발 간 등 록 번 호
11-1620000-000634-01

2016년도 인권상황실태조사
연구용역보고서

바이오 정보 수집, 이용 실태조사

국가인권위원회

바이오 정보 수집, 이용 실태조사

이 보고서를 “바이오 정보 수집, 이용 실태조사”의 최종보고서로 제출합니다.

2016. 11. 29.

연구수행기관 : (사) 인도주의실천의사협의회
연구책임자 : 이상윤 (인도주의실천의사협의회)
공동연구원 : 김병수 (동국대학교)
오병일 (정보인권연구소)
이은우 (법무법인 지향)
장여경 (진보네트워크센터)
최규진 (인하대학교)

이 보고서는 연구용역 수행기관의 결과물로서, 국가인권위원회의 입장과 다를 수 있습니다

<제목 차례>

<표 차례>

<그림 차례>

요 약 문

Ⅰ. 서론

가. 연구의 배경 및 필요성

2007년 당시 정보통신부와 한국정보보호진흥원(KISA, 現 한국인터넷진흥원)이 만든 '바이오 정보 보호 가이드라인'은 바이오 정보를 "지문, 얼굴, 홍채, 정맥, 음성, 서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함한다"고 규정하고 있다.

바이오 정보는 모든 사람에게 존재한다는 '보편성'과 함께, 사람마다 다르다는 '고유성'(혹은 유일성)을 가지고 있으며, 대체로 그 정보가 평생 변하지 않는다는 '불변성'을 가지고 있기 때문에 개인 식별(identification)이나 인증(authentification) 목적으로 공공 및 민간의 다양한 분야에서 활용되고 있다.

바이오 정보의 활용도가 높아지면서 그 위험성에 대한 우려도 커지고 있다. 바이오 정보가 본인 식별이나 인증을 위해 활용되는 것은 그 유일성, 불변성 때문인데, 바로 그와 같은 특성 때문에 개인의 프라이버시에 미치는 영향도 치명적일 수 있기 때문이다.

바이오 정보의 프라이버시 침해 등 인권 침해 우려는 이미 오래전부터 제기되어 왔지만, 이에 대응하기 위한 법제도의 개선은 별다른 진척이 없는 상황이다. 정보통신부가 2005년 및 2007년에 가이드라인을 발표하였고, DNA 정보 수집을 목적으로 한 법률, CCTV 규제에 대한 내용이 「개인정보 보호법」에 들어가 있을 뿐, 바이오 정보에 초

점을 맞춘 별도의 법적 규제는 없는 상황이다. 바이오 정보의 산업 측면의 성장 가능성만 주목이 되고 있을 뿐, 바이오 정보가 장기적으로 프라이버시권에 미칠 영향에 대한 논의는 빈약한 실정이다.
본 연구는 공공 및 민간 영역에서, 그리고 국내 및 세계적으로 바이오 정보의 기술 발전 및 도입 실태, 바이오 정보의 유출이나 바이오 인증의 도입에 따른 제반 피해의 실태, 바이오 정보의 수집 및 이용과 관련된 법제의 국내외 현황, 바이오 인증에 대한 시민들의 인식 현황 등을 파악하고, 이를 기초로 바이오 정보 관련 법제도 및 정책의 개선 방안을 제안하고자 한다.

나. 연구의 범위 및 내용

국내에서 '바이오 정보'는 '생체정보'와 보통 같은 의미로 사용되며, 주로는 '생체인식 정보(biometric data)' 혹은 바이오인식 정보를 의미한다. 그러나 바이오 정보 혹은 생체정보가 반드시 생체인식 정보인 것은 아니다. 최근 웨어러블 기기나 디지털 헬스케어 서비스의 도입과 함께 수집되고 있는 체온, 심박수, 칼로리, 혈당 등의 정보 역시 바이오 정보이며, 특정 개인과 결부될 경우 개인정보라고 볼 수 있지만, 생체인식 정보인 것은 아니다. 이러한 정보를 지칭하는 용어로는 건강 정보 혹은 건강관련 정보(data concerning health)가 있다. 본 연구에서는 바이오 정보를 생체정보와 동일한 의미로 사용하되, 이를 생체인식 정보, 유전정보, 건강관련 정보로 구분하여 분석한다.

Ⅱ. 바이오 정보 수집, 이용 현황

가. 생체인식 정보 수집, 이용 현황

생체인식이란 '자동화된 장치에 의하여 개인의 신체적, 행동적 특성을 통하여 신원을 인증(authentication)하거나, 신원을 식별(identification)하는 것을 말하며, 이를 위해 사용되는 신체적, 행동적 특징에 관한 정보를 생체인식 정보라고 한다. 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 결제수단 등의 용도로 폭넓게 도입되고 있다.

우선 공공행정 분야에서 많은 나라들이 국민들의 신원확인을 위해 지문, 홍채, 얼굴 등 생체인식 정보를 사용하고 있다. 신분증 역시 기존의 종이나 플라스틱 형태에서 신용카드와 같이 내장된 칩을 가진 전자신분증으로 변화하고 있으며, 칩 내에 생체인식 정보를 포함하고 있다. 이 외에도 생체인식 기술은 선거관리나 원조 제공 등 여러 행정목적으로 활용되고 있다. 한국에서는 수차례 전자주민증 논란이 있었지만 아직 도입되지 않았고, 다만 전 국민의 지문 및 사진 등을 전산화하여 데이터베이스로 집적하고 있다.

범죄 예방 및 수사를 위해 지문, DNA, 얼굴 등 다양한 생체인식 정보가 활용되고 있다. 전산화된 지문은 경찰의 수사 목적을 위해 활용되고 있으며, 얼굴 정보는 CCTV, 블랙박스, 채증장비, 바디캠 등 수많은 영상정보 수집장치 및 웨어러블 장비를 이용하여 수집되고 있

다. 범죄예방, 주차단속 등 다양한 목적으로 설치된 CCTV는 매년 빠르게 증가하고 있는데, 법적 근거도 없이 이미 100여 곳에서 설립, 운영되고 있는 CCTV 통합관제센터를 통한 개인정보의 목적 외 이용 문제, 차량이나 얼굴 등을 자동인식할 수 있는 지능형 CCTV 등이 논란이 되고 있다. 지능형 CCTV와 같이 영상정보 수집장치와 얼굴인식 기술이 결합할 경우, 개인의 인권에 미치는 부정적 영향이 막대할 수 있고 국가 감시의 우려도 불러일으킬 수 있다. 이미 미국에서는 얼굴인식 시스템이 수사 목적으로 광범하게 사용되고 있는데, 최근 발표된 <영구적인 라인업(The Perpetual Line-Up) - 미국에서 규제되지 않는 미국의 얼굴인식 시스템> 보고서에 따르면 이를 규제할 수 있는 법제는 미비한 상황이다. 한국의 수사기관 역시 범죄자 얼굴인식 시스템의 개발과 도입에 박차를 가하고 있다.

생체인식 기술은 오랫동안 건물 등 보안 및 출입통제 목적으로 활용되어 왔다. 국가간 이동을 통제하는 '출입국 관리'의 목적으로도 활용되고 있다. 특히 미국에서의 911 테러 이후 생체인식 전자여권이 도입되고 공항에서도 생체인식을 통한 출입국 수속 시스템이 추진되고 있다. 현재 세계 대부분의 국가에서 생체인식 전자여권을 도입하고 있다. 한편 일반적인 출입통제 목적의 생체인식 장치는 일반 가정의 도어락에서부터 보안시설의 출입통제, 그리고 출퇴근 확인 및 근태관리용도로까지 광범하게 보급되어 있다. 이와 같은 생체인식 기기는 구성원들의 동의도 없이 설치하고 지문날인 등 생체인식 정보 제공을 강요하여 종종 논란이 되고 있다.

최근 스마트폰에 지문, 홍채, 얼굴 인식 등 다양한 생체인식 기술이 도입되고 있다. 스마트폰의 생체인식 기술은 스마트폰 자체의 보안뿐만 아니라, 온라인 결제를 위한 인증 시스템으로도 활용될 수 있다. 스마

트폰은 카메라, 마이크, 지문센서, 중력센서, 터치패드 등 다양한 종류의 생체인식 기술을 탑재하고 있어 다양한 용도로 활용될 수 있다.
금융분야는 자칫하면 커다란 재산적 손실을 야기할 수 있기 때문에 엄격한 본인 인증이 요구되어 왔다. 특히 최근 모바일 금융거래가 증가하고 핀테크가 활성화되면서 금융분야에서 비대면 거래가 증가하면서, 기존의 비대면 인증수단을 보완하거나 대체할 수 있는 수단으로 생체인식 기술이 주목받고 있다. 초기에는 금고나 전산실 등의 출입통제 목적으로 생체인식 기술을 활용해 왔지만, 현재는 ATM, 텔레뱅킹, 오프라인 결제, 모바일 뱅킹 등 다양한 금융서비스에서 활용되고 있다.
얼굴인식 등 생체인식 기술은 기업들의 마케팅 목적으로 활용될 수 있다. 소비자 모르게 얼굴 인식을 하여 특성에 맞는 광고를 내보내는 서비스, 페이스북의 이름표 추천 서비스 등의 사례가 있다.

나. 유전정보 수집, 이용 현황

국내에서 신원확인 목적의 유전정보는 주로 수사기관과 군대에서 수집하고 있다. 그런데 유전정보는 식별정보와 함께 가족과 공유하는 생물학적 특징을 포함하고 있어서 수집 및 활용에 있어서 각별한 주의가 필요하다.
검찰과 경찰이 공동으로 운영 중인 범죄자 디엔에이데이터베이스에는 2015년 3월 현재 212,966건(수형인 87,938, 구속피의자 42,561, 현장수거물 82,467)의 디엔에이신원확인정보가 보관되어 있다. 국립과학수사연구원이 운영 중인 실종아동 등의 데이터베이스에는 2016년 6월 현재 22,041(아동 16,402, 지적장애인 3,211, 치매환자 233, 보호자 2,195) 건의 디엔에이신원확인정보가 입력되어 있다. 최근 들어 군대에서의 수집도 활발히 진행되고 있는데, 2016년 8월 현재 유해발굴사

업단은 46,311(유해 10,673, 유가족 35,638)건의 디엔에이신원확인정보를, 국군의학연구소는 93,901명의 군인 혈액을 보관하고 있다.

다. 건강관련 정보 수집, 이용 현황

일반적으로 건강관련 정보라고 하면 의료기관에서 환자-의사 관계에서 생성되는 정보를 의미한다. 하지만 최근 건강관련 정보는 전통적인 병원시스템 외에도 다양한 경로를 통해서 수집.이용되고 있다. 이를 보다 체계적으로 정리하면, 주체 및 경로에 따라 크게 다음 두 가지 형태로 나누어 볼 수 있다. 첫째는 전통적인 병의원 진료를 통해서 얻어지는 개인 진료정보에 근간한 건강관련 정보이다. 두 번째는 개인 라이프로그(LifeLog)를 통한 건강관련 정보이다.

특히 최근 한국사회에서는 '맞춤형건강', '정밀의료', '원격의료'와 같은 개인 건강관련 정보를 바탕으로 한 미래형 건강관리체계가 제시되며, 이의 근간이 되는 디지털화된 건강관련 정보의 수집·이용에 많은 관심이 쏠리고 있다. 이중 의료기관에서 생성하는 건강관련 정보는 이미 법적으로나 사회체계상으로 특별히 관리되어 왔고, 상대적으로 관리와 활용에 대한 논의가 축적되어 온 반면, 의료기관 외에서 생성되는 건강관련 정보는 훨씬 빠르게 수집·이용이 늘어나고 있는 데 비해 그에 맞는 분석이나 관리에 대한 논의가 뒤따르지 못하고 있다.

건강관련 정보의 핵심 수집·이용 수단으로 주목받고 있는 웨어러블 디바이스는 착용 형태, 기능 등에 따라 세부 분류가 가능하다. 착용형태에 따라서는 시계형, 안경형, 액세서리형, 셔츠형, 신발형 등으로 분류할 수 있으며, 기능에 따라서는 비교적 단순한 기능만을 제공하는 기본형과 모바일 OS를 기반으로 어플리케이션을 자유롭게 설치하고 실행할 수 있는 스마트형으로 나눌 수 있다.

웨어러블 디바이스는 그 기술의 발전 수준에 따라 다시 세 가지로 구분할 수 있다. 즉, 휴대 및 착용하는 Portable 형태, 신체에 밀접하게 부착하는 Attachable 형태, 생체이식을 할 수 있는 Eatable 형태로 나눌 수 있다. Portable 형태의 경우 스마트폰과 같이 휴대하거나 안경, 시계, 팔찌 등의 착용형 디바이스를 지칭하며, 현재 상용화된 기기들이기도 하다. Attachable 형태는 패치와 같이 피부에 직접 부착할 수 있는 형태로 향후 3~5년 이후 본격적인 상용화가 예상된다. Eatable 형태는 인간의 신체에 직접 삽입·이식하거나 복용하는 형태의 디바이스를 말한다. 아직은 개발단계 수준이나 수집할 수 있는 건강관련 정보의 종류나 그 정보의 정확성에 있어 다른 단계의 디바이스와는 질적으로 다르기 때문에 향후 진정한 의미의 개인 건강관련 정보의 생성·관리가 가능해질 수 있는 단계로 기대를 모으고 있다.

웨어러블 디바이스의 성장은 헬스케어 분야를 통해 성장할 것이라는 게 전문가들의 중론이다. 물론 그 기술이 예방이나 진단과 같은 원격의료의 형태로 발전하기까지는 시간이 다소 걸리겠지만 먼저 레저, 웰니스, 피트니스 콘텐츠를 시작으로 빠르게 성장할 것으로 보인다. 이미 피트니스와 웰니스 분야에서 많은 웨어러블 디바이스를 통해 자신의 운동상황, 심장박동수, 수면상태 등을 수치화된 데이터 수집을 통해 체크하고 있으며, 의료분야에서의 활용도 점차 증가하고 있다.

모바일 헬스케어 산업에서 가장 큰 비중을 차지하고 있으며 성장이 기대되는 건강관련 정보를 모니터링 하는 웨어러블 디바이스의 세계 시장은 2015년 3,930백만 달러에서 연평균성장율(CAGR) 41.9%로 2020년에는 32,142백만 달러에 이를 것으로 전망되며, 이중 국내 시장은 2015년 649억 원에서 2020년 5,302억 원에 이를 것으로 예상된다.

Ⅲ. 바이오 정보 수집, 이용과 정보 인권

가. 생체인식 정보 활용시 문제점과 피해사례

생체인식 정보의 활용도가 높아지면서 그 위험성에 대한 우려도 커지고 있다. 유출되었을 경우 변경할 수 있는 비밀번호나 신용카드 등과 달리, 생체인식 정보는 한번 유출되면 그 피해를 복구하는 것이 거의 불가능하다. 또한, 생체인식 정보를 추출하는 과정에서 원 바이오 정보에서 부가적인 정보가 추출될 가능성을 배제할 수 없으며, 사용자가 인식하지 못하는 사이에 채취될 수 있는 위험이 존재한다. 생체인식 기술 자체의 한계나 시스템의 불완전성 때문에 생체인식 기술을 지나치게 신뢰할 경우에도 문제가 생길 수 있다.

생체인식 시스템 역시 정보시스템의 하나이므로 시스템의 각 단계에서 보안 취약점이 발생할 수 있다. 이미 바이오 정보가 위조되거나 유출된 사례, 혹은 그 위험성을 경고하기 위한 실험이 다수 공개되었다. 생체인식 정보의 유출과 도용은 개인에게 불편함, 금전적 손실, 범죄 피의자로의 오해, 심지어 생명에의 위협까지 다양한 문제를 야기할 수 있다. 기업들이 상업적 목적으로 바이오 정보를 수집하거나 생체인식 기술을 활용함으로써 소비자들의 프라이버시를 침해할 우려도 높아지고 있다.

무엇보다 민간 및 공공영역에서 수집, 축적된 생체인식 정보가 노동자, 시민을 감시하는 용도로 사용될 위험성이 크다. 정부가 시민 개개인을 엄격하게 식별하고 인증하는 것 자체가 시민에 대한 차별을 포함해서 체계적이며 광범위한 인권 침해를 가져올 수 있다. 시민을 잠재적 범죄자 취급하거나 감시를 강화함으로써 정부에 대한 비판을 위축시킬 수 있다. 특히, 중앙집중적 바이오 정보 데이터베이스의 구축

이나 자동화되고 은밀해진 개인식별은 감시의 위험성을 증폭시킨다. CCTV 통합관제센터와 같이 한번 수집된 바이오 정보는 또 다른 목적으로 활용될 가능성도 크다. 생체인식 기술로 인한 인권 침해를 최소화하기 위해서는 활용되는 기술의 특성(예를 들어 특정 대상에 대한 검색인가, 무차별 검색인가, 혹은 특정 대상에 대한 데이터베이스인가, 무차별 데이터베이스인가 등)에 따라 적절한 감독 체제가 마련될 필요가 있다.

나. 유전정보 활용시 문제점과 피해사례

사건 해결을 위해 DNA 신원확인정보를 개별적으로 활용할 경우 DNA 채취 과정에서 충분한 설명에 근거한 동의(informed consent) 문제가 제기된다. 현재는 동의서를 받는 자발적 형태로 이루어지고 있으나 수사 과정이라는 특수한 상황에서 일반인들이 채취를 거부하기는 쉽지 않다.

특히 용의자를 특정하기 위해 사건 현장 주변에서 많은 사람들의 DNA를 수집 분석하는 집단검색(mass screening)의 경우 방법의 적절성과 채취 범위를 둘러싸고 논란이 되고 있다.

DNA데이터베이스는 입력 대상, 가족검색, 다른 데이터베이스와의 연동을 통해 확장될 수 있다. 현재의 시스템에 대해 수사기관이 전 국민의 지문과 주민등록번호를 보유하고 있는 상황에서 입력 대상 범죄가 지나치게 광범위하다는 비판이 제기되고 있다. 입력 대상 범죄의 범위도 논란이지만 집행유예나 벌금형까지 DNA를 수집해 사망시까지 보관하는 것이 과연 적절한지도 논의가 필요하다.

가족검색을 수사에 사용할 경우 데이터베이스에 수록된 특정인의 가족 또한 평생 유전자 감시를 받게 되는데 이들은 인지나 동의 없이

수시로 수사선상에 오를 가능성이 있다. 일종의 데이터베이스의 우회적 확장이라고 할 수 있다. 이 과정에서 숨기고 싶었던 또는 알지 못했던 가족 관계가 공개될 수 있다. 사회적 가족관계와 생물학적 가족관계는 다를 수 있는데, 입양, 혼외 출생, 성씨 변경 등이 노출되게 된다.

수사목적 이외의 확장이나 다른 신원확인 DNA 데이터베이스와의 연동도 우려사항이다. 현행 디엔에이법은 이미 수사 목적 이외의 행정적 목적으로 DNA 신원확인정보를 활용할 수 있도록 규정하고 있는데 장기적으로 현재 구축된 실종아동 데이터베이스, 향후 구축이 계획되고 있는 군대 데이터베이스와 연동될 가능성이 있다.

DNA 신원확인정보는 숫자로 입력되지만 신원확인 이외의 생물적 특성을 알 수 있어 논란이 되고 있다. 염색체 이상의 유전질환은 디엔에이신원확인 정보만으로도 어느 정도 예측이 가능하다. 즉 DNA 프로파일링을 통해 염색체 이상의 '유전병'을 간접적으로 확인할 수 있는 것이다. 특히 차세대염기서열분석법(NGS, Next Generation Sequencing)을 이용하면 신원확인정보 이외의 생물학적 특징(피부, 머리카락, 눈의 색 등)과 질병정보 등을 얻을 수 있다.

DNA 프로파일링 결과에 대해서도 논란이 있는 경우가 있다. 대부분의 경우 정확성이 높지만 어떤 경우에는 동일인일 확률이 낮거나 분석이 불가능할 수 있다.

범죄자 데이터베이스는 현재의 입력 범죄 대상이 적절한지에 대한 논의가 필요하다. 입법 취지에 맞게 흉악범을 대상으로 해야 하며 집단검색, 가족검색에 대한 사회적 논의와 규정을 마련해야 한다. 또한 분석 과정에서 디엔에이신원확인정보 이외의 유전정보 확인(Y 염색체, 미토콘드리아 DNA, 기타 생물학적 정보 등)을 우선 금지하고 그 필

요성에 대한 논의를 시작해야 한다. 실종아동 등의 데이터베이스에서는 채취 대상을 엄격히 제한할 필요가 있다. 법률의 입법 취지는 실종아동의 신상정보가 부족하거나 장기미아일 경우 디엔에이신원확인정보를 활용하는 것이었다. 그러나 채취 대상이 정신지체 장애인이나 치매 환자로까지 확대되고 있으며, 실종아동의 경우도 신상정보가 명확하거나 굳이 필요하지 않은 경우에도 채취하고 있는 것으로 보인다. 6.25 전사자 유해 발굴 사업에 사용되고 있는 동의서 양식을 수정해 신원확인 목적의 유전자 검사만 가능하도록 활용 범위를 제한해야 한다. 특히 법률적 기반 없이 추진되고 있는 군인들에 대한 광범위한 혈액 채취는 중단해야 한다.

다. 건강관련 정보 활용시 문제점과 피해사례

최근 한국사회에서는 '맞춤형건강', '정밀의료', '원격의료'와 같은 개인 건강관련 정보를 바탕으로 한 미래형 건강관리체계가 제시되며, 이의 근간이 되는 디지털화된 건강관련 정보의 수집·이용에 많은 관심이 쏠리고 있다. 그러나 의료기관에서 생성하는 건강관련 정보는 이미 법적으로나 사회체계상으로 특별히 관리되어 왔고, 상대적으로 관리와 활용에 대한 논의가 축적되어 온 반면, 의료기관 외에서 생성되는 건강관련 정보는 훨씬 빠르게 수집·이용이 늘어나고 있는 데 비해 그에 맞는 분석이나 관리에 대한 논의가 뒤따르지 못하고 있다.

건강관련 정보를 수집·이용하는 수단인 웨어러블 디바이스의 시장은 빠르게 성장하고 있지만 아직까지 건강관련 정보에 대한 기술적, 제도적, 사회·문화적으로 검토해야 할 지점이 많으며, 우려되는 부작용 또한 적지 않다. 우선 지적할 수 있는 문제점은 효용성과 정확성 문제이다. 많은 웨어러블 디바이스가 생산하고 있는 심전도 정보만

하더라도 벌써 유수의 의학저널에서 그 효용성과 정확성에 대해 의문을 제기하고 있다. 즉, 냉정한 검토를 토대로 추진하지 않으면, 불필요한 건강 소비가 발생할 수 있고, 오히려 건강관리에 피해를 입힐 수 있다. 또한 당장은 아니더라도 장래에 이러한 웨어러블 디바이스가 생산한 건강관련 정보가 공적으로 인정하는 정보가 될 경우 그 심각성은 더욱 커진다. 이미 미국에서는 여러 제품에 (민간) 보험이 적용되고 있으며, 현재 한국 정부도 시범사업이긴 하지만 만성질환관리에 웨어러블 디바이스를 활용하고 있는 만큼 이러한 문제에 대해 신중한 논의가 필요하다.

가장 신중히 고려할 것은 보안 문제이다. 점차 단순히 디바이스 안에서만 건강관련 정보를 생성·관리하는데 그치지 않고 이 정보를 중앙 클라우드로 수집하고 처리(피드백 제공 등)하고 있으며, 심지어 고객들에게 통합적인 건강관리서비스를 제공한다는 명목으로 건강관련 정보를 기업들끼리 공유하는 형태(애플의 Healthkit과 같은 플랫폼)로까지 나아가고 있다. 이처럼 건강관련 정보의 수집·이용은 상업적으로 빠르게 성장하고 있는 반면 보안과 관련된 제도적 장치가 뒷받침되지 못하고 있는 게 현재의 상황이다. 이미 외국에서는 이러한 문제의식이 확산되면서 미국, 영국, 네덜란드를 중심으로 개인정보 유출과 프라이버시 침해를 우려해 웨어러블 디바이스 출시 반대 운동까지 벌어지고 있다. 이러한 사회적 반향 때문에 미국의 경우 2013년 웨어러블 디바이스의 안전성을 제고하는 '웨어러블 디바이스(어플리케이션 포함) 가이드라인'을 공포하기도 했다.

한국의 상황에 초점을 맞춰 정리해 보면, 현재 한국은 원격의료의 사전단계라고 할 수 있는 만성질환관리 시범사업에 웨어러블 디바이스를 사용하는 등 정부 차원에서 건강관련 정보의 적극적인 활용을

추진하고 있다. 반면 건강관련 정보의 효용성, 정확성, 그리고 보안 문제에 대한 고민은 충분치 못한 상황이다. 아울러, 미국에서 건강관련 정보를 수집.이용하는 여러 웨어러블 디바이스 제품들이 점차 보험 적용을 받고 있는 상황으로까지 나아가고 있는 점을 주목할 필요가 있다. 머지않아 한국에서도 민간보험회사를 중심으로 보험 적용이 시도될 것이며, 이는 전국민건강보험에도 영향을 미칠 것이다. 그러나 주요 민간보험회사들이 주요 IT기업은 물론 주요 의료기관까지 거느린 대기업의 계열사인 한국의 특수성을 고려하면 건강관련 정보는 미국보다 훨씬 심각하고 복잡한 문제를 안고 있음을 간과해서는 안 된다. 따라서 단순히 상업적인 성장에 급급할 것이 아니라 한국의 특수성을 고려하여 위에 언급한 효용성의 문제, 정확성의 문제, 보안의 문제에 대해 인권적으로 신중히 검토할 필요가 있다.

Ⅳ. 바이오 정보 이용에 대한 시민 인식 조사 결과

조사 대상자의 61%는 생체인식기술을 사용한 경험이 없었다. 아직까지는 생체인식기술을 이용한 생체인식 정보 활용이 보편화되지 않았음을 알 수 있다.

금융거래시 생체인식기술을 활용하는 것에 대해서 시민의 44%가 반대하였다. 시민들은 다른 사용 목적에 비해 금융거래 목적의 생체인식기술 사용에 대해서 특히 조심스러운 태도를 보였다. 출퇴근 확인이나 보안 목적의 사용보다는 사용 규모가 광범위하고 피해 발생시 그 규모와 심각성이 크다는 인식 때문인 것으로 생각된다.

조사대상자의 55%가 생체인식 기술 활용시 생체인증 정보 수집 기관

의 정보 남용 가능성을 우려했다. 생체인식 정보 도용 및 위조 가능성을 우려하는 시민도 51%에 달했고, 수집된 생체인식 정보의 외부 유출을 우려하는 시민도 33%에 이르렀다. 일반 시민들은 생체인식 기술의 활용과 관련하여 정보 수집 기관의 정보 보안 능력 및 의지를 가장 우려한다는 것을 알 수 있다. 도용 및 위조시 그 피해가 크고 심각하기 때문에 도용 및 위조 가능성에 대해서도 크게 우려하고 있었다.

조사 대상자의 81%가 시계, 스마트폰의 어플 등을 통해 신체 정보 및 건강 정보를 측정하거나 입력하여 건강관리를 하는 기술을 이용해 본 적이 없다고 응답하였다. 이러한 기술은 생체인식 기술에 비해 더 보편화되지 않은 상태임을 알 수 있다.

모바일 기기 등을 활용한 건강관련 정보 수집에 대해 일반 시민의 69%가 개인 건강 정보의 유출을 우려하는 것으로 조사되었다. 생체인식 정보에 견줘 모바일 기기 등을 통한 건강관련 정보 유출 위험을 더 크게 인식하고 있었다. 이는 생체인식 정보에 견줘 모바일 기기를 활용한 건강관련 정보 보안 및 보호에 대한 논의나 대책이 부족한 현실의 한 단면을 반영하는 것이다.

일반 시민의 86%는 생체인식 정보와 건강 정보는 다른 개인정보에 비해 더 엄격하게 규제되고 보호되어야 한다고 생각하고 있었다. 생체인식 정보와 건강 정보는 더욱 민감한 개인정보로 인식하고 있었다.

생체인식 기술 및 모바일 기기 등을 활용한 건강관리서비스가 보편화되지 않은 상태이지만, 일반 시민들은 이러한 서비스 활용에 필수적인 생체인식 정보 및 건강관련 정보 보호 수준에 상당한 우려를 하고 있었다. 특히 금융서비스 목적의 생체인식 정보 활용 및 모바일 기기 등을 활용한 건강관리서비스 목적의 건강관련 정보 활용에 대해 우려가 컸다.

시민들은 관련 정보 수집 기관의 정보 보호 수준에 대해 가장 큰 우려를 하고 있었고, 도용 및 위조 가능성에 대한 우려도 컸다. 일반 시민들은 생체인식 정보와 건강관련 정보에 대해서는 일반 개인정보 보호 수준보다 더 엄격한 규제와 보호를 요구했다.

Ⅴ. 바이오 정보 관련 국내외 법제도 현황

해외의 보호 수준을 감안할 때 바이오 정보의 수집, 이용, 결합, 제공 및 판매 등 처리와 관련한 국내 법률의 규범은 다소 모호한 수준이다. 반면 세계 여러 나라가 생체인식 정보, 유전정보, 건강관련 정보를 민감정보로서 특별한 보호를 규정하고 있는 경향은 우리에게 시사하는 바가 크다.

우선 생체인식 정보와 관련하여 그 민감성에 부합하는 보호규정을 정비할 필요가 있다. 특히 여러 법령에서 서로 다른 용어로 정의하고 있는 '생체인식 정보'의 법령용어를 정비하여야 한다. 또한 생체인식 정보를 비롯하여 유전정보 및 건강관련 정보 등 바이오 정보 전체적으로 통일적인 규율을 적용할 수 있어야 한다.

바이오 정보에 대한 보호를 위하여 현행 개인정보 보호법상의 민감정보에 대한 보호 조치를 제고할 필요가 있다. 특히 개인정보처리자가 민감정보의 처리를 위해 정보주체로부터 동의를 구할 때 그 동의 요건을 보다 명시적으로 규정할 필요가 있다.

바이오 정보 보호의 민감성에 비추어 가장 중요한 것은 사전 예방이다. 그런 의미에서 현재 제도적 영향력을 크게 발휘하고 있지 못한 개인정보 영향평가 제도 또한 실질화하여 바이오 정보의 처리에 적용할 수

있어야 한다. 더불어 프라이버시 중심설계(Privacy by design) 및 프라이버시 중심설정(Privacy by default)에 대해 적극적으로 도입할 필요가 있다. 실효성을 거두고 있지 못한 개인정보 감독기구의 독립성 강화도 필수적이다. 개인정보 영향평가의 강화, 프라이버시 중심설계 및 설정 및 감독 강화는 유럽 제29조 개인정보보호 작업반은 물론 국가인권위원회도 2013년 <정보인권 보고서>에서 제언한 바 있다.

단기적으로는 위와 같은 내용으로 현행 개인정보 보호 관련 법령을 정비하여 생체인식 정보를 비롯한 바이오 정보를 보호할 수 있겠다. 장기적으로는 바이오 정보 보호에 관해 특화된 법률을 마련할 필요도 있어 보인다. 바이오 정보가 처리되는 모든 생애주기에 있어 목적제한, 최소수집, 비례성, 적합성, 투명성, 안전장치가 보장될 필요가 있다.

Ⅳ. 정책 제언

이상의 연구 결과를 토대로 개인정보 보호 관련 법률의 개선을 제안하였다.

‘개인을 특정하게 식별할 수 있는 생체인식 정보(biometric data for the purpose of uniquely identifying a natural person)’를 의미하는 법령용어를 ‘생체인식 정보’로 일관되게 정비한다. 민감정보로서 바이오 정보를 명확히 규정하고 전체적으로 통일적이고 강화된 보호규정을 적용한다. 바이오 정보의 처리에 대한 정보주체의 동의 요건을 강화한다. 개인정보 영향평가를 실질화하여 바이오 정보의 처리에 대하여 실시한다. 프라이버시 중심설계를 도입하여 바이오 정보의 처리에 대하여 적용한다. 바이오 정보에 대하여 독립적인 개인정보 감독기구의 사전 사후 감독을 강화한다. 바이오 정보의 민감한 특성을

고려한 특별한 보호조치를 도입한다. 이는 ▲원본정보가 아닌 - 특징정보의 사용 ▲중앙집중형보다 분산저장형 권장 ▲갱신과 파기 보장 ▲암호화 저장 ▲목적달성 후 자동삭제 ▲목적내 데이터베이스 규모의 최소화 및 식별정보 분리 ▲프로파일링 규제 등을 포함한다.

또한, 각 기관별 과제를 도출하여, 각 기관에서 향후 정책 개선에 반영할 수 있도록 하였다.

우선 국회에는 개인정보 보호 관련 법률에서 바이오 정보의 보호가 체계적이고 통일적으로 반영될 수 있도록 개선할 것과 함께, 수사 목적의 개인정보 수집에 대한 규제 강화, 전 국민 지문날인에 대한 재검토 및 법적 근거 마련, 영상정보처리기기 및 얼굴인식 기술에 대한 법제 개선, 전자적 노동감시 통제를 위한 법제 마련, 디엔에이 관련 법제의 개선, 스마트기기나 웨어러블 디바이스를 통해 수집된 건강관련 정보의 보호 등을 제안하였다.

정부에는 생체인식 시스템에 대한 투명한 공개, 생체인식 시스템의 신중한 도입 및 개인정보 영향평가의 실시, CCTV 통합관제센터 운영 재검토, 바이오 정보 오남용에 대한 사회적 감독 강화, 웨어러블 디바이스의 부작용을 방지하기 위한 연구 및 관리 등을 제안하였다.

기업에는 생체인식 기술의 신중한 도입 및 대체수단 제공, 생체인식 정보 보호를 위한 기술 및 자율규제 개발, 건강관련 정보 활용에 대한 신중한 접근, 프로파일링 처리에 대한 정보주체의 권리 보장 등을 제안하였다.

제1장

서론

제1장 서론

가. 연구의 배경 및 필요성

2007년 당시 정보통신부와 한국정보보호진흥원(KISA, 現 한국인터넷진흥원)이 만든 '바이오 정보 보호 가이드라인'은 바이오 정보를 "지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함한다"고 규정하고 있다(개인정보의 안전성 확보 조치 기준 제2조 제14호).

바이오 정보는 모든 사람에게 존재한다는 '보편성'과 함께, 사람마다 다르다는 '고유성'(혹은 유일성)을 가지고 있으며, 대체로 그 정보가 평생 변하지 않는다는 '불변성'을 가지고 있기 때문에 개인 식별(identification)이나 인증(authentification) 목적으로 공공 및 민간의 다양한 분야에서 활용되고 있다.

한국은 이미 1970년부터 열손가락 지문 날인을 시작했고, 이렇게 수집된 지문은 경찰의 수사목적을 위해 활용되어 오고 있다. 검찰과 경찰은 90년대 중반부터 유전자은행 설립을 위해 노력해 왔으며, 결국 2004년 '장기미아'를 찾는다는 명분하에 「실종아동등의 보호 및 지원에 관한 법률」이 통과되어 유전자 데이터베이스가 도입되었다. 또한, 2009년에는 「디엔에이 신원확인정보의 이용 및 보호에 관한 법률」 통과를 계기로 범죄자를 대상으로 한 유전자 데이터베이스 구축이 시작되었다. 한편, 범죄예방 및 시설안전 등을 목적으로 공공 및 민간 영역에서 CCTV의 도입이 급증하고 있으며, 최근에는 이를 '통합관제센터'를 통해 통합 관리하는 방향으로 나아가고 있다.

민간에서도 인터넷의 발전으로 인한 비대면 거래의 확대, 2000년을 전후로 한 모바일 기기의 확대, 이와 결부된 핀테크의 성장, 사물인터넷(IoT)이나 웨어러블 기기의 도입, 헬스케어와 원격 의료 도입 등과 맞물려 바이오 정보의 활용도가 높아지고 있다. 지문을 이용한 개인 스마트폰 보안에서부터, 지문·정맥·홍채 정보 등을 활용한 금융거래나 결제 서비스, 스마트 기기를 활용한 자가 건강 측정 및 원격 의료 서비스 등이 등장하고 있는 것이다. 특히, 한국적 상황에서는 주민등록번호의 남용으로 인한 개인정보 유출의 문제, 그리고 편의성과 접근성에서 문제를 노출한 공인인증서의 문제가 불거지면서, 바이오 인식(Biometrics)을 통한 새로운 인증 방식이 대안으로 제시되고 있는 상황이다. 2014년 전 세계 모바일 바이오 인증 시장의 매출액 규모는 16억 2천만 달러 규모이며, 같은 해 국내의 바이오 인식 제품의 매출액 규모는 1,867억 원 규모로 추산되고 있다.

개인 식별 수단으로 바이오 정보를 사용하는 것과 별개로, 최근 '맞춤형 건강관리' 혹은 '자가 건강관리'에 대한 관심이 증가함에 따라 바이오 정보를 활용한 건강관리 서비스 시장이 증가하고 있다. 바이오 정보를 활용한 건강관리 서비스 영역은 아직까지 널리 상용화되고 있지는 않지만, 그 확장성과 상품성에 대해서는 장밋빛 전망이 제출되고 있다. 이는 기본적으로 '건강한 사람을 더욱 건강하게' 만들기 위한 목적으로 현재도 이루어지고 있는 각종 상담, 교육, 운동처방, 식단관리, 생활습관 교정 등의 서비스에 정보통신기술을 접목하여, 보다 대규모로 보다 표준화된 방식으로 이를 상품화하려는 전략이다. 일상생활 중에 바이오 정보를 모니터링하여, 대규모로 집적된 바이오 정보에 근거하여 상담, 교육, 운동, 생활습관 교정 등을 제공하는 것이다.

한편, 유전자 등의 바이오 정보는 그 분석 기술이 발달하고 비용이 낮아짐에 따라, 그것을 분석하고 해석하여 소비자에게 제공하는 다양한 상품 서비스 영역이 개발되고 상용화되고 있다. 이는 의료기관에서 이루어지는

의료 행위와 별개로 바이오 정보를 매개로 실험실과 소비자 사이의 직접 거래가 이루어지는 영역이다.

이와 같이 바이오 정보의 활용도가 높아지면서 그 위험성에 대한 우려도 커지고 있다. 바이오 정보가 본인 식별이나 인증을 위해 활용되는 것은 그 유일성, 불변성 때문인데, 바로 그와 같은 특성 때문에 개인의 프라이버시에 미치는 영향도 치명적일 수 있기 때문이다. 즉, 유출되었을 경우 변경할 수 있는 신용카드 등과 달리, 한번 유출되면 그 피해를 복구하기 거의 불가능하다. 개인정보 유출로 인한 신원 도용의 문제 외에도, 인식 오류로 인한 피해, 장애인 접근권의 문제 등도 지적되고 있다. 또한 DNA나 얼굴 인식과 같이 수집된 정보들이 인증 목적의 정보 외에도 다른 정보 역시 포함할 수 있기 때문에, 친족 등의 프라이버시 침해나 목적 외 이용 등의 문제도 제기된다. 무엇보다 이렇게 수집, 축적된 바이오 정보가 국가 감시의 용도로 사용될 위험성도 크다. 이미 범죄 예방을 목적으로 수집이 허용된 DNA 정보가 집회, 시위자 혹은 정부에 비판적인 인사에 대해서도 수집되고 있다는 우려가 제기되고 있다. 특히, 한국의 경우 수사 목적의 개인정보 접근에 대한 규제가 미약하고, 전 국민 단일 식별자인 주민등록번호의 존재, 비밀정보기관인 국가정보원에 대한 통제 미약 등의 요인에 의해, 바이오 정보가 국가 감시의 목적으로 사용될 위험성이 더욱 크다고 할 수 있다.

