 감시 시스템을 설치, 활성화를 금지 하는 것으로서 2019년 10월 법으로 제정되어 2020년 1월에 3년의 기간으로 발효되었다. 이 법이 제기하는 안면인식기술(Facial recognition) 이용의 한시적 금지의 주요 근거는, 안면인식기술로 인하여 시민의 자유(civil liberties)와 헌법상의 프라이버시권(constitutional right to privacy), 익명성(anonymity), 공공장소에서의 표현의 자유에 대한 냉각효과, 그리고 인종과 여성에 대한 인식의 부정확성, 과잉치안된 공동체(overpoliced communities)에 대한 기술 발달에 대한 인권의 반비례성이었다(Asvatha Babu, Saif Shahin, CHAPTER 13 'Not Ready for Prime Time': Biometrics and Biopolitics in the (Un) Making of California's Facial Recognition Ban, 2021, p. 229).

2) 박진완, 우리 헌법상의 일반적 인격권의 보장체계, 한국공법학회, 공법연구 제33집 제1호, 2004, 308면

이 제기되는 것이다.

본고는 이러한 규범 통제적 관점에서, Ⅱ장에서는 법해석론적 관점에서 안면인식기술이 적용된 생체인식정보의 우리나라 「개인정보보호법」에 따른 정보의 보호밀도와 동법에 따른 범죄예방단계에서 정보처리를 분석하고, 최근 유럽인권법원에서 안면인식기술을 적용한 CCTV 판례[3]에서 제시된 유럽수준의 규범을 Ⅲ장에서 소개를 통하여, 과도한 개인정보의 수집과 이용, AI기술의 발달에 따른 위험의 제고 현상에서 인격권의 기본권 체계에 대한 재이해와 더불어 위축되는 일반적 행동의 자유권의 기본권 심사 체계의 실질성에 대하여 Ⅳ장에서 검토하기로 한다.

Ⅱ. 안면인식기술을 활용한 생체인식정보에 대한 개인정보보호법상의 규율

1. 안면인식기술과 생체인식정보

안면인식 기술은 사람 얼굴의 특징(얼굴의 굴곡, 눈 코 입의 간격 및 각도 등)을 수많은 점(노드 포인트)으로 분석하여 개개인을 인식하는 기술이다. 각 개인의 특징은 이미 데이터베이스에 저장된 안면인식 정보와 비교하여 판단하는 패턴 인식 기술 방식이다.[4]

안면인식(Facial recognition)은 얼굴정보를 비교하는 인공지능의 한 형태로 '일대일 매칭', '일대다 매칭'의 방식으로 대조를 위한 얼굴정보는 정지 사진, 저장된 비디오 영상, 라이브 비디오 영상 혹은 현존하는 사람에게서 가져올 수 있다. '일대일 매칭'은 인간이 단순하게 수행할 수 있는 프로세스를 자동화하는 것이며, '일대다 매칭'은 단시간에 임의의 많은 수의 비교 이미지를 일치 여부를 인공지능의 의하여 자동 판단가능하게 하는 것을 의미한다.[5]

---

3) GLUKHIN v. RUSSIA 판례(2023.07.04.) ; 유럽인권협약의 체약국이었던 러시아 국민이 제기한 개인소원 판례로서, 이 판결에는 안면인식기술을 적용한 CCTV 에 대한 유럽의 규범수준으로 다양한 법률과 지침을 제시하고 있다.

4) 이진천, IT 이야기, 안면인식 기술에 따른 사회의 변화, 2020, 92면

5) Matthew B. Kugler, PUBLIC PERCEPTIONS CAN GUIDE REGULATION OF PUBLIC FACIAL RECOGNITION, 25 Colum. Sci. & Tech. L. Rev. 1, 2023, p. 7

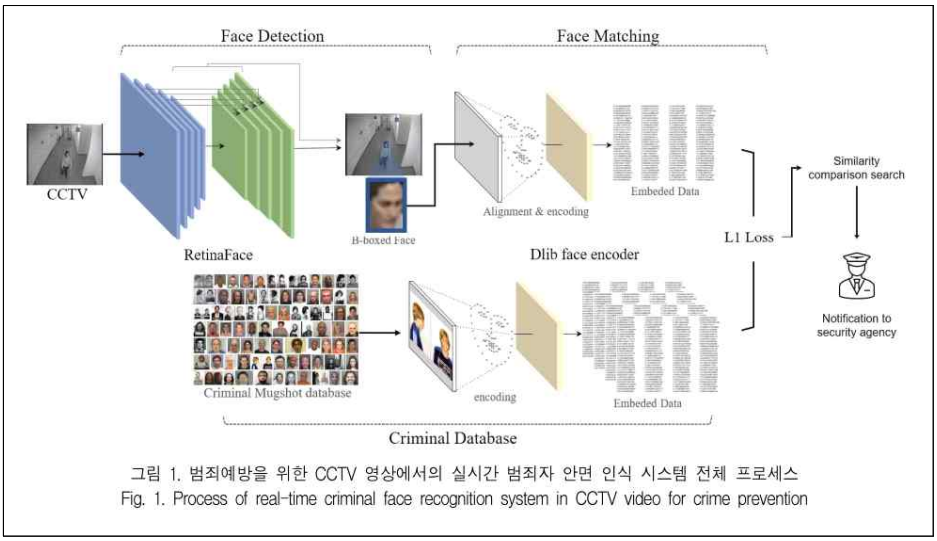

그림 1. 범죄예방을 위한 CCTV 영상에서의 실시간 범죄자 안면 인식 시스템 전체 프로세스
Fig. 1. Process of real-time criminal face recognition system in CCTV video for crime prevention

출처, 김현빈 외 4인, 범죄예방을 위한 CCTV 영상 기반의 실시간 안면인식 시스템, 한국정보기술학회논문지 제19권 제8호, 2021

유럽 일반 개인정보 보호법(General Data Protection Regulation, 이하 GDPR) 제4조 제14항에서 생체인식정보(biometric data)는 “안면 영상이나 지문정보와 같이 특정 기술처리로 얻어진 자연인의 신체적, 생리적, 행태적 특성과 관련된 정보로서, 자연인을 고유하게 식별할 수 있도록 해주거나 확인해주는 것”으로 정의되어있으며, 사진정보처리는 특정 개인 식별이나 인증 가능한 구체적인 기술 수단을 통해 처리되는 경우에 한해서만 생체인식정보에 포함된다.[6] 우리나라 「개인정보 보호법 시행령」 제18조(민감정보의 범위) 제3호에서 “개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적[7]으로 일정한 기술적 수단을 통해 생성된 정보”로 정의하고 있으므로 안면인식정보는 민감정보의 범위에 포함되는 것으로 해석된다.

