발 간 등 록 번 호
11-1620000-000717-01

2018년도 인권상황실태조사
연구용역보고서

4차 산업혁명 시대에서 정보인권 보호를 위한 실태조사

국가인권위원회
Nation Human Rights Commission of Korea

발 간 등 록 번 호
11-1620000-000717-01

2018년도 인권상황실태조사
연구용역보고서

4차 산업혁명 시대에서 정보인권 보호를 위한 실태조사

국가인권위원회
Nation Human Rights Commission of Korea

4차 산업혁명 시대에서
정보인권 보호를 위한 실태조사

2018년도 국가인권위원회 인권상황실태조사
연구용역보고서를 제출합니다.

2018. 11. 29.

연구수행기관 : 사단법인 참세상
연구책임자 : 이광석 (서울과학기술대학교 교수)
공동연구원 : 김상민 (문화사회연구소 소장)
김성윤 (문화사회연구소 연구원)
김영선 (노동시간센터 연구위원)
박종식 (연세대 사회발전연구소 연구원)
오병일 (정보인권연구소 연구위원)
홍석만 (참세상연구소 연구실장)
홍지은 (법무법인 지음 변호사)
보조연구원 : 이미루 (진보네트워크센터 활동가)
김소형 (문사사회연구소 연구원)

이 보고서는 연구용역수행기관의 결과물로서,
국가인권위원회의 입장과 다를 수 있습니다.

목 차

<표 차례>

<표6-4>신기술 서비스를 통해서 개인정보가 수집되는 사실에 대한 인지도 ····· 198
<표6-5>기업과 공공기관의 개인정보 보호에 대한 신뢰도 ····· 199
<표6-6>개인정보를 활용한 서비스들에 대한 인식 ····· 201
<표6-7>수집된 개인정보들을 동의 없이 활용하는 것에 대한 견해 ····· 204
<표6-8>인공지능이 입사에 당락을 좌우할 경우 응답자들의 견해 ····· 206
<표6-9>휴일/퇴근 후 스마트기기를 통한 업무지시 경험 ····· 207
<표6-10>4차 산업혁명 신기술을 활용한 인사 관리 및 조직 관리 견해 ····· 208
<표6-11>신기술과 정보인권 문제 개선을 위한 정책들에 대한 견해 ····· 210
<표6-12>정보인권 보호 및 개선에 책임이 있는 기관/단체 ····· 212
<표6-13>전문가 인터뷰 응답자 특성 ····· 214
<표6-14>알고리즘 차별 대처 방안에 대한 다차원적 견해 ····· 223

<그림 차례>

<그림2-1>정보인권의 확장성 ····· 15
<그림2-2>4차 산업혁명 시대 정보인권 침해 특징 ····· 24
<그림2-3>정보인권 주체에 따른 침해 특징들 ····· 27
<그림3-1>4차 산업혁명의 작동 원리 ····· 29
<그림3-2>현재 IoT의 방향: 영역의 확대와 기술의 융합 ····· 32
<그림3-3>빅데이터 세계시장 규모 예측: 2011-2026 ····· 36
<그림3-4>국내 빅데이터 시장규모 추이: 2013~2016 ····· 36
<그림3-5>인공지능(AI) 국내외 시장 규모 및 전망 ····· 40
<그림3-6>미국의 인공지능 스피커 현황 ····· 43
<그림3-7>플랫폼의 작동 방식 ····· 50
<그림3-8>플랫폼의 종류 구분 ····· 50

【 요 약 】

O 본 연구는 4차 산업혁명 관련 요소 기술들, 즉 사물인터넷, 클라우드, 빅데이터, 인공지능, 생체인식, 플랫폼 기술 등이 정보 주체에 미치는 인권 침해적 특징을 구체화하고 이에 대한 해결책을 제시하고자 한다. 연구 목적을 구체적으로 보면 다음과 같다.

- 4차 산업혁명 시대 정보인권 개념 정의와 이에 기반한 법제도적 대응 방안 마련
- 4차 산업혁명 시대 정보 주체들에 미치는 정보인권 침해에 대한 사회적 환기
- 항상적인 디지털 접속 환경에서의 새로운 프라이버시 보호 방안 마련
- 상시적인 데이터 연결과 가짜 정보와 여론으로 인한 '사회 피로'와 민주주의 위기 진단
- 4차 산업혁명 시대 정보인권의 지위 제고와 시민들의 기술 성찰성 함양

O 무엇보다 연구 방향은 시민들이 어떻게 4차 산업혁명 기술을 체감하는지, 이로부터 어떠한 정보인권 침해 유형들을 특징화할 수 있는지, 이에 대해 어떤 대안적 법·제도적 해법들이 존재하는지를 탐구한다. 연구의 주요 방향은 다음과 같다.

- 4차 산업혁명 시대 요소기술들이 초래하는 정보인권의 새로운 침해 문제 파악
- 4차 산업혁명 시대 부상하는 신기술 침해 양상에 대한 선진 사례 분석 및 응용
- 신기술 국면 정보 침해의 양상과 특징 분석 및 유형화
- 시민 데이터의 소유, 관리, 처분 문제에 대한 정보주체의 데이터 주권적 개입 마련

O 연구 내용은 크게 네 부분으로 나뉜다.

1) 정보인권 정의 및 재개념화 및 4차 산업혁명 요소 기술들의 현황
2) 신기술을 통한 정보 침해의 특성 및 양상 분석
3) 신기술 관련 국내외 최신 법제도 동향 검토 및 시사점 고찰
4) 4차 산업혁명 관련 시민 의견 설문조사 및 서면 인터뷰, 그리고 이들 분석을 통해 최종 4차 산업혁명 시대 가능한 정보인권 정책 및 해법을 제안했다.

O 연구 방법론: 본 연구는 4차 산업혁명 시대 정보인권의 특징과 이로부터 시민들의 관련 인식에 대한 실태 조사에 초점을 맞췄다. 이를 위해 문헌 조사, 시민 설문 조사, 전문가 의견 조사의 방법론을 활용했다.

(1) 문헌 조사의 경우, 정보인권의 개념을 정의하고 4차 산업혁명 관련 선행 연구와 학술 단행본들을 검토하고, 4차 산업혁명 관련 기술 동향들을 살펴보았다. 무엇보다 4차 산업혁명 국면 국내외 법률 및 정책 동향과 시사점을 고찰하는 장에서 보다 집중적으로 문헌 조사를 실시했다.

(2) 시민 설문 조사의 경우, 조사대상은 시민 1,000명을 표본으로 수집했다. 연구진들의 수차례에 걸친 사전 설문지 작업을 통해 조사 내용을 크게 4차 산업혁명에 대한 인식 정도, 4차 산업혁명, 특히 플랫폼을 매개한 데이터 수집의 부작용 및 인권침해요소 인식 정도, 4차 산업혁명과 노동(일자리) 불안정의 변화 인식 정도, 4차 산업혁명과 개인정보 보호 필요성 및 보호방안, 정책 개선방안에 대한 의견으로 구조화했다.

(3) 전문가 심층 의견 조사의 경우, 시민 설문지 내용의 보완적 기제이자 4차 산업혁명 시대 정보인권의 과제에 대한 보다 전문가적 식견을 얻기 위해 관계자 혹은 전문가 심층 답변 조사를 이메일을 경유해 실시했다. 조사대상은 학계, 산업계, 시민사회, 정부 및 공공기관 포함해 총 30명의 의견을 청취하고 그 내용을 정리했다. 조사 내용은 우선 4차 산업혁명의 부작용 및 인권침해의 원인과 요소, 개인정보 유출 사고의 이유와 이를 막기 위한 효과적인 방안, 가명정보의 활용 범위와 신뢰성 문제, 알고리즘 편향성과 차별에 대한 현재 상태와 극복 방안, 그리고, 빅데이터 등 개인정보 남용이 여론의 왜곡과 공동체의 민주주의에 미치는 부정적 영향과 대응책을 묻는 질문들로 구성됐다.

본 연구는 다음과 같은 문헌연구를 통해 다음과 같은 내용 분석을 수행했다.

1) 문헌조사 1장과 2장에서는 '정보인권'의 개념적 정의를 하고, 4차 산업혁명 시대 더욱 논쟁의 핵심 축이 되어갈 수밖에 없는, 데이터 활용론 혹은 정보 보호론의 이분법적 논의를 넘어서고자 했다. 이 연구 보고서는 보편적 인권만큼이나 정보화 사회의 보편적 권리로서 '정보인권'의 개념을 적극 강조하면서도, 동시에 기술에 대한 시민의 성찰을 강

조하는 '데이터 리터러시(데이터 문해력)'등과 결합해 적극적인 시민 인권의 구축 마련이 필요함을 강조했다. 정보인권과의 연장선상에서 기술 소비자 주도형 데이터 사회의 합리적 미래를 구상하려는 목적을 지닌 '데이터 주권' 개념 또한 점검했다. 2장 2절에서는 4차 산업혁명 요소기술 관련 정보인권의 문제를 본격적으로 다룬 대표적 문헌들을 분석했다. 주로 데이터, 플랫폼, 알고리즘 기술과 인공지능 기술 등이 현실 사회에 어떤 영향을 미치고 정보인권과 어떤 새로운 관계를 형성하고 있는지에 대한 기존의 이론적 논의들을 고찰했다.

2) 3장은 동시대 정보인권 보호를 위해 현재 4차 산업혁명 기술들의 면면을 분석했다. 사실상 이 장은 신기술 동향에 친숙하지 않은 일반 독자들의 이해를 돕는데 중점을 두었다. 4차 산업혁명이라 명명할 때 이에 속하는 핵심적 요소기술들이 무엇인지 그리고 이들의 국내외 기술 수준과 동향이 어떠한지, 각 기술의 도입과 적용으로 인해 어떤 정보인권의 침해 가능성을 내포하는지를 살펴보았다. 물론 이 장에서 소개되는 각 신기술들은 독립적으로 작동하기도 하지만, 관련 요소 기술들, 즉 빅데이터, 사물인터넷, 인공지능, 생체인식, 플랫폼 기술 등은 상호 중첩 연계되어 작용하면서 새로운 형태의 정보 침해 유형을 만들어내고 있다고 보았다.

3) 4장은 실제 4차 산업혁명의 신기술이 어떤 새로운 정보 침해 양상을 낳는지를 살펴보았다. 4차 산업혁명이 가져오고 있는 정보인권의 침해 영역들, 구체적으로 데이터 대량 수집·생성 및 유출, 개인 식별과 타깃팅, 알고리즘의 심화된 차별, 감시의 지능화과 고도화, 정신적 자율성 침해 및 민주적 가치 파괴에 초점을 맞춰 분석했다. 구체적으로 보면 다음과 같다.

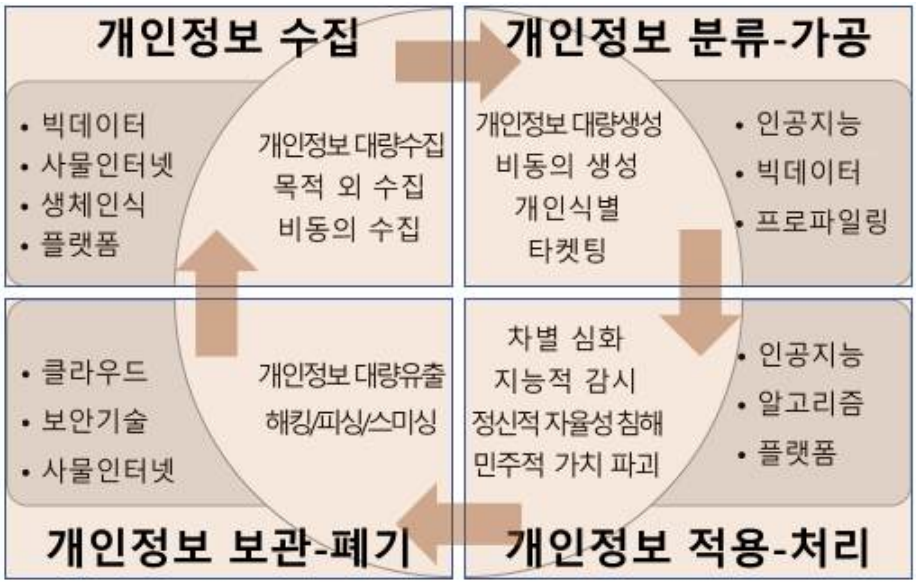
(1) 사물인터넷과 각종 소셜 플랫폼 등을 매개해 나타는 빅데이터 대량 생성 및 유출로 인한 개인정보 및 자기정보통제권 침해의 새로운 양상을 분석했다.

(2) 개인 식별과 타깃팅에서는, 빅데이터 알고리즘이 고도화하면서 나타나는 프로파일링(profiling) 및 패턴 인식의 강화 경향, 비식별 정보들 사이 결합 위험성, 그리고, 온라인 타깃팅에 의한 사용자 정보 오남용 및 궁극적으로 데이터 알고리즘 분석 자체의 투명한 접근을 가로막는 '블랙박스(black box)' 문제를 분석했다.

(3) 알고리즘 기술의 사회적 적용에 따른 사회의 차별을 유형화했다. 즉 알고리즘을 통한 노동 시간 차별의 일상화 사례들, 플랫폼노동자의 노동 취약성 문제, 사회적 소수자의 배제 및 노동 강화의 수단에 활용되는 방식, 기업 인사 및 작업 수행 등 알고리즘 기술에 의한 면접 선발이나 수행성 평가에 활용되는 방식 등 취업, 금융, 보험, 공공영역에서 어떻게 활용되는가를 살펴보았다.

(4) 지능 감시의 확대와 고도화에서는 인공지능 범죄예측 시스템, 생체인식 시스템, 지능형CCTV, 정보수사기관의 저인망식 정보수집과 분석, 해킹 기술 등 통신 감시의 진화 양상을 분석했다.

(5) 마지막으로, 전자적 상시 연결로 인한 정신적 침해 및 사회적 스트레스 급증, 그리고 민주주의적 가치 파괴를 논의했다. 가령, 신기술을 매개해 사회적 약자의 전자적 연결/접속의 피로도가 급상승하고, 불안정 노동 계층의 노동시간 외 강제적 전자 연결로 인한 노동 피로도가 늘고, 카카오톡 등 사회적 위계문화와 결합해 조직사회 피로감과 정신침해, 소셜미디어의 댓글조작 등 가짜뉴스나 여론조작으로 인해 나타날 수 있는 동시대 민주주의의 위기 등을 살펴보았다. 앞서 다섯 가지 유형적 특징은 다음 그림과 같이 정보 주체의 활동 매순간 4차 산업혁명의 요소기술들이 개입하며 개인정보 라이프사이클의 전 과정에서 다양한 형태의 침해 발생의 소지를 야기함을 분석했다.



본 연구는 문헌연구를 통해 4차 산업혁명 시대 개인정보의 유출에서부터 정신적 자율성의 침해에 이르기까지 정보인권 침해가 개인정보의 수집과 분류, 가공과 폐기에 이르는 전 과정에서 발생하고 있음을 확인했다. 이에 기초해 정보인권 침해를 막기 위해서는 각 단계마다 발생할 수 있는 위험과 문제에 따른 대응과 이를 해결할 제도적인 장치들을 마련하는 것이 시급함을 강조했다.

4) 5장은 개인정보에 대한 권리를 중심으로 4차 산업혁명의 요소 기술들과 정보화 국면 이래 적용된 데이터와 뉴미디어 기술들이 초래하는 다양한 인권 침해와 피해를 방지하기 위해 국내외적으로 어떤 국제적 규범 혹은 제도적, 법률적, 행정적 장치와 합의안이 이뤄졌는지를 분석했다. 크게는 신기술에 대한 법제적 대응을 개인정보 침해와 차별 등 개인정보에 대한 권리 측면 및 권력기관에 의한 지능형 감시 측면으로 나누어 검토했다.

해외의 경우에는 신기술을 매개한 정보인권의 침해에 대응한 해외 규범적 합의나 법제도적 변화를 살피는데 주목적을 두었다. 구체적으로는 신기술에 대한 국제적 규범 마련을 위한 노력으로 최근 미국 '아실로마 인공지능 원칙' 마련이나 유럽 등의 빅데이터, 인공지능, 사물인터넷 및 알고리즘에 개인정보 보호 원칙이나 규범과 더불어, 보다 실질적으로 새로운 정보인권 관련 규제 프레임을 중심으로 1990년대 초부터 마련된 유엔의 디지털 시대 프라이버시 보호 권리에 대한 권고, 유럽연합의 일반개인정보보호규정(GDPR)을 중점적으로 살펴보았고, 그 외 정보인권 관련 유엔, 유럽집행위원회 등의 결의안과 미국의 '소비자 프라이버시 권리장전' 등을 포함 개인정보보호 법제를 분석했다. 국내의 경우에는 최근 헌법개정안으로 제출된 '정보기본권'을 신설하는 내용을 비롯해 최근 정보인권과 관련한 법률적 쟁점들을 분석했다. 즉 5장은 4차 산업혁명 시대 관련 국내외 법률과 정책 사례들의 점검을 통해서 정보인권 보호의 필요성을 확인하고 우리 현실에 적합한 정보 정책 개선안과 대안을 도출하는데 그 의의를 두었다.

위의 분석을 통해서,

(1) 우선 해외 국가들은 빅데이터, 사물인터넷, 인공지능 등 새로운 기술 환경에 대비하여 개인정보를 보호하면서도 안전하게 활용할 수 있는 법제도적 장치를 마련하는데 노

력했다. 특히 유럽연합은 GDPR이라는 통일적인 개인정보 보호규범을 마련하여 유럽연합 역 내에서 개인정보의 원활한 이전과 개인정보의 활용을 촉진하면서도 새로운 환경 속에서 정보주체의 권리가 침해되지 않도록 하고 있음을 확인했다. 가령, 프로파일링을 포함한 자동화된 의사결정에 대한 거부권과 설명요구권, 개인정보이동권, 삭제권, 개인정보 보호 중심 디자인과 기본설정, 개인정보 영향평가, 국외 이전된 개인정보의 보호, 개인정보 침해에 대한 강력한 처벌 등이 그것이다.

(2) 한국의 경우, 새로운 기술 환경에 대비한 법제도의 구축이 한참 지연되고 있다. 개인정보의 보호 및 활용에 대한 사회적 합의를 시도하고 개인정보 보호법제의 개선과 감독기구의 일원화를 논의하는 단계다. 이러한 혼란의 배경에는 국내 개인정보 보호법제와 감독기구가 분산되어 있는 현실이 존재한다. 행정안전부, 방송통신위원회, 금융위원회 등이 각자 자기 영역에서의 규범화를 추진하고, 국회에서도 소관 상임위원회에서 각각 법제 개선을 추진하기 때문에 통일적인 개인정보 규범수립에 한계가 발생하게 된 것이다. 이는 각 국의 개인정보 보호규범의 통일을 통해 단일 시장을 촉진하기 위한 GDPR 제정과 비교된다.

결국, 본 연구보고서는 신기술 시대 정보인권 보호를 위해 해외에서 이뤄지는 공통의 규범과 법제도 상황을 고려하면, 학계를 비롯한 다양한 이해관계자의 합의를 통한 윤리규범의 수립, 프라이버시 친화적인 기술의 개발, 기업들의 자율규제, 개발자·정책담당자·시민에 대한 교육 등이 함께 고려될 필요가 있다고 판단했다.

5) 본 보고서의 6장은 일반 시민 설문 조사와 전문가 의견 조사를 종합해 이에 대한 결과를 분석했다. 시민 대상의 설문조사의 경우, 일반시민 1천명을 성별, 연령별, 직업별 표본으로 나눠 정보인권 관련 설문조사를 진행했다. 전문가 의견 청취의 경우, 30명의 학계, 시민사회, 산업, 정부 및 공공기관의 관련자와 전문가들과의 심층면접을 통해 4차 산업혁명 기술 발전과 인권 침해 우려에 대한 사회적 인지 수준과 침해의 종류 및 예방과 정책 대안에 대한 의견을 검토했다. 구체적으로, 4차 산업혁명에 대한 인식 정도, 부작용 및 인권침해 요소 인식 정도, 4차 산업혁명과 노동(일자리)의 변화 인식 정도, 개인정보 보호 필요성 및 보호 방안, 정책 개선방안에 대한 의견 조사 등에 집중해 다층적인 설문

과 면접조사를 실시했다.

(1) 먼저 일반 시민설문 조사의 주요 결과는 다음과 같다.

첫째, 4차 산업혁명과 정보인권 보호 둘 다 중요하게 생각하나, 정보인권을 보다 중요하게 고려하는 인식이 우리 사회에서 조금 더 우세했다.

둘째, 개인정보를 활용하여 안전과 건강수준 향상 등 직접적으로 도움이 될 서비스에 대해서는 대체로 긍정적으로 바라보지만, 금융과 신용평가 등 편익이 불확실한 부분에 대한 개인정보의 활용에는 부정적 의견이 많았다.

셋째, 가명정보를 정보주체의 동의 없이 가공하는 것에 대해서는 반대 의견을 보다 분명히 했다. 이는 개인정보를 수집, 관리하는 공공기관이나 기업에 대해 나타난 낮은 신뢰와 함께 살펴볼 필요가 있다.

넷째, 정책방향과 관련해서 전반적으로 개인정보 보호를 위한 보다 강력한 조치들을 요구하고 있고, 특히 4차 산업혁명의 발달을 위해 개인정보 활용 규제를 완화하는 것에 대해서는 반대 의견이 많았다.

결론적으로, 시민의식조사 설문에서 대체로 많은 이들이 4차 산업혁명 요소기술들이 주는 생활상의 편의나 범죄예방 등 효율성의 효과로 인해 쉽게 개인 정보 주체로서의 데이터 권리 보호를 쉽게 양도하는 경향이 높았다. 그럼에도 불구하고, 일반적으로 신기술의 발전을 위해서 인권보호 수준을 낮추어서는 안 된다는 시민 의견이 조금 더 우세했다.

(2) 전문가 의견 조사의 주요 결과는 다음과 같다.

전문가들 사이의 개인적 견해 차이가 있음에도 불구하고, 시민사회·법조계·학계·공공부문 등에서 정보인권에 대한 적극적 의견을 제시하는 데 반해, 산업계에서는 4차 산업혁명 기술 및 경제 행위에 대한 규제를 우려하는 차원에서 상대적으로 유보적인 의견을 보이는 것이 일반적이었다. 또한 몇몇 응답자들의 경우에는 기술과 정보인권의 일반적 관계보다는 4차 산업혁명 시대의 글로벌 환경과 기술적 특성으로 인해 재편되는 정보인권 논점을 강조하는 경향을 보였다. 구체적으로 보면 7가지 질문에 대한 답변들은 다음과 같다.

첫째, 4차 산업혁명의 정보인권 침해 쟁점과 원인: 전반적으로 4차 산업혁명이 인권 및 민주주의에 대한 위협 요소가 될 수 있다는 관점이 우세했다. 다만, 학계와 공공부문의 일부 전문가들은 부정적 판단을 유보하고 효과를 직접적으로 예단하기 어렵다는 의견을 보였으며, 업계에서는 인권 위협 요소가 있더라도 이를 윤리적·기술적으로 극복할 수 있다는 논점을 제시하고 있다.

둘째, 개인정보 유출의 원인과 대처방안: 개인정보 유출 문제에 관해 대다수 전문가들은 개인정보 유출이 보안 의식과 기술을 둘러싼 한국사회의 '총체적'인 문제라고 진단했다. 특히, 주목할 점은 학계를 중심으로 해서, 개인정보 유출과 관련하여 적잖은 전문가들은 '주민등록번호' 체계 자체에 근본적인 문제가 있다고 지적했다.

셋째, 가명정보의 목적 외 활용 범위 및 조건: 가명정보 문제와 관련해서는 대다수 전문가들은 가명정보의 활용 범위가 '공익적'·'비영리'적 목적에 부합하는 것이어야 한다고 보았다. 가명처리가 되더라도 개인정보가 상업적 거래의 대상이 되어선 안 된다는 문제의식이 지배적이었다. 또한 가명정보가 활용될 때 정보주체의 동의가 선행되어야 한다는 강조도 두드러진다.

넷째, 알고리즘 편향성 및 차별의 현실성과 극복 방안: 인공지능 알고리즘에 의한 의사결정이 사회적 편견과 차별을 야기할 수 있겠느냐는 질문에 거의 모든 전문가들이 지극히 현실적으로 가능한 이야기라고 응답했다. 세부적인 메커니즘에 대한 이해방식에서 다소 엇갈린 평가가 있을 뿐이었다.

다섯째, 지능형 감시 기술의 남용 방지 방안: 지능형 감시 기술에 대해서 대다수 전문가들이 일관적인 논점을 제시하는 데 비해, 상대적으로 산업계 전문가들은 대립적인 견해를 보였다. 대다수 전문가들은 이 문제에 대한 사회적 원칙이 우선해야 한다는 관점이 지배적이었다. 지능형 감시 기술을 견제할 새로운 기술적·윤리적 '규범'의 확립과 감시 기술의 '투명성'을 높이는 방향을 모색할 것을 주문했다.

여섯째, 맞춤 정보 서비스의 편향성과 정치적 활용에 대한 사회적 대응 방안: 응답한 전문가들 대다수가 맞춤 정보 서비스가 선택의 다양성을 줄이고 정치적으로도 악용될 수 있다는 점에 동의했다. 소비자들에게 알고리즘 기술이 제시하는 서비스 및 상품 선택지가 다양한 것처럼 보이지만, 실제로는 창의적인 선택의 기회를 제한하고 궁극적으로는 인간의 '자유의지'라는 것 자체를 훼손할 가능성이 있다고 보았다.

이외에도, 정보인권 보호를 위한 첨언으로 일부 전문가들은 4차 산업혁명 시대 정보인권을 보호하기 위해 '근본적인 접근'이 필요하다고 강조했다. 특히 공공부문의 인공지능 알고리즘 활용이 민주주의를 위협하는 압력으로 작용할 수 있다는 의견들을 제출했다.

O 보고서의 결론은 마지막 7장에 해당하는 내용인데, 보고서의 결론이자 4, 5, 6장에서 살핀 정보인권 침해 양상과 현 상태에 대한 시민의식과 전문가 의견 조사를 통해 제시되는 대안적 해법과 권고안을 제시했다. 이는 4차 산업혁명과 정보인권 보호·증진 조화를 위한 법률과 정책 개선방안에 대한 제언에 해당한다. 마찬가지로 4차 산업혁명 기술발전의 근본 방향에 대한 비판적 점검 및 개인정보 보호 제도 관련 법령 개선에 대해 제언했다. 구체적으로 보면 다음과 같다.

(1) 개인정보 보호법제의 개혁

첫째, 근본적으로 개인정보 보호체계 효율화가 필요하다. 4차 산업혁명에 대비한 개인정보 보호정책의 수립을 위해서는 개인정보 보호 법제를 개인정보보호법을 중심으로 정비하고, 조직적으로는 개인정보보호위원회를 중심으로 신기술에 대응한 개인정보 법제의 개선 추진이 마련돼야 한다.

둘째, 개인정보 보호 법제 개선이 다음과 같은 구체적 측면들에서 체계적으로 이뤄져야 한다. ▲기술 시스템의 '투명성' 보장: 인공지능 등 신기술 시스템에 대해 설명, 감사, 검증이 가능한 방식으로 설계가 되어야 하고, 정보주체의 권리로서 설명을 요구할 권리 보장, ▲설계단계에서 정보인권 보호: '개인정보 보호 중심 설계(Privacy by Design)'의 원칙을 도입하고 시스템의 복잡성과 불투명성이 증가하면서 설계 단계에서부터 인권에 미치는 영향 고려, ▲개인정보 처리 전 과정에서 정보주체의 통제권 강화: 제대로 된 정보 주체의 데이터 처분, 이동, 삭제, 거부 등에 대한 사용자 권리 확보 강화

셋째, 국내 개인정보 보호 법제 개선을 위한 권고 사항은 다음과 같다. ▲기술 시스템 관련 투명성 원칙의 규정 마련, ▲개인정보, 특히 기업들의 고객정보가 남용되지 않도록 최소한의 가명/익명 처리의 개념 신설, ▲프로파일링 등 자동화된 처리에 대한 정보주체의 설명권 요구 등 권리 신설, ▲개인정보 보호 중심설계 및 기본설정(Privacy by Default)의 의무화, ▲인공지능 등 신기술이 인권 전반에 미치는 영향을 평가하기 위한

개인정보영향평가의 제도화, ▲생체정보 등 민감 정보의 범위 확대, ▲주민등록번호 체계 개편

(2) 지능화된 국가 감시 통제 절차와 감독체계의 마련되어야 한다. 신기술로 갈수록 지능화된 국가 감시에 대한 대응은 정보수사기관의 개인정보 처리 실태의 투명성과 통신수사 과정에서의 인권 보호를 취할 수 있는 필수 전제이나 현재 그 대응이 미약한 상황이다. 다음과 같은 정책 대안을 제시하고자 한다.

첫째, 정보수사기관의 무분별한 개인정보 활용에 대한 통제 마련

둘째, 정보수사기관이 보유한 개인정보파일 및 시스템에 대한 감독

셋째, 유무선 통신 관련 국가 감시나 통제에 대한 감독 및 규제 마련, 예컨대, 관련 통신자료(가입자 정보)와 통신사실 확인 자료의 보호, 통신 감청 제한, 통신자료 통지와 통신사실 확인 자료 보관 의무화 폐지 등이 마련되어야 함

(3) 향후 중장기 연구과제 제안들

첫째, 신기술을 매개한 노동 감시를 체계적으로 통제할 수 있는 법제 마련과 이에 대한 실태 연구: 한편으로, 작업장 내 혹은 플랫폼 노동 등 불완전 노동 환경에서 발생하는 지능화된 노동 감시를 규제하기 위한 법제와 이에 대한 감독 시스템이 마련될 필요. 다른 한편으로, '연결되지 않을 권리(right to disconnect)'의 보장: 특히 노동자들의 일과 외 시간 연결되지 않을 권리 보장을 통해 노동시간 외의 일과 관련된 업무의 차단뿐만 아니라, 비 노동시간에서도 개인정보가 축적되는 다양한 환경을 정보주체가 '차단'할 수 있는 노동권의 보장

둘째, 인권영향평가와 차별에 대한 규제안 마련: 개인정보 외의 분야에서는 인권영향평가에 대한 제도화가 미흡한 상황. 국가인권위원회는 인공지능 등 신기술이 인권 전반에 미치는 영향을 평가하기 위한 인권영향평가의 제도화를 고민할 필요. 그리고 유럽 GDPR 등을 참고해 기술로 인한 신기술을 매개한 새로운 차별의 문제들을 최소화하기 위한 윤리적, 기술적, 제도적 방안이 마련되어야 함

셋째, 대중 참여를 통한 개인정보의 자기통제력 확대 방안: 개인정보의 라이프사이클 전체에서 개인정보 자기결정권의 행사가 그 어느 때보다 중요해진 만큼 개인정보에 대해

정보주체가 자신의 권리를 행사할 수 있는 역량과 기술 환경 전반에 대한 성찰성 강화 및 시민의 리터러시(literacy) 확대 방안 필요

마지막으로, 정부(공공기관), 기업, 소비자/사용자 주체 각각의 구체적인 정책 권고 사항들은 다음과 같다.

(1) 정부와 관련 공공 기관은 시민의 인권을 보호해야할 책임이 있는 주체인 동시에, 스스로 인권침해의 당사자가 될 수 있는 존재다. 그렇기 때문에 신기술과 관련된 정책 결정자, 그리고 민간 영역의 감독자로서 중요한 공적 역할을 수행해야 한다. 정부는 원칙적으로 인공지능 시스템이나 도구를 도입할 때 인권 원칙이 준수될 수 있도록 보장해야 한다. 나아가 개인정보의 수집과 처리가 세계적인 수준에서 이루어지고 있는 만큼, 해외의 개인정보 감독기구와 협력하고 국제적으로 통일적인 규범이 만들어질 수 있도록 노력해야 한다.

(2) 기업은 신기술 개발에 관여하는 개발자, 프로그래머, 데이터 관리자들이 제품의 설계부터 출시에 이르는 전 과정에서 개인정보를 포함한 인권 보호에 대한 책임 의식을 가질 수 있도록 윤리 원칙을 수립할 필요가 있다. 또한, 이에 근거하여 개인정보 보호 중심 디자인이나 기본 설정, 개인정보 영향평가 등 문제점을 수정할 수 있는 체계를 마련해야 한다. 보다 근원적으로 기업의 책임성을 보장하기 위해 관련 법제를 구축하고 감독기관이 모니터링하는 것도 중요하지만, 기업 스스로 자율규제 체제를 만든다면, 사회 전체적인 효율성과 실효성을 높일 수 있을 것이다.

(3) 시민, 소비자/사용자, 노동자로서 개인의 역량 역시 중요하다. 시민 스스로 문제점을 인식하고 문제제기하지 않는다면 자신의 피해를 구제하기 힘들뿐더러, 기업의 관행과 제도의 변화 역시 끌어내기 힘들기 때문이다. 정부 역시 시민의 문제제기가 없다면 인권 침해적 관행을 교정하려는 노력을 게을리 할 것이다. 특히, 기술의 복잡성과 시스템의 불투명성이 높아가는 상황에서 시민 스스로 리터러시를 확대하려는 풀뿌리 기술문화가 확산되어야 한다.

제1장 서론

제1절 연구 목적 및 필요성

온라인과 오프라인, 사물과 사물, 기술과 인간의 융합을 핵심으로 하는 4차 산업혁명 또는 디지털 전환(digital transformation)이 세계적으로 확산되고 있다. 빅데이터, 사물인터넷(IoT), 인공지능(AI), 플랫폼, 자율주행, 무인드론 및 바이오 기술 등 4차 산업혁명의 핵심기술들은 사회를 구성해 왔던 기존 패러다임을 빠른 속도로 바꿔 이를 재구성할 것으로 전망된다. 이런 가운데, 4차 산업혁명은 그동안 존재했던 정보통신기술(ICT)의 발달에 따른 인권 침해 우려를 넘어서 유리알 사회로의 진입을 낳게 해, 정보인권 침해에 대한 위기가 유래 없이 고조되고 있다. 특히 인공지능과 결합한 빅데이터 처리 기술이 발전하고 빅데이터가 상업적 가치를 갖게 되면서 개인정보의 생성 및 유출 위험을 더 확대시키고 있다.

일례로, 건강보험심사평가원은 2014년부터 2017년까지 3년간 민간보험사에게 공공데이터라는 명목으로 진료내역 등이 담긴 핵심 개인정보를 제공했다. 10여개 민간보험사와 연구기관에 보험상품 연구 및 개발 등을 위해 요청한 6,420만 명의 '표본 데이터셋'을 돈을 받고 제공하기도 했다. 또한, 페이스북은 2010년 의회 선거에서 "페이스북 알고리즘을 조정해 정치 시스템에 영향을 줄" 목적으로 '투표 메가폰'이라는 캠페인을 진행해 실제 투표율을 조절할 수 있음을 보였다. 나아가 데이터분석업체 캠브리지 애널리티카는 지난 2016년 미국 대선에서 페이스북 앱을 통해 5,000만 명의 개인정보를 무단으로 수집하고 이를 통해 트럼프 당선 캠페인을 은밀히 진행했다는 사실이 드러나 충격을 주고 있다.

노동 영역에서의 정보인권 침해의 강도 또한 기술적으로 깊어지고 있다. 단순한 노동에 대한 정보감시와 노동현장에서 GPS 정보를 포함해 노동자 개인의 개별 활동까지 세밀하게 감시 가능한 방법으로 이루어지고 있다. 2014년 KT는 직원 개인 스마트폰에 카메라, 현재위치, 일정, 문자 등 12개 항목에 접근할 수 있는 모바일 앱을 설치하라는 명령에 거부한 노동자를 징계했다. 이에 해당 노동자는 법원에 소송을 제기했고 법원은 KT가 노동자의 개인정보 자기결정권을 침해했다고 판결했다. 당시 재판부는 "과학기술이 진보하면서 기업의 노동 감시활동이 전자 장비와 결합해 확대됨에 따라 노동자의 인

격권·사생활 침해 우려가 고조되고 있다"며 "서비스 제공자(사용자)가 단말기 정보를 얼마나 수집하고 어디까지 활용할지 정확히 알 수 없는 상황에서 노동자는 개인정보 자기결정권을 존중해 줄 것을 요구할 수 있다"고 판시했다. 노동부문의 경우, 디지털 감시기술이 발달함에 따라 작업장이라는 공간 중심의 정보통제에서 개인에게 직접 투사되는 방식으로 바뀌면서 문제가 '심화'되고 있다. 4차 산업혁명 관련 기술의 발달로 인해 '빅브라더'라는 감시사회를 넘어서 <대량살상 수학무기>와 <블랙박스사회>에서 언급했던 '신'이 통제하는 초감시 사회로의 진입이 우려되고 있는 상황이다.

4차 산업혁명 관련 기술 발전에 따라 온라인 공간과 오프라인 공간의 경계가 흐려지고 융합하는 상황에서 그동안 주로 정보통신기술에 의하여 디지털화된 정보 즉, 정보통신 온라인 공간의 정보를 대상으로 삼았던 '정보인권'(Human Rights in the Digital Age; ICT and the Human Rights; right to information)도 인권의 보호대상으로서 정보의 경계가 흐려지고 오프라인과 융합이 일어나고 있다. 그에 따라 현재 정보통신 공간의 정보인권 침해를 넘어서 다양하면서도 확장된 형태의 인권침해가 발생하고 있다. 4차 산업혁명의 기술발전에 따라 이런 양상은 더 확대하리라 예상되며, 정보인권 개념에 새로운 기술침해 유형을 발굴하고 그 보호 대상 및 인권적 대응 또한 새롭게 확대해야 함을 의미한다. 특히, 본 연구를 위해 정보인권 이슈에 새롭게 제기되는 쟁점이자 연구 수행의 필요성은 다음과 같다.

첫째, 4차 산업혁명 시대 새로운 정보인권 개념 정의와 이에 기반을 둔 법제도적 대응방안 마련이 시급하다. 정보프라이버시권의 핵심인 개인정보를 필요로 하는 빅데이터, 가상・증강현실(VR・AR), 사물인터넷, 생체정보, 인공지능 등 4차 산업혁명의 핵심 요소기술들은, 다양한 개인정보의 대량 수집・활용・공유를 전제하는 경우가 많아 개인정보 자기결정권 등 정보인권 보호와 상충이 우려된다. 단순히 개인 정보의 경제적 활용론 뿐만 아니라 무차별적 정보인권 침해에 대한 사회적 대응 방안이 마련될 필요가 있는 것이다. 데이터 수집 장치, 인공지능 센서, 자율주행, 무인드론 등 고도의 기술들은 데이터의 수집뿐만 아니라 데이터 통합에 따른 방대한 개인정보의 침해가 예상된다. 특히 인공지능 등을 활용한 예측과 감시 기술의 발전은 사회적 차별과 갈등을 확대하고 생산현장에서 노동의 감시통제를 더 확대할 우려를 낳고 있다. 또한, 생명공학에서는 개인 생체정보 등의 수집 및 이용에 따른 개인정보 침해와 기술 윤리 문제가 발생하고 있다. 인권침

해와 관련된 과학기술의 윤리적 문제에는 4차 산업혁명과 관련된 기술이 국가에 의한 감시는 물론 특히 군사기술로도 이용이 가능하고, 로봇병사, 무인드론형 무기 개발이 가사화되면서 윤리적, 인권적 판단과 갈등을 빚고 있다.

무엇보다 온라인 플랫폼에서 광대한 범위의 데이터 수집과 처리를 통해 이윤을 취하는 닷컴, 플랫폼 기업들의 정보인권 침해를 좀 더 눈여겨봐야 할 대목이다. 인간의 감정이나 정서를 데이터화 하면서 이를 산업화 하는 페이스북, 트위터, 네이버, 구글 등 소셜미디어(SNS) 업체에 의한 개인정보 데이터의 생성, 보존, 유출이 심각한 인권적 문제를 야기하고 있다. 이들 기업의 약관에 따라 사용자 개인정보의 모든 데이터가 기업 손에 들어가게 되고 정보주체인 사용자들은 실제 자기정보에 대한 어떠한 통제권도 행사하지 못하고 있다. 최근 '잊힐 권리(the right to be forgotten)'에 대한 강조는 개인정보의 생성뿐 아니라 유지와 보존도 자기정보통제의 내용으로 확대됨을 의미한다. 다른 한편으로, 플랫폼 사용자들의 정서 및 선호에 대한 개인정보의 생성 및 유통 과정에 개입해 여론이나 정서의 조작을 가능케 해 상품 평가나 구매와 같은 일상적인 수준뿐 아니라 선거시기 정치적 의사결정을 왜곡하며 민주주의의 핵심 원리들을 침해하는 사례들이 발생하고 있다. 앞서 2016년 미국 대선에서 페이스북을 통한 여론조작과 한국에서도 선거 시기 댓글부대의 운용, 드루킹 댓글 조작 사건 등이 대표적인 사례이다. 이 사례들은 선거 결과에 직접적인 영향을 미친다는 점에서 민주주의 기본적 전제를 허무는 대표적인 기본권 침해 사례로 볼 수 있다.

둘째, 4차 산업혁명으로 말미암아 현실 사회에서 상대적으로 취약한 지위에 놓인 노동주체들에 미치는 영향력에 대한 사회적 관심과 비판적 평가가 시급하다. 4차 산업혁명이 야기하는 생산과 자원·서비스 배치에서의 변화는 인간노동을 로봇이나 인공지능으로 대체해 일자리를 축소할 뿐만 아니라 '불안정' 노동 유형을 심각하게 확대하면서 기존에 취약했던 노동과정과 형태를 더 굴절된 형태로 변화시키고 있다. 이에 따라 4차 산업혁명 기술의 발전과 함께 물리적 공간과 융합된 '정보인권'으로서 노동권을 어떻게 변형시키고 침해시키는지에 대한 분석도 필요하다. 플랫폼 경제의 발달과 생산의 디지털 전환에 따라 크라우드 워커(crowd worker)와 클릭 워커(click worker)의 형성, 우버(Uber)나 에어비앤비(AirBnB)와 같은 네트워크 기반형 공유경제 혹은 '긱경제'(gig economy)에서 자영업과 임금노동자의 중간형태의 고용이 발생하면서 야기되는 노동권 침해 등 4차 산

업혁명이 야기하는 정보인권으로서 노동권 침해 양상을 해석하고 이 부분에서 다양한 침해사례가 조사, 연구될 필요가 있다. 특히, 국내 유통 시장의 틈새를 밀고 들어와 우후죽순 격으로 생성되고 있는 플랫폼 사업자들은 중소 상인들과 사용자를 연결해 유통 수익을 남기는 새로운 유형의 O2O(Online to Offline) 기업들이다. 이들 플랫폼들은 대체로 이미 존재하는 시장에 브로커로 참여해 유통 효율성을 증대시키면서도 이윤 배분의 옥상옥 구조를 만들어내고 있다. 더 우려되는 부분은 O2O 플랫폼을 위해 오토바이 배달과 알바 일을 하는 수많은 프리랜서들이다. 알바 노동자들은 밑바닥 노동을, 그리고 대부분의 중소 가맹 점주들은 본사의 '갑질'은 물론이고 플랫폼 사업자가 강요하는 유통 수수료의 큰 부담까지 떠안고 있다.

셋째, 첨단의 거의 모든 곳에 편재하는 기술 권력의 확장성으로 인해 현대인들의 '홀로 남겨질 권리'로서 프라이버시가 사라져가면서, 변화하는 환경에 대응한 새로운 프라이버시 접근법이 필요하다. 4차 산업혁명의 요소 기술들이 점차 일반화하게 되면 개인들의 프라이버시가 사실상 '제로 상태(0)'에 이르게 되면서, 이의 대응은 단순히 이미 사라져버린 사적 영역의 안전을 지키려는 일보다는 다른 사람들과의 사회적 관계에서 발생하는 프라이버시의 '사회성'(the social)에 대한 공통의 실제 해법을 좀 더 필요로 한다.[1)]

사적 영역을 해체하기 위한 신기술의 진화는 오늘도 계속되고 있다. 예를 들어, 사각지대 없이 360도를 비추는 CCTV처럼 다양하게 진화하는 광학 장치, 첨단 뉴로 마케팅 기법, 전자태그(RFID) 칩 등을 활용한 사물인터넷이나 지리위치정보시스템(GPS), 데이터 수집 알고리즘 기법 등은 사생활 영역을 아예 무위화하는 새로운 기술 권력 수단으로 등장한다. 기술에 의한 사적 영역의 흡수는 물론이고, 직접적으로 개별 인간 신체에 작동하는 프라이버시 침해 기술들의 진화도 동시에 급격히 이뤄지고 있다. 이들 기술은 최소한의 홀로 남을 권리조차 무위로 만드는 기술적 장치들이다. 예컨대, 개별화된 신체의 바코드 삽입, 신체 피부 아래 틈입한 감시용 칩, 눈동자를 흐르는 개별 인식의 데이터베이스 장치, 인간 게놈 지도를 통한 생체 정보의 관리 등에서 우린 순수하게 사적인 것으로 정의되는 프라이버시의 소멸을 얼마든지 예상할 수 있다. 프라이버시는 사적인 권리이기도 하지만 공적 권리이기도 하다. 이는 법・제도적으로 그 권리를 인정받는다는 의미에서도 그렇지만, 개별 프라이버시의 집단성 혹은 사회성 때문에도 그러하다. 신기술의 위

1) 이광석, 2017,『데이터 사회 비판』, 책읽는수요일.

협 속 프라이버시 부재의 상황에서는 개별 정보인권의 보호도 중요하지만, 시민권, 소비권, 노동권 등 주체들의 연합적 사회 지위와 맞물린 국가와 기업 등 권력의 오·남용과 침해에 대한 대응이 무엇보다 중요하다. 사적이고 공적인 영역은 이미 씨줄과 날줄처럼 얽혀 있고, 디지털 기술로 인해 개인 정보는 무방비로 노출되고 있기 때문이다. 프라이버시의 공적·사적 영역 구분이 이렇게 흐트러지고 인간관계 결속의 밀도가 높아지면서, 개인의 사생활이 점차 집단적 프라이버시 문제로 '사회화'하는 경우가 흔하다. 일례로, 밴드나 카톡방처럼 특정인의 개인적 사담이 의도치 않게 다른 사람과의 정보와 뒤섞이는 것은 이젠 흔한 일이 됐다. 이제는 나와 직접적으로 관계된 정보만을 관리해서는 해결할 수 없는 새로운 사회 관계적 차원의 '공동 프라이버시(communal privacy)'가 존재하게 된 것이다. 즉 정보와 데이터가 한데 뒤섞이면서 개별화된 호명보다 정보의 공동 프라이버시 침해 상황이 증가하고 있고, 이에 대한 사회적 대응이 시급하다.

넷째, 4차 산업혁명 기술로 인해 데이터 주체로부터 흘러나온 '데이터 부스러기'의 소유권 문제가 더욱 첨예해져 감에 따라 이에 시민 데이터 주권적 개입이 필요한 대목이다. 빅데이터 등이 대상으로 하는 정보의 수집과 이용은 대부분 개인들의 다양한 활동을 집적한 공공정보를 기반으로 하지만 이를 통한 지적 생산물이 대부분 플랫폼 노동 등으로 흘러 들어가 사적으로 전유되고 있어 정보문화 향유권과 정보 접근권이 심각하게 침해되고 있다. 사용자들이 자발적으로 온라인 플랫폼 활동을 통해 만든 콘텐츠를 플랫폼 소유자가 배타적으로 독점하는 등 사적으로 전유함으로써 정보 접근과 소유권 충돌이 우려된다. 정보문화 향유권과 관련해서 지식재산권과의 충돌은 이전까지 주로 의약품 복제와 또래간(p2p) 정보 거래 문제로 첨예하게 나타났었다. 4차 산업혁명과 인공지능 등의 발달에 따라 과거보다 지식 생산의 사적인 전유는 더 광범위하고 복잡한 형태로 문제들이 발생할 것이다. 대표적으로 공공정보 및 개인정보 빅데이터를 자동 알고리즘 분석 기법으로 생산한 결과물이나 이를 기반으로 기계학습(machine learning)과 딥러닝(deep learning)을 진행한 인공지능 기계가 만들어낸 지적 제작품 혹은 예술품이 과연 누구의 소유일 것인가의 문제 등이 난제로 등장하면서 지식재산권 관련 논쟁에서 새로운 국면을 형성하고 있다.

마지막으로, 정보인권 침해와 만성화된 전자적 연결 상태로 인한 '사회적 피로'와 사회병리의 증가이다. 한국은 다른 어느 나라 보다 빠르게 정보입국이 되었으나 그에 따른

소셜미디어 사용이나 카카오톡 이용 등이 사회문화적 차원의 위계 구조와 쉽게 접 붙으면서 신기술을 매개한 사회적 약자의 전자적 연결/접속의 피로도를 급상승시키고 있다. 4차 산업혁명의 요소기술들, 예컨대, 특정 사회계층의 생체정보 수집, 인공지능 기반 회사 면접, 사회복지 관련 데이터 알고리즘 분석과 차별, 사물인터넷 등 24시간 신체 데이터 정보 감시, 카톡방을 통한 직원 행동과 노동 통제 등은 이제 흔한 정보인권 침해 기법이 되 가고 있다. 이는 조직 문화의 효율성을 위해 신종 기술을 도입하는 명분을 갖고 있으나, 다양한 형태의 사회적 스트레스와 피로 지수를 상승시키고 궁극에는 정보인권을 침해하는 새로운 변수로 등장하는 경향을 갖고 있다. 이에 대한 국가 차원의 대비책이 필요한 대목이다.

이처럼 4차 산업혁명과 디지털 전환 기술의 발전에 따라 정보인권 침해에 대한 우려가 커지고 있고 개인정보보호에 대한 국제 기준이 높아지고 있지만, 여전히 국내에서는 기초적인 개인정보보호법 수준에 머물러 있다. 유럽연합(EU)은 1995년부터 운영되어 온 개인정보보호지침(Data Protection Directive 95/46/EC)을 대폭 강화해, 2018년 5월 25일부터 강력한 프라이버시 보호를 내용으로 하는 일반개인정보보호규정(General Data Protection Regulation: GDPR)을 본격 적용하는 등 대응에 나서고 있다. 유엔과 OECD에서는 데이터 거버넌스에 대한 권고를 지속적으로 진행하고 있다. 이와 같은 국제 환경에 맞춰 우리도 신기술 환경에 맞춰 적절한 정보인권 보호 대책을 강구하는 일이 시급하다고 본다.

본 정보인권 실태 조사 및 정책 연구는 이 같은 4차 산업혁명 시대 신기술로 인해 새롭게 야기되는 다양한 정보인권 침해 사례를 조사하고, 4차 산업혁명과 정보인권 침해 및 인식 정도에 대한 실태를 분석하고 관련 분야에 종사하는 전문가들의 의견조사를 종합해 현실주의적 대안을 구상하고자 한다. 즉 정보인권의 핵심적인 침해가 우려되는 개인정보 보호 및 관련 내용에 대한 새로운 기준과 가이드라인 및 정책 대안 마련을 직접적인 과제로 삼는다. 구체적으로는, 신기술 영역을 매개해 정보인권 침해가 새롭게 야기되는 양상들을 최대한 구체화해 살펴 정보인권 침해의 실태를 조사하고 분석한다. 이를 통해서 4차 산업혁명의 요소 기술들이 지닌 기술적 가능성과 혁신의 계기를 억누르지 않으면서도 정보인권 보호와 인권 향상과 조화롭게 어우러질 수 있는 민주적인 기술 설계 가능성을 검토한다.

제2절 연구내용 및 범위

본 연구는 4차 산업혁명의 시대 관련 요소 기술들, 즉 빅데이터, 사물인터넷, 인공지능, 바이오, 플랫폼 기술 등이 야기하는 정보 주체에 대한 인권 침해적 특징들을 살피고 이에 대한 문제 해결책을 제시하는데 있다. 무엇보다 이 연구 보고서는 시민들이 어떻게 4차 산업혁명 기술을 체감하는지, 이로부터 어떠한 정보인권 침해 유형들을 특징화할 수 있는 지, 이에 대해 어떤 대안적 법제도적 해법들이 존재할 지를 탐구한다.

먼저 2장 1절은 '정보인권'의 개념적 정의를 하고 4차 산업혁명 시대 더욱 논쟁의 핵심 축이 되어갈 수밖에 없는, 데이터 활용론 혹은 개인정보 보호론의 이분법적 논의틀을 넘어서고자 한다. 이 연구 보고서는 보편적 인권만큼이나 정보화 사회의 보편적 권리로서'정보인권'의 개념을 적극 강조하면서도, 동시에 좀 더 시민의 기술 성찰성을 강조하는 '데이터 리터러시(데이터 문해력)'등과 결합해 적극적인 시민 인권의 구축 마련이 필요함을 강조한다. 정보인권과의 연장선상에서 기술 소비자 주도형 데이터 사회의 합리적 미래를 구상하려는 목적을 지닌 '데이터 주권' 개념 또한 점검하고 있다. 2절에서는 4차 산업혁명 요소기술 관련 정보인권의 문제를 본격적으로 다룬 대표적 문헌들을 살피고 있다. 주로 데이터, 플랫폼, 알고리즘 기술과 인공지능 기술 등이 현실 사회에 어떤 영향을 미치고 정보인권과 어떤 새로운 관계를 형성하고 있는지에 대한 기존의 이론적 논의들을 살핀다.

3장은 동시대 정보인권 보호를 위해 현재 4차 산업혁명 기술들의 면면을 살피고 있다. 사실상 이 장은 신기술 동향에 친숙하지 않은 일반 독자들의 이해를 돕는데 중점을 두고 있다. 4차 산업혁명이라 명명할 때 이에 속하는 핵심적 요소기술들이 무엇인지 그리고 이들의 국내외 기술 수준과 동향이 어떠한지, 각 기술의 도입과 적용으로 인해 어떤 정보인권의 침해 가능성을 내포하는지를 살피고 있다. 물론 이 장에서 소개되는 각 신기술들은 독립적으로 작동하기도 하지만, 관련 요소 기술들, 즉 빅데이터, 사물인터넷, 인공지능, 생체인식, 플랫폼 기술 등은 상호 중첩 연계되어 작용하면서 새로운 형태의 정보침해 유형을 만들어내고 있음을 상정한다.

4장은 실제 4차 산업혁명의 신기술이 어떤 새로운 정보 침해 양상을 낳는지를 살핀다.

4차 산업혁명이 가져오고 있는 정보인권의 침해 영역들, 구체적으로 개인정보의 대량 수집·생성 및 유출, 개인식별과 타깃팅, 알고리즘의 심화된 차별, 감시의 지능화과 고도화, 정신적 자율성 침해 및 민주적 가치 파괴에 초점을 맞춰 살핀다. 구체적으로 보면, 1) 빅데이터 대량 생성 및 유출로 인한 개인정보 및 자기정보통제권 침해의 새로운 양상을 살피고 있다. 2) 개인 식별과 타깃팅에서는, 빅데이터 알고리즘이 고도화하면서 나타나는 프로파일링 및 패턴 인식의 강화 경향과 알고리즘 자체의 '블랙박스(blackbox)' 문제를 분석한다. 3) 알고리즘 기술의 사회적 적용에 따른 사회의 차별을 유형화한다. 즉 알고리즘을 통한 차별의 일상화 사례들, 사회적 소수자의 배제 및 노동 강화의 수단에 활용되는 방식, 기업 인사 및 작업 수행 등 알고리즘 기술에 의한 선발이나 수행성 평가에 활용되는 방식 등 취업, 금융, 보험, 공공영역에서 어떻게 활용되는가를 살핀다. 4) 지능 감시의 확대와 고도화에서는, 인공지능 범죄예측 시스템, 생체인식 시스템, 정보수사기관의 저인망식 정보수집과 분석, 해킹 기술 등 통신 감시의 진화 양상을 살피고, 노동과정에서도 이 감시기술이 어떻게 나타나고 있는지 나타나고 있는지 고찰한다. 5) 마지막으로, 전자적 상시 연결로 인한 정신적 침해 및 사회적 스트레스 급증, 그리고 민주주의적 가치 파괴를 논의한다. 가령, 신기술을 매개해 사회적 약자의 전자적 연결/접속의 피로도가 급상승하고, 불안정 노동 계층의 노동시간 외 강제적 전자 연결로 인한 노동 피로도가 늘고, 카카오톡 등 사회적 위계문화와 결합해 조직사회 피로감과 정신 침해, 소셜미디어의 댓글조작 등 가짜뉴스나 여론조작으로 인해 나타날 수 있는 동시대 민주주의의 위기 등을 살펴본다.

이어서 5장은 4차 산업혁명의 요소 기술들과 정보화 국면 이래 적용된 데이터와 뉴미디어 기술들이 초래하는 다양한 인권 침해와 피해를 방지하기 위해 국내외적으로 어떤 제도적, 법률적, 행정적 장치와 합의안이 이뤄졌는지를 살피고 있다. 해외의 경우에는, 신기술을 매개한 정보인권의 침해에 대응한 해외 법제도적 변화를 살피는데 주목적을 둔다. 구체적으로는, 새로운 정보인권 관련 규제 프레임을 중심으로 1990년대 초부터 마련된 유엔의 디지털 시대 프라이버시 보호 권리에 대한 권고, 유럽연합의 일반개인정보보호규정(GDPR)을 중점적으로 살피고, 그 외 정보인권 관련 유엔, 유럽집행위원회 등의 결의안과 미국의 경우 오바마 행정부 시절 '소비자 프라이버시 권리장전(Consumer Privacy Bill of Right)'등을 포함 개인정보보호 법제를 분석하고 있다. 국내의 경우에는

최근 헌법개정안으로 제출된 '정보기본권'을 신설하는 내용을 비롯해 최근 정보인권과 관련한 법률적 쟁점들을 서술하고 있다. 즉 5장은 4차 산업혁명 시대 관련 국내외 법률과 정책 사례들의 점검을 통해서 정보인권 보호의 필요성을 확인하고 우리 현실에 적합한 정보 정책 개선안과 대안을 도출하는데 그 의의를 두고 있다.

본 보고서의 6장은 일반 시민 설문 조사와 전문가 의견 조사를 종합해 이에 대한 결과 분석을 시도하고 있다. 시민 대상의 설문조사의 경우에, 일반시민 1천명을 성별, 연령별, 직업별 표본으로 나눠 정보인권 관련 설문조사를 진행했다. 전문가 의견 청취의 경우, 30여명의 학계, 산업계, 정부 및 공공기관의 관련자와 전문가들과의 심층면접을 통해 4차 산업혁명 기술 발전과 인권 침해 우려에 대한 사회적 인지 수준과 침해의 종류 및 예방과 정책 대안에 대한 의견을 검토하고 있다. 구체적으로, 4차 산업혁명에 대한 인식 정도, 부작용 및 인권침해 요소 인식 정도, 4차 산업혁명과 노동(일자리)의 변화 인식 정도, 개인정보 보호 필요성 및 보호 방안, 정책 개선방안에 대한 의견 조사 등에 집중해 다층적인 설문과 면접조사를 시행했다.

마지막 7장은 이 글의 결론이자 4, 5, 6장에서 살핀 정보인권 침해 양상과 현 상태에 대한 시민의식과 전문가 의견 조사를 통해 제시되는 대안적 해법 마련을 적고 있다. 이는 4차 산업혁명과 정보인권 보호·증진 조화를 위한 법률과 정책 개선방안에 대한 제언에 해당한다. 4차 산업혁명 기술발전의 근본 방향에 대한 비판적 점검 및 개인정보 보호 제도 관련 법령 개선에 대한 제언을 시도하고 있다. 특히, 국회, 정부, 업계, 사용자 등 각 이해관계자에 대한 권고 및 정책 제안을 포함한다.

<표1-1> 연구 흐름도

연구 목표

· 4차 산업혁명 시대 새로운 정보인권 개념 정의와 이에 기반한 법제도적 대응 방안 마련
· 4차 산업혁명 시대 취약한 지위의 정보 주체들에 미치는 정보 침해에 대한 사회적 환기
· 사생활이 부재할 정도의 항시적인 접속 환경에서 새로운 프라이버시 보호 방안 마련
· 항상적인 데이터 연결과 가짜 정보 · 여론으로 인한 '사회 피로'와 민주주의 위기 진단
· 4차 산업혁명 혹은 신기술 시대 정보인권의 지위 제고와 시민들의 기술 성찰성 함양

연구 방향

· 4차 산업혁명 시대 요소기술이 초래하는 정보인권의 새로운 침해 문제 파악
· 4차 산업혁명 시대 부상하는 신기술 침해 양상에 대한 사례 분석 및 응용
· 신기술 시대 정보 침해의 양상과 특징 분석 및 유형화
· 시민 데이터의 소유, 관리, 처분에 대한 정보주체의 데이터 주권적 개입 마련

핵심 연구	연구 방법	주요 내용
① 4차 산업혁명 시대 정보 침해와 보호에 관한 논의 검토	문헌 조사	• 2장: 정보인권 정의 및 관련 문헌 연구 • 3장: 4차 산업혁명의 요소 기술에 대한 관련 기관 및 업체 자료 분석 • 4장: 신기술에 따른 정보인권 침해의 특성 및 양상 분석 • 5장: EU, 영국, 미국, 일본 등 신기술 관련 해외 사례 연구 및 최신 법률 동향 검토, 시사점 고찰
② 4차 산업혁명에 대한 인식 및 정보인권 쟁점 공유	시민 설문 조사	• 6장: 1,000명의 시민 표본을 통해 4차 산업혁명에 대한 인식을 측정하고 정보인권 침해의 원인, 양상 등 일반 대중의 의견 분석
	전문가 및 관계자 인터뷰	• 6장: 각계각층의 30여명 전문가 및 이해관계자를 대상으로 서면 인터뷰
③ 4차 산업혁명 시대, 정보인권 침해에 대한 대안적 정책 마련	IT 민주주의 정책론	• 7장: ①과 ②의 연구내용을 토대로 대안적인 정책 제시, 특히 정보주체별(시민, 소비자, 노동자) 정보인권 보호 방안 마련

제2장 4차 산업혁명 시대 정보인권과 접근 모델링

제1절 정보인권의 개념화 및 선행연구 검토

1. 신기술 국면 정보인권의 개념화

1948년 인류의 보편적 생존 권리인 '인권' 개념이 「세계인권선언」(the Universal Declaration of Human Rights: UDHR)을 통해 천명되고 이에 근거해 인간의 기본 권리들이 역사 속에서 안착되었다. 당시 인간의 보편적 인권선언이 주로 물질적 측면에서 인간다운 생활을 누릴 권리에 대한 규정이라고 볼 수 있다면, 근대 사회 이후 인권은 좀 더 확장적 면모를 보여 왔다. 먼저 문화적 측면에서 휴식과 여가의 권리, 문화생활로의 참여, 감상, 향유 권리 등 '인간다운 생활을 누릴 권리'[2] 혹은 참다운 삶을 향유하고 문화적 다양성 속 공존을 위한 권리, 즉 '문화권(right to culture)'이 보편적 인권의 영역으로 확대되었다. 2001년 유네스코의 「세계 문화다양성 선언」 제 5조는 "문화적 권리란 모든 사람들이 스스로 선택한 언어로 자신의 작품을 창조하고 배포할 자유와 문화다양성을 존중하는 교육과 훈련을 받을 수 있는 권리, 그리고 자신이 선택한 문화적 생활에 참여하고 실천할 수 있는 권리"로 정의한다. 기존 보편적인 인권 논의로 포함하지 못했던 문화적 자유와 다양성 신장에 대한 높은 '추상' 수준의 인권 정의로 볼 수 있다. 이제 정보통신기술의 급진전과 보편적 확대와 함께 새로운 신기술을 수용하는 시민들에게 '정보인권'은 기존 보편적 인권의 차원에서 다시 해석되고 확장되어야 할 또 다른 보편 권리의 영역으로 새롭게 부상하고 있다.

역사적으로 보면, 이미 2003년부터 유엔이 주관하고 국제통신연합(ITU)가 주최한 「정보사회 세계정상회의(WSIS: World Summit on the Information Society)」를 계기로 '정보사회'의 인권, 즉 '정보인권'을 보편적 인권의 틀에서 사유하려는 여러 시도들이 이뤄졌다. 정보인권은 정보통신기술이 인간 삶의 일반화된 구성물이 된 오늘의 세계에서 보편적 인간의 소통 자유를 보장하기 위해 마련됐다고 볼 수 있다. 정보인권이란 용어는 국내에서 같은 해에 등장[3]했고, 국가인권위원회가 2003년 주최했던 "정보화 사회에서의 인

2) 김기곤, 2011, 「한국사회의 문화권 구성과 제도화」, 『민주주의와 인권』, 11(2): 207-238.

권” 토론회에서 공식적으로 알려지기 시작했다. 사회적으로는 교육부의 ‘교육행정정보시스템(NEIS)’ 도입 논란 이후 ‘개인정보 자기결정권’ 등 시민의 온라인 인권이 부각되면서 정보인권 개념이 대중들에게 중심 의제이자 용어로 떠오르는 계기가 됐다.

우리에게 정보인권 개념은, 헌법 제 10조에 명시된 “모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다”라는 기본 인권적 정의의 측면에서, 그 가운데 정보의 유통에 관한 개인의 기본적 권리를 통칭하는 뜻으로 해석할 수 있다. 즉 정보인권은 “정보가 수집·가공·유통·활용되는 과정과 그 결과로 얻어진 정보가치에 따라 인간의 존엄성이 훼손되지 않고 이를 통해 삶의 조건이 개선될 수 있도록 하는 최소한의 권리”로 정의할 수 있다.[4)]

이는 정보통신기술이 인간 삶의 보편적 환경이 되는 현실 속에서 인간의 정보 접근과 표현의 자유, 사적 정보의 보호를 통해 개개인이 정보유통에 대한 통제력을 지닐 수 있도록 보장하는 권리 개념으로 볼 수 있다.[5)]

무엇보다 현실적으로 전통적 인권의 내용들, 표현의 자유, 알 권리, 사생활의 비밀과 자유, 정보통신의 비밀보장 등에 더해서, 새롭게 온라인 프라이버시권, 정보접근권, 정보문화향유권, 온라인상 표현의 자유 침해 등이 급격히 늘고 쟁점화하면서 ‘정보인권’은 헌법적 권리 해석을 근본적으로 견지하면서도 디지털 기술 환경에서 발생하는 독특한 동시대 인권 현상의 또 다른 해석 영역으로 바라볼 수 있다.[6)]

동시대 정보인권의 특징은 다음과 같다. 먼저 이는 보편적 인권의 일부로 사유되기도 하지만, 신기술 형성의 맥락에 의해 그 내용이 항시 새롭게 구성 중에 있다. 현대 신기술 환경이 매개된 인간 삶의 보편 인권 해석을 ‘정보인권’이라 본다면, 오늘날 이의 중요 요소 권리 유형들로 정보프라이버시권, 인터넷에서의 표현의 자유, 정보접근권, 정보문화향유권 등이 새롭게 제기됐다.[7)] 무엇보다 4차 산업혁명 시대 각광받는 인류의 신기술이

---

3) 오병일, 2003, 「정보사회 세계정상회의를 계기로 본 정보인권」, 『문화과학』, 제35호, 문화과학사.
4) 이민영, 2010, 「정보인권의 법적 의의와 좌표」, 『공동학술세미나 - 정보인권의 법적 보장과 그 구체화』, 국가위원회.
5) 이인호, 2009, 「정보인권의 개념과 헌법적 보장체계」, 국가인권위원회.
6) 정민경, 2012, 「국가인권위원회 10년: 정보인권과 국가위원회의 역할」, 『이슈리포트 <액트온>』, 진보네트워크센터.
7) 국가인권위원회, 「정보인권보고서」, 2013.

보편화되면, 그 권리에 새로운 해석이 가미되거나 유형에 변화가 있을 수 있다. 예를 들어, '잊힐 권리', '보편적 디자인/설계 권리(the right to universal design)', '알고리즘, 인공지능, 사물인터넷 등 이의 통제 투명성에 관한 권리' 등이 신기술의 등장과 함께 부각된 정보인권의 신생 영역들로 볼 수 있다.[8] 이로부터 새로운 형태의 정보인권 침해 사례를 발굴하고 유형화함으로써 이에 대한 정보 권리적 시각에서의 정책 대안 마련이 좀 더 구체화할 수 있을 것이다. 물론 '정보인권'을 보편주의적 시각에서만 접근하는 것도 문제지만, 그 모든 문제를 시대 상황과 국면으로 상대화해 해석하는 것 또한 피해야 할 요소다.[9]

둘째, 이들 정보인권의 유형들은 국가가 위로부터 상명하달 식으로 시민에게 부여하는 권리 개념과 내용이 아니다. 국민국가와 세계시민으로서 국민들 각자와 시민사회의 지속적 요구와 투쟁이라는 아래로부터의 동학을 통해 구성되는 새로운 실천 권리 개념으로 봐야 한다.[10] 즉 정보인권은 국가가 시민에게 부여하는 권리 개념으로 국한하기 보단 시민 스스로 새로운 환경 아래 아래로부터 형성하려는 적극적 쟁취의 권리 개념으로 볼 수 있다. 달리 말해 우리는 정보인권을 사회운동과 실천의 과정에서 만들어내야 할 '시민권의 정치' 항목으로 봐야 한다.[11]

셋째, 정보인권은 디지털 정보나 데이터를 매개해 발생하는 정보인권 침해 사례로부터 시민, 소비자, 노동자, 사회적 소수자 등을 보호하기 위한 방어적이거나 수세적인 정의법으로만 쓰여서는 곤란하다. 인권의 정치 실천적 맥락을 고려한다면, 인간의 민주적 정보소통을 위한 데이터 인권 보호 관점을 넘어서서, 좀 더 적극적으로 누군가 데이터를 갖고 성찰적으로 행하는 비판적 기술 권리 행사와 기술 역량의 배양 개념으로 해독할 필요가 있다. 정보인권이 곧 인간 주체의 데이터 보호 권리를 포함해 데이터 신기술을 자

---

8) Goggin, Gerard, Adriadne Vromen, Kimberlee Weatherall, Fiona Martin, Adele Webb, Lucy Sunman & Francesco Bailo. 2017. Digital Rights in Australia. Departments of Media and Communications, and University of Sydney.

9) 인권의 보편주의나 상대주의를 넘어서려는 논의는 철학자 지젝의 논점에서도 관찰된다. "인권을 정치투쟁의 우연적 영역과 별개의 비역사적인 '본질주의적' 피안(피안)으로, 역사로부터 면제된 보편적인 '천부적 인간권리'설정해서는 안되겠지만, 인권을 시민의 정치화하는 구체적인 역사과정에서 생겨난 사물화된 물신으로 간단히 도외시해서도 곤란하다." 슬라보예(Slavoj Žižek), 2006, 김영희(역), 「반인권론」, 『창작과비평』, 34(2), 404쪽.

10) Mouffe, ed., 1992. Dimensions of Radical Democracy: Pluralism, Citizenship, Community. New York: Verso.

11) 장미경, 2001, "시민권(citizenship) 개념의 의미 확장과 변화", 『한국사회학』, 35(6): 59-77.

기화하는 디지털 문식 역량(literacy)으로 연결되는 지점까지 살펴야 하는 대목이다. 정보인권의 접근과 시각이 기본적으로 정보 보호 대상으로서 개인이라는 수동적 해석과 접근에 줄곧 머물러 있었음을 인정한다면, 시민 주체의 정보와 데이터를 보다 비판적이고 성찰적으로 대응할 수 있는 능력까지 신장하는데 이르러야 할 것이다.

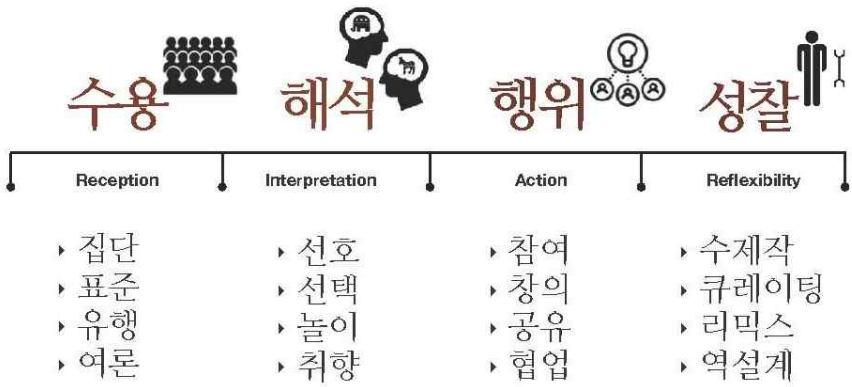
근래 크게 각광받고 있는 '데이터 주권(data sovereignty)' 개념은 정보인권과 유사하나 조금 차이를 갖는다. 데이터 주권 개념은 단순히 개인 정보 보호를 수세적인 방식으로 해석하거나 사업자들을 위해 데이터 활용 대세론을 옹호하려 하기 보단 좀 더 본질적으로 시민 주도형 데이터 사회의 합리적 미래를 구상하려는 목적을 지닌다. 데이터 주권은 데이터 주체의 보호와 활용 사이 접점을 찾기 어려운 대치 상황에서 이에 대한 화해책으로 고안되었다.

데이터 주권은 원래 데이터가 수집되고 저장되는 바로 그 국가 경계 내 법과 통치에 따라야 한다는 인터넷 영토론이다. 처음에 이 용어는 해외 다국적 닷컴기업들이 자국에 서버를 두고서 아예 국경을 넘어 국내 사용자들에게 플랫폼 서비스를 제공하면서 발생하는 다양한 문제들, 데이터 열람, 정정, 삭제, 이동에 관한 자국민의 데이터 권리들이 제약을 받으면서 주목을 받았다. 즉 데이터주권은 데이터의 현지 보관이나 해외 반출 금지 등 '데이터 국지화(data localization)'의 문제와 관련돼 있다. 최근에 데이터 주권은 데이터 국지화에서 좀 더 확장적인 의미로 쓰인다. 마치 국가 영토 개념 속에서 자국민의 주권 보호 마냥, 즉 개별 신체로부터 생성되는 정보와 데이터 부스러기의 생성, 처리, 선택 등에 있어서 보다 개인이 적극적으로 개입해 데이터 처분까지 직접 행할 수 있는 신체정보의 자율권으로 확대돼 쓰이고 있다. 하지만, 짐짓 우려되는 지점은 데이터 주권이 개별 정보 주체에게 자신의 데이터 활용과 처분에 대한 본인 판단과 자율권을 크게 향상시킬 수 있는 것처럼 보이지만, 반대로 보면 한국사회처럼 정보 오남용이 심각한 경우에 이 개념이 일종의 정부와 기업에 데이터 활용의 명분을 부여하는 알리바이처럼 보일 수도 있다는 우려감을 주고 있다.

결국, 정보인권과 데이터 주권 개념 모두 나름 한계를 지니고 있다는 점에서, 장기적으로 보자면 지능정보사회 시대에 대응한 과학기술을 성찰적으로 바라볼 수 있는 보편의 시민 능력을 확보하는 방법을 찾는 일이 더 중요해 보인다. 오늘날 시민 정보인권과 데이터 주권은 기실 전통적 의미에서 정보 내용을 비판적으로 해석하거나 콘텐츠를 생산하

는 단계를 넘어서서 데이터와 정보로 구성된 코드를 짜고 이를 담는 소프트웨어와 하드웨어 제작 및 디자인 설계에 적극적으로 개입할 수 있는 성찰적 역량 계발까지 고려해야 한다. 더 이상 인간의 논리적 통제력 아래 남아있지 않을 4차 산업혁명 신기술의 시대에 이와 같은 시민 정보역량에 맞춘 정보인권의 적극적 해석이 더욱 필요한 시점이다. <표1-1>에서 보는 것처럼, 이제까지 정보통신기술에 대한 리터러시(literacy)는 주로 개인에게 입력되는 정보에 대한 수용과 비판적 해석에 집중된 경향을 보였다. 즉 정보와 데이터를 어떻게 수용하고 해석하고 배제할 것인가의 문제에 주로 치우쳤고, 이에 각 주체는 대단히 기술 수용에 있어 수세적 입장에 놓여 있었다고 볼 수 있다.

사용자의 생산자적 지위(즉 미디어 다양성 측면에서 콘텐츠 제작 능력 강화)가 바뀌고, 최근 4차 산업혁명의 신기술 여파로 하드웨어-소프트웨어 제작력(메이킹 문화)이 주목받으면서 데이터와 정보 기술의 변조 및 성찰적 재설계 등이 주목받기 시작하고 있다. 즉 기술을 성찰적으로 바라보는, 현실 기술미디어 지형에 관한 '비판적' 기술 해석, 생산, 제작 능력이 정보역량의 핵심으로 떠오르고 있는 것이다.



<그림2-1> 정보인권의 확장성

정보인권이나 데이터 주권 개념과 범위는 향후에 이와 같이 전통 미디어의 해독력을 상징했던 미디어 리터러시(literacy)나 정보 침해 보호의 범위를 넘어서서 기술미디어 전반의 생산과 제작에 비판적으로 개입하는 능력을 교육하고 진흥하는 쪽으로 나아갈 필요가 있다. 이는 기존 정보 보호와 정보 자유와 향유의 기본 권리를 넘어서서, 억압적 권력의 기술설계와 디자인에 문제제기하고 이를 재설계하는 성찰적 능력을 보장하는 길이

기도 하다. 궁극적으로 정보인권과 데이터주권은 정보미디어기술로 매개된 인간 문명에 대한 구조적 비판과 기술디자인을 제대로 읽을 수 있는 국민의 성찰적 안목을 증대하는 쪽으로 독려하고, 이를 통해 다양한 대안적 기술 플랫폼과 시민이 주축이 된 정보통신기술·미디어 운용 기회를 확대하는 데까지 나아가야 한다.

2. 4차 산업혁명과 정보인권 침해 관련 선행연구 검토

정보통신기술의 발전에 따른 정보인권 침해 우려는 인터넷이 형성되던 초창기 시절부터 제기되어 왔다. 전자공간을 매개해 프라이버시와 인권 침해가 늘면서 이제 '정보인권'이라는 개념이 만들어지고 논쟁 지점들을 형성하기에 이르렀다.[12] 최근 개헌 논의에서도 대통령 개헌안과 국가인권위원회 개헌안에 기본권으로서 정보인권의 주요 내용들이 반영될 정도로 정보인권 보호의 필요성이 강조되고 있다. 이런 상황에서 4차 산업혁명, 특히 디지털 전환과 플랫폼 독점이 급속하게 이뤄짐에 따라 온라인 영역을 넘어서 오프라인과 융합된 형태로 더 확장된 정보인권 침해 가능성이 제기되고, 여러 현실적 문제들이 나타나고 있다. 대표적으로 캐시 오닐(2017)[13]은 <대량살상 수학무기>에서 빅데이터와 프로파일링으로 인한 차별과 불평등 심화 문제를 지적한다. 수학 이론, 빅데이터, IT기술이 결합해 만들어낸 빅데이터 모형이 정치는 물론 교육, 노동, 서비스, 행정, 보험 등 우리가 상상할 수 있는 모든 분야에서 막대한 영향력을 행사하고 있다고 말한다.

크리스티앙 푹스(Christian Fuchs)[14]는 빅데이터 기반 경제, 4차 산업혁명으로 진행된 경제변화의 모습을 잘 설명한다. 빅데이터를 기반으로 서비스를 제공하는 기업에게 데이터와 이를 생산하는 사용자는 유동자본이라고 할 수 있다. 기업 입장에서 개인화 서비스의 재료가 되는 빅데이터를 사용자가 24시간, 노동시간의 제한도 없이 무료로 생산해 제공한다고 분석한다. 이런 의미에서 개인의 데이터 생산 활동은 기업이 대가를 주지 않는 부불노동(unpaid labour)이다. 또한 빅데이터는 그것을 활용할 때 발생할 수 있는 프라이버시 침해와 감시 및 통제와 같은 근본적인 문제를 동반한다. 특히 경제적 감시(economic surveillance), 즉 타깃 마케팅이나 개인 맞춤형 서비스 운영을 위해 상시적으

12) 국가인권위원회, 「정보인권보고서」, 2013.
13) 캐시 오닐, 2017, 대량살상 수학무기, 흐름출판
14) Fuchs, Christian. 2014. Social Media: A Critical Introduction. London: Sage.

로 개인을 모니터링 하는 것은 프라이버시 침해와 감시의 일상화를 의미한다고 주장한다.

4차 산업혁명을 경제적으로 구현하고 있는 구글, 페이스북, 트위터 등 SNS 관련 기업 또는 웹 2.0 자본이 선도하는 디지털 경제의 형성과 우버와 에어비앤비 등 공유기업들의 발전과 함께 플랫폼 경제의 형성과 작동 방식은 개인정보 침해 문제에 주목을 끌고 있다. 안드레예비치(2011)[15]는 네트워크 속 인구들이 플랫폼에서 창출하는 가치를 사적으로 전용할 뿐만 아니라, 그들의 활동에서 분출되는 감정의 파동을 실시간으로 포착하고 상업적으로 관리·활용하는 빅데이터 경제로 진화하고 있다고 진단한다. 현대 경제에서 생산적으로 조정되고 조종되어 상품이나 브랜드에 대한 소비자들의 관심, 선호, 애착, 평판 형성과 구축의 밑바탕이 된다. 그래서 소비자들에 대한 인구학적 정보를 수집하는 것을 넘어서서, 그들의 지배적 정서나 감정의 파동을 실시간으로 탐색하고 활용하는 것에 집중한다. 문제는, 빅데이터 기반 플랫폼 경제가 '참여 감시(participatory surveillance)'에 기반한다는 사실이다.[16] 즉 예전에 기업들은 몰래 숨어 타깃 마케팅이나 개인 맞춤형 서비스 운영을 위해 상시적으로 개인을 모니터링 해왔다면, 이제는 사용자 놀이와 참여를 이끌어내며 프라이버시 침해와 감시의 일상화를 만들어내고 있다. 이와 같은 감시 유형은 언제 어디서나 즐거이 자신의 개인 위치, 생체, 데이터 정보를 자진해서 내놓는 현대인의 자발적 정보 제공의 측면을 묘사하며, 그와 같은 자발적 정보 제공 행위를 우리 모두가 일상적으로 체화하고 있다는 점에서 정보인권 침해의 작동은 꽤 자연스럽기까지 하다.

최근 소셜 미디어는 소비자들의 인지 정보와 선호 데이터를 수집하고 분석하기 위한 중요한 플랫폼이 되고 있다. 그만큼 이러한 개인정보들을 가지고 이를 소비할 시장을 형성할 뿐만 아니라 정서와 선호, 여론을 조작하는 일까지 가능케 하고 있다. 이항우(2014)[17]는 '애딘포메이션(adinformation)'이라는 개념을 통해, 구글의 주요 수익원인 광고 사업을 위해 구글이 어떻게 '유용한 광고는 곧 좋은 정보'라는 관념을 확산시키고, 그 속에서 구글 브랜드에 대한 사용자의 정서 등을 어떻게 동원하는지 분석한다. 또한 '디프라

15) Andrejevic, Mark. 2011. "The Work That Affective Economics Does." Cultural Studies 25(4-5): 604~620.

16) Anders Albrechtslund, Online Social Networking as Participatory Surveillance, First Monday, Volume 13, Number - 3 March 2008.

17) 이항우, 2014, "구글의 정동 경제(Affective Economy)", 『경제와사회』, 여름호(통권 제102호).

이버싱(deprivacing)'이라는 개념을 통해, 개인 데이터가 구글에 의해 어떻게 수집되고 활용되는지 그리고 그 속에서 사용자의 프라이버시가 침해받는 방식을 강조한다.

프랭크 파스콸레(2016)[18]는 <블랙박스 사회>에서 누구나 데이터베이스에서 '신용도 낮음', '의료비 높음', '소득 감소' 등의 모욕적인 평판으로 분류될 수 있으며, 평판 시스템은 오류나 불공정성 때문에 냉대 받는 (대개 보이지 않는) 새로운 소수자를 만들어낸다고 분석한다. 알고리즘은 차별이라는 근본적인 문제에서 자유롭지 않다. 알고리즘 내의 부정적이고 근거 없는 가정이 편견으로 굳어지기 때문이다. 알고리즘도 인간이 프로그래밍하는 것이다 보니 개발자의 가치관이 소프트웨어에 이식된다. 알고리즘은 흔히 너무도 인간적인 편견이 반영된 데이터를 사용하고 있는 것이다. 이 결과 차별이 일상화되고 내재화 된다.

이렇게 수집된 다양한 개인정보 및 인지, 평판, 선호와 관련된 정보는 지식재산권이라는 법제도적 장치를 통해 기업이 배타적으로 소유하는 것을 가능케 했다. Lee 외(2012)[19]에 따르면, 모든 사용자들을 자동적으로 규제하여 복제나 배포의 수단을 근원적으로 박탈하는 '디지털 저작권 관리 시스템(DRM)'이 기존의 법률적 수단보다 훨씬 더 구체적이고 효과적인 저작권 침해 방지 장치로 등장하게 되었다. 디지털 저작권 관리 시스템은 음악, 비디오, 도서, 소프트웨어 등의 데이터를 디지털 방식으로 암호화하여 특정한 소프트웨어와 기기에 의해서만 재생될 수 있도록 하는 기술 시스템이다. 또한 구글, 페이스북과 같은 SNS 기업의 이용약관에 의해서도 수집된 개인정보는 정보 생성 주체인 사용자의 자기통제를 불가능하게 만들고 있다. 가령, 유튜브는 "유튜브에 콘텐츠를 업로드하거나 게시하면, 당신은 유튜브에 그 콘텐츠를 서비스 제공과 관련하여 그리고 유튜브 사업 및 서비스 제공과 관련하여 사용하고, 재생산하고, 배포하고, 파생 작품을 만들고, 전시하고 공연할 전 세계적, 비배제적, 로열티를 지불하지 않는, 이전 가능한 라이선스(재라이선스할 권리와 함께)를 준다"(YouTube, 2013)라고 약관에 규정하고 있다.

한편, Askitas and Zimmermann(2015)[20]에 따르면, 현대의 노동 시장 동학에 대해 생각할 때, 특히 노동 시장 매칭에서 온라인 공간의 역할이 증가하는 것과 관련하여 기술

18) 파스콸레, 2016, 『블랙박스 사회: 당신의 모든 것이 수집되고 있다』, 안티고네.
19) Lee, Edwards, Bethany Klein, David Lee, Giles Moss and Fiona Philip. 2012. "Framing the Consumer: Copyright Regulation and the Public." Convergence, 19(1).
20) Askitas N. and Zimmermann K.F. "The internet as a data source for advancement in social sciences", 2015, International Journal of Manpower, 36 (1), 2-12.

이 주도하는 변화가 노동 조직에 미치는 영향을 반드시 고려해야한다. 21세기가 시작될 무렵 노동 매칭에 대한 웹의 역할이 연구되었지만 인터넷과 온라인 공간의 중요성은 그 이후로 극적으로 증가했다. 4차 산업혁명의 기술들이 빠른 속도로 진화하면서 노동시장도 온라인과의 융합이 확대되고 노동 조직 자체가 변화하고 있다. 4차 산업혁명과 일자리 문제에 대해서는 그동안 많은 연구가 진행되었다(예컨대 Acemoglu 외(2016)[21], Gregory 외(2016)[22], Autor(2015)[23], Frey and Osborne(2013)[24] 참조). 이중 로봇과 인공지능(AI)에 의해 인간노동이 대체될 것이라는 전망 즉, 노동의 소멸과 여느 산업혁명 시기와 같이 없어진 일자리에 대해 새로운 일자리가 생겨날 것이라는 낙관적인 전망이 교차한다. 특히 일자리의 양적 문제보다도 일자리의 질과 종류에 대한 분석이 주목을 끌고 있다. 디지털 경제 및 플랫폼 경제의 형성에 따라 노동인권과 노동과정이 다양한 양식으로 변화하고 있다.

Rudiger Krause(2017)[25]은 디지털화가 기술과 경제의 프로세스를 변화시킬 뿐 아니라, 노동조건, 업무장비, 노동조직에도 영향을 미친다고 본다. 디지털화는 제조업을 넘어 노동생활 전반에서, 특히 가치창출과 일자리 창출에서 중요성이 점점 커지고 있는 서비스업에서도 두드러지고 있는 현상이다. 디지털 노동세계에서 보호의 필요성으로 첫째, 법현실적 현상으로서의 노동과 생활의 경계가 사라지는 상황, 둘째, 근로가 없는 시간(휴식시간)의 보호, 셋째, 산업안전보건, 넷째, 정신적 스트레스로부터의 보호, 다섯째, 정보의 자기결정에 대한 보호로 규정한다. 그의 논의를 좀 더 확대해본다면, 최근 점점 치밀해져가는 노동통제와 데이터 전유의 기술적 장치를 막을 수 있는 일시적 수단으로 외부 연결 단절의 방법이 유효할 수 있다. 예를 들어, 실제 2017년 1월부터 프랑스는 시·공간적으로

21) Acemoglu, D and P Restrepo (2016) “The Race Between Machine and Man: Implications of Technology for Growth, Factor Shares and Employment” NBER Working Paper No. 22252

22) Arntz, M, T Gregory, and U Zierahn (2016) “The Risk of Automation for Jobs in OECD Countries,” OECD Social, Employment and Migration Working Papers, No. 189, OECD

23) Autor, D. (2015), “Why are there still so many Jobs? The History and Future of Workplace Automation”, Journal of Economic Perspectives, Vol. 29, No. 3.

