

스마트도시와 얼굴인식정보의 법적 개선에 관한 연구

A Study on Legal Improvement of Smart City and Information of Facial Recognition

김 명 엽*

Kim, Myung Yeop

목 차

- | | |
|---------------------------|--------------------------|
| I. 서론 | IV. 스마트도시와 얼굴인식정보 법제의 개선 |
| II. 스마트도시법과 개인정보보호 | V. 결론 |
| III. 스마트도시와 얼굴인식정보의 법적 문제 | |

스마트도시는 도시의 경쟁력과 삶의 질 향상을 위하여 스마트도시 기술을 활용하여 건설된 스마트도시기반시설 등을 통하여 언제 어디서나 스마트도시서비스를 제공하는 도시를 말한다.

스마트도시가 적법하게 추진되기 위해서는 개인정보의 적법한 처리가 필수적으로 담보되어야 한다. 특히 스마트도시에서 지능형 CCTV를 이용한 얼굴인식정보는 생체정보 중 특정 개인을 인증·식별할 목적으로 처리되는 정보로서 생체인식정보에 해당한다. 얼굴인식정보는 활용 범위가 현재까지 명확하게 법적 근거가 없으므로 이를 구체화하는 개선작업이 필요하다. 따라서 본 논문에서는 스마트도시와 얼굴인

<https://doi.org/10.35148/ilsire.2022..25.63>

투고일: 2022. 11. 6. / 심사완료일: 2022. 11. 22. / 게재확정일: 2022. 11. 29.

* 한국법제발전연구소 연구실장, 법학박사

Ph.D., S.C at Korea Laws Reform Institute

식정보의 법적 내용을 개관하면서, 스마트시티구현을 위한 얼굴인식 정보의 활용에 대한 장단점과 얼굴인식정보의 수집 및 이용에 대하여 법적 측면에서 스마트시티 시민의 동의권의 문제점을 파악하였다. 스마트도시는 도시의 안전관리 및 도시서비스의 제공과정에서 얼굴인식과 같은 개인의 정보가 수집, 이용, 제공, 보유, 관리 및 파기되는 경우에도 관계 법령에 따라 필요한 목적의 범위에서 적법하고 안전하게 취급되어야 한다는 기조에 따라서 법적 개선방안을 제시하였다.

[주제어] 스마트시티, 개인정보보호, 얼굴인식, 옵트아웃, 동의권

I. 서론

1. 스마트도시의 정의

2000년대 초반들어 스마트도시는 전세계적으로 확산되고 있으며, 우리나라는 ubiquitous city, U-City라는 명칭으로 스마트도시 사업이 시작되었다. 2008년에 제정된 유비쿼터스도시의 건설등에 관한 법률이 2017년에 스마트도시조성 및 산업진흥등에 관한 법률(이하 ‘스마트도시법’이라고 함)로 개정되었다. 다음은 스마트도시에 대한 여러 정의를 살펴보기로 한다.

1.1 ISO

도시와 관련된 사람들(거주자, 기업, 방문객)에게 서비스와 삶의 질을 변화시키기 위해, 도시의 지속가능성과 탄력성 및 속도를 향상시키고, 도시가 시민사회에 어떻게 영향을 주는지, 협력적 리더십 수단들에 어떻게 적용되는지, 도시 운영 구성요소들과 도시 시스템에서 어떻게 작동하는지, 데이터와 통합기술을 어떻게 사용하는지를 근본적으로 개선시키

는 도시라고 한다.¹⁾

1.2 EU 위원회

스마트도시는 디지털 솔루션을 활용하여 주민과 기업의 이익을 위해 전통적인 네트워크와 서비스를 더욱 효율적으로 만드는 곳이다. 스마트도시에서는 디지털 기술을 활용하여 시민을 위해 더 나은 공공서비스를 제공하고, 자원을 효율적으로 사용하며, 환경에 미치는 영향을 줄인다. 또한 기존의 네트워크와 서비스에 디지털 기술을 결합하여 그 효율성을 높임으로써 주민과 기업에게 편리함을 제공한다. 뿐만 아니라 자원을 적게 소비하고 탄소배출을 감소하는 차원을 넘어선다. 더 똑똑한 교통, 상하수도, 조명과 난방 등을 포함하며, 상호 소통을 높이고 시민의 요구를 만족할 수 있는 거버넌스, 도시 안전, 고령화 친화적 도시 등도 포함한다. 궁극적으로 시민의 삶의 질을 개선하고 도시의 지속가능성을 높이고자 한다.²⁾

1.3 ITU³⁾

스마트도시는 시민과 기업의 이익을 위해 디지털 솔루션을 활용해 전통적인 네트워크와 서비스를 더욱 효율적으로 만드는 곳으로, 더 나은 자원 사용과 더 적은 쓰레기배출을 위한 디지털 기술의 사용을 통해 교통망, 향상된 상수도 및 폐기물 처리 시설, 건물의 조명 및 난방을

1) ISO, “Sustainable cities and communities — Indicators for smart cities”, <<https://www.iso.org/standard/69050.html>>, 검색일: 2022.10.05.

2) European Commission, “Smart cities”, <https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en>, 검색일: 2022.10.05.

3) 국제전기통신연합(ITU, International telecommunication union)은 정보통신 기술과 네트워크의 발전, 전세계 ICT의 확산을 주도하기 위해 설립된 UN 산하의 ICT 전문 국제기구로서, 1865년 유럽 유선전신의 국제협력을 위해 만국전신연합으로 출발하여, 1947

위한 더 효율적인 방법을 의미하며, 더 상호작용적이고 반응적인 도시 행정, 더 안전한 공공 공간, 그리고 고령 인구의 요구를 충족시키는 도시를 지향한다.⁴⁾

1.4 IDC⁵⁾

스마트도시는 주로 ICT를 활용하여 도시의 경쟁력 및 삶의 질을 향상시키고 도시의 지속가능성을 추구하는 도시라고 할 수 있다.⁶⁾⁷⁾

1.5 우리나라 스마트도시법

스마트도시법에서는 도시의 경쟁력과 삶의 질의 향상을 위하여 건설·정보통신기술 등을 융·복합하여 건설된 도시기반시설을 바탕으로 다양한 도시서비스를 제공하는 지속가능한 도시라고 정의한다.⁸⁾ 이

년 UN의 정보통신 전문기구가 된 세계 최고(最古)의 국제기구로서 ITU의 주요 업무는 ① 전기통신 기술 표준 제정·관리 ② 주파수의 국제 분배, 국제 전파규칙 제·개정 ③ 개도국의 ICT 발전과 정보격차 해소를 위한 기술 및 망구축 지원 등으로 ICT 분야의 가장 필수적인 사항을 담당하고 있다. 외교부, “국제전기통신연합(ITU) 상세현황”, <https://overseas.mofa.go.kr/ch-geneva-ko/brd/m_23753/view.do?seq=2&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=1>, 검색일: 2022.10.06.

4) European Commission, “Smart cities”, <https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en>, 검색일: 2022.10.6.

5) 인터내셔널 데이터 코퍼레이션은 미국의 IT 및 통신, 컨슈머테크놀로지 부문 시장조사 및 컨설팅 기관이다. 1964년 패트릭 맥거번 등이 설립했다.

6) IDC, “IDC Government Insights: Worldwide Smart Cities and Communities Strategies”, <https://www.idc.com/getdoc.jsp?containerId=IDC_P23432>, 검색일: 2022.10.08.

7) 노재인/박형수/명승환, “디지털 트윈을 활용한 스마트시티 재난관리 방안 연구: 인천광역시 사례를 중심으로”, 한국지역정보학회지 제25권 제1호, 한국지역정보학회, 2022, 2쪽.

8) 스마트도시법 제2조 제1호

처럼 스마트도시의 개념은 ICT 중심의 기술주도형으로 시작하였고,⁹⁾ 시간이 흐르면서 시민 삶의 질 향상을 위한 도시서비스에 초점을 맞춘 도시주도형으로 진화하였다.¹⁰⁾

1.6 소결

스마트도시는 정보통신기술(ICT) 등 삶의 질 향상, 도시운영 및 서비스의 효율성, 경쟁력 향상을 위한 혁신도시라고 할 수 있다. 경제적·사회적 및 환경적 측면에서 현재 및 미래 세대의 요구를 충족시키는 가장 포괄적인 정의로 볼 수 있다.¹¹⁾

이처럼 스마트도시는 관련 도시서비스의 성과를 개선하기 위해 주로 인프라에 투자하고 있다. ICT를 기반으로 한 새롭고 업그레이드된 인프라의 도입으로 도시는 모든 면에서 삶의 질을 향상시킴으로써 시민들에게 더욱 효율적이고 지속가능하며 변화를 추구하고 있으며 시민들의 삶을 개선하기 위해 데이터의 수집, 집계 및 사용을 지속적으로 개선하기 위한 인프라를 구축하고 있다.¹²⁾

-
- 9) 기술적인 측면을 강조하면 Intelligent city, Digital city, Ubiquitous city, Hybrid city, Information city 등으로 불리기도 하고 도시 내의 사람 활동을 강조하면 Creative city, Learning city, Humane city, Knowledge city 등으로 구분할 수 있다. 허정화, “스마트시티는 미래의 도시로 충분인가?”, 인간과 평화 제3권 제1호, 평화나눔연구소, 2022, 196쪽.
- 10) 임치현/김광재, “스마트시티에 대한 통합적 이해의 시도 : 인간과 기계의 협업”, 문명과 경제 제4호, 포항공과대학교 융합문명연구원, 2021, 223쪽.
- 11) National Library of Medicine, “A Regulatory View on Smart City Services”, <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6358906/>>, 검색일: 2022.10.10.
- 12) The White House, “FACT SHEET: Administration Announces New “Smart Cities” Initiative to Help Communities Tackle Local Challenges and Improve City Services”, <<https://obamawhitehouse.archives.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help>>, 검색일: 2022.10.15.