또한 개인정보 자동화 처리에 관한 개인의 보호를 위한 협약 자문 위원회의 안면 인식 가이드라인(2021, ETS 108, 이하 협약(Convention) 108+)에서 안면 인식(Facial recognition)에 대하여 “안면 템플릿(face templates)[8]를 사용하여

6) GDPR 전문 51
7) 생체인식정보는 특정 개인을 인증·식별하기 위한 목적으로 처리되는 정보이며 일반적인 생체정보는 인증·식별하기 위한 목적 없이 개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 처리되는 정보로서 이 둘을 모두 포함하는 개념으로 생체정보라고 한다(개인정보보호위원회, 생체정보 보호 가이드라인, 2021, 4면).
8) 컴퓨터 소프트웨어가 사용하는, 표준화된 비실행 파일의 하나이다(위키백과, https://ko.wikipedia.org/

개인을 식별하거나 확인하기 위하여 개인의 얼굴이 포함된 디지털 이미지를 자동으로 처리하는 것"으로 정의하고, 모든 이미지 처리가 민감 정보 처리를 포함하는 것은 아니므로 이미지 처리가 개인의 고유한 식별 또는 인증을 허용하는 특정 기술 수단을 통해 처리되는 경우가 생체 인식 정보(biometric data)의 정의에 포함되는 것으로 한다.[9)]

우리나라의 경우도 이와 다르지 않으며, 생체인식정보를 개인을 인증 또는 식별 목적으로 입력장치 등을 통해 수집·입력되는 '생체인식 원본정보'와 이로부터 특징점을 추출하는 등의 기술적 수단을 통해 생성되는 '생체인식 특징정보'로 구분하고, '생체인식 원본정보'는 일반적인 개인정보로, '생체인식 특징정보'는 민감정보로 보호밀도를 달리하고 있다.[10)] 생체인식정보는 정보주체의 고유한 정보이자 유일한 식별자이므로 각국은 이를 민감정보로 분류하고 일반 개인정보에 비하여 더 강한 보호를 하고 있다. 생체인식정보가 특히 민감정보로 분류되는 까닭은 다음과 같다.

첫째, 정보의 변경이 어렵다는 점이다. 유출이나 특별한 사정이 있는 경우, ID나 패스워드는 물론, 식별자인 이름, 주민등록번호도 변경이 가능하지만, 생체인식정보의 기본 골격에 해당하는 얼굴, 지문, 홍채 등은 간단히 바꿀 수는 없다.

둘째, 생체인식정보를 통해 부가적인 정보가 추출될 우려가 있다는 점이다. 예를 들어, 안면 이미지로부터 본래 수집목적과는 무관한 인종이나 건강상태 등 특이정보가 추출되어 이용될 위험도 있다.

셋째, 정보주체가 인식하지 못하는 사이에 이러한 정보가 수집될 수 있다는 점이다. 특히, 안면 이미지의 경우, 현재 공적 영역과 사적 영역의 구분 없이 무수히 설치된 CCTV 등을 통해 정보주체가 그 수집에 대한 인식이나 감각 없이 실시간 그리고 원격으로 손쉽게 수집될 수 있다. 최근에는 카메라의 기능 향상과 분석기능의 발달로 인하여 손가락으로 V자를 그려서 찍은 사진에서 손쉽게 지문정보를 취득할 수 있고, 이것이 범죄에 악용될 수도 있다는 주장이 제기되기도 한다.[11)]

---

wiki/%ED%85%9C%ED%94%8C%EB%A6%BF).

9) The Guidelines on Facial Recognition (2021) by the Consultative Committee of the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108)

10) 개인정보보호위원회, 생체정보 보호 가이드라인, 2021, 4면

11) 김송옥·권건보, 안면인식기술을 이용한 생체인식정보의 활용과 그 한계, 헌법학연구 제27권 제1호, 2021, 124면

2. 범죄예방차원에서 생체인식정보 이용의 개인정보보호법상의 근거

민감정보 처리에서 수반될 수 있는 기본권 침해에 대한 법적용에 대하여는 개인정보의 특성 상, 기본권과 자유와 관련해 “특히 민감한 개인정보는 기본권 및 자유 침해의 위험을 야기할 수 있기 때문에 구체적으로 보호받아야 하며, …법에 따라 구체적인 상황에서 처리가 허용되는 경우가 아닌 이상, 처리되어서는 안 되며, 이러한 처리에는 구체적인 요건과 함께 이 법(GDPR)의 일반원칙 및 기타 규정은 특히 합법적 처리를 위한 조건과 관련하여 적용”[12]되어야 할 필요가 있다. 특히 인공지능 기술의 발달로 안면인식기술을 통한 지능형 영상감시에서 그 의미가 더욱 중요해졌고 할 수 있다.[13]

생체인식정보는 민감정보에 포함되므로, 「개인정보 보호법」의 민감정보 처리 규정에 따라 규율된다. 법 제23조 제1항은 민감정보에 대하여 원칙적으로 정보처리가 금지되나 예외적 정보처리를 허용하고 있다. 동법 제1항 제1호는 “정보주체에게 제15조 제2항 각 호[14] 또는 제17조 제2항[15] 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우”, 그리고 제2호에서는 “법령에서 민감정보의 처리를 요구하거나 허용하는 경우”로 한정하고 있다.

「개인정보 보호법 시행령」 제18조(민감정보의 범위) 단서에는 “다만, 공공기관이 법 제18조 제2항 제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.”고 규정하고 있으므로, 생체인식정보가 「개인정보 보호법」 제18조(개인정보의 목적 외 이용ㆍ제공 제한) 제2항에서 정한 사유, 즉 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무[16]를

12) GDPR 전문 51

13) Wolff/Brink/v. Ungern-Sternberg(Hrsg.) BeckOK Datenschutzrecht, 46. Edition, 2023, Rn. 141

14) 법 제15조 제2항의 각 호는 정보주체의 동의에 의하여 적법하게 개인정보의 수집과 이용하는 경우, 정보주체에게 개인정보의 수집ㆍ이용 목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 통보하고, 어느 호의 사항의 변경의 경우에는 재차 통보 후 재동의를 받도록 규정하고 있다.

15) 법 제17조는 개인정보의 제3자 제공 시, 정보주체에게 개인정보를 제공받은 자, 개인정보를 제공받은 자의 개인정보 이용 목적, 제공하는 개인정보의 항목, 개인정보를 제공받은 자의 개인정보 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 통보하도록 규정하고 있다.

16) 가령, 범죄예방에 관련된 소관 업무에 대한 법률적 근거는 「국가경찰과 자치경찰의 조직

수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우(제5호), 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우(제6호), 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우(제7호), 법원의 재판업무 수행을 위하여 필요한 경우(제8호), 형 및 감호, 보호처분의 집행을 위하여 필요한 경우(제9호)에 속하는 경우에는 해당 정보는 시행령에 의해 민감정보의 범위에서 제외된다.