24) Frey, C B and M A Osborne (2013) “The Future of Employment: How Susceptible are Jobs to Computerisation?” Mimeo. Oxford Martin School.

25) Rudiger Krause, “노동세계의 디지털화: 과제와 규제의 필요성”, 『국제노동브리프』, 2017년 3월호, 한국노동연구원

외부에 ‘연결되지 않을 권리(le droit de la deconnexion)’를 시행해 중요한 노동자 정보 권리로 삼고 있다. 이는 주 중 35시간 법정 노동시간에 더해 일과 외 그리고 주말에 경영자가 전화하거나 문자를 보내는 것을 불법화하는 디지털 시대의 노동인권 조항이라 평가된다. 외부로부터의 자율적 연결 차단권은 디지털 시대 노동 휴식권의 보장을 뜻하지만, 비노동시간의 영역까지 틈입한 기업의 통제력을 일시 제거한다는 점에서 시사하는 바가 크다. 기술로 매개해 개인의 신체를 거의 24시간 기업 지배의 자장 속에 놓으려는 현실을 제어하기 위해서 프랑스 정부는 일단 몸에 부착된 모바일 기계 장치의 가동을 멈추는 선택을 취했다. 연결되지 않고 외부 접속에서 순간 절연할 권리는, 현대 첨단 기술에 기댄 기업의 시·공간 통치 기제를 막기 위한 최소한의 정보인권으로 사유되는 셈이다.

4차 산업혁명과 디지털 전환의 확산 속에서 정보인권 침해의 우려가 제기 되면서 이에 대한 법적 제도적 분석도 이뤄지고 있다. 우선, 데이터 분석이 증가하면서 서로 다른 데이터를 연계, 결합하여 개별 데이터베이스로는 분석할 수 없는 새로운 의미를 찾고자 하는 시도가 증가하고 있다. 그러나 개인정보가 포함된 데이터가 활용될 경우, 연계, 결합을 통한 개인정보 침해 위험은 훨씬 높아지게 된다. 이와 관련해 이은우 외(2017)[26]는 주요 국가의 데이터 연계・결합 시 대상, 허용범위, 원칙, 안전조치 등에 관한 법규정 및 운영사례를 조사 분석하고, 정보주체의 권리가 침해되지 않는 데이터 연계의 원칙, 기준 마련 및 관련 법제도 개선사항을 제안하고 있다. 특히, 보건의료 영역을 비롯한 학술연구 및 통계 목적의 데이터 연계 현황을 분석하고, 관련 법제의 정비뿐만 아니라 연구 제안서의 검토, 안전시설, 연구자 교육 등 데이터 거버넌스 구축의 필요성을 제기하고 있다.

권건보 외(2017)[27]는 지능정보사회의 개인정보 환경변화를 분석하고 유럽, 북미 등 주요국가에서 이에 어떻게 대응하고 있는지 관련 법제를 분석하였다. 이를 토대로 국내 개인정보 보호법제의 현황과 문제점을 분석하고, 지능정보사회에 대응한 개인정보 보호법제의 정비 방안을 제시하고 있다. 즉, "현행 개인정보보호 관련 법제는 개인정보보호법과 정보통신망법, 신용정보보호법 등 다수의 개인정보 관련 입법이 병존함으로 인하여 입법

26) 이은우 외, 데이터 연계・결합 지원제도 도입방안 연구, 2017.12, 개인정보보호위원회 정책연구용역.

27) 권건보 외, 지능정보사회 대응을 위한 개인정보보호 법제 정비방안, 2017.12, 개인정보보호위원회 정책연구용역 보고서

체계상의 불일치나 중복, 수범자의 법적 혼란, 중복규제로 인한 사업자의 부담증가 등의 문제를 야기하고" 있고, "개인정보보호 법제의 집행기관과 감독기구도 개인정보보호위원회, 행정안전부, 방송통신위원회, 금융위원회 등으로 분산되어 있어 통일적이고 전문적인 개인정보보호의 기능을 수행하기 어렵게 하고" 있으며, 인공지능, 빅데이터, 사물인터넷 등 기술의 발전 및 그에 따른 개인정보의 침해 위험도를 고려하지 않는 현행 법제의 규제방식 및 규율의 적정성을 문제로 지적하고 있다. 이에 개인정보 보호법제를 개인정보보호법을 중심으로 일원화하고 개인정보보호위원회로 하여금 개인정보보호에 관한 집행 및 감독의 기능까지 통합하여 수행하도록 할 것을 제안하고 있다.

한편, 이상윤 외(2016)[28]는 바이오정보를 생체인식 정보, 유전정보, 건강관련 정보로 구분하고, 바이오 정보의 수집, 이용과 관련한 국내외 현황과 피해사례를 조사하였으며, 관련 국내외 법제도 현황을 검토하고 개인정보 보호관련 법제의 개선 사항을 권고하였다. 이에 따르면, 생체인식 정보의 법령용어를 정비하고, 바이오 정보를 민감 정보로 보호해야 하며, 정보주체의 동의권 강화, 개인정보 영향평가 실시, 프라이버시 중심설계 적용, 개인정보 감독기구의 감독 강화 및 특별한 보호조치 등을 제안하고 있다.

그 외에도 이인호 외(2017)[29]는 한국의 분산된 개인정보 감독체계의 문제를 보다 집중적으로 분석하고 있다. 유럽연합, 영국, 프랑스, 독일 등 해외의 개인정보보호 수행체계에 대한 분석을 토대로 개인정보 보호 수행체계의 기본모델과 필수조건을 규정하고 한국의 개인정보보호 수행체계의 현황과 문제점, 그리고 개선방안을 분석하고 있다. 이에 따르면 개인정보보호 수행체계는 '보호와 활용의 균형'을 이념으로 통합형 모델을 취하는 것이 바람직하며, 감독기능, 조사기능, 집행기능, 민원처리기능, 지원기능, 정책형성기능 등의 기능과 권한을 갖춰야 한다. 또한, 정부로부터의 독립성과 전문성을 확보할 수 있어야 한다.

28) 이상윤 외, 바이오 정보 수집, 이용 실태조사, 2016.11. 국가인권위원회 2016년도 인권상황실태조사 연구용역보고서.

29) 이인호 외, 한국의 개인정보보호 수행체계 발전방안 연구, 2017.6, 개인정보보호위원회 정책연구용역 보고서.

제2절 연구 설계 및 방법론

본 연구는 4차 산업혁명 시대 정보인권의 특징과 이로부터 한국 시민들의 관련 인식에 대한 실태 조사에 초점을 맞추고 있다. 이를 위해, 이 연구는 문헌 조사, 시민 설문조사, 관계 전문가 자문의 세 가지 구체적인 방법론적 접근을 취하고 있다.

먼저 문헌 조사의 경우에는, 정보인권의 개념을 정의하고 4차 산업혁명 관련 선행 연구와 학술 단행본들을 검토하고, 4차 산업혁명 관련 기술 동향들을 살피는데 주로 이뤄지고 있다. 무엇보다 4차 산업혁명 국면 국내외 법률 및 정책 동향과 시사점을 고찰하는 장에서 보다 집중적으로 문헌 조사를 실시하고 있다. 가령, 국내외 정보인권 관련 제도 분석을 위해, 국제기준, 가이드라인, 현행법령 등 언론 기사, 관련 시민단체 및 기관의 공개 자료 분석 및 국내 공공기관 정보 및 관련 법률 및 정책안이 분석되었다.

본 연구의 핵심 파트이기도 한 시민 설문 조사의 경우에, 조사대상은 일반 시민 1,000명을 표본 수집해 이뤄졌다. 본 연구의 연구진들의 수차례에 걸친 사전 설문지 작업을 통해 조사 내용은, 크게 4차 산업혁명에 대한 인식 정도, 4차 산업혁명, 특히 플랫폼을 매개한 데이터 수집의 부작용 및 인권침해요소 인식 정도, 4차 산업혁명과 노동(일자리) 불안정의 변화 인식 정도, 4차 산업혁명과 개인정보 보호 필요성 및 보호방안, 정책 개선 방안에 대한 의견을 묻고 있다. 이를 전문 설문조사 업체를 통해 성별, 연령병, 지역별 비율 등을 고려해 설문 조사를 실시하고 그 결과를 토대로 분석하고 있다.

시민 설문지 내용의 보완적 기제이자 4차 산업혁명 시대 정보인권의 과제에 대한 보다 전문가적 식견을 얻기 위해 관계자 혹은 전문가 심층 답변 조사를 이메일을 경유해 실시했다. 조사대상은 학계, 산업계, 정부 및 공공기관 포함해 총 30명의 의견을 청취하고 그 내용을 정리 요약했다. 구체적으로, 학계 및 법조계의 법률 전문가, 개인정보 및 기술 전문가, 공공기관 정책 담당자, 포털 등 업계 담당자를 대상으로 한다. 조사 내용은, 우선 4차 산업혁명의 부작용 및 인권침해의 원인과 요소, 개인정보 유출 사고의 이유와 이를 막기 위한 효과적인 방안, 가명정보의 활용 범위와 신뢰성 문제, 알고리즘 편향성과 차별에 대한 현재 상태와 극복 방안, 그리고, 빅데이터 등 개인정보 남용이 여론의 왜곡과 공동체의 민주주의에 미치는 부정적 영향과 대응책을 묻는 질문들로 구성됐다.

종합하면, 기존 정보인권 관련 논의의 점검과 이론적 접근, 기존 법제도적 해석은 주

로 문헌 분석을 통해 이뤄졌고, 시민 설문과 전문가 설문은 현재 4차 산업혁명 시대 정보인권의 의식 상태와 향후 대안 정책을 구성하는데 활용하고 있다.

제3절 4차 산업혁명 시대 정보인권 접근 모델링

4차 산업혁명 요소 기술들, 특히 이 보고서에서 3장에서 소개되는 사물인터넷, 빅데이터, 인공지능, 생체기술, 플랫폼기술은 이전의 디지털 일반의 무한복제적, 비경쟁재적, 네트워크적 특성에 덧붙여 다음과 같은 좀 더 확장된 기술의 특성을 확보해왔다.

신기술 각각은 모든 사물의 연결에서 오는 데이터 통제의 편재성, 빅데이터 분석 기술의 실시간성과 패턴 인식, 인공지능 알고리즘에 의한 특정 기능의 사회적 위임과 자동화 기제, 생체기술의 생체 데이터를 매개한 표적화된 신원 통제, 플랫폼 기술에 의한 자원의 효율성 극대화하고 사용자 데이터 포획을 야기한다. 이는 기술적으로 인류에게 긍정점을 시사하기도 하지만, 정보인권과 관련해 새로운 층위에서의 문제점을 드러내기도 한다. 즉 4차 산업혁명의 신기술을 특징으로 매개된 '정보인권' 침해는 이전과 많은 다른 특징들을 보여주고 있다. 이제까지 드러난 4차 산업혁명 시대 정보인권 침해의 주요 특징들을 보자면 다음과 같다.

<그림 2-2> 4차 산업혁명 시대 정보인권 침해 특징

첫째 빅데이터, 사물인터넷 등 대량 개인정보의 수집·생성과 유출을 꼽을 수 있다. 기존의 정형화된 데이터의 정보 오남용과 활용 보다는 소셜미디어 등 좋아요와 댓글, 사용자 위치정보 등 '비정형(informal)' 데이터의 대량 수집과 실시간 가공을 통해 얻는 '빅데이터' 분석이 중심 특징으로 자리잡아가고 있다. 이미 존재하는 공공정보와 기업의 소비자/사용자 정보는 빅데이터로 기능을 하고 있고, 사물인터넷과 인공지능 등이 합류하면서 사용자 데이터의 생성과 집적, 분석을 자동화하고 세밀화하고 있다. 문제는 일반 정보사용자들이 비정형 데이터의 오남용에 대한 적절한 대응을 하기가 쉽지 않고, 플랫폼 기술 등 데이터 수집 메커니즘 자체에 대한 인식이 적고, 국경 너머 시민 데이터 유출의 경우 접근성이 떨어져 문제 해결이 쉽지 않다는 점까지 고려해야 한다. 빅데이터 대량 유출 및 오남용 문제는, 국내 사용자들이 주로 머물며 이용하는 지배적 플랫폼들에서 사용자 정보와 데이터 관리와 취급의 투명성을 확보하는 일이 급선무로 떠오른다.

둘째, 빅데이터의 대량 주조와 유통 과정에서 다양한 기술이 포괄하는 개인정보의 상호 결합을 통한 '프로파일링'과 온라인 공간에서 개인 식별을 확산하는 '타깃팅'(targeting) 기술의 발전으로 개인정보가 (재)식별되고 특정의 목적으로 인지되는 경향이 더욱 확산될 것이다. 특정 신원의 프로파일링 기법을 통한 확증이 인권 침해의 소지를 지닌다는 점은 미국의 9.11 테러 이후 미 정보기관의 활동에서도 이미 드러난 일이다. 무엇보다 데이터 알고리즘 분석의 힘은 패턴 분석을 통해 미래 예측을 행하는 능력에서 나오는데, 이를 과신하면서 특정 인물의 시민 인권 위협은 물론이고 이를 시스템에 응용시 체제 위험까지도 키울 수 있는 가능성 또한 잠재해 있다.

셋째, 인공지능과 각종의 처리 프로세서를 통해 인간의 개입 없는 자동적인 알고리즘을 통한 감시와 차별의 확산이 이뤄지는 문제 또한 불거지고 있다. 특정의 자동화 기술이 인간의 판단을 대신하면서 이를 사회적으로 '위임'하는 일이 점점 잦아지고 있다. 예컨대, 사회복지시스템 등은 몇 가지 복잡한 기준 데이터나 입력 값을 통해 복지 수혜 대상자를 결정하는 일을 대신함으로써 사회적으로 취약 계층들이 온라인을 통한 복지 혜택에 접근하려는 의지 자체를 사실상 무너뜨리는 경우가 흔하다. 사회적으로 자동화 기술을 매개해 판단을 위임하는 것이 문제이기도 하거니와 그 판단을 어디까지 기술에 위임할 것인가를 고민하는 노력이 요구된다.

넷째, 감시도 지능화하여 특정 권력 감시가 개인의 세세하고 은밀한 영역까지 확대하

고 일상적으로 이뤄지는 형태로 발전하고 있다. 감시기술의 첨단화는 물론이고 감시 자체가 강제력을 동반하기 보다는 사용자의'자발적'혹은 암묵적 동의 기제를 활용해 '놀면서' 개인 정보를 내주는 '참여감시'의 형태까지도 보여주고 있다.[30] 이는 언제 어디서나 기꺼이 자신의 개인 위치, 생체, 데이터 정보를 자진해서 내놓는 현대인의 자발적 정보 제공의 측면을 묘사한다. 동시대 지능형 감시 기제는 자발적 정보 제공 행위가 일상적으로 체화된 현실 안에서 작동하고 있다고 볼 수 있다. 예를 들면, 사용자들에게 카카오톡은 '놀이'의 일종이지만, 이 플랫폼을 통해 사용자 데이터는 쉽게 시장 가치화하거나 국정원과 검찰 등의 대민사찰 기제로 오남용된 전력이 있다.

다섯째, 이제 정서, 선호, 의식 등 감정세계와 정신의 내밀한 영역까지 표시되고 축적되며 알고리즘을 통해 분석되거나, 끊임없이 전자적으로 연결될 것을 (비)강제적으로 종용하면서 현대인은 사회적 스트레스와 정신적 자율성 침해에 크게 시달리고 있다. 특히, 국내 노동의 불안정성이 증대하면서 휴대전화를 통해 일과 외 스트레스 지수를 상승시키는 모바일문화가 확대되고 있다. 이의 자정 작용이 사회적으로 합의되지 않는다면, 노동하는 현대인의 삶의 질 개선은 요원할 것이다. 게다가 소셜미디어를 통해 가짜뉴스와 댓글조작 등이 범람하면서 과연 대중이 무엇이 팩트의 영역으로 다루어야 할지에 대해 판단불능의 상태 또한 만들고 있다. 이는 시민들의 가치 판단 혹은 정신 자율성 침해로 나타나고, 궁극적으로는 또 다른 형태의 민주주의 위기를 양산한다.

4차 산업혁명 시대에 정보인권 침해의 이와 같은 특징들이 국내외적으로 지배적인 경향으로 나타나고 있다고 볼 수 있다. 이를 정보 권리 주체들로 보자면, 첫째, 국가와 시민적 권리에 대한 정보인권의 침해 대상으로 시민, 둘째, 기업에 의한 정보 피해 당사자로서 소비자/사용자, 셋째, 노동 활동의 주체이며 기업 고용주에 의한 감시와 차별의 대상으로서 노동자로 구분해 볼 수 있을 것이다. 물론 여성, 청소년, 성소수자 등 사회적 약자를 근거로 정보인권의 주체를 나눠 볼 수도 있겠으나, 본 연구에서는 주로 이 세 주체, 즉 시민(국가), 소비자/사용자(기업-공급자), 노동자(기업-고용주)를 주로 해 정보인권의 침해 유형과 사례를 살피고 그에 대한 정책 개선과 대안을 고민하려 한다. 이 세 정보 주체들과 동시대 발생하는 정보인권의 침해 특징을 연결해 세부적으로 살펴보면 다

30) Albrechtslund, Anders. 2008. Online social networking as participatory surveillance, First Monday, 13(3), March.

음과 같은 표를 얻을 수 있다.

<그림 2-3> 정보인권 주체에 따른 침해 특징들

시민, 소비자, 노동자 각 주체별로 신기술로 매개되는 정보 침해 특징들을 살핌으로써, 정책 대응의 범위와 대상이 좀 더 분명해지는 효과를 얻을 수 있다. 물론 시민, 소비자, 노동자로서 정보주체는 한 개인이 지닐 수 있는 다면적 주체 영역이긴 하지만, 정보인권 침해 사안이 발생하는 경로와 문제 대응을 위해 그 범위와 대상을 지정해 접근할 수 있도록 한다는 점에서 좀 더 분명하다. 본 연구에서는 다섯 가지 침해 특징을 중심으로 사례 분석과 쟁점을 구체적으로 논의하겠으나, 각 특징을 논하면서 이 세 정보인권의 주체 가운데 특별히 강조되어야 하는 대상에 좀 더 방점을 두고 세부 논의를 이끌어가고 있다. 예를 들어, 모바일 연결을 통한 정신적 침해나 사회적 스트레스 지수는 오정보에 시달리는 시민이나 광고에 파묻힌 소비자 영역에도 해당되는 사항이지만 국내에서 사실상 노동자로서 정보주체에 대한 인권침해(노동시간 외 카톡방이나 문자 메시지를 통한 스트레스 압박 등) 문제와 좀 더 밀접히 연결돼 있기 때문이다.

제3장 신기술 동향과 정보인권의 쟁점

제1절 신기술들의 생태계

사물인터넷(IoT), 빅데이터, 인공지능, 생체인식, 플랫폼 기술은 각기 어느 정도는 독자적인 기술로 간주하여 이해할 수 있지만 결코 그 자체로 단일한 기술로 발전할 수 없다. 어느 하나의 기술이 다른 기술의 토대 위에 있지 않거나 다른 기술의 발전의 토대가 되지 않는 경우가 없다. 예컨대 인공지능이나 자율주행 자동차는 빅데이터의 구축 없이는 불가능하며, 빅데이터는 또한 사물인터넷이나 플랫폼 기술 없이는 구축될 수 없다. 드론이나 자율주행 자동차는 그 자체로 움직이는 사물인터넷이자 데이터를 수집하는 플랫폼이고, 인공지능은 수집된 빅데이터를 학습하여 자율주행 자동차를 가능하게 한다.

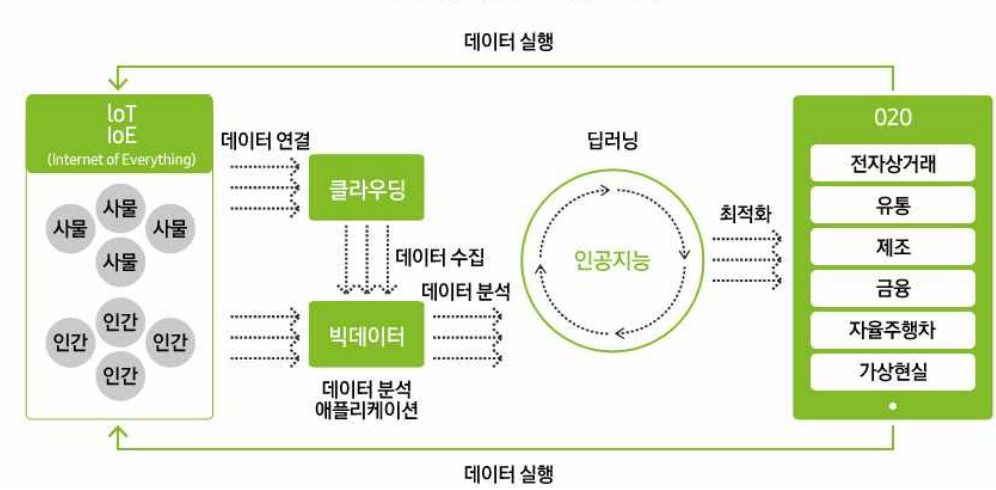
따라서 이들 기술은 겉보기로는 분리되어 있으나 전체적으로는 서로가 서로를 되먹임하는 하나의 거대한 생태계를 구성한다고 할 수 있다. 이 기술들은 흔히 4차 산업혁명의 핵심 요소들로 언급되는데, 시장이나 정부에서 굳이 4차 산업혁명이라는 용어를 사용하는 이유는 각각의 기술들 모두를 포괄하면서도 서로서로 연결되어 다른 기술의 발전에 결정적인 영향을 끼치는 기술들의 구성을 칭할 수 있는 편의가 있기 때문이다.

이러한 기술들은 근본적으로는 자연계와 인간 사회에서 생산 및 추출 가능한 모든 종류의 데이터를 원료로 삼아 각 영역에서 발전하고 있다고 볼 수 있다. 또한 이 기술들을 데이터를 어떤 단계에서 어떻게 사용하는가에 따라 다음과 같이 분류할 수 있다.

- 사물인터넷은 인간 및 비인간(사물)에서 발생가능한 모든 데이터를 센싱, 측정, 수집하는 기술을 의미한다. (데이터 자원은 모바일 기기들과 클라우드 컴퓨팅을 통해 수집되고 저장, 축적, 혹은 확산된다.)
- 빅데이터는 거대한 데이터를 수집하고 분석, 처리할 수 있는 여러 기술들의 조합을 일컫는다.
- 인공지능은 축적, 분석된 데이터를 통해 기계를 학습, 훈련시켜 인간의 판단이나 결정과 유사하게 시뮬레이션할 수 있도록 만드는 기술을 말한다.

· 생체인식 기술은 센서를 통해 수집되는 데이터 중에서도 인간의 신체의 특징을 포착하거나 그와 관련되어 생성되는 데이터를 활용하여 사용자의 신원 등을 확인하는 기술을 말한다.

· 플랫폼 기술은 데이터가 순환하는 환경(생태계)을 조성함으로써 앞서의 기술들을 서로 연결하고 그 과정에서 새로운 가치를 산출하는 기술을 의미한다.



<그림3-1> 4차 산업혁명의 작동 원리

이러한 핵심 기술들 이외에도 4차 산업혁명의 대표적 기술로는 로봇, 드론, 무인자동차, 3D 인쇄, 나노 기술 등이 거론된다. 물론 이러한 기술들은 4차 산업혁명을 이끌어가는 핵심적인 기술이기도 하지만 핵심 기술들의 응용 혹은 융합 기술, 나아가 플랫폼 기술에 포함시킬 수 있다. 아래 상술하는 다섯 가지 핵심기술은 각각이 4차 산업혁명이라 칭하는 산업구조의 혁신적 변화를 선도한다고 볼 수 있지만, 중요한 점은 여러 기술들의 상호 연결성 혹은 데이터를 중심으로 한 순환적 산업 생태계의 구성에 대한 인식이다. 그러한 인식을 통해, 전체 순환하는 산업의 구조 내에서 특정한 기술의 여러 측면에서 발생 가능한 정보인권과 관련한 쟁점 혹은 문제에 대하여 자세하게 점검해 볼 수 있기 때문이다.

따라서 이 장에서는 정보인권 침해의 구체적 사례나 위험성에 대해 깊이 들여다보기

보다는 각 기술들의 기본적인 개념과 특성, 시장 동향, 그리고 정보인권 쟁점 발생의 가능성을 점검하는 것을 목표로 한다. 그리하여 다음 장에서 사회, 산업, 일상의 영역에서 여러 기술적 과정을 통한 정보인권의 침해가 발생하는 구체적인 사례들을 살펴보는데 기초적인 이해를 제공한다.

제2절 신기술 동향: 핵심 기술을 중심으로

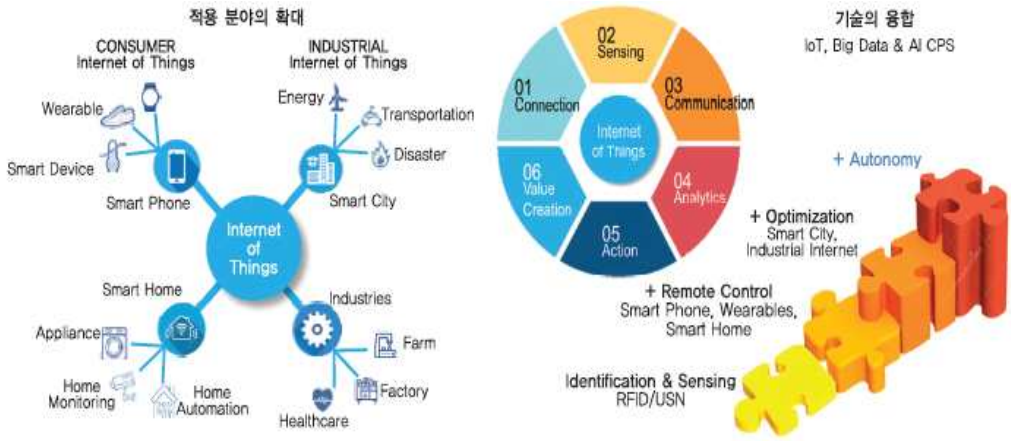
1. 사물인터넷

1) 개념 및 특징

사물인터넷(IoT)은 몸에 부착하거나 착용할 수 있는 웨어러블(wearable) 디바이스와 다양한 사물이나 장소에 설치되는 스마트 센서와 같은 ICT 디바이스/단말기를 통해 사물이나 인간 주변의 다양한 데이터를 측정, 수집하고 인터넷을 통해 통신하는 것을 의미한다. 인간, 사물, (통신)서비스라는 세 가지 구분되는 행위자들이 구성하는 환경에서 인간의 명시적 개입 없이 상호 협력적으로 센싱, 네트워킹, 데이터 처리 등의 지능적 관계를 형성하는 연결망 자체를 뜻하기도 한다.

현재 사물인터넷의 발전 방향은 '적용 분야의 확대'와 '기술의 융합'이라고 할 수 있다. 영역의 확대라는 측면에서는 초기 IoT가 주로 웨어러블, 스마트 기기, 스마트홈 등 일반 소비자를 대상으로 했다면, 최근에는 전 산업분야로 확대되면서 산업 IoT로 발전하고 있다. 기술 융합이라는 측면에서는 초기 IoT가 센서/단말, 무선통신, 원격제어 등을 중심으로 한 연결 통신 서비스에 집중되었다면, 최근에는 빅데이터, 인공지능, 가상물리시스템 등의 기술과의 융합을 통해 데이터 분석, 예측, 자율제어를 통한 새로운 가치창출로 이어지고 있다.[31]

31) 김현, 황승구, "IoT의 과거, 현재 그리고 미래", 전자통신동향분석 제33권 제2호, 2018년 4월, 3쪽.



<그림3-2> 현재 IoT의 방향: 영역의 확대와 기술의 융합

2) 현황

매킨지(2016.6.)는 전세계 IoT 시장의 규모가 2015년 9억 달러에서 2020년 37억 달러로 연평균 32.6% 성장할 것으로 보고, 잠재적 경제 효과는 2025년까지 2조7천억 달러에서 최고 6조2천억 달러까지 예측하고 있다.

"시장조사회사 IDC는 2016년 G20 국가들을 대상으로 사물인터넷 개발 기회 지수(Internet of Things Development Opportunity Index)와 국가별 순위를 발표한 바 있으며, 여기서 한국은 미국에 이어 2위를 차지하였다. IDC는 한국이 다른 상위권 국가들에 비해 상대적으로 GDP 규모가 크지 않음에도 불구하고 통신 인프라, 정부 지원, 사물인터넷 투자 등 비즈니스 환경 측면에서 다른 국가들보다 앞서 있다고 높게 평가하였다."[32]

32) 김용균, "스마트홈을 넘어 다양한 분야로 확산되는 IoT", 주간기술동향, 정보통신기술진흥센터, 2018. 4. 25., 17쪽.

<표3-1> 국내 업체들의 사물인터넷 관련 동향(IITP)

구분	기업명	최근 동향
스마트 가전	삼성전자	- 2018년부터 출시되는 모든 가전제품에 OCF 인증을 받을 계획 - 사물인터넷 기기용 보안 칩 솔루션 개발 - NB-IoT 연동이 가능한 IoT 위치 알림이 「커넥트 태그」 출시
	LG전자	- 일반 가전에 부착하여 제품 상태를 파악하고 원격으로 제어할 수 있는 스마트씽큐 센서와 허브 출시 - 문을 두드려 냉장고 내용물을 볼 수 있고 스마트씽큐 앱과 연동할 수 있는 IoT 냉장고 「LG 디오스 노크온 매직스페이스 냉장고」 출시
	동부대우전자	- SK텔레콤 스마트 홈 서비스에 연결될 수 있는 IoT 벽걸이 드럼 세탁기 「미니」 출시
	쿠쿠전자	- LG유플러스와 손잡고 IoT@home 앱과 연동되는 IoT 밥솥, IoT 공기청정기, IoT 생수기 등 3종 출시
	SK매직	- 이동식 습도 센서와 IoT 기능을 적용한 「매직 안심 가습기」 출시
	경동나비엔	- IoT 보일러 「나비엔 콘덴싱 스마트 톡」 출시
	귀뚜라미보일러	- 원격 제어뿐만 아니라 사용자 생활패턴을 분석하고 학습하는 IoT 보일러 「거꾸로 IoT 콘덴싱 가스보일러」 출시
	린나이코리아	- SK텔레콤/LG유플러스 스마트 홈 서비스와 연동 가능한 IoT 보일러 「스마트 와이파이 보일러」 출시
	코웨이	- 공기질 측정이 가능한 IoT 공기청정기 「아이오케어」 출시
	콜러노비타	- LG유플러스 IoT@home 앱과 연동할 수 있는 IoT 비데 출시
특정 산업용 제품	이도링크	- IoT 가스원격검침기 개발
	모다정보통신	- 일본 히타치에 IoT 모듈과 단말기 공급
	바른전자	- KB국민은행에 IoT 디지털저금통 「리브통」을 공급하고, 세계에서 가장 작은 크기의 로라 통신 모듈 개발
	솔루엠	- SK텔레콤 로라 망을 기반으로 위치를 확인할 수 있는 「키코」, 「키코 카드」, 「키코 미니」 출시

사물인터넷 사업을 영위하는 국내 사업체 수는 2,118개로 조사되었으며, 사물인터넷 사업 분야별 사업체 수는 서비스 분야 사업체가 1,098개사(51.8%)로 가장 많았고, 다음으로 제품기기, 플랫폼, 네트워크 순으로 조사되었다.[33]

33) 한국사물인터넷협회, “2017년도 사물인터넷 산업 실태조사”, 정보통신산업진흥원, 2017.

3) 쟁점

사물인터넷이 사회적으로 수용되기 위해서는 이러한 사회적 신뢰가 필요한데 사물인터넷의 경우는 기존의 인터넷에 비해 상대적으로 어려운 과제들이 있다. 예를 들면 사용자들이 인지하지 못하는 인공지능의 알고리즘들, 숨겨져 있는 기기와 센서들은 사용자들에게 막연한 불안감을 주는 요인들이다. 또한 사물인터넷은 기존의 인터넷에 비해 현실세계에 훨씬 더 많은 영향을 주게 될 것이므로 사물인터넷의 오작동이나 해킹으로 인한 피해는 매우 치명적이다.[34]

사물인터넷 환경이 정착되기 전까지는 데이터의 훼손, 기기의 오작동 등으로 인한 손실이 기존 인터넷 환경에 비해 많이 발생할 것으로 예상된다. 사물인터넷 환경 하에서는 발생한 손실에 대한 책임 소재를 가리기가 더 어려워지며 개발자/공급자와 사용자 사이에 존재하는 정보의 비대칭성으로 인해 사용자에게 불리한 결정이 내려지기 쉽다.

사물인터넷 환경은 스마트 전력계나 웨어러블 디바이스와 같이 개인의 생활을 관찰하는 기기나 센서들이 편재하는 세계다. 따라서 개인의 생활의 모든 측면이 수치화되어 타인, 특히 기업들에게 점점 더 많이 드러남에 따라 사적인 공간은 점점 더 축소된다.

2. 빅데이터

1) 개념 및 특징

빅데이터는 다양한 센서, 단말기 등을 통해 수집된 방대한 크기의 데이터를 뜻하는데, 빅데이터의 기술은 이렇게 수집, 축적된 데이터를 빠른 속도로 저장, 분석함으로써 데이터의 의미를 찾고 그 결과를 의사결정 과정에 반영할 수 있도록 돕는다.

대부분의 거대 글로벌 인터넷/미디어 플랫폼 기업들은 본질적으로 빅데이터와 사물인터넷의 결합을 통해 수익을 창출한다. 구글, 애플, 아마존 등은 클라우드와 빅데이터의

34) 박유리 외, “인터넷의 진화와 사회경제적 패러다임 변화연구: 사물인터넷을 중심으로”, 정보통신정책연구원, 2015.

경쟁력을 가진 플랫폼 사업자로서, 저가의 인터넷 연결 디바이스들을 보급하고 이를 통해 수집되는 빅데이터를 축적, 분석함으로써 소비자/사용자에 대한 정보를 얻어 미래의 수익을 보장받는다. 또한 이 정보를 다른 사업자들(예를 들어 광고업)에 판매함으로써 수익을 극대화할 수 있다.

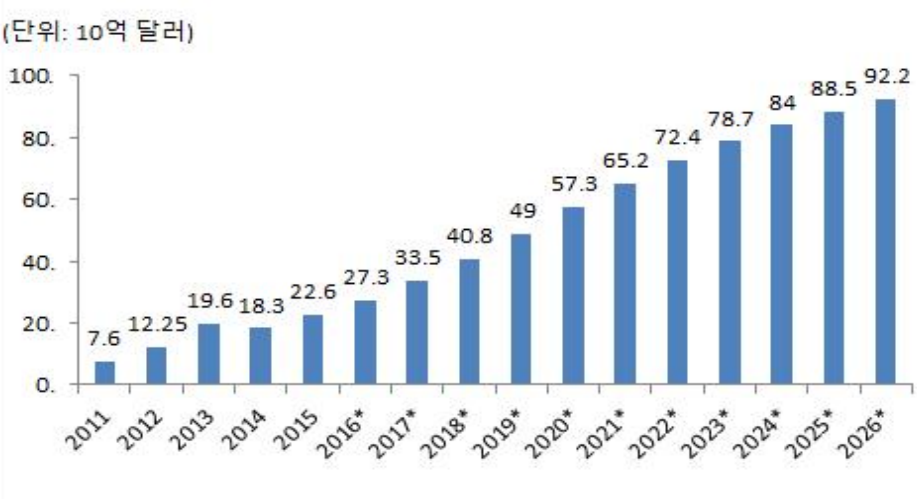
빅데이터 시대에는 데이터가 바로 경제적 자산이 된다. 이에 따라 한국 정부 또한 빅데이터를 활용하여 정부의 역량을 강화하고 보다 나은 공공서비스를 제공하기 위해 다양한 정부/민간 데이터 융합분석을 추진해오고 있다. 대표적인 예로, 과학기술정보통신부(舊 미래창조과학부)와 질병관리본부는 KT가 가진 통신 데이터를 활용하여 해외 감염병 예방을 위한 민·관 빅데이터 융합사업을 추진하였다. 서울시에서는 빅데이터 분석을 통해 실제로 시민이 필요로 하는 심야버스노선을 개발하고 2013년부터 해당 노선을 운행하는 일명 '올빼미버스' 서비스를 시행하고 있다. 또한 한국교통연구원은 일부 구간에서만 관측되던 공공의 관측교통량 자료와 전국 단위로 수집되는 민간의 내비게이션 자료를 융합하여 전국의 미관측 도로의 교통량을 추정할 수 있는 'ViewT 1.0'을 2017년 9월부터 서비스하기 시작하였다.

2) 현황

글로벌 시장조사 기관인 IDC에 의하면 2025년 전 세계의 데이터 생산량은 약 163ZB 정도의 크기가 될 것으로 예측되며, 이는 2016년에 생성된 16.1ZB보다 약 10배정도 늘어난 규모이다.[35]

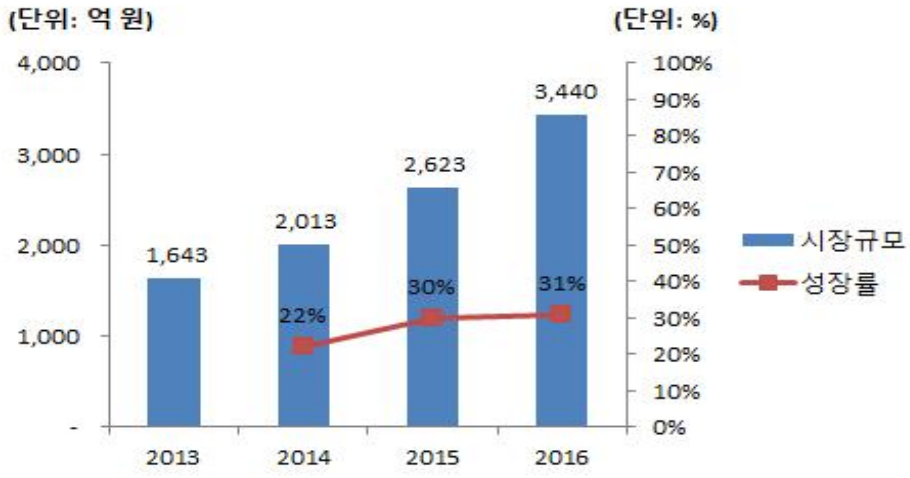
시장조사기관인 Wikibon에 따르면 소프트웨어, 하드웨어, 서비스를 모두 포함한 세계 빅데이터 시장은 앞으로 10년 후인 2026년에 총 922억 달러의 규모로 성장할 것으로 전망된다. 이는 2014년 기록했던 183억 달러에서 약 404% 증가한 수치이며, 2014년부터 2026년까지의 연평균 성장률은 14.4%에 달한다.

35) 박선우, "빅데이터 시대와 데이터 융합", 『정보통신방송정책』, 제30권 1호, 2018.



<그림3-3> 빅데이터 세계시장 규모 예측: 2011-2026

한국정보화진흥원의 '2016년 빅데이터 시장현황 조사'에 따르면 2016년 한국의 빅데이터 시장 규모는 전년대비 31.1% 성장한 3,439.6억원이었다. 뿐만 아니라 국내 빅데이터 시장은 최근 3년(2014~2016년) 동안 연평균 27.9%의 성장률을 기록하며 매우 빠른 속도로 그 규모가 확대되고 있다.



<그림3-4> 국내 빅데이터 시장규모 추이: 2013~2016

2016년 국내 빅데이터 시장의 영역별 비중을 살펴보면 민간시장 71%, 정부·공공시장 29%로 이루어져 아직까지는 민간영역이 빅데이터 시장을 주도하고 있는 것으로 보인다. 그러나 정부·공공시장의 경우 정부의 적극적인 빅데이터 활용정책에 따라 전년 대비 43.1%의 높은 성장률로 시장비중이 2%p 증가하였으나, 민간시장은 전년 대비 26.8% 성장하는 데 그쳐 시장비중이 오히려 하락하였다.

한국은 2013년 「공공데이터 제공 및 이용 활성화에 관한 법률」을 제정한 이후 공공데이터를 적극적으로 개방하려고 노력하고 있다. 이 때문에 한국은 2017년 OECD 공공데이터 개방 평가에서 1위를 차지했고, 현재 한국의 데이터 개방 정도는 세계적으로도 매우 높은 수준이라고 할 수 있다. 행정안전부에서는 공공기관이 생성 또는 취득하여 보유하고 있는 공공데이터를 한 곳에서 제공하는 통합창구로 공공데이터포털(https://www.data.go.kr)을 운영하고 있다. 2011년 7월 '국가공유자원포털'이란 이름으로 처음 포털을 개방한 이후, 공공데이터포털에서 제공하고 있는 데이터 건수는 2013년 5,272건에서 2017년 12월 현재 24,636건으로 약 5배가량 늘어났다.

국내 기업의 경우 KRG가 국내 매출 500억 원 이상 209개 기업을 대상으로 조사한 빅데이터 도입현황에 따르면 2017년 8.3%였던 도입률이 2018년에는 15.6%로 7.3%p 증가한 것으로 나타났다. 빅데이터를 도입한 기업 중 52.9%는 실제 업무에서 빅데이터를 활용하고, 35.3%가 파일럿 수준이었으며, 11.8%가 개념 이해 수준으로 나타나 빅데이터가 업무 수행 과정에 있어서 적지 않은 비율로 실제 활용되고 있는 것으로 분석됐다.[36]

3) 쟁점

지금까지 고의에 의해서든 기술적 한계에 의해서든 개인정보 빅데이터를 유출해 온 국내 기업 및 정부 조직에 대한 처벌은 실제 피해의 규모만큼 제대로 이루어지지 않았다. 유출된 개인정보 빅데이터들은 제3자에 판매되어 다양한 범죄나 불법적 마케팅에 활용되고 있다. 각종 인터넷 쇼핑몰이나 게임회사, 그리고 금융권 및 미디어 기업 등에서 국민 1천만 명 이상의 개인 정보가 유출되는 사고가 2014년 이후 지속적으로 발행하고 있으며, 실제로 이렇게 유출되거나 불법적으로 수집된 개인정보의 빅데이터는 또한 불법

36) "올해 국내 빅데이터 시장 규모 5600억…전년비 30.2% 증가", 데이터넷, 2018. 5. 9.

적으로 유통되기에 이른다. 문제는 이렇게 유출된 개인정보 빅데이터가 어느 정도의 피해를 개인에게 입히고 있는지 계산해내는 것이 불가능하다는 점이다.

빅데이터는 대량의 개인정보가 수집 및 관리되므로 사업자의 고의 또는 과실에 의해 개인정보가 침해 혹은 누설될 수 있다. 정부부처에서는 '개인정보 비식별 조치 가이드라인'을 2016년부터 시행하고 있지만 빅데이터로 수집된 개인정보는 여전히 재식별될 가능성이 잔존한다. 수집 및 분석된 빅데이터에 의해 개인이 식별가능하게 되면, 그 데이터를 가진 기업체나 기관은 각 개인의 모든 것을 그 개인보다 더 잘 알 수 있다. 이를 통해 맞춤형 광고로 개인에 접근하거나 개인이나 집단을 타깃으로 하여 다양한 상품을 팔거나 사업을 수행할 수 있게 된다.

나아가 국가기관은 수집된 개인정보를 통해 국민의 활동이나 상황을 무분별하게 감시하고 통제할 수 있게 된다. 주로 인터넷이나 각종 통신기기 등을 통해 대량으로 생산되는 국민들의 데이터는 국가 정보기관에 의해 수집되면서 국민들을 무차별적으로 감시하는 수단으로 쓰일 수 있다.

3. 인공지능

1) 개념 및 특징

인공지능은 기계적인 프로세스로서 빅데이터(즉 수치화되어 주어진 경험)를 통해 사태의 패턴을 학습하고 그에 기반하여 사람의 판단이나 지식과 매우 유사한 방식으로 주어진 과제를 수행하고 문제를 해결하도록 지원하는 기술을 말한다. 인공지능 기술은 단순히 하나의 단일한 기술이 아니라 여러 수준의 다양한 기술들을 포괄하여 그렇게 부르는 경향이 있다. 흔히 인공지능(AI)은 머신러닝 기술과 같은 협의의 기술을 가리키며 이는 인공지능 토대(AI Foundation) 기술로 이해할 수 있다. 나아가 가상 비서 소프트웨어와 같은 지능형 앱(Intelligent Apps)이나 로봇청소기와 같은 다양한 스마트홈 기기들을 가리키는 지능형 사물(Intelligent Things)도 광의의 인공지능 기술에 포함할 수 있다.

인공지능 기술은 그것의 원료가 되는 데이터를 빠른 속도로 수집, 전달, 저장, 분석하는 기술(ICBM - IoT, Cloud, Big Data, Mobile)의 발전에 기반하고 있다. 따라서 인공지

능 기술은 그 자체의 발전과 동시에 다른 핵심 기술들의 발전을 이끌어내고 있다. 이 기술들은 하나의 거대한 생태계를 구성하면서 사회 전반에 걸친 혁신과 파급력을 행사할 것이다.

인공지능 기술은 4차 산업혁명이라고 불리는 현재의 기술 혁신의 과정에서 핵심적인 위치를 차지한다. 그 이유는 다양한 종류의 기술과 장치들을 통해 수집 및 축적된 온갖 종류의 빅데이터가 분석 및 마이닝 과정을 통해 결과적으로 여러 인공지능을 개발 및 향상시키는데 사용되기 때문이다. 또한 이 인공지능 알고리즘들은 다시 전자상거래, 유통, 자율주행, 가상/증강 현실과 같은 구체적인 플랫폼 기술과 생체인식, 금융 및 보험, 변호사, 상담, 기자, 번역, 큐레이터, 감별사, CCTV 분석, 자연재해 예측 등의 작업(및 직업)들에 적용되기 때문이다. 즉 인공지능 기술은 데이터를 통해 만들어지고 다시 데이터를 통제하여 다양한 업무를 수행하는 역할을 한다.

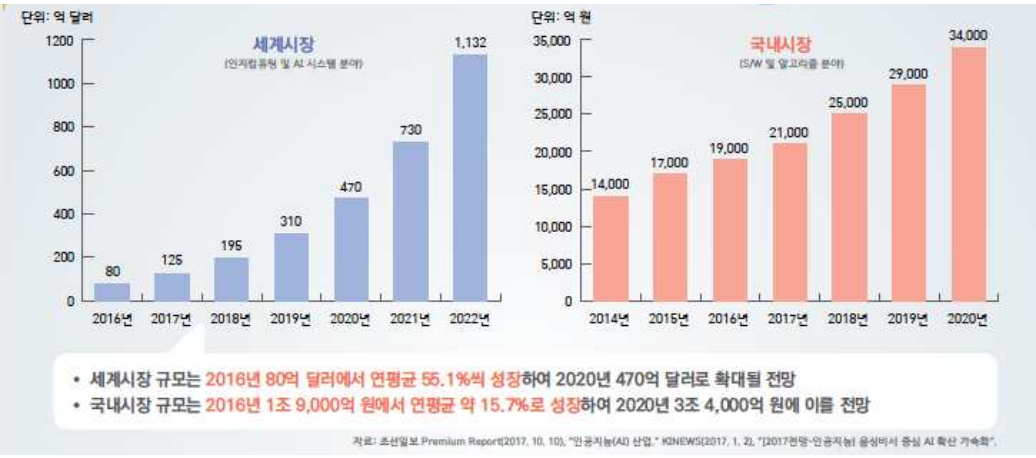
다수의 글로벌 IT기업들은 현재 인공지능이라고 불리는 기술의 상당 부분은 인공지능 비서, 음성 비서 등으로 불리고 있는 인공지능 스피커 보급을 확산하는데 노력을 기울이고 있다. 그 이유는 음성 및 언어 데이터를 선점하기 위해서이며 확보한 데이터를 기반으로 자사의 플랫폼 및 서비스 확장을 위한 발판으로 삼기 위해서다. 이미지 데이터에 비해 상대적으로 부족한 음성 데이터를 빠른 시간 안에 방대하게 수집할 수 있는 데이터 수취 장치로 인공지능 스피커가 적극 활용되고 있다. 이렇게 수집된 음성 데이터는 음성 인식 기술을 향상하는데 사용되고 나아가 다양한 지식과 엔터테인먼트 산업에 활용될 가능성을 지니고 있다.

2) 현황

가트너는 2018년 인공지능(AI)으로 파생될 글로벌 비즈니스 가치가 전년 대비 70% 증가한 1조 2,000억 달러에 달할 것이며, 2022년에는 3조 9,000억 달러에 달할 것으로 전망했다. 그리고 가트너 리서치 부사장인 존 데이비드 러브록은 “AI는 연산능력, 규모, 속도, 데이터 다양성, 심층신경망(DNN) 발전 등으로 향후 10년간 가장 파괴적인 기술로 자리매김할 것”이며, “2017~2022년 기업들이 AI 기반 제품과 서비스를 위해 가장 주목할 부분은 한가지의 기능에 특화돼 틈새시장을 공략하는 솔루션으로, 기업 경영진들은

특정한 영역에 특화된 전문 공급업체들의 AI 기반 제품에 투자할 것으로 예상된다"고 밝혔다.[37]

조선일보의 2017년 한 리포트에 따르면(과학기술정보통신부 R&D KIOSK에서 재인용), 인공지능의 2018년 세계시장 규모는 195억 달러(한화 약 21조원)로, 국내시장 규모는 2조 5천억원으로 전망된다.



<그림3-5> 인공지능(AI) 국내외 시장 규모 및 전망

대중적으로 가장 잘 알려진 인공지능으로는 구글의 '알파고'와 IBM의 '왓슨'이다. 이들 인공지능 수십만 가지의 바둑 기보나 지식을 반복하여 학습하고 시뮬레이션함으로써 인간의 능력을 벗어난 지능을 얻게 되었다고 할 수 있는데, 이들 인공지능은 단순한 바둑이나 퀴즈에 뛰어난 것에 머무르지 않고 의학 진료, 금융 투자, 기후 예측, 콜센터 응답 등 인간의 능력을 대신하여 미래를 예측하거나 결정을 내리는 다양한 분야로 응용되고 있다. 인공지능 기술이 응용되는 가장 대표적인 분야로는 의료, 법률, 금융 분야다.

의료 분야에서는 수많은 개인들의 의료 및 건강데이터를 분석하고 학습한 결과에 기반한 인공지능이 환자의 발암여부나 의료영상 분석을 통한 질병의 진단을 내릴 수 있게 되었다. 의료 분야에서 대표적인 인공지능 적용 영역은 임상의사지원시스템과 신약개발

37) CIO Korea, "2018년 글로벌 인공지능 비즈니스 가치 1조 2,000억 달러" 가트너 전망, 2018.4.26.

이다. 인공지능 기반의 임상의사지원시스템은 넘쳐나는 의료 정보를 학습 및 분석하여 의사, 간호사, 환자를 유기적으로 연결함으로써 적절한 수준의 기술과 서비스로 의료의 질을 높일 수 있을 것으로 보인다. 의료 분야에서 인공지능 기술이 적용되는 사례로는 미국 메모리얼 슬로언 케터링 암센터 등과의 협업하고 가천대 길병원과 부산대병원 등에 유전 변이 정보를 제공하고 있는 IBM의 왓슨, 성장기 자녀 성장문제를 진단하기 위한 골연령 측정 소프트웨어인 '뷰노-메드본에이지'(Vuno-Med BoneAge), 흉부 엑스레이 영상에서 폐암, 결핵 등을 진단하는 '루닛'(Lunit) 등이 있다. 신약개발 영역에도 인공지능을 통해 비용과 시간을 절약될 것으로 기대된다. 제약회사 얀센은 영국의 인공지능업체 베네볼렌트AI(BenevolentAI)와 제휴하여 임상단계 후보 물질에 대한 평가 및 난치성 질환을 표적으로 한 신약 개발에 착수했으며, 미국 스타트업인 투사(twoXAR)는 단백질의 상호작용과 진료기록 및 유전자 발현 등 방대한 의학 데이터로 신약을 개발 중이다. 국내 스타트업 기업인 스탠다임은 약물 상호작용을 포함한 약물 구조 데이터베이스에 적용하는 알고리즘을 통해 종양학 분야 및 파킨슨병, 자폐증 등에 대한 약물효능을 검증하고 있다.

법률 분야에서는 문서화되어 있는 방대한 판례 등 법률 정보를 분석하는 인공지능 시스템이 사용되고 있으며 국내에서도 법률 자문시스템을 개발하는 중이다. 인공지능은 재판에 필요한 자료 수집과 범인의 개인정보를 통해 분석한 재범률을 토대로 재판관의 형량 결정에 관한 정보를 제공할 수 있으며, 기업의 재무제표 및 유사 부정 사례를 학습한 후 장부 데이터를 해석하여 부정 의혹 사실을 발견, 회계 담당자에 보고함으로써 범죄와 부정에 관한 사전예방 장치의 기능도 수행할 수 있다. 인공지능은 전자증거개시(E-Discovery)에서도 활용되고 있다. 방대한 데이터를 검색하는 검색엔진기술에 AI를 도입하여 증거가 되는 데이터를 보다 빠르고 정확하게 추출할 수 있도록 해준다. 또한 전자증거개시와 시스템 리뷰 데이터 분석 기술을 사용하여 카테고리를 통합, 관련성 높은 문서를 추리하여 예측 코딩작업을 통한 문서패턴·사람·장소·목적을 판별한 후 데이터 항목에 식별자를 부여하여 솔루션에 의한 링크를 함으로써 빅데이터로부터 더욱 효율적인 증거 검토 및 판별을 가능하게 하고 있다. 국내 법무법인 '대륙아주'는 인텔리콘 메타연구소의 법률 인공지능 시스템을 2017년 도입하였다.

금융 분야에서는 로보어드바이저란 이름으로 투자를 인공지능 기법으로 수행하는 시

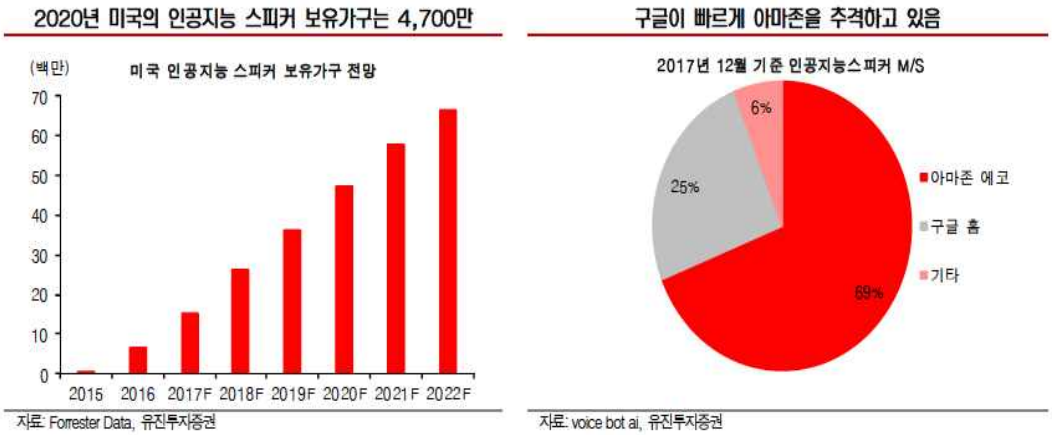
스템이 인간 투자자보다 높은 수익률을 올리고 있다고 하여 주목받고 있다. 대표적인 예로 싱가포르 개발은행에서는 인공지능 기술을 도입하여 우수고객의 투자선호도를 파악하여, 맞춤형 투자자문을 한다든지 자산을 관리하는 서비스를 활발히 펼치고 있다. 또한 P2P 서비스를 장착한 핀테크(FinTech) 분야에서도 방대한 온라인 데이터를 분석하여 개인신용 평가나 포트폴리오 추천에 활용하는 인공지능 기술이 폭넓게 도입되고 있다. 투자은행 골드만삭스는 주식 트레이딩에 인공지능 '켄쇼'(Kensho)를 활용하며 2000년대 초반 600여 명에 달했던 트레이더들을 현재 2명까지 줄였다. 금융 산업의 패러다임이 변화함에 따라 인공지능은 주식, 채권, 외환 등에 대한 투자결정뿐만 아니라 대출승인, 자산배분, 금융컨설팅 등 주요의사 결정까지 인간의 역할을 대신하고 있다. 씨티그룹은 IBM의 '왓슨'을 도입하여 신용평가에 활용하고 있으며, 일본의 미쓰비시 도쿄 UFJ 은행은 20개 언어를 구사하고 인간의 감정을 분석할 수 있는 인공지능 로봇 '나오'를 통해 안내, 환전, 송금 등에 활용하고 있다. 중국 텐센트의 위뱅크는 인공지능을 통해 대출심사를 2.4초 만에 마무리하고 40초 안에 통장에 입금되는 서비스를 제공하고 있다.

<표3-2> 해외 주요 IT 기업의 인공지능 관련 제품들

기업	제품/프로젝트	특 징
구글	알파고 텐서플로우	2016년 알파고(Alpha Go) 인공지능 바둑 프로그램은 딥러닝 기술과 MCTS 알고리즘을 사용. 오픈소스 기반의 인공신경망 알고리즘 텐서플로우(Tensorflow)은 이미지인식과 스팸메일 필터링 학습에 적용.
IBM	왓슨(Watson)	의료, 금융, 마케팅, 관광 등 인공지능 기반 다양한 영역에서 지식서비스를 제공. 최근 블루믹스 플랫폼을 통해 다양한 클라우드 기반 왓슨 API 제공.
MS	코타나 테이 아담(ADAM)	미래에 발생할 결과를 예측하여 도움을 주는 가상 비서 코타나(Cortana), 인공지능 채팅봇 테이, 시각 정보 내에서 사물을 인식하는 아담 프로젝트.
애플	시리(SIRI) 타이탄	스마트폰에서 개인비서 기능을 제공하기 위해 인공지능 기술 접목. 무인전기자동차 개발을 위한 프로젝트 타이탄(Titan).
페이스북	딥페이스 빅서	사용자의 프로필 사진이미지를 인식하는 기술. 인공지능 분석 서버 빅서(Big Sur).
아마존	알렉사	사람의 말투, 억양, 문맥을 파악하는 클라우드 기반 음성인식 인공지능 알렉사(Alexa), 드론 배송과 로봇에 의한 물류창고 관리 등.
바이두	스톡마스터	뉴스, 주식시장, 바이두 검색엔진 데이터에 인공지능 기술을 적용하여 주가와 테마주를 예측

국내 인공지능 및 기계학습 기술은 일부 IT 기업을 중심으로 기술개발 진행 중이나 해외대비 기술 수준과 투자 규모는 미미하다. 네이버랩에서는 음성인식을 통한 검색, 사진 분류 등에 딥러닝 기술을 적용 중이며, 다음 카카오는 여행지 추천과 즉답 검색 서비스에 머신러닝 기술을 활용하고 있다. 엔씨소프트는 AI랩을 통해 인공지능 기반의 게임개발에 힘쓰고 있다. 그러나 현 단계 국내외적으로 가장 대중적인 인공지능 기술은 음성인식에 기반한 가정용 인공지능 스피커라고 할 수 있다.

글로벌 기업들의 인공지능 스피커 시장점유율 확보를 위한 경쟁이 치열해지면서 인공지능 스피커 시장이 빠르게 성장 중이다. 아마존의 에코는 2016년 1,100만대 판매되었으며 2017년에는 그 2배가 넘는 2,400만대 이상이 판매되었다. 구글 또한 2016년 10월 구글 홈을 출시, 출시 후 1년 만에 판매량이 1,400만대를 돌파하며 아마존의 뒤를 추격 중이다. 미국의 인공지능 스피커 보유가구는 2016년 660만 가구에서 2020년에는 4,700만 가구로 증가할 것으로 예상된다.[38)]



<그림3-6> 미국의 인공지능 스피커 현황

국내 기업들도 잇달아 인공지능 음성인식 스피커를 출시하면서 관련 서비스 영역을 확대하고 나섰다. 국내 미디어 기업들인 SK텔레콤(누구), KT(기가지니), 카카오(카카오미

38) 정호윤, "인공지능 비서가 그리는 새로운 인터넷 지형도", Issue Report: 인터넷/인공지능(AI), 유진투자증권, 2018. 4. 17.

니), 네이버(클로바, 프렌즈) 등이 기기를 출시하며 차세대 고객 서비스 플랫폼으로 거듭나기 위한 행보를 시작했다. 한국의 인공지능 스피커 시장이 점점 커질 것으로 전망하고 있지만 음성인식 등 기본적 기능에 대한 소비자 만족도가 아직은 낮은 편이라, 아마존 구글 등 선도 업체들이 진입한다면 국산 AI 스피커 입지가 흔들릴 것이란 우려도 있다.

3) 쟁점

인공지능 기술은 현실적으로 흔히 4차 산업혁명이라고 부르는 혁신의 흐름 중에서 가장 파괴적이라고 볼 수 있다. 그런 만큼 인공지능 기술의 발전이 인간 사회에 미칠 부정적 영향에 대해서도 많은 논의가 진행되고 있다.

우선 인공지능 기술이 어떤 결정을 내렸다고 할 때, 그것이 어떠한 과정이나 논리에 따라 그러한 결정이 내려졌는지 알기 어렵다는 점이 문제다. 일명 블랙박스와 같은 속성을 지니고 있기 때문에 내부의 알고리즘이 알려지지 않은 채 부적절한 결정이 내려질 수 있다. 또한 소스가 되는 빅데이터 혹은 그것을 분석하는 사람과 플랫폼에 내재된 편향 때문에 인종, 민족, 성별, 사회적 계층 등에 대해 편향된 결과를 내놓을 수 있다. 이로써 특정한 인구통계학적 특성을 가진 사람들은 인공지능에 의해 불합리하게 차별받거나 배제될 가능성이 높다. 예컨대 인공지능은 현 상태를 평가하고 미래를 예측하는 결정을 내리는 영역에서 광범위하게 사용될 것인데, 그 미래 예측의 알고리즘은 인간이 배제되기 때문에 공정한 것이 아니라 오히려 인간적 편견에 사로잡혀 옳지 못한 판단을 내리게 될 위험성이 다분하다.

다른 한편으로는 인공지능에 의한 인간의 노동과 일자리 대체가 문제로 대두되고 있다. 인공지능으로 인하여 인간의 일자리에는 당장 위협이 없으며 오히려 일자리가 늘어난다는 전망도 종종 등장하지만, 대체로 인공지능의 비약적인 발전에 따른 미래의 일자리에 대한 우려는 점점 커지고 있다. 한국의 경우, "노동시장 일자리의 43%가 자동화 고위험군으로 나타났다. 2017년 상반기 기준 전체 취업자 약 2,660만 명 중에 1,136만 명이 향후 인공지능에 의해서 대체될 가능성이 높은 일자리에 종사"[39]하는 것으로 분석된다.

39) 김건우, "인공지능에 의한 일자리 위험 진단," LG경제연구원, 2018.

4. 생체인식

1) 개념 및 특징

생체인식 기술(biometrics)은 인간의 특정 생체 정보나 행동 특징 정보를 자동화된 장치로 추출하여 본인 여부를 판별하는 기술이다. “생체인식에 사용될 수 있는 신체적 특징으로는 지문, 얼굴, 홍채, 정맥, 망막, 손모양 등이 있으며, 음성, 자판입력(keystroke), 필적, 걸음걸이 등이 행동적 특징에 속한다. 이러한 생체인식 정보는 보편성, 고유성, 영구성 등의 특징을 갖는다. 생체인식 기술은 공공행정, 민간 및 공공영역의 출입통제 등 보안, 범죄예방 및 수사, 스마트폰 등 정보통신기기 인증, 금융 영역의 본인인증 및 결제 수단 등의 용도로 폭넓게 도입되고 있다.”[40] 지문인식, 홍채인식, 정맥인식, 얼굴인식, 음성인식, 행동인식과 같은 생체인식 기술들은 각 기술별 특성에 따라 장단점이 존재한다.

얼굴인식 기술은 인간이 다른 사람을 인지할 때 가장 많이 사용하는 것이 얼굴이기 때문에 가장 자연스러운 생체 인식 기술이라고 할 수 있다. 얼굴 인식을 통해 고객 맞춤형 정보 제공(마케팅), 거짓말 탐지, 범죄 용의자 탐지(휴대용 단말기를 이용한 범죄 용의자 단속), 보안인증, 엔터테인먼트(닮은 사람 찾기), 인물 사진 관리 지원, 졸음운전 방지 등에 활용된다.

음성인식은 음성으로부터 추출한 독특한 특성을 이용하는 인식기술로 음성 경로, 비강과 구강의모양 등에 의한 음성학적 특성을 이용. 인식의 대상으로 삼는 화자에 따라 화자독립과 화자종속인식 기술로 분류된다. 휴대폰 음성인식, 내비게이션, 보안 및 금융분야, 발음교정 등의 교육 분야, TV 프로그램 검색, 콜센터 음성처리, 중증 장애자들을 위한 환경 제어 등의 분야에 활용된다. 음성인식은 인간에게 친숙한 정보 전달 방법이기 때문에 별도의 학습이나 훈련 없이도 기기를 손쉽게 사용할 수 있으며, 손과 발이 자유롭지 못한 상황에서도 정보를 입력할 수 있다는 장점이 있다. 국내외의 다양한 인공지능 음성인식 스피커 개발붐은 음성인식 기술이 얼마나 일상적으로 보급될 수 있는 것인지 방증한다.

---

40) 국가인권위원회, “바이오 정보 수집, 이용 실태조사,” 2016.

<표3-3> 생체인식 기술간 특징 비교

구분	보편성	유일성	영구성	획득성	정확성	수용성	기만성
지문	중	상	상	중	상	중	상
얼굴	상	하	중	상	하	상	하
홍채	상	상	상	중	상	하	상
정맥	중	중	중	중	중	중	상
음성	중	하	하	중	하	상	하
행동	중	하	하	상	하	상	중

※출처 정보통신기술진흥센터(2017) 수정인용

2) 현황

2015년 AMI(Acuity Market Intelligence) 보고서에 따르면, 세계 생체인식 시장은 2014년 74.6억 달러에서 매년 14.5% 씩 성장하여, 2019년에는 146.8억 달러의 시장을 형성할 것으로 전망된다. 또한 2015년 한국과학기술정보연구원 KMR(2015)에 따르면, 국내 생체인식 시장규모 역시 2014년 2,310억 원에서 매년 14.6% 씩 성장하여, 2020년에는 4,916억 원의 규모로 시장을 형성할 것으로 추정된다.[41] 분야별로는 지문인식이 생체인식 시장 중 66%로 가장 큰 매출을 차지하고 얼굴인식이 12%로 그 다음을 차지하는 가운데 홍채인식(7%)은 매출규모는 크지 않지만 큰 성장세를 보이고 있다.

핀테크, 헬스 케어, 위치기반서비스, 개인화 서비스가 확대되면서 금융, 모바일, 의료복지, 출입관리, 공공서비스, 자동차, 검역, 범죄수사 등 광범위한 분야에 적용이 예상되며, 생체인식 기술은 특히 스마트폰에 적용되는 것을 계기로 폭발적으로 성장하고 스마트홈 등을 중심으로 생활 저변으로 확산될 전망된다.

애플은 반도체 지문인식센서 제조업체인 AuthenTech(3억 5,600만 달러) 인수 후 아이폰, 아이패드에 지문인식 센서를 지속적으로 탑재했고, 삼성전자는 갤럭시 S6 이후 프리미엄 제품에 지문 및 홍채 인식 기술을 탑재해 삼성페이 등과 결합, 보안 강화 및 개인 차별화 서비스를 제공한다. 국내의 경우 공인인증서 의무 폐지(2015년 3월)가 확정되면서

41) 김기일, KISTI Market Report 2016-18.

인터넷 뱅킹, 온라인 쇼핑 등에서 본인 인증 수단으로써 생체인식 기술이 적용 및 활용되는 계기가 마련되었다.

여러 생체인식 중에서도 얼굴인식은 최근 가장 활발하게 개발, 적용되고 있는 분야로, 인공지능 기술과 결합하여 응용분야가 점점 확대되고 있다. 얼굴인식은 금융 분야에서 개인 인증에도 사용될 수 있지만 원래는 CCTV 등에 찍힌 영상으로부터 사람의 얼굴을 구분하고 확인하는 보안용으로 사용하기 위하여 개발됐다. 최근 얼굴인식 기술을 이러한 용도에 도입하는 데에 가장 적극적인 나라는 중국인데, 주요 공항 및 기차역에서 이미 이 시스템을 도입했으며, 주요 시설들을 순찰하는 공안의 상당수는 얼굴인식 기능이 탑재된 '스마트 선글라스'를 착용하여 수많은 인파 속에서도 범죄용의자, 외국의 스파이 등을 순식간에 찾아낸다고 한다.

<표3-4> 주요 ICT 기업 생체 인식 기술 도입 동향

구분	생체인식 관련 서비스, 특허 동향
	○ (지문) 손가락 하나로 본인확인 가능한 지문인식센서를 탑재한 아이폰5S를 출시('13.9.)한 이후 화면에 가해진 압력의 세기를 구분해 인식하는 포스터치를 적용한 아이폰6S·6S+ 출시('15.9.) ○ (홍채) 대만의 부품업체 신텍(Xintec)에서 홍채인식 칩 생산을 준비하고 있으며 '17년 공개될 차기 아이폰에 탑재될 것으로 전망 ○ 생체인식 기술 보안업체 프라이베리스(Privaris) 소유의 특허 31건 가운데 26건을 취득('15.6.) 하는 등 기술 강화 노력
Google	○ (지문) '15년 출시한 안드로이드M 6.0(마시멜로)과 안드로이드 페이에 지문인식 기능을 정식 추가하며 생체인식 기술을 지원했으며 향후 생체인식 기술 활용을 확대할 것으로 예상 ○ (얼굴) 블루투스를 이용해 매장 내 사용자를 인식, 계산대 앞에 서면 자동으로 얼굴을 촬영해 구글에 등록된 사진과 비교해 일치하면 결제가 이루어지는 '핸즈 프리' 서비스 공개('16.3.)
SAMSUNG	○ (지문) 갤럭시 S6('15)에 지문인식 기능을 탑재하고 이를 기반으로 한 모바일 결제서비스인 '삼성 페이'를 공개 ○ (홍채) 갤럭시노트7에 홍채인식을 적용해 모바일뱅킹 이용 시 본인인증 수단으로 활용, 향후 가전제품뿐만 아니라 원격의료·출입통제·행정서비스 등에서 서비스를 확대할 예정 ○ (정맥) 스마트워치 자외선센서를 이용해 손등 부위의 정맥 구조를 스캔한 후 본인 인증에 활용하는 기술에 관한 특허를 출원(2.4)
Microsoft	○ (다중) 윈도10에 비밀번호 대신 지문·홍채·얼굴 등으로 로그인 할 수 있는 윈도헬로 기능 탑재
amazon	○ (얼굴) 사용자가 스마트폰을 귀에 갖다 대면 전면 카메라가 사용자 귀 모양을 인식해 잠금을 해제하는 특허를 취득('15.6.) ○ 스마트폰으로 셀카를 찍으면 얼굴 특징을 인식하는 생체인식 소프트웨어를 활용해 사용자 인증을 하는 특허를 출원(3.10)
Alibaba.com	○ (얼굴) 얼굴인식을 통해 결제를 진행하는 '스마일 투 페이'를 선보였으며 자사 간편 결제서비스인 '알리페이'에 적용할 계획

3) 쟁점

생체인식 기술은 손쉽게 스마트폰에 탑재될 수 있기 때문에 급성장하고 있으며, 향후 사물인터넷(IoT), 웨어러블 기기 및 서비스 확대와 함께 금융, 의료, 보안, 공공 등 다방면에서 활용될 전망이다. 일상적으로 광범위하게 사용되면서 애초의 그 기술의 위험성에 대한 인지도가 점점 낮아지고 있다.

생체 정보가 본인 식별이나 인증을 위해 활용되는 것은 그 유일성, 불변성 때문인데, 바로 그와 같은 특성 때문에 개인의 프라이버시에 미치는 영향도 치명적일 수 있다. 유출되었을 경우 변경이나 무효화할 수 있는 신용카드 등과 달리, 한번 유출되면 그 피해를 복구하기가 거의 불가능하다고 할 수 있다. 개인정보 유출로 인한 신원 도용의 문제 외에도, 인식 오류로 인한 피해, 장애인 접근권의 문제 등도 피할 수 없다. 또한 DNA나 얼굴인식과 같이 수집된 정보들이 인증 목적의 정보 외에도 다른 정보 역시 포함할 수 있기 때문에, 친족 등의 프라이버시 침해나 목적 외 이용 등의 문제도 제기된다.[42]

지문인식의 경우 공항 내 자동출입국심사, 도어락, 보안게이트, 휴대폰 본인 인증, ATM거래, 사회보장등록(연금지급, 건강보험) 등 상당히 폭넓은 분야에서 보편화되어 사용되고 있는 기술로, 특히 스마트폰 및 은행 관련 앱 등에서 기본적으로 사용되면서 자연스럽게 일상생활에 녹아들었다. 그러나 센서를 통해 인식된 지문 데이터가 어떤 방식으로 수집되고 사용될 수 있는지 사용자가 알기 어렵다. 또한 국가기관이 보유하고 있는 전 국민의 지문 데이터는 국민의 감시에 악용될 소지가 충분하다.

얼굴인식 기술은 현재 가장 대중적으로 인기를 끌며 급속히 발전 중인 기술로, 스마트폰에서도 본인 인증, 은행 결제 및 엔터테인먼트의 도구로 사용되기 시작하였다. 얼굴인식 기술은 조명 및 환경과 영상의 각도에 민감하며, 변장, 세월이 흐르면서 생기는 얼굴 변화, 성형수술, 쌍둥이의 유사한 얼굴 특징 등을 구분하는데 단점이 있다. 하지만 스마트폰이나 개인 사용자가 자발적으로 사진을 올리는 페이스북과 같은 SNS에서 획득된 얼굴 데이터는 특정 개인 사용자를 구분하고 분류할 정도로 정확성을 얻고 있다. 요즘에는 알고리즘에 의한 안면인식 착오로 인해 범죄자나 요주의인물로 잘못 분류되면서 고초를

42) 국가인권위원회, “바이오 정보 수집, 이용 실태조사,” 2016.

겪는 사례가 자주 보인다. 특히 일상생활 현장 곳곳에 촘촘하게 설치되어 있는 감시카메라(CCTV 및 자동차용 블랙박스)나 몰래카메라에 노출되는 개인들의 얼굴 데이터가 악용될 수 있는 위험이 상존한다.

음성인식 기술은 아직 낮은 수준의 인식률과 알고리즘의 오류로 인해 특히 인공지능 스피커를 통한 여러 가지 실수와 개인정보 유출 사례 등이 보고된바 있다. 음성에 즉각적으로 반응해야 하는 특성상 항상 켜져 있으면서 음성에 민감하게 반응하고 경우에 따라 스스로 녹음을 할 필요가 있기 때문에 음성인식 기술이 발전할수록 개인정보의 유출의 위험은 더욱 커진다. 해킹이나 도청을 통한 사생활 침해의 위험을 넘어서 음성인식 환경 내의 모든 소리 데이터가 수집되면서 개인과 사용자 그룹 전체의 환경 데이터가 특정한 방식으로 오용될 가능성이 있다.

생체인식 기술은 사업체나 국가기관에서 출입 보안을 목적으로 사용되기도 하지만 근무자 및 노동자의 출퇴근 및 근태 감독의 명목으로 일상적인 감시를 가능하게 한다.

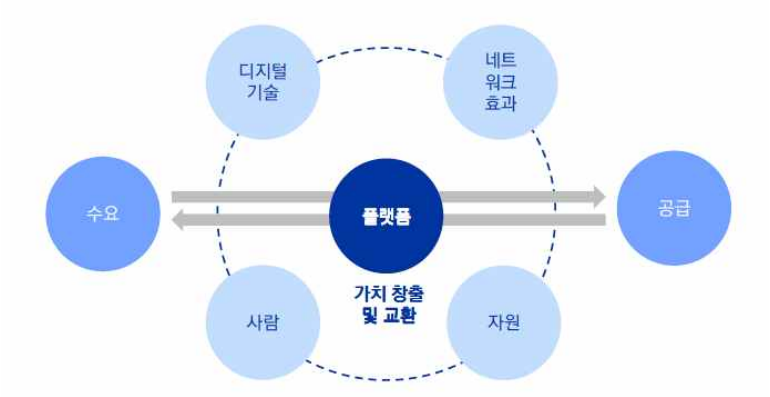
5. 플랫폼

1) 개념 및 특징

플랫폼은 데이터가 순환하는 생태계를 조성함으로써 여러 신기술들(사물인터넷, 빅데이터, 인공지능, 생체인식 기술 등)을 실생활에서 실현하고 또 그 실현을 통해 다시금 데이터가 순환하도록 하는 역할을 한다. 즉 플랫폼 기술은 다양한 핵심 기술들을 연결함으로써 새로운 기능을 수행할 수 있도록 기반을 조성하는 일종의 종합(융합) 기술이라고 볼 수 있다. 따라서 지금까지 위에서 보아왔던 4차 산업혁명의 핵심 기술들은 플랫폼 기술을 기반으로, 플랫폼 사업이나 서비스, 플랫폼 노동의 형태를 통해서 구체적으로 우리의 일상에서 구현된다.

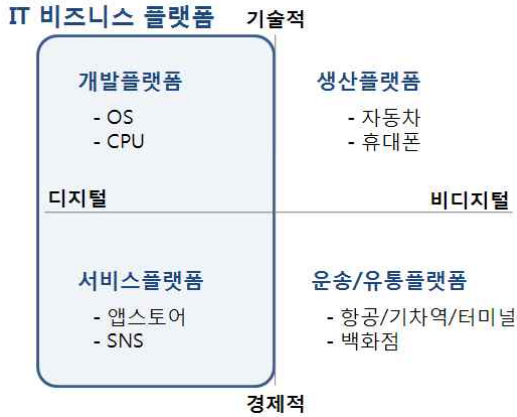
플랫폼의 기능은 기본적으로 수요와 공급을 연결해주는데 있다. 그런 의미에서 우버나 에어비앤비 같은 혁신적 모델이 아니라도, 전통시장과 증권거래소 또한 플랫폼의 속성을 지니고 있다. 이처럼 플랫폼은 오래된 사업 모델 중 하나지만, 디지털 기술이 발달한 오늘날 그 중요성은 더욱 부각되고 있다. 과거 플랫폼이 수요(소비자)와 공급(생산자)을 연

결해주는데 그쳤다면, 새로운 플랫폼 모델은 디지털 기술을 이용해 사람과 조직, 자원을 유기적으로 연결하고, 이를 통해 가치를 창출하고 교환할 수 있게 해 준다. 흔히 O2O(Online to Offline) 상거래의 주요한 수단이 된다.



<그림3-7> 플랫폼의 작동 방식

플랫폼 기술을 적용한 기업들이나 그 자체로 플랫폼인 기업들이 모두가 디지털 혹은 IT 기업들인 것은 아니다. 운영체제(OS)나 CPU 설계 및 제조에 관련된 개발플랫폼과 앱스토어나 SNS와 같은 서비스플랫폼을 IT 비즈니스 플랫폼이라고 한다면, 그 외에 전통적 산업인 자동차, 선박, 항공기를 제조하는 기업들의 생산플랫폼과 운송 및 유통플랫폼 등으로 나눌 수 있다.



<그림3-8> 플랫폼의 종류 구분

플랫폼 비즈니스 모델의 특징은 생산자와 소비자가 다양하게 연결되는 방향에 있으며, 플랫폼을 통해 생산자와 사용자가 적절하게 매칭되는 구조를 가지는데 이를 '양면시장'(Two-sided Market)이라고 부른다. 그리고 양면시장이 활성화하려면 네트워크 효과(Network Effect)가 필수적이다. 네트워크 효과란 특정 집단의 사용자 수가 많으면 많을수록, 그리고 그들의 상호작용이 많으면 많을수록 높은 이익이나 효율을 얻는 것을 말한다. 예를 들어 수십억 명에 이르는 페이스북의 월간 사용자 수는 그만큼 페이스북에 실리는 광고가 많은 사람들에게 노출된다는 것을 의미하므로 기업은 높은 광고비나수수료를 지불하고서라도 페이스북 플랫폼에 들어가려고 한다.

플랫폼 비즈니스의 수익 모델은 크게 중개 수수료, 구독료, 광고료, 라이센싱, 아이템 판매 등으로 구분된다. 애플의 앱스토어, 우버, 에어비앤비, 알리바바 등이 중개 수수료 모델을 선택하고 있다. 구독료는 제품이나 서비스에 대한 비용을 한 번 또는 지속적으로 미리 지급하는 고객을 확보하는 수익 모델이다. 예를 들어 채용에 특화된 버티컬 플랫폼 링크드인은 기본적인 서비스를 무료로 제공하면서 고급 정보 서비스는 프리미엄 구독료를 받는다. 세 번째는 광고다. 구글과 페이스북처럼 거대한 사용자집단을 가진 플랫폼 기업은 매출 대부분이 광고 수익으로 발생한다. 구글의 2015년 매출액 745억 달러의 90%가 광고에서 나온 것으로 나타났다. 네 번째는 라이센싱이다. 라이센싱은 계약된 조건에 따라 제품이나 서비스를 사용할 권리를 개인이나 기업에 제공하는 것을 말한다. 예를 들어 아마존 웹서비스(AWS)는 기업이 대규모의 IT 인프라에 투자하지 않고도, 마치 전기처럼, 사용한 만큼만 지불하는 클라우드 서비스를 제공한다. 다섯 번째는 아이템 판매다. 플랫폼에서 유용하게 사용할 수 있는 기능을 판매해 수익을 창출하는 모델로 게임 아이템, 캐릭터, 기프티콘 판매 등이 일반적이다.

국내에서는 카카오와 라인 등 모바일 메신저 기반의 플랫폼 비즈니스 모델 외에 아직까지 성공한 플랫폼 비즈니스모델이 많지 않다. 수익 모델도 취약한 편이다. 또한 주로 음식 배달이나 대리 운전과 같은 낮은 인건비(노동력)에 기반하며 중개 수수료의 취득을 통해 작동하는 온/오프라인 유통 및 운송 플랫폼이 주를 이룬다.

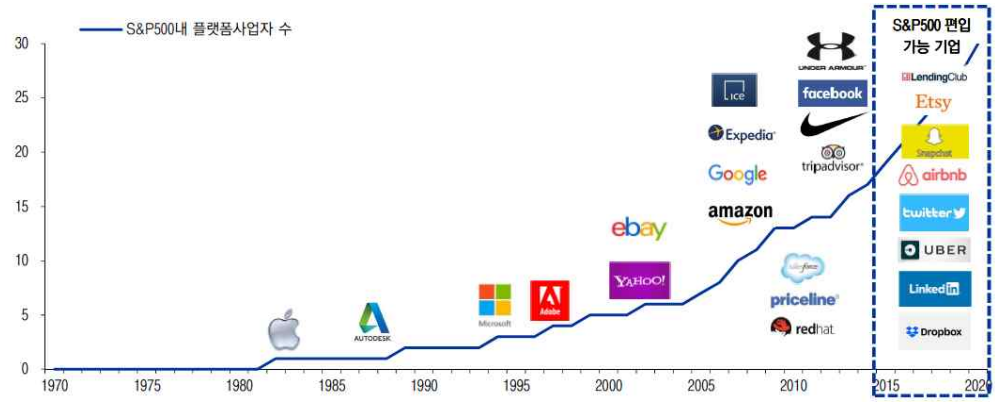
다른 한편 스마트폰이 보편화되면서 모바일 메신저나 SNS와 같은 온라인 플랫폼들이 업무 지시나 보고에 일상적으로 사용되는 경우가 늘어나고, 업무시간 외 혹은 회사 밖에서도 플랫폼을 통한 보이지 않는 노동이 증가하고 있다. 디지털 기술이 노동의 효율을 높이면서 노동시간을 단축한다고 하지만 결과적으로는 노동시간이 연장되는 효과를 내고 있다.

2) 현황

플랫폼 기술은 최근 대부분의 정보기술 기반 기업들뿐만 아니라 전통적인 제조 및 서비스 기업들의 운용의 근간이 되는 기술로 부상하고 있다. 이는 플랫폼과 네트워크를 사용하는 여러 행위자들 사이의 상호작용을 통해 발생하는 데이터를 가공하고 분석하는 등의 방법을 통해 새로운 가치를 발생하는 기술을 의미한다.

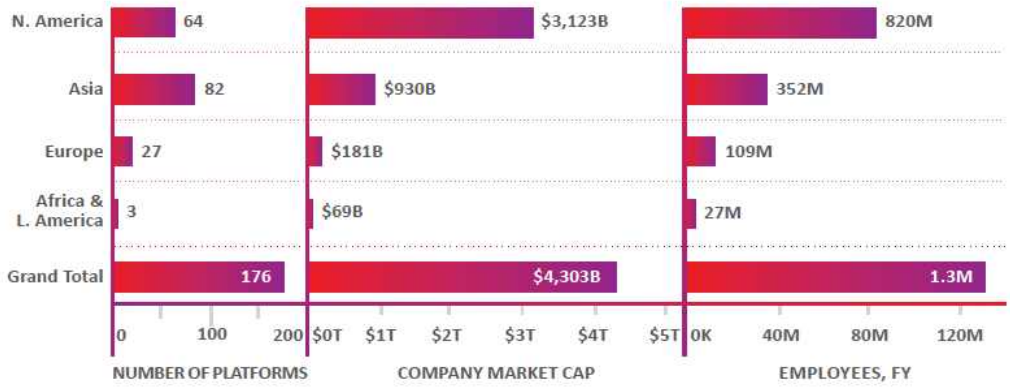
앞서의 빅데이터, 인공지능, 사물인터넷, 생체인식 기술 등의 주요 핵심 기술뿐만 아니라 여러 응용 기술도 각자 플랫폼 기술을 구축하여 독자적인 사업 모델을 개발하기도 한다. 예컨대, 빅데이터 플랫폼이나 IoT 플랫폼이 존재하기도 하며 VR 콘텐츠 플랫폼이나 블록체인 플랫폼이 존재하기도 한다. 이 보고서에서는 다양한 플랫폼 기술을 활용하여 새로운 사업 모델을 구축함으로서 기존의 노동, 업무, 소비의 환경을 완전히 바꾸어 내는 파괴적 기술, 사업, 문화적 현상에 한정한다.

플랫폼 기술은 지난 10여 년간 소셜 미디어, 관광, 출판, 음악의 영역에 한정되지 않고 운송, 은행, 헬스케어, 에너지에 이르기까지 그 범위를 확장시키고 있다. 플랫폼 기업들은 경제 발전에 상당히 기여하고 있는데, 다양한 방식으로 생산성을 높였기 때문이다. 다른 여러 자원 중에서 주택, 자동차, 사업장, 심지어 다양한 노동과 같은 자원들을 더욱 효율적으로 사용(공유)할 수 있게 해주는 플랫폼의 능력 덕분에 소위 '공유경제(sharing economy)'라고 불리는 사업 영역이 급부상하게 되었다.



<그림3-9> S&P500 내 플랫폼 기업들 확장 추세

플랫폼 기술 시장과 플랫폼 비즈니스의 규모에 대해서는 단순한 집계가 불가능하다. 플랫폼 기술이나 비즈니스 모델을 도입하지 않는 기업이 지금의 경제체제 내에서 존재하지 않을 수도 있을 만큼 플랫폼 기술은 광범위하게 확산되어 있다. 2015년의 조사에 따르면, 세계적으로 알려진 (본격적인) 플랫폼 기업 176개의 시장 규모는 4조30억 달러이며 1백30만 명의 고용이 이루어지고 있다. 현재는 훨씬 더 많은 수의 기업을 포함하며 시장 규모도 대폭 늘어났을 것으로 예상된다.



<그림3-10> 지역별 플랫폼 기업

국내에서도 다양한 플랫폼 기술의 적용을 통해 여러 플랫폼 사업과 일자리가 활성화

되고 있는 중이다. 앱으로 승객과 일반 자동차를 연결해주는 우버와 같은 외국의 대행 플랫폼 서비스가 2013년 국내에 진출했다가 국내 택시 업계의 반발과 현행법의 위반 등의 이유로 철수한 사례가 있지만, 국내의 카카오 대리운전이나 택시와 같은 공유 경제의 형태를 띤 플랫폼 서비스는 국내에서 확립된 이후 지속적으로 확장되고 있다.

<그림3-11> 국내외 인력중개 플랫폼들

다른 한편 배달대행 중에서도 음식배달의 경우에는 매우 다양한 플랫폼이 경쟁하고 있다. 플랫폼 사업과 사용자의 수가 늘어나고 있는 것과 함께 플랫폼 노동자의 수도 늘어나고 있다. 특히 배달대행 앱, 대리운전 앱(카카오드라이버), 가사노동 중개 앱 등 디지털 플랫폼을 기반으로 일하는 플랫폼 노동의 증가로 이어지고 있다. 현재 국내 비정규직 900만 명 중 플랫폼 노동자는 약 9만 명 수준으로 추정된다.[43] 플랫폼 기술이나 사업의 종류는 나날이 늘어나고 있으나 여전히 플랫폼의 정의나 범위가 명확하지 않은 이유로 국내 플랫폼 경제의 규모 자체는 아직 알려지지 않고 있다.

3) 쟁점

43) Ibid.