2. 우리나라 스마트 도시프로젝트

우리나라의 예를 들면 스마트도시는 U-City 기반 CCTV 통합 관제센터의 확장형이라고 할 수 있다. 우리나라에서 추진하는 스마트도시의 종류를 보면 다음과 같다.

2.1 국가시범도시

국가시범도시는 4차 산업혁명 관련 기술을 개발계획이 없는 부지에 자유롭게 실증·접목을 조성하기 위해 실행되었다. 또한 창의적인 비즈니스 모델을 구현할 수 있는 혁신산업 생태계를 조성하여 미래 스마트도시 선도모델을 제시하는 것을 목표로 추진 중에 있다.

국가시범도시(세종, 부산)는 창의적인 비즈니스 모델을 구현할 수 있는 혁신산업 생태계를 조성하여 미래 스마트도시 선도모델을 제시하는 것을 목표로 4차 산업혁명 신기술의 테스트베드로서 현재 사업 중이다.¹³⁾

2.2 실증도시

대구광역시와 시흥시는 실증도시로서 연구목적에 따라 2개 유형(도시문제 해결형, 비즈니스 창출형)으로 구분된다. ‘도시문제 해결형’은 교통·안전·도시행정 등 도시들이 공통적으로 겪고 있는 문제 해결을 위해 대규모 도시를 대상으로 하는 실증연구로 2018년 국토교통부의 공모 절차를 거쳐 대구광역시가 실증도시로 선정됐다. 대구광역시는 스마트모빌리티 활성화(교통), 사고범죄 긴급구난 대응(안전), 재난 조기경보 대응(도시행정) 등의 연구 수행을 위한 체계적인 계획이 높은

13) 세종특별자치시, “국가시범도시”, <https://www.sejong.go.kr/kor/sub04_1405.do>, 검색일: 2022.10.10.

평가를 받았다. ‘비즈니스 창출형’은 에너지·환경·복지 등 새로운 산업을 스마트도시에 적용하기 위해 중소규모의 도시에서 리빙랩(Living Lab) 형태로 추진하는 연구로 경기도 시흥시가 실증도시로 선정됐다. ‘지속가능한 스마트 프로슈밍시티’를 연구목표로 제시한 시흥시는 지역 산업의 쇠퇴, 고령인구 증가, 도시과밀 등 중소도시의 보편적 특성을 다양하게 보유하고 있어 실증연구의 적합성을 인정받았다.¹⁴⁾ 플랫폼 중심의 하드웨어적 구성과 물리적 보안 위주의 인프라 구축사업만이 진행된 상황이다.

2.3 지역거점 스마트도시 조성사업

「지역거점 스마트도시 조성사업」은 지역 주도의 스마트도시 전국 확산을 위하여 지역에 거점을 조성하는 스마트도시건설사업으로 도시별 3년간 최대 240억원(국비·지방비 5:5 매칭)을 지원한다. 2022년 지역거점 스마트도시 조성사업은 총 8곳의 지자체가 신청해 2:1의 경쟁률을 보였으며, 광주·창원·해남·횡성 4곳이 선정되었다.

「중소도시 스마트도시 조성사업」은 지역 수요와 여건을 고려해 중소 규모 도시 내 도시문제 해결을 위한 스마트 솔루션을 구축하는 스마트도시 체감도 제고사업으로 도시 별로 1년간 국비 20억원(지방비 1:1 매칭)을 지원한다.

2022년 중소도시 스마트도시 조성사업은 총 49곳의 지자체가 신청해 3:1의 경쟁률을 보였으며, 경기 구리시·군포시·의정부시, 경남 통영시·함안군, 경북 경주시·안동시, 부산 부산진구, 서울 양천구, 울산 울주군, 전남 곡성군, 전북 익산시·전주시, 충남 계룡시·예산군, 충북 괴산군 16곳이 선정되었다.

14) 국토교통부 보도자료, “데이터 기반 스마트시티 연구개발 본격착수”, 2018, 2-3쪽 참조

3. 스마트도시와 데이터

스마트도시와 일반 도시의 결정적인 차이는 데이터라고 할 수 있다. ICT에 기반하여 도시에서 발생하는 각종 데이터를 수집, 저장, 분석하여 도시의 건축, 개발, 관리운영상의 문제점을 파악하고 데이터에 근거하여 도시의 문제를 해결하는 것이 스마트도시의 중심내용이다.

또한 스마트도시의 특성상 다른 정보와 쉽게 결합하여 개인을 식별할 수 있는 정보로서 개인정보에 해당할 개연성이 높다.¹⁵⁾

스마트도시에서 발생하는 각종 데이터는 스마트도시 통합운영센터 운영자, 스마트도시기반시설 소유자, 스마트도시서비스 제공자 등 서로 데이터 제공이 필연적이다. 따라서 스마트도시가 적법하게 추진되기 위해서는 개인정보의 적법한 처리(수집, 이용 및 제공 등)가 필수적으로 담보되어야 한다.

그러나 스마트도시의 이러한 장점은 단점을 내포하고 있다. 스마트도시의 정부와 관리자는 많은 다른 공간을 통해 연결된 보안 카메라와 지능형 시스템에 접근할 수 있기 때문에, 시민들은 익명성을 유지하는데 어려울 수밖에 없다. 예를 들면 얼굴인식 카메라와 같은 시스템은 사생활이나 사적인 공간의 개념을 크게 변화시킬 것이다. 또한 스마트도시 곳곳에 설치된 보안 카메라로 수집한 데이터를 추적하고 중앙 집중화할 수 있는 정부는 더 큰 힘을 갖게 될 것이다. 이는 시민의 데이터를 통제할 수 있으며, 여론을 조작할 수도 있다. 그 이유는 스마트도시의 시민들은 거의 전적으로 자신의 생활과 삶에 대한 정보를 정부의 네트워크에 의존할 것이기 때문에, 의사 결정에서 자율성을 잃고 무능해질 수 있다. 이는 스마트도시 전체가 거대한 감시체제인 파놉티콘(panopticon)이 될 수 있다는 불안감이 있다. 즉 디지털 기술의 발달에

15) 이혜원, “스마트도시와 개인정보 보호”, IT와 법연구 제20집, 경북대학교 IT와 법연구소, 2020, 84쪽.

따른 감시, 검열 등 시민들에 대한 통제의 강화는 오히려 시민의 권리를 위협할 수 있다. 이는 민주주의의 위기이다.¹⁶⁾ 스마트도시에서 처리되는 개인정보 빅데이터에 대한 관리적 보안등 개인정보보호 관리체계가 충분하지 않다.¹⁷⁾

따라서 본 논문에서는 스마트도시의 성공적인 안착은 스마트도시에서 개인정보 보호를 위한 법정정책 기반이 필수적이므로, 이를 위한 법적 개선방안을 제시하고자 한다.

II. 스마트도시법과 개인정보보호

스마트도시는 IoT(Internet of Things)를 활용함으로써 효율적인 운영을 할 수 있는 도시로 재난방지, 관광, 환경보호 등에 다양한 적용이 가능하다. 한편 IoT 도입으로 도시운영 시스템이 네트워크로 연결되기 때문에 사이버 공격의 대상이 될 위험이 있으며, 실제로 해킹 가능한 교통 시스템이 있는 것으로 보고되고 있다. 이처럼 스마트도시 시스템이 공격당하면 도시 기능이 마비될 수 있을뿐 아니라 오픈 데이터 외에도 개인정보 등의 클로즈드 데이터도 취급되기 때문에 그러한 데이터는 적절히 관리가 필요하다. 스마트도시의 핵심은 사물인터넷과 다양한 기술들을 활용해 데이터를 수집하고, 이를 통해 개인에게 맞는 편리한 서비스를 제공하는 것이다. 하지만, 개인 맞춤 서비스를 받기 위해서는 그만큼 개인에 대한 정보를 공유해야 하는 것이다.

