https://doi.org/10.33778/kcsa.2020.20.3.099

코로나19 대응을 위한 책임 있는 디지털 기술의 활용 방안★

김 홍 준*, 엄 정 호**

요 약

신종 코로나 바이러스(SARS-CoV-2)로 인한 팬데믹이 확산되는 추세로 단기간 내 종식을 기대하기 힘든 상황이다. 디지털 기술의 활용은 코로나19 억제에 대해 가시적인 성과를 보여주고 있지만, 개인정보호호 측면에서는 논란이 되고 있다. 본 논문에서는 코로나19 팬데믹에 대한 우리나라 및 각국의 대응 현황을 살펴보고, 디지털 도구를 활용하되 개인정보를 보호하는 방향에 대해 제언한다. 팬데믹 억제를 위해서는 데이터 수집 및 처리가 필수적이지만 개인정보보호를 고려하여 꼭 필요한 수준과 범위로 제한해야 하고, 국제적 규모의 협력과 한시적이고 투명한 개인정보 이용, 이를 위한 법적·제도적 기반 확립이 필요하다. 오늘날 이 같은 데이터와 알고리즘 활용은 지속적으로 증가할 것이므로, 이와 더불어 개인정보보호를 위한 기술·제도적 보완 노력이 계속되어야 한다.

Responsible usage of digital technologies to manage SARS-CoV-2 pandemic

Hongjun Kim*, Jung Ho Eom**

ABSTRACT

The COVID-19 pandemic have been spreading continuously across the world, hence it is difficult to expect coming to an end in a short period of time. The use of digital technology has shown tangible results in suppressing COVID-19, but raised privacy and data-protection concerns. In the context of the global efforts to deal with the coronavirus pandemic, various digital technologies are taking on a role in surveillance, monitoring, and forecasting. Also the Korea government manages Corona crisis based on legal basis. In this paper, Korea and each country's response to the Corona 19 pandemic are shown, and suggests ways to protect personal information while using digital tools. Large-scale data collection and processing is essential for the suppression of pandemic, but it should be limited to the level and scope required privacy. Also international cooperation, temporary and transparent use of personal information, the corresponding legal basis are necessary. As the use of data and algorithms is expected to continue to increase, technical and institutional efforts to reinforce privacy protection must continue.

Key words : COVID-19, SARS-CoV-2, Privacy, Digital Contact Tracing

접수일(2020년 08월 20일), 수정일(2020년 09월 14일), 게재확정일(2020년 09월 27일)

★ 이 논문은 2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2019S1A5C2A03082827)

* 대전대학교 컴퓨터공학과 (주저자)

** 대전대학교 군사학과 (교신저자)

1. 서 론

2019년 12월, 중국에서 확산되기 시작한 신종 코로나 바이러스(SARS-CoV-2)와 이로 인해 발병하는 질병인 코로나 바이러스 감염증-19(코로나19)가 전 세계적으로 확산되고 있으며 감염 건수 또한 지속적으로 증가하고 있다. 우리나라는 다소 안정된 국면을 맞고 있지만, 중남미, 인도뿐만 아니라 미국, 유럽 등 선진국에서도 확진자와 사망자가 쏟아지고 있는 상황으로 현 추세로 보았을 때 단기간 내 종식을 기대하기 힘든 상황이다. 이에 따라 WHO (World Health Organization) 사무총장은 2020년 1월 30일, 코로나19로 인한 국제적 공중 보건 비상사태(PHEIC, Public Health Emergency of International Concern)로 선언하였다. 코로나19 이전에 유발된 국제적 공중 보건 비상사태인 2002년 SARS와는 비교가 힘들 정도로 감염자를 많이 발생시키고 있다.

코로나19 바이러스 팬데믹에 대응하기 위한 전 세계적인 노력 중에서 디지털 기술의 활용은 즉각적이고, 가시적인 결과를 보여준다. 하지만, 개인정보보호 측면에서는 지속적으로 논란이 되고 있다. 각국은 바이러스 확진자의 위치 추적을 통해 동선을 파악하고 의료 데이터를 수집하는 등의 대처로 바이러스 확산을 차단하는데 효과를 보고 있지만, 근본적으로 개인정보호호의 권리와 국가의 공공 이익 추구가 상충됨에 따라 정보보호 측면에서 개인정보가 남용되고 있지 않은가에 대한 논의도 끊임없이 제기되고 있다.

코로나19는 스마트폰, 빅데이터, 인공지능 시대 최초의 팬데믹으로 이에 대처하기 위한 디지털 도구들의 급격한 확산을 초래하고 있다[1]. 이를 통해 물리적 거리와 검역 조치를 모니터링하고, 접촉 추적과 감염 클러스터의 탐지를 용이하게 한다. 초기 인류시대부터 2003년까지 생산된 데이터의 양은 오늘날 몇 분 안에 생성되고, 이를 기반으로 한 기계학습 모델링은 감염원을 추적하거나 미래 확산을 예측하는 데 큰 잠재력을 갖고 있다[2]. 특히 코로나19와 같이 신규 병원체로 인한 발병의 경우, 공식적인 데이터가 부족하고 신뢰할만한 수준의 예측이 불가능하기 때문에, 휴대전화 및 기타 디지털 장치로부터 수집되는 디지털 데이터가 중요한 가치를 지닌다. Wu[3]는 WeChat 어플리케이션과 Tencent의 디지털 서비스로부터 얻은 개인의 이동 데이터를 결합하여 코로나 확산 예측 모델의 가능성을 보여준 바 있다. 또한, 휴대전화 데이터는 이미 2010년 아이티 콜레라 전염병 사태 때 이를 통한 확산 예측에 도움이 된 바 있고[4], 2014년~2016년 서아프리카 에볼라 전염병 사태 때는 빅데이터 분석의 효과를 충분히 보여주었다[5].