플랫폼 기술은 기본적으로 플랫폼 참여자(사용자)의 데이터를 확보하는 것에서 시작한다. 물론 인간 노동자나 관리자의 활동이나 상태 데이터만이 해당되는 것은 아니다. 제조업 등의 산업 플랫폼에서는 재료, 기계 부속품, 엔진 등의 사물 데이터도 포괄된다. 심지어 농업 플랫폼에서는 드론을 통해 취득한 날씨나 기후 데이터, 작물들의 상태와 같은 환경 데이터까지 포함된다. 플랫폼에서 IoT의 센서나 사용자를 통해 입력, 수집, 축적된 빅데이터는 분석, 순환됨으로써 결과적으로 자동화된 플랫폼 알고리즘의 업데이트에 기여한다. 문제는 인간의 생체 데이터를 포함한 온갖 종류의 데이터를 빨아들이고 그것을 자동화된 알고리즘(혹은 인공지능)을 훈련, 개선하는 과정에서 무분별하게 식별화된 개인의 정보들을 수집, 활용하게 된다는 점이다. 그리고 그 과정은 누구에게도 알려지지 않고 어떤 방식으로도 알아내기가 어렵다.

플랫폼 기술은 플랫폼 기업뿐만 아니라 플랫폼 사용자(생산자와 소비자를 모두 포함) 모두에 편의와 효율성을 제공하는 것처럼 인식된다. 하지만 플랫폼 기업의 특성상 생산자(노동자)가 그 기업에 정규직으로 고용되는 방식이 아니라 대체로 임시적으로 혹은 일시적으로 계약을 체결하는 방식으로 고용이 이루어진다. 소비자(고객)의 경우에는 무료로 혹은 아주 소량의 수수료를 지불하고 편리하게 클릭 몇 번으로 상품을 주문하거나 서비스를 이용할 수 있다. 그리고 어떤 면에서는 생산자(노동자)도 매우 효율적으로 혹은 유연하게 자신의 노동 시간을 활용할 수 있는 이점이 있다. 하루에 여러 가지의 직업을 가지고 여러 시간에 쪼개어 일할수도 있고 원하는 일을 여러 플랫폼을 통해 할 수도 있다. 그러나 플랫폼 노동 속에서 노동자들은 고용되기보다는 개인사업자로 분류되어 불안정 노동의 보편화에 기여하는 셈이다. 모든 것이 자동화된 플랫폼 기술의 이면에는 여전히 파편화된 인간의 노동이 놓여있다.

국내의 경우 주로 플랫폼 기업의 숫자가 많지 않고 특정한 업종, 예컨대 중개업(부동산)이나 운송(음식 배달, 택배, 택시)에 플랫폼 기술이 집중적으로 활용되는데, 이 과정에서 자동화된 알고리즘에 의한 매칭, 작업 배치, 오더 등으로 인해 실제 현장에서 이루어지는 노동의 강도나 시간, 감시나 통제 등에 대해서는 누구도 크게 신경 쓰지 않는다. 자동화 알고리즘과 플랫폼 기술에 의한 효율적이고 편리한 서비스만 부각되고 그 이면의 인간의 노동은 지워진다.

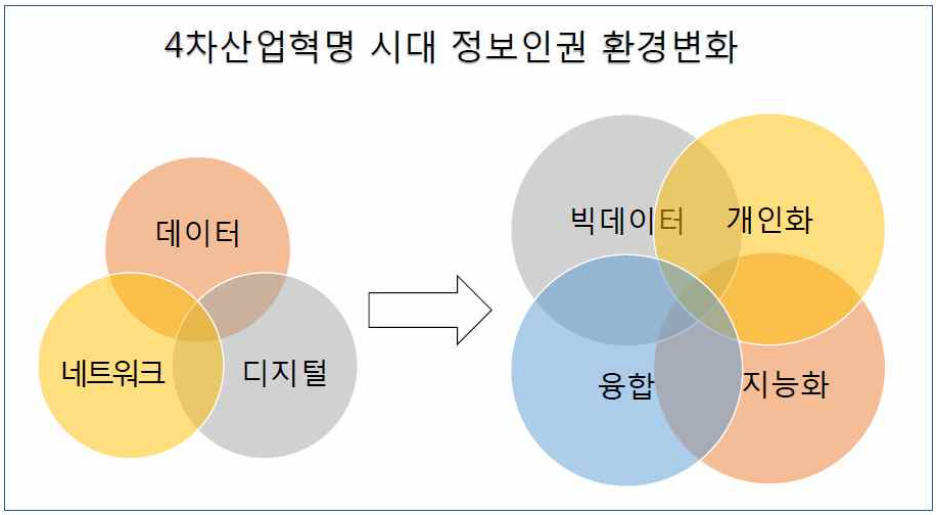
결과적으로 플랫폼 기술들이 거대한 생태계를 이루는 기술문화적 환경에서 인간은 한편으로는 플랫폼을 되먹임하는 파편화된 데이터-주체(소비자의 입장)가 되고 다른 한편으로는 플랫폼의 이면 혹은 아래에서 불안정 크라우드 노동자(생산자의 입장)가 된다.

제4장 4차 산업혁명 시대 정보인권 침해 사례 및 특징 연구

1절 4차 산업혁명 시대 정보인권 침해 양상과 범주

온라인과 오프라인, 사물과 사물, 기술과 인간의 융합을 핵심으로 하는 4차 산업혁명 또는 디지털 전환(digital transformation)이 확산되고 있다. 이에 따라 빅데이터, 사물인터넷, 인공지능, 로봇공학, 자율주행, 드론 및 바이오 기술 등 4차 산업혁명을 이끄는 핵심기술들은 기존 사회의 패러다임을 빠르게 재구성할 것으로 전망된다.

이 가운데 신기술을 매개로 한 정보인권의 구성 환경 또한 바뀌고 있다. 최근까지 개인정보는 디지털화되면서 데이터로 집적되고 네트워크를 통해 정보인권의 침해가 확산됐다. 디지털, 데이터, 네트워크화된 개인정보는 4차 산업혁명을 이끄는 신기술 발전에 따라 단순한 양적인 팽창을 넘어 질적인 변화를 거치면서 그 침해의 범위와 양상이 매우 넓어지고 있다.



<그림4-1> 4차 산업혁명 시대 정보인권 환경변화

첫째, 빅데이터와 사물인터넷, 플랫폼 기술 등이 발달하면서 이전과는 다른 규모로 다

량의 개인정보가 수집되고 유출된다. 또 단순한 데이터베이스화를 넘어서 빅데이터로 형성되고 이런 빅데이터들의 결합을 통해 새로운 다량의 개인정보가 생성되고 있다. 이에 따라 개인정보의 유출 규모도 확대되고 피해도 커지고 있다.

둘째, 빅데이터와 사물인터넷, 인공지능 기술이 상호 결합해 자율주행, 드론 등의 기술을 구성하면서 복합적 차원의 개인정보가 생성되고 있다.

셋째, 개인 식별의 위험성이 높아지고 있다. 빅데이터, 사물인터넷의 데이터마이닝과 프로파일링 기술이 발전하면서 개인정보 간 결합을 통해 개인 식별이 가능해지는 위험이 상존한다. 또한 인터넷과 SNS 사용이 확대하면서 플랫폼 기업들의 타깃팅 기법이 발전하면서 개인 식별화의 상업적 요구들이 커지고 있고 그에 따른 침해도 다수 발생하고 잇다.

넷째, 감시 기술이 지능화되고 고도화되고 있다. 인공지능을 통한 알고리즘 통제가 가능하고, 지능형 CCTV와 드론 등이 결합하여 지능화된 다차원적인 감시가 가능해 졌다.

다섯째, SNS 및 인공지능과 알고리즘 처리 기술이 결합하면서 감정이나 선호 및 의사결정에 영향을 주는 개인정보의 노출 및 수집과 유출이 확대되고 있다. 개인의 정신적 자율성이 침해 될 뿐 아니라 나아가 여론이나 선거와 같은 공동체의 민주적 가치에 대한 침해도 빈번해지고 있다.

2절 정보인권 침해 사례와 유형

1. 개인정보의 대량 수집과 유출

1) 빅데이터

빅데이터는 문자 그대로 빅데이터로서 엄청난 양의 개인정보를 포함하고 있다. 빅데이터는 디지털 정보사회에서 '21세기 원유'로 각광 받으면서 최근 몇 년 사이 폭발적으로 증가했다. 여기에 소셜미디어의 사용 패턴은 물론 각종 감정 및 선호 관련 정보도 빅데이터로 형성되고 있다. 또한 공공기관이 보유하고 있는 기관별 자료 역시 국민 전체의 다양한 개인정보로 구성된 빅데이터다. 최근 빅데이터와 인공지능, 사물인터넷, 블록체인이 결합하면서 이전과는 질적으로 다른 수준의 개인정보가 만들어지고 있다. 이렇게 생성된 개인정보는 다시 빅데이터 형태로 구축되면서 더욱 복잡한 형태로 상호 결합한다.[44]

빅데이터가 확산되면서 개인정보의 대량 유출 사고가 빈발하고 있다. 2008년 인터넷쇼핑몰 옥션에서 1,800만 명의 고객 정보가 유출되면서 대량 개인정보 유출 문제가 시작됐다. 2011년 포털사이트 네이트에서 3,500만 명, 게임회사 넥슨에서 1,320만 명의 개인정보가 유출된 데 이어 2014년 금융권에서는 역대 최대인 1억 건 이상의 개인정보가 새나갔다.[45]

<표4-1> 2014년 이후 대량 개인정보 유출 사례

일 시	기 관	유출 내용	유출 규모

44) 이 과정에서 프로파일링 등을 통해 개인정보가 재식별되거나 새로운 개인정보가 만들어질 위험이 상존한다. 이는 뒤에서 자세히 검토한다.

45) 2013년 6월 경 KCB 신용평가사 직원이 카드사로 파견을 나가 주요 카드사인 국민, 롯데, 농협의 고객 개인정보를 유출시켜 대출모집인과 대출광고업자에게 정보를 넘겼다. 그럼에도 카드사는 7개월 동안 인지하지 못했다. 그 사실은 2014년 1월 검찰 발표로 알려지게 되었다. 이 사건으로 KB국민카드 5,300만 건, 롯데카드 2,600만 건, NH농협카드 2,500만 건 등 총 1억400만 건의 개인정보가 유출됐으며, 중복을 제외한 피해 고객 수는 2,000만 명에 달했다.

2014.1	KB국민카드, 롯데카드, NH농협은행	개인정보유출	2,000만 명 (1억400만 건)
2014.3	KT	개인정보유출	1,200만 명
2014.3	SKT, LG U+ 등	개인정보유출	1,230만 명
2014.3	국토교통부	개인정보유출	2,000만 명
2015.9	뽐뿌	개인정보유출	200만 명
2016.7	인터파크	개인정보유출	1,030만 건
2017.4	야피존	가상화폐유출	55억 원
2017.6	빗썸	개인정보유출	3만 6천명
2017.7	유진투자선물, 디비피아 등 20개 업체	개인정보유출	3,300만 건
2017.9	이스트소프트	개인정보유출	13만 건
2017.9	하나투어	개인정보유출	100만 건
2017.12	유빗(구 야피존)	가상화폐유출	172억 원
2018.6	코인레일	가상화폐유출	400억 원
2018.6	빗썸	가상화폐유출	350억 원

국회에 따르면, 2012년부터 5년간 해킹 등으로 116건의 유출 사건이 발생했고, 이로 인해 5,342만개 이상의 개인정보가 빠져나간 것으로 드러났다. 유출 규모조차 파악이 안 되는 사건도 23차례에 달해 실제 유출된 개인정보 규모는 이보다 더 심각할 것으로 추정된다. 개인정보 유출 후 사후 관리도 문제다. 실제 유출된 개인정보의 회수 여부를 살펴보면 전체사건의 61%인 71건, 개인정보 2,934만개가 회수 됐을 뿐, 회수 여부가 확인이 안 되는 것도 2,400만 개에 달한다.[46)]

이처럼 대량의 개인정보 유출은 해킹 외에도 상업적 목적에 따른 기업 간 거래에 의해서도 발생한다. 2015년 홈플러스는 경품행사로 모은 개인정보와 패밀리카드 회원정보 2,400만여 건을 보험사에 231억7,000여 만 원에 팔았다. 홈플러스는 경품행사 응모권의 고지사항을 1㎜ 크기 글자로 기재해 알아보기 어렵게 했는데, 대법원에서 개인정보보호법 위반으로 유죄를 선고했다(대법원 2017. 4. 7. 선고 2016도13263).

2015년 환자 개인정보 및 진료·처방 등 질병정보를 병원과 약국으로부터 불법 수집해

46) 조선비즈, “최근 5년간 개인정보 5000만개 이상 유출 … 정부 사후 관리 전혀 안돼”, 2017.10.2.

판매한 '지누스사'(병원 보험청구 심사 프로그램 회사), '약학정보원'(약국 경영관리 프로그램 지원 재단법인), 'IMS헬스코리아'(다국적 의료통계회사), 'SK텔레콤' 등 네 곳이 기소됐다. 이 업체들은 약 4,400만 명의 47억 건에 달하는 환자 개인정보 및 질병정보를 병원과 약국으로부터 수집·판매함으로써 122억 3천만 원의 이익을 챙겼다. 지누스사와 약학정보원은 병원과 약국에서 수집한 환자 개인정보 및 질병정보를 19억 3천만 원에 다국적 의료통계회사 IMS헬스코리아에 팔아 넘겼고 IMS헬스코리아는 이를 미국 본사에 보냈다. 미국 본사에서는 이 정보를 병원별·지역별·연령별로 특정 약의 사용현황 통계를 만들어 특정 약을 판매하는 국내 제약회사에 70억 원을 받고 팔았고, 해당 제약회사는 이 정보를 특정 약의 마케팅에 활용했다.[47] 또한 SK텔레콤은 전자처방전 사업을 통해 2만3천여 개의 병원으로부터 전송받은 처방전 7,802만 건을 가맹점 약국에 건당 50원을 받고 판매해 36억 원의 수익을 챙겨 개인정보보호법 위반 혐의로 기소됐다.[48]

한편, 공공기관이 보유한 개인정보도 팔려 나갔다. 공공기관인 건강보험심사평가원은 2014~2016년 사이 가입자 6,420만 명(연인원)의 성별·나이·진료 내역 데이터를 민간보험사에 팔았다.

해외에서도 개인정보의 상업적 거래가 빈번히 문제가 되고 있는데, 페이스북은 스탠퍼드대 의대, 미국심장학회 등과 익명화된 환자 데이터를 공유하는 합의를 맺었다. 그러나 2016년 대선에서 페이스북 사용자 5천만 명의 개인정보가 불법 활용됐다는 스캔들이 터지면서 이 프로젝트는 잠정 중단됐다.

2) 사물인터넷(IoT)

사물인터넷은 센서를 통한 방대한 양의 데이터 수집과 활용을 전제하기 때문에 개인정보의 수집과 유출 위험을 증가시킨다. 사물인터넷의 구성 범위는 첫째, 가정에서 사용

47) 특히 이 사건에서 한국IMS, 약학정보원, 지누스 등은 식별정보를 암호화하였으므로 개인을 식별할 수 없는 정보로 개인정보가 아니며, 이 거래가 위법이라면 빅데이터 산업의 싹을 자르는 결과가 될 것이라고 주장하고 나섰다. 이에 따라 개인정보의 비식별조치에 대한 논란이 일었고 정부는 2016년 비식별조치 가이드라인을 만들었다. 그럼에도 이에 대한 논란은 현재까지도 계속되고 있다. 이 사건 개인정보 비식별조치에 대해 시민단체는 "서울중앙지방법원 2015고합665 개인정보보호법위반 등에 관한 의견서"를 제출했다(https://act.jinbo.net/wp/28717/).

48) 참여연대, "그 많은 내 개인정보는 누가 다 가져갔을까", 참여연대 이슈리포트, 2018.10.10.

되는 가전 기기에 부착된 센서를 통해 집안 내 상황에 대한 정보를 비롯해 행태 등의 민감 정보를 수집하는 '스마트 홈' 둘째, 집 내부의 전기 사용을 파악하는 '스마트 그리드' 셋째, 차량의 센서를 통해 차량 상태 및 운전 습관과 위치 정보 등을 수집하는 '스마트 카' 넷째, 건상 상태, 질병 여부, 신체정보를 수집하는 '스마트 헬스' 다섯째, 도시 차원에서 앞선 내용들을 종합한 '스마트 시티' 등이다. 사물인터넷이 발전할수록 개인의 대부분의 일상 활동이 기록, 수집된다.

사물인터넷으로 인한 정보인권 침해는 개인정보의 수집과 유출 문제로 구분해서 볼 수 있다. 우선 개인정보 수집에 있어서는 정보주체의 동의 없는 수집, 목적 외 수집이 문제가 된다. IoT 기기를 이용하는 데는 현재에도 방대한 종류의 개인정보 수집에 대한 사용자 동의를 구하고 있다. 하지만 기업은 IoT 기기를 통해 생성된 개인정보 중에서 정보주체가 동의한 정보 외에도 동의를 구하지 않은 개인정보를 수집하기도 한다. 현대자동차 블루링크(Blue link)와 기아자동차 유보(UVO)는 차량의 원격 제어 및 도난 시 위치 추적, 길찾기 등 서비스를 무선으로 제공해주는 서비스다. 그런데 현대자동차는 이 서비스를 제공하면서 운전자의 동의 없이 서비스 사용자들의 각종 운행 정보를 자동 전송받았다. 이 서비스와 연결되면 내비게이션 설정 정보와 즐겨찾기, 최근 목적지, GPS 정보, 주행 일자, 운행시간은 물론 운전자 휴대폰 전화번호부도 현대자동차 서버로 들어갔다. 게다가 기아자동차는 '위치 정보사업자' 허가도 받지 않은 채 각종 운전자 정보를 수집해 온 것으로 언론에 보도되었다.[49]

또한 IoT 기기의 개발, 인공지능의 기계학습을 위해서도 개인정보가 필요하기 때문에 정보주체가 알 수 없는 개인정보의 수집이 이뤄지고 있다. IoT 기기의 이용기록은 사물인터넷의 지능화에 기여하기 때문에 사용자들의 사용기록을 필요로 한다. 이 과정에서 정상적인 동의 절차를 거쳐 이용기록을 수집하는 경우도 있지만, 확인되지 않는 경우도 있다. 가령, 사용자가 인공지능 스피커에 호출 신호를 보내기 전까지 인공지능 스피커는 대기모드로 있다고 알려져 있지만, 자신을 호출하는지 안하는지 매 순간 판단을 해야 하기 때문에 대기모드라 하더라도 기기에 사용자의 음성이 항상 입력되고 IoT 기기에 의해 판단되고 있다. 즉 사용자가 호출 신호를 보내지 않더라도 인공지능 스피커는 사용자의 일상적인 대화를 모두 듣고 있다. 실제 미국에서는 2016년 12월 수사당국이 아마존의 인

49) SBS, "즐겨 찾는 곳·운행시간까지 … 현대기아차, 무차별 정보 수집", 2018.10.10.

공지능 스피커인 알렉사를 이용한 범죄자의 이용기록과 대화 등 녹음기록을 제출하라고 아마존에 요구하기도 했다. 아마존은 미국 수정헌법 1조를 들어 이 요구를 거부했지만 인공지능 스피커의 서버에 정확히 어떤 내용이 수집되고 저장되는지는 공개하지 않고 있다.[50]

한편, IoT 기기를 통한 개인정보의 유출 문제도 빈번히 발생하는데, 대부분 해킹과 사이버 공격 형태를 띠고 있다. 2017년 회사원 A씨 등 13명은 4월 17일부터 9월 3일까지 보안이 허술한 1,402대의 IP 카메라에 2,354회나 무단접속한 후, 개인 사생활을 엿보거나 불법 촬영 또는 녹화영상을 탈취했다. 해킹된 IP 카메라는 CCTV가 인터넷에 연결되어 개인 PC나 스마트폰 등을 통해 제어하고 실시간으로 영상을 확인할 수 있는 카메라로, 홈 CCTV나 웹캠 등으로 불리며 최근 집안 애완동물 관리 등의 목적으로 보편화되고 있다[51].

또 다른 사례로 2016년 4월 여수 버스정보 안내시스템이 해킹되어 버스정보 안내시스템에 음란 동영상이 70분간 노출되었다. 2016년 펜테스트 파트너스(PenTest Partners)사는 IoT 초인종을 해킹해 와이파이 패스워드를 획득하는 방법을 시연했다. 집 밖에 설치되는 IoT 초인종을 분해하면, Wi-Fi에 연결하기 위한 무선 모듈이 존재하고 이를 통해 네트워크 접근 권한을 획득하여 다른 장비를 공격할 수 있었다.

또한, 인터넷에 연결된 컴퓨터와 노트북 등의 데이터를 암호화해 인질로 삼는 랜섬웨어나 사이버 공격도 사물인터넷을 통한 정보인권 침해로 볼 수 있다. 대표적으로 2017년 워너크라이(Wannacry)의 랜섬웨어 공격은 한국은 물론 전세계적으로 진행됐고 피해자가 속출했다. 2016년 6월 말에는 DDoS 공격을 수사하는 과정에서 아마존에서 판매하고 있는 CCTV 2만 5천대로 구성된 봇넷이 발견되기도 했다. CCTV에 악성코드를 탑재해 DDoS 봇넷에 악용될 수 있도록 했다. 2016년 말, 미국 동부를 덮친 '미라이 봇넷(Mirai botnet)'은 IoT 기기를 사이버 공격에 악용한 사례다. '미라이 봇넷'은 CCTV, 무선 공유기 등 보안이 허술한 다수의 IoT 기기에 악성코드를 설치하고 인터넷 트래픽을 라우팅하는 DYN 서버를 공격하는 방식으로 이뤄졌다. 이로 인해 10만 대의 기기가 감염돼 트위터, 뉴욕타임즈를 비롯한 주요 웹사이트들을 마비시키는 대규모 혼란을 초래했다. 최근에

50) 뉴시스, 'AI 스피커' 음성 데이터 수집 논란…"삭제 요청해야", 2017.7.18.
51) 이 사례는 아래에 나오는 지능형 CCTV의 침해 사례로도 볼 수 있다. 사물인터넷에 CCTV나 렌즈가 설치되어 있으면 지능형 CCTV와 같은 기능을 한다.

도 '미라이' 변종 악성코드와 'IoT 리퍼' 등 IoT 기기의 여러 취약점을 노린 보안 위협은 끊이지 않고 있다.[52]

그동안 보안전문가들은 사물인터넷에 연결된 기기들이 언제든 해킹될 수 있다는 사실을 증명해 보였다. 앞서 IoT 초인종 해킹을 통해 스마트 홈 시스템을 장악하는 것을 보여주었다. 2015년 7월에는 보안전문가들이 커넥티드 카의 해킹을 통한 원격 제어를 시연해 보였다. 이들은 크라이슬러의 체로키 차량을 해킹해 유커넥트 시스템에 접속하여 자동차의 펌웨어를 변경해 운전자로부터 차량의 제어권을 탈취했다. 차량의 IP만 알면 해킹 가능하며 차량의 IP를 알아내는 방법까지 확인했다. 현대기아차도 마찬가지다. 2016년 말 미국 사이버 보안업체 '래피드7'은 현대차 블루링크를 해킹해 원격으로 시동을 거는데 성공했다.[53] 또 다른 보안업체는 삼성페이의 카드 정보를 탈취한 후 다른 장비에 심어 불법 결제하는데 성공하기도 했다.[54]

이처럼 현재에도 IoT 기기를 통한 개인정보 수집 및 유출, 해킹 등으로 적지 않은 피해를 보고 있지만 앞으로 사물인터넷의 확대, 빅데이터와 플랫폼의 결합, 인공지능을 통한 분석 등으로 개인정보 유출 피해가 급증할 것으로 보인다. 2020년에 사물인터넷으로 연결된 기기의 수가 200억 개를 넘어설 것으로 전망된다(Mark Hung, 2017). 시간이 갈수록 사물인터넷의 연결은 확대될 것이고 이 정보들은 상호 결합돼 기업 내부에 축적될 수 있다. 가령, 대형마트의 상품과 같이 유지 및 관리되어야 하는 사물에 빅데이터 기술과 사물인터넷 기술이 결합될 경우, GPS를 통한 위치 확인, 유통 기한 관리, 상품의 온도 확인 등 모든 정보들을 자동화하고 여기에서 또 다른 새로운 빅데이터가 양산된다.

IoT 기기 중에는 이용기록 뿐만 아니라 지문, 홍채 같은 바이오 정보를 수집·저장하는 기기들도 적지 않다. 또한 금융 및 건강 등 개인의 민감 정보들이 망라하여 수집될 수 있다. 이 정보들이 정보주체의 동의 없이 수집되거나 수집된 정보들이 상업적 혹은 정치적 목적으로 악용된다면 개인에게 치명적인 문제를 일으킬 수 있다.

3) 플랫폼과 SNS

52) 연합뉴스, "미 동부 마비시킨 디도스 공격 '사물인터넷' 이용", 2016.10.23
53) 오토헤럴드, 블루링크가 뚫렸다. 보안업체 원격 시동 성공, 2017.4.26.
54) 조선일보, "삼성페이 결제 때… 2m 안팎 거리에서 해킹 가능" 논란, 2016.8.7.

4차 산업혁명이 온라인과 오프라인, 사물과 사물, 기술과 인간의 융합을 특징으로 한다면, 이의 수요와 공급을 매개하는 플랫폼 기술을 통한 개인정보의 수집과 유출 문제를 고려하지 않을 수 없다. 플랫폼 기술은 3장에서 살펴본 바와 같이 여러 형태로 존재할 수 있으나, 디지털 기반의 서비스 플랫폼은 다양한 개인정보를 수집하고 확산시키고 있다. 페이스북, 트위터, 카카오톡, 인스타그램, 유튜브 등 소셜네트워크서비스(SNS)는 물론이고 구글과 네이버 등 검색과 포털 기업 그리고 이러한 플랫폼의 기반이 되는 어플리케이션 역시 개인의 서비스 이용 결과에 따라 대량의 개인정보가 생성되고 수집된다. 또한 우버나 에어비앤비와 같은 사용자 평판과 서비스 이용을 공유하는 이른바 공유기업에서도 많은 개인정보가 수집되고 있다.

한국전자통신연구원(ETRI)의 사이버보안연구단은 2013년 '빅데이터 개인정보 분석 기술'을 개발해, 페이스북 657만개, 트위터 277만개 등 한국인 SNS 사용자 계정 934만개를 대상으로 개인정보 노출현황을 분석하고 그 결과를 발표했다. 페이스북과 트위터를 합친 934만개 계정 중에서 3개 이상 정보가 노출된 계정 수는 386만개로 약 41%에 달했다. 트위터와 페이스북에 노출된 이름, ID 등 간단한 정보를 이용, 최소 17만 개의 트위터 계정과 페이스북 계정을 서로 연결할 수 있는 것으로 파악됐다. SNS 계정에 들어있는 개인정보들을 서로 연결하면 개인의 프라이버시 침해는 물론, 피싱 사기나 타깃광고, 마케팅 등에 악용될 소지가 높다고 보았다.[55]

플랫폼의 형태 및 사용자들의 이용 특성에 따라 다양한 정보가 생성되고 유통·확산되는데, 이에 따른 피해도 매년 수를 헤아릴 수 없을 정도로 많이 발생하고 있다. 피해유형도 사실상 모든 유형을 포괄한다. 해킹, 상업적 내부거래, 타깃팅, 정치적 악용, 감시 등 대부분의 개인정보 침해 유형이 플랫폼 기업을 통해서 발생한다. 빅데이터 형태의 개인정보 유출도 대부분 금융이나 플랫폼 기업에서 다수 발생했다. 한편, 플랫폼이 사물인터넷과 결합해 개인정보의 수집이 눈덩이처럼 커져가고 있다. 또 플랫폼이 사물인터넷의 플랫폼으로 결합되고 통합되면서 사물인터넷이 만들어내는 각종 개인정보를 통합하는 역할도 플랫폼이 하고 있다.

55) 최대선 외, 소셜네트워크서비스 개인정보 노출 실태 분석, 정보보호학회논문지 (v.23, no.5), 2013.

2. 개인 식별과 타깃팅

1) 개인 식별과 프로파일링

프로파일링은 개인의 상황과 행동을 평가, 분류하거나 예측하기 위한 자동화된 정보처리를 의미한다. 즉, 자동화된 정보처리 과정에서 개인이 드러나는 것을 프로파일링으로 간주한다. 프로파일링의 가장 기초적인 작업은 개인정보의 결합이다. 가령, 비식별 조치를 한 A데이터 세트와 B데이터 세트를 서로 결합하면 C와 D라는 새로운 데이터 세트로 만들어진다. 처음에는 이름 없는 평균적인 표본의 데이터들이지만 상호 결합하는 과정을 통해 지역이 분류되고, 연령, 성별, 나이, 직업과 주소가 찾아지고 결국 개인이 드러난다.

개인 식별과 프로파일링은 정보주체가 제공한 개인정보 외에 새로운 개인 정보를 형성한다는데 문제가 있다. 따라서 비식별 정보라 하더라도 프로파일링 된다면 정보주체의 동의 없이 개인정보를 수집 또는 생성한 상황이 되며 개인정보가 유출된 것과 같은 위험이 발생한다. 더군다나 정보 결합과 프로파일링으로 개인이 식별되면 애초에 제공됐던 정보보다 더 세밀하고 민감한 정보가 생성되기 때문에 문제 심각성은 더 커질 수 있다.

미국 하버드대학교 라타냐 스위니 교수 연구팀의 2015년 논문 '처방전 데이터상 공유되는 대한민국 주민등록번호의 익명성 해제'를 보면, 연구팀은 한국인 사망자 2만3,163명의 처방전 데이터의 암호화된 주민등록번호를 전부 해제하는 데 성공했다. 연구팀은 암호화된 주민등록번호를 논리적 추론 방식과 자동탐색실험, 두 가지 방식으로 모두 해제했다. 논리적 추론 방식은 각각의 자리에서 발견되는 문자의 빈도를 통해 어떤 자리의 어떤 수가 어느 문자로 치환됐는지를 추론하는 방식인데, 논문은 한국의 주민등록번호는 임의번호가 아닌 생년월일과 성별 등 인구통계학적 개인정보를 담고 있기 때문에 더 쉽게 풀 수 있었다고 밝혔다.[56]

앞에서 예로 든 빅데이터 형태의 개인정보의 상업적 거래 및 유출은 일정한 비식별 조치를 취하고 있지만 다른 비식별화된 빅데이터와 결합하면서 다시 개인이 식별되는 위험에 노출되어 있다. 2016년 통계청은 신혼부부 5만가구의 인구 데이터와 민간 신용정보회사의 부채·신용등급 정보 등을 연계한 분석 자료를 공개했다. 통계청은 인구주택총조

56) 한겨레, "복지부 빅데이터의 위험성 … 개인정보 암호화해도 풀 수 있다", 2016.9.25.

사에서 확보한 같은 주소지의 부부 명단에 신용평가회사의 등급을 혼합해 결과값을 얻었다. 남편과 아내 모두 신용등급이 3~4등급 이내인 경우가 46.7%에 달해 신혼부부의 대출 상환 능력을 판단할 때 가구 단위로 고려할 필요가 있다는 시사점을 내놨다. 하지만 본인이 아닌 배우자의 신용등급은 금융권의 대출심사 기준이나 고려사항이 아니었다. 민법상 부부별산제의 원칙에도 어긋난다는 비판이 존재했다. 더구나 신용평가회사가 다른 형태의 프로파일링을 통해 가구정보를 확보하면 정부와 같은 데이터를 갖게 된다. 당시 민간데이터 활용은 법적 근거 없이 민간기업과 체결한 업무협약에 따라 이뤄진 것이어서 시민단체의 비판이 뒤따랐고 더는 관련 업무가 추진되진 못했다.

<표4-2> 전문기관을 통한 비식별 정보 결합 사례(2016.8.~2017.9.)

	전문기관	신청기관 (신청건수)	상대기관 (상대건수)	결합건수
1	한국인터넷진흥원	SK텔레콤 (18,029,816)	한화생명 (4,595,857)	2,185,596
2	한국정보화진흥원	LG CNS (약 970,000)	LG 유플러스 (약 1,090,000)	약 960,000
3		W홈쇼핑 (약 70,000)	BC카드 (약 50,000)	약 50,000
4		SK텔레콤 (29,000,573)	한화생명 (약 9,170,000) SCI평가정보 (약 37,000,000)	약 2,480,000
5	금융보안원	한국주택금융공사 (150,036)	주택도시보증공사 (364,248)	6,680
6		NICE평가정보 (5,000)	그릿연구소 (4,668)	3,900
7		신한카드 (106,562)	코리아크레딧뷰로 (125,192)	46,157
8		신한카드 (28,862)	코리아크레딧뷰로 (106,680)	20,519
9		KB국민카드 (18,267,641)	LG유플러스 (6,608,917)	2,497,714
10		보험개발원 (154,640,520)	현대자동차 (5,545,708)	154,640,520
11		보험개발원 (154,640,520)	현대자동차 (5,545,708)	154,640,520
12	한국신용정보원	NICE평가정보 (2,903,595)	KT (13,961,710)	712,842
13		한화손해보험 (3,955,524)	한화생명보험 (7,108,800)	878,749
14		삼성생명 (7,630,803)	삼성카드 (8,466,576)	2,345,867
15		삼성생명 (7,579,973)	삼성카드 (8,466,576)	2,321,835
16		삼성생명 (7,644,495)	삼성카드 (8,466,576)	2,349,649
17		삼성생명 (7,555,249)	삼성카드 (8,466,576)	2,317,027
18		삼성생명 (8,019,019)	삼성카드 (428,293)	107,073
19		삼성생명 (8,014,487)	삼성카드 (8,106,386)	2,313,824

20		삼성생명 (8,014,487)	삼성카드 (8,284,128)	2,356,213
21		삼성생명 (8,014,487)	삼성카드 (8,466,263)	2,409,998
22		삼성생명 (8,014,487)	삼성카드 (8,465,547)	2,409,992
23		삼성생명 (8,014,487)	삼성카드 (7,855,900)	2,237,917
24		삼성생명 (8,014,487)	삼성카드 (8,466,581)	2,410,101
25		삼성생명 (8,014,487)	삼성카드 (8,466,581)	2,410,101
26		삼성생명 (8,014,487)	삼성카드 (8,462,743)	2,409,211

(출처. 더불어민주당 진선미 의원실)

2017년 국정감사에서는 정부의 '비식별 가이드라인' 도입 이후 개인정보 결합물 3억 4,000만여 건이 기업에 제공된 사실이 드러났다. 보험개발원은 1억5,000만 건의 개인정보를 현대자동차 고객정보와 두 차례에 걸쳐 결합했다. 삼성생명과 삼성카드는 두 회사에 동시에 가입된 240만여 고객의 가입건수·보험료·가입기간·가입상품 및 카드이용 정보 등을 13차례나 결합했다. SK텔레콤과 한화생명도 동시 가입된 약 218만 명의 데이터를 결합했다. 한화생명은 직업·신용대출건수·총신용대출금액·최근신용등급 등 항목을 내놓고, SK텔레콤은 통신료 연체금액·멤버십 사용금액·통신료 미납횟수 등을 내놓아 서로 나눠 가졌다.

앞선 사례에서 건강보험심사평가원(심평원)은 가입자 6,420만 명(연인원)의 성별·나이·진료 내역 등 2014~2016년 데이터를 민간보험사에 팔았다. 여기서 심평원은 '표본 데이터 세트' 형태로 총 87건을 제공했는데, '표본 데이터 세트'란 전체 건강보험 가입자의 성이나 연령 같은 특성이 잘 반영된 100만 명 이상 단위의 표본을 뽑아내 구성한 자료다. 100만 명을 표본으로 한 고령자 표본부터 110만 명 단위의 입원환자·소아청소년 환자 표본, 그리고 140만 명을 표본으로 한 전체 표본까지 있다. 이 자료에는 성이나 연령과 같은 일반내역뿐 아니라 어떤 진료행위를 받았는지가 담긴 상병내역, 진료과목 등이 담긴 진료내역, 그리고 원외처방내역까지 모두 포함되어 있다. 심평원과 비슷하게 국민건강에 대한 빅데이터를 보유하고 있지만 민간 보험사에 제공하지 않은 국민건강보험공단은 "민간 보험사의 경우 건강보험 진료데이터를 분석하여 특정 질환 유병자, 기왕력자 또는 위험요인 보유자에 대해 민간 보험의 가입 차별 등으로 악용될 가능성이 있어 제공하지 않는다"고 밝혔다.

<그림4-2> 개인정보 비식별 자료 생성 유통의 현장적용을 위한 실증 최종 보고서 내용

이처럼 비식별 조치한 개인정보가 재식별되는 사례는 상당수 존재한다. <개인정보 비식별 자료 생성 유통의 현장적용을 위한 실증 최종 보고서>(미래창조과학부, 2017.4.30)는 비식별 조치 가이드라인을 적용해 검증한 결과를 담고 있다. MBC는 이 비식별 조치한 자료들 가운데 신림동에 사는 30대 여성을 뽑아, 이름과 휴대전화번호 등을 알아볼 수 없게 처리된 5건의 자료를 추렸다. 그런데 신림동에 사는 37살 김 모 씨가 폐암 치료를 받은 적이 있다는 정보와 대조하니 5건 중 한 건만 특정됐다. 결국, 이 한 건의 정보가 김 씨의 자료라는 걸 알 수 있었고 신용등급이나 연체율 같은 민감 정보들까지 모두 김 씨의 것으로 확인됐다.[57]

<그림4-3> 개인정보 비식별 자료의 식별 가능성(MBC 방송화면 캡처, 2018.9.15)

57) MBC, "한 건의 정보만 결합돼도 누군지 안다", 2018.9.15

이 자료에서 신용도와 관련된 전체 기록 791만 1천여 건 가운데 숫자로 된 민감 정보로 대조를 했더니 765만 6천여 건이 공격에 취약한 것으로 나타났다. 이는 정보를 결합했을 때 96%는 식별이 가능하다는 얘기이며 동질 그룹에 속하는 민감 정보로는 99%까지 식별이 가능하였다.

2) 가명정보 재식별화의 위험성

빅데이터 양산 및 처리 기술이 발전하고 정부가 보유하고 있던 기존의 공공 데이터와 결합하면서 프로파일링이 폭발적으로 늘어날 위험에 놓여 있다. 특히 데이터 공개와 관련해서는 2016년 '개인정보의 비식별 조치 가이드라인'을 빅데이터 산업 활성화를 위해 만들었다. 비식별 조치는 기업들의 고객 정보 공유를 허용하는 것이 골자다. 개인정보를 가이드라인에 따라 비식별 조치를 하면 개인정보가 아닌 것으로 보고 정보 주체의 동의 없이도 활용·유통할 수 있다.

2017년 새 정부 들어서도 빅데이터 활용과 프로파일링을 위한 개인정보 규제완화 조치는 확대됐다. 행정안전부는 2017년 8월 9일 인공지능과 빅데이터, 사물인터넷 등 첨단 기술을 활용해 공공행정을 혁신하는 '차세대 전자정부' 정책을 발표했다. 이 정책의 지능형 정부 과제의 예로서 제시된 개인의 주변 상황과 자주 이용하는 서비스 이력을 추력 관리하여 맞춤형 서비스를 제공하기 위하여 비콘, GPS, 상황인지 등을 통하여 개인의 상황을 인식하고, 인공지능, 빅데이터 등을 활용하여 개개인에게 적합한 정보를 제공하는 것은 프로파일링에 기초한다.[58]

또한, 2018년 3월 19일 금융위원회의 '금융분야 데이터 활용 및 정보보호 종합방안'도 같은 기조 위에서 발표됐다. 금융위원회는 빅데이터 활용의 궁극적 목적이 '포용적 금융 실현'이라며, 개인의 사전 동의 확보와 정보 보유 기간을 최대 5년까지로 엄격히 제한하는 개인정보보호법과 신용정보법 등의 규제를 완화하겠다고 밝혔다. 정보의 주체가 누구인지 알기 어렵게 한 조처(비식별 처리)를 한 데이터는 개인 동의 없이도 마음껏 분석·

58) 행정안전부, "국민의 일상과 함께하는 '지능형 정부': 행안부, 「4차 산업혁명 대응 전자정부협의회」 개최", 보도자료, 2017.8.9.

가공할 수 있는 길을 열기로 했다. 또 개인의 금융거래 정보가 대량 집적된 신용정보원이나 보험개발원은 원자료에서 추출한 표본 데이터베이스를 중소형 금융사나 핀테크 기업, 연구기관에 제공하는 방안도 추진된다. 고객 동의를 전제로 금융회사에 축적된 개인정보를 끌어와 예금·대출·카드거래 통합 조회 서비스를 제공하고, 스타트업·핀테크 기업들이 활용할 수 있는 정보를 팔아 돈을 버는 '본인 신용정보관리업'도 도입하기로 했다.[59]

지금까지 개인정보보호법·정보통신망법·신용정보보호법 등에선 가명정보와 익명정보를 구분하는 개념이 없었다. 가명정보란 개인정보의 일부만 삭제하여 누군지 알아볼 수 없도록 조치된 정보다. 익명정보란 어떤 기술적 수단을 써도 개인임을 식별할 수 없는 정보여서 논란이 없었지만, 가명정보는 그 자체로는 개인 식별이 불가능하나 추가적인 정보와 결합하면 개인 식별이 가능해 논란이 됐다. 위에서 예로든 2016년 비식별 조치 가이드라인도 이런 문제를 안고 있었다. 그런데 2018년 8월, 정부는 가명정보와 익명정보를 구분하고 가명정보도 보안을 강화해 정보주체의 동의 없이도 사용할 수 있게 하겠다는 방침을 밝혔다.

비식별화된 개인정보라 하더라도 재식별화의 위험이 큰 만큼 매우 신중한 접근이 요구된다. 특히 가명정보의 경우 다른 데이터와 결합하면 언제든 재식별 될 가능성이 있기 때문에 데이터 보안을 강화하고 처벌 수위를 높인다고 재식별화의 위험이 사라진다고 볼 수 없다.

3) 타깃팅: 온라인 광고

특정한 개인들을 식별하는 타깃팅(Targeting)도 개인 식별의 주요한 위험 요소다. 타깃팅의 가장 대표적인 형태는 온라인 광고다. 광고는 사용자 관심사에 기반한 광고가 효과적이며, 관심사에 기반한 광고를 제공하기 위해서는 광고를 보는 사람을 구분할 수 있는 식별자(identifier)와 이 식별자가 어떤 것에 흥미를 가지고 있는지에 대해 알기 위해 '관심사 프로파일링(interest profiling)'을 필요로 한다. 그래서 광고 공간을 판매하는 판매자(Publisher)는 광고 아이디를 활용하거나 휴대폰번호, IMEI(단말기 고유 일련번호), 쿠키

59) 한겨레, "동의 없어도 … 암호화된 금융 개인정보 거래 허용 논란", 2018.3.19.

와 같은 다양한 식별자를 활용해 사용자를 식별하고, 특정 식별자에 해당하는 사용자가 직접 제공한 정보 또는 웹브라우징 히스토리 등과 같은 데이터를 수집한다.[60]

쿠키 중에는 일반적으로 리셋이 가능한 쿠키와 달리 리셋이 불가한 에버쿠키나 핑거프린팅 기술을 광고에 활용하는 경우 사용자가 본인의 식별자를 삭제할 수 없다는 점에서 프라이버시 침해를 야기할 수 있다는 주장이 강하게 제기됐다. 이런 쿠키는 사라지지 않는 영구 식별자(permanent identifier)로 기능한다. 미국에서는 영구 식별자를 사용하여 광고를 집행한 기업들이 고소를 당하기도 했는데, 실제 재판까지 가지는 않고 합의했다.[61]

이외에도 단일 픽셀 이미지(1픽셀로 육안으로 표시되지 않는 이미지)를 흔히 웹 버그(web bug) 또는 웹 비컨(web beacon)이 있다. 웹 비컨은 웹페이지에 심어놓은 매우 작은 그래픽이미지 파일인데, 사용자가 모르는 사이에 사용자에 관한 정보를 유출해가거나 심지어 사용자의 시스템을 파괴할 수도 있는 기술이다. 이들은 웹페이지 및 이메일이 로드되거나 특정 이벤트가 발생할 때, 사용자의 정보와 행동 내역을 서버에게 전달한다.

또한, 웹사이트에 설치된 광고를 통해서도 사용자의 활동이 수집될 수 있다. 해당 광고의 서버는 사용자가 어느 웹사이트의 어떤 페이지에서 광고를 요구하는지 알 수 있으며, 이에 따라 시간대별 행동, 관심사 등의 정보 획득한다. 가령, 수많은 온라인 광고업체들은 사람들이 방문한 사이트에 대한 정보를 수집한 다음 ISP 같은 고객에게 광고 공간을 팔기 위해 이 정보를 사용하고, 이용하는 사람들에 대해 많이 알면 알수록 그들의 고객은 광고를 더 정확하게 타깃팅 할 수 있다.

이러한 온라인 광고는 개인식별과 프로파일링을 수행함에도 불구하고 '광고'라는 목적에 제한되는 것처럼 보여 가시적인 피해가 그리 크지 않아 보인다. 일반적으로 웹사이트에서 계속 반복되는 광고 정도의 피해로 여기고 있다. 그러나 온라인 광고 알고리즘은 식별과 프로파일링을 동시에 할 수 있기 때문에 전혀 다른 목적을 위해서도 동일하게

---

60) 이런 문제들 때문에 온라인 광고는 지금까지도 개인정보의 자기통제권 침해 측면에서 논의되어 왔다. 사용자 통제권 보장을 위해 현재 추적금지(Do Not Track, DNT) 헤더 표준화가 진행되고 있다. 사용자가 브라우저에서 '추적금지'를 설정하면, 브라우저는 모든 HTTP 요청에 DNT 헤더를 붙여주고, 웹사이트 서버에서 이를 감지하는 경우 추적이 금지된다. 또 사용자에게 쿠키 목록을 보여주고, 이를 삭제할 수 있는 기능도 논의되고 있으며, 삭제 기능을 제공하는 경우 어느 범위까지 삭제를 해주어야 하는지도 현재 논란이 되고 있다.

61) 네이버개인정보보호위원회, "2018년 다섯 번째 보안 강연 - 온라인 광고와 프라이버시" 블로그글, 2018.9.4.

작동할 수 있다. 또 광고를 목적으로 수집된 세밀한 사용자 정보가 다른 의도로 팔려나가기도 한다. 가령, 페이스북 가입정보와 활동 정보를 수집한 캘리포니아 애널리티카가 2016년 미국 대선에서 불법적인 트럼프 지지운동을 벌인 것도 동일한 수법이 사용됐다. 이처럼 온라인 광고는 식별자를 구분한다는 점에서 개인 식별의 가장 흔한 방식이며, 개인을 특정할 수 있는 타깃팅의 가장 대중적인 출발점이다.

3. 차별의 심화: 알고리즘 차별

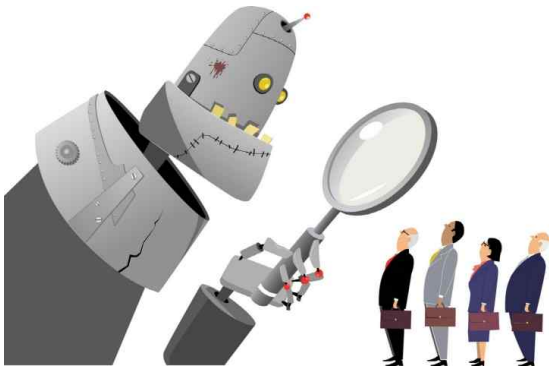
알고리즘에 의한 차별에는 직접차별, 간접차별, 기계학습에 의한 차별 등이 있다(Wagner, 2016). 직접차별은 채용이나 서비스 이용 등에서 직접적인 차별 요소를 포함한 경우를 말한다. 가령, 특정 연령 이하의 어린이와 함께 식당을 이용하지 못한다거나 특정 지역 출신의 사람을 채용에서 배제하는 경우다. 간잡차별은 이런 요소를 직접적으로 포함시키지 않았지만 특정 집단 등에 불리한 결과를 초래하는 경우를 말한다. 마지막으로 기계학습의 알고리즘에 의한 차별로 인공지능 등의 기계학습을 통해 차별적 결과를 가져오는 것을 말한다. 4차 산업혁명의 기술발달로 인공지능의 기계학습이 강화되고 효과를 보면서 기계학습에 의한 알고리즘 차별이 확대되고 있어 심각한 우려를 낳고 있다.

빅데이터, 사물인터넷, 플랫폼에서 형성된 개인정보가 인공지능과 결합하여 학습되고 분석되면서 인간의 개입 없는 자동화된 결정이 이루어지고 있다. 대부분 기계학습에 의한 알고리즘에 의한 자동분석과 결정 과정인데, 이 알고리즘 자체가 일정한 편향을 노정하고 있어 차별적인 결과를 낳고 있다.

1) 인공지능 면접

세계 최대 전자상거래 기업 아마존은 2014년부터 인공지능 채용 시스템을 개발해오다 알고리즘에서 여성 차별적 인식이 드러나자 폐기했다. 아마존은 영국 스코틀랜드 에든버러에 엔지니어링팀을 꾸리고 AI 채용 프로그램을 개발해왔다. 500대의 컴퓨터가 구직 희망자의 지원서를 약 5만 개 키워드로 분석해 1개에서 5개까지의 별점을 매기는 프로그램이다. 그러나 개발이 1년쯤 진행되었을 무렵 아마존 자체 AI 채용시스템이 여성 지원자

를 선호하지 않는다는 사실이 드러났다. AI가 10년간의 아마존 지원자 데이터를 분석한 결과 남성 지원자가 압도적으로 많았기 때문이다. 이 채용 프로그램은 이력서에 '여성'이라는 단어가 들어가거나 동아리 항목에 '여성 체스 클럽'이라는 문구가 들어간 지원자를 감점했으며, 여대를 나온 2명의 지원자 원서에도 불이익을 줬다. 성별에 대한 편향만이 문제가 아니었다. 키워드를 자체 분석하는 AI 채용 프로그램의 알고리즘 때문에 지원자의 기술이나 능력보다는 지원서에 쓴 능력과 관련 없는 단어들이 더 중요해졌다. 실제로 '실행했다(executed)' '데이터를 수집했다(captured)'는 단어를 지원서에 쓴 경우 좋은 평가를 받았다. 아마존은 인공지능의 시스템 개선에 나섰지만 공정성 확보에 실패했다고 판단해 지난해 초 AI 채용 프로그램을 자체 폐기했다.[62]



<그림4-4> 인공지능 면접[63]

이런 AI 채용 프로그램은 음성뿐만 아니라 얼굴 표정 또는 뇌파까지 파악해 지원자의 면접 내용을 최적으로 판단할 수 있는 분석 방법으로 활용되고 있다. '기계 문지기'들의 평가는 취업 정보를 구할 때든 면접을 볼 때든 다양한 부문으로 확대되고 있다. 아래는 해외의 AI 채용 프로그램 사례들이다.[63][64]

62) 머니투데이, "아마존, 'AI채용시스템' 폐기 … 알고리즘이 남성 선호", 2018.10.11.
63) 이뉴스투데이, "채용시장 AI 활용 확대...면접관 사라지나", 2018.6.19.
64) Forbes, "How AI Is Changing The Game For Recruiting", 2018.1.29.

<표4-3> 해외 AI 채용 프로그램 [64]

프로그램	특 징
Workforce Reay HR	크로노스社가 개발한 프로그램으로 채용 과정에서의 '추측'을 제거해 업무 생산성, 직무 수행력, 잠재력이 높고 장기 근무할 최적의 인재를 선별할 수 있다고 광고
X.ai	스케줄 관리 문제에 대처할 수 있는 솔루션 제공
ClearFit	자동으로 채용 후보자를 찾고 순위를 매겨 모집인의 시간을 절약
Filtered	자동생성 코딩을 통해 채용 후보자를 기술적으로 평가하는 데 도움
Harver	직무와 관련해 후보자를 평가하는 매력적인 테스트 생성. 새로운 유형의 심사를 만듦.
Ansaro	모든 직원 데이터를 통합하여 더 스마트한 방법으로 고용하는 데 도움이 되는 예측 모델 구성.
Brilent	모든 후보자를 자동으로 찾아서 순위를 지정
Ideal	인터뷰 대상자를 식별 할 수 있는 신규 및 기존 이력서 수천 개를 화면으로 제공.
왓슨	IBM의 인공지능인 '왓슨'을 활용해 신입사원 서류 심사. 그간 회사가 축적한 면접 질문과 데이터를 숙지한 인공지능은 회사가 선호하는 인재상을 기준으로 지원자가 제출한 서류를 종합적으로 판단. IBM은 1차 면접 단계까지 인공지능을 활용. 인공지능이 전화인터뷰나 화상면접으로 지원자와 대화를 나눈 후 뽑은 선정자는 인사 담당자와 심층 면접을 치르고 최종 채용 여부가 결정
유니레버	유니레버는 인공지능으로 지원자의 페이스북이나 트위터 같은 소셜미디어 정보를 분석. 인공지능이 소셜미디어 낸 구인광고를 통해 지원한 지원자의 SNS 정보를 분석해서 성격이나 가치관을 판단하고 1차 합격자를 선정

국내 채용시장에서도 인공지능 면접이 바람이다. 기업들은 시간과 비용을 줄일 수 있을뿐더러[65] 객관적이고 투명한 방법이라며 AI 면접을 도입하고 있다. 비용 절감과 평가의 공정성 논리가 앞세워진다. 인공지능 면접에는 지원자의 언어, 목소리, 표정, 행동 나

65) 인공지능이 자기소개서를 평가하는데 걸리는 시간은 평균 3초다. 1만 명의 자기소개서를 평가하는 데 8시간이면 가능하다. 같은 일은 인사 담당자 10명이 하루 8시간씩 작업한다해도 7일이 필요하다(중앙일보, "인공지능 면접 치러보니 … '표정·목소리·뇌파까지 분석'", 2018.3.11.).

아가 심장박동, 맥박, 뇌파 등의 생체데이터까지 활용된다.

<표4-4> 국내 AI 채용 프로그램[66]

기업 및 프로그램	특 징
SK C&C	인공지능 '에이브릴'을 활용해 SK하이닉스 지원자를 대상으로 AI 면접
롯데	상반기 공채에 인공지능(AI) 평가 시스템을 도입. 지원자가 '직무 관련 보유역량 기술서'를 통해 직무와 관련한 경험이나 경력 등을 기술하면 인공지능이 지원자의 작성 내용을 분석해 인재상 부합도와 직무 적합도, 표절 여부 등을 평가. 롯데백화점·롯데마트·롯데제과·롯데칠성·롯데정보통신·대홍기획 6개사에 시범 적용한 후 적용 계열사를 점차 확대할 계획
LG하이프라자	신입사원 공채에서 AI 면접을 1차 전형으로 활용
JW중외제약	정기 공채의 인적성검사를 AI 면접으로 대체
한미약품	영업직 지원자를 대상으로 AI 면접
한국방송통신전파진흥원	신입공채 인적성, 직무역량 평가에 AI 면접 도입
한국보건산업진흥원	AI를 활용한 상반기 신입 채용을 진행. 필기시험을 통과한 지원자를 대상으로 자기소개서와 같은 기본 질문과 탐색질문, 직군별 심층 구조화 질문 등을 인공지능이 온라인으로 진행하는데 활용 초기 단계이므로 AI 전형 분석결과는 면접관의 참고 자료로만 사용
사람인	빅데이터 분석과 AI를 기반으로 한 매칭 서비스 '아바타 서치' 출시. 사용자의 개인의 이력서, 사용자 행동 패턴 안에 숨어있는 니즈까지 반영된 맞춤 서비스를 제공. 딥러닝을 이용한 자연어처리 기반의 '챗봇'을 도입해 사용자와 대화를 하는 방식의 추천 서비스도 제공 계획

캐시 오닐은 빅데이터 알고리즘에 대한 문제를 전면에 제기한다. 알고리즘은 과연 공정한가? 그의 결론은 많은 알고리즘이 개발자의 목표와 이념을 반영하고 있고 사회적 편견이 투영된 데이터를 토대로 만들어지기에 불평등을 심화하고 확증 편향(confirmation bias)을 강화한다는 것이다.[67] 그는 인간에게서 차별하는 법을 배운 컴퓨터는 인간들보다

66) 중앙일보, "인공지능(AI) 면접 치러보니 … "표정·목소리·뇌파까지 분석"", 2018.3.11.

67) 캐시 오닐, 『대량살상수학무기』, 김정혜 역, 흐름출판, 2017, 48쪽.

한 술 더 떠서 기가 막힐 만큼 효율적으로 차별적으로 심사한다고 비판한다.

2) 금융 및 보험에서의 차별

알고리즘으로 결정되는 영역에서는 인공지능 면접과 같이 취업 부문 외에도 다양한 영역에서 발생하고 있다. 대표적으로 대출 금리나 보험료율을 결정하는 신용평가에서 인종이나 성차별적 요소들이 코드화 되면서 차별을 야기한다. 미국의 경우, 신용카드 발급 등에서 중요한 평가 기준이 되는 신용평가점수는 주로 재무 정보를 취합해 만들어진다. 재무정보 외에 인종, 학력, 출신지, 심지어는 범죄기록, 언어 사용 능력 등 온갖 데이터가 수집되어 신용도를 예측하는 e점수가 널리 쓰이고 있다.

e점수를 활용해 단기소액대출을 제공하는 스타트업 회사 제스트 파이낸스 사는 대출 신청자 1인당 최대 1만 개의 데이터를 수집·분석해 위험도를 측정한다. 데이터 가운데는 온라인으로 대출신청서를 작성할 때 맞춤법을 맞게 쓰는지, 구두점은 제대로 찍는지, 신청서를 읽는데 얼마나 시간이 걸리는지, 이용약관을 꼼꼼히 확인하는지 등의 데이터도 포함된다. 이는 '규칙을 준수하는 사람'이 신용도가 높다고 판단한 것인데, 이 때문에 교육 수준이 낮은 저소득층이나 이민자들이 높은 이율의 대출을 받게 됐다. 캐시 오닐은 이런 행태가 인종이나 가난에 대한 차별임에도 불구하고 알고리즘에 교묘하게 숨겨져서 드러나지 않는다고 비판한다. e점수는 대출이나 보험뿐만 아니라 일자리를 구하고, 아파트를 빌리거나 심지어 데이트·결혼 상대를 소개해주는 업체에까지 평가 잣대로 확장되어 쓰이고 있는데, 이는 곧 사회 곳곳에서 빅데이터 알고리즘의 차별적 판단이 확산된다는 뜻이기도 하다.[68]

2018년 7월 뉴욕금융서비스부(NYDFS)는 의사 진단이나 혈액 및 소변 샘플을 제출하지 않고도 의료보험에 가입할 수 있는 간소화 보험 가입의 문제점을 밝혀내고 있다. 보험사가 수집한 것으로 추정되는 데이터에는 ▲신용 보고서 ▲구매 습관 ▲주택 소유 여부 ▲교육 수준 등이 포함됐다. 또, 보험사가 해당 데이터를 보험 승인 여부를 판단하는 알고리즘에 포함시킨 것으로 추정된다. 미국소비자연맹은 "보험사가 개인의 생활수준과 교육 정도, 소득, 심지어 인종이나 민족 등을 근거로 사람을 차별할 수 있다"며 "이 때문

68) 캐시 오닐, 같은 책, 262~264쪽.

에 간소화 보험 가입을 경계해야 한다"고 주장했다. 미국 전국보험감독관협회(NAIC)는 보험사들이 사용하고 있는 소비자 데이터와 알고리즘, 보험 승인 '예측 분석' 방법 등을 조사하고 있다.[69]

한편, AI와 빅데이터에 기반한 신용평가 방법이 기존의 신용평가방법의 한계를 극복하는 대안이라 강조되기도 한다. 회계정보 외의 정성적 요소에 대한 평가가 어렵다는 점은 현 신용평가체계의 구조적 한계로 지적받는다. 기업신용평가구조에서 정성적 평가의 비중은 기업특성에 따라 59%까지 산정돼있을 정도로 높지만 이들을 평가할 만한 객관적 근거는 부족한 경우가 많다. 이를 극복하기 위해 제시된 것이 텍스트 마이닝과 같은 빅데이터 분석기법이다. 인터넷과 SNS, 언론기사와 같은 텍스트 데이터 속에서 유의미한 단어들을 추출해내는 텍스트 마이닝은 투자자와 소비자의 심리와 같은 정성적 평가의 근거들을 수집·분석하는 데 활용될 수 있다.

그러나 AI 및 빅데이터 신용평가기법은 신용등급이 도출된 이유를 설명하기 어렵다는 문제가 있다. 바둑계를 재패한 알파고를 만들어낸 딥마인드 사도 알파고의 수를 설명하지 못하는 것처럼, 신용평가사들도 '알고리즘이 결정했다'는 설명 외에 다른 합리적인 설명을 하지 못하고 있다. 신용등급이 이자율은 물론 기업과 개인의 대외적인 신뢰에 지대한 영향을 미치는 만큼, 자동화된 신용평가체계가 의뢰자의 신용등급을 깎아낼 경우 이로 인한 문제가 커질 수 있다.

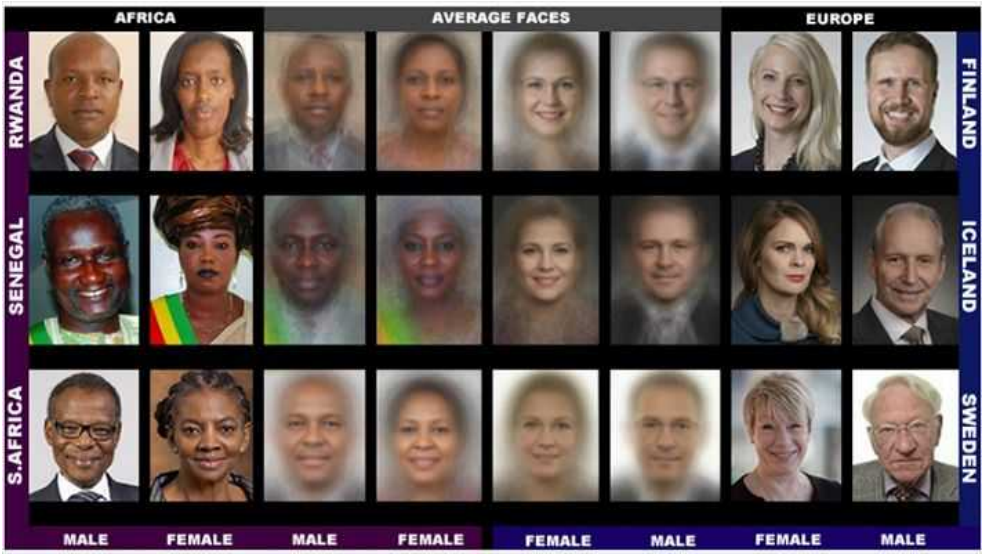
3) 얼굴인식 프로그램[70]

인공지능의 얼굴인식 문제는 기계학습(machine learning)이 확산된 이후 계속 지적되어 왔다. 2015년 구글의 이미지 인식 사진앱 출시 초기에 아프리카계 미국인을 '고릴라'라고 표시하면서 논란을 빚어 공식 사과한 바 있다. 2016년 인공지능 'Beauty.AI'가 심사하는 국제미인대회에서 유색인종 여성들은 단 한 명도 입선하지 못하면서 인종 차별과 관련된 논란 발생하기도 했다.

---

69) MReport, "美 보험사의 간소화 보험 절차, 득일까 실일까?", 2018.7.3.

70) 인공지능 알고리즘에 의한 얼굴인식 문제는 인식 과정의 알고리즘적 편향에 따른 차별과 인식의 결과인 얼굴인식이 주로 감시 영역에서 사용된다는 점에서 감시·통제문제와 중첩된다. 여기서는 알고리즘의 차별 문제를 주로 다루고 감시 통제 문제는 뒤에서 다룬다.



<그림4-5> 인종, 성별 평균 얼굴 및 인식 정도[71)]

2018년 초 메사추세츠공과대학 미디어랩의 연구에 따르면, 여러 종류의 인종과 성별로 구성된 사진 이미지를 이용해 상용화된 얼굴인식 시스템으로 실험한 결과 백인 남성의 경우 인식률이 99%에 달했지만 피부색이 검은 여성의 경우 인식 오류가 35%에 달하는 것으로 나타났다. 피부색과 사람의 성별을 토대로 얼굴인식 시스템의 결과를 분석한 이 실험은 마이크로소프트, IBM, 중국의 메그비 등 3곳의 상용화 된 AI 얼굴인식 기능을 사용해 의학계에서 피부 색조 구분 표준으로 사용하는 '피츠패트릭(Fitzpatrick)의 6가지 피부유형 분류'에 따라 아프리카 3개국과 북유럽 3개국의 국회의원 얼굴 사진 1270개 데이터를 대상으로 진행됐다. 실험에서 백인 남성들의 얼굴 오인식률은 1%에 그쳤고, 백인 여성에 대한 오인식률은 7%로 다소 높아졌다. 흑인 남성은 최대 12%까지 오인식률이 올라갔고, 흑인 여성은 최대 35%까지 오인식률이 발생했다. 업체별로는 마이크로소프트가 21%, IBM과 메그비는 35%였다.

한편, 조지타운대 로스쿨 프라이버시 및 테크놀로지 센터는 1억1700만 명의 성인이 사

71) Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Joy Buolamwini, MIT Media Lab, 2018.1.15.

법기관에서 사용하는 얼굴인식 네트워크에 데이터화 되어 있는 것으로 추정하며 특히 아프리카계 미국인의 경우 데이터 오류가 가장 많은 것으로 나타났다고 밝혔다.[72]

4) 알고리즘을 통한 노동시간의 차별과 통제

가. 온콜스케줄링 프로그램

업주가 종업원들의 근무 시간을 편의대로 지정하기 위해 종업원들을 상시 대기시키는 것을 '온콜 스케줄링(on-call scheduling)'이라고 부른다. 교대제를 짜는 방식에서는 물량이나 수요, 인원, 근무일정, 피크타임, 고객의 방문 패턴 정도의 요소들을 고려하는데 그쳤을 것이다. 또한 요소들을 분석해 예측한 인력을 현장에 투입하기까지는 어느 정도 시간적 간격이 발생할 수밖에 없었다. 요소들을 아무리 잘 버무려도 인력의 과소 산출이나 과잉 투입이라는 문제를 피하기는 어려웠다. 최근 빅데이터 알고리즘을 활용한 스케줄링 프로그램은 비용·편익을 계산하는 새로운 도구로 활용되고 있는데, 이는 단순히 비용·편익의 계산에 머무르는 것이 아니라 자본이 골칫거리로 여겨왔던 것들을 제거할 수 있는 혁신적인 수단으로 동원되고 있다.

온콜스케줄링의 한 형태인 클로프닝(clopening)은 클로징(closing)과 오프닝(opening)의 합성어인데, 종업원이 밤늦게까지 일하다 매장 문을 닫고 퇴근한 뒤 몇 시간 후 새벽에 다시 출근해 매장 문을 여는 상황을 가리키는 서비스업계의 신조어다. 클로프닝과 관련한 애로사항으로 수면 부족 문제가 거론되는데, 클로프닝을 담당하고 있는 직원의 60% 이상이 7시간도 채 안 되는 휴식시간에 힘들어 한다는 응답은 최적의 인력을 산출한다는 알고리즘이 어떻게 노동의 고충을 양산하는지를 가늠해 볼 수 있다. 통근 거리가 꽤 되는 경우 매장에서 잠을 자야하는 경우가 발생하고 최소의 휴식권[73]조차 보장받지 못하는 문제들이 보고된다. 유럽연합 지침인 최소 11시간 휴식 시간 기준에 비춰보면, 11시간 미만의 휴식시간인 응답자가 90%에 육박한다.[74]

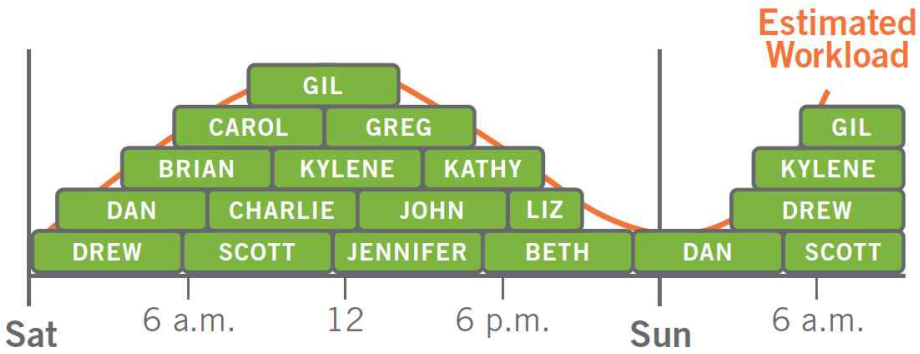
---

72) 노컷뉴스, "인공지능 얼굴인식 기술도 '피부색·성 차별'", 2018.2.12.

73) 한국노동안전보건연구소, "운전노동자 노동시간, '특별히' 더 짧아야 한다", 오마이뉴스, 2018.1.2.

74) The Center for Popular Democracy, The Grind: Striving for Scheduling Fairness at Starbuks, 2015, pp. 11. 참고로 UCLALabor Center에 따르면, 판매노동자의 44% 정도가 클

스타벅스는 인력 산출을 최적화하기 위해 크로노스 같은 스케줄링 프로그램[75]을 활용한다. 이는 영업 패턴, 날씨, 보행 패턴, 교통량, 트윗 양, 실시간 검색어, 고객 패턴, 고객 평가 등의 여러 요소와 거대 데이터를 투입해 교대제 인력을 산출한다. 이를테면 미세먼지가 심각해 보행량이 줄 것으로 예측되는 날이면 일기 예보를 실시간으로 반영해 인력을 산출하는 것이다. 실검이나 트윗 양도 빅데이터 알고리즘의 원료로 하여 수요의 변화를 예측한다. 트위터의 트윗 양을 분석해 올해 추석 세일 때 작년보다 쇼핑객이 얼마나 증감할 것이라는 예측을 할 수도 있다.



<그림4-6> 크로노스의 인력 예측 사례[76]

이것은 빅데이터 알고리즘을 통해 인력을 과소로 또는 과잉으로 산출할 리스크를 제로화해 노동비용을 최적화할 수 있는 '적합한' 기술 양식을 확보한 것이라 말할 수 있다. 물론 여기서 '최적의' 인원 투입은 빅데이터 알고리즘에 따른 것이지 현장 노동자들의 집합적인 이해와 요구를 반영한 것은 아니다. 또한 요소들의 인풋이 왜 그러한 아웃풋으로 나왔는지 그 알고리즘을 노동자는 알 수 없다. 주목해야 할 점은 느슨한 시간을 깨끗하게 제거하고 불필요한 인력을 줄이고 필요에 따라 실시간으로 조정하는 이와 같이 물

로프닝을 경험했고, 그 가운데 61%는 10시간 미만의 휴식시간도 갖지 못했다. 자세한 내용은 UCLALabor Center, Hour Crisis, 2018, pp. 37.

75) Kronos 같은 관련 프로그램들로 Dayforce, ADP workforce, Xero, Gusto, Zenefits, Epicor, Namely, PeopleSoft, AccountEdge, Justworks 등이 언급된다. 이 모두가 크로노스와 같이 보행 패턴, 교통량, 트윗 양 등의 거대 데이터를 활용해 교대제를 짜는 것은 아니지만 핵심은 과소·과잉의 인력을 최소화하는 혁신 수단이라고 광고된다는데 있다.

76) Kronos, "Kronos Scheduling Solution Guide", 2013, pp.4.

류적으로 타당한 방식이 노동의 불안정성을 극단화한다는 점이다. 노동자의 스트레스도 이만저만이 아니다. 삶의 불안정성도 높아지고 노동자들은 스케줄의 종속성도 높아졌다고 한다. 데이비드 와일이 말하는 '쪼개질 대로 쪼개진 노동'의 현재 버전인 셈이다. 이러한 문제에 처한 노동자를 캐시 오닐은 '알고리즘의 노예'라고 지적한다.[77]

이 같은 방식의 온콜스케줄링 프로그램은 스타벅스를 비롯해 맥도날드, 월마트, UPS, DHL 등으로 빠르게 확산되고 있다. 캐시 오닐은 시간, 비용, 재고를 절감하기 위한 적기 생산방식이 특정 업종에 제한하지 않고 빅데이터 알고리즘을 매개로 서비스 업종을 비롯해 여러 부문으로 확대대고 있음을 지적하면서 'JIT(just in time) 경제의 확장'이라고 진단한다. 데보라 코웬의 '적시 일자리의 세계'란 표현도 유사한 문제제기다. 작업장 내 여유 시간, 느슨한 시간 등의 빈틈을 제거하기 위해 장착했던 관리 기술들, 이를 상징적으로 이미지화한 <모던타임즈>의 자동급식기가 산업시대의 '낭비 제거' 방식이라면, 크로노스 등의 온콜스케줄링 프로그램은 낭비·비효율·골칫거리라고 여겨지는 모든 것들을 완전히 제거해 오로지 필요에 따라 실시간으로 노동력을 편취하는 기술적 환경이 구축되었음을 말해준다.

나. 플랫폼 노동

노동시간과 관련한 알고리즘 차별의 또 다른 형태로 플랫폼 노동을 들 수가 있다. 신기술이 배치되면서 새롭게 등장한 배달앱 알바를 비롯해 긱 워크(gig work), 크라우드 워크(crowd work), 우버 워크(uber work), 온디맨드 워크(on-demand work) 등 다양한 형태의 노동을 플랫폼 노동으로 구분한다. 플랫폼 노동은 전통적 의미의 노동시간, 노동과정, 노동관계, 노동의 권리, 노동자 정체성 등에 커다란 변화를 야기하고 있다. 특히 플랫폼 노동자들은 노동법이나 사회보장법의 사각지대(grey zone)에 놓이면서 극단화된 노동의 불안정성과 프라이버시 침해의 위험을 그대로 감수해야하는 상황이다. 많이 알려진 사례이긴 하지만, 기사 한 줄을 인용해보자.

> 배달앱 소속 … 오토바이로 치킨 배달 아르바이트를 하던 한 고교생이 무단횡단을 하던 보행자와 충돌해 척수가 손상됐다.[78]

77) 캐시 오닐, 같은 책 208쪽; 데이비드 와일, 『균열 일터』, 송연수 역, 황소자리, 2015, 32쪽.

‘배달앱 소속’이라는 문구에서 보듯 노동관계는 신기술이 활용돼 ‘고용계약 관계’가 ‘사업계약 관계’로 바뀌었다. 이 방식으로 사용자의 책임 회피와 비용 삭감이 극대화되고 있다. “배달원을 직접 고용하면 월급을 포함해 보험처리 등 복잡한 게 많다. 배달대행 업체를 이용하면 수수료만 지급하기 때문에 신경 쓸 일이 적다”는 어느 업주의 말은 이를 그대로 보여준다. 배달대행업체가 홍보하는 문구를 보면, ‘신경 쓸 일’들로 사고 발생 시 발생한 비용에 대한 부담, 직원 관리, 인력 모집, 사고 위험 부담 등을 꼽고 있다.

<표4-5> 배달대행업체가 홍보하는 ‘배달대행 이용시 장점’[79]

1. 사고 발생 시 추가비용(오토바이 수리비, 직원 보험료 등) 없이 업무에 전념할 수 있다.
2. 직원의 잦은 지각, 무단 결근, 기타 속 썩임 없이 운영할 수 있다.
3. 부족한 배달 직원 모집 압박감에서 해방된다.
4. 동시다발적으로 발생하는 주문을 처리할 수 있다.
5. 배달 직원의 사고 위험 부담에서 해방돼 심리적으로 안정된다.

배달앱이 확산되자 음식점들은 배달대행 업체를 끼고 배달을 외주화하기 시작했다. 이 과정에서 배달 노동자는 ‘사업자’ ‘공급자’ ‘파트너’가 됐다. ‘독립노동자’로 불리기도 한다. 앞선 사건의 판결은 산재 보상을 받을 수 없는 것으로 결론 났다. 배달앱 소속의 노동자는 개인사업자이지 근로자로 인정하기 어렵다는 이유였다.

플랫폼 노동자는 일하는 시간을 얼마나, 또 어떻게 쪼개든지 스스로 통제할 수 있고, 특정한 시공간에 구속되지 않고 원하는 스케줄대로 일할 수 있다는 점에서 ‘자율적’ ‘독립적’이라고 이야기된다. ‘디지털 노마드’라는 신조어처럼 장밋빛 언어들로 채색되기도 한다. 그러나 플랫폼 노동자들은 콜 캐치에 대한 자유도가 높을지는 몰라도 일거리가 어떻게 할당되는지, 업무 과정의 어디까지가 모니터·기록·평가되는지, 수집된 데이터가 어떻게 쓰이는지, 데이터들이 어떠한 과정을 거쳐 그러한 결과로 나왔는지 알 수 없다.

실제 플랫폼 노동자는 업무 처리에 대한 관리·평가를 받아 등급이 매겨지고 등급에 따라 콜을 다르게 배정받기도 하는데 정작 등급이 왜 그렇게 산정되는지 그 과정을 노동

78) 경향신문, 법원, ‘배달 알바’ 중 척수 다친 고교생 산재 불인정, 2015.10.11
79) 한겨레21, “사고책임은 누가 대행해 줍니까”, 2016.8.18.

자는 정확히 알지 못한다. 『블랙박스 사회』의 저자 프랭크 파스콸레는 그 과정들이 '도저히 명확히 알 수 없는 알고리즘에 의해 작동'하기에 '블랙박스' 같은 것이라고 지적한다. 플랫폼 노동자들의 자율성은 코드화된 알고리즘, 데이터의 오남용 등 정보 착취의 위험에 취약하다.[80] 우리는 알고리즘 모형에 의해 A, B, C, D로 분류되어도 정작 누구도 그 모형을 제대로 알기는 어렵다.[81]

4. 지능형 감시

1) 국가 정보기관의 저인망식 정보수집과 빅데이터

대량 수집되는 데이터, 감시 기술의 발전에 의해 국가의 감시능력이 고도화하는 것은 우려할만하다. 인터넷 시대에도 국가에 의한 감시 통제 우려가 작지 않았지만, 4차 산업혁명의 핵심기술인 빅데이터, 사물인터넷 및 인공지능, 생체인식 기술 등이 발전하면서 국가 감시 능력도 그에 비례해 확장하고 있다. 미국 국가안보국(NSA)의 인터넷 대량감시가 문제가 된 것은 특정한 혐의 없이 '일단 수집'하는 무차별 감시였다는 점이다. 또한, 마이크로소프트, 구글, 페이스북, 야후, 애플, 스카이프 등 한국에서도 많이 이용하고 있는 글로벌 사업자들이 이에 협조한 것이 드러나기도 했다.

애드워드 스노든에 의해 밝혀진 바에 따르면, 미국 정부가 프리즘(PRISM)이라는 프로그램을 통해 이메일과 검색엔진, 인터넷 전화인 '스카이프' 통화, 그리고 기타 미국인들이 지난 몇 년간 사용해온 전자 통신 내역을 감시해오고 있었다. 이에 따르면 AOL, 애플, 페이스북, 구글, 마이크로소프트, 스카이프, 팔톡(PalTalk), 야후, 유튜브 등 가장 유명한 웹서비스 업체들 다수가 프리즘 프로그램에 협력했다고 한다. 보도에 따르면, 미국 국가 안보국(National Security Agency: NSA)이 이들 기업의 서버에 '직접 접속권'을 가지고 있다. 해당 기업 대부분은 프리즘과의 관련성을 부인했지만 그들이 NSA의 이러한 행위를 알지 못했는지, 아니면 알면서도 모르는 척 했는지는 확실치 않다.

2015년도 이탈리아 해킹팀 의뢰내역 중 한국 국가정보원의 의뢰를 받은 내역이 드러

80) 프랭크 파스콸레, 『블랙박스 사회』, 이시은 역, 안티고네, 2016, 10쪽.

81) 캐시 오닐, 같은 책, 57쪽.

났다. 해당 의뢰내역 중 카카오톡 검열 및 스마트폰 갤럭시 출시 때 마다 해킹업체에 '뚫어달라'며 요구했다고 한다. 그 와중에 국가정보원은 '스파이웨어'를 요구하며 적법한 영장 절차를 무시하고 휴대전화에 스파이웨어를 심어 감시하려고 했다. 이후 지속적으로 '국가안보 차원의 이동통신 감청 설비 의무화'법안을 발의하며 이동통신 기기를 감청하려는 시도를 하고 있다.

2) 범죄예측 시스템

빅데이터를 통해 범죄가 일어날 시간과 장소를 예측하고 이에 대한 정보를 경찰에 전달해 범죄를 사전에 방지하는 것을 '예측 치안'이라고 한다. 일반적으로 빅데이터를 활용한 범죄예방 프로그램은 첫째, 범죄에 대한 예측 둘째, 범죄자에 대한 예측 셋째, 범죄자 신원에 대한 예측 넷째, 피해자에 대한 예측의 네 가지 범주로 이뤄지고 있다. 기본적으로 범죄(자) 예측은 불특정 다수를 대상으로 하고 이 과정에서 불특정 다수의 개인정보가 무차별적으로 수집되고, 특정 집단이 잠재적 범죄자로 의심되어 실시간 감시 대상이 되기도 한다.

2016년 2월 경찰청은 '빅데이터 기반 범죄분석 프로그램' 개발을 공표했다. 이 사업의 한 축은 국가가 운영 중인 국가통합형사사법정보시스템인 킥스(KICS), 경찰청 과학수사센터의 시아스(CIAS·범죄첩보분석시스템), 112시스템 등의 데이터를 경찰은 모두 활용하겠다고 밝혔다. 이 시스템들은 여전히 베일에 싸여 있는데, 2011년 한나라당 박대해 의원이 경찰청으로부터 제출받은 자료를 보면 킥스(KICS)는 피의자 3085만 명, 피해자 2226만 명, 참고인 192만 명의 정보가 킥스 시스템에 집적돼 있는 것으로 나타났다. 이전에 경찰이 보유하다가 킥스에 통합된 범죄정보관리 시스템 심스(CIMS)는 애초 경찰 조서를 작성할 때 묻는 자질구레한 정보들까지 관리하고 있었다. 인권감시단체들은 집회·시위 현장에서 경찰이 촬영하는 체증 영상도 포함돼 있을 것으로 추정한다.[82]

이 사업의 또 다른 축은 것은 민간·공공의 공개 데이터들이다. 이는 사실상 온라인상의 모든 정보를 포함한다. 사업 계획서에는 '날씨, 지역 특성, 이벤트 등 외부 변인'을 수집하겠다고 했지만 온라인상의 모든 정보를 수집 대상으로 삼을 우려가 크다. 경찰청은

82) 한겨레, SNS 등 온갖 개인정보 긁어모아 … 위험한 범죄예측 시도, 2016.2.5.

사업 주체가 검색, 크롤링(인터넷의 자동 정보수집 기술), 인덱싱, 필터링 등 정확하고 빠른 데이터 수집 기술을 가져야 한다고 명시했다.

<그림4-7> 빅데이터 기반 범죄분석 프로그램 흐름도[83)]

나아가 경찰청은 빅데이터 기반의 첨단 범죄 분석 프로그램인 '클루(CLUE)'를 개발 중이라고 밝혔다. 클루는 '범죄분포 이해도구(Crime Layout Understanding Engine)'의 축약 표현이다. 2016년 2월부터 개발에 착수한 경찰청은 2018년 말까지 개발을 완료하고 2019년 초부터 시범운영에 들어갈 계획이다. 클루는 경찰이 보유한 범죄·사건 관련 데이터에 날씨, 나이·성별 인구, 공시지가 등 총 52종 1억3000여건의 공공데이터를 더해 범죄유형을 심층 분석하고 과거 유사 사건 등을 제시한다.

이에 대해 시민단체들은 경찰의 정보활동이 민주적으로 통제되지 않으면 이런 첨단시스템은 국민의 헌법상 권리를 과잉 침해한다고 경고하고 나섰다. 특히 경찰 내부 데이터, SNS 등 공개된 국민들의 개인정보, 사물인터넷 등 다른 정보와 결합해 개인이 식별될 개인정보를 비롯하여 시스템 원천이 될 국민 개인정보를 목적 외로 사용할 때의 적법성 또한 검증해야 한다고 주장한다. 개인정보의 수집·작성 및 배포는 "법률에 특별한 규정"이 있거나 직무의 수행을 위하여 "불가피한 경우"에 한하여 허용이 된다(개인정보보호법 제15조제1항 제2호, 제3호). 이는 법률에 의한 구체적이고 명확한 위임이 있을 때(법률유보) 혹은 비례성의 원칙에 따라 직무수행에 필요불가결한 요청이 있을 때(비례성의 원칙)에만 가능함을 의미한다.

83) Ibid.

<표4-6> 범죄예측 기술

바이브라(Vibra) 이미지	전정기관의 반응에 의한 머리 움직임을 특수영상으로 시각화 표현. 공격적인 생각을 품거나 거짓말할 때 화면에 붉은색 표시와 함께 경고음.
	2010년 경찰청이 도입해 활용 중
아이트래커(시선추적장치)	눈동자에서 나오는 적외선을 감지해 눈의 움직임을 알아내는 원리. 시선의 집중도를 통해 전두엽의 대뇌피질을 분석, 거짓말이나 공격성을 가려냄.
	국내 수사기관에서 거짓말탐지기의 보완적 장치로 사용 중
지능형 전자발찌	전자발찌 착용자의 맥박, 혈중알코올노동 등 측정. 비명 등 외부 정보와 작용자의 이동 패턴 등을 감지 분석해 과거 범죄 때 패턴과 비교를 통해 범죄 가능성 예측.
	법무부에서 2016년부터 시행
빅데이터 기반 첨단 범죄 분석 클루(CLUE)	범죄·사건 관련 데이터에 날씨, 나이·성별 인구, 공시지가 등 총 52종 1억3000여건의 공공데이터를 더해 범죄 유형을 심층 분석하고 과거 유사 사건 등을 제시한다.
	2019년 초 한국 경찰청에서 시범운영 계획 중
범죄자 평가 시스템(OASYS)	런던 전역에서 최근 5년간 발생한 조직 범죄 데이터베이스와 소셜네트워크서비스 활동 동향 등을 분석해 우범자를 사전에 가려내는 시스템
	런던 경찰청에서 시행
범죄감시시스템(DAS)	도시 내 CCTV, 자동차 번호 감지기 등 각종 센서에서 취합된 정보와 국세청, 톨게이트, 911녹음파일 등 20여 개의 정보를 통합해 의심스러운 정황이 발생할 경우 일선 경찰관이 관련 정보를 제공한
	뉴욕 경찰국에서 시행
인공지능 위험측정도구(HART)	인공지능 분석을 통해 용의자의 재범행률을 세 단계(높음·보통·낮음)로 측정해 구금 여부와 시간, 보석 석방 조건 등을 제시
	영국 더럼시 경찰국에서 시행

해외에서도 이러한 범죄예측 프로그램은 다소 광범위하게 운영되고 있다. 빅데이터, 인공지능과 결합하면서 더욱 고도화되고 있으며 이에 따른 인권침해 논란도 끊이지 않고 있다. 미국에서는 콤파스(COPAS), 프리드폴(PredPol), 크라임스캔(CrimeScan), 크러시(C.R,U.S.H) 등의 프로그램을 활용하고 있다. 뉴욕경찰국(NYPD)은 여기에서 한 단계 더 나아가 실시간 감시, 대응시스템을 연계한 범죄감시 시스템 '다스(DAS, Domain Awareness System)'를 테러리스트 및 범인 추적에 활용하고 있다. 이 시스템은 범죄 예

측을 기반으로 도시 내 CCTV, 자동차 번호 감지기 등 각종 센서에서 취합된 정보와 국세청, 톨게이트, 911녹음파일 등 20여 개의 정보를 통합해 의심스러운 정황이 발생할 경우 일선 경찰관에 관련 정보를 제공한다.

범죄 예측은 물론 범죄자 신원에 대한 예측도 단지 검거를 위한 분석 활동에만 사용되지 않고 광범위한 프로파일링을 기반으로 활용된다. 미국 플로리다의 경우, 100만 명 이상 소년범의 범죄기록을 기반으로 프로파일링을 실시하고 맞춤형 교화프로그램을 개발했다. 뿐만 아니라 프로파일링을 지리학, 수사심리학 등과 연계해 활용하고 있다.

영국은 범죄자 평가 시스템(OAsys-Offender Assessmenat System)이라는 재범 예측 프로그램을 활용하고 있다. 특히 런던 경찰국(MPS)은 런던 전역에서 최근 5년간 발생한 조직 범죄 데이터베이스와 SNS 활동 동향 등을 분석해 우범자를 사전에 가려내고 있다. 영국 더럼시 경찰은 용의자 구금을 결정하는 데 인공지능 기반 위험측정도구인 '하트(HART, Harm Assessment Risk Tool) 프로그램을 2017년 5월에 도입했다. HART는 용의자의 재범행률을 세 단계(높음·보통·낮음)로 측정해 구금 여부와 시간, 보석 석방 조건 등을 제시한다. 이 같은 범죄자 평가 시스템은 인권단체들로부터 인권침해 가능성이 제기되었고, 특히 하트(HART)에서 '높음' 단계에 소수인종 용의자가 백인 용의자의 두 배 이상 포함돼 논란이 일었다.