16) 이승욱/배덕현/김성온, “스마트시티 거버넌스에 대한 비판적 고찰: 중국의 스마트시티 정책을 사례로”, 공간과 사회 제70권 제1호, 한국공간환경학회, 2019, 275쪽.

17) 정환석/이상준, “스마트시티 속 개인정보보호 강화 방안 연구”, 정보보호학회논문지 제30권 제4호, 한국정보보호학회, 2020, 706쪽.

1. 스마트도시와 개인정보보호법의 관계

개인정보보호법은 개인정보 처리에 관한 사항을 규정하고 있는 일반 법이므로, 다른 법률에 개인정보 보호에 관한 특별한 규정이 있으면 해당 법률이 우선적으로 적용되며 그렇지 않은 경우에는 개인정보보호법이 적용된다. 스마트도시법에서는 스마트도시의 관리 및 스마트도시 서비스 제공과정에서 개인정보가 처리되는 경우에 관계 법령에 따르도록 규정한다.¹⁸⁾

따라서 기반시설 관리청, 서비스제공자 등이 처리하는 정보, 스마트 도시 통합운영센터 등에 제공·연계되는 정보에 개인정보가 포함된다면 개인정보보호법상 의무를 준수해야 한다.

2. 개인정보보호원칙의 외국사례

2.1 OECD 가이드라인¹⁹⁾

개인정보보호법은 경제개발협력기구(OECD)가 국가간 경제활성화를 위해 어떻게 하면 프라이버시를 보호하면서 유통을 활발하게 할 수 있을 것인지를 연구한 결과 제정한 「개인정보의 국제유통과 프라이버시 보호에 관한 가이드라인」(Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data)은 각국의 개인정보보호법률에 중요한 영향을 끼치고 있으며, 각국 정부와 민간이 네트워크 환경에서 효율적인 프라이버시보호를 위해 범세계

18) 스마트도시법 제21조(개인정보 보호) 스마트도시의 관리 및 스마트도시서비스의 제공 과정에서 개인의 정보가 수집, 이용, 제공, 보유, 관리 및 파기되는 경우에는 관계 법령에 따라 필요한 목적의 범위에서 적법하고 안전하게 취급되어야 한다.

19) OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", <<https://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm#part2>>, 검색일: 2022.10.12.

적 규제 수단의 채택을 촉구하였다.²⁰⁾

- ① 수집 제한 원칙: 개인정보는 본인에게 통지 또는 동의를 얻은 후 적법하고 공정한 수단으로 수집한다.
- ② 데이터 내용의 원칙: 개인정보는 그 이용 목적에 따른 필요한 범위 내에서 정확, 완전, 최신 상태로 유지한다.
- ③ 목적 명확화의 원칙: 개인정보 수집의 목적을 밝힌다.
- ④ 이용 제한 원칙: 수집한 개인정보는 명확화된 목적 이외에는 사용하지 않는다. 다만 데이터 주체의 동의가 있는 경우 또는 법률의 규정에 의한 경우는 예외로 한다.
- ⑤ 안전 확보 원칙: 개인정보는 분실·파괴·수정·공개 등의 위험에 대해 합리적인 안전보호조치를 강구한다.
- ⑥ 공개 원칙: 개인정보에 관한 정책, 개발, 운용 등은 일반적으로 공개한다.
- ⑦ 개인 참가 원칙: 정보주체(본인)는 자신의 정보의 소재를 확인하거나 삭제, 정정할 권리가 있으며 관리자는 적절하게 그러한 요청에 대응할 필요가 있다.
- ⑧ 책임의 원칙: 관리자는 이상의 원칙을 책임지고 이행할 필요가 있다.

2.2 GDPR상 개인정보보호원칙²¹⁾

유럽연합(EU)의 일반개인정보보호법(General Data Protection Regulation, “GDPR”)이 2018년 5월 25일부터 시행되었다. GDPR은 개인정보 보호와 관련하여 EU 회원국들에 공통적으로 적용되고 법적 구속력을 갖는 개

20) 원신희, “온라인프라이버시 보호에 관한 美, EU의 정책동향 및 전망”, 월간 KIEP 세계경제 제24권, 대외경제정책연구원, 2000, 17쪽.

21) GDPR TEXT, “제5조 GDPR. 개인정보 처리 원칙”, <<https://gdpr-text.com/ko/read/article-5>>, 검색일: 2022.10.12.

인정보보호법이다. 특히 GDPR은 기업에게 개인정보에 대한 보호의무와 제한을 부과하고 있다.²²⁾

- ① 적법성·공정성·투명성의 원칙: 개인정보는 정보주체에 대해 적법하고, 공정하며, 투명하게 처리되어야 한다.²³⁾
- ② 목적제한의 원칙: 개인정보는 구체적이고 명시적이며 적법한 목적을 위해 수집되어야 하고, 해당 목적과 양립되지 않는 방식으로 추가 처리되어서는 안 된다.²⁴⁾ 공익적 기록보존의 목적, 과학적 또는 역사적 연구목적, 또는 통계적 목적을 위한 추가 처리는 제89조(1)에 따라 본래의 목적과 양립되지 않는 것으로 보지 않는다.
- ③ 데이터 최소화 원칙: 처리되는 목적과 관련하여 적절하고, 타당하며, 필요한 정도로만 제한되어야 한다.²⁵⁾
- ④ 정확성의 원칙: 개인정보는 정확해야 하고, 필요한 경우 최신의 것이어야 한다. 처리 목적과 관련하여 부정확한 개인정보는 지체없이 삭제 또는 정정되도록 모든 적절한 조치가 시행되어야 한다.²⁶⁾

22) 김성현/이창무, “EU GDPR과 국내 개인정보보호 법제 비교분석”, 융합보안논문지 제18권 제5호, 한국융합보안학회, 2018, 85쪽.

23) 개인정보 처리를 위한 적법성의 근거로서 GDPR은 제6조 및 제7조에서 동의, 계약, 법적 의무, 중대한 이익, 공적 업무수행, 적법한 이익 등의 6가지를 제시하고 있다.

24) 예를 들면 위치추적 등에 대한 법적 근거와 안전장치가 마련되어야 하고 개인 데이터의 추가 사용에 관한 목적 및 명시적 제한에 대한 명확한 기준과 관리자 식별이 포함되어야 한다. European Data Protection Board, “Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak”, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf>, pp.7-8. 검색일: 2022.10.15.

25) 예를 들면 시민의 상태, 통신 식별자, 장비 디렉터리 항목, 메시지, 통화 로그, 위치 데이터, 장치 식별자 등을 포함할 수 있는 관련 없거나 필요하지 않은 정보를 수집해서는 안 된다. *Ibid.*, p.9.

26) 정확성의 원칙은 데이터의 구체적인 사용에 따른 위험의 결과와 관련하여 파악되어야 한다. 부정확한 개인 데이터는 시민의 권리와 자유에 위협이 될 수 있다. European Data Protection Board, “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”, <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_2019_04_dataprotection_by_design_and_by_default.pdf>, p.21. 검색일: 2022.10.14.

- ⑤ 기간제한의 원칙: 처리목적 달성에 필요한 기간 동안만 정보 주체를 식별할 수 있는 형태로 보관되어야 한다.²⁷⁾ 개인정보는 제89조(1)²⁸⁾에 따라 개인정보 주체의 권리 및 자유를 보호하기 위해 본 규정이 요구하는 적절한 기술 및 관리적 조치를 시행하여 공익적 기록보존 목적, 과학적 또는 역사적 연구목적, 통계적 목적을 위해 처리되는 경우 더 오랜기간 동안 보관될 수 있다.
- ⑥ 무결성과 기밀성의 원칙: 개인정보의 적절한 보안을 보장하는 방식으로 처리해야 한다. 보장 방식은, 적절한 기술 및 관리적 조치를 사용하여, 개인정보가 무단으로 또는 불법적으로 처리된 다거나 우발적으로 소실, 파기, 손상되었을 경우의 보호조치 등을 포함한다.²⁹⁾
- ⑦ 책임성의 원칙 : 개인정보관리자는 제1항이 준수되도록 할 책임이 있으며, 이를 입증할 수 있어야 한다.³⁰⁾

27) 이와 관련하여 참고할 자료로는 검색엔진 제공자의 개인데이터수집 기간은 6개월이며, 개인정보를 6개월 이상 보유할 경우 서비스에 엄격히 필요하다는 점을 종합적으로 입증해야 한다. European Commission, “Opinion 1/2008 on data protection issues related to search engines”, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf>, p.19. 검색일: 2022.10.15.