이러한 법해석에 기초하여 경찰이 범죄예방을 목적으로 고정형 혹은 이동형 영상정보를 이용하여 개인정보 수집·이용하는 경우는 최초의 적법성 요건에 따르게 된다. 이는 「개인정보 보호법」 제15조 제1항 제3호 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우에 해당하여, 수집과 이용에 있어서 정보주체의 동의를 요건으로 하지 않는다. 이후 수집된 영상 정보를 안면인식기술을 통하여 생체인식정보를 생성해내는 경우, 즉 동법 제18조의 목적 외 이용하게 되는 경우는 동조 제2항 제5호에 따라 보호위원회의 심의·의결을 거친 경우에는 민감정보에서 제외하는 것으로 해석된다.

결과적으로 범죄예방단계에서 안면인식기술을 활용한 생체인식정보의 생성과 이용은 개인정보보호위원회에서 가능 여부를 결정하게 된다. 이는 수사와 공판에서 소관 업무 기관이 비민감정보로서 이용하게 할 수 있는 것과는 달리 상대적으로 예방단계에서의 국가안전보장 및 사회질서라는 공익적 목적이 정보주체의 인격권의 보호라는 사적 이익에 비하여 우월하다고 볼 수 없다는 가치판단에 따르는 것으로 판단된다.

공공기관이 민감정보를 활용하여 공권력의 행사할 때에는 입법부에 의한 민주적 통제가 요청되지만, 이의 구체적 실현 방식은 엄격한 삼권분립에 기초하여 사법기관에 의한 통제 방안과 완화된 삼권분립에 의한 독립된 위원회에 의한 전문 행정기관에 의한 통제 방식이 있을 수 있다.[17] 그러나 어느 방식에

및 운영에 관한 법률(이하, 경찰법)」 제3조(경찰의 임무)에서 정하고 있다.
제3조(경찰의 임무) 경찰의 임무는 다음 각 호와 같다.
1. 국민의 생명·신체 및 재산의 보호
2. 범죄의 예방·진압 및 수사
3. 범죄피해자 보호
4. 경비·요인경호 및 대간첩·대테러 작전 수행
5. 공공안녕에 대한 위험의 예방과 대응을 위한 정보의 수집·작성 및 배포
6. 교통의 단속과 위해의 방지
7. 외국 정부기관 및 국제기구와의 국제협력
8. 그 밖에 공공의 안녕과 질서유지

17) 우리나라에 비하여 엄격한 삼권분립 원리에 가까운 미국의 경우, 독립 규제 위원회(independent regulatory agency)를 두어 제한된 범위에서 적용하기 위하여 신속하고 유연한 행정을 위

따르더라도, 정보주체에 대한 보호밀도가 높은 안면이식기술의 활용 여부를 소관 기관의 재량에 맡길 수 없다는 것은 명백하며, 이와 더불어 개인정보보호위원회가 법 제2항 제5호의 심의·의결의 경우에도 일정한 요건에 따라 기속되어야 하는 것이 타당하다고 할 수 있다.[18]

반면, 「통신비밀보호법」 상의 통신제한조치를 동일한 수준에서 비교할 수는 없지만, 국가안전보장, 질서 유지 차원에서 공권력의 행사라는 측면에서 비례적 관계에서 살펴보는 것은 의미있는 것으로 생각된다. 안면인식기술이 정보주체의 신원을 식별하는 용도임에 비하여, 직접적인 사생활 침해가 될 수 있는 통신 제한 조치(감청)은 「통신비밀보호법」에 따라 범죄수사(법 제5조)[19], 국가안보(법 제7조)는 법원에 의한 사법통제를 요건으로 하고 있으며, 법 제5조와 제7조의 요건을 갖추었으나, 사법적 통제 절차를 거칠 수 없는 긴급한 사유에 한하여 긴급통신제한 조치를 행할 수 있다. 즉 예방단계에서 통신제한조치를 할 수 없는 것으로 볼 수 있으므로, 안면인식기술의 활용 또한 범죄 예방단계에서는 제한적으로 행사될 수 있도록 해야 한다. 통신제한조치와 안면인식기술의 사용은 각 기본권의 보호영역을 달리하고, 보호밀도 역시 상이할 수 있지만, 그 제한은 비례적 관계에 따르는 것은 명확하다.

Ⅲ. 안면인식기술을 적용한 CCTV 판례 : GLUKHIN v. RUSSIA[20] 판례(2023.07.04.)

1. 사건 개요

하여 분리된 정부의 기능들을 하나의 체제 내에서 권한을 행사하도록 하고 있고, 이는 견제와 균형의 원리 속에서 효율적인 행정 기능의 실현이라는 목적에 기초한다(정하명, 미국 행정법상의 독립규제위원회의 법적 지위, 공법연구 제31집 제3호, 2003, 148면).

18) 안면인식기술이 정보주체의 신원을 식별하는 용도임에 비하여, 직접적인 사생활 침해가 될 수 있는 통신 제한 조치(감청)은 「통신비밀보호법」에 따라 범죄수사(법 제5조), 국가안보(법 제7조)는 법원에 의한 사법통제를 요건으로 하고 있으며, 법 제5조와 제7조의 요건을 갖추었으나, 그 절차를 거칠 수 없는 긴급한 사유에 한하여 긴급통신제한 조치를 행할 수 있다. 즉 예방단계에서 통신제한조치를 할 수 없는 것으로 볼 수 있으므로, 안면인식기술의 활용 또한 범죄 예방단계에서는 매우 제한적으로 행사될 수 있도록 해야 한다.

19) 동법 제6조에 규정된 범죄수사를 위한 통신제한조치의 허거절차에서 법원의 허가서에는 통신제한조치의 종류·그 목적·대상·범위·기간 및 집행장소와 방법을 특정하여 기재하도록 하고 있다(동조 제6항)

20) 러시아 연방는 우크라이나 침공으로 유럽평의회 각료위원회와 의회에서 대표권이 정지되었고, 2022년 9월 16일부터 유럽인권협약 가입국으로서의 지위를 상실하였다.

2017년 5월 모스크바 시장의 공식 웹사이트에는 3500대 이상의 CCTV 카메라가 설치되었고, 동년 9월에는 3000대 이상의 CCTV에 안면 인식 시스템이 탑재되었다. 또한 2018년 봄에는 모스크바 지하철에 안면인식 CCTV 카메라가 설치되었다. 2020년 9월 1일까지 모스크바에 설치된 모든 CCTV(당시에는 약 175,000개, 2022년에는 220,000개 이상)에 실시간 안면 기술이 탑재되었다.

