해외 개인정보보호 동향 보고서

월간동향

2019년 7월

KISA 한국인터넷진흥원

스마트시티와 개인정보보호 논란: 주요 사례와 관련 정책 동향

< 목 차 >

1. 개요 및 배경

▶ 스마트시티는 “도시 공간에 신기술을 접목하여 각종 문제를 해결하고, 삶의 질을 개선할 수 있는 도시 모델”로서[1] 모든 인프라를 네트워크화하고 다양한 데이터를 기반으로 운용하는 것이 특징

- IoT 전문 컨설팅 업체 Strategy of Things에 따르면, 스마트시티에 대한 정의는 매우 다양하지만 기술을 기반으로 정부 효율성, 지속성, 보건복지, 이동성, 경제발전, 공공안전, 삶의 질 향상 등을 추구한다는 점에서는 공통적
- 최근에는 다양한 혁신기술을 도시 인프라와 결합해 구현하고 융·복합할 수 있는 공간이라는

1 출처: 스마트시티 추진전략('18.1.29, 4차 산업혁명위원회, 관계부처합동)

의미의 “도시 플랫폼”이라는 의미로도 활용[2]

- 스마트 도시 기반시설 등을 통하여 행정·교통·복지·환경·방재 등 도시의 주요 기능별 정보를 수집한 후 그 정보를 서로 연계하여 제공하는 스마트시티 서비스의 범위도 확대되는 추세

▶ 네트워크와 센서 기반으로 다양한 도시 기능을 실시간으로 제어 및 운용하는 스마트시티는 삶의 질 개선과 도시의 효율성 향상이라는 순기능과 더불어 방대한 데이터 이용에 따른 개인정보보호 문제를 야기

- 개인의 위치 정보에서 일상 활동에 이르기까지 다양한 유형의 데이터를 상시적으로 수집·이용·공유·저장하는 과정에서 개인정보 유출 및 정보주체의 권리 침해 가능성도 확대
- 살아있는 개인을 식별할 수 있는 데이터는 해당 정보주체에게 귀속되지만 적법한 목적을 위해서는 이 같은 데이터에 대한 접근·처리·공유가 허용되므로 스마트시티 환경에서 다양한 개인정보의 활용이 가능

▶ 도시공간이 자동화된 센서와 알고리즘에 점점 더 의존하게 됨에 따라, 시민들의 활동 현황을 실시간으로 파악할 수 있는 데이터를 수집하고 이를 바탕으로 행동을 제약하거나 차별을 조장하는 정책 결정이 이뤄질 수 있다는 우려도 심화

- 스마트시티 기술 부문에서 개인 식별이 가능한 정보들과 다양한 정보들을 연결해 개인의 프로필 정보를 완성함으로써 개인정보 침해를 가속화할 수 있다는 문제점은 Brookings Institution의 보고서 <Getting Smarter About Smart Cities> 이후 지속적으로 제기
- 캐나다 토론토 라이어슨 대학의 개인정보보호 및 빅데이터 연구소 소장인 Ann Cavoukian 박사는 특히 대중교통 시스템의 폐쇄회로 감시 카메라, 얼굴인식을 비롯한 각종 생체 인식 시스템, 스마트 유틸리티 계량기 및 스마트 그리드, 원격 헬스케어 분야에서 개인정보 침해의 우려가 크며, Privacy by Design이 중요하다고 지적[3]
- 이에 따라, 스마트시티 생태계에 참여하는 각종 기업, 조직, 지역 정부 등은 데이터 컨트롤러 또는 프로세서로서 개인정보 이용 규정을 준수하고 개인정보보호를 위한 조치를 취하는 것이 필요
- 단, 대부분의 개인정보보호법제가 스마트시티 환경 자체를 염두에 두고 제정 및 실행된 것은 아니라는 점에서 개인정보의 오남용 방지를 위한 다양한 도전 과제들에 직면

2 http://www.molit.go.kr/USR/WPGE0201/m_36673/DTL.jsp
3 http://www.brantfordexpositor.ca/2017/05/08/expert-urges-big-data-privacy