28) GDPR 제89조 제1항은 그러한 안전조치는 특히 데이터 최소화 원칙이 준수되도록 기술 및 관리적 조치를 이행해야 한다. 그러한 조치에는 가명처리 방식으로 그러한 목적들을 달성할 수 있다면 가명처리가 포함될 수 있다. 정보주체의 식별을 허용하지 않거나 더 이상 허용하지 않는 추가 처리를 통해 그러한 목적들이 달성될 수 있는 경우에는 그러한 방식으로 이루어져야 한다고 규정한다.

29) 개인데이터에 대한 비정상적 접근을 예방하고 악성프로그램으로부터 발생할 수 있는 데이터의 손상을 방지하고, 비정상적 접근 및 개인데이터의 변경 사항을 모니터링 하기 위한 자동화된 감시시스템의 구축이 필요하다. European Data Protection Board, “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”, <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf>, p.24. 검색일: 2022.10.17.

30) European Data Protection Board, “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”, <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf>, p.6. 검색일: 2022.10.17.

2.3 일본의 슈퍼시티법

2020년 5월 제정된 일본의 슈퍼시티법은 도시의 디지털 전환을 위한 공공 부문과 민간 부문 간의 협력을 개선하는 것을 목표로 한다. 이는 기존의 국가전략특구법을 개정한 것으로 슈퍼시티법이라고 한다.³¹⁾ 슈퍼시티로 선정된 도시는 자율주행차 개발과 이용 등 의료, 교육, 에너지, 범죄예방, 교통 등에 AI와 빅데이터를 투입한다. 일본의 슈퍼시티는 주민의 눈높이에서 지역의 당면 과제를 해결하기 위해 첨단적 서비스를 삶에 구현시킨 형태의 도시이다.³²⁾ 그러나 일본의 슈퍼시티법에서는 스마트도시 시민의 개인정보보호를 위한 별도의 규정이 존재하지 않는다. 일본의 데이터 및 개인정보에 관한 법제도는 민관의 데이터 활용과 개인정보 보호에 관한 법적 기반으로서 민관 데이터 활용 추진 기본법, 개인정보를 취급하는 민간사업자의 감독에 주안점을 둔 개인정보 보호에 관한 법률, 행정기관의 개인정보 취급에 초점을 맞춘 행정기관이 보유한 개인정보 보호에 관한 법률 등이 있었다.³³⁾ 그러나 2021년 5월 디지털 사회 형성을 도모하기 위한 관계 법률의 정비에 관한 법률이 공포되었다. 동법은 “개인정보보호에 관한 법률”, “행정기관이 보유하는 개인정보보호에 관한 법률” 및 “독립행정법인 등이 보유하는 개인정보보호에 관한 법률”의 3법을 개인정보보호에 관한 법률로 통합함과 동시에 지방공공단체의 개인정보보호제도를 포함하여 전체 소관을 개

개인정보관리자는 데이터 보호 원칙을 구현하도록 설계된 적절한 기술적 및 조직적 조치를 구현하고, GDPR의 요구사항을 충족하고 데이터 주체의 권리를 보호하기 위해 개인정보 보호장치를 마련해야 한다.

31) 内閣府, “スーパーシティ、デジタル田園健康特区について”, <<https://www.chisou.go.jp/tiiki/kokusentoc/supercity/openlabo/supercity.pdf>>, p.2. 검색일: 2022.10.17.

32) 조미향·이정찬, “주민 중심의 지역 당면 과제 해결을 위한 일본 슈퍼시티 구상의 내용과 시사점”, 국토이슈리포트 제42호, 국토연구원, 2021, 1쪽.

33) Liquidous, “日本における個人情報に係る法制度の検討”, <<https://liquidous.com/lisearch/journal/2020/05/31/267/>>, 검색일: 2022.10.17.

인정보보호위원회로 일원화하는 것을 특징으로 한다.³⁴⁾

특히 개인 데이터 이용정지권이나 소거권, 제3자 제공권이 법적으로 강화되었다. 예를 들면 개인 데이터를 정보 주체의 동의 없이 제3자에게 제공할 수 있는 옵트아웃 규정의 범위가 더욱 제한되었다.

3. 외국법제의 시사점

EU는 스마트도시와 관련된 법령을 제정하지 않았고, 일본은 스마트 도시법(슈퍼시티법)을 제정하였으나, 스마트도시에서 개인정보보호에 관하여는 자국의 개인정보보호 법제들을 운영하고 있다. 그 이유는 EU 나 일본 역시 옵트아웃방식을 채택하고 있으므로 굳이 특별법을 제정할 필요가 없이 스마트도시에서 발생하는 개인정보와 관련된 문제들을 처리할 수 있기 때문이다.

외국의 입법례와 비교하여 보면 개인정보의 처리와 관련하여 정보 주체의 동의를 원칙으로 하고 예외적으로 동의가 필요 없는 경우를 엄격하게 규정하고 있는 우리 법제는 스마트도시와 관련된 개인정보를 처리하는 과정을 볼 때 현실과는 거리가 먼 제도라고 할 수 있다.³⁵⁾

Ⅲ. 스마트도시와 얼굴인식정보의 법적 문제

1. 얼굴인식기술 현황

현재 스마트도시의 많은 곳에서 얼굴인증이나 교통정체 정보 등을

34) 자세한 내용은 김경석, “디지털사회를 대비한 일본의 법률정비와 의미 - 디지털사회형 성기본법을 중심으로 -”, 국제법무 제13권 제2호, 제주대학교 법과정책연구원, 2021, 5-7쪽 참고

35) 이해원, 앞의 논문, 113쪽.

예측하는 AI 기술이 사용되기 시작했다.³⁶⁾ 자율주행과 얼굴인증 카메라가 확산되고 있고, 중국에서는 교통 체증이나 안전 영역을 벗어나는 사람들을 대상으로 얼굴인식 프로그램을 사용하여 경고를 하거나 범인을 검거하는데 활용하고 있다.³⁷⁾ 이처럼 얼굴인식 기술(FRT)³⁸⁾은 공공 및 민간 부문 조직 모두 FRT 기능을 통합하여 운영 생산성을 높이고 공공 안전을 개선할 수 있다는 장점이 있다.

이러한 얼굴인식 기술은 1990년대 초반의 개발에서 2000년대 들어 더 크고 실질적인 데이터 세트의 생성과 2014년부터 딥 러닝 기술의 통합으로 인해 상용화로 발전했다.³⁹⁾

예를 들면 생산성 및 효율성의 제고, 정확성의 제고 등으로 많은 영역에서 활용되고 있다. 특히 높은 정확성, 신속성, 비접촉성으로 금융, 보안, IT 등 다양한 산업군에서 활용되고 있다.⁴⁰⁾ 최근에는 코로나로 인해 열 스캐너가 장착된 공공장소에서 얼굴인식 시스템의 사용이 증가했다. 이것을 계기로 장기적으로 스마트도시와 지방자치단체의 다양한 분야

36) 국제 앰네스티(Amnesty International) 보고서에 따르면 전 세계적으로 적어도 64개국이 얼굴인식 시스템을 적극적으로 사용하고 있는 것으로 분석하였다. CARNEGIE, "The Global Expansion of AI Surveillance", <<https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>>, 검색일: 2022.10.20.

37) 한국인터넷진흥원, 해외 주요국의 안면인식 기술 활용 동향- 미국, 중국, 일본, 2018년 해외 개인정보보호 동향분석, 2018, 64쪽.

38) 얼굴인식 기술은 개인의 얼굴의 가시적인 물리적 구조를 저장된 얼굴 템플릿과 비교하여 개인의 신원을 확인하거나 개인을 고유하게 식별하는 데 사용되는 컴퓨터 프로그램을 말한다. National Telecommunications and Information Administration, "Privacy Best Practice Recommendations For Commercial Facial Recognition Use", <https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recognition.pdf>, p.2. 검색일: 2022.10.20.

39) For an overview of the technological evolution see : Inioluwa Deborah Raji/Genevieve Fried, "About Face: A Survey of Facial Recognition Evaluation", <<https://arxiv.org/pdf/2102.00813.pdf>>, 검색일: 2022.10.20.

40) 최새술, 안면인식기술 도입의 사회적 논란과 시사점: 미국사례 중심으로, ETRI 기술정책 브리프, 2020, 1쪽.

에서 얼굴인식 기술 사용을 늘리는 데 도움이 될 수 있다.

머신러닝과 같은 인공지능(AI) 영역 내의 기술들은 딥러닝과 컴퓨터 비전 알고리즘을 포함하여, 컴퓨터가 이미지와 비디오의 내용을 보고, 수집하고, 처리가 가능하게 된다. 알고리즘은 대규모 데이터 세트에서 얼굴 특징과 속성을 학습하고 추출하도록 정기적으로 훈련되며 이제 딥 러닝이 지배적이다.