2019년 8월 12일 정치 운동가 콘스탄틴 코토프(Konstantin Kotov)는 러시아 형법 제2121조에 의해 집회·시위를 조직하거나 개최하기 위한 절차에 대한 반복적 위반 혐의로 체포·기소되었다. 이에 Glukhin은 2019년 8월 23일, 콘스탄틴 코토프의 실물 크기의 모형을 들고 모스크바 지하철에서 공공질서나 안전에 대한 어떠한 위험을 초래하지 않는 평화적인 방법으로 단독 시위를 하였다. 2019년 8월 24일 모스크바 경찰은 지하철 역에 설치된 CCTV에 녹화된 영상을 입수하고 스크린 샷을 사건 파일에 저장하고, 26일에 사진과 영상의 남성을 식별하기 위해 수사활동을 실시하여 Glukhin의 주소를 확보한 후, 30일 지하철 역에서 그를 체포(체포 시 CCTV 안면인식시스템을 통하여 그의 신원을 확인)하였고, 기소 후 법원은 20,000 루블의 벌금을 선고하였고, 항소 법원도 집회·시위에 관한 절차 위반이라는 이유로 유죄 판결을 유지하였다.

Glukhin은 유럽인권협약 제34조[21]를 근거로 개인소원을 청구하였고, 유럽인권법원은 사생활 존중권과 표현의 자유가 침해되었다는 판시를 통하여 Glukhin의 주장을 인용하고, 실시간 안면인식기술의 사용은 긴급한 사회적 필요(pressing social need)에 부합하지 않는다고 판시하였다.

2. 유럽인권법원에서 언급한 관련 국제 자료

(1) UN 인권 최고 위원회(United Nations High Commissioner for Human Rights)권고

UN 인권 최고 위원회(United Nations High Commissioner for Human Rights)의 “평화적 시위를 포함한 집회에서 인권의 증진과 보호에 대한 새로운 기술의 영향(Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests)”[22]

21) 유럽인권협약 제34조에 의하여 모든 자연인, 비국가적 기관 그리고 인적집단은 유럽인권협약 가입국가에 의한 유럽인권협약 그리고 그 부속의정서 속에 포함된 권리침해를 이유로 하여 유럽인권법원에 개인소원을 청구할 수 있다

22) UN Doc. A/HRC/44/24

이라는 보고서에는 아래와 같이 적시되어 있다.

■ 실질적인 안전조치가 없는 경우, 집회 중 치안당국이 안면인식 기술의 사용하는 것은 개인정보보호, 표현의 자유, 평화로운 집회에 대한 권리에 심각한 악영향을 미친다. 사람의 이미지는 타인과 구별하는 고유의 특성을 가지므로 동의 없이 안면 이미지를 녹화, 분석 및 보관하는 것은 개인정보의 침해이며, 안면인식 기술이 집회에서 사용되면 이러한 침해가 무차별적으로 발생한다.

■ 집회는 전통적으로 집회참가자가 식별되는 것을 방지하기 위하여 일정 수준의 보호를 허용하여 왔다. 안면인식기술의 배포는 실시간 식별은 물론 표적 감시 및 추적이 가능해져, 공공장소에서 시위를 하거나 자신의 견해를 표현하는 자유를 위축시킨다.

■ 시청각 녹음 및 안면 인식 기술의 사용은 적법성, 필요성, 비례성의 원칙을 충족하는 경우에만 사용해야 하며, 평화로운 시위에서는 그 사용을 삼가야 하며, 예외적으로 폭력, 총기 등의 사용이 임박하고 심각한 범죄 행위가 의심되는 때에 안면인식 기술 사용이 허가되며 이때에도 비례성의 입증이 필요하며, 기존 녹화 및 녹음물은 심각한 범죄 용의자의 집회 참여를 식별하는 용도로만 사용해야 한다.

■ 평화로운 집회에서 안면 인식 기술 사용은 권장되지 않지만, 이를 사용할 경우에는 명확한 법적 근거가 있어야 하며, 개인정보를 보호할 규제를 마련하고, 범죄 수사 및 폭력 범죄 기소에 필요한 특정 부분을 제외한 모든 데이터는 즉시 삭제되어야 한다. 관련 당사자는 범죄 수사 혹은 기소를 방해하는 경우를 제외하고 합법적인 목적과 법적 근거 없이 저장된 개인정보에 접근, 정정, 삭제할 권리를 보장해야 한다.

■ 또한, 평화로운 집회에서 안면 인식 기술의 사용은 효율적인 개인정보를 보호할 수 있는 규율을 담고 있는 규제 상항에 놓여야 한다. 독립적이고 공정한 데이터 보호 기관과 안면 인식 기술 조치를 승인할 사법 성격의 기관의 참여를 고려해야 한다. 또한 모든 상황에서 녹음, 녹화, 안면인식 기술 사용에 대해 투명해야 하며, 그 사용 시기를 항상 일반인에게 알려

야 한다.

이에 따라, UN 인권 최고 위원회(United Nations High Commissioner for Human Rights)는 평화적 집회의 군중을 식별하기 위하여 안면인식 기술을 사용을 금지하고, 구체적으로 범죄행위에 가담하거나 가담할 것이라는 징후가 없고 그러한 녹음 녹화가 법률에 의해 필요한 보호조치가 없는 한 안면인식 기술의 사용의 자제를 권고하였다.

(2) 유럽평의회(Council of Europe)

1) 유럽평의회 각료회의(Committee of Ministers): 치안 영역에서 개인정보 이용 규율 권고[23]

유럽평의회 각료회의(Committee of Ministers)는 개인정보 수집 원칙 2(Principle 2 – Collection of data)에서 치안 목적으로 개인정보 수집하는 것은 실질적 위험의 예방 또는 특정 범죄의 진압하는 데 필요한 경우에 한 것으로 제한되어야 하며, 이 규정의 예외는 특정 국가의 입법 주체에 의해야 하며, 특정 인종, 특정 종교적 신념, 성적 행동 또는 정치적 견해를 가지고 있거나 법으로 규정되지 않은 특수한 운동(movements)과 조직(organisations)에 속한다는 근거로 개인정보를 수집하는 것은 금지되어야 하며, 이러한 특정 범주 요소의 수집은 특별한 조사를 위해 절대적으로 필요한(absolutely necessary) 경우에만 수행될 수 있음을 권고하고 있다.

2) 개인정보 자동화 처리에 관한 개인의 보호를 위한 협약 자문 위원회의 안면 인식 가이드라인(2021, ETS 108, 이하 협약(Convention) 108+)[24]

안면인식(Facial recognition) “안면 템플릿(face templates)[25]를 사용하여 개인을 식별하거나 확인하기 위하여 개인의 얼굴이 포함된 디지털 이미지를 자동으로 처리하는 것”으로 정의하고, 모든 이미지 처리가 민감 정보 처리를 포함하는 것은 아니므로 이미지 처리가 개인의 고유한 식별 또는 인증을 허용하

23) 1987.9.17. 채택, Recommendation No. R (87) 15

24) The Guidelines on Facial Recognition (2021) by the Consultative Committee of the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108)

25) 컴퓨터 소프트웨어가 사용하는, 표준화된 비실행 파일의 하나이다(위키백과, https://ko.wikipedia.org/wiki/%ED%85%9C%ED%94%8C%EB%A6%BF).