일상적인 모니터링을 기반으로 건강관리 서비스를 제공하기 위한 바이오 정보 수집과 이용은 새로운 문제를 야기한다. 예를 들어 환자 낙상을 예방하기 위해 가정에 설치된 센서는 환자가 개인적으로 행하는 가정 생활 모두를 감시하고 관련 정보를 전송하게 된다. 환자와 가족과의 관계, 환자의 내밀한 내면 생활 등이 여과 없이 기록되고 전송되는 것이다. 이와 같은 방식으로 수집된 바이오 정보에 대해서는 정보 주체가 그 정보에 대한 권리를 주장하기 힘들다는 난점이 존재한다. 관련 업체들이 다양하

고 복잡한 약관이나 동의서의 형태로 개인의 정보 권리를 제약하기 때문이다. 이러한 영역에서의 바이오 정보 수집, 이용은 바이오 정보에 대한 자기 관리권, 통제권에 대한 논란을 불러일으킨다는 점에서 사회적 논의가 필요하다.

유전자 정보 등 바이오 정보를 활용한 유전자/건강 상담은 그 근거와 효과는 차치하고서라도, 그러한 바이오 정보 활용이 개인의 직업 선택권을 제약하거나, 특정 유전자를 가진 이들을 차별하는데 악용될 수 있다는 점에서 심각한 문제를 내포하고 있다.

바이오 정보의 프라이버시 침해 등 인권 침해 우려는 이미 오래전부터 제기되어 왔지만, 이에 대응하기 위한 법제도의 개선은 별다른 진척이 없는 상황이다. 정보통신부가 2005년 및 2007년에 가이드라인을 발표하였고, DNA 정보 수집을 목적으로 한 법률, CCTV 규제에 대한 내용이 「개인정보 보호법」에 들어가 있을 뿐, 바이오 정보에 초점을 맞춘 별도의 법적 규제는 없는 상황이다.

지난 2016년 3월 16일, 금융보안원은 '바이오 정보 사고사례 및 대응방안 조사' 보고서를 발표하였는데, 이 보고서는 바이오 정보가 위조 혹은 유출된 몇 가지 사례를 제시하고 있다. 예를 들어, 지난 2014년에는 실리콘 위조지문을 통해 주민센터에서 인감증명서를 발급받아 50억 원대 부동산 불법 명의 이전을 한 사례가 있었고, 독일 해커단체인 CCC는 구글에서 찾은 푸틴 러시아 대통령의 사진으로 홍채를 복제할 수 있음을 증명하기도 했다. 지난 2015년에는 미국 연방 인사관리처 전·현직 공무원 개인정보 2,200만 건과 함께, 지문정보 560만 건이 유출되기도 했다. 아직 바이오 정보가 활용되는 초기임을 생각하면, 그 활용도가 높아질수록 바이오 정보의 유출과 위조 등은 증가할 것으로 예상된다. 최근 한국IBM의 발표에 따르면, 사이버 공격의 대상도 신용 정보에서 생체정보(바이오 정보)로 이동하고 있다고 한다.

이러한 상황임에도 바이오 정보의 산업 측면의 성장 가능성만 주목이 되고 있을 뿐, 바이오 정보가 장기적으로 프라이버시권에 미칠 영향에 대한 논의는 빈약한 실정이다.

따라서, 본 연구는 공공 및 민간 영역에서, 그리고 국내 및 세계적으로 바이오 정보의 기술 발전 및 도입 실태, 바이오 정보의 유출이나 바이오 인증의 도입에 따른 제반 피해의 실태, 바이오 정보의 수집 및 이용과 관련된 법제의 국내외 현황, 바이오 인증에 대한 시민들의 인식 현황 등을 파악하고, 이를 기초로 바이오 정보 관련 법제도 및 정책의 개선 방향에 대해 제안하고자 한다.

나. 연구의 범위 및 내용

1) 연구의 범위 설정

연구의 범위를 정하기 위해 우선 관련 개념부터 정리할 필요가 있다. 이는 향후에 법적인 규율 대상을 명확히 규정하기 위해서도 필요하다.

국내에서 '바이오 정보'는 '생체정보'와 보통 같은 의미로 사용되며, 주로 '생체인식 정보(biometric data)' 혹은 바이오인식 정보를 의미한다. 2007년 당시 정보통신부와 한국정보보호진흥원(KISA, 現 한국인터넷진흥원)이 만든 '바이오 정보 보호 가이드라인'은 바이오 정보를 "지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함한다"고 규정하고 있다.

이 용어는 같은 기관들이 이보다 앞선 2005년 발표한 '생체정보보호가이드라인'에서 규정한 '생체정보'로부터 달라진 것이다. '생체정보'가 '바이오 정보'라는 용어로 바뀐 배경에는 관련 산업의 진흥을 도모하고자 하

는 정부의 의도가 있는 것으로 짐작된다. 생체정보라는 용어가 생체실험 등 부정적인 이미지를 연상시켜 국민들의 반감을 자아낼 수 있는 반면, 바이오 정보는 최첨단 생명공학의 이미지를 줄 수 있기 때문이다(박정훈·김행문, 2008). 다만 2007년 가이드라인에서는 관련 업계에서 생체정보와 생체인식 정보를 분리하여 후자를 가이드라인에서 배제하자는 주장에 대한 대응으로서, '원본정보' 및 '특징정보'를 정의에 모두 명확히 포함하였다.

현행 국내 법령은 '바이오 정보'와 '생체정보' 개념을 혼재해서 사용하고 있으며, 그 개념이 포괄하는 구체적인 정보의 범위도 명확하게 정의하고 있지 않다. 예를 들어 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 시행령(제15조 제4항 제2호)에서는 '바이오 정보'라는 개념을 사용하고 있는 반면, 「전자금융거래법」(제2조 제10호 라목)에서는 '이용자 생체정보'라고 되어 있다.

그러나 바이오 정보 혹은 생체정보가 반드시 생체인식 정보인 것은 아니다. 최근 웨어러블 기기나 디지털 헬스케어 서비스의 도입과 함께 수집되고 있는 체온, 심박수, 칼로리, 혈당 등의 정보 역시 바이오 정보이며, 특정 개인과 결부될 경우 개인정보라고 볼 수 있지만, 생체인식 정보인 것은 아니다. 이러한 정보를 지칭하는 용어로는 건강 정보 혹은 건강관련 정보(data concerning health)가 있다.

국내 「개인정보 보호법」 제23조는 '민감정보'를 정의하면서 건강 정보를 포함하고 있지만, 건강 정보가 포괄하는 범위가 어디까지인지는 명확하지 않다. 「생명윤리 및 안전에 관한 법률」에서는 "개인식별정보, 유전정보 또는 건강에 관한 정보 등 개인에 관한 정보"를 '개인정보'라고 정의하면서 '건강에 관한 정보'라는 용어를 쓰고 있지만, 마찬가지로 '건강에 관한 정보'가 어떤 정보인지에 대해서는 규정하고 있지 않다. 다만, KISA 개인정보보호 포털에서는 개인정보의 유형과 종류를 구분하면서, '신체적 정보'에

는 홍채, 지문 등 신체 정보(생체인식 정보)와 건강상태, 진료기록, 신체장애, 장애등급, 병력 등 의료·건강 정보가 포함된다고 설명하고 있다.

[그림 1] 신체적 정보의 유형 (출처 : KISA 개인정보 보호 포털)

이처럼 국내에서는 바이오 정보, 생체정보, 생체인식 정보, 건강정보, 건강관련 정보 등의 정의나 구체적인 포괄 범위가 명확하지 않은 상황이다. 한편, 2016년 제정된 유럽 개인정보보호규정(General Data Protection Regulation)도 제9조 특정범주의 개인정보 처리(Processing of special categories of personal data)에서, 유전정보(genetic data), 생체인식 정보(biometric data for the purpose of uniquely identifying a natural person), 건강관련 정보(data concerning health)로 구분하고 있다.

본 연구에서는 바이오 정보를 생체인식 정보뿐만 아니라, 유전정보, 건강관련 정보를 포괄하는 개념으로 사용할 것이다.

[그림 2] 바이오 정보의 개념

본 연구는 과제의 명칭을 수용하여 포괄적인 의미로서 통칭할 때는 '바이오 정보'라는 용어를 사용하되, 세부적으로는 생체인식 정보, 유전정보, 건강관련 정보로 구분하여 분석할 것이다. 그러나 본 연구진은 정책제언에서 '바이오 정보' 대신 '생체인식 정보', '유전정보', '건강관련 정보'로 명확히 개념 규정할 것을 제안하고 있다. 심우민(2016)이 지적한 바와 같이 '바이오 정보'라는 용어사용은 법문의 국문사용 원칙을 별론으로 하더라도 생명 및 유전공학 등의 분야에서 활용되고 있는 바이오 정보(bioinformation)의 개념과 다소 혼동될 여지가 있기 때문이다(박정훈·김행문, 2008). 현행 법령에서도 '생체정보' 용어는 법령에서 사용되고 있는 반면, '바이오 정보'는 시행령이나 가이드라인에서 사용되고 있는 것에 불과하다.

한편, 「공공보건의료에 관한 법률」(이하 '의료법') 19조에서 보호하고 있는 진단서, 처방전, 진료기록, 전자의무기록 등 개인 진료정보 역시 건강관련 정보라고 볼 수 있겠지만, 그 자체로 별도의 심도 깊은 연구가 필요한 영역이기 때문에 본 연구에서는 제외하는 것으로 한다. 다만, 건강관련 정보에 대한 실태를 서술하는 과정에서 관련이 있는 경우에 한하여 서술에 포함하였다.

2) 연구의 내용 및 방법

생체인식 정보, 유전정보, 건강관련 정보 각각에 대해 문헌조사 등을 통해 현재 국내외 수집 및 이용 현황과 더불어 기술 발전 현황을 정리하였다.

이어, 생체인식 정보, 유전정보, 건강관련 정보 별로 수집 및 이용시의 문제점 및 피해 사례를 정리하였다.

바이오 정보 수집 및 이용에 대한 일반 시민의 지식, 인식, 태도 등을 알아보기 위해 여론조사기관에 의뢰하여 19세 이상 국민 1,000명에 대한 전화설문조사를 실시하였다.

바이오 정보 관련 국내외 법령 및 가이드라인 등을 검토·분석하였으며, 연구자들의 토론을 통해 도출된 정책적 시사점을 바탕으로 정책제언을 정리하였다. 정책제언은 기본적인 개선 방향 및 원칙을 두고, 국회, 정부, 업체 등 각 기관들이 참고할 수 있도록 기관별 과제를 제안하였다.

제2장

바이오 정보 수집, 이용 현황

제2장 바이오 정보 수집, 이용 현황

가. 생체인식 정보 수집, 이용 현황

1) 생체인식 정보의 특성

생체인식이란 '자동화된 장치에 의하여 개인의 신체적, 행동적 특성을 통하여 신원을 인증(authentication)하거나, 신원을 식별(identification)하는 것을 말한다(이은우, 2004). 그리고 이를 위해 사용되는 신체적, 행동적 특징에 관한 정보를 생체인식 정보라고 할 수 있다. 생체인식에 사용될 수 있는 신체적 특징으로는 지문, 얼굴, 홍채, 정맥, 망막, 손모양 등이 있으며, 음성, 자판입력(keystroke), 필적, 걸음걸이 등이 행동적 특징에 속한다. 생체인식 기술은 통상 원래의 바이오 정보로부터 특징정보(template data)를 추출하여 사용하는데, 원본정보와 특징정보 모두 생체인식 정보라고 할 수 있을 것이다.

이와 같은 생체인식 정보들은 보통 다음과 같은 특성을 가진다. 첫째, 보편성(Universaility). 모든 사람에게 있는 특징이어야 한다. 그렇지 않다면 생체인식 기술이 처리하지 못하고 오류가 발생할 것이다. 둘째는 고유성(Uniqueness). 서로 다른 개인을 식별할 수 있기 위해서는 사람마다 가지고 있는 정보가 달라야 한다. 즉, 그 개인에게 고유한 정보여야 한다. 셋째, 영구성(permanency). 평생 변하지 않는 특성을 가지고 있어야 한다. 그렇지 않고 시간이 지나면서 혹은 어떤 영향으로 변화한다면 해당 개인을 더 이상 식별하거나 인증할 수 없게 될 것이다. 생체인식 기술에 사용되는 생체인식 정보들은 대체로 변하지 않는 속성을 가지고 있으나, 지문이 없어진 사람이 있는 것과 같이 실제로는 예외적인 경우가 발생하며, 얼굴 인식과 같이 화장이나 성형 등 외부적인 요인에 의해 인식 성능이 영향을 받는다.

2) 인증 및 식별 수단과 생체인식

생체인식은 개인의 신원 인증(authentication)과 신원 확인(identification)에 사용된다. 인증은 '나'라고 주장하는 사람이 정말 '나'인지를 확인하는 과정, 보다 넓게는 어떤 사람이 적절한 권한을 가지고 있는지 확인하는 과정이다. 이에 반해 식별은 '내가 누구인지'를 확인하는 과정이다. 인증은 1:1 방식이라고도 부르며, 식별은 데이터베이스에 등록된 여러 생체인식 정보 가운데 일치하는 하나를 찾아내는 방식이기 때문에 1:N 방식으로 불린다. 아이디가 다른 사람으로부터 나를 구별해주는 식별자이고 비밀번호가 나임을 인증하는 방법이라면, 생체인식 정보는 식별자이자 인증 수단의 역할을 한다고 볼 수 있겠다.

생체인식 이전에도 다양한 인증 방법이 사용되어 왔는데, 이는 지식 기반, 소유 기반, 생체기반 인증으로 나눌 수 있다.(IT world, 2015)

지식 기반의 인증 방식은 내가 알고 있는 것을 토대로 나를 인증하는 방법이다. 대표적인 것이 비밀번호이다. 이는 관리가 편하고 구축하기 쉽지만, 당사자가 잊어버리거나 제3자가 추측 등을 통해 알아내거나 유출될 수 있어서 보안성이 낮다.

소유 기반의 인증방식은 내가 갖고 있는 '징표' 혹은 공유한 정보를 통해서 나를 인증한다. 오프라인에서는 신분증이 대표적이며, 온라인 인증을 위한 OTP(One Time Password), 보안카드, 공인인증서, 토큰 등을 들 수 있다. 이는 비밀번호보다 안전성이 높지만, 기기의 제조 및 발급 비용이 들고, 항상 휴대하고 다녀야하기 때문에 불편하고 분실 위험이 있으며, 다른 사람이 훔치거나 잃어버렸을 경우 신원 도용의 위험이 존재한다.

이에 반해 생체인식 방식은 휴대가 간편하고 비밀번호처럼 잊어버릴 위험이 없으며 분실이나 도난의 위험이 적다. 그러나 인식 시스템 구축을 위한 비용이 많이 들고, 한번 유출될 경우 프라이버시 침해의 위험이 매우 크다.

3) 생체인식 시스템의 작동 과정

생체인식 기술의 절차는 통상 등록(registration)단계와 인증 및 식별단계로 나뉘어진다. 등록단계는 바이오 정보를 인식하여 특징점을 추출한 후 데이터베이스에 저장하는 단계이며, 여기서 저장된 정보는 인증이나 식별단계에서 추출된 생체인식 정보와 비교되게 된다. 이를 그림으로 나타내면 아래와 같다. (IT world, 2015)

[그림 3] 생체인식 기술 절차에 따른 특징 (출처: ITWorld, 2015)

생체인식 기술의 정확성을 평가하는데 사용되는 중요한 지표로는 본인거부율(False Rejection Rate, FRR)과 타인수락율(False Acceptance Rate, FAR) 등이 있다. 본인거부율은 생체인식 시스템의 에러로 개인을 식별하지 못하는 등 인식을 거부할 확률이며, 타인수락율은 타인의 생체인식 정보를 특정인의 것으로 잘못 인식할 수 있는 확률이다. 이 두 비율이 낮을수록 정확도가 높다고 할 수 있다. 예를 들어 금융거래에 생체인

식 정보가 활용될 경우, 본인거부율이 높으면 고객의 인증에 실패하여 고객의 불편을 초래하게 되며, 타인수락율이 높으면 금융 사고를 초래하게 될 것이다. 아래 표는 생체인식 기술 정확도를 지문, 홍채, 손바닥정맥, 손가락정맥, 음성, 얼굴 별로 비교한 연구결과이다.

[표1] 생체인식 기술 정확도 비교 (이재득, 2014)

구분	본인거부율	타인수락율
지문	0.1~0.5%	0.001~0.01%
홍채	0.0001~0.1%	0.000083~0.0001%
손바닥정맥	0.01~0.1%	0.00008~0.0001%
손가락정맥	0.01~0.3%	0.0001~0.001%
음성	1%	0.1%
얼굴	1~2.6%	1~1.3%

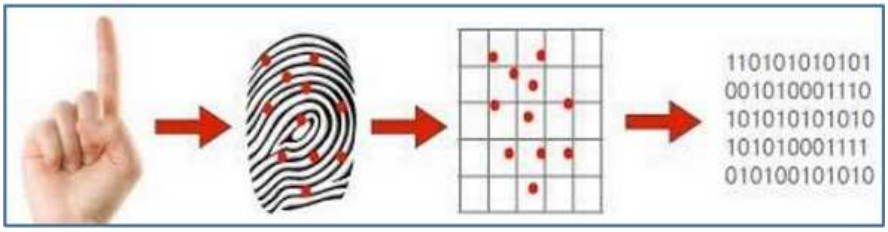
이 표에서 보여주는 바와 같이, 현재 최고의 인식률을 자랑하는 기술은 홍채인식 기술로 약 100만 번에 한 번꼴로 오류가 발생할 정도로 정밀하다.

4) 생체인식 정보의 종류와 기술[1)]

가) 지문 인식(fingerprint recognition)

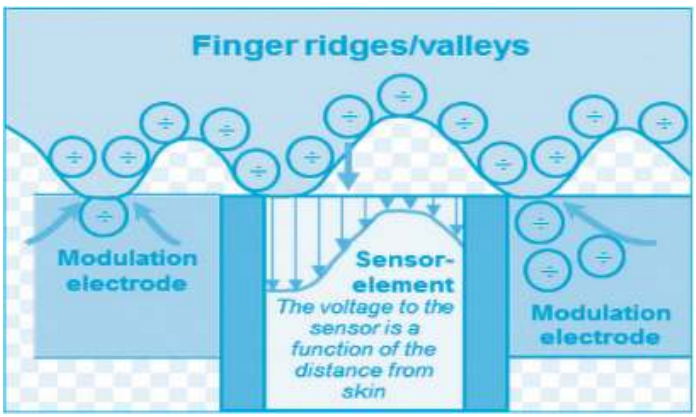
지문은 가장 오래된 생체인식 방법 중 하나이며, 현재 가장 많이 사용되고 있는 생체인식 기술이다. 고대 바빌론 시대에 지문을 이용하여 신분 확인을 했다고 하며, 현대적인 의미에서는 1684년 영국 왕립협회 소속이었던 네에미아 크류(N Gruw)가 처음으로 모든 사람의 지문이 각각 다르다는 것을 알게 되면서 지문인식 기술이 발전하였다. 지문인식은 보통 지문 융기의 분기점, 끝점 등으로 구성되는 특징점의 위치와 속성을 추출, 저장, 비교하는 알고리즘을 채용한다.

1) 아래 각 생체인식 기술의 특성은 이재득(2014), 최우현(2015), Rupinder Saini, Narinder Rana (2014)를 참고한 것이다.

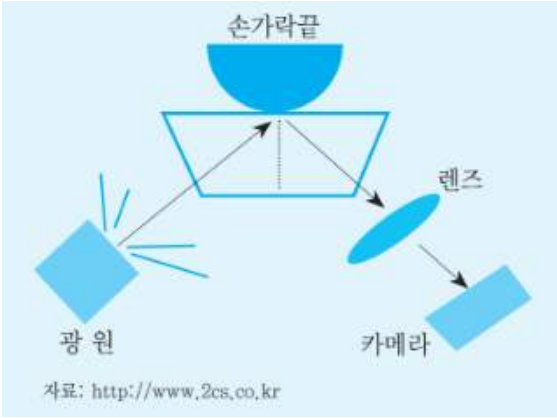


[그림 4] 지문인식 (출처 : Learn Biometrics, https://www.tutorialspoint.com/biometrics/physiological_modalities.htm)

지문인식은 인식방법에 따라 정전용량 방식, 광학 방식, 초음파 방식 등으로 구분이 가능하며 주로 정전용량 방식과 광학 방식이 많이 사용된다. 정전용량 방식은 손가락 피부와 센서 표면의 간격에 따른 정전용량의 차이를 통해 얻어진 지문 영상을 사용하는 방식이며, 광학 방식은 복사기와 같이 강한 빛을 쏘아 반사된 이미지를 통해 인식하는 방식이다.



[그림 5] 정전방식 지문인식 방법
(출처 : www.idx.no, 이재득(2014)에서 재인용)



[그림 6] 광학방식 지문인식 방법 (출처: 이재득, 2014)

정전용량 방식은 사용자의 지문 입력 방식에 따라 스와이프 (Swipe) 방식과 에어리어(Area) 방식으로 나눌 수 있다. 스와이프 방식은 센서에 손가락을 위에서 아래로 문질러 지문을 입력하며, 에어리어 방식은 센서에 손가락을 단순히 대기만 하면 인식할 수 있다. 에어리어 방식은 지문 인식이 빠르고 정확하지만 센서 소형화가 어렵고 가격이 스와이프 방식보다 3배 이상 비싸다. 스와이프 방식은 센서 크기가 작아 다양한 모양과 크기로 적용 가능하지만 인식률이 낮다는 단점이 있다. 삼성전자의 갤럭시 S5가 스와이프 방식을 채택했으며, 애플 아이폰 5S는 에어리어 방식을 채택하였다. 이후 삼성전자도 갤럭시 S6와 S6엣지에서는 에어리어 방식을 선택하였다.

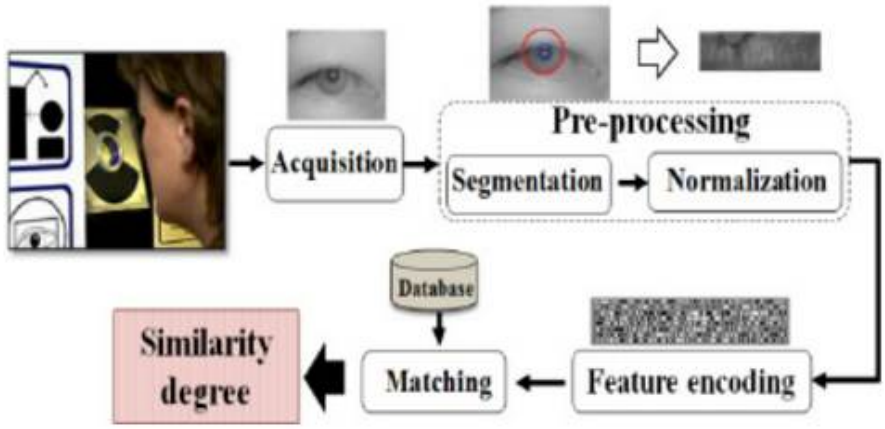
지문은 평생 같은 형태와 모양을 유지하며, 상처가 생겨도 변하지 않는다. 지문은 다른 생체인식 기술에 비해 인식장치가 소형화되고 비용이 저렴하며, 사용자에게 친숙하고 편리하다는 점에서 단일 생체인식 기술 중에서는 가장 많이 활용되고 있다. 그러나 지문영상을 채취할 때 물기나 땀이 인식장치에 묻어있는 경우 오인식률이나 오거부율 등이 크게 높아지고, 인식기에 직접 접촉해야 하기 때문에 여러 사람이 이용하는 경우

불쾌감이나 위생 문제를 야기할 수 있으며, 불의의 사고나 후천적인 요인으로 지문이 변화하거나 없어질 수 있다는 점이 한계이다.[2] 또한, 우리의 지문은 여러 곳에 남겨질 수 있다. 그래서 범죄수사에 이용될 수 있는 것이겠지만, 역으로 정보주체에게는 자신의 지문이 유출되거나 도용될 가능성이 크다는 것을 의미한다.

나) 홍채 인식(Iris Recognition)

홍채인식은 안구 중앙의 검은 동공과 흰자위 사이에 있는 도넛 모양의 홍채를 이용한 인증 기술이다. 홍채인식 장치의 적외선 카메라가 홍채를 이미지화한 후, 홍채인식 알고리즘으로 사용자 고유의 홍채 코드를 생성, 등록 후 비교하는 방식이다. 홍채는 생후 10개월 경에 고유한 구조가 형성되어, 후천적인 상처나 질병과 같은 요소를 제외하면 평생 변하지 않는다. 일란성 쌍둥이도 서로 다른 형태의 홍채를 가지고 있어 개인을 식별하는데 훨씬 정확하다고 한다. 본인인증에 실패할 확률이 100만분의 1 정도로 정확도가 높을 뿐 아니라, 인식 속도도 빠르다. 홍채 인식은 통상 10cm 정도 거리에서 이루어지는데, 지문과 달리 비접촉 방식이고 콘택트렌즈나 안경을 착용해도 인식이 가능하기 때문에 불쾌감이 낮고 위생적이라는 장점이 있다. 높은 정확도 때문에 보안성을 요구하는 공항(미국, 캐나다, 영국, 네덜란드, 아이슬란드 등) 등에서 사용되고 있다(윤재호 등, 2016).

2) 인구의 약 2% 정도가 상처나 유전적 요인으로 지문인식을 사용할 수 없다고 한다. (Rupinder Saini, Narinder Rana (2014))



[그림 7] Iris Recognition System (출처 : ResearchGate, https://www.researchgate.net/figure/264825250_fig1_Fig-1-Architecture-for-iris-recognition-system)

그러나 홍채인식 시스템도 고해상도의 사진을 통해서 우회할 수 있음이 드러난 바 있다.[3] 또한, 홍채인식 장치의 정확도는 특이한 조명 등에 의해 영향을 받을 수 있고, 홍채인식 장치가 눈에서 일정거리 이상 가까워야 하며, 당뇨병 등 질병에 의해 홍채가 변할 수도 있다. 다른 생체인식에 비해 홍채인식 장치는 비싸며, 홍채인식 기기가 고정식일 경우에는 서로 다른 키를 가진 사람들에게 불편을 초래할 수 있다.

다) 정맥 인식 (Vein Recognition)

정맥인식은 사람마다 고유한 혈관형태를 갖고 있다는 특성을 이용한다. 정맥인식은 혈관인식 위치에 따라 손가락정맥, 손등정맥, 손바닥정맥 등으로 나눌 수 있다. 대부분의 정맥인식 장치는 근적외선이 헤모글로빈에 흡수

3) 2014년 독일 해커단체 CCC는 블라디미르 푸틴 러시아 대통령의 고해상도 사진을 이용하여 생체인식 시스템을 우회할 수 있음을 시연한 바 있다. (한국경제, "[Focus] 인증 기술 진화… 비번→패턴→지문→홍채→?", 2016년 8월 12일)

되는 성질을 이용하여 정맥 이미지를 추출한다. 혈관 분포를 지도의 도로망처럼 단순화한 뒤, 분기점 간 거리나 각도 등 각 분기점 정보를 저장한다.

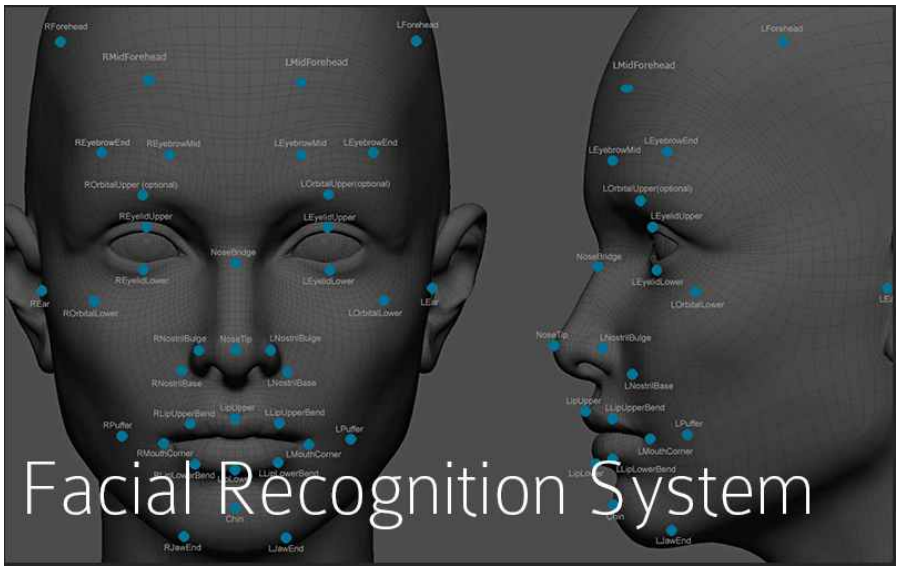
[그림 8] Palm Vein Recognition (출처 : IDENTYTECH Solutions, http://www.identytech.com/palm-vein-recognition/)

사람의 혈관은 유전적 형질이 같은 일란성 쌍둥이조차도 형태가 달라 인식 정확도가 높으며, 피부 내에 존재하는 정맥을 이용하기 때문에 외부로의 노출이나 복제가 거의 불가능하다는 장점이 있다. 또한 지문이 없거나 손가락이 없는 사용자도 사용할 수 있다. 그러나 정맥인식 장치의 구조가 소형화하기 어렵고 전체적인 비용이 증가하는 단점이 있다.

라) 얼굴 인식

얼굴 인식은 각 개인 얼굴의 특징을 이용한다. 카메라를 통해 입력된 화상으로부터 각 개인마다 독특한 부위를 측정 단위로 추출하는 것인데, 독특한 부위가 어떠한 곳인지 결정하는데 이 기술의 정확도가 달려있다. 얼굴 영역을 추출하는 방법으로는 2차원이나 3차원 얼굴 영상을 이용하는 방식과 얼굴에서 발생하는 열을 이용하는 방식이 있다. 얼굴을 열상을 이용하는 방식은 적외선 카메라를 사용하여 얼굴 혈관에서 발생하는 열

을 촬영한 후 디지털 정보로 변환하여 저장하는 방식인데, 얼굴에 미미한 손상이 발생하더라도 본인거부율이 낮은 장점이 있지만, 영상 획득을 위해 사용하는 적외선 빛에 대해 사람들이 거부감을 가질 수 있다는 단점이 있다.



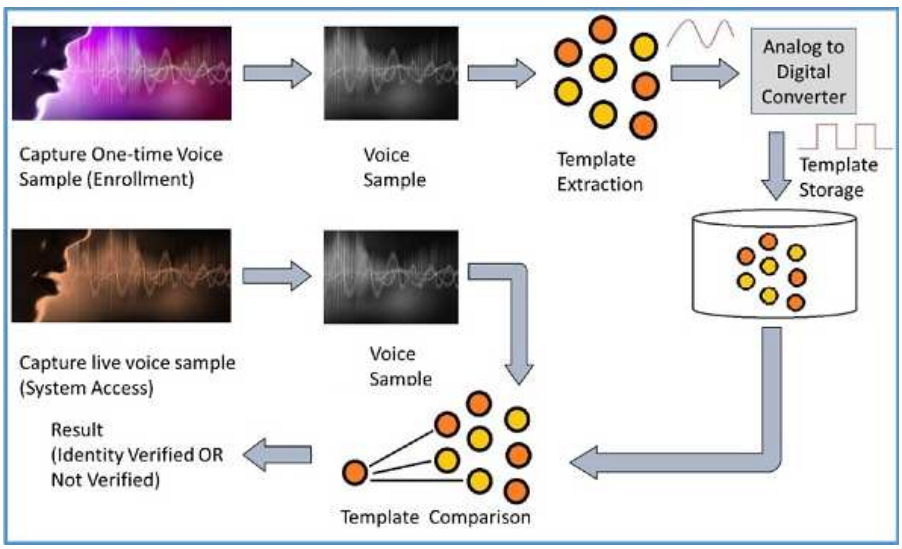
[그림 9] face recognition system (출처 : HK Systems Limited, http://hksl.com.hk/case-study.html#face)

얼굴인식 역시 비접촉으로 개인식별이 가능하여 거부감이 적다는 장점이 있으나, 카메라의 설치 각도와 조명의 밝기에 민감하고, 카메라의 성능에 따라 인식률에 차이가 있을 수 있으며, 변장 및 성형과 같이 얼굴의 후천적인 변화와 표정 변화, 유사한 얼굴 특징을 가진 사람에 의한 인식 오거부율 등의 약점이 있다. 또한, 다른 생체인식 시스템에 비해 비용이 많이 든다. 얼굴인식 시스템은 공항, 공원 등에 설치되어 많은 사람들 가운데에 특정 개인을 식별해낼 수 있으며, 다른 인식 시스템과 달리 대량

인식처리가 가능하다. 반면, CCTV 등을 통해 본인도 모르게 촬영된 영상이 활용될 경우 프라이버시를 크게 위협할 수 있다.

마) 음성인식 (Voice Recognition)

음성인식은 사용자의 음성으로부터 추출한 독특한 특성을 이용하는 인식기술로 음성 경로, 비강과 구강의 모양 등에 의한 음성학적 특성을 이용한다. 인식단말기를 통해 음성을 입력받은 후 특징을 추출하여 기존에 저장된 음성 데이터베이스와 비교해 가장 유사한 음성을 찾아내는 방식이다. 음성적 특성들은 억양에 영향을 받지 않으며 음성의 경우, 비강, 구강의 형태에 의존하기 때문에 비슷하게 흉내내는 방식으로는 모방이 불가능하다.



[그림 10] Voice Recognition System (출처 : Learn Biometrics, https://www.tutorialspoint.com/biometrics/voice_recognition.htm)

음성인식은 다른 생체인식 기술과 다르게 PC, 휴대폰, 태블릿 PC 등에 기본적으로 탑재되어 있는 마이크를 인식단말기로 이용할 수 있어, 인식단말기의 보급·구입에 대한 부담이 적다는 장점이 있다. 또한, 다른 생체인식과 다르게 손 등을 움직일 필요가 없으며, 자연스러운 음성 자체를 이용하기 때문에 손이 불편한 사람들에게 도움이 된다. 텔레뱅킹과 같이 원거리에서도 음성 취득이 가능하여 다른 생체인식이 불가능한 분야에서 적용이 가능하다. 그러나 주변소음 등 외부환경이나 마이크 등 음성인식 장치의 성능에 따라 인식률이 달라지는 것이 단점이다. 이미 녹음된 음성을 이용한 해킹에도 취약할 수 있다.

바) 필체인식 (Signature)

필체인식 혹은 서명인식은 개인서명의 고유한 특징을 이용하여 인증하는 기술이다. 이미 작성된 서명을 인식하는 정적인 방법과 서명하는 과정을 동적으로 파악하는 방법으로 구분한다. 동적서명 인식은 새로운 서명 샘플과 원본 데이터 서명의 모양을 단순히 비교하는 방법이 아니라 원본 데이터와 샘플링된 데이터가 쓰여지는 방법을 비교하는 것으로 서명시간, 속도, 압력, 종이로부터 펜이 떨어진 횟수 등을 이용한다.

서명은 오래 전부터 계약 체결 등 서류에 대한 증빙 목적으로 이용되어 온 친숙한 인증 방법으로 사용이 편리하고 비용이 저렴하다는 장점이 있으나 정확도가 떨어지고 위조가 가능하다는 것이 단점이다.(윤재호 등, 2016)

5) 주요 활용 분야별 현황

생체인식 기술은 공공행정, 민간 및 공공영역의 출입통제 등 보안, 범죄예방 및 수사, 스마트폰 등 정보통신기기 인증, 금융 영역의 본인인증 및 결제수단 등의 용도로 폭넓게 도입되고 있다. 아래 표는 생체인식 기술 도입 사례를 주요 분야별로 정리한 것이다.

[표2] 생체인식 기술 도입 현황

영역	도입 사례
공공행정	생체인식 전자주민증, 선거 관리, 난민 원조, 무인민원발급기 등
출입통제	전자여권, 출입국관리, 시설안전, 근태관리(출퇴근관리), 식당/도서관/기숙사 등 이용자 관리 등
범죄예방 및 수사	방범용 및 주차단속 등 공공질서를 위한 CCTV, 범죄정보관리 및 범인식별, 체납차량 단속 등
IT보안	스마트폰 및 컴퓨터 인증 등
금융	ATM 등 본인인증, 지불결제 수단 등
마케팅	고객 연령, 성별 등 성향분석, 포인트 적립 등
서비스	인터넷 얼굴식별 서비스, 페이스북 '이름표추천' 기능 등
의료	환자 본인식별, 원격의료 등

아래에서는 주요 활용 분야별 현황을 좀 더 자세하게 검토해보았다.

가) 공공 행정

(1) 주민 생체인식 정보수집

많은 나라들이 국민들의 신원확인을 위해 지문, 홍채, 얼굴 등 생체인식 정보를 사용하고 있다. 주민등록시 기본적인 개인정보와 함께 생체인식 정보 역시 수집되며, 이렇게 수집된 정보는 선거인 확인, 의료나 복지 등 공공 서비스 제공 등 공공 행정의 여러 영역에서 신원확인을 목적으로 활용되고 있다. 생체인식을 활용한 개인식별과 인증은 전통적인 방식에 비해 국민들의 신원확인을 위한 보다 효과적이고 안전한 도구로 인식되고 있기 때문이다. 선진국 뿐만 아니라, 체계적인 신원확인 시스템이 갖춰져있지 않은 아프리카, 아시아, 남미 등 개발도상국에서도 생체인식 시스템의 도입이

급증하고 있다. 그러나 개발도상국에서는 개인정보 보호를 위한 법제가 미비한 경우가 많아서 프라이버시 침해에 대한 우려가 나오고 있다.