얼굴 감지 및 분석에 대한 접근 방식은 인공지능을 통해 더 빠르고 정확한 식별을 허용함으로써 조명이 불량하고 대상이 방해되는 경우에도 대상자의 얼굴을 인식할 수 있다. AI를 기반으로 하여 얼굴인식 시스템은 실제 FRT 애플리케이션의 출현을 촉진하고 있다. 그러나 동시에 이러한 생체 인식 기술은 매우 민감한 개인 데이터를 수집한다.⁴¹⁾

2. 스마트도시와 얼굴인식정보의 장점과 단점

2.1 얼굴인식정보의 장점

스마트도시를 개발하는 중심축 중 하나는 신체적으로 취약한 사람들을 위해서도 유용하게 이용될 수 있다. 얼굴인식은 위험에 처한 사람들을 식별하고 그들이 가장 필요로 할 때 도움을 받을 수 있도록 사용되어야 한다. 예를 들면 알츠하이머병에 걸린 사람은 보다 세분화된 의료 애플리케이션에서 법정대리인의 동의하에 안전한 데이터베이스에 정보를 업로드할 수 있다.

스마트도시에서 환자들은 지원 시스템 역할을 하는 안전한 데이터베이스를 선택할 수 있다. 환자가 실종되고 방향감각이 상실되는 상황에서, 스마트도시 관리자는 FRT를 사용하여 그들을 식별하고, 법정대리인

41) European Commission, Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, 2021, p. 8.

에게 연락하거나 병원과 연결시키는 기술은 응급 서비스에 대한 압력을 완화시킬 것이다.

얼굴인식을 통해 통합된 범죄 데이터베이스는 범죄자로 예상되는 얼굴을 은행, 현금자동입출금기, 백화점 등 범죄 예상 장소에서 지속적으로 추적할 것이다. 사법 당국은 이러한 정보를 통해 범죄가 발생하기 전에 개입할 수 있다.⁴²⁾

2.2 스마트도시와 얼굴인식정보의 단점

그러나 스마트도시 정책에 있어서 얼굴인식 정보는 프라이버시 등의 법적, 윤리적 과제를 해결해야 하는 문제가 남아 있다.

얼굴인식 기술은 식별목적을 위한 얼굴 이미지를 비교하거나 저장할 수 있다. AI 기반 얼굴인식 기술을 통한 생체 인식은 매우 민감하고 개인 데이터를 수집하면서 더 정교한 기술과 알고리즘을 배치한다. AI와 IoT 기술의 조합이 증가함에 따라 개인 데이터를 포함한 더 많은 데이터가 장치(예: 보안 감시 카메라 또는 자율주행 차량)를 통해 지속적으로 수집되고 분석된다. 얼굴인식 기술은 개인의 프라이버시를 침해하고 데이터 보호에 취약하다.⁴³⁾ 얼굴은 사람에게 고유한 것이므로 이러한 개인정보의 탈취로 인하여 범죄에 악용된다면 큰 문제이다. 즉 사생활의 붕괴가 일어나는 것이다. 또한 얼굴인식기술은 인공지능의 편향성으로

42) MXFACE, “Face Recognition: 5 Ways It Helps Smart Cities Become Even Smarter”, <<https://mxface.ai/face-recognition-for-smart-cities>>, 검색일: 2022.10.22.

43) 미국 하와이 소재 연방 제9 항소법원은 2022년 2월, “페이스북과 일리노이 집단소송 사건 원고 측의 합의를 조속히 이행하라”고 명령하면서 소송 참가자 160만명에게 60일 이내에 보상금 397달러씩을 지급하도록 하였다. 이 집단소송은 2015년 일리노이 주민 3명이 페이스북의 얼굴 인식-태그 제안 기능이 일리노이주 개인 생체정보 보호법에 위배된다며 시카고 연방법원에 소장을 제출하면서 시작되었다. 오피니언뉴스, “페이스북, ‘개인생체정보보호법’ 위반 · · · 보상금 지급판결”, <<https://www.opinionnews.co.kr/news/articleView.html?idxno=64202>>, 검색일: 2022.10.22. 참조.

인하여 차별의 문제를 제기한다.⁴⁴⁾ 예를 들면 얼굴인식 알고리즘은 높은 분류 정확도(90% 이상)를 자랑하지만 이러한 결과는 보편적이지 않다. 점점 더 많은 연구들이 인구통계학적 그룹에 걸쳐 다양한 오류율을 노출하고 있으며, 여성, 흑인, 18-30세의 피험자들에게서 일관되게 가장 낮은 정확도가 발견된다.⁴⁵⁾

3. 얼굴인식기술에 대한 법적 문제

3.1 법적 근거의 미비

얼굴 데이터를 수집할 때는 시민들의 동의를 받는 것이 문제이다. 다만 현실적으로 시민들로부터 이러한 동의를 받기가 쉽지 않다. 개인 식별용 얼굴 사진은 ‘개인정보’에 해당하므로, 식별 대상자들로부터 동의를 받고,⁴⁶⁾ 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.⁴⁷⁾ 민감정보에 해당하는 얼굴 사진의 경우 개인정보 보호법 제23조 제1항에 의해 민감정보의 처리에 대한 별도의 고지, 동의가 필요하다. 그러나 스마트도시의 도로나 건물에 설치된 CCTV를 통하여 교통량의 흐름을 파악하고, 이를 분석한 후, 최적의 교통신호와 가장 빠른 길 안내를 하는 것은 개인정보보호의 예외에 해당하는 법적근거가 분명하므로 별 문제는 없다. 그러나 도로교통의 원활화라는 1차 목적달성을

44) 이창민, “안면인식정보 보호 및 안면인식기술 규제에 관한 미국법 연구”, 저스티스 제179권, 한국법학원, 2020, 6쪽.

45) SITN, “Racial Discrimination in Face Recognition Technology”, <<https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology>>, 검색일: 2022.10.22.

46) 개인정보보호법 제15조 제1항 제1호.

47) 개인정보보호법 제15조 제1항 제2호.

위해 만들어진 정보를 범죄자 수색이라는 목적으로 사용되는 경우는 그것을 활용할 수 있는 법적 근거가 미비하다고 할 수 있다.⁴⁸⁾ 이는 개인정보보호법 제25조의 적용이 어렵다고 본다.

3.2 정보수집에 대한 정보주체의 동의 여부

개인정보처리자는 개인정보를 수집할 수 있으며 정보 주체의 동의를 받은 경우에는 그 수집 목적의 범위에서 이용할 수 있다.⁴⁹⁾ 또한 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보 주체의 권리보다 우선하는 경우에는 그러하지 아니하다. 또한 스마트도시법 제37조에서도 예외를 두고 있다.⁵⁰⁾ 그러나 개인의 얼굴인식 정보를 수집하여 2차 목적에 사용하는 경우까지 개인정보 주체인 시민의 명시적 또는 묵시적 동의가 있다고 할 근거 조항이 명확하지 않다. 또한 시민들이 얼굴정보 이용에 대한 동의내용을 파악하기가 쉽지 않다.

3.3 수집정보활용을 위한 관리주체의 권한의 모호성

스마트도시법과 동법 시행령에서는 통합운영센터의 권한 범위나 업무 범위에 대해 구체적으로 정의한 바가 없다. 따라서 실제로 통합운영센터가 할 수 있는 행위가 불분명하다. 한편 지방자치단체 조례로 통합운영센터 운영계획의 수립 및 관리와 운영에 필요한 사항을 정할 수 있다.⁵¹⁾ 그러나 그 위임의 범위가 포괄적이므로 포괄위임금지원칙을

48) 오세원/선종수, “스마트도시에서 정보 수집·보관 및 이용에 관한 법적 고찰”, 공공정책연구 제38권 제1호, 동아대학교 지방자치연구소, 2021, 265쪽.

49) 개인정보보호법 제15조 제1항.

50) 익명 처리된 개인정보의 활용에 대한 다른 법령의 배제를 규정하여 특정 개인을 알아볼 수 없도록 익명 처리하여 정보를 활용하는 경우에는 개인정보보호법을 비롯하여 위치정보법과 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’ 등의 적용을 배제하는 규정을 두고 있다.

위반하는 문제가 발생할 수 있다.⁵²⁾

IV. 스마트도시와 얼굴인식정보 법제의 개선

1. 얼굴인식정보에 대한 법적 통제의 필요성

1.1 미국

미국 통신정보관리청(NTIA)은 얼굴인식과 관련된 이해당사자들을 모아, 얼굴인식 기술의 상업적 활용을 위한 자발적 지침인 모범사례 권고사항을 발표하였다. 주요 권고사항은 개인정보의 수집·저장·이용을 투명하게 진행할 것, 얼굴 템플릿데이터 관리 방안(Facial template data management practices)을 개발할 것, 얼굴템플릿 데이터의 공개나 공유에 대한 정보 주체의 통제를 허용할 것, 데이터 보호를 위한 적절한 보안 조치를 실행할 것, 안면 템플릿 데이터의 활용과 관련해 고객이 기업과 연락을 취해 시정할 수 있는 방안을 제공할 것 등이다.⁵³⁾

미국 생체정보 보호법 중 가장 강력한 것으로 평가받는 일리노이주의 생체정보 보호법(BIPA, Biometric Information Privacy Act, 2008년 도입)으로, 이 법은 기업이 개인정보를 이용 시, 반드시 서면 동의를 받을 것을 의무화하고 있다.⁵⁴⁾

51) 스마트도시법 제19조 제6항.