본 논문은 팬데믹 억제를 위한 디지털 도구 사용 및 기술, 그리고 개인정보활용을 위한 법적·제도적 기반과 관련된 국내·외 현황에 대해서 우선 기술하고, 개인정보보호를 위한 법적·기술적 방향의 정책을 4가지로 제언한다. 2장에서 코로나19 대응을 위한 디지털 도구와 기술의 활용으로 개인정보호호 측면에서 발생하는 문제점들과 그에 대한 분석 내용에 대해 기술하고, 3장에서는 이 같은 문제의 해결을 위한 기술·제도적 접근 방법과 그 현황에 대해 다룬다. 4장에서 책임 있는 디지털 기술 활용 방안들을 제시하고, 5장에서는 결론과 함께 향후 전망을 기술한다.

2. 개인정보보호 문제 제기와 분석

최근 수천만 명의 사용자, 특히 통화 데이터 기록 및 소셜 미디어의 대규모 데이터 수집으로 인해 개인정보 및 데이터 보호문제가 제기되고 있다. 코로나19는 전염병이 강한 질병으로 앞으로 수십억 명의 사람들을 감시해야 할 상황에 놓이게 될지도 모르는 상황이므로 그 중요성은 점점 더 커지고 있다. 특히 2020년 현재는 데이터 집약적 시대로 유비쿼터스 환경에서 수집되는 데이터 및 디지털 감시 도구는 개인정보보호 문제를 쉽게 약화시킬 수 있다. 뉴욕타임즈 보고서[6]에 따르면, 수집된 데이터가 감시 목적을 달성하기 위해 어떻게 교차 확인되고, 재사용되는지 투명하지 않으며, 한 예로 알리바바가 제작하고 정부가 운영하는 Alipay Health Code를 들고 있다. 이는 누구를 격리해야하는 지에 대한 의사결정을 지원하고, 경찰과 그 정보를 공유하는 것으로 보인다.

과도한 정보 수집과 처리의 불투명성은 많은 사람들에게 공포감을 심어줌과 동시에 삶의 질 저하로 이어질 수 있다. 데이터를 수집하는 일부 국가 및 관련 기관에서는 개인정보가 익명화되어 있어 특정 개인을 추적할 수 없고, 바이러스 예방을 위해 필수적

인 데이터만을 사용할 것이라 주장하지만, 중국, 싱가포르, 이스라엘과 같이 무분별하게 데이터를 수집하는 행위는 사람들에게 상당한 공포감을 야기한다. 페이스북의 경우에도 팬데믹 대처를 돕기 위해 몇몇 국가에 분석된 데이터를 보냈고, 정부에 따라 그 데이터에 지나치게 접근하여 개인의 삶의 질을 저하시킬 수 있다.

세계 어느 곳에서든 개인정보에 대한 권리는 절대적이고, 어떠한 상황에서도 어겨져서는 안 되기 때문에, 비록 코로나19 대응에 있어 예측과 감시를 위한 디지털 데이터와 알고리즘이 가장 중요하다하더라도 이를 책임감 있게 사용하는 것이 무엇보다 중요하다. 해당 데이터에 대한 제공 동의 여부가 불명확하고, 데이터를 제공하는 기관의 투명성이 부족하면 문제가 될 수 있다. 따라서 데이터 수집 및 처리 조건이 명확해야 하고, 개인정보보호 및 기밀유지를 위해 데이터 보호규정을 준수해야 한다. 그렇지 않으면, 대중의 신뢰가 약해져 사람들이 공중보건지침이나 권고를 준수하지 않게 될 것이며, 그에 따른 상황은 더 악화될 수 있다.

우리나라는 메르스 대응 초기에 나타난 문제점을 고려하여 2015년 7월 6일, '감염병의 예방 및 관리에 대한 법률'을 개정, 팬데믹에 대응하기 위한 개인정보 수집의 법적 근거로 삼고 있다[7]. 국가 및 지방자치단체의 책무를 확대하는 내용과 함께 감염병 예방 및 관리를 위한 정보시스템 구축에 대한 내용이 추가되었다. 또한, '재난 및 안전관리 기본법' 제38조 제2항에 의거하여 주의 이상의 위기경보가 발령되는 경우, 감염병 환자의 이동경로 및 수단, 진료의료기관, 접촉자 현황 등 국민들이 감염병 예방을 위하여 알아야하는 정보를 정보통신망 게재 또는 보도자료 배포 등의 방법으로 신속히 공개하여야 한다.

이러한 법적 근거에도 불구하고, 정부가 공개하는 정보들로부터 어렵지 않게 확진자의 신원 유추가 가능하여 개인정보보호 문제가 발생한다. 심각한 건강상의 문제를 일으키지 않을 때, 사람들은 바이러스 자체를 두려워하는 만큼 혐오 시선도 두려워하기 때문에 은폐의 가능성이 높아지게 된다. 또한, 정보 공개로 인한 사생활 침해와 영업 손실에 대한 불만은 계속 존재하고, 공개하는 정보의 범위는 역학적 매개변수를 감안하여 계속 변경될 수 있기 때문에 개인정보보호에 한계가 있다는 것은 여전히 딜레마일 수밖에 없다. 월스트리트 저널[8]에 따르면, 한국, 싱가포르, 홍콩, 영국, 그리고 독일 등이 공개하는 접촉자 정보 비교 결과, 한국 정부가 가장 많은 유형의 개인식별정보를 공개하고 있는 것으로 밝혀졌다. 또한, 보건소 직원들이 문건을 주고받는 과정, 인터넷 카페, 확진자 관련 정보를 취급하는 경찰 등 여러 가지 경로를 통해 확진자뿐만 아니라 의심환자의 주소, 나이, 성별, 성씨, 동선 등의 개인정보가 유출되는 사례가 발생하여 '사회적 낙인' 등 2차 피해로 이어지고 있다. 그러나 영리 또는 부정한 목적을 가지고 개인정보를 제공받았다고 해석하기 어렵기 때문에 개인정보보호법 위반으로 처벌하긴 어렵다[9].