2. 주요 사례

(1) 캐나다 토론토의 “SideWalk Toronto” 프로젝트

▶ Alphabet의 자회사 Sidewalk Labs가 캐나다 토론토에서 진행 중인 “SideWalk Toronto” 스마트시티 프로젝트의 개인정보 침해 우려가 확산되면서, Ann Cavoukian 박사가 온타리오주 개인정보보호 커미셔너 자리를 사임하는 등 갈등이 지속되는 상황

- Alphabet의 자회사 Sidewalk Labs는 캐나다 토론토 교외의 수변(水邊) 지역에 324만㎡ 규모의 스마트시티 건설을 위해 약 9억 9,000만 달러를 투자하기로 결정
- Sidewalk Labs가 제시한 스마트시티 비전의 핵심은 다양한 종류의 센서를 사용하여 도시에서 일어나는 일에 대한 실시간 정보를 수집하는 것이 특징
  - 이러한 센서에는 Wi-Fi 안테나, 자동차 교통량을 자동적으로 계측하는 차량 계수기, 신호등과 가로변 기둥에 부착된 공기 질 측정기 등이 포함
- 그러나 도시 곳곳에 설치되는 센서들로 인해 시민들이 과도한 감시에 노출되고 비윤리적인 데이터 수집이 이루어질 수 있다는 주장이 지속적으로 제기

▶ Sidewalk Labs는 센서를 통해 수집된 개인정보를 광고 목적 등으로 판매하지 않는다는 내용을 스마트시티 마스터플랜에 포함시키는 등 개인정보보호 기능을 강화한 방안을 제시

- Sidewalk Labs의 Dan Doctoroff CEO는 기자회견을 통해, 명시적 동의 없이는 제3자에게 개인정보를 공개하지 않고 개인정보를 판매하지도 않을 것임을 약속
- 이와 함께, 센서를 통한 데이터 수집 과정에서 영지식 증명기술(Zero-Knowledge Proofs, ZKP[4] 과 디지털 서명 등 보안 강화를 위한 암호화 기술을 대거 적용하기로 결정
- 그러나 영국의 언론매체 Guardian 등 주요 언론은 Sidewalk Labs의 토론토 스마트시티 프로젝트가 감시 자본주의의 가장 진화된 버전이 될 것이라고 지적
- 시민단체들은 이번 스마트시티 조성 프로젝트를 무효화해야 한다며 법정 소송을 준비

4 네트워크상에 흘러 다니는 정보의 양을 0(zero)에 가깝게 만드는 기술. 영지식 기법을 이용한 인증에서는 주장자 A의 키에 대한 정보를 전혀 유출하지 않으면서, 주장자 A가 키를 알고 있다는 사실만을 증명함으로써 인증이 이루어짐. 영지식 기술 기반의 인증을 사용하면 인증 시 키에 대한 정보의 유출이 전혀 없기 때문에 인증 횟수가 늘어나도 키의 안전도가 보장됨 (출처: IT용어사전, 한국정보통신기술협회)

(2) 중국 항저우와 베이징의 "City Brain" 프로젝트

▶ 중국의 Alibaba가 제공하는 스마트시티 플랫폼 City Brain에서 비밀번호 없이도 웹 브라우저로 접속 가능한 스마트시티 데이터베이스가 노출되면서 개인정보보호의 취약성을 재확인[5]

- City Brain은 빅데이터 컴퓨팅과 인공지능 심층 신경망을 이용해 도시 전역의 정보를 수집하고 이를 중앙에서 분석해 차량 흐름 등을 효과적으로 제어하는 등 중국의 대표적인 스마트시티 플랫폼으로 각광
- Alibaba는 항저우에서 2016년 4월부터 City Brain 시범 프로젝트를 통해 104개의 신호등을 자동으로 제어함으로써 교통 체증 시간을 15% 감축하는 성과를 창출하고, 이후 1,300개의 신호등과 3,700개의 교통 카메라에 City Brain 기술을 적용
- City Brain은 사고 감지, 혼잡 탐지, 차량 통행량 계산, 차량 분류, 교통 신호등 최적화, 트래픽 시뮬레이션 등 시내 교통 개선을 위한 주요 기능들을 제공하는 한편 도시 곳곳에 설치된 카메라를 통해 정교한 얼굴인식 시스템을 구축
- 그러나 2019년 5월 City Brain 플랫폼에서 호스팅 되는 Elasticsearch 데이터베이스가 일반에게 노출되면서, City Brain 기술이 얼굴인식 기술을 통한 감시 활동에 이용될 수 있다는 점이 부각