52) 오세원/선종수, 위의 논문, 267쪽.

53) National Telecommunications and Information Administration, “Privacy Best Practice Recommendations For Commercial Facial Recognition Use”, <https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recognition.pdf>, pp.1-3. 검색일: 2022.10.23.

54) *Ibid.*, p.5.

1.2 EU

유럽 연합의 기본권 헌장은 민간생활의 FT의 사용에 대한 명시적 동의를 요구하고 있다.⁵⁵⁾ 참고로 이러한 동의는 전자적 방법을 포함한 서면 진술이나 구두진술 등으로, 정보주체가 개인정보의 처리에 대해 자유롭게 제공하여야 하는데, 구체적으로, 고지된 명확한 합의를 나타내 주는 적극적인 행위로써 제공되어야 한다. 동의표현 방법에는 인터넷 웹사이트의 개인정보처리 동의란 체크, 정보사회서비스에 대한 기술적 설정 선택 또는 본인의 개인정보처리 수락을 의미하는 정보주체의 행동이나 기타 진술이 포함된다. 따라서 침묵, 사전 자동체크된 개인정보처리동의나 부작위는 동의에 해당되지 않는다. 동의는 단일 또는 복수의 동일한 목적을 위한 모든 처리 활동에 유효하다. 복수의 목적으로 개인정보를 처리하는 경우, 각 목적에 대한 동의를 받아야 한다. 만약 정보주체의 동의를 전자방식의 요청에 따라 제공하는 경우, 그 요청은 명확하고 간결하게 제공되어야 하며, 관련 서비스 이용을 불필요하게 방해해서는 안된다.⁵⁶⁾ 또한 동의가 자유롭게 제공되기 위해서는, 정보주체와 정

55) European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2020. EU기본권헌장 제7조(사생활과 가정생활의 존중) 모든 사람은 자신의 사생활과 가정생활, 집과 의사소통에 대한 존중을 받을 권리를 가진다. EU기본권헌장 제8조(개인정보의 보호) ① 모든 사람은 자신과 관련된 개인정보를 보호받을 권리를 가진다. ② 개인정보는 오로지 신의와 성실원칙에 따라 특정한 목적을 위해 당사자의 동의 또는 법률의 근거 아래 처리되어야 한다. 모든 개인은 그에 관해 수집된 정보에 대한 접근할 권리와 수정을 요구할 권리가 있다. 즉 기본권헌장 제8조 제1항에서 개인정보보호권을 명시적으로 보장할 뿐만 아니라, 제8조 제2항에서 정보접근권과 수정요구권과 같은 정보주체의 권리와 개인정보의 적법한 처리기준을 규정하면서 핵심적인 정보보호원칙들을 언급하고 있다. 정애령, “사생활보호와 개인정보보호의 관계에 관한 연구- 유럽연합 기본권헌장을 중심으로 -”, 공법학연구 제17권 제3호, 한국비교공법학회, 2016, 56쪽.

56) REGULATION (EU) No XXX/2016 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data(General Data Protection Regulation) (Text with

보처리자 간의 명백한 불균형이 존재하는 특정 상황과 같은 경우에는 동의를 합법적인 근거로 제시해서는 안된다. 특정 상황이란 특히 정보처리자가 공공기관이기 때문에 동의가 자유롭게 제공될 것 같지 않은 경우이다. 개별적인 사례에서 적절하다고 판단되는 경우도 있겠으나, 별개의 개인정보처리 행위에 대해 별도의 동의를 받지 않는 경우이거나, 서비스 제공 등의 계약의 이행이 동의없이 이루어질 수 있음에도 불구하고 동의에 근거하여 진행되는 경우에는 해당 동의는 자유롭게 제공된 것이라고 볼 수 없다.⁵⁷⁾

그리고 2021년 4월 공개된 EU 인공지능(AI)법 초안은 생체 인식, 신용 평가 등 ‘고위험 AI’에 대한 규제를 포함한 인공지능법(Artificial Intelligence Act) 초안을 발표하였으며, 동 법안은 회원국 간의 협의, 승인을 거쳐 2023년 이후 시행될 것으로 예상된다. 그 중 FRT의 사용을 제한하는 것도 목표의 하나이다. 즉 공개적으로 접근할 수 없는 자연인의 실시간 원격 생체 인식 식별(RBI)에 AI 시스템의 사용을 금지할 것을 제안하였다.⁵⁸⁾

구체적으로 EU는 고위험 AI에 대해 적절한 위험 평가 및 관리 시스템, 고품질의 데이터 세트, 추적을 위한 로그자료 확보 등을 요구하고, 시스템에 대한 모든 정보가 포함된 상세 문서, 명확하고 적절한 정보의 제공, 리스크 최소화를 위한 인적 감독 조치, 높은 수준의 보안 및 정확도 등을 마련하도록 하였다.

고위험 AI에는 시민들의 생명 및 건강에 위협이 되는 인프라로서 교통 등, 신용 점수와 같은 필수적인 민간 또는 공공서비스 등이 포함되며, 시험 채점, 수술 보조 로봇, 이력서 분류 소프트웨어, 법적 증거의 신뢰성

EEA relevance), p.19

57) *Ibid.*, p.43.

58) European Parliament, “Regulating facial recognition in the EU”, <[https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf)>, p.25(4.2.2.2. Scenarios for FRT regulation.), 검색일: 2022.10.24.

판단, 이주 또는 망명 및 국경 통제, 사법 행정 및 민주적 절차에 사용되는 경우 등은 허용된다. 특히 원격 생체인식시스템의 경우 실종 아동의 수색, 생명이나 신체적 안전을 위한 테러범 탐색, 범죄자의 탐지 및 위치 확인 등과 같은 세가지의 경우에만 제한적으로 허용된다.⁵⁹⁾

1.3 영국

2019년 영국 정보국(Information Commission's Office)은 런던 킹스 크로스 개발(안면 인식 카메라 기술)에 대한 조사를 개시하였다. 그 이유는 수백만 개의 개인 생체 데이터가 유출되었을 수 있다는 폭로 때문이었다.⁶⁰⁾ 시민들의 얼굴을 합법적으로 스캔하는 것은, 시민들을 식별하기 위한 것으로 사생활에 대한 잠재적인 위협이기 때문이다.

1.4 생체정보보호 가이드라인

2021년 개인정보위원회가 발표한 생체정보 가이드라인은 얼굴 사진(영상)의 경우에 얼굴 사진(영상)에서 특징점 등을 기술적으로 추출하여 개인의 인증·식별 목적으로 출입통제(얼굴인식) 시스템 등에 사용하는 경우는 생체인식정보에 해당하며, 얼굴 사진(영상)에서 특징점 등을 기술적으로 추출하지만 특정 개인의 인증·식별목적이 아닌 성별, 감정 상태(웃는 모습, 화난 모습 등)를 알아보기 위해 사용되는 경우는 일반적인 생체정보에 해당한다고 보았다.⁶¹⁾ 따라서 원본정보는 생체인식정보를 전자적으로 처리하는 과정에서 유출되거나 오·남용되는 경우 개인

59) *Ibid.*, p.26.

60) MercoPress, "UK investigation into breaches in the storage of public's biometric data", <<https://en.mercopress.com/2019/08/19/uk-investigation-into-breaches-in-the-storage-of-public-s-biometric-data>>, 검색일: 2022.10.25.

61) 개인정보보호위원회, 생체정보보호 가이드라인, 2021, 4쪽.

정보 침해 위험성이 크므로 원본정보의 안전한 보관을 위해 저장 시 암호화, 원본정보를 특징정보 생성 후에도 보관하는 경우 다른 개인정보와 분리 보관하는 등 별도의 보호조치가 필요하며, 일반적인 얼굴 사진·동영상, 음성파일 등을 차후에 인증·식별 목적의 특징정보 생성에 사용하는 경우, 해당 정보는 생체인식정보에 해당하게 되므로 생체인식정보에 적용되는 보호조치를 이행해야 한다.⁶²⁾

2. 스마트도시 건설시 개인정보보호 적용설계

스마트도시에서 얼굴인식 기술의 사용과 성공 여부는 시민들의 생활을 보호하는데 도움이 될 규제와 표준을 개발하는 것에 달려 있다고 해도 과언이 아니다.

얼굴인증 기술 사용으로 편의성이 향상될 것으로 보이는 경우는 어린이 등하교 및 길을 잃거나 병으로 쓰러진 고령자를 발견하여 응급구조를 하는 것과 같은 안전에 관심이 높을 것으로 보인다. 또한 범죄자의 특징이나, 밀입국 등 방법에 활용, 은행이나 ATM, 현금 카드나 신용카드로의 개인 인증에의 활용이 필요할 것으로 보인다.