생체인식 기술은 우선 기본적인 국민식별(혹은 주민등록) 시스템에 도입되고 있다. 멕시코, 인도, 아르헨티나 등의 정부는 생체인식 국민식별 시스템을 개발하고 있다.(Privacy International, 2013) 인도는 세계에서 가장 거대한 생체인식 데이터베이스를 갖고 있는 나라다. 인도는 '아드하르(Aadhaar)'라는 국민식별번호를 가지고 있는데, 이는 인도고유식별국(Unique Identification Authority of India , UIDAI)이 발급하는 12자리 임의번호이다. 인도 주민이면 누구나 아드하르 번호를 신청할 수 있다. 등록 과정에서 이름, 생년월일, 성별, 주소, 핸드폰번호 및 이메일 주소(선택) 등 기본적인 개인정보와 열손가락 지문, 두개의 홍채정보, 사진 등 생체인식 정보를 제공해야 하며, 이 정보들은 중앙의 데이터베이스에 저장된다. 아드하르는 신용카드나 여권 발급시 등 기본적인 신분 증명과 정부의 복지 프로그램 등을 제공받기 위해 사용된다.[4] 아드하르는 2010년 9월 29일 첫 발급이 시작되었으며, 현재까지 10억4천만 개의 번호가 발급되었다. 그러나 아드하르의 법적 근거가 되는 「아드하르법」은 2016년 7월 12일에야 제정이 되었으며, 이 법에 따라 인도고유식별국은 전자정보기술부 산하의 법정기관이 되었다.[5]

1800년대 후반부터 수사 목적의 지문인식 시스템을 구축하는 등 생체인식 기술의 활용도가 높았던 아르헨티나는 2011년에 Sibios(Sistema Integrado de Identificación Biométrica)라는 통합생체인식식별시스템을 구축하였다. 이는 기존의 ID 카드 데이터베이스와 아르헨티나 국민등록소(RENAPER)를 통합한 것으로 국민들의 기본 정보와 디지털 사진이미지

4) Unique Identification Authority of India, "About Aadhaar", https://uidai.gov.in/beta/your-aadhaar/about-aadhaar.html

5) Unique Identification Authority of India, "About UIDAI", https://uidai.gov.in/beta/about-uidai/about-uidai.html

및 지문정보를 포함하고 있다.[6]

이스라엘은 2009년 「생체인식 데이터베이스 법」을 통과시켰으며 모든 국민들의 지문과 얼굴 정보의 데이터베이스를 갖고 있다. 사우디아라비아 역시 마찬가지다. 남아프리카공화국도 한국과 마찬가지로 광범위한 국가적 지문 데이터베이스를 운영하고 있다.[7]

(2) 생체인식 신분증

신분증도 기존의 종이나 플라스틱 형태에서 신용카드와 같이 내장된 칩을 가진 전자신분증으로 변화하고 있다. 태국은 지문정보를 내장하고 있는 스마트 ID 카드를 도입했는데, 이는 세계에서 가장 큰 IC 카드 프로젝트로 여겨지고 있다. 알바니아, 콜롬비아, 이라크, 모로코는 생체인식 전자주민증을 갖고 있다.[8] 헝가리는 2016년 1월 전자주민증(eID) 발급을 시작했다. “One-Stop Card”라고 불리우는 이 카드는 지문인식 데이터, 사회 보장 및 조세번호 등을 통합한 것이다. 1월 4일 발급을 시작한 후 5일 만에 39,204명이 신청했다고 한다.[9] 요르단도 2016년에 지문 및 홍채 정보를 포함한 전자주민증 발급을 시작했다.[10]

---

6) Privacy International, “Ignoring repeated warnings, Argentina biometrics database leaks personal data”, 2013년 12월 9일, https://www.privacyinternational.org/node/342

7) YourNewsWire.com, The Global Rise Of Biometric ID Cards, 2016.2.6, http://yournewswire.com/the-global-rise-of-biometric-id-cards/

8) 위키피디아, List of national identity card policies by country, https://en.wikipedia.org/wiki/List_of_national_identity_card_policies_by_country (2016.10.16 방문)

9) 위키피디아, List of national identity card policies by country, https://en.wikipedia.org/wiki/List_of_national_identity_card_policies_by_country (2016.10.16 방문)

10) planet biometrics, “Jordan to roll out biometric smart IDs ‘next week’ ”, 2016년 6월 30일, http://www.planetbiometrics.com/article-details/i/4673/

그러나 국가가 국민들의 생체인식 정보 데이터베이스를 보유하거나, 생체인식 전자주민증을 발급하는 것에 대한 시민사회의 반발도 크게 일어나고 있다. 호주, 캐나다, 뉴질랜드, 영국, 미국 등의 나라에서 생체인식 전자주민증에 대한 반대운동이 성공적으로 이루어졌다.[11] 2007년 세르비아에서도 시민들의 반대로 생체인식 주민증 계획이 철회되었다.[12]

2012년 3월 22일 프랑스 헌법위원회는 프랑스의 생체인식 신분증의 도입이 위헌이라고 결정했다. 프랑스 의회는 2012년 3월, 생체인식 신분증 발급에 관한 「신원 보호법」을 제정하였는데, 신분증 안의 칩에는 주소, 개인의 키, 눈동자 색깔, 얼굴사진, 지문 등 개인 정보가 내장된다. 별도의 옵션 칩에는 전자 정부 및 전자 상거래에 사용될 수 있는 온라인 인증 및 전자서명이 담길 수 있다. 프랑스 개인정보 감독기구(CNIL)는 2011년 10월, 중앙집중적 생체인식 데이터베이스를 비판하는 보고서를 발행하였지만 프랑스 의회는 이를 무시하였다. 이에 이 법안에 반대하는 의원들이 이 법안이 프라이버시권 및 무죄추정의 원칙 등 시민들의 기본권을 침해한다고 헌법위원회에 이의를 제기한 것이다.[13]

영국에서는 2006년 「신분카드법」(Identity Cards Act 2006)이 통과되어, 국가신분증을 발급하기 시작했는데, 이들 정보는 국가신분등록소(National Identity Register, NIR)에 데이터베이스로 저장되었다. 이 법은 NIR에 50가지 범주의 개인정보들을 저장하도록 했는데, 이에 열손가락 지문, 디지털화된 얼굴 이미지, 홍채 이미지 등이 포함되었다. 인권단체, 법률가, 보안 전문가, 정치인 등이 이 계획에 반대하였으며, 사회적인 논란이 확대되었다. 2010년 총선에서 보수/자유민주연합이 집권하면서 ID 카드 계획은 폐기되었다.[14] 2010년 12월에 통과하여 2011년 1월 21일 시행된

11) EFF, https://www.eff.org/issues/national-ids

12) EDRi, Serbia rejects biometric ID cards, 2007년 1월 31일

13) EDRi, France: Biometric ID database found unconstitutional, 2012년 3월 28일

「신분문서법」(Identity Document Act 2010)에 의해 기존에 발급된 ID 카드의 효력은 정지되었고, NIR에 저장된 데이터도 삭제되었다.[15] 독일에서는 2005년 생체인식 여권을 도입하면서 생체인식 데이터베이스를 생성하지 않기로 결정했다.[16]

(3) 선거 관리 및 원조 제공

투명한 선거 관리를 목적으로 한 생체인식 정보의 사용도 증가하고 있다. 솔루션에 따라 선거인 명부 등록, 투표, 검수 등 선거 관리의 각 단계에서 사용될 수 있다. 지문, 정맥, 얼굴, 홍채인식 기술 등이 사용된다.[17] 필리핀, 가나, 케냐에서는 선거에서 선거인 생체인식 등록을 사용한 바 있다.

원조 제공 프로그램에도 사용된다. 지난 2010년 유엔난민고등판무관(UNHCR)은 생체이식 정보에 대한 정책을 발표하면서, 난민 캠프에서 난민 등록의 체계화를 위해 생체인식 정보 수집 시스템을 도입한다고 밝혔다. 이후 UNHCR은 부룬디, 에티오피아, 케냐, 이집트, 마케도니아, 말레이시아, 파키스탄, 탄자니아, 리베리아, 세네갈, 남수단, 시리아 등에서 난민을 식별하고 추적하기 위해 "ProGress"라는 시스템을 통해 생체인식 등록 시스템을 채택하였다. 세계은행은 수혜자의 효과적인 식별을 위해 베닌과 케냐에서 도시 빈민 등록을 위한 생체인식 시스템을 지원하였다. (Privacy International, 2013)

---

14) 위키피디아, "Identity Cards Act 2006", https://en.wikipedia.org/wiki/Identity_Cards_Act_2006 (2016년 10월 29일 방문)

15) GOV.UK, "Identity cards and new Identity and Passport Service suppliers", https://www.gov.uk/guidance/identity-cards-and-new-identity-and-passport-service-suppliers

16) Privacy International, 2013

17) ttp://www.biometricupdate.com/biometric-news/elections-biometric-news

(4) 한국, 전자주민증 논란과 지문정보 전산화

한국에서는 수차례 전자주민증 논란이 되었지만 아직 도입되지는 않았다. 1996년 전자주민카드를 둘러싼 논쟁은 한국에서 개인정보 보호에 대한 문제의식이 시작된 계기가 되었다. 1995년 4월 내무부는 전자주민카드 시행계획을 발표하였는데, 시민사회는 중앙집중적인 전자주민카드가 가져올 개인정보 유출과 감시의 가능성에 대하여 우려하였다. 결국 1999년 2월에 전자주민카드 반대를 공약으로 제시한 김대중 정부가 당선되고 IMF 경제위기에 따른 긴축 재정의 필요성이 겹치면서 전자주민카드 시행계획은 백지화되었다.

이후 2005년 참여정부, 2010년 이명박 정부에서 또다시 전자주민증 도입이 시도되었으나 결국 실패하였다. 이명박 정부 당시 전자주민증은 IC칩에 주민등록번호, 지문 등 12개 신원확인 항목을 수록할 계획이었다. 한편, 2001년 4월 보건복지부는 의료기관의 부당·허위청구를 근절하겠다는 명목으로 전자건강카드 실시계획을 발표하였다. 그러나 시민사회는 민감한 건강정보가 민간에 의해 오남용될 가능성에 대하여 크게 우려하였고, 결국 이 계획은 2002년 1월 백지화되었다.

전자주민카드 사업은 중단되었지만, 지문 정보는 전산화되기 시작했다. 정부는 1999년 주민등록증을 일제 경신하면서 플라스틱 전자주민증으로 교체하기로 하고 국민들에게 새로이 지문날인을 받기 시작했는데, 이는 전 국민 지문을 전산으로 입력하고 경찰이 범죄수사용으로 관리하기 위해서였다.

2005년 3월부터는 주민등록법 시행령 개정을 통해 주민등록번호와 지문만으로도 무인민원발급기를 이용할 수 있도록 하였다. 2014년에는 '사전투표제도'가 도입되었는데, 이를 위해 '본인확인기'가 사용되었다. 본인확인기는 신분증 스캐너와 지문(손도장)입력장치, 서명입력장치가 하나로 결합된 기계장치다. 신분증 스캐너는 선거인명부 등재여부를 확인하는 데 활용

되며, 지문입력장치와 서명입력장치는 선거인의 투표용지 수령 여부를 확인·기록한다.[18] 경찰청이 열손가락 지문 정보를 보유하고 있는 것과 달리 행정자치부는 엄지손가락 지문 정보를 보유하고 있으며, 이를 본인 확인 용도로 사용해왔다. 그런데 2015년 국정감사에서 인감증명 발급 시 지문인식기 약 89%, 무인민원발급기 약 68%라는 낮은 지문인식률이 문제로 지적되면서 경찰청이 보유한 지문자동검색시스템(AFIS) 지문정보를 이용할 계획을 세우고 있다. 행정정보공동이용센터를 중심으로 주민등록 중앙정보시스템과 경찰청시스템이 연계하려는 것이다.[19]

나) 범죄예방 및 수사

범죄 예방 및 수사를 위해 지문, DNA, 얼굴 등 다양한 생체인식 정보가 활용되고 있다. 한국은 이미 1970년대부터 열손가락 지문 날인을 시작했고, 이렇게 수집된 지문은 경찰의 수사 목적을 위해 활용되고 있다. 검찰과 경찰은 90년대 중반부터 유전자은행 설립을 위해 노력해 왔으며, 2004년 「실종아동등의 보호 및 지원에 관한 법률」이 통과되어 유전자 데이터베이스가 도입되었고, 2009년 「디엔에이신원확인정보의 이용 및 보호에 관한 법률」 통과를 계기로 범죄자를 대상으로 한 유전자 데이터베이스 구축이 시작되었다. 한편, 범죄예방 및 시설안전 등을 목적으로 공공 및 민간 영역에서 CCTV의 도입이 급증하고 있으며, 최근에는 이를 '통합관제센터'를 통해 통합 관리하는 방향으로 나아가고 있다. (진보네트워크센터, 2016)

(1) 경찰의 지문정보 활용

지문은 과학 수사 영역에서 가장 오래전부터 사용되어 온 생체인식 정보이다. 한국에서 지문감식은 1948년 내무부 치안국에 '감식과 지문계'가

18) 뉴시스, 최초도입 사전투표장치, 이렇게 구성된다, 2014.5.22

19) 전자신문, 인감증명서 발급, 지문 닳아도 걱정할 필요없네, 2016.9.21

설치되면서 시작되었다. 전 국민을 대상으로 한 지문 정보의 수집은 1968년 주민등록증을 발급받을 때 좌우 엄지손가락 지문을 날인하도록 하면서 시작되었고, 1975년에는 십지지문을 등록하도록 하였다. 지문 정보의 전산화는 1990년 경찰이 지문검색시스템(IFIS)를 구축하면서 시작되었다. 금고 이상 전과자의 패턴 특징을 DB로 저장한 뒤 범죄 현장에서 발견된 지문 패턴과 대조하는 방식이었다. 초기에는 저장장치 용량이 얼마 되지 않아 패턴 특징만 저장할 수 있었으나, 현재 경찰이 운용하는 지문자동검색시스템(AFIS)은 지문 이미지까지 저장할 수 있고, 현장 지문의 특징을 입력하면 컴퓨터가 주민등록 지문 DB에서 특징이 유사한 지문을 자동으로 여러 개 찾아준다. 패턴만 선명하다면 온전한 크기의 20%만 남은 '조각지문' 혹은 '쪽지문'만 갖고도 일치하는 지문을 찾아낼 수 있다고 한다. 지문 감식을 통한 신원 확인 성능도 갈수록 좋아지고 있는데, 2004년에는 의뢰받은 1만9천577건 중 8천460건(43.2%)만 확인에 성공했지만, 2014년에는 1만9천632건 중 1만1천494건(58.5%)까지 성공률이 높아졌다.[20]

미국에서는 연방수사국(FBI)이 국가적 차원의 지문인식 및 범죄경력 시스템(The Integrated Automated Fingerprint Identification System, IAFIS)을 운영하고 있다. IAFIS는 범죄자 파일에서 7천만 개, 민간인 지문 3천1백만 개, 그리고 미국 및 국제 법집행기관으로부터 획득한 테러리스트로부터 7만3천 개의 지문 정보를 보유하고 있다. 지문 정보는 지역, 주, 연방의 법집행 기관으로부터 입력된다. 이 기관들은 범죄자 체포, 고용시 배경 조사, 그리고 US-VISIT 프로그램으로부터 지문 정보를 획득한다.[21]

---

20) 연합뉴스, <한국의 과학수사> ①'빼도박도 못하는 증거' 지문, 2016.5.28

21) 위키피디아, Integrated Automated Fingerprint Identification System, https://en.wikipedia.org/wiki/Integrated_Automated_Fingerprint_Identification_System#cite_note-autogenerated1-1 (2016.10.16 방문)

(2) 방범용 CCTV 등 얼굴인식 수집장치

얼굴 정보는 CCTV, 블랙박스, 채증장비, 바디캠 등 수많은 영상정보 수집장치 및 웨어러블 장비를 이용하여 수집되고 있다. 한국에서 방범용 CCTV는 2002년 서울 강남구와 강남경찰서가 처음으로 도입하였다. 이에 대하여 국민을 잠재적 범죄자로 취급하고 사생활을 침해한다는 비판과 더불어 아무런 법률적 규범 없이 경찰과 지방자치단체의 자의적인 운영에 맡겨져 있다는 점에서 논란이 제기었지만, 공공기관이 설치한 CCTV는 빠르게 증가하고 있다.

2016년 10월 11일 진선미 의원이 발표한 자료에 따르면, 행정자치부에서 제출받은 자료를 분석한 결과 범죄예방과 교통정보수집 등을 위해 공공기관에서 사용하는 CCTV가 해마다 10만대씩 증가하고 있다고 한다. 중앙행정기관과 지방자치단체가 사용하는 CCTV는 2011년 약 36만대였지만 2012년에는 46만대, 2013년에는 56만대로 증가했고, 가장 최근인 2015년에는 73만대로 집계되었다. 4년간 약 40만대, 해마다 10만대씩 증가한 것이다.

목적별로 살펴보면 '범죄예방'과 '시설 안전'을 위한 CCTV가 중앙행정기관과 지자체를 가리지 않고 가장 많이 증가한 것으로 나타났다. 방범용 CCTV는 2011년 14만대에 불과했으나 2015년에는 무려 34만대로 20만대가 증가했다. 시설안전용 CCTV의 경우 2011년에는 20만대였지만 2015년에는 36만대로 11년 대비 16만대가 증가했다. 나머지 교통단속 및 교통정보수집용 CCTV는 4년간 각각 1만대 증가에 그친 것으로 나타났다.[22]

22) 진선미 의원 보도자료, 2018년, "공공기관 CCTV 100만 시대"진입, 2016.10.11

[표3] 2015년 말 기준 공공기관 CCTV 설치 대수 현황 (단위 : 대)

기관별	목적별	2011년	2012년	2013년	2014년	2015년
중앙행정기관 (교육기관 포함)	범죄예방	90,727	112,016	154,644	163,569	173,649
	시설안전	135,589	153,916	170,746	212,854	229,866
	교통단속	5,308	6,038	6,422	7,054	7,228
	교통정보수집	1,055	5,094	6,570	7,077	8,451
	계	232,679	277,064	338,382	390,554	419,194
지방자치단체	범죄예방	51,064	76,152	105,454	127,869	167,109
	시설안전	71,754	96,031	107,256	119,727	133,465
	교통단속	6,328	9,008	10,689	11,873	14,015
	교통정보수집	2,477	3,491	3,942	5,007	5,449
	계	131,623	184,682	227,341	264,476	320,038
합 계	범죄예방	141,791	188,168	260,098	291,438	340,758
	시설안전	207,343	249,947	278,002	332,581	363,331
	교통단속	11,636	15,046	17,111	18,927	21,243
	교통정보수집	3,532	8,585	10,512	12,084	13,900
	계	364,302	461,746	565,723	655,030	739,232

공공기관에서 설치한 CCTV만 범죄예방 및 수사 목적으로 사용될 수 있는 것은 아니다. 민간에서 설치한 CCTV 역시 필요한 경우 수사기관이 수사목적으로 접근할 수 있다. <2015년 정보화통계집>에 따르면, 민간 및 공공영역에서 CCTV 설치, 운영대수는 795만 6천여대로 추정이 된다. 전체적으로 32.7%의 사업체에서 CCTV를 설치하고 있었으며, 금융 및

보험업의 설치운영 비율이 71.7%로 가장 높게 나타났다.(한국정보화진흥원, 2016)

그러나 한번 도입된 CCTV가 애초의 도입 목적과 다른 용도로 사용되거나 제3자 제공되는 것에 대한 우려가 제기되고 있다. 2013년에는 대한문 부근에 설치된 CCTV가 쌍용자동차 농성장을 실시간 감시해온 것이 드러났다. 해당 CCTV에 대한 열람 신청을 통해 감시 여부를 확인한 결과 경찰과 집회 참가자들이 충돌했던 시간대에 유독 집회 참가자들을 향해 CCTV카메라를 줌하고 회전하는 경우가 많았다. 2014년 5월에는 광주 우체국 앞 세월호 촛불집회를 방범용 CCTV 2대로 실시간 감시한 사례가 있었다.[23)]

CCTV의 목적 외 이용과 관련하여 또 하나의 큰 쟁점은 '통합관제센터'의 운영이다. 지방자치단체에서 설립한 CCTV는 본래 시설안전, 주차단속 등 그 설치 목적별로 수집 및 운영되고 있었다. 그런데 2011년 1월, 당시 안전행정부는 2015년까지 전국 230개 모든 지방자치단체에 CCTV 통합관제센터 구축을 지원하겠다고 밝히고 <지방자치단체 영상정보처리기기 통합관제센터 구축 및 운영 규정>을 제정하여 시행해오고 있다. 행정자치부와 한국정보진흥원이 운영하는 영상정보자원 지원센터에 따르면, 불법주정차단속, 불법 쓰레기 투기 단속, 방범, 하천감시, 문화재보호, 농수산물 도난 예방, 초등학교 방범 목적 등으로 설치된 CCTV 영상들이 통합관제 시스템을 통해 통합되고 관리 된다.[24)] 2014년 장하나 의원이 진보네트워크센터와 함께 전국 지방자치단체 101곳의 CCTV통합관제센터의 운영 현황을 전수 조사한 결과 전국 대부분의 통합관제센터에서 위법을 저지르고 있었던 것으로 나타났다. 전체 관제센터의 84%에 경찰이 파견되어 있는데, 이 자체가 제3자에 대한 개인 영상정보의 실시간 송출

---

23) 광주드림, "CCTV 시민을 감시하다", 2014년 10월 6일, http://www.gjdream.com/v2/simin/view.html?news_type=105&uid=459733

24) 영상정보 지원센터, "통합관제센터 소개", http://www.ncctv.or.kr/front/cctv/controlIntro1.do

및 상시 관제행위로서「개인정보 보호법」위반이라는 것이다.[25]

국가인권위원회는 2013년 발간한 <정보인권 보고서>에서 △지자체 CCTV 통합관제센터의 설치·운영 목적을 구체화하고 △개인영상정보 공유를 최소화하는 한편 공유·제공 요건·절차를 마련하며 △개별 CCTV별로 운영결과를 매년 투명하게 지역주민과 언론에 공개하고 △설치·운영 목표의 설정, 관리·운영지침 제정·운영 등에 있어서 지역주민·인권단체·지역전문가 등의 참여를 보장할 것을 제안하였다.[26] 개인정보보호위원회 역시 2016년 8월 김앤장법률사무소에 'CCTV 통합관제센터에서 처리되는 개인영상정보의 보호강화 방안 연구'용역을 발주하면서 "통합관제센터는 설치 근거 법령이 없다"고 밝혔다.[27]

CCTV의 성능도 고도화되고 있다. 기존의 아날로그 CCTV에서, 디지털화되고, 네트워크로 연결되며, 고화질·고성능을 갖춘 '지능형 CCTV'로 진화하고 있다. 지능형 CCTV는 영상에서 이상행위를 스스로 감지하고 관제센터에 이를 통지해주는 기능 등을 제공한다.[28] 예를 들어, 지능형 CCTV는 고성과 같은 소리에 자동으로 반응하거나, 침입, 배회, 군집과 같은 행동패턴을 인식하여 문제상황인지를 판단하고, 얼굴을 인식하여 실종자인지 검색해준다.[29] 이와 같은 지능형 CCTV는 정부가 구축 중인 재난안전통신망

25) 장하나 의원실, <CCTV 통합관제센터> 현황 최초 전수조사 발표, 2014년 3월 24일, http://act.jinbo.net/wp/wp-content/uploads/2014/03/20140324report.pdf; 민주당 장하나의원실, 진보네트워크센터, 인권단체연석회의, "시민을 감시하는 제3의 눈, CCTV", 영상정보기기로 인한 인권침해 증언대회 및 제도개선 방향 토론회 2014년 3월 25일, http://act.jinbo.net/wp/7928

26) 국가인권위원회, 정보인권보고서, 2013.3.27

27) 오마이뉴스, "CCTV감찰 문제없다 vs 인권침해·개인정보법 위반", 2016년 10월 13일

28) IT조선, "지능형 CCTV의 진화가 가져올 변화", 2015년 2월 13일, http://it.chosun.com/news/article.html?no=2795759

29) 경찰청, "CCTV가 소리를 듣는다? 비명나면 알아차리는 '지능형 관제서비스'", 2013년 9월 26일, http://polinlove.tistory.com/6824

사업에서 통합관제센터와 함께 중요한 한 요소로 인식되고 있다.

관악구는 지난 2013년 6월부터 289대의 지능형 CCTV를 기반으로 '문제 차량 자동 검색 및 검거영치 시스템'을 구축해 운영하고 있다. CCTV 영상을 분석하여 인식된 차량번호를 경찰청 DB 및 세부 DB와 비교해 문제차량을 검출하고, 이를 업무처리자에게 실시간으로 통보하고 이동경로를 확인해 영치 및 검거를 하는 것이다. 이 CCTV는 250미터 앞에 있는 차량번호까지 정확하게 포착한다고 한다. 관악구는 2013년 6월부터 2014년 12월까지 과태료 차량 1만5127건, 자동차세 미납 차량 19만 8999건, 범죄 차량 8553건 등을 검거했다.[30]

한편, 경찰청은 과태료 미수납액의 과다 문제를 개선하기 위한 목적으로 2015년에 '차량번호자동판독기(AVNI)[31] 활용 체납차량 현장적발 시스템'을 구축하였다. 2015년 현재 7개 지방경찰청(서울, 부산, 대구, 인천, 경기, 충북, 전북)에 체납차량 현장 적발차량을 배치하고 있다.(국회예산정책처, 2016) AVNI는 차량번호를 자동으로 인식할 수 있는 장치이다. 나아가 경찰청은 전국 5,000여 개의 CCTV를 통해 특정 차량의 이동경로를 실시간으로 확인할 수 있는 '수배차량 검색시스템(WASS)'을 도입했다. 이 시스템은 CCTV의 차량번호를 인식하여 한 서버에 수집하고 검색한다.[32] 전자발찌를 훼손하고 달아난 성범죄자가 이 시스템을 통해 조기에 검거되기도 했다.[33] 그러나 기존의 범죄수배차량 검색시스템인

30) IT조선, "[재난망 컨퍼런스] 임동현 관악구청 주무관 "지능형 CCTV는 재난망 탑재 서비스로 손색 없을 것"", 2015년 2월 11일, http://it.chosun.com/news/article.html?no=2795691

31) AVNI, Automatic Vehicle Number Identification

32) MK뉴스, "전국CCTV 통합관리…경찰 '이글아이' 도입", 2015년 9월 15일, http://news.mk.co.kr/newsRead.php?year=2015&no=888906

33) MoneyS, "'전자발찌' 강경완 검거 일등공신 '수배차량검색시스템(WASS)'은 무엇?", 2016년 7월 21일, http://www.moneys.news/news/mwView.php?type=1&no=201607211457802

‘온라인조회시스템’과 WASS는 아직 자동연계 되고 있지 않다.[34]

앞서 관악구의 지능형 CCTV도 마찬가지이지만, AVNI는 차량번호를 인식하는 것이기는 하지만, 차량번호는 소유주의 개인정보와 연결되어 있다는 점에서 차량번호 역시 개인정보로 간주할 수 있다. 그런데 이와 같이 개인정보를 수집하는 경찰 시스템이 개인정보 수집에 대한 구체적인 법적 근거없이 도입되고 있는 것은 문제로 지적될 수 있다.

차량에 설치되는 영상정보 수집장치인 ‘블랙박스’ 역시 설치가 증가하고 있으며, 교통사고 조사뿐만 아니라 범죄 수사에도 활용되고 있다. 2015년 현재 블랙박스 설치 대수는 642만 6천여 대로 추정이 되고 있다.(한국정보화진흥원, 2016) 2014년부터 서울시 택시의 블랙박스 설치가 의무화되었고,[35] 구급차[36] 및 연안여객선[37]에도 블랙박스 설치가 의무화되었다. 차량 블랙박스가 범죄수사에 이용되면서, 지방자치 단체와 경찰도 범죄 발생 가능성이 높은 지역의 주민 차량에 블랙박스를 설치해 범죄 예방에 활용하고 있다.[38] 시민들이 자신의 블랙박스에 찍힌 교통질서 위반행위 등을 경찰에 신고하기도 한다.[39] 그러나 고정형의 CCTV가 그나마 「개인정

6380&outlink=1

34) 이뉴스투데이, “권은희 ‘경찰청 33억짜리 수배차량 검색시스템 무용지물’” 2016년 9월 29일, http://www.enewstoday.co.kr/news/articleView.html?idxno=610681

35) 민중의 소리, “서울시, 내년부터 택시 내 블랙박스 설치 의무화”, 2013년 7월 26일, http://www.vop.co.kr/A00000660517.html

36) 노컷뉴스, “구급차에 CCTV·블랙박스 의무화”, 2015년 4월 20일, http://www.nocutnews.co.kr/news/4401041

37) 국제신문, “500t 이상 연안여객선 블랙박스 설치 의무화”, 2014년 9월 11일, http://www.kookje.co.kr/news2011/asp/newsbody.asp?code=0200&key=20140912.22014200504

38) MBC, “블랙박스 450만 시대…범죄 예방 vs 사생활 침해 논란”, 2015년 6월 3일, http://imnews.imbc.com/replay/2015/nw1800/article/3710667_17808.html

39) 동양일보, “내 차안의 경찰관, 블랙박스!”, 2014년 9월 22일,

보 보호법」 제25조에 의해 규제되고 있는 반면, 이동형인 블랙박스의 경우에는 이를 규제할 근거가 없어 프라이버시 침해 위험성이 더욱 크다. 자신도 모르게 길거리의 CCTV 뿐만 아니라 차량의 블랙박스에 찍힐 수 있고, 이렇게 촬영된 정보가 인터넷에 올라갈 수도 있다.

최근 소형 무인 비행기인 '드론'이 대중적으로 보급되고 있는데, 향후 범죄수사용으로도 확대될 가능성이 크다. 이미 300미터 상공에서도 사람의 얼굴을 식별할 수 있는 드론이 개발되고 있다.[40]

(3) 영상정보 수집장치와 얼굴인식 기술의 결합

CCTV 등 영상정보 수집장치를 통해 수집된 영상이 얼굴인식 기술과 결합되면 범죄수사의 효율성을 획기적으로 높일 수 있지만, 무수하게 설치된 CCTV를 고려하면 자칫 <1984>에서 예견한 감시사회로 들어서는 것이 아닐까 하는 우려도 높아진다.

지난 2001년 1월 미국 플로리다주 탬파시 경찰은 미식축구 슈퍼볼 결승전이 열린 제임스 스타디움에 운집한 수만 명의 관중 속에서 지명수배자 19명을 찾아내 검거했는데, 이를 위해 얼굴인식 기술이 사용되었다. 경기장 출입구에서 비디오 카메라로 촬영한 관객들의 얼굴사진을 3,000명의 지명수배자 데이터베이스와 실시간 비교한 것이다. 미 법무부 이민국(INS)과 교정시설, 운전면허 발급기관, 카지노 등에서 활용되고 있는 비사지 테크놀로지(Viisage Technology)사의 얼굴인식 기술(FaceFinder)이 사용되었다.(구본권, 2014) 그러나 이 사건은 미국에서 자동 얼굴인식 기술의 프라이버시(불합리한 압수수색을 당하지 않을 권리)와 관련한 사회적 논란을 불러일으켰다. 이 시스템의 옹호자들은 공공 공간에서의 프라이버시는 기대할 수 없으며, 기존에도 경찰은 경기장에서 쌍안경 등으로 모니터링을 해

---

http://www.dynews.co.kr/news/articleView.html?idxno=226740

40) http://photohistory.tistory.com/15204

왔다는 것이다. 그러나 미국시민자유연맹(ACLU)이나 전자프라이버시정보센터(EPIC)와 같은 인권단체들은 카메라와 얼굴인식 시스템은 과거의 관행과는 다르다며, 이러한 관행이 허용된다면, 프라이버시를 보호받을 수 있는 곳은 집밖에 없을 것이라고 주장하고 있다.[41]

2013년 4월 보스턴 마라톤 대회에서의 폭탄테러범도 얼굴인식 기술을 통해 며칠 만에 검거되었다. 사고 현장 부근의 CCTV를 확보한 뒤, 얼굴인식 기술로 분석하고 용의자들을 압축해나가는 수사기법이 사용되었다.(구본권 2014) 국내에서도 단순 CCTV가 아니라 얼굴과 행동 패턴 등을 인식할 수 있는 지능형 CCTV가 도입되고 있다. 이미 국내 주요 공공기관과 출입보안이 강화된 특정구역에서는 보안 강화를 위해 얼굴인식 시스템이 공급되어 있으며, 2015년에 개최된 광주 하계유니버시아드대회에도 행사 출입 보안강화에 적용되었다.[42]

미국에서는 얼굴인식 시스템이 수사 목적으로 광범하게 사용되는 것으로 보인다. 그러나 남용을 방지하고 시민들의 프라이버시를 보호할 규제 체제는 미비한 상황이다. 2016년 10월 18일, 미국 조지타운대학교 로스쿨 산하 프라이버시기술센터는 1년여에 걸쳐 FBI와 지방, 주 경찰의 얼굴인식 시스템을 조사하여, <영구적인 라인업(The Perpetual Line-Up) - 미국에서 규제되지 않는 미국의 얼굴인식 시스템> 보고서를 발표하였다.[43] 이 보고서에 따르면, 1억 1,700만의 미국 성인들이 수사기관의 얼굴인식 시스템의 영향을 받은 것으로 나타났다. 그러나 이 시스템은 적절한 규제를 받지 않고 있었는데, 일부 기관은 기술의 남용을 방지할 보호장치를 갖추

41) Wired, “Call It Super Bowl Face Scan I”, 2001년 2월 2일, https://www.wired.com/2001/02/call-it-super-bowl-face-scan-i/

42) 디지털타임즈, “[발언대] 얼굴인식시스템 확산의 선결과제”, 2015.12.7

43) Center on Privacy&Technology at Georgetown Law, “The Perpetual Line-UP, Unregulated Police Face Recognition in America”, 2016.10.18, https://www.perpetuallineup.org/

고 있었지만, 그렇지 않은 경우가 더 많았다.

최소 26개주에서 수사기관은 운전면허증 사진 데이터베이스에서 얼굴인식 검색을 실행했다. 이런 방식으로 최소 둘 중 한명의 미국 시민들이 검색당했다. 연구팀은 기존 FBI의 지문이나 DNA 데이터베이스는 주로 범죄혐의자의 정보들로 이루어져 있었지만, 운전면허증 사진 데이터베이스의 검색은 주로 일반 시민을 포함하고 있다는 점에서 차이가 있으며, 전례가 없는 매우 문제가 많은 방식이라고 지적하고 있다.[44)]

시카고, 달라스, 로스엔젤레스 등 주요 경찰서에서는 감시 카메라에서 실시간 얼굴인식을 실행하고 있었다. 이는 거리를 걷고 있는 사람들의 얼굴을 지속적으로 스캔하는 것이다. 그러나 어떠한 주도 얼굴인식을 규제하는 포괄적인 법률을 가지고 있지 않았다. 이는 권한 남용으로 이어질 수 있는데 예를 들어, 피넬라스(Pinellas) 카운티 보안관의 시스템은 700만 플로리다 운전자를 대상으로 아무런 범죄 혐의 없이도 매월 3,000건의 검색을 한다.

얼굴인식은 지문인식보다 덜 정확하지만, 대부분의 경찰서는 정확도 테스트를 구매 조건으로 하지 않고 있었다. 또한, 식별 결과에 대한 판단은 주로 경찰관이 하는데, 대부분의 경찰서는 훈련된 담당 경찰관을 두지 않고 있었다. 이러한 문제에도 불구하고, 대부분의 수사기관들은 이 시스템에 대한 정보를 공개하지 않고 있어, 적절한 사회적 감독을 받지 않고 있었다. 또한, 이 보고서는 얼굴인식 기술이 더 어두운 피부색을 범죄자로 인식하는 경향이 있어 인종차별에 기반한 불균형을 나타내고 있다고 지적하고 있다.

미국 FBI는 1999년 7월부터 IAFIS 시스템을 운영해왔다. IAFIS 시스템

44) 한국에서도 집회 채증 사진 등을 근거로 집회 참가자에 대한 소환이 이루어지고 있는데, 이에 따라 한국의 경찰들도 얼굴인식 시스템을 이용하는 것은 아닌지에 대한 의문이 제기되고 있다. 그러나 경찰은 현재까지 경찰은 얼굴인식 시스템 이용을 부인하고 있으며, 수사관들의 육안 식별을 통해 판단한다고 답변하고 있다.

은 자동화된 지문검색, 전자적 이미지 저장, 지문정보의 전자적 교환, 텍스트기반 검색 기능 등을 제공하였다. 2010년 이후 IAFIS 시스템은 차세대식별시스템(Next Generation Identificatiion, NGI)으로 대체되고 있다. NGI는 세계에서 가장 큰 전자적인 생체인식 및 범죄기록 정보 데이터베이스를 제공한다.

NGI는 2011년 2월 첫 단계를 시작한 이후, 개선된 자동 지문검색 기능, 숨겨진 지문검색(latent search) 기능, 모바일 지문인식 기능, 전자적 이미지 저장 기능 등을 도입해왔으며, 18,000개 수사기관에 이 서비스를 제공하고 있다. 2013년 5월, FBI는 국가손바닥지문(장문)시스템(National Palm Print System, NPPS)을 구축하였다. 또한 FBI는 2013년 9월 홍채인식 시범서비스(Iris Pilot, IP)를 시작했다. 이를 통해 프라이버시 및 정책, 홍채 이미지 수집 지침, 홍채 카메라 요구사양, 홍채 이미지 압축 사양, 홍채 이미지 질적 지표 등을 개발해나갈 계획이다. 또한 생체인식 정보의 국가적 데이터베이스를 구축, 제공한다.[45] FBI는 2016년 현재 43만여 명의 피체포자 홍채인식 정보를 수집했다고 한다.[46]

2014년 9월 15일, FBI 형사정보서비스부(CJIS)는 NGI의 모든 기능을 완료했음을 공표하였다.[47] NGI는 두 가지의 새로운 서비스를 도입하였다. 그 하나는 랩백(Rap Back)으로서 특정인(예를 들어, 학교 교사와 같이 신원확인이 되어야 하는 직업을 가진 사람이나 보호관찰자)의 신원변

45) FBI, “Next Generation Identification (NGI)”, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi

46) The Verge, “The FBI has collected 430,000 iris scans in a so-called ‘pilot program’”, 2016년 7월 12일, http://www.theverge.com/2016/7/12/12148044/fbi-iris-pilot-program-ngi-biometric-database-aclu-privacy-act

47) FBI, “FBI Announces Full Operational Capability of the Next Generation Identification System”, 2014년 9월 15일, https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operational-capability-of-the-next-generation-identification-system

동 사항을 해당 기관에게 자동으로 알려주는 기능이다. 또 하나는 주간사진시스템(Interstate Photo System, IPS)인데, 이는 수사기관에 범죄자 신원과 관련된 사진 검색 기능을 제공한다. IPS는 얼굴인식 기능을 통해 수백만 범죄자 사진을 검색할 수 있도록 한다.

범죄자 얼굴인식 시스템은 한국의 수사기관도 이미 도입하고 있다. 지난 2014년 4월, 경찰청은 '3D 얼굴인식 및 3D 얼굴영상 변환 시스템 개발 사업' 입찰을 공고했다. 제안서에서 경찰청은 이 사업의 추진 배경으로 "CCTV 및 블랙박스 등 영상정보처리기기 설치 급증으로 이를 활용한 수사기법 필요성 증가"하고 있기 때문이라고 밝히고 있다. 기존에 경찰은 이미 구속피의자에 대해 2D 사진 자료를 구축하고 있었다. 그런데 이 자료는 정면 및 측면 얼굴만 존재하여 CCTV에서 획득된 범죄 용의자의 다양한 얼굴 각도에 대해서 얼굴인식 성능이 현저하게 낮은 문제점이 존재하였다. 이 때문에 경찰은 이번 사업을 통해 기존 2차원 얼굴 영상을 3차원으로 변환하여 데이터베이스화하고, CCTV 등의 영상에서 용의자 얼굴을 3차원으로 인식할 수 있는 시스템을 개발하여 이를 대조, 신원확인할 수 있는 시스템을 개발하고자 한 것이다.[48]

2015년에는 이를 개선하기 위해 '3D 얼굴인식 검색 및 변환 시스템 고도화' 사업을 발주하였다. 이 사업은 △ 3차원 얼굴인식 기술의 고도화, △ 기존 저해상도 얼굴 데이터 활용을 위한 얼굴 영상의 고해상도화 기술 개발, 얼굴의 일부 가림이 존재시 이를 자동으로 인식하여 용의자의 신원을 파악할 수 있는 기술에 대한 선행 개발(얼굴 특징점 세분화), △ 용의자의 연령대를 얼굴 정보를 통하여 자동으로 인식하는 기술을 적용하여 용의자 후보군 검색 범위 축소기술 개발, △ 1:1 및 N:1 얼굴 인식 결과의 법적 증거물 채택 수준의 객관성 확보를 위한 통계적 분석 (statistical analysis) 기반의 본인 검증 확률 도출 방법 개발, △ 특징점 위치 오류보정 수행

48) 경찰청, "3D 얼굴인식 및 3D 얼굴영상 변환 시스템 개발 사업 제안요청서", 2014년 3월, 나라장터 입찰공고번호 20140437312 - 00

및 3D DB 추가 변환, △ 3D 인식 시스템의 KICS[49] 연동 시 관련사건 및 인물 정보의 표출이 가능한 모듈 개발, △ 3차원 얼굴 모델링의 추가 (3D 얼굴 모델의 형태 및 텍스쳐 영상 품질 향상) 등을 목적으로 한다.[50]

이어 경찰청은 2016년에 6월에도 2차 고도화 사업을 발주하였는데, 이 사업은 △ 3차원 얼굴인식 기술에 대한 지속적인 개발, △ 저조도 얼굴 영상을 자동으로 보정하여 인식 정확도를 향상시키는 얼굴 영상 전처리 및 인식 기술에 대한 지속적인 개발, △ 3D수법영상 촬영장비에서 촬영된 3D 스캔 데이터를 3D 스캔 검색 DB로 추가 생성 등을 목적으로 하고 있다.[51]

이와 같은 얼굴인식 기능에 대한 지속적인 개선과 함께, 3D 얼굴사진 촬영장비를 구매하여 구속피의자의 영상을 3차원으로 촬영하여 보관하고 있다. 2016년 현재 경찰청은 서울, 인천, 경기 지역 15개 경찰서에 3D 촬영장비를 보급했다고 한다.[52] 경찰청의 제안서에 따르면, 3D 얼굴사진 촬영장비는 그림과 같이 구성된다.[53]

---

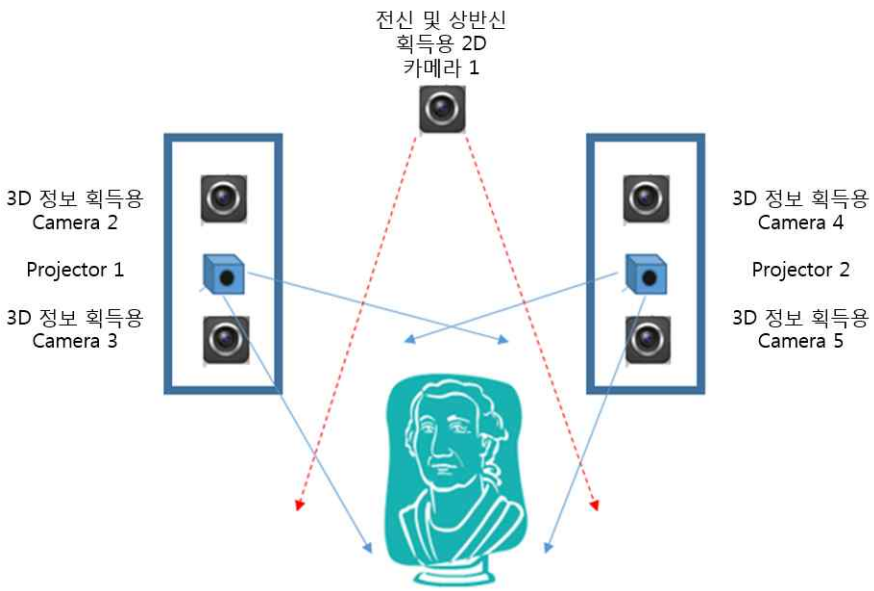
49) KICS(Korea Information system of Criminal-justice Services)는 형사사법 정보시스템으로 각 수사시스템의 관문역할을 수행하며, 수사지식공유, 범죄통계, 사건관리 기능으로 사용되고 있으며, 2011년 8월에 운영이 시작되었다.