는 특정 기술 수단을 통해 처리되는 경우가 생체 정보(biometric data)의 정의에 포함된다.

이러한 안면인식 기술이 기존의 감시 시스템에 통합하는 것은 개인의 인지 혹은 협력(awareness or co-operation)이 요구되는 것이 아니므로, 개인정보보호에 관한 권리뿐만 아니라 다른 기본권에도 심각한 위험을 초래한다. 기본권의 침해로부터 협약(Convention) 108+에서는 적법성, 법에 의한 특정 이용의 엄격한 제한, 안면인식기술에 디지털 이미지 통합, 공공 영역에서 안면인식 기술 이용에 관한 지침을 제공하고 있다.

ⅰ) 적법성(Lawfulness)

협약 108+ 제6조에 근거하여 생체 인식 데이터와 같은 특수 범주의 데이터 처리는 해당 처리가 적절한 법적 근거에 의해 보완적이고 적절한 안전조치가 국내법에 명시되어 있는 경우에만 승인된다. 이러한 안전조치는 관련 위험과 보호되어야 할 이익, 권리 및 자유의 조정이 요구된다. 이 지침에서도 GDPR 제9조의 특정 범주의 개인정보 처리와 마찬가지로, 원칙으로 특정 범주 개인정보 처리를 금지하면서도 당사자의 명시적 동의와 공익이 우선하는 때를 예외적 허용 사유로 제시하고 있으며, 안면인식 기술 사용의 필요성은 목적에 대한 비례성, 정보주체의 권리에 미치는 영향과 함께 평가됨과 동시에 법적 규율 방안[26]의 마련을 제시하고 있다.

ⅱ) 법에 의한 특정 이용의 엄격한 제한

안면인식 기술의 이용에 따른 침해의 수준과 관련 기본권들의 침해 수준은 사안에 따라 상이하며, 민주적 과정에 따른 각 국의 법률에 따라 엄격하게 제한되거나 금지하는 경우도 있다. 특히 '통제되지 않은 환경(uncontrolled environments)'[27]에서 안면인식 기술의 사용은 인간의 존엄성, 프라이버시 권 및 기타 기본권에 부정적인 위험의 영향을 고려하여 민주적 논의의 대상이 되어야 하며, 충분한 분석이 완료될 때까지 그 사용이 유예될 가능성을 제시한다.

---

26) 이에 포함될 내용으로, 구체적인 용도와 의도된 목적에 대한 자세한 설명, 사용된 알고리즘의 최소 신뢰성과 정확성, 사용된 사진의 보존 기간, 이러한 기준을 감사(auditing)할 수 있는 가능성, 정보처리 과정의 추적가능성, 안전조치로 되어 있다. 이들은 정보처리의 투명성과 깊은 관련을 가지는 것으로 평가할 수 있다.

27) '통제되지 않은 환경'이란 개념적 의미에는 쇼핑 센터, 병원, 학교와 같은 공공 혹은 준공공의 공간을 포함하여, 개인이 자유롭게 접근할 수 있는 장소가 포함되어 있다.

iii) 안면인식기술에 디지털 이미지 통합

입법자는 디지털 형식으로 제공되는 이미지를 처리하여 생체인식 템플릿을 추출 혹은 해당 이미지를 다른 목적으로 이용하기 위하여 최초의 이미지[28]를 구체적인 법적 근거 없이 생체인식 시스템에 통합하는 것을 금지할 것을 제시한다. 이는 디지털이미지에서 생체인식 템플릿을 추출하는 것은 민감정보의 처리를 포함하므로 이용 영역과 분야에 따른 다양성을 고려하여 법적 근거를 보장할 필요가 있다. 이러한 이유로 온라인에 공개된 디지털 이미지를 사용하거나 감사 카메라로 촬영한 디지털 이미지를 이용하는 것에 대하여 정보주체가 명백히 이용가능하게 하여도 합법적인 것으로 간주되지 않는다.

iv) 공공 영역에서 안면인식 기술 이용

협약 108+은 공공기관과 정보주체의 힘의 불균형으로 말미암아, 원칙적으로 동의를 안면인식 기술을 통하여 생체 정보처리에서 법적 근거가 될 수 없다고 보며, 이에 대하여는 법집행을 목적으로 한 입법자의 특별한 규칙 제정이 요구되며, 이 규칙에는 안면인식 기술의 사용이 엄격하게 필요하고(strictly necessary), 사용 목적에 비례적인(proportionate) 관계를 보장하고 필요한 안전조치(necessary safeguards)가 제공되는 것을 내용으로 한다.

통제된 환경 또는 통제되지 않은 환경 모두에서 개인 식별 목적의 안면인식 기술을 사용한 생체 정보처리는 법집행 목적으로 제한되며, 보안 영역의 관할 기관에서만 수행되어야 하며, 이 때에도 기본권에 대한 잠재적 침해 위험을 고려하여 확인 혹은 식별에 따른 다양한 필요성 및 비례성을 규정할 수 있다. 특히 안면인식 기술의 침해 가능성으로 인하여 통제되지 않은 환경에서 법집행기관은 장소와 시기를 포함한 엄격한 규제를 정당화할 입증 의무가 부여되도록 해야 한다.

3. 유럽 연합(EUROPEAN UNION) 차원에서의 규율

유럽 연합 차원의 안면인식 기술 사용에 관한 규율은 GDPR 제9조(특정범주의 개인정보 처리)[29]과 유럽데이터보호위원회(European Data Protection Board,

28) 가령, 소셜 미디어의 이미지를 생체인식 시스템에 법적 근거 없이 통합하는 것에 대한 금지이다.

29) GDPR 제9조 제1항에서는 특정 범주의 개인정보 처리를 금지하고 있으며, 동법 제2항은 적용 예외 사유로 GDPR 제정 전, 지침(Directive (EU) 2016/680)으로 존재하였던 (a)유

이하 EDPB)에 의한 법집행 분야에서 안면인식 기술의 이용에 관한 지침(Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 2023.4.26.)에서 상세하게 규율되어 있다.

유럽 기본권 헌장(Charter of Fundamental Rights of the European Union) 제52조 제1항[30]에 따라 관련 법은 행정기관이 개인정보의 수집 및 비밀 감시 조치에 부여받은 권한의 조건과 상황을 시민들에게 명확히 제시해야 하고, 이는 민주사회에서 법치주의에 따라 개인에게 부여된 최소한의 보호수준을 보장하기 위해 행정 기관(public authorities)의 재량권의 범위와 행사방식을 합리적으로 명확히 할 것을 요청하는 것이며, 이는 기본권 헌장 제8조(개인정보 보호)를 위한 적절한 안전조치이다.