따라서 스마트도시 및 스마트도시서비스의 기획·설계 단계부터 스마트도시 내 개인정보 처리의 모든 과정에 개인정보보호 중심 설계(Privacy by Design, PbD)를 적용하여 예상되는 침해위험 요인을 사전에 분석하고 예방 조치를 할 필요가 있다. PbD는 기술이나 서비스 기획의 초기부터 폐기 단계까지 정보 주체의 이익을 우선 보호하는 관점에서 개인정보보호를 사전적으로 내재화하여 설계하는 원칙과 실행전략을 말한다.

원칙은 모든 종류의 개인정보에 적용될 수 있지만 의료정보나 재무데이터, 얼굴인식정보 등과 같은 민감한 데이터에는 특히 강력하게 적용되

62) 개인정보보호위원회, 위의 가이드라인, 6쪽.

어야 한다. 개인정보보호를 위한 대책의 강도는 데이터의 기밀성의 높이에 상응하는 경향이 있다. 따라서 사전적이고 예방적인 개인정보보호 문제를 도시설계 및 운영에 적용해야 한다. CCTV에 의해 촬영된 시민의 얼굴에 대한 이미지 암호화를 통하여, 권한이 있는 자만 이미지를 복호화해서 접근할 수 있는 비밀키를 제공하는 것이다.⁶³⁾ 개인정보보호법 시행령 제18조 제3호에서 규정한 바와 같이 얼굴템플릿 같은 정보는 민감정보로서 강력한 법의 보호를 받을 것으로 기대한다.

3. 동의는 옵트아웃방식으로의 전환

스마트도시에서의 기반시설에 설치된 CCTV에 의한 개인정보의 수집은 공익적 목적으로 공공장소에 설치된 CCTV에 의한 개인정보 수집에 해당하므로 정보 주체의 동의가 없더라도 적법성에는 문제가 없다고 본다.⁶⁴⁾ 그러나 IoT 환경에서의 작은 센서를 통하여 얼굴 정보와 같은 개인정보수집은 정보 주체인 시민의 동의와는 거리가 멀다. 그 이유는 자신의 개인정보가 수집되고 있다는 사실 자체를 모르기 때문이다. 이러한 사정하에서 정보 주체의 동의를 받는다는 사실 자체가 현실적으로 어려우며, 개인정보처리에 동의한 시민에게만 스마트도시에 입주할 수 있도록 하자는 주장은 설득력이 있다고 보기 어렵다. 정부도 개인정보 제공자에 한하여 입주한다는 방침을 정하였다는 기사가 있었지만,⁶⁵⁾

63) 김남심/지성우, “Privacy by design제도에 대한 규범적 고찰”, 성균관법학 제30권 제4호, 성균관대학교 법학연구원, 2018, 48쪽.

64) 스마트도시에서는 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보와 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보는 개인정보보호법 제58조에서 동의에 대한 적용의 일부 제외를 규정하고 있다. 그러나 개인정보처리자는 목적을 위하여 필요한 범위에서 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치, 개인정보의 처리에 관한 고충처리, 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하여야 한다.

다음 날 공식적으로 그러한 사실을 부인하였다.⁶⁶⁾ 개인정보보호법제에서 동의의 형식화와 비현실화는 동의제도의 한계에 직면하며, 그것은 동의제도가 개인정보의 실질적 보호에는 기여도가 떨어질 수 밖에 없다.⁶⁷⁾

스마트도시에는 주로 시민의 안전, 도시의 정보제공, 의료 등 시민에게 삶에 기본적으로 필요한 공공서비스를 제공하는 경우가 대부분이므로, 개인정보주체인 시민으로서는 관련 서비스의 이용에 동의하지 않는 경우가 드물 것이다. 따라서 개인정보의 필수적인 동의 사항에 대해서는 원칙적으로 디폴트 규칙을 동의로 설정하고 부동의하는 사람에 대해서만 개인정보의 공유를 옵트아웃방식으로 하는 것도 동의방식의 하나로 선택할 수 있다. 우리 개인정보보호법이 옵트인 방식을 채택하고 있으므로⁶⁸⁾ 이 방식을 채택하기 위해서는 법개정이 필요하다. 이를 통하여 스마트도시에서 시민의 개인정보를 수집단계에서 통제보다는 이용단계에서의 통제로의 전환이 필요하다.⁶⁹⁾

65) 정부는 민간과 함께 이들 도시에 국내 최고 수준의 정보통신기술(ICT)과 인프라스트럭처를 조성할 예정이다. 정부·민간 투자로 조성되는 최고 주거 환경인 만큼 특별한 입주 조건이 따라붙는다. 스마트도시 특위 관계자는 스마트도시 국가시범단지는 시민 스스로 실험체가 돼 빅데이터 기술 등을 통해 도시문제를 해결해 도시를 발전시켜 나가는 리빙랩 구현이 최우선 목적이라며 “개인의 생활패턴 등 분석이 가능해야 하는 만큼 스마트도시 내 입주자격을 개인정보 제공자에 한해 제한할 방침”이라고 말했다. 매일경제, “[단독] 스마트시티 입주하려면 개인정보 제공 동의해야”, <<https://www.mk.co.kr/news/realstate/view/2018/08/510465>>, 검색일: 2022.10.27 참조.

66) 대한민국 정책브리핑, “[참고] 스마트시티에 개인정보 제공 동의자만 입주하는 방침 없음”, <<https://www.korea.kr/news/pressReleaseView.do?newsId=156288134>>, 검색일: 2022.10.27.

67) 권영준, “개인정보 자기결정권과 동의 제도에 대한 고찰”, 법학논총 제36권 제1호, 전남대학교 법학연구소, 2016, 718쪽.

68) 실제 적극적 동의방식인 옵트인은 더 잦은 클릭, 더 많은 서명을 유발함에도 불구하고 개인정보보호에 있어서 그다지 의미있는 효과를 보여주지 못하고 있다. 자세한 내용은 김현경, “정보주체의 권리보장과 ‘동의’제도의 딜레마”, 성균관법학 제32권 제3호, 성균관대학교 법학연구원, 2020, 121쪽.

69) 권영준, 앞의 논문, 722쪽.

4. 얼굴인식정보 법제에 대한 신뢰성의 확보

얼굴인식 기술의 이용을 금지하기보다는 개인의 신원을 증명할 별다른 수단이 없는 실종아동이나 신분증을 두고 나간 치매노인을 찾는 과정에서 얼굴인식 기술의 활용은 실종자를 찾는 유일한 수단일 수도 있다. 이처럼 시민의 안전과 건강을 지키는 등 스마트도시의 시민의 편익을 높이기 위한 얼굴인식 기술의 유용성을 인정하고, 얼굴인식 기술의 신뢰성을 확보할 수 있는 방안을 모색하는 것이 필요하다. 현재 지방자치단체에서 설치 운영하는 CCTV 통합 관제센터는 스마트도시법에 따른 핵심사업이라고 할 수 있다. 2022년 서울시는 예고했던 치매 어르신 실종 방지 지능형 CCTV 확대가 본격 추진된다. 이는 인공지능이 얼굴 정보를 학습한 후 CCTV 영상을 통해 치매 노인의 위치를 파악하는 기술을 활용하는 것이다.⁷⁰⁾

그러나 카메라에 촬영된 영상에서 특정 정보주체를 인식하고 이를 추적하는 기능이 있는 지능형 CCTV는 개인정보 보호법에 따른 CCTV의 운영이 아니므로, 개별적인 동의가 필요하며, 시민의 편익을 위한다는 전제하에 무단으로 사용되는 경우에는 위법한 것이 된다. 또한 얼굴인식은 개인의 위치정보로도 기능할 수 있으므로, 위치정보의 보호 및 이용 등에 관한 법률 제2조 제2호에서 규정하고 있는 위치정보에 해당할 수 있다. 따라서 현재 제안된 개인영상정보의 보호 등에 관한 법률안과 같이 개인영상정보처리자는 영상정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 당초 촬영 목적의 범위에서 개인영상정보를 이용하거나 제3자에게 제공할 수 있도록 하고, 개인영상정보처리자는 가명처리 등의 기술적·관리적 조치를 통해 영상정보주체를 알아볼 수 없도록 하는 방법으로 통계작성, 과학적 연구, 공익적

70) 디멘시아뉴스, “2022년도 스마트시티 투자 지속…치매 반사이익 기대”, <<https://www.dementiaNews.co.kr/news/articleView.html?idxno=4833>>, 검색일: 2022.10.27.