▶ Alibaba는 Elasticsearch 데이터베이스의 운영 주체를 밝히지 않았으나, 이 시스템은 얼굴인식 데이터를 수집하도록 설계된 카메라를 포함하여 여러 개의 데이터 수집 거점으로 구성

- Elasticsearch 데이터베이스에서는 베이징 동부에 있는 2개 이상의 지역에서 주민들을 감시해온 정황이 발견되었으며, 그 중에는 도시 내 대사관 밀집 지구로 알려진 량마챠오(亮马桥,liangmaqiao)도 포함된 것으로 확인
- Elasticsearch 데이터베이스는 사람들의 표정, 선글라스와 마스크 착용 상태, 대략적인 연령, 신체적인 매력 등에 대한 사항을 분석하여 저장
  - 예컨대 얼굴인식 시스템을 통해 해당 정보주체의 민족적 특성을 감지하고, 한족의 경우“汉族”으로 표기하고 무슬림인 위구르족의 경우 “维族”으로 구분하여 표기하는 등 차별적인 데이터 처리를 진행
- Elasticsearch에 저장된 데이터에는 카메라에 사람이 감지될 때마다 날짜, 시간, 위치, 해당 인물의 특징이 설정되고, 일부 기록에는 범죄 용의자 이름과 주민등록번호가 포함된 것으로 확인
- 이 시스템은 공안 당국이 보유한 자료에서 데이터를 공유하여 요주의 인물이나 범죄 용의자를 특정할 수 있다는 점에서 정부 기관을 고객으로 두고 있을 가능성을 시사

5 https://techcrunch.com/2019/05/03/china-smart-city-exposed/

3. 정책 동향

(1) EIP-SCC의 ISO/IEC 27570 표준 프로젝트

▶ 유럽의 스마트시티 촉진을 위한 조직인 EIP-SCC(The European innovation partnership on smart cities and communities)는[6] 스마트시티의 혁신과 개인정보보호의 양립을 위해 "시민 중심의 데이터 접근(citizen-centric approach to data)" 계획을 추진

- 2015년부터 시작된 EIP-SCC 이니셔티브는 스마트시티의 데이터 처리와 개인정보보호 문제를 해결하기 위해 다양한 웹 세미나와 워크샵을 운영했으며, 이를 토대로 ISO/IEC 27570 표준 프로젝트(스마트시티의 개인정보보호 지침)를 진행
- ISO/IEC 27570 표준은 다음과 같은 과제의 해결방안을 중점적으로 모색[7]
  - 스마트시티 관점에서 ICT 생태계 거버넌스 관리
  - 스마트시티 관점에서 ICT 생태계의 데이터 공유 동의사항 관리
  - 스마트시티 관점에서 ICT 생태계의 위험 관리
  - Privacy by Design을 통한 프라이버시 보장
  - 개인정보 관리 문제에 대한 시민 참여 프로세스 구현

(2) CNIL의 커넥티드 차량과 개인정보에 관한 패키지 보고서

▶ 프랑스 CNIL은 스마트시티의 GDPR 준수를 위한 프로그램의 일환으로, 2018년 커넥티드 차량의 개인정보 관련 패키지 보고서(Connected vehicles and personal data)를 발간

- CNIL은 커넥티드 자동차를 통해 수집된 개인정보를 처리하는 것이 GDPR의 프레임워크에 비춰볼 때 개인정보보호 측면에서 위험을 초래할 수 있다고 판단
- 서비스 제공자가 위험을 제한 할 수 있는 조치를 취하기 위해 개인정보보호 영향평가를 실시하고 위험을 분석할 것을 제안
- 특히 차량 이용자들이 자신들의 데이터에 대한 투명성과 통제권을 확보할 수 있도록 하고 했으며, Privacy by Design을 강조
- CNIL은 "지속 가능한 혁신"을 지원하기 위해 다음과 같은 세 가지 사례별로 커넥티드 차량의 개인정보보호 시나리오를 제시
  - 첫째, 차량의 데이터가 서비스 제공 업체로 전송되지 않는 경우