3) 지능형 CCTV를 활용한 감시

경찰의 CCTV를 활용한 집회 감시는 잘 알려진 바 있다. 2014년 도로에 설치된 교통정보수집용 CCTV를 조작해 세월호 참사 추모집회를 불법 감시한 것으로 확인된 바 있다. 집회 참가자를 향해 줌인과 줌아웃도 수차례 반복한 것으로 드러나 "교통관리를 위해서만 사용했다"는 해명도 거짓으로 드러났다. 여기에 경찰은 인간의 개입 없이 모니터 요원이 CCTV를 보며 추적하지 않고 지능형 관제 시스템을 도입해 추적하려는 대상을 즉시 인지하도록 하고 있다. 지능형 관제란 CCTV 영상을 실시간으로 분석해 특정인의 행동인식, 차량번호의 자동감지 등 지능형 기술을 CCTV 관제에 적용하는 것이다. 경찰은 이 기술을 활용해 민간인 차량을 지속적으로 수배 하는 기술로 활용하기도 했다.

이 같은 지능형 감시는 CCTV-Deep learning으로 확대하고 있는데, 2018년 1월 LG유

플러스 CCTV가 지나가는 사람들의 얼굴을 촬영, 성별과 나이를 알아내고 기록하는 기술을 선보였다. 성별과 나이를 알아내는 기술은 딥러닝 기반의 인공지능이지만, 수많은 정보를 실시간으로 전달하는 일은 네트워크가 맡는다. 이처럼 폐쇄형이었던 CCTV가 4차 산업혁명 시대를 맞아 개방형으로 변화하면서 ICBAM(IoT, Cloud, Bigdata, AI, Mobile)과 융합되고, 저화질 영상에서 초고화질 영상으로, 영상을 촬영하고 확인하는 것을 넘어 상황을 판단하는 등 사람의 역할을 대신하는 지능형으로 발전하고 있다.

<그림4-8> 아마존 얼굴인식 시스템 소개 프레젠테이션[84)]

하지만 이런 기술들은 전체 시민들을 대상으로 다양한 개인정보를 수집하고 감시 기능을 확대해 지능적 판옵티콘 사회를 형성한다는 우려를 자아내고 있다. 아마존은 2018년 중반 미국 경찰, 중앙정보국(CIA), 이민세관단속국(ICE) 등 수사기관·법집행기관에 얼굴인식 소프트웨어인 '레코그니션(Rekognition)'을 제공하기로 계약했다. 레코그니션은 교통단속 카메라, CCTV 등에 잡힌 불특정 다수 행인의 사진을 수사기관에 보관된 머그샷(피의자 식별용 얼굴사진)과 실시간으로 대조해 용의자를 추적할 수 있는 프로그램이다. 그런데, 이에 대해서 아마존 직원 450명은 제프 베이조스 최고경영자 앞으로 의견광고 형식의 서한을 발송했다. 이들은 레코그니션이 대중을 감시할 새로운 '빅 브라더'가 될 것이라는 경고했다. 직원들은 "우리는 견제받지 않는 새롭고 강력한 감시도구가 국가의

84) Image & Video Rekognition based on AWS, Ranju Das 유튜브 화면 캡처

손에 쥐어졌을 때, 무고한 사람들이 볼 수 있는 피해를 역사의 교훈을 통해 알고 있다"고 강조했다. 이 소프트웨어는 미국 상하원의원 28명의 얼굴을 범죄자로 잘못 식별한 적도 있다. 특히 유색 인종에서 오류가 자주 발생했다. 미국시민자유연맹(ACLU)은 아마존의 얼굴인식 시스템에 1만 명의 머그샷을 올려 정확한 인식 여부를 테스트한 결과 28명의 얼굴에서 오류가 발견됐다고 밝혔다. 오류가 나타난 사람들이 대부분 유색인종이었다는 점에서 ACLU 측은 프로그램에 인종차별적 요소가 있다고 주장했다.[85]

한편, 중국은 '톈왕'(하늘의 그물) 시스템을 천명했는데, 2000만개의 CCTV로 안면 인식 기술 등을 활용해 움직이는 사물을 추적, 판별하는 인공지능 폐쇄회로와 범죄 용의자 데이터베이스를 연동해 범인을 가려낸다는 것이다. 이 외에도 안경형 안면인식 기기를 도입해, 기기의 앞쪽으로 지나가는 사람 중 얼굴의 70% 이상이 찍힌 이들을 인식해 2~3분 내 범죄자 데이터베이스와 대조하는 식으로 작동한다. 분리 독립 움직임을 이유로 탄압받는 신장위구르자치구에서는 지난해 초부터 반체제 인사 통제를 목표로 겹겹의 감시망이 구축됐다. 안면인식을 통해 집이나 직장 등 특정한 곳에서 300m 이상 벗어나면 경보가 울리는 식으로, 인체 정보 수집과 스마트폰 자료 추출, 음성 분석, 차량 위성추적기 부착 의무화 등 기술이 전면적인 '경찰국가'를 만들고 있다는 보도가 잇따른다.[86]

최근 지능형 CCTV에 이동성까지 완비된 드론은 다양한 영역에서 활용 가능하지만 감시와 공격 무기로서도 각광받고 있다. 산업용 드론은 재난·재해에 완벽히 활용 할 수 있도록 시각, 후각, 지리 능력을 갖출 수 있도록 개발됐다. 영상분석알고리즘을 통해 시각(안면인식, 모션감지, 자세감지, 불꽃감지 기능 등)을 탑재했고 후각(기상감지: 온도·안개, 대기감지: 미세먼지)도 탑재했다. 현재 이 드론은 주로 해양 구조, 재난 등의 상황에서 활용하고 있으나, 통신사와 연계해 어디서든 실시간으로 끊김 없는 화면을 볼 수 있다. 이 같은 드론은 산불감시와 같은 공익적 목적으로 사용될 수 있지만 사람을 대상으로도 '감시'가 가능하다. 가령, KT와 화성시가 함께 구성한 안전관제시스템도 살펴 볼 필요가 있다. 경광등을 장착한 드론이 이륙한 뒤 100m 지점에서 고정익 변환으로 사각지대를 촬영하고, 저속(20Km/h) 영상을 지상으로 전송한 다음, 고속(70Km/h)로 이동하며 고화질 영상을 지상관제 요원에게 끊김 없이 전송했다. 이들은 공익적 목적 등으로 사용될

85) MBC, "얼굴인식 소프트웨어 … 범죄자 식별에 쓰인다지만 불안해", 2018.10.20.

86) 한겨레, "'AI 안경' 쓴 경찰, '당신 범인이지'…촘촘해지는 중국 '감시사회'", 2018.2.8.

수 있지만 모두 지능적이고 지속적인 감시를 하는데 동원될 수도 있다.

실제 지능형 드론을 통한 감시 사례도 종종 발생하고 있다. 2018년 중국 정부가 민간인 감시를 위해 새처럼 생긴 드론을 활용해 온 사실이 드러났다. 30개 이상의 중국 정부 및 군 기관들이 민간인 감시용 드론을 이용해 왔다고 언론이 보도했다. 암호명 '비둘기'인 감시 프로그램으로 새처럼 생긴 드론에 전자 모터로 구동되는 크랭크 진자운동을 활용해 실제 새들의 날갯짓을 그대로 흉내 냈다. 각 드론에는 고선명 카메라와 GPS 안테나, 비행 통제 시스템이 장착돼 있다.[87]

한편, 사물인터넷과 정보기술의 발달로 휴대전화, PC는 물론이고 로봇청소기, 비디오게임기, 홈 CCTV와 텔레비전, 냉장고 등 일상에서 쓰이는 각종 전자제품이 네트워크로 연결되고 렌즈가 포함되는 경우가 많아지면서 감시와 유출위험이 커지고 있다. 2018년 11월 경찰은 반려동물을 관찰하기 위한 홈 CCTV를 해킹해 여성 5,000여 명의 사생활을 엿보고 불법 촬영한 10명을 입건했다. 2017년에는 가정·영업용 매장의 IP 카메라 1,400여 대를 해킹해 여성이 옷 갈아입는 모습 등을 엿보고 영상을 유포한 일당이 경찰에 적발됐다. 2015년에는 아프리카TV 방송진행자의 PC의 웹카메라를 해킹해 사생활을 훔쳐보고 이를 온라인에 게시한 혐의로 항소심에서 징역 1년 6개월을 받았다.[88]

5) 노동 감시

노동에 대한 데이터화는 디지털 모바일 시대에 양산되고 있는 새로운 노동 과정에 '적합한' 관리·감시 양식으로 떠오르고 있다. 업무 처리 과정이 실시간으로 데이터화된다는 사실은 새롭게 구획한 우산 아래 주체·객체를 통합 관리하는 것이 수월해졌다는 의미인 동시에 감시통제의 개인화, 일상화, 나아가 지능화와 연결되는 대목이다. 이전의 노동 감시는 작업장을 전제하고 집단적으로 감시한 후 사후적으로 평가하는 방식이었다. 판옵티콘(panopticon)은 말 그대로 특정한 공간의 전범위를 눈으로 관찰 감시하는 장치를 말한다. 이에 비해 업무용 앱이나 배달 앱은 특정한 공간 안팎을 가릴 것 없이 개별 노동자에 직접 관통하는 방식으로 노동자 주체의 종·추적(tracking and tracing)을 가능하게 할

87) ZDNetKorea, "중국 정부, 새처럼 생긴 드론으로 민간인 감시", 2018.8.3.
88) 동아일보, "렌즈만 보면 무섭다"…'원격 몰카' 된 집안 가전제품, 2018.11.6.

뿐만 아니라 더 중요한 점은 그것이 실시간으로 가능하다는 사실이다. 작업장에 CCTV를 설치 녹화해 문제 발생의 A, B, C, D를 사후적으로 그리고 시간 순으로 판단 평가하는 것이 아니라 앱으로 추출된 데이터를 통해 개별 노동자의 이동 동선, 결재-성과 보고 등의 업무의 전 과정을 실시간으로 맵핑(지도화)하는 게 가능하다. 심지어 노동자의 품행까지 통치할 수 있다. 일일이 관찰하지 않고도 작업장 안팎에서 노동자의 행동 하나하나까지 데이터화할 수 있는 일종의 데이터감시(dataveillance)다. 기술철학자 베르나르 스티글러는 이를 알고리즘 통치성이라고 말하기도 한다.[89] 혹자는 전자통치라고 한다.

가. 데이터 감시: 업무용 앱

업무용 앱은 많은 기업들에서 활용되고 있는 업무 관리 시스템이다. 그리 새로운 것은 아니다. 업무 혁신을 앞세워 스마트오피스, 모바일오피스 등 업무 환경을 재편하려했던 21세기 초반부터 등장했다. 업무용 앱 도입 바람은 증권사, 보험사 등의 금융권을 비롯해 주요 대기업은 물론 한국정보사회진흥원, 중앙선거관리위원회, 한국인터넷진흥원, 에너지관리공단, 도시철도공사, 국민건강보험공단, 한국관광공사 등 공공기관까지 거셌다.[90] 최근 업무용 앱은 삼성그룹 제조계열사는 물론이고 LG그룹, SK그룹, 포스코 등 대기업 다수에서 광범위하게 활용 중이다. 이외에도 KB국민카드는 직원들에게 업무용 앱 설치를 요구했고, 피죤의 경우 노동조합 활동을 하는 직원들에게 실시간으로 영업 사원의 위치를 파악할 수 있는 앱 설치를 지시했다. 포스코 역시 광양제철소에 출근하는 하청 노동자들에게 통화내역 열람이 가능한 앱을 설치하라고 요구했다.

업무용 앱이 문제로 부각됐던 사례는 2014년 KT가 업무용 앱 설치를 지시했고, 이에 직원 이 모씨가 개인정보 침해 우려를 들어 앱 설치를 거부하면서 촉발된 사건이다. KT는 무선 통신의 품질을 측정하는 안드로이드 기반 앱을 만들고 설치 방법 등에 대한 교육을 실시한 뒤 업무지원단 소속 직원 283명 중 일부에게 개인 스마트폰에 이 앱을 설치하라고 지시했다. 해당 앱은 위치 정보는 물론 개인 스마트폰의 카메라, 연락처, 개인정보(달력 일정), 저장소, 문자메시지, 계정 정보 등 12개 항목에 접근 권한을 가지고 있었

89) 프랭크 파스콸레, 같은 책 40쪽; 베르나르 스티글러·아리엘 키루, 『고용은 끝났다, 일이여 오라!』, 권오룡 역, 문학과지성사, 2015, 85쪽.

90) 디지털데일리, “MDM 솔루션 시장, 마침내 꽃 피우나”, 2012.9.25.

다. 업무지원부 경기지원팀에 근무하던 이씨는 앱 설치 대상에 포함되자 개인정보 침해가 우려된다는 이유로 앱 설치를 거부하고 업무수행을 위한 사업용 단말기를 따로 지급해 주거나 다른 부서 배정을 요청했다. 그러나 KT는 인사위원회를 열어 이씨가 '성실 의무'와 '조직 내 질서존중의 의무'를 위반했다며 정직 1개월의 징계를 내리고 정직 기간이 끝나자 이 씨를 타 부서로 전보발령 냈다. 이에 이씨는 KT의 업무지시가 개인정보 보호법을 위반한 것으로, 앱 설치 거부를 징계사유로 삼을 수 없다며 소송을 제기했고 재판부는 이 씨의 손을 들어줬다. 재판부는 "원고가 이 사건 앱의 설치를 거절해 업무수행을 하지 못했다는 것만으로 성실의무를 위반했다고 볼 수 없다"며 "달리 피고 회사의 업무지시 필요성이 원고의 개인정보 자기결정권에 대한 제한의 불이익보다 더 크다고 볼 수 없다"고 판시했다.[91] 이 사건은 항소심에서도 같은 판결을 받아 직원 이 씨가 승소했다(서울고등법원 2018. 6. 26. 선고 2017나2024180 판결).

노동자 폭행 등 갑질 논란을 일으킨 웹하드 업체 위디스크(회장 양진호)는 해킹앱을 개발해 직원들의 통화 기록, 메시지, 연락처 등 수 만건을 실시간으로 들여다보며 도·감청했다는 언론보도가 나왔다. 2018년 11월 언론 보도에 따르면, 이 업체 회장은 2011년 말쯤부터 '하이톡'이라는 사내 메신저 개발을 추진했다. 이 과정에서 회장은 직원들이 휴대폰에 '하이톡'을 깔면 자동으로 도청 프로그램 '아이지기'가 몰래 설치되도록 해킹 소스를 끼워 넣었다. 본래 '아이지기'는 자녀 안전을 확인하기 위한 프로그램으로 고안됐다. 휴대폰에 있는 전방, 후방 카메라를 원격으로 촬영해서 주변을 살피거나 실시간 위치 추적을 하는 기능 등이 포함돼 사실상 '실시간 감시'를 할 수 있는 장치다. 2012년경부터 직원들을 도청하기 시작해 통화·문자 메시지·주소록·통화 녹음 파일 등 피해 규모가 약 10만 건에 이르는 것으로 파악됐다.[92]

업무용 앱의 대표적인 형태는 MDM(Mobile Device Management)이다. 이는 회사 IT부서가 직원의 스마트 기기를 원격으로 관리하는 방식으로 개인 프라이버시를 과도하게 침해하는 문제를 안고 있다. 기업들은 ICBAM(Iot, Cloud, Bigdata, AI, Mobile) 기술을 버무리면서 업무의 매끄러운 흐름·순환·의사소통을 최대화하는 방향의 업무 환경을 재편하

91) 법률신문, "'개인정보 침해우려' 회사 업무용 앱 설치 거부했다고 징계는 '부당'", 2017.4.10.; 미디어오늘, "'감시하려는 거 아니냐' 노동자, 앱 설치 명령 거부할 수 있다", 2017.4.10.

92) 경향신문, "양진호, 직원 수십명 휴대폰 해킹해 실시간 감시하기도", 2018.11.8.

고 있는데, 업무용 앱의 형태도 ICT 기술의 속도만큼이나 빠르게 진화하고 있다. 사실 업무용 앱의 변화는 프라이버시 침해, 보안 침해 등에 대한 문제 제기의 속도보다 더 빨라 보이는 정도다. MDM의 다음 버전으로 MAM이 등장했고 MAM, UEM, EMM, BYOD, BYOT, BYOP 등 업무 편리성을 제고한다는 신기술의 새로운 이름들은 계속 버전 업 중이다.

<표4-7> 업무용 앱 비교[93)]

방 식	특 징
MDM (Mobile Application Management)	**IT 부서가 원격**으로 직원 소유 또는 기업 소유의 스마트폰이나 태블릿, 기타 **디바이스**를 등록한 후, 직원이나 직원의 업무에 특화된 프로파일을 통해 이를 추적하고 관리하고 보호하는 방식. 그러나 MDM은 이처럼 개인 영역을 과도하게 침해
MAM (Mobile Application Management)	디바이스 자체가 아니라 기업용 애플리케이션과 관련 **데이터만을 관리·통제**하는 방식. 물리적인 디바이스 전체는 건드리지 않고 기업이 업무용 애플리케이션과 관련 콘텐츠에 대한 액세스를 통제
UEM (Unified Endpoint Management)	IT 부서가 스마트폰과 태블릿, 노트북, 데스크톱, 그리고 사물인터넷 디바이스까지 **모든 하드웨어를 하나로 포괄해 원격으로 제어**하고 보호
EMM (Enterprise Mobility Management)	다양한 소프트웨어 **관리 툴을 하나의 우산 아래** 모으는 것. MDM과 MAM을 통해 생성된 기업 데이터도 관리.
BYOD (Bring Your Own Device)	**개인 단말기**를 사무실에 가져와 업무용으로 사용하는 것. 개인의 단말기 정보를 시스템에 등록해 업무 시스템 접근만 허가. 업무를 언제 어디서든지 처리할 수 있게 하는 편리성을 제공. 기업은 단말기를 지원하지 않아도 되고 교체 비용, 라이선스 구입비, 유지 비용 등 비용적인 측면에서 절감. 개인이 소유한 스마트 기기를 직장에 가져와 업무에 활용하도록 허용하는 것을 BYOD라고 하는데, BYOT(Bring Your Own Technology), BYOP(Bring Your Own Phone), BYOPC(Bring Your Own PC) 등 다양한 방식으로 변용

프라이버시 침해, 보안 침해 등에 대한 문제들이 계속됨에도 많은 기업에서 업무 효율과 편리성을 이유로 새로운 업무용 앱을 더욱 활용하고 있는 모양새다. 배달앱이나 GPS 트래커가 새로운 형태의 노동인 플랫폼 노동에 적용되는 기술 장치들이라면, 업무용 앱은 기존 정규 노동자에게 플랫폼 노동을 덧대기 위해 배치된 기술 장치라고 볼 수 있다.

93) ITWORLD, “모바일 관리 솔루션 MDM, MAM, EMM, UEM의 차이”, 2017.7.11.

두 형태 모두 노동을 탈공간화하는 동시에 위치 추적을 포함해 업무의 전과정을 실시간으로 데이터화 할 수 있다.

나. 업무의 일상 침투: 시간권리를 무력화하는 SNS 업무지시

2015년 직장인의 공감을 산 신조어 1위는 '메신저 감옥' 'SNS 감옥' '카톡 감옥'이었다. 'SNS 감옥'은 스마트폰으로 언제나 연락이 가능해지면서 사무실을 벗어나도 업무에서 벗어나지 못하는 상황을 빗댄 표현이다. 업무의 일상 침투는 빈번하고 지시종속성도 상당하다. 노동시간의 외연적 연장이나 내포적 연장과도 다른 양상이다. 누군가 공장을 '완화된 감옥'이라 불렀다는 점에 빗대어 보면, 디지털 모바일 시대의 일상은 '투명한 감옥'이 되었다고 말할 수 있다.

<그림4-9> '새벽불림' 당하는 노동자 [94)]

2013년 국가인권위원회가 내놓은 <정보통신기기에 의한 노동인권 침해 실태조사>에 따르면, 퇴근 후나 휴일에 업무지시를 받았다는 응답이 63%였다. 2015년 취업포털 사이트 <사람인>의 조사에서도 직장인의 69%가 업무시간 외에 메신저로 업무 연락을 받았다. 그 가운데 88%는 즉시 업무 처리를 해야 했고, 심지어 60%는 회사로 복귀해야 했다. 2015년 한국노동연구원이 내놓은 <스마트기기의 사용이 근로자의 일과 삶에 미치는 영향>에 따르면, 비율은 70.3%로 더욱 높았다. 많은 사람들이 업무시간 외에도 SNS 업무지시를 받아 '정기적으로' 일을 하고 '항시 대기' 상태에 놓여있다. 일터와 일상의 경계

가 허물어지면서 보이지 않는 노동시간이 증가했다. 이러한 공짜 노동의 비중은 날로 높아지고 있다. 업무의 일상 침투로 피로도와 스트레스 또한 그만큼 증가했다. 퇴근 이후에도 일거리 네트워크에 연결돼 '항시 대기'상태에 놓인 지금의 모습은 디지털 노동이 만든 새로운 질병의 일면이라 말할 수 있다. '항시 대기' 스트레스는 퇴근 후는 물론 주말, 휴일, 휴가를 가리지 않는다. 이는 단지 스트레스와 피로도의 문제가 아니다. 시간권리의 침해 상황이다. 내 시간인지 회사의 시간인지 그 구분이 점점 모호해지는 상황이 가속화되고 있다.

5. 정신적 자율성 침해와 민주적 가치의 파괴

1) 정신적 자율성 침해

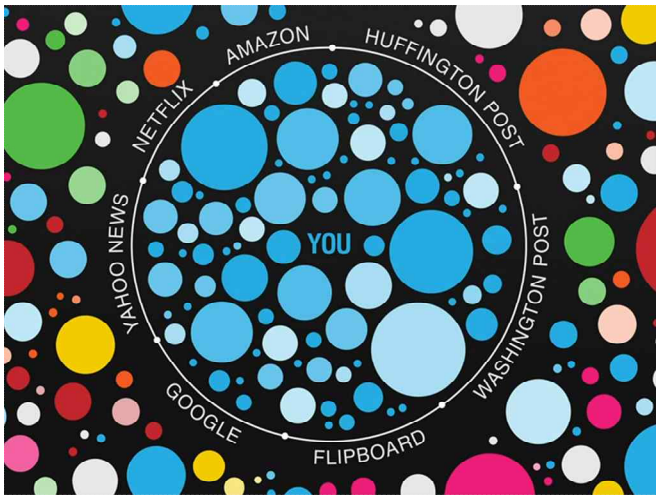
헌법은 사생활 보호를 기본권으로 규정하고 여기에는 양심과 성적 영역과 같은 내밀한 영역, 인격적인 감정세계 존중의 권리와 정신적인 내면생활이 침해받지 않을 권리가 포함된다[95]. 정보인권이 정보통신 온라인 영역의 사생활 보호라고 한다면, 온라인 영역에서 감정세계와 정신적인 내면생활 등이 침해받지 않을 권리를 포함한다. 특히 빅데이터와 인공지능, 프로파일링 등 4차 산업혁명 관련 기술 발전과 커뮤니케이션 수단이 SNS로 확대되고 플랫폼을 통해 드러나면서 감정세계와 내면생활의 노출이 일상적으로 일어나고 있다. 좋아요, 싫어요 등 감정과 정서의 표시뿐 아니라 선호, 의식, 판단과 믿음과 같은 여론의 형성의 기본 정보들이 온라인상에 데이터와 개인정보로 상존한다. 이러한 정보들이 광범위하게 노출되고 수집, 평가, 분석되면서 감정세계와 내면생활이 침해받을 가능성이 더욱 커지고 있다. 이처럼 물리적 생활영역에 대한 개인정보 뿐 아니라 감정세계와 정신적 내면생활에 대한 개인정보를 통한 침해의 확대는 여론과 선호 조작의 가능성을 높이고 반복적, 지속적, 편향적 정보의 노출로 개인의 내면적 의식을 침해하고

94) 월스트리트저널, 2015.5.20.

95) "구체적으로 사생활의 비밀과 자유가 보호하는 것은 개인의 내밀한 내용의 비밀을 유지할 권리, 개인이 자신의 사생활의 불가침을 보장받을 수 있는 권리, 개인의 양심영역이나 성적 영역과 같은 내밀한 영역에 대한 보호, 인격적인 감정세계의 존중의 권리와 정신적인 내면생활이 침해받지 않을 권리 등입니다"(헌재 2003. 10. 30. 2002헌마518).

지배할 수 있다. 이를 '정신적 자율성(mental autonomy)의 침해'로 규정한다.[96][97]

'필터 버블(filter bubble)'은 인터넷 정보제공자가 맞춤형 정보를 사용자에게 제공해 사용자는 필터링 된 정보만을 접하게 되는 현상을 지칭한다.[98] 개인 맞춤형 콘텐츠 추천을 통해 나타난 광고가 대표적이다. 특정 상품이나 장소 등을 검색한 후에 구글이나 페이스북에서 자신이 검색한 여행지의 호텔이나 패키지 상품 광고가 뜨는 것을 경험해 보았을 것이다. 클릭 하나하나가 데이터가 되고 개인을 파악하는데 이용된다. 광고를 제공하는 업체들은 소비자/사용자 정보를 바탕으로 사용자가 관심을 가질만한 광고 콘텐츠를 내보낸다.



<그림4-10> 필터 버블(filter bubble) 현상[99]

96) 서창록, 리스크와 이익의 뉴 프론티어(New Frontier) 비즈니스와 인권에 대한 4차 산업혁명의 영향, 제4회 국제인권심포지엄 자료집, 법무부 외, 2018.6.5.

97) 유엔 의사표현의 자유 특별 보고관의 '의사표현의 자유권 증진과 보호(Promotion and protection of the right to freedom of opinion and expression)'에 따르면, 세계인권선언 19조 및 시민적, 정치적 권리에 관한 국제규약 19조에 근거하여 인공지능 기술과 미디어 및 검색 왜곡, 광고 등 콘텐츠 큐레이션이 결합하여 의견을 형성할 권리를 방해한다고 규정한다. 의사표현의 자유의 필수 요소는 "의견을 형성하고 추론을 통해 이를 발전시킬 수 있는 권리"를 말하며, 유엔 인권위원회는 이 권리가 개인의 신념, 이데올로기, 반응 및 위치를 발전시키는데 과도한 강요로부터 자유를 요구한다고 결론지었다. 따라서 강제적인 정신적 개입, 주입식 프로그램 또는 개인의 특정 의견 수렴 또는 의견 변경을 강요하는 폭력적 위협은 인권규약 제19조를 위반한다고 강조한다.

98) Eli Pariser, The Filter Bubble, Penguin, 2011.

99) Proto.Ink 홈페이지 참조

사용자는 플랫폼이 제공하는 서비스를 이용하려면 자신이 원하든 원하지 않든 일정량의 광고에 노출될 수밖에 없다. 기업들은 해당 서비스를 무료로 사용하는 대가라며 광고를 노출시킨다. 대부분의 사용자에게 플랫폼을 통한 광고주의 광고는 부(음)의 효용으로 여겨진다. 그러나 사용자의 검색이력 또는 빅데이터 등을 활용한 광고는 관련 기술을 활용하여 개별 사용자의 관심과 선호에 반응하여 소비자에게 광고 상품을 제공하고 추천한다. 이는 사용자들의 행위 패턴 및 삶 전체가 데이터로 수집·가공·저장·활용되는 상황을 여실히 보여준다. 이와 같은 데이터가 유사-자발성에 기초하여 소비자의 필요를 과장하고 확대하며 기업의 이윤 활동으로 전유한다. 또한 수집된 데이터에 근거해서 소비자들을 분류하고 나아가 차별적으로 대우하게 된다. 여기서 다시 알고리즘의 편향과 결합하여 사용자 개인이 자신의 취향이나 선호를 알고리즘 체계에 의해 거꾸로 확증 판단하게 되는 '필터 버블' 현상이 일어난다.

전 세계 20억 명 이상이 이용하는 페이스북은 담벼락 포스팅의 많은 수가 광고로 채워지고 있다. 광고의 내용이 부적절한 경우도 있고 가짜 상품 광고도 버젓이 등장하면서 페이스북 광고는 계속 논란을 일으켜 왔다. 넘쳐나는 광고와 사용자의 감정적인 소모를 불러일으키는 원하지 않는 포스팅의 표출 이외에 개인정보 침해에 따른 위험 역시 페이스북이 안고 있는 중대한 이슈이다.

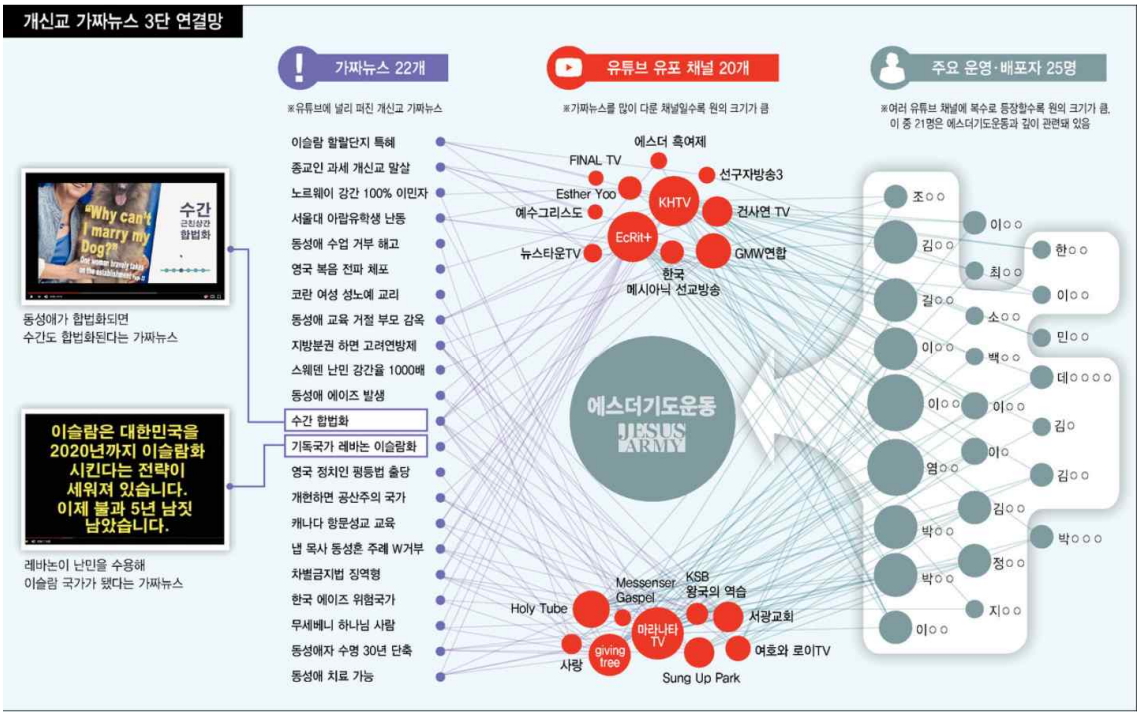
또한, 2016년 공정거래위원회는 대표적인 O2O 서비스 사업자들인 배달 앱 운영 사업자들이 소비자들의 불만족 이용 후기는 비공개 처리하고 거짓 이용후기의 작성이나 주문건수 조작, 광고상품을 구입한 음식점은 맛과 서비스가 우수한 것처럼 표시하여 소비자를 기만한 행위를 적발했다.[100]

알고리즘으로 분석되는 개인 맞춤형 콘텐츠 추천 시스템에 편향적 의식과 판단 또는 왜곡된 정보를 유발하는 콘텐츠가 결합하면 침해의 정도는 더 커지게 된다. 넘쳐 나는 정보 속에서 특정 정보만 공급받거나 받아들이면 정치·사회적인 문제에서 고정관념과 편견을 강화하는 계기가 되고 다시 편견이 확대되는 악순환이 반복된다.

미국 조사업체 <버즈피드(BuzzFeed)>가 2016년 11월 17일 분석 기사에 따르면, 미국 대선 전 3개월간 가장 인기 있었던 가짜 뉴스 20개의 페이스북 내 공유, 반응, 댓글 수는

100) 공정거래위원회 보도자료, 2016.7.29.

871만 1천 건으로 <뉴욕타임스>, <워싱턴포스트> 등 주요 매체의 기사보다 더 많은 반응을 이끌어냈다. 특히 '프란치스코 교황이 트럼프 지지를 발표했다'거나 '클린턴 후보가 ISIS에 무기를 판매했다'는 식의 터무니없는 내용도 특정 성향을 가진 사람들에게 좋은 소식이기 때문에 비슷한 성향의 그룹에서 빠르게 공유되고 확산력을 가진다.[101] 한국에서도 유사한 사례가 속출했다. 일부 시민들은 가짜 뉴스와 상관없이 입맛에 맞는 내용만을 유튜브를 통해 찾아보고 SNS로 확산한다.[102]



<그림4-11> 가짜뉴스 형성 경로 예시[103]

한편, 감정세계와 내면의 의식이 드러나고 수집되는 온라인 공간의 의존도가 확산하면서 이에 따른 스트레스와 피로도 정보인권 침해 문제로 볼 수 있다. 일상의 상당부분이 SNS에 강박되어 일상의 시간을 지배한다. 이것이 노동현장에서는 업무시간 외에도 업무

101) 네이버지식백과, "필터버블", 2018.11.13. 검색.
102) JTBC, "사실 여부 떠나 듣고 싶은 뉴스만 … 유튜브에 갇힌 노인들", 2018.7.23.

를 지배하는 수단이 될 뿐만 아니라 일상생활에서는 삶의 외양을 지배하며 내적·외적 사생활을 끊임없이 외부로 노출하는 것을 강요한다.

이를 'SNS 피로증후군'으로 표현하기도 한다. 2017년 한 조사에 따르면, SNS 사용자 10명 중 3명 정도(31.7%)는 'SNS 피로증후군'을 경험한 것으로도 나타났다. 그 결과 SNS의 영향력이 확대되고 있음에도 불구하고 실제로 SNS를 적극적으로 활용하는 사용자는 줄어들고 있는 것으로 조사됐다. 예전보다는 SNS 이용이 감소했다는 응답자(33%)가 증가했다는 응답자(20.5%)보다 많았다. SNS 이용이 줄어든 이유로는 SNS에 대한 흥미와 관심이 떨어지고(43.9%, 복수응답), SNS를 사용할 필요성을 점점 느끼지 못한다(39.3%)는 점을 주로 많이 꼽았다. 사생활이 불특정 다수에게 노출되는 것이 싫고(34.1%), SNS를 관리하는 데 너무 많은 시간과 노력이 들어가는 것 같다(29.7%)고 생각하는 사람도 많았다.[104]

2) 여론 조작과 민주적 가치의 파괴

확증편향(confirmation bias)은 선입관을 뒷받침하는 근거만 수용하고, 자신에게 유리한 정보만 선택적으로 수집하는 것을 말한다. 보고 싶은 것만 보고 믿고 싶은 것만 믿는 현상인데, 정보의 객관성과는 상관없다. 필터버블이 정보의 공급자에 의해 발생하는 문제라면 확증편향은 그 결과로 수용자가 갖는 태도를 말한다. 왜곡된 정보의 소통은 확증편향을 일으킨다. 2018년 10월, 김포의 한 어린이집 보육교사가 아동학대로 오인 받아 인터넷 커뮤니티 사이트에 사실관계에 대한 확인도 없이 비난이 일고 보육교사의 신상이 공개됐다. 이 보육교사는 엄청난 비난 속에 해당 아동의 가족들에게 폭행당하고 경찰 조사까지 받게 되자 자살에 이르렀다.[105] 개인이 받아들이고 판단하는 정보의 조작, 왜곡, 편향이 개인적 차원에서 정신적 자율성을 침해하는 것으로 나타난다면, 공동체 차원에서는 개인의 정신적 자율성 침해의 결과로 공동체 전체의 여론을 왜곡하고 조작하며, 공동체 운영의 민주적 가치들을 훼손하고 파괴하는 데까지 나아가고 있다.

선호 등의 감정 세계와 옳고 그름과 믿음 등의 의식적 판단에 영향을 미치는 정신적

103) 한겨레신문, 2018.9.28.
104) 매일경제, "SNS 피로증후군 "이제 흥미가 떨어졌다"", 2017.7.10.
105) 국민일보, 학대 의심 받은 교사 투신, 2018.10.17.

자율성을 침해 받으면서 여론과 민주적 의사결정 및 선거 등 공동체 운영의 민주적 가치들이 훼손되고 파괴되고 있다. 일상적인 여론조작은 물론 정치적인 의사결정에도 영향을 미친다. 18대 대선 때는 국가정보원을 비롯하여 국가보훈처, 행정안전부, 군사이버사령부 등 거대한 국가기관이 총체적으로 개입이 되어 120만개 넘는 댓글과 여론조작 등을 하면서 국가차원의 조직적인 선거부정을 저질렀다. 또한 경제공진화 모임의 드루킹은 각종 선거에 개입해 여론을 조작했다. 드루킹은 매크로 프로그램인 '킹크랩'을 이용해 1달 사이에 5,533개 기사의 댓글 22만1,729개에 대해 1,131만116회에 이르는 공감·비공감 조작했다.[106] 이 사건들은 선거 등에 영향을 미칠 목적으로 의도적으로 기사의 댓글 등을 조작하고 대중의 여론을 호도한 사건이다.

<그림4-12> 드루킹의 여론 조작 방법[107]

선거와 의식 조작의 가장 드라마틱한 사례는 2016년 미국 대선 당시 정보 분석 회사인 캠브리지 애널리티카(Cambridge Analytica)가 도널드 트럼프 후보의 선거 운동에 활용하기 위해 페이스북 활동을 조작한 사례다. 애널리티카는 페이스북 앱을 통해 5천만 명의 개인정보를 확보하고 인공지능으로 페이스북 활동을 프로파일링해 정치성향을 확인했다. 그 후 특정 사람에게만 보이는 '다크 포스트(dark post)'를 보내 트럼프에게 유리한 글을 타임라인에 계속 올려놓거나, 광고처럼 보이지 않게 설계된 광고 메시지인 '네이티

106) 중앙일보, ""한달만에 1131만 조작" … 네이버도 뚫는 드루킹 '킹크랩 2'", 2018.7.22.
107) 연합뉴스 2018.4.24.일자

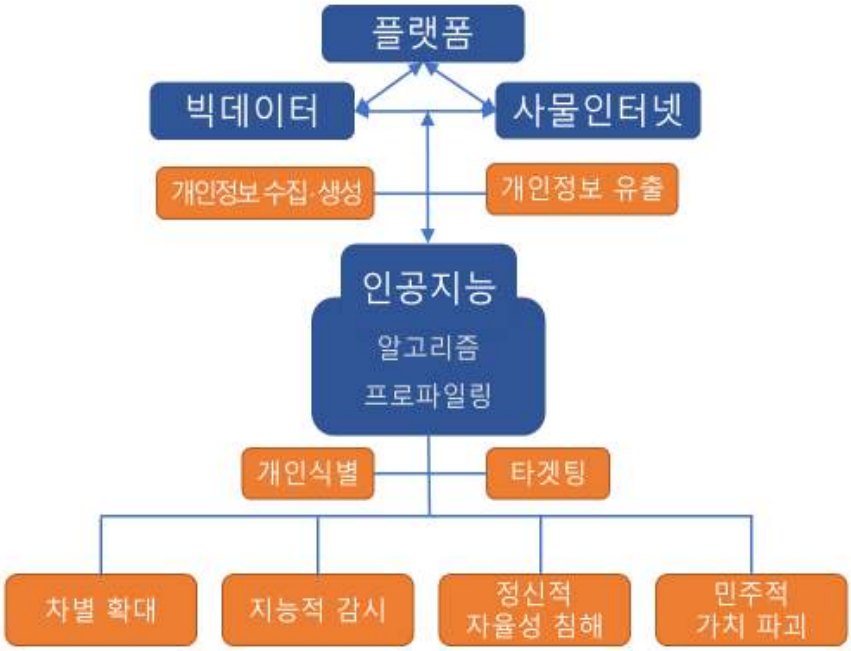
브 광고'를 노출하게 만들어 트럼프 지지가 대세인 것처럼 보이게 했다. 유권자를 상대로 일종의 세뇌공작을 벌인 것이다.

또한, 2016년 필리핀 대선에서는 자동 프로그램인 '트위터 봇' 계정이 두테르테 선거운동을 무작위로 진행했다. 같은 해 치러진 미국 대선에서도 러시아가 배후로 추정되는 트럼프 지지 '봇' 활동이 있었다. 최근 태국, 베트남, 미얀마, 말레이시아 등 동남아시아 국가와 홍콩, 대만 등 일부 동아시아 국가, 스리랑카를 비롯한 남아시아에서도 선거를 앞두고 트위터 계정이 급증하고 있다. '봇'을 통한 선거운동이 의심되는 상황이다.[108]

108) 연합뉴스, "페이스북 사태가 호기? … 동남아 국가들 선거전 악용·단속 우려", 2018.4.5.

3절 시사점

4차 산업혁명의 기술 발전에 따른 정보인권 침해는 새로운 조건 속에서 보다 복잡하고 다양한 양상을 보여주고 있다. 무엇보다 사물인터넷, 빅데이터, 플랫폼과 인공지능이 결합하면서 개인정보의 수집에서부터 분류와 처리, 폐기에 이르는 전 과정에서 정보인권 침해의 새로운 유형이 나타나고 있다. 특히 알고리즘 처리와 프로파일링은 개인을 식별하고 특정함으로써 차별과 감시는 물론 정신적 자율성과 공동체의 민주적 가치를 파괴하는 정보인권 침해의 주요한 원천이 되고 있다.

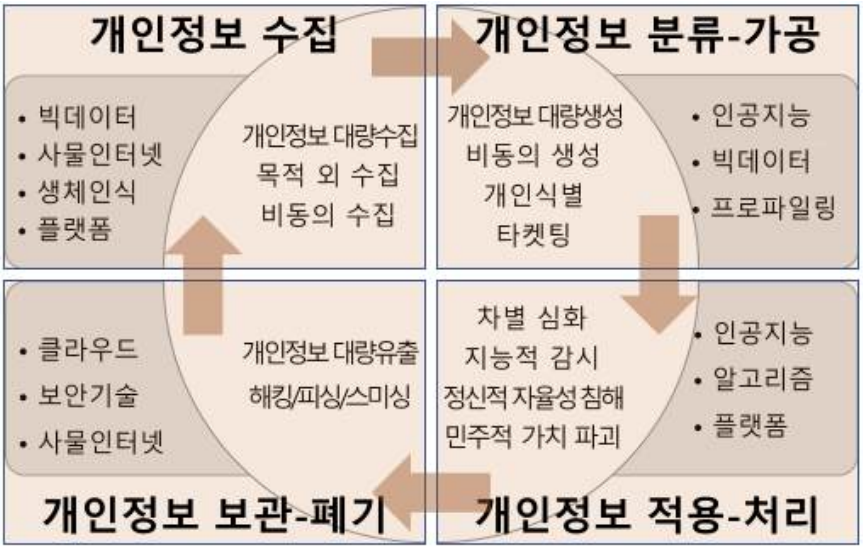


<그림4-13> 4차 산업혁명 기술과 정보인권 침해 유형

빅데이터, 사물인터넷, 플랫폼과 인공지능이 상호 결합하면서 개인정보의 수집과 생성을 기하급수적으로 늘려 놓았다. 이에 따라 해킹은 물론이고 상업적 거래, 정치적 목적으로도 개인정보 유출 위험이 늘어나 유출 규모나 피해 규모도 커지고 있다. 또한 광고와 여러 목적의 개인 식별과 타깃팅이 확대되고, 알고리즘이나 프로파일링을 통해서 개인정

보가 결합·분석·식별되면서 다양한 정보인권 침해를 낳고 있다. 알고리즘을 통한 사회, 정치, 경제적 차별이 확대하고 CCTV와 드론 등 지능적 감시기술이 발달하면서 국가에 의한 감시 통제 뿐 아니라 노동현장의 감시도 확대하고 있다. 또한 정서나 선호, 판단 등 개인의 의식 및 내면 생활 등에 관한 개인정보의 노출과 수집이 확대되면서 의사(opinion)는 물론 정신적 자율성을 침해하고 나아가 공동체의 여론과 민주적 의사결정 등 민주적 가치를 훼손하고 파괴하는 일까지 벌어지고 있다.

또한, 4차 산업혁명 기술 발달에 따른 새로운 유형의 정보인권 침해 사례를 살펴 본 것과 같이 개인정보의 수집부터 폐기까지의 개인정보 라이프사이클[109] 전 과정에서 다양한 형태의 침해가 발생함을 확인할 수 있다.



<그림4-14> 생애주기별 개인정보 침해유형 및 관련 기술

우선 개인정보 수집 단계에서는 빅데이터와 사물인터넷, 바아오 기술과 플랫폼 등을 통해 다량의 개인정보가 수집된다. 여기에는 정보주체가 동의하지 않았거나 정보 수집 목적을 벗어난 개인정보도 대량 수집된다. 특히 사물인터넷 등을 통한 사용자의 사용이

109) 개인정보 라이프사이클이란 개인정보가 기업 또는 정부기관에 의해 수집, 저장, 이용, 파기되기까지의 일련의 과정을 체계화한 것이다. 관련 기관과 연구자에 따라서는 서로 다르게 구분하는데, 여기서는 수집, 분류-가공, 적용-처리, 보관-폐기의 4단계로 구분한다.

활발해질수록 다양한 개인정보가 빅데이터화 되면서 수집된다. 여기에는 개인 신상 정보뿐 아니라 바이오 정보와 개인의 내밀한 정보까지 포함된다.

둘째, 개인정보의 분류와 가공 단계에서는 인공지능, 빅데이터는 물론 이를 통해 정보결합과 프로파일링이 이뤄진다. 여기서 새로운 개인정보가 대량 생성되고 다시 개인정보와 결합함으로써 개인 식별이 이뤄지고 있다. 비식별 정보, 가명정보라 할지라도 재결합을 통해 개인 식별이 이뤄진다.

셋째, 개인정보의 처리와 적용 단계에서는 개인정보가 인공지능, 플랫폼 등과 결합된 알고리즘 처리를 통하면서 정보인권 침해의 핵심적 문제들을 발생시키고 있다. 우선 인공지능 기계학습의 알고리즘 편향성으로 인해 채용에서부터 금융, 보험은 물론이고 기본적인 식별과정에서 특정집단에 대한 차별이 확대되고 있다. 뿐만 아니라 노동과정에서도 알고리즘과 데이터화에 기반한 차별이 확산되고 있다. 또한, 빅데이터, 인공지능 등의 분석도구를 활용해 국가기구의 저인망식 감시와 범죄예측시스템의 도입, 지능형 CCTV와 드론 그리고 노동현장에서 작업장 밖으로까지의 데이터와 알고리즘 감시가 확대됨을 확인할 수 있다. 끝으로 개인의 선호나 선택 등 취향과 감정세계를 결정하는 정보와 판단, 믿음 등 의식을 주관하는 정보들이 편향적으로 수용됨으로써 정보주체의 의사와 정신적 자율성을 침해하고 공동체의 민주적 가치들을 파괴하는 일이 발생하고 있다.

넷째, 개인정보의 보관 및 폐기의 단계에서는 개인정보들이 클라우드 기술 등으로 이동되고 확산됨에도 불구하고 제대로 관리되지 못하고, 보안기술의 발달에도 불구하고 해킹 기술 또한 고도화 하면서 다양한 유출 문제를 야기하고 있다. 일반적인 수준의 해킹은 물론이고 랜섬웨어 등을 통한 협박, 피싱, 스미싱, 봇넷 등 다양한 사이버 공격을 일으킨다. 특히 사물인터넷으로 네트워크의 결합이 확대하면서 이러한 사이버 공격들은 유형을 달리하면서 매우 다양하게 나타날 것으로 예상된다.

제5장 4차 산업혁명 시대 정보인권 관련 국내외 법제 동향

앞서 4장에서 빅데이터, 인공지능, 사물인터넷 등 신기술의 발전에 따른 정보인권 침해 사례 및 유형에 대해서 살펴보았다. 이러한 정보인권 침해를 사전에 예방하고 정보주체의 피해를 구제하기 위해서는 적절한 법제도가 마련될 필요가 있다. 2018년 9월, 하버드대 버크만센터가 발표한 <인공지능과 인권, 기회와 위험(Artificial Intelligence & Human Rights: Opportunities & Risks)>에 대한 보고서[110]에서 지적한 바와 같이, 인공지능을 비롯한 신기술은 인권에 부정적 영향뿐만 아니라 긍정적 영향을 미칠 수 있고, 프라이버시권, 평등권, 표현의 자유, 집회결사의 자유, 노동권 등 서로 다른 권리에 영향을 미칠 수 있다. 신기술에 대응하는 법제도는 이에 따른 다양한 영향에 대한 평가에 기반을 두어야 할 것이다.

이 장에서는 개인정보에 대한 권리를 중심으로 4차 산업혁명 관련 국내외 법제 동향 및 쟁점을 분석한다. 신기술에 대한 법제적 대응을 개인정보 침해와 차별 등 개인정보에 대한 권리 측면 및 권력기관에 의한 지능형 감시 측면으로 나누어 검토한다.

제1절 해외 법제 동향 및 분석

1. 신기술에 대응한 규범 수립을 위한 국제적 노력

최근 인공지능 시스템 및 알고리즘 개발에 있어 윤리적 규범을 수립하기 위한 노력이 국제적으로 이루어져 왔다. 우선 2016년 12월, 국제전기전자기술자협회(IEEE)는 <윤리적으로 조율된 설계(Ethically Aligned Design)>[111]에 대한 권고안을 발표하면서 인공지능 및 자동시스템 개발 시 책임성, 투명성, 인식제고, 개인정보보호, 고용문제 등 윤리적 측면을 고려한 설계가 필요함을 강조하였다.

---

110) Filippo A. Raso, Hannah Hilligoss, Vivek Krishnamurthy, Christopher Bavitz, Levin Kim. 2018. “Artificial Intelligence & Human Rights: Opportunities & Risks”. The Berkman Klein Center for Internet & Society Research Publication Series(2018.9.25).

111) IEEE 홈페이지(ethicsinaction.ieee.org) 참조.

2017년 1월, 인공지능 연구자와 학자들이 미국 캘리포니아주 아실로마에 모여 인공지능이 가져올 가능성과 위협, 그리고 이 기술이 인류에 혜택을 줄 수 있도록 할 방안에 대해 토론하고 23개의 원칙을 발표했다.[112] 이 원칙은 특히 인공지능 알고리즘과 시스템의 '윤리와 가치' 측면에서 투명성, 책임성, 인간의 개입, 개인정보에 대한 권리 등의 원칙을 포함하였다.

아실로마 인공지능 원칙(Asilomar AI Principles)

연구 이슈(Research Issues)

1) 연구 목표: 인공지능(AI) 연구의 목표는 지향하는 바가 없는 지능이 아니라 유익한 지능을 창출하는 것입니다.
2) 연구비 지원: AI에 대한 투자에는 다음과 같이 컴퓨터 과학, 경제, 법, 윤리 및 사회 연구 등의 어려운 질문을 포함한, 유익한 사용을 보장하는 연구를 위한 기금이 동반되어야 합니다.

- 미래의 인공지능 시스템이 오작동이나 해킹없이 우리가 원하는 것을 수행할 수 있도록 매우 탄탄하게 만들 수 있는 방안은 무엇입니까?
- 인류의 자원과 목적을 유지하면서 자동화를 통해 우리가 계속 번영할 수 있는 방안은 무엇입니까?
- AI와 보조를 맞추고 그와 관련된 위험을 관리하기 위해 법률 시스템을 보다 공정하고 효율적으로 업데이트 할 수 있는 방안은 무엇입니까?
- AI는 어떠한 가치들에 따라야 하며, 그것이 가져야 하는 법적, 윤리적 상태는 무엇입니까?

3) 과학-정책 관계: AI 연구자와 정책 입안자간에 건설적이고 건전한 교류가 있어야 합니다.
4) 연구 문화 :AI 의 연구자와 개발자간에 협력, 신뢰, 투명성의 문화가 조성되어야 합니다.
5) 경쟁 회피: AI 시스템을 개발하는 팀들은 안전 기준에 대한 질낮은 해결책을 피하기 위해 적극적으로 협력해야 합니다.

윤리와 가치(Ethics and Values)

112) Future of Life Institute. ASILOMAR AI PRINCIPLES(futureoflife.org/ai-principles 참조).

6) 안전: AI 시스템은 작동 수명 전반에 걸쳐 안전하고 안정적이어야 하며, 적용과 실현이 가능하다면 검증 할 수 있어야 합니다.

7) 오류 투명성: AI 시스템이 해를 입히는 경우 그 이유를 확인할 수 있어야 합니다.

8) 사법의 투명성: 사법 결정에 있어 자동화된 시스템이 개입할 경우, 권한있는 인간 기관이 감사할 수 있는 충분한 설명을 제공해야 합니다.

9) 책임성: 고급 AI 시스템의 설계자와 제조자는 그것의 사용, 오용 및 행위의 도덕적 함의에 있어서, 그것을 형성할 책임과 기회가 있는 이해관계자 입니다.

10) 가치의 준수: 고도로 자율적인 AI 시스템은 그것이 작동하는 동안 목표와 행동이 인간의 가치와 반드시 일치하도록 설계되어야 합니다.

11) 인간의 가치: AI 시스템은 인간의 존엄성, 권리, 자유 및 문화 다양성의 이상과 양립할 수 있도록 설계되고 운영되어야 합니다.

12) 개인 정보 보호: AI 시스템이 개인정보 데이터를 분석하고 활용할 수 있는 경우, 사람들은 자신이 생성한 데이터에 접근해 관리 및 제어할 권리를 가져야 합니다.

13) 자유와 개인 정보: 개인정보에 대한 AI 의 적용이 사람들의 실제 또는 인지된 자유를 부당하게 침해해서는 안됩니다.

14) 이익 공유: AI 기술은 가능한 많은 사람들에게 혜택을 주고 역량을 강화해야 합니다.

15) 공동 번영: AI에 의해 만들어진 경제적 번영은 모든 인류에게 이익이 되도록 널리 공유되어야 합니다.

16) 인간 통제: 인간은 인간이 선택한 목적을 달성하기 위해, 의사 결정을 AI 시스템에 위임할 것인지 여부와 방법에 대해 선택할 수 있어야 합니다.

17) 비전복: 고도로 발전된 AI 시스템의 통제를 통해 부여되는 권력은 건강한 사회가 의존하는 사회적 시민적 과정을 전복하기보다, 존중하고 개선해야 한다.

18) AI 무기 경쟁: 치명적인 자동화 무기의 군비 경쟁은 피해야 합니다.

장기적 이슈(Longer-term Issues)

19) 능력치에 대한 주의: 합의가 없으므로, 미래 AI의 능력 상한선에 대한 강한 가정은 피해야 합니다.

20) 중요성: 고급 AI는 지구 생명체의 역사에서 중대한 변화를 나타낼 수 있으며, 그에 상응

하는 관심 및 자원을 통해 계획되고 관리되어야 합니다.

21) 위험 요소: AI 시스템이 초래하는 위험, 특히 치명적인 또는 실존적 위험은 예상되는 영향에 상응하여 대비하고 완화 노력을 기울여야 합니다.

22) 재귀적 자기 개선: 질과 양을 빠르게 증가시킬 수 있도록 스스로 개선 또는 복제할 수 있도록 설계된 AI 시스템은 엄격한 안전 및 통제 조치를 받아야 합니다.

23) 공동 선: 수퍼 인텔리전스는 광범위하게 공유되는 윤리적 이상에만 복무하도록, 그리고 한 국가 또는 조직보다는 모든 인류의 이익을 위해 개발되어야 합니다.

일본의 경우 2017년 총무성 정보통신정책연구소가 <인공지능 개발원칙>을 발표하였다(조성은 외, 2018: 99)[113]. 이 원칙에는 ① 연계의 원칙, ② 투명성의 원칙, ③ 제어 가능성의 원칙, ④ 안전의 원칙, ⑤ 시큐리티의 원칙, ⑥ 프라이버시의 원칙, ⑦ 윤리의 원칙, ⑧ 사용자 지원의 원칙, ⑨ 책임의 원칙 등이 포함되었다.

① 연계의 원칙

o 개발자는 AI시스템의 상호접속성과 상호운용성에 유의한다.

- 상호접속성·상호운용성 관련 정보 공유, 국제표준 준용, 데이터 형식 표준화, API 포함 인터페이스 또는 프로토콜 오픈화 대응 노력, IP 라이선스 계약 공정화

② 투명성의 원칙

o 개발자는 AI시스템 입출력의 검증 가능성과 판단 결과의 설명 가능성에 유의한다.

- 제3자 생명, 신체, 자유, 프라이버시, 재산 등의 영향에 유의

③ 제어 가능성의 원칙

o 개발자는 AI시스템의 제어 가능성에 유의한다.

- 위험가능성 평가 위해 실험실 내부 또는 샌드박스 활용 고려, 다른 AI에 의한 감독 및 대처 가능여부 검토

113) 조성은, 이원태, 이시직. 2018. "4차 산업혁명 대응 법제 정비 연구". 방송통신정책연구 17-방통-83.

④ 안전의 원칙

o 개발자는 AI시스템이 액추에이터 등을 통해 사용자와 제3자의 생명·신체·재산에 위해를 미치는 것이 없게 배려한다.

- 국제표준 참조, 학습에 의한 프로그램의 변화 가능성 유의(사전검증노력/R&D단계 고려/이해관계자에 설계 취지 설명)

⑤ 시큐리티의 원칙

o 개발자는 AI시스템의 보안에 유의한다.

- AI 시스템의 신뢰성·강건성 유의, 사전 검증·타당성 확인, 보안중심설계(Security by Design) 설계

⑥ 프라이버시의 원칙

o 개발자는 AI시스템에 의해 사용자와 제3자의 프라이버시가 침해되지 않도록 배려한다.

- 프라이버시 영향평가 실시, 개인정보보호 중심설계(Privacy by Design)

⑦ 윤리의 원칙

o 개발자는 AI시스템 개발에 있어서 인간의 존엄과 개인의 자율을 존중한다.

- 생명윤리 관련 논의 참조, 학습데이터에 편견 등 부당 차별 금지, 국제인권법 또는 국제인도법 근거로 인간가치 훼손금지

⑧ 사용자 지원의 원칙

o 개발자는 AI시스템이 사용자를 지원해 사용자에게 선택의 기회를 적절히 제공하는 것이 가능하도록 배려한다.

- 사용자 조작 용이 노력, 적시 기능 제공, 사회적 약자의 이용성 확보, 학습에 의한 시스템 변화 관련 정보 제공

⑨ 책임의 원칙

o 개발자는 사용자를 포함한 이해관계자에 대해 책임을 완수하도록 노력한다.

- 개발한 AI 시스템에 대한 책임완수, 사회적 수용성 향성 위해 정보제공 및 의견 청취 등 이해관계자의 적극적인 피드백 강구, 개발 AI시스템에 대한 정보 공유·협력

이원태(2018)는 이상과 같이 언급되어 온 알고리즘 규제원칙을 책임성, 책무성, 투명성, 공정성으로 구분하고 다음과 같이 비교했다.[114]

<표5-1> 4가지 알고리즘 규제원칙 개념 비교

알고리즘 규제원칙	주요 내용
알고리즘 책임성 (algorithmic responsibility)	○ 알고리즘으로 인해 야기되는 사고나 손해에 관련된 법적(legal) 책임성 혹은 윤리적/도덕적(ethical/moral) 책임성으로 간주되며, 의무(duty)와 연관된 규범 ○ 또한 배상책임(liability), 유죄성(culpability)과도 유사한 맥락에서 사용되기도 함
알고리즘 책무성 (algorithmic accountability)	○ 책임성, 설명가능성(explainability), 정확성, 감사가능성(auditability), 공정성 등을 포괄하는 개념으로, 투명성이 동반될 때 증진될 수 있음
알고리즘 투명성 (algorithmic transparency)	○ 편향과 위해의 인지, 접근가능과 시정, 책무성, 설명가능성, 데이터 출처 공개, 감사가능성, 검증과 테스팅 등을 포괄하는 개념 ○ 혹은 데이터 투명성, 모델 투명성, 추론 투명성 등으로 세분화될 수 있음
알고리즘 공정성 (algorithmic fairness)	○ 앞의 개념들에 비해, 수학적으로 형식화하는 시도들이 가장 많이 이루어짐 ○ 보호집단(protected group, 예: 인종, 성별, 종교 등)에 속한 개인이나 집단이 받은 알고리즘 의사결정 결과가 (예: 취업, 대학 입학, 대출 승인 등) 다른 개인이나 집단이 받은 결과와 비교해 차이가 날 때, 이 차이가 보호 특성에서 기인하지 않아야 한다는 원칙 ○ 세분화된 공정성의 지표들 간에 상호 충돌하는 경우가 있기 때문에 one-size-fit-all 적용은 곤란함

2018년 9월, 하버드대 버크만센터는 <인공지능과 인권, 기회와 위험(Artificial Intelligence & Human Rights: Opportunities & Risks)>에 대한 보고서를 발표하였다. 이 보고서는 특히 최근 인공지능 윤리 관련 논의에서 인권적 함의가 반드시 고려되어야 한다고 강조한다. 국제인권법 규범은 인공지능이 개인과 사회에 미치는 영향을 검토하고

114) 이원태, "인공지능 알고리즘의 법규범 이슈와 정책과제", 정보인권연구소 제1차 정보인권포럼 (2018. 10. 12).

평가하고 시정할 수 있는 체제를 갖추고 있다는 것이다. 특히 인공지능의 개발 및 실행을 기업이 선도하고 있는 만큼, AI가 인권을 존중하는 방식으로 배치될 수 있도록 유엔 기업과 인권 이행지침(United Nations Guiding Principles on Business and Human Rights)[115]이 중요하다는 것을 강조한다.

이 보고서는 인권영향평가 방법을 적용하여 현재 인공지능의 구동이 프라이버시권에 가장 큰 영향을 미치는 것으로 결론을 내렸으며, 평등권, 표현의 자유, 집회결사의 자유, 노동권 등 다른 권리들도 상당히 영향을 받는 것으로 보았다. 유감스럽게도 이들 권리에 인공지능이 미치는 영향은 긍정적이기보다 갈수록 부정적인 것으로 나타났다. 인공지능이 인권에 미치는 영향은 고르지 않았다. 취약한 집단에 속해 있는 사람은 긍정적이건 부정적이건 다른 사람보다 훨씬 더 강력한 영향을 받는 것으로 드러났다.

이에 보고서는 다음과 같은 시사점을 제시하였다. 첫째, 인권영향평가 방법 등을 이용한 기업의 인권 실사는 인공지능이 인권에 미치는 부정적 영향을 줄일 수 있다. 둘째, 비국가적인 고충처리와 구제 체제가 인공지능이 불가피하게 야기하는 부정적인 영향의 일부에 대해서는 효율적으로 시정할 수 있겠지만 반드시 그런 것은 아니다. 셋째, 인공지능이 인권에 미치는 부정적 영향에 대응하는 효율적인 구제체제를 마련하는 데 있어 정부가 중요한 역할을 수행한다. 넷째, 인공지능의 분배 결과 문제를 다루는 데 있어 정부가 민주적 절차를 통해 역할 하는 것이 필수적이다.

UN 표현의 자유 특별보고관인 데이비드 케이 역시 인공지능에 의한 인권 위협을 방지하기 위한 인권영향평가를 강조하고 있다. 그는 2018년 8월 29일 UN 총회에 제출한 보고서[116]에서 인공지능 기술이 인권에 중대한 위협이 될 수 있다고 지적했다. 우선 인공지능은 그 작동이 사용자에게 숨겨져 있다는 점에서, 그리고 인공지능에 의한 정보의 개인화는 편향을 강화하고 도발적 콘텐츠나 가짜뉴스를 촉진할 수 있다는 점에서 사용자의 자기결정권과 자율성을 침해한다. 둘째, 프로파일링과 사용자 타게팅은 개인정보의 대량수집과 사용자가 제공하지 않은 민감 정보의 추정 등을 통해 프라이버시권을 위협할 수 있다. 셋째, 인공지능에 의한 온라인 콘텐츠 편집과 필터링은 표현의 자유와 차별받지

115) UN Human Rights Office of the High Commissioner. Guiding Principles on Business and Human Rights. 2011.

116) UN. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/73/348. 2018.8.29

않을 권리를 위협할 수 있다.[117] 특별보고관은 인권영향평가가 인공지능에 의한 인권적 영향을 해결하기 위한 하나의 도구가 될 수 있다고 본다. 기업과 정부는 인공지능의 개발, 구매, 이용 단계 이전에 인권영향평가를 시행할 필요가 있는데, 이는 자체적인 평가와 외부적인 감사를 포함한다.

빅데이터, 인공지능, 사물인터넷 및 알고리즘에 개인정보 보호 규범을 구체적으로 적용하기 위한 국제적 노력도 이루어지고 있다.

유럽 개인정보보호감독관(European Data Protection Supervisor, 이하 'EDPS')은 <빅데이터의 문제 해결에 관한 의견서(2015)>[118]를 통해 빅데이터 활용을 통한 사회적, 개인적 이익이 존재하는 것은 사실이나, 이와 동시에 방대한 양의 개인정보처리가 개인의 권리와 자유에 미칠 영향에 대해 우려를 표하면서 "우리는 더 이상 우리 행동에 기반을 두고 판단되지 않고, 우리가 어떻게 행동할 것 같은지 데이터가 나타내는 바에 기반을 두고 판단될 것이다(We are no longer judged on the basis of our actions, but on the basis of what all the data about us indicate our probable actions may be)."라고 경고하였다. 빅데이터 처리가 사회적으로 불공정하고 차별적인 의사결정을 야기할 수 있으며 사회문화적으로 분리하고 배제하는 기존의 스테레오타입을 강화하고 창조적 활동과 혁신에 위축을 불러올 수 있다는 것이다. EDPS는 빅데이터 사회에서 해결되어야 할 대표적인 위험요소로는 투명성 부족과 정보의 불균형 문제를 꼽았다. 빅데이터 분석의 경우 일반인들은 해당 알고리즘 및 분석틀 등을 명확히 이해하기가 쉽지 않고, 개인들의 이해도도 제각각이기 때문에 개인정보이용을 위한 동의를 받는다 해도 그 이해도가 상이하다. 빅데이터 사용으로 인해 정보처리자와 정보주체간의 정보의 불균형이 더욱 악화될 수 있다는 것이다. 빅데이터 처리는 개인정보보호의 핵심 원칙에도 악영향을 줄 수 있다. 대량의 데이터를 수집·분석하는 과정에서 정보의 오류가 있을 수 있고, 오류가 포함된 정보를 기반으로 개인의 행동이나 생활 패턴 등을 예측하여 불평등한 결과를 초래할 수 있다. 또한 개인의 모든 생활이 수집·분석되는 상황에서 개인이 철저한 익명성을 보장받지

117) EDRi. UN Special Rapporteur analyses AI's impact on human rights. 2018.11.7
118) EDPS, 2015. "Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability", Opinion 7/2015(2015.11.19), https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf.

못한다면 정보주체가 자신의 행동을 미리 검열하게 되고, 이는 자유로운 의사표현 및 행동을 제약하는 결과를 가져 온다. 온라인을 통한 토론, 집회의 자유권 행사 등 민주사회를 지속하는데 필요한 자유를 억압하는 결과도 초래할 수 있다.

이에 EDPS는 의견서에서 각 기업이 비즈니스 모델과 상관없이 원칙적으로 개인정보보호법을 준수할 것을 요구했다. 특히 개인정보보호의 책임감 있고 인간 존엄성과 인권을 존중하는 지속 가능한 빅데이터 개발을 위한 필수요소로 1) 개인정보 처리의 투명성 2) 정보주체의 개인정보 통제권 강화 3) 사용자 친화적인 개인정보보호의 설계 4) 정보처리자의 강한 책임감을 주문하고 있다.

<그림5-1> 유럽 EDPS의 빅데이터의 문제 해결에 관한 의견 (2015)

유럽연합의 29조 개인정보보호작업반(WP29) 역시 2014년 9월 16일 발표한 <사물인터넷 최근 발전에 대한 의견서>[119]에서 유사한 의견을 발표한 바 있다. 즉, 사물인터넷은 '눈에 잘 띄지 않는 방식으로 구석구석에 편재하는(pervasive) 서비스를 제공'하기 때문에 사용자들은 실제적으로 제3자의 모니터링 아래에 놓일 수 있고, 물건들 사이, 물건과 개

119) ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 14/EN WP 223. 2014.9.16

인 기기 사이, 개인과 다른 물건 사이, 그리고 물건과 후단의 시스템 사이의 데이터 흐름을 통제하기 어렵기 때문에 애초 설정된 목적을 벗어난 이용의 가능성이 크고 원 소스의 데이터를 가공하여 다양한 목적에 활용할 수 있다. 이러한 데이터의 흐름을 사용자가 인식하고 통제하기 어려운 상황에서 충분한 정보에 기반을 둔 사용자의 동의가 가능한가에 대한 문제를 제기하고 있다. 이에 따라 사용자의 동의를 얻는 고전적인 방식은 사물인터넷 환경에서 적용하기 힘들 수 있게 된다. 이와 함께, 수집된 데이터로부터 정보주체에 대한 추론 가능성, 행동 패턴의 과다한 노출과 프로파일링, 서비스 이용 시 익명성 유지의 한계 등의 위험성을 지적하고 있다.

IoT 기기의 보안은 특히 취약할 수 있는데, IoT 기기는 통상 보안 요구사항을 만족시키기에는 컴퓨팅 자원이 제한적일 수 있고, 사물인터넷 업체는 보안 이슈에 대한 경험이 없는 경우가 많으며, 많은 기기들이 저렴하고 수명이 짧아 취약점이 발견되어도 업데이트나 패치가 되지 않을 가능성이 높아지기 때문이다. 또한, 여러 기기가 연결되고 서로 다른 처리 단계에서 여러 이해관계자들이 관여할 경우, 전체적인 보안 수준을 어떻게 조정할 것인지의 문제도 발생하게 된다.

WP29는 제품 수명주기 전반에 걸쳐 사용자가 자신의 개인정보를 완벽하게 통제할 수 있어야 하며, 사물인터넷의 가입자뿐만 아니라 그 영향을 받는 모든 정보주체의 개인정보 보호가 필요하다는 입장이다. WP29는 모든 이해관계자에게 해당하는 권고로서 1) 프라이버시 영향평가의 수행, 2) 가능한 한 원본 데이터의 삭제, 3) 프라이버시 보호 중심 설계 및 기본설정 원칙의 적용, 4) 사용자 자기정보통제권 보장, 5) 정보 제공, 거부권 안내, 동의 요청의 방식은 가능한 한 사용자 친화적인 방식으로 할 것, 6) 정보주체에게 정보를 제공할 수 있는 방식으로 기기 및 애플리케이션을 설계할 것 등을 제시했다.

영국 정보보호감독관(Information Commissioner's Office, ICO)은 2016년 <빅데이터, 인공지능, 머신러닝과 개인정보보호>라는 제목의 보고서를 발간하였다.[120] ICO는 이 보고서에서 영국 및 유럽연합 법제도에서 보장하는 개인정보 보호 원칙을 개괄하면서 빅데이터, 인공지능 및 머신러닝 환경에 적용되는 정보인권 규범을 제시하고자 하였다. ICO는 우선 인공지능, 머신러닝 등 신기술의 발전을 가능하게 한 연료로서 빅데이터가 상당

120) ICO. Big data, artificial intelligence, machine learning and data protection. 2017.9.4

부분 개인정보로 구성된다는 점을 지적하였다. 그런데 빅데이터는 △알고리즘의 사용, △처리의 불투명성, △'모든 데이터'를 수집하는 경향, △데이터의 목적 외 사용(repurposing), △새 유형의 데이터 사용 등의 특성으로 개인의 권리에 미치는 영향이 지대하다. 예를 들어, 자동차보험료 온라인 견적양식, 피트니스 트래커의 달리기 통계, 지역 쇼핑센터 센서, 소셜미디어 게시물 등 방대하고 상이한 데이터세트로 구성되는데 이 데이터세트는 개인에 대한 정보를 담고 있다(ICO, 2017: 9~13)[121]. 공정성 원칙에서 보았을 때, 데이터세트에서 추출한 정보를 토대로 정보주체에 대해 결정을 내리거나 정보주체의 개인적 선호·행동·태도를 분석·예상하는 빅데이터 프로파일링(profiling) 분석은 개인에게 강압적인 효과를 미칠 수 있다. 예를 들어 어떤 맞춤광고는 인종을 토대로 사용자를 차별하는 프로파일링 처리에 기반했을 수 있으며, 특정 그룹의 저조한 상환기록을 토대로 유사한 다른 그룹의 신용한도가 낮아질 수 있다. 그럼에도 머신러닝 같은 빅데이터 분석법의 복잡성은 정보주체가 자신의 개인정보 처리에 대해 보장받아야 하는 투명성의 원칙을 오히려 위협한다(ICO, 2017: 19~28). ICO는 빅데이터가 그 구동 과정에 개인의 권리를 반영하고 결과 또한 정보주체의 기대를 벗어나지 않았을 때, 그 사회적 혜택 또한 널리 느껴질 수 있을 것이라고 지적하였다.

미국 역시 오바마 정부 시절, 백악관을 중심으로 빅데이터 등 신기술이 프라이버시에 미치는 영향을 연구하고 보고서를 발표한 바 있다. 2014년 1월, 오바마 대통령은 존 포데스타 고문에게 빅데이터와 프라이버시 문제에 대한 검토를 요청했고, 5월에 보고서인 <빅데이터: 기회를 포착하고 가치도 보존하기>가 발표되었다.[122] 이 보고서는 빅데이터가 사람의 생명, 경제, 공공서비스 효율화 등 다양한 영역에서 놀라운 기회를 제공함과 동시에, 정부와 시민 간 권력 균형에 변화를 가져올 수 있다는 점, 개인의 사적인 상세정보를 노출할 수 있다는 점, 알고리즘과 자동화된 처리가 차별적인 결과를 낳을 수 있다는 점 등에 대한 우려를 제기하였다. 이러한 혁신의 기회를 포착함과 동시에 프라이버

121) ICO(Information Commissioner's Office). 2017. "Big Data, Artificial Intelligence, Machine Learning and Data Protection". 개인정보보호위원회 번역. http://www.pipc.go.kr/cmt/not/ntc/selectBoardArticle.do?nttId=5541&bbsId=BBSMSTR_000000000118&bbsTyCode=BBST03&bbsAttrbCode=BBSA03&authFlag=Y&pageIndex=1.

122) White House Executive Office of the President. BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES. 2014.5.1

시 등 가치를 보존하기 위하여 보고서는 6가지 권고를 하고 있다.

- 소비자 프라이버시 권리장전을 개선할 것. 소비자는 빅데이터 시대에 자신의 개인정보가 어떻게 사용되는지 명확하고, 이해하기 쉽고, 합리적인 기준을 보장받을 자격이 있기 때문이다.
- 국가개인정보유출법을 통과시킬 것. 2011년 정부 사이버보안 입법 제안의 방침에 따라, 개인정보유출에 대한 단일한 국가기준을 규정해야 한다.
- 프라이버시 보호를 비 미국인에게 확대할 것. 프라이버시는 세계적인 가치로서, 연방정부가 비 미국인의 개인식별정보를 다루는 방식에 반영되어야 하기 때문이다.
- 학교 학생에 대해 수집하는 정보를 교육 목적으로만 사용할 것. 개인정보가 부적절하게 공유되거나 사용되지 않도록 학생들을 보호함으로써, 더 나은 학습 결과를 이끌어 내기 위해서이다.
- 차별을 중단하기 위한 전문 기술을 확대할 것. 연방정부는, 취약 계층에 차별적인 영향을 미치는 빅데이터 분석 관행과 결과를 알아낼 수 있는 전문 기술을 확립해야만 한다.
- 전자통신프라이버시법을 개정할 것. 읽지 않거나 일정 기간 이상 읽지 않은 채 남겨진 이메일 간에 낡은 구별을 제거하는 등, 온라인 디지털 콘텐츠의 보호 기준을 물리적인 세계에서 주어진 것과 일치하도록 보장해야 한다.

이어 2016년 5월에는 <빅데이터: 알고리즘 시스템, 기회 및 시민권> 보고서[123]가 발간되었다. 이 보고서는 신용 대출, 고용, 고등교육, 형사처벌 등에 대한 사례 연구를 검토하면서, 어떻게 빅데이터 기술이 편견을 감지하고 차별을 방지하는데 사용될 수 있는지, 또한 기술이 세심하거나 의도치 않게 차별을 영속시키고, 악화시키고, 은폐하는 방식에서 수반되는 위험을 서술하고 있다.

한편, 사물인터넷과 관련해서는 미연방거래위원회(FTC)가 2015년 1월, <사물인터넷: 연결된 세계에서의 프라이버시와 보안>이라는 보고서[124]를 발간하였다. 이 보고서에서는 사물인터넷의 확대로 인해 건강, 금융, 위치정보 등 민감 정보의 수집 증가, 빅데이터 분

123) White House Executive Office of the President. Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights. 2016.5.
124) FTC Staff Report . The Internet of Things: Privacy & Security in a Connected World. 2015.1

석을 통한 민감 정보에 대한 추정(프로파일링), 보험, 신용, 고용 등의 영역에서 특정 그룹에 대한 차별, 민감 정보에 대한 도청 위험성을 지적하며, 이러한 프라이버시 및 보안 위협은 소비자의 신뢰를 저해할 수 있음을 경고하고 있다. 앞서 WP29의 의견서와 마찬가지로 IoT 기기의 보안 위협을 지적하고 있는데, IoT 기기에 대한 무단 접근 및 개인정보 남용의 위험성뿐만 아니라, DDOS 공격이나 악성 이메일 발송 등 다른 시스템에 대한 공격 수단으로 악용될 수 있고, 자율주행차의 해킹과 같이 개인 안전을 위협할 수 있다. 이에 FTC는 △보안중심 설계(security by design), △모든 피고용인에 대해 보안에 대한 훈련, △관련 서비스 제공자들이 합리적 보안 조치를 유지하고 감독할 것, △시스템 내의 중대한 위험이 있을 경우, 몇 가지 단계에서 보안 조치를 구현하는 defence-in-depth 접근을 취할 것, △무단 접근을 제한할 수 있도록 합리적인 접근통제 조치를 취할 것, △생애 주기 전반에 걸쳐 제품에 대한 지속적인 모니터링 등을 권고하고 있다.

2018년 10월 개최된 제40회 국제개인정보보호감독기구 회의(International Conference of Data Protection and Privacy Commissioners, 이하 'ICDPPC')에서는 <인공지능 윤리 및 개인정보 보호에 대한 선언>을 발표하였다.[125] 이 선언은 인공지능이 사용자 및 사회에 상당한 혜택을 가져올 수 있다는 점을 인정하면서도, 빅데이터 처리 및 인공지능 알고리즘이 갈수록 불투명해지고 있으며 전반적인 인공지능 시스템의 개발이 대규모 개인정보 세트의 처리에 의존적이기 때문에 개인정보 보호 및 프라이버시에 영향을 미칠 수 있다는 사실을 경고하였다. 또 머신러닝 기반 인공지능 시스템을 학습시키는데 사용되는 데이터세트에서 내재적인 편향성이 발견되는 바, 이는 특정 개인 및 집단에 부당한 차별을 야기하는 의사결정을 낳을 수 있고, 특정 서비스나 내용에 대한 이용을 제한할 수 있으며, 표현 및 정보의 자유와 같은 개인의 권리에 간섭하거나 개인, 사회, 직업 생활의 어떤 측면에서 사람들을 배제하는 결과를 낳을 수 있기 때문에 광범위하고 전통적인 인권 문제가 심각한 위협을 받고 있다는 것이다. 따라서 인공지능과 머신러닝 시스템의 발전으로 촉발된 현재의 문제들을 해결하고 인권을 증진하고 보장하기 위해 국제적인 대응

125) ICDPPC. Declaration on Ethics and Data Protection in Artificial Intelligence. 40th International Conference of Data Protection and Privacy Commissioners. 2018.10.23.

과 기준을 시급히 채택할 필요가 있으며, 개인정보 감독기구들 또한 인권기구들과 협력해야 할 필요성이 커지고 있다고 보았다.

ICDPPC는 모든 인공지능 시스템의 생성, 개발 및 사용에 있어서 인간 존엄성, 차별금지 및 기본적 가치를 비롯하여 개인정보에 대한 권리 및 사생활에 대한 권리 등 인권을 완전히 존중해야 하며, 사람들이 인공지능 시스템을 통제하고 이해할 수 있도록 해결책을 마련해야 한다고 보고 가이드라인을 발표하였다. 공정성, 책임성, 투명성 및 명료성, 프라이버시 기본설정 및 프라이버시 중심 설계 등 윤리적 설계, 정보주체 권리 보장, 차별금지 등으로 요약할 수 있는 6가지 가이드라인의 내용은 다음과 같다.

ICDPPC 인공지능 윤리 및 개인정보 보호에 대한 선언 (2018)

1. 인공지능 및 머신러닝 기술은 기본적인 인권을 존중하며 설계되고 개발 및 이용되어야 하고, 다음과 같은 공정성 원칙을 따라야 한다.

a. 인공지능시스템을 본래 목적과 일치되게 사용하고 개인정보가 수집된 본래 목적에서 벗어나는 방식으로 사용되는 일이 없도록 보장함으로써 개인의 합리적인 기대 수준을 감안한다.

b. 인공지능의 사용이 개인에게 미치는 영향 뿐 아니라 집단이나 사회 일반에 미치는 집합적인 영향도 고려한다.

c. 인공지능 시스템이 인간 발전을 촉진하고 이를 방해하거나 위협하지 않는 방식으로 개발되도록 보장하고 특정한 용도에 대해서는 기술하고 한정할 필요가 있다.

2. 인공지능시스템이 보장해야 할 책임성 뿐 아니라 그것이 미치는 잠재적인 영향 및 결과에 대해 다음과 같이 지속적으로 주의하고 경계한다.

a. 인공지능 시스템에 대한 사후감사, 지속적인 모니터링 및 영향평가를 실시하고 감독 체제에 대한 정기적인 검토 등을 통해 개인, 감독기구 및 기타 제3자에 이르기까지 모든 관련 이해관계자들의 책임성을 촉진한다.

b. 행위자 및 이해관계자의 전 단계에 협력 기준 개발과 모범사례 공유 등을 포함하여 집합적, 공동의 책임을 도모한다.

c. 인공지능에 대해 상당한 수준의 정보를 갖추기 위해 인식을 제고하고 교육하고 연구하고

훈련시키고, 인공지능과 그것이 사회적으로 미칠수 있는 영향을 이해할 수 있도록 노력한다.

d. 신뢰할 수 있는 제3자(TTP) 마련이나 독립적인 윤리위원회 설립 등 관련된 모든 행위자들에 대해 가시적인 거버넌스 절차를 수립한다.

3. 인공지능 시스템의 투명성 및 명료성(intelligibility)이 향상되어야 하며, 다음과 같이 그 효과적인 구현을 목표로 한다.

a. 설명 가능한 인공지능(explainable artificial intelligence)에 대한 공공과 민간의 학술연구에 투자한다.

b. 혁신적인 통신 방식의 개발 등을 통해 투명성, 명료성, 접근가능성을 향상시키고 각각의 관련 당사자에게 필요한 다양한 수준의 투명성 및 정보를 고려한다.

c. 특히 알고리즘 투명성 및 시스템 감사가능성을 향상시켜 제공되는 정보의 의미성을 보장하는 한편, 기관의 관행을 보다 투명화한다.

d. 개인이 인공지능시스템과 직접 상호작용하거나 이들 시스템에 개인정보를 제공하여 처리되도록 할 때 언제든지 적절히 정보를 제공받을 수 있도록 보장하여 개인정보에 대한 자기결정권을 보장한다.

e. 시스템이 개인의 기대에 계속 일치하는지 확인하고 전반적으로 인간적으로 통제할 수 있도록 인공지능 시스템의 목적과 효과에 대한 적절한 정보를 제공한다.

4. 전반적인 "윤리적 설계(ethics by design)" 접근의 일환으로서, 인공지능 시스템은 다음과 같이 프라이버시기본설정(privacy by default)과 프라이버시중심설계(privacy by design) 원칙을 적용함으로써 책임감 있게 설계되고 개발되어야 한다.

a. 정보주체의 프라이버시권과 개인정보에 대한 권리를 보장하기 위해, 정보처리 수단을 결정할 때나 정보를 처리하는 순간 모두에서 개발 중인 시스템의 유형에 비례적인 기술 및 관리적 조치 및 절차를 실행한다.

b. 인공지능 프로젝트의 시작 단계 및 관련 개발의 모든 단계에서 개인과 사회에 미칠 것으로 예상되는 영향에 대해 평가하고 문서화한다.

c. 모든 인공지능 시스템의 개발과 운영의 일환으로 윤리적이고 공정한 시스템 이용과 인권 보장을 위한 요건을 구체적으로 명시한다.

5. 다음과 같이 모든 개인의 역량을 향상해야 하고, 개인의 권리 실현이 증진되어야 할 뿐 아니라, 대중 참여의 기회가 창출되어야 한다.

a. 개인정보에 대한 정보공개권, 열람권, 처리반대권, 삭제권 등 개인정보 및 사생활에 대한 권리를 적절하게 보장하고 교육 및 인식 제고 캠페인을 통해 이러한 권리들을 향상시킨다.

b. 차별금지, 표현 및 정보의 자유 등 관련된 권리를 보장한다.

c. 개인의 발전 및 의견에 영향을 미치는 기술들에 대해 반대할 권리 및 이의를 제기할수 있는 권리를 확인하고, 자동화된 처리가 개인의 권리에 상당히 영향을 미칠 때 오로지 여기에 기반하는 의사결정에 종속되지 않도록 개인의 권리를 적절히 보장하고, 부적절할 때는 그러한 의사결정에 문제를 제기할 수 있는 권리를 보장해야 한다.

d. 적응형 인터페이스 및 접근도구 등을 통해 개인 역량을 동등하게 향상시키고 대중적인 참여를 확대하기 위해 인공지능 시스템의 성능을 이용한다.

6. 인공지능에서 개인정보의 사용으로 초래될 수 있는 불법적인 편향과 차별은 다음과 같이 감소되고 완화되어야 한다.

a. 인권 및 차별금지에 대한 국제법적 규범을 준수한다.

b. 편향을 식별하고 조치하고 완화할 수 있는 기술적 방식에 대한 연구에 투자한다.

c. 자동화된 의사결정에서 사용되는 개인정보가 정확하고 최신이며 가능한한 완전하도록 보장하는 합리적인 조치를 취한다.

d. 편향과 차별을 다루는 구체적인 지침과 원칙을 정교화하고 이 문제에 대한 개인 및 이해당사자의 인식을 제고한다.

2. 신기술의 발전과 정보인권 보호를 위한 법제

1) 개요

최근 급격히 발전한 인공지능 등 신기술이 정보인권에 미치는 영향이 커져가면서, 각국에서는 이에 대응하는 법제도를 마련하기 위해 노력해왔다. 앞서 본 바와 같이 4차 산업혁명에서 주로 거론되는 빅데이터의 활용, 사물인터넷, 인공지능 등의 기술들은 프라이

버시권과 개인의 존엄성, 권리 및 자유에 영향을 미칠 수 있다. 특히 빅데이터의 활성화와 함께 비식별 처리 기술이 적용된 경우에도 정보를 결합하여 개인의 신원을 추론 하는 것이 가능해진다. 뿐만 아니라 사물인터넷 등을 활용하여 개인의 일상을 센서를 통해 수집하고 기기 간 교류가 가능한 형태로 저장하기 때문에 대부분의 정보가 개인정보라 할 수 있다. 특히 이런 정보는 개인의 건강정보, 사고방식 및 심리적 기질 등과 관련한 민감한 개인정보를 포함하고 있어 개인정보보호 강화의 필요성이 더욱 대두되고 있다.

개인정보에 대한 권리를 기본권으로 보장하고 있는 유럽연합의 경우, 일찍이 1995년부터 '자동화된 개인정보의 처리'를 규율하기 위한 목적으로 개인정보보호지침(Directive 95/46/EC)을 마련하여 적용해 왔다. 그러나 신기술의 발전으로 인해 기존 개인정보보호 법제의 개정 필요성이 증대되었고, 이에 유럽의 일반개인정보보호규정인 GDPR이 2016년 5월 EU 의회에서 승인을 얻어 2018년 5월부터 효력을 발휘하기 시작했다. GDPR의 경우 기존의 개인정보보호지침[126]이 포함하지 못하던 기술 발전으로 인한 새로운 규정들을 포함하여 개인정보보호를 강화하고자 하였으며, 디지털 단일 시장(Digital Single Market)에 대한 EU의 기본 계획에 따라 EU 가입국 내 정보의 자유이전을 보장하고자 하였다.[127]

앞서 언급한 바와 같이 EDPS는 <빅데이터의 문제 해결에 관한 의견서>에서 지속 가능한 빅데이터 개발을 위한 필수 요소로 1) 개인정보 처리의 투명성 2) 정보주체의 개인정보 통제권 강화 3) 사용자 친화적인 개인정보보호의 설계 4) 정보처리자의 강한 책임감 등 4가지를 제안하고 있다. GDPR은 이러한 문제의식을 수용하여 '잊힐 권리(right to be forgotten)', '정보이동권(right to portability)', '(알고리즘에 대해) 설명을 요구할 권리(right to explanation)' '프로파일링 거부권' 등 정보 주체의 권리를 강화하기 위한 규정들을 새롭게 포함하고 있다.

