안면인식기술의 법적 쟁점

Ⅰ. 서론

Ⅱ. 안면인식 기술의 이해
1. 안면인식 기술의 메커니즘 및 종류
2. 국내외 안면인식 기술 도입 현황
3. 국내 기업의 안면인식 기술 발전 및 해외 기술과의 유사성 검토

Ⅲ. 안면인식 기술 도입 시 공통적으로 문제되는 법적 이슈
1. 데이터 수집 단계에서의 법적 리스크
2. 안면인식 기술 배치 단계에서의 개인정보 보호법상 쟁점

Ⅳ. 주요 안면인식 기반 사업별 법적 쟁점 검토
1. AI를 이용한 채용 면접
2. 금융 서비스
3. 경찰의 범죄자 검거
4. 출입 및 보안

Ⅴ. 결론

이민재
서울대학교
법학전문대학원 11기

김유진
한국과학기술원(KAIST)
문화기술대학원

Ⅰ. 서론

안면인식기술(face recognition technology)은 2014년 페이스북의 DeepFace를 필두로 합성곱신경망(convolutional neural network; "CNN")의 도입을 통해 급격한 성능 향상을 이루어 냈다. 국내에서도 2018년을 기점으로 여러 업계에서 이 기술을 도입하기 시작했고, 최근 COVID-19 대유행으로 비대면 거래가 확대되면서 각광받고 있다. 본 연구는 먼저 안면인식기술의 종류와 작동 원리를 확인하고, 현업에서 사용되는 모델의 구체적인 구조를 분석하였다. 이를 바탕으로 안면인식기술을 현실에 적용할 경우의 공통적 법적 쟁점과 구체적인 사안별 쟁점을 검토하였다.

Ⅱ. 안면인식기술의 이해

1. 안면인식기술의 메커니즘 및 종류

안면인식기술은 얼굴 사진을 변형해 인물의 얼굴이 정면을 똑바로 응시하게 하는 alignment/frontalization 작업을 수행한 후 ① 얼굴의 특징점을 탐지하는 detection과 ② 탐지한 특징점을 바탕으로 인식을 수행하는 recognition이라는 두 단계의 핵심 작업을 거치게 된다. 수작업과 확률론을 사용하던 이전의 안면인식기술과는 달리 2014년 페이스북의 DeepFace를 시작으로 CNN이 일반화되었고, 이를 통해 특징점 탐지 및 얼굴 인식 작업의 성능이 큰 폭으로 향상되었다.[1] 현재 사업화된 기술에서는 detection과 recognition 두 단계 모두 신경망 구조를 사용하며 평균 97-99%의 높은 성능을 보이고 있다.

안면인식기술을 제품에 사용하기 위해서는 먼저 앞서 기술한 detection과 recognition 두 단계를 용이하게 수행할 수 있도록 충분히 큰 규모의 데이터셋을 이용하여 인공지능 모델을 학습시켜야 한다. 학습된 안면 인식 모델이 사용되는 사업의 분야는 매우 다양하나, 각 사업에서 사용하는 recognition의 목적에 따라 크게 ① 얼굴 인증(face verification)과 ② 얼굴 식별(face identification)로 구분할 수 있다.[2] 얼굴 인증은 1대 1 (one-to-one) 방식의 recognition으로, 한 사람의 모습이 여러 각도와 상황, 조도 등에 따라 다르게 찍혀 있는 사진들을 저장한 데이터셋을 바탕으로 어떠한 사람이 식별해야 하는 사람과 일치하는지에 대한 여부를 검토하는 시스템이며, 스마트폰과 태블릿PC 등의 잠금 해제 시스템이 대표적인 예이다. 얼굴 식별은 1대다(one-to-many), 또는 다대다(many-to-many) 방식의 recognition 방식으로, 어떠한 그룹의 여러 사람의 얼굴들이 저장된 데이터셋을 바탕으로 어떠한 사람이 해당 그룹의 일원으로 인식되는지 여부를 검토하는 시스템이며, 공항 출입자 식별 시스템, 결제 시스템, 범죄자 식별 시스템 등에 활용된다.

1) Y. Taigman, M. Yang, M. Ranzato and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification Proceedings of the IEEE conference on computer vision and pattern recognition, 2014, pp. 1701-1708.

2) I. Masi, Y. Wu, T. Hassner and P. Natarajan, "Deep Face Recognition: A Survey," 2018 31st SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI), 2018, pp. 471-478.

2. 국내외 안면인식기술 도입 현황

안면인식기술 시장의 규모는 2019년을 기준으로 43억 달러에 달하며, 2027년까지 연평균 14.8% 성장하여 130억 달러의 시장 규모를 형성할 것으로 예상된다.[3] 또한 상품화되지 않고 공적인 목적으로 사용되는 안면인식기술과 기업 내부적 목적으로 사용되는 기술까지 포함한다면 그 규모는 훨씬 더 방대할 것으로 추정할 수 있다. 공공부문의 경우, 예컨대 FBI는 이미 세계 최대의 안면인식 감시 시스템을 사용하고 있으며, 1억 1700만 명 이상의 미국인들의 이미지를 데이터베이스로 보유하고 있다.민간부문의 경우, 포드와 인텔이 추진중인 프로젝트 모빌(Project Mobil)은 대시보드에 위치한 카메라를 통해 스캔된 이미지를 안면인식 기술로 처리해 차량의 주요 운전자인지 등을 식별하는 방식으로 보안을 강화하고자 한다. 금융업에서도 보안과 편의성 확대를 위해 안면인식기술을 적극 도입하고 있다. HSBC, USAA등 이미 다양한 은행사들이 애플의 아이폰과 같은 핸드폰 기기에 존재하는 안면인식 시스템(예컨대 아이폰의 경우에는 페이스 ID)을 통해 모바일 뱅킹에 안전하게 로그인할 수 있게끔 하고 있다. 보다 독특한 시도들도 존재한다. 코카콜라나 맥도날드 등 식음료업에서는 안면인식기술을 통해 고객의 반응을 측정하고 이를 반영하며, MAC 등 화장품 회사는 오프라인 매장 내에 증강현실 화면을 통해 가상으로 화장을 해볼 수 있는 서비스를 마련해두기도 하였다.

현재 한국에서도 안면인식기술에 대한 기술 개발 및 응용이 활발하게 시도되고 있다. LG CNS에서는 '얼굴인식 출입 서비스'를 개발하여, 출입 게이트에서 안면인식 후 출입문 개폐여부를 결정하는 시스템을 개발해 자사에서부터 활용하고 있다. 이는 회사의 기존 내부 인사 데이터베이스를 활용하므로 별도의 데이터 수집 과정이 필요하지 않은 서비스이다.[4] 결제의 경우, 카카오는 카카오페이를 활용해 결제할 때 안면인식만으로 비밀번호 없이 본인 인증이 가능하도록 하였다.[5] 신한카드는 아예 오프라인 상에서 설치된 기기에서 안면인식을 통해 바로 결제를 가능케하는 '신한 Face pay' 서비스를 개시했다.[6]

3. 국내 기업의 안면인식기술 발전 및 해외 기술과의 유사성 검토

국내 기업들의 안면인식기술의 개발 현황은 논문과 특허를 통해 개략적으로 확인할 수 있다. 국내 기업의 논문 및 특허 등과 함께 카카오뱅크,[7] 삼성전자, 마이다스아이티[8]에서 발표한 특허를 검토한바, 대부분의 시스템은 안면인식기술의 구성을 face detection과 face recognition 두 단계로 나누어 전자를 영상 수집부, 후자를 영상 분석부로 제안하였으며, CNN 구조를 사용하였다. CNN은 현재 영상 인식 및 분석기술에서 가장 대표적으로 사용되고 있는 모델 형태로 사진 입력의 모든 부분에 작은 필터를 반복하여 적용해 이미지의 세부 특징을 추출하는 것을 목표로 하는 인공신경망 구조이다. Face detection 단계에서는 특정 얼굴을 대표할 수 있는 얼굴의 특징점(feature)을 찾는 과정이 필요하다. 이 과정

3) Fortune Business Insight, Market research report, 2020. 7, https://www.fortunebusinessinsights.com/industry-reports/facial-recognition-market-101061

4) LG CNS 블로그, "'마스크 써도 알아본다!' LG CNS, AI 얼굴인식 출입 게이트 도입", 2020.02.11., https://blog.lgcns.com/2189