특히 공개적으로 접근 가능한 공간에서 개인의 원격 생체식별은 개인의 사생활 침해 위험이 높으며, EDPB는 생체 인식을 기반으로 개인을 인종, 성별, 정치적 또는 성적 지향에 따라 분류하는 AI지원 안면 인식 시스템은 기본권 헌장과 양립하지 않은 것으로 간주하며, 또한 자연인의 감정을 추론하기 위해 안면인식 기술 또는 그와 유사한 기술을 사용하는 것은 바람직하지 않으며, 온라인으로 접근가능한 사진(소셜 네트워크를 통한 접근)을 통해 생체인식 처리에 활용하는 것은 유럽연합의 엄격한 필요성(the strict necessity)을 충족할 수 없다고 보았다.

Ⅳ. 안면인식기술 활용으로 인한 헌법적 가치의 재이해

1. 다른 기본권의 전제 조건으로서 일반적 인격권

안면인식기술은 CCTV 영상이나 사진에서 추출한 생체인식정보를 활용하는

럽연합 또는 회원국 법률에 의하여 승인된 경우 (b)정보주체 또는 다른 자연인의 중대한 이익을 보호하기 위한 경우 (c) 그러한 처리가 정보주체에 의해 명백히 공개된 데이터와 관련된 경우, 이 외에 현재의 GDPR에는 7가지를 추가하여 10가지의 예외 사유를 규정하고 있다.

30) Article 52(1) Any limitation on the exercise of recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

것으로 생체인식정보는 실시간 CCTV 영상 혹은 기존의 영상를 통해서도 수집가능하다. 특히 통제되지 않는 환경에서 실시간 원격으로 생체인식정보 기반의 신원확인기술을 활용하는 것은 개인의 프라이버시를 침해할 위험이 높고, 이러한 대량 감시를 수반하는 공권력의 행사는 민주주의 사회에서 예외적으로 허용되어야 하며,[31] 이는 민주적 통제로서 입법권에 의하여 규율되는 것이 타당하다고 할 수 있다.

이러한 보장은 개인이 외부로부터 어느 정도 단절된 상태로 자신의 정체성 형성을 위한 사적인 영역의 보호에 기여하는 일반적 인격권에 기초하며, 사회적 영역, 사적인 영역, 그리고 은밀한 영역에 대한 다양하고 특별한 보호의 필요성의 제기로부터 비례성 원칙의 적용과 각 영역의 엄격한 영역이론에 대한 극복의 기회가 보호영역의 해석과 재정립이라는 기본권 심사의 첫 단계로서 검토되어야 할 기회가 제공되어야 하기 때문이다.[32]

인격권에 대한 전통적 영역이론의 극복은 정보처리 및 통신기술의 발달로 은밀한 정보에 이르기까지 접근 가능하게 하고 자료를 저장·축적 기술의 발달은 개인의 인격성에 대한 모자이크를 조립가능하게 되어 이에 대한 통제로서 개인정보자기결정권을 인격권에 근거하여 보장하게 된 것이다.[33]

그러나 독일 기본법과 달리 헌법 제17조에 사생활의 비밀과 자유를 명문으로 규정하고 있는 우리 헌법은 개인정보자기결정권과 사생활의 비밀과 자유의 독자적 기본권으로서 독립된 보호영역에 관한 정립이 요청된다. 개인정보자기결정권은 사생활의 비밀과 자유를 보장하기 위하여 그 침해에 대한 위험의 보호를 핵심적 보호영역으로 보는 것이 타당하다.

2. 일반적 행동의 자유권의 실질화

고정형·이동형 영상 정보를 활용한 안면인식기술(FRT)의 이용가능성은 자

31) 김송옥, 경찰의 안면인식기술 사용과 관련한 영국판결의 헌법적 함의 - R(Bridges) v. Chief Constable of South Wales Police 사건을 중심으로, 세계헌법연구 제28권 제3호, 2022, 72면

32) 박진완, 우리 헌법상의 일반적 인격권의 보장체계, 한국공법학회, 공법연구 제33집 제1호, 2004, 311면

33) 박진완 교수는 개인정보자기결정권이라는 기본권의 도출과 그 이해로서, 한 개인에 대한 다양한 정보의 수집과 조합을 통하여 본질적으로 보호받아야 할 개인의 사적 영역에 대하여 사적 영역의 정보가 아니라 하더라도 정보의 조합에 의하여 얼마든지 개인의 사생활이 드러날 수 있는 위험에 대한 보호의 필요성을 제시하고 있다(박진완, 우리 헌법상의 일반적 인격권의 보장체계, 한국공법학회, 공법연구 제33집 제1호, 2004, 321면).

연인의 행위를 위축시키는 효과를 가져오고 이는 생활전반에 영향을 미친다. ICT기술의 발달의 편익의 역작용으로 인하여 불문의 헌법상 기본권으로 인정되는 일반적 행동의 자유권에 대한 이해를 재고할 필요성이 제기된다.

일반적 행동의 자유는 독일의 인격의 자유로운 발현권(독일 기본법 제2조 제1항)을 우리 헌법재판소가 수용한 것으로[34] 독자적인 개별적 기본권에 비하여 포괄적인 기본권으로서 명문화된 개별 기본권에 대하여 보충적 성격을 가진다. 이는 헌법 제10조 행복추구권에서 도출되는 기본권으로서 계약의 자유와 같은 사적 영역의 주요 행위를 소극적 보호 영역으로 하고 있으므로, 기본권 심사의 기준도 목적, 수단 간의 합목적성의 심사가 아닌 합리적 심사에 그치고 있다.

그러나 이러한 사회적으로 중요한 행위를 보호내용으로 한다면 실질적으로 자기결정에 따른 행위의 선택은 보장받기가 어렵고, 구체적 개별적 사례에서 성문화된 개별 기본권에 대한 보충적 지위는 여전히 인정되어야 하겠지만, 공공장소에서 마땅히 보장되어야 할 익명성은 사라지고 인공지능 기술을 수반한 개인정보의 이용이 빈번한 시대에서 전반적인 일반적 행동의 자유의 위축은 사생활의 자유, 개인정보자기결정권, 표현의 자유라는 구체적 법익에 포함되지 않은 때에는 독자적인 보호의 심사기준의 변화가 요청될 수 있을 것이다.

따라서 경찰이 범죄예방 차원에서 안면인식기술을 탑재한 CCTV를 운영하는 경우 이중의 비례성 심사가 필요할 수도 있다. 특정 대상의 감시자와 일반인들에 대한 일반적 행동의 자유권에 대한 각각의 심사가 주장되기도 한다.[35]

3. 인격권에 기초한 EU AI 법안 고위험 인공지능에 대한 규율

EU AI법안은 위험기반 규제방식은 인공지능기술의 위험을 ①절대적 위험(unacceptable risk), ② 고위험(high risk), ③제한적 위험(limited risk) ④ 최소위험(low or minimal risk)으로 구분하고 있고 각 위험의 단계마다 상이한 규율밀도를 구성하고 특히 절대적 위험의 인공지능 활용은 금지되어 있다. 절대적 위험이란 사람의 안전, 생존, 권리에 대한 명백한 위협으로서, 금지된 위험

34) 장영철, 일반적 행동자유권에 관한 고찰, 서울시립대학교 법학연구소, 서울법학 제28권 제1호, 2020, 3면

35) Roßnagel, A. Die „Überwachungs-Gesamtrechnung - Das BVerfG und die Vorratsdatenspeicherung. NJW. 2010, S. 1240 ; 박원규, 경찰의 안면이식기술 사용에 관한 법적 검토, 입법과 정책 제11권 제2호, 2019, 256

을 의미하며, 구체적으로는 유해한 조작적 잠재의식조종기술 사용, 장애인 등 특정 취약계층에 대한 착취, 공공기관의 사회적 평판기록(social scoring) 목적, 법집행기관의 공공장소 실시간 생체정보 판독 시스템(Real-time remote biometric identification systems) 관련 인공지능기술이다.