팬데믹 관련 디지털 통제는 정부에 대한 불신이 높아지고 있으며, 이는 정부에 대한 국민들의 낮은 신뢰도를 보이고 있는 이탈리아, 프랑스 및 미국과 같은 국가에서 뚜렷하게 나타나고 있다. 특히 정부기관이 수집한 개인정보의 유출을 경험한 사람이 많은 중국의 경우, 특정 지역 출신이라는 개인정보가 감시나 차별로 이어지기도 한다.

또한, 원격회의, 교육, 진료가 급격히 증가함에 따라 화상회의 프로그램의 사용이 확대되고, 이로 인해 회의정보보호 이슈도 발생한다. 온라인 화상 프로그램 중 하나인 'zoom'을 이용하는 사람들이 급격하게 늘어남에 따라 해커들의 주요 공격 대상이 되면서 전화를 대신 받거나 이를 통해 개인정보를 얻는 등의 문제가 생기고 있다. 온라인 화상회의로 인한 사생활과 정보보안의 위협은 'zoombombing'이라 불리며, FBI는 이와 관련한 위협을 알리는 보도 자료를 발표하기도 하였다.

3. 코로나19 대응을 위한 기술·제도적 접근

3.1 제도적 접근

국내 정부 기관들은 코로나 감염자의 움직임을 감시하게 위해 감시 카메라, 모바일 위치 데이터, 신용카드 결제 기록 등을 사용하고 있다. 개인정보보호법에 따라 민감정보는 원칙적으로 그 처리가 제한되지만, 공공의 안전을 위해 긴급히 필요하여 일시적으로 개인정보를 처리하는 경우, 제58조에 의거하여 제3

장부터 제7장까지를 적용하지 않는다[10]. 또한, 개인정보처리 주체가 정부나 공공기관 또는 일반 개인정보처리자인지를 구분하지 않고 있다. 특히 개인정보를 '일시적'으로 처리한다는 의미가 불명확하기 때문에 공공의 안전과 안녕을 위한 경우라면 필요 이상의 장기간 수집, 보관, 처리를 효과적으로 제한할 방법이 없다. 정보 수집 및 이용 동의 또한 민감정보를 일반 개인정보와 구분하지 않음으로써 제58조에 의해 동의절차가 생략되는 경우 민감정보를 특별히 더 보호해야 한다는 취지가 무색하게 된다. 이처럼 공익적 목적에서의 건강정보 처리에 대해 정보주체의 권리 행사를 포괄적으로 배제하는 것은 긴급한 상황에서의 적시적이고 효과적인 대처를 가능하게 하는 반면, 공익이라는 이름으로 개인의 개인정보보호 권리를 제약하는 것을 당연시 할 수 있다는 문제점이 존재한다.

유럽 연합은 개인정보보호 법령인 GDPR (General Data Protection Regulation)을 2018년 5월 25일부터 시행하고 있으며 공중 보건을 위한 개인정보처리를 '특별한 유형의 개인정보처리'로 규정한다. 한국의 개인정보보호법 제58조와 같은 포괄적 법 적용 배제 규정을 두지 않아 정보주체의 권리 및 처리되는 특별한 유형의 개인정보의 보호 등이 그대로 적용된다. 또한, 유럽 데이터 보호위원회는 코로나19 대응 시 사용되는 개인정보보호의 중요성에 대한 성명을 발표하여 데이터 보호 규정의 특정 조항을 명시하였다. 한국과 마찬가지로 공중보건 분야에서 공공의 이익을 위한 경우에만 개인정보처리를 허용하되 그러한 처리가 추구하는 목표에 상응하고, 데이터 보호 및 보호권에 대한 권리의 본질을 존중하며, 데이터 주체의 권리와 자유를 보호해야 한다고 명시한 바 있다.

미국은 코로나 바이러스로 인해 환자가 자신의 개인 기록을 의료 제공자와 공유하는 것을 방지하도록 하는 법률(HIPPA)을 완화하여 비상사태에서는 위험이 확대되지 않도록 필요한 데이터를 합리적으로 사용하고 공개할 수 있도록 조정하였다. HIPPA 규정의 적용을 받는 보호 의료 제공자는 의료용 zoom과 skype와 같은 소프트웨어를 사용하기도 하지만, 코로나 바이러스가 빠른 속도로 확산되며 HHS (Health and Human Services)라는 화상 채팅 애플리케이션을 개설하기로 협의하였다. 이에 따라 고용주들은 사업장에서 확진자가 발생했을 경우, HIPPA와 같은 권한을 부여받는데, 감염의 예방을 위해서라면 다른 노동자들에게 정보를 공유할 수 있다. 이는 위치, 질병, 혹은 고용자나 그의 아이의 죽음, 가족관계 등을 포함한다. 미국 내 학생 데이터의 개인정보보호를 위해 학생교육 기록을 보호하는 FERPA 연방법 또한 비상사태의 경우, 교육기관 및 대학이 사전 서면 허가 없이 학생 교육기록부에서 이름, 식