5) 조선일보, 카카오페이, 얼굴인증 기능 도입…사용자 편의성 높여, 2019.09.25., http://it.chosun.com/site/data/html_dir/2019/09/25/2019092502235.html

6) 인공지능신문, "국내 최초, AI 얼굴인식결제 솔루션 '신한카드, 페이스페이' 상용화", 2020.04.09, https://www.aitimes.kr/news/articleView.html?idxno=15991

7) 최호열(카카오뱅크). 비식별화된 이미지를 이용한 신경망 학습 방법 및 이를 제공하는 서버. 1020200010271, 2020.06.28

8) 이형우; 이상우 (주식회사 마이다스아이티 (주)마이다스인). 온라인 인재분석을 통한 면접 자동화 시스템. 1020190041574, 2019.04.23

9) 오디노키크그랩안드레비치; 솔로마틴이반안드레비치; 파투코브알렉세이미카일로비치; 이희준; 에피모브유리세르게비치; 유주완; 이광현; 나티욱비탈리세르게비치; 에레메브블라디미르알렉세비치 (삼성전자주식회사). 생체 인식 기반의 사용자 인증 방법 및 장치. 1020190082227, 2020.05.07

10) 최호열; 이동열 (주식회사 카카오뱅크). 딥러닝 기반의 신분증 진위판단장치 및 신분증 진위판단방법. 1020200018242, 2020.06.16

에서 단순한 수작업으로 눈, 코, 입 등의 위치를 특정하는 고전적인 방법에 비해 CNN 모델 구조는 훨씬 더 많은 특징점을 발견해낼 수 있어 높은 성능을 보이므로 많은 안면인식시스템에 사용되고 있다. Face recognition 단계에서는 앞선 단계에서 추출한 특징점을 바탕으로 이미지들 간의 유사도를 계산한다. 해당 단계에서도 인공신경망 모델을 사용하는 기술이 많았고, 대부분 CNN을 사용하는detection단계보다는 모델 구조의 선택이 좀 더 자유로운 모습을 보였다.

다만, 논문 및 특허에서 기술의 세부적인 사안에 대해서는 언급하지 않거나 매우 빈약하게 서술하는 경우가 대부분이었다. 예를 들어 해당 기술에서 영상 수집부를 구현하기 위해 사용한 CNN 모델의 구조 등 사용된 모델의 간략한 형태와, 학습에 사용된 데이터의 형식에 대한 설명 등은 포함되어 있으나[9] 그 기술과 발표된 다른 기술들을 비교하기 위해 필요한 세부적인 구조에 대한 설명은 포함되어 있지 않았다. 모델의 구조를 도면으로 제시하는 등 세부 사안에 대하여 언급한 경우[10]에도 구현에 필요한 세부 함수나 파라미터까지 확정하지는 않았으나, 이는 불가피한 측면도 있을 것이다. 이러한 정보를 바탕으로 판단컨대, 국내에서도 각 기업이 그들이 처한 특정 상황에 적합한 고유의 기술을 개발하고 있으며, 외국의 모델들과 안면인식기술이 구성되는 단계나 사용하고 있는 모델 구조가 전체적인 면에서는 유사하다고 평가할 수 있다.

Ⅲ. 안면인식기술 도입 시 공통적으로 문제되는 법적 이슈

1. 데이터 수집 단계에서의 법적 리스크

얼굴 데이터를 수집할 때는 저작권자와 초상권자(주로 사진에 찍힌 당사자)로부터 사진의 수집과 상업적 이용에 대한 동의를 받는 것이 관건이다. 다만 현실적으로 권리자로부터 이러한 동의를 받아 내기가 쉽지 않고, 비용도 많이 들기 때문에 실무에서 안면인식 연구자/사업자들은 다양한 대안을 강구하고 있다. 구체적으로 ① 직접 수집 ② 온라인 플랫폼 상의 이미지 스크래핑, ③ 웹상에 공개되어 있는 데이터셋 사용, ④ 데이터셋 구입의 방법을 주로 사용한다. 본 항목에서는 이러한 얼굴 사진 수집 방법들의 각 법적 리스크와 현실적인 제약조건을 평가해 보았다(단, 직접 수집을 제외한 경우에는 개인정보 수집에 대한 쟁점은 배제한다).

1) 직접 수집

안면인식기능이 있는 인공지능을 학습시키기 위한 데이터를 수집하는 가장 기본적인 방법은 해당 사업자가 직접 이용자로부터 데이터를 수집하는 것이다. 안면인식기반 서비스의 이용자로부터 직접 얼굴 데이터를 수집하여 이 데이터를 안면인식 인공지능 모델의 학습에 사용하는 것은 '수집 목적의 범위 내에서 이용'에 해당한다. 따라서 정보주체의 동의를 받는다면 얼굴 데이터를 이용하

는 것이 가능하다(개인정보 보호법 제15조 제1항 제1호). 다만, 이용자의 수, 혹은 동의의 건수가 학습에 충분하지 않을 수 있다. 이 경우 기업들은 원래 다른 목적으로 수집한 데이터를 별도의 동의를 받고 안면인식기반 인공지능을 학습하기 위해 사용할 수밖에 없다(개인정보 보호법 제18조 제2항 제1호). 2020년 개정을 통해 신설된 개인정보 보호법 제15조 제3항에 따른 동의 없는 개인정보의 추가적인 이용이 가능한지에 대해서는, 아직 유관기관의 명확한 가이드라인 기타 결정례가 나오지 않아, 목적 외 이용이 형사처벌 대상인 현실에서 기업들이 이를 근거로 개인정보를 활용하기는 쉽지 않은 실정이다.

2) 온라인 플랫폼 상에 공개된 이미지 스크래핑(scraping)

사진이 공유되는 온라인 플랫폼에서 이미지를 스크래핑하는 방법은 인물 사진을 대량으로 확보할 수 있는 효과적인 방법이다. 실제로 연구 목적으로 인스타그램, 페이스북, 유튜브와 같은 글로벌 대형 플랫폼에서 사진과 영상을 긁어모아 데이터셋을 구성하는 경우가 상당히 많은 것으로 알려져 있다.[11] 이와 관련해서는 플랫폼의 운영주체, 사진에 대한 저작권자(촬영자 또는 저작권 양수인), 사진에 찍힌 사람의 권리의 침해 문제의 측면에서 각각 분석할 필요가 있다.

(1) 온라인 플랫폼 운영자의 문제제기 시 법적 리스크

온라인 플랫폼 이미지의 스크래핑의 경우 데이터셋의 제작 또는 소재의 갱신·검증·보충에 인적 또는 물적으로 상당한 투자가 이루어진 경우로 볼 수 있으면 저작권법상 데이터베이스권의 침해에 해당할 수 있고, 이와 더불어 저작권법상 부정경쟁행위, 특히 부정경쟁방지법 제2조 제1호 차목의 '타인의 상당한 투자나 노력으로 만들어진 성과 등을 공정한 상거래 관행이나 경쟁질서에 반하는 방법으로 자신의 영업을 위하여 무단으로 사용함으로써 타인의 경제적 이익을 침해하는 행위'에 해당할 여지도 있다. 대법원이 구인·구직 채용정보업체인 잡코리아가 경쟁사인 사람인을 상대로 낸 소송에서 경쟁 플랫폼의 데이터에 대한 스크래핑을 저작권법상 데이터베이스권 침해로 판단한 원심 판결(서울고등법원 2017. 4. 6. 선고 2016나2019365 판결)을 그대로 인용하였다(대법원 2017. 8. 24. 선고 2017다224395 판결). 아울러, 서울중앙지방법원은 엔하위키가 리그베다위키를 미러링 방식으로 포킹한 행위가 부정경쟁방지법 제2조 제1호 (차)목의 부정경쟁행위에 해당한다고 판단한 바 있다(서울중앙지방법원 2015. 5. 14. 자 2014카합1141 결정). 주로 이용자 생성 콘텐츠로 구성된 데이터셋을 스크래핑한 사안에 대한 이들 판례를 종합하면 스크래핑에 대한 법적 리스크를 배제할 수 없는 실정이다. 참고로 미국의 경우에는 경쟁 플랫폼 간 스크래핑 행위를「컴퓨터 사기 및 남용 방지법」(Computer Fraud and Abuse Act) 위반으로 본 판례가 있으나[12] 경쟁관계가 아닌 경우에는 최근 데이터 분석 업체 HiQ랩스가 구직·구인 SNS '링크드인'에 공개돼 있는 사용자 프로필 데이터를 스크랩해 이용한 사안에서 제9연방항소법원이「컴퓨터 사기 및 남용 방지법」위반에 해당하지 않는다고 보는 등[13] 상대적으로 덜 엄격하게 해석하고 있다.