GDPR은 정보주체의 권리를 강화함과 동시에 정보처리자의 책임을 강화하기 위한 다양한 규정도 두고 마련하였다. 정보보호와 관련 전문지식을 갖춘 개인정보보호 담당관(Data Protection Officer, DPO)을 지정하게 하고, 민감한 정보를 대규모로 처리하는 기업

126) EU의 입법체계에서 Directive(지침)의 경우 EU회원국내 입법 지침의 역할을 하며 각 가입국가가 입법 재량권을 가졌다. Regulation(규정)의 경우 EU역내 일반적 적용은 물론 모든 회원국에 직접적으로 효력을 발휘하게 된다.

127) EDPS(2015) *Meeting the Challenges of Big Data: A call for transparency, user control, data protection by design and accountability* Opinion 7/2015

들의 경우 개인정보 영향평가를 실시하도록 규정하고 있다. 해킹 등 유출사고 발생 시 감독기구에 신고하고 정보주체에게 통지하도록 하고 있으며, 개발단계에서부터 개인정보 보호 문제를 고려하도록 하는 프라이버시 보호 중심설계 및 기본설정을 의무화 하고 있다. 이와 동시에 강력한 처벌 규정을 두어 기업이 개인정보보호 업무를 보다 신중히 처리하게끔 하고 있다. 또한 구글, 페이스북 등 다국적 기업의 제품이나 서비스 이용을 통해 EU 시민의 개인정보가 제3국으로 이전됨에 따라, 국가 간 적정성 평가 등을 통해 EU 시민의 개인정보가 제3국에서도 안전하게 보호될 수 있도록 하고자 하였다.

GDPR은 유럽연합 역내 뿐 아니라 온라인에서 유럽 시민의 개인정보를 처리하는 세계 여러 나라에도 적용되기 때문에 세계적으로 영향을 미치는 국제규범이 되어가고 있다[128].

개인정보보호에 관한 일반법을 갖고 있는 EU와 달리, 미국은 공공 및 민간부문을 아우르는 종합적이고 포괄적인 입법방식을 채택하고 있지 않다. 연방 차원에서는 1974년 프라이버시법(Federal Privacy Act of 1974)이 있으며, 각 주(州)에서도 프라이버시 보호 관련 법률을 갖고 있다. 민간부분에서는 연방정부의 직접규제를 통한 보호보다는 시장의 자율규제에 더욱 의존하는 경향을 가지고 있다. 즉, 원칙적으로는 민간 부문에서는 시장 자율규제에 맡기고 다만, 연방정부가 개입해야할 필요가 있는 특정 영역, 예컨대, 공공, 금융, 통신, 교육, 의료, 비디오 감시, 근로자 정보 등의 영역에 대하여 영역별로 접근하는 방식을 택하고 있다(이상경, 2017: 1).[129] 미국은 의료정보, 통신정보, 신용정보 등을 제외하고는 동의권과 관련하여 별도로 명문상 규정을 두고 있지 않기 때문에, EU 등 다른 나라에 비하여 상대적으로 빅데이터의 활용에 유리한 법적 환경을 가지고 있는 것으로 통상적인 평가를 받는다(이은우, 2018).

그러나 오바마 정부 하에서 미국 역시 빅데이터 등 변화하는 정보통신환경에 대응하여 개인정보 보호를 강화하는 움직임을 보여 왔다. 2012년 2월, 오바마 정부는 디지털 경제의 성장을 도모하면서도 동시에 소비자의 프라이버시 보호 개선을 위한 전면적 청사진

128) 구글과 페이스북은 개인정보보호법이 없는 미국에서 캘리포니아 주법에 따라 영업을 해왔으나 GDPR 발효 첫날 유럽 시민단체에 의해 피소되었다. “EU GDPR 발효…페북·구글 첫날부터 피소”, 매일경제 2018.5.27. 참조.

129) 이상경, 남정아. 미국의 개인정보 보호법제 연구. 개인정보보호위원회 연구용역. 2017.12

으로 '온라인 프라이버시의 프레임워크'[130]을 발표하였다. 이 프레임워크는 '소비자 프라이버시 권리장전(Consumer Privacy bill of Rights)'을 포함하고 있는데, 이는 1970년대 이래 사실상 '모델 프라이버시법'으로 역할을 해온 '공정 정보 관행 규약(Code of Fair Information Practices, FIPPs)'을 최근의 IT 환경에 적합하도록 대폭 보완한 것이다(이상경, 2017: 48). 소비자 프라이버시 권리장전은 △자기정보 통제권(Individual Control), △투명성(Transparency), △맥락의 존중(Respect for Context), △정보보안(Security), △접근성 및 정확성 강화(Access and Accuracy), △최소수집의 원칙(Focused Collection), △책임성 강화(Accountability) 등 7개의 원칙을 제시하고 있다.

이어 2010년 3월 26일, 미 연방거래위원회(FTC)는 인터넷 사용자들의 프라이버시 보호를 위해 <급속한 변화의 시대의 소비자 개인 정보 보호> 보고서[131]를 발간하였다. 이 보고서는 기업들과 정책 결정자를 위한 권고안을 담고 있는데, 추적 금지(Do-Not-Track) 옵션의 제공, 프라이버시 중심 설계(Privacy by Design), 데이터 브로커에 대한 규제 등의 내용을 담고 있다.

그러나 이러한 오바마 행정부의 개인정보 보호 강화 정책이 트럼프 행정부 내에서 이어질 수 있을지는 의문이다. 예를 들어, 인터넷 사용자의 개인정보 보호를 위해, 2016년 미 연방통신위원회(FCC)가 제정한 '광대역 및 기타 통신·서비스 고객의 개인정보보호에 관한 FCC 규칙'은 2017년 12월 시행 예정이었지만, 2017년 4월 트럼프 정부의 의회에서 폐기되었다.

한편, 미국의 분야별 법률 체계는 개인정보를 적절히 보호하는데 한계가 있으며, 이에 유럽연합과 같이 개인정보 보호를 위한 단일한 보호 법안이 필요하다는 주장도 제기되고 있다.[132]

일본의 경우, 변화하는 IT 환경에 대응하기 위하여 2015년 개인정보보호법을 전면 개정하였다. 개정의 취지는 통해 글로벌 경쟁을 위하여 IT·정보를 전략적으로 활용하여 혁신적 신산업·서비스의 창출과 산업 전반의 성장을 촉진하는 사회를 실현한다는 것이다.

130) White House, Consumer Data Privacy in a Netwokred World - A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. 2012.2
131) FTC, Protecting Consumer Privacy in an Era of Rapid Change. 2012.3
132) Reforming the U.S. Approach to Data Protection and Privacy. https://www.cfr.org/report/reforming-us-approach-data-protection

이번 개정으로 일본은 총리실 산하에 개인정보보호위원회를 설립하여 그간 분야별로 각 부처가 관할하던 개인정보 보호에 관한 업무를 총괄하도록 하였다. 또한, 개인정보의 보호와 활용 측면을 고려하여 '익명가공정보(匿名加工情報編)' 개념을 도입하였는데, 이는 정보주체의 동의 없이 제3자에게 제공할 수 있도록 함으로써 빅데이터 분석 등 개인에 관한 정보를 활용하여 산업진흥에 도움이 되게 하는 동시에 개인정보를 보호할 목적을 가지고 있다. 다만 익명가공정보를 취급하는 경우에는 개인정보보호위원회 규칙으로 정하는 기준에 따라 준수해야할 의무가 법에 규정되어 있다(이은우, 2018: 11).

아래에서는 정보주체의 권리로 새롭게 주목받고 있는 프로파일링 및 자동화된 처리에 대한 정보주체의 권리, 개인정보 이동권, 그리고 정보처리자에 대한 책임성 강화 조치 등에 대해 살펴보고자 한다. 이러한 제도들을 선도적으로 입법에 반영하고 있는 곳이 유럽연합이기 때문에, 유럽연합의 GDPR을 중심으로 살펴볼 것이다.

2) 프로파일링과 정보주체의 권리

프로파일링이란 개인에 대한 평가 및 개인의 업무실적, 경제상태, 위치, 건강, 선호, 신뢰성이나 행동 등을 분석 또는 예측하기 위해 이루어지는 개인정보의 자동화된 처리를 말한다.[133] 이를 위해 빅데이터 기술을 활용하여 방대한 양의 개인정보를 수집하고 이를 기반으로 특정 개인의 미래 행동과 인격(personality) 등을 파악하여 개인의 인적 특성을 자의적으로 재단하고 결정하게 된다(김종길, 2009).[134] 이때 정보 처리를 위해 활용하는 것이 자동화 알고리즘으로 이는 때론 정보 주체의 통제를 넘어, 민감 정보를 침해하기도 하며 부적절한 영역의 개인 정보는 물론 사생활 침해까지 야기 할 수 있다.

유럽연합 제29조 작업반이 <개인에 대한 자동화된 처리 및 프로파일링에 대한 가이드라인>[135]에서 자적하고 있듯이, 최근 민간과 공공 부문 할 것 없이 프로파일링과 자동화된 의사 결정이 증가하고 있다. 특히 금융, 재정, 보건의료, 조세, 보험, 마케팅, 광고 등의 분야에서 의사결정을 보조하기 위한 방법으로 프로파일링이 점점 더 자주 사용되고

133) UK ICO(2017), Feedback request – profiling and automated decision-making", 5-6p.
134) 김종길(2009). 기술위험의 사이버화와 프라이버시권. 사회이론, (35), 267
135) ARTICLE 29 DATA PROTECTION WORKING PARTY(2017), "Guidelines on Automated individual decision-making and Profiling for the purpose of Regulation", 2016/679.

있다. 제29조 작업반은 빅데이터 분석이 일상화되고 인공지능, 머신러닝 분야의 기술 발전으로 이런 식의 의사 결정이 높은 효율성을 보장하고, 인적·물적 자원을 절약할 수 있게 해 사회 및 경제 전반은 물론 개인과 조직에도 유용한 방법이 될 수 있음을 인정하고 있으나, 프로파일링 및 자동화된 의사결정은 개인의 권리 및 자유에 중대한 영향을 야기할 수 있기에 적절한 안전조치가 필요함을 강조하고 있다. 자동화된 의사 결정에 있어 의사 결정 과정의 처리가 불투명하여 각 개인이 어떤 정보가 활용되거나, 어떤 내용이 포함되는지 알 수 없는 문제가 있다.

게다가 프로파일링은 기존 고정관념이나 사회 분열을 영속화시켜 사람을 특정 범주로 국한하고 선택을 제한할 수도 있다. 개인의 지난 행적, 구매이력, 소비 패턴이나 취향 등을 프로파일링하여 제시하고 지속적으로 비슷한 것들을 노출시킬 경우 오히려 상품 및 서비스에서 선택권을 침해당할 수 있는 것이다.

유럽은 GDPR 제정 이전에도 프로파일링에 대한 규범을 수립하기 위해 노력해 왔다. 그 배경에는 개인이 방문한 웹사이트들 뿐 아니라 유럽 외부의 기업들이 쿠키 등을 활용하여 시민들이 인지하지 못하는 새 사용자를 관찰 및 추적하는 것이 가능해졌다는 문제의식이 있었기 때문이다.[136]

유럽평의회의 '프로파일링 맥락상 개인정보의 자동화된 처리에서 개인의 보호'[137]에서는 프로파일링을 통해 사용자(정보주체)는 물론 서비스 제공자, 크게는 사회·경제적 측면에서의 편익을 증진시킬 수 있다고 하더라도, 불투명하고 부정확한 프로파일링은 개인이 특정 상품이나 서비스에 접근 하는 것 자체를 차단하기 때문에 차별금지의 원칙을 위반하는 결과로 이어질 수 있음을 강조했다. 이에 따라 유럽평의회는 프로파일링 맥락상 개인정보의 수집 및 처리 조건과 관련해 다음과 같이 권고하고 있다.

> 3. 프로파일링 맥락상 개인정보의 수집 및 처리 조건
>
> A. 합법성

136) 프로파일링에 대한 규제의 유례는 유럽연합이 제정한 '유럽연합 지침 95/46'의 '정보주체의 반대할 권리' (제14조) 및 '자동화 처리될 대상의 결정' (제15조)에서 찾아 볼 수 있다.

137) Council of Europe, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2010)13 and explanatory memorandum.

3.1. 프로파일링 맥락상 개인정보의 수집 및 처리는 공정하고, 합법적이며, 균형적이고, 명시된 입법 목적에 부합해야 한다.

3.2. 프로파일링 맥락에서 개인정보의 활용은 수집하고자 하는 목적 혹은 처리하고자 하는 목적에 충분하고 적절하되 과도해선 안 된다.

3.3. 프로파일링 맥락에서 개인정보의 활용은 수집 및 처리 목적에 필수적으로 요구되는 기간 이상으로 정보주체의 식별 가능한 형태로 저장 되어선 안 된다.

3.4. 프로파일링 맥락에서 개인정보의 수집 및 활용은 다음과 같은 경우에만 실행 될 수 있다:

a. 법으로 규정되어 있는 경우 또는,

b. 법으로 허용되어 있는 경우 그리고,

— 정보 주체 혹은 그 또는 그녀가 자유롭게 구체적으로 사전 동의를 제공한 경우

— 정보 주체가 참여하는 계약의 이행을 위해 필요하거나 정보 주체가 요청한 사전 계약 조치의 이행을 위해 필요한 경우

— 공익을 위한 업무를 수행하거나 처리자에게 위임된 공적 권한을 집행하거나 제3자의 공개된 개인정보를 집행하는 경우

— 정보 주체의 기본권 및 자유에 의해 거부되는 경우를 제외하고, 프로파일이나 정보에 접근 할 수 있는 처리자나 제3자 혹은 당사자의 정당한 이익을 위한 목적을 위해 필요한 경우

— 정보 주체의 필수적인 이익을 위해 필수적인 경우

3.5. 본인 의지로 자유롭고 구체적이며 사전 동의에 의해 동의를 표현 할 수 없는 개인에 대한 프로파일링의 맥락에서 개인정보의 수집 및 처리는 법에 명시된 적절한 안전장치가 존재 할 때 정보 주체의 정당한 이익이 발생하거나 공공의 이익에 반하는 경우를 제외하고는 금지된다.

이 외에도 모든 이들이 상품이나 서비스에 대한 정보에 접근 할 수 있어야 하며, 개인정보를 제공하지 않아도 이런 정보에 충분히 접근 할 수 있어야 한다고 권고한다.

GDPR은 프로파일링을 포함한 전적으로 자동화된 개인에 대한 의사결정에 특화된 규정으로 이런 유형의 처리가 개인에 대해 잠재적인 역효과를 미칠 수 있는 경우를 일반적으로 금지하고 있다. GDPR이 정의하는 프로파일링이란 개인의 직장에서의 역량, 경제적 상황, 건강, 개인의 취향, 신뢰성, 태도 및 위치 혹은 이동경로를 예측하기 위한 자동

화된 정보처리를 의미한다.[138] 자동화된 처리 방식은 데이터의 축적, 논리적 혹은 산술적 데이터 처리 방식을 사용하여 정보의 수정, 삭제, 검색, 혹은 전파하는 경우를 의미한다. 프로파일링은 일련의 통계적 추론을 포함하는 절차로서, 대개 다양한 출처의 데이터를 이용하여 사람에 대해 예측하는 데 사용된다.

EU GDPR

제22조 (프로파일링을 포함한 개인에 대한 자동화된 의사결정)

1. 정보주체는 프로파일링 등, 본인에 관한 법적 효력을 초래하거나 이와 유사하게 본인에게 중대한 영향을 미치는 자동 처리에만 전적으로 의존하는 결정의 적용을 받지 않을 권리를 갖는다.
2. 결정이 하기 각 호에 해당하는 경우에는 제1항이 적용되지 않는다.

(a) 정보주체와 정보처리자 간에 계약을 체결 또는 이행하는데 필요한 경우

(b) 정보처리자에 적용되며, 정보주체의 권리와 자유, 정당한 이익을 보호하기 위한 적절한 조치에 대해 규정하는 유럽연합 또는 회원국 법률이 허용하는 경우

(c) 정보주체의 명시적인 동의에 기반하는 경우

3. 제2항의 (a) 및 (c)에 규정된 경우, 정보처리자는 정보주체의 권리 및 자유와 정당한 이익, 최소한 정보처리자의 인적 개입을 확보하고 본인의 관점을 피력하며 결정에 대해 이의를 제기할 수 있는 권리를 보호하는데 적합한 조치를 시행해야 한다.
4. 제2항에 규정된 결정은 제9조 (1)항에 규정된 특정 범주의 개인정보에 기반해서는 아니된다. 단, 제9조 (2)항의 (a)와 (g)가 적용되고 또한 정보주체의 권리와 자유, 정당한 이유를 보호하는 적절한 조치가 시행되는 경우는 예외로 한다.

위의 GDPR 제22조(1)의 규정은 프로파일링이 누군가에 대해 법적 효력이나 중대한 영향을 미칠 경우 전적으로 자동화된 처리에 기반을 둔 의사결정의 적용을 받지 않을 권리를 명시하고 있다. 물론 예외적인 규정도 존재하나, 해당 규정은 원칙적으로 개인에게 중대한 효과를 미치는 경우 프로파일링을 포함한 전적으로 자동화된 개인에 대한 의사결정은 금지됨을 의미한다. 또한 정보주체의 권리와 정당한 이익을 보호하기 위한 조치를

138) General Data Protection Regulation, Art. 4(4).

취할 것을 명시하며, 해당 조치는 정보를 제공받을 권리, 인적 개입을 요구할 권리 및 결정에 대해 이의를 제기할 권리(제22조3)를 포함한다.

GDPR은 프로파일링에 대해 개인정보보호의 기본원칙을 적용하는 것은 물론, 정보주체의 권리와 민감 정보 보호의 목적으로 (1) 정보를 제공받을 권리 (2) 열람권 (3) 정정권, 삭제권, 처리제한권 (4) 반대할 권리를 보장하고 있다.

○ 정보를 제공받을 권리

프로파일링이 정보주체의 권리에 미치는 위험성을 고려하면, 정보처리자는 정보주체의 손쉬운 정보 접근을 보장할 뿐 아니라 정보주체가 그 사실을 확인하게끔 하는 노력을 기울여야 한다. 정보처리자는 정보주체에게 프로파일링을 포함한 전적으로 자동화된 의사결정에 대해 정보주체에게 이런 유형의 활동에 관여되었다고 알려야 하고, 관련 로직에 대한 유의미한 정보를 제공해야 한다. 또한 처리의 중대성과 예상 결과를 설명해야 한다.

하지만 머신러닝의 증가와 복잡성으로 인해 자동화된 의사결정 절차나 프로파일링의 작동 방식을 이해하기란 쉽지 않다. 따라서 정보처리자는 전체 알고리즘에 대한 공개 혹은 사용 알고리즘의 복잡한 작동 방식에 대한 설명을 할 것이 아니라, '관련 로직에 대한 유의미한 정보'를 제공할 때 정보주체에게 간편한 방식을 찾아 이면의 근거나 그 결정에 도달한 근거 기준에 대해 설명해야 한다.

○ 열람권

정보처리자는 프로파일링을 포함하여 전적으로 자동화된 의사결정에 대해 정보주체에게 열람권을 제공해야 한다. GDPR 제15조는 정보주체에게 프로파일링을 수립하기 위해 사용된 데이터의 범주 등 프로파일링을 위해 사용된 개인정보에 대한 세부사항을 획득할 권리를 부여하고 있다. 뿐만 아니라 정보 주체는 프로파일에 대한 정보와 프로파일을 생성할 때 투입된 데이터에도 접근 할 수 있다.

○ 정정권, 삭제권, 처리제한권

프로파일링은 예측 요소와 관련되어 있어 부정확성의 위험이 존재한다. 데이터 자체의

문제 뿐 아니라 데이터를 처리하는데 이용된 알고리즘이 잘못되었을 수도 있기 때문이다. GDPR 제16조부터 제19조는 이와 관련된 정보주체의 권리를 강화하여 부정확한 정보에 기반을 둔 결과의 경우 이를 정정할 것을 요청하거나 데이터의 정확성에 문제제기를 할 수 있도록 한다.

○ 반대할 권리

정보처리자는 반대할 권리의 세부사항을 정보주체가 확실히 인식할 수 있도록 명확하게 제시해야 한다. 정보주체는 프로파일링을 포함하여 개인정보의 처리를 반대할 수 있으며, 정보주체가 이 권리를 행사하면 정보주체의 이익이나 권리를 넘어서는 의무적인 정당한 근거가 제시되지 않는 한 정보처리자는 프로파일링을 중단하고 개인정보를 삭제해야 한다.

앞서 설명한 GDPR 제22조(1)은 법적이고 중대한 효과를 미치는 프로파일링을 포함한 전적으로 자동화된 개인에 대한 의사결정에 대한 금지에 해당한다. 정보처리자는 GDPR 제22조(2)가 적용되는 세 가지 예외적인 경우에만 이러한 프로파일링을 처리 할 수 있다. 다만 이런 예외적인 경우에 해당하더라도 제22조(3)에 의해 정보주체를 보호하기 위한 추가 단계가 필요하다. 즉, 정보주체는 '최소한 정보처리자의 측에서 인적 개입을 확보할 권리, 정보주체의 관점을 표현할 권리 및 결정에 이의를 제기할 수 있는 권리'가 있다. 정보처리자는 정보주체에게 이런 권리를 행사할 수 있는 쉬운 방법을 제공해야만 한다.

프로파일링에 있어 인적 개입은 중요한 요소이다. 이런 검토는 결정내용을 변경할 수 있는 적절한 권한과 능력을 가진 누군가에 의해 시행되어야 한다. 검토자는 모든 관련 데이터에 대해 평가하고 이를 이해할 수 있어야 한다.

3) 정보독점과 정보이동권

현재 인터넷 환경은 구글, 페이스북, 애플, 아마존 등 소수 거대 IT 기업들의 플랫폼 독점이 심화되고 있는 상황이다. 이들 플랫폼 기업들은 사용자들이 제공·생성한 정보들을 보유·관리하고 있는데, 서비스 이용과 관련하여 사용자들이 제공한 정보에는 단지 사용자들의 개인정보 뿐만 아니라 서비스 이용 내역도 포함되어있는 만큼 정보주체의 권리

를 보다 적극적으로 반영할 필요가 있다. EU의 개인정보보호지침에도 이와 유사하게 정보주체의 자기정보에 대한 접근권(열람권)을 보장하고 있긴 하지만, 이 권리는 요청된 정보를 제공하면서 정보처리자가 선택한 포맷으로 제한되어 있었다.

EU GDPR은 개인정보처리자에게 제공한 자신의 개인정보를 정보주체가 체계적으로 작성되고 일반적으로 사용되며 기계 판독이 가능한 형식으로 수령을 받거나, 다른 정보처리자에게 해당 개인정보를 이전할 권리로 '정보이동권'을 신설하였다. 정보이동권은 하나의 IT환경에서 다른 IT환경으로 쉽게 자신의 개인정보를 이동, 복제, 전송할 수 있는 정보주체의 권리를 보장함으로써, 사용자의 선택권·통제권 및 소비자 권리 증진에 기여한다. 또한 개인정보에 대한 개인의 권리 및 통제의 보장을 통해 정보주체와 처리자 사이에 '재균형(re-balance)'의 기회를 제공한다. 뿐만 아니라 소규모 신규 사업자들이 이미 방대한 사용자 개인정보를 보유하고 있는 기존의 거대 IT 기업들과 경쟁할 수 있는 환경을 촉진 할 수 있다. 제29조 작업반의 가이드라인[139]에 따르면 정보이동권은 사용자의 선택, 통제, 권한을 지원하기 위한 권리로 정보 주체가 자신의 개인정보를 통제 할 수 있도록 하는 수단으로 작용한다.

GDPR

제20조 정보이동권

1. 정보주체는 정보처리자에게 제공한 본인에 관련된 개인정보를 체계적으로 작성되고 일반적으로 사용되며 기계 판독이 가능한 형식으로 수령 받을 권리가 있으며, 개인정보를 제공받은 정보처리자를 방해하지 않고 다른 정보처리자에게 해당 개인정보를 이전할 권리를 갖는다.

(a) 제6조 (1)항의 (a)나 제9조 (2)항의 (a)에 따른 동의나 제6조 (1)항의 (b)에 따른 계약을 기반으로 하는 처리의 경우

(b) 자동 수단을 통해 처리가 수행되는 경우

2. 제1항에 따른 본인의 정보이동권을 행사하는 데 있어, 기술적으로 가능한 경우, 정보주체는 해당 개인정보를 한 정보처리자에서 다른 정보처리자로 직접 이전하게 할 권리를 갖는다.

139) ARTICLE 29 DATA PROTECTION WORKING PARTY, WP 242 rev.01 Guidelines on the right todata portability, 5 April 2017, 1 – 22pp.

3. 본 조문의 제1항에 규정된 권리의 행사는 제17조를 침해해서는 아니된다. 해당 권리는 공익 상의 업무를 수행하기 위해 또는 정보처리자에게 부여된 공식 권한의 행사를 위해 필요한 처리에는 적용되지 않는다.
4. 제1항에 규정된 권리는 다른 개인의 권리와 자유를 침해하지 않아야 한다.

정보이동권의 주요 내용은 (1) 個人정보를 받을 권리 (2) 개인정보를 한 정보처리자에서 다른 정보처리자로 이전할 권리 (3) 정보처리자의 책임 (4) 정보주체의 정보이동권과 기타 다른 권리의 관계로 구성되어 있다.

○ 개인정보를 받을 권리(Aright to receive personal data)

정보주체가 정보처리자에 의해 처리된 개인정보를 받고, 그것을 다른 정보처리자에게 전송하지 않은 상태에서 추가적인 이용을 위해 개인 기기에 저장할 권리를 의미한다. 이 권리는 특히 정보이동권에서 정보를 '체계적으로 작성되고 일반적으로 사용되며 기계 판독이 가능한 형식'으로 제공하도록 함으로써 정보주체에게 개인정보 자체를 관리하고 재사용할 쉬운 방법을 제공한다. 이런 방식은 정보주체가 적극적으로 개인정보를 관리함으로써 정보주체의 권리를 강화하는 효과를 가진다.

○ 개인정보를 한 정보처리자에서 다른 정보처리자로 이전할 권리

정보주체는 자신의 정보를 획득·재사용할 수 있을 뿐만 아니라, 그 정보를 다른 서비스 제공자에게 전송할 권리를 갖는다. 이를 통해 소비자가 특정 서비스에 고착(lock-in)되는 효과를 방지함으로써 소비자의 역량을 강화하는 효과를 가진다. 뿐만 아니라 정보주체의 통제 하에서 정보처리자 사이에 안전한 방식으로 개인정보를 공유하고 혁신할 기회를 촉진하게 된다. 이는 정보처리자간 (정보주체의 동의를 전제로) 정보의 공유를 통해 서비스 및 소비자 경험을 풍부하게 할 수도 있다.

○ 정보처리자의 책임

요청을 받은 정보처리자는 정보주체나 개인정보를 이전받는 다른 업체의 정보처리에는 책임을 지지 않는다. 또한 정보처리자는 이 조항을 근거로 필요이상의 기간 동안 개

인정보를 보유할 의무를 가지는 것은 아니며, 향후 정보제공 요청을 위해 정보처리자가 애초 필요한 기간 이상으로 정보를 보유할 필요는 없다.

○ 다른 권리와의 관계

정보이동권의 행사를 위해 다른 권리 행사를 제한하진 않는다. 테이터를 이전한 후에도 해당 서비스를 계속해서 이용할 수 있다. 즉, 정보이동을 한다고 해서 원 데이터가 바로 삭제되는 것은 아니다. 또한 정보이동권 하에서 요청된 개인정보가 자신의 요청을 충분히 만족하지 못할 경우, 정보주체는 GDPR 제15조에서 규정한 접근권에 따라 개인정보를 추가로 요청할 수 있다.

4) 개인정보 보호 중심 디자인과 기본설정

개인정보 보호 중심 디자인(Privacy by design) 개념은 앤 캅부키안(Ann Cavoukian)박사가 네덜란드의 데이터 보호국과 응용과학 연구 조직과 함께 했던 작업을 통해 1995년에 제시됐다.[140] 개인정보 보호 중심 디자인은 2010년 국제 개인정보보호 감독기구 회의(ICDPPC)에서 필수 요소로 결의되었다.

앞서 언급했듯이, 미 연방거래위원회(FCC) 역시 <급속한 변화의 시대의 소비자 개인정보 보호> 보고서에서 권고 사항 중의 하나로 이 개념을 제시한 바 있다. FCC는 'Privacy by Design'은 개인정보보호를 위해서 설계 단계부터 사용자의 프라이버시를 고려해야 한다는 개념으로서, 설계 단계에서 기업이 서비스・상품 성격 및 개인정보 주기를 반영한 취급방침을 마련하고 이를 통해 기술적 보호, 최소수집, 목적에 합당한 보유기간 설정, 개인정보 파기 방침, 정보 정확성의 유지 등을 보장하도록 하는 것이라 설명하고 있다.

유럽연합기본권사무소(European Union Agency for Fundamental Rights, FRA)는 유럽 개인정보보호법 핸드북(Handbook on European data protection law)[141]에서 개인정보 보호 중심 디자인이 적용 될 때, 개인정보의 가명처리가 프라이버시를 강화할 수 있는 기술로 작동할 수 있다고 보았다. 이는 정보처리 시스템의 구조 내에 개인정보 보호가

140) https://en.wikipedia.org/wiki/Privacy_by_design#History_and_background
141) FRA(2018), Handbook on European data protection law, p132.

함께 이루어져야 함을 의미한다.

영국의 개인정보감독기구인 ICO는 <빅데이터, 인공지능, 머신러닝 및 정보보호>[142]에서 빅데이터 분석에 개인정보 보호 중심 디자인(Privacy by Design) 해결책을 포함하는 다양한 기술적·조직적 조치를 통해 개인정보를 보호 할 수 있으며, 데이터 보호와 프라이버시 권리는 빅데이터 분석이 성공적으로 개발되기 위한 토대임을 강조하고 있다.

개인정보 보호 기본설정(Privacy by default)은 제품이나 서비스를 대중에게 공개할 때에 최종사용자가 어떤 추가적인 작업을 하지 않아도 기본적인 프라이버시 (보호) 설정이 되어있어야 함을 의미한다.[143] EU GDPR 또한 정보처리자가 개인정보를 반드시 필요한 목적에 의해서만 처리할 수 있도록 하는 수단을 기본 설정으로 포함하게끔 하고 있다.[144] GDPR 제25조는 개인정보 보호 중심 디자인 및 기본설정(Privacy by Design and by Default)을 다음과 같이 규정하고 있다.

GDPR

제25조 (개인정보 보호 중심 디자인 및 설정)

1. 최신 기술과 실행 비용, 처리의 성격과 범위, 상황, 목적뿐 아니라 처리로 인해 개인의 권리와 자유에 대해 발생할 수 있는 변경 가능성과 중대성의 위험성을 참작하여, 정보처리자는 처리 수단을 결정한 시점과 처리 당시 시점에서, 데이터 최소화 등 개인정보보호의 원칙을 이행하고 본 규정의 요건을 충족하고 정보주체의 권리를 보호하기 위해, 처리에 필요한 안전조치를 포함하기 위해 고안된 가명처리 등, 적절한 기술 및 관리조치를 이행해야 한다.
2. 정보처리자는 기본설정을 통해, 처리의 개별 특정목적에 필요한 정도에 한하여 개인정보가 처리될 수 있도록 보장하기 위한 적절한 기술 및 관리조치를 이행해야 한다. 이러한 의무는 수집되는 개인정보의 양, 해당 처리의 범위, 개인정보의 보관기간 및 접근용이성에 적용된다. 특히, 이러한 조치는 개인정보가 관련 개인의 개입 없이 불특정 다수에게 열람되지 않도록 기본설정을 통해 보장한다.

142) ICO(2017), Big data, artificial intelligence, machine learning and data protection, p66.
143) https://www.ics.ie/news/what-is-privacy-by-design-a-default
144) FRA(2018), Handbook on European data protection law, p184.

3. 제42조에 근거한 공식 인증 메커니즘은 본 조항의 제1항 및 제2항에 규정된 요건의 준수를 입증하는 요소로 이용될 수 있다.

GDPR의 해당 규정은 권고사항이 아닌 '해야 한다'고 정의된 의무규정이다. 즉 정보처리의 수단을 결정한 시점과 실제로 처리 당시의 시점을 동시에 의무 이행의 시기로 규정하여 계속적인 이행의무가 있음을 명확하게 하고 있다. 또한 '최신기술'(제25조의 1항)로 규정하는 것은 개인정보를 활용하는 서비스들이 최신 기술을 활용하는 경우가 많기 때문에, 일반화된 기술이나 특정 기술이 아닌 최신기술을 고려의 요소로 하여 적절한 기술적 및 관리적 조치를 하도록 한 것이다.

이런 규정은 개인정보 처리의 성격, 범위, 구체적 상황, 목적, 처리로 인해 개인의 권리와 자유에 대해 발생할 수 있는 위험을 인정하고 위험기반 접근(risk based approach)을 구체화한 규정이라 할 수 있다. 개인정보처리의 기본원칙은 물론 정보주체의 권리를 보호하기 위한 처리에 필요한 안전조치와 가명처리 등 적절한 기술 및 관리조치를 개인정보의 수집 시작 이전 단계부터 철저히 준비하도록 한다.

특히 제25조 2항은 페이스북과 같은 소셜미디어에 적용할 수 있다. 개인정보가 관련 개인의 개입 없이 불특정 다수에게 열람되지 않도록 기본 설정을 통해 보장해야 한다. 즉, 사용자의 추가적인 설정이나 개입이 있기 전에 불특정 다수에게 노출되지 않도록 설정되어 있어야 한다. 이는 기술적인 맥락에서 개인정보 처리에 대한 이해가 부족한 상황에서 정보주체인 사용자를 돕는 것을 목적으로 한다.

5) 개인정보 영향평가

개인정보 영향평가(Data protection impact assessment)는 환경영향평가, 기술영향평가 등에서부터 유래한 개념으로 1990년대 중반부터 활용되기 시작했다. 정보처리자가 새로운 기술을 도입하고자 할 때 그 처리 유형이 개인의 권리와 자유에 높은 위험을 초래할 가능성이 있는 경우, 개인정보를 처리하기 이전에 예상되는 개인정보 처리에 대한 영향평가를 수행해야 한다. 이러한 개인정보 영향평가는 정보시스템의 개인정보 침해요인을 파악하고 개선방안을 수립하는 정책적 측면에 대한 제도이다.[145]

145) 김일환(2017) 현행 개인정보보호법체계상 감독기구 법제정비방안에 관한 연구, 미국헌법연구,

개인정보 영향평가는 문제발생 이전에 문제를 해결할 수 있는 수단이 된다. 투자가 이루어지기 이전에 프라이버시 문제를 진단하고 안전조치를 마련하여 사용자의 개인정보침해가 발생하기 이전에 시정할 수 있게 한다. 또한, 프라이버시 위협으로부터 개인정보보호를 위한 조치를 시도했음에 대한 증거를 제공하여 책임이나 부정적인 여론, 명성이 침해되는 것을 감소시켜 주기도 한다. 이는 해당 서비스를 활용하는 사용자에게도 신뢰를 줄 수 있다.

GDPR은 개인정보 영향평가를 의무적으로 수행해야 하는 경우(제35조 제3항)를 명시하고 있으며, 개인정보 영향평가를 위해 어떤 내용을 포함해야 하는지 규정하고 있다(제35조 제7항).

GDPR

제35조 개인정보보호 영향평가

1. 처리의 성격과 범위, 상황, 목적을 참작하여, 특히 신기술을 사용하는 처리 유형이 개인의 권리와 자유에 중대한 위험을 초래할 수 있는 경우, 정보처리자는 정보를 처리하기 전에 개인정보의 보호에 대한 예상되는 처리 작업에 대한 영향평가를 수행해야 한다. 한 번의 평가를 통해 유사한 중대한 위험을 초래하는 비슷한 일련의 처리 작업을 해결할 수 있다.

3. 제1항에 규정된 개인정보보호 영향평가는 특히 다음 각 호의 경우 요구되어야 한다.

(a) 프로파일링 등의 자동화 처리에 근거한, 개인에 관한 개인적 측면에 대한 체계적이고 광범위한 평가이며 해당 평가에 근거한 결정이 해당 개인에게 법적 효력을 미치거나 이와 유사하게 개인에게 중대한 영향을 미치는 경우

(b) 제9조 (1)항에 규정된 특정범주의 개인정보에 대한 대규모 처리나 제10조에 규정된 범죄 경력 및 범죄 행위에 관련된 개인정보에 대한 처리 또는

(c) 공개적으로 접근 가능한 지역에 대한 대규모의 체계적 모니터링.

7. 평가는 최소한 다음의 각 호를 포함해야 한다.

(a) 가능한 경우, 정보처리자가 추구하는 정당한 이익을 포함한 예상되는 처리 작업과 처리 목적에 대한 체계적인 설명

28(2), p. 233.

(b) 목적과 관련한 처리 작업의 필요성과 비례성에 대한 평가
(c) 제1항에 규정된 정보주체의 권리와 자유에 대한 위험의 평가
(d) 정보주체 및 기타의 관련 개인의 권리와 정당한 이익을 고려하여, 개인정보보호를 보장하고 본 규정의 준수를 입증하기 위해, 안전조치, 보안조치 및 메커니즘 등, 위험을 해결하기 위해 예상되는 조치.

또한 개인정보 처리 전에 영향평가를 실시하도록 규정하고 있어 '개인정보 보호 중심 디자인과 초기 설정'의 규정과도 일치한다. 영향평가 결과를 공개하도록 의무화하고 있진 않으나, 개인정보보호 영향평가 시 해당 처리가 고위험을 초래할 수 있는 경우, 정보처리자는 처리 이전에 감독기관에 자문을 구해야 하고 영향평가 결과를 감독기관에 제공해야 한다.

GDPR과 달리 아직 민간부문에 대해서까지 개인정보 영향평가를 의무화하고 있는 나라는 많지 않다. 공공부문에 대한 개인정보 영향평가를 법적으로 또는 정책적으로 의무화하고 있는 나라로는 미국, 캐나다, 홍콩, 영국, 호주, 뉴질랜드 등이 있다. 영국은 2007년 12월에 유럽연합 회원국 중 개인정보 영향평가제도를 도입한 최초의 국가이다. 그러나 민간영역에서는 법적으로 의무화 되어 있지 않으며, 영국 개인정보보호기구(ICO)가 권고할 수 있도록 하고 있다. 캐나다는 2002년 세계에서 최초로 공공부문에 대한 개인정보 영향평가를 의무화 하다. 이어 미국도 공공부문에 대한 개인정보 영향평가를 의무화하였다. 그러나 캐나다와 미국 두 나라 역시 민간부분에 대해서 개인정보 영향평가를 의무화하고 있지 않다(이상경, 2017).

이미 현행 개인정보보호법은 개인정보영향평가 제도를 두고 있다(제33조). 그러나 그 대상이 공공기관으로 한정되어 있고, 이 경우에도 단지 개인정보파일에 포함된 정보주체의 숫자를 기준으로 시행 여부를 규정하고 있다. 또한, 개인정보보호법은 행정안전부장관이 개인정보보호위원회의 심의, 의결을 통해서 개인정보영향평가 결과에 대하여 의견을 제시할 수 있다고 규정하고 있으나, 현재까지 개인정보보호위원회에 심의, 의결을 요청한 사례는 없다. 지금까지 개인정보영향평가가 어떻게 수행되었는지 체계적으로 공개되어 있지도 않다. 즉, 아직은 개인정보영향평가가 내실 있게 운영되고 있지 못한 상황이다.

이를 개선하기 위해서는 첫째, 개인정보 영향평가를 민간 영역으로 확대해야 하며, 둘

째, 단지 개인정보파일에 포함된 정보주체의 규모가 아니라 정보주체에 심각한 영향을 줄 수 있는 모든 시스템을 대상으로 해야 한다. 셋째, 개인정보보호위원회가 영향평가에 대해 사전에 자문하고 시행 결과를 검토하는 등 감독기능을 강화할 필요가 있다.

6) 개인정보보호담당관

개인정보 보호 담당관(Data Protection Officer, DPO)은 조직 내에서 데이터 보호 문제의 주요 접점을 제공하는 자로, 기존 개인정보보호 지침에서는 의무사항이 아니었지만 GDPR 하에서는 공공기관, 대규모의 체계적인 모니터링에 종사하는 조직 또는 민감한 데이터의 대규모 처리에 종사하는 조직의 경우에 DPO를 의무적으로 지정해야 한다.

GDPR은 개인정보보호 담당관이 개인정보 보호와 관련한 모든 문제에 시의 적절하게 관여하도록 보장해야 한다는 규정을 두고 있으며 개인정보보호와 관련된 모든 사안에서 최대한 이른 시점부터 DPO가 관여하는 것이 중요하다고 한다. 뿐만 아니라 DPO를 조직 내의 논의 파트너로 대하고 정보처리를 담당하는 관련 작업반의 일원이 되도록 하는 것이 중요하다고 규정하고 있다. 이런 권한은 개인정보보호 담당관이 감사 역할을 하는 것과는 다른 성격임을 의미한다.

GDPR

제4절 개인정보보호 담당관

제37조 개인정보보호 담당관의 지정

1. 다음의 각 호의 경우 정보처리자와 수탁처리자는 개인정보보호 담당관을 지정해야 한다.

(a) 법원이 사법능력을 행사하는 경우를 제외하며, 공공기관 또는 기구에 의해 처리가 수행되는 경우

(b) 정보처리자나 수탁처리자의 핵심 활동이 처리의 성격과 범위 및/또는 목적 상 정보주체에 대한 정기적이고 체계적인 대규모의 모니터링을 요하는 처리 작업들로 구성되는 경우

(c) 정보처리자 또는 수탁처리자의 핵심 활동이 제9조에 따른 특정범주의 개인정보와 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보에 대한 대규모의 처리로 구성되는 되는 경우

2. 개인정보보호 담당관을 각 사업장에서 쉽게 접근할 수 있는 경우, 사업체 집단은 한 명의

개인정보보호 담당관을 임명할 수 있다.

3. 정보처리자 또는 수탁처리자가 공공기관이나 기구인 경우, 조직의 구조나 규모를 고려하여, 이러한 다수의 기관이나 기구를 위해 한 명의 개인정보보호 담당관이 지정될 수 있다.
4. 제1항에 규정되지 않은 경우, 정보처리자 또는 수탁처리자 또는 정보처리자나 수탁처리자의 범주를 대변하는 조합 및 기타 기구는, 유럽연합 또는 회원국 법률에서 요구하는 경우, 개인정보보호 담당관을 지정할 수 있거나 지정해야 한다. 개인정보보호 담당관은 정보처리 자 또는 수탁처리자 대변하는 해당 조합 및 기타 기구를 대행할 수 있다.
5. 개인정보보호 담당관은 직무상의 자질, 특히 개인정보보호법과 실무에 대한 전문가적 지식과 제39조에 규정된 업무를 수행할 수 있는 능력에 근거하여 지정된다.
6. 개인정보보호 담당관은 정보처리자 또는 수탁처리자의 직원일 수 있으며, 서비스계약에 근거하여 업무를 수행할 수 있다.
7. 정보처리자 또는 수탁처리자는 개인정보보호 담당관의 상세 연락처를 발표하며 이를 관련 감독기관에 통보한다.

DPO는 GDPR에 규정된 의무를 수행해야 한다. 유럽연합 또는 회원국의 개인정보보호 조문과 개인정보보호와 관련된 정보처리자 또는 수탁처리자의 정책의 준수에 관해 모니터링을 하며, 책임 배정, 인식 제고, 처리 작업 등에 관련된 직원 교육과 관련 감사 등을 포함하며 GDPR 제35조에 따라 개인정보보호 영향평가에 관한 자문을 제공하고 평가의 이행을 감시하기도 한다. 또한 GDPR이 내부적으로 준수되고 있는지 감독하는 것을 지원할 의무(제39조(1)(b), 전문 97)를 가진다. DPO는 감독기관과의 협력 및 연락책으로서의 역할도 한다. DPO는 사전협의를 포함해 처리와 관련한 감독기관의 연락책으로서 활동해야 하며 기타 관련 사안에 대해 필요한 경우 논의해야 한다.

3. 지능형 감시에 대한 법제적 대응

정보통신기술의 발전과 인터넷의 전 세계적 확산은 범죄 수사 분야에도 많은 변화를 가져왔다. 해킹이나 바이러스의 유포와 같이 기존에는 없었던 사이버 범죄가 등장했고, 폭력이나 사기와 같은 전통적인 범죄도 인터넷을 매개로 이루어졌다. 범죄 행위가 이루어지는 곳과 피해가 발생하는 지역이 다르고, 여러 국가에 걸쳐 영향을 미치기도 하며,

공격자의 추적이 어렵고 증거가 조작되거나 인멸되기 쉽다는 특성 때문에 최근 십여 년간 사이버범죄에 대응하기 위한 새로운 수사기법과 국가 간의 공조도 발전해왔다. 동시에 정보통신기술, 특히 빅데이터나 생체인식과 같은 신기술의 발전은 정보수사기관의 역량을 강화하기 때문에 이에 따른 권한 남용과 시민 감시와 같은 새로운 인권 침해 문제를 야기하기도 한다. 지난 2013년 스노든의 폭로로 드러난 미 국가안보국(NSA)의 인터넷 대량감시가 대표적인 사례이다.

정보수사기관의 경우 그 특수성 때문에 일반적인 개인정보 보호원칙의 적용이 배제되는 경우가 많다. 그러나 일정한 예외를 인정하더라도 민주사회의 기본 원리 상 정보수사기관과 같은 권력 기관에 대해서는 권한 남용을 방지하기 위한 독립적인 감독 메커니즘이 마련될 필요가 있다. 신기술의 발전에 따라 정보수사기관의 실질적인 권력이 변화할 수 있는 만큼, 이에 대한 감독 메커니즘도 이에 대응할 필요가 있다.

1) 유엔의 프라이버시 결의안

2013년 6월, 미국 정보기관의 전요원인 에드워드 스노든이 미국 정보기관들이 구글등 미국 통신·인터넷 기업들의 협조를 받아 전 세계 사용자의 개인정보 및 통신정보를 수집해 왔다는 사실을 폭로하였다. 그 이후 국제적으로 지능형 대량 감시에 대한 많은 사회적 토론이 촉발되었고, 최근 유엔 규범은 디지털 시대 프라이버시권을 국제인권법에서 보장하는 수준으로 보호하기 위해 각국의 조치를 촉구하고 있다. 대표적으로 2013년 12월 유엔 총회는 통신감시와 관련된 절차와 관행, 법률을 재검토할 것과 독립적이고 효율적인 감독 체계 등 국가 감시를 통제하는 조치를 각국 정부에 권고하는 <디지털시대 프라이버시권 결의안>[146]을 채택하였다.

유엔총회 디지털시대 프라이버시권 결의안(2013년 12월 18일)

4. 모든 국가들에 다음을 요청한다.

(a) 디지털 통신의 맥락에서 프라이버시권을 존중하고 보호할 것

(b) 관련 국내법이 국제인권법상 의무를 준수하도록 하는 등, 권리 침해를 종식시키고 그 침

146) Resolution adopted by the General Assembly on 18 December 2013: 68/167. The right to privacy in the digital age.

해를 방지하는 조건을 창출하기 위한 조치를 취할 것
(c) 국제인권법상 모든 의무를 완전하고 효율적으로 이행함으로써 프라이버시권을 보장하기 위한 목적에서, 대량 감시, 감청 및 수집을 비롯한 각국 통신감시, 감청, 개인정보 수집과 관련한 절차와 관행, 법률을 재검토할 것.
(d) 국가의 통신 감시, 감청 및 개인정보 수집에 대해 적절한 투명성과 책임성을 보장하는 독립적이고 효율적인 국내 감독 체계를 설립하거나 운영할 것

이러한 유엔 총회 결의에 따라 보고를 요청받은 유엔 인권최고대표는 그 이듬해인 2014년 펴낸 <디지털시대 프라이버시권 보고서>에서 디지털 시대 커뮤니케이션 기술은 정부, 기업, 개인이 감시, 도청, 개인정보 수집을 실행할 수 있는 능력 또한 향상시켜 왔다고 우려하였다. 이제 국가는 동시적, 침투적, 표적적이거나 광범위한 감시를 수행할 수 있는 능력을 그 어느 때보다 막대하게 보유하게 되었으며, 지구적 정치경제사회가 깊이 의존하고 있는 기술 플랫폼은 대량 감시에 취약할 뿐 아니라 이를 촉진하는 환경이다. 반면 많은 국가에서 프라이버시 보호를 위한 입법과 집행이 제대로 이루어지지 않고 있고 무엇보다 감독이 효과가 없었다는 점에 대해 우려를 나타냈다. 이에 유엔 인권최고대표는 국제 인권법에 반하는 전자감시 정책 및 수단들에 대한 모든 평가들은 변화하는 문제의 속성을 고려해서 반드시 다듬어져야 한다는 점, 그리고 효과적이고 독립적인 감독을 위한 조치들이 취해져야 함을 권고했다.[147]

유엔은 2015년과 2017년에 <디지털 시대의 프라이버시권에 대한 결의안>을 통해 프라이버시권 등 오프라인에서 사람들이 가진 것과 동일한 권리가 온라인에서도 보호되어야 한다고 선언하였다. 특히 2017년 결의안[148]은 국가 뿐 아니라 기업이 자의적이고 불법적인 방식으로 프라이버시권에 간섭하는 것에 대하여 통제하는 조치를 취하고, 시민들의 디지털 리터러시와 기술 역량을 함양하기 위해 교육 기회를 장려할 것을 각국에 촉구하였다. 개인의 자유롭고, 명시적이고, 충분한 설명에 따른 동의 없이 개인정보가 판매되고, 다목적으로 재판매되며, 타 기업에 공유되는 피해에 대하여 우려를 표하고, 이에 대한 규

147) The Office of the United Nations High Commissioner for Human Rights. 2014. “The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights”, A/HRC/27/37, 30 June 2014.
148) The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 27 February to 24 March 2017.

제, 예방 조치 및 구제대책을 취할 것을 각국에 요구하기도 하였다.

유엔 인권이사회 디지털시대 프라이버시권 결의안(2017년 3월 22일)

5. 모든 국가들에 다음을 요청한다.

(a) 디지털 통신의 맥락을 포함하여, 프라이버시권을 존중하고 보호할 것.

(b) 관련 국가 입법이 국제인권법상 의무를 준수하는 등 프라이버시권 침해를 종결시키고 침해 방지 여건을 창출하는 조치를 취할 것.

(c) 국제인권법상 의무를 완전하고 효과적으로 이행하여 프라이버시권을 옹호하기 위하여, 대량의 감시·감청·수집 등 통신 감시, 감청, 개인정보 수집에 관한 절차, 관행, 입법을 검토할 것.

(d) 국가의 통신 감시, 감청, 개인정보 수집에 대해 투명성과 책임성을 적절하게 보장하기 위한, 독립적이고 효과적이며 적정하게 자원이 할당되고 불편부당한 사법적, 행정적, 혹은 의회의 국내 감독 체제를 수립하거나 유지할 것.

(e) 불법적이거나 자의적인 감시에 의해 프라이버시권이 침해된 개인들에게 국제인권 의무에 상응하는 효과적인 구제대책을 제공할 것.

(f) 효과적인 제재 및 구제대책을 포함하는 적정한 규제를 개발·유지·시행하여, 개인·정부·기업·민간 단체들의 불법적이거나 자의적인 개인정보 수집·처리·보관·이용으로 인한 프라이버시권 침해와 유린으로부터 개인을 보호할 것.

(g) 이러한 측면에서 모든 개인, 특히 여성은 물론, 아동, 취약 계층과 소수자들에 영향을 미칠 수 있는 디지털시대 프라이버시 침해와 유린에 대해, 예방 조치와 구제대책을 추가적으로 개발하고 유지할 것.

(h) 자신의 프라이버시를 효과적으로 보호하는 데 필요한 디지털 리터러시와 기술적인 능력을 함양하기 위해 모든 이에게 양질의 교육 및 평생 교육 기회를 장려할 것.

(i) 기업들에 대하여 프라이버시권을 자의적이고 불법적인 방식으로 간섭하는 조치를 취하도록 요구하는 것을 삼갈 것.

(j) 국가 기관이 사적인 사용자 데이터나 정보에 대한 제공을 요청할 때 기업들이 적정하고 자발적인 투명성 조치를 도입할 수 있게끔 적절한 조치를 고려할 것.

(k) 개인의 자유롭고, 명시적이고, 충분한 설명에 따른 동의 없이 개인정보가 판매되고, 다목적으로 재판매되며 타기업에 공유되는 피해에 대응하는 규제, 예방 조치와 구제대책을 개발하고 유지할 것.

유엔 인권이사회는 디지털 시대 프라이버시권에 대한 보다 체계적인 대응을 위해, 2015년 7월 13일 조셉 카나타치를 프라이버시 특별보고관을 임명하였다. 그는 2017년 3월에 제출한 보고서[149]에서 최근의 감시법을 비판하며 각국 정부에 프라이버시권을 디지털 시대 보편 권리로 보장할 것을 요구하였다. 즉, 프라이버시권은 누구나 향유할 자격이 있으므로 자국 국민들뿐만 아니라 외국인의 프라이버시권도 보편적으로 존중되도록 해야 한다는 것이다. 이 보고서에서 그는 사이버 공간의 감시를 규제하는 세계적인 수준의 법적 수단이 필요하다고 제안하기도 하였다.

2) 통신 분야의 개인정보보호

유럽 차원에서 마련된 개인정보 보호규범을 그 특정한 부문으로서 통신 분야에 적용하는 규범이 수립되어 왔다(FRA, 2018: 326~330)[150]. 특히 통신네트워크는 그 위에서 수행된 통신의 청취와 조사에 대한 기술적 가능성이 있기 때문에, 통신서비스 사용자의 권리에 대한 부당한 간섭에 대처하기 위하여 특별한 정보보호규칙이 필요하다.

우선 유럽평의회는 1995년 특히 전화서비스에 대하여 전기통신분야에서의 정보보호에 관한 특별규정[151]을 발표하였다. 이 권고에 따르면, 전기통신분야에서 개인정보의 수집 및 처리의 목적은 사용자를 네트워크에 접속시키는 것, 개별적 전기통신서비스를 이용할 수 있게 하는 것, 요금청구, 확인, 최적의 기술적 작동의 보장과 네트워크서비스의 발전으로 제한되어야 한다. 이러한 전기통신분야 정보보호지침을 보완하고 특화하기 위하여 2002년 프라이버시 및 전자통신에 관한 지침, 이른바 'e-Privacy지침'이 채택되어 2009년 개정되었다. 이 지침의 적용은 공공전자네트워크에서의 통신서비스로 제한되는데, 여기서 보호되는 전자통신의 비밀성은 통신의 내용에 관계될 뿐 아니라, 누구와 언제 그리고 얼

149) Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. A/HRC/34/60. 2017.2.24

150) FRA(European Union Agency for Fundamental Rights and Council of Europe). 2018. "Handbook on European data protection law: 2018 edition".

151) Recommendation Rec(95)4 to member states on the protection of personal data in the area of telecommunication services, with particular reference to telephone services

마 동안 통신을 하였는지에 대한 트래픽 데이터(메타 데이터)와, 정보가 어디로부터 연락되었는지와 같은 위치정보와도 관계된다.

e-Privacy 지침 제15조에 따르면, 범죄수사 등 다른 목적을 위해 전자네트워크 통신 정보에 대해 접근하기 위해서는, 유럽 인권협약 제8조 제2항에서 규정되고 기본권헌장 제8조와 제52조에 의해 확인된 개인정보보호권에 대하여 간섭하는 것을 정당화하기 위한 요건을 충족하여야 한다. 특히 전자통신에서 공공기관에 의한 간섭은 중요한 문제이다. 감청과 같은 통신 감시 또는 간섭 수단은 법률에 의해 규정되어 있고, 그것이 국가안보, 공공의 안전, 국가의 금전적 이익 또는 범죄의 진압을 보호하고, 또는 정보주체나 타인들의 권리와 자유를 보호하기 위하여 민주사회에서 필요한 조치를 형성하는 경우에만 허용될 수 있다.

2017년 1월, 유럽 집행위원회는 e-Privacy 지침을 대체하는 새로운 e-Privacy 규정안을 채택하였다[152]. GDPR이 유럽연합 기본권헌장 제8조(개인정보보호)를 주로 규율하는 데 비해, e-Privacy 규정은 기본권헌장 제7조(사생활존중권)를 유럽연합 법체계에 통합하는 데 그 목적이 있다. 이 규정은 이전 지침의 규정을 신기술 및 시장 현실에 적용하고 포괄적이며 GDPR과 일관된 체제를 수립하고자 한다. 그런 점에서 e-Privacy 규정은 GDPR의 특별법으로서, 개인정보를 구성하는 전자통신 데이터에 그 원칙을 적용한다. 새 규정은 개인정보가 아닐 수도 있는 통신 내용 및 메타데이터를 포함하여 모든 '전자통신 데이터'의 처리를 관장한다. GDPR 집행 체제가 이 규정에도 적용된다.

유럽에서는 전자통신 데이터가 그 본래 목적인 네트워크 관리, 요금청구 등 통신사업자의 정당한 이익을 넘어서는 목적으로 보관 및 이용되는 데 대한 논란이 커지고 있다. 국가기관은 범죄수사 등 공익적 효용성을 주장하며 전자통신 데이터의 장기간 보관을 요구해 왔고, 기업들은 사용자 프로파일링 및 인공지능의 머신러닝을 위한 빅데이터 기반으로서 통신데이터에 주목해 왔다. 그러나 전자통신 데이터의 보관 및 이용은 인터넷 표현의 자유는 물론 개인정보에 대한 권리 등 사용자의 권리에 밀접한 영향을 끼친다. 최근 e-Privacy 규정의 제정을 앞두고 유럽 시민사회는 △전송중이거나 보관된 통신 비밀의 보호 △보안을 약화시키는 예외조항 반대 △동의 없는 이용 반대 △프라이버시 중심

152) e-Privacy 규정은 본래 2018년 5월 25을 GDPR 시행에 맞추어 채택될 예정이었으나 유럽의회 및 이사회의 합의에 따라 결정될 예정이다.

설계(Privacy by Design) 및 프라이버시 기본설정(Privacy by Defualt)을 수용할 것을 요구하였다[153].

한편, 유럽연합에서는 2006년 일명 데이터보관지침(directive 2006/24/EC)이 제정된 후 그 국내법 이행을 둘러싸고 10여 년간 치열한 논쟁이 이루어졌다(민영성 외, 2016)[154]. 이 지침은 공중 통신망 운영자(통신사업자) 또는 공중 전자적 통신서비스제공자(정보통신서비스제공자)에 의해서 생성되거나 처리되는 특정 데이터의 보관과 관련하여 이들의 책임을 회원국이 규정하도록 하여 테러와 같은 중대한 범죄의 예방, 확인 및 소추의 목적으로 데이터를 사용할 수 있도록 확보하는 데 그 목적이 있다(지침 제1조)[155]. 공중 통신망 운영자 및 공중 전자적 통신서비스 제공자는 자신의 통신서비스를 제공하는 과정에서 생성되거나 처리되는 통신 데이터를 최소 6개월에서 최대 2년까지 저장하여 보관해야 한다(제3조 및 제6조). 제공자가 보관해야 할 통신정보는 트래픽데이터, 위치데이터, 가입자 및 사용자를 특정하는 데 필요한 모든 관련 데이터로서(제2조 제1항) 6가지 범주에 달한다.

오스트리아에서는 데이터보관지침을 국내법으로 이행한 관련 규정들에 대하여 헌법소원이 제기되었다. 오스트리아 캐른트너(Kärntner) 주정부, 1만 명이 넘는 일반 시민 등 청구인들은 헌법소원청구서에서 범죄의 혐의와 상관없이 예방적으로 대량 데이터를 보관하는 것은 기본권을 침해한다고 주장하였다. 특히 보관된 데이터가 당사자와 관련된 개인정보를 노출시키는 바, 사용자의 통신 행태나 행동프로파일이 작성될 수 있고 이를 통하여 통신의 내용도 추론할 수 있다고 하였다. 오스트리아 헌법재판소는 기본적으로 청구인들의 주장을 수용하면서 유럽사법재판소에 해당 지침이 EU 기본권헌장 제7조(사생활존중권)와 제8조(개인정보보호) 그리고 제11조(의사표현 및 정보의 자유)와 일치하는지 선결을 요청하였다.

---

153) EDRi(European Digital Rights), "Dear MEPs: We need you to protect our privacy online!", 2017. 10. 5, https://edri.org/dear-meps-we-need-you-to-protect-our-privacy-online/.

154) 민영성·박희영. 2016. “통신정보보관제도의 정당성: 유럽사법재판소 및 오스트리아 헌법재판소 판결의 관점에서", 법학논문집 제40집 제1호(중앙대학교 법학연구원), pp. 449~473.

155) 유럽연합 데이터보관지침과 이를 국내법으로 이행한 유럽연합 회원국의 규정들의 핵심적인 특징은 범죄혐의와는 상관없이 국민의 모든 통신데이터를 국가기관이 미리 저장하여 보관한다는 점에 있다. 한국의 통신비밀보호법 시행령 상 통신사실 확인 자료의 보관 제도(동법 시행령 제41조 제2항)는 범죄 혐의와 상관없이 사전에 저장되어 보관되고 있으므로 데이터보관에 해당한다. 민영성 외(2016: 468~469) 참조.

유럽사법재판소는 2014년 4월 8일 이 지침은 유럽연합 기본권헌장 제7조(사생활존중권)와 제8조(개인정보보호권)를 위반하여 처음부터 무효라고 판결하였다. 첫째, 지침은 데이터보관에 관한 규정만을 포함하고 보관된 데이터의 보호와 접근에 관한 절차적 요건이 부재하다. 보관된 데이터에 대한 접근이 감독기관이나 독립 관청으로 통제받고 있지 않으며, 직업상 비밀유지를 위한 면제 조항도 없다. 둘째, 지침은 데이터 저장 및 접근에 대한 실질적 제한이 부재하다. 광범위한 데이터보관은 거의 모든 유럽인들의 기본권을 침해하기 때문에 절대적으로 필수적인 경우로만 제한되어야 하며, 만일 사람들이 직접적이든 간접적이든 적어도 중대한 범죄와 연관되어 있지 않다면, 이들 데이터의 저장은 적정하지 않다. 효과적인 범죄 대응의 차원에서도 광범위한 저장은 필요하지 않다. 중대범죄의 정의나 보관 기간의 정의가 광범위한 점도 비판받았다.

유럽사법재판소는 이 사건 이후로도 다른 사건에 대한 결정에서 대량 통신 데이터의 의무적인 보관이 유럽 기본권 헌장을 침해한다는 취지를 계속 확인하였다[156]. 유럽 시민사회는 최근 e-Privacy 지침의 제정에 있어서도 유럽사법재판소 결정의 취지를 반영할 것을 촉구하고 있다[157].

3) 정보수사기관의 감시와 개인정보보호

컴퓨터를 이용한 개인정보처리가 늘어난 1980년대 중반부터 유럽에서는 유럽평의회[158] 차원에서 경찰의 개인정보 처리에 대한 원칙을 수립해 왔다. 특히 최근 빅데이터를 이용한 범죄 탐지 및 수사기법이 발달하면서 유럽연합은 2018년 5월 GDPR과 동시에 경찰지침을 발효시켜 범죄수사에 있어서 개인정보보호를 강화하였다.

한편 주요국가 정보기관의 인터넷 대량 감시 사실이 폭로된 후 유럽에서는 개인정보 보호 적정성 평가기준 등 개인정보 보호에 대한 규범이 강화되었다. 유럽인권재판소 또한 정보기관의 감시로부터 정보인권을 보호하기 위한 규범을

156) Digital Rights Ireland - joined cases 293/12 and 594/12 and Tele2-Watson, joined cases C-203/15 and C-698/15.

157) EDRi, "ePrivacy: Civil society letter calls to ensure privacy and reject data retention", 2018.4.24, https://edri.org/eprivacy-civil-society-letter-calls-to-ensure-privacy-and-reject-data-retention/.

158) 유럽평의회와 유럽연합의 관계를 요약하면 다음과 같다. 유럽평의회 47개국 중 과반이 넘는 28개국이 유럽연합 소속이고 유럽경제지역(EEA) 국가인 노르웨이, 아이슬란드, 리히텐슈타인 등 3개국은 비EU회원국이지만 개인정보보호지침 등 유럽연합법의 적용을 받는다.

강화해 가고 있다.

(1) 범죄수사와 개인정보보호

범죄수사 영역에서 개인정보 보호와 관련한 유럽평의회의 대표적인 규범은 1987년 제정된 이른바 '경찰 권고'(Recommendation (87)15)이다. 유럽평의회 경찰 권고는, 당사자에게 중대한 영향을 미치는 경찰기관의 개인정보 처리에 대해 상세한 개인정보 보호 규범을 제시하기 위해 마련되었으며 기술적 감시 또는 다른 자동화된 수단에 의한 정보의 수집에 대한 원칙 등 주요 개인정보 보호 원칙을 제시하였다.

권고는 ① 통제 및 고지(Control and notification), ② 정보 수집(Collection of data), ③ 정보 보관(Storage of data), ④ 경찰의 정보 사용(Use of data by the police), ⑤ 정보 전달(Communication of data), ⑥ 공개성, 경찰파일에 대한 접근권, 정정권 및 이의제기권(Publicity, right of access to police files, right of rectification and right of appeal), ⑦ 보관 기간 및 정보 갱신(Length of storage and updating of data) ⑧ 정보 보안(Data security) 등 8가지 분야에 대한 원칙을 담고 있다. 경찰기관의 개인정보 수집에 대하여 실질적인 위험 방지 또는 특정 범죄의 기소를 위해 필요한 경우로 제한하고 있으며, 제한 없는 무차별적인 개인정보 수집을 허용하지 않는다. 추가적인 정보 수집은 구체적인 법률에 근거하여야 한다. 민감 정보의 처리는 특정 수사에서 절대적으로 필요한 것으로 제한되어야 한다. 정보주체가 알지 못한 사이에 개인정보가 수집되는 경우, 그에 대한 공개가 더 이상 수사를 방해하지 않는 한 곧바로 정보주체에게 정보수집 사실을 통지해야 한다. 기술적 감시 또는 다른 자동화된 수단에 의한 정보의 수집 또한 특정한 법규정에 근거하여야 한다(FRA, 2018: 277).

권고는 개인정보를 저장할 때 행정정보와 경찰정보 간에 구별하고, 용의자, 유죄판결을 받은 자, 피해자, 증인 등 서로 다른 유형의 정보주체 간에 구별하고, 확실한 사실로 간주되는 정보와 의심 또는 추측에 근거한 정보 간에 명확히 구별해야 한다고 하였다. 특히 경찰정보가 사용되는 목적은 엄격하게 제한되어야 하며, 이는 경찰정보의 제3자 제공에서 매우 중요한 원칙이다. 경찰에 의한 정보처리는 국내 개인정보보호법의 준수를 보장하기 위하여 독립적 감독을 받아야 한다. 정보주체들은 자신의 개인정보에 대한 접근권을 보장받는다. 효과적인 경찰수사 및 형사처벌을 위하여 정보주체들의 접근권이 제

한되는 경우, 정보주체는 국내법에 의해 개인정보보호감독기관 또는 다른 독립적 기구에 이의를 제기할 권리를 가져야 한다(FRA, 2018: 278~279).

유럽평의회가 경찰 권고로 개인정보보호 규범을 수립한 데 비하여 유럽연합의 경우 개인정보보호지침인 1995년 95/46/EC 지침이 경찰 및 형사사법분야에 적용되지 않았기에 이 분야 개인정보보호규범이 모호한 상태라고 평가받았다. 그러나 2016년 이른바 경찰 지침(일명 police directive)[159]이 의결되어 GDPR과 함께 2018년 5월 발효되었다. 경찰 지침은 범죄 예방·수사·탐지·기소, 형사처벌 집행 및 공공안전 보호·위험 방지 등 형사 사법 문제를 소관하는 기관이 해당 목적으로 개인정보를 수집하고 처리할 때, 개인정보를 보호하는 것을 목적으로 한다[160].

경찰기관에 의해 국내법 또는 유럽연합 법에 따라 합법적이고 필수적이며 비례적으로 수집된 개인정보의 경우 법집행 목적을 위해 처리될 수 있다. 이 정보가 다른 목적에 사용될 때는 GDPR이 적용된다. 개인정보 보관은 필수적인 기한 이상으로 보관되어서는 안 되며, 기한 내 삭제되거나 이에 대한 정기 검사가 이루어져야 한다. 보관된 개인정보는 소관 기관이 수집, 전송, 이용 목적 하에서 처리하는 경우에만 사용할 수 있다. 개인정보를 공유할 때는 로그기록 및 서면 보관이 의무화된다(FRA, 2018: 282~291).

지침은 형사사법 분야의 특수성을 고려하면서도 GDPR의 원칙과 정의를 상당부분 채택하고 있으며, 이로 인하여 형사 사법기관 또한 GDPR에 규정된 독립적인 감독기구[161]에 의해 감독을 받고, 개인정보보호담당관(Data Protection Officers)을 지정하고, 개인정보 영향평가 또한 받아야 할 의무가 새롭게 도입되었다. 경찰 지침은 정보주체가 자신의 개인정보가 처리되는 데 대한 정보를 제공받고 열람, 정정, 삭제 및 처리제한권을 행사할 수 있도록 원칙적으로 보장하였다. 다만 범죄수사 등의 이유로 정보주체가 그 권리 행사

159) Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

160) 지침은 회원국 형사사법기관들이 국내적으로 처리하는 개인정보는 물론, 다른 회원국 형사사법기관들이나 제3국 또는 국제기구와 처리하는 개인정보에도 적용된다. 다만, 국가안보를 목적으로 하거나 유럽연합 자체 기관에 의해 처리되는 개인정보를 포괄하지는 않는다.

161) 이 지침의 목적을 위해 설립되는 감독기구는 GDPR에 의해 설립되는 감독기구와 같을 수 있으나, 회원국은 독립성 요건에 부합하는 다른 기구를 지명할 수도 있다.

를 제한받는 경우에는 개인정보 감독기구를 통해 자신의 권리를 간접적으로 행사할 수 있다[162].

특히 신기술 환경에 대응하여 경찰기관 등 이 지침의 적용을 받는 개인정보처리자는 개인정보보호 중심설계 및 기본설정(data protection by design and by default) 원칙을 채택해야 한다. 신기술 사용 등 정보주체의 권리에 매우 위험한 결과를 초래할 수 있는 처리를 수행하는 경우, 개인정보처리자는 그 처리 전에 개인정보 영향평가를 수행해야 한다.

(2) 정보기관의 감시와 정보인권

에드워드 스노든이 주요국가 정보기관의 인터넷 대량 감시와 기관 간 정보공유 사실을 폭로한 후, 유럽에서는 개인정보 보호에 대한 규범이 강화되었다. 스노든 사건과 관련한 유럽사법재판소의 판결 이후 개인정보보호 적정성 평가기준이 강화된 것이 대표적이다.

개인정보보호 적정성 평가란 제3국의 개인정보보호 수준이 유럽연합이 보장하고 있는 것과 "실질적으로 동등한지(essentially equivalent)"를 평가하는 제도로서 1995년 개인정보보호지침(95/46/EC) 이래 2018년 GDPR에 그 근거 규정을 두고 있다. 적정성 결정이 내려지면 해당 국가의 기업들은 개별적인 추가 조치 없이도 유럽연합으로부터 역외 제3국으로 개인정보를 이전할 수 있게 된다.

2013년 6월 에드워드 스노든의 폭로 직후, 오스트리아 페이스북 사용자인 막스 슈렘스는 페이스북 아일랜드가 개인정보를 미국으로 이전하지 못하도록 조치해줄 것을 요청하는 진정을 아일랜드 개인정보보호청장에게 제기하였다. 2014년 7월 아일랜드 고등법원은 이 사건이 2000년 유럽연합-미국 간에 체결한 세이프하버 협정의 적정성과 관련이 있다고 보고 유럽사법재판소에 그에 대한 판단을 구했다. 2015년 10월 6일 유럽사법재판소는 유럽연합-미국 세이프하버 협정에 대해 무효 판결을 내렸다.

이 판결에서 문제가 된 것은 세이프하버 원칙이 스스로 인증한 미국의 기업에 적용될 뿐 미국의 공공기관에는 그 준수가 요구되지 않으며, 미국이 적정한 보호수준을 조치하

162) 또 국가안보 관련 개인정보 처리(security related processing)에는 정보주체의 열람권, 삭제권 등 권리 행사에 일부 예외를 인정하였고, 최소처리(data minimisation), 목적제한(purpose limitation) 등의 원칙 적용에 있어서도 융통성을 두었다.

도록 충분한 규정을 포함하고 있지도 않다는 것이었다. 유럽 집행위원회는 자체 분석 보고서에서 미국의 기관이 개인정보에 수집 목적 외로 접근할 수 있고 국가 안보에 필요하고 비례적인 이상으로 개인정보를 처리할 수 있다고 보았다. 그럼에도 세이프하버 원칙은 '국가안보, 공익, 법집행 요구조건에 필요한 한도에서' 그 적용이 제한될 수 있는데, 국가안보 등의 목적을 위해 개인정보가 침해될 때 이를 제한하기 위한 규칙이나 효과적인 법적 보호를 보장하고 있지 않았다.

유럽사법재판소의 무효 판결 이후, 유럽연합 집행위원회와 미국 정부는 세이프 하버 협정을 대체할 새로운 체제로서 EU-US 프라이버시 쉴드(Privacy Shield)를 마련하였다. 프라이버시 쉴드는 이전 세이프하버 협정에 비하여 미국의 공공기관이 개인정보에 접근할 경우에 대한 대응책을 포함했다는 점에서 두드러진다. 프라이버시 쉴드에 따르면 미국의 공공기관은 국가 안보나 법집행 등 공익에 필요한 한도 내에서 개인정보에 접근할 수 있다. 또 이를 감독하기 위한 '옴부즈만(Ombudsperson)' 메커니즘을 미 국무부에 두도록 하였다.

이처럼 최근 유럽에서는 정보기관을 포함한 공공기관의 개인정보 접근과 대량 감시 문제가 전보다 중요하게 간주되고 있다. 유럽연합의 개인정보 관련 유권해석기구인 제29조 작업반은 유럽사법재판소의 판결을 반영하여 2016년 4월 13일 <유럽의 필수 보장원칙(European Essential Guarantees)> 작업문서[163]를 채택했다. 이 문서는 유럽에서 타국으로 개인정보가 이전될 때 법집행이나 국가 안보를 명분으로 한 감시 조치로 정보주체의 권리가 제한될 경우 준수해야 할 4가지 핵심적인 조건을 규정하였다(이은우, 2018: 53)[164].

- 개인정보의 처리는 명확하고 정확하며 접근 가능한 규칙을 기반으로 해야 한다.(법적 기반)
- 추구하는 정당한 목적에 관하여 필요성과 비례성이 입증될 필요가 있다.
- 개인정보의 처리는 독립적인 감독을 받아야 한다.
- 개인에게 효과적인 구제조치가 제공될 필요가 있다.

163) Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)

164) 이은우, 심우민, 오병일. 2018. "EU GDPR등 개인정보보호 규범 및 감독기구의 국제표준 확립 필요성 연구", 개인정보 보호위원회 연구보고서.

위와 같이 강화된 기준들은 향후 적정성 평가에 적용될 예정이다. GDPR 제45조 제2항에서도 보호수준의 적정성을 평가할 때 “관련 공공 안전, 방위, 국가 안보, 형사법을 포함한 일반적 및 영역별 관련 법제와 공공 기관의 개인정보에 대한 접근, 그리고 그러한 법제의 이행”을 고려할 필요가 있다고 규정하고 있다.

한편, 유럽인권재판소 또한 정보기관의 감시로부터 정보인권을 보호하기 위한 규범을 강화하였다. 2018년 9월 13일, 유럽인권재판소는 2000년 영국 수사권한 규제법의 대량감시 프로그램의 인권침해를 인정하였다[165]. 우선 안전조치나 민주적인 감독 장치가 없는 대량 감청은 유럽인권조약 제8조(사생활 및 가족생활/통신의 권리)를 위반하는 것이다. 또 송수신자의 인적정보, 통신일시, 위치를 비롯한 통신 메타데이터의 무제한적인 수집은 조약 제8조 및 제10조(표현의 자유)를 위반하는 것이다. 유럽 시민단체들은 이번 판결이 메타데이터의 대량 수집과 감시의 침해 사실이 인정되었다는 점에서 환영하였다[166]. 메타데이터는 누군가의 생활에 대해 많은 사실을 아주 잘 드러내고 사생활에 대한 권리를 침해할 수 있기 때문에 그에 대한 대량 감시는 통신의 내용에 대한 감시보다 덜 침해적이지 않다는 것이다.

165) 58170/13, 62322/14 및 24960/15 사건.
166) “ECtHR gives a half-hearted victory against UK mass surveillance”. https://edri.org/ecthr-gives-a-half-hearted-victory-against-uk-mass-surveillance/.

제2절 국내 법제 동향 및 분석

한국에서는 2005년 헌법재판소가 개인정보 자기결정권을 헌법상 기본권으로 인정하면서 그 주요 배경으로서, 컴퓨터를 통한 개인정보 처리가 자동화되고 결합되면서 개인의 인적 사항 등이 정보주체 의사와 무관하게 국가, 기업 등 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 정보환경이 등장했다는 점을 들었다[167]. 또한 20대 국회에서의 개헌 논의 과정에서, 각 계에서 제안하고 있는 헌법개정안에서도 정보기본권을 명시적으로 보장하는 방안이 지지를 받고 있다. 2018년 문재인 대통령도 '정보기본권'을 신설하는 내용으로 헌법개정안을 발의하였다.

빅데이터 등 신기술 발전에 따른 개인정보 보호 이슈와 관련해서는 2013년경부터 논란이 지속되어 왔다. 행정안전부와 방송통신위원회 등이 공개된 개인정보 및 자동 수집되는 개인정보의 처리에 대한 가이드라인을 만들었으며, 2016년에는 빅데이터 산업 활성화를 위해 개인정보의 비식별 처리를 통한 활용을 허용하는 <개인정보 비식별 조치 가이드라인>이 만들어졌다. 그러나 명시적인 법적 근거 없는 가이드라인의 제정은 개인정보보호법 위반 논란을 불러왔다. 이에 문재인 정부는 개인정보보호법 개정을 통해 가명처리 된 개인정보의 산업적 활용을 추진하고 있는데, 이에 시민사회는 반발하고 있다. 그러나 2013년부터 개인정보의 활용 범위 및 조건을 둘러싼 논란만 이어졌을 뿐, 프로파일링, 데이터 이동권, 개인정보 보호 중심 디자인 및 기본설정 등 지능정보사회에서의 기술변화에 대응한 법제적인 대응은 이루어지지 않고 있다. 아직 학계를 중심으로 국내외 담론에 대한 소개만 이루어지고 있을 뿐이다.

더구나 현행 개인정보보호법 체계에는 신기술로 인한 정보인권침해를 통제 할 수 있는 규정이 부족한 것은 물론이고, 개인정보 보호법제 및 감독기구들이 분산되어 있어 각 법제 사이의 중복규제, 법적 정합성 미흡, 정보주체의 실질적인 권익 보장의 어려움 등의 실질적인 한계를 가지고 있다(권건보, 2017).[168] 2011년 개인정보보호법이 제정되었음에도 불구하고, 정보통신망법, 위치정보법, 신용정보법 등 다수의 개인정보 보호법제가 혼재되어 있고, 개인정보 감독기구 역시 행정안전부, 개인정보보호위원회, 방송통신위원회,

167) 헌재 2005. 5. 26, 99헌마513, 2004헌마19(병합).
168) 권건보(2017), 지능정보사회 대응을 위한 개인정보보호 법제 정비방안, 아주대학교 산학협력단, 개인정보보호위원회

금융위원회 등으로 분산되어 있기 때문이다. 다행히 문재인 정부에서 개인정보 감독체계 효율화를 국정과제로 내세웠고, 개인정보의 활용 이슈와 더불어 개인정보 보호법제 및 감독기구의 개편이 함께 논의되고 있다.

이 절에서는 우선 국내 개인정보 보호체계의 현황 및 문제점을 검토한 후, 빅데이터 산업 활성화를 명분으로 도입된 개인정보의 비식별 조치를 둘러싼 논란 등 신기술에 대응한 국내의 법제적 대응을 검토한다. 이어 정보수사기관의 개인정보 접근 및 통신수사와 관련된 법제의 문제점을 분석한다.

<표5-2> 최근 정보기본권 관련 헌법개정안 비교

구분	사생활/통신의 자유와 비밀 관련	표현의 자유/알 권리 관련	정보기본권 관련
현행	제17조 모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다. 제18조 모든 국민은 통신의 비밀을 침해받지 아니한다.	제21조 ① 모든 국민은 언론·출판의 자유와 집회·결사의 자유를 가진다. ② 언론·출판에 대한 허가나 검열과 집회·결사에 대한 허가는 인정되지 아니한다. ③ 통신·방송의 시설기준과 신문의 기능을 보장하기 위하여 필요한 사항은 법률로 정한다. ④ 언론·출판은 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해하여서는 아니된다. 언론·출판이 타인의 명예나 권리를 침해한 때에는 피해자는 이에 대한 피해의 배상을 청구할 수 있다.	신설
2017. 6. 국가인권위원회 헌법개정안 (연구포럼안)	제19조 ① 모든 사람은 사생활의 자유를 가지며 그 비밀을 침해받지 아니한다. ② 모든 사람은 통신의 자유를 가지며 그 비밀을 침해받지 아니한다.	제26조 ① 모든 사람은 언론·출판의 자유를 가지며 이에 대한 허가나 검열은 금지된다. ② 언론·출판매체의 다원성과 다양성은 존중된다. ③ 언론·출판은 아동·청소년의 권리나 타인의 명예를 침해하여서는 아니된다.	제25조 ① 모든 사람은 알 권리를 가진다. ② 모든 사람은 자신의 정보를 보호받고 그 처리를 결정할 권리를 가진다.
2018. 1. 국회헌법개정 특별위원회 자문위원회안	제21조 ① 모든 사람은 사생활의 자유를 가지며, 사생활의 비밀을 침해받지 아니한다. ② 모든 사람은 통신의 비밀을 침해받지 아니한다.	제29조 ① 모든 사람은 자유롭게 자신의 의사를 표현할 권리를 가지며, 이에 대한 허가나 검열은 금지된다. ② 언론매체의 자유와 다원성, 다양성은 존중된다. ③ 언론·출판이 타인의 명예나 권리를 침해한 때에는 피해자는 이에 대한 배상 또는 정정 등을 청구할 수 있다.	제28조 ① 모든 사람은 알권리 및 정보접근권을 가진다. ② 모든 사람은 자신의 정보에 관한 결정권을 가진다. ③ 모든 사람은 정보문화향유권을 가진다. ④ 국가는 개인별·지역별 정보격차를 해소하고 정보독점으로 인한 폐해를 예방 및 시정하기 위하여 노력하여야 한다.
2018. 2. 민주사회를위한 변호사모임	제23조 ① 모든 사람은 사생활의 자유를 가지며 사생활의 비밀을 침해받지 아니한다.	제31조 ① 모든 사람은 자유롭게 자신의 의사를 표현할 권리를 가지며, 이에 대한 허가나 검열은 금지된다.	제30조 ① 모든 사람은 알 권리를 가진다. ② 모든 사람은 정보접근권을 가진다. ③ 모든 사람은 자기의 정보에 관한 결정권

개헌특별위원회안	② 모든 사람은 통신의 자유를 가지며 통신의 비밀을 침해받지 아니한다.	② 언론매체의 자유와 독립은 보장되며, 국가는 언론매체의 다원성과 다양성이 강화되도록 노력하여야 한다. ③ 언론·출판이 타인의 명예나 권리를 침해한 때에는 피해자는 이에 대한 배상 또는 정정 등을 청구할 수 있다.	을 가진다. ④ 모든 사람은 정보문화향유권을 가진다. ⑤ 국가는 개인별·지역별 정보격차 및 정보독점으로 인한 폐해를 해소하기 위하여 노력하여야 한다. ⑥ 국가는 공공의 문제에 관하여 누구나 자유롭고 효과적으로 의견을 교환할 수 있도록 필요하고도 충분한 정보를 제공하여야 한다.
2018. 2. 참여연대 분권·자치·기본권 연구모임	제16조 ① 모든 사람은 사생활의 자유를 가지며 사생활의 비밀을 침해받지 아니한다. ② 모든 사람은 자기의 정보에 대한 결정권을 가진다. 제19조① 모든 사람은 통신의 자유를 가지며 통신의 비밀을 침해받지 아니한다. ② 모든 사람은 법률이 정하는 바에 따라 경제적 능력등에 구애됨이 없이 통신시설 또는 통신상의 편의를 누릴 권리를 가진다.	제25조 ① 모든 사람은 자유롭게 자신의 의사를 표현할 권리를 가지며, 이에 대한 허가나 검열은 금지된다. ② 언론매체의 자유와 다원성·다양성은 존중된다. ③ 언론·출판이 타인의 명예나 권리를 침해한 때에는 피해자는 이에 대한 배상 또는 정정을 청구할 수 있다.	제26조 ① 모든 사람은 알 권리와 정보문화향유권을 가진다. ② 모든 사람은 국가가 보유한 정보에 대한 접근권을 가진다. ③ 국가는 개인별·지역별 정보격차 및 정보독점으로 인한 폐해를 해소하기 위하여 노력하여야 한다. ④ 국가는 공공의 문제에 관하여 누구나 자유롭고 효과적으로 의견을 교환할 수 있도록 누구에게나 필요하고도 충분한 정보를 제공하여야 한다.
2018. 3. 대통령 발의안	제17조 ① 모든 사람은 사생활의 비밀과 자유를 침해받지 않는다. ② 모든 사람은 주거의 자유를 침해받지 않는다. 주거에 대한 압수나 수색을 하려 할 때에는 적법한 절차에 따라 청구되고 법관이 발부한 영장을 제시해야 한다. ③ 모든 국민은 통신의 비밀을 침해받지 않는다.	제20조 ① 언론·출판 등 표현의 자유는 보장되며, 이에 대한 허가나 검열은 금지된다. ② 통신·방송·신문의 기능을 보장하기 위하여 필요한 사항은 법률로 정한다. ③ 언론·출판은 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해해서는 안 된다. 언론·출판이 타인의 명예나 권리를 침해한 경우 피해자는 이에 대한 배상·정정을 청구할 수 있다.	제22조 ① 모든 국민은 알권리를 가진다. ② 모든 사람은 자신에 관한 정보를 보호받고 그 처리에 관하여 통제할 권리를 가진다. ③ 국가는 정보의 독점과 격차로 인한 폐해를 예방하고 시정하기 위하여 노력해야 한다.

1. 국내 개인정보 보호체계 현황 및 문제점

1) 국내 개인정보 보호법제 현황 및 문제점

개인정보 보호에 관한 일반법인 개인정보 보호법이 제정되기 전까지는 민간분야에 대한 일반법의 역할을 한 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』(정보통신망법)을 비롯하여, 『위치정보의 보호 및 이용 등에 관한 법률』(위치정보법), 『신용정보의 이용 및 보호에 관한 법률』(신용정보법), 『의료법』 등 분야별 개별법이 적용되어 왔다. 2011년 제정된 개인정보보호법은 공공부문과 민간부문의 모든 개인정보처리자에게 적용되는 법으로 개인정보의 수집, 이용, 제공 등 개인정보 처리 단계에 따른 보호의 기준을 구체화하고 있다. 특히 정보주체의 개인정보 침해가 우려되는 경우에는 공공기관에 대하여 개인정보 영향평가를 위한 적극적인 노력을 요구하는 등 개인정보의 효율적인 보호를 위한 수단을 포함하고 있다(이인호, 2017).[169]

그런데 개인정보보호법 제정과 함께 기존에 개별 영역을 규율했던 법률들을 정비해야 했지만, 여전히 각 개별법들이 유지됨으로 인해 많은 혼란을 야기하고 있다.

첫째, 법제 간에 중복, 유사 규정이 존재하여 수범자의 혼란을 초래하거나 모든 법률을 준수해야 하는 부담을 야기하게 된다. 동일한 행위에 대해 법률에 따라 벌칙이 상이한 경우가 발생하며, 상이한 제재조치는 법의 집행에 있어 형평성을 저해하는 문제로 이어질 수 있다. 예를 들어, 정보주체의 동의 없이 개인정보를 수집한 경우, 개인정보 보호법은 제75조에서 5천만 원 이하 과태료를 부과하고 있는 반면, 정보통신망법 71조는 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처하도록 하고 있다. 이 경우 수범자는 기준으로 삼아야 할 법률을 파악하기 힘들게 되며, 위법사항이 발생하는 경우에도 어떤 법을 기준으로 벌칙이 정해지느냐에 따라 그 수준이 상이한 경우가 발생한다.

둘째, 조항의 해석 및 법률 적용의 우선 순위에 있어 혼란을 초래한다. 개인정보보호법 제6조는 '다른 법률과의 관계'를 아래와 같이 규정하고 있는데, 만일 정보통신망법 등 다른 법률을 특별법으로서 우선 적용한다면 일반법으로서 개인정보 보호법이 유명무실해지는 결과를 초래할 수 있다.

169) 이인호(2017), 한국의 개인정보보호 수행체계 발전방안 연구, 중앙대 산학협력단, 개인정보보호위원회.