Table 1 Country level data protection and management guidelines

국가	개인정보보호관련 법률	예외 조항(법률)	특징
대한민국	개인정보보호법	개인정보보호법 제58조, 감염병의 예방 및 관리에 관한 법률 제4조 14-17항, 재난 및 안전관리 기본법 제38조 2항	개인정보보호법 제58조에 의거하여 제3장에서 제7장까지를 적용 배제
유럽	일반정보보호규정(GDPR)	GDPR 제9조(특별한 유형의 개인정보 처리)	공중보건 영역에서 공익을 위하여 필요한 경우를 민감정보 처리가 가능한 경우로 규정
미국	프라이버시법(The Privacy Act of 1974)	의료정보보호법(HIPPA), FERPA연방법	공공 부문과 민간 부분을 포괄하는 종합적인 법률은 존재하지 않고, 연방 및 주 단위로 프라이버시 보호관련 법률이 존재

별번호 등 개인의 신원을 구별하거나 추적하는 데 사용할 수 있는 정보를 보건기관에 보고할 수 있다. FERPA의 예외조건에 따르면, 학생이나 다른 사람에게 위험이 되는 상황일 경우, 특정 학생을 식별하지 않는 방식으로 당사자의 동의 없이 본인의 개인정보를 관련 기관에 제공할 수 있도록 하고 있다.

3.2 기술적 접근

팬데믹 위기 억제와 함께 우리에게 많은 편의성을 제공하는 위치 기반 서비스(LBS, Location Based Service)의 경우, 네트워크 트래픽 흐름을 모니터링하여 역추적하거나, 공통 센서 노드를 손상시키고, 데이터 패킷의 정보를 분석함으로써 소스 노드의 실제 위치를 쉽게 찾을 수 있다[11]. 따라서 공격 시나리오를 예상하고, 소스 위치를 보호하는 여러 가지 방법들에 대한 연구들이 이루어지고 있다. MIT Media Lab.[12]의 한 연구진은 코로나19 대응 솔루션의 개인정보보호를 위해 데이터 수집, 데이터 변환, 안전한 데이터 교환, 위험 평가 및 알림 단계로 개인정보를 처리하는 시스템을 제안하였다.

1단계(데이터 수집): 앱이 설치된 핸드폰 사용자의 GPS 위치 정보를 매 분마다 시각과 함께 저장하고, 이렇게 저장된 일련의 GPS 위치 점들은 사용자의 위치 이력을 나타낸다.

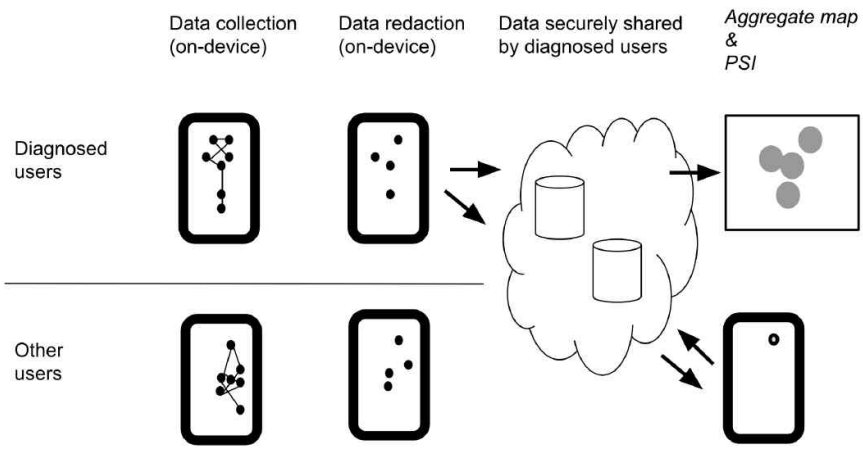
2단계(데이터 수정 및 변환): 개인정보를 보호하기 위해 수집된 데이터를 변환 및 암호화한다. 이러한 데이터는 질병 전파 기간이 지나면 해당 장치와 서버 모두에서 삭제된다.

3단계(안전한 데이터 교환): 클라이언트 역할을 하는 모바일 앱은 지정된 서버와 보안 채널을 설정하고, 이 보안 채널 내에서 지정된 지역에 대해 선택한 기간 동안 확진자의 이동 데이터를 요청한다. 서버가 소유한 확진자의 이동 데이터는 2단계를 통해 개인식별정보를 포함하지 않으며 PSI (Private Set Intersection) 프로토콜을 통해 확진자와 다른 사람 간의 이동 경로가 일치하는 지 찾는다.

4단계(위험 평가 및 통지): 확진자와 이동 경로가 일치하는 경우, 앱은 사용자에게 위험을 알리고, 진단 및 자가 격리를 권장한다. 또한 선택적으로 확진자와 일치하는 경로 및 지점을 사용자에게 표시한다.

또한 독일의 FZI 연구센터[13]는 중앙 집중방식과 분산방식의 이중적 접근을 통해 개인정보보호를 강화하는 방법을 발표하였고, Demirag와 Ayday[14]는 보건 기관(서버)과 개인(클라이언트) 사이의 APSI (Authorized Private Set Intersection) 기반 프로토콜을 연구하는 등 지속적으로 개인정보보호권을 침해하지 않는 방법들에 대한 연구들이 수행되고 있다.