11) NBC, "Facial recognition's 'dirty little secret': Millions of online photos scraped without consent", 2019.3.12, https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921

12) Craigslist Inc. v. 3Taps Inc., 942 F. Supp.2d 962 (N.D. Cal. 2013).

13) TNW, 2019.9.10, "US court says scraping a site without permission isn't illegal", https://thenextweb.com/security/2019/09/10/us-court-says-scraping-a-site-without-permission-isnt-illegal/

14) Octoparse, "5 Things You Need to Know Before Scraping Data From Facebook", 2019.1.30, https://www.octoparse.com/blog/5-things-you-need-to-know-before-scraping-data-from-facebook

15) Cnet, "Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection", 2020.2.5, https://www.cnet.com/news/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/

다만, 플랫폼 운영자의 문제 제기 시 구체적인 결론은 플랫폼 운영자의 이용약관, 사업 형태와 추정적 의사 등에 따라 판단될 수밖에 없어, 소셜미디어(이하 "SNS")와 검색엔진의 경우를 나누어 평가할 필요가 있다(특히 이용약관 위반은 법 위반과 별도의 계약위반 책임의 근거가 될 수 있다).

인물 사진이 집중적으로 업로드 되는 SNS 플랫폼은 얼굴 사진을 수집하기 위한 최적의 공간이나, 인스타그램, 페이스북, 틱톡 등 대부분의 주요 SNS 플랫폼은 약관에서 스크래핑을 금지하고 있으며, 자체적인 기술을 통해 의심스러운 행위가 감지된 계정이나 IP를 차단함으로써 스크래핑을 제재하고 있다.[14] 2020년 2월 페이스북과 구글이 미국의 대표적인 안면인식 사업자인 Clearview AI에 자사 플랫폼에서의 스크래핑을 멈추라는 중지요청(cease-and-desist letter)를 발송하기도 하였다. 특히 구글 산하 유튜브는 서비스 약관이 개인을 식별할 수 있는 데이터의 수집을 금지하고 있다고 명시적으로 밝혔으며, 페이스북은 Clearview AI의 행위가 서비스 약관 위반인지를 확인 중이며 만약 그렇다면 추가 조치를 취할 것이라고 발표했다.[15] 앞서 살펴본 국내 판결 등을 종합할 때 SNS 플랫폼의 스크래핑은 상당한 법적 위험을 내포한다고 할 수 있다.

이와는 달리 구글 등의 검색 엔진에서 특정 검색어를 입력한 후 나오는 사진들을 다운로드 하는 방식으로 스크래핑할 수도 있다. 구글은 현재까지 단 한 번도 스크래핑 행위에 대해 법적 조치를 취한 적이 없고, 의심되는 계정 혹은 IP를 차단하는 식으로만 대응하고 있다. 현실에서 구글 검색 결과에 대한 무수한 스크래핑 시도와 차단이 계속되고 있고, 구글이 아무런 법적 조치를 취하지 않는 이유에 대해 추측만 무성한 상태이다. 미국 2위 검색 엔진인 bing의 경우에는 검색 결과에 대한 API를 제공하고 있어서 사실상 bing의 시스템의 도움을 받아 스크래핑을 하는 것이 가능한 것으로 보이며, 스크래핑을 bing 측이 금지하고 있다는 별다른 약관 규정도 찾을 수 없었다. 결과적으로 검색 엔진을 통한 검색 결과의 스크래핑은 현실적인 법적 리스크가 상대적으로 작다고 볼 수 있다.

(2) 사진 업로더의 문제제기 시 법적 리스크

페이스북, 인스타그램, 틱톡 등 대부분의 대형 온라인 플랫폼 이용 약관에 의하면 이들 플랫폼은 사진, 영상 매체의 소유권을 주장하지 않으며, (적법한 권한을 가진) 업로더가 사진을 소유한다고 정하고 있다. 따라서 개인이 자신의 사진이나 영상을 플랫폼에 업로드한 경우 플랫폼은 저작권자가 아니다(플랫폼이 저작권자로 규정된 약관은「약관의 규제에 관한 법률」위반으로서 무효로 해석될 가능성이 높다). 다만 플랫폼들은 약관에 의해 비독점적이고, 양도 가능하며, 로열티가 없으며, 영구적인 전세계적인 라이선스를 부여받고, 앞서 살펴보았듯이 경우에 따라서 저작권법상 데이터베이스제작자로서 보호를 받을 뿐이다. 따라서 온라인 플랫폼에서 인물 사진을 스크래핑 한 경우에, 업로더 또는 제3자의 사진에 대한 저작권을 침해하는 행위인지가 쟁점이다.

원저작자의 동의 없이 저작물(사진)을 스크래핑해서 인공지능의 학습에 사용하는 것은 원칙적으로 저작권 침해에 해당하는 것으로 보인다.[16] 다만 저작권법 제35조의3의 공정이용의 법리가 적용된다면 저작권이 제한되어 동의 없이도 데이터의 수집 및 이용이 가능해진다. 공정이용 여부의 판단에는 ① 비영리성을 지니거나, 영리적인 이용이더라도 변형적 이용(transformative use)이나 비표현적 이용(non-expressive use)에 해당하는지 여부, ② 저작물의 종류 및 용도, ③ 이용분량 ④ 원저작물의 시장 또는 가치에 미치는 영향이라는 4가지 주요 기준이 적용된다.[17] 사진을 인공지능 학습에 사용하는 것은 전형적인 변형적 이용에 해당해 공정이용이라고 보는 견해가 유력하며,[18] 저작물의 종류 및 용도 부분에서도 별다른 문제는 없다. 안면인식 인공지능을 학습시켜서 개시하는 서비스가 원저작물의 시장 또는 가치에 끼치는 영향은 미미할 것이 분명하다. 다만 인공지능의 학습에는 통상 많은 분량의 저작물이 들어가기 때문에 3번째 요건으로 인해 공정이용에 해당하지 않을 수 있는 약간의 여지가 생긴다.

그러나 3번째 요건에도 불구하고, 공정이용의 법리가 적용되어 사진 스크래핑이 저작권 침해에는 해당하지 않는다고 보는 것이 합리적이라 생각된다. 2019년 개정된 일본 저작권법이 데이터 분석을 위한 저작권제한 규정을 도입해 컴퓨터에 의한 정보처리 및 그 결과의 제공에 수반되는 경미한 이용 등이 저작권의 침해에 해당되지 않는다는 점을 명백히 했으며, 문화체육관광부도 이를 참조하여 빅데이터 활용 등 정보의 대량 분석(데이터마이닝) 과정에서 저작물을 자유로이 이용할 수 있도록 하는 저작권 면책규정을 도입하려는 움직임을 보이고 있어, 이러한 입법 정비가 이루어질 경우 법적 불확실성은 해소될 것으로 생각된다.

16)
단, 특수한 경우로 사용자가 크리에이티브 커먼즈 라이선스(이하 CC)를 부여할 수 있는 옵션이 있는 플랫폼이 있는데, 야후의 사진 서비스인 플리커(Flickr)가 대표적이다. 이러한 플랫폼에 올라온 사진들을 스크래핑 할 경우 초상권이나 저작권은 문제가 되지 않을 것이다. 다만 실제로 영리 사업을 하려면 CC 중에서도 상업적인 용도를 허용하는 옵션이 선택된 극소수 사진만을 사용할 수 있다는 한계가 있다.

17)
법률신문, "인공지능과 데이터법", 2020.02.10, https://m.lawtimes.co.kr/Content/Info?serial=159295

18)
정상조, "인공지능시대의 저작권법 과제", 계간 저작권 31권 제2호(2018.6), 한국저작권위원회, 49면.