개인정보보호법

제6조(다른법률과의 관계) 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.

셋째, 각 법률의 소관 부처가 달라 규제 기관 간 규제 영역 확보를 위한 경쟁을 하거나, 국회의 개별 상임위원회에서 전체적인 개인정보 보호체계에 대한 고려 없이 법 개정이 이루어짐에 따라 법률 간의 차이가 심화하고 있다. 실제로 개인정보보호법 제정 이후에도 행정안전부, 방송통신위원회, 금융위원회는 30여 차례가 넘도록 경쟁적으로 법률 및 시행령 개정을 추진한 바 있다(이은우 외, 2018: 101).[170]

넷째, 개인정보보호법을 제외한 다른 법률들은 대부분 개인정보 보호규정과 동시에 각 산업의 진흥을 위한 내용을 함께 고려하고 있어, 각 부문마다 개인정보보호 관련 정책의 불일치가 발생 할 수 있다. 즉, 4차 산업혁명과 관련한 신기술을 발전시키기 위해 빅데이터 활용 및 개인정보 활용을 추진하는 한편 개인정보 보호를 위한 방안을 강구해야 하는 상황이 되는데 이 경우 개인정보보호에 방점을 두기보다는 해당 산업의 발전에 더 집중하여 정책을 추진하는 경우가 나타날 수 있다.[171] 예를 들어 개인정보의 결합·분석을 통해 통합적인 금융 데이터베이스를 구축하고자 할 경우, 이 과정에서 나타날 수 있는 여러 문제에 관해 고민하고 규정하는 대신 개인 신용정보 유출을 방지하기 위한 개인정보 비식별 조치를 지원하는 데만 역점을 둘 수 있다.

따라서 신기술에 대응하기 위한 법제 개선에 앞서, 현재와 같이 분산된 개인정보 보호 법제를 체계적이고 통일적으로 정비할 필요가 있다. 각 영역에 고유한 특수한 규율은 특별법의 형식으로 남겨두더라도, 개인정보 보호와 관련한 중복되는 규율의 경우 개인정보보호법을 중심으로 정비해야 할 것이다.

2) 국내 개인정보 감독기구 현황 및 문제점

개인정보 감독기구 역시 분산된 수행체제를 갖고 있다. 개인정보 보호법에 근거한 대

170) 이은우 외, EU GDPR등 개인정보보호 규범 및 감독기구의 국제표준 확립 필요성 연구- 국제규범의 변화와 국내 개인정보 보호체계 효율화 방안 -, 개인정보보호위원회 연구용역, 2018.6

171) 김일환(2017), 현행 개인정보보호법체계상 감독기구 법제정비방안에 관한 연구, 미국헌법연구 28(2), 2017.8, 219-273.

통령 소속의 개인정보보호위원회와 행정안전부가 개인정보 감독기구의 역할을 수행하고 있는 동시에, 민간 정보통신분야의 개인정보보호 업무는 방송통신위원회, 신용정보보호는 금융위원회가 담당하고 있다. 이러한 분산된 개인정보 보호 수행체계는 개인정보처리자의 법 준수상의 어려움, 대규모의 개인정보 침해사고 발생 시 컨트롤타워 부재, 개인정보 감독기관의 독립성과 자율성 문제 등 여러 문제에 직면해 있다(권건보, 2017).[172]

국내 개인정보 감독기구의 가장 큰 문제는 독립성이 부재하다는 것이다. 개인정보 감독기구와 관련한 국제 규범은 감독기구의 독립성을 핵심적인 요건으로 규정하고 있다. GDPR 역시 유럽사법재판소 판결 등을 통해 확립된 감독기구 규범을 구체적으로 반영하고 있는데, ① 감독기구의 완전한 독립성, ② 직무권한의 독립성, ③ 양립불가 업무의 겸직금지, ④ 직무수행 및 권한행사에 필요한 인적, 기술적 및 재정적 지원 보장, ⑤ 직원 인사의 자율성, ⑥ 예산의 독자성을 독립성 요건으로 규정하였다(이은우 외, 2018: 25).

그러나 국내의 경우 행정안전부는 스스로 국민들의 방대한 개인정보를 보유하고 있는 개인정보처리자이자 국무총리의 지휘를 받고 있는 중앙행정기관으로서 독립성을 보장하기 어려우며, 방송통신위원회는 독립적 합의체 기관이긴 하지만, 감독과 동시에 ICT 산업 육성을 동시에 맡고 있다. 개인정보보호위원회 역시 인사·예산권 등을 보유하고 있지 않아 독립성이 없고, 개선 권고, 의견 조정 및 제시, 분쟁 조정 권고, 의견청취 등의 업무에 집중되어 있어 그 권한이 다른 기관에 비해 매우 약하다. 실제 개인정보관리 수준 및 실태파악을 위한 조사권한, 위반행위 조사를 위한 자료제출요구 및 검사, 위반자에 대한 시정조치나 징계권고 혹은 과태료 부과 등 주된 집행 권한은 행정안전부에 의해 이루어진다.

둘째, 수행 체계의 분산으로 개인정보 보호를 위한 물적, 인적 자원을 효과적으로 결집하기 힘들다. 동일한 기능을 수행하는데 분야별로 인적, 물적 자원이 분산될 경우 개인정보보호에 필요한 충분한 인적, 물적 자원의 확보가 어렵기 때문이다(이인호, 2017).

셋째, 통일적인 개인정보 보호정책의 수립이 힘들다. 각 규제기관이 관할 영역을 두고 경쟁하거나 같은 사안에 대해 서로 다른 입장을 내놓을 수 있기 때문이다. 예를 들어, 유럽연합의 개인정보 적정성 평가와 관련해서도 방송통신위원회와 개인정보보호위원회가 부처 간 이견[173]을 보인 바 있으며, 후술하겠지만 비식별 조치와 관련해서도 개인정보보

172) 권건보(2017), 지능정보사회 대응을 위한 개인정보보호 법제 정비방안, 아주대학교 산학협력단, 개인정보보호위원회

호위원회는 다른 정부부처와 다른 의견을 낸 바 있다.

이와 같이 분산된 현행 개인정보 보호체계는 국제적인 규범에 부합하지 않고 국내적으로도 개인정보 보호에 대한 국민들의 신뢰를 약화시키는 요인이 되어 왔다. 따라서 세계적인 추세에 발맞춰 공공과 민간을 통합하여 감독, 집행하는 단일의 독립적인 감독기구를 구축할 필요가 있다.

3) 개인정보 보호체계 개편을 위한 법률안 현황

20대 국회에 개인정보 감독기구의 재편과 관련한 법안이 여러 개 발의되었다. 소병훈(의안번호 2006865), 송희경(의안번호 2007083), 변재일(의안번호 2010738), 진선미(의안번호 2012312), 인재근(의안번호 2016621), 이재정(의안번호 2016668) 의원이 대표발의한 개인정보보호법 개정안인데, 모두 개인정보보호위원회를 중앙행정기관으로 격상하고 개인정보 감독기구로서의 권한을 부여하는 내용을 포함하고 있다. 2018년 11월 15일, 인재근 의원이 대표발의 한 안은 사실상 정부안인데 의원입법의 형식으로 발의한 것이다.

소병훈, 송희경 의원안의 경우 개인정보보호위원회가 "그 권한에 속하는 사무를 독립적으로 수행"한다고 규정하고 있음에도 불구하고, 변재일, 진선미, 인재근 의원안과 같이 "독립적인 업무 수행을 위하여 같은 법(정부조직법) 제18조를 적용하지 아니한다"는 규정을 포함하지 않고 있어 독립성 보장에는 한계가 있다. 인재근 의원이 대표발의한 안은 개인정보보호위원회의 일부 권한[174]에 대해서만 정부조직법 제18조를 적용하지 않는 것으로 하고 있는데, 이에 따라 개인정보의 보호와 관련된 법령의 개선, 정책·제도·계획 수립·집행 등 다른 업무는 국무총리가 행정감독권을 행사할 수 있도록 되어 있다. 이에 대해 시민사회단체는 개인정보보호위원회의 독립성에 대한 중대한 침해이며, 기본 정책 방향에 대해서 정부의 기조에 따라 통제하겠다는 것이라고 비판하고 있다.[175]

---

173) 개인정보보호위원회 결정, 제2017-25-198호, EU 부분적정성 평가 전환 추진 개선에 관한 건, 2017.11.13

174) 개인정보보호법 개정안 (인재근 의원 대표발의)
제7조
② 보호위원회는「정부조직법」제2조에 따른 중앙행정기관으로 본다. 다만, 다음 각 호의 사항에 대하여는「정부조직법」제18조를 적용하지 아니한다.
1. 제7조의8제1항에서 정하는 소관사무 중 제3호 및 제4호의 사무
2. 보호위원회의 심의·의결 사항 중 제1호에 해당하는 사항

175) 건강과대안 등. [기자회견] 개인정보 판매와 공유를 허용하는 개인정보보호법 반대한다!.

한편, 변재일, 진선미 의원안은 개인정보보호위원회의 업무 지원을 위해 '개인정보보호원'과 같은 공공기관을 설립하도록 하고 있다.

위원회의 구성은 각 의원 안별로 차이가 있다. 개인정보보호위원회의 업무량과 전문성을 고려할 때, 변재일, 진선미, 이재정 의원안과 같이 상임위원의 수를 최소한 3명 이상으로 할 필요가 있어 보인다.

<표5-3> 국회발의 개인정보보호법 개정안 비교: 개인정보보호위원회 구성

진선미 의원안	5명 (위원장 1명 포함 전원 상임)
송희경 의원안	9명 (위원장 1명, 상임위원 2명 포함)
소병훈 의원안	9명 (위원장 1명, 상임위원 2명 포함)
변재일 의원안	9명 (위원장 1명, 상임위원 3명 포함)
인재근 의원안	7명 (위원장 1명, 부위원장 1명 등 상임위원 2명 포함)
이재정 의원안	9명 (위원장 1명, 부위원장 2명 등 상임위원 3명 포함)

시민사회는 "행정안전부, 방송통신위원회, 금융위원회 등에 분산된 개인정보 감독 기능을 개인정보보호위원회로 일원화"할 것을 요구해왔다.[176] 그러나 소병훈, 송희경, 변재일 의원안의 경우에는 개인정보보호법 개정만을 다루고 있어 개인정보호보위원회를 중앙행정기구로 격상하기는 하지만 현재 행정안정부의 권한만일 이관하는 것으로 되어 있다. 진선미 의원은 개인정보보호법 개정안과 함께, 정보통신망법에서 개인정보 관련 조항을 삭제하는 개정안(의안번호 2012308)을 함께 발의하여 방송통신위원회의 권한 역시 개인정보보호위원회로 이관하고 있다. 이재정 의원안과 정부안인 인재근 의원안 역시 행정안전부와 방송통신위원회 권한만을 개인정보보호위원회로 이관하고 있어 한계로 지적된다.

2. 신기술의 발전과 법제적 대응

1) 빅데이터 시대 개인정보의 보호와 활용

(1) 개인정보의 비식별 처리 논란

2018.11.21. https://act.jinbo.net/wp/40024/

176) 경제정의실천시민연합 등. 빅데이터 활성화 위해 개인정보 보호체계와 감독기구 일원화 시급하다!. 2018.5.17.

국내에서 빅데이터 분석 목적의 개인정보 활용은 '비식별 처리된 개인정보'의 적법성을 두고 논란이 계속되어 왔다. 개인정보보호법 등 현행 개인정보 보호법제는 '비식별'이라는 개념을 포함하고 있지 않다. 그러나 정부는 이미 수집된 개인정보를 수집 목적 외로 활용하기 위해 가이드라인에 '비식별'이라는 개념을 도입하여 비식별 처리된 개인정보를 일정한 조건 하에 활용할 수 있도록 하였고, 이는 자연스럽게 개인정보보호법 위반 논란을 야기하였다. 법에 근거하지 않은 '비식별' 개념을 사용했을 뿐만 아니라, 가이드라인에 따라 비식별 개념도 변화하여 혼란을 심화시켰다.

'비식별(de-identification)'이란 개인정보에서 식별자를 제거하는 것을 의미하는데, 식별자 제거의 정도에 따라 그 결과는 다른 정보와 결합하여도 더 이상 개인을 식별할 수 없는 익명정보(anonymised data)가 될 수도 있고, 다른 정보와 결합하면 개인을 식별할 수 있는 가명정보(pseudonymised data)가 될 수도 있다. 예를 들어 미국의 국가기술표준원(NIST)은 'de-identification'과 'anonymization'이라는 용어를 설명하면서, 'anonymization'은 "재식별이 불가능한 de-identification이 된 정보"라는 의미를 함축하며 de-identification이 된 정보는 재식별이 불가능하기도 하고 가능하기도 한다고 설명하고 있다.[177]

○ 공공정보 개방·공유에 따른 개인정보 보호 지침 (2013.9)

국내에서 처음 비식별 개념이 도입된 것은 2013년 9월 발표된 <공공정보 개방·공유에 따른 개인정보 보호 지침>인 것으로 보인다.[178] 동 지침은 "공공정보 개방 공유 및 개인 맞춤형 서비스 확대에 따른 개인정보 침해 요소에 대한 선제적 보호조치 강화 및 안전한 활용 기반 마련"을 목적으로 마련된 것인데, '비식별화'를 "개인정보의 일부 또는 전부를 삭제하거나 다른 정보로 대체함으로서 다른 정보와 쉽게 결합하여서도 특정 개인을 식별하기 어렵도록 하는 일련의 조치"로 규정하고 있다. 동시에 "비식별화된 정보가 다른 정보와의 연계(매칭) 등을 통해 특정 개인을 알아볼 수 있는 개인정보가 되는 것"을 '재식별화'로 규정하였는데, 이는 비식별화된 정보가 다시 재식별될 수 있음을 염두에 둔 것이다.

국내 개인정보보호법은 제2조 1호에서 개인정보란 "살아 있는 개인에 관한 정보로서

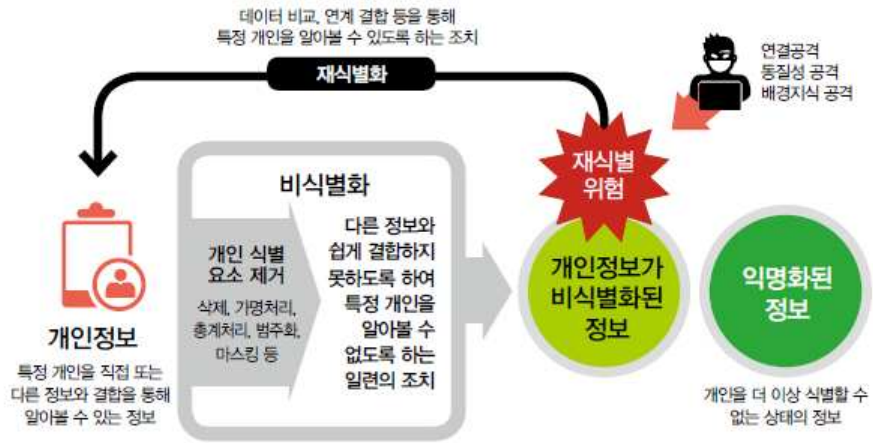
177) NIST(2016), "De-Identifying Government Datasets (2nd Draft)", NIST Special Publication (SP) 800-188(2016. 12. 15), 10p

178) https://www.privacy.go.kr/nns/ntc/selectBoardArticle.do?nttId=4935

성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다"고 정의하고 있는데, 따라서 비식별화된 정보 역시 다른 정보와 결합하여 재식별될 수 있다면 개인정보에 해당한다. 그럼에도 불구하고 동 지침은 개인정보를 애초 수집 목적 외로 분석, 활용하려는 경우, 그 법적 근거가 없을 때에는 "비식별화 조치 후 분석"할 수 있도록 하고 있다. 또한, "공공정보 개방·공개 시에는 특정 개인을 알아볼 수 있는 요소를 삭제하거나 비식별화 처리 후 개방·공개 가능"하도록 하고 있다. 그러나 이는 개인정보의 목적 외 이용 및 제공에 해당하여 개인정보보호법 위반이 될 수 있다.

○ 개인정보 비식별화에 대한 적정성 자율평가 안내서(2014. 12.)

2014년 12월 행정자치부와 한국정보화진흥원은 <개인정보 비식별화에 대한 적정성 자율평가 안내서>를 발표했다. 2013년의 지침이 공공정보의 활용을 위한 것이라면, 이 안내서는 공공 및 민간의 개인정보처리자를 모두 대상으로 하고 있다. 이 안내에서도 비식별화, 익명화, 재식별화를 구분하고 있다. 익명화는 "비식별화 조치의 궁극적인 상태로, 개인에 대한 재식별이 더 이상 불가능한 상태"로 규정하였다.



<그림5-2> 개인정보 비식별 및 재식별 개념179)

179) 개인정보 비식별화에 대한 적정성 자율평가 안내서(2014. 12.)

- 비식별화(de-identification): 정보의 일부 또는 전부를 삭제·대체 하거나 다른 정보와 쉽게 결합하지 못하도록 하여 특정 개인을 알아볼 수 없도록 하는 일련의 조치
- 익명화(Anonymization): 비식별화 조치의 궁극적인 상태로, 개인에 대한 재식별이 더 이상 불가능한 상태
- 재식별화(re-identification): 비식별화한 개인정보를 다른 정보 또는 데이터와 비교, 연계, 결합 등을 통해 특정 개인을 알아볼 수 있도록 하는 일련의 조치

또한 이 "안내서를 이용해서 개인정보 비식별화에 대한 적정성을 평가하고, 관련 데이터를 공개 또는 제공하는 것에 대한 책임은 해당 개인정보처리자에게 있"음을 밝히고 있다. 즉, 이 안내서에 따라 조치를 했다고 해서 개인정보보호법의 적용을 배제하는 것은 아니라는 것이다.

○ 빅데이터 개인정보보호 가이드라인(2014. 12.)[180]

방송통신위원회는 "창조경제의 핵심인 빅데이터 산업의 활성화를 도모하고 동시에 개인정보의 오·남용을 방지"하기 위해,[181] 2013년 말부터 <빅데이터 개인정보보호 가이드라인> 제정을 추진하였다. 이 가이드라인은 공개된 개인정보, 이용내역정보, 그리고 이 정보들의 분석을 통해 새로 생성된 정보 등의 처리 원칙을 규정하고자 한 것이었다. 그러나 시민사회단체들은 이 가이드라인이 빅데이터 산업 활성화를 위해 개인정보 보호법제를 훼손하는 행정행위라며 반발하였다.[182]

가이드라인은 비식별화를 "데이터 값 삭제, 가명처리, 총계처리, 범주화, 데이터 마스킹 등을 통해 개인정보의 일부 또는 전부를 삭제하거나 대체함으로써 다른 정보와 쉽게 결합하여도 특정 개인을 식별할 수 없도록 하는 조치"로 규정하였다. 그런데 비록 공개된 개인정보와 이용내역정보를 대상으로 하고 있기는 하지만, 비식별화 조치를 한 경우에는 개인정보 보호법제의 적용을 배제하고 있다. 즉, 정보통신서비스 제공자가 개인정보가 포함된 공개된 정보를 비식별화 조치한 경우에는 사용자의 동의 없이 수집·이용할

180) 동 가이드라인은 관계부처 합동으로 마련한 <개인정보 비식별 조치 가이드라인>이 2016.7.1.자로 시행됨에 따라 폐지되었다.

181) 방송통신위원회, 빅데이터 개인정보보호 가이드라인 수정(안), 2014.3.19. p8

182) 경실련, 진보네트워크센터, 함께하는시민행동. 방통위의 「빅데이터 개인정보보호 가이드라인(안)」에 대한 시민단체 입장. 2013.12.30.

수 있고(제4조 제1항), 사용자의 동의를 받지 않아도 비식별화 조치를 취한 후 이용내역 정보를 수집·이용할 수 있으며(제5조 제1항), 정보주체의 동의가 없어도 비식별화 조치하여 수집한 공개된 정보 및 이용내역정보를 정보 처리시스템을 통해 조합·분석하여 새로운 정보를 생성할 수 있고(제6조 제1항), 정보주체의 동의를 받지 않고도 비식별화 처리된 공개된 정보 및 이용내역정보를 자신의 서비스 제공업무 수행을 위해 내부에서 이용할 수 있고(제9조 제1항), 비식별화 처리된 공개된 정보, 이용내역정보, 생성 정보는 사용자 동의 없이 제3자 제공이 가능하다(제10조)고 하고 있다. 이는 비식별화 조치된 개인정보를 개인정보보호법의 적용을 받지 않는 익명정보로 간주하는 것으로, 앞서 보았던 지침이나 안내서와 차이가 있다. 또한 비식별화는 여전히 법에 근거를 두고 있는 개념이 아니고, 재식별을 전제로 하고 있다는 점에서 익명정보보다 낮은 수준임에도 불구하고 사실상 개인정보 보호규범을 배제하고 있다는 점에서 문제가 있다.[183]

개인정보보호위원회 역시 동 가이드라인이 개인정보보호법 등에 부합하지 않는 내용을 일부 포함하고 있으므로 관련 법제에 맞게 재검토할 것을 권고한 바 있다.[184] 특히 공개된 개인정보와 이용내역정보의 처리가 문제가 되었는데, 개인정보보호위원회는 "현행 개인정보보호법 및 정보통신망법은 '공개된 개인정보' 나 '이용내역정보'를 달리 취급하여 규정하고 있지 않으므로 .... 정보주체로부터 명시적인 동의를 받도록 하며, 다만 다른 법률에 특별한 규정이 있는 등의 몇 가지 예외 사유에 한정하여 동의 없는 수집을 허용하고, 그 수집 목적의 범위 내에서만 수집된 개인정보를 이용할 수 있도록 하는 규정들 (개인정보보호법 제15조, 정보통신망법 제22조, 제24조 등)은 '공개된 개인정보' 및 '이용내역정보'에도 그대로 적용된다"고 보았으며, 이에 따라 "제한없이 일반 공중에게 공개되었다 하여 개인정보보호법이나 정보통신망법의 규제를 받지 않는다거나 구체적 사정을 고려함이 없이 해당되는 모든 정보주체가 그 수집에 필요한 동의를 한 것으로 해석하거나 간주할 수는 없다"고 판단하였다.

○ 개인정보 비식별조치 가이드라인 (2016. 6.)

---

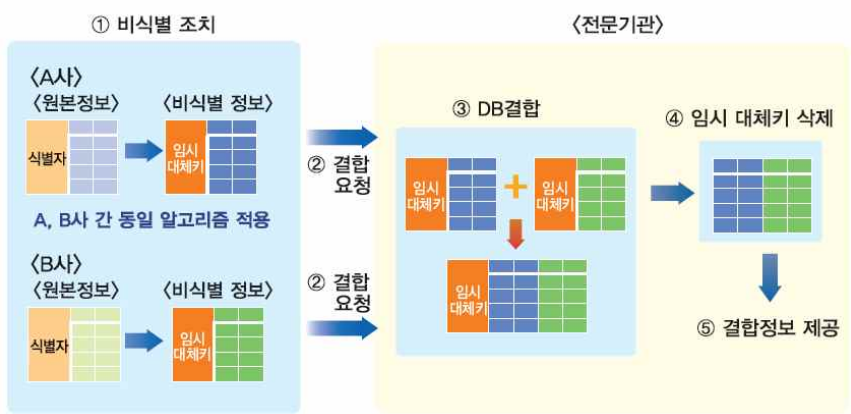
183) 경실련, 진보네트워크센터, 함께하는시민행동. 방송통신위원회의 「빅데이터 개인정보보호 가이드라인」 통과에 대한 입장. 2014.12.24.

184) 개인정보보호위원회 결정. 2014 의결 제16호(2014. 7. 30.). 「빅데이터 개인정보보호 가이드라인(안)」관련 진정 건

행정자치부, 방송통신위원회 등 여러 정부부처의 가이드라인 발표가 제각각 이루어지자, 2016년 7월 정부는 관계부처 합동(국무조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부)으로 <개인정보 비식별조치 가이드라인>을 발표하였다. 특히, 이 가이드라인은 빅데이터 분석에 활용하기 위해 서로 다른 정보집합물(데이터셋)을 결합하는 공공기관 및 민간 기업의 업무를 지원하기 위하여 개인정보 비식별 조치 '전문기관'을 설립하도록 하였다.

이 가이드라인은 비식별 조치를 "정보집합물에서 개인을 식별할 수 있는 요소를 전부 또는 일부 삭제하거나 대체하는 등의 방법을 활용, 개인을 알아볼 수 없도록 하는 조치"로 규정하고 있으며, 이 가이드라인에 따라 정보주체를 알아볼 수 없도록 비식별 조치를 적정하게 한 비식별 정보는 "개인정보가 아닌 것으로 추정"되며, 따라서 빅데이터 분석 등에 이용하거나 제3자에게 제공할 수 있다고 한다. 동시에 불특정 다수에게 공개하는 것은 식별 위험이 크므로 원칙적으로 금지하고, 비식별 조치된 정보가 유출되는 경우 다른 정보와 결합하여 식별될 우려가 있으므로 필수적인 보호조치를 이행하도록 하고 있다. 비식별 정보가 여전히 재식별의 가능성이 있음을 인지하고 있음에도 불구하고, 개인정보가 아닌 것으로 추정하여 개인정보보호법 적용을 배제하고 있는 것이다.

이 가이드라인의 독특한 점은 통신, 금융, 교육 등 분야별로 전문기관을 지정하여 기업 간 정보집합물의 결합을 지원할 수 있도록 했다는 점이다. 전문기관이 정보집합물을 결합하는 절차는 아래 그림과 같다.



185)

<그림5-3> 임시 대체키를 통한 기업 간 정보집합물 결합 절차[185)]

185) 개인정보 비식별조치 가이드라인 (2016.6)

가이드라인 발표 후인 2016년 8월, 각 부처에 의해 개인정보 비식별 조치 전문기관이 지정되었으며, 9월에는 전반적인 운영 지원을 위해 한국인터넷진흥원(KISA)에 '개인정보 비식별 조치 지원센터'가 설치되었다. 그리고 동 가이드라인에 의해 2016년 8월부터 2017년 9월까지 26차례에 걸쳐 총 347,522,005건의 민간 기업의 데이터가 결합된 것으로 나타났다. (이은우 등, 2017)[186] 시민사회단체들은 이 가이드라인 제정 당시부터 비판을 해왔지만, 2017년 국정감사를 통해 3억 4천여만건의 사용자 개인정보가 동의 없이 결합되어 기업에 제공된 것이 드러나자, 비식별 전문기관과 20개 기업을 개인정보보호법 등 위반으로 검찰에 고발하였다.[187]

이 가이드라인에 대해 다음과 같은 비판이 제기되고 있다. 우선, 이 가이드라인이 법적 근거가 없다는 점이다. 하위 법령이나 가이드라인 등은 상위법이 위임한 한도 내에서 규정되어야 하는데, 이 가이드라인은 개인정보보호법 등의 위임 범위를 넘어섰다는 것이다. 현재의 개인정보 보호법제는 '비식별' 개념을 두고 있지 않은데, 비식별 처리된 개인정보를 개인정보가 아닌 것으로 보는 것은 개인정보보호법의 개인정보 처리 원칙을 넘어선 것이라는 점이다.

이는 비식별 조치의 개념과 법적 성격이 모호하다는 점에서 기인한다. 가이드라인은 동 가이드라인에 따라 적정하게 비식별 조치를 한 경우 '개인정보가 아닌 것으로 추정'해주고 있다. 여기서 추정된다는 의미는 "개인정보에 해당한다는 반증이 없는 한 개인정보가 아니되, 개인정보라는 반증이 나오는 경우 개인정보로 본다는 뜻"이라고 설명하고 있다. 그런데 개인정보가 아니라면 개인정보보호법 적용을 받지 않기 때문에 자유롭게 이용하거나 제3자 제공 가능함에도 불구하고, 가이드라인은 향후 재식별될 가능성을 우려하여 불특정 다수에게 공개하는 것은 금지하고 있어 재식별 조치가 익명조치에 이르지 못할 수 있음을 전제하고 있다.

따라서 개인정보 침해에 대한 책임 소재 역시 모호해진다. 동 가이드라인은 비식별 정보를 재식별하여 이용하거나 제3자에게 제공한 경우에 대한 형사처벌만을 언급하고 있을 뿐, "당초 평가단 평가시 '적정'으로 판단할 만한 상당한 근거가 있었다면, 추후에 재식

186) 이은우 등. 데이터 연계·결합 지원제도 도입방안 연구. 개인정보보호위원회 연구 용역. 2017.12

187) 건강사회를위한약사회 등. 시민단체, 고객정보 3억4천여만 건 무단결합한 비식별화 전문기관 및 20개 기업 고발. 2017.11.9.

별 되었다는 이유만으로 책임을 부과하는 것은 곤란"하다고 하고 있다. 그렇다면 가이드라인에 따라 비식별 조치하여 활용하였으나 향후 개인식별 등의 문제가 발생했을 경우, 해당 피해자는 개인정보처리자, 비식별조치 평가단, 정부 중 누구에게 책임을 물어야 할 것인지 모호해진다.

특히, 정보집합물의 결합은 개인정보보호법 위반 소지가 높은데, 일반적인 비식별 조치의 경우 비식별 조치가 충분하게 되었다면 그 결과 익명정보가 될 수도 있지만, 전문기관에 의한 정보집합물 결합은 원래의 보유기업이 정보집합물 원본을 가지고 있고 개별 데이터를 고유하게 식별할 수 있는 임시대체키를 포함한 정보집합물을 전문기관에 제공했다는 점에서 익명정보로 보기에는 무리가 있다. 따라서 이는 정보주체의 동의없는 제3자 제공으로서 개인정보보호법 위반에 해당한다.

더불어 해외에서는 데이터 결합이 주로 공공 데이터를 대상으로, 학술 연구 및 통계작성을 목적으로, 데이터 결합에 관련된 각 기관(보유기관, 연계기관, 제공기관 등)의 분리를 고려하여 이루어지고 있는 반면, 동 가이드라인에 의한 정보집합물 결합은 민간 기업의 데이터를 대상으로 하고 있으며, 결합 목적에 있어서 제한을 두고 있지 않고, 결합된 정보집합물을 각 기업에 다시 제공하는 등 데이터 결합 단계별로 기능 분리가 제대로 이루어지고 있지 않다는 비판이 제기된다(이은우 등, 2017).

한편, 개인정보보호위원회 역시 비식별 조치라는 용어를 '익명처리/가명처리'로 통일할 것을 권고하고 있다. 동 가이드라인에 대해 법적 근거가 없다는 비판이 일자, 주요 내용을 법제화하려는 목적으로 개인정보보호법 등의 개정안이 국회에 발의된 바 있는데, 개인정보보호위원회는 이에 대한 검토 의견서[188]에서 비식별 조치라는 "'특정 개인의 식별가능성(identifiability)을 없애는 행위'를 지칭하는 용어가 혼란스럽게 사용 중으로 명칭 및 개념 정의가 정립되지않아 인식과 해석 및 국내외적 의사소통을 저해"하고 있음을 지적하였다. 이에 따라 "빅데이터 활용, 공공정보 공개 등 개인정보보호 핵심 이슈에 관한 명칭 및 정의를 입법 초기 단계에서 국제적 통용성(interoperability)을 갖추도록 정립"하는 것이 필요하다며, 익명처리/가명처리로 용어를 통일할 것을 권고하였다.

188) 개인정보보호위원회 결정 제2017-14-122호. 「개인정보 보호법」 일부개정 법률안 의견 조회에 관한 건. 2017.6.26.

(2) 가명정보의 활용 범위를 둘러싼 논란

시민사회단체들이 비식별 전문기관과 20개 기업을 고발한 이후, 가이드라인이 공식적으로 폐지되지는 않았지만 사실상 사문화되었다. 그러나 문재인 대통령 역시 '4차 산업혁명' 시대의 적임자임을 표방하였고, 빅데이터 환경에서 개인정보의 보호 및 활용을 어떠한 규범하에 할 것인지에 대한 과제는 여전히 남아있었다. 대통령 산하 4차산업혁명위원회는 '규제·제도혁신 해커톤'이라는 이름으로, 4차 산업혁명 관련 주요 이슈에 대해 정부, 산업계, 시민사회, 학계 등 관련 이해관계자들이 모여 끝장 토론 방식으로 합의를 모아 나가는 행사를 개최하였는데, '개인정보의 보호와 활용의 조화' 의제도 2차[189] 및 3차[190] 해커톤을 통해 다루어졌다.

2차 해커톤에서는 비식별화라는 용어보다는 '개인정보, 가명정보, 익명정보'로 개인정보와 관련된 법적 개념체계를 정비하기로 합의하였다.

2차 해커톤 합의 내용

① 개인정보 관련 법적 개념체계 정비
- 개인정보와 관련된 법적 개념체계는 개인정보, 가명정보, 익명정보로 구분하여 정비하기로 하였다. 그리고 익명정보는 개인정보보호법의 적용대상이 아니라고 합의하여 개인정보와 구분하였다.

② 익명정보 개념은 법에 명시하지 않음
- '익명정보'개념을 명확히 하기 위하여'익명정보'정의를 법에 명시하는 대신 EU GDPR 전문(26)을 참조하여'개인정보'의 개념을 보완하기로 논의하였다.

③ '가명정보'에 대한 법적 근거 마련
- '가명정보'의 정의 및 활용에 관한 법적 근거를 마련하기로 하였다.

④ 개인정보의 보호와 활용에 대한 지속적 논의 진행
- 개인정보 보호와 활용에 관한 주요 이슈들에 대해서 추가적인 논의를 진행하기로 하였다.

189) https://www.4th-ir.go.kr/topic/6/detail/11

190) https://www.4th-ir.go.kr/topic/7/detail/13

2차 해커톤에서 큰 틀에서의 합의는 이루어졌으나, 여러 의제에 대한 상세한 논의가 이루어지지 못했기 때문에 3차 해커톤에서 개인정보 이슈가 다시 다루어졌다. 가명정보의 활용과 보호, 익명처리의 절차·기준·평가 등, 데이터 결합, 개인정보 보호체계 등의 이슈가 토론되었는데, 이 모든 의제에 대해 합의가 도출된 것은 아니었다.

가명정보와 관련해서는 가명정보의 활용 목적과 범위가 쟁점이 되었다. 해커톤 합의사항을 보면 다음과 같이 되어있다.

3차 해커톤 합의 내용

가. 가명정보의 활용 목적과 범위

○ 가명정보는 ① 공익을 위한 기록 보존의 목적, ② [학술 연구 / 학술 및 연구]* 목적, ③ 통계 목적을 위하여 당초 수집 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다고 합의하였다.

* [학술 연구 / 학술 및 연구]: 연구의 범위에 관하여 이견이 있어 참석자 일부는 '학술 연구' 라는 표현을, 다른 일부는 '학술 및 연구'라는 표현을 지지하였다.

○ 그리고 이를 위해서는 가명처리를 포함한 기술적, 관리적 조치 등 안전조치가 취해져야 한다는 점에 동의하였다.

○ 위 [학술 연구 / 학술 및 연구] 목적에는 산업적 연구 목적이 포함될 수 있고, 통계 목적에는 상업적 목적이 포함될 수 있다는 점에 동의하였다.

나. 최초 수집목적과 양립되는 추가적인 개인정보 처리

○ 정부는 유럽연합 일반개인정보보호법(EU GDPR) 등 해외 입법례를 참조하여, 가명처리 여부 등 여러 사정을 고려하여 개인정보를 당초 수집한 목적과 상충되지 아니하는 목적으로 활용할 수 있도록 하는 제도를 마련한다는 점에 합의하였다.

시민사회 참석자들은 개인정보인 가명정보를 당초 수집 목적 외의 용도로 이용하거나 제3자에게 제공하는 것은 정보주체의 권리를 일정하게 제약하는 것임에도 불구하고, 이를 허용하는 것은 학술 연구 및 통계 작성이 사회 전체에 혜택을 주는 공익적인 가치가 있기 때문에 그 활용 범위를 '학술 연구 및 통계'로 제한해야 한다는 입장이었고, 반면 산업계는 빅데이터 산업 발전을 위해 산업적 연구 및 시장 조사 등으로 폭넓게 허용해

야 한다고 주장하였다.[191]

익명처리와 관련해서는 <개인정보 비식별조치 가이드라인>과 같이 특정 가이드라인에 따르면 무조건 익명정보라고 간주하는 것이 아니라, 정부가 익명처리의 적정성을 평가하기 위한 절차와 기준을 마련할 수 있되, 이러한 절차와 기준은 기술적 중립성에 입각한 것이어야 하며, 강제적인 것이거나 최종적인 것으로 해석되어서는 안 된다고 합의하였다.

그러나 데이터 결합과 관련해서는 합의에 이르지 못하였다. 시민사회는 데이터 연계는 개인정보 침해의 위험성이 높고, 해외에서는 민간 기업의 데이터를 결합하는, 그리고 이를 공공기관이 지원하는 사례를 찾기 힘들기 때문에 국내에서도 섣불리 허용해서는 안 된다는 입장인 반면, 산업계는 민간 기업의 데이터 연계도 허용하되 절차적인 통제방안을 마련하자고 주장하였기 때문이다.

개인정보 보호체계와 관련해서는 정보통신망법, 신용정보법, 위치정보법은 각 부문에서 고유하게 규정할 필요가 있는 사항을 제외하고, 개인정보 보호와 관련한 중복, 유사 조항에 대해서는 통일적 규율이 필요하다는 점에 합의하였으나, 구체적인 방안까지 논의하지는 못하였다.

그러나 해커톤은 사회적 논의를 위한 공간일 뿐 정책을 결정하는 곳은 아니기 때문에, 궁극적으로는 각 정부부처에서 해커톤에서의 합의를 반영하여 정책 방안을 수립하고, 국회에서 관련 법제를 개정해야 하는 과제가 남아있다.

2) 4차 산업혁명과 국회의 동향

(1) 국회 4차 산업특별위원회의 활동

2017년 11월 9일, 국회는 '4차 산업혁명 특별위원회'를 구성하였다. 다른 나라에 비해 한국은 4차 산업혁명에 대한 대응속도가 뒤쳐지고 있다고 진단하고, 국회 차원에서 이에 대응하기위한 정책 및 입법 권고를 하기 위한 것이다. 김성식 의원을 위원장을 맡은 국

191) 시민사회에서 학술 연구 목적에 산업적 연구 목적이 포함될 수 있다는 것에 합의한 것은 학술 연구가 대학에서 수행하는 연구 뿐만이 아니라 '학술적 가치가 있는 한' 산업적 연구의 일부도 포함될 수 있다는 의미이다. 관련하여 유럽연합의 일반개인정보보호규정(GDPR)은 전문(recital) 159에서 "과학적 연구 목적의 개인정보 처리는 기술의 발전과 실증, 기초연구, 응용연구 및 민간 투자 연구(privately funded research) 등을 포괄하는 광범위한 방식으로 해석되어야 한다"고 규정하고 있다.

회 4차 산업혁명 특위는 전체회의, 소위원회 회의, 정책간담회 등의 활동을 진행하였으며, 혁신·창업활성화·인적자본 소위원회(1소위)와 규제개혁·공정거래·사회안전망 소위원회(2소위) 등 2개의 소위원회에서 18개의 의제를 검토하였다. 18개 의제는 다음과 같다.

(1) 스타트업 생태계 활성화
(2) 기술벤처 육성 기반강화 프로젝트
(3) 대·중소·스타트업 기업간 개방적·협력적 혁신 시스템 강화
(4) 중소기업 혁신역량 강화 대책
(5) 국가 R&D 체계 혁신 및 연구 협업체계 개선방안
(6) 일자리 변화에 대응하는 직업훈련 및 평생교육체계 혁신과제
(7) SW 및 STEAM 교육 강화
(8) 융합형·협력적 인재 양성을 위한 교육개혁 과제
(9) 기술탈취 등 관련 징벌적 손해배상제도 강화 및 하도급 대책
(10) 데이터/네트워크/플랫폼 독점 대책 및 공정거래 강화를 위한 정책과제
(11) 개인정보 보호와 활용 방안
(12) 공공정보 공개 및 클라우드 활성화
(13) 블록체인의 응용확대 방안
(14) 신산업 및 신기술 활성화를 위한 규제개선
(15) 고용보험 제도의 획기적 강화 및 일자리 안전망 사각지대 해소 대책
(16) 기본소득 보장정책과 그 재원으로서 로봇세 도입 논의
(17) 일하는 저소득층을 지원하는 근로장려세제(EITC) 강화
(18) 고령층 및 장애인 등 취약계층을 위한 지능정보기술 개발추진
(출처: 국회 4차 산업혁명 특별위원회 활동결과보고서. 2018.5.)

2018년 5월 19일 활동을 종료한 특위는 <국회 4차 산업혁명 특별위원회 활동결과보고서>를 발표하였다.[192] 이 보고서에는 정책 및 입법권고안이 담겨있는데, 특히 개인정보의 보호와 활용 관련해서는 특별권고안으로 포함되어 있다. 이 권고안은 개인정보 보호와 활용에 관한 전향적인 규제 개혁이 필요하고 신뢰에 바탕을 둔 '개인정보의 안전한

192) http://blog.naver.com/PostView.nhn?blogId=okkimss&logNo=221288328368&redirect=Dlog&widgetTypeCall=true&directAccess=false

활용’의 실행이 시급하다며, 5건의 정책권고와 4건의 입법권고를 채택하였다.

[정책권고](5건)

① 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한법률」, 「위치정보 보호 및 이용 등에 관한 법률」, 「신용정보 이용 및 보호에 관한 법률」 등 개인정보를 규정하고 있는 법률에서 중복조항을 정비하고, 거버넌스에 대한 논의를 실시할 것

② 비식별화된 개인정보 활용 방안을 터주되 그 과정에서 고의적으로 재식별화 하거나, 의도하지 않았지만 재식별되는 데 소홀했을 경우 강력한 사후 처벌 방안을 마련해 개인정보를 보호할 것

③ 강력한 사후 규제를 전제로 익명가공정보도 적극 활용할 수 있도록 길을 터놓은 일본 기준을 참고해 개인정보 활용 수준을 검토할 것.

④ 과학기술정보통신부는 개인정보 활용에 대한 국민 불신을 안심시킬 수 있는 홍보 대책을 마련하고, 해외의 성공한 사례 중 개방적인 사례를 적극적으로 검토할 것

⑤ 현행 법률에서 정보주체의 동의 없이 개인정보를 수집·이용할 수 있는 상황을 구체화할 것

- 개인정보 활용의 이익형량에 관한 규정인 「개인정보 보호법」 제15조 제1항제6호 “개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우” 중 “명백하게”의 의미를 구체화하는 개인정보보호위원회의 해석 조치 필요

[입법권고](4건)

① 「개인정보 보호법」 및 관련 법률에서 개인정보·가명정보의 개념을 보다 구체화할 것

- 가명처리(가명화, 가명조치 등) 및 가명정보의 개념 정립

② 가명정보 개념을 신설할 경우, 정보주체의 동의 없이 가명정보를 목적 외 이용하거나 제3자에 제공할 수 있는 상황을 구체화할 것

- 공익을 위한 기록 보존, 학술 연구(산업적 연구 포함), 통계(상업적 목적 포함) 목적의 경우 가명정보의 목적 외 이용 또는 제3자 제공이 가능하도록 입법화할 것
- 가명처리 및 가명정보 결합 등을 안전하고 체계적으로 관리할 컨트롤타워를 갖춘 경우에는 상업적 목적으로 가명정보의 목적 외 이용 또는 제3자 제공이 가능하도록 입법화 할

것
- 단, 가명처리 방식·절차 등을 구체화하여 가명정보 자체의 식별가능성을 차단하고, 비식별화된 개인정보 활용 과정에서 고의적으로 재식별화 하거나, 의도하지 않았지만 재식별되는 데 소홀한 경우, 강력한 사후적 처벌 강화 조치를 전제로 함

③ 가명처리된 개인정보의 결합을 추진할 기관에 대한 근거를 가이드라인(현행)이 아닌 법률로 규정할 것

④ 행정안전부 산하인 개인정보보호위원회를 독립기구로 위상을 강화해 개인정보보호 방안을 총괄하고 전향적인 정보 활용 방안을 마련할 것

그러나 특위 내에서 이와 관련된 내용이 얼마나 충실하게 이루어졌는지는 의문이다. 특위의 특별권고안을 보면, "미국과 영국은 개인 신원이 드러나지 않게 처리된 정보를 '비식별정보', '익명정보'로 정의하고, 자유로운 활용을 제도적으로 보장하고 있음…. 하지만 한국은 엄격한 규제 일변도의 개인정보보호법 때문에 데이터 산업이 제대로 성장하지 못하고 있음. 부실한 개인정보 관리에 대한 불신, 이로 인한 개인정보 유출 피해의 심각성을 우려해 익명 정보조차 활용이 불가능함에 따라 혁신 서비스를 지향하는 산업계의 불만이 꾸준히 제기되고 있음"이라고 서술하는 등 특위 역시 기본적인 개념부터 혼란스럽게 사용하고 있기 때문이다. 사실 국내에서도 익명정보는 개인정보가 아니기 때문에 개인정보보호법의 적용을 받지 않고 있다.

국회 4차 산업혁명 특위의 정책 권고가 바로 정책이 되는 것도, 혹은 입법 권고대로 입법이 되는 것도 아니다. 입법의 경우 각 상임위원회에서 처리되어야 하는데, 특위의 권고가 참조될 수는 있을 것이다.

(2) 20대 국회에 발의된 개인정보 관련 법안 및 쟁점

<개인정보 비식별조치 가이드라인>에 대해 법적 근거가 없다는 비판이 제기되고, 해커톤을 통해 개인정보의 보호와 활용에 관한 논의가 진행되면서 국회에서도 이러한 논의를 반영한 법안들이 발의되기 시작하였다.

○ 비식별조치 개념 법제화

'비식별조치' 개념을 법에 수용하고자 한 법안에는 김병기(의안번호 2004238), 송희경

(의안번호 2007083), 김정우(의안번호 2012423) 의원이 각각 대표발의 한 개인정보보호법 개정안과 이은권(의안번호 2002160), 강길부(의안번호 2004602), 윤영석(의안번호 2006618) 의원이 대표발의 한 정보통신망법 개정안 등이 있다.

이 법안들은 <개인정보 비식별조치 가이드라인>의 주요 내용을 포함하고 있는데, 예를 들어 김병기 의원안의 경우 현행 개인정보보호법에서 통계작성 및 학술 연구 목적으로의 개인정보의 목적 외 활용을 규정하고 있는 제18조 2항 4호를 삭제하고 제22조의2(비식별정보의 이용·제공 등)을 신설하였다.

> 제22조의2(비식별정보의 이용·제공 등) ① 개인정보처리자는 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우에 한하여 개인정보를 전부 또는 일부 삭제하거나 대체하여 다른 정보와 결합하여도 개인을 알아볼 수 없도록 조치(이하 "비식별조치"라 한다)할 수 있다.

그런데 해커톤 논의에서 비식별 조치의 법적 모호성에 대해 공감하면서 개인정보와 관련된 법적 개념체계를 개인정보, 가명정보, 익명정보로 구분하여 정비하기로 합의한 만큼, 국회에서도 이러한 합의를 고려할 가능성이 높다. 앞서 언급했듯이, 개인정보보호위원회도 비식별 조치를 법제화하려는 위 법안들에 대한 검토 의견서에서 비식별 조치라는 용어를 '익명처리/가명처리'로 통일할 것을 권고하고 있다.

○ 가명정보의 활용 범위

학술연구 등의 목적을 위한 개인정보의 수집목적 외 제공과 관련하여는 오세정(의안번호 2012289), 진선미(의안번호 2012312) 의원이 대표발의 한 개인정보보호법 개정안에서 다루고 있다. 현재 개인정보보호법 제18조 2항 4호는 '통계작성 및 학술연구 등의 목적'을 위해 필요한 경우 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우에는 목적 외 이용 및 제3자 제공이 가능하도록 하고 있는데, 오세정 의원안은 '통계작성, 연구개발 및 시장조사 등의 목적을 위하여'로 그 범위를 더욱 확대하고 있다. 반면 진선미 의원안은 '통계작성 및 학술연구 등의 공익적 목적을 위하여'로 엄격히 제한하고 있다.

<표5-4> 국회발의 개인정보보호법 개정안 비교: 가명처리된 개인정보의 활용

현행 개인정보보호법	제18조(개인정보의 목적 외 이용·제공 제한) ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다. 4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
오세정 의원안	제18조 2항 4호 삭제 제22조의2(가명정보의 이용·제공 등) ① 개인정보처리자는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 통계작성, 연구개발 및 시장조사 등의 목적을 위하여 가명정보를 정보주체의 동의 없이 개인정보의 목적 외의 용도로 이용하거나 제3자에게 제공할 수 있다.
진선미 의원안	제18조 2항 4호. 4. 통계작성 및 학술연구 등의 공익적 목적을 위하여 가명정보를 제공하는 경우. 이 경우 가명정보의 제공은 제공의 목적과 관련성이 있다고 합리적으로 인정되는 범위에서 이루어져야 한다.
인재근 의원안(정부안)	제18조 2항 4호 삭제 제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다. ② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함하여서는 아니 된다. 제28조의3(정보집합물의 결합) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 개인정보처리자간 정보집합물의 결합은 대통령령으로 정하는 기준에 따라 보안시설을 갖춘 전문기관이 수행한다. ② 결합을 수행한 기관 외부로 결합된 정보집합물을 반출하려는 개인정보처리자는 제2조제1호다목 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다. ③ 제1항에 따른 결합 절차와 방법, 전문기관의 지정권자, 지정 및 지정취소 기준·절차, 관리감독, 제2항에 따른 반출 및 승인절차 등 필요

	한 사항은 대통령령으로 정한다.
이재정 의원안	제18조 2항 4호. 4. 통계작성 및 학술연구, 공익적 기록보존의 목적을 위하여 필요한 경우로서 제28조의2에따라 개인정보를 제공하는 경우 제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 학술연구, 공익적 기록보존을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다. 다만, 이 경우 더 이상 개인을 알아 볼 수 없는 익명처리로 목적을 달성할 수 있는 때에는 이에 의하여야 한다. ② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함하여서는 아니 된다.

개인정보보호위원회는 오세정 의원안에 대한 검토의견서[193]에서 “EU 일반 개인정보보호규정(GDPR)과 같이 정보주체에 대한 고지 의무와 관련된 조항의 적용을 제외하여 개인정보처리자가 해당 의무를 준수하기 위하여 가명정보를 재식별 해야만 하는 불합리한 모순점을 개선하는 등 전반적으로 적절한 개정으로 판단”되지만, 가명정보의 처리 목적에 연구 개발, 시장 조사 등을 포함하여 상업적 목적으로 활용할 수 있도록 명시적으로 규정하고 있는 것에 대해서는 “국내외적으로 가명정보의 상업적 활용 여부 및 범위 등에 대한 논란이 있는 점을 고려할 때 개정에 신중을 기할 필요”가 있다고 권고하고 있다.

한편, 같은 날 발표한 진선미 의원안에 대한 검토의견서[194]에서는 “‘공익’을 추가할 경우 가명정보 활용 범위가 ‘공익 목적의 통계작성 및 학술연구’로 축소될 수 있는데, 이 경우 기술발전 등에 기여하는 ‘상업적 목적의 연구’, ‘시장 조사’ 등을 원천적으로 차단하는 것으로 해석될 우려가 있어 신중한 접근이 필요”하다고 권고하고 있다. 즉, 개인정보보호위원회는 오세정 의원안의 경우 지나치게 가명정보의 활용 범위를 넓힌 것으로, 진선미 의원안은 좁게 설정한 것으로 보고 있다. 앞서 본 바와 같이, 가명정보의 활용범위와 관련해서는 시민사회와 산업계 간의 견해차가 존재하며, 국회에도 각각의 견해를 반영한 개정안이 발의되었다고 볼 수 있다.

193) 개인정보보호위원회 결정 제2018-08-079호. 「개인정보 보호법」 일부개정안 (의안번호 12289) 의견 조회에 관한 건. 2018.4.9.

194) 개인정보보호위원회 결정 제2018-08-078호. 「개인정보 보호법」 일부개정안 (의안번호 12312) 의견 조회에 관한 건. 2018.4.9.

정부는 애초에 산업적 연구를 포함한 개념으로 '연구'라는 용어를 사용[195]하고자 하였으나, 결국 발의된 개정안에는 '과학적 연구'라는 용어로 포함되었다. 그러나 법안의 제안이유에서 "새로운 기술·제품·서비스의 개발 등 산업적 목적을 포함하는 과학적 연구, 시장조사 등 상업적 목적의 통계작성, 공익적 기록보존 등의 목적으로도 가명정보를 이용할 수 있도록" 하겠다고 밝히고 있어, 기업들이 고객정보를 가명처리하여 판매 및 공유하는 것을 허용하고 있다는 시민사회의 비판을 받고 있다. 유럽에서는 연구 공동체와 데이터 거버넌스 체제가 오래 동안 형성되어 왔기 때문에 '과학적 연구(scientific research)'라는 개념의 의미하는 바가 명확할 수 있으나, 그러한 환경이 아직 성숙하지 않은 한국 사회에서 이 개념이 어떻게 활용, 혹은 남용될지 미지수이기 때문에, 과학적 연구 범위를 둘러싼 논란은 당분간 계속될 것으로 보인다.

(3) 20대 국회에 발의된 규제완화 관련 법안 및 쟁점

개인정보에 대한 규율을 다루는 개인정보보호법이나 정보통신망법과 별개로, 국회에는 사물인터넷, 자율주행자동차 등 신기술 혹은 새로운 사업모델을 활성화하기 위한 목적의 법안들이 다수 발의되었다. 이들 법안들은 기존의 규제가 혁신적인 기술의 개발 및 산업의 발전에 저해가 된다고 보고 특정 부문 혹은 지역에서 일부 규제를 완화해주는 것을 주 내용으로 하고 있다.

대표적인 것이 이학재 의원을 비롯하여 125명의 의원이 공동발의한 '지역전략산업 육성을 위한 규제프리존의 지정과 운영에 관한 특별법안'(의안번호 2000026)이다. 일명 '규제프리존법'이라 불리는 이 법안은 지역별 특성에 맞는 지역전략산업의 육성을 위하여 규제특례가 적용되는 구역을 '규제프리존'으로 정하고(제2조 2호), 법령에서 명확한 제한이나 금지가 있지 않는 한 지역전략산업 등을 허용하며(제4조 제1항), 규제프리존 내 특정 사업에 대해 특정한 규제를 완화해주는 것을 내용으로 하고 있다.

이 중에 개인정보와 관련된 조항도 포함되어 있는데, 자율주행자동차 산업을 위한 위치정보의 보호 및 이용 등에 관한 법률 적용 면제(제36조), 규제프리존 내 영상정보 수집에 대해 개인정보보호법 면제(제39조), 사물인터넷을 통한 수집 정보에 대한 정보통신망법 적용 면제(제40조) 등이 이에 해당한다.[196] 이들 조항은 '비식별화' 조치를 취하면 해

195) 한겨레. 정부, 가명정보 결합 데이터 외부반출도 허용 추진. 2018.9.18

당 법의 특정 조항이 적용되지 않도록 하고 있다.

규제프리존법안은 박근혜 정부 당시, 19대 국회에서 2016년 3월 24일 발의되었으나 임기만료로 폐기되었다가, 20대 국회가 출범 직후인 2016년 5월 30일 다시 발의되었다. 그러나 보건의료, 환경, 개인정보, 경제민주화 등 여러 영역의 시민사회단체들은 공동으로 이 법안에 대해 비판을 하였는데, 이 법안이 공공적 목적의 규제를 완화하여 시민의 생명과 안전, 공공성 침해 등의 위험성을 내포하고 있으며 법률의 명확성 및 원칙에도 위배되는 등 법률의 문제점도 심각하다는 것이다.[197] 특히 전경련 등 대기업들이 규제프리존과 관련된 규제완화를 요구하였고, 또 관련된 이권에 최순실이 개입한 정황이 드러나면서 규제프리존법은 최순실과 재벌의 이해관계를 위한 법이라는 비판이 더해졌다.[198] 박근혜 전 대통령이 탄핵되어 물러나고 2017년 초에 있었던 대통령 선거 과정에서도 문재인 후보와 안철수 후보가 규제프리존법을 둘러싸고 대립각을 세우기도 했었다. 문재인 후보측이 규제프리존법 통과에 찬성한 안철수 후보를 '이명박·박근혜 정권의 계승자'라고 비판했기 때문이다.[199]

그러나 문재인 정부에서도 '혁신 성장'이라는 기치 하에 더불어민주당이 다수의 규제

---

196) 제36조(「위치정보의 보호 및 이용 등에 관한 법률」 등에 관한 특례) 규제프리존 내 지역전략산업과 관련된 자율주행자동차 전자장비의 인터넷 주소를 이용하여 자동수집장치 등에 의해 개인정보 및 위치정보를 수집하고 수집한 개인정보에 대하여 데이터 값 삭제, 총계처리, 범주화, 데이터 마스킹 등을 통하여 개인정보의 일부 또는 전부를 삭제하거나 대체함으로써 특정 개인을 식별할 수 없도록 하는 조치(이하 "비식별화"라 한다)를 한 경우에는 「위치정보의 보호 및 이용 등에 관한 법률」 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 적용하지 아니한다.

제39조(「개인정보 보호법」에 관한 특례) 규제프리존 내 지역전략산업과 관련하여 역내사업자는 영상정보를 수집하여 특정개인을 알아볼 수 없도록 조치하는 경우에는 「개인정보 보호법」 제25조제1항에도 불구하고 시·도에서 정한 조례에 따라 영상정보처리기기를 설치·운영할 수 있다.

제40조(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 관한 특례) ① 규제프리존 내 지역전략산업과 관련하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제3호에 따른 정보통신서비스 제공자 중 역내사업자에 대하여는 규제프리존 내 설치된 사물인터넷 기반을 통하여 수집한 같은 법 제2조제6호에 따른 개인정보에 대하여 비식별화를 하는 경우에 같은 법 제24조 및 제24조의2를 적용하지 아니한다.

197) 건강권실현을위한보건의료단체연합 등. 시민사회, 규제프리존법 폐기 요구하는 의견서 발표. 2016.5.3.

198) 경제민주화실현전국네트워크 등. 최순실이 청탁한 규제프리존법 폐기 촉구 기자회견. 2017.2.28

199) 한국일보. 문재인-안철수의 새로운 전선, 규제프리존 법안. 2017.4.10.

완화 법안을 발의하였고, 야당에서도 규제프리존법과 서비스산업발전법 등의 통과를 요구하면서 다시 논란이 불거졌다.

더불어민주당은 '국민의 생명이나 안전, 환경을 저해하는 규제특례는 제한'하겠다면서도, '규제없이 신제품·신서비스를 테스트해 볼 수 있는 규제샌드박스 도입'을 내용으로 하는 규제혁신 5법을 발의한다고 밝혔다.[200] 규제혁신 5법은 행정규제기본법의 개정안(민병두 의원 대표발의, 의안번호 2012332), 금융혁신지원특별법 제정안(민병두 의원 대표발의, 의안번호 2012338), 산업융합촉진법 개정안(홍익표 의원 대표발의, 의안번호 2012342), 정보통신진흥및융합활성화법 개정안(신경민 의원 대표발의, 의안번호 2012348), 지역특화발전특구규제특례법 개정안(김경수 의원 대표발의, 의안번호 2012489)을 지칭한다.

규제혁신 5법은 신기술 도입 시 기존 법령에 공백이 있거나 불합리 할 경우 우선 허가를 내주거나, 제한된 범위에서 실험을 할 수 있도록 허용을 하는 방식으로 기존 규제의 일부를 완화시키는 내용을 포함하고 있는데, 여기에 개인정보 보호법제도 포함되어 있다. 산업융합촉진법 개정안, 정보통신 진흥 및 융합 활성화 등에 관한 특별법 개정안, 지역특화발전특구에 대한 규제특례법 개정안 등은 '개인을 식별할 수 있는 요소의 전부 또는 일부를 삭제하거나 대체함으로써 다른 정보와 결합하여도 더 이상 특정 개인 또는 개인의 위치를 알아볼 수 없도록 하는 조치를 한 경우'에는 관련 개인정보 보호법제에도 불구하고 이를 이용하거나 제3자에게 제공할 수 있도록 하고 있으며, 지정 검증기관으로부터 해당 조치의 적정성을 검증받도록 하고 있다. 또한, 금융혁신지원특별법 제정안은 혁신금융사업자에게 특례를 인정받는 부분에 대해 금융관련법령의 규정을 적용하지 않도록 하고 있는데, 금융관련법령에 개인정보보호법도 포함된다. 즉, 혁신금융사업자로 인정을 받으면 개인정보보호법의 일부 조항이 적용되지 않을 수 있다는 것이다.

이에 대해 시민사회단체들은 비판적 입장을 표명했는데, 산업융합촉진법 개정안 등에서 규정한 조치가 가명조치인지 익명조치인지 모호한데, 어느 정도의 조치인가에 따라 개인정보보호법의 적용 여부가 달라질 수 있다는 것이다. 또한 지정 검증기관의 검증을 통과할 경우 이것이 해당 업체에 대한 면책을 부여하는 것인지 역시 모호하다고 비판하고 있다. <개인정보 비식별조치 가이드라인>과 마찬가지로 자칫 검증기관이 제대로 검증

200) 더불어민주당 보도자료. 문재인정부 규제혁신 추진을 위한'규제혁신5법'발의. 2018.2.27

하지 않을 경우 개인정보 침해에 대해서도 책임을 면제해줄 수 있기 때문이다. 금융혁신지원특별법 개정안의 경우에는 개인정보보호법 자체를 배제한다는 점에서 더욱 비판을 받고 있다. 또한 해커톤 등을 통해 개인정보보호법에 개인정보의 보호와 활용에 대한 일반 원칙이 논의되고 있고 개인정보 보호법제의 정비도 되지 않은 상태에서, 이러한 예외적 조치를 먼저 추진하는 것은 적절하지 않다고 지적하였다.[201]

산업융합촉진법 개정안 및 정보통신 진흥 및 융합 활성화 등에 관한 특별법 개정안은 2018년 9월 20일 국회를 통과하였는데, 시민사회의 의견을 수용하여 개인정보 관련 내용은 삭제되었다. 그러나 지역특화발전특구에 대한 규제특례법 개정안은 관련 법안들을 병합하여 국회 산업통상자원중소벤처기업위원회 대안(의안번호 2015705)으로 통과되었는데, 여러 문제점을 포함하고 있어 비판을 받고 있다.[202] 보건의료, 환경 등 다른 분야의 문제는 차치하고 개인정보 관련 문제만 보더라도, '비식별' 개념 대신'가명처리'라는 개념을 사용하기로 사회적인 합의가 형성되고 있고 국회 역시 4차 산업혁명특위 활동을 통해 이 점을 인식하고 있음에도 불구하고 다시 '비식별' 개념을 도입하였다. 이에 따라, 비식별화 조치된 개인정보는 수집 목적 외로 자유롭게 이용하거나 제3자에게도 제공할 수 있도록 함으로써 개인정보의 목적 외로 남용될 우려가 있다. 시민사회는 기본법인 개인정보보호법의 개정이 논의되고 있는 상황에서 예외 조항을 먼저 신설한 것에 대해서 적절하지 않다고 비판하고 있다.

3. 지능형 감시에 대한 법제적 대응

신기술의 발전에 따라 국내 정보수사기관의 역량도 고도화되고 있으며, 이에 따른 인권 침해 논란도 불거지고 있다. 2014년 카카오톡 대화내용에 대한 압수수색 논란, 인터넷 패킷감청과 기지국 수사를 둘러싼 논란, 국가정보원의 해킹 프로그램 RCS 사용 논란 등이 대표적이다. 국내에서 역시 정보수사기관은 일반적인 개인정보 보호원칙의 예외를 상당히 인정받고 있으며, 투명한 감독 체제도 부재하기 때문에 정보수사기관의 감시 역량에 대한 정확한 실태조차 제대로 파악되지 않고 있는 상황이다. 또한 새로운 기술 환경

201) 경실련 등. [성명] 개인정보보호 무력화하는 규제 샌드박스 반대한다. 2018.8.16

202) 규제자유특구법(규제프리존법) 설명 기자 간담회. 2018.10.11. https://act.jinbo.net/wp/39689/

에서 정보수사기관의 활동이 어떠한 원칙과 절차에 따라 이루어져야 하는지에 대한 논의는 거의 이루어지고 있지 못하다. 다만, 2018년에 그간의 통신수사 관행에 대해 헌법재판소가 제동을 걸었기 때문에 2019년에는 현행 법제를 개선하기 위한 논의가 진행될 전망이다.

현재 수사기관의 통신 정보를 포함한 개인정보의 수집, 처리와 관련해서는 개인정보보호법, 전기통신사업법, 통신비밀보호법 등 다양한 법률에서 규정하고 있다. 아래에서는 범죄수사와 관련된 각 법률의 주요 내용 및 쟁점을 검토한다.

1) 수사기관의 개인정보 접근 및 처리

수사기관이 법 집행 목적으로 필요할 경우 개인정보에 접근할 필요성은 인정할 수 있을 것이다. 그러나 이는 법에 근거해야 하고, 필요성과 비례성 원칙에 부합해야 하며, 해당 개인에게 효과적인 구제조치를 제공해야 한다. 그러나 현행 개인정보보호법이 이러한 조건을 충족하고 있는지는 의문이다.

개인정보보호법은 제18조 제2항 7호에서 '범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우' 공공기관은 보유하고 있는 개인정보를 목적 외로 이용하거나 제3자 제공할 수 있도록 하고 있다. 제18조 제2항은 '정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때'에는 공공기관이 제공하지 않을 수 있는 여지를 남기고 있지만, 자의적인 판단에 의존할 수밖에 없다. 제18조 5항은 제3자에게 제공하는 경우 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청'하도록 하고, 요청을 받은 자는 개인정보의 안전성 확보를 위해 필요한 조치를 해야 한다고 규정하고 있다. 그러나 이러한 조치가 제대로 이루어지고 있는지 감독할 수 있는 메커니즘을 제공하지 않고 있다.

> 제18조(개인정보의 목적 외 이용·제공 제한)
>
> ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를

목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우

⑤ 개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

개인정보를 요구할 수 있는 범죄의 종류, 제공할 수 있는 정보의 범위 역시 한정되어 있지 않다. 또한 개인정보의 제3자 제공에 대해 (최소한 사후에라도) 해당 당사자에게 통지하는 절차도 없고, 따라서 정보주체가 자신의 권리구제를 요청하기도 힘들다. 따라서 수사기관은 필요에 따라 영장도 없이 피의자뿐 아니라 가족 등 다른 사람의 개인정보에도 자유롭게 접근할 수 있는 셈이다.

이와 관련되어 다음과 같은 사례가 발생한 바 있다. 지난 2014년 경찰은 철도 파업에 가담했던 노동자를 수사하는 과정에서 국민건강보험공단 등 공공기관으로부터 영장도 없이 철도노조 집행부와 가족의 개인정보를 제공받았다. 이에는 진료기록이나 처방내역 등 민감한 정보도 포함되어 있었다.[203] 또 다른 사례로는 2015년 12월 김포경찰서가 김포지역에서 일하고 있는 장애인 활동보조인들에 대한 대대적인 경찰조사를 하면서, 김포시청으로부터 200여명이 넘는 이용인과 활동보조인에 대한 개인정보를 제공받은 사례가 있다.[204] 두 사건의 당사자들은 이 조항이 영장주의 원칙, 명확성의 원칙, 최소침해의 원칙에 반한다며 헌법소원을 제기하였다.

2018년 8월 30일, 이 두 사건에 대한 헌법재판소의 결정이 있었는데, 철도노조 노동자의 건강보험 요양급여내역 수년치가 경찰에 제공된 사건[205]에 대해서는 위헌 결정을 내

203) 인권단체연석회의 공권력감시대응팀 등. 철도파업 휴대전화 실시간 위치추적 및 공공기관의 개인정보 경찰 제공에 대한 헌법소원 청구 기자회견. 2014.5.13

204) 경기장애인차별철폐연대 등. 김포경찰서·김포시청의 개인정보공유에 대한 헌법소원 청구 기자회견. 2016.6.14.

205) 진보네트워크센터 등. 철도노조 노동자의 건강정보 제공 사건, 위헌으로 확인되다. 2018.8.31.

린 반면, 김포경찰서와 김포시청의 활동지원관련 무작위 개인정보공유에 각하 및 기각 결정[206]을 내렸다. 헌재는 철도노조 사건에서는 건보공단이 보유하고 있는 요양급여정보가 건강상태에 대한 총체적인 정보를 구성할 수 있는 민감 정보로서 특별히 보호받아야 하고, 건강정보 제공으로 인한 개인정보자기결정권 침해가 매우 중대하다고 보았다. 또한, 경찰이 당시 청구인들의 소재를 파악하기 위해서 건강보험 정보를 제공받은 것이 불가피하지 않았고, 2년 또는 3년 치에 해당하는 건강정보를 제공받은 것은 침해의 최소성과 법익의 균형성을 침해한 행위로 보았다. 반면, 김포경찰서 사건에서는 그와 같은 판단을 하지 않았다.

두 사건 모두에서 헌재는 경찰에 개인정보를 제공한 법적 근거인 개인정보보호법 제18조 제2항 제7호 심판청구에 대해서는 각하로 결정하였다. 즉, 경찰이 정보 제공을 요청한 것은 강제력이 없는 임의수사에 해당하므로 영장주의가 적용되지 않으며, 개인정보의 제공 여부는 건보공단이나 김포경찰서와 같은 제공기관의 재량에 달린 문제라고 본 것이다. 그러나 제공기관의 경우에는 제공할 개인정보가 수사에 반드시 필요한 것인지 판단하기 힘들기 때문에 수사 기관의 요청이 있을 때 이를 거부하기 쉽지 않다. 공공기관이 보유한 막대한 개인정보에 대한 수사기관의 접근에 대해 그 남용을 방지할 수 있는 아무런 통제 절차가 없고 정보주체가 이의를 제기할 수 있는 수단 역시 없는 문제에 대해 헌법재판소는 아무런 답을 제시해주지 못했다.

정보수사기관이 보유하고 있는 개인정보 파일에 대한 감독이 제대로 이루어지고 있지 않은 점도 문제다. 개인정보보호법 제32조는 공공기관이 보유하고 있는 개인정보 파일을 행정안전부에 등록하도록 하고 있는데, 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일 및 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일은 예외로 하고 있다. 즉, 정보수사기관이 보유하고 있는 개인정보 파일은 행정안전부에 등록이 되어 있지 않기 때문에, 어떠한 개인정보를 어떠한 법적 근거 하에 얼마나 수집하고 있는지 제대로 감독할 수 있는 시스템이 부재한 상황이다.

---

https://act.jinbo.net/wp/39270/

206) 경기장애인차별철폐연대 등. 김포경찰서와 김포시청의 활동지원관련 무작위 개인정보공유에 대한 헌법재판소의 나쁜 결정을 규탄한다. 2018.9.16. https://act.jinbo.net/wp/39548/

2017년 10월, 국정감사에서 이재정 의원이 경찰청으로부터 제출받은 자료에 따르면,[207] 경찰청은 소속 기관을 포함하여 총 83개의 개인정보 시스템을 운영하고 있으며 총 37억여건의 개인정보를 보유하고 있다고 한다. 이 중 경찰청이 직접 운영하고 있는 개인정보 시스템은 50개, 보유 개인정보는 총 36억여 건이다. 가장 많은 개인정보를 보유하고 있는 시스템은 형사사법정보시스템(KICS)로서 27억여건의 개인정보를 보유하고 있으며, 이어 ▲교통경찰업무관리시스템(5억3000여건) ▲지문자동검색시스템(5387만여건) ▲지리적프로파일링(4079만여건) ▲수배차량검색시스템(3712만여건) 등의 순으로 나타났다. 문제는 이들 개인정보 시스템이 특별한 법적 근거가 있는 것이 아니라, 대부분 경찰법이나 경찰관직무집행법에 의존하여 운영되고 있다는 점이다.

빅데이터와 인공지능 등 신기술을 범죄 대응에 활용하기 위한 시스템 구축도 진행되고 있다. 2016년 12월 27일 정부부처 합동으로 발표된 <지능정보사회 중장기 종합대책>에 따르면, 추진과제의 하나로 '지능형 범죄 대응 시스템 구축을 통한 범죄 예방 및 검거역량 강화'를 명시하고 있다. 이에 따르면, 2022년까지 경찰청에서 운영 중인 각종 범죄 자료를 통합 DB화하고 분석하여 수사의 정확성을 높이는 범죄정보 통합분석 프로그램 구축, CCTV, IoT센서 등에서 수집되는 특이행동, 상황 등의 정보를 종합 분석하여 범죄발생 징후를 탐지·예방할 수 있는 시스템 개발 활용하겠다고 한다. 또한 2030년까지 제한된 정보(예: 측면촬영, 착모)만으로도 인공지능을 통해 용의자의 얼굴을 생성하고 특정할 수 있는 프로그램을 개발·적용하겠다는 계획이다. 실제로 경찰청은 2016년 초에 '빅데이터 기반 범죄 분석 프로그램 개발' 프로젝트를 발주를 공고했다.[208]

이러한 움직임과 관련하여 현재 국회에는 '범죄예방 기반 조성에 관한 법률안'(윤재옥 의원 대표발의, 의안번호 2001241)이 계류 중이다. 이 법은 범죄예방을 위한 환경개선 사업인 범죄예방디자인(CPTED: Crime Prevention Through Environmental Design) 개념을 도입하는 것인데, 10조에서 범죄예방정보통합정보시스템 구축을 명시하고 있다. 인권단체들은 이 시스템이 국가감시 시스템이 될 수도 있음을 우려하면서, 이 법안이 경찰에 과도한 권한을 부여하고 있다고 비판하고 있다. 공공안전을 위한 범죄 수사에 이와 같은 신기술의 도입이 필요하다고 할지라도, 권력기관에 대한 사회적 신뢰 획득을 위해서는

207) 중앙일보. 경찰, 개인정보 37억건 보유…형사사법정보시스템 27억건. 2017.10.15

208) 한겨레. 한국 경찰, '마이너리티 리포트' 만든다. 2016.2.4

권한 남용을 방지할 수 있는 감독과 통제 시스템이 함께 마련될 필요가 있다.

2) 통신수사와 통신비밀보호

인터넷 및 통신 서비스와 관련된 사용자의 정보는 전기통신사업자가 보유하고 있는 가입자정보인 통신자료, 송수신자나 송수신 시간 등 통신 내역에 관한 통신사실 확인자료, 그리고 통신 내용으로 구분된다. 그런데 수사기관이 각각의 정보에 접근하는 것과 관련해 모두 논란이 제기되고 있다.

첫째, 전기통신사업법 제83조 3항은 정보수사기관이 요청할 경우, 전기통신사업자가 보유하고 있는 이름, 주민등록번호, 주소 등 가입자 정보(통신자료)를 제공할 수 있도록 하고 있다. 법원의 영장 없이 요청사유, 해당 사용자와의 연관성, 필요한 자료의 범위를 기재한 서면으로 하면 된다. 이에 대해 헌법소원과 민사소송이 제기된 바 있는데, 2012년 헌법재판소는 통신자료 제공은 국가기관이 아니라 기업의 재량에 맡겨져 있어 이 조항만으로 기본권이 직접 침해된다고 볼 수 없다고 결정하였다.[209] 한편, 2016년 3월 대법원은 통신자료 제공에 기업의 손해배상 책임이 없다고 판결하였다.[210] 결국 사용자 입장에서는 통신자료를 제공한 기업과 제공받은 국가기관, 어느 쪽으로부터도 권리구제를 받을 수 없는 상황이 된 것이다. 그러나 그 이후에도 통신자료 제공은 지속적으로 논란이 되고 있는데, 시민사회는 이 조항이 과잉금지원칙과 명확성의 원칙, 영장주의 원칙 등을 위반했다며 재차 헌법소원을 제기한 상황이다.[211] 한편, 2014년 2월 10일 국가인권위원회는 정부에 가입자 정보를 통신사실확인자료처럼 법원 허가를 받아서만 취득할 수 있도록 하고 법원 허가를 “피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당사건과 관계가 있다고 인정할 수 있는 것”에 한정할 것을 권고하였다.[212] 그러나 정부는 이 권고를 불수용하였다.

둘째, 통신사실확인자료와 관련해서는 소위 ‘기지국 수사’와 실시간 위치추적 문제가

209) 2010헌마439

210) 대법원 2016. 3. 10. 선고 2012다105482 판결

211) 민주사회를위한 변호사모임 등. [기자회견] 통신자료 무단수집 피해자 5백 명 헌법소원 심판 청구. 2016.5.18

212) 국가인권위원회 결정.「 전기통신사업법」통신자료제공제도와「 통신비밀보호법」 통신사실확인자료제공제도 개선권고. 2014.2.10

논란이 되고 있다. 통신사실확인자료의 제공은 통신비밀보호법 제13조에 따라 이루어지는데, 검사나 사법경찰관이 관할 지방법원의 허가를 받아 전기통신사업자에게 요청하게 된다. 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분을 한 때에는 30일 이내에 그 사실을 당사자에게 통지하도록 하고 있다(제13조의3).

‘기지국 수사’는 특정 시간대에 특정 기지국에 접속한 모든 통신내역(통신사실확인자료)을 일괄 수집하는 수사기법이다. 시민사회는 기지국 수사가 집회 참가자에 대한 감시를 목적으로 악용되어 왔으며, 특정인에 대한 개인정보가 아닌 불특정 다수에 대한 개인정보를 수집하는 것은 저인망식 감시로서 위헌이라고 비판하고 있다.[213]

실시간 위치추적은 통신사가 특정인에 대한 (통신사실확인자료 허가 시점에서) 미래의 위치정보를 거의 실시간으로 수사기관에 제공하는 방식으로 이루어진다. 앞서 언급했던 2014년 철도 파업 가담 노동자에 대한 경찰 수사 과정에서도 조합원뿐만 아니라 그 가족의 휴대전화와 인터넷 사이트 접속 위치를 실시간으로 추적하여 논란이 되었다. 당사자들은 이에 대해서도 헌법소원을 청구하였는데, 통신사실확인자료에 대한 수사기관의 접근 범위를 통신사가 이미 보유하고 있는 과거의 통신내역에 한정하지 않고, 미래의 통신내역까지 확장하여 휴대전화의 실시간 위치추적을 가능하게 하는 것은 비례성 원칙에 위배된다는 것이다.

통신사실확인자료에 대한 법원의 허가는 감청에 비해 그 요건이 느슨하다. 예를 들어 통신제한조치(감청)의 경우에는 ‘법률에 열거된 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여’ 허가할 수 있도록 하고 있다.(통신비밀보호법 제5조 1항) 또한 통신제한조치가 가능한 범죄도 구체적으로 열거하고 있다. 반면, 통신사실확인자료의 경우에는 단지 ‘수사 또는 형의 집행을 위하여 필요’하면 범죄 피의자인지 여부를 불문하고 법원의 허가를 받아 요청할 수 있도록 되어 있다(통신비밀보호법 제13조).

2018년 6월 28일, 헌법재판소는 실시간위치추적과 기지국수사에 대해 헌법불합치 결정을 내렸다.[214] 이 결정은 2011년 희망버스 활동가들에 대한 실시간 위치추적(2건), 2012

213) 진보네트워크센터 등. [보도자료] 기지국수사에 대한 헌법소원 청구. 2012.6.14

214) 헌법재판소 2018. 6. 28. 선고 2012헌마191, 550(병합), 2014헌마357(병합) 전원재판부 결정

년 인터넷언론 참세상 기자에 대한 기지국 수사(1건), 2013년 철도노조 집행부에 대한 실시간 위치추적(1건) 사건 등 4건에 대해 함께 이루어진 것이다. 헌법재판소는 실시간 위치추적의 경우, '수사의 필요성'만을 그 요건으로 하여 절차적 통제가 제대로 이루어지지 못하고 있기 때문에 과잉금지원칙에 반하여 청구인들의 개인정보자기결정권과 통신의 자유를 침해하고, 정보주체에게 위치정보 추적자료 제공사실이 부실하게 통지되는 것 또한 헌법에 불합치한다고 보았다. 기지국수사의 경우, 수사편의 및 효율성만을 도모하면서 수사기관의 제공 요청 남용에 대한 통제가 충분히 이루어지고 있다고 보기 어렵기 때문에 헌법에 불합치하다고 보았다. 범죄와 아무런 관련도 없는 사람들의 정보를 대량으로 제공받는 것은 예외적으로 허용되어야 하며, 수사기관의 남용을 방지할 수 있는 여러 조치들을 마련하여 정보주체의 기본권 보장과 조화를 꾀하기 위한 방안이 마련되어야 한다는 것이다.

지금까지 통신사실확인자료의 침해적 성격을 통신내용보다 다소 낮은 것으로 간주해 왔던 것에 반대, 통신사실 확인자료는 비 내용적 정보이기는 하나 여러 정보의 결합과 분석을 통하여 정보주체에 관한 다양한 정보를 유추해내는 것이 가능하므로 통신내용과 거의 같은 역할을 할 수 있다고 헌법재판소가 인정한 것은 중대한 의미가 있다.

셋째, 통신내용의 감청과 관련해서는 패킷 감청이 논란이 되고 있다. 패킷감청이란 심층패킷분석(Deep Packet Inspection, DPI) 기법을 이용하여 인터넷 회선 전체에 대해 감청을 집행하는 것이다. 인터넷 회선 전체를 감청한다는 것은 이메일 뿐 아니라 대상자가 인터넷으로 통신하는 모든 내용, 예를 들어 자주 방문하는 사이트, 주로 소통하는 대상, 거래관계 등에 대한 내용을 감청할 수 있다는 점에서 사생활과 통신의 비밀과 자유에 대한 기본권을 심각하게 침해하게 된다. 특히 매해 두 번 발표되는 통신제한 및 통신사실확인자료 제공 현황에 따르면, 감청 건수 중 국가정보원의 감청 비율이 95% 이상에 달한다.[215] 패킷감청에 대해서도 헌법소원이 제기되었는데, 2011년 3월 29일 제기된 첫번째 헌법소원은 2016년 2월 25일 청구인 사망을 이유로 심판 종료가 선언되었다. 이후 2016년 3월 29일, 공안기구감시네트워크는 두 번째 헌법소원을 제기하였다.[216]

2018년 8월 30일, 헌법재판소는 패킷감청에 대해 헌법불합치 결정을 내렸다.[217] 법원의

215) 한국 인터넷 투명서 보고서 자료 참조. http://transparency.or.kr

216) 공안기구감시네트워크. 국가정보원의 '패킷감청'에 대한 두번째 헌법소원 청구 기자회견. 2016.3.29

허가범위를 넘어 수사기관이 취득하는 자료가 무한히 확대될 가능성이 농후하므로 기본권 침해를 최소화하기 위한 감독 내지 통제장치가 강하게 요구됨에도, 별다른 통제장치를 마련하지 않은 것은 위헌이라는 것이다.

한편, 유엔 시민적 정치적 권리규약 위원회(UN Human Rights Committee)는 2015년 11월 5일 한국의 자유권 보호실태를 검토하고 권고문을 발표하였는데, '사적 통신에 대한 사찰, 감시, 및 감청'(Monitoring, surveillance and interception of private communication) 분야에서 "42. 위원회는 전기통신사업법 제83조제3항에 따라 수사기관이 수사목적을 이유로 영장 없이 전기통신사업자에게 사용자 정보를 요구한다는 것에 대해 우려한다. 집회 참가자들을 특정하기 위한 소위 '기지국 수사'의 집행 및 이에 대한 불충분한 규제, 그리고 폭넓은 감청의 이용, 특히 국정원에 의한 감청과 이에 대한 불충분한 규제에 대해서도 우려한다"고 밝혔으며, 이어 "43. 대한민국 정부는 국가 안보를 위한 감시를 포함해 모든 감시가 규약에 부합하도록 보장하기 위해 필요한 법 개정을 하여야 한다. 특히 사용자 정보는 영장이 있을 때만 제공해야 하고, 국정원의 통신수사를 감독할 수 있는 기제를 도입해야 하며 기지국 수사가 자의적으로 이루어지지 않도록 보호수단을 강화해야 한다"고 권고한 바 있다.[218]

앞서 본 바와 같이 2018년 6월에는 실시간위치추적과 기지국수사에 대해서, 8월에는 패킷감청에 대해 헌법재판소는 헌법불합치 결정을 내렸다. 이에 따라 국회는 헌법에 부합하는 방향으로 현행 통신비밀보호법을 개정해야 하는 과제를 안게 되었다. 2020년 3월 31일까지 개정 입법을 해야 하므로, 2019년에는 국회에서 통신비밀보호법 개정 방안에 대한 논의가 진행될 것으로 예상된다.

전화 통신을 중심으로 한 시대에는 1:1 통신이 주류를 이루었지만, 최근에는 이메일과 SNS에서 볼 수 있는 바와 같이 일대다 혹은 다대다 통신이 일반화되고 있다. 다시 말해 수사기관이 통신 내용이나 기록에 접근할 때, 단지 피의자의 권리만 제한되는 것이 아니라 훨씬 많은 사람의 권리에 영향을 미칠 수 있는 것이다. 또한 사물인터넷 시대의 통신 개념은 과거의 통신 개념과 달라지고 있다. 즉, 사람과 사람의 통신이 아니라, 사람과 기

---

217) 헌재 2018. 8. 30. 2016헌마263

218) UN Human Rights Committee. Concluding observations on the fourth periodic report of the Republic of Korea. Adopted by the Committee at its 115th session (19 October-6 November 2015)

계, 기계와 기계의 통신이 일반화되고 있는 것이다. 물론 기계와 기계의 통신 역시 사물인터넷의 소유자, 사용자, 혹은 주변인 등 많은 개인과 연결될 수 있다. 이러한 상황에서 어디까지 '통신'으로 보아야하며, 보호의 대상이 되어야 하는지 근본적인 재검토가 필요하다.

제3절 시사점

해외 각 국은 빅데이터, 사물인터넷, 인공지능 등 새로운 기술 환경에 대비하여 개인정보를 보호하면서도 안전하게 활용할 수 있는 법제도적 장치를 마련하기 위해 노력하고 있다. 특히 유럽연합은 GDPR이라는 통일적인 개인정보 보호규범을 마련하여 유럽연합 역 내에서 개인정보의 원활한 이전과 개인정보의 활용을 촉진하면서도 새로운 환경 속에서 정보주체의 권리가 침해되지 않도록 하고 있다. 프로파일링을 포함한 자동화된 의사결정에 대한 거부권과 설명요구권, 개인정보이동권, 삭제권, 개인정보 보호 중심 디자인과 기본설정, 개인정보 영향평가, 국외 이전된 개인정보의 보호, 개인정보 침해에 대한 강력한 처벌 등이 그것이다. 또한 대부분의 유럽연합 국가들은 독립적인 개인정보 감독기구를 두고 개인정보보호법의 실효적인 집행을 보장하도록 하고 있다. 유럽연합은 전자통신 분야 및 범죄수사 영역에서도 기존 지침의 개정을 통해 GDPR에 준하는 수준의 보호를 제공하고 하고 있다. 특히 범죄수사 분야에도 독립적인 감독기구에 의한 감독을 요구하고 있는 점은 한국에 시사하는 바가 크다. 유럽연합은 개인정보에 대한 정보주체의 통제권을 기본권으로 인정하고 있고 공공과 민간을 포괄하는 단일한 개인정보보호법을 두고 있다는 점에서 한국과 유사하기 때문에 국내 개인정보보호법 개정 과정에서 참조할 필요가 있다.

그러나 한국은 새로운 기술 환경에 대비한 법제도의 구축이 한참 지연되고 있다. 이미 2013년경부터 빅데이터 등 환경 변화에 대비하기 위해 <공공정보 개방·공유에 따른 개인정보 보호 지침>, <빅데이터 개인정보보호 가이드라인> 등을 마련하였으나 법적인 근거가 없는 '비식별' 개념을 사용한다던가, 개인정보 보호법제의 개정이 아니라 정부 가이드라인을 통해 손쉽게 새로운 규범을 형성하려고 한 것이 오히려 사회적인 논란을 초래하고 법제 개선을 지연시키는 결과를 초래하였다. 결국 2018년에 와서야 해커톤을 통해 개인정보의 보호 및 활용에 대한 사회적 합의를 시도하고 개인정보 보호법제의 개선과 감독기구의 일원화를 논의하는 단계에 와있다.

이러한 혼란의 배경에는 국내 개인정보 보호법제와 감독기구가 분산되어 있는 현실이 존재한다. 행정안전부, 방송통신위원회, 금융위원회 등이 각자 자기 영역에서의 규범화를 추진하고, 국회에서도 소관 상임위원회에서 각각 법제 개선을 추진하기 때문에 통일적인

개인정보 규범수립에 한계가 발생하게 된 것이다. 이는 각 국의 개인정보 보호규범의 통일을 통해 단일 시장을 촉진하기 위해 GDPR을 제정한 것과 비교된다. 국내에서도 2011년 개인정보보호법 제정과 함께 정보통신망법, 신용정보법 등 관련 법제를 정비하고, 개인정보보호위원회를 독립적인 감독기구로 설립하였다면 보다 통일적인 개인정보 보호규범과 기술 환경에 조응한 발전된 논의를 진행할 수 있었을 것이다.

이에 신기술에 대응하기 위한 법제 개선을 위한 시사점을 다음과 같이 정리해볼 수 있다.