특히 공공기관의 사회적 평판기록(social scoring), 법집행기관의 공공장소 실시간 생체정보 판독 시스템(Real-time remote biometric identification systems) 간에는 생체인식정보를 매개로 하여 프로파일링(사회적 평판)과 같은 목적 실현의 개연성이 높아질 수밖에 없다. 프로파일링과 관련된 EU 인공지능법은 제5조 제1항에 명시된 공적인 범용사회적 평점 시스템(general purpose social scoring)으로 공공기관이 일정 기간에 걸쳐 사람의 신뢰도를 사회적 행동 또는 인지 · 예측된 개인적 · 인격적 특성에 기해 평가 · 분류하기 위한 시스템으로서, 그 사회적 평점이 데이터가 본래 생성 · 수집된 맥락과 무관한 사회적 맥락에서, 또는 일정한 사람이나 그 집단 전체에게 정당화하기 어렵거나 사회적 행동 또는 그 심각성에 상응하지 않는 해롭거나 불리한 처우로 이어질 수 있는 인공지능에 의한 프로파일링을 금지하는 것이라 할 수 있다.[36]

Ⅴ. 결론 및 제언

ICT기술의 발달로 인하여 개인정보의 활용이 증가하는 추세에서 개인정보 자기결정권, 사생활의 비밀과 자유에 대한 권리에 대한 침해 가능성 또한 점증하는 것은 분명하다. 정보주체의 권리를 구체화한「개인정보보호법」등은 이러한 위험성에 대하여 개별 기본권을 보장하는 기능을 하며, 정보주체는 개별 기본권의 지위에서 터잡아 주관적 권리를 행사할 수 있다.

그러나 범죄 예방이라는 공익적 목적 아래 정당성을 가진 공권력의 행사라 하더라도 일반 국민의 관점에서는 CCTV와 결합된 영상정보처리 기기의 이용은 자유로운 인격을 발현할 일반적 행동의 자유를 위축하는 효과를 가진다. 기본권 구제 시에 개별 기본권에 대하여 구체적 사안에서 보충적으로 나타나는 일반적 행동의 자유는 지금과 같은 정보화시대에는 구체적 사안에서가 아니라 일상 생활 전반에 그 위축 효과가 발생하므로 총합적인 수준에서 권리 침해가

36) 주민호, 자동화된 의사결정에 대한 기본권의 실효적 보장, 경북대학교 법학연구원, 법학논고 제82집, 2023, 68면

논의될 필요가 있고, 이는 기본권 심사 체계에서도 기존 합리성 심사를 넘어서야 할 당위를 가진다고 할 수 있다.

우리나라의 경우, 범죄예방을 위하여 CCTV에서 안면인식기술을 통한 생체식별정보 처리에서 「개인정보보호법」에 의한 적용 가능 여부는 법해석상 개인정보위원회가 심의·의결을 통하여 소관 기관의 행정 행위를 통제할 수 있도록 하고 있다.

이는 불특정 다수를 대상으로 개인 식별 목적으로 통제되지 않은 장소에서 실시간 안면인식기술의 사용은 공권력에 의한 법 집행이 목적일 경우 기본권 침해의 위험성이 높기 때문에 이에 대한 법집행기관에 대한 전문적 행정통제로서 개인정보위원회의 기능이 중요하다고 할 수 있다. 다만 이러한 경우에도 구체적 위험에 대한 개별 요건 명확히 함으로써 행정적 전문성을 가진 기관이라 하더라도 일정한 기속적 행정에 따르게 하는 것이 법치주의에 의한 적법절차의 실현에서 의의가 있다고 할 수 있다.

이는 인공지능의 편향성의 문제에서 야기되는 평등권 등과 같은 기본권 침해에 속하는 단속적 외부효과(discrete exteranality)는 사후적 통제를 통하여 문제를 해결할 수 있음에 비하여, 과학기술은 활용하여 범죄를 예방하는 것은 체계적 외부효과(systemic externality)에 속하므로 이는 사전적인 엄밀한 통제적 수단을 규범적 차원에서 갖추는 것이 요청되기 때문이다.

이러한 관점에서 범죄의 예방 단계에서 개인정보위원회가 다른 소관 업무기관의 안면인식 기술의 이용에 대하여는 기본권심사체계에 따른 과잉금지원칙에 입각한 기본권 정당화 심사와 같이, 기본권 침해 가능성의 위험과 이에 대한 공익과의 관계를 중심으로 일정한 해석상의 기준이 있어야 하며, 이러한 기준은 공익적 목적에 따른 공권력의 행사와 기본권 침해 가능성의 관계 속에서 예방단계에서 범죄예방을 위한 안면인식기술의 이용이 범죄발생의 가능성과 그 위험에 따라 이를 준별하는 것이다.

첫째, 절대적 위험에 해당하는 통제되지 않은 환경, 즉 공공장소에서 인공지능을 이용한 안면인식 기술 사용은 금지되어야 한다. 이는 EU AI법안에서 제시하는 바와 같이 인간의 안전, 생존, 권리에 대한 명배한 위협이 되므로 자유로운 인격의 발현에서 도출되는 일반적 행동의 자유, 표현의 자유, 집회 및 시위에 관한 자유 및 모든 기본권의 행사를 위축시킬 수 있다.

둘째, 안면인식기술 이용은 국가안전보장 및 질서유지를 위하여 장소적 보호의 목적이 명백한 경우에서만 가능하도록 해야 한다. 이러한 경우에는 고도의 위험성이 예정되는 장소로서 국가 기간 시설 특히 군사기지 및 군사시설,

외교 시설 및 공항과 같은 곳이 해당하며, 이는 법적, 사회적, 문화적인 가치에 대한 합의가 분명한 곳에 해당하다고 볼 수 있다.