50) 경찰청, “제안요청서, 3D 얼굴인식 검색 및 변환 시스템 고도화”, 2015년 3월, 나라장터 입찰공고번호 20150518934 - 00

51) 경찰청, “제안요청서, 3D 얼굴인식 시스템 고도화 2차”, 2016년 6월, 나라장터 입찰공고번호 20160603299 - 00

52) 서울신문, “3D 데이터로 성범죄·강도 재범 잡는 시대”, 2016년 8월 25일, http://www.seoul.co.kr/news/newsView.php?id=20160825009031

53) 경찰청, “제안요청서, 3D얼굴사진 촬영장비 구매 사업”, 2015년 3월, 나라장터 입찰공고번호 20151022774 - 00



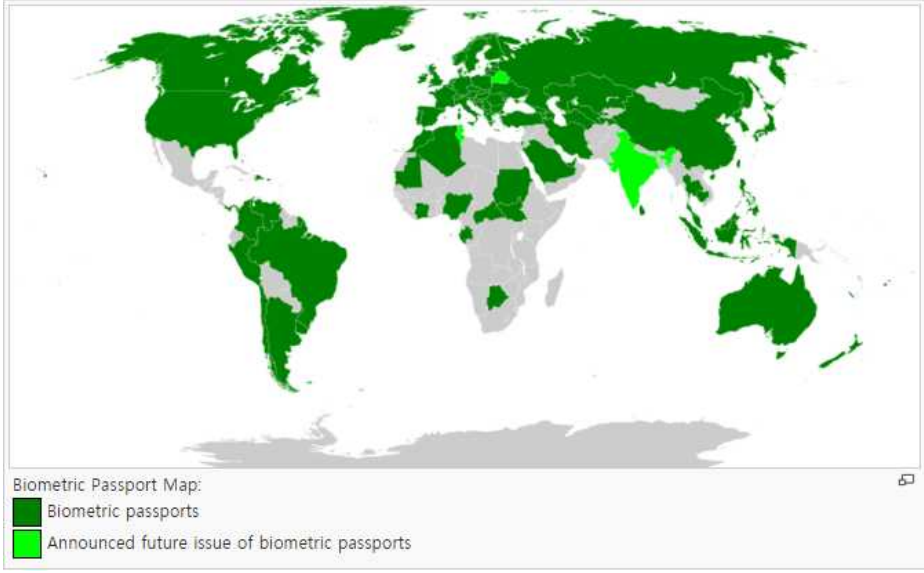
[그림 11] 3D 얼굴사진 촬영장비

여기서도 문제는 이와 같이 고도화된 생체인식 장치들이 구체적인 법률적 근거나 사회적인 검토없이 경찰청의 자체적인 판단만으로 도입된다는데 있다. 통상 수사기관에 의한 개인정보 수집은 경찰법 3조, 경찰관직무집행법 2조상 '치안정보의 수집, 작성 및 배포' 조항에 의해 정당화되는데, 기술발전으로 인해 심각해지는 프라이버시 침해의 위험성을 고려할 때 이것이 충분한지는 의문이다. 미국에서도 논란이 되었듯이, 수사기관이 과거에도 범죄 용의자의 지문, 얼굴 등 바이오 정보를 비롯한 개인정보를 수집해왔다고 하더라도, 첨단기술을 이용한 자동화된 수집, 데이터베이스의 구축, 자동화된 검색 기능 등을 고려할 때 개인에게 미치는 영향은 과거와 비할 바 없이 커졌기 때문이다.

다) 보안 및 출입통제

(1) 생체인식 전자여권

생체인식 기술은 오랫동안 건물 등 보안 및 출입통제 목적으로 활용되어 왔다. 국가간 이동을 통제하는 '출입국 관리'의 목적으로도 활용되고 있다. 특히 미국에서의 9·11 테러 이후 생체인식 전자여권이 도입되고 공항에서도 생체인식을 통한 출입국 수속 시스템이 추진되고 있다. 현재 세계 대부분의 국가에서 생체인식 전자여권을 도입하고 있다.[54]



[그림 12] 생체인식 전자여권 지도 (출처 : 위키피디아 "biometric passport")

생체인식 전자여권은 비접촉식 스마트카드 기술을 이용하는데, 여권 안에 칩이 내장되어 있다. 이 칩 안에 기본적인 여권 정보와 함께 디지털

54) 위키피디아, "Biometric passport", https://en.wikipedia.org/wiki/Biometric_passport (2016년 11월 1일 방문)

사진, 지문인식, 홍채인식 정보 등이 수록된다. 여권과 칩의 사양은 국제민간항공기구(International Civil Aviation Organization's, ICAO)의 표준 Doc 9303에서 규정하고 있다.

미국은 9·11 테러이후 「국경 보안과 비자 개혁 법안」(Enhanced Border Security and Visa Entry Reform Act)을 제정하였다. 이 법은 미국의 비자면제를 받는 국가들에게 생체인식 전자여권을 도입할 것을 의무화하였다. 미국의 비자면제 프로그램에 가입된 국가는 총 27개국으로, 대부분이 EU의 국가들이며, 일본, 싱가포르 등을 포함한다. 위 법이 제정된 후 이 국가들은 미국의 비자면제국가로 남기 위해 일제히 전자여권을 도입하기 시작했다. 애초에 미국은 2004년 10월 26일까지로 시한을 정했으나, 각국의 반발 및 국제 표준의 미확정 등으로 두 차례 도입시한이 연기되기도 했으며, 2006년 경에 생체인식 전자여권의 도입이 완료되었다.[55]

이러한 생체인식 전자여권의 확산을 우려하며, 2005년 9월, 개인정보 보호 및 프라이버시 커미셔너 27차 국제회의에서는 전자여권 사용에 대한 결의안이 채택되기도 했다. 결의안은 생체인식 기술의 위험성을 제한할 수 있는 안전장치가 마련되어야 하며, 법적으로 강제되는 생체인식 정보 수집과 동의에 기반한 수집이 구별되어야 하고, 전자여권의 생체인식 정보는 소지자의 신원 확인 용도로만 제한되어야 한다고 촉구했다.[56]

한국에서도 생체인식 전자여권 도입이 사회적 이슈가 되었다. 2007년 2월 외교통상부는 전자여권 도입을 위한 공청회를 개최하고 이어 여권법 개정안을 발의하였다. 인권단체들은 개인정보 유출 가능성과 프라이버시 침

55) 진보네트워크센터, "[보도자료] 미국이 정한 도입시한에 맞춰 도입된 세계 각국의 생체여권(전자여권)", 2007년 9월 10일, http://act.jinbo.net/wp/3523/

56) 27th International Conference of Data Protection and Privacy Commissioners, "Resolution on the use of biometrics in passports, identity cards and travel documents", 2005년 9월 16일, http://privacyconference2011.org/htmls/adoptedResolutions/2005_Montreux/2005_M4.pdf

해 문제를 제기하며 이에 반대하였지만, 정부는 미국과 비자면제협정을 이유로 전자여권 도입을 강행하였다. 2008년 2월 국회는 논란 끝에 지문수록을 2년 유예하는 내용으로 여권법을 개정하였다. 그러나 2009년, 국회는 전자여권에서 민감한 생체인식 정보인 지문을 삭제하기로 하고 다만 여권발급 과정에서 본인 여부를 확인하기 위한 목적으로 지문정보를 수집했다가 3개월 후 삭제하는 내용으로 여권법을 개정하였다.[57]

(2) 출입국 관리

미국 국토안보부는 출입국 통제를 위해 생체인식 정보를 포함하는 몇 개의 프로그램을 운영해 왔다. 미국방문자및이민자신분표시기술(The United States Visitor and Immigrant Status Indicator Technology, US-VISIT)은 미국을 방문하는 외국인의 개인 정보를 수집하고 국경에서의 여행자 통제를 위한 국토안보부의 프로그램으로, 지문과 디지털 사진을 포함한 생체인식 정보를 수집한다. 처음에는 입국을 위해 비자가 필요한 방문자에게만 적용되었지만, 2004년 9월 이후 미국 비자면제국의 여행자들에게도 적용되었다. 2009년 1월부터 미국 시민이 아닌 모든 사람들을 대상으로 확대되었다.[58] US-VISIT은 2013년 3월에 생체인식 신원관리소(Office of Biometric Identity Management, OBIM)로 대체되었다. OBIM은 연방, 주, 지역 정부기관의 위험인물에 대한 정확한 판단을 돕기 위해 생체인식 정보를 수집, 분석하고, 주요 감시대상에 대한 목록을 관리한다.[59] NEXUS는 미국과 캐나다 사이의 여행자를 대상으로 한 프로그램으로 항공, 바다, 육지를 통한 이동에 모두 적용된다. 미국과 캐나다의 시민과 영주권자를 대상으로 하는데 강제적인 것은 아니며, 사전에 등록한

57) 진보네트워크센터, 지문수록 백지화 여권법 개정안 수정가결에 대한 진보네트워크센터 논평, 2009년 4월 24일, http://act.jinbo.net/wp/3862/

58) EPIC, “US-VISIT”, https://epic.org/privacy/us-visit/

59) https://www.dhs.gov/obim

사람들을 대상으로 보다 빠른 출입국 심사절차를 제공한다. 여행자가 RFID 방식의 회원 카드를 제시하고, 생체인증을 위해 자신의 홍채 정보를 제공하게 된다.[60]

한국은 자동출입국심사(Smart Entry Service) 시스템을 운영하고 있다. 자발적으로 희망하는 사람을 대상으로 하며, 희망자는 여권 및 지문, 얼굴 등 생체인식 정보를 사전에 등록해야 한다. 홍콩의 e-Gate, 네덜란드의 Privium, 미국의 Global Entry, 호주의 Smart Gate 등 40여 개국에서 자동출입국심사대를 이용한 출입국심사를 실시하고 있다고 한다.[61] 미국, 영국, 캐나다, 호주, 독일, 두바이 등은 공항 출입국 관리를 위해 홍채인식 기술을 활용하고 있다.[62]

(3) 출입통제 및 근태관리용 생체인식 장치

생체인식 장치는 일반 가정의 도어락에서부터 보안시설의 출입통제, 그리고 출퇴근 확인 및 근태관리용도로까지 광범하게 보급되어 있다. 특히 저렴한 지문인식기가 가장 많이 보급되어 있는데, 지문인식 도어락이나 출퇴근용 지문인식기의 경우 10만 원대 제품부터 수십만 원대까지 일반 쇼핑몰에서도 판매되고 있다.

60) http://www.biometrics.gov/referenceroom/federalprograms.aspx

61) http://www.ses.go.kr/

62) 주간조선, “금융부터 건강관리까지 홍채 인식 기술이 바꾸는 세상”, 2420호, 2016년 8월 15일

[그림 13] 시중에 판매되는 지문인식 도어락 사례

출퇴근용 지문인식기는 기존의 출퇴근 카드를 대체하거나 병행해서 일반 업체, 공공기관, 학교, 사회복지시설[63] 등에 설치되고 있는데, 근태관리 및 초과근무수당의 부당수급을 방지하기 위한 목적으로 활용되고 있다. 생체인식 기기의 정확한 설치 현황은 파악된 것이 없지만, 2013년도 국가인권위원회 인권상황실태조사 연구용역으로 만들어진 <정보통신기기에 의한 노동인권 침해 실태조사> 보고서에 따르면, 직장에 도입된 정보통신 기기 중 '지문 및 생체인식' 기기가 2005년 8.6%에서 2013년 23.8%로 크게 증가하였다.[64]

---

63) 연합뉴스, "사회복지시설에 지문인식기…'투명성↑' vs '인권침해'", 2016년 3월 7일, http://www.yonhapnews.co.kr/bulletin/2016/03/07/0200000000AKR20160307158200065.HTML?input=1195m

64) 한국법제연구원, "정보통신기기에 의한 노동인권 침해 실태조사", 2013년도

이미 2005년에 여러 공공기관, 기업체, 은행에서 근태관리 및 출입통제용으로 정맥인식기를 설치하고 있다는 것이 기사화된 바 있다.[65] 2015년 광주시의 경우 본청과 사업소에 지문인식기 65개가 설치돼 설치율은 100%에 달한다고 하며, 광주경찰청은 본청에 홍채인식기를 설치해 초과근무 현황을 기록하고 있다. 일선 5개 경찰서에는 지문인식기가 모두 설치돼 사실상 100%에 달하는 것으로 나타났다.[66]

한 홍채인식기 업체는 적용 사례로 세계무역센터에 출입하는 3000명 이상의 건설노동자들의 신원 인증, 캐나다 전역 29개 공항에 설치되어 직원 20만 명의 홍채 등록, 바이오 연구소 보안, 십자형 회전 및 일반 회전문에서의 직원과 방문객 인식, 휘트니스 클럽에서의 회원 인식, 교도소에서의 수감자 식별, 국제공항에서의 보안구역 통제, 호텔에서 VIP 고객과 직원을 위한 보안, 보안시설 내 보안키 접근 통제, 데이터센터 사용자 보안 등의 사례를 제시하고 있다.[67]

국가인권위원회 인권상황실태조사 연구용역보고서, 2013년 12월 21일, p63

65) 한겨레, "'정맥인식기' 근태관리 논란", 2005년 3월 10일, http://www.hani.co.kr/arti/17022.html

66) 광남일보, "광주지역 학교 지문인식기 설치율 29%", 2015년 4월 5일, http://www.gwangnam.co.kr/read.php3?aid=1428225330208003018

67) http://www.irisid.co.kr/productssolutions/irisaccessinaction/

[그림 14] 시중에 판매되고 있는 출퇴근 지문인식기 사례

[그림 15] 시중에 판매되는 홍채인식기 사례

생체인식 기기가 우리 사회에 얼마나 보급되어 있는지에 대한 통계는 없지만, 생체인식 보안산업의 현황을 보면 대략 그 규모를 짐작할 수 있을 것이다. 물리보안산업 중 생체인식 산업의 매출 현황은 다음과 같다.

[표 4] 물리보안산업 중 생체인식 시스템 매출 현황

(출처 : 한국정보보호산업협회, 2015)(단위: 100만원, %)

분류	2013년	2014년	2015년	증감률(%)
얼굴인식시스템	56,086	53,299	57,299	7.5
지문인식시스템	98,983	106,765	112,564	5.4
홍채인식시스템	1,163	2,529	2,687	6.2
정맥인식시스템	5,863	5,783	6,293	8.8
기타 (음성인식 및 기타)	10,336	6,151	7,276	18.3
총계	172,431	174,527	186,119	6.6

그러나 이와 같은 생체인식 기기를 구성원들의 동의도 없이 설치하고 지문날인 등 생체인식 정보 제공을 강요하여 종종 논란이 되고 있는데, 이미 2000년대 중반부터 이러한 갈등이 발생하였다. 2005년 서울대에서 기숙사에 정맥인식기를 설치하여 학생들이 국가인권위원회에 진정서를 제출한 바 있으며[68], 연세대, 공주대, 충남대 등에서 대학 도서관에 지문인식기를 설치하여 인권침해 논란이 일기도 했다. 국가인권위원회는 중앙도서관에서 열람실 좌석 이용시 학생들의 지문 인식 시스템을 설치, 운영하고 있는 것은 사생활의 비밀과 자유를 침해할 우려가 높다며, 총장과 교육인적자원부 장관에게 개인정보 보호에 필요한 조치를 취할 것을 권고한 바 있

68) 한겨레, “서울대 기숙사에 정맥인식기, 학생들 “인권침해다” 진정서”, 2005년 8월 9일

다. (2005. 7. 25.자 04진인3372 결정) 같은 해 전라북도 중고등학교의 급식시설에 지문인식기를 설치해 지역 시민단체와 전교조가 이에 반발하였고, 국가인권위원회는 이에 대해서도 인권침해라고 판단하였다.[69] 2007년에도 경기도 학교의 교사들이 지문등록 강요에 반발하였다.[70] 한편, 2016년, 법원은 출퇴근 지문인식을 거부한 교수에 대한 징계가 부당하다고 결정하였다.[71]

구성원들의 동의없이 생체인식 기기가 도입되는 것도 문제지만, 설사 동의가 있더라도 충분히 자발적인 동의가 될 수 있는지는 의문이다. 생체인식 기기를 도입하는 기관(기업)과 자신의 생체인식 정보를 제공해야 하는 구성원(노동자)의 관계가 권력의 불균형이 있을 수밖에 없기 때문이다. 이 때문에 어쩔 수 없이 자신의 생체인식 정보를 제공해야 하는 사람들은 이를 '감시'로 인식하게 된다. 2013년 국가인권위원회의 '스마트 기기에 의한 노동감시 관련 위원회 진정 및 상담 사례 통계분석' 자료에 따르면, 전자감시 기구를 활용한 노동감시 사례에서 생체인식 정보를 통한 감시가 77건, 10.8%로 나타났다.[72]

2012년 6월 14일, 국가인권위원회는 공익근무 요원에게 출퇴근용 카드

---

69) 오마이뉴스, "도둑밥 먹는 학생 잡으려고 지문인식기 설치?", 2005년 4월 12일, http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?cntn_cd=A0000248585 관련하여, 국가인권위원회는 "각급 학교에서 급식과 관련하여 학생식당에 지문인식기를 설치한 것은 인권침해라고 판단하여 피진정인에게 이의 방지를 위해서 각급 학교에 대한 지도와 관리감독을 철저히 할 것과 피진정인의 감독기관의 장인 교육인적자원부 장관에게 유사 사례의 방지를 위해 계속적으로 관리 조치할 것"을 권고한 바 있다. (2005. 8. 31.자 05진인1055 결정)

70) 오마이뉴스, "경기도 학교들, 교사 지문 등록 강요 '논란'", 2007년 4월 9일, http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0000403178

71) KBS, "법원 "출퇴근 지문인식 기록 거부한 교수 징계 부당"", 2016년 4월 14일. http://news.kbs.co.kr/news/view.do?ncd=3263958&ref=A

72) 참세상, 전자 노동감시, 10년 새 50배 이상 증가, 2013년 3월 5일, http://www.newscham.net/news/view.php?board=news&nid=69543

발급 및 재발급 시 비용이 많이 들고 복무 관리가 편리하다는 이유로 출퇴근용 카드발급시스템 대신에 지문등록시스템을 도입하여 지문을 찍도록 강요한 사안에 대해서 지문 정보는 개별식별 정보이자 민감정보에 해당하여 개인정보자기결정권을 침해할 수 있으며, 침해의 최소성 및 법익의 균형성에 어긋나 과잉금지 원칙에 위반될 뿐만 아니라 이를 시행할 법률상의 근거가 미비하여 법률유보 원칙을 위반할 소지가 있다고 결정하였다.

그 이전 2007년에도 국가인권위원회는 CCTV와 생체인식 기기를 포함한 사업장 내 전자감시 시스템의 설치, 이용에 관하여 근로자의 인권을 보호하기 위한 법령 및 제도를 개선할 것을 권고하였다.[73] 관련하여 근로자의 최소한의 보호 장치로서, △ 사용자가 전자감시 이외에는 다른 방법을 찾을 수 없다는 불가피성을 사전에 객관적인 방법으로 제시하도록 할 것, △ 전자감시의 상세 내용에 대한 공개, △ 근로자들의 참여와 평가 보장, △ 사전 설명과 교육을 전제로 한 근로자의 동의 등을 제시했는데, 현재 도입되고 있는 생체인식 기기와 관련하여 이러한 절차들이 제대로 준수되고 있는지 의문이다.

라) 컴퓨터 및 스마트폰 인증, 보안

최근 스마트폰에 지문, 홍채, 얼굴 인식 등 다양한 생체인식 기술이 도입되고 있다. 스마트폰의 생체인식 기술은 스마트폰 자체의 보안뿐만 아니라, 온라인 결제를 위한 인증 시스템으로도 활용될 수 있다. 스마트폰은 카메라, 마이크, 지문센서, 중력센서, 터치패드 등 다양한 종류의 생체인식 기술을 탑재하고 있어 다양한 용도로 활용될 수 있다. 그러나 개인 전용 기기로서의 스마트폰이 이미 수많은 민감한 개인정보를 담고 있는 상황에서, 위치정보와 생체인식 정보 등 민감한 정보들을 더 많이 다루게 될수록 스마트폰 해킹으로 인한 프라이버시 침해 위험은 더욱 커질 수 있다.

---

73) 국가인권위원회, “사업장 전자감시에서 근로자의 인권보호를 위한 법령·제도 개선권고”, 2007년 11월 12일

스마트폰에 먼저 도입된 생체인식 기술은 지문인식이다. 최초로 지문인식 기능을 탑재한 스마트폰은 2011년 4월에 출시된 모토롤라사의 아트릭스다. 이후 2013년 9월, 애플은 지문인식 기술인 터치 ID(Touch ID)를 내장한 아이폰 5s를 출시하였다. 애플의 터치 ID는 2012년에 지문센서 전문업체인 어센테크(AuthenTech)를 인수하면서 거둬들인 기술이다. 애플의 지문인식 방식은 단순히 센서에 손가락을 대면 인식이 되는 에어리어(Area) 방식이다. 그리고 터치 ID에 등록된 사용자 지문은 이미지 파일이 아닌 암호화된 데이터로 특별히 보안 영역에 저장되고 다른 동작과 별도로 관리되기 때문에 해킹이나 탈옥으로 관리자 권한을 얻는다고 해도 쉽게 정보를 빼낼 수 없고 암호 해독이 불가능하다고 한다. 삼성전자는 2014년 2월 출시한 갤럭시 S5에서부터 지문인식 기술을 도입했다. 삼성은 지문인식 기술인 패스(Pass)를 통해 잠금 화면 해지, 갤러리 내 사진 보호 등을 설정할 수 있다. 갤럭시 S5는 손가락을 위에서 아래로 문질러 지문을 스캔하는 스와이프(Swipe) 방식을 사용하고 있다. 이후 애플은 2014년 10월에 출시된 아이폰6와 아이폰6+에도 지문 영역을 넓히고 스캔 해상도를 개선한 에어리어(Area) 방식의 센서를 적용했으며, 삼성전자도 갤럭시S6와 갤럭시S6엣지 모델에는 기존 스와이프(Swipe) 방식이 아닌 에어리어(Area) 방식을 선택했다.(송초롱 등, 2015)

아이폰 5s의 지문인식　　홈버튼에 내장된 터치 ID

[그림 16] 아이폰 터치 ID (출처 : IT World)

그러나 아이폰 5s와 삼성전자의 갤럭시 S5 모두 치명적인 보안상 결함을 노출했다. 아이폰 5s의 경우 손가락을 갖다대는 방향에 따라, 날씨와 조건에 따라 인식에 실패하는 경우가 발생하였으며, 특히 고해상도로 촬영해 이를 인쇄한 지문으로도 터치 ID 인식시스템을 작동시킬 수 있는, 치명적인 보안상 결함이 발생했다. 갤럭시 S5 역시 아이폰 5s와 같은 방식으로 지문인식 기능이 뚫렸다.(IT world, 2015)

얼굴 인식 기능은 삼성전자의 '갤럭시 넥서스'에서 처음 도입되었는데 이는 2011년 10월 구글이 발표한 안드로이드 4.0(아이스크림 샌드위치)를 채택한 것으로, 안면인식 기술을 통한 잠금 해제 기술인 페이스 언락(Face Unlock) 기능을 포함하고 있다. 기존에 등록한 본인 얼굴을 복합적으로 인식, 저장해서 잠금을 풀 때의 모습을 비교하여 일치 여부를 가려낸다. 그러나 이 역시 소유자가 아닌 사람이 소유자의 사진으로 잠금을 해제할 수 있는 등 보안에 문제를 드러냈다. 애플 역시 얼굴 인식 기능을 준비 중인데, 2010년 스웨덴 얼굴 인식 업체인 폴라로즈를 인수한 데 이어, 2013년에는 이스라엘 3차원(3D) 영상 인식 센서 제조사인 프라임센스를 인수하였다.(송초롱 등, 2015)

2016년 8월 출시된 삼성전자의 '갤럭시 노트7'은 홍채인식 기능을 탑재해 출시 전부터 관심을 모았다. 갤럭시 노트7은 기기 상단에 홍채 인식 전용 카메라와 적외선(IR) LED가 탑재돼 사용자의 홍채를 인식한다. 홍채 인식 정보는 디지털 정보로 바뀌어 암호화되는데, 암호화된 정보는 녹스 보안 영역 트러스트존에 저장된다.[74] 그러나 갤럭시 노트7은 잇따른 배터리 발화 사고로 사회적인 우려를 야기했으며 결국 2016년 10월 단종이 결정되었다.

74) 데일리그리드, "'갤럭시노트7' 홍채인식, 원리가 뭐야? "개발자 그건 바로…"", 2016.10.5 http://www.dailygrid.net/news/articleView.html?idxno=43021

마) 금융

금융 분야는 자칫하면 커다란 재산적 손실을 야기할 수 있기 때문에 엄격한 본인 인증이 요구되어 왔다. 특히 최근 모바일 금융거래가 증가하고 핀테크가 활성화되면서 금융분야에서 비대면 거래가 증가하고 있다. 현재 아이디와 패스워드, 공인인증서, 보안카드, ARS(자동응답전화) 본인확인 등 비대면 거래를 위한 복잡한 인증 시스템이 활용되고 있다. 생체인식 기술은 별도의 보관이나 암기가 불필요하고 도용이나 양도가 불가능하다는 점에서 기존의 비대면 인증수단을 보완하거나 대체할 수 있는 수단으로 주목 받고 있다.

생체인식 기술의 도입과 별개로 금융기관은 이용자의 지문 정보를 관행적으로 수집해왔다. 금융실명제에 따라 은행에서 계좌를 개설할 때 신분증으로 본인확인을 하게 되는데, 금융기관은 관행적으로 신분증의 앞면과 뒷면을 복사하거나 스캔하여 파일로 이를 저장해온 것이다. 그러나 지난 2014년 10월, 국가인권위원회는 이는 이용자의 개인정보자기결정권을 침해하는 행위라며, 금융위원회와 방송통신위원회에 금융기관과 통신사가 본인확인을 위해 수집해온 지문 정보를 모두 파기하도록 지도하고, 안전행정부 장관에게도 본인확인을 위하여 주민등록증에 수록된 지문 정보를 수집 이용하지 않도록 「주민등록법」제25조 등 관련 법령을 개선할 것을 권고하였다.[75]

국내 금융 영역에서 생체인식 기술이 처음 도입된 것은 2001년 우리은행이 ATM기기에 지문인식 기술을 도입하면서 부터이다. 그러나, 단말기 보급, 이용 가능한 단말기 제한, 생체인식 기술의 정확성, 저조한 고객 이용률 등의 문제로 인하여 금융시장에서 생체인식 기술이 널리 활용되지는 못하였다(이재득, 2014).

최근 금융 영역에서 생체인식 기술이 주목받고 있는 배경에는 모바일 결제 등 핀테크 활성화와 비대면 거래의 증가가 있다. 2014년 전체 온라인 쇼핑 거래액은 45조 2천 440억 원으로, 이중 모바일 쇼핑이 32.7%(14조 8

75) 국가인권위원회, “본인확인을 위한 신분증 사본 저장에 따른 지문정보 수집에 대한 제도 개선 권고”, 2014년 10월 22일

천 90억 원)를 차지했다. 또한 금융서비스 전달 체계도 비대면거래가 88.7%(2014년)로 계속 증가 추세에 있다.(장상수, 2015) 이와 함께, 그동안 온라인 뱅킹의 주된 인증 수단으로 사용되어온 공인인증서가 Active-X 등의 사용에 의해 인터넷 익스플로러라는 특정한 브라우저에서만 작동되고 이용에 불편을 초래하는 것에 대한 사회적인 불만이 증가되면서 보다 간편하면서도 안전한 대체 인증에 대한 요구도 높아졌다.

2015년 5월, 금융위원회는 '실명확인방식 합리화 방안'을 발표하였는데, 이에 따르면 '①신분증 사본 제시 ②영상통화 ③현금카드 등 전달 시 확인 ④기존 계좌 활용 방식 중 2가지 방법으로 중복 확인'하도록 하였으며, 이와 함께 금융회사가 '이에 준하는 새로운 방식'을 개발, 사용하는 것도 허용하였다.[76] 그리고 2015년 12월, 금융위원회는 「금융실명법」·「전자금융거래법」에 따른 실명확인을 '복수의 비대면 방식'으로 수행할 수 있도록 허용하는 유권해석을 내렸다. 생체인증은 '이에 준하는 새로운 방식'에 포함되어 비대면 방식의 하나로 활용될 수 있게 되었다. 신한은행은 국내 최초로 비대면 방식을 적용한 계좌개설 업무를 시작하였으며, 생체인증 등 비대면 실명확인을 거쳐 대면창구 업무의 상당부분을 대체하는 무인(無人) '스마트점포(디지털 키오스크)'를 출시하였다.[77]

금융영역에서 초기에는 금고나 전산실 등의 출입통제 목적으로 생체인식 기술을 활용해 왔지만, 현재는 ATM, 텔레뱅킹, 오프라인 결제, 모바일 뱅킹 등 다양한 금융서비스에서 활용되고 있다. 생체인식 기술 적용 비율이 가장 높은 분야는 ATM인데, 지문 및 정맥 인식 기술이 활용되고 있다. 특히, 일본에서는 카드나 통장을 대신해 손바닥 정맥을 이용해 현금 인출과 송금이 가능하도록 설계된 ATM이 약 8만대 운영 중인 것으로 알려져 있

76) 금융위원회 보도자료, 이제 집이나 직장에서 은행·증권사 계좌를 열 수 있습니다, 2015.5.18

77) 금융위원회 보도자료, 임종룡 금융위원장, 국내 제1호 비대면 실명확인 통장 발급. 2015.12.2

다. 이는 지진이나 쓰나미 등 자연 재해가 발생하여 카드나 통장을 잃어버려도 은행 사용을 가능하게 하기 위한 것이다.[78] 텔레뱅킹 서비스에는 특성상 음성인식 기술이 사용된다. 해외 은행들은 음성인식 기술을 고객센터 본인인증, 텔레뱅킹 PIN번호, 패스워드 대체용으로 사용하고 있다.

오프라인 결제시장에서는 지문, 얼굴, 정맥인식 등 다양한 생체인식 기술이 활용되고 있는데, 주로 비금융기관 신생 스타트업 기업들을 중심으로 출시되고 있다. 이들은 결제절차의 간소화, 결제대기시간 단축 등 사용자 편의성을 가장 큰 장점으로 내세우고 있다.

최근 스마트폰을 통한 모바일 쇼핑이 증가하면서 향후에는 모바일 결제 중심으로 이동할 가능성이 크다. 지문인식 기술이 현재 가장 많이 사용되지만, 음성, 얼굴, 홍채인식 등을 통한 모바일 결제 서비스도 출시되고 있다. 스마트폰은 카메라, 마이크, 지문센서, 중력센서 등 다양한 생체인식 센서를 이미 탑재하고 있기 때문에, 모바일 결제서비스와의 결합이 용이하다. 애플은 2013년 아이폰5s에 터치ID라는 지문인식 기술을 탑재하고 아이튠즈 앱스토어에서 앱을 구매하거나 다운받을 때 지문인식으로 비밀번호 입력을 대체한 바 있다. 삼성전자도 2014년 2월 자사의 스마트폰 갤럭시S5에 지문인식 기술을 탑재하면서 국내에서는 삼성월렛, 해외에서는 Paypal과 각각 연동한 서비스를 출시하였다(이재득, 2014).

최근 셀카로 본인인증 여부를 확인하는 기술도 도입되고 있다. 마스터카드는 2016년 10월, 유럽에서 얼굴 인식 기술을 탑재한 '아이덴티티 체크 모바일(Identity Check Mobile)'이라는 앱을 출시했다. 이 앱은 이용자가 온라인에서 신용카드로 결제할 때 스마트폰 화면을 응시하면 이를 설정 단계에서 저장한 사진과 비교해 본인 여부를 확인한다. 2016년 9월 HSBC는 얼굴인식 기술을 이용해 온라인으로 계좌를 개설할 수 있도록 했는데, 이용자가 셀카를 찍으면 이를 운전면허증이나 신분증 사진과 비교해 비대

78) the 300, 한번 털리면 대체 불가…'몸키(key) 보호법' 눈뜨나, 2016.9.8, http://the300.mt.co.kr/newsView.html?no=2016090714307631057

면으로 계좌를 개설해주는 방식이다.[79]

국내외 주요 생체인식 기술 도입 사례는 아래 표와 같다.

[표5] 해외 주요 금융기관 생체인식 기술 도입 사례 (출처 : 김동진, 2016)

국가	기업명	도입내용	비고
미국	Bank of America	모바일뱅킹 인증을 위해 지문인증 도입	
	J.P. Morgan	서비스 로그인 시 인증을 위해 지문인증 도입	
	Citi group	신용카드 고객 인증을 위해 음성인증 도입	
	USAA	스마트뱅킹 인증을 위해 얼굴 및 음성, 애플의 지문 (Touch ID) 도입	
	Wells Fargo	자사 고객 인증을 위해, 안구인식 및 다중 바이오인증(얼굴 및 행동적 특징) 기술 도입	
	다수 금융사	구글 Abacus 프로젝트 Trust API를 통한 다수의 행동적 특징을 활용한 인증방식 내부 테스팅	테스트중
	MasterCard	결제 시스템에 Nymi 사의 스마트 밴드를 활용한 심전도 인증 기술 도입	테스트중
캐나다	RBC		
	Tangerine	스마트뱅킹 인증을 위해 얼굴, 지문 및 음성 인증 도입	

79) IT조선, "'셀카'로 본인 여부 확인하는 얼굴 인식 기술 도입 확산", 2016년 10월 18일, http://it.chosun.com/news/article.html?no=2825317

영국	Halifax (Lloyds Banking Group)	자사 전자금융서비스를 위한 심장박동 인증 기술 도입	시범운영
	Barclays	Hitachi 사의 손가락 정맥 인증 기술 도입	
	HSBC	스마트뱅킹 인증을 위해 음성 및 지문(Touch ID) 인증 도입	
러시아	Sberbank	ATM에서 사용 가능한 모든 거래에 음성인증 도입	
	Itautec	지점 ATM 거래에 지문인증 도입	
스코틀랜드	RBS	스마트뱅킹에 지문(Touch ID)인증 도입	
볼리비아	BBVA Prevision AFP	연금 수령 위한 얼굴인증 시스템 도입	개발중
핀란드	Uniqul	얼굴인증 기반 결제 시스템 개발	
호주	St George Bank	스마트뱅킹 인증 위한 지문인증 도입	
	National Australia Bank	폰뱅킹 및 ATM 인증을 위해 음성인증 도입	
중국	Alibaba	자사 온라인 쇼핑몰 결제 시 얼굴인증(스마일 투 페이) 도입	
일본	NTT Docomo	스마트폰 기반 간편결제를 위한 홍채인증 도입	
	Japan Post Bank	ATM 이용시 인증을 위해 손가락 및 손바닥 정맥인증 도입	
	Mega Bank		
	Trust Bank		
	Regional Bank		
	Local Bank		

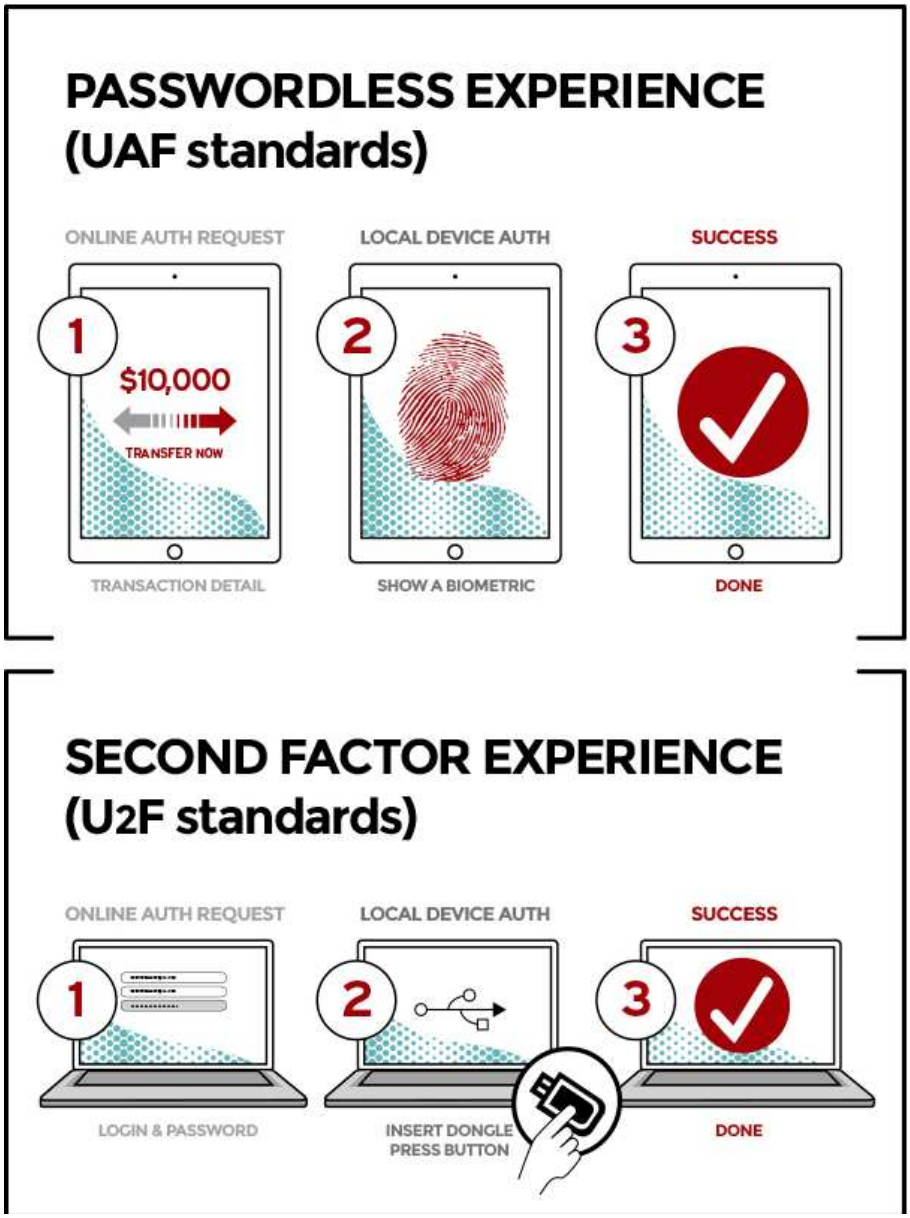
[표6] 국내 주요 금융기관 생체인식 기술 도입 사례 (출처 : 김동진, 2016)

<table>
<tr><th>기업명</th><th>도입내용</th><th>도입시기</th></tr>
<tr><td>NH농협은행</td><td>키오스크를 통한 셀프뱅킹시스템에 후지쯔 사의 손바닥 정맥 인증 방식 도입</td><td>2015년</td></tr>
<tr><td>NH손해보험</td><td>스마트뱅킹 이용 시 본인인증을 위해 지문인증 방식 도입</td><td>2016년</td></tr>
<tr><td>주요카드사</td><td>직원의 PC 접근제어용으로 지문인증 방식 도입</td><td></td></tr>
<tr><td>하나카드</td><td>삼성페이 등 바이오인증 기술이 적용된 간편결제 플랫폼을 통해
간접적으로 지문인증 등 도입</td><td>2015년</td></tr>
<tr><td>롯데카드</td><td>간편결제 시스템인 모비페이에 지문인증 방식 도입</td><td>2016년</td></tr>
<tr><td>쿠팡 로켓페이</td><td rowspan="4">스마트폰 간편결제 인증을 위해 지문인증 도입
※ 로켓페이, 네이버페이는 현재 TouchID 지원 애플 단말만 지원</td><td>2016년</td></tr>
<tr><td>11번가 시럽페이</td><td>2016년</td></tr>
<tr><td>네이버페이</td><td>2015년</td></tr>
<tr><td>페이코</td><td>도입검토</td></tr>
<tr><td>토스</td><td>간편송금시 인증을 위해 지문인증 도입
※ 현재 TouchID지원 애플 단말만 지원하며, 확대예정</td><td>2016년</td></tr>
</table>

생체인식 인증이 자리잡기 위해 중요한 요소 중 하나는 표준화인데, 현재 FIDO(Fast IDentity Online) 얼라이언스[80]가 이를 주도하고 있다.