전 세계 국가들의 코로나19에 대한 기술적 접근 현황을 살펴보면, 우선 싱가포르, 중국, 한국 등 아시아 국가들이 디지털 도구들을 빠르고 효율적으로 사



(Fig.1.) High-level schematic showing the major steps in the system's process for privacy-preserving contact tracing[12]

용하기 시작하였고, 유럽은 이를 모델로 삼고 있다. 이와 동시에 데이터 보호 및 기본적인 개인 권리에 대한 우려는 고려되지 않았다는 회의론도 존재한다. 전염병 및 기술 거버넌스를 다루는 경험에서 유럽과 미국, 아시아의 근본적인 차이점은 존재하고, 위기 대응을 위한 디지털 기술의 사용 측면에서도 단순히 기술뿐만 아니라 정치, 경제, 그리고 사회 간의 복잡한 상호 작용을 반영한다.

코로나19 바이러스가 시작된 중국은 전염병을 억제하기 위해 디지털 기술을 광범위하게 사용하고, 불투명한 데이터 수집 및 처리를 통해 시민들을 제어하고 있다. 체온을 측정하는 동안 공공장소에서 얼굴을 인식하기 위해 적외선 기술과 결합하여 얼굴인식 소프트웨어를 배포하는가 하면, 개인정보를 기반으로 개개인의 건강상태를 인코딩하는 기능을 Alipay, WeChat과 같은 보편적으로 많이 사용하는 애플리케이션에 포함시켜 이 결과를 녹색, 노란색, 혹은 빨간색 QR코드로 표현한 후 개인의 이동을 제한한다. 각각의 색상 코드가 어떻게 결정되는지, 누가 접근할 수 있는지, 추후 이 데이터가 어떻게 활용되는지 불명확하다. 이는 중국 내 감시 정책이 확장되고 있는 한 예에 불과하며, 이러한 조치들이 언제 해제될지 알 수 없을 뿐만 아니라 합법적인 목적으로 수집된 데이터가 향후 다른 정치적, 경제적 목적으로 사용될 가능성이 존재한다.

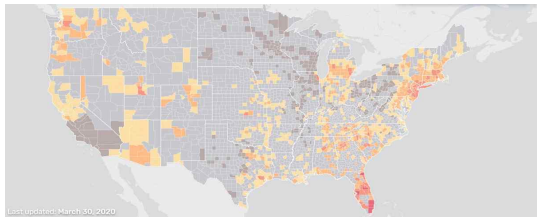
싱가포르는 강력한 사회적, 기술적 제한 정책을 통해 바이러스 확산을 억제하고자 노력한다. 신속한 대응과 공항 상태 점검, 엄격하게 강제되는 거리두기 규칙, 그리고 광범위한 검진 등을 통해 2020년 3월말까지 코로나19 바이러스를 성공적으로 제어하기 위한 모델로 간주되었지만, 이후 사회 및 정치적 취약계층인 외국인 이주 노동자들 사이에 감염자 수가 급격히 증가하여, 현지 인구의 감염 건수가 적음에도 불구하고 공공생활과 경제에 대한 폐쇄조치를 다시 취하고 있다. 싱가포르의 초기 성공 요인 중 하나는 아날로그와 디지털 측정을 결합한 엄격한 추적 정책이다. 국민들의 신기술에 대한 높은 수준의 수용 경향에도 불구하고, 자발적 애플리케이션 사용은 약 20% 수준에 불과하므로, 엄격한 수동 접촉 추적 정책을 보완하여 감염자들의 격리를 모니터링 하는데 이용된다.

외신에서 바라본 한국과 대만은 과거의 2015년 메르스나 2003년 사스 팬데믹의 경험을 통해 빠르게 코로나19에 대응하고 있는 것으로 보도되고 있다. 양국은 싱가포르와는 달리 비상 상태를 선포하거나 사회와 경제생활을 포괄적으로 폐쇄하지 않았다. 또한, 중국을 오가는 여행자들이 상대적으로 많음에도 불구하고, 세계 보건기구(WHO)의 대면 감염 가능성 확인을 기다리지 않고 중국의 고위험 지역 여행자들을 위한 검역조치를 취하여 빠르게 대응하였다.

특히 한국은 2015년 메르스 팬데믹 당시 감염자들의 소재 정보를 공개하지 않은 것을 크게 비판받았고, 그 결과 전염병 대처 정책을 세울 때 투명성과 개방성을 기반으로 한 전략을 수립하였다. 그 전략에는 감염자의 이동 경로 정보를 게시하고, 격리된 모든 개인의 위치에 대한 정보에 접근할 수 있게끔 하는 정책이 포함된다. 보건복지부는 감염 추적을 위해 개인 정보를 요청하여 사용하고, 자동화 플랫폼을 통해 데이터 교환을 하며, GPS가 부착된 웨어러블 디바이스를 통해 추적하고 모니터링하고 있다.

대만은 대중의 불신을 불러일으키지 않고, 빅데이터 분석을 통해 코로나19에 대처하는 유망한 방법을 보여준 바 있다[15]. 건강보험 데이터베이스를 세관 데이터베이스의 여행 이력 데이터와 통합하여 사례 식별을 수행하고, QR코드 스캔 및 온라인 보고를 통해 바이러스 감염 억제를 추진한다. 그리고 이러한 조치들은 빈번한 건강검진 및 검역 대상자에 대한 격려를 포함하여 공공커뮤니케이션 전략과 결합하여 수행된다.