(3) 사진에 찍힌 사람의 문제제기 시 법적 리스크

얼굴 사진의 스크래핑은 초상권 침해 여부가 추가적으로 문제된다. 서울중앙지방법원은 일반인 A가 특정 상표의 옷을 입은 사진을 인스타그램에 올리자 그 상표의 옷을 판매하는 B가 A의 동의 없이 자신이 영업에 활용하는 네이버 밴드에 그 사진을 게시한 사안에서, A가 사진을 게시한 인스타그램의 이용약관이 ① 사용자의 콘텐츠를 임의로 사용하고 공유할 수 있는 것으로 정하고 있더라도 이를 영리의 목적으로 사용하는 것까지 허락하는 것으로 해석할 수 없고, ② B 등이 자신들의 영업을 홍보하기 위한 영리 목적으로 甲의 사진을 무단으로 사용한 것은 A가 예상하거나 허락한 범위를 넘는 것으로서 A의 자기정보에 대한 통제권 및 초상이 영리적으로 이용당하지 않을 권리를 정면으로 침해하는 위법한 행위이며, ③ B 등의 위법행위는 특별한 사정이 없는 한 A의 정신적 고통을 수반하므로, B는 초상권 침해로 A가 입은 정신적 고통에 대한 위자료를 지급할 의무가 있다고 보았다(서울중앙지방법원 2016. 7. 21. 선고 2015가단5324874 판결 (확정)).

안면인식 사업을 위한 사진 스크래핑에 이 요건에 대입해보면, 영리의 목적으로 사진을 사용하는 것이고, 초상권자가 예상하거나 허락한 범위를 넘는 위법한 행위로 해석될 수 있다. 물론 단순히 사진을 수집해서 인공지능 모델을 학습시키는데 쓰는 것은 정신적 고통을 수반하지 않는 특별한 사정에 해당한다고 볼 여지가 있으나(저작권법의 공정이용의 법리와 유사한 취지), 위 판결 등으로 볼 때 초상권자인 본인의 동의가 없으면 상당한 법적 리스크가 있을 것이다.

3) 공개된 데이터셋 사용

스타트업 기업들에게는 온라인상에 공개된 얼굴 사진 데이터셋을 사용하는 것이 유효한 선택지일 수 있다. 그러나 한국인 대상의 국내 데이터셋은 그 한정적인 규모로 인해 실효성이 떨어진다. 국제적 공개 데이터셋에는 아시아인 대상 데이터가 충분하지 않고 이러한 공개 데이터셋을 사용하는 것에는 법적 문제가 발생할 수 있다. 차례로 살펴보면 이하와 같다.

(1) AI Hub(정부 기관)가 공개한 '한국인 안면 이미지 AI데이터'

한국정보화진흥원이 운영하는 AI 통합 플랫폼인 AI허브는 AI 학습용 데이터 구축·확산 사업의 일환으로 1000명의 한국인에 대해 인당 32,400장의 사진을 수집해 총 32,400,000장의 사진을 제공하고 있다. 국내 기업 및 대학, 연구기관, 개인 등 누구나 AI HUB의 계정을 발급받아 포털에서 제공한 데이터를 활용 가능하다. AI HUB가 제공한 한국인 안면 이미지 데이터를 활용하여 제품·서비스 개발을 할 수 있으며, 결과물에 데이터의 출처만 명시해주면 된다.[19] 따라서 기업들은 얼마든지 이 데이터셋을 다운받아 안면인식 인공지능을 학습시키는데 사용할 수 있다. 대부분의 국제적 데이터셋이 인종적으로 편향되어 있으며, 아시아인 대상 데이터가 부족하다는 통계 자료[20]를 통해서도 확인할 수 있듯, 한국인 대상의 데이터셋은 국내 기업의 안면인식 알고리즘 학습을 위해 매우 소중한 자료이다.

그러나 이 데이터셋이 안면인식기술 개발에 최적화된 구성이라고 보기는 어렵다. 해당 데이터셋은 인당 32,400장의 사진을 수집하기 위해 20개의 각도, 30개의 조도, 6종의 얼굴을 가리는 물체의 사용, 3개의 표정, 3개의 해상도를 사용하였다. 그러나 이러한 데이터 수집 방식은 안면인식, 얼굴 합성, 얼굴 검출 등 대부분의 주제에 적합하지 않다. 다양한 각도의 사진은 얼굴의 3D reconstruction 작업에는 적합할 수 있으나 대부분 정면을 촬영하는 상황을 상정하는 recognition 작업에는 활용도가 낮다. 조도 및 해상도의 경우 데이터 전처리를 위해 사용하는 data augmentation으로도 충분히 구현 가능하므로[21] 실용성이 높다 단정할 수 없다. 마지막으로, 다양한 얼굴을 인식해야 하는 안면인식 알고리즘의 특성상 학습에 사용할 데이터셋으로는 최대한 많은 인원의 얼굴 데이터를 수집하는 것이 중요하다. 통상적으로 기업에서는 모델의 학습을 위해 10,000명 이상의 데이터를 사용하고 있으며, 국제적 데이터셋 또한 상당한 인원수를 대상으로 수집한 데이터로 이루어져 있다.[22] 따라서 1000명에 불과한 본 데이터셋은 심층학습 인공지능을 학습시키기에는 충분하다고 보기는 어렵다.

19)
https://www.ai-challenge.kr/sub03/file_down/id/391

20)
Grother, Patrick J., Mei L. Ngan, and Kayee K. Hanaoka. "Face recognition vendor test part 3: demographic effects." (2019).

21)
Wang, Xiang, Kai Wang, and Shiguo Lian. "A survey on face data augmentation." arXiv preprint arXiv:1904.11685 (2019).

22)
http://www.robots.ox.ac.uk/~vgg/data/vgg_face2/meta_infor.html

(2) 국제적으로 공유되는 데이터셋

국제적으로 기업, 연구 센터, 대학 등에서 수집하여 공개한 얼굴 데이터셋은 60개 이상 존재한다.[23] 전세계의 개발자 및 연구자들은 대규모 데이터를 쉽게 구할 수 있고, 공개된 데이터셋을 사용함으로써 개발한 모델의 연구 성과를 기존 연구 결과와 명확하게 비교하고 평가할 수 있다는 장점 때문에 대부분의 경우 이러한 데이터셋을 사용하는데, 대표적인 사례로는 Large-scale CelebFaces Attributes Dataset ("CelebA") 데이터셋,[24] VGGFace2 ("VGG") 데이터셋,[25] 그리고 Diversity in Faces ("DiF") 데이터셋[26] 등이 있다. CelebA 데이터셋은 홍콩과학기술대학교의 Multimedia Laboratory가 2015년에 공개한 데이터셋으로, 인터넷 스크래핑을 이용하여 10,000명 이상의 인원에 대해 수집한 총 200,000개 이상의 이미지로 이루어져 있다. 규모가 아주 큰 것은 아니지만 아시아인의 데이터가 상당 부분 포함되어 있어 국내 연구진과 기업에서 활발히 참고하고 있는 것으로 알려져 있다. VGG 데이터셋은 옥스포드 대학의 Visual Geometry Group에서 2018년에 발표한 데이터셋으로, 구글 이미지 검색을 이용하여 9000명 이상의 인원에 대해 수집한 총 3,300,000개 이상의 이미지로 이루어져있다. 공개된 얼굴 관련 데이터셋 중 큰 규모의 데이터셋에 속하며, 다양한 상황에서의 다양한 포즈, 감정, 조도의 데이터를 포함하고 있다. 또한 다른 데이터들보다 비교적 고른 인종, 나이, 성별 분포를 보인다. DiF 데이터셋은 IBM에서 2019년에 공개한 데이터셋으로, 야후(Yahoo)의 사진 서비스인 Flickr에서 수집된 YFCC-100M 데이터셋을 이용하여 이 중 활용도가 낮은 데이터를 제거하거나 가공하는 전처리 과정을 거쳐 일부를 선별한 데이터셋이다. 총 약 1,000,000개의 이미지로 이루어져 있으며 기존의 데이터셋보다 더 다양한 종류의 얼굴과 더 많은 얼굴 정보를 담고 있다.