80) FIDO 얼라이언스는 생체인식 기술을 활용한 인증방식에 대한 개방형 기술 표준을 정하기 위해 2012년 7월 설립되었으며, 구글, 녹녹랩스, 디스커버파이낸셜 서비스, 레노버, 마스터카드, 마이크로소프트, 뱅크오브아메리카, 블랙베리, 알리바바, 오버추어테크놀로지, 페이팔 등이 주도하고 있다. 국내 업체로는 삼성전자, LG전자, SK텔레콤, 크루셜텍 등 190여 개 업체가 참여하고 있다.(ITworld, 2014) https://fidoalliance.org

FIDO 얼라이언스는 비(非) 비밀번호 인증 표준인 UAF(Universal Authentication Framework)와 이중인증 표준인 U2F(Universal 2nd Factor), 두 개의 인증 표준을 갖고 있다. FIDO 인증의 특징은 생체인식 정보가 이용자의 단말기에 저장되며, 인증절차 역시 단말기 내에서 이루어진다. 이용자의 단말기에서 서비스 제공회사 서버로는 생체인식 정보가 아니라 개인키로 암호화된 본인인증 정보가 전송되며, 서비스 제공회사는 해당 개인키와 매핑되는 공개키로 복호화하는 과정을 통하여 본인인증 결과를 확인한다.(ITworld, 2015;이재득, 2014)



[그림 17] FIDO 인증의 이용자 경험 방식(출처 : FIDO)

바) 마케팅 및 서비스

얼굴인식 등 생체인식 기술은 기업들의 마케팅 목적으로 활용될 수 있다. 소비자 행태 분석을 통해 개별 소비자에게 적합한 광고를 내보내는 식이다.

지난 2013년 영국의 대형 소매유통업체인 테스코(Tesco)는 영국의 450개 주유소에 옵팀아이즈(OptimEyes)라는 스크린을 설치하여 소비자들의 얼굴을 인식하고, 개별 소비자의 특성에 맞는 광고를 내보내는 기술을 도입하였다. 이 기술은 소비자의 눈을 인식하여 연령과 성별을 판단한다.[81] 알맥스(Almax)라는 이탈리아 업체는 마네킹에 카메라와 음성 녹음 기기를 설치하여, 소비자들의 얼굴을 스캔하였는데, 이를 '아이씨 마네킹(EyeSee Mannequin)'이라고 부른다. 이 기술은 소비자의 성별, 연령뿐만 아니라, 얼마나 오랫동안 마네킹을 보고 있었는지도 분석한다. 이 회사는 분석만 할뿐, 소비자들의 이미지나 동영상을 저장하지는 않기 때문에 프라이버시 침해는 없다고 주장한다.[82] 이러한 분석결과를 마케팅에 활용할 수 있는데, 예를 들어 마네킹을 설치한 한 의류업체는 할인기간의 첫째날과 둘째날에는 남성들이 여성보다 더 많이 소비를 많이 한다는 것을 발견하고 제품 진열을 바꾼 바 있으며, 특정 출입구로 들어오는 고객 중 3분의 1 이상이 아시아인이라는 사실을 발견하고 중국어를 할 수 있는 직원을 그 입구에 배치하기도 했다고 한다.[83]

---

81) The Guardian, "Tesco's plan to tailor adverts via facial recognition stokes privacy fears", 2013년 11월 4일, https://www.theguardian.com/business/2013/nov/03/privacy-tesco-scan-customers-faces

82) abc news, "Department Store Mannequins Are Watching You. No, Really.", 2012년 11월 26일, http://abcnews.go.com/Technology/department-store-mannequins-watch-eyesee-analyzes-shoppers-webcams/story?id=17813441

83) 중앙일보, "[J Report] 마네킹 눈 속, 마케팅 비밀", 2015년 4월 15일, http://news.jtbc.joins.com/article/article.aspx?news_id=NB10850367

이와 유사한 이름인 'EyeSee'라는 업체는 이용자의 컴퓨터에 설치된 웹캠을 통해 눈동자 움직임을 추적하여 이용자가 관심을 가지고 있는 콘텐츠를 분석하는 기술, 이용자의 표정을 분석하는 기술 등을 보유하고 있다.[84] 이탈리아의 한 커피 업체는 판촉의 일환으로 얼굴인식 기능을 사용했다. 공항에 얼굴인식 기능을 가진 커피 자판기를 설치한 후, 하품을 하는 승객들에게 무료로 커피를 제공하였다.[85]

이용자에게 제공되는 새로운 서비스에 생체인식 기술이 이용되기도 한다. 페이스북은 딥페이스라는 얼굴 인식 기술을 보유했다.[86] 이 기술을 통해 페이스북은 이용자들이 페이스북에 올린 사진 속 인물이 누구인지 파악해서 태그할 수 있도록 돕는 이름표 추천(tag suggestion) 기능을 제공하고 있다. 이 기술은 2개의 사진에 등장하는 사람이 동일 인물인지 97%의 정확도로 판단해낸다고 한다. 심지어 페이스북은 사람들의 얼굴이 보이지 않는 상태에서도 헤어스타일, 몸매, 자세, 복장 등의 인식을 통해 사람을 식별해내는 기술을 연구하고 있다.[87] 구글 역시 이미지 인식 기술을 보유하고 있다. 구글 고글스(Goggles)는 이용자가 사진을 찍어 제공한 이미지를 분석하여 그 이미지와 관련된 자료를 검색해주는 모바일 앱이다.[88] 예를 들어, 이 앱을 이용해 에펠탑을 찍으면 에펠탑과 관련된 자료를 검색할 수 있다. 그러나 구글은 프라이버시 침해 우려 때문에 이 기능을 얼굴 인식에는 적용하지 않을 것이라고 밝혔다.[89][90]

---

84) http://eyesee-research.com/category/technology/

85) DIGIDAY, "How 5 brands have used facial recognition technology", 2015년 9월 7일, http://digiday.com/brands/5-campaigns-used-facial-recognition-technology

86) 전자신문, "[이슈분석]얼굴 스캔만 해도 누구인지 안다...얼굴 인식의 진화", 2016년 7월 1일, http://news.naver.com/main/read.nhn?mode=LSD&mid=shm&sid1=105&oid=030&aid=0002497960

87) CIO Korea, "안면 인식 기술의 발전… 프라이버시는 이제 글렀는가?", 2015년 7월 1일, http://www.ciokorea.com/news/25756

88) https://play.google.com/store/apps/details?id=com.google.android.apps.unveil&hl=ko

나. 유전정보 수집, 이용 현황

1) 유전정보의 특징과 활용

유전정보(genetic information)는 개인이나 그 가족의 인체유래물질(DNA, 단백질 등)에서 나온 유전적 특징에 대한 정보를 말한다. 유전정보는 주로 유전자 검사(genetic testing)를 통해 얻을 수 있는데, 유전자 검사는 개인을 식별하거나 특정한 질병 또는 상태의 원인을 확인할 목적으로 유전자, 염색체, 유전자 산물(단백질)을 분석하는 행위를 말한다.

유전자 검사는 목적에 따라 크게 세 가지 영역으로 나눌 수 있다. 첫째, 의료 및 연구 목적 (DNA testing, Biobank)의 유전자 검사는 유전병과 같은 특정한 질환의 확인이나 유전자 변이를 연구하기 위해 진행된다. 둘째, 상업적 목적(Direct-to-consumer genetic testing)의 검사는 기업들이 의료기관을 통하지 않고 직접 소비자를 상대로 서비스를 진행하는 영역이다. 유전병 보다는 일상적인 질병, 건강 상태에 대한 유전적인 위험 측정을 주로 해주며 이를 근거로 상담 및 예방차원의 처방을 진행하기도 한다. 셋째, 신원확인 목적 (DNA profiling, DNA database)의 검사는 개인마다 고유하면서 신원확인과 관련된 유전적 특징들을 추출해 DNA 프로필을 만들기 위해 진행하며 주로 수사기관이나 친자확인 업체에서 활용한다.

유전정보는 다음과 같은 특징을 가지고 있다. 첫째, 식별정보를 포함하고 있다. 부모로부터 물려받은 유전정보는 생물학적 정보와 함께 식별정보를 포함하고 있어 개인 식별, 친자 확인, 가족관계를 알 수 있다. 둘째, 매우 소량의 신체 유래 물질에서도 추출이 가능하다. 머리카락, 타액, 정액, 담배꽁초,

89) 가수나 영화배우와 같은 유명인들은 검색이 된다.

90) Readwrite, “Google Goggles for People? Google Says No Plans for Face Recognition App”, 2011년 3월 31일, http://readwrite.com/2011/03/31/google_goggles_for_people_google_working_on_facial

지문은 물론이고 심지어는 악수한 손을 통해서도 얻을 수 있다. 이러한 성격으로 인해 당사자의 인지나 동의 없이도 유전정보의 수집과 분석이 가능하다. 셋째, 유전정보를 통해 개인의 생물학적 특징을 알 수 있다. 단일 유전자 이상으로 생기는 유전병은 발병 전 예측이 가능하며 유전정보를 공유하고 있는 가족들의 유전적 상태도 알 수 있다. 또한 예측력은 떨어지지만 유전병이 아닌 일부 질병이나 외모와 같은 생물학적 특성도 파악 가능하다. 넷째, 전용 가능성이 높은 정보이다. 신원확인 용으로 채취한 DNA 정보를 연구용으로 사용할 수 있고 반대의 경우도 가능하다. 실제로 국내 수사기관들은 신원확인/수사 목적으로 수집한 정보를 연구 목적으로 사용하고 있다. 다섯째, 유전정보는 상업적 가치가 있다. DNA 염기서열 정보는 특허 출원의 대상으로 상업적 가치를 가진 정보이며 이로 인해 DNA 소유권을 둘러싼 복잡한 문제가 발생하기도 한다(김병수, 2014).

2) 공공영역에서의 DNA 정보 수집[91)]

가) DNA 프로파일링

유전자 검사 중 특정인의 유전체(genome)에서 상대적으로 희귀한 위치들을 특성화시켜 그 양상을 분리해 내는 과정을 DNA 프로파일링(profiling)이라고 하며 여기서 나온 정보를 DNA 프로필(DNA profile) 또는 디엔에이신원확인정보라고 한다. 즉 DNA 프로필은 DNA 상의 다수의 위치에서 얻은 유전형의 조합이라고 할 수 있다(Bulter, 2010:25)

프로파일링에 필요한 DNA는 타액, 혈액, 정액, 뼈, 머리카락, 피부조직 등 신체 유래물질에서 추출할 수 있다. 이 기법은 주로 친자확인, 사체확인, 범인검거 등에서 활발히 이용되고 있으며 국내에서는 주로 수사기관, 군대, 바이오 기업들이 활용하고 있다.

---

91) 이 절에서는 신원확인 목적의 DNA 수집만을 다룬다.

[표 7] CODIS DNA 데이터베이스 입력 예시

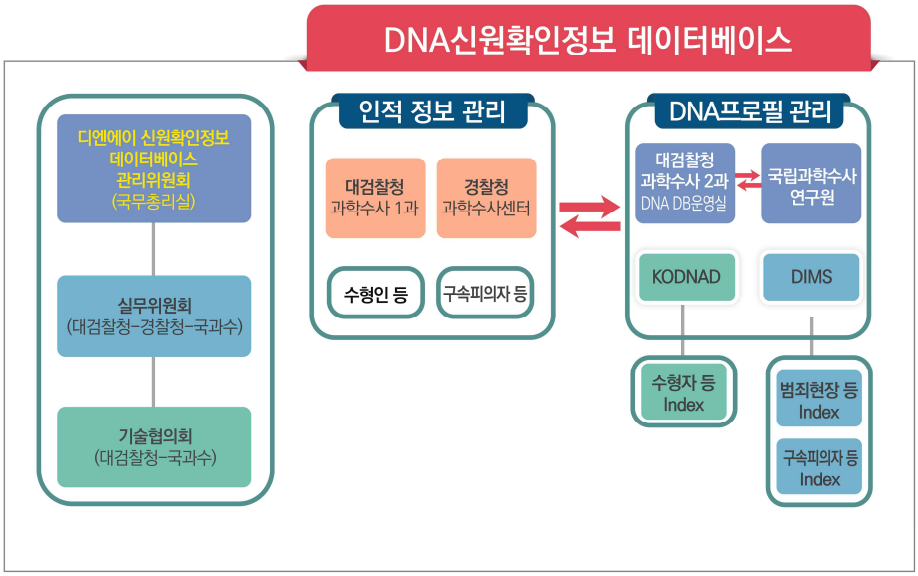
Agency ID VADFS-N	Sample ID 1999082605	Analyst ID JMB	Category Convicted Offender	
Marker	Allele 1	Allele 2	Date	Time
AMEL	X	Y	15-FEB-2000	17:38:30
CSF-1PO	10	10	15-FEB-2000	17:38:30
D13S317	11	14	15-FEB-2000	17:38:30
D16S539	9	11	15-FEB-2000	17:38:30
D18S51	14	16	15-FEB-2000	17:38:30
D21S11	28	30	15-FEB-2000	17:38:30
D3S1358	16	17	15-FEB-2000	17:38:30
D5S818	12	13	15-FEB-2000	17:38:30
D7S820	9	9	15-FEB-2000	17:38:30
D8S1179	12	14	15-FEB-2000	17:38:30
FGA	21	22	15-FEB-2000	17:38:30
TH01	6	6	15-FEB-2000	17:38:30
TPOX	8	8	15-FEB-2000	17:38:30
VWA	17	18	15-FEB-2000	17:38:30

나) DNA 데이터베이스[92)]

(1) 개요

우리나라의 DNA데이터베이스는 2010년 1월 제정된 「디엔에이신원확인정보의 이용 및 보호에 관한 법률」(이하 '디엔에이법')에 따라 수집 활용되고 있다. DNA 데이터베이스는 검찰, 경찰/국립과학구사연구원이 각각 수집 보관하면서 상호 연동하는 이원적 형태로 운영되고 있다. 검찰은 수형인이나 형 확정자, 경찰/국과수는 구속피의자와 현장 수거물에 대해 수집, 분석, 보관한다.

92) 범죄자 DNA 데이터베이스는 <DNA 신원확인정보 데이터베이스 운영 백서>(2015, 디엔에이데이터베이스 관리위원회)와 데이터베이스 관리위원회 회의록 중 일부를 참고하였다.



[그림 18] DNA 데이터베이스 시스템 구성도

(2) DNA의 수집 및 보관

디엔에이법 5조 1항에 따르면 △방화와 실화, △살인, △약취와 유인, △강간과 추행, △절도와 강도, △폭력행위에 대한 처벌법 위반, △성폭력 범죄, △아동 성폭력 범죄, △특정범죄가중처벌법 위반, △ 마약관리에관한법률 위반, △군형법 위반 등 11개 범죄에 대해서 DNA를 수집 할 수 있다. 수형인과 형 확정자는 검찰에서, 구속피의자와 현장 수거물은 경찰이 수집한다. 현장 수거물에는 피해자의 신체 내외부, 소지품이나 범죄 실행과 관련된 사람의 것도 포함된다. 채취 대상자가 채취를 거부할 경우 검찰은 <디엔에이감식시료채취영장>을 청구할 수 있다.

수집된 DNA는 대검찰청 과학수사과와 국립과학수사연구원에서 분석되어 데이터베이스에 입력된다. 입력된 디엔에이신원확인정보는 상호 검색되는데 범죄수사 뿐만 아니라 변사자의 신원확인이나 기타 데이터베이스 상호간 대조가 필요할 경우도 공유된다.

검체는 디엔에이신원확인정보를 확인 한 후 바로 폐기한다. 데이터베이스에 입력된 디엔에이신원확인정보는 사망시까지 보관되며 무죄, 면소, 공소기각 판결 또는 공소기각 결정이 확정된 경우에는 직권 또는 본인의 신청에 의하여 삭제된다.

(3) DNA 데이터베이스 등록 현황[93)]

[표8] DNA 데이터베이스 전체 현황(2010. 7.26 - 2015.3.31.)

년도	합계	수형인등	구속피의자	현장증거물
2010	52,764	10,185	5,292	37,287
2011	42,173	21,480	10,474	10,219
2012	36,332	16,375	8,911	11,046
2013	37,311	17,677	8,366	11,268
2014	36,064	18,254	7,678	10,132
2015	8,322	3,967	1,840	2,515
합계	**212,966**	87,938	42,561	82,467

- 수형인 등의 등록 현황

디엔에이법 5조에 따른 채취 대상자는 실형 확정자 이외에 벌금, 집행유예 등을 받은 수형인 외 형확정자로 나눌 수 있다. 전체의 40% 인 33,327건이 수형인 이었으며, 수형인외 형확정자로 등록된 사람은 전체의 60%인 50,644건이었다. 수형인외 형 확정자 중 벌금형은 9,342건 , 집행유예 등은 41,302건으로 집행유예 등이 전체의 약 82%를 차지하고 있다.

93) 전체 현황은 2015년 3월31일까지이며 나머지 현황 자료는 2014년 12월 31일 기준으로 작성하였음.

[표9] 수형인 등의 DNA 등록 현황

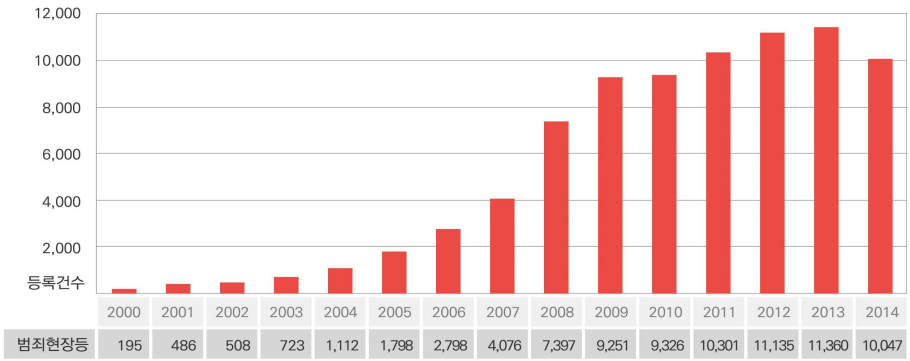
연도	수형인	수형인외 형확정자	계
2010	9,476	654	10,130
2011	16,017	5,348	21,365
2012	3,695	12,655	16,350
2013	2,307	15,562	17,869
2014	1,832	16,425	18,257
계	33,372	50,644	83,971

- 구속 피의자 등의 등록 현황

2014년까지의 총 등록건수는 40,953건으로 구속피의자등의 경우는 일반 경찰관서와 해양경비안전서, 군검찰 그리고 대검찰청에서 직접 구속한 피의자로 나누어서 관리하고 있다. 구속피의자 등의 약 93%는 일반 경찰관서에서 채취한 것으로 38,269건의 디엔에이신원확인정보가 등록되어 있고, 전체 6%인 2,456건은 검찰청에서 구속한 피의자 디엔에이신원확인정보이다. 그 밖에도 해양경비안전서에서 구속한 피의자의 등록건수는 173건 군검찰에서 구속한 피의자의 디엔에이신원확인정보는 55건이 등록되어 있다.

- 범죄 현장 등의 등록 현황

디엔에이법 7조에 따라 채취된 범죄 현장 등의 디엔에이신원확인정보는 법 시행 이전인 2000년 데이터부터 보관하고 있으며 현재까지 총 80,523건의 정보가 등록되어 있다.



[그림 19] 연도별 범죄현장등 데이터베이스 수록 현황

- 범죄 유형별 현황

수형인등은 「폭력행위 등 처벌에 관한 법률」 위반이 28,302건으로 전체 등록 건 중 가장 많았고 구속피의자 등의 경우 절도, 강도 등이 10,859건으로 전체 등록사건 중 가장 많았다.

[표10] 수형인의 연도별 범죄유형

연도	2010	2011	2012	2013	2014	계
방화 등 [제5조 제1항 제1호]	116	355	332	298	302	1,403
살인 등 [제5조 제1항 제2호]	149	2,307	653	243	49	3,401
약취유인 등 [제5조 제1항 제3호]	31	38	19	29	34	151
강간추행 등 [제5조 제1항 제4호]	479	1,490	1,433	2,388	3,495	9,285
절도·강도 등 [제5조 제1항 제5호]	2,505	5,089	3,139	2,802	2,198	15,733
폭력행위등처벌에관한법률위반 [제5조 제1항 제6호]	1,696	3,952	6,771	7,860	8,023	28,302
특정범죄가중처벌에관한법률위반 [제5조 제1항 제7호]	2,990	3,405	521	357	258	7,531
성폭력범죄의처벌등에관한특례법위반 [제5조 제1항 제8호]	410	2,470	1,212	1,384	1,496	6,972
마약류관리에관한법률위반 [제5조 제1항 제9호]	1,587	1,596	1,313	1,307	1,326	7,129
아동·청소년의성보호에관한법률위반 [제5조 제1항 제10호]	167	663	957	1,201	1,076	4,064
군형법 [제5조 제1항 제11호]	0	0	0	0	0	0
계	10,130	21,365	16,350	17,869	18,257	83,971

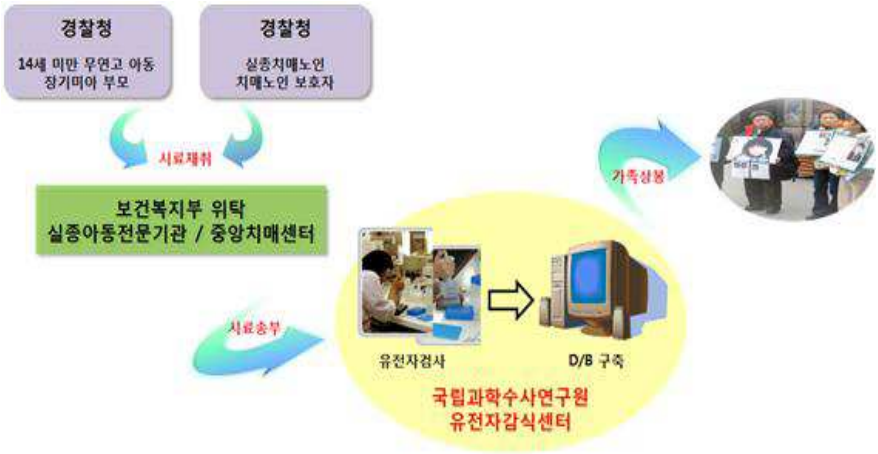
[표11] 구속피의자 등의 연도별 현황

연도	2010	2011	2012	2013	2014	계
방화 등 [제5조 제1항 제1호]	119	224	177	190	208	918
살인 등 [제5조 제1항 제2호]	373	799	659	645	625	3,101
약취유인 등 [제5조 제1항 제3호]	7	15	21	24	40	107
강간추행 등 [제5조 제1항 제4호]	280	573	507	642	717	2,719
절도·강도 등 [제5조 제1항 제5호]	1,542	3,065	2,316	2,155	1,781	10,859
폭력행위등처벌에관한법률위반 [제5조 제1항 제6호]	599	1,296	1,540	1,275	1,457	6,167
특정범죄가중처벌에관한법률위반 [제5조 제1항 제7호]	889	1,271	982	955	780	4,877
성폭력범죄의처벌등에관한특례법위반 [제5조 제1항 제8호]	709	1,347	1,176	1,275	985	5,492
마약류관리에관한법률위반 [제5조 제1항 제9호]	583	1,452	1,104	895	849	4,883
아동·청소년의성보호에관한법률위반 [제5조 제1항 제10호]	192	440	432	412	354	1,830
군형법 [제5조 제1항 제11호]	0	0	0	0	0	0
계	5,293	10,482	8,914	8,468	7,796	40,953

다) 실종아동 DNA 데이터베이스

(1) 개요

2005년 5월 31일 제정된 「실종아동등의 보호 및 지원에 관한 법률」에 따라 경찰청장은 실종아동 등의 발견을 위해서 유전자 검사 대상물을 채취할 수 있다. 채취된 검체는 국립과학수사연구원에서 분석된 후 데이터베이스에 입력·보관 된다.



[그림 20] 실종아동 데이터베이스의 개요

(2) DNA 정보의 수집, 보관, 활용, 폐기

DNA 채취는 경찰관이 진행하며 대상에는 △18세 미만아동, △지적장애인, △치매환자, △정신의료기관 입원 아동, △보호시설 입소자였던 무연고 아동, △ 실종아동 등을 찾고자 하는 가족이 포함된다.

DNA 채취 전 서면동의를 받는데 검사대상자가 미성년자, 심신상실자 또는 심신미약자일 때에는 본인 외에 법정대리인의 동의를 받아야 한다. 심신상실, 심신미약 또는 의사무능력 등의 사유로 본인의 동의를 받을 수 없을 때에는 본인의 동의를 생략할 수 있다. 신상정보와 유전정보는 각각 따로 보관된다.

수집된 검사대상물은 분석 후 폐기되며, 분석된 DNA 정보는 △ 실종아동 등이 보호자를 확인하였을 때 △ 검사대상자 또는 법정대리인이 요청할 때 △유전자 검사일로 부터 10년이 경과되었을 때 폐기된다. 다만, 검사대상자 또는 법정대리인이 요구하면 10년이 경과된 이후에도 보존 기관을 연장 할 수 있다. 검사 대상자나 법정대리인은 유전자 검사 기록을 열람할 수 있다.

(3) 수집 현황 94)

2005년부터 시작된 사업으로 2016년 6월까지 22,041명의 DNA 프로필을 수집했는데, 이중 보호자는 2,195명이다. 2011년부터는 18세 미만의 아동뿐만 아니라 지적장애인과 치매 노인의 DNA 프로필도 수집 보관하고 있다.

[표12] 실종아동 등에 대한 DNA 데이터베이스 구축 현황

연도	계	18세미만 아동	지적장애인	치매환자	보호자
2005	1,245	1,089			156
2006	4,452	4,323			129
2007	2,960	2,681			279
2008	1,790	1,618			172
2009	1,441	1,324			117
2010	1,852	1,731			121
2011	1,163	255	808	-	100
2012	1,193	386	544	83	180
2013	2,125	1,055	815	64	191
2014	1,461	732	421	46	262
2015	1,743	928	525	21	269
2016.1~6	616	280	98	19	219
	22,041	16,402	3,211	233	2,195

94) 국립과학수사연구원에 대한 정보공개 청구 결과(진보넷, 2015.9.23.)와 진선미 의원실이 공개한 자료(2016.8.15.)를 통해 재구성

라) 국방부 DNA 데이터베이스[95)]

(1) 전사자 유해 DNA 데이터베이스

국방부는 2008년 3월 21일에 제정된 「6·25 전사자유해의 발굴 등에 관한 법률」에 따라 전사자 유해와 유가족에 대한 유전자 검사를 실시한 후 자료를 데이터베이스로 구축해 활용하고 있다. 유전자 검사의 결과는 신원이 확인되거나 유전자 검사에 동의한 사람이 폐기를 요청할 때까지 보관한다.

유해 DNA는 국방부에서 수집 분석하나 유가족의 DNA는 국방부가 위탁한 민간 바이오 기업에서 진행한다. 그러나 검체의 폐기나 DNA 제공자의 검사 기록 열람권은 법률에 규정되어 있지 않다.

[표13] 전사자 유해 DNA 데이터베이스 분석 체계

수집기관	분석기관	
	국방부	외부위탁 (유가족 DNA)
유해발굴감식단	조사본부	다우진유전자연구소, 디엔에이링크, 코젠바이오텍, 한국유전자정보센터, 휴먼패스

95) 김병기 의원실의 질의에 대한 국방부 답변 (2016.8.24.)

[표14] 국방부 조사본부에 등록된 DNA 현황

구분	유해(개)	유가족(개)	비고
계	10,673	35,638	
2000~2007	737	3,813	
2008	244	2,163	
2009	691	4,594	
2010	1,619	2,839	
2011	2,039	4,806	
2012	1,890	5,286	
2013	934	3,239	
2014	1,020	2,689	
2015	1,301	2,785	
2016	198	3,424	진행중

(2) 전사/순직자 발생 대비 혈액 채취

국방부는 전사/순직자 발생 대비 명목으로 93,000명의 군인 혈액 샘플을 보관하고 있다.[96]

[표15] 국방부의 연도별 혈액 채취 현황

구 분	계	'09	'10	'11	'12	'13	'14	'15	'16
채취건수	93,901	5,647	4,576	3,206	14,125	26,279	12,140	18,708	9,220

채취 대상자는 해외파병 장병, 항공기 조종사, 함정근무자, 폭발물 취급자, 특수부대 요원이며 일반 장병으로까지 확대하고 있다. 채취된 혈액은 국군의학연구소에서 보관하며 군 소속, 계급, 군번, 생년월일, 채혈일자, 동의서 작성일자를 입력하여 별도의 번호를 부여해 관리하고 있다. 보관 기관은 병사의 경우 채혈일로부터 10년, 간부는 정년까지이다.

96) 국방부는 <국유단지침 429('08. 4. 13) 전사/순직자 신원확인용 혈액샘플 보관체계 구축계획>에 따라 채취, 보관하고 있다.

다. 건강관련 정보 수집, 이용 현황

1) 건강관련 정보의 정의 및 분류

일반적으로 건강관련 정보라고 하면 의료기관에서 환자-의사 관계에서 생성되는 정보를 의미한다. 하지만 최근 건강관련 정보는 전통적인 병원시스템 외에도 다양한 경로를 통해서 수집.이용되고 있다. 이를 보다 체계적으로 정리하면, 주체 및 경로에 따라 크게 다음 두 가지 형태로 나누어 볼 수 있다.

첫째는 전통적인 병의원 진료를 통해서 얻어지는 개인 진료정보에 근간한 건강관련 정보이다. 과거에는 종이차트와 필름 형태로 생성되어 병의원별로 관리되어 왔지만, 최근에는 전자의무기록(EMR)의 확산과 함께 빠르게 디지털 데이터화되고 있다. 과거 일반적으로 건강관련 정보라고 하면 병의원에서 생성되고 관리되어 온 이 데이터들을 의미했다.

두 번째는 개인 라이프로그(LifeLog)를 통한 건강관련 정보이다. 각종 '스마트 기술'의 개발로 한 개인의 일상생활 활동에 관한 데이터가 기록되고 이를 기반으로 개인의 생활을 보다 효율적으로 관리할 수 있게 되었다. 그 중에서도 '웰빙'에 대한 관심이 고조되며 건강관련 정보 로깅(Logging)이 주목받고 있다. 이미 많은 사람들이 스마트폰과 웨어러블 기기를 통해 개인의 운동, 식이, 수면 등 각종 건강관련 정보를 생성하고 활용하고 있다. 과거 건강관련 정보가 거의 의료기관에서만 생성되고 관리되었던 데에서 벗어나 개개인이 스마트폰이나 웨어러블 기기를 통해 자신의 데이터를 스스로 생성·관리하기 시작한 것이다(김주한, 2015). 라이프로깅 기술은 개인 맞춤형 서비스로 점점 발전할 전망이다. 특히, 우리가 '데이터를 소비한다' 또는 '특정 서비스를 이용한다'는 의미는 무엇인가? 이런 서비스나 기술은 가치 중립적으로 활용되지 않는다. 지극히 이기적인 인간의 편리를 쉽게 보여주는 기능을 넣기 위해, 개인 정보를

더 많이 요구하게 된다. 라이프로깅이란 일순간의 기록이라기보다 인간의 전 삶의 주기를 관통하여 특정 개인의 평생의 양태를 추적하는 기술로 발전 중에 있다. 그래서 한번 특정 서비스나 플랫폼에 라이프가 로깅(접속)되는 순간, 그에 대한 전 삶에 대한 의료 또는 관련 정보가 수록되고 열람되고 분석된다.

특히 최근 한국사회에서는 '맞춤형건강', '정밀의료', '원격의료'와 같은 개인 건강관련 정보를 바탕으로 한 미래형 건강관리체계가 제시되며, 이의 근간이 되는 디지털화된 건강관련 정보의 수집·이용에 많은 관심이 쏠리고 있다. 이중 의료기관에서 생성하는 건강관련 정보는 이미 법적으로나 사회체계상으로 특별히 관리되어 왔고, 상대적으로 관리와 활용에 대한 논의가 축적되어 온 반면, 의료기관 외에서 생성되는 건강관련 정보는 훨씬 빠르게 수집·이용이 늘어나고 있는 데 비해 그에 맞는 분석이나 관리에 대한 논의가 뒤따르지 못하고 있다.

본 연구는 이러한 문제의식하에 의료기관에서 생성되는 건강관련 정보를 제외한, 위의 분류에서 두 번째로 분류했던, 각 개인이 여러 디지털 기기를 통해 생성하는 건강관련 정보에 초점을 맞춰 그 수집·이용 현황과 특성, 그리고 그에 따른 문제점 등을 살펴보고자 한다.

2) 건강관련 정보의 주요 수집·이용 수단과 전망

앞서 언급했듯이 전통적인 의료기관 이외에서 생성되는 건강관련 정보는 라이프로그(Lifelog)라는 차원에서 이루어지고 있다. 이는 '개인의 전반적인 일상생활의 기록이나 정보'를 의미하며, 이러한 정보의 생성은 "일상의 기록을 획득하거나 관리하기 위한 목적"으로 특수 제작된 컴퓨터를 통해 이루어진다. 물론 일기나 소셜미디어에 올리는 기록 등도 라이프로그 데이터라고 할 수 있지만 최근에는 이런 소셜정보 외에 사물인터넷으로부터 수

집되는 라이프로그 정보로 확장되고 있다. 정리하면, 라이프로그 차원에서의 수집.이용되는 건강관련 정보는 웨어러블 컴퓨터(wearable computer)와의 연계를 전제로 한다(김주한, 2015).

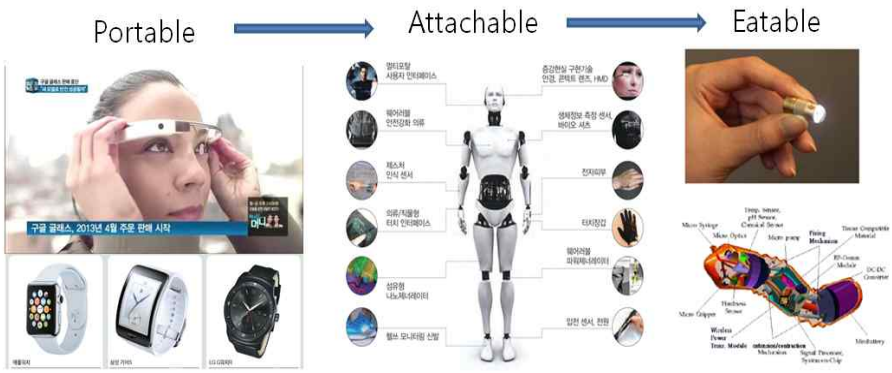
이 웨어러블 컴퓨터는 문자 그대로 소지하거나 몸에 부착하는 형태의 디지털 기기를 말하며 현재 '스마트폰'과 '웨어러블 디바이스'가 이를 대표하고 있다. 최근에는 스마트폰과 웨어러블 디바이스의 경계도 점차 허물어지고 있다. 웨어러블 디바이스에도 어플리케이션이 적용 가능한 경우가 많고 스마트폰과 연계된 웨어러블 디바이스도 출시되고 있다. 또한 사물인터넷(Internet of Things, IoT)을 통한 건강관련 정보 수집도 활발히 추진되고 있어, 향후 스마트폰과 웨어러블 디바이스 그리고 사물인터넷이 결합되어 다양한 형태로의 발전이 기대되는 상황이다(HT R&D 이슈리포트, 2013).

즉, 건강관련 정보의 수집과 이용 그리고 관리에 대한 논의를 진행하기 위해서는 이러한 정보가 일차적으로 기록, 수집, 저장되는 이들 웨어러블 컴퓨터에 대한 분석과 이해가 선행되어야 한다. 또한 건강관련 정보의 관리 역시 이들 기기에 대한 관리를 수반할 수밖에 없다. 특히 빠르게 우리의 생활 속에 자리를 잡아 가고 있는 웨어러블 디바이스에 대한 면밀한 검토가 시급하다. 현재 파악되는 대부분의 자료들은 기술적, 산업적 측면에 초점을 맞춘 것들이지만, 인권적인 측면에 대한 이해를 위해서도 각종 기기들이 건강관련 정보를 수집하는 기술적 원리와 그 정보를 산업적으로 어떻게 활용하고 있는지에 대해 파악할 필요가 있을 것이다. 나아가 관리체계 마련의 시급성을 위해 이 분야의 산업적 전망까지도 가늠해볼 필요가 있다.

우선 건강관련 정보의 핵심 수집·이용 수단으로 주목받고 있는 웨어러블 디바이스는 착용 형태, 기능 등에 따라 세부 분류가 가능하다. 착용형태에 따라서는 시계형, 안경형, 액세서리형, 셔츠형, 신발형 등으로 분류

할 수 있으며, 기능에 따라서는 비교적 단순한 기능만을 제공하는 기본형과 모바일 OS를 기반으로 어플리케이션을 자유롭게 설치하고 실행할 수 있는 스마트형으로 나눌 수 있다(박광만·석왕헌·고순주, 2014).

웨어러블 디바이스는 그 기술의 발전 수준에 따라 다시 세 가지로 구분할 수 있다. 즉, 휴대 및 착용하는 Portable 형태, 신체에 밀접하게 부착하는 Attachable 형태, 생체이식을 할 수 있는 Eatable 형태로 나눌 수 있다. Portable 형태의 경우 스마트폰과 같이 휴대하거나 안경, 시계, 팔찌 등의 착용형 디바이스를 지칭하며, 현재 상용화된 기기들이기도 하다. Attachable 형태는 패치와 같이 피부에 직접 부착할 수 있는 형태로 향후 3-5년 이후 본격적인 상용화가 예상된다. Eatable 형태는 인간의 신체에 직접 삽입·이식하거나 복용하는 형태의 디바이스를 말한다. 아직은 개발 단계 수준이나 수집할 수 있는 건강관련 정보의 종류나 그 정보의 정확성에 있어 다른 단계의 디바이스와는 질적으로 다르기 때문에 향후 진정한 의미의 개인 건강관련 정보의 생성·관리가 가능해질 수 있는 단계로 기대를 모으고 있다(심수민, 2014).