한편, 유럽은 국가들마다 다양한 선호도를 바탕으로 여러 가지 접근 방식을 적용한다. 메르스 및 사스 팬데믹에 대한 경험이 적었기 때문에 팬데믹 대응 정책들이 낮은 치사율을 보이는 감염병을 대상으로 설계되었을 뿐만 아니라 기술 거버넌스 및 의료 정



(Fig.2.) Kinsa, US Health Weather Map (March 30, 2020)

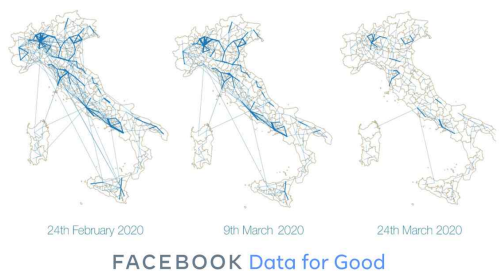
책에서 개인정보보호를 중요하게 생각하는 경향이 있다. 아직도 범 유럽적인 접촉 추적 애플리케이션의 개발 및 배포에 대한 논쟁이 계속되고 있으며, 개인정보가 스마트폰에 저장·관리되는 분산 솔루션을 선호하는 집단과 중앙서버에 저장하는 중앙 집중식 솔루션을 선호하는 집단 간 분쟁도 일어나고 있다. 독일의 경우, 중앙 집중식 솔루션의 데이터 저장 및 처리에 대한 사회적 우려 때문에 초기에 선정하였던 중앙 집중식 솔루션을 버리고 분산 솔루션을 적용하고 있다.

파리 지하철에서는 사람들이 마스크를 쓰고 있는지 확인하기 위해 얼굴 인식 소프트웨어를 사용하고 있고, 폴란드에서는 검역 애플리케이션에 얼굴인식기능을 추가하였으며, 리히텐슈타인에서는 추적용 손목밴드를 사용하여 시범 프로젝트를 진행하는 등 각국에서 디지털 도구들을 사용하여 바이러스 확산 억제를 위해 노력하고 있다. 정부와 대학이 협력하고 있는 한 예로 옥스퍼드 대학과 영국의 보건 서비스 디지털 혁신 부서는 다양한 연령층, 가정 유형, 이동 패턴 등을 고려하여 접촉 추적 애플리케이션을 제작한 바 있다[16].

미국은 구글, 애플, 페이스북 등 거대 기업들과 고객 데이터를 활용해 코로나가 퍼지지 않게 하는 방안을 놓고 협의하고, 백악관과 질병통제예방센터에서는 개인의 위치정보에 접근할 수 있는 권리를 주도록 요구하고 있다. 또한, 'Kinsa Health'는 스마트 온도계의 데이터를 활용해 인플루엔자의 발생률을 확인 및 예측할 수 있고, 코로나19 바이러스 지도도 확인이 가능하도록 제공하고 있다. 페이스북의 'Data for Good' 플랫폼은 통계 데이터를 사용하여 질병 예방 지도를 지원하고, 보건 기관들이 질병 전염을 감시하며 사람들이 어떻게 이동하는 지 예측하는 것을 돕는다. 페이스북은 유저들과 직접적인 방법으로 정보를 주고받는 데 비해[17], Unacast는 제3자로부터 많은 데이터를 제공받고 있고, 이는 Unacast의 공급업체뿐만 아니라 애플리케이션에 넣는 소프트웨어 개발 키트 즉, SDK도 포함한다. Unacast는 휴대폰 위치 데이터를 수집하고 분석하여 소매, 부동산, 마케팅, 관광 산업 등에 데이터를 제공하는 회사로 최근 사회적 거리 점수판이라는 것을 공개하여 미국의 각 주가 얼마나 사회적 거리 두기를 하는 가에 대해 등급을 부여한 바 있다. 소비자들은 어떤 애플리케이션이 해당 SDK를 사용하는 지 알 수가 없으므로 애플리케이션 이용 시 허가해야 하는 권한 중 하나인 위치 정보를 제공하는 권한을 넘겨주게 되면 자신의 위치 데이터가 Unacast로 제공되게 된다. Unacast뿐만 아니라 다른 많은 회사들도 이런 형태의 데이터를 수집하고 있으며, 이러한 데이터 처리를 금지하는 연방 규정이 존재하지 않기 때문에 지속적인 사생활 침해가 발생할 가능성이 높다.

그 밖에도 대테러 용도를 위해 익명으로 수집한 휴대폰 데이터를 코로나 감염자 색출하는 데 이용하는 이스라엘과, 코로나 치료를 위한 애플리케이션을 출시하여 정부가 수백만 명의 위치 정보를 수집하고 감시하는 용도로 이용하는 이란 등 각국은 다양한 방법으로 디지털 도구를 활용하고 이에 따른 개인정보보호 문제가 존재한다.

운영체제 간 호환성은 블루투스를 통한 효과적인 디지털 추적을 위한 전제 조건[18]이기 때문에 구글과 애플의 독점적 시장 지배 등 개인정보보호 문제 외에도 민간 기업의 경제적, 정치적 영향에 따라 각국의 정책들이 결정되기도 한다. 구글과 애플은 초기에 분산된 접근 방식을 지지했으며, 이를 전제로 한 프로그래밍 인터페이스를 개발하였다. 이러한 이유로 영국 또한 중앙 집중식 보다는 분산 솔루션을 고려하고 있다. 이에 반해 프랑스는 중앙 집중식 솔루션을 고수하고 있으며, 두 회사가 이를 위해 협조하도록 압박한다.



(Fig.3) Data for Good: Facebook's platform for analyzing data on COVID-19

4. 책임 있는 디지털 기술 활용 방안

대규모 데이터(large-scale data) 수집은 팬데믹을 억제하는 데 도움이 될 수 있지만, 개인정보보호 및 대중을 무시하는 경우, 정책에 대한 불신으로 인해 그 효과가 떨어질 수밖에 없다[19]. 따라서 개인정보보호를 고려한 제도 및 정책적 접근, 기술적 접근 그리고 국제적 협력을 통해서 적절히 디지털 기술을 활용하도록 해야 한다.