이들은 얼굴 인식 인공지능 학습이라는 뚜렷한 목적을 가지고 만들어진 데이터셋으로, 얼굴 인식 알고리즘에 사용하기 위해 필요한 특성들을 갖추었다는 장점이 있다. 그러나 많은 양을 확보하기 위해 직접 이미지를 모으지 않고 인터넷에 게시된 사진들을 활용하였기에 데이터 수집 방법과 공개 조건에 대하여 법적 문제가 남게 된다. CelebA은 약관에서 이 데이터셋을 오직 비상업적인 연구 목적으로 사용해야 함을 명시하고 있고, 다운 받은 데이터셋 자체를 팔거나 제3자에게 넘기는 것을 금지하고 있다.[27] DiF의 경우에도 상업적인 사용은 금지되어 있다. Creative Commons Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)를 채택한 VGG는 이용약관상 상업적인 사용을 허용하고 있는 소수의 공개된 데이터셋 중 하나이나, 이 경우에도 초상권자, 저작권자들의 권익 침해 문제가 완전히 해소되는 것은 아니다.

4) 데이터셋 구입

마지막으로, 타 기업들로부터 데이터셋을 구입하는 방안을 고려해 볼 수 있다. 그러나 앞서 언급했던 대형 온라인 플랫폼들의 경우 상당수의 기업들이 (이

23) https://www.kairos.com/blog/60-facial-recognition-databases의 목록을 참조함

24) http://mmlab.ie.cuhk.edu.hk/projects/CelebA.html

25) http://www.robots.ox.ac.uk/~vgg/data/vgg_face2/index.html

26) Michele Merler, Nalini K. Ratha, Rogério Schmidt Feris, John R. Smith, "Diversity in Faces", CoRR abs/1901.10436 (2019), pp.1-2.

27) http://mmlab.ie.cuhk.edu.hk/projects/CelebA.html

용약관상 문구를 불문하고) 공식적으로 데이터 판매를 부정하고 있어 이러한 플랫폼으로부터 데이터를 구입하기는 쉽지 않을 것으로 전망된다. 현재 국내 대기업들은 실무상 주로 중국 혹은 국내의 데이터 용역업체로부터 필요한 데이터셋을 구매하고 있다. 다만 이러한 방법은 데이터 셋 구입에 수천만원 이상의 비용이 지출될 수 있을 정도로 금전적인 부담이 크므로, 대기업이 아니면 택하기 어렵다는 한계가 있다. 또한 구입하는 데이터의 크기, 성질 및 구입가액을 구체적으로 정하여 계약서를 작성하는 과정이 상당히 까다로울 수 있다.

5) 소결

결국 위 4가지 방안 중 손쉽게 다량의 데이터를 확보할 수 있으면서도 법적 위험이 적은 방법은 마땅치 않다. 직접 데이터를 수집하는 경우에는 이용자로부터 직접 동의를 받기 때문에 법적 위험이 적으나, 이는 이미 많은 이용자를 확보하고 있는 사업자만이 사용할 수 있는 방법이다. 데이터를 구입하는 방법은 높은 비용 부담으로 인해 몇몇 대기업을 제외하고는 사용하기 어려울 수 있다. 온라인 플랫폼을 스크래핑하거나 공개된 데이터셋을 사용할 경우에는 양질의 사진을 다량으로 획득할 수 있으나, 경우에 따라 플랫폼 운영자, 저작권자, 초상권자의 권리 침해에 대한 법적 문제제기가 있을 수 있다.

2. 안면인식기술 배치 단계에서의 개인정보 보호법상 쟁점

현재 다양한 안면인식기반 사업이 시행되고 있지만, 이들의 기본적인 구조는 크게 다르지 않다. 우선 식별하고자 하는 개인들의 얼굴 사진을 저장해 놓는다. 이후 설치된 카메라를 통해 실시간으로 앞에 있는 사람들의 사진/영상을 촬영하며 이 인물이 식별대상인과 일치하는지를 확인한다. 이 과정에서 주된 법적 쟁점은 ① 식별대상인의 얼굴 사진 정보 수집 ② 실시간으로 인물들을 식별하는 카메라의 설치 두 부분에서 발생한다.

1) 개인을 식별하기 위해 수집된 얼굴 사진

(1) 개인정보 해당 여부

식별대상 인물의 얼굴 사진은 개인정보 보호법 제2조 제1호에 따른 개인정보에 해당한다. 경찰관이 성매매업소 운영자에게 경찰청 생활질서계 단속 경찰관의 얼굴사진을 넘겨준 사안에서 해당 얼굴사진을 개인정보로 전제한 하급심 판결례(창원지방법원 2016. 9. 28. 선고 2016고단2630 판결)도 있다. 나아가 얼굴 사진이 2020년 개정된 개인정보 보호법 제23조, 시행령 제18조 제3호의 '개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보', 즉 '생체인식정보'에 해당하여 민감정보

에 해당하는지 여부가 문제되는데, 아직 명확한 가이드라인에 제시되고 있지 않아 법적 불확실성이 있으나, 특히 생체인증에 활용될 수 있을 정도의 해상도가 있을 경우 민감정보에 해당할 수도 있을 것이다.[28)]

28) 김현희, "생체정보의 활용 및 보호를 위한 법제 정비방안 연구", 한국법제연구원 연구보고서 (2016.6), 한국법제연구원, 29면

(2) 개인정보의 수집, 이용을 위한 동의

개인 식별용 얼굴 사진은 '개인정보'에 해당하므로, 식별 대상자들로부터 동의를 받고(제15조 제1항 제1호), 개인정보의 수집 · 이용 목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 알려야 한다(동조 2항). 민감정보에 해당하는 얼굴 사진의 경우 개인정보 보호법 제23조 제1항에 의해 민감정보의 처리에 대한 별도의 고지, 동의가 필요하다.

(3) 개인정보의 안전성 확보조치 기준에 의한 암호화의 문제

개인정보에 대한 구체적인 보호방법은 (정보통신서비스 제공자 이외의 경우)「개인정보의 안전성 확보조치 기준」(이하 "안전성 기준")이, (정보통신서비스 제공자의 경우)「개인정보의 기술적·관리적 보호조치 기준」('보호조치 기준')이 규율하고 있는데, 안전성 기준 제7조, 보호조치 기준 제6조 제2항 제7호, 제3항에 의하면 '바이오정보'에 해당하는 얼굴 사진은 그 송·수신, 저장을 위해 암호화해야 한다.

관련하여, 얼굴사진을 비밀번호 대신 인증정보로 활용할 경우, 비밀번호는 일방향 암호화(해시 암호화)하여 저장해야 한다고 규정한 안전성 기준 제7조 제2항, 보호조치 기준 제6조 제1항을 얼굴사진에도 유추적용해야 할지가 문제가 된다. 다만, 얼굴 사진을 일방향 암호화하여 보관하게 되면 안면인식기술을 사용하는 것은 기술적으로 매우 어렵다. 우선 일부 암호 기법의 경우 고화질의 얼굴사진 데이터를 암호화하면서 그 용량이 상당히 커져 이를 적절하게 처리할 수 있는 데이터베이스를 확보하는 것이 매우 부담스러워질 수 있다. 더 결정적인 문제는 식별용 얼굴 사진과 개인의 얼굴을 실시간으로 촬영한 사진이 서로 완전히 일치하지 않는다는 데에 있다. 대표적인 일방향 암호화의 방법인 해시 함수는 불연속적이고 불규칙적이기 때문에 조금이라도 입력값이 다르면 서로 완전히 다른 출력값이 도출된다. 따라서 암호화된 얼굴 사진으로 인물을 식별하는 것이 현재 기술 수준으로는 쉽지 않다(다만 미래에 동형암호,[29)] 취소 가능한 바이오 템플릿[30)] 기술이 더 발달된 후 이러한 기법들을 적용한다면 암호화 상태에서도 사진의 비교가 가능하게 될 여지는 있다). 이러한 현실적•기술적 한계를 고려하면 비밀번호 저장에 있어 일방향 암호화를 의무화한 규정을 얼굴 사진에 유추적용 하지 않는 것이 타당하다.

얼굴 사진의 일방향 암호화가 현실적으로 가능해지는 것을 넘어 암호화 상태에서 인공지능의 학습 데이터로 활용이 가능하다면, 일방향 암호화된 얼굴 사진이 개정 개인정보 보호법상의 가명정보 혹은 익명정보에 해당해 기업이 이를

29) 선형대수학적 기법을 통해 암호화 상태에서도 연산이 가능한 것이 특징이다. 다만 동형암호를 사용하고 딥러닝 기법을 이용한 이미지 동일성 비교는 현재 상태에서는 불가능하며, 향후 기술이 더 발전해도 실제로 정확한 인물 식별이 가능해질 것이라 단언할 수 없다. 또한 동형암호 사용시 연산속도가 현저히 저하되게 되므로 신속한 인물 인식이 요구되는 안면인식서비스에 적용되기 어렵다는 문제도 있다.