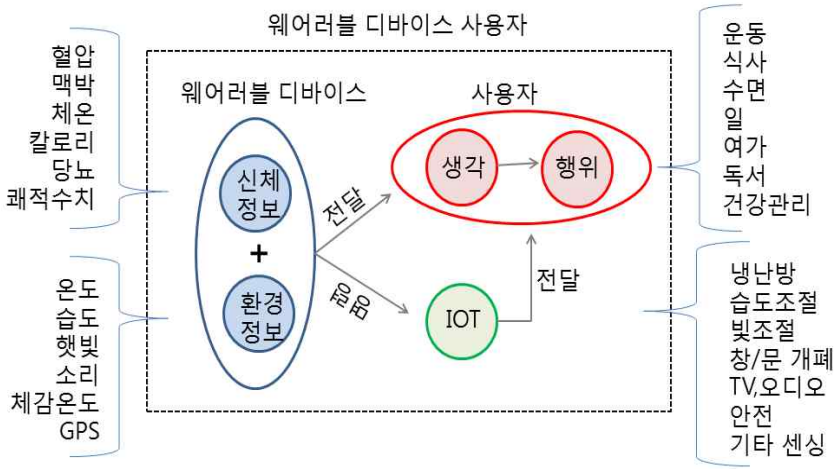


[그림 21] 건강관련 정보 수집·이용을 위한 웨어러블 디바이스의 진화

※ 자료 : 심수민(2014), “2014 웨어러블 디바이스 산업백서”, 디지에코보고서 참조.

3) 건강관련 정보의 수집·이용 과정 및 주요 기술

웨어러블 디바이스나 스마트폰을 이용한 건강관련 정보 수집·이용의 기능적 메커니즘은 우선 아래 그림에서 보는 바와 같이 사용자의 신체변화 정보(움직임, 생체 신호 등)와 사용자 주위를 둘러싼 환경정보(온도, 습도 등)를 기기를 통해 수집하는 과정에서 시작한다. 이렇게 웨어러블 디바이스나 스마트폰을 통해 수집된 정보를 사용자에게 제공하거나 주변의 사물인터넷(IoT)에 명령을 전달하고, 최종적으로는 이를 바탕으로 사용자가 적절한 행동을 하도록 유도하거나 그러한 행동을 서포트하는 방식으로 진행된다.



[그림 22] 웨어러블 디바이스 사용자의 기능적 메커니즘

※ 자료 : 최보성(2015), "웨어러블 디바이스 기술 및 시장동향", S&T Market Report vol.26, 연구성과실용화진흥연구원, 2015.2 참조.

이러한 과정에는 많은 기술의 밀접한 연결이 필요하다. 대표적인 기술만 보더라도, 소형 전자기기에 탑재되는 고용량 고효율 소형 배터리 기술, 블루투스 등과 같이 단거리의 한계를 극복하는 광대역 통신 기술, 장시간 착용에 따른 부품의 저발열, 저전력, 소형화를 위한 기술, 인체의 곡선이나 의류에 쉽게

부착 될 수 있는 플렉서블 기술, 생체신호 및 환경변화를 감지하는 스마트 센서 기술 등이 필요하다(S&T Market Report vol.26, 2015).

웨어러블 디바이스 자체에만 초점을 맞춰 필요한 기술과 장치를 살펴보면, 크게 전원부, 송수신부, 운영체계, 센서, 인터페이스로 나누어볼 수 있다.

[표16] 웨어러블 디바이스의 주요 장치와 기능

주요 장치	기능
전원부	기기 자체의 구동을 가능하게 하는 전력 부분. 대용량일수록 좋으나 디자인에 대한 고려가 필요하며, 현재 저전력 소모기술에 대한 연구가 활발함.
송수신부	정보를 확인·분석하기 위해 실시간 무선 통신 연결을 통해 수집된 정보를 보내고 받는 역할을 하는 장치임.
운영체계	주요 기술들의 효율적 연동·동작과 응용 서비스 개발을 손쉽게 하기위한 보안 강화된 저전력 운영체제가 필요함.
센서	센서는 정보 및 에너지를 물리적·화학적·생물학적 수단을 사용하여 검출하는 장치로 정확하고 신뢰할 수 있는 정보 제공이 관건임.
인터페이스	사용자가 정보를 확인할 수 있도록 표시하는 부분. 최근 자판 입력 대신 음성인식 인터페이스 개발이 주목받고 있음.

※ 자료 : 김장원, 홍승균, 정한민(2014), “웨어러블 컴퓨팅 환경에서의 센서 역할 및 활용 방향”, 정보통신기술진흥센터, 2014년 참조.

특히 웨어러블 디바이스 장치 중 에너지를 물리적, 화학적, 생물학적 수단을 사용하여 신체로부터 정보를 검출해내는 센서 장치가 건강관련

정보 수집에 있어 핵심부분이라고 할 수 있다. 현재 개발되어 적용되고 있는 주요 건강관련 정보 센서는 이동하는 물체의 가속도나 충격을 측정하는 가속도 센서, 대기 중 혹은 국소 부위의 온도를 측정하는 온도 센서, 다양한 종류의 음파를 측정하는 음향 센서, 피사체로부터 반사된 빛을 디지털 이미지화 하는 이미징 센서, 인체의 심장 박동을 측정하는 심장 박동 센서, 혈액 내 산소 포화도를 측정하는 맥박 센서, 인체의 혈류 속 혈당을 측정하는 혈당 센서 등이 있다("웨어러블 컴퓨팅 환경에서의 센서 역할 및 활용 방향", 정보통신기술진흥센터, 2014년).

다양한 센서 기술이 발달함에 따라 고도의 보안 기술 또한 중요시 되고 있다. 건강관련 정보의 수집·이용과 관련한 인권 및 법적 문제와는 별도로 웨어러블 디바이스 자체의 보안 문제가 중요한데, 데이터 해킹이나 디바이스 장치의 도난 또는 무단 사용의 문제가 생길 수 있기 때문이다. 이 때문에 최근 엄격한 보안 프로토콜 및 높은 수준의 암호화, 사용자 인증 생체 인식 사용 등으로 보안이 강화되는 추세이다(S&T Market Report vol.26, 2015).

특히 사물인터넷은 사물에 부착하는 센서와 네트워크 장치이기 때문에 경량화 암호가 적용되어야 한다. 통상 모든 물리적 제품도 경량화를 시도하면 내구성 등 여러 가지 한계를 가지게 된다. 마찬가지로, 경량화 암호화 기법을 적용한 사물 인터넷 제품은 보안 능력이 기존의 제품보다 떨어질 수밖에 없다. 그러나 이들이 다루는 정보는 그 어느 때보다 민감해진다. 예를 들어, 센서 기반의 웨어러블 속옷은 가볍고 편한 속옷이라는 특징 때문에 강력한 암호화 방식과 물리적 장치를 포함하기 어렵다. 뿐만 아니라, 속내의의 가격이 제한적이기 때문에 경제적 한계도 발생한다. 과연 이런 경제적 기술적 한계로 암호 기법 적용에 제한이 따르는 웨어러블과 사물 인터넷의 정보보호는 안전하다고 할 수 있을까? 따라서 이에 대한 면밀한 연구가 추가적으로 수행되어야 한다.

4) 건강관련 정보 수집 기술 및 형태에 따른 분류[97]

가) 스마트폰 및 스마트폰과 연동된 기기[98]

(1) 어플리케이션만으로 구동되는 제품

간단한 만보기 수준의 어플리케이션은 수없이 많이 존재한다. 그러나 심박수와 같은 건강관련 정보를 수집·이용하기 위해선 어플리케이션만으로는 어렵고 삼성의 갤럭시S5처럼 심박수를 측정해주는 내장된 센서를 가진 스마트폰이 있어야 한다. 하지만 최근 보다 간편하게 스마트폰에 별도로 설치된 심박수 센서를 통해서가 아니라 기존의 스마트폰 기능을 이용해 건강정보를 수집하는 어플리케이션이 출시되고 있다.

[그림 23] Azumio사의 심박수 측정 어플리케이션

출처: https://www.azumio.com

97) 최근 새롭게 주목받는 기기들을 위주로 선정했으며, 많은 부분 “In-Depth: Revisiting Topol’s Top Ten Digital Health Targets By Brian Dolan April 25, 2014”를 참조하였고, 그밖에 Healthcare Business(www.chiwon.com)에서 주목한 기기들을 주로 다루었음. 또한 구글 렌즈처럼 아직 상용화되지 않은 제품들은 제외하였음.

98) 각 기기의 사진과 설명은 해당 제품의 회사 홈페이지와 제품 소개 블로그를 참조함.

대표적으로 Azumio사는 아이폰 카메라에 손가락 끝을 대면 심박수를 측정해주는 어플리케이션을 개발하여 출시하였다. 물론 이 역시 아이폰에 내장된 카메라의 센서를 이용하는 것이지만 심박수 측정을 위한 별도의 센서가 아닌 기존 스마트폰의 보편적 기능을 이용하여 건강관련 정보를 수집할 수 있다는 점에 그 특징이 있다.

(2) 스마트폰에 내장된 별도의 센서를 통해 건강관련 정보를 수집·이용하는 제품

[그림 24] 삼성 갤럭시S5의 심박수 측정 센서

출처: www.phonearena.com

2014년 출시된 삼성 갤럭시S5는 별도의 센서를 부착, 스마트폰 최초로 심박수 측정하여 건강관련 정보를 수집하는 기능을 탑재하였다. 최근 출시된 갤럭시S7에도 심박측정 센서를 장착하였으며, S헬스 어플리케이션을 이용해 측정한 심박수를 일별, 주별로 저장·기록할 수 있다. 또한 S헬스는 산소포화도 수치까지 측정할 수 있는 기능을 갖추었다.

삼성뿐만 아니라 주요 스마트폰 제조업체들은 경쟁적으로 피트니스 또는 헬스케어 관련 기능을 강화하는 추세이며, 이에 따라 스마트폰 자체에 센서를 내장하여 다양한 건강관련 정보를 수집할 수 있는 단말기를 출시하고 있는 추세이다.

(3) 스마트폰 부착형 건강 관련 정부 수집·이용 제품

[그림 25] AliveCor사의 심전도 측정기
출처: https://store.alivecor.com

하드웨어적으로 스마트폰에 부착할 뿐만 아니라 소프트웨어적으로 스마트폰과 연동시켜 건강관련 정보를 수집할 수 있는 제품으로는 대표적으로 미국 AliveCor사의 심전도 측정기가 있다. 심장질환을 앓고 있거나 심혈관계 건강이 좋지 못한 사람들이 심전도를 수시로 측정할 수 있도록 만든 제품이다. 이 제품은 스마트폰 케이스에 끼워 사용하는 형태로 양 손을 패드에 대면 스마트폰에서 심장리듬을 확인할 수 있다. 병원에서 측정하는 12개의 심전도 중 Lead I만 확인가능하나, 심방세동(Atrial Fibrillation) 측정이 가능한 수준으로 이미 FDA승인도 취득했다. 기기 외에 AliveCor사에 비용을 추가로 지불하면 전문의가 24시간 내에 기기에서 수집된 건강관련 정보를 판독해주는 서비스까지 제공한다.

AliveCor가 간헐적인 심전도를 측정하는 기기인 반면, Mega Electronics라는 핀란드 회사가 만든 eMotion ECG는 지속적으로 심전도를 측정해준다. 3개의 전극을 가슴에 부착하면 블루투스를 통해 스마트폰으로 심전도가 전송되어 표시된다. 이 제품 역시 FDA 승인을 받은 상태로, 심장 리듬에 문제가 발생할 경우 GPS를 이용해 응급구조대에 신고가 취해지는 서비스까지 가능하도록 설계되어 있다.

심장질환과 더불어 당뇨병은 웨어러블 디바이스와 관계된 기업들이 가장 많은 관심을 가지고 있는 분야이기도 하다. 미국만 해도 2,000만 명이 넘는 당뇨병 환자가 있는 것으로 알려져 있다. 또한 당뇨병 관리가 다른 중증 질환 관리의 기본 조건이 되기에 매일 매일의 관리가 중요하므로 어느 건강관련 정보보다 수요가 높다고 할 수 있다.

[그림 26] iBG star 제품 외형
출처: www.mystarsanofi.com/web/products/glucometers/ibgstar

현재 당뇨병 관리를 위한 가장 선구적인 스마트폰 부착형 제품은 iBG Star이다. 유명 다국적 제약회사인 사노피에서 만든 제품으로 그림에서처럼 스마트폰에 연결해 혈액을 전용 스틱에 떨어뜨리면 혈당이 측정되는 방식이다. 이밖에 LabStyle Innovation사의 Dario라는 제품도 iBG star와 유사한 방식으로 스마트폰에 연결해 사용하는 방식을 택하고 있다.

이와는 조금 다른 형태로 기존의 혈당 측정계와 스마트폰을 연결해주는 기기도 있다. GLOOKO라는 회사의 제품인데 이 제품은 어플리케이션을 통해 혈당 정보를 수집함으로써 원격의료와 유사한 피드백까지 제공한다. 현

재 GLOOKO는 Josline Diatebes center, 삼성전자와 계약을 체결하고 기기 및 관련 서비스 제공을 준비 중인 것으로 알려져 있다.

천식환자에게 있어 환절기나 컨디션이 좋지 않을 경우 미리 폐활량 측정을 할 필요가 있기 때문에 Portable 폐활량계들은 오래전부터 출시되어 왔다. 하지만 최근 스마트폰과 연동시킨 제품들이 연이어 출시되고 있어 천식을 앓고 있는 사람들의 건강관련 정보 수집이 늘어날 것으로 예상된다.

[그림 27] 천식환자들을 위한 폐활량 측정기인 My Spiroo
출처: https://www.pinterest.com/pin/24558760444188663/

대표적으로, 폴란드 벤처기업이 만든 My Spiroo라는 제품은 아이폰의 이어폰잭에 연결하여 사용하는 형태로, 입으로 불어 폐활량을 측정할 수 있다. 이 기기는 GPS 위치 정보까지 수집을 하여 응급조치 서비스가 가능하도록 설계되어 있다.

나) 주요 웨어러블 디바이스[99)]

(1) 손목밴드형 웨어러블 디바이스

웨어러블 디바이스 중 현재 생산량으로 보나 대중적 관심도로 보나 가장 중심적인 기기는 '스마트밴드'로 불리는 손목밴드형 웨어러블 디바이스다. 이 스마트밴드의 가장 중요한 기능 중 하나는 운동 부족과 만성병에 시달리는 현대인들에게 건강관리 기능을 제공하는 데 있다. 이 시장을 선도하고 있는 것은 2007년 재미교포 제임스 박이 창업한 핏빗(Fitbit)이다.

[그림 28] 손목밴드형 웨어러블 디바이스의 선두주자인 Fitbit

핏빗은 다양한 제품군을 가지고 있는데 만보계 기능의 '집(Zip)'에서부터 보급형 모델인 '플렉스(Flex)', 고급형 '차지(Charge) HR'과 '서지(Surge)'까지 총 7개의 모델을 가지고 있다. 가장 많은 인기를 얻고 있는 차지HR의 경우 시계, 만보계, 칼로리 소모량 측정, 수면 기록에 덧붙여 심박수 측정 기능까지 갖추고 있다.

이런 핏빗이 선두를 달리고 있는 손목밴드형 웨어러블 디바이스 시장에 여러 IT 기업들과 스포츠 기업들이 새로운 제품을 내놓으며 경쟁하고 있는 형국이다. 대표적으로 애플워치를 들 수 있다. 애플워치의 피트니스 기능은 기본적으로 하루 칼로리 소모량, 운동량, 심박수를 표시해줄 뿐 아니라 시

99) 각 기기에 대한 설명은 해당 기기의 공식 홈페이지와 제품 소개 블로그를 참고함.

간당 움직임을 추적해 너무 오래 앉아있을 경우 사용자가 움직이도록 권고하는 등 보다 적극적인 서포트 기능을 제공하고 있다.

미국 나이키사의 FUELBAND는 이동거리와 일상 생활 속의 활동량, 빈도, 부하를 측정하고 'NIKEFUEL'이라는 독자적인 지표를 통해 자신이 정한 목표를 달성하기 위한 운동량을 제시한다. 활동량 데이터는 스마트폰 등으로 실시간 확인할 수 있으며 Nike+93이라는 유저 데이터베이스에 수집된 정보가 축적된다. 또한 경쟁을 통한 운동증진을 도모하기 위해 각 개인이 생성한 건강관련 정보를 친구로 등록한 다른 유저들과 공유할 수 있다.

국내에는 잘 알려져 있지 않은 일본의 경우를 살펴보면 도코모 헬스케어의 '무브 밴드(move band)'가 대표적이다. 무브 밴드는 일본의 대표적 통신기업인 NTT 도코모와 의료기기 전문 업체인 오므론사가 합작하여 만든 도코모 헬스케어의 손목밴드형 웨어러블 기기다. 걸음 수와 이동거리, 칼로리 소모량, 수면 시간 등의 건강관련 정보를 와이파이로 스마트폰에 전송하고 도코모 헬스케어가 제공하는 어플리케이션으로 관리할 수 있게 되어 있다. 또한 나이키의 FUELBAND와 마찬가지로 활동 기록을 친구와 공유할 수 있다.

손목밴드형 웨어러블 디바이스를 이용한 다양한 제품 개발은 국내에서도 활발히 진행되고 있다. 대표적으로 삼성의 갤럭시 기어(GALAXY Gear)를 들 수 있다. 갤럭시 기어는 삼성 갤럭시 스마트폰에 대응한 손목시계형 웨어러블 기기다. 블루투스를 이용해 갤럭시 스마트폰 본체와 연결시켜 통화, 문자, SNS 등을 확인할 수 있을 뿐 아니라 본체 뒷면에 부착된 센서를 통해 심박수를 측정할 수 있다. 또한 어플리케이션 'S Health'에 연결하면 실시간으로 심박수에 따른 건강정보 피드백을 받을 수 있다.

이밖에 국내 스타트업과 공공기관에서도 손목밴드형 웨어러블 디바이스 개발에 관심을 기울이고 있다. 대표적으로 대구소방안전본부가 응급상황 발생시 노령 환자들의 생존율을 높이기 위해 기획한 RFID기반 응급환자인

식시스템인 '119안심팔찌'를 꼽을 수 있다. 이 밴드형 웨어러블 디바이스는 사용자가 갑자기 쓰러지거나 이상증세를 보일 때, 119 구급차가 현장에 도착하는 즉시, 구비된 정보인식기(RFID Reader)를 통해 환자의 안심팔찌에 내장된 응급 정보를 즉시 확인하고 출력할 수 있는 서비스를 제공한다. 이 정보에는 환자의 간단한 인적사항과 주 진료병원, 보호자, 주요 질환형태, 복용약물내역 등이 포함되어 있다.

(2) 부착형 웨어러블 디바이스

[그림 29] 부착형 웨어러블 디바이스인 Conventis의 Piix

대표적인 부착형 웨어러블 디바이스로는 Corventis 회사가 내놓은 Piix 제품을 들 수 있다. Piix는 가슴부위에 직접 부착하여 심장박동리듬을 측정하여 부정맥을 측정할 수 있는 기기이다. 30일까지 지속적으로 사용할 수 있으며, 측정된 정보는 모니터링 센터로 보내지게 되며 전문의의 판독을 거쳐 그 결과를 다시 사용자에게 통보해주는 시스템을 갖추고 있어 사실상 원격의료를 대비한 제품이라고 할 수 있다.

그밖에 Piix와 유사한 제품으로 무선 심전도 모니터링 패치인 Corvertis 사의 Nuvant 제품이 있다. 2013년 출시된 Echo Therapeutics사의 Symphony CGM system은 중증 당뇨질환자들의 복부에 부착하여 연속 혈당 측정할 수 있으며, Avery Dennison사의 Metria 제품의 경우 피부에 부착하여 심박수, 활동량, 수면시간을 측정할 수 있다.

(3) 입는 형태의 웨어러블 디바이스

입는 형태의 웨어러블 디바이스로는 접촉 면적이 넓고 측정 부위가 광범위한 만큼 스마트폰이나 손목밴드형 디바이스보다 훨씬 다양하고 정밀한 건강 관련 정보를 수집할 수 있다. 입는 형태의 웨어러블 디바이스로는 미국 IT 벤처기업인 Viviometrics사의 라이프셔츠가 대표적이다. 이 라이프셔츠는 착용자의 심전도, 폐기능, 전신 움직임, 심부온도, 피부온도, 기침 및 호기말 이산화탄소 분압(end tidal CO2) 등을 측정할 수 있다. 액센추어 테크놀로지 랩에서 만든 라이프셔츠의 경우 심폐기능에 이상이 감지되면 센서가 자동으로 의료기관과 연계된 콜센터로 알리고, 의료진은 수집된 건강관련 정보를 토대로 환자에게 어떤 변화가 있는지 파악하고 조치를 취할 수 있다.

그러나 입는 형태의 웨어러블 디바이스는 비교적 정밀한 건강 정보 수집이 가능한 반면 다른 형태의 기기에 비해 다소 불편한 점이 많다. 때문에 아직까지는 일반인보다 군인이나 중증 질환자 혹은 임상시험 참가자들을 대상으로 활용하고 있다.

(4) 착용형 웨어러블 디바이스

대표적인 착용형 웨어러블 디바이스로는 구글 글래스를 들 수 있다. 구글 글래스가 수집하는 건강관련 정보는 아주 다양하지만, 다른 기기와의 가장 큰 차이점이 시각 정보를 통해 건강관련 정보를 수집·이용할 수 있다는 점이다. 따라서 이 시각 정보를 활용한 다양한 기능들이 개발되고 있다. 예를 들어 사용자가 먹는 음식을 시각 센서로 파악하여 건강한 식사를 유도할 수 있다. 또한 의료 현장에서 구글 글래스를 통해 환자정보를 실시간으로 받아보거나, 원격의료지원, 수술 교육 등에 활용할 수 있다.

안경 형태의 웨어러블 디바이스로는 일본의 JINS사의 밈(MEME)도 주목할 필요가 있다. 이 제품은 구글 글래스의 프라이버시 논란을 의식한 듯 촬영기능은 없앴으며, 주로 눈을 관찰해 피로도와 졸음 등 건강관련 정보의 수집·이용에 초점을 맞추었다. 즉, 눈은 얼마나 자주 깜빡이는지 혹 피로가

쌓여 졸음이 찾아오고 있는지 등을 관찰해 상황에 맞는 적절한 피드백을 해주는 것이 이 안경의 주된 기능이다.

다) 피드백을 제공하는 확장된 어플리케이션 및 플랫폼

최근 스마트폰이나 웨어러블 디바이스는 자체 기기 안에서만 건강관련 정보를 수집하고 처리하는 경우도 있지만 통신망과 연결해 보다 확장된 기능을 제공하는 방향으로 나아가고 있다. 특히 통신망과 연결해 구체적인 피드백을 제공하는 확장된 형태의 건강 관리 어플리케이션, 그리고 이러한 건강 관련 어플리케이션을 통합적으로 관리하는 플랫폼 형태로 빠르게 발전하고 있다.

특정 질환에 한정되지만 확장된 건강 관리 어플리케이션 중 가장 앞서 나가고 있는 WellDoc의 BlueStar를 보면, 당뇨 관리를 위한 통합 모바일 어플리케이션 서비스를 제공하고 있다. 구체적으로 당뇨 환자들이 혈당을 입력하면 그 수치에 따라 어떻게 대처할지에 대해 상세한 피드백을 제공한다. 예를 들어 저혈당이 나오면 어떤 음식을 섭취하고 10분 뒤에 혈당을 다시 체크하라고 알려주는 식이다. 임상시험을 통해 이미 FDA 승인을 받았으며, 일부 보험회사들의 보험 적용도 받기 시작했다. 이와 유사한 형태로 Weight Watchers, Agile Health의 Voxiva, 유럽에서 출시된 mySugar, Glucose Buddy 등 역시 확장된 당뇨 관련 건강 관리 어플리케이션을 구축하고 있다.

이러한 어플리케이션을 통합적으로 관리하는 플랫폼으로서는 애플의 Healthkit이 대표적이다. 2014년 6월 발표된 헬스킷은 기존 애플의 스타일과는 달리 다양한 어플리케이션 및 기기와의 연계성을 강화하였다. 예를 들면 A어플리케이션을 통해 측정한 혈압을 B라는 피트니스 어플리케이션과 연동할 수 있는 형식이다. 또한 이 모든 데이터를 의료 기관에서 제공하는 진료 어플리케이션과 공유할 수도 있다. 즉, 애플은 헬스킷을 통해 모든 어플리케이션 간에 건강관련 정보를 공유하고 각각의 서비스가 가지고 있는 한계를 보완하여 모바일 상의 '간이진료소'를 구축하고 있다. 이는 건강

관리에 대한 관심이 높아지면서 이에 대한 시장에서의 선점이 중요해짐에 따라 통신망을 통한 건강 관리 서비스 시장의 표준 플랫폼으로 자리잡기 위한 노력으로 보인다.

구체적으로 현재 헬스킷에서 자체적으로 제공하는 기능만 보더라도 상당히 다채로운데, 신장이나 체지방률, 심박수는 물론 운동량, 영양소별 섭취 현황, 혈중 알코올 농도, 심지어 넘어진 횟수까지 기록하고 있다. 또한 응급시를 대비해 헬스킷에 기저질환, 약물 부작용 여부, 복용중인 약, 긴급 연락처 등 자신의 의료 정보를 미리 입력해 두면 비상시 잠금화면에서도 타인이 사용자의 의료 정보에 접근할 수 있도록 하고 있다.

애플의 헬스킷 외에도 최근 구글핏과 삼성S헬스 역시 건강관련 정보의 통합적 관리를 위한 플랫폼 구축 경쟁에 뛰어들고 있다.

라) 사물인터넷(Internet of Thing, IoT)

사물인터넷을 통한 건강관련 정보 수집·이용은 주로 치매 노인들을 대상으로 한 서비스에 활용되고 있다. 헬스 센스(Healthsense)의 e-이웃 원격 모니터링 시스템(eNeighbor remote monitoring system)을 들 수 있다. 이 시스템은 집안에서 치매 환자들에게 발생할 수 있는 각종 상황에 대처할 수 있도록 한 서비스로, 집안에 Wifi 기반의 통신 서비스를 설치하여 치매 환자에게 발생할 수 있는 위험 상황을 알려주고 보호자가 모니터링할 수 있도록 해 준다. 환자의 활동 정도(ADL)를 체크하는 기능은 물론 주변 응급기관과 연계하여 응급구조 요청을 할 수도 있다.

집안에서뿐만 아니라 외출 시에도 치매 환자들을 관리하기 위한 서비스가 개발되고 있다. 대표적으로 GTX corporation은 GPS 기반의 스마트 신발 깔창을 이용하여 치매 환자 위치를 추적하는 서비스를 제공하고 있다. 자동으로 사용자의 위치가 전송되어 보호자가 원할 때 웹 혹은 핸드폰 어플리케이션을 이용하여 위치를 추적할 수 있다. 또한 일정 범위를 정해놓고 사용자가 그곳을 벗어날 경우 보호자에게 알려주는 기능을 갖추고 있다.

5) 건강관련 정보 제품 시장 현황(웨어러블 디바이스를 중심으로)

가) 최근 해외 동향

전세계 웨어러블 디바이스에 관한 정보를 수집·분석하고 이에 관한 산업적 전망을 제시하고 있는 International Data Corporation(IDC)의 Worldwide Quarterly Wearable Device Tracker 최신 연구조사 결과에 따르면, 2016년 한해 연말까지 웨어러블 디바이스 제품의 출하량은 약 1억 개에 달할 것으로 예상된다. 이는 2015년에 대비 29% 성장한 수치다. 또한 향후 5년간 연평균(CAGR) 20.3%로 성장해 2020년에는 출하량 규모가 2억1360만대에 이를 것으로 전망된다.

[표17] 웨어러블 디바이스 제품 생산량 추이(2016년 2020년은 예상치)

주요 웨어러블 디바이스 출하량 및 시장점유율(단위 백만)							
웨어러블 제품	2015 출하량	2015 시장 점유율	2016 출하량	2016 시장 점유율	2020 출하량	2020 시장 점유율	5년평균 ('16-'20)
손목밴드 및 시계	71.5	90.6%	93.2	91.5%	172.1	80.6%	32.1%
안경	0.1	0.2%	0.2	0.2%	18.8	8.8%	201.2%
옷	0.4	0.6%	2.2	2.2%	15.6	7.3%	62.6%
기타	6.8	8.7%	6.2	6.1%	7.1	3.3%	3.5%
합계	79.0	100%	101.9	100%	213.6	100%	20.3%

※ 자료 : http://www.idc.com/getdoc.jsp?containerId=prUS41530816

주목할 점은 이 웨어러블 디바이스와 건강관련 정보와의 긴밀한 연관성이다. IDC's Worldwide Quarterly Device Trackers 연구조사를 총괄하는 라이

언 리스(Ryan Reith)는 “웨어러블 디바이스의 폭발적인 성장은 피트니스 밴드가 이끌었다”는 점을 강조했으며,[100] IDC의 웨어러블 연구팀을 이끄는 라몬 라마스(Ramon Llamas) 리서치 매니저는 “웨어러블 디바이스가 걸음걸이를 추적하고 환자의 행동을 분석하고, 그 정보가 제2, 제3의 파트와 공유하여 피드백을 받을 수 있는 형태”로 빠르게 진화할 것으로 내다봤다.[101]

이처럼 웨어러블 디바이스의 성장은 헬스케어 분야를 통해 성장할 것이라는 게 전문가들의 중론이다. 물론 그 기술이 예방이나 진단과 같은 원격의료의 형태로 발전하기까지는 시간이 다소 걸리겠지만 먼저 레저, 웰니스, 피트니스 콘텐츠를 시작으로 빠르게 성장할 것으로 보인다(편석준, 2016) 이미 피트니스와 웰니스 분야에서 많은 웨어러블 디바이스를 통해 자신의 운동상황, 심장박동수, 수면상태 등을 수치화된 데이터 수집을 통해 체크하고 있으며, 의료분야에서의 활용도 점차 증가하고 있다(이윤희·이중정, 2016).

웨어러블 디바이스 중에서도 건강관련 정보와 관련 있는 제품만 따로 추적하기란 쉽지 않은데, BCC Research(2014) 발표에 따르면, 전체 웨어러블 디바이스 시장 중 헬스케어 모니터링 디바이스 시장은 2013년 4억2,700만 달러에서 2018년 12억3,500만 달러로 연평균 23.7% 양적 성장할 것이며, 디바이스의 출하량 역시 2013년 1,030만 대에서 2018년 3,300만 대로 연평균 26.2% 성장할 것이라고 한다(“Wearable Computing: Technologies, Applications and Global Markets”, BCC Research 2014) 또한 헬스케어 모바일 디바이스, 센서, 칩 등으로 구성된 모바일 헬스 시장을 통해 헬스케어 관련 웨어러블 디바이스 시장의 비

100) International Data Corporation (IDC) News Letter, 2015.4.6. http://www.kr.idc.asia/newsletters/newsletters.aspx?prid=188

101) IDC press release: IDC Forecasts Wearables Shipments to Reach 213.6 Million Units Worldwide in 2020 with Watches and Wristbands Driving Volume While Clothing and Eyewear Gain Traction 15 Jun 2016

중을 추산해 보면 전세계적으로 2013년부터 2018년 사이 평균 54.9%의 성장이 예상되며, 그 중에서도 모니터링 관련 시장의 비율이 전체 시장의 약 59%가량 될 것으로 전망된다.

정리해 보면, 모바일 헬스케어 산업에서 가장 큰 비중을 차지하고 있으며 성장이 기대되는 건강관련 정보를 모니터링하는 웨어러블 디바이스의 세계 시장은 2015년 3,930백만 달러에서 연평균성장율(CAGR) 41.9%로 2020년에는 32,142백만 달러에 이를 것으로 전망되며, 이중 국내 시장은 2015년 649억 원에서 2020년 5,302억원에 이를 것으로 예상된다.

[표18] 건강관련 정보 연관 웨어러블 디바이스 시장(단위 백만 달러)

2015년	2016년	2017년	2018년	2019년	2020년	연평균
3,930	5,874	9,036	13,995	21,292	32,142	41.9%

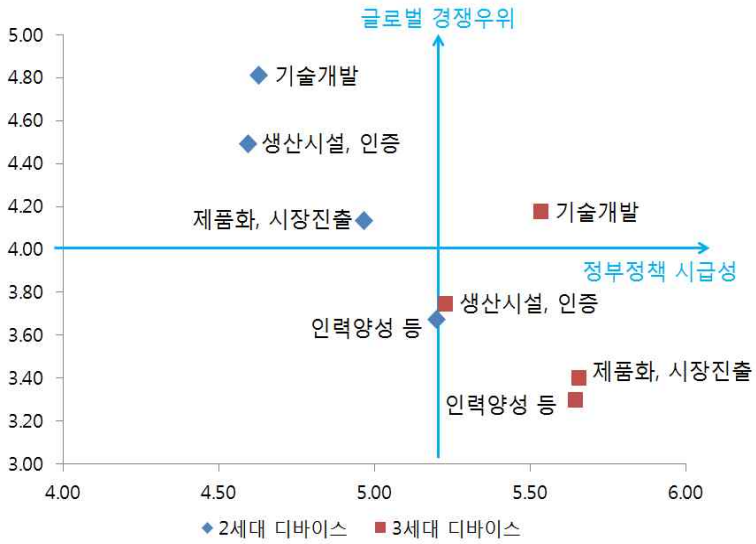
※자료 : “Mobile health technology & Global market”, BCC Reseach(2014), “Wearable Computing: Technology, Applications and Global markets”, BCC Research(2014), “Worldeide Medical Market Forcast to 2018, Espicom(2013), 이윤희·이중정(2016), “생체신호 모니터링 디바이스”, KISTI maket report 2016-25, 3쪽

나) 최근 국내 동향

현재 우리나라의 웨어러블 디바이스 산업은 냉정히 말해 반도체나 스마트폰처럼 꾸준히 발전을 거듭해온 분야는 아니다. 휴대폰 사업(정부가 말하는 2세대 스마트 디바이스)까지는 세계시장에서 경쟁력을 유지해왔으나 보다 진일보된 형태의 웨어러블 디바이스로의 전환에는 다소 뒤쳐진 상황이다.

정부의 진단을 보더라도 “스마트폰 시장을 제외한 주요부품 및 새로운 디바이스 개발을 위한 핵심 기술 및 산업경쟁력이 부족하고, 중소·벤처의 디바이스 개발 인프라 및 투자 환경은 여전히 낮은 상황으로 다품종·소량

생산 중심의 시장 환경 변화에 취약"한 상황이며, 중소기업청 통계상으로도 전자부품·디바이스 중소기업 설비투자가 2011년 6,464억원에서 2013년 3,699억으로 오히려 감소한 상황이다("K-ICT 스마트 디바이스 육성 방안", 미래창조과학부·산업통상자원부, 2015).



[그림 30] 국내 웨어러블 디바이스 산업의 전망 진단

※ 자료 : "K-ICT 스마트 디바이스 육성 방안(안)", 미래창조과학부·산업통상자원부, 2015.

※ 2세대 디바이스는 휴대폰 태블릿을 의미하며, 3세대의 경우가 본격적인 웨어러블 기기에 해당한다. 7점 척도로 평가하여 결과의 평균값(경쟁우위 3.95점, 시급성 5.2점)을 기준으로 높고 낮음 구분한 것이다.

정부는 이런 분석 하에 2015년 3월 25일 'K-ICT 전략에서 창조경제 실현을 위한 9대 전략산업'으로 "소프트웨어, IoT, 클라우드, 정보보안, 스마트 디바이스, 5G, UHD, 디지털콘텐츠, 빅데이터"를 지정하였다. 즉, 창조

경제의 주요 전략사업 중 하나로 스마트 디바이스를 선정하여 유망 기업을 육성 지원하겠다는 것이다. 그러나 이 계획은 “디바이스 분야에 특화된 기획 및 성과관리를 위한 지원이 미흡”한 점이 지적되어, 2015년 9월 22일 보다 세분화된 “K-ICT 스마트 디바이스 육성 방안(안)”에 따라 본격적인 웨어러블 디바이스에 대한 지원이 이루어지고 있는 상황이다.

한편, 국내 웨어러블 디바이스를 선도하고 있는 삼성은 웨어러블 디바이스 사업과 관련해 중요한 전략사업으로 가상현실(VR) 디바이스 제품과 함께 2016년 웨어러블 디바이스 시장의 50% 이상을 차지하는 스마트 밴드 사업을 언급하며 특히, “헬스케어 산업과 연계하여 시장을 이끌고 있음”을 강조하였다.[102)]

사실 삼성은 웨어러블 디바이스 개발 초창기부터 건강관련 정보와 긴밀하게 연관시켜 왔다. 이미 2011년 8월 스마트폰에 BT기술(혈관탄성도와 맥파전달속도)을 결합시킨 카드형 혈압계 허가를 획득했는데, 이 제품은 자동전자혈압계·카드형 혈압계·스마트폰 등으로 구성돼 혈압 및 심전도 등의 건강관련 정보를 스마트폰으로 전송하는 기능이 구현된다. 2014년 출시된 갤럭시S5는 국내에서 출시된 휴대폰 가운데 최초로 심박 측정 기능을 탑재한 제품이기도 했다.[103)]

최근 삼성은 스마트폰과 연동되는 웨어러블 심전계 제품의 제조인증도 획득했는데, 이 제품에는 삼성전자가 2015년 말부터 양산에 들어간 다양한 생체신호 수집·처리 기능을 하나의 반도체칩에 통합한 바이오 프로세서가 적용됐다. 이 바이오 프로세서는 체지방과 골격근량 및 심박수, 심전도 측정 등 모바일 헬스케어를 위해 가장 대표적인 5가지 센서 기능을 내장한 것으로 알려졌다.[104)]

---

102) “삼성이 주도하는 웨어러블 마켓 트렌드”, 삼성뉴스룸, 2016.7.1.

103) “식약처 ‘갤럭시S5 의료기기 아니다’”, 2014년 3월 5일자 경향신문

104) “원격의료가 공공의료 확충 수단? 대기업을 위한 정책 아니다?” 2016년 9월 27일자 라포르시안

한국 내에서 웨어러블 디바이스를 건강관련 정보와 관련지어 작성한 구체적인 데이터가 존재하지 않아 이에 대한 분석이 쉽지 않으나, 정부는 삼성과 같은 주요 웨어러블 선두 기업들을 파트너로 노령자 건강관리 사업과 연관지어 웨어러블 디바이스의 활용을 구상하고 있는 것으로 보인다.

특히 올해 정부가 진행하는 만성질환관리 시범사업에는 몸에 착용하거나 부착해 사용하는 웨어러블 디바이스가 사용되는 것으로 알려졌다. 이 시범사업에서는 웨어러블 디바이스를 통해 측정된 운동량 등 건강정보는 다시 스마트폰을 통해 의료기관에 전송되고 이를 의사가 판독하여 상담과 피드백을 제공하는 방식으로 진행될 예정이다.[105)]

[표19] 건강관련 정보 모니터링 국내 웨어러블 디바이스 시장(단위 억원)

2015년	2016년	2017년	2018년	2019년	2020년
649	968	1,485	2,310	3,509	5,302

※ 자료 : “Worldeide Medical Market Forcast to 2018, Espicom(2013)에 언급된 해외시장 대비 국내 헬스케어 시장 규모 1.5%를 기준으로 가정하여 예측한 값, 이윤희·이중정(2016), “생체신호 모니터링 디바이스”, KISTI maket report 2016-25, 3쪽 참조.

105) “복지부 ‘모바일 헬스케어 개념 접목해 웨어러블 디바이스 사용’…‘삼성 등 대기업 위한 정책’ 논란 커질 듯, 2016년 1월 19일자 라포르시안

제3장

바이오 정보 수집, 이용과 정보 인권

제3장 바이오 정보 수집, 이용과 정보 인권

가. 생체인식 정보 활용시 문제점과 피해사례

1) 생체인식 정보의 특성과 위험성

생체인식 정보의 활용도가 높아지면서 그 위험성에 대한 우려도 커지고 있다. 생체인식 정보가 본인 식별이나 인증을 위해 활용되는 것은 그 유일성, 불변성 때문인데, 바로 그와 같은 특성 때문에 개인의 프라이버시에 미치는 영향도 치명적일 수 있기 때문이다. 즉, 유출되었을 경우 변경할 수 있는 비밀번호나 신용카드 등과 달리, 생체인식 정보는 한번 유출되면 그 피해를 복구하는 것이 거의 불가능하다.