따라서 책임 있는 디지털 기술 활용 방안을 다음 4가지로 정리하여 제언한다.

1. 공중 보건 위협의 심각성에 비례하여 꼭 필요한 수준으로 데이터 수집 범위를 제한한다.

2. 국제적 규모의 데이터 수집 및 모범 사례 공유 등의 국제적 협력을 추진한다.

3. 한시적이고 투명한 개인정보 이용·처리와 이를 위한 법적·제도적 기반을 확립한다.

4. 개인정보보호권을 유지하기 위해 새롭게 등장하는 디지털 (보안)기술을 활용한다.

4.1 제도 및 정책적 방안

코로나19 대응을 위해, 사회는 공공의 이익과 개인의 기본권 사이, 정부의 행동과 개인의 책임 사이에서 어려운 균형적 역할을 수행해야 한다. 특히 국가가 수집하게 되는 개인정보에는 감염된 사람들의 사회적 상호 작용 및 움직임에 대한 정보가 포함될 수 있으므로 책임감 있게 처리해야 한다. 911테러 이후 미국 전역에 카메라와 네트워크가 확산되고, 제정된 미국 애국자법(Patriot Act)을 통해 국가의 광범위한 감시 체계가 시작되었듯이, 팬데믹 위기가 지나간 후에도 코로나19 대응을 위해 도입되었던 감시기술이 일상생활에 내재될 가능성도 적지 않으며, 이는 곧 정부가 수많은 사람들을 감시하는 상황을 초래할 수 있다. 정부는 싱가포르와 이스라엘과 같이 국민들의 개인정보를 광범위하게 수집하고 이를 공개하는 극단주의에 맞서야 하고, 개개인의 디지털 삶을 유지하기 위해 모든 기기는 일반인들이 신뢰할 수 있는 수준으로 개인정보가 보호되도록 보장할 필요가 있다.

데이터 관리 정책은 데이터 수집과 처리 모두를 통제해야 하고, 선택적인 데이터 수집, 한시적이고 투명한 개인정보 이용과 그 타당성 확보에 힘써야 한다. 데이터 수집의 범위는 공중 보건 위협의 심각성에 비례하고, 특정한 공중 보건의 목적을 달성하기 위해 필요한 수준으로 제한되어야 한다. 또한, 개인 식별이 가능한 정보를 수집하는 디지털 추적 조사 기술은 그 필요성이 과학적으로 정당화되어야 한다. 대중에게 공개되는 정보의 유형은 발생지역에 대한 시간과 장소 등 가능한 최소 내용으로 해당 목적 범위 내로 제한하여 과도한 정보의 공개를 지양하고, 보건 당국은 사용자 스스로 자신의 휴대폰에 자발적으로 애플리케이션을 설치할 수 있도록 하는 등의 소통을 해야 한다. 공공의 안전을 위한 긴급성 판단 기준과 절차를 정하여, 신속하고 합법적인 결정이 이루어질 수 있도록 해야 한다. 이들을 모두 충족하는 대안의 한 예로 익명화된 모바일 위치 데이터를 사용하는 방법이 있을 수 있다.

데이터 처리 시에는 데이터의 품질 및 보안 제어가 필요하다. 개인용 디지털 장치로부터 발생하는 데이터가 사용될 때 흔히 발생하는 데이터 무결성 문제는 하나 이상의 요인으로 작은 오류를 유발할 수 있으며, 이는 대규모 예측 모델에 과도한 영향을 줄 수 있기 때문이다. 더 나아가 데이터 유출, 불충분하고 비율적인 개인 식별 정보 제거, 데이터 셋의 치우침(biases)은 공중 보건 서비스의 불신을 초래하는 주요 원인이 될 수 있다. 따라서 데이터의 접근과 사용 시 이를 공개하여 투명한 소통 정책이 펼쳐져야 한다.

4.2 기술적 접근 방안

기술적 접근은 일정 기간 동안 같은 경로를 지나간 사람을 추적하는 방식을 적용하는 밀접 접촉자 추적 모니터링 애플리케이션의 익명화, 자발적인 애플리케이션 설치 및 암호 업데이트, 애플리케이션 사용자의 위치정보의 암호화, 한시적 작동, 동의에 의해서만 공개되는 정보 등을 통해 개인정보보호권을 유지하면서 위치정보가 신호정보로 동선을 파악할 수 있는 블루투스, GPS와 같은 디지털 기술을 활용하는 것이 필요하다.

4.3 국제적 협력 방안

국제적 규모의 책임 있는 데이터 수집 및 처리 표준을 위해 모범 사례를 식별하고 이를 공유하는 등의 국제적 협력이 요구된다. 코로나19 바이러스의 큰 불확실성으로 인해 대책에 대한 효과는 지속적으로 모니터링 되고, 변화하는 상황에 따라 전반적인 전략에 맞추어 조정되어야 하므로 지역의 사회·경제적 영향 등에 따라 다양한 방식을 적용하고 있는 각국의 우수 사례를 공유하고, 이를 확산시켜야 한다. 또한, 데이터 보호 및 교환 시 사용하는 국내 및 국가간 표준 솔루션이 필요하고, 특히 개인정보에 대한 국제적 협력 및 협의는 민간 기업을 포함하여 진행되어야 한다.