기록보존을 위하여 개인영상정보를 추가로 이용하거나 제3자에게 제공할 수 있도록 하는 방안이 있다. 그리고 개인영상정보처리자는 개인영상 정보가 분실, 도난, 유출 등이 되지 아니하도록 영상정보처리기기 및 개인영상정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하도록 하도록 하여,⁷¹⁾ 얼굴인식정보의 규제에 대한 스마트도시의 시민에 대한 신뢰를 갖도록 하는 것이 중요하다.

V. 결론

스마트도시는 시민의 편익을 위하여 행정, 물류, 교통, 관광, 재난관리, 의료, 복지, 교육, 금융, 환경, 기타 민간 서비스 등의 각종 서비스를 제공할 수 있도록 시민들의 데이터를 수집·제휴·공유하는 것이 필요하다. 이러한 측면에서 스마트도시는 정보통신기술(ICT) 등 삶의 질 향상, 도시운영 및 서비스의 효율성, 경쟁력 향상을 위한 혁신도시라고 할 수 있다. 그러나 스마트도시에서는 데이터 연계 기반을 통해 다양한 주체가 데이터를 연계하고 공유하게 되는데, 이것은 개인정보보호에 관련된 문제가 발생한다. 특히 얼굴인식기술은 1990년대 초반의 개발에서 2000년대 들어 더 크고 실질적인 데이터 세트의 생성과 2014년부터 딥 러닝 기술의 통합으로 인해 상용화로 발전했다. 그러나 스마트도시와 얼굴인식에 따른 개인정보의 문제는 장점과 단점이 존재한다. 얼굴인식 기술은 개인의 프라이버시를 침해하고 데이터 보호에 취약하다. 개인정보보호법 제23조 제1항에 따른 얼굴 데이터수집은 민감정보에 해당하며, 스마트도시에서 일일이 시민의 동의를 받는 것이 쉽지가 않다.

따라서 개인정보보호법과 스마트도시법의 얼굴인식정보에 따른 개인정보의 보호관련 법제의 개선이 필요하다. 예를 들면 EU의 인공지능

71) 이용준, 개인영상정보의 보호 등에 관한 법률안 검토보고, 국회정무위원회, 2021, 2-3쪽.

법(Artificial Intelligence Act) 초안은 공개적으로 접근할 수 없는 자연인의 실시간 원격 생체 인식 식별(RBI)에 AI 시스템의 사용을 금지할 것을 제안하였다. 그러나 스마트도시의 얼굴인식정보는 시민의 생명·신체의 안전과 고령자보호 등을 위하여 긍정적으로 운용될 수 있다.

이를 위해서 개인정보보호법상의 얼굴인식정보수집에 대한 동의 방식을 옵트인 방식에서 옵트아웃방식으로 개정할 필요성이 있다. 또한 개인영상정보의 보호 등에 관한 법률안과 같이 개별법을 제정하여 촬영 목적의 범위에서 얼굴인식정보와 개인영상정보를 이용하거나 제3자에게 제공할 수 있도록 하고, 얼굴인식기술의 안전성 확보에 대한 법적 개선이 이루어져야 한다.

참고문헌

1. 학술지

- 김경석, “디지털사회를 대비한 일본의 법률정비와 의미 - 디지털사회형 성기본법을 중심으로 -”, 국제법무 제13권 제2호, 제주대학교 법과정책연구원, 2021, 1-30쪽.
- 김남심/지성우, “Privacy by design제도에 대한 규범적 고찰”, 성균관법학 제30권 제4호, 성균관대학교 법학연구원, 2018, 35-63쪽.
- 김성현/이창무, “EU GDPR과 국내 개인정보보호 법제 비교분석”, 융합 보안논문지 제18권 제5호, 한국융합보안학회, 2018, 83-92쪽.
- 노재인/박형수/명승환, “디지털 트윈을 활용한 스마트시티 재난관리 방안 연구: 인천광역시 사례를 중심으로”, 한국지역정보화학회지 제25권 제1호, 한국지역정보화학회, 2022, 1-33쪽.
- 오세원/선종수, “스마트도시에서 정보 수집·보관 및 이용에 관한 법적 고찰”, 공공정책연구 제38권 제1호, 동아대학교 지방자치연구소, 2021, 255-282쪽.
- 이승욱/배덕현/김성온, “스마트시티 거버넌스에 대한 비판적 고찰: 중국의 스마트시티 정책을 사례로”, 공간과사회 제70권 제1호, 한국 공간환경학회, 2019, 271-322쪽.
- 이창민, “안면인식정보 보호 및 안면인식기술 규제에 관한 미국법 연구”, 저스티스 제179권, 한국법학원, 2020, 5-45쪽.
- 이해원, “스마트도시와 개인정보 보호”, IT와 법연구 제20집, 경북대학교 IT와 법연구소, 2020, 83-128쪽.
- 임치현/김광재, “스마트시티에 대한 통합적 이해의 시도 : 인간과 기계의 협업”, 문명과 경계 제4호, 포항공과대학교 융합문명연구원, 2021, 219-255쪽.

- 정애령, “사생활보호와 개인정보보호의 관계에 관한 연구- 유럽연합 기본권헌장을 중심으로 -”, 공법학연구 제17권 제3호, 한국비교공법학회, 2016, 51-80쪽.
- 정환석/이상준, “스마트시티 속 개인정보보호 강화 방안 연구”, 정보보호학회논문지 제30권 제4호, 한국정보보호학회, 2020, 705-717쪽.
- 조미행/이정찬, “주민 중심의 지역 당면 과제 해결을 위한 일본 슈퍼시티 구상의 내용과 시사점”, 국토이슈리포트 제42호, 국토연구원, 2021, 1-12쪽.
- 허정화, “스마트시티는 미래의 도시로 충분한가?”, 인간과 평화 제3권 제1호, 평화나눔연구소, 2022, 191-207쪽.

2. 웹자료

- 외교부, “국제전기통신연합 (ITU) 상세현황”, <https://overseas.mofa.go.kr/ch-geneva-ko/brd/m_23753/view.do?seq=2&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=1>, 검색일: 2022.10.06.
- 内閣府, “スーパーシティ、デジタル田園健康特区について”, <<https://www.chisou.go.jp/tiiki/kokusentoc/supercity/openlabo/supercity.pdf>>, 검색일: 2022.10.17.
- European Commission, “Smart cities”, <https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en>, 검색일: 2022.10.15.
- European Data Protection Board, “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”, <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201904_dataprotection_

by_design_and_by_default.pdf>, 검색일: 2022.10.15.

European Data Protection Board, “Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak”, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf>, 검색일: 2022.10.15.

ISO, “Sustainable cities and communities — Indicators for smart cities”, <<https://www.iso.org/standard/69050.html>>, 검색일: 2022.10.05.

National Library of Medicine, “A Regulatory View on Smart City Services”, <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6358906/>>, 검색일: 2022.10.10.

OECD, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, <<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#part2>>, 검색일: 2022.10.12.

The White House, “FACT SHEET: Administration Announces New “Smart Cities” Initiative to Help Communities Tackle Local Challenges and Improve City Services”, <<https://obamawhitehouse.archives.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help>>, 검색일: 2022.10.15.

3. 보고서

최새술, 안면인식기술 도입의 사회적 논란과 시사점: 미국사례 중심으로, ETRI 기술정책 브리프, 2020.

한국인터넷진흥원, 해외 주요국의 안면인식 기술 활용 동향- 미국, 중국, 일본-, 2018년 해외 개인정보보호 동향분석, 2018.

[Abstract]

A Study on Legal Improvement of Smart City and Information of Facial Recognition

Kim, Myung Yeop*

A smart city uses information and communication technology(ICT) to improve operational efficiency, share information with the public and provide a better quality of government service and citizen welfare.

One emerging technology that is becoming more important for smart cities is Facial Recognition Technology(FRT). Both public and private sector organizations can enhance operational productivity and improve public safety by integrating FRT capabilities. It compares an individual's face presented at the point of access to a database of authorised persons to determine whether there is a match. And it is helpful for vulnerable citizens. However, Act On The Promotion Of Smart City Development And Industry does not have any special regulations on personal information Protection.

This paper: (1) provides an overview the legal systems for facial recognition. (2) highlights concerns arising from merits and demerits of the facial recognition information and from its potential impacts on citizen's consent rights (3) takes stock of the legal improvement, especially Personal Information Protection Act and Act On The Promotion Of Smart City Development And Industry currently applicable to facial recognition. (4) Raise the issue of legal bases to ground the processing of personal data in smart city, This issue is crucial, as the need to have an appropriate legal basis for the processing is essential to ensure a facial recognition's legality. It is essential that obtain consent in the smart city, given that data collection happens in a public space and is not freely given. How consent

* Ph.D., S.C at Korea Laws Reform Institute

can be used in the smart city, and what other legal bases can be used instead of consent. It gives citizens more control over their personal data as facial recognition and the ability to opt out at any time. These rules will put in place much better safeguards and rights for citizens.

[Key Words] smart city, personal information protection, facial recognition, opt-out, consent right, privacy by design