30) 원본 생체 이미지를 변환한 바이오 템플릿을 암호로 사용하는 일방향 암호화 기법이다. 원본 생체 이미지와 완전히 동일하지 않더라도 대략적인 구조가 동일한 이미지는 동일성을 인정받게 하는 것이 이 기법의 핵심이다. 그러나 이 기술은 기본적으로 딥러닝 안면인식기술과 경쟁하는 또다른 안면인식기법에 해당하는데, 딥러닝 기법만큼의 정확도와 신속성을 갖추도록 기술을 발전시키거나 딥러닝 기법과 이 기법을 복합적으로 사용하는 방안을 찾아야 한다는 과제가 남는다.

31) 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 또는 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다("표준 개인정보 보호지침」제2조 제11호)

활용할 수 있을지가 미래에 법적 쟁점이 될 수 있을 것이다. 다만 이러한 논의가 본격화되기까지는 수많은 기술적인 문제가 해결되어야 할 것이므로 본 연구에서는 이를 본격적으로 다루지 않았다.

2) 얼굴 인식을 위해 설치된 카메라 관련 법적 이슈

얼굴 인식을 위해 설치된 카메라가 개인정보 보호법 시행령 제3조 소정의 '영상정보처리기기'에 해당한다면 동법 제25조 제1항이 적용되어 해당 조항 각호의 예외에 해당해야만 '공개된 장소'[31)]에 영상정보처리기기를 설치 · 운영하는 것이 허용된다. 이때 영상정보처리기기운영자는 동법 시행령 24조에 의해 영상정보처리기기가 설치되었음을 정보주체가 알 수 있게 해야 한다. 다만 공개된 장소에 영상정보처리기기를 설치, 운영하여 처리되는 개인정보에 대해서는 수집·이용에 따른 동의 등 일부 개인정보 보호법상의 규제의 적용이 배제되는 장점도 있다(제58조 제2항).

Ⅳ. 주요 안면인식 기반 사업별 법적 쟁점 검토

본 항목에서는 대표적인 국내외 안면인식기술 도입 사례들에 대한 국내 법상 쟁점들을 살펴본다.

1. AI를 이용한 채용 면접

많은 다국적 기업들이 채용 과정에 AI를 도입하여 채용 업무의 효율성을 끌어올리고, 인간(채용담당자)의 주관성에 의한 문제를 억제하려는 시도를 하고 있다. 이러한 해외에서의 시도는 주로 1차 서류 평가를 자동화하는데 집중되는 경향을 보이고 있다. 반면, 국내에서는「채용절차의 공정화에 관한 법률」(이하 "채용절차법")의 도입으로 인해 서류절차의 변별력이 낮아지면서 면접과정의 중요성이 크게 증가하였고, 마이더스 아이티의 인공지능 채용면접 프로그램 inAIR가 많은 기업들에 채택되어 일명 'AI 역량검사'가 확산되고 있다. 이는 효율성 제고와 주관성 통제 뿐 아니라 학연 · 지연 · 혈연으로 대표되는 불공정한 요소의 개입을 근절할 수 있다는 기대를 받고 있다.

AI 역량검사의 핵심은 답변 과정에서 지원자의 얼굴에 나타난 표정, 안면색상과 음성을 분석해 호감도를 평가하는 것이다. 따라서 이 과정에서 지원자의 얼굴 영상을 수집하고 보관하는 작업이 필수적으로 수반된다. 관련하여 30인 이상 사업장에 적용되는 채용절차법 제4조의3 제1호는 구인자가 구직자에 대하여 그 직무 수행에 필요하지 않은 구직자 본인의 용모 · 키 · 체중 등의 신체적 조건을 수집하는 것을 금지하는데, AI역량검사가 얼굴 영상 정보를 수집하는 것이 이를 위반하였는지가 문제될 수 있다. 당해 조문이 2019. 4. 16에 신설되어 연혁이 짧고, 이에 관한 별다른 판례가 축적되지 않은 상태이나, 전반적으로 외모(눈 마주침, 눈 깜빡임, 표정, 외모적 호감도 포함)가 독립적인 변수로서 인공지능 알고

리즘의 평가기준에 평가되는지를 기준으로 당해 조문 위반 여부를 판단하여야 할 것이다. 시각 장애인이 불이익한 평가를 받을 수밖에 없는 구조라면「장애인차별금지 및 권리구제 등에 관한 법률」(이하 "장애인차별법") 위반도 문제될 수 있고, 공기업이나 준정부기관의 경우 공정성과 투명성의 원칙에 부합하는지에 대한 평가도 필요하다(「공기업·준정부기관 경영 및 혁신에 관한 지침」 제23조 제1호 참조).

2019년 11월, 인권 단체 EPIC (Electronic Privacy Information Center)은 HireVue의 인공지능 기반 채용지원자 사전평가서비스가 불공정하고 기만적인 거래 관행에 해당한다며 미국 연방거래위원회(Fair Trade Commission; "FTC")에 신고하였다.[32] EPIC은 HireVue가 FTC가 안면인식기술로 정의한[33] 기술을 사용함에도 불구하고 지원자들에게 이를 사용하지 않는다고 잘못된 설명을 하는 한편, 생체 데이터의 광범위한 수집과 비밀스러운 알고리즘을 통해 기존 채용 방식에 비해 나을 게 없는 평가를 통해 많은 지원자들의 고용의 기회를 박탈하였으므로 기만적인 거래관행에 해당한다고 주장한바, 이에 대한 FTC의 판단은 향후 채용 면접 AI에 대한 국내에서의 법적 평가에 있어 참조가 될 수 있을 것으로 생각된다.

2. 금융 서비스

1) 안면인식 기반 금융서비스의 도입과 금융규제 샌드박스

안면인식 기반 금융서비스의 선두주자는 중국 알리페이의 칭팅, 텐센트의 칭와이며, 국내에서는 2020년 4월 신한카드가 신한 페이스페이(Face Pay)를 출시하면서 본격적으로 서비스가 시작되었다. 뒤를 이어 한화투자증권, KB증권, DGB대구은행이 안면인식기술을 이용한 비대면 계좌개설서비스를 제공하기 시작하였다. 이러한 은행들의 서비스는 금융위원회의 '금융규제 샌드박스' 지정 서비스에 선정되어 한시적으로 가입 단계의 실명확인 규제가 면제되어 안면인식기술을 도입할 수 있었다. 금융혁신지원특별법(이하 "금융혁신법")에 따른 '혁신금융서비스 지정'(금융혁신법 제4조 내지 제12조)이 그 근거가 되었다.

페이스페이는 규제 샌드박스의 적용으로 인해 사용자들이 서비스에 처음 가입해 안면인식정보(얼굴사진)를 등록할 때 기존의 실명확인 방법이 아닌, 휴대폰 인증과 신용카드 인증(ARS)방식을 사용할 수 있게 하였다. 안면인식정보는 전자금융거래법 제2조(정의) 제10호 라목의 '이용자의 생체정보'에 해당하여 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 '접근매체'에 해당한다. 그리고 동법 제6조 제2항 및 전자금융감독규정 제34조 제3호를 종합하여 볼 때 접근매체를 발급하기 위해서는 본인확인이 필요하며, 그 중에서도 실명확인의 방법에 따라야 한다. 금융위원회의 유권해석에 따르면 실명확인을 위해서는 ① 신분증 사본 제출, ② 영상통화, ③ 접근매체 전달시 확인, ④ 기존계좌 활용, ⑤ 기타 이에 준하는 새로운 방식(생체인증 등) 중 2가지를 적용하면 된다.[34] 결국 규제 샌드박스 적용을 통해 이러한 번거로운 실명확인 절차를 휴대폰 인증과 신용카드 인증(ARS)방식으로 대신함으로써 페이스페이의 가입이 매우 간편해졌다.