첫째, 우선 혼란스러운 개인정보 보호법제를 정비하고 개인정보 감독기구의 일원화를 시급하게 추진해야 한다. 여전히 국내에서는 빅데이터 등 산업 활성화를 위해 가명정보의 활용 범위를 어떻게 할 것인지에 대해서만 논란이 될 뿐, 프로파일링, 개인정보이동권, 개인정보 보호 중심 디자인과 기본설정, 개인정보영향평가, 개인정보 국외이전 등 중요한 논의는 학계에서만 간헐적으로 이루어지고 있을 뿐, 이에 대한 입법 논의는 시작도 못하고 있다. 이는 개인정보 보호에 대한 일관되고 효율적인 논의를 위한 컨트롤타워가 부재하기 때문이다. 기본적인 개인정보 보호체계가 정비되지 않는다면 부처간의 경쟁과 혼란만이 지속될 우려가 있다. 만시지탄이지만 문재인 정부에서 개인정보 보호체계 효율화를 위한 작업을 시작한 것은 다행이다.

둘째, 개인정보보호위원회를 중심으로 개인정보 감독기구를 일원화한 이후, 개인정보보호위원회는 여러 이해관계자와 함께 4차 산업혁명에 대응하는 새로운 규범에 대한 논의를 시작해야한다. 이는 프로파일링 등 몇 개 조항을 도입하는 것에 그쳐서는 안되며, 개인정보보호법 전체 체계의 연관성을 고려해야 할 것이다. 예를 들어, GDPR에서 과학적 연구 및 통계 목적 등으로 (가명처리된) 개인정보의 활용을 허용하는 것은 그만큼 정보주체의 권리와 정보처리자의 책임성 등 관련 조항의 뒷받침이 있기 때문이다. 한편, 국내에서는 제3조 개인정보보호원칙이 형해화되고 모든 개인정보처리자에게 관련 규정이 동일하게 적용되는 등 경직적인 부분이 있는데, 최근 국제적인 추세인 위험 기반(risk-based)의 접근, 비례적인 법률 의무, 개인정보처리자의 책임성 강화 조치 등을 고려할 필요가 있다.

셋째, 갈수록 지능화되는 국가 감시를 통제할 수 있는 절차와 감독체계가 마련되어야

한다. 그 동안 수사기관의 개인정보 접근 및 통신수사와 관련해서 많은 문제제기가 있었음에도 불구하고, 국회에서는 시대적 변화에 조응한 원활한 법 개정이 이루어지지 않았다. 다행히 2018년 헌법재판소는 공공기관 개인정보의 무영장 제공, 기지국 수사와 실시간 위치추적, 인터넷 패킷감청 등에 대해 헌법불합치 결정을 내렸고 이에 국회에서 관련한 법 개정이 이루어질 예정이다. 현재 국내 법제는 지능화된 국가 감시에 대한 대응은 고사하고, 정보수사기관의 개인정보 처리 실태의 투명성과 통신수사 과정에서의 인권 보호조치 등도 미약한 상황이다. 스노든에 의한 인터넷 대량 감시에 대한 폭로 이후, 유엔에서도 국가 감시를 감독할 수 있는 메커니즘을 마련할 것을 각 국에 촉구하고 있으며, 유럽연합은 적정성 심사 과정에서 국가 감시에 대한 통제 장치를 중요한 기준으로 삼고 있다. 이러한 국제적인 상황뿐만 아니라, 지능화되는 국가 감시로부터 국민들의 인권을 보호하기 위해서 국가 감시를 통제할 수 있는 적법 절차 및 감독 메커니즘이 구축되어야 한다.

넷째, 신기술에 의한 인권침해 문제에 대응하기 위한 종합적인 접근이 필요하다. 정보인권 보호를 위한 법제도는 당연히 필요하지만, 이것으로 충분한 것은 아니다. 여러 보고서에서 지적하고 있다시피, 학계를 비롯한 다양한 이해관계자의 합의를 통한 윤리 규범의 수립, 프라이버시 친화적인 기술의 개발, 기업들의 자율규제, 개발자·정책담당자·시민에 대한 교육 등이 함께 고려될 필요가 있다.

제6장 4차 산업혁명과 정보인권에 대한 관계 시민 및 관계 전문가 인식 조사

제1절 시민설문조사

1. 설문조사 개요

이번 연구 과제를 위해서 연구팀에서는 일반인들의 4차 산업혁명과 정보인권에 대한 인식조사를 진행했다. 설문조사는 2018년 10월 12일~16일 5일 동안 오픈서베이 패널(모바일 어플리케이션을 통한 응답 수집)을 대상으로 전국 1,000명의 시민들을 대상으로 진행하였다. 설문지는 사전에 연구팀에서 준비한 구조화된 설문지를 바탕으로 진행하였으며, 표본오차는 95% 신뢰수준 ±3.10%P이다.

먼저 설문응답자들의 기본적인 현황을 살펴보면, 성별로는 남녀 각 500명씩이며, 연령대는 29세 이하, 30대, 40대는 각 200명, 50대는 201명, 60세 이상이 199명이다. 지역은 수도권이 510명으로 절반을 조금 넘었으며, 강원권 30명, 충청권 100명, 영남권 250명, 제주를 포함한 호남권에서 110명이 조사에 응답하였다. 성별과 연령대는 사전에 연구팀과 리서치회사에서 표집인원수를 임의로 할당하였으며, 지역의 경우에는 지역별 인구수를 반영하여 할당표집을 하였다.

다음으로 학력별 분포를 확인한 결과 대학교 졸업이 512명으로 절반을 조금 넘었으며, 고졸 이하가 242명, 전문대졸 161명, 대학원졸 85명의 순서로 나타나고 있다. 직업의 경우에는 사무기술직이 245명으로 가장 많았으며, 다음으로 전업주부가 161명, 자유전문직 105명, 학생 96명, 자영업 90명의 순서로 나타나고 있다[219].

219) 직업별 분포에서 확인할 수 있듯이 기능직이나 판매영업서비스직 응답자가 상대적으로 낮고, 주부 응답자가 상대적으로 높다는 점을 염두에 두고 결과를 해석할 필요가 있다.

<표6-1> 응답자들의 인구사회학적 특성

		명	%			명	%
성별	남	500	50.0	학력	고졸 이하	242	24.2
	여	500	50.0		전문대졸	161	16.1
연령대	29세이하	200	20.0		대학교졸	512	51.2
	30대	200	20.0		대학원졸 이상	85	8.5
	40대	200	20.0	직업	사무기술직	245	24.5
	50대	201	20.1		기능작업직	55	5.5
	60세이상	199	19.9		자유전문직	105	10.5
지역	수도권	510	51.0		자영업	90	9.0
	강원권	30	3.0		판매영업서비스	63	6.3
	충청권	100	10.0		경영관리직	75	7.5
	영남권	250	25.0		전업주부	161	16.1
	호남권(제주)	110	11.0		학생	96	9.6
					무직	49	4.9
					기타	61	6.1
합계		1,000	100.0	합계		1,000	100.0

2. 문항별 인식조사 결과

정보인권에 대한 인식 설문조사에서는 가장 먼저 4차 산업혁명에 대해서 어느 정도 알고 있는가를 질문하였다. '전혀 들어본 적 없다'는 응답은 4.0%에 불과한 것으로 나타나 전반적으로 4차 산업혁명에 대해서는 어느 정도 인지하고 있음을 확인할 수 있다. 다만 4차 산업혁명의 의미나 세부적인 내용은 잘 모르는 응답자들이 많았고, '의미와 내용 모두 잘 알고 있다'는 응답자는 20.1%에 불과하였다.

주요 독립변수별로 확인한 결과 성별로는 남성이 여성보다 상대적으로 4차 산업혁명에 대해서 스스로 잘 알고 있다고 생각하는 비율이 높았으며, 연령대가 낮을수록 전반적으로 잘 이해하고 있다고 생각하는 응답자의 비율이 높았다. 그리고 지역별로는 수도권 응답자들이 4차 산업혁명에 대해서 잘 이해하고 있다고 생각하는 응답자 비율이 높다는

점을 확인할 수 있다.

<표6-2> 4차 산업혁명에 대한 이해 정도

		전혀 들어본 적 없다	용어는 들어봤으나 의미는 잘 모른다	의미는 알고 있으나 세부적인 내용은 모른다	의미와 내용을 잘 알고 있다	전체
성별	남	15 3.0%	104 20.8%	261 52.2%	120 24.0%	500 100.0%
	여	25 5.0%	172 34.4%	222 44.4%	81 16.2%	500 100.0%
연령	29세이하	8 4.0%	46 23.0%	91 45.5%	55 27.5%	200 100.0%
	30대	10 5.0%	47 23.5%	97 48.5%	46 23.0%	200 100.0%
	40대	5 2.5%	44 22.0%	114 57.0%	37 18.5%	200 100.0%
	50대	4 2.0%	64 31.8%	94 46.8%	39 19.4%	201 100.0%
	60세이상	13 6.5%	75 37.7%	87 43.7%	24 12.1%	199 100.0%
지역	수도권	18 3.5%	132 25.9%	230 45.1%	130 25.5%	510 100.0%
	강원권	0.0 0.0%	9 30.0%	20 66.7%	1 3.3%	30 100.0%
	충청권	6.0 6.0%	31 31.0%	55 55.0%	8 8.0%	100 100.0%
	영남권	9.0 3.6%	77 30.8%	118 47.2%	46 18.4%	250 100.0%
	호남권	7.0 6.4%	27 24.5%	60 54.5%	16 14.5%	110 100.0%
전체		40 4.0%	276 27.6%	483 48.3%	201 20.1%	1,000 100.0%

다음으로 4차 산업혁명에 대해서 전혀 들어본 적이 없는 40명을 제외한 960명에 대해 4차 산업혁명 기술을 응용한 6가지 기술/서비스를 실제 이용하거나 체험한 경험에 대해서 4가지 수준으로 보기를 구분해서 질문을 했는데, 기술/서비스별로 이용 경험의 정도에서 다소 차이를 보이고 있음을 확인할 수 있다. 스마트워치(삼성스마트워치, 애플워치

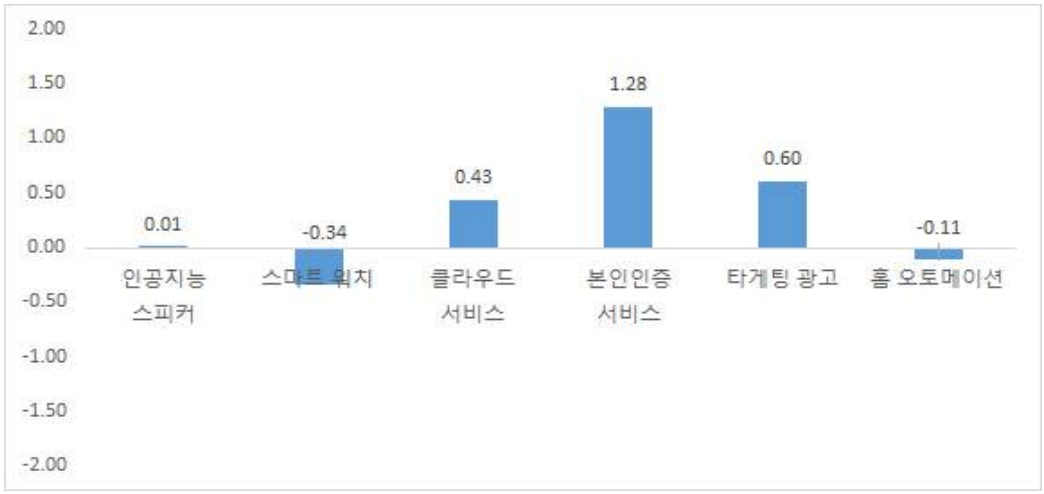
등)와 홈 오토메이션(스마트 홈 시스템, 놀이터 CCTV 등), 인공지능 스피커(기가지니, 빅스비, 누구 등)는 접해보지 못했다는 응답이 50%를 상회하였으며, 이 중에서도 스마트워치를 접해본 적이 없다는 응답자 비율이 65.8%로 가장 높게 나타나고 있었다.

<표6-3> 4차 산업혁명 응용 기술/서비스의 이용 경험

	인공지능 스피커 (기가지니, 빅스비, 누구 등)		스마트워치 (삼성스마트워치, 애플워치 등)		클라우드 서비스 (구글 드라이브, 아이클라우드 등)	
	명	%	명	%	명	%
아예 접해본 적이 없다	102	10.6	108	11.3	102	10.6
들어봤지만 접해본 적은 없다	409	42.6	523	54.5	296	30.8
가끔씩 접하고 있다	311	32.4	231	24.1	334	34.8
자주 접한다	138	14.4	98	10.2	228	23.8
합계	960	100	960	100	960	100
	본인인증서비스 (지문, 홍채, 안면 인식 서비스)		타게팅 광고 (구글 애드센스, 유튜브 추천 영상 등)		홈 오토메이션 (스마트 홈 시스템, 놀이터 CCTV 등)	
	명	%	명	%	명	%
아예 접해본 적이 없다	48	5.0	109	11.4	105	10.9
들어봤지만 접해본 적은 없다	227	23.6	227	23.6	436	45.4
가끔씩 접하고 있다	226	23.5	370	38.5	307	32.0
자주 접한다	459	47.8	254	26.5	112	11.7
합계	960	100	960	100	960	100

4차 산업혁명 기술을 활용한 대표적인 서비스에 대한 응답 결과를 수치화해 접해본 적이 없으면 (-), 접해본 적이 있으면 (+), 그리고 ± 내에서 경험 정도의 차이에 따라서 각각 1점과 3점으로 환산하여 평균값을 구해 6가지 기술/서비스에 대한 접근정도를 확인하였다. 6가지 기술/서비스 중에서는 본인인증 서비스(지문, 홍채, 안면 인식 서비스)

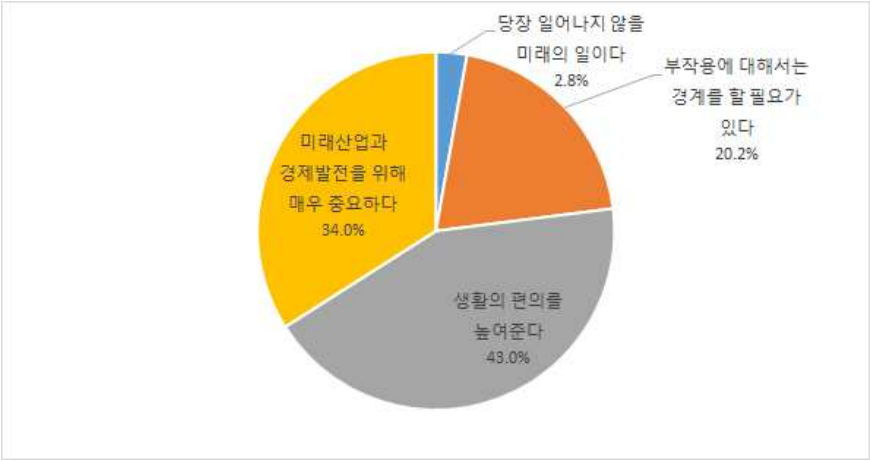
의 접근정도가 1.28로 가장 높았으며, 다음으로 타게팅 광고(구글 애드센스, 유튜브 추천 영상 등), 클라우드 서비스(구글 드라이브, 아이클라우드 등)의 접근정도가 각각 0.60, 0.43로 (+)로 나타났다. 반면 홈 오토메이션과 스마트 워치는 접근정도 값이 (-)로 나타나 상대적으로 대중적인 접근정도가 낮음을 확인할 수 있다.



<그림6-1> 4차 산업혁명 응용 기술/서비스에 대한 접근 정도

* 아예 접해본 적이 없다 -3, 들어만 봤다 -1, 가끔씩 접한다 1, 자주 접한다 3점으로 변환하여 평균값을 계산.

다음으로 응답자들에게 4차 산업혁명에 대해서 평소에 어떻게 생각하고 있는가를 질문하였는데, 생활의 편의를 높여준다는 응답이 41.0%로 가장 높게 나타났으며, 미래 산업과 경제발전을 위해 매우 중요하다는 응답도 34.0%로 두 번째로 많아 전반적으로 4차 산업혁명에 대해서 긍정적인 견해가 75%에 육박하고 있음을 확인할 수 있다. 반면 부작용에 대해서 경제를 할 필요가 있다는 신중론은 20.2%, 당장 일어나지 않을 미래의 일이라는 부정적 견해는 2.8%에 불과한 것으로 나타나고 있다. 이와 같은 결과는 전반적으로 4차 산업혁명이 다소 우려스러운 점이 있기는 하지만 4차 산업혁명을 피할 수 없을 뿐 아니라 중요하고 편리함을 제공할 것으로 기대하고 있다고 해석할 수 있을 것이다.



<그림6-2> 4차 산업혁명에 대한 견해

다음으로 정보인권에 대한 시민들의 인지 정도와 정보인권 보호에 대한 신뢰 정도를 질문하였는데, 응답자들은 신기술 서비스를 활용하여 개인정보가 수집되고 있다는 점에 대해서는 어느 정도 인지하고는 있었으나, 개인정보 보호에 대해서는 전반적으로 신뢰하지 않고 있음을 확인할 수 있다.

'인공지능 스피커, 스마트워치, 클라우드 서비스, 드론 등 신기술 서비스를 통해 귀하의 개인정보가 수집되는 경우가 있다는 것을 알고 있는가'라는 질문에 대해서 '대충 짐작하는 정도이다'가 43.8%로 가장 많았으며, 전체적으로 알고 있다는 응답이 모르고 있다는 응답보다 조금 높게 나타나고 있음을 확인할 수 있다(5점 척도로 환산한 값은 0.178).

<표6-4> 신기술 서비스를 통해서 개인정보가 수집되는 사실에 대한 인지도

	명	%	5점 척도 평균값
전혀 모르고 있다	101	10.1	0.178
별로 모르고 있다	90	9.0	
대충 짐작하는 정도이다	438	43.8	
조금 알고 있다	272	27.2	
아주 잘 알고 있다	99	9.9	
합계	1,000	100.0	

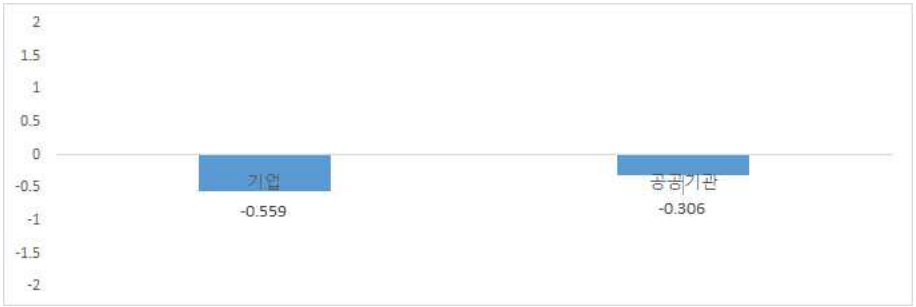
* 5점 척도는 '전혀 모르고 있다' ~ '아주 잘 알고 있다'를 각 -2, -1. 0, 1, 2점으로 변화해서 평균값을 계산.

다음으로 '포털서비스, 통신회사 및 보험회사 같은 기업들'과 '의료기관이나 정부기관 같은 공공기관들'이 수집한 사용자들의 개인정보를 보호하는 것에 대해 어느 정도로 신뢰하는지를 질문했는데, '보통이다'를 제외하면 기업과 공공기관 모두 전반적으로 신뢰한다는 응답보다는 믿을 수 없다는 응답이 조금 더 많아서 개인정보 보호에 대해 대체로 불신하고 있음을 확인할 수 있다.

<표6-5> 기업과 공공기관의 개인정보 보호에 대한 신뢰도

	기업들의 개인정보 보호		공공기관들의 개인정보 보호	
	명	%	명	%
전혀 믿을 수 없다	150	15.0	91	9.1
별로 믿을 수 없다	351	35.1	282	28.2
보통이다	419	41.9	486	48.6
조금 신뢰한다	68	6.8	124	12.4
매우 신뢰한다	12	1.2	17	1.7
합계	1,000	100.0	1,000	100.0

기업들과 공공기관들의 개인정보 보호 신뢰 정도에 대한 응답결과를 5점 척도로 환산하여 정보보호 신뢰도 점수를 -2점에서 2점의 폭으로 확인한 결과 기업과 공공기관 모두 정보보호 신뢰도 점수가 마이너스로 나타나 개인정보 보호에 대해 부정적으로 인식하고 있음을 확인할 수 있다. 특히 공공기관들(-0.306)보다는 기업들(-0.559)의 개인정보 보호에 대한 신뢰도가 낮다는 점을 확인할 수 있다.

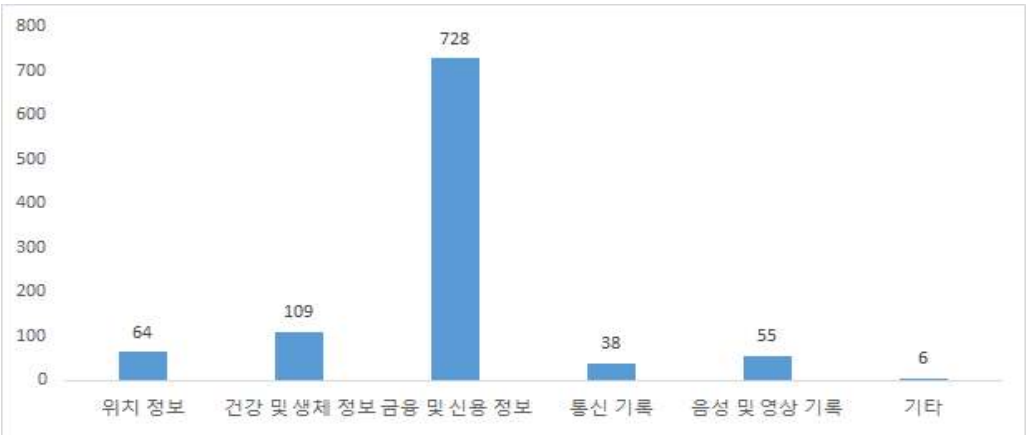


<그림6-3> 기업과 공공기관의 정보보호에 대한 신뢰도

* 신뢰도는 '전혀 믿을 수 없다' ~ '매우 신뢰한다'를 각 -2, -1. 0, 1, 2점으로 변화해서 평균값 계산.

현재 개인정보 보호 수준에 대해서는 전반적으로 신뢰도가 낮은 상태인데, '개인정보 중에서 가장 먼저 보호되어야 하는 것은 어떠한 정보라고 생각하는가'라는 질문에 대해서 응답자들은 '금융 및 신용정보'라는 응답이 728명으로 압도적으로 많았다. 다음으로 '건강 및 생체 정보' 109명, '위치정보' 64명의 순서로 나타나고 있다. 금융 및 신용정보를 가장 보호해야할 개인정보로 선택한 조사 결과는 금융/신용정보 노출로 인한 사고 뉴스 등을 많이 접하여 가장 일상생활과 밀접한 정보라고 판단하기 때문이라고 해석해야 할 것이다.

반면 아직까지 위치 정보나 건강 및 생체정보로 인한 피해는 구체적이지 않고, 통신 기록과 음성/영상 기록은 범인검거 등에 활용되면서 어느 정도 개인정보 활용에 대해서 긍정적으로 생각하기 때문이라고 해석할 수 있다.



<그림6-4> 가장 보호되어야 할 개인정보

다음으로 개인정보를 활용해서 제공되는 서비스들에 대한 견해를 질문하였다. 이번 설문조사에서는 구체적으로 다음의 4가지 서비스 <1) 온라인 쇼핑몰이나 온라인 서점에서는 사용자의 개인정보나 상품 조회 및 구매 이력을 활용해 '개인별 맞춤 광고'나 '상품 추천 서비스 2) 이동통신업체에서는 고객 자녀의 안전을 위해 자녀의 위치정보를 수집 및 활용한 '등하교 안심 서비스' 3) 자율자동차에서 운행 습관이나 위치, 동선 정보 등이 서비스 업체로 전송 4) 스마트 폰이나 스마트 의료 기기에 심박수 등 개인 생체 정보가

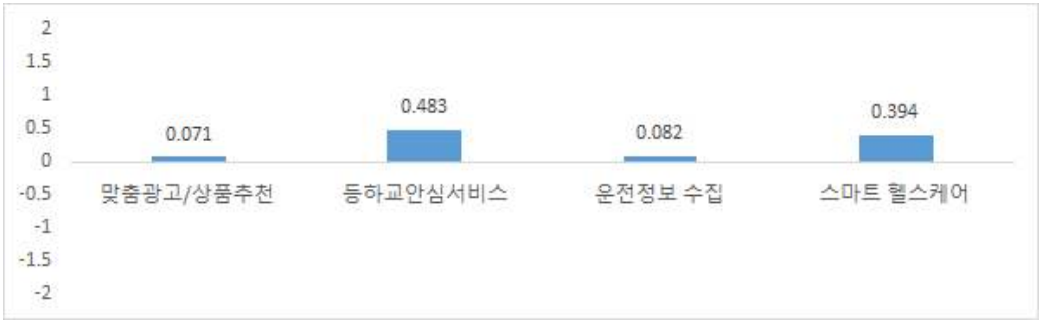
기록되고 전송되는 '스마트 헬스 케어'서비스>에 대해서 어떻게 생각하는가를 조사하였다.

전체적으로 개인 정보들을 활용하여 서비스를 제공하는 것에 대해서는 '보통이다'를 제외하면 어느 정도 긍정적으로 인식하고 있음을 확인할 수 있으며, 특히 '등하교 안심서비스'와 '스마트 헬스케어'에 대해서 상대적으로 긍정적인 인식이 높게 나타나고 있었다.

<표6-6> 개인정보를 활용한 서비스들에 대한 인식

	맞춤광고/ 상품추천		등하교 안심서비스		운전습관 동선수집		스마트 헬스케어	
	명	%	명	%	명	%	명	%
매우 부정적	55	5.5	38	3.8	67	6.7	35	3.5
다소 부정적	163	16.3	98	9.8	192	19.2	120	12.0
보통이다	476	47.6	339	33.9	392	39.2	364	36.4
약간 긍정적	268	26.8	393	39.3	290	29.0	378	37.8
매우 긍정적	38	3.8	132	13.2	59	5.9	103	10.3
합계	1,000	100.0	1,000	100.0	1,000	100.0	1,000	100.0

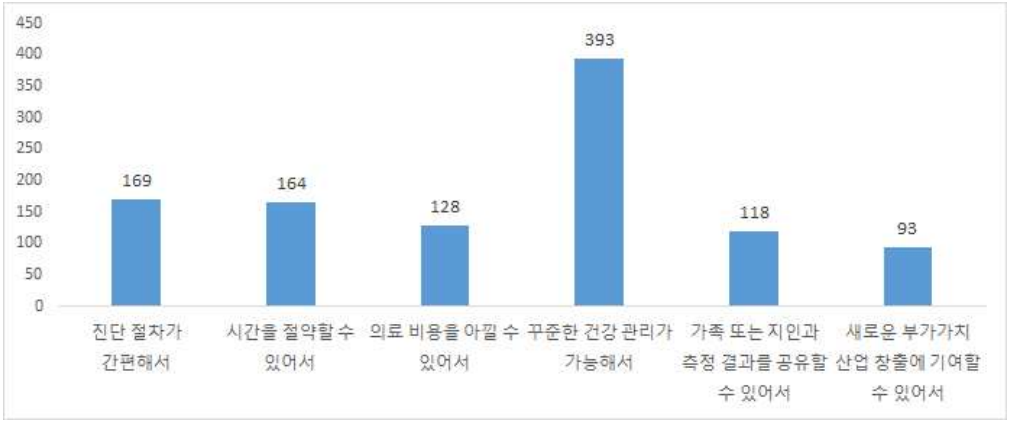
응답결과를 5점 척도로 환산하여 평균값을 구한 결과 4가지 서비스 모두 플러스(+)로 나타나고 있어서 다소 긍정적임을 확인할 수 있으며, 등하교 안심서비스의 환산값이 0.483으로 나타나 4가지 개인정보 활용 서비스 중에서 가장 긍정적으로 인식하고 있었으며, 스마트 헬스케어가 0.394로 두 번째로 긍정적으로 인식하고 있었다. 운전정보 수집은 0.082, 맞춤광고와 상품추천은 0.071로 상대적으로 가장 낮게 나타나고 있다. 개인 정보를 활용하여 안전과 건강수준 향상에 직접적으로 도움이 될 것이라고 기대할 수 있는 서비스에 대해서는 대체로 긍정적인 응답이 높게 나타나고 있음을 확인할 수 있다.



<그림6-5> 개인정보를 활용한 서비스들에 대한 응답 결과

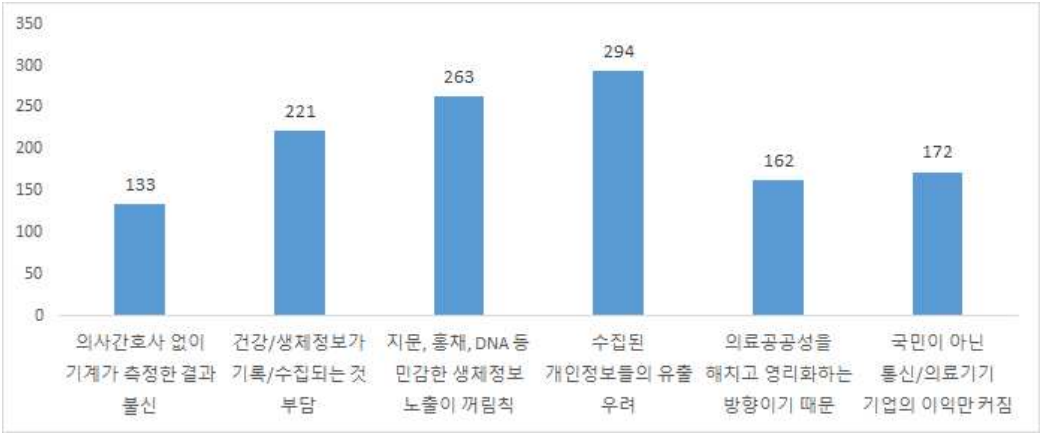
* '매우 부정적' ~ '매우 긍정적'을 각 -2, -1. 0, 1, 2점으로 변화해서 평균값 계산.

그리고 스마트 헬스케어 질문에 대해서는 긍정적인 응답자들과 부정적인 응답자들에게 각각 그렇게 생각하고 있는 이유는 무엇인지에 대해서 추가로 질문하였다. 긍정과 부정 이유를 각 6개씩 보기를 제시하고 중복 응답이 가능하도록 하도록 하였다. 스마트 헬스케어 시스템에 대해서 '꾸준한 건강관리가 가능해서'를 선택한 응답자가 393명으로 긍정적으로 생각하는 가장 큰 이유로 꼽고 있었으며, 다음으로 '진단절차가 간편해서', '시간을 절약할 수 있어서'라는 이유가 많았으며, '새로운 부가가치 산업 창출에 기여할 수 있어서'이라는 응답은 93명으로 상대적으로 가장 적었다. 스마트 헬스케어 시스템에 대해서 산업적인 차원에서의 필요성보다는 개인들의 건강수준 향상에 도움이 되는 관점에서 이해하고 있음을 확인할 수 있다.



<그림6-6> 스마트 헬스케어 시스템에 대해 긍정적으로 판단하는 이유(중복응답)

스마트 헬스케어 시스템에 대해서 부정적으로 판단하는 이유에 대해서는 '수집된 개인정보들의 유출 우려'가 294명으로 가장 많았으며, 다음으로 '지문, 홍채, DNA 등 민감한 신체정보 노출이 꺼림직'하다는 이유를 선택한 이들이 263명으로 두 번째로 많았으며, '건강/생체정보의 기록/수집되는 것이 부담'은 221명이 선택하여 세 번째였다. 스마트 헬스케어에 대해 부정적으로 생각하는 원인은 전반적으로 스마트 헬스케어 시스템을 통한 정보수집 및 유출에 대한 우려가 가장 크다는 점을 확인할 수 있다.



<그림6-7> 스마트 헬스케어 시스템에 대해 부정적으로 판단하는 이유(중복응답)

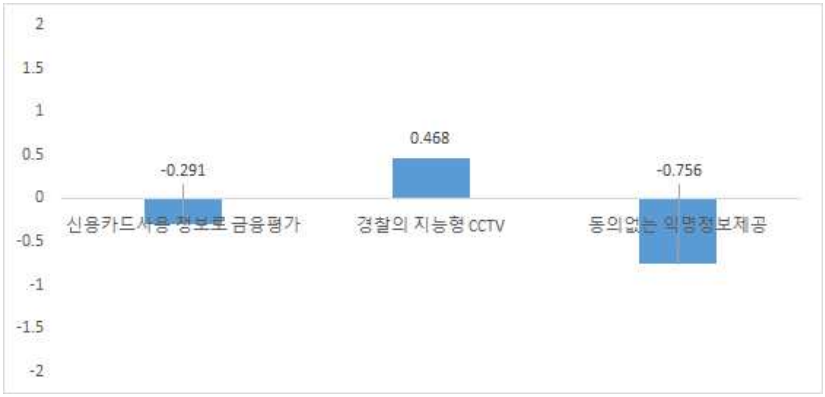
다음으로 개인들에게 직접적으로 수집된 정보들을 재가공하여 사용하는 것에 대해서 응답자들은 어떻게 생각하는가를 질문하였다. 여기서 활용된 재가공 사례는 1) 신용카드 사용정보를 활용한 신용도 평가 2) 경찰의 지능형 CCTV를 활용한 범죄 예방 3) 수집된 개인정보를 동의없이 익명/가명 처리하여 활용하는 것 3가지였다.

응답결과 '신용카드 정보의 신용평가 활용'과 '가공된 개인정보를 동의없이 가명/익명으로 제공'하는 것에 대해서는 부정적인 응답들이 상대적으로 많았으며, '경찰의 지능형 CCTV 설치'에 대해서는 상대적으로 긍정적인 응답이 많다는 점을 확인할 수 있다.

<표6-7> 수집된 개인정보들을 동의 없이 활용하는 것에 대한 견해

	카드사용정보를 통해 신용평가에 활용		범죄예방 목적의 경찰의 지능형 CCTV		가공된 개인정보를 동의없이 익명제공	
	명	%	명	%	명	%
매우 부정적	113	11.3	46	4.6	312	31.2
다소 부정적	270	27.0	116	11.6	288	28.8
보통이다	431	43.1	324	32.4	260	26.0
약간 긍정적	167	16.7	352	35.2	124	12.4
매우 긍정적	19	1.9	162	16.2	16	1.6
합계	1,000	100.0	1,000	100.0	1,000	100.0

응답결과를 긍정과 부정을 구분해서 평균값을 구한 결과 경찰의 지능형 CCTV 설치에 대해서는 (+) 0.468점으로 긍정적으로 생각하고 있었으나, 신용카드 사용정보를 이용한 신용도 평가에 대해서는 (-)0.291, 동의 없는 익명/가명 정보제공에 대해서는 (-)0.756으로 부정적으로 생각하고 있었다. 특히 동의를 얻고서 수집한 개인정보라고 하더라도 이를 익명으로 처리한 이후에 동의 없이 활용하는 것에 대해서는 매우 부정적임을 확인할 수 있다. 아울러 지능형 CCTV를 통해서 수집된 개인정보를 범죄예방 목적으로 활용하는 것에 대해서는 긍정적인 응답이 매우 높게 나타나고 있는데, 개인 및 공동체의 안전수준 향상을 위해서라면 개인정보를 수집하고 활용하는 것에 대해서는 용인할 수 있다는 태도를 보이고 있다고 해석할 수 있다.

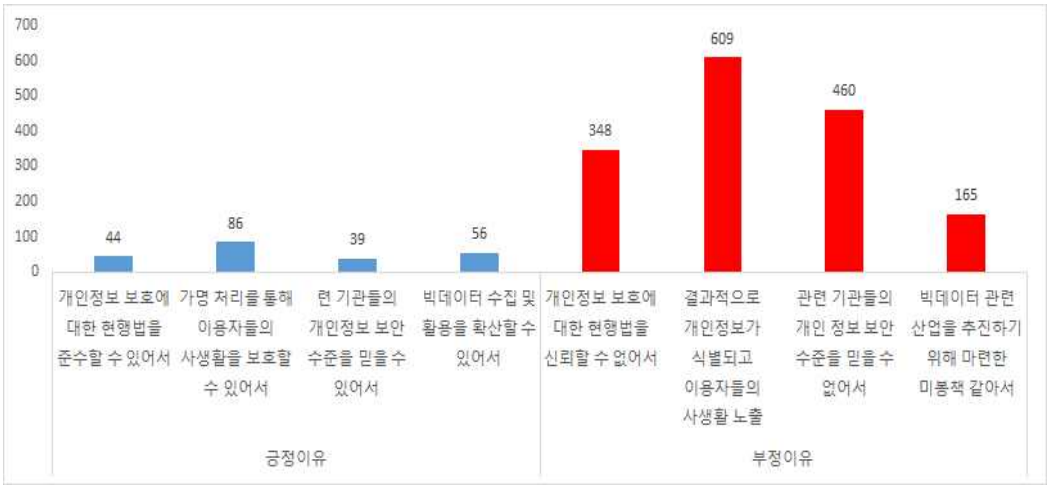


<그림6-8> 수집된 개인정보들을 동의 없이 사용하는 것에 대한 점수

* '매우 부정적' ~ '매우 긍정적'을 각 -2, -1. 0, 1, 2점으로 변화해서 평균값 계산.

다음으로 앞서 스마트 헬스케어와 마찬가지고 '수집된 개인정보를 가명/익명으로 처리해서 동의 없이 제공하는 것'에 대해서 긍정적 또는 부정적 이유를 추가로 질문한 결과(중복응답), 우선 긍정적인 이유보다는 부정적인 이유들이 훨씬 많아 전반적으로 개인정보들을 재가공 하더라도 이를 무단으로 활용하는 것 자체에 대해서는 부정적이다.

긍정적인 이유 중에서는 '가명처리를 통해서 사생활이 보호할 수 있다'는 응답을 86명이 선택하여 가장 많았으며, 두 번째로는 '빅데이터 수집/활용에 대한 신뢰'한다는 응답자가 56명이었다. 반면 부정적인 이유로는 '결과적으로 개인정보가 식별되고 사용자들의 사생활이 노출'되는 것에 대한 우려가 609명으로 압도적으로 많았으며, 가명정보를 받은 '관련 기관들의 개인정보 보안 수준을 믿을 수 없어서'라는 응답자가 460명으로 두 번째로 많았다.



<그림6-9> 개인정보를 가명/익명으로 동의 없이 제공하는 것에 긍정/부정 이유(중복응답)

최근 기업에서도 4차 산업혁명의 영향으로 진전된 기술을 인사노무 관리에 활용하려는 시도들이 일부 분야에서 나타나고 있다. 대표적으로 인공지능(AI)을 활용한 면접과 퇴근 후에 SNS나 이메일을 통한 업무지시를 들 수 있다.

취업 현장에서는 인공지능이 면접자의 표정, 목소리, 뇌파, 심장박동 등 감지하는 시스

템이 일부 도입되고 있는데, 취업 면접을 볼 때 인공지능이 면접의 당락을 좌우한다면, 이에 대해서 어떻게 생각하는지를 질문하였다. 응답 결과는 전반적으로 부정적으로 생각한다는 응답이 많았으며, 응답결과를 -2점 ~ +2점의 범위의 점수로 확인한 결과 -0.632로 나타나 전체적으로 기업들의 인공지능 면접에 대해서는 다소 부정적임을 확인할 수 있다.

<표6-8> 인공지능이 입사에 당락을 좌우할 경우 응답자들의 견해

	명	%	5점 척도 평균값
매우 부정적으로 생각한다	251	25.1	-0.632
다소 부정적으로 생각한다	295	29.5	
보통이다	311	31.1	
약간 긍정적으로 생각한다	121	12.1	
매우 긍정적으로 생각한다	22	2.2	
합계	1,000	100	

* '매우 부정적' ~ '매우 긍정적'을 각 -2, -1. 0, 1, 2점으로 변화해서 평균값 계산.

다음으로 직장생활 경험이 있는 응답자 868명을 대상으로 휴일 또는 퇴근 이후 휴대전화(스마트기기) 또는 이메일 등을 통해 업무관련 지시를 받거나 전달한 경험을 질문했는데, '가끔씩 경험하고 있다'는 응답이 370명(42.6%)로 가장 많았으며, '자주 경험하는 일이다'는 응답도 133명(15.3%)이었다. 그리고 휴일/퇴근 후 업무지시를 받은 적이 전혀 없다는 응답은 170명(19.6%)에 불과한 것으로 나타나고 있다.

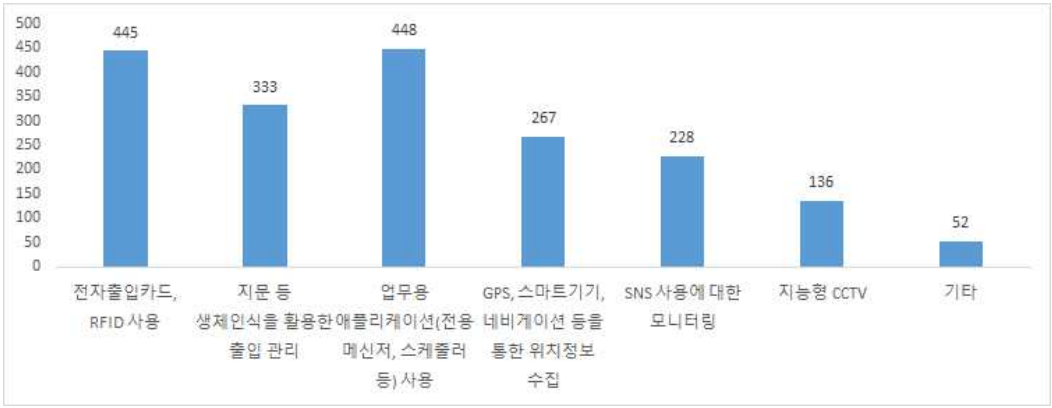
주부나 자영업자, 무직 등이 포함된 경우 응답결과가 차이가 있을 것으로 예상되어 현재 직장인들만을 대상으로 휴일/퇴근 후 스마트기기를 통한 업무지시 경험을 확인한 결과 경험하고 있다(가끔씩 및 자주)는 응답이 65.4%로 현재 직장인 중에서는 약 2/3 정도가 업무시간 이외에 업무지시를 받은 경험이 있었다.

<표6-9> 휴일/퇴근 후 스마트기기를 통한 업무지시 경험

	전체		현재 직장인*	
	명	%	명	%
전혀 그렇지 않다	170	19.6	70	13.2
그렇지 않은 편이다	195	22.5	114	21.4
가끔씩 경험하고 있다	370	42.6	258	48.5
자주 경험하는 일이다	133	15.3	90	16.9
합계	868	100	532	100.0

* '현재 직장인'은 직업에서 자영업자, 주부, 학생, 무직, 기타를 제외한 응답자만 선택

다음으로 직장생활을 하면서 경험한 4차 산업혁명과 관련된 신기술의 유형들을 체크하게 한 결과(중복응답 가능) 전용 메신저, 스케줄러, 업무관리 프로그램 등 업무용 애플리케이션이 448명으로 가장 많았으며, 전자출입카드, RFID 사용도 445명으로 거의 비슷한 수준으로 많았다. 생채인식 정보를 활용한 출입관리도 333명이었으며, SNS 사용 모니터링은 228명으로 상대적으로 적었으며, 지능형 CCTV는 가장 적었다. 다만 SNS 사용 모니터링의 경우에는 실제로 이루어지고 있음에도 불구하고 응답자들이 인식하고 있지 못할 가능성이 있다.



<그림6-10> 직장생활을 하면서 경험한 신기술 유형(중복응답)

신기술을 활용한 인사관리 및 조직관리 전반에 대해서 어떻게 생각하는가를 질문에 대해서는 전체적으로 긍정적으로 생각한다는 응답(약간 및 매우)이 상대적으로 더 많았으며, 그 결과 전체적인 응답결과도 약간 긍정적(0.099)인 것으로 나타나고 있다. 위의 스마트기기를 활용한 업무지시 경험과 마찬가지로 현재 직장인들만 선택하여 확인한 결과 부정적으로 생각하는 응답자의 비율이 상대적으로 조금 더 높아서 5점 청도의 평균은 0.077로 조금 낮아졌다. 직장인들이라고 하더라도 기업에서 신기술을 활용한 인사 및 조직관리에 대해서는 약간 긍정적이라고 할 수 있는데, 이는 정보기술을 통한 노동과정 및 인사관리에 대한 통제에 대한 인식보다는 업무용 메신저 등을 활용한 업무의 편리성이나 전자출입카드를 통한 보안과 안전에 대한 긍정적인 인식이 많기 때문이라고 할 수 있다. SNS 사용에 대한 모니터링이나 지능형 CCTV 경험이 상대적으로 낮은 것도 이와 같은 결과에 어느 정도 영향이 있을 것으로 짐작할 수 있다.

<표6-10> 4차 산업혁명 신기술을 활용한 인사 관리 및 조직 관리 견해

	전체		현재 직장인*	
	명	%	명	%
매우 부정적으로 생각한다	51	5.1	33	6.1
다소 부정적으로 생각한다	155	15.5	82	15.1
보통이다	490	49.0	260	47.9
약간 긍정적으로 생각한다	252	25.2	146	26.9
매우 긍정적으로 생각한다	52	5.2	22	4.1
합계	1,000	100.0	543	100.0
5점 척도값	0.099		0.077	

* '현재 직장인'은 직업에서 자영업자, 주부, 학생, 무직, 기타를 제외한 응답자만 선택

현재 4차 산업혁명의 신기술은 시민들의 삶을 편리하게 하고 경제 발전에도 도움을 준다는 입장과 반면 이 때문에 시민들의 정보인권이 억제될 위험이 있다는 입장이 공존하고 있는 상황인데, 응답자들은 4차 산업혁명과 정보인권 중에서 어느 쪽에 더 중점을 둘 것인지, 아니면 균형이 필요하다고 생각하는지를 5개 문항을 보기로 제시하면서 질문

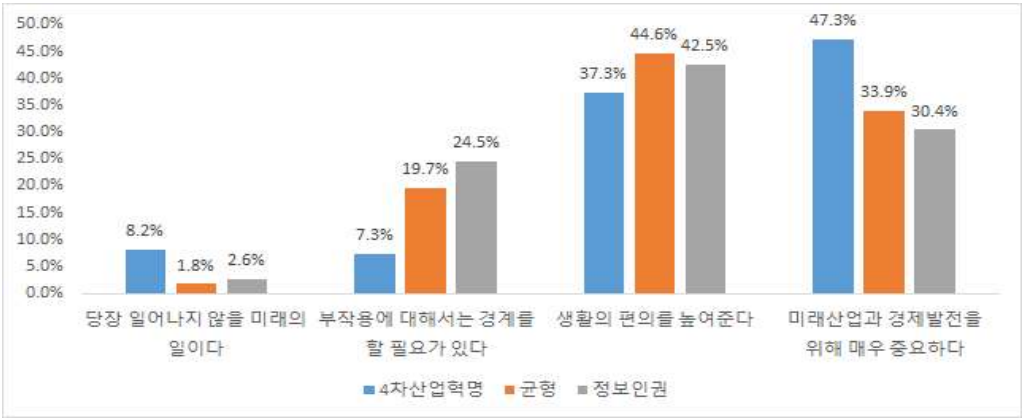
하였다.

응답 결과는 '둘 모두 균형적으로'라는 응답이 502명으로 가장 많았는데, 이를 제외했을 때 정보인권이 중요하다(우선적 및 최우선)는 응답자가 388명, 4차 산업혁명이 중요하다(우선적 및 최우선)는 응답자가 110명으로 정보인권을 보다 중요하다는 인식이 한국사회에서는 좀 더 우세하다고 할 수 있다. 4차 산업혁명과 정보인권 모두 우선적, 최우선으로 강도를 파악하는 문항으로 구분되어져 있기에 최우선을 2점, 우선적을 1점으로 차이를 두고 4차 산업혁명을 -로, 정보인권을 +로 해서 응답인원수로 평균값을 구해본 결과 0.374점으로 응답자들은 전반적으로 정보인권을 보다 중요하게 생각하고 있음을 확인할 수 있다.

<그림6-11> 4차 산업혁명과 정보인권 중 우선하는 가치

* 정보인권(+)과 4차 산업혁명(-)과 최우선(2), 우선적(1)으로 평균점수: 0.374

아울러 4차 산업혁명에 대한 견해를 4차 산업혁명을 중요시하는 그룹, 균형 그룹, 정보인권 중요시하는 그룹으로 구분해서 비교한 결과 4차 산업혁명을 중요하게 생각하는 그룹은 산업과 경제 차원에서 중요성을 강하게 인식하고 있었으며, 정보인권을 중요하게 생각하는 그룹은 상대적으로 부작용에 대해서 경계할 필요가 있다는 응답비율이 상대적으로 높았다. 산업적 관점을 강조하는 그룹과 인권을 중요하게 생각하는 그룹 간의 4차 산업혁명에 대한 견해 차이를 확인할 수 있었다.



<그림6-12> 4차 산업혁명에 대한 견해를 4차 산업혁명과 정보인권에 대한 입장으로 구분

신기술과 정보인권이 충돌할 수 있는 상황에서 이를 개선하기 위해 사회적으로 고민되고 있는 4개의 정책들을 보여주고 각 정책안들에 대해서 응답자들의 견해를 5점 척도로 질문하였다. 4개의 정책안들은 다음과 같다. 1) 4차 산업혁명의 성공을 위해서 정보인권 보호를 목적으로 하는 '규제를 완화'한다. 2) 사생활 침해 등 피해를 입은 사람들에 대한 '사후적 구제' 제도를 마련한다. 3) 기업이나 정부의 신기술 남용을 '관리·감독'할 제도적 장치를 마련한다. 4) 기업이나 정부가 신기술 사용에 앞서 정보인권 보호 '가이드라인'을 준수하도록 규제한다.

첫 번째 정보인권보호 규제를 완화해야 한다는 제안에 대해서는 불필요하다는 의견이 조금 많았으며, 다른 3개의 제안에 대해서는 중요하다는 의견들이 압도적으로 많은 것을 확인할 수 있다.

<표6-11> 신기술과 정보인권 문제 개선을 위한 정책들에 대한 견해

	정보인권 보호 관련한 규제 완화		사생활침해 피해자 위한 '사후구제'		'관리감독'할 제도적 장치		정보인권 보호 '가이드라인' 강제	
	명	%	명	%	명	%	명	%
매우 불필요	71	7.1	10	1.0	4	0.4	4	0.4
다소 불필요	261	26.1	52	5.2	24	2.4	20	2.0
보통	430	43.0	233	23.3	206	20.6	190	19.0
약간 중요	193	19.3	374	37.4	364	36.4	359	35.9
매우 중요	45	4.5	331	33.1	402	40.2	427	42.7
합계	1,000	100.0	1,000	100.0	1,000	100.0	1,000	100.0

정보인권 보호 관련한 규제를 완화해야 한다는 입장에 대해서는 유일하게 부정적으로 값이 나타나 4차 산업혁명을 위해서 인권을 경시할 수는 없다는 의견이 조금 우세하다는 점을 확인할 수 있다. 다음으로 피해자에 대한 사후구제제도 도입에 대해서는 0.964로 구제제도의 필요성에 공감대가 높았다. 신기술 남용에 대한 관리·감독할 제도적인 장치와 정보인권 보호를 위한 가이드라인 준수하도록 규제해야 한다는 입장에 대해서는 각각 1.136, 1.185로 4차 산업혁명으로 인한 인권침해를 막기 위한 제도적 장치에 대해서 높은 긍정적인 반응을 확인할 수 있다.

<그림6-13> 신기술과 정보인권 문제 개선을 위한 정책들에 대한 평균값(5점 척도)

* 설문보기 매우 불필요~매우 중요 5개를 -2,-1,0,1,2점으로 환산하여 평균값 계산.

마지막으로 정보인권 보호 및 개선에 책임이 있다고 생각하는 기관/단체는 어디인지 순서대로 3곳을 선정하도록 질문하였다. 1순위에서는 행정기관이 265명으로 가장 많았고, 다음으로 수사기관(검찰, 경찰)이 240명, 국회 및 정당이 200명으로 세 번째로 많았다. 반면 시민단체(38명)나 일반 개인(79명)은 1순위에서 상대적으로 적었으며, 민간기업도 83명으로 낮았다. 2순위에서는 수시기관(검찰, 경찰)이 가장 많았으며, 3순위는 다시 행정기관이 가장 많았다. 행정기관과 수사기관과 같은 공공영역에서 정보인권 보호 및 개선에 책임이 크고, 시민단체와 개인, 민간기업과 같은 사적영역은 인권보호와 개선의 책임이 상대적으로 낮게 생각하고 있었다.

<표6-12> 정보인권 보호 및 개선에 책임이 있는 기관/단체

	1순위		2순위		3순위	
	명	%	명	%	명	%
국회 및 정당	200	20.0	125	13.0	105	11.4
수사기관_검찰,경찰	240	24.0	281	29.3	199	21.5
법원	93	9.3	121	12.6	151	16.3
행정기관	265	26.5	263	27.4	205	22.2
민간기업	83	8.3	87	9.1	127	13.7
시민단체	38	3.8	39	4.1	51	5.5
일반 개인	79	7.9	43	4.5	86	9.3
기타	2	0.2				
합계	1,000	100.0	959	100.0	924	100

3. 설문조사 종합 분석

이번 설문 결과를 볼 때, 시민들은 4차 산업혁명이 우려스러운 점이 있기는 하지만 4차 산업혁명을 피할 수 없을 뿐 아니라 중요하고 편리함을 제공할 것으로 기대하고 있다. 또한, 신기술 자체를 받아들이는 것에 대해서 큰 거부감은 없다고 볼 수 있을 것이다. 다만 생활의 편리와 안전수준 향상을 위해서 신기술이 필요하다면 도입을 하되, 신기술 도입으로 인한 부정적인 문제점들에 대해서는 적절하고 다양한 보호조치들은 준비해야 한다고 생각하고 있었다. 특히 신기술의 발전을 위해서 인권보호 수준을 낮추어서는 안 된다는 의견이 조금 더 많다는 점도 확인할 수 있었다.

이 설문조사 결과를 토대로 다음과 같은 시사점을 도출할 수 있다.

첫째, 4차 산업혁명과 정보인권 보호 둘 다 중요하게 생각하지만 그 가운데서도 정보인권을 보다 중요하게 고려하는 인식이 우리 사회에서 조금 더 우세하다고 할 수 있다.

둘째, 개인정보를 활용하여 안전과 건강수준 향상 등 직접적으로 도움이 될 서비스에 대해서는 대체로 긍정적으로 바라보지만, 금융과 신용평가 등 편익이 불확실한 부분에 대한 개인정보의 활용에는 부정적 의견이 많았다.

셋째, 가명정보를 정보주체의 동의 없이 가공하는 것에 대해서는 반대 의견을 보다 분명히 했다. 이는 개인정보를 수집, 관리하는 공공기관이나 기업에 대해 나타난 낮은 신뢰와 함께 살펴볼 필요가 있다.

넷째, 정책방향과 관련해서 전반적으로 개인정보 보호를 위한 보다 강력한 조치들을 요구하고 있고, 특히 4차 산업혁명의 발달을 위해 개인정보 규제를 완화하는 것에 대해서는 반대 의견이 많다고 할 것이다.

제2절 전문가 인터뷰 결과

1. 조사 개요

본 연구의 전문가 인터뷰 조사는 4차 산업혁명에 동반될 가능성이 있는 정보인권 관련 쟁점을 수집하여, 문제점의 원인 및 대처 방안의 방향성을 정립하고자 수행되었다. 2018년 10월 15일부터 약 30일 동안 각계 전문가 30명을 대상으로 서면 인터뷰했으며, 이렇게 수집된 응답 내용을 토대로 심층 분석을 시도하였다.

서면 인터뷰 참여자는 4차 산업혁명 및 정보인권 주제 관련 전문가들로서, 시민사회, 법조계, 학계, 산업계, 공공부문 등 5개 분야에서 각 5~7명으로 구성되었다. 응답자들의 신원 특성을 요약하면 다음과 같다.

<표6-13> 전문가 인터뷰 응답자 특성

분야	인원	직업군	구분자
시민사회	6명	활동가, 연구원	c-1 ~ c-6
법조계	6명	법무법인 변호사	l-7 ~ l-12
학계	6명	대학 교수	a-13 ~ a-18
산업계	7명	기업 임직원	i-19 ~ i-25
공공부문	5명	연구원, 위원	p-26 ~ p-30

서면 인터뷰 질문 문항은 총 6개로 구성되었으며, 각 질문은 다음과 같은 주제들로 분류될 수 있다. △4차 산업혁명의 정보인권 침해 쟁점과 원인, △개인정보 유출의 원인과 대처방안, △가명정보의 목적 외 활용 범위 및 조건, △알고리즘 편향성 및 차별의 현실성과 극복 방안, △지능형 감시 기술의 남용 방지 방안, △맞춤 정보 서비스의 편향성과 정치적 활용에 대한 사회적 대응 방안 등(질문지는 '첨부 1. 4차 산업혁명과 정보인권 전

문가 조사 설문지' 참조).

조사 결과의 전반적 경향을 살펴보면 다음과 같이 정리할 수 있다. 응답한 전문가들 사이의 개인적 견해 차이가 있음에도 불구하고, 시민사회·법조계·학계·공공부문 등에서 정보인권에 대한 적극적 의견을 제시하는 데 반해, 산업계에서는 4차 산업혁명 기술 및 경제 행위에 대한 규제를 우려하는 차원에서 상대적으로 유보적인 의견을 보이는 것이 일반적이었다. 또한 몇몇 응답자들의 경우에는 기술과 정보인권의 일반적 관계보다는, 4차 산업혁명 시대의 글로벌 환경과 기술적 특성으로 인해 재편되는 정보인권 논점을 강조하는 경향이 보이기도 했다.

정보인권과 관련된 전문가 답변들에서는 다수에게서 발견되는 '지배적 의견', (주로 산업계에서 제기된) '대립적 의견', 그밖에 색다른 관점을 제시하는 '특기할 만한 의견' 등의 경향성이 나타났다. 이에 따라 이하에서도 이 세 가지 응답군 성격을 고려하여 4차 산업혁명 및 정보인권의 쟁점을 서술하고자 한다.

2. 4차 산업혁명의 정보인권 침해 쟁점과 원인

전반적으로 4차 산업혁명이 인권 및 민주주의에 대한 위협 요소가 될 수 있다는 관점이 우세했다. 다만, 학계와 공공부문의 일부 전문가들은 부정적 판단을 유보하고 효과를 직접적으로 예단하기 어렵다는 의견을 보였으며, 업계에서는 인권 위협 요소가 있더라도 이를 윤리적·기술적으로 극복할 수 있다는 논점을 제시하기도 했다.

대개의 경우는 정보인권의 침해 가능성을 우려하는 편이었다. 광범위하게 수집되는 '데이터'가 소수에게 '집중'됨으로써 권력이 형성되고 감시 문제를 비롯한 '통제' 문제, 그리고 사회적 '차별'이 강화될 것이라는 의견이었다. 특히 시민사회 전문가들일수록 이와 같은 문제를 '민주주의'에 위협이 된다는 의견을 분명히 했다.

> "많은 영역에서 결과의 타당성에 기반해 자동화된 의사결정을 정당화하려는 움직임이 확산될 것입니다. 이는 지배적 패러다임에 반하는 가치, 문화, 존재의 부정과 무시, 특정 집단에 대한 배제와 차별, 민주주의의 축소 등의 결과로 이어질 수 있습니다."(c-2)

"빅데이터 데이터 처리기법의 발달은 지금까지는 처리되기 어려웠던 비정형 혹은 방대한 규모의 데이터 처리를 가능하게 합니다. 노동자와 소비자의 일거수 일투족이 자신들이 인지하지 못하는 새 사물인터넷 등 모든 환경에서 체계적으로 수집되어 기록될 것이며 데이터셋으로 교환될 것입니다. 그리고 이러한 데이터셋으로 학습한 인공지능 알고리즘은 채용, 보험 지급, 대출 등 사회생활에서 정보주체를 평가하고 예측하고 나아가 사람에 대한 의사결정을 자동으로 수행할 것입니다. 사회적 차별을 학습한 인공지능 알고리즘은 또다시 사회적 편견과 차별을 강화할 것이지만 정보주체는 이러한 상황을 쉽게 인지할 수도 없을 것입니다. 이는 인권과 민주주의에 대한 중대한 위협입니다."(c-5)

이와 반대되는 전문가 의견도 있었다. 산업계의 경우 대부분 정보인권 침해 가능성을 인정하면서도, 이를 기업의 '윤리'나 '역량'을 강화하고 대안적인 보안'기술'을 개발함으로써 극복할 수 있으리라는 낙관적 전망을 내놓기도 했다.

"프라이버시를 침해를 하는 개인정보의 오남용과 AI 알고리즘에 입각한 개인 인권 침해 사례(범죄자 예측의 오판단) 등 인간의 기본적 인권 및 행복추구권을 저해하는 현상이 우려됩니다. 이를 방지하기 위한 개인정보를 다루는 기업의 윤리성을 어떻게 담보할 것인가와 AI의 잘못된 오류에 대한 피해 책임을 어떻게 처리할 것인가에 대한 사전적 사회적 논의가 필요하다고 생각합니다."(i-19)

"밀레니엄시대 때, 2000년이 되는 순간 1900년도와 2000년도의 인식을 못해 전산망이 큰 혼란이 올 것처럼 이야기 했던 시대가 있었습니다. (중략) 블록체인과 같은 또 다른 새로운 물결들이 초기의 생각했던 일자리 상실에 대한 걱정을 해소시킬 것이고, 프라이버시와 같은 문제들도 새로운 분리된 암호화 기술을 통해 한층 더 강력한 프라이버시가 생겨나게 될 것입니다."(i-24)

일부 전문가들은 4차 산업혁명과 글로벌 환경의 맥락에서 위의 두 부류와는 색다른 견해를 내비쳤다. 4차 산업혁명 과정에서는 기계적으로 이뤄지는 프로파일링이 '제어가 불가능'하며(a-16) 그 효과 또한 쉽게 '예측하기 어렵기 때문'에(p-30) 기존의 개인정보 문제와는 전혀 다른 차원의 섬세한 접근이 요청된다는 의견이 눈에 띈다. 또한 산업계 일부에서는 인권 보호 차원의 경제 규제가 글로벌한 환경에서는 국내 기업의 경쟁력을 떨어뜨리는 '역차별'이 될 수 있음을 우려하기도 했다(i-22).

3. 개인정보 유출의 원인과 대처방안

개인정보 유출 문제는 2000년대 중반부터 있어왔던 문제인 만큼 문제의 원인을 진단하거나 대처방안을 모색하는 데 있어 전반적으로 비슷한 문제의식이 공유되고 있었다.

대다수 전문가들은 개인정보 유출이 보안 의식과 기술을 둘러싼 한국사회의 '총체적'인 문제라고 진단했다. 또한 이런 환경에서 개인정보를 통한 '금전적 동기'가 사태를 직접적으로 야기한다는 의견이 지배적이었다. 게다가 수집되는 데이터의 범위가 확대되고 '데이터 융합'의 중요성이 커지는 상황에서 생체정보를 비롯한 개인들의 소위 '민감 정보'가 중요해짐에 따라 개인정보 유출 문제는 과거보다 더 심각해질 수 있다는 우려가 제기되었다.

> "빅데이터의 활용과 사물인터넷의 확장 등은 다양한 데이터 결합이 필수적입니다. 따라서 4차 산업혁명 시대에서 개인정보의 활용은 불가피하므로 이에 대한 유출 사고가 빈발할 것으로 보입니다."(p-27)

개인정보 유출에 대처하기 위해서는 문제 원인의 규모가 총체적인 만큼 사전·사후 단계를 아우르는 '총체적 조치'가 있어야 한다는 의견들이었다. 또한 직접적인 피해 및 손해를 볼 수 있는 시민들 개개인 그리고 기술·관리적 일선에서 복무하는 처리자들에 대한 개인정보 리터러시 함양 등 '교육'적 조치가 있어야 한다는 의견도 적지 않았다(l-7, p-28, p-29). 유출 사고 발생 시 판례 해석 및 민형사상 처벌을 강화해야 한다는 의견이 공통적이었는데, 개인정보 유출에 따르는 '사회적 비용'을 높이거나 개인정보의 시장가치

를 낮춤으로써 범법행위의 동기를 낮출 수 있다는 전망이었다(c-5, a-17, i-23, i-25). 더 구체적으로는 법조계 전문가들을 중심으로'집단대표소송제', '징벌적손해배상제' 등을 현실화해야 한다는 의견들도 다수 있었다(c-1, l-8, l-9, l-12, p-30).

이상과 같은 견해에 대립적인 것으로 보이는 의견들도 제출되었다. 이들 역시 '민감정보' 문제의 심각성에 초점을 두는데, 이런 우려는 다수 전문가들과는 다소 다른 시각 차이를 보인다. 정확히 말한다면 앞으로는 과거의 개인정보 유출 논점과는 전혀 다른 프레임이 요구된다는 맥락에 가까웠다. 또한 개인정보 유출 사태에 '금전적 동기'가 있다는 의견을 공유하면서도, 이런 동기는 기업 생리 때문(시민사회 전문가들의 주된 관점)이 아니라 기업 행위와 무관한 개인들의 '해킹' 때문이라고 지적했다(l-17, i-23).

그렇기 때문에 개인정보 유출에 대한 처벌 등 대처방안에 있어서도 다수 의견과 비슷해 보이지만 상대적으로 구체적인 법제적 제안이 제시되지 않는 등 미묘한 차이를 드러내는 편이다. 오히려 개인정보 '비식별화' 등의 기술적 조치로 유출 문제 피해에 원천적으로 대처할 수 있다는 낙관적인 의견이 제시되기도 했다.

> "개인정보의 가명화 등을 통해 가명화된 정보가 유출되더라도 바로 식별이 불가능한 실질적인 보호가 필요하지 싶습니다. 과거처럼 가명화 등을 할 수 없어 필요에 의해 최소한으로 축적되었던 진성 개인정보가 유출되어 피해가 발생하는 것이 더 위험할 것입니다."(i-22)

> "유출이란 말 그대로 사고 상황입니다. 그리고 개인관련 정보와 프라이버시 침해 분리되어 이해돼야 한다고 생각합니다. 개인관련 데이터는 비식별화하여 4차 산업혁명의 또 하나의 자본으로 활용가능토록 하되 오히려 기업이 어떻게 개인정보를 관리를 잘하도록 할 것인가에 대한 기술적, 관리적, 물리적 조치를 강화하고 총괄 부서에서 관리·감독·제재하는 것이 필요하다고 생각합니다."(i-19)

주로 학계를 중심으로 해서, 개인정보 유출과 관련하여 적잖은 전문가들은 '주민등록번호' 체계 자체에 근본적인 문제가 있다고 지적하기도 했다(l-12, a-13, a-15, a-16). 특히 몇몇 전문가들은 4차 산업혁명 신기술 상황에서는 개인정보가 어떤 식으로든 활용될 수

밖에 없다고 진단하면서, 문제는 유출된 개인정보가 구체적 개인을 특정할 수 있게 되는 상황에 있다고 보았다. 그런 까닭에 실제 현실화 가능성은 낮다고 평가하면서도 주민등록번호를 중심으로 하는 국가적 DB 체제를 폐지하는 것이 옳다고 강조했다.

> "개인정보에 대한 침해가 다른 나라에 비해 특히 우리나라에 있어 심각했던 이유는 '주민등록번호'라는 전국민을 대상으로 한 매우 독특한 식별체계가 존재했기 때문입니다. 이러한 근본적인 위험요소는 현재의 행정망이 존재하는 한 앞으로도 지속될 것 같습니다. 따라서 그 개인정보 유출을 넘어 프라이버시권 및 기타의 침해에 대한 위험의 정도도 다른 나라에 비해 우리나라가 더욱 심각할 것으로 예상합니다. 가장 효과적인 방안은 행안부가 주민등록번호로 정렬된 현재의 DB운영체계를 포기하기로 결심을 해야 할 것인데, 글쎄요, 기대가능성이 매우 낮다고 봅니다."(a-16)

4. 가명정보의 목적 외 활용 범위 및 조건

가명정보 문제와 관련해서는 '제도혁신 해커톤' 등 최근의 합의 추세에 전반적으로 동의하면서도 세부적으로는 분야별·개인별로 미세한 온도 차이를 보였다.

우선 대다수 전문가들은 가명정보의 활용 범위는 '공익'적·'비영리'적 목적에 부합하는 것이어야 한다고 보았다. 가명처리가 되더라도 개인정보가 상업적 거래의 대상이 되어선 안 된다는 문제의식이 지배적이었다. 또한 가명정보가 활용될 때에도 정보주체의 동의가 선행되어야 한다는 의견도 있었다.

> "가명화 처리를 하더라도 개인정보주체의 동의 없이 활용해도 될 수 있도록 하는 범위는 매우 제한적이고, 필요성이 인정되는 영역으로 한정해야 합니다. (중략) 가명처리를 하는 것은 안전관리를 위한 것이므로, 개인정보 주체의 동의를 받지 않아도 정보 활용이 가능하도록 하는 것은 위험 기반 평가가 엄격하게 이루어져야 합니다."(l-9)
>
> "정보주체가 자신의 개인정보 처리에 대하여 충분히 인지하고 결정하지 못

한 상황에서 '학술연구 및 통계'의 목적으로 가명정보를 활용한다는 것에 대해 반대하는 입장입니다. 특히 의료정보는 건강정보 등 민감한 개인정보가 많아 4차 산업혁명론이나 지능정보사회론을 이유로 무차별적으로 활용하는 것은 국민의 정보인권을 크게 침해하여 사회적 자본의 필수인 신뢰가 훼손되는 심각한 위기에 처하게 될 것입니다."(p-27)

가명정보의 활용 조건에 관해서는 '학술 연구 목적'이라는 가이드라인이 아직 확정적이지 않은 상황이 지적되었다. 영리활동을 위한 기초 연구도 학술 연구 목적으로 볼 수 있을 것인지, 나아가 학술 연구의 공공적 목적이 무엇인지 등등에 관한 문제는 논쟁적이기 때문이다. 주로 시민사회 분야를 중심으로 하는 전문가들이 학술 연구를 어떻게 이해하고 정의할 것인지에 대한 더 많은 논의가 있어야 한다고 지적했다(c-1, c-4, l-9).

산업계 전문가들은 가명정보 활용 목적의 공익성을 주로 소비자 '편의성' 차원에서 이해하려는 경향을 보였다. 가명정보 활용을 통해 서비스의 질을 높이고 잠재적인 고객을 파악하는 도움을 얻을 수 있다는 의견이었다.

"가명 정보의 경우 특정 개인임을 알 수 없도록 한 정보이고 수집된 정보를 통해 고객 패턴, 소비 성향 등을 파악해 맞춤형 상품을 제공하여 사용자 편의성을 높일 수 있다는 장점이 있습니다. 다만, 가명 정보라 하더라도 다른 정보와 결합돼서 악용될 소지가 있다는 우려가 있는 것으로 알고 있습니다. 이 부분은 여러 가지 안전 장치가 단계별로 마련될 필요가 있다는 점에는 이견이 없으나 우려 때문에 산업 발전을 위한 최소한의 정보 활용도 안 된다는 점은 과도한 측면이 있습니다."(i-21)

이와 같이 가명정보를 활용하기 위해서는 개인의 프라이버시 침해 등 범법 행위를 '엄벌'하는 조건이 뒤따라야 한다는 의견을 제시했다. 산업계 전문가들 중 일부는 단계별 규제안을 제시하기도 했다. 이를테면 연구개발 단계에서는 가명정보 활용을 허용하고, 상품출시 단계에서는 가명정보 활용을 규제하는 것도 좋은 방법이 될 수 있다는 의견이었다(i-20).

가명정보의 활용가능성이 높아진 신기술 맥락에서는 과거와는 다른 논점이 필요하다는 의견도 있었다. 산·학·연 연계성이 커진 상황에서 순수학문 목적이 현실적으로 불가능하게 됐다는 지적에서부터(a-16), 가명정보의 특성상 기존의 이해방식으로는 실제 효과를 예측하기 곤란하다는 의견(a-15), 그만큼 '위험관리' 차원의 새로운 사회적 합의틀이 필요하다는 주장 등이 제시되었다(p-30).

> "정부 및 산업계에 종사하는 전문가 집단들의 신기술에 대한 입법대응은 너무나 개념법학적인 사고방식에 얽매여 있는 것이 아닌가 합니다. 개념 정의할 수 없는 것을 개념정의하고, 이에 입각하여 법률 요건과 그에 따른 효과를 설정하는 매우 고리타분한 입법방식입니다. 물론 과거 산업사회 시절에는 이러한 방식이 규제자와 수범자 모두에게 효율적일 수 있었겠지만, 이러한 입법방식은 현재와 같은 예측이 불가능한 불확정적 법현실에서는 유지되기 어려운 방식이고, 혼란을 좁히기보다는 가치간 반목을 극단화하는 결과를 초래할 수 밖에 없습니다.
>
> 향후 개인정보 및 프라이버시 보호 문제에 있어 개인 식별 가능성을 '절대적'인 개념 표지로 하는 접근방식은 지양하고, 위험 관리적 차원에서 접근하는 방향성을 구현해나가야 할 필요가 있습니다."(a-15)

5. 알고리즘 편향성 및 차별의 현실성과 극복 방안

인공지능 알고리즘에 의한 의사결정이 사회적 편견과 차별을 야기할 수 있겠느냐는 질문에 거의 모든 전문가들이 지극히 현실적인 이야기라고 응답했다. 세부적인 메커니즘에 대한 이해방식에서 약간 엇갈린 평가가 있을 뿐이었다. 다만, 이를 극복하기 위한 방안에 관해서는 여러 의견들이 쏟아졌다. 기술적인 측면, 사회적인 측면, 그리고 법제도적인 측면 등을 통해 응답자들의 의견을 정리해볼 수 있었다.

먼저 편향성과 차별의 현실성에 대한 진단을 살펴보자. 편견과 차별의 시작은 알고리즘 가동 직전 단계에서부터 시작된다는 의견들이었다. 다만, 알고리즘 '설계자'의 사회적 편견으로부터 시작된다는 진단(c-1, c-4, i-21, p-28)과 수집 및 창출되는 '데이터' 또는 '빅

데이터’ 자체로부터 시작된다는 진단 등으로 나뉘었다(c-5, l-9, l-12).

좀 더 심각한 수준의 진단도 제시되었다. 설계자나 데이터에 문제가 있다면 알고리즘 작동 이전에 편견 및 차별을 사전적으로 대응하는 것이 가능하겠지만, 몇몇 응답자들은 4차 산업혁명 상황에서는 이런 대응이 점점 더 어려워질 것이라고 전망했다(a-16, a-17). 인공지능의 딥러닝 또는 기계학습에 오게 되면 의사결정 과정에서 편견이 발견되고 차별이 문제시되더라도, 이런 현상이 어떤 논리에 의해 나타나게 된 것인지 개발자조차 해독하기 어려워진다는 것이다. 한 마디로 말해 제어불능 상황이 나타날 수 있다는 경고에 가까웠다.

> “편견적인 알고리즘이 인간을 잘못 판단할 수 있다는 가능성은 매우 현실적이라고 생각됩니다. 이에 대한 제 의견은 매우 원론적인데, 학습의 기초가 되는 데이터의 객관성을 검증하고, 적절한 범위에서 학습데이터를 공개하며, 자동화된 의사결정에 대해 정보주체의 이의제기권, 설명요구권을 보장하고, 무엇보다 인간의 중요한 행위에 대해 자동화된 의사결정 기술에만 의존하지 않는 사회 시스템을 구축하는 것이 필요하다고 생각합니다. 다만, 알고리즘의 설명의무와 관련하여, 딥러닝에 의하여 구현된 알고리즘, 일종의 소스코드는 전문가도 해독이 불가능하다는 점이 지적되고 있어서, 설명의무, 책임성과 같은 규범적인 의무를 부과하더라도 이것이 실제로 이행되기 어렵다는 우려가 있습니다.”(l-11)

문제 진단이 세부적으로 갈리는 만큼, 알고리즘 차별 극복 방안도 다양한 수준에서 제시되었다. 대다수의 경우 규범주의적, 민주주의적, 인본주의적 원칙을 확립하고 준수해야 한다는 의견들이었다. 응답 결과를 요약하면 다음의 표와 같다.

<표6-14> 알고리즘 차별 대처 방안에 대한 다차원적 견해

기술적 대응	설계자의 가이드라인 준수, 알고리즘의 규범 학습
사회적 대응	시민적 통제, 이를 위한 시민 역량 강화, 헌장 수준의 사회적 원칙 확립, 다양한 관계자들의 거버넌스 구현, 인공지능의 판단은 참조 수준으로만 제한적 적용(인간에 의한 최종 의사결정)
법제도적 대응	설명요구권 및 이의제기권 보장, 데이터 및 알고리즘 공개·투명성

실제로 알고리즘에 대한 시민들의 '설명요구권'을 보장하고(l-11, p-27), 기술 개발 및 적용 전 과정에서 '시민적 통제'가 가능해야 하며(c-1, l-8, l-11), '사회적 원칙'을 확립함으로써 설계자를 위한 '가이드라인'이 제시되어야 한다는 의견(c-4, a-14, i-21)이 주류를 이루었다. 그중에서도 p-30은 알고리즘 '기술에 대한 사회적 개입'의 가능성을 시사하기도 했다.

"크라우드 소싱 기반의 팩트체커(fact checker)와 같이 알고리즘 설계 및 활용단계에서 다수의 보편적 동의 기제가 작동하면서 알고리즘의 편향성 및 차별성을 통제하는 것, 즉 알고리즘을 사회적 감시체계 하에 두는 방안을 고려할 수 있습니다. 예컨대, 미MIT대 정보과학자 이야드 라완(Iyad Rahwan) 교수는 알고리즘 개발단계에서 '시민의 보편적 동의'가 알고리즘에 반영되어 선입견이나 편견을 최소화함으로써 알고리즘 기반의 의사결정을 새로운 사회계약의 형태로 통제할 수 있는 'society-in-the-loop'라는 사회참여 기반의 알고리즘을 제안한 바 있는데 이러한 알고리즘에 대한 사회적 감시 모형을 참고할 필요가 있습니다. 이러한 방안은 개별기업의 내부적 절차나 기준에만 맡기기보다는 알고리즘 투명성과 책임성의 관점에서 처리가능한 기준 및 절차에 대한 사회적 합의를 형성하기 위한 방안이라고 할 수 있습니다."(p-30)

"인간의 편향성에 따라 인공지능 알고리즘이 짜인다면 불투명성이 존재할 수 있다는 의견에는 동의합니다. 알고리즘의 측면에서 의사결정을 하는 과정은 설명이 가능하지 않아서 인간의 관여가 필요하고, 윤리적 설계가 우선되

어야 합니다. 해당 AI의 목적을 설계할 시 인간과 사회에 대한 이해도를 높이는 알고리즘으로 개발하도록 유도하는 것이 현재는 낫습니다."(i-24)

다만 세부적으로는 이견들이 없지 않았다. 예컨대 알고리즘 기술이 규범적 원칙을 학습하더라도 데이터의 사회적 성격상 기존의 사회적 편견을 극복할 수 없을 것이라는 전망(c-5)이 제시되었는가 하면, 인공지능 특성상 데이터가 축적되고 시행착오를 거칠수록 자기 학습의 결과로 편견을 극복할 것이라는 낙관적 전망(i-20)도 제시되었다.

법제도적 대응 측면에서도 관점 차이가 엿보였다. 주로 산업계에서 다른 의견들이 제시되었는데, 이들은 최소한의 공적 인프라를 통해 차별을 최소화해야 한다는 데 동의하면서도 시민적 통제와 같은 장치에 대해서는 다소 소극적인 태도를 보였다. 기술 개발 차원에서 편견의 작용을 방지하는 데 초점을 두는 것으로 설계자의 '윤리'적 원칙 준수 내지는 알고리즘 '기술 자체'의 자가 발전을 통해 문제 상황을 상쇄할 수 있다는 입장이었다.

일부 전문가는 조금 더 근본적인 차원에서 대처방안을 모색할 것을 주문하기도 했다. 현행 법 체계에서는 신기술 개발의 속도에 탄력적으로 대응하기 어렵다는 지적이었다. 그런 맥락에서 몇몇 전문가들은 현명한 차별 극복 방안은 시민적 통제든 거버넌스든 윤리적 설계든 다양한 수준의 공식적 의견수렴 절차를 강제하는 새로운 법규범 패러다임을 구상할 때 가능하다고 주장하기도 했다.

"이를 사전적으로 규제하기 위한 법적 시도는 사실상 불가능에 가깝습니다. 그리고 특정 인공지능 서비스의 문제점을 포착하여 이를 규제하고자 법제화하더라도, 그러한 법령들은 또 다른 기술적 발전 속에서 변화되어야 하는 상황입니다. 즉 법 및 제도를 통한 규제가 기술적 발전 속도를 따라가지 못하는 상황이 발생합니다. 이에 저는 학술적으로 응답적 법(responsive law) 패러다임이 도입될 것이라고 주장합니다. (중략) 이러한 응답적 법 패러다임이라는 것은 상황 변화에 법규범이 유연하게 대처하는 상황을 의미하는 것으로 이해해볼 수 있고, 이를 위해서는 상시적으로 인공지능 및 그 기술적 활용에 대한 데이터를 확보하고 있어야 하고, 이에 대해 시민들을 향해 공식적인 의견수렴

을 할 수 있는 절차를 다소간 강제할 필요가 있습니다.”(a-15)

“기술의 발전과 적용은 피할 수 없습니다. 단 깨어 있는 개인들에 의한 자기 권리 모니터링, 인권과 국익에 대한 균형 있는 시각을 가진 정부, 이에 대한 시민단체의 견제가 기술 남용을 막을 수 있는 장치가 될 것입니다.”(i-25)

6. 지능형 감시 기술의 남용 방지 방안

범죄예방 시스템, 노동 감독 시스템 등 이른바 지능형 감시 기술에 대해서도 대다수 전문가들이 비교적 일관적인 논점을 제시하는 데 비해, 상대적으로 산업계 전문가들은 대립적인 견해를 보이는 형국이 나타났다.

먼저 사회적 원칙이 우선해야 한다는 관점이 지배적이었다. 대다수 전문가들은 지능형 감시 기술을 견제할 새로운 기술적·윤리적 ‘규범’의 확립이 필요하다는 공통된 응답을 제시했다. 그리고 이와 같은 규범은 감시 기술의 ‘투명성’을 높이는 방향으로 원칙을 잡아야 한다는 의견들이었다.

“이러한 기술들이 필요 이상으로 남용되지 않을 수 있는 방안은 ‘디지털시대 프라이버시권’의 규범적 확보와 실천입니다. 즉 개인정보 수집, 처리, 공유가 상당히 증가함에도 개인들이 자신의 개인정보를 재사용, 판매, 다목적 재판매하는 데 대해 자유롭고 명시적이며 충분한 설명 및 인지한 후 동의하도록 해야 합니다.”(p-27)

“신기술 확대는 삶의 편익을 높이지만, 반대로 원치 않는 개인정보 수집과 활용, 감시와 통제의 수단으로 악용될 수 있는 부작용도 명백합니다. 인권과 권리침해, 차별과 혐오 유발 등 부작용이 명백하거나 가능성이 큰 분야는 원칙적으로 사용을 금지해야 합니다. 또한, 허용된 내용이라도 이를 남용할 우려가 커 이에 대한 안전장치와 처벌을 강화할 필요가 있습니다. 처리의 투명성을 높이기 위한 사전 정보제공과 사후 소비자 선택권 확대도 필요합니다.”(c-4)

이를 위해서는 정보인권을 보호하고 감시 기술을 규제할 법률적 요건, 절차, 한계 등을 세부적으로 명료화하는 것이 필요하다는 의견(c-1, c-3, l-8, i-20, p-29)이 제기되었다. 또한 정보주체인 시민들이 참여할 수 있는 사회적 '합의' 및 민주적 '통제'와 '거버넌스'를 현실화해야 한다는 주장들(c-5, l-9, a-15, a-17)도 있었다.

그에 반해 산업계는 지능형 감시 기술에서도 다른 분야들과 전반적으로 대립적인 의견을 내비쳤다. 물론 기술적 목적의 도덕성을 판별해야 하고 인권을 바탕으로 하지 않는 신기술의 적용을 방지해야 한다는 의견들도 있었다. 그러나 보안 기술에 대한 국민적 호응에서 보는 것처럼 부작용보다는 '순작용', '효용성', '사업성' 등을 감안해 프라이버시 침해 같은 요소는 기업의 '윤리' 부분에 책임을 맡기자는 의견이 주를 이루었다(i-22, i-23, i-24).

이외에도 몇 가지 눈여겨볼 만한 의견들 또한 제시되었다. 상당수 전문가들이 법률적 제한의 명료화를 주문했던 데 비해 l-9는 현행 법령을 갈수록 융합·진화하는 감시기술에 맞춰 탄력적으로 대응이 가능한 '유기적 시스템'으로 변화시켜야 한다고 주장했다. 또한 사회적 원칙과 규범에 있어서 a-13은 시민 및 노동자가 감시 기술을 역-감시할 수 있는 '상호감시' 체제를 제안했으며, p-30은 기술 피드백 과정에 '노동자 참여'의 중요성을 역설하기도 했다.

> "위험기반 접근에 기초해서, 기술이나, 수단에 대한 영향평가가 활성화되어야 합니다. 체크리스트 통과의례형 영향평가가 아니라, 진정으로 정성적인 영향평가가 이루어져야 합니다."(l-9)
>
> "상호감시체제(subveillance) 그리고 맥락상의 프라이버시(contextual privacy) 개념의 발전이 필요하다고 봅니다."(a-13)

한 가지 더 특기할 만한 것은 (특히 법률 전문가들을 중심으로) 정보인권에 대한 신기술의 '영향 평가' 제도를 요청하는 목소리들이 적지 않았다는 것이다(l-9, l-10, p-30). 이들의 주장은 4차 산업혁명 신기술로 인한 각종 문제들을 사전에 대응할 수 있다는 점에서 주목할 만한 의견이었다. p-30은 사용자·노동자 등에 대한 영향 평가가 있어야 지능형 감시 기술을 제어할 수 있다고 봤고, l-9는 정성적인 영향 평가를 통해 기술을 규율·

통제해야 한다고 봤으며, l-10은 적어도 공공부문에서라도 개인정보의 영향 평가를 실시해야 한다고 봤다.

7. 맞춤 정보 서비스의 편향성과 정치적 활용에 대한 사회적 대응 방안

응답한 전문가들 대다수가 맞춤 정보 서비스가 선택의 다양성을 줄이고 정치적으로도 악용될 수 있다는 점에 동의했다. 소비자들에게 알고리즘 기술이 제시하는 서비스 및 상품 선택지가 다양한 것처럼 보이지만, 실제로는 창의적인 선택의 기회를 제한하고 궁극적으로는 인간의 '자유의지'라는 것 자체를 훼손(c-1)할 가능성이 있기 때문이다. p-30은 4차 산업혁명 시대의 미디어 환경이 초래하는 문제점을 다음과 같이 정리해주기도 했다.

> "SNS 상에서 흔히 나타나는 디지털 네트워크 특성, 즉 자아중심적 네트워크(ego-centric network)를 통한 '선택적 노출(selective exposure)'과 '유유상종 효과(homophily effect)', 즉 편향적인 정보(뉴스) 선택 경향이 강화되어 극화(polarization), 극단화(extremization), 집단극화(group polarization)의 양상을 초래하기 쉽습니다. 심리학적으로는 자신의 주장과 일치하는 정보는 쉽게 받아들이고 그렇지 않은 정보는 무시하는 경향인 '확증편향(confirmation bias)'으로 인해 자신의 정치성향과 비슷한 가짜뉴스나 편향된 정보를 더욱 많이 소비하는 일도 빈번하게 나타납니다. 특히 개인 맞춤형 알고리즘을 적용해 필터링된 정보만을 받게 되는 이른바 '필터 버블(filter bubble)'은 이 같은 확증편향을 더욱 강화시킬 우려가 있습니다. 이것은 페이스북 등 글로벌 서비스만의 문제가 아닙니다. 최근 국내 포털에서 검토한다는 AI알고리즘 기반의 개인맞춤형 뉴스추천 서비스 또한 사용자들 간의 편향과 대립을 부추길 수 있는 우려가 제기됩니다. 물론 이러한 네트워크 효과 및 심리적 효과를 경제적·정치적 목적으로 이용하는 사람들이 더 문제입니다. 특히 적대적 대립이 고착화된 정치구조, 양극화된 정치문화에서 이러한 양상이 더욱 심화될 우려가 있습니다."(p-30)

대다수 전문가들이 선호의 편향성과 정치적 오남용 소지를 문제 삼았다. (비록 여론 조작 등은 인권 이슈와 무관하다는 입장(i-22)도 있었지만) 가짜 뉴스나 여론 조작 등 정치적 악용 사례에 대해 비판적인 입장을 취한 것은 거의 모든 전문가들이 대동소이했다. 게다가 이와 같은 개인정보들은 취향, 사상, 신념, 견해 등에 관한 것이어서 생체정보 등과 마찬가지로 사실상 '민감 정보'에 가깝다는 의견들(l-10, a-17)도 있었을 정도로 문제의 심각성을 지적하기도 했다.