이러한 문제에 대응하기 위하여 재발급 가능한 템플릿(특징정보) 기술[106]이 개발되고 있는데, 이는 템플릿 정보가 유출되더라도 이를 폐기하고 새로운 템플릿을 재발급 가능하도록 하는 기술이다. 재발급 가능한 생체인식(Renewable Biometrics) 기술이라고도 불리며, ISO/IEC 표준으로도 제정된 바 있다(김동진, 2016).

또 다른 문제는 생체인식 정보를 추출하는 과정에서 원 바이오 정보에서 부가적인 정보가 추출될 가능성을 배제할 수 없다는 것이다. 예를 들어, 얼굴 정보로부터 인종, 건강상태, 정신상태 등 본인 인증과는 무관한 정보가 추출되어 이용될 수 있다. DNA 정보에서도 유전정보 외에 질병 정보 등 다른 생물학적 정보를 추출할 수 있다. 이에 따라 민감한 사생활 침해 및

106) 재발급 가능한 템플릿 기술은 생체인식 템플릿 대신 별도의 비교정보를 사용한다. 비교정보는 템플릿을 이용하여 생성하며, 재발급 가능한 알고리즘에 의해 생성되기 때문에 유출되더라도 폐기 및 재발급이 가능하며 비교정보로부터 템플릿의 역추출이나 복원은 불가능하기 때문에 템플릿은 안전하다고 한다. (김동진, 2016)

목적 외 이용의 가능성 문제가 제기될 수 있다. 이 때문에 원 바이오 정보와 생체인식 정보의 분리 보관이나 생체인식 정보 추출 후 원 바이오 정보를 폐기해야 한다는 대안이 제안되고 있다.

또한, 바이오 정보는 사용자가 인식하지 못하는 사이에 채취될 수 있는 위험이 존재한다. 나도 모르게 CCTV나 몰래 카메라에 촬영될 수도 있고, 내가 마신 컵에서 지문이나 DNA를 채취할 수도 있다. 공공 및 민간 영역에서 생체인식 데이터베이스가 구축되고, 이러한 생체인식 정보가 유출된다면 바이오 정보의 은밀한 채취를 통한 범죄의 가능성도 커질 수 있다. 법적으로는 정보주체의 동의가 없거나 법률에 근거가 없는 개인정보의 수집은 금지되지만, CCTV와 같이 개별적인 동의를 받기 힘든 생체인식 기술의 도입이 확대된다면, 혹은 생체인식 기술의 확산으로 불법적인 바이오 정보 수집이 확대된다면 정보주체에 실질적으로 미치는 위험성은 커질 것이다.

2) 생체인식 기술의 불완전성

비록 생체인식 기술이 그 정확성과 보안성을 근거로 각광을 받고 있지만, 이는 자칫 생체인식 기술에 대한 과도한 신뢰를 부여할 수 있다. 생체인식 기술 역시 완전하지 않으며, 또한 각 생체인식 기술마다의 취약점을 가지고 있음을 인식해야 한다. 즉, 각 생체인식 기술은 일정한 오류율을 가지고 있으며, 특정한 신체적 질병이나 외부 조건에 따라 인식률이 떨어질 수 있기 때문이다. 이 때문에 생체인식 기술이 애초에 의도했던 효과를 가져오지 못할 수도 있으며, 이용자를 차별하거나 이용자의 재산, 신체 등에 피해를 야기할 수도 있다. 예를 들어 금융거래에 생체인식 정보가 활용될 경우, 본인거부율이 높으면 고객의 인증에 실패하여 고객의 불편을 초래하게 되며, 타인수락율이 높으면 금융 사고를 초래하게 될 것이다. 출입통제에 사용될 경우, 정당한 권한이 있는 사람이 건물에 들어가지 못하거나(본인거부), 침입자가 건물에 들어가는 사태(타인수락)가 초래될 수 있다.

국제 정보인권단체인 프라이버시 인터내셔널은 2013년 보고서에서 생체인식 기기에 대한 과도한 의존이 가져온 실패사례를 소개하고 있다. 케냐 정부는 선거 과정의 투명성을 높이기 위해 생체인식을 통한 선거인 등록을 시행한 바 있다. 2012년 선거에서 2억9300만 달러의 비용을 지출했으나, 그 결과는 처참했다. 생체인식 기기가 지문인식에 실패한 경우가 많아, ID 카드 번호를 시스템에 수작업으로 입력해야 했다. 또한, 아프리카에서 종종 투표소로 이용되는 학교 교실은 전기 시설이 제대로 갖춰지지 않았고, 선거 관리인이 식별 번호를 잊어버려 시스템에 접근하지 못하는 경우도 있었다.

앞서 소개한 유엔난민고등판무관(UNHCR)이 난민 식별을 위해 생체인식 기술을 도입한 사례에서도, 데이터 불량이나 인식 오류가 발생할 경우 난민들이 건강이나 식량 등 적절한 지원을 받지 못할 수 있다. 프라이버시 인터내셔널의 2008년 연구에 따르면, 수집되는 지문정보의 정확성이 낮거나 각 지역마다 서로 다른 시스템이 사용되는 등의 문제가 있었다. 또한 능력있는 관리자가 없어 시스템이 고장나서 스탭들이 수작업으로 입력해야 하는 경우도 있었다고 한다.(Privacy International, 2013)

생체인식 기기의 취약점 때문에 장애인 등 특정 소수자를 배제하게 될 위험성도 제기되고 있다. 얼굴 인식 시스템은 검은 피부를 가진 사람을 스캔하는데 어려움이 있다고 하며, 홍채 인식은 백내장을 가진 사람이나 신체 장애가 있는 사람에 대한 정확도가 떨어진다. 단일한 생체인식 기술을 통해 특정한 서비스가 제공된다면, 장애인 등이 서비스 제공에 차별을 받을 수 있다. 따라서 생체인식 기술이 도입되더라도, 인식이 되지 않는 사람이나 혹은 자신의 생체인식 정보 제공을 꺼리는 사람을 고려하여 항상 대체인증을 위한 수단을 제공할 필요가 있다.

금융영역에서 생체인식 기술이 주로 보조 인증수단으로 쓰이는 이유도 이 때문이다. 금융서비스는 무엇보다 안전성과 범용성이 중요한데, 단일한 생체인식 기술은 나름의 취약점을 가지고 있기 때문이다. 이러한 문제 때

문에 다중 생체인증 기술이 제안되고 있는데, 이는 여러 개의 생체인식 기술을 복합적으로 사용하여 정확성을 높이기 위한 방법이다. 결합 방식에 따라 다중방식(multi-modal), 다중개체(multi-instance), 다중 알고리즘(multi-algorithms), 다중센서(multi-sensor), 다중샘플(multi-sample) 등 다양한 모델이 제안되고 있다.

[표20] 다중 생체인증 기술 모델 (출처 : 이재득, 2014;김동진, 2016)

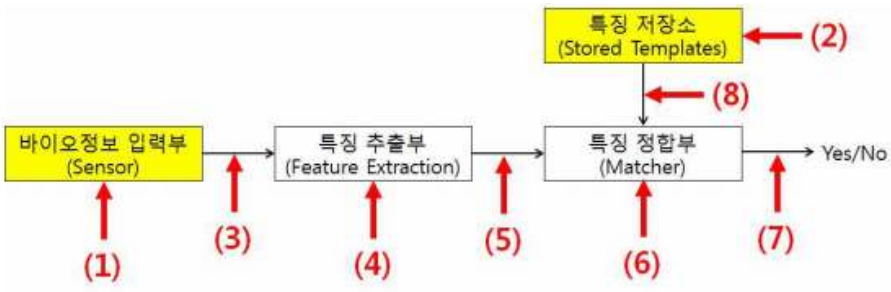
구분	특징
다중방식 (multi-modal)	2개 이상의 서로 다른 바이오 정보를 융합 (예 : 지문 + 얼굴, 지문 + 정맥 등)
다중개체 (multi-instance)	다수의 인스턴스를 획득 및 융합 (예 : 엄지 지문 + 검지 지문, 왼쪽 눈 홍채 + 오른쪽 눈 홍채 등)
다중 알고리즘 (multi-algorithms)	단일 바이오 샘플에 다수의 특징정보 추출 알고리즘을 적용하여 특징정보 추출 및 융합
다중센서 (multi-sensor)	단일 인스턴스를 다양한 센서로 획득하여 융합 (예 : 얼굴 2D이미지 + 3D이미지, 지문 광학센서 + 정전센서 등)
다중샘플 (multi-sample)	단일 개체 생체인식 정보 대하여 여러 표현방식으로 정보 추출

수사기관이 생체인식 정보를 활용할 때 생체인식 기술의 한계로 인해 식별 오류가 발생할 경우에도 큰 문제가 될 수 있다. 무고한 사람이 범죄 혐의자가 되거나, 혹은 범죄자를 놓칠 수 있기 때문이다. 2016년 미국 수사기관의 얼굴인식 시스템을 연구, 조사하여 보고서를 발표한 프라이버

시&기술센터는 국가표준기술연구소(NIST)에 얼굴인식 시스템 정확도 테스트의 범위와 주기를 확대할 것을 권고했다. 인종, 성, 연령 등에 기반한 알고리즘적 편향이 있는지 정기적으로 테스트하고, 기존의 정확성 테스트 주기를 강화할 것을 주문했다. 특히, 실시간 얼굴 인식에 대한 테스트를 강화할 것을 요구했다.(Center on Privacy&Technology, 2016) 이는 얼굴인식 시스템과 관련한 권고이지만, 지문, 홍채 등 다른 생체인식 시스템의 운영에도 참고할 만하다.

3) 바이오인증 시스템의 보안 위협

바이오인증 시스템 역시 정보시스템의 하나이기 때문에 여느 정보시스템과 마찬가지로 보안위협이 존재한다. 금융보안원은 바이오인증 시스템의 구성 및 보안상 취약점을 다음과 같이 분석하고 있다. 바이오인증 시스템은 센서를 통해 바이오 정보를 취득하는 입력부, 취득된 바이오 정보로부터 특징정보를 추출하는 특징 추출부, 특징정보 및 개인정보 등을 저장하는 특징 저장소, 저장된 특징정보와 새로 입력된 특징정보를 비교하여 인증여부를 결정하는 특징 정합부 등 4개의 모듈로 구성이 되는데, 각 단계에서 취약점이 존재할 수 있다.



[그림 31] 생체인증 시스템상 보안 취약점 (출처 : 금융보안원, 2016)

(1) 위조지문, 고해상도 사진 등 위조된 바이오 정보를 센서에 입력하여 인증을 우회
(2) 저장소에 침투하여 기 저장된 특징정보를 조작, 삭제, 유출
(3) 불법 취득한 바이오 정보를 재생(replay)하여 인증
(4) 위조된 특징정보를 임의로 생성
(5) 정상적인 특징정보를 임의의 위조된 특징정보로 대체
(6) 특징 정합부에서 인증 결과값을 임의로 변경
(7) 최종 인증결과를 조작
(8) 저장소에서 정합부로 전송되는 특징정보를 절취 또는 타인의 정보로 대체

현재까지 주된 피해사례는 (1) 바이오 정보의 위조와 (2) 바이오 정보의 유출에서 나타나고 있으나, 바이오인증 서비스의 확산과 해킹 기술의 진화에 따라 (3)~(8)의 단계에서도 문제가 발생할 수 있다.

4) 바이오 정보의 위조

바이오 정보가 위조로부터 안전한 것은 아니다. 바이오 정보가 위조될 수 있다면, 위조된 바이오 정보를 통해 타인이 내 신원을 도용하는 것이 가능할 것이다. 이미 현재 활용되고 있는 생체인식 기술과 관련하여 바이오 정보 위조 사건이 발생하거나, 혹은 위조가 가능하다는 실험 결과가 발표되고 있다.

지난 2015년 경북지역 소방 공무원이 실리콘으로 제작한 위조 지문을 이용하여 근태관리용 지문인식 단말기를 부정 인식한 사례가 발생하였다. 애플 아이폰 5s, 삼성전자의 갤럭시 S5 지문인식 잠금 기능도 가짜 지문으로 해제될 수 있음이 드러났다. 독일의 해커단체 CCC는 러시아 대통령 푸틴의 고해상도 사진을 출력하여 홍채 복제가 가능함을 시연하였다.

DNA도 쉽게 위조될 수 있다. 지난 2009년 이스라엘의 유전자 분석 업체인 '뉴클릭스' 연구팀은 국제 법의학 저널(FSI)에 발표한 논문에서 혈액 속의 DNA

를 슬쩍 다른 사람의 것으로 바꾸거나 특정인의 DNA를 인공적으로 만드는 실험에 성공했다고 밝혔다. 이것이 가능하다면, 범죄 현장에 악의적으로 타인의 DNA를 남김으로써 범죄를 뒤집어씌울 수도 있는 것이다.[107]

만일 생체인식 기술에 과도한 신뢰성이 부여된다면, 만에 하나 식별 오류나 악의적인 위조 등으로 인해 오히려 개인의 신원이 부정당하거나 혹은 반대로 신원을 도용당했을 때 이를 구제하기가 더욱 힘들어질 수 있다.

이러한 바이오 정보 위조를 막기 위해 위조 지문을 판별하기 위한 기술 등 보안 기술도 발전하고 있다. 본인 인증 시 생체 세포 및 조직의 괴사 여부까지 판별하는 기술(빛의 파장으로 모세혈관 내 혈액량 측정(2011년), 헤모글로빈 탐지 기술(2013년) 등)[108], 바이오 정보 해킹을 방지하기 위해 사람 몸을 전송 수단으로 사용하는 기술도 개발되었다고 한다.[109] 그러나 보안 기술과 해킹 기술이 함께 발전하는 것과 같이 발전된 생체인식 기술을 해킹하기 위한 기법들이 앞으로도 계속 나올 가능성을 배제할 수 없다.

[표21] 바이오 정보 위조 사고 사례 (출처 : 금융보안원, 2016; 김동진, 2016 재구성)

사고 사례	시기	주된 내용
근태관리 악용	2015.2	- 경북지역 소방 공무원 3명이 2012년부터 2년간 실리콘으로 제작한 위조지문을 이용하여 근태관리용 지문인식 단말기에 부정 인식하여 초과근무 수당 수령 - 근태관리용 단말을 정맥인식 방식으로 교체 예정

107) 조선닷컴, “DNA 증거 무용지물 되나… “간단히 조작 가능””, 2009년 8월 20일, http://news.chosun.com/site/data/html_dir/2009/08/20/2009082000131.html

108) KB금융지주경영연구소, 금융산업에서 생체인식 기술의 활용 현황과 전망, 2014.6.2

109) 전자신문, 사람 몸이 데이터 전송수단?…해킹 원천봉쇄, 2016.10.5

	2013.3	- 브라질 상파울루 의사인 Ferreira는 동료의사 등 6명의 실리콘 위조지문을 제작하여 교대로 근태관리를 악용, 실근무를 하지 않고 급여를 수령하는 유령사원임이 적발됨. 경찰은 상파울루 내 300명 이상의 근로자가 유령사원으로 추정된다고 발표
불법 부동산 명의 이전	2014.10	- 박모씨 등 4명은 중국 위조범에 의뢰하여 3D 프린터를 이용한 실리콘 위조지문을 제작. 주민센터의 지문센서가 위조여부를 탐지하지 못해 인감증명서 등 필요서류를 발급받아 50 억대 부동산을 불법으로 명의 이전
사진으로부터 지문 복제 (컨퍼런스 시연)	2014.12	- 독일의 해커단체 CCC는 독일 국방장관의 기자회견 사진 등 여러 각도의 사진 및 VeriFinger 소프트웨어를 이용하여 지문 복제[110]
사진으로부터 홍채 복제 (컨퍼런스 시연)	2014.4	- 독일의 해커단체 CCC는 구글 검색을 통해 러시아 대통령 푸틴의 고해상도 사진을 출력하여 홍채 복제(Print attack). 위조지문은 별도 제작이 필요하나, 홍채는 사진 출력만으로 복제 가능
삼성 갤럭시 S5 잠금장치 해제 (동영상 시연)	2014.4	- 독일의 시큐리티리서치랩스는 목재용 접착제에 사용자 지문을 복제하여 지문인식 잠금장치 해제 - 위조지문을 이용해 갤럭시 S5와 연동된 페이팔(PayPal) 결제도 가능
아이폰 6/5S 지문인식 잠금장치 해제 (동영상 시연)	2014. 9 (아이폰6) 2013. 9 (아이폰5S)	- 고해상도 사진을 이용하여 실리콘으로 위조지문을 제작, 아이폰 6/5S의 지문인식 잠금장치 해제

지문인식 지불시스템 해킹	2008.2	- 네덜란드 최대의 식료품 체인업체가 지문인식 지불시스템(Tip2Pay)을 도입하였으나, 실리콘으로 제작한 위조지문을 탐지하지 못해 정상적으로 대금을 결제
차량 절도를 위한 손가락 절단	2005.3	- 말레이시아 4인 강도는 지문인식시스템이 도입된 벤츠 S-클래스 차량을 절도하기 위해 회계사 Kumaran의 손가락을 절단. 해당 지문인식 시스템이 살아있는 생체조직 여부를 판별하는 기능을 탑재하고 있어, 절단 한 손가락으로 차량구동이 불가하여 검거
DNA 위조 (실험)	2009	- 이스라엘의 유전자 분석 업체인 '뉴클릭스' 연구팀은 국제 법의학 저널(FSI)에 발표한 논문에서 혈액 속의 DNA를 슬쩍 다른 사람의 것으로 바꾸거나 특정인의 DNA를 인공적으로 만드는 실험에 성공했다고 밝힘.
스마트폰 생체인증 우회(실험)	2016	- 미국 미시간주립대 연구진, 총 비용 $500 미만으로 일반 2D프린터를 이용하여 출력한 위조 지문을 통해 최신 스마트폰의 바이오인증을 우회한 사례 발표 - 연구진들은 지문을 스캔한 후에 일반 2D 프린터와 AgIC 은(Silver) 전도성 잉크를 사용하여 전용 종이에 출력하고, 출력한 지문으로 인증에 성공

110) 뉴시스, ""손가락 사진만으로 지문 복제 가능하다"… 생체보안 장치 안정성 '도마'", 2014.12.30

5) 바이오 정보의 유출

바이오 정보 데이터베이스의 증가에 따라 해킹이나 내부자 유출 등으로 인해 바이오 정보가 유출될 가능성을 배제할 수 없다. 2016년 3월, 한국 IBM은 '2016 IBM 엑스포스(X-Force) 보안 동향 및 위험 보고서'를 발표했는데, 이에 따르면 사이버 공격의 대상이 신용 정보에서 바이오 정보로 이동하고 있다고 한다. 100만 건 이상의 정보유출 사건이 전 세계적으로 5건 정도 있었는데 모두 헬스케어 분야에서 바이오 정보가 유출된 사례다.[111] 지난 2015년 6월에는 미국 연방 인사관리처의 데이터베이스가 해킹되어 미국 전·현직 공무원의 개인정보 2,200만 건과 함께 지문정보 560만 건이 유출되기도 했다.[112]

아르헨티나에서는 2013년 대선 과정에서 온라인 선거인명부등록 시스템의 취약점이 발견되었다. 취약점이 알려졌음에도 불구하고 아르헨티나 정부는 이에 대한 조취를 취하지 않았고 데이터베이스의 사진 정보가 다운로드될 위험에 노출되었다. 2013년 10월, 한 16세 소년이 온라인 데이터베이스를 어떻게 해킹할 수 있는지 올렸고, 한 개발자도 사진 이미지를 다운받을 수 있는 사이트를 공개했다. 결국 정부가 이를 막기 위한 조치를 취했지만, 그 사이에 얼마나 많은 개인 사진들이 유출 되었는지는 모른다.[113]

중앙 데이터베이스에 집적된 바이오 정보(혹은 생체인식 정보) 뿐만 아니라, 스마트폰에 저장된 바이오 정보 역시 안전한 것은 아니다. 점점 더 많은 스마트폰에 생체인식 센서가 장착되고 있지만, 일부 스마트폰은 저

111) 디지털데일리, 사이버공격, 신용정보에서 생체정보 탈취로 이동, 2016.3.30

112) VOA, "미 연방 인사관리처 "560만명 지문 정보 유출"", 2015년 9월 24일, http://www.voakorea.com/a/2976925.html

113) Privacy International, "Ignoring repeated warnings, Argentina biometrics database leaks personal data", 2013년 12월 9일, https://www.privacyinternational.org/node/342

장된 바이오 정보를 안전하게 저장하지 않기 때문이다. 파이어아이 연구원들은 일부 스마트폰 종류에서 대규모로 지문을 탈취하는 것을 시연한 바 있다.(IDG Tech Report, 2015) CD/ATM에 부착된 위장 카드리더기를 통해 신용카드 번호가 무작위로 유출된 범죄가 빈번히 발생한 것과 같이 위장 바이오센서를 통해 바이오 정보를 무작위로 수집하는 범죄가 발생할 가능성도 배제할 수 없다.(윤재호 등, 2016) 이렇게 유출된 바이오 정보 혹은 생체인식 정보는 다시 판매되거나 신원 도용 등에 악용될 수 있다.

바이오 정보 유출은 경우에 따라 개인에게 치명적인 피해를 야기할 수도 있다. 예를 들어, 앞서 소개한 유엔난민고등판무관(UNHCR)이 난민 식별을 위해 생체인식 기술을 도입한 사례와 관련하여, 프라이버시 인터내셔널은 난민의 속성 상 데이터가 안전하게 보관되어야 할 필요성을 강조하고 있는데, 만일 난민들의 데이터가 본국 정부에 유출된다면, 난민들에게 비극적인 결과를 초래할 수도 있기 때문이다.(Privacy International, 2013)

아직 생체인식 정보의 실제 유출 사례는 많지 않지만, 향후 생체인식 기술의 보급 확대에 따라 유출의 가능성은 높아질 것이다. 한국은 대규모 개인정보 유출 사고를 수차례 경험한 바 있으며, 생체인식 정보 역시 예외가 될 수 없다. 생체인식 정보의 활용이 많아질수록 그 가치가 높아질 것이며, 이에 따라 생체인식 정보를 탈취하기 위한 시도도 많아질 것이다. 특히, 대규모 데이터베이스일수록 높은 가치를 가지기 때문에 해킹이나 내부자 유출의 위험성이 높아지며, 한번 유출될 경우에 피해도 커지게 된다. 따라서 가능한 한 생체인식 정보의 데이터베이스 구축을 피하고 분산·관리하는 방향으로 시스템을 설계할 필요가 있다.

[표22] 바이오 정보 유출 사례 (출처 : 금융보안원, 2016 재구성)

사고 사례	시기	주요 내용
미국 연방 인사관리처의 지문 유출	2015.6	- 중국집단의 APT공격에 의해 DB가 해킹되어 미국 전·현직 공무원의 개인정보 2,200만 건 및 지문정보 560만 건 유출 (미국 전체 인구의 약 7% 수준) - 개인 신상정보, 건강기록, 금융정보 및 퇴직관련 기록 등이 유출되어 신용정보 도용뿐만 아니라 정부부처 임직원 행세까지 가능해 미국 역사상 가장 파급력이 큰 유출사고 중 하나로 기록됨 - 미국 연방 인사관리처는 올해 1,000여 명의 사이버보안 전문가를 채용할 계획
미국 에너지국 지문정보 유출	2013.1	- 서버 14대, 워크스테이션 20대 등이 해킹되어 직원 수백 명의 개인정보, 사진 및 지문정보 유출. 중국이 공격의 배후에 있을 가능성을 제기 했지만 입증할 만한 증거는 없음
브라질 온라인 선거인명부 시스템의 사진정보 유출	2013.10	- 시스템 취약점에 대한 사전 경고에도 불구하고 취약점을 방치하여 유권자들의 사진정보가 유출 위험에 처함. 취약점이 보완될 때까지 실제 얼마나 유출되었는지는 알려지지 않음.

6) 바이오 정보의 상업적 이용과 프라이버시 침해

기업들이 상업적 목적으로 바이오 정보를 수집하거나 생체인식 기술을 활용함으로써 소비자들의 프라이버시를 침해할 우려도 높아지고 있다. 최근 빅데이터 기술이 주목을 받고 있는데, 가장 활용도가 높은 빅데이터 개인정보로 통신, 금융 정보등과 함께 의료정보가 주목을 받고 있다. IMS 헬스 코리아는 전국 약국과 병원에서 4,400만 명에 달하는 우리 국민의 건강정보 47억 건을 전국의 약국과 병원에서 사들여 빅데이터 처리한 후 제약

회사에 재판매하여 70억 원의 이득을 올렸으며, 현재 형사기소되어 재판을 받고 있다.[114] 바이오 정보 역시 빅데이터 분석을 위해 활용되거나 상업적 판매의 대상이 될 우려가 있다.

앞서 언급한 테스코의 얼굴인식 기술은 프라이버시를 둘러싼 논란을 불러일으켰는데, 프라이버시 단체들은 걷고 있는 소비자들의 얼굴을 스캔하는 것은 동의없는 정보 수집의 문제를 야기한다고 비판하며, 최소한 소비자들에게 자신들의 얼굴 및 행태 정보가 수집된다는 것을 알리고 선택권을 주어야 한다고 주장했다.[115] 이렇게 수집된 생체인식 정보의 제3자 제공 역시 소비자의 동의가 필요하다. 영리적인 목적의 생체인식 정보 수집 및 제3자 제공과 관련해서는 소비자들의 선택권을 얼마나 보장할 것인지가 관건일 것으로 보인다.

페이스북의 '이름표 추천(tag suggestion)' 기능은 내 의도와 무관하게 나에 대한 여러 정보들을 노출함으로써 프라이버시 침해 가능성이 크다. 예를 들어, 친구가 나와 찍은 사진에 내 이름이 태깅되어 있다면, 나의 친구 관계나 내가 어디에 있었는지 등이 드러나게 된다. 독일과 오스트리아를 비롯한 유럽연합 국가의 정보보호 당국은 이 기능이 프라이버시를 침해한다고 지적했고, 페이스북은 2012년 9월 유럽연합 전역에서 이 기능이 작동하지 않도록 수정했다.(구본권, 2014) 그런데 2014년 테크크런치의 보도에 의하면, 페이스북은 이 기능을 슬며시 되살린 것으로 보인다. 즉, 유럽의 페이스북 이용자라도 자신이 올린 사진 속 인물이 미국에 등록된 페이스북 이용자라면, 그 이용자가 설정에서 이 기능을 켜두었다면, 추천 기능이 작동하였다.[116]

---

114) 진보네트워크센터 등, "빅데이터 시대 소비자 권리 침해를 우려한다", 2016년 6월 30일, http://act.jinbo.net/wp/9594/

115) The Guardian, "Tesco's plan to tailor adverts via facial recognition stokes privacy fears", 2013년 11월 4일, https://www.theguardian.com/business/2013/nov/03/privacy-tesco-scan-customers-faces

7) 바이오 정보를 이용한 감시의 문제

민간 및 공공영역에서 수집, 축적된 생체인식 정보가 노동자, 시민을 감시하는 용도로 사용될 위험성도 크다.

프라이버시 인터내셔널은 정부가 시민 개개인을 엄격하게 식별하고 인증하는 것 자체가 시민에 대한 차별을 포함해서 체계적이며 광범위한 인권 침해를 가져올 수 있다고 경고하고 있다. 1930년대 독일에서의 유대인 박해, 남아프리카공화국의 인종격리정책(아파르트헤이드), 1994년 르완다 대학살 등 인종, 민족, 종교 등에 기반한 박해에 관련된 수많은 역사적 사건들은 식별 시스템을 통해 이루어졌다. (Privacy International, 2013)

국내에서도 정부가 수집, 축적하는 바이오 정보 데이터베이스를 둘러싼 논란이 계속되어 왔다. 전 국민으로부터 열손가락 지문날인을 강요하고, 경찰이 이를 전자적으로 보관하면서 범죄수사 목적으로 사용하는 것은 전 국민을 잠재적 범죄자 취급하는 것이라는 비판도 오래 전부터 제기되었다. 지문날인 제도에 대해 1999년, 2004년 헌법소원이 제기되었으나, 헌법재판소는 2005년 5월 이에 대해 합헌 결정을 내렸다.

범죄 예방을 목적으로 수집되고 있는 DNA 정보가 국가 정책에 대해 문제제기를 하다 공권력과 충돌한 시민들에 대해서도 수집되고 있는 것에 대한 비판도 제기되었다. 애초에 강력범죄 예방을 명분으로 수집되기 시작하였으나 실제 운영 과정에서는 그 범위가 확대되고 있으며, 이 과정에서 정부에 대한 비판을 위축시키는 효과를 낳고 있기 때문이다.

생체인식 기술은 민간 영역에서도 노동자 등 정보주체에 대한 감시 용도로 활용되고 있다. 예를 들어, 공공기관이나 민간업체에 활용되고 있는 출퇴근 확인용 지문인식기는 노동자를 통제하는 수단의 성격을 가지고 있다.

---

116) TechCrunch, “Euro Facebook Users Can Use Tag Suggest, For Photos Of U.S. Friends Who Have It Enabled”, 2014년 9월 2일, https://techcrunch.com/2014/09/02/facebook-has-restored-some-facial-recognition-in-europe-tagging-u-s-friends-photos/

출퇴근 확인용 지문인식기, 학생식당 지문인식기 등의 사례에서 국가인권위는 인권침해 결정을 내린바 있다.

또 한 가지 고려해야할 점은 공공기관이 수집하는 바이오 정보만 국가감시에 활용될 수 있는 것은 아니라는 점이다. 특히 정보수사기관은 필요에 따라 영장 등 일정한 요건을 갖추면 민간 업체가 보유하고 있는 개인정보에도 접근할 수 있다. 따라서 민간 영역에서의 바이오 정보 수집 증가는 궁극적으로 정부에 의해서도 사용될 수 있음을 인식해야 한다. 예를 들어, 공공기관에서 전 국민의 홍채 정보를 수집하는 것은 큰 사회적 논란을 낳을 수 있고 관련 법제도 마련 등 절차가 필요하지만, 개인의 동의에 기반한 홍채 정보가 민간에서 광범하게 수집되어 있고 필요에 따라 경찰이 이에 접근할 수 있다면 사실상 동일한 효과를 가져올 수 있기 때문이다.

따라서 개인정보 유출에 대한 우려뿐만 아니라, 국가 감시에 대한 우려를 고려할 때 중앙집중적인 방식으로 바이오 정보 데이터베이스를 운영하는 것은 매우 위험하다. 앞서 언급했던 <영구적인 라인업> 보고서에서 지적했듯이, 미국 FBI가 운전면허 DB의 사진들을 범죄수사 목적으로 검색한 것은 '무차별 감시'라고 볼 수 있다. 중앙집중적 바이오 정보 데이터베이스는 이와 같은 형태의 무차별 감시에 취약하다.

캐나다의 프라이버시 커미셔너는 개인정보, 특히 생체인식 정보를 중앙이 아니라 스마트카드와 같은 단말에 분산해서 저장해야 한다고 촉구했다. 그래야 개인들이 자신들의 생체인식 정보에 대해 보다 많은 통제권을 행사할 수 있기 때문이다. 반면, 중앙에 집적된 데이터에 대한 정보주체의 통제권은 한계가 있을 수밖에 없다. 독일 역시 2005년 생체인식 여권을 도입하면서 생체인식 데이터베이스를 생성하지 않기로 결정했다. 2013년 7월 생체인식 시스템 시범사업을 시작한 이스라엘에서도 생체인식 데이터베이스에 대한 논란이 있었다. 비판자들은 중앙집중 데

이터베이스는 수백만 이스라엘 국민들의 생체인식 정보를 도난, 남용에 취약하게 할 뿐만 아니라 국가 감시 목적에 이용될 수 있다고 우려하며, 단지 스마트 칩만으로도 목적을 달성할 수 있다고 주장했다.(Privacy International, 2013) 가능하면 정보주체 본인이 자신의 생체인식 정보를 보유하고 인증하는 방식으로 설계하는 것이 프라이버시 보호 측면에서는 바람직할 것이다.

한번 수집된 개인정보는 애초 수집 목적 외로 사용될 수 있는 가능성, 혹은 또 다른 목적으로 사용하고자 하는 욕구가 항상 존재한다. 국내 개인정보 보호법이나 국제 개인정보 보호원칙에서 '목적명확화의 원칙'을 강조하는 것도 이 때문이다. 특히, 정부가 개인정보 데이터베이스를 보유하고 있을 때에는 필요하다면 법을 제·개정해서라도 애초 수집 목적 외로 사용하고자 할 수 있다. 국내에서 이미 구축되고 있는 CCTV 통합관제센터 역시 애초 수집 목적 외로 CCTV 정보를 이용하는 것이지만, 정부는 관련법을 제정해서라도 이를 추진하고자 하고 있다. 그 자체로 보자면 비용절감과 효율성을 위한 사업으로 인식될 수도 있지만, 이와 같은 애초 수집 목적 외 활용이 증가할수록 정보주체의 권리는 형해화될 수밖에 없다.

생체인식 기술을 통한 자동화되고 은밀해진 개인식별은 감시의 위험성을 증폭시킨다. 과거에도 사람을 몰래 추적하거나, 지문을 통한 수사기법 등이 사용되어 왔지만, 유사한 것처럼 보이는 행위가 생체인식 기술과 결합한 자동화된 컴퓨터 장치를 통해 이루어질 때 개인에게 미치는 영향은 질적으로 달라질 수 있다. 사람들은 항상 얼굴을 드러내놓고 다니지만 길거리에서도 어느 정도의 익명성은 보장되었다. 그러나 CCTV에 얼굴인식 장치가 도입된다면, "사실상 우리의 얼굴이 바로 우리의 명찰"이나 마찬가지가 될 것이다.[117] 어디에든 내 신체의 일부분인 DNA와 지문이 남겨진다는 것이 과거에는 큰 문제가 아니었지만, 지금은

117) CIO Korea, "안면 인식 기술이 우려스러운 이유", 2016년 6월 26일, http://www.ciokorea.com/news/13057

나를 추적할 수 있는 정보를 흘리고 다니는 것이나 마찬가지다. 또한, 군중 속에서 경찰들이 수배 중인 범죄자를 찾는 것과 사람들의 얼굴을 자동 인식하여 데이터베이스의 수배자 사진과 매칭시키는 것은 다르다. 나도 모르게 이러한 생체인식 정보의 수집이 이루어진다는 점에서 정보주체의 통제권을 보장하기는 힘들다.

미국 FBI와 지방, 주 경찰의 얼굴인식 시스템을 조사하여, <영구적인 라인업(The Perpetual Line-Up) - 미국에서 규제되지 않는 미국의 얼굴인식 시스템> 보고서를 발표한 조지타운대학교 로스쿨 산하 프라이버시기술센터는 얼굴인식 시스템의 위험성을 분석하기 위해 다음과 같이 위험 요소를 구분하였는데[118], 이는 생체인식 시스템 전반에도 의미가 있을 것으로 보인다. (Center on Privacy&Technology at Georgetown Law, 2016)

첫째, 특정 대상에 대한 검색인가, 무차별 검색인가. (Targeted vs. Dragnet Search) 전통적인 법 원칙은 구체적인 범죄 혐의가 있는 대상에 대해 법원의 허가를 받아 수사하는 것을 기반으로 하고 있다. 무차별 검색은 범죄 혐의자가 아닌 일반인의 프라이버시를 침해하며, 또한 익명 표현의 자유도 위축시킬 수 있다.

둘째, 특정 대상에 대한 데이터베이스인가, 무차별 데이터베이스인가. (Targeted vs. Dragnet Database) 경찰청이 보유하고 있는 지문정보는 범죄자만의 것이 아니라, 모든 성인 국민들을 대상으로 하고 있다는 점에서 위험성이 더 크다. 경찰청의 수배차량 검색시스템은 전국 5,000여 개의 CCTV를 통해 차량번호를 인식하여 한 서버에서 수집하고 검색하는데, 모든 차량을 대상으로 한다는 점에서 무차별 데이터베이스나 마찬가지다. 차량번호 역시 개인정보에 해당한다고 할 때, 이러한 시스템이 허용된다면, 길거리 CCTV가 실시간으로 사람들의 얼굴을 인식하고

118) https://www.perpetuallineup.org/risk-framework

수배자 DB와 대조하는 미래를 상상하는 것도 어렵지 않을 것이다. 유전자 데이터베이스 역시 특정 범죄자를 대상으로 하고는 있지만, 정부 비판적인 집회 주최자까지 그 대상으로 하고 있다는 점에서 채취 대상에 대한 재검토가 필요하다.

셋째, 공개적인 검색인가, 은밀한 검색인가(Transparents vs. Invisible Searches). 검문을 해서 신원확인을 하는 것은 공개적인 검색이라고 볼 수 있다. 이때 당사자는 자신이 검색 당하고 있음을 알 수 있고 문제제기 할 수 있다. 그러나 디지털 기술의 발전으로 은밀한 검색 가능성이 높아지고 있다. 수배차량 검색시스템뿐만 아니라, 지방자치단체가 운영하는 '문제 차량 자동검색 시스템' 역시 당사자가 인식하지 못한 채 이루어지는 문제가 있다.

넷째, 실시간 검색인가, 사후 검색인가. (Real-time vs. After-the-Fact Searches) 실시간 위치추적과 마찬가지로 실시간 검색의 위험성이 더 크며, 이는 더 엄격한 조건 속에서 이루어져야 한다.

다섯째, 오랫동안 정착된 방식인가, 새로운 방식인가. (Established vs. Novel Use) 새로운 방식이 도입될 때는 그 영향에 대한 면밀한 검토가 필요하다. 비록 과거로부터 행해왔던 방식과 유사하더라도, 새로운 기술 시스템의 영향은 질적으로 달라질 수 있다는 점을 고려해야 한다. 예를 들어, 수사기관이 범죄자의 사진을 과거부터 보관해왔다고 하더라도, 이를 디지털화하고 얼굴인식을 통해 자동 식별하는 것은 개인의 인권에 미치는 영향이 크게 달라지기 때문이다.

현재 한국 정부, 특히 수사기관이 보유하고 있는 생체인식 정보에 대해서도 이와 같은 위험 요소에 기반하여 면밀하게 평가하고, 운영의 원칙을 정립할 필요가 있다.

나. 유전정보 활용시 문제점과 피해사례

1) DNA 신원확인정보의 개별적 활용

사건 해결을 위해 DNA 신원확인정보를 개별적으로 활용할 경우 DNA 채취 과정에서 충분한 설명에 근거한 동의(informed consent) 문제가 제기된다. 데이터베이스에 강제로 입력되는 특정 범죄자와 달리 수사 과정에서는 수사기관의 자의적 판단에 따라 사건 현장의 주변인물, 용의자 등에 대한 DNA 채취가 진행된다. 현재는 동의서를 받는 자발적 형태로 이루어지고 있으나 수사 과정이라는 특수한 상황에서 일반인들이 채취를 거부하기는 쉽지 않다. 이렇게 수집된 DNA는 현장 수거물 데이터베이스에 등록되어 사건이 해결될 때까지 보관되고 있는 것으로 보이지만 명확한 규정은 공개되지 않고 있다.

특히 용의자를 특정하기 위해 사건 현장 주변에서 많은 사람들의 DNA를 수집 분석하는 집단검색(mass screening)의 경우 방법의 적절성과 채취 범위를 둘러싸고 논란이 되고 있다. 2010년 10월 목포에서 여대생 살인사건이 발생하자 경찰은 전과자, 용의자와 주변 인물 등 1,100명의 DNA를 수집해 분석하였으나 범인을 검거하지 못했다. 집단검색의 조건과 수집된 DNA의 활용 범위에 대한 규정이 필요하다.