안면인식기술을 이용한 비대면 계좌개설서비스의 경우,「금융실명거래 및 비밀보장에 관한 법률」(이하 "금융실명법") 준수 여부가 문제된다. 금융실명법 제3조 제1항은 금융거래는 실지명의로 하여야 함을 규정하고 있으며, 이는 비대면 계좌개설이라고 하여 예외가 될 수 없다. 그리고 금융위원회의 비대면 실명확인 가이드라인(유권해석에 해당하는「비대면 실명확인 관련 구체적 적용방안」)은 금융실명법상 비대면 실명확인 의무 이행을 위한 방법으로 ① 실명확인증표 사본 제출, ② 영상통화, ③ 접근매체 전달과정에서 확인, ④ 기존계좌 활용, ⑤ 기타 이에 준하는 방법(등록된 생체정보 등) 중 2가지 이상을 중첩하여 활용할 것을 규정하고 있다. 혁신금융서비스 지정으로 인해 해당 기업들은 영상통화 대신 실명확인증표의 사진과 얼굴촬영화면을 대조하는 안면인식기술을 비대면 금융거래시 실명확인 방법으로 활용할 수 있도록 특례를 부여 받았다.[35]

2) 현행 금융규제법상의 문제점

면제된 실명확인 규제 이외에도 여전히 다양한 금융법상 쟁점이 남아 있다.[36] 먼저 신용정보 보호를 위해「신용정보의 이용 및 보호에 관한 법률」(이하 "신용정보법")을 준수하여야 한다. 신용정보법상의 개인신용정보 수집, 위탁, 제공 등에 대한 규제는 상당 부분 개인정보 보호법의 내용과 비슷하므로 중복적으로 검토하지는 아니한다. 한편, 안면인식결제의 경우에는 오인 결제 발생 시 전자금융거래법(이하 "전금법")과 여신전문금융업법(이하 "여전법") 등의 규정이 문제되게 된다.

앞서 살펴보았듯이 안면인식기술은 일정 확률로 고객을 다른 고객과 오인하는 문제가 필연적으로 존재한다. 필터 카메라처럼 인물 오인이 별다른 피해를 가져오지 않는 경우도 많지만, 안면인식 결제 시스템을 통해 결제하려는 고객이 아닌 다른 고객의 카드(혹은 계좌)에서 돈이 빠져나간다면 법적 문제가 발생하게 될 것이다. 알리페이에 의하면 이 회사의 안면인식 결제 시스템의 인식성공률은 99.9%에 달한다고는 하나, 안면인식 결제가 광범위하게 사용되게 된다면 오인 결제된 0.1%의 거래 대금도 액수가 매우 커질 수 있다.

기기의 오인으로 인한 타인의 카드 결제로 안면인식 결제 시스템 제공자가 전금법과 여전법상의 책임을 이용자에 대해 부담할 수 있다. 전금법 제9조(금융회사 또는 전자금융업자의 책임) 제1항은 접근매체의 위조나 변조로 발생한 사고, 계약체결 또는 거래지시의 전자적 전송이나 처리 과정에서 발생한 사고의 경우 금융회사 또는 전자금융업자가 이용자의 손해를 배상해야 한다고 규정하고 있다.[37] 또한 여전법 제16조 (신용카드회원등에 대한 책임)가 적용될 경우 안면인식 시스템의 오인 결제가 당해 조문의 제1항 혹은 제5항에 해당하여 회원이 카드 분실 · 도난 통지를 한 후의 카드 사용 등에 따른 책임을 신용카드업자가 부담

32) EPIC's FTC Complaint In re HireVue, 2019. 11. 6, Ehttps://epic.org/privacy/ftc/hirevue/

33) Facing Facts - Best Practices for Common Uses of Facial Recognition Technologies, 2012. 10, FTC.

34) 금융위 유권해석 변경, 2015.12, http://www.fsc.go.kr/info/ntc_bref_view.jsp?bbsid=BBS0029&page=1&sch1=&sword=&r_url=&menu=7210100&no=30908

35) 다만 이에 대해 신분증 진위확인시스템을 통해 사진의 위·변조 확인이 가능한 주민등록증·운전면허증으로 실명확인증표를 제한하고 신분증 진위확인시스템을 통해 사진의 위·변조 여부가 없음이 확인된 경우에 한하여 안면인식기술을 적용하며, 혁신금융서비스를 이용하여 비대면 실명확인을 진행할 수 있는 고객을 '개인'으로 한정하는 등의 부가조건이 걸려 있다

36) 안면인식 결제 사업의 경우 신용카드 계좌에 연동되어 결제가 이루어지게 하거나, 직불카드, 직불전자지급수단(일명 체크카드), 혹은 선불전자지급수단(카카오페이 등)과 연동될 것이며, 이에 따라 별도의 개별 법령상 쟁점이 발생할 수 있다.

37) 다만 동조 제2항은 그 책임의 전부 또는 일부를 이용자가 부담하는 예외 상황에 대해 규정하고 있다.

할 여지도 있다. 게다가 여전법 제17조 제1항의 각호(도난, 위변조 등)에 해당한다면, 원칙적으로 가맹점에게 해당 거래에 따른 손실을 부담하게 할 수도 없다.

안면인식 기기의 오인 결제는 크게 ① 구매자의 고의나 과실 없이 오인 결제되는 경우, ② 타인의 계좌에서 돈이 빠져나간다는 것을 안 뒤에도 고의나 과실로 계속 안면인식을 사용한 경우 ③ 애초부터 고의로 사진 도용, 가면, 딥페이크 등 인위적인 수단을 이용하여 결제한 경우로 나눠 볼 수 있다. 위 3 분류 중 어디에 속하느냐에 따라 전술한 전금법 제9조와 여전법 제16조, 제17조 해당 여부가 달라져 안면인식 결제 사업자의 책임 여부가 달라질 수 있다.

안면인식을 통한 비대면 계좌개설의 경우, 인공지능의 오인으로 인해 실제 명의자가 계좌를 개설하지 못하게 되거나, 명의자가 아닌 다른 사람을 이용해 명의자 본인도 모르는 사이에 계좌를 개설하는 문제가 발생할 수 있다. 명의자가 계좌를 개설하지 못하는 경우는 명의자가 조금 번거롭더라도 다른 실명확인 방법을 사용하여 계좌를 개설할 수 있으므로 큰 문제가 되지 않을 것이다. 그러나 명의자와 얼굴이 비슷한 타인, 또는 딥페이크 기술 등을 이용해 차명계좌를 개설한 경우에는 이것이 차명거래에 사용되는 등 범죄에 악용될 가능성이 있다.

요컨대 금융업의 특성상 안면인식 시스템의 오인으로 인한 피해규모가 커질 수 있으며, 현행 금융규제법상 이로 인한 손해는 안면인식기술을 도입한 기업 측에서 부담할 가능성이 있어, 결국 기술적으로 정확도가 매우 높은 안면인식 모델을 구현하기 위해 기업 스스로 많은 노력을 기울여야 할 상황인 것으로 판단된다.

3. 경찰의 범죄자 검거

우선 범죄현장에서 발견된 범인의 사진을 국민 전체의 얼굴 사진 데이터베이스와 대조하여 범인의 신원을 확인하는 방식이 있다(이하 "범인 신원 확인용 안면인식")[38]. 두번째는 도시 각지에 깔린 CCTV가 실시간으로 행인들의 얼굴과 추적중인 범죄자의 사진을 대조하며 범인을 찾는 방식이 다(이하 "수배자 검거용 안면인식"). 전국적인 CCTV망과 전국민 데이터베이스를 모두 갖춘 중국의 톈왕(天網) 프로젝트가 대표적이다. 이러한 두 방법을 복합적으로 활용할 수도 있다. 결론적으로 범인 신원확인용이든 수배자 검거용이든 경찰이 안면인식기술을 사용하기 위한 일응의 법률상 근거는 존재하나, 위헌의 소지가 있어 곧바로 도입하는 것은 어려울 것으로 생각되는데, 그 상세는 이하와 같다.