> "앞에서 설명한 바와 같이 개인의 사상, 신념, 정치적 견해 등에 관한 정보를 수집·분석하는 행위는 현행법 위반이며, 누구를 막론하고 이를 엄중하게 집행하여야 합니다. 개인의 행태정보를 수집하여 맞춤형 광고 또는 맞춤형 서비스를 제공하는 행위도 결국은 개인의 성향을 분석하는 행위에 해당하므로 민감 정보에 준해서 엄격히 이를 제한하여야 합니다."(l-10)

문제는 이런 사안들을 기술적으로 제어하는 것이 점점 더 불가능해지고 있다는 점에 있다(i-25, p-28). 특히나 소비자 맞춤형 정보 서비스는 불가피한 추세에 가까울 정도여서 별다른 방도가 없다는 지적(a-13, a-16)이 있을 정도였다. 따라서 꽤 많은 전문가들이 개인정보의 상업적 활용 제한, 모니터링 실시, 영향 평가를 통한 개선 같은 해법보다는, 시민들의 '미디어 리터러시'와 정보인권에 관한 '시민 의식'과 '감수성'을 강화해야 한다는 주장(c-2, c-5, c-6, l-12, l-15, i-21, p-30)을 펼쳤다. 사용자가 자기 정보에 대한 통제권을 행사하고 프로파일링 등으로 인한 부작용에 대비하기 위한 '교육'적 체계가 있어야 하고, 그래야만 정보의 편향성이나 정치적 악용 같은 문제들을 사회적으로 '자정'할 수 있다는 주장들(a-14, p-28)과도 일맥상통하는 부분이었다.

> "공중파 TV가 처음 등장했을 때 이 미디어의 폭력성과 모방성에 대한 사회적 우려가 높았고, 시민들을 바보로 만드는 '바보상자'의 획일성, 과장광고 및 소비자 기만에 대한 질타가 높았습니다. 그러나 이러한 문제에 대해서는 국가 주도의 어떠한 규제나 해법도 성공적이지 못했습니다. 오늘날 공중파 미디어에 대한 시민들의 이해도가 분명 수십 년 전보다는 상당히 높아졌는데, 이는

결국 시민들의 리터러시 증진이 이루어졌기 때문이라고 생각합니다. 이 미디어에 대한 리터러시 교육이 사회적으로 이루어졌고 시민사회는 공중파 미디어의 메시지를 비판적으로 수용하였습니다."(c-5)

"유튜브 가짜뉴스 등 다양한 디지털 매체를 통한 편향된 정보는 사회를 분열시키는 기제로 작용하고 있으나 이를 기술적으로 제어하기는 불가능합니다. 사회적 자정이 가능하도록 문화와 제도를 변화시켜야 함에도 불구하고 (하략)"(p-28)

가짜뉴스나 여론 조작과 달리 맞춤 정보 서비스에 관해서는 상대적으로 관대한 입장도 제시되었다. 이들은 맞춤 서비스의 편향성보다 '유용성'에 주목하기를 요청하며(l-11), 위법 행위가 있는 부분만 통제하는 방향으로 사회적 비평과 공론을 형성해야 한다고 주장했다(i-23, i-25). 또한 산업계의 일부 전문가들은 여론 왜곡 등 정치적 오남용 문제에 있어서도 사업자의 '기술적 필터링'과 고의적·악의적 조작에 대한 '모니터링' 장치가 현실적이라고 보았다(i-19, i-20).

몇몇 응답자들은 민감 정보의 활용을 제한하는 것이 지구적 시장 환경에서는 '역차별' 효과를 낳을 수 있다고 우려하기도 했다(l-10, i-20). 이밖에도 l-9는 취향·선호 등의 필터링 알고리즘을 '공개'하는 한편 플랫폼의 '독점'을 방지하기 위해서라도 플랫폼 '거버넌스'를 도입하거나 아예 '정보이동권'을 도입해 시장에 '경쟁' 요소를 도입해야 한다고 주장했다.

8. 정보인권 보호를 위한 첨언

적지 않은 전문가들은 4차 산업혁명 시대의 정보인권을 보호하기 위해서는 '근본적인 접근'이 필요하다고 보았다. 규제 완화 추세가 야기하는 정보 주체의 '데이터에 대한 권리' 후퇴 상황(c-4, a-14) 속에서 특히나 공공부문의 인공지능 알고리즘 활용은 민주주의를 위협하는 압력으로 작용하고 있다(a-17)는 문제의식의 소산이기도 하다. 물론 산업계에서 주장하는 것처럼 첨단 기술을 통한 장기 계획을 구축한다면(i-24) 정보인권 문제 또한 자연스럽게 해결될 것이라는 낙관적 전망이 없는 것은 아니다. 그러나 정보인권 문제

에 관한 대다수 접근들이 과거 시대의 규제 패러다임에 머무름으로써 기술의 발전 속도를 따라잡지 못한다는 주장에 대해서도 경청을 해볼 필요가 있을 것으로 판단된다.

> "세계 경제를 주도하고 있는 것은 디지털 기술을 적극 활용한 기업들로 기술을 제약하고 거부하는 것은 21세기 쇄국주의가 될 뿐입니다. 하지만 무분별한 정보남용은 디지털 프롤레타리아를 양산하고 자본주의의 병폐를 가속화시키는 기폭제로 작용할 것입니다. 따라서 앞에서 언급하였다시피 아날로그적 사고로 접근하는 현재 시점의 정보에 대한 규제와 정책을 디지털적 사고로 전환하여 적극 활용하지 않으면 국내 경제가 쇠퇴하거나 사회가 양극화되는 결과로 나타나게 될 것입니다."(p-28)

새로운 상상력이 힘을 얻으려면 시민들의 의식이 밑바탕이 되어야 하며 그런 까닭에 상당수 전문가들 역시 '교육'의 중요성을 강조했던 것으로 풀이된다. 물론 시민의 각성을 요청하는 차원은 다양할 수 있다. 개인정보 오남용 방지를 위한 기초적 '윤리' 교육(i-19)에서부터, 정보인권에 대한 기초 소양 및 '미디어 리터러시' 교육(p-28, p-30), 기술 개발 및 활용에 대한 사회적 합의에 참여할 수 있는 시민적 '역량' 교육(l-9, i-21)에 이르기까지 다원적 수준의 정보인권 교육 체계에 대한 고민이 형성되고 있었다.

이와 같은 문제의식이 무엇보다 신기술에 대한 '시민' 중심 '민주주의' 실현에 초점이 있음은 분명해 보인다. a-13은 정보인권의 개념적 범주에 표현 및 사상의 자유뿐 아니라 '알 권리'도 포함되어야 한다고 역설하며, l-12는 정보인권을 아예 표현의 자유에 준하는 '기본권'으로 보장해야 한다고까지 주장했다. 이와 같은 법제적 구상이 4차 산업혁명에서 민주주의의 수호라는 문제의식과 닿아 있음은 자명하다. c-2 같은 경우도 기술에 대한 '시민적 통제'를 이뤄야만 4차 산업혁명과 민주주의가 공존할 수 있다고 주장했다. 최근의 신기술들이 보이는 '시민 의존성'을 생각해보더라도 이런 주장은 더욱 강화될 것으로 보인다.

> "오늘날 인류가 보편적으로 인터넷과 모바일 기술의 혜택을 향유하고 있는 것은 시민의 힘 때문입니다. 시민들은 군사적 목적으로 개발되었던 컴퓨터와

인터넷 기술을 사회적으로 적극 수용하고 때로는 정보인권을 요구하며 기술의 사회적 영향력에 개입해 왔습니다. 온라인 서비스 기반의 시민들이 생성해 낸 데이터와 이들의 개인정보입니다. 따라서 4차 산업혁명의 실체가 있다면 그것은 기술이 결정하거나 기업의 이윤 창출에 복무하는 것이 아니라 사용자(소비자), 시민들에 의해 완성되어야 할 것입니다."(p-27)

규제냐 탈규제냐 하는 논쟁은 확실한 답을 얻기 어려운 문제일 수 있다. a-14처럼 개인정보 및 민감 정보의 활용을 '최소 범위'로 한정해야 한다는 주장도 있을 수 있고, a-15처럼 개인정보 데이터 활용에 대응하여 일련의 '정보인권 영향평가'를 도입하는 것이 타당하다는 지적도 있을 수 있으며, p-26처럼 특별히 (종종 논외로 치부되곤 하는) '노동자 및 취업자 전반'의 인권을 보호하기 위한 입법 요청도 있을 수 있다. 심지어 c-5는 이렇게까지 심화된 경계와 비판적 입장을 피력하기도 했다.

"최근 데이터를 처분할 수 있는 권리에 주안점을 둔 정부와 산업계의 이슈 공세가 계속되고 있습니다. 최근 '마이데이터', 데이터주권 등의 용어가 '정보인권'을 대체하는 언론보도가 급격히 늘어난 데에도 이와 같은 배경이 있다고 생각합니다. 개인정보를 자유롭게 처분하고 매매할 수 있는 정보주체의 권리를 강조하는 용어는 결국 상품으로서 개인정보를 부각시킵니다. 마일리지 서비스 등 이미 비현금성 개인정보 거래가 이루어지는 시대인데 현금화하는 게 어째서 문제냐고, 소비자에게 필요한 것은 '마이데이터'를 더 높은 가격을 받고 파는 경제적 주권이 중요한 것이 아니냐는 주장이 확산되고 있는 듯합니다."(c-5)

국내 기업의 경쟁력을 위해 정보인권에 대해 유연한 사고를 할 필요가 있다는 주장도 만만치 않다. 그래서 국내법적 규제만으로는 글로벌 기업 규제에 실패함으로써 또 다른 문제가 초래될 것이라는 우려 역시 그런 맥락에서 나온다(i-22). 국가 경쟁력의 실추가 없도록 데이터 활용의 '자유도'를 높여야 한다는 의견이나(i-19), 개인과 기업의 윤리의식과 책임감을 높이고 객관적 모니터링을 실시하는 데 집중하고 정보인권에 관해서는 '유연적 사고'를 가져야 한다는 의견이 대표적이다(i-21). 4차 산업혁명 신기술에서는 정보인

권 문제마저도 '기술적 조치'들로 극복할 수 있다는 주장에 대해서도 다각적인 검토를 해볼 만한 여지가 있는 것으로 보인다.

> "4차 산업혁명 시대에서 중요한 것은 우리나라가 경쟁국들에 비해 차세대 경제성장을 위한 기반기술에 뒤쳐져서는 안 된다는 것이고, 이를 위해서는 첫째, 실질적인 보호수준을 높이기 위한 가명화 등 기술적인 조치들을 통해 개인정보 유출우려가 극복이 되어야 하며, 둘째, 국가나 기업의 빅브라더 우려도 사전적인 규제보다 사후적인 규제로 풀 수 있는 장치를 고민해야 할 것입니다. 정보인권과 개인의 의사와 판단의 왜곡, 이로 인한 민주주의의 후퇴까지 연결 짓는 것은 다소 지나친 논리적 비약이라고 사료 됩니다."(i-22)

물론 정보인권 시민교육이나 민주주의 실현이 시민사회와 산업계를 극단점으로 하는 이해관계망에서 어느 한 쪽에 일방적으로 힘을 실어주기 위해 제시되는 것은 아니다. i-23은 정보인권 보호만으로는 혁신을 통한 이익을 포기하는 상황이 올 것이라 경계하기도 했지만, 실제 대다수 전문가들은 4차 산업혁명 규제 자체가 목적은 아님을 시사했다. 일례로 소비자·노동·시민사회운동 등에서 전문가에 준하는 안정적 교육 체계 도입을 주장한 l-9는 인권·공정경쟁·프라이버시·혁신 등의 가치가 '조화'와 '균형'을 이뤄야 한다고 지적하기도 했다. 이것은 개인정보보호위원회의 철학·전문성·사명감 부족에 대한 '질타'이기도 하지만(l-10), 경제 논리에 치우친 정부를 '견제'하기 위한 시민 각성의 요청일 수도 있고(p-29), 개인정보를 적극 보호하는 기업에 대한 '독려'일 수도 있다(c-3).

> "시민(정보주체)들의 각성이 필요합니다. 정보인권 침해양상이 훨씬 더 정교하고 복잡해진 상태에서 이를 통제·감독하려면 정부가 적극 나서야 하는데, 막상 정부는 관련 산업 활성화, 규제완화 논의 등으로 인해 제약이 있습니다. 이에 대해 정부로 하여금 자신들의 권리를 보호하게 만드는 궁극적 힘은 시민 스스로에게 있다고 봅니다. 따라서 시민들에 대한 정보인권 교육, 최신 동향(빅데이터, 사물인터넷 등)에 대한 이해도 강화(리터러시) 노력 및 이를 통한 시민들의 조직적 연대활동이 필요하다고 봅니다.

이외에 정부는 균형 잡힌 시각에서 산업계와 정보주체의 이해충돌을 잘 조정해야 하는 임무를 충실히 수행할 필요가 있고, 업계에서는 스스로 자정작용을 통해 과도한 정보인권 침해를 억제해야 할 것입니다."(p-29)

제7장 정보인권 보호와 확장을 위한 법제도 및 정책 제안

제1절 법제도 및 정책 개선 방향

빅데이터, 사물인터넷, 인공지능 등 4차 산업혁명의 주축이 되는 신기술은 시민의 안전, 효율적인 서비스 등 우리들의 삶에 혜택을 주는 것이 사실이다. 동시에 사회의 기존 규범을 해체하고 실업과 같은 새로운 사회 문제를 야기하거나 인권을 위협할 가능성도 존재한다. 특히 개인정보 등 정보인권을 침해하거나 기존의 차별을 고착화시킬 가능성 또한 어느 때보다 높아지고 있다. 기술의 발전과 경제 성장이 개인의 기본적 권리의 희생 위에서 전개되는 것이 아니라 이와 조화를 유지하고 인권을 강화할 수 있도록, 신기술을 우리 사회에 어떠한 원칙과 규범 하에서 도입할 것인지에 대한 사회적 합의가 절실하다.

정보주체로서 개인은 여러 차원의 관계 속에 놓여있다. 즉, 시민으로서, 소비자/사용자로서, 노동자로서 국가, 기업, 고용주와 관계를 맺는다. 신기술로 인한 정보인권 침해는 정보주체가 맺는 관계에 따라서 다양한 양상으로 나타날 수 있으며, 인권 침해를 예방하거나 권리를 구제하는 방식도 다를 수 있다. 신기술 하에서 정보인권 보호를 위한 정책 및 제도는 정보주체를 둘러싼 이와 같은 다양하고 복잡한 관계를 고려할 필요가 있다.

지금까지의 검토를 토대로 본 연구에서는 4차 산업혁명 시대 정보인권 보호를 위해 다음과 같은 방향에서 정책적, 제도적 대안이 필요하다고 권고한다.

1. 개인정보 보호법제의 개혁

신기술의 발전으로 가장 위협을 받을 수 있는 권리가 정보주체의 개인정보 자기결정권인 만큼, 4차 산업혁명에 대응하는 개인정보 보호법제의 개혁이 이루어질 필요가 있다. 앞서 본 바와 같이, 유럽연합, 미국, 일본 등 각 국가 역시 새로운 환경에서 정보주체의 권리 보호와 안전한 활용을 도모하기 위한 새로운 규범을 신설하는 등 개인정보 보호법제의 개혁을 추진하고 있다. 반면, 한국에서는 최근 몇 년 동안 '비식별화'를 둘러싼 사

회적 논란만이 지속되었을 뿐 실질적인 법제 개선은 지체되었고, 비효율적 법제와 감독 체계 역시 발목을 잡아왔다.

1) 개인정보 보호체계 효율화

현재 국내 개인정보 보호법제는 개인정보보호법, 정보통신망법, 신용정보법, 위치정보법 등으로 분산되어 있어 수범자의 혼란과 중복규제를 야기하고 있다. 개인정보 감독권한도 행정안전부, 방송통신위원회, 금융위원회, 개인정보보호위원회 등으로 분산되어 있어 효율적인 감독과 통일적인 개인정보 보호정책 수립에 장애가 되고 있다. 또한 각 소관부처가 경쟁적으로 관할 영역을 확대하려고 하면서 법제 간 혼란은 심화되고 있다. 이와 같은 분산된 개인정보 보호체계 하에서는 4차 산업혁명 시대의 효과적인 개인정보 보호정책을 수립하기 힘들다.

4차 산업혁명에 대비한 개인정보 보호정책의 수립을 위해서는 개인정보 보호법제를 개인정보보호법을 중심으로 정비할 필요가 있다. 또한 독립적인 개인정보 감독기구의 설립은 개인정보보호의 핵심적 요소인 만큼 개인정보보호법이 실효성 있게 집행되기 위해서는 개인정보보호위원회를 독립적인 중앙행정부처로 격상하고 감독권한을 일원화할 필요가 있다. 특히, 개인정보보호위원회의 독립성 보장이 중요한데, 개인정보보호위원회는 민간영역 뿐만 아니라 공공영역, 특히 정보수사기관의 개인정보 처리와 관련해서도 실효성 있게 감독할 수 있어야 하기 때문이다.

문재인 정부에 들어와 다행히 개인정보 보호법제 개선과 감독기구 일원화를 추진하고 있고, 관련 개정안이 국회에 발의되어 있는 상황이다. 그러나 신용정보법의 개인정보보호법으로의 통합 및 금융위원회의 감독권한을 개인정보보호위원회로 이관하는 문제는 배제되어 있다. 개인 신용정보의 경우 법제 간 혼란과 중복규제의 문제는 해결되지 않고 남아있게 된다. 금융위원회가 개인 신용정보의 활용 촉진을 위해 적극적인 행보를 보이고 있는 바, 개인정보보호위원회의 개인정보 정책과 충돌할 경우 기관 간 갈등과 수범자의 혼란을 야기할 우려가 있다.

4차 산업혁명에 대응한 개인정보 보호법제의 개선과 일관된 추진을 위해서도 신용정보법까지 포함하여 개인정보 보호법제 및 감독기구의 일원화가 이루어질 필요가 있다.

2) 개인정보 보호법제 개선의 방향

4차 산업혁명에 대응하기 위해 현행 개인정보보호법을 다음과 같은 방향으로 개선할 필요가 있다.

첫째, 시스템의 투명성이 보장될 필요가 있다.

아실로마 인공지능 원칙, 일본 정보통신정책연구소의 <인공지능 개발원칙>, 유럽 개인정보보호감독관의 <빅데이터의 문제 해결에 관한 의견서(2015)>, 영국 정보보호감독관의 보고서, 국제 개인정보보호 감독기구 회의(ICDPPC)의 <인공지능 윤리 및 개인정보 보호에 대한 선언> 등 대부분의 연구자 및 공공기관은 인공지능 등 신기술에 대한 대응에 있어서 '투명성'의 중요성을 지적하고 있다. 사물인터넷의 확대로 서로 다른 기기나 시스템 사이에서 수많은 정보처리 과정이 수행되면서, 개인정보의 수집부터 처리까지 어떻게 작동되는지 정보주체가 인지하기 힘들고, 이에 따라 통제권이 무력화될 우려가 있다. 또한 인공지능 알고리즘의 경우 개발자들도 그 결과가 발생한 메커니즘을 파악하기 힘들다. 따라서 시스템의 투명성이 보장되지 않으면 오류의 발견뿐만 아니라 차별의 시정이나 정보주체의 권리 행사가 불가능하다. 인공지능 알고리즘에 대한 로직의 공개, 정보주체의 설명을 요구할 권리 보장, 사후에 설명, 감사, 검증이 가능한 방식의 설계 등 시스템의 투명성을 보장할 수 있는 방식의 제도적 장치가 필요하다. GDPR에서도 제5조 (a)에서 개인정보는 "정보주체에 대해 합법적으로, 공정하게, 투명한 방식으로 처리되어야(적법성, 공정성, 투명성)"함을 규정하고 있으며, 개인정보처리자의 신원 및 처리 목적 등을 정보주체에 고지하도록 하고 정보주체에 설명을 요구할 권리를 부여하는 등의 구체적인 규정을 두고 있다.

둘째, 설계단계에서부터 정보인권을 보호할 수 있도록 해야 한다.

시스템의 복잡성과 불투명성이 증가하면서 설계 단계에서부터 인권에 미치는 영향을 고려할 필요가 커지고 있다. 비단 개인정보 뿐만 아니라, 윤리 및 보안 측면에서도 설계 단계에서 이러한 영향을 고려할 것을 요구하고 있다. 국제 개인정보보호 감독기구 회의(ICDPPC)도 이를 권고하고 있고, 유럽 GDPR 제25조에서는 개인정보보호 중심 디자인 및 기본설정(Privacy by Design and by Default)을 규정하고 있다. 비단 프라이버시 측면에서 뿐만 아니다. 국제전기전자기술자협회(IEEE)는 <윤리적으로 조율된 설계(Ethically

Aligned Design)>에 대한 권고안을 발표하면서 인공지능 및 자동시스템 개발 시 책임성, 투명성, 인식제고, 개인정보보호, 고용문제 등 윤리적 측면을 고려한 설계가 필요함을 강조하였으며, 정보통신정책연구소, 미연방거래위원회(FTC) 등은 보안 중심 설계(Security by design)을 제안한 바 있다. 특히 신기술 환경에서의 서비스는 기기제작자, 소프트웨어 개발자, 플랫폼 사업자 등 다양한 이해관계자들이 연결되어 있고, 이들 사이에 개인정보를 포함한 정보의 흐름이 형성되기 때문에 연결 고리의 한 단계에서의 취약점이 전체 시스템에 영향을 미칠 수 있다.

셋째, 개인정보의 수집 및 처리의 전 과정에서 정보주체의 권리가 보장되어야 한다.

유럽연합 제29조 작업반은 사물인터넷에 대한 의견서에서 "사용자는 제품 수명주기 전반에 걸쳐 자신의 개인정보를 완전하게 통제할 수 있어야 한다"고 제안한다. 센서를 기반으로 자동화된 정보 수집이 보편화된 사물인터넷 환경에서 전통적인 방식의 사전 동의는 어려워지고 이에 따라 정보주체의 권리가 심각하게 침해될 수 있다. 또한 대량으로 수집, 축적된 개인정보는 프로파일링을 통해 개인의 민감한 행태나 성향을 파악하는데 이용될 수 있고, 집적된 개인정보는 정보주체의 의사와 무관하게 활용될 가능성이 크다. 이처럼 취약해질 수 있는 정보주체의 통제권을 보완할 수 있는 조치들이 마련되어야 한다. 예를 들어, 프로파일링을 포함한 자동화된 처리에 대한 정보주체의 거부권, 개인정보 이동권, 사용자 동의 없이 이용기록을 추적할 수 없도록 하는 '추적 금지(do-not-track)' 정책 등을 고려할 필요가 있다.

3) 국내 개인정보 보호법제 개선을 위한 권고

이러한 원칙하에 국내 개인정보 보호법제에 다음과 같은 제도들의 도입을 검토할 필요가 있다.

○ 투명성 원칙의 규정

현행 국내 개인정보보호법은 제3조에서 개인정보보호원칙을 규정하고 있는데, 제5항에서 "⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며"라고 규정하여 일부 투명성 원칙을 포함하고 있다. 그러나 이 원칙이 비단 개인정보 처리방침의 공개만을 의미하는 것은 아닐뿐더러, 4차 산업혁명 시대에 그 중요성

이 커지고 있기 때문에, 보다 일반적인 원칙으로 천명할 필요가 있다.

○ 가명/익명 처리의 개념 신설

대통령산하 4차산업혁명위원회 주최의 해커톤 및 국회 4차산업혁명특별위원회 등의 논의를 통해 유럽연합의 GDPR에서의 개념을 수용하여 개인정보, 가명정보, 익명정보의 개념을 신설할 필요성에 대해서는 일정한 사회적 합의가 형성되었다. 그러나 전문가 설문조사 결과에서도 볼 수 있듯이, 전문가 사이에서도 개인정보의 목적 외 활용에 대한 견해 차이가 크게 나타나고 있다. 현재 국회에는 가명처리 된 개인정보의 활용을 확대하는 방향의 개정안이 발의되어 있는데, 그 활용 범위 및 수반되는 안전조치를 둘러싼 논란은 계속되고 있다. 국회에서 합의안이 통과하더라도 실제 이행과정에서의 논란을 불가피한데, 과학적 연구의 범위나 활용시 안전조치 등과 관련하여 유럽에서는 역사적으로 형성되어 온 관행이 있는 반면, 국내에서는 사회적으로 합의된 관행과 공통규범이 부재하기 때문이다. 향후 개인정보보호위원회에서 구체적인 가이드라인을 제시할 필요가 있으며, 이행 과정의 모니터링을 통해 개인정보, 특히 기업들의 고객정보가 남용되지 않도록 할 필요가 있다.

○ 프로파일링 등 자동화된 처리에 대한 정보주체의 권리 신설

프로파일링과 같이 개인의 권리에 중대한 영향을 미치는 자동화된 의사결정에 대한 정보주체의 권리를 보장할 필요가 있다. 정보주체의 명시적인 동의나 법률에 규정된 경우 등을 제외하고, 정보주체는 자동화된 처리에만 전적으로 의존하는 결정을 받지 않을 권리를 보장받아야 한다. 투명성 보장을 위해 정보주체는 이러한 결정에 설명을 요구하고, 이의를 제기하며, 인적 개입을 요청할 권리를 갖는다. 정보처리자는 프로파일링 등의 처리가 이루어졌는지, 관련 로직은 어떠한지 등에 대한 의미 있는 정보를 정보주체에 제공할 의무가 있다.

○ 개인정보 보호 중심설계(Privacy by Design) 및 기본설정(Privacy by Default)

설계단계에서부터 개인정보 보호를 고려하여 설계하도록 하는 개인정보 보호 중심설계와 사용자에게 기본으로 제공되는 설정을 개인정보 친화적으로 설정하도록 하는 개인

정보 보호 기본설정을 우리 법제에도 도입할 필요가 있다. 이러한 원칙은 단순히 서비스 제공자 혹은 개인정보처리자로 한정되지 않으며, 서비스 활용의 물적 기반을 제공해 주는 기기 제조업자나 소프트웨어 개발업체 등 특정 서비스에 관여하고 있는 모든 이해당사자에게 적용되어야 한다.

○ 개인정보영향평가 제도 강화

이미 현행 개인정보보호법은 개인정보영향평가 제도를 두고 있으나 그 대상이 공공기관에 한정되어 있고 내실 있게 운영되고 있지 않다. 이를 개선하기 위해서는 첫째, 개인정보 영향평가를 민간 영역으로 확대해야 하며, 둘째, 단지 개인정보파일에 포함된 정보주체의 규모가 아니라 정보주체에 심각한 영향을 줄 수 있는 모든 시스템을 대상으로 해야 한다. 셋째, 개인정보보호위원회가 영향평가에 대해 사전에 자문하고 시행 결과를 검토하는 등 감독기능을 강화할 필요가 있다.

○ 민감 정보의 범위 확대

현행 개인정보보호법은 제23조에서 이미 민감 정보에 대한 특별한 보호를 규정하고 있다. 그러나 시대 변화에 맞게 민감 정보의 범위도 확대되어야 한다. 특히, 생체인식 기술의 발전에도 불구하고 생체인식 정보가 민감 정보에 포함되어 있지 않은 것은 큰 문제다. 다문화 사회로의 변화를 고려하여 민족, 인종과 관련된 정보 역시 민감 정보에 포함될 필요가 있다.

○ 주민등록번호 체계 개편

전문가 설문조사에서 많은 전문가가 지적하고 있다시피, 국내 개인정보 보호에 있어 가장 큰 취약점 중 하나는 주민등록번호 제도이다. 어느 나라나 국민식별번호는 존재하지만, 주민등록번호의 경우 번호체계에 개인정보를 포함하고 있어 그 자체로 개인정보 노출의 위험성이 있고 특정 개인의 주민등록번호 추정이 용이하다는 점, 주민등록번호가 범용적으로 수집, 활용되면서 서로 다른 개인정보를 연결하는 연계키로 기능하고 있다는 점, 이미 대다수 국민들의 주민등록번호가 유출된 상황이라는 점 등이 문제로 지적되고 있다. 이미 2014년 5월 26일, 국가인권위원회가 권고한 바와 같이 주민등록번호의 번호체

계를 변경하고, 주민등록번호의 수집을 제한하여 서로 다른 영역에서는 수집 목적별로 다른 번호를 사용하는 등의 개혁이 필요하다. 이미 개인정보보호법에서는 법령에 규정되어 있지 않은 경우 주민등록번호의 수집을 규정하고 있지만, 주민등록법 개정을 통해 주민등록번호 체제의 개편이 이루어져야 한다.

2. 지능화된 국가 감시 통제 절차와 감독체계의 마련

갈수록 지능화되는 국가 감시를 통제할 수 있는 절차와 감독체계가 마련되어야 한다. 미국 백악관이 빅데이터 보고서에서 지적하고 있다시피, 신기술은 정부와 시민간 권력관계의 균형에 변화를 가져올 수 있다. 과거에는 통제의 의도가 있어도 기술적인 한계로 권력의 영향력이 제한적일 수 있었던 반면, 신기술은 과거보다 훨씬 세밀하게 통제할 수 있는 역량을 권력 기관에 제공하기 때문이다. 미국 국가안보국의 인터넷 대량감시와 한국 국가정보원의 해킹 프로그램 사용은 은밀한 국가감시의 일단을 보여준다.

국내에서는 그 동안 수사기관의 개인정보 접근 및 통신수사와 관련해서 많은 문제제기가 있었음에도 불구하고, 국회에서는 시대적 변화에 조응한 원활한 법 개정이 이루어지지 않았다. 다행히 2018년 헌법재판소는 공공기관 개인정보의 무영장 제공, 기지국 수사와 실시간 위치추적, 인터넷 패킷감청 등에 대해 헌법불합치 결정을 내렸고 이에 국회에서 관련한 법 개정이 이루어질 예정이다. 그러나 현재 국내 법제는 지능화된 국가 감시에 대한 대응은 고사하고, 정보수사기관의 개인정보 처리 실태의 투명성과 통신수사 과정에서의 인권 보호조치 등도 미약한 상황이다.

스노든에 의한 인터넷 대량 감시에 대한 폭로 이후, 유엔에서도 국가 감시를 감독할 수 있는 메커니즘을 마련할 것을 각 국에 촉구하고 있으며, 유럽연합은 적정성 심사 과정에서 국가 감시에 대한 통제 장치를 중요한 기준으로 삼고 있다. 이러한 국제적인 상황뿐만 아니라, 지능화되는 국가 감시로부터 국민들의 인권을 보호하기 위해서 국가 감시를 통제할 수 있는 적법 절차 및 감독 메커니즘이 구축되어야 한다. 예를 들어, 정보수사기관이 보유하고 있는 개인정보 처리 시스템 역시 일정 수준에서 공개되어야 한다. 국회, 국가인권위원회, 혹은 정보수사기관에 대한 새로운 독립적 감독기구가 정보수사기관의 권한 남용 여부를 감독할 수 있어야 한다.

지능화되고 있는 국가 감시 체제에 대한 통제를 위해 다음과 같은 제도의 도입을 검토할 필요가 있다.

○ 정보수사기관에 대한 무분별한 개인정보 제공에 대한 통제

현행 개인정보보호법은 '범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우' 영장이 없이도 공공기관이 보유하고 있는 개인정보를 정보수사기관에 제공할 수 있도록 되어 있다. 정보제공 여부에 대해 정보주체에 통지할 수 있는 절차나 권리 침해 시 구제 방안도 없다. 필요할 경우 정보수사기관이 개인정보에 접근할 수 있다고 하더라도, 권한 남용을 방지할 수 있도록 법원의 허가를 받도록 하고 개인정보 제공 시 정보주체에게 통지하는 절차를 도입해야 한다.

또한, 개인정보보호법 제58조는 '국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보'의 경우 개인정보보호법 제3장부터 제7장까지 통째로 적용을 배제하고 있는데, 정보주체의 권리를 일부 제한할 수 있다고 하더라도 이와 같이 일괄 제한하는 것이 아니라 권리 제한이 필요한 경우를 구체적으로 명시할 필요가 있다.

○ 정보수사기관이 보유한 개인정보파일 및 시스템에 대한 감독

현재 개인정보보호법은 공공기관이 보유하고 있는 개인정보파일에 대한 등록을 의무화하고 있으나, 정보수사기관의 경우 예외가 인정되고 있다. 이렇게 되면 정보수사기관이 어떠한 개인정보를 수집, 처리하고 있는지 감독이 불가능해질 뿐만 아니라, 인공지능과 같은 신기술을 이용한 새로운 시스템 역시 무분별하게 도입할 수 있다. 필요하다면 일반에 공개되지 않더라도 최소한 개인정보 감독기구로의 등록은 의무화하여 개인정보가 적정하게 수집, 처리되고 있는지 감독이 가능하도록 해야 한다. 더불어, 정보수사기관이 인권침해 가능성이 큰 정보시스템을 도입할 경우 필수적으로 개인정보영향평가를 수행하고 감독기구의 검토를 받도록 해야 한다.

○ 통신자료(가입자 정보)의 보호

현재 포털이나 통신사가 보유하고 있는 가입자 정보, 즉 전기통신사업법 상 통신자료의 경우에도 법원의 통제 없이 정보수사기관의 '협조요청'만으로 제공할 수 있도록 되어

있으며, 정보주체에의 통지도 이루어지고 있지 않다. 전기통신사업법의 개정 혹은 통신비밀보호법의 개정을 통해 “피의자가 죄를 범하였다고 의심할만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있을 경우” 법원의 허가를 받아 통신자료를 제공받을 수 있도록 하고 사용자에 대한 통지 의무를 부과할 필요가 있다.

○ 통신사실확인자료의 보호

기지국 수사와 위치정보 추적에 대한 헌법재판소의 헌법불합치 결정으로 관련 조항도 개정되어야 한다. 국가인권위원회 역시 지난 2014년에 통신사실확인자료 제공의 허가요건인 ‘수사 또는 형의 집행을 위한 필요성’이 지나치게 모호하여 수사기관의 남용을 방지하기 어렵고 사생활 보호에 미흡하다고 지적한 바 있다. 헌법재판소가 통신사실확인자료 역시 통신내용과 같이 강력한 보호가 필요한 민감한 정보로 인정한 바, 통신제한조치(통신감청)에 준하는 엄격한 보호가 필요하다. 즉, 통신사실확인자료 제공대상 범죄를 감청 대상 범죄와 같이 한정하고, 제공의 요건 역시 ‘다른 수사방법으로는 수사의 목적을 달성하기가 불가능하거나 현저히 곤란한 경우’에 한하여 예외적이고 보충적인 수사방법으로 활용하도록 제한할 필요가 있다.

한편, 기지국 수사의 경우에는 피의자를 특정하지 않고 특정 기지국에 접속한 모든 사람의 통신사실확인자료를 일괄해서 받는 것이므로, 대상 범죄를 중범죄로 제한하고 기지국 수사를 불가피하게 허용할 수밖에 없는 실질적인 요건을 구체화할 필요가 있다.

○ 통신 감청의 제한

헌법재판소가 패킷감청에 대해 헌법불합치 결정을 내린만큼, 감청 요건을 보다 엄격하게 제한할 필요가 있다. 감청은 범죄혐의를 전제로 수사 목적으로만 가능하도록 제한해야 하며, 피내사자의 경우 감청 대상에서 제외해야 한다. 감청 요건도 ‘범인의 체포나 증거 수집이 불가능하거나 현저히 어려운 경우’로 엄격히 규정할 필요가 있다. 아울러 영장 청구 시에 수사기관이 통신제한조치의 구체적인 종류와 집행방법 대상 범위 기간 등을 특정하도록 명시하고, 감청의 요건을 충족하는 사유를 구체적으로 소명하도록 규정할 필요가 있다.

○ 통지 제도의 개선

수사의 필요에 의해 통신사실확인자료가 제공되거나 감청이 시행되더라도 정보주체는 이에 대해 알 권리가 있다. 그렇지 않으면, 수사기관의 부당한 행위에 대해 권리 구제를 요청할 수조차 없기 때문이다. 현행 통신비밀보호법의 규정으로는 아예 통지를 받지 못할 경우(기소중지결정이나 계속 수사 중인 경우)가 발생하는데, 일정한 기간이 경과하면 당사자에게 통지해주도록 하되, 예외적으로 법원의 허가를 얻어 유예하는 방식으로 개선될 필요가 있다.

○ 통신사실확인자료 보관 의무화 폐지

2014년 유럽사법재판소는 데이터보관지침에 대해 무효 판결을 내렸다. 국내에서도 통신비밀보호법 제15조의2 전기통신사업자의 협조 의무 조항 및 시행령을 통해 통신사실확인자료에 따라 일정기간 보관을 의무화하고 있다. 이에 따라 범죄혐의와 상관없이, 전기통신사업자의 서비스 제공 목적과 무관하게 모든 사용자의 통신 내역이 단지 수사의 필요성 때문에 보관되고 있는데, 이는 개인정보 보호원칙에 벗어날 뿐만 아니라 무죄 추정의 원칙에도 반한다. 수사기관이 서비스 제공을 위해 보관되어 있는 통신 내역에 법적 절차에 따라 접근할 수는 있지만, 단지 수사 편의를 위해 일정기간 보관을 의무화하는 제도는 폐지될 필요가 있다.

3. 중장기적인 연구 과제

다음과 같은 주제에 대해서는 대응 방안 마련을 위한 연구가 이루어질 필요가 있다.

1) 노동 감시를 통제할 수 있는 법제 마련

현행 개인정보 보호법제는 기업-소비자, 국가-시민의 관계에서의 개인정보 규제는 상당히 진전된 규범을 가지고 있지만, 기업-노동자 관계에서 개인정보 및 감시를 둘러싼 규율은 매우 미흡한 상황이다. 노동관계법령상 노동 감시에 대해서는 <근로자참여 및 협력증진에 관한 법률> 이외에 관련 규정을 찾아볼 수 없다. 이 규정도 감시 장비는 노사 양자의 협의 사항으로 규정하고 있을 뿐 노동 감시의 목적으로 활용하거나 노동자의 사생

활을 침해하는 것에 대한 내용은 없다.

정보주체의 동의는 기업 내의 불평등한 역학 관계 속에서 형식화되기 쉬우며, 기업에 의한 지능화된 감시 역시 기업의 보안이나 업무 효율화라는 명분으로 합리화되곤 한다. 반면, 플랫폼 노동 등 불안정 노동이 확대되면서 노동조합을 통한 노동자의 조직화는 갈수록 힘들어지고 있기 때문에, 노동조합을 매개로 한 노동 감시의 견제 역시 한계가 있을 수밖에 없다. 설사 노동조합을 통해 저항한다고 하더라도 특정 사업장 내에 국한될 뿐이다. 따라서 작업장 내의 지능화된 노동 감시를 규제하기 위한 법제와 이에 대한 감독 시스템이 마련될 필요가 있다.

한편, 연결되지 않을 권리의 도입을 검토할 필요가 있다. 연결되지 않을 권리는 노동시간 외의 일과 관련된 업무의 차단뿐만 아니라, 비 노동시간에서도 개인정보가 축적되는 다양한 환경을 정보주체가 '차단'할 수 있다는 의미를 지닌다.

프랑스는 노동법에 시·공간적으로 외부에 '연결되지 않을 권리'를 규정해 2017년 1월부터 시행하고 있다. 주 중 35시간 법정 노동시간에 더해 일과 외 그리고 주말에 경영자가 전화하거나 문자를 보내는 것을 불법화하는 디지털 시대의 노동·정보인권 조항이라 평가된다. 외부로부터의 자율적 연결차단권은 디지털 시대 노동 휴식권의 보장을 뜻하지만, 비 노동시간의 영역까지 틈입한 기업의 장악력을 일시 제거한다는 점에서 시사하는 바가 크다. 기술로 매개해 개인의 신체와 관련 정보를 거의 24시간 기업의 자장 속에 놓으려는 현실을 제어하기 위해 프랑스 정부는 일단 몸에 부착된 모바일 기계 장치의 가동을 멈추는 선택을 취했다. 연결되지 않고 외부 접속에서 순간 절연할 권리는, 현대 첨단 기술에 기댄 기업의 시·공간 통치 기제를 막기 위한 최소한의 정보인권으로 사유되는 셈이다.

2) 인권영향평가와 차별에 대한 규제

하버드대 버크만센터가 <인공지능과 인권, 기회와 위험>에 대한 보고서에서 지적한 바와 같이 인공지능 등 신기술은 인권에 긍정적, 부정적 영향을 미칠 수 있으며, 그 영향은 비단 개인정보 자기결정권 뿐만 아니라 표현의 자유, 집회결사의 자유, 노동권 등 인권 전반에 걸쳐있다. UN 표현의 자유 특별보고관 역시 신기술이 표현의 자유, 프라이버시권, 차별받지 않을 권리 등을 위협할 수 있다며 인권영향평가의 중요성을 강조하고 있

다. 정부는 이러한 인권영향평가가 효과적으로 시행될 수 있도록 보장할 수 있는 제도적 장치를 마련해야 한다.

개인정보와 관련해서는 이미 개인정보 영향평가가 제도화되어 있다. 현재 국내에서는 공공분야에서만 개인정보 영향평가를 시행하고 있는데, 이를 개인정보 침해 위험성이 큰 민간분야로 확대할 필요가 있다. 그러나 개인정보 외의 분야에서는 인권영향평가에 대한 제도화가 미흡한 상황이다. 국가인권위원회는 인공지능 등 신기술이 인권 전반에 미치는 영향을 평가하기 위한 인권영향평가의 제도화를 고민할 필요가 있다.

앞서 제4장에서 구체적으로 살펴보았듯이, 신기술로 인한 가장 큰 위협 중의 하나는 알고리즘에 의한 차별 문제이다. 또한 5장에서 보았던 여러 보고서에서도 신기술이 보험, 신용, 고용 등의 영역에서 특정 그룹에 대한 차별을 야기할 수 있음을 경고하고 있다. 이와 같은 신기술로 인한 차별의 문제를 최소화하기 위한 윤리적, 기술적, 제도적 방안이 마련될 필요가 있다. 앞서 언급했던 프로파일링을 포함한 자동화된 처리에 대한 거부권, 인적 개입을 요구할 권리 등 정보주체의 권리는 이와 관련된 하나의 대책이 될 수 있다. 또한 AI 개발을 위한 윤리규범이나 기업의 자율규제 원칙으로 만들어져 기업 스스로 데이터 수집 및 알고리즘 개발 단계에서 차별적 요소를 최소화하도록 노력해야 한다. 백악관 보고서에서 권고했다시피 차별을 중단하기 위한 전문 기술의 개발 및 확대 역시 필요할 것이다. 더불어 개인정보보호위원회 및 국가인권위원회는 신기술로 인한 차별이 발생하지 않는지 모니터링하고, 피해를 구제할 수 있도록 해야 한다.

3) 시민의 역량 강화

개인정보의 수집과 활용이 폭발적으로 늘어나는 4차 산업혁명 시대에서 개인정보관련 정책은 보호 중심의 기존 체계에서 정보주체의 스스로의 선택 중심으로 변화해 가고 있다. 때문에 현재의 환경 하에서 정보주체들은 보호의 객체가 아닌 주체로서 더더욱 많고 복잡한 개인정보 관련 선택들에 직면하게 된다.

개인정보의 라이프사이클 전체에서 개인정보 자기결정권의 행사가 그 어느 때보다 중요해진 만큼 개인정보의 수집, 생성, 관리는 물론 파기 등 사후처리 과정 전반에 대해 정보주체가 자신의 권리를 행사할 수 있는 역량 강화 방안이 마련될 필요가 있다. 이를 위해서 우선 인공지능 등 4차 산업혁명 기술과 관련된 리터러시를 강화하는 것이 요구된

다. 이는 정규 교육과정을 통해서 뿐만 아니라, 국가인권위원회나 개인정보보호위원회와 같은 기관들의 교육 프로그램, 혹은 대중매체를 통한 홍보 등 다양한 경로를 통해 이루어질 수 있다.

또한 시스템 전반의 투명성이 보장될 필요가 있다. 가령, 인공지능 면접 프로그램의 분석 결과는 데이터 그 자체가 아니라 코딩된 연산 결과에 따른 것이기에 알고리즘을 명확하게 이해할 수 있도록 투명한 설명을 요구할 권리가 주어지지 않는다면 여전히 그것은 블랙박스로 남게 된다. 통제가 안 되는 데이터와 알고리즘은 데이터의 조작, 악용의 위험을 높이고 사회적 편견을 강화할 경향이 다분하다. 빅데이터 알고리즘의 자동화된 의사결정이 우리 삶에 깊숙이 파고드는 지금의 맥락에서 알고리즘이 어떻게 작동하는지에서부터, 아웃풋(자동화된 의사결정)이 어떻게 만들어지는지 까지 정보주체가 그 프로세스를 명확하게 이해할 수 있도록 돕는 장치가 필요하다.

제2절 부문별·기관별 정보인권 정책 권고

1. 정부 (공공기관)

정부는 시민의 인권을 보호해야할 책임이 있는 주체임과 동시에, 스스로 인권침해의 당사자가 될 수 있는 존재다. 그렇기 때문에, 신기술에 의한 인권적 영향에 대한 정부의 인식과 책임은 무엇보다 중요하다.

UN 표현의 자유 특별보고관이 권고했듯이, 정부는 인공지능 시스템이나 도구를 도입할 때 인권 원칙이 준수될 수 있도록 보장해야 한다. 예를 들어, 공개적 의견수렴 절차를 거치거나 인권영향평가를 수행할 수 있을 것이다.

정부는 신기술과 관련된 정책 결정자, 그리고 민간 영역의 감독자로서 중요한 역할을 한다. 즉, 기업들이 신기술을 개발하고 상품을 출시하는데 있어 인권영향평가 등 필요한 조치를 취할 수 있도록 규제를 마련하고 감독을 해야 하며, 피해 구제를 위한 절차를 마련해야 한다. 하버드 버크만센터 역시 인공지능이 인권에 미치는 부정적 영향에 대응하는 효율적인 구제체제를 마련하는데 있어서 정부가 중요한 역할을 수행하며, 인공지능의 분배 결과 문제를 다루는데 있어서도 정부가 민주적 절차를 통해 역할하는 것이 필수적임을 지적하고 있다. 또한 미시적인 측면에서의 인권 침해 방지와 구제뿐만 아니라, 인공지능 기술이 소수의 손에 독점되지 않도록 경쟁 정책을 유지할 필요성에 대한 UN 표현의 자유 특별보고관의 지적도 주목할 만하다.

특히 개인정보보호위원회 및 국가인권위원회의 역할은 중요하다. 개인정보보호위원회는 개인정보 감독기구로서 일관된 개인정보 보호정책을 수립하고 민간 부문뿐만 아니라 공공 부문까지 개인정보 보호가 효과적으로 이루어질 수 있도록 감독해야 할 책임이 있다. 특히 빠르게 발전하는 기술 환경 속에서도 개인정보 보호를 보장하기 위한 혁신적인 제도를 발 빠르게 고민할 필요가 있다. 나아가 개인정보의 수집과 처리가 세계적인 수준에서 이루어지고 있는 만큼, 해외의 개인정보 감독기구와 협력하고 국제적으로 통일적인 규범이 만들어질 수 있도록 노력해야 한다.

국가인권위원회의 역할 또한 매우 중요하다. 신기술이 비단 개인정보의 권리에만 영향을 미치는 것이 아니기 때문이다. 4차 산업혁명 시대에 국가인권위원회의 역할은 다음과

같은 측면에서 고민할 필요가 있다. 첫째, 신기술의 인권적 영향을 평가하는 인권영향평가의 제도화를 위한 방안을 마련해야 한다. 둘째, 신기술의 도입이 차별에 미치는 영향을 모니터링하고 이를 구제할 수 있는 방안을 마련해야 한다. 셋째, 국가, 특히 정보수사기관에 의한 지능형 감시를 규제할 수 있는 방안을 마련해야 한다.

개인정보보호위원회와 국가인권위원회를 중심으로 정부는 아직 학계나 시민사회를 중심으로 이루어지고 있는 4차 산업혁명 시대의 윤리 및 인권 보호의 원칙을 마련하고, 정부, 업계, 그리고 일반 시민의 인식을 고양할 수 있는 교육과 캠페인을 진행할 필요가 있다.

2. 기업

기술 개발의 주체이자 신기술을 활용한 상품과 서비스의 공급자로서 기업의 책임 역시 지대하다. GDPR에서도 개인정보 보호에 있어서의 기업의 책임성을 중요시하고 있다. 기업은 신기술 개발에 관여하는 개발자, 프로그래머, 데이터 관리자들이 제품의 설계부터 출시에 이르는 전 과정에서 개인정보를 포함한 인권 보호에 대한 책임 의식을 가질 수 있도록 윤리 원칙을 수립할 필요가 있다.

또한, 이에 근거하여 개인정보 보호 중심 디자인이나 기본 설정, 개인정보 영향평가 등 문제점을 수정할 수 있는 체계를 마련해야 한다. 이는 비단 내부에서뿐만 아니라, 외부 감사나 감독기관이 사후에 감독할 수 있도록 보장하는 것을 포함한다. 자신이 개발, 출시한 시스템이 어떻게 작동하는지 투명하게 공개하고, 사용자의 불만을 접수하고 피해를 신속하게 구제하는 시스템도 마련해야 한다.

기업의 책임성을 보장하기 위해 관련 법제를 구축하고 감독기관이 모니터링하는 것도 중요하지만, 기업 스스로 자율규제 체제를 만든다면, 사회 전체적인 효율성과 실효성을 높일 수 있을 것이다. 특히, 신기술의 영향이 명확하지 않은 상황에서 새로운 법제의 마련이 많은 시간이 소요될 수 있으므로, 관련 법제의 마련 이전에도 관련 기업들이 스스로 자율규제를 통해 인권 보호를 위한 규범을 실행할 수 있다. 예를 들어, 미국의 자동차 제조사 연합은 자율주행자동차와 관련한 개인정보 보호를 위해 <자동차 기술 및 서비스를 위한 프라이버시 원칙(Privacy Principles for Vehicle Technologies and

Services)>을 제정한 바 있다.[220] 이 원칙은 투명성, 선택권, 맥락 존중, 수집 최소화, 데이터 보안, 무결성과 접근, 책임성 등의 원칙으로 구성되어 있다.

3. 소비자/사용자

시민, 소비자/사용자, 노동자로서 개인의 역량 역시 중요하다. 시민 스스로 문제점을 인식하고 문제제기하지 않는다면 자신의 피해를 구제하기 힘들뿐더러, 기업의 관행과 제도의 변화 역시 끌어내기 힘들기 때문이다. 실제로 기업의 관행을 변화시키는 것은 정부의 규제 때문이 아니라, 소비자의 반응 때문일 경우가 많다. 정부 역시 시민의 문제제기가 없다면 인권 침해적 관행을 교정하려는 노력을 게을리 할 것이다.

물론 시민의 역량 강화를 위한 국가적인 노력 역시 필요하다. 특히, 기술의 복잡성과 시스템의 불투명성이 높아가는 상황에서 시민들의 리터러시는 더욱 중요해질 수밖에 없다.

220) Auto Alliance. PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES. 2014.11.12

참고문헌

국내외 참고 문헌

참 고 문 헌

1. 국내 자료

[1] 개인정보보호위원회 결정 제2017-14-122호.「개인정보 보호법」일부개정 법률안 의견 조회에 관한 건. 2017.6.26.

[2] 개인정보보호위원회 결정 제2018-08-078호. 「개인정보 보호법」 일부개정안 (의안번호 12312) 의견 조회에 관한 건. 2018.4.9.

[3] 개인정보보호위원회 결정 제2018-08-079호. 「개인정보 보호법」 일부개정안 (의안번호 12289) 의견 조회에 관한 건. 2018.4.9.

[4] 과학기술정보통신부. 2017 R&D KIOSK 제45호. 2018. 2.

[5] 건강과대안 등. [기자회견] 개인정보 판매와 공유를 허용하는 개인정보보호법 반대한다!. 2018.11.21. https://act.jinbo.net/wp/40024/

[6] 건강권실현을위한보건의료단체연합 등. 시민사회. 규제프리존법 폐기 요구하는 의견서 발표. 2016.5.3.

[7] 건강사회를위한약사회 등. 시민단체. 고객정보 3억4천여만 건 무단 결합한 비식별화 전문기관 및 20개 기업 고발. 2017.11.9.

[8] 경기장애인차별철폐연대 등. 김포경찰서·김포시청의 개인정보공유에 대한 헌법소원 청구 기자회견. 2016.6.14.

[9] 경기장애인차별철폐연대 등. 김포경찰서와 김포시청의 활동지원관련 무작위 개인정보공유에 대한 헌법재판소의 나쁜 결정을 규탄한다. 2018.9.16. https://act.jinbo.net/wp/39548/

[10] 경제민주화실현전국네트워크 등. 최순실이 청탁한 규제프리존법 폐기 촉구 기자회견. 2017.2.28.

[11] 경제정의실천시민연합 등. [성명] 개인정보보호 무력화하는 규제 샌드박스 반대한다. 2018.8.16

[12] 경제정의실천시민연합 등. 빅 데이터 활성화 위해 개인정보 보호체계와 감독기구 일원화 시급하다!. 2018.5.17.

[13] 경제정의실천시민연합 등. 방통위의 「빅 데이터 개인정보보호 가이드라인(안)」에 대한 시민단체 입장. 2013.12.30.

[14] 경제정의실천시민연합 등. 방송통신위원회의 「빅 데이터 개인정보보호 가이드라인」 통과에 대한 입장. 2014.12.24.
[15] 공안기구감시네트워크. 국가정보원의 '패킷감청'에 대한 두번째 헌법소원 청구 기자회견. 2016.3.29
[16] 국가인권위원회. 정보인권보고서. 2013.
[17] 국가인권위. 「신용정보의 이용 및 보호에 관한 법률 일부개정법률안」에 대한 의견표명. 2016. 10. 13.
[18] 국가인권위원회. 바이오 정보 수집. 이용 실태조사. 2016.
[19] 권건보 외. 지능정보사회 대응을 위한 개인정보보호 법제 정비방안. 개인정보보호위원회 정책연구용역 보고서. 2017.12
[20] 규제자유특구법(규제프리존법) 설명 기자 간담회. 2018.10.11. https://act.jinbo.net/wp/39689/
[21] 김건우. 인공지능에 의한 일자리 위험 진단. LG경제연구원. 2018.
[22] 김기곤. 한국사회의 문화권 구성과 제도화. 민주주의와 인권 11(2): 207-238. 2011
[23] 김기일. KISTI Market Report. 2016.
[24] 김용균. 스마트홈을 넘어 다양한 분야로 확산되는 IoT. 주간기술동향. 정보통신기술진흥센터. 2018. 4. 25.
[25] 김일환. 현행 개인정보보호법체계상 감독기구 법제정비방안에 관한 연구. 미국헌법연구 28(2). 2017.
[26] 김종길. 기술위험의 사이버화와 프라이버시권. 사회이론 (35). 2009
[27] 김현. 황승구. IoT의 과거. 현재 그리고 미래. 전자통신동향분석 제33권 제2호. 2018년 4월.
[28] 남지원. 플랫폼 통해 일감 맡는 '노동자 아닌 노동자들'. 경향신문. 2018. 10. 29.
[29] 데이비드 와일. 균열 일터. 송연수 역. 황소자리. 2015.
[30] 민영성·박희영. 통신정보보관제도의 정당성 : 유럽사법재판소 및 오스트리아 헌법재판소 판결의 관점에서. 법학논문집 40(1). 중앙대학교 법학연구원. 449~473. 2016.
[31] 민주사회를위한 변호사모임 등. [기자회견] 통신자료 무단수집 피해자 5백 명 헌법소원 심판청구. 2016.5.18
[32] 박선우. 빅데이터 시대와 데이터 융합. 정보통신방송정책 30(1). 정보통신정책연구원. 2018.
[33] 박유리 외. 인터넷의 진화와 사회경제적 패러다임 변화연구: 사물인터넷을 중심으로. 정보

통신정책연구원. 2015.
[34] 베르나르 스티글러·아리엘 키루. 고용은 끝났다. 일이여 오라!. 권오룡 역. 문학과지성사. 2015.
[35] 슬라보예(Slavoj Žižek). 김영희(역). 반인권론. 창작과비평 34(2): 404쪽. 2006.
[36] 오병일. 정보사회 세계정상회의를 계기로 본 정보인권. 문화과학 통권 제35호. 문화과학사. 2003.
[37] 윤일영. 바이오와 보안의 융합. 생체인식 기술. 융합연구정책센터. 2018.
[38] 윤현기. 올해 국내 빅데이터 시장 규모 5600억…전년비 30.2% 증가. 데이터넷. 2018. 5. 9.
[39] 이광석. 데이터 사회 비판. 책읽는수요일. 2017.
[40] 이민영. 정보인권의 법적 의의와 좌표. 공동학술세미나 - 정보인권의 법적 보장과 그 구체화. 국가위원회. 2010.
[41] 이상경, 남정아. 미국의 개인정보 보호법제 연구. 개인정보보호위원회 연구용역. 2017.12
[42] 이상윤 등. 바이오 정보 수집·이용 실태조사. 국가인권위원회 2016년도 인권상황실태조사 연구용역보고서. 2016.11
[43] 이원태. 인공지능 알고리즘의 법규범 이슈와 정책과제. 정보인권연구소 제1차 정보인권포럼. 2018.
[44] 이은우 등. 데이터 연계·결합 지원제도 도입방안 연구. 개인정보보호위원회 연구 용역. 2017.12
[45] 이은우, 심우민, 오병일. EU GDPR등 개인정보보호 규범 및 감독기구의 국제표준 확립 필요성 연구. 개인정보 보호위원회 연구보고서. 2018.
[46] 이인호. 정보인권의 개념과 헌법적 보장체계. 국가인권위원회. 2009.
[47] 이인호 등. 한국의 개인정보보호 수행체계 발전방안 연구. 개인정보보호위원회 정책연구용역 보고서. 2017.6.
[48] 이항우. 구글의 정동 경제(Affective Economy). 경제와사회 여름호(통권 제102호). 2014.
[49] 인권단체연석회의 공권력감시대응팀 등. 철도파업 휴대전화 실시간 위치추적 및 공공기관의 개인정보 경찰 제공에 대한 헌법소원 청구 기자회견. 2014.5.13
[50] 장미경. 시민권(citizenship) 개념의 의미 확장과 변화. 한국사회학 35(6): 59-77. 2001.
[51] 정민경. 국가인권위원회 10년: 정보인권과 국가위원회의 역할. 이슈리포트 <액트온>. 진보네트워크센터. 2012.
[52] 정보통신산업진흥원. 2017년도 사물인터넷 산업 실태조사. 2017.

[53] 정호윤. 인공지능 비서가 그리는 새로운 인터넷 지형도. Issue Report: 인터넷/인공지능(AI). 유진투자증권. 2018. 4. 17.
[54] 조성은. 이원태. 이시직. 2018. "4차 산업혁명 대응 법제 정비 연구". 방송통신정책연구 17-방통-83.
[55] 중앙일보. 경찰. 개인정보 37억건 보유…형사사법정보시스템 27억건. 2017.10.15
[56] 진보네트워크센터 등. 서울중앙지방법원 2015고합665 개인정보보호법위반 등에 관한 의견서. 2016. 12. 9.
[57] 진보네트워크센터 등. 철도노조 노동자의 건강정보 제공 사건. 위헌으로 확인되다. 2018.8.31. https://act.jinbo.net/wp/39270/
[58] 최대선 외. 소셜네트워크서비스 개인정보 노출 실태 분석. 정보보호학회논문지 23(5). 2013.
[59] 최재홍. 4차 산업혁명. 세계 각국과 기업은 어떻게 준비하고 있을까?. 삼성증권 뉴스룸.
[60] 캐시 오닐. 디지털 골상학. 대량살상수학무기. 김정혜 역. 흐름출판. 2017.
[61] 프랭크 파스콸레. 블랙박스 사회. 이시은 역. 안티고네. 2016.
[62] 한겨레. 정부. 가명정보 결합 데이터 외부반출도 허용 추진. 2018.9.18.
[63] 한겨레. 한국 경찰. '마이너리티 리포트' 만든다. 2016.2.4
[64] 한국소비자원. 사물인터넷 관련 개인정보관리에서의 소비자권익 강화 연구. 2017.
[65] 한국일보. 문재인-안철수의 새로운 전선. 규제프리존 법안. 2017.4.10.
[66] 한국정보화진흥원. 2016 빅데이터 시장현황조사.
[67] CIO Korea. 2018년 글로벌 인공지능 비즈니스 가치 1조 2.000억 달러. 가트너 전망. 2018. 4. 26.
[68] ICO(Information Commissioner's Office). Big Data. Artificial Intelligence. Machine Learning and Data Protection. 개인정보보호위원회 번역. 2017. http://www.pipc.go.kr/cmt/not/ntc/selectBoardArticle.do?nttId=5541&bbsId=BBSMSTR_000000000118&bbsTyCode=BBST03&bbsAttrbCode=BBSA03&authFlag=Y&pageIndex=1.
[69] Latanya Sweeney. Ji Su Yoo. 처방 데이터상 공유되는 대한민국 주민등록번호의 익명성 해제 번역문(국회도서관 번역). 2016.
[70] Rüdiger Krause. "노동세계의 디지털화: 과제와 규제의 필요성. 국제노동브리프". 2017년 3월호. 한국노동연구원

2. 국외 자료

[1] Acemoglu. D and P Restrepo. The Race Between Machine and Man: Implications of Technology for Growth. Factor Shares and Employment. NBER Working Paper No. 22252. 2016.

[2] Anders Albrechtslund. Online Social Networking as Participatory Surveillance. First Monday. Volume 13. Number – 3 March 2008. http://firstmonday.org/ojs/index.php/fm/article/view/2142/1949

[3] Andrejevic. Mark. The Work That Affective Economics Does. Cultural Studies 25(4–5): 604~620. 2011.

[4] Albrechtslund. Anders. Online social networking as participatory surveillance. *First Monday*. 13(3). March. 2008. http://firstmonday.org/ojs/index.php/fm/article/view/2142

[5] Arntz. M. T Gregory. and U Zierahn. The Risk of Automation for Jobs in OECD Countries. OECD Social. Employment and Migration Working Papers. No. 189. OECD. 2016.

[6] Askitas N. and Zimmermann K.F. The internet as a data source for advancement in social sciences. International Journal of Manpower. 36 (1). 2–12. 2015.

[7] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Automated individual decision–making and Profiling for the purpose of Regulation. 2016/679. 2017.

[8] ARTICLE 29 DATA PROTECTION WORKING PARTY. WP 242 rev.01 Guidelines on the right todata portability. 5 April 2017.

[9]Auto Alliance. PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES. 2014.11.12

[10] Autor. D. Why are there still so many Jobs? The History and Future of Workplace Automation. Journal of Economic Perspectives. Vol. 29. No. 3. 2015.

[11]Council of Europe. The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13 and explanatory memorandum.

[12] Digital Rights Ireland – joined cases 293/12 and 594/12 and Tele2–Watson, joined cases C–203/15 and C–698/15.

[13] EDRi. "ePrivacy: Civil society letter calls to ensure privacy and reject data retention". 2018.4.24.

https://edri.org/eprivacy-civil-society-letter-calls-to-ensure-privacy-and-reject-data-retention/.

[14] EDRi. UN Special Rapporteur analyses AI's impact on human rights. 2018.11.7.

[15] EDRi(European Digital Rights). "Dear MEPs: We need you to protect our privacy online!". 2017. 10. 5. https://edri.org/dear-meps-we-need-you-to-protect-our-privacy-online/.

[16] EDPS. Meeting the challenges of big data : A call for transparency. user control. data protection by design and accountability. Opinion 7/2015. 2015. https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf.

[17] Eli Pariser. The Filter Bubble. Penguin. 2011

[18] Filippo A. Raso. Hannah Hilligoss. Vivek Krishnamurthy. Christopher Bavitz. Levin Kim. Artificial Intelligence & Human Rights: Opportunities & Risks. The Berkman Klein Center for Internet & Society Research Publication Series. 2018.9.25.

[19] Frey. C B and M A Osborne. The Future of Employment: How Susceptible are Jobs to Computerisation?. Mimeo. Oxford Martin School. 2015.

[20] FTC. Protecting Consumer Privacy in an Era of Rapid Change. 2012.3.

[21] FTC Staff Report . The Internet of Things : Privacy & Security in a Connected World. 2015.1.

[22] FRA(European Union Agency for Fundamental Rights and Council of Europe). Handbook on European data protection law. 2018.

[23] Fuchs. Christian. Social Media: A Critical Introduction. London: Sage. 2014.

[24] Future of Life Institute. ASILOMAR AI PRINCIPLES. https://futureoflife.org/ai-principles/

[25] Goggin. Gerard. Adriadne Vromen. Kimberlee Weatherall. Fiona Martin. Adele Webb. Lucy Sunman & Francesco Bailo. Digital Rights in Australia. Departments of Media and Communications. and University of Sydney. 2017.

[26] ICDPPC. Declaration on Ethics and Data Protection in Artificial Intelligence. 40th International Conference of Data Protection and Privacy Commissioners. 2018.10.23.

[27] Joy Buolamwini. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. MIT Media Lab. 2018.1.15.

[28] Lee. Edwards. Bethany Klein. David Lee. Giles Moss and Fiona Philip. Framing the Consumer: Copyright Regulation and the Public. Convergence. 19(1). 2012.

[29] Mark Hung. Leading the IoT. Gartner. 2017.
[30] Mouffe. ed.. Dimensions of Radical Democracy: Pluralism. Citizenship. Community. New York: Verso. 1992.
[31] NIST(2016), “De-Identifying Government Datasets (2nd Draft)”, NIST Special Publication (SP) 800-188(2016. 12. 15), 10p
[32] Ralph Finos. Wikibon Big Data in the Public Cloud Forecast: 2016-2026. 2016.
[33] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations. 2018.8.28.
[34] Reforming the U.S. Approach to Data Protection and Privacy. https://www.cfr.org/report/reforming-us-approach-data-protection
[35] Report of the Special Rapporteur on the right to privacy. Joseph A. Cannataci. A/HRC/34/60. 2017.2.24
[36] Resolution adopted by the General Assembly on 18 December 2013 : 68/167. The right to privacy in the digital age.
[37] The Center for Global Enterprise. Global Platform Survey. 2015.
[38] The Center for Popular Democracy. The Grind: Striving for Scheduling Fairness at Starbuks. 2015.
[39] The Office of the United Nations High Commissioner for Human Rights. The right to privacy in the digital age : Report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/27/37. 30 June 2014.
[40] The right to privacy in the digital age. A/HRC/34/L.7/Rev.1. 27 February to 24 March 2017
[41] UK ICO. Feedback request - profiling and automated decision-making. 2017.
[42] UN Human Rights Committee. Concluding observations on the fourth periodic report of the Republic of Korea. Adopted by the Committee at its 115th session 19 October-6 November 2015.
[43] UN Human Rights Office of the High Commissioner. Guiding Principles on Business and Human Rights. 2011.
[44] UN. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/73/348. 2018.8.29
[45] Wagner. Ben. Global Free Expression: Governing the Boundaries of Internet Content. Cham.

Switzerland:Springer International Publishing. 2016.

[46] White House. Consumer Data Privacy in a Netwokred World – A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. 2012.2

[47] White House Executive Office of the President. Big Data: A Report on Algorithmic Systems. Opportunity. and Civil Rights. 2016.5.

[48] White House Executive Office of the President. BIG DATA: SEIZING OPPORTUNITIES. PRESERVING VALUES. 2014.5.1

부록

전문가 및 시민 설문지

[부록 1] 4차 산업혁명과 정보인권 전문가 조사 설문지

1. 현재 한국사회에서 4차 산업혁명 이름하에 기술 및 생산환경을 질적으로 바꾸려는 논의들이 활발히 이루어지고 있습니다. 이에 문재인 정부도 '대통령산하 4차산업혁명위원회'를 구성하는 등 4차 산업혁명에 적극 대응하고 있습니다. 한편, 4차 산업혁명 혹은 신기술의 도입에 따라 일자리 상실과 프라이버시 침해 등 여러 우려도 제기되고 있습니다. 관찰하시건데, 4차 산업혁명의 신기술 도입에 따른 '정보인권' 침해와 관련하여, 가장 심각하게 대두될 문제가 무엇이고 그 원인은 무엇이라고 생각하십니까?

2. 이미 한국 사회에서는 대량의 개인정보 유출 사고가 발생한 바 있습니다. 이에 더하여 빅데이터의 활용과 사물인터넷의 확장 등으로 개인정보의 유출 위험이 어느 때보다 높아질 것이라는 우려가 있습니다. 한국 사회에서 개인정보 유출 사고가 빈발하는 주된 이유는 무엇이고, 개인정보 유출을 막기 위한 효과적인 방안은 무엇이라고 생각하십니까?

3. 최근 가명정보의 활용 범위를 둘러싼 논란이 커지고 있습니다. 가명정보란 특정 목적으로 수집된 개인정보를 가명화 처리한 후 목적 외로 활용할 수 있도록 허용하는 정책입니다. 시민사회는 가명정보의 사용을 '학술연구 및 통계' 목적으로 제한해야 한다고 주장하고 있습니다. 반면 산업계는 가명정보의 사용을 기업의 영리적인 연구 목적까지 확대해야 한다고 주장합니다. 가명정보의 목적 외 활용의 범위 및 활용 조건과 관련한 선생님의 의견은 어떠신지요?

4. 취업 현장에서 면접자의 표정, 목소리, 뇌파, 심장박동 등을 감지하는 인공지능 시스템이 도입되는 등, 최근 인공지능 기술을 다양한 분야에서 도입하고 있습니다. 그런데 인공지능 알고리즘이 여성이나 소수자에 대한 사회적인 편견을 그대로 반영한다든가, 인공지능에 의한 의사 결정이 사회적인 차별을 야기할 수 있다는 우려도 제기되고 있습니다. 이와 같은 알고리즘 편향성과 차별에 대한 우려는 현실적인 것인지, 그렇다면 이를 극복하기 위한 방안은 무엇인지 선생님의 의견은 어떠신지요?

5. 빅데이터나 인공지능과 같은 신기술은 수사기관에 의해서도 활용되고 있습니다. 예를 들어, 얼굴이나 움직임을 인식하는 지능형 CCTV가 도입되고 빅데이터에 기반한 범죄예측시스템이 개발되고 있습니다. 생산현장에서도 마찬가지입니다. RFID 카드를 넘어 인공지능과 스마트폰

앱 등을 통하여 실시간으로 노동자의 활동을 감시할 수 있는 기술이 발전하고 있습니다. 물론 이러한 감시 기술은 범죄 예방이나 기밀 유출 방지 등의 목적을 위해 도입됩니다. 이러한 기술들이 필요이상으로 남용되지 않을 수 있는 방안은 무엇이라고 생각하십니까.

6. SNS 상의 각종 선호 정보(좋아요, 싫어요 등)나 사용자의 이용기록에 근거한 광고 등 개인의 내밀한 정신적, 정서적 정보들도 수집, 활용되고 있습니다. 개인 맞춤형 서비스는 사용자에게 편의를 제공할 수도 있지만, 자신도 모르는 정보 이용의 편식과 공동체의 소통 부재에 대한 우려도 제기되고 있습니다. 한편, 이러한 정보들은 상업적인 목적을 넘어 정치적으로 이용될 수도 있는데, 미국 대선과정에서 페이스북의 개인정보가 활용된 사례는 개인정보의 남용이 여론의 왜곡과 공동체의 민주주의에 부정적 영향을 미칠 가능성을 보여줍니다. 이에 대한 사회적인 대응이 필요한 것인지, 필요하다면 어떠한 방안이 있을 수 있는지 선생님의 의견을 듣고 싶습니다.

7. 끝으로, 선생님의 전문 영역에서 정보인권 보호를 위해 하고 싶은 말씀을 부탁드립니다.

[부록 2] 2018 정보인권 실태조사 시민설문지

— 4차 산업혁명 시대에서 정보인권 보호를 위한 실태조사

패널님의 소중한 의견이 큰 도움이 됩니다. 각 질문에는 정답이 없으니 귀하의 경험과 생각을 바탕으로 솔직하게 응답해주세요

> * **4차 산업혁명이란?**
> 4차 산업혁명은 정보통신기술의 융합에 기반한 총체적인 산업 혁신을 일컫습니다. 빅 데이터 분석, 인공지능, 로봇공학, 사물인터넷, 무인 운송 수단(무인 항공기, 무인 자동차), 3D 인쇄, 나노 기술과 같은 분야의 새로운 기술 혁신이 대표적인 사례로 꼽힙니다.

Q1. 먼저, 4차 산업혁명 기술과 관련한 질문을 드리겠습니다. 귀하는 4차 산업혁명*에 대해 들어보신 적이 있습니까?

① 전혀 들어본 적 없다 ☞ 선택 시 8번 문항으로 이동
② 용어는 들어봤으나 의미는 잘 모른다
③ 의미는 알고 있으나 세부적인 내용은 모른다
④ 의미와 내용을 잘 알고 있다

Q2. 귀하는 4차 산업혁명 기술을 응용한 다음의 서비스를 실제 이용하거나 체험한 적이 있습니까?

인공지능 스피커 (기가지니, 빅스비 등)

① 아예 접해본 적이 없다

② 들어봤지만 접해본 적은 없다
③ 가끔씩 접하고 있다
④ 자주 접한다

Q3. 귀하는 4차 산업혁명 기술을 응용한 다음의 서비스를 실제 이용하거나 체험한 적이 있습니까?

스마트워치 (삼성스마트워치, 애플 워치 등)

① 아예 접해본 적이 없다
② 들어봤지만 접해본 적은 없다
③ 가끔씩 접하고 있다
④ 자주 접한다

Q4. 귀하는 4차 산업혁명 기술을 응용한 다음의 서비스를 실제 이용하거나 체험한 적이 있습니까?

클라우드 서비스 (구글 드라이브, 아이클라우드 등)

① 아예 접해본 적이 없다
② 들어봤지만 접해본 적은 없다
③ 가끔씩 접하고 있다
④ 자주 접한다

Q5. 귀하는 4차 산업혁명 기술을 응용한 다음의 서비스를 실제 이용하거나 체험한 적이 있습니까?

본인 인증 서비스 (지문, 홍채, 안면 인식 서비스)

① 아예 접해본 적이 없다
② 들어봤지만 접해본 적은 없다
③ 가끔씩 접하고 있다
④ 자주 접한다

Q6. 귀하는 4차 산업혁명 기술을 응용한 다음의 서비스를 실제 이용하거나 체험한 적이 있습니까?

타게팅 광고 (구글 애드센스, 유튜브 추천 영상 등)

① 아예 접해본 적이 없다
② 들어봤지만 접해본 적은 없다
③ 가끔씩 접하고 있다
④ 자주 접한다

Q7. 귀하는 4차 산업혁명 기술을 응용한 다음의 서비스를 실제 이용하거나 체험한 적이 있습니까?

홈 오토메이션
(스마트 홈 시스템, 놀이터 CCTV 등)

① 아예 접해본 적이 없다
② 들어봤지만 접해본 적은 없다
③ 가끔씩 접하고 있다
④ 자주 접한다

Q8. 4차 산업혁명에 대한 귀하의 평상시 견해는 다음 중 어떤 생각에 가장 가까운 편입니까?

① 당장 일어나지 않을 미래의 일이다
② 부작용에 대해서는 경계를 할 필요가 있다
③ 생활의 편의를 높여준다
④ 미래산업과 경제발전을 위해 매우 중요하다

Q9. 다음으로, 정보인권*과 관련한 귀하의 견해를 여쭙겠습니다. 귀하는 인공지능 스피커, 스마트워치, 클라우드 서비스, 드론 등 신기술 서비스를 통해 귀하의 개인정보가 수집되는 경우가 있다는 것을 알고 계십니까?

*** 정보인권이란?**

최근 정보 인권으로 주목받고 있는 것은 표현의 자유, 프라이버시권, 정보 공유의 권리, 접근권입니다. 이 권리들은 정보와 커뮤니케이션과 관련이 있기 때문에 정보 사회에서 필수적으로 보장받아야 하는 권리입니다. 동시에 행정 효율과 이윤 창출을 꾀하는 정부와 시장 주도의 정보화로 인하여 위협받고 있는 권리이기도 합니다.

① 전혀 모르고 있다 ② 잘 모르는 편이다 ③ 대충 짐작하는 정도이다
④ 대체로 알고 있다 ⑤ 아주 잘 알고 있다

Q10. 귀하는 포털서비스, 통신회사 및 보험회사 같은 기업들이 이용자의 개인정보를 보호하는 것에 대해 어느 정도로 신뢰하십니까?

① 전혀 믿을 수 없다 ② 대체로 믿지 못하는 편이다 ③ 보통이다
④ 대체로 신뢰하는 편이다 ⑤ 매우 신뢰한다

Q11. 귀하는 의료나 금융기관 같은 공공기관과 정부가 이용자(국민)의 개인정보를 보호하는 것에 대해 어느 정도로 신뢰하십니까?

① 전혀 믿을 수 없다 ② 대체로 믿지 못하는 편이다 ③ 보통이다
④ 대체로 신뢰하는 편이다 ⑤ 매우 신뢰한다

Q12. 귀하의 개인정보 중 가장 먼저 보호되어야 하는 것이 있다면 다음 중 어떤 것입니까? 하나만 골라 응답해주십시오.

① 위치 정보 ② 건강 및 생체 정보 ③ 금융 및 신용 정보
④ 통신 기록 ⑤ 음성 및 영상 기록 ⑥ 기타 ( )

Q13. 요즘 온라인 쇼핑몰이나 온라인 서점에서는 이용자의 개인정보나 상품 조회 및 구매 이력을 활용해 '개인별 맞춤 광고'나 '상품 추천 서비스'를 하고 있습니다. 이러한 서비스에 대해 귀하는 어떻게 생각하십니까?

① 매우 부정적으로 생각한다 ② 대체로 부정적으로 생각하는 편이다
③ 보통이다 ④ 대체로 긍정적으로 생각하는 편이다
⑤ 매우 긍정적으로 생각한다

Q14. 최근 이동통신업체에서는 고객 자녀의 안전을 위해 '등하교 안심 서비스' 등을 제공하고 있습니다. 서비스 업체에서 자녀의 위치정보를 수집 및 활용한다면, 이에 대해 어떻게 생각하십니까?

① 매우 부정적으로 생각한다 ② 대체로 부정적으로 생각하는 편이다
③ 보통이다 ④ 대체로 긍정적으로 생각하는 편이다
⑤ 매우 긍정적으로 생각한다

Q15. 귀하께서 차후에 자율주행자동차를 이용한다고 가정해보겠습니다. 이때 귀하의 운행 습관이나 위치, 동선 정보 등이 서비스 업체로 전송된다면, 이에 대해 어떻게 생각하십니까?

① 매우 부정적으로 생각한다 ② 대체로 부정적으로 생각하는 편이다
③ 보통이다 ④ 대체로 긍정적으로 생각하는 편이다
⑤ 매우 긍정적으로 생각한다

Q16. 스마트 폰이나 스마트 의료 기기에 심박수 등 개인 생체 정보가 기록되고 전송되는 '스마트 헬스 케어'사업이 추진되고 있습니다. 한쪽에서는 4차 산업혁명의 유망 산업이라는 점에서 도입을 강력히 요구하고, 다른 쪽에서는 의료의 영리화와 개인정보 유출을 우려하며 반대하기도 합니다.

① 매우 부정적으로 생각한다 ☞ 18번 문항으로 이동
② 대체로 부정적으로 생각하는 편이다 ☞ 18번 문항으로 이동
③ 보통이다
④ 대체로 긍정적으로 생각하는 편이다 ☞ 17번 문항으로 이동
⑤ 매우 긍정적으로 생각한다 ☞ 17번 문항으로 이동

Q17. [16번 문항에서 긍정적으로 답한 경우에만] '스마트 헬스 케어' 시스템에 대해 긍

정적으로 생각하신 이유는 무엇입니까? (복수응답 가능)

① 진단 절차가 간편해서
② 시간을 절약할 수 있어서
③ 의료 비용을 아낄 수 있어서
④ 꾸준한 건강 관리가 가능해서
⑤ 가족 또는 지인과 측정 결과를 공유할 수 있어서
⑥ 새로운 부가가치 산업 창출에 기여할 수 있어서
⑦ 기타 ( )

Q18. [16번 문항에서 부정적으로 답한 경우에만] '스마트 헬스 케어' 시스템에 대해 부정적으로 생각하신 이유는 무엇입니까? (복수응답 가능)

① 의사나 간호사 없이 기계가 측정한 것을 믿을 수가 없어서
② 건강 및 생체 정보가 기록되고 수집되는 게 부담스러워서
③ 신원 확인이 가능한 민감한 생체 정보(지문, 홍채, DNA 등) 노출이 꺼림칙해서
④ 수집된 개인정보들이 유출될 것 같아서
⑤ 의료의 공공성을 해치고 영리화 하는 방향이기 때문에
⑥ 국민이 아닌 통신 및 의료 기기 기업의 이익만 키울 뿐이어서
⑦ 기타 ( )

Q19. 최근에는 고객의 신용카드 사용 패턴을 빅데이터 형태로 활용한 개인별 맞춤형 서비스 상품 등이 제공되고 있기도 합니다. 이렇게 수집된 개인정보는 보험료 산정 및 신용평가 등의 목적으로 금융기관에 제공됩니다.

① 매우 부정적으로 생각한다　② 대체로 부정적으로 생각하는 편이다
③ 보통이다　④ 대체로 긍정적으로 생각하는 편이다
⑤ 매우 긍정적으로 생각한다

Q20. 경찰이 범죄 예방 및 단속을 위해 지나가는 시민의 얼굴을 인식하고 신원을 확인할 수 있는 지능형 CCTV를 설치한다면, 이에 대해 어떻게 생각하십니까?

① 매우 부정적으로 생각한다 ② 대체로 부정적으로 생각하는 편이다
③ 보통이다 ④ 대체로 긍정적으로 생각하는 편이다
⑤ 매우 긍정적으로 생각한다

Q21. 최근에는 개인정보 유출 및 사생활 침해 문제 때문에, 수집된 개인정보 중 신원 확인이 가능한 일부 정보를 제거(익명 또는 가명으로 처리)하여 활용하는 데이터 융합기술이 대안으로 떠오르고 있습니다. 일각에서는 데이터를 조합하는 과정에서 결과적으로 개인의 신원이 밝혀질 우려가 있다는 지적도 있습니다.

귀하의 동의 없이 귀하의 개인정보가 '익명/가명' 형태로 다른 기관에 제공된다면, 이에 대해서는 어떻게 생각하십니까?

① 매우 부정적으로 생각한다 ☞ 23번 문항으로 이동
② 대체로 부정적으로 생각하는 편이다 ☞ 23번 문항으로 이동
③ 보통이다
④ 대체로 긍정적으로 생각하는 편이다 ☞ 22번 문항으로 이동
⑤ 매우 긍정적으로 생각한다 ☞ 22번 문항으로 이동

Q22. [21번 문항에서 긍정적으로 답한 경우에만] '개인정보 익명/가명' 처리에 대해 긍정적으로 생각하신 이유는 무엇입니까? (복수응답 가능)

① 개인정보 보호에 대한 현행법을 준수할 수 있어서
② 가명 처리를 통해 이용자들의 사생활을 보호할 수 있어서
③ 관련 기관들의 개인정보 보안 수준을 믿을 수 있어서
④ 빅데이터 수집 및 활용을 확산할 수 있어서
⑤ 기타 ( )

Q23. [21번 문항에서 부정적으로 답한 경우에만] '개인정보 익명/가명' 처리에 대해 부정적으로 생각하신 이유는 무엇입니까? (복수응답 가능)

① 개인정보 보호에 대한 현행법을 신뢰할 수 없어서
② 결과적으로는 개인정보가 식별되고 이용자들의 사생활이 노출되어서
③ 관련 기관들의 개인 정보 보안 수준을 믿을 수 없어서
④ 빅데이터 관련 산업을 추진하기 위해 마련한 미봉책 같아서
⑤ 기타 ( )

Q24. 최근 취업 현장에서는 인공지능이 면접자의 표정, 목소리, 뇌파, 심장박동 등 감지하는 시스템이 도입되고 있습니다. 취업 면접을 볼 때 인공지능이 면접의 당락을 좌우한다면, 이에 대해서 어떻게 생각하십니까?

① 매우 부정적으로 생각한다　② 대체로 부정적으로 생각하는 편이다
③ 보통이다　④ 대체로 긍정적으로 생각하는 편이다
⑤ 매우 긍정적으로 생각한다

Q25. 귀하께서는 직장 생활 경험이 있으십니까?

① 예
② 아니오

Q26. 귀하께서는 휴일 또는 퇴근 이후 휴대전화(스마트기기) 또는 이메일 등을 통해 업무관련 지시를 받거나 전달한 경험이 있으신가요?

① 전혀 그렇지 않다　② 그렇지 않은 편이다
③ 가끔씩 경험하고 있다　④ 자주 경험하는 일이다

Q27. 다음 중 직장생활에서 경험해 보신 신기술을 모두 골라주세요. (복수응답 가능)

① 전자신분증(출입카드, RFID) 사용

② 지문 등 생체인식을 활용한 출입 관리

③ 업무용 애플리케이션(전용 메신저, 스케줄러, 업무관리 프로그램 등) 사용

④ GPS, 스마트기기, 네비게이션 등을 통한 위치정보 수집

⑤ SNS 사용에 대한 모니터링

⑥ 지능형 CCTV

⑦ 기타 ( )

Q28. 기업이 4차 산업혁명 신기술로 인사 관리 및 조직 관리를 한다면 이에 대해 어떻게 생각하십니까?

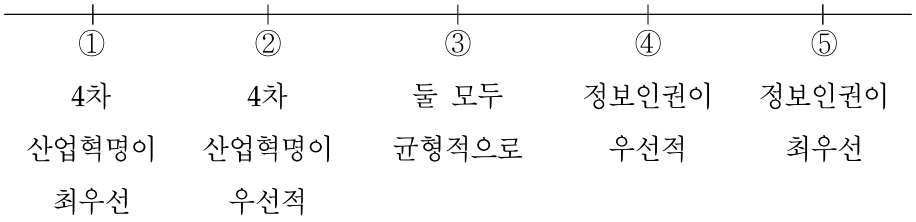
① 매우 부정적으로 생각한다 ② 대체로 부정적으로 생각하는 편이다

③ 보통이다 ④ 대체로 긍정적으로 생각하는 편이다

⑤ 매우 긍정적으로 생각한다

Q29. 4차 산업혁명의 신기술은 시민들의 삶을 편리하게 하고 경제 발전에도 도움을 준다는 진단이 있습니다. 그렇지만 이 때문에 시민들의 정보인권이 억제될 위험이 있다는 반론도 있습니다.

귀하께서는 관련 법률과 제도를 도입 및 운영할 때 '4차 산업혁명'과 '정보인권' 중 어느 가치가 더 우선해야 한다고 보십니까?



Q30. 다음은 신기술과 정보인권 문제를 개선하기 위한 정책 방향들입니다. 각 정책 방향이 얼마나 중요하다고 생각하시는지 답변해주십시오.

4차 산업혁명의 성공을 위해서 정보인권 보호 등의 '규제를 완화'한다

①	②	③	④	⑤
매우 불필요	불필요 한 편	보통	중요한 편	매우 중요

Q31. 다음은 신기술과 정보인권 문제를 개선하기 위한 정책 방향들입니다. 각 정책 방향이 얼마나 중요하다고 생각하시는지 답변해주십시오.

사생활 침해 등 피해를 입은 사람들에 대한 '사후적 구제' 제도를 마련한다

①	②	③	④	⑤
매우 불필요	불필요 한 편	보통	중요한 편	매우 중요

Q32. 다음은 신기술과 정보인권 문제를 개선하기 위한 정책 방향들입니다. 각 정책 방향이 얼마나 중요하다고 생각하시는지 답변해주십시오.

기업이나 정부의 신기술 남용을 '관리·감독'할 제도적 장치를 마련한다

①	②	③	④	⑤
매우 불필요	불필요 한 편	보통	중요한 편	매우 중요

Q33. 다음은 신기술과 정보인권 문제를 개선하기 위한 정책 방향들입니다. 각 정책 방향이 얼마나 중요하다고 생각하시는지 답변해주십시오.

기업이나 정부가 신기술 사용에 앞서 지켜야 할 정보인권 보호 '가이드라인'을 마련한다

① 매우 불필요 ② 불필요 한 편 ③ 보통 ④ 중요한 편 ⑤ 매우 중요

Q34. 귀하는 다음 중 어떤 기관이나 단체가 정보인권 보호 및 개선에 책임이 있다고 생각하십니까? (다음 중 우선순위별로 최대 3개까지 응답해주세요.)

1순위 : _____
2순위 : _____
3순위 : _____

① 국회 및 정당 ② 수사기관 (검찰, 경찰) ③ 법원 ④ 행정기관
⑤ 민간기업 ⑥ 시민단체 ⑦ 일반 개인 ⑧ 기타 ( )

Q35. 귀하의 최종 학력은 어떻게 되십니까?
① 고졸 이하 ② 전문대졸 ③ 대학교졸 ④ 대학원졸 이상

설문에 응해주셔서 감사합니다.

4차 산업혁명 시대에서
정보인권 보호를 위한 실태조사

| 인쇄일 | 2018년 11월 29일
| 발행일 | 2018년 11월 29일
| 발행처 | 국가인권위원회
| 주　소 | 04551 서울시 중구 삼일대로 340 나라키움 저동빌딩
http://www.humanrights.go.kr
| 문의전화 | 인권정책과 02)2125-9827
| 제작 | 플러스　플러스 02)2267-2290

ISBN : 978-89-6114-662-3 93330　　비매품