셋째, 집회·시위 현장에서 폭력 행사와 같은 범죄발생의 위험성이 현존하는 것이 명백한 경우에 제한적으로 사용 가능하다. 표현의 자유의 행사로서 집회·시위의 자유는 헌법상 보장되는 권리로서 이에 참여하는 자에 대한 익명성의 보장은 당연히 수반되어야 한다. 특히 평화적인 집회에 대하여 사용하는 것은 민주적 가치에서 용인될 수 없다. 다만 이에 대한 예외적인 경우로서 폭력 및 총기 사용이 임박한 경우와 같이 심각한 범죄가 의심되는 때에는 적법성, 필요성, 비례성에 따라 안면인식기술의 이용이 가능하다고 할 수 있으나, 이러한 경우는 개인정보법 해석상으로 수사에 준하는 행위로 볼 수 있으나, 이에 의한 절차적 이행의 긴급성으로 인하여 사후적인 통제가 필요하다.

또한 안면인식기술이 탑재된 CCTV의 이용은 중대한 법익보호를 위하여 긴급한 필요가 있을 때, 그 이용 목적에 행정기관은 엄격하게 기속되고, 해당 법집행기관에 의해서만 수행에 제한되며, 기본권의 잠재적 침해위험까지 고려하여 식별에 의한 다양한 필요성 및 이에 따른 비례적 조치가 수반되도록 구제적으로 정할 필요가 있다. 이렇게 확보한 정보도 대상 인물과의 비교만을 위하여 사용하고 일치하지 않은 경우에는 정보의 즉각적인 삭제가 필요하고, 이에 대한 입증의무는 법집행기관이 가지며 이에 대한 통제의 주체는 보호위원회가 되어야 한다.

마지막으로 안면정보는 대체 가능성이 없는 개인정보이므로 국가기관이 수집한 정보가 해킹 등으로 유출된다면 그 피해가 광범위하여 회복하기 힘들다는 특징을 가진다. 따라서 영상보안기술을 적용하여 원데이터를 암호화하여 분리 보관하는 안전조치가 필요하다.

[참고문헌]

개인정보보호위원회, 생체정보 보호 가이드라인, 2021
권양섭, 범죄예방과 수사에 있어서 빅데이터 활용과 한계에 관한 연구, 한국법학회, 법학연구 제17권 제1호(통권 제65호), 2017
김송옥, 경찰의 안면인식기술 사용과 관련한 영국판결의 헌법적 함의 - R(Bridges) v. Chief Constable of South Wales Police 사건을 중심으로, 세계헌법연구 제28권 제3호, 2022
김송옥 · 권건보, 안면인식기술을 이용한 생체인식정보의 활용과 그 한계, 헌법학연구 제27권 제1호, 2021
김일환, 국가를 통한 생체정보의 이용에 대한 헌법적 통제방안에 관한 고찰, 토지공법연구 제24집, 2004
_____, 생체인식정보의 보호와 이용에 관한 법제정비방안에 관한 연구, 유럽헌법연구, 제30권, 2019
박진완, 우리 헌법상의 일반적 인격권의 보장체계, 한국공법학회, 공법연구 제33집 제1호, 2004
방석호, 안면인식기술(FRT)활용에 대한 법적 통제론, 홍익법학 제24권 제4호, 2023
양종모, 인공지능 알고리즘의 편향성, 불투명성이 법적 의사결정에 미치는 영향 및 규율 방안, 법조 제66권 제3호(통권 제723호), 2017
이권일, 생체인식정보의 보호와 활용에 대한 헌법적 고찰 - 개인정보보호법 시행령 개정령안에 대한 분석을 겸하여-, 부산대학교 법학연구 제61권 제2호 (통권 104호), 2020
이병규, AI의 예측능력과 재범예측알고리즘의 헌법 문제 - State v. Loomis 판결을 중심으로, 한국비교공법학회, 공법학연구 제21권 제2호, 2020
이상경, 생체인식정보의 활용과 개인정보보호에 관한 비교법적 고찰-미국의 법제를 중심으로, 서울법학 제26권 제3호, 2018
이성기, 생체인식정보와 감시: 수사기관의 얼굴 인식기술을 활용한 신원확인 행위의 법적 근거와 한계에 관한 연구, 법과 정책연구 제18집 제1호, 2018
이숙연, 인공지능 관련 규범 수립의 국내외 현황과 과제, 법조 제72권 제1호(통권 제757호), 2023
이원상, 범죄예방을 위한 첨단과학기술 활용에 따른 법제도적 쟁점 고찰, 형사정책연구 제27권 제2호(통권 제106호), 2016
장영철, 일반적 행동자유권에 관한 고찰, 서울시립대학교 법학연구소, 서울법학 제28권

제1호, 2020
정하명, 미국 행정법상의 독립규제위원회의 법적 지위, 공법연구 제31집 제3호, 2003
주민호, 자동화된 의사결정에 대한 기본권의 실효적 보장, 경북대학교 법학연구원, 법학논고 제82집, 2023
최정일, 빅 데이터 분석을 기반으로 하는 첨단과학기법의 현황과 한계 - 범죄예방과 수사의 측면에서, 법학연구 제20권 제1호, 2020

Asvatha Babu, Saif Shahin, CHAPTER 13 'Not Ready for Prime Time': Biometrics and Biopolitics in the (Un) Making of California's Facial Recognition Ban, 2021
Wolff/Brink/v. Ungern-Sternberg(Hrsg.) BeckOK Datenschutzrecht, 46. Edition, 2023
Matthew B. Kugler, PUBLIC PERCEPTIONS CAN GUIDE REGULATION OF PUBLIC FACIAL RECOGNITION, 25 Colum. Sci. & Tech. L. Rev. 1, 2023
Paal/Pauly, DS-GVO BDSG3. Auflage 2021BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg46. EditionStand, 2023
Roßnagel, A. Die „Überwachungs-Gesamtrechnung - Das BVerfG und die Vorratsdatenspeicherung. NJW. 2010.

[Abstract]

A Constitutional Study of Crime Prevention Using Artificial Intelligence

- Focusing on normative controls on facial recognition technology (FRT) -

Joo, Minho* · Choung, Teaok**

This paper discusses the legal justification for the use of facial recognition technology in crime prevention. In order to do so, it identified the European-level guidelines for the use of facial recognition technology from the European Court of Human Rights' decision(Glukhin v. Russia) from a comparative legal perspective and presented the criteria for the use of facial recognition technology in crime prevention.

The use of facial recognition technology is prohibited in principle as sensitive information with a high degree of protection, and the use of the technology allows for continuous tracking individuals, so it is likely to violate fundamental rights. However, it can be used only when there is an exceptionally public purpose, so its use in the crime prevention stage is limited to cases where law enforcement agencies have a high risk of crime. Normative controls are still necessary in these cases.

Under the current law, the use of facial recognition technology in crime prevention is subject to the control of the Personal Information Protection Commission, so clarity on the procedures and requirements is needed.

Keywords : Crime Prevention, Facial Recognition, GDPR, Protection of personal information, European Court of Human Rights

* First Author, Ph.D in Law / Researcher, Law Research Institute of Kyungpook National University

** Corresponding Author, Prof., Grdaduate School of Data Science, Kyungpook National University