1) 범인 신원 확인용 안면인식
— 경찰의 전 국민의 얼굴 사진 습득 및 사용의 가부

경찰이 범인 신원 확인용 안면인식을 도입하기 위해서는 전 국민의 얼굴 사진이 축적되어 있는 데이터베이스를 확보하여야 한다. 경찰은 이미 CCTV에 잡힌 범죄자의 얼굴사진으로 용의자를 특정하는 '3차원(3D) 안면인식시스템'을 전

38)
AP New, "Detroit police challenged over face recognition flaws, bias", 2020.6.24., https://apnews.com/article/business-us-news-ap-top-news-theft-arrests-9406d44edad083ee04e28646ead58ec7

39)
매일경제, "14만 범죄자 얼굴 3D로 저장… CCTV찍히면 즉각대조 가능", 2017.3.6, https://www.mk.co.kr/news/society/view/2017/03/154029/

국 경찰서에 보급하고 있으나,[39] 이 데이터베이스는 전과가 있어 경찰에게 얼굴 사진 기록이 남게 된 사람들만 대상으로 한다. 나아가 전국민의 얼굴 사진 데이터베이스를 확보한다면, 초범이나 아직 잡힌 적이 없는 범죄자의 경우에도 수사가 용이해질 것이다. 이때 경찰이 전 국민의 얼굴 사진을 확보할 수 있는 가장 합리적인 방안은 다른 공공기관에서 전국민 얼굴 데이터셋을 넘겨받는 것이다. 사용할 수 있는 데이터셋은 주민등록증 사진 정보나, 운전면허증 사진 정도가 있을 것이다. 이러한 데이터셋에 수록된 개인정보를 공공기관이 타 공공기관에 제공할 수 있는 직접적인 근거는 개인정보 보호법 제18조(개인정보의 목적 외 이용 · 제공 제한) 제2항이다. 해당 조항은 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보처리자가 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있는 경우를 각호에 열거하고 있다. 그 중 제7호는 '범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우'를 명시하고 있다.

이때 얼굴 사진 데이터베이스를 넘기는 것이 '제3자의 이익을 부당하게 침해할 우려가 있을 때'에 해당하여 허용되지 않을 수 있다는 문제제기가 있을 수 있으나, 이에 대한 명확한 판단기준을 제시한 하위 법규나 판례는 없다. 다만 헌법재판소는 경찰이 지문정보(개인정보에 해당)를 타 공공기관에서 제공받은 후 이를 보관 · 전산화 하여 범죄수사목적으로 이용하는 것이 개인정보자기결정권의 과도한 침해에 해당하지 않는다고 보았다(헌법재판소 2005. 5. 26. 99헌마513 결정). 이 결정은 경찰청장이 범죄수사목적을 위하여 다른 기관에서 지문정보를 제공받는 것을 허용하는 명문의 규정이 없더라도, 「공공기관의 개인정보 보호에 관한 법률」 제10조 제2항 제6호에 의해 허용되는 것으로 해석되어야 한다고 보았다. 「공공기관의 개인정보보호에 관한 법률」의 폐지로 인해 조문이 그대로 이관된 개인정보 보호법 제18조 제2항 제7호의 해석 기준 역시 같다고 볼 수 있을 것이다. 또한 위 헌법재판소 결정은 경찰법 제3조 및 경찰관직무집행법 제2조 역시 경찰이 지문정보를 타 공공기관에서 제공받아 범죄수사목적으로 사용할 수 있는 근거로 제시하였다. 이상의 논의를 종합해보면, 경찰이 수배자 검거용 안면인식 시스템 운영을 위해 권한 있는 공공기관에서 주민등록증이나 운전면허증 등의 얼굴 사진을 제공받아 데이터베이스를 구축하는 것은 일응 법률상 근거는 있다고 볼 수는 있다.

그러나 '전 국민의 얼굴 사진 정보'를 경찰이 '사전적으로 양도' 받는 것은 비록 법률상 근거가 있다고 하더라도 헌법상 허용되는 경찰작용이라고 장담할 수 없다. 우선 위 헌법재판소 결정이 개인정보 자기결정권을 경시한 잘못된 판단이라는 비판이 헌법학계에서 자주 제기되었다. 또한 위 결정은 범죄자 등 특정인만이 아닌 17세 이상 모든 국민의 열 손가락 지문정보를 수집하여 보관하도록 한 것이 과잉금지원칙에 위배되지 않는다고 보았는데, 얼굴 사진의 경우 지문과는 달리 전문적인 지식 없이도 누구나 개인을 식별할 수 있는 개인정보로서 인격권, 사생활의 비밀과 자유, 개인정보 자기결정권과 같은 개인의 권익 침해가 더 크다.

따라서 범죄수사목적으로 경찰이 전국민 얼굴 사진을 확보하는 것이 헌법에 위반되지 않는다고 단정하기는 어렵다.

2) 수배자 검거용 안면인식
— 공공장소에 안면인식기술 탑재 CCTV를 설치할 수 있는지 여부

수배자 검거용 안면인식을 도입하기 위해서는 전국 각지에 안면인식기술 기능을 탑재한 CCTV가 설치되어야 한다. 경찰은 이미 예방적 경찰작용의 일환으로서 각 지역에 수많은 방범용 CCTV를 직접 배치하여 사용하고 있으며, 그 법적 근거는 범죄의 예방 및 수사를 위하여 필요한 경우 공개된 장소에 영상정보처리기기를 설치 · 운영할 수 있게 한 개인정보 보호법 제25조 제1항 제2호이다. 안면인식기술이 탑재된 CCTV의 경우 기존 CCTV의 범죄 예방 목적에 더해 용의자의 소재를 탐지한다는 범죄 수사 목적이 크게 부각되는데, 이 역시 개인정보 보호법 제25조 제1항 제2호에 부합한다. 그러나 수배자 검거용 안면인식은 헌법의 과잉금지원칙에 위배된 개인의 사생활의 과도한 제한으로 해석될 여지가 있다. 수배자 검거용 안면인식 CCTV는 그 효율성을 높이기 위해 다수의 일반 시민들이 통행하는 지역에 주로 배치하여야 하므로, 예방적 경찰작용을 위해 주로 우범지역 위주로 배치되는 기존 CCTV보다 더 침익적일 수 있다. 우리나라가 외국에 비해 낮은 범죄율과 높은 검거율을 이미 기록하고 있어, 안면인식 CCTV가 과잉금지원칙 중 특히 침해의 최소성 및 법익의 균형성을 충족시킬 수 있는지 여부 또한 명확하지 않다.

4. 출입 및 보안

앞서 살펴보았듯이 이미 건물의 출입 통제 및 보안 유지 용도로 안면인식기술이 이미 활용되고 있다. 공공기관 혹은 기업 오피스 건물 내부의 자동출입 시스템의 경우, 카메라가 공공장소에 설치되는 것이 아니며, 사진 혹은 영상이 촬영되는 인물들 역시 식별대상자로 한정되기 때문에 특별한 법적 문제가 있다고 할 수는 없다.

주택의 경우, 기업들이 아파트 단지 내에 설치된 CCTV에 안면인식 기능을 탑재하여 거주민이거나 허가 받은 출입자 아닌 자가 탐지되면 경보를 울리는 보안 시스템의 구축 방안을 검토하고 있다. 이러한 사업에 대해서도 개인정보 보호법에 따라 ① 입주민들의 동의를 얻어 얼굴 사진 데이터베이스를 구축하고, ② 현행법과 실무상 허용되는 CCTV 운용 범위 내에서 안면인식 CCTV를 배치하여야 할 것이다. 다만, 아파트 등 공통주택의 경우 타 사안들에 비해 CCTV 배치 및 운용의 법적 근거가 명확한 편이다. 아파트 일정한 요건을 충족하여 의무관리대상 공동주택에 해당하는 경우에는 「주택건설기준등에 관한 규정」 제39조(영상정보처리기기의 설치)가 적용되는데, 이 조항에 의해 개인정보 보호법 시행령 제3조(영상정보처리기기의 범위) 소정의 폐쇄회로 텔레비전이나 네트워크 카메라를 의무적으로 설치하여야 한다.

V. 결론

이상, 헌법과 개인정보 보호법을 비롯한 관련 법령의 검토를 통해, 안면인식기술의 도입이 일반적으로 허용될 수 있으나, 이미지 스크래핑이나 웹상 공개된 데이터셋 사용의 경우 초상권과 저작권 침해 문제가 발생할 수 있고, 개별 사안별(AI채용면접, 안면인식 금융서비스, 범죄자 검거 목적 활용)로 쟁점이 존재한다는 점을 확인할 수 있었다. 이러한 법적 불확실성의 해소를 위해 안면인식기술들에 적용되는 법제를 명확하고 간소하게 정비하는 방안을 검토할 필요가 있다고 생각된다.