---

6 https://www.trialog.com/en/europe-is-working-on-privacy-guidelines-for-smart-cities/
7 EIP-SCC는 2019년 5월 17일 벨기에 브뤼셀에서 개최된 스마트시티 및 커뮤니티에 대한 EIP 총회에서 ISO/IEC 27570에 대한 최신 내용을 발표

- 둘째, 차량의 데이터가 서비스 제공 업체로 전송되지만 차량에 대한 자동적인 조치가 이루어지지는 않는 경우
- 셋째, 차량의 데이터가 원격으로 서비스 제공자에게 전송되어 차량에 대한 자동적인 조치가 이루어지는 경우

(3) 미 피츠버그 시의회의 데이터 공유 협약

▶ 미국 피츠버그 시의회(city council)는 주민들에 대한 스마트시티 서비스 역량을 강화하기 위해 2019년 5월 “다양한 주체들(various entities)”과 데이터를 공유하는 협약에 시정부 부서들이 참여할 수 있도록 임시 승인[8]

- 공유 대상 데이터에는 커뮤니티 기반 내비게이션 앱 Waze와 차량공유 업체 Uber가 제공하는 교통 정보도 포함되어 시 당국의 인프라 계획에도 도움이 될 것으로 기대
- 시의회에서 이 같은 협력 방안을 계속 주장해 온 Deb Gross 의원에 따르면, 이번 승인 조치에 따라 시정부 부서들은 시의회의 사전 승인을 받지 않고서도 데이터 기업들과 협약을 맺을 수 있는 권한을 확보
- 한편, 이번 승인 내용에는 피츠버그시가 2014년 채택한 개방형 데이터 정책에 의거하여 이미 공개 금지된 데이터를 재판매하거나 개인정보를 공개하지 않는다는 합의가 포함되고, 시정부의 법무 당국이 각각의 계약서를 검토하도록 조치

(4) GDPR 시행의 긍정적 영향

▶ 한편, 유럽 지역의 경우 GDPR의 시행으로 정보주체의 권한이 강화됨에 따라 스마트시티 프로젝트 확산에도 긍정적인 변화가 이루어질 것으로 기대[9]

- 일각에서는 GDPR에 따라 동의 여건이 강화되는 등 개인정보 이용 조건이 까다로워지면서 데이터 기반의 스마트시티 운영에 제약이 될 것이라는 우려도 제기
- 그러나 스마트시티에서 자동으로 수집된 데이터를 기업이나 조직이 처리하는 과정에서 정보주체 개인들의 권한이 크지 않았다는 점이 그동안 스마트시티 프로젝트에 대한 시민들의 호응을 저해한 요인이었음에 주목
- GDPR 시행 이후 스마트시티 프로그램에서 수집 및 이용되는 데이터에 대한 정보주체의 동의 권한이 강화되고, 개인정보의 열람·정정·삭제 권한이 보장됨에 따라 스마트시티의 개인정보보호 환경에 대한 신뢰 기반을 확보

8 https://www.post-gazette.com/local/city/2019/05/16/Councilwoman-Deb-Gross-tech-companies-data-sharing-waze-uber-ford-pittsburgh/stories/201905150128
9 https://technology.ihs.com/603153/how-the-new-gdpr-helps-smart-cities-adoption-in-the-eu

• 이에 따라 장기적으로는 스마트시티의 개인정보보호 및 보안 강화를 통한 시민 참여 확대와 안전한 프로젝트 진행이 이루어질 것이라는 전망이 제기

4. 시사점

▶ 스마트시티는 도시생활의 광범위한 영역을 포괄하여 다양한 혁신을 시도하는 단계이며, 아직까지 체계화된 스마트시티 서비스나 데이터 보안 및 개인정보보호에 대한 완전한 해결책이 제시되지는 않은 상황