5. 결론 및 향후 전망

종식기미를 보이지 않고 있는 코로나19대응을 위해 디지털 기술은 전 세계적으로 활용되고 있으며, 이에 따라 공공의 이익과 개인정보보호권의 상충 문제는 지속적으로 제기되고 있다. 미국, 유럽, 그리고 아시아 각국의 대응 현황을 기술·제도적 측면에서 살펴보고, 개인정보보호를 고려한 디지털 기술 활용 방안에 대해 기술하였다.

정보 주체의 자율적 동의를 통한 선택적 데이터 수집, 획득된 데이터의 한시적 사용, 이들을 위한 명문화와 법제도의 보완, 익명화 및 암호화를 위한 기술적 지원, 그리고 투명성 확보가 이루어진다면 코로나19와 앞으로 있을 새로운 팬데믹에 대응하여 개인정보보호를 고려한 디지털 기술의 효율적인 사용이 가능할 것이다.

점점 더 많은 국가들이 디지털 기술을 이용하여 진행 중인 코로나19 팬데믹에 대응하게 될 것이고, 데이터와 알고리즘은 우리가 가지고 있는 도구 중 가장 좋은 것이므로 개인정보보호를 위한 기술적, 제도적 보완노력이 계속해서 더해질 것으로 예상된다.

참고문헌

[1] S.-C. Fischer, K. Kohler, and A. Wenger, “Digital Technologies in Corona Crisis Management,” CSS Analyses in Security Policy, Vol. 264, pp. 1-4, 2020.

[2] S.V. Scarpino and G. Petri, “On the predict ability of infectious disease outbreaks,” Nature Communications, Vol. 10, pp. 1-8, 2019.

[3] J.T. Wu, K. Leung, and G.M. Leung, “Now casting and forecasting the potential domestic and international spread of the 2019-nCoV outbreak originating in Wuhan, China: a modelling study,” The Lancet, Vol. 395, pp. 689 - 697, 2020.

[4] L. Bengtsson et al., “Using Mobile Phone Data to Predict the Spatial Spread of Cholera,” Scentific Reports, Vol. 5, pp. 1-5, 2015.

[5] M. Bates, “Tracking Disease: Digital Epidemiology Offers New Promise in Predicting Outbreaks,” IEEE Pulse, Vol. 8, pp. 18 - 22, 2017.

[6] P. Mozur, R. Zhong, and A. Krolik, The New York Times https://www.nytimes.com /2020/03/01/business/china-coronavirussurveillance.html, 2020.

[7] M. Park, “COVID-19 contact tracing and Privacy,” BRIC View 2020-TX6, pp. 7-15, 2020.

[8] L. Lin and T.W. Martin, “How Coronavirus is Eroding Privacy,” The Wall Street Journal, Apr. 2020.

[9] S.J. Jung, “Legal Review and Suggestion for Investigation of Violations of Personal Information Protection Act,” Korean Journal of Public Safety and Criminal Justice, Vol. 29, No. 1, pp. 231-254, 2020.

[10] J. Lee, “Remarks on Corona Virus and Processing of Personal Information-Is it always right to use personal information for a variety of purpose?,” KISA REPORT, Vol. 2, pp. 6-11, 2020.

[11] J. Jiang, G. Han, H. Wang, and M. Guizani, “A survey on location privacy protection in

Wireless Sensor Networks," Journal of Network and Computer Applications, Vol. 125, pp. 93-114, 2019.

[12] A. Berke et al., "Assessing Disease Exposure Risk with Location Data: A Proposal for Cryptographic Preservation of Privacy," https://arxiv.org/pdf/2003.14412, 2020.

[13] W. Beskorovajnov et al., "Contact Tracing against the Coronavirus by Bridging the Centralized - Decentralized Divide for Stronger Privacy," pp. 1-29, 2020.

[14] D. Demirag, E. Ayday, "Tracking and controlling the spread of a virus in a privacy-preserving way," pp. 1-7, 2020.

[15] C.J. Wang, C.Y. Ng, and R.H. Brook, "Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing," JAMA;The Journal of the American Medical Association, https://doi.org/10.1001/jama.2020.3151, 2020.

[16] S. Talukder, Md.I.I. Sakib, and Z. Talukder, "Giving Up Privacy For Security: A Survey On Privacy Trade-off During Pandemic Emergency," International Journal on Cryptography and Information Security, Vol. 10, No. 3, 2020.

[17] S.Talukderand and B.Carbunar, "A study of friend abuse perception in facebook," ACM Transactions on Social Computing, Vol. 1, No. 1, 2020.

[18] G. Yaron, "Security analysis of the covid-19 contact tracing specifications by APPLE INC. and GOOGLE INC.,", 2020.

[19] M. Lenca and E. Vayena, "On the responsible use of digital data to tackle the COVID-19 pandemic," Nature Medicine, Vol. 26, pp. 463-464, 2020.

〔저자소개〕

김 홍 준 (Hongjun Kim)
2004년 2월: 한국과학기술원 전자전산학과 학사
2007년 2월: 한국과학기술원 전자전산학과 석사
2014년 2월: 한국과학기술원 전기및전자공학과 박사
2014년 2월~2015년 4월: 삼성전자 S/W Lab. 책임연구원
2015년 5월~현재: 대전대학교 컴퓨터공학과 조교수
email : hjkim99@dju.kr
<관심분야> 이동로봇, 건전성관리시스템, 기계학습

엄 정 호 (Jung-ho Eom)
1994년 2월 공군사관학교 항공공학과 학사
2003년 2월 성균관대학교 전기전자 및 컴퓨터공학과 석사
2008년 2월 성균관대학교 컴퓨터공학과 박사
2011년 3월~현재 대전대학교 군사학과 부교수
email : eomhun@gmail.com
<관심분야> 네트워크/시스템 보안, 내부자보안, 사이버전