• 이와 관련, 과학전문매체 Scientific American은 네트워크와 센서 기반으로 다양한 도시 기능을 실시간으로 제어 운영하는 것만이 스마트시티의 핵심은 아니며, 보안과 개인정보보호, 사법체계, 시민의 권리에 이르기까지 근본적인 사회 환경에 대한 고민이 중요하다고 지적

• 개인정보보호 영역에서는 광범위한 기술적 변화 과정에서 개인정보보호 규칙을 도시의 디지털 혁신 전략에 통합하는 것이 스마트시티의 주요 도전 과제라는 주장도 제기[10]

▶ 스마트시티 환경에서 개인정보보호의 가치를 실현하기 위해 다음과 같은 원칙을 기반으로 데이터의 수집·이용·공유·저장 과정을 추진하는 것이 필요

• 데이터 최소화(Data Minimization): 해당 목적의 수행에 절대적으로 필요한 데이터에 한정하여 수집하고 처리하는 최소 데이터셋(Minimum Data Set, MDS) 방식을 통해 스마트시티에서 데이터 수명주기 동안 안전하게 개인정보를 관리

• 비식별화(De-Identification): 비식별 처리는 개인정보보호를 위한 완벽한 해결책이 아니며 재식별 위험이 상존하고 있지만[11], HITRUST 비식별 처리 프레임워크(HITRUST De-Identification Framework) 등의 지침을 통한 비식별 수준 향상 노력도 지속

• 데이터 거버넌스(Data Governance): 데이터 관련 정책과 프로세스를 관리하는 데이터 거버넌스는 개인정보보호를 장려하고 강화하기 위한 중요한 수단으로서, 스마트시티의 개인정보보호 수준에 대한 평가 및 개선을 지원

• Privacy by Design: 개인정보와 민감한 데이터를 이용하는 시스템을 설계할 경우 적용되는 7가지 원칙은 스마트시티 이니셔티브의 설계와 운영에도 적용되며, 이를 통해 프라이버시가 강화된 사람 중심의(user-centric) 스마트시티의 구현이 촉진될 것으로 기대

10 https://www.hitachi-systems-security.com/blog/an-introduction-to-smart-city-privacy/
11 예컨대 Harvard University Data Privacy Lab과 MIT의 연구진은 각각 공개된 데이터와 뉴스항목, 빅데이터와 이동성 관련 조사 등을 통해 개인정보의 재식별화가 가능하다는 것을 증명

Reference

1. Forbes, Are Privacy Concerns Halting Smart Cities Indefinitely?, 2019.1.8.
2. Government Europa, Smart city data protection under GDPR, 2018.11.16.
3. IDG, Why GDPR means Smart Cities need to move on from an 'Open Data' approach, 2018.2.1.
4. Intelligent Transport, Smart laws: exploring data and privacy regulation in smart cities, 2018.12.17.
5. NextGov, Report: Smart Transportation Systems Pose 'Profound' Privacy Risks, 2019.5.29.
6. Privacy News Online, Here's why Google thinks you should trust it with unprecedented quantities of your city's urban data, 2019.7.12.
7. Reuters, Alphabet commits to data privacy in Toronto smart city master plan, 2019.6.25.
8. SmartCitiesWorld, Sidewalk Labs releases principles of good street design, 2019.4.29.
9. South China Morning Post, Smart cities: are we sleepwalking into a Big Brother future of constant surveillance in the name of improved efficiency and safety?, 2018.8.15.
10. TechCrunch, Security lapse exposed a Chinese smart city surveillance system, 2019.5.3.
11. Trialog, Europe is working on privacy guidelines for smart cities, 2019.6.12.
12. Wired, Barcelona is leading the fightback against smart city surveillance, 2018.5.18.

2019년 7월

KISA 한국인터넷진흥원

KISA 한국인터넷진흥원

발 행 일 2019년 7월
발 행 및 편 집 한국인터넷진흥원 개인정보보호본부 개인정보정책기획팀
주 소 전라남도 나주시 진흥길 9 빛가람동 (301-2) Tel 1544-5118