2) DNA 데이터베이스의 활용

가) DNA 데이터베이스의 확장

DNA데이터베이스는 입력 대상, 가족검색, 다른 데이터베이스와의 연동을 통해 확장될 수 있다. 데이터베이스 설립 논쟁 당시 입력 범위를 둘러싸고 논란이 있었는데, 데이터베이스의 적극적 옹호자들은 살인 강간과 같은 흉악범들만 입력해서는 효율적 활용이 힘들다고 주장하고 있다. 이러한 주장을 반영해 현행 디엔에이법은 11개 범죄에 대해서 DNA를 채취하고 있

다. 수사기관이 전국민의 지문과 주민등록번호를 보유하고 있는 상황에서 입력 대상 범죄가 지나치게 광범위하다는 비판이 제기되고 있다. 디엔에이법이 국회를 통과하기 전 대법원은 "디엔에이감식정보의 채취 대상 범죄의 범위가 지나치게 넓고, 수사 단계에서까지 디엔에이감식시료채취가 허용되는 문제점들을 안고 있어, 법률안과 같은 내용의 입법에는 반대"[119]한다고 밝힌 바 있다. 데이터베이스 설립 후에도 이러한 논쟁은 계속 되고 있는데, 2014년 8월 헌법재판소의 재판관 9명중 5명은 "주거침입, 재물손괴 등으로 인한 폭력행위 등 처벌에 관한 법률 위반죄의 경우는 상대적으로 죄질이 경미하고 재범의 위험성도 높다고 보기 어려우며, 재범의 위험성은 대상자의 직업과 환경, 당해 범행 이전의 행적, 그 범행의 동기, 수단, 범행 후의 정황, 개전의 정 등 여러 사정을 종합적으로 평가하여 행위자별로 판단해야 할 문제이지, 특정 범죄전력만 가지고 도식적으로 일반화할 수 있는 문제가 아니다"[120]라며 현행 법률에서 지정한 범죄 항목에 문제를 제기하기도 하였다.

입력 대상 범죄의 범위도 논란이지만 집행유예나 벌금형까지 DNA를 수집해 사망시까지 보관하는 것이 과연 적절한지도 논의가 필요하다. 검찰이 보유하고 있는 수형인등의 등록현황을 보면 전체의 60%가 벌금형이나 집행유예로 수형인 보다 오히려 많다.

범죄 현장의 DNA 신원확인정보가 데이터베이스의 신원확인정보와 맹목적중(cold hit)이 아닌 부분 일치가 나올 경우 범죄 현장의 신원확인정보는 데이터베이스 신원확인정보의 형제자매나 친족일 가능성이 있는데 이를 수사에 활용해서 용의자를 압축하는 것을 가족검색(familial searching)[121]이라

119) 대법원이 국회에 보낸 의견서 (2009. 11.9. 10쪽)

120) 「디엔에이신원확인정보의 이용 및 보호에 관한 법률 부칙」 제2조 제1항 위헌확인 (2014. 8. 28. 2011헌마28·106·141·156·326, 2013헌마215·360(병합))

121) 국내 법의학자들은 "친족검색은 부모 형제 또는 삼촌 조카와 같이 혈연관계가 있는 사람들이 혈연관계가 전혀 없는 사람들보다 대립유전자를 공유할 가능

고 한다. 친족 간에 DNA 신원확인정보를 공유하는 성격을 수사에 활용하는 것이다. 예를 들면 관련이 없는 사람은 DNA 신원확인정보 26개 중 8개를 공유하지만 형제자매는 16개를 공유한다. 가족검색을 수사에 사용할 경우 데이터베이스에 수록된 특정인의 가족 또한 평생 유전자 감시를 받게 되는데 이들은 인지나 동의 없이 수시로 수사선상에 오를 가능성이 있다. 일종의 데이터베이스의 우회적 확장이라고 할 수 있다.

이 과정에서 숨기고 싶었던 또는 알지 못했던 가족 관계가 공개될 수 있다. 사회적 가족관계와 생물학적 가족 관계는 다를 수 있는데, 입양, 혼외출생, 성씨 변경 등이 노출되게 된다. 기술적 정확성은 떨어지지만 용의자가 적다면 수사기관에서 적극 활용할 것으로 보인다. 영국의 경우 2011-2012년 사이 29건의 가계 검색을 진행한 바 있고, 우리나라 데이터베이스도 가족검색이 가능한 구조를 가지고 있다[122].

가족검색과 관련해 Y 염색체와 미토콘드리아 DNA를 분석하는 기법도 사용되고 있다. Y 염색체는 부계 유전이 되기 때문에 Y 염색체 마커를 쓰면 성씨(surname)를 알아내는데 도움이 될 수 있다. 미토콘드리아 DNA은 모계를 추적하는데 활용할 수 있다.

수사목적 이외의 확장이나 다른 신원확인 DNA 데이터베이스와의 연동도 우려사항이다. 현행 디엔에이법은 이미 수사 목적 이외의 행정적 목적으로 DNA 신원확인정보를 활용할 수 있도록 규정하고 있는데 장기적으로 현재 구축된 실종아동 데이터베이스, 향후 구축이 계획되고 있는 군대 데이터베이스와 연동될 가능성이 있다.

성이 높다는 이론을 기반으로 하며, DNA DB를 활용하여 수사적 정보를 제공하는 새로운 방법"으로 소개하고 있다. (이숭덕 외, 2011)

122)가족 중 전과자 있으면 당신 DNA도 들춰질 수 있다(한겨레 2015.9.10.) http://www.hani.co.kr/arti/society/society_general/708256.html

나) 생물학적 정보의 획득

DNA 신원확인정보는 숫자로 입력되지만 신원확인 이외의 생물적 특성을 알 수 있어 논란이 되고 있다. 다운증후군(Down syndrome), 제이콥스증후군(Jacobs syndrome), 터너증후군(Turner's syndrome), 클라인펠터증후군(Klinefelter syndrome) 등과 같은 염색체 이상의 유전질환은 디엔에이신원확인 정보만으로도 어느 정도 예측이 가능하다. 즉 DNA 프로파일링을 통해 염색체 이상의 '유전병'을 간접적으로 확인할 수 있는 것이다. 특히 차세대염기서열분석법(NGS, Next Generation Sequencing)을 이용하면 신원확인정보 이외의 생물학적 특징(피부, 머리카락, 눈의 색 등)과 질병정보 등을 얻을 수 있다. DNA 신원확인정보 자체도 평생 불변하면서 가족과 공유하는 성격으로 인해 매우 민감한 정보라고 할 수 있는데, 이것 이외에 추가적으로 유전정보를 얻을 수 있는 것이다. 이러한 형태의 정보 수집은 현행 디엔에이법에서 규정하고 있지 않으나 범죄수사에 활용되고 있다.

다) DNA 신원확인정보의 한계

DNA 신원확인정보는 일종의 위치정보로 특정한 시공간에 누군가의 생체유래물질이 있었다는 것을 말해 준다. DNA 신원확인정보가 법정에서 유일 증거로 채택된 경우도 있지만 대부분 추가적인 증거와 결합되어야 완결된 증거로서 활용이 가능하다. 또한 DNA 데이터베이스가 구축되어 활용되고 있지만 여기에 저장되지 않은 초범의 경우에는 데이터베이스로 검거할 수 없다.

DNA 프로파일링 결과에 대해서도 논란이 있는 경우가 있다. 대부분의 경우 정확성이 높지만 어떤 경우에는 동일인일 확률이 낮거나 분석이 불가능할 수 있다. DNA가 열이나 자외선 등으로 분해되거나 현장 수거물처럼 양히 극히 적은 경우 또는 여러 사람의 DNA가 혼합되어 있을 경우는 정확도가 떨어진다.

3) 군대 등에서의 활용

가) 유해 발굴 사업

6.25 전사자 신원확인 위해 유해와 유가족들의 DNA를 채취하면서 수집 목적과 맞지 않는 동의서를 사용하고 있다. 동의서 양식에 “본래 목적 외로 검사대상물을 이용하거나 타인에게 제공하는 것에 대한 동의 여부”를 포함시켜 신원확인 목적이 아닌 다른 유전자 검사를 허용하고 있다.

유해의 DNA는 국방부에서 유가족의 DNA는 훈령에 근거해서 바이오기업에 위탁하고 있다. 그러나 바이오기업에게 유가족의 DNA 검체를 제공하고 분석 결과를 받으면서도 유전정보 보호를 위한 구속력 있는 장치가 없다.

나) 전사/순직자 발생 대비 혈액 채취

국방부는 전사/순직자 발생 대비를 위해 아무런 법률적 기반 없이 93,000명의 군인 혈액 샘플을 채취 보관하고 있다. 상시 파병이나 전투가 있는 미군과 달리 한국군은 제한적으로 해외파병을 진행하고 있다. 게다가 전사/순직자의 신원확인에 어려움이 있을 경우 전사/순직자의 신체유래물질에 얻은 DNA정보와 가족들의 DNA를 분석하여 비교하면 신원확인이 확인이 가능하다. 굳이 사전에 군인들로부터 혈액을 수거해 보관할 필요가 없는 것이다. 혈액에서는 신원확인에 필요한 DNA 정보 이외에 질병 정보와 같은 다양한 유전정보를 얻을 수 있는데 당사자 몰래 채취한 혈액에서 직무적합성과 관련된 유전자 검사를 진행할 수도 있다. 개인의 DNA를 국가가 수집하기 위해서는 그 필요성과 방법 등에 대해서 충분한 사회적 논의가 필요하며 법률에 기초해서 진행되어야 한다.

법률이 없을 뿐만 아니라 동의서 양식에서도 문제가 있는데, 다양한 유전정보를 추출할 수 있는 혈액을 보관하면서도 신원확인 목적 이외로도 사용할 수 있게 하고 있다.

다. 건강관련 정보 활용시 문제점과 피해사례

건강관련 정보는 최근 '스마트 헬스케어'라는 이름아래 산업적으로 큰 주목을 받고 있다. 애플, 구글, 삼성, IBM 등 글로벌 IT 기업 대부분이 이 분야에 엄청난 투자를 하고 있으며, 주요 선진국의 국가 차원의 관심과 지원도 적극 이루어지고 있다.

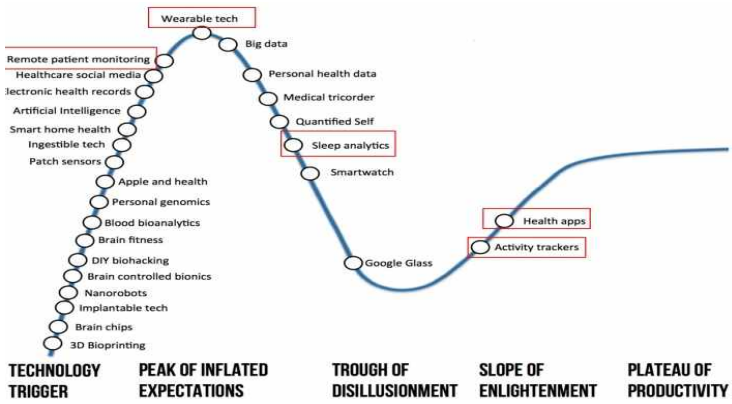
그러나 빠르게 성장하고 있는 만큼 기술적, 제도적, 사회·문화적으로 뒷받침되지 못한 지점이 많으며, 우려되는 부작용 또한 적지 않다. 우선 업계에서 홍보하는 장밋빛 전망을 쫓아가려면 기술적으로 보완해야 할 문제가 많다.

우선 지적할 수 있는 문제점은 일반적으로 웨어러블 디바이스에 대해 지나치게 과장된 사례가 많다는 것이다. 즉, 그 유용성이 크지 않음에도 불구하고 과장된 효능을 제시하는 제품들이 적지 않다. 일례로 수면 관리 웨어러블 디바이스 어플리케이션을 내놓았던 Zeo Sleep Manager가 2013년 서비스를 중단한 사례를 들 수 있다. 이 제품은 웨어러블 디바이스 분야의 선구적인 제품으로 수면의 질을 웨어러블 디바이스로 조절할 수 있다고 하여 많은 주목을 받았었다. 그러나 그 효용성에 대한 회의적인 반응이 쌓이며 결국 서비스를 중단하게 된 것이다. 최근 2016년 9월 22일자 저명한 학술지인 JAMA(Journal of the American Medical Association)에서도 임상시험 결과를 제시하며 피트니스용 웨어러블 디바이스를 사용한 체중감량에 대해 회의적인 시각을 제시한 바 있다(John M. Jakicic et al.. 2016).

그러나 이처럼 수면 관리나 피트니스 수준에서 효용성에 문제가 생긴다면 그나마 다행일 것이다. 보다 의학적인 접근을 하고 있는 웨어러블 디바이스의 경우에도 그 효용성에 의문을 제기하는 목소리는 적지 않다. 많은 웨어러블 디바이스가 주목하는 심전도 측정만 보더라도 그 유용성에 대해 의학적으로 냉정한 검토가 필요하다. 2012년 미국 예방의학 Task Force(US Preventive Services Task Force)는 예방적 심전도 측정 기준을 강화하여, 저위험 인구에서 검진 목적으로 검사를 할 필요가 없다고 권고하였다. 왜냐

하면 무증상의 저위험 성인에서 검진 목적으로 심전도를 시행하는 것이 오히려 해를 끼칠 수도 있기 때문이다. 만약 실제 병이 없는데 검사에서 이상 소견이 발견되어 불필요한, 침습적인 검사나 시술을 받게 될 수도 있는 등 과도한 스크리닝 검사에 따른 해악이 발생할 수 있다는 것이다.[123]

즉, 장밋빛 전망은 어디까지나 관련 업계의 '전망'이며, 현실적으로는 소형화, 소비 전력을 최소화 등 웨어러블 디바이스에 대한 회의적인 시각을 없앨만한 적지 않은 기술적 과제가 남아 있다. 또한 현시점만 놓고 웨어러블 디바이스 시장을 엄밀히 평가해 볼 때, 현재 많은 업체들이 웨어러블 디바이스 개발 경쟁에 뛰어들고 있는 것에 비해 혁신적 기술 개발이 이루어졌다고는 볼 수 없다. 이러한 회의적인 반응이 대두되며 웨어러블 시장은 일차 거품이 꺼지기 시작한 상황이라고 할 수 있으며, 보다 내실 있는 콘텐츠를 통해 재도약을 모색해야 하는 단계라고 보는 것이 냉정한 평가라고 할 수 있다(일본총무성 정보통신백서, 2016).



[그림 32] 웨어러블 디바이스 시장의 사이클

※ 자료 : 이제관(2015), "헬스케어 웨어러블 디바이스 적용기술 서비스 사례와 주요과제", 대한병원정보협회 발표 슬라이드.

123) 김치원, 모바일 심전도 AliveCor: 기대와 현실의 괴리, Health Business 참조(http://www.chiweon.com/alivecor/)

두 번째로는 이 웨어러블 디바이스들이 생산하는 건강관련 정보에 대한 정확성 문제이다. 조금 다른 차원의 문제이긴 하지만 최근 논란이된 fMRI 정확성 문제는 많은 시사점을 던져주고 있다. 최첨단 의료기기인 기능성자기공명영상(fMRI) 장치의 데이터 분석 소프트웨어[124]에 치명적인 버그가 있다는 사실이 15년 만에 밝혀져진 것이다. 스웨덴과 영국 공동연구진은 최근 fMRI의 결과를 분석하는 프로그램의 오류 비율이 70%에 달한다는 사실을 알게 됐으며, 이를 이용한 일부 분석 결과가 부정확했을 것이라는 내용의 연구 결과를 미국국립과학원회보(PNAS)에 발표했다. 즉, fMRI 분석 데이터에서는 문제가 있다고(활성화된다고) 표시된 뇌의 영역에서 실제로는 아무 일도 일어나지 않았을 수 있다는 것이다. 지난 15년간 이 소프트웨어를 이용한 fMRI의 분석 결과를 인용한 연구 중 일부는 무효가 될 수도 있는 것이다. 연구진에 따르면 실제 이 소프트웨어를 이용한 연구결과가 4만 건에 달하는 것으로 알려졌다.[125]

다시 말해, 인류가 만들어낸 가장 정밀한 의료기기 중 하나인 fMRI에도 이러한 오류가 나타나는데 이보다 훨씬 낮은 수준의 정밀도를 갖춘 웨어러블 디바이스가 생산하는 건강관련 정보를 어떻게 신뢰할 수 있는가 하는 문제가 제기될 수 있는 것이다.

이처럼 웨어러블 디바이스가 생산한 건강관련 정보에 대한 정확성 문제를 신중히 검토하지 않고 현재와 같이 활용성만을 강조할 경우 실제 다양한 문제들이 발생할 수 있다. 가장 기본적인 웨어러블 디바이스 기능인 체중이나 칼로리만 하더라도 사용자의 운동량 조절에 많은 영향을 끼칠 수 있다. 더 발전된 형태의 디바이스가 제공하는 심박수나 혈압, 혈당, 폐활량의 경우 작은 오차라도 건강관리에 상당한 문제를 초래할 수 있다.

---

124) 연구진이 버그를 발견한 프로그램은 fMRI 분석을 위해 세계적으로 가장 많이 쓰이는 소프트웨어 패키지(SPM, FSL, AFNI)다. 버그의 명칭은 '3dClustSim'이다.

125) http://nownews.seoul.co.kr/news/newsView.php?id=20160707601004

실제로 최근 연구에서 전세계적으로 가장 대중적인 웨어러블 디바이스인 핏빗(Fitbit)의 심박동 모니터기가 매우 부정확하다는 결과가 나오기도 했다. CNBC 보도에 따르면 심장동을 측정하는 3개 핏빗 제품을 대상으로 집단 소송을 진행하는 로펌인 Lieff Cabraser가 위임받은 연구에서 이같이 나타났다. 43명이 건강한 성인의 심박동수를 측정한 결과 핏빗 제품들이 격한 운동 동안 1분에 20회 이상까지 심박동수를 잘못 계산한다는 것을 CSPU(California State Polytechnic University) 연구팀이 발견한 것이다.[126]

애플워치에 대한 유사한 제보도 이어지고 있다. 애플워치를 차고 운동할 때 부정확한 심박측정 수치가 나온다는 것이다. 애플서포트커뮤니티에 여러 명의 애플워치 사용자들이 높은 충격을 주는 운동을 할 때 부정확한 심박수가 측정되는 사례를 제시하고 있다. 일부 사용자는 새롭게 교환을 받았음에도 똑같은 문제가 발생한다며 이 기능에 근본적인 문제를 제기하고 있다. 실제 애플워치가 적용하고 있는 기술인, 사용자 손목에 있는 혈류량의 흐름을 감지하고 분석해 심박수를 검출하는 이른 바 광혈류측정기는 근본적인 한계를 지적받아 왔다. 예를 들어 애플워치 출시 초기에 문신을 한 사람의 손목에서는 심박을 측정할 수 없다는 사실이 드러나기도 했다.[127]

일반적인 피트니스용 웨어러블 디바이스가 아닌 보다 심혈관에 특화된 웨어러블 디바이스의 경우에도 유사한 문제가 존재한다. 심장 관련 분야의 권위 학술지인 Circulation에 2010년에 실린 리뷰 논문은, 웨어러블 디바이스를 통한 부정맥 측정은 진단적 가치가 있는 부정맥이 시작되는 시점을 잡아낼 수 없으며, 짧게 지나가는 부정맥은 놓치기 쉽다고 지적했다. 또한 부정맥 발생 시 어지러워 몸을 가누지 못하는 경우가 많은데 환자가

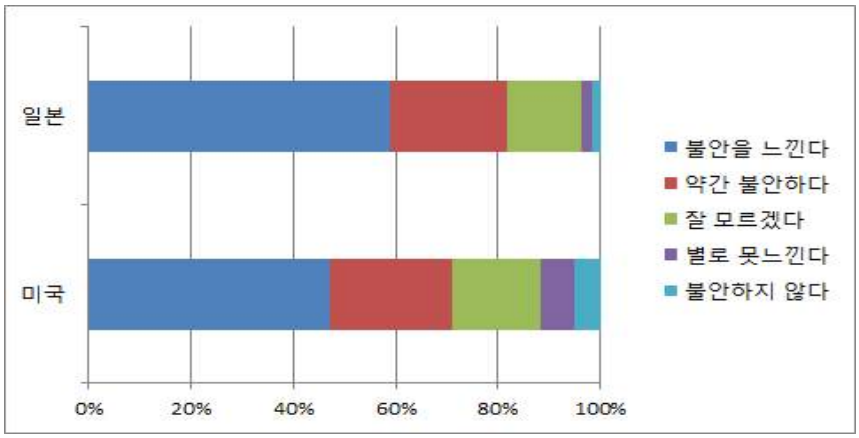
126) 한 핏빗 구매자는 오렌지에서 심박수가 측정된 사진을 올리기도 했다. http://www.telegraph.co.uk/technology/2016/05/23/fitbits-heart-rate-tracking-is-wildly-inaccurate-study-finds/

127) “애플워치 심박수 측정기능 이상… 이유는?” 2015년 10월 24일 전자신문

제대로 측정기를 작동시킬 수 있는지 의문이라고 지적했다. 실제, 심전도 측정을 위한 부착형 웨어러블 디바이스를 착용한 환자의 4분의 1이 증상 발생 시 증상이 있음을 알리는 장비를 작동시키지 못했다.

또한 당장은 아니더라도 장래에 만일 이러한 웨어러블 디바이스가 생산한 건강관련 정보가 공적으로 인정하는 정보가 될 경우 그 심각성은 더욱 커진다. 실제 비만, 고혈압, 당뇨, 부정맥 등은 보험가입 및 보험료 책정에 있어 중요하게 고려되는 문제이기에 이에 대한 우려는 결코 기우가 아니다. 이미 미국에서는 여러 제품에 보험이 적용되고 있으며, 현재 한국 정부도 시범사업이긴 하지만 만성질환관리에 웨어러블 디바이스를 사용하고 있는 만큼 이러한 문제에 대해 신중한 논의가 필요하다.

세 번째 웨어러블 디바이스가 생산하는 건강관련 정보에 대해 고려할 문제점은 바로 보안 문제이다. 웨어러블 디바이스의 개발 및 보급이 활발해 지면서 보안 위협에 대한 이슈도 떠오르고 있는데, 가장 먼저 스마트 안경이 문제로 떠올랐다. 스마트 안경을 착용하며 바라본 장면이 타인과 공유될 수 있기 때문이다. 또한 웨어러블 디바이스를 착용한 상태에서의 모든 생활 패턴 또는 민감한 개인 기록이 디바이스에 저장되어 해킹 피해가 발생할 가능성도 있다.



[그림33] 웨어러블 디바이스 사용시 느끼는 불안감(사용시 도촬/추적될 우려 등을 느끼는지)
※ 자료 : 2014년 일본총무성 정보통신백서 참조

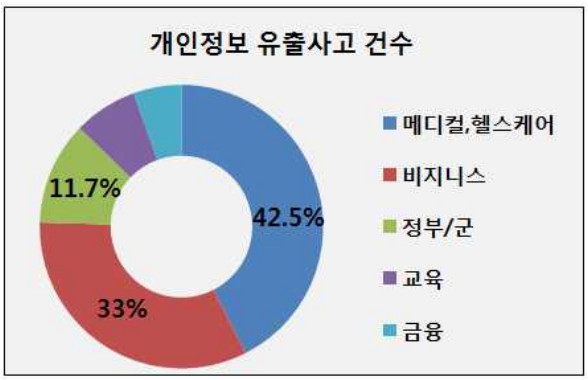
그림에서 보듯이 IT 선진국인 미국과 일본에서 웨어러블 디바이스 사용시 보안에 대해 느끼는 불안감을 조사한 결과를 보면 7-80%에 가까운 사용자들이 불안을 호소하고 있다. 정확히 건강관련 정보에 관한 조사는 아니지만 일반적으로 건강관련 정보의 보안에 대해 더 예민한 것을 고려하면 이에 대한 고민이 반드시 필요하다고 할 것이다.

실제 건강관련 정보를 생산하는 대부분의 웨어러블 디바이스 업체는 합법적이건 비합법적이건 기술상으로는 어렵지 않게 사용자의 건강관련 정보를 수집·저장할 수 있다. 대표적으로 사용자의 심전도와 활동량 등을 측정해 사용자에게 이에 대한 분석을 통해 피드백을 제공하고 있는 iRhythm은 주식상장을 위한 기업 가치를 높이기 위함인지 2016년 9월 말 발표한 보고서에서 자신들이 500,000명 이상의 환자로부터 모은 1억2천5백만 시간 이상의, 세계 최대의 부착식 심전도(ambulatory echocardiogram) 데이터를 축적하고 있다고 주장했다.[128]

128) http://medcitynews.com/2016/09/irhythm-technologies-ipo-registration/

게다가 점차 웨어러블 디바이스의 통신망을 이용한 어플리케이션 활용도가 증가하면서 해킹 위험성은 더욱 커지고 있다. 즉, 단순히 디바이스 안에서 건강관련 정보를 생성하는데 그치지 않고 이 정보를 수집하고 처리(피드백 제공 등)하는 확장된 형태의 어플리케이션을 만드는 작업으로 이어지고 있으며, 이러한 어플리케이션은 다시 애플의 Healthkit과 같은 플랫폼으로 집적되고 있다. 고객들에게 통합적인 건강관리서비스를 제공한다는 차원에서 이러한 작업은 더욱 활발해질 전망이다. 그리고 그에 따라 보안 문제는 커질 수밖에 없다.

실제 건강관련 정보는 해킹의 주요 타겟이 되고 있다. 미국의 신용도용범죄정보센터(Identity Theft Resource Center) 통계분석 보고서를 보면 2005년부터 각 분야별 데이터 침해 사고에 대해 분석하고 있는데, 데이터 침해 사고 발생 중 43.8%가 의료 관련 정보였다. 이는 2005년 이후 약 300% 가량 증가한 수치였다. 일반적으로 가장 해킹이 많을 것으로 예상하는 금융 관련 정보의 침해 사고가 3.7%인 것을 감안하면 이에 대한 대비책이 시급함을 여실히 보여주고 있다(김진숙, 2014).



[그림 34] 미국 분야별 개인정보 유출사고 현황

※ 자료 : ITRC, 2014

건강관련 정보를 수집·이용하는 웨어러블 디바이스의 정보 해킹 차원이 아니라 사용자의 건강 자체에 직접적인 영향을 줄 수 있음을 보여준 사례도 있다. 글로벌 보안 컨퍼런스 'Black-hat(블랙햇4)'에서는 2013년 7월 원격의료 기계에 대한 해킹 실험을 시연했다. 의사의 원격조정으로 체내에서 심장박동이나 인슐린 농도를 조절함으로써 생명을 유지시켜주는 체내삽입형 의료장치들의 주파수를 해킹하는 실험이 시연된 것이다. 이 시연에서 유명한 해커이자 IOActive의 보안 연구원인 바너비 잭(Barnaby Jack)은 해킹을 통해 모의 환자를 사망에 이르게 할 수 있음을 보여주었다.

미국 회계감사원(Government Accountability Office, GAO) 역시 유사한 시험을 통해 전자 의료기기의 승인 및 규제를 담당하는 FDA가 이 같은 위험성을 간과하고 있다면서 보안상 위험성을 원격의료와 관련된 웨어러블 디바이스 제품을 승인하는데 있어 기준 중 하나로 포함시키고, 사이버 안전을 관할하는 다른 정부 기관과 공조할 것 등을 권고하였다.[129]

이처럼 건강관련 정보를 수집·이용하는 제품들은 빠르게 발전하고 있는 반면 보안과 관련된 제도적 장치가 뒷받침되지 못하고 있다는 문제의식이 확산되면서 미국, 영국, 네덜란드 등에서는 시민단체를 중심으로 웨어러블 디바이스의 개인정보 유출과 프라이버시 침해를 우려하는 웨어러블 디바이스 출시 반대 운동이 추진되고 있다.[130]

이러한 분위기 속에 미국의 경우 2013년 웨어러블 디바이스의 안전성을 제고하는 '웨어러블 디바이스(어플리케이션 포함) 가이드라인'을 공포하기도 했다. 이로 인해 어플리케이션의 기능이 소비자의 건강을 위협하

129) 블랙햇 공식 홈페이지 참조(http://www.blackhat.com/)

130) 대표적으로 'Stop the Cyborgs'라는 단체가 있다. 이 단체는 웨어러블 기술을 통한 big data의 무분별한 생성과 악용, 그로인한 개인정보의 유출 및 프라이버시 침해 등의 사회문제에 대항하기 위해 생성된 시민단체로, 특히 구글 글라스가 가져온 문제점에 대해 강력히 문제제기 하고 있다.

거나 안전에 영향을 미치는 경우 FDA로부터 의료기기에 준하는 규제를 받아야 하는 조치가 취해졌다.

현재 한국은 원격의료의 준비단계라고 할 수 있는 만성질환관리 시범사업에 웨어러블 디바이스를 사용하는 등 정부 차원에서 적극적인 실용화를 추진하는 상황이다. 때문에 더더욱 이러한 보안 문제에 대해 심각히 고려해야 할 시점이라고 판단된다.

아울러 미국에서는 건강관련 정보를 수집.이용하는 여러 웨어러블 디바이스 제품들이 점차 보험 적용을 받고 있는 상황으로까지 나아가고 있는 점을 주시할 필요가 있다. 이는 전국민건강보험이 완비되지 않은 미국의 상황에서 민간보험회사들의 경쟁이 낳은 결과라고 할 수 있겠지만, 이러한 흐름은 국제적으로 영향을 끼쳐 한국에서도 민간보험회사를 중심으로 보험 적용이 시도될 수 있다. 그러나 주요 민간보험회사들이 주요 IT기업은 물론 주요 의료기관까지 거느린 대기업의 계열사인 한국의 특수성을 고려하면 건강관련 정보는 미국보다 훨씬 심각하고 복잡한 문제를 안고 있다. 따라서 단순히 글로벌 추세만을 쫓을 것이 아니라 한국의 특수성을 고려하며 위에 언급한 효용성의 문제, 정확성의 문제, 보안의 문제에 대해 인권적으로 신중히 고민할 필요가 있다.

또한 치매환자의 증가에 따라 웨어러블 디바이스나 사물인터넷을 활용하여 치매환자의 신체기능과 행동, 위치를 면밀하게 감시할 수 있는 상황으로 나아가고 있는데, 이러한 것이 개인의 프라이버시와 상충되는 지점은 없는지 그리고 이것이 치매환자 관리가 아닌 다른 목적으로 쓰일 경우 초래할 수 있는 문제 등 인권적인 측면에서 예의주시할 지점들이 결코 적지 않다.

제4장

바이오 정보 이용에 대한 시민 인식 조사 결과

제4장 바이오 정보 이용에 대한 시민 인식 조사 결과

가. 조사 목적 및 내용

바이오 정보 활용 및 보호에 대한 인식, 태도 등을 파악함으로써 정보 인권 보호를 위한 정책을 마련하고자 실시하였다.

조사 내용은 생체인식기술 사용 경험, 생체인식기술 사용에 대한 의견, 신체정보 및 건강관리 기술에 대한 의견, 의료정보 제공에 대한 의견 등으로 구성하여 시민 인식 조사를 시행하였다.

[표23] 바이오 정보 인식 조사 내용

항목	세부 내용
생체인식기술 사용 경험	생체인식기술 사용 여부 경험한 생체인식기술 생체인식기술 사용 목적
생체인식기술 사용에 대한 의견	금융거래 목적의 생체인식기술 사용 의향 출퇴근 확인용 생체인식기술 사용에 대한 의견 보안 목적의 생체인식기술 사용에 대한 의견 국가의 지문정보 수집에 대한 의견 생체인식기술을 통한 본인인증 시스템에 대한 우려
신체정보 및 건강관리 기술에 대한 의견	신체 정보 및 건강관리기술 사용 여부 수집된 신체정보 및 건강정보의 유출에 대한 우려 생체정보와 건강정보의 보호에 대한 의견
의료 정보 제공에 대한 의견	수집된 의료정보 제공에 대한 동의(제약·보험회사) 통계적·학술 목적의 의료정보 제공에 대한 동의 대가 제공시 의료정보 제공에 대한 동의

나. 조사의 설계 및 방법

시민 인식 조사는 대한민국에 거주하는 만19세 이상의 성인남여 1,000명에 대해 전화면접 조사 형식으로 진행되었다. 표본 오차는 95% 신뢰수준에 오차범위는 ±3.1%였다.

[표24] 바이오 정보 인식 조사 설계 및 방법

구 분	내 용
조 사 대 상	대한민국에 거주하는 만19세 이상의 성인 남·녀
조 사 규 모	전국에 거주하는 성인 남·녀 1,000명
조 사 방 법	구조화된 설문지를 이용한 전화면접법
피조사자 선정방법 (표본추출방법)	무작위 추출법
표 본 오 차	95% 신뢰수준에 오차범위 ± 3.1%p
조 사 기 간	9월 22일 ~ 9월 26일
자료처리방법	수집된 자료는 EDITING ⇨ CODING/PUNCHING ⇨ CLEANING의 과정을 거쳐 SPSS 통계프로그램을 이용해 처리
조 사 기 관	(주)한길리서치센타
응 답 률	10.49%

다. 응답자 특성

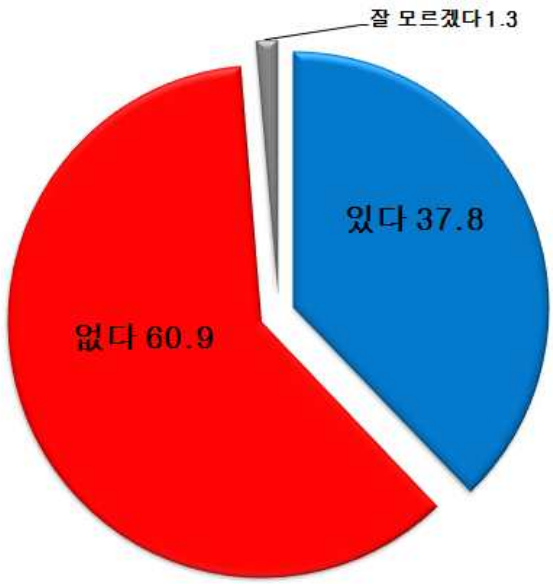
응답자의 특성은 실제 조사 결과에 가중치를 부여하여 남성, 여성, 연령대가 고르게 분포하도록 조정하였다.

[표 25] 인식 조사 응답자의 특성

		사례수	비율(%)
전체		1,000	100.0%
성별	남자	495	49.5%
	여자	505	50.5%
연령별	19세이상 20대	177	17.7%
	30대	179	17.9%
	40대	208	20.8%
	50대	199	19.9%
	60대 이상	237	23.7%
광역지역별	서울	198	19.8%
	부산/경남권	157	15.7%
	대구/경북권	101	10.1%
	인천/경기권	297	29.7%
	호남권	101	10.1%
	충청권	104	10.4%
	강원권	30	3.0%
	제주권	12	1.2%
직업별	사무직	218	21.8%
	영업직	15	1.5%
	의사/변호사 전문직	78	7.8%
	공무원/교원	21	2.1%
	판매/서비스	108	10.8%
	정보통신서비스	11	1.1%
	농/임/축/어업	30	3.0%
	생산직	25	2.5%
	학생	85	8.5%
	무직/기타	408	40.8%
인터넷 사용시간	1시간이하	397	39.7%
	1-2시간	202	20.2%
	2-3시간	128	12.8%
	3시간이상	273	27.3%

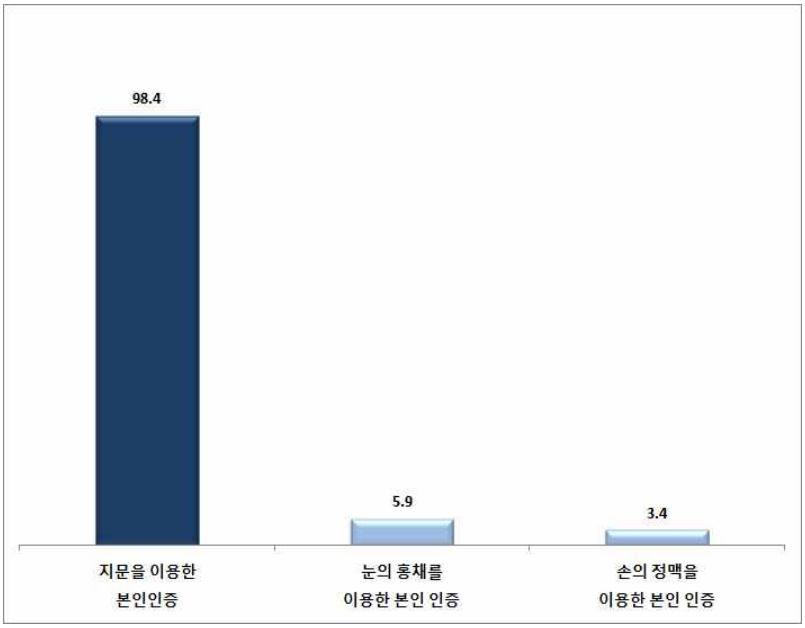
라. 조사 결과

1) 생체인식기술 사용 경험 여부



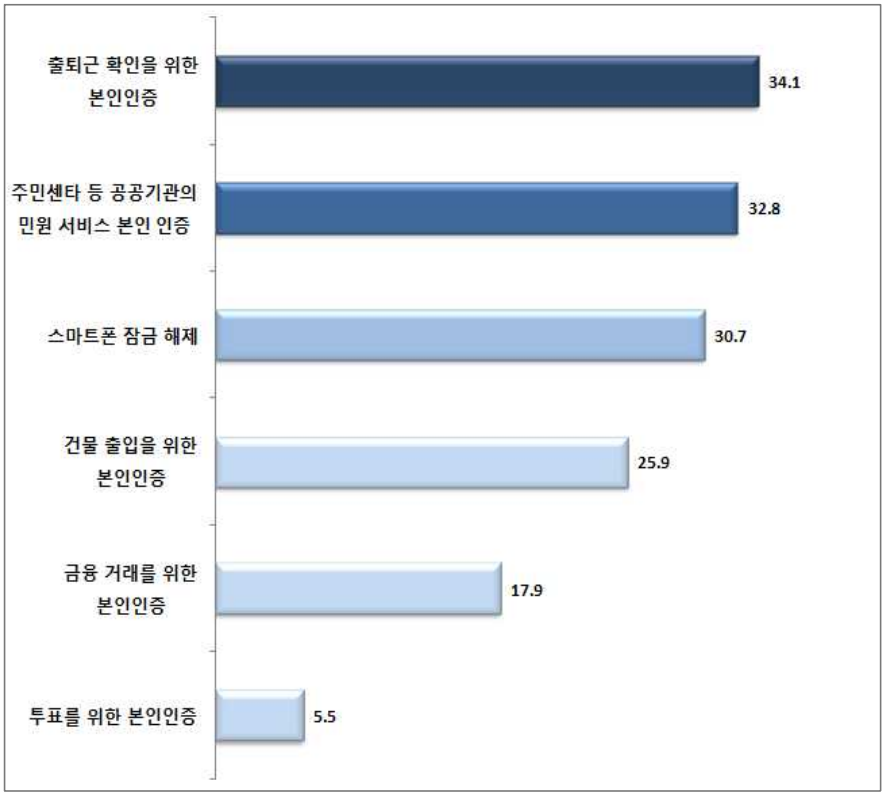
[그림 35] 생체인식기술 사용 경험

시민들은 생체인식기술 사용 경험 여부에 대하여 60.9%가 사용한 적이 없다고 응답한 반면 37.8%는 사용한 적이 있다고 응답하였다. 아직까지 다수의 시민들이 생체인식기술 사용 경험이 없음을 알 수 있다. 그러므로 이후 이루어진 생체인식기술에 대한 인식 및 태도에 대한 응답은 사용 경험이 부족한 상태에서 이루어진 점이라는 것을 고려할 필요가 있다.



[그림 36] 생체인식 기술별 사용 경험

생체인식기술을 사용한 적이 있다고 응답한 시민(N=378)들이 경험한 생체인식기술로 98.4%가 지문을 이용한 본인인증이라고 응답하였다. 다음으로는 눈의 홍채를 이용한 본인인증 5.9%, 손의 정맥을 이용한 본인인증 3.4%순이었다. 지문을 이용한 본인 인증 기술에 대한 경험이 많음을 알 수 있다.



[그림 37] 목적별 생체인식기술 사용 경험

생체인식기술을 사용한 적이 있다고 응답한 시민(N=378)들은 생체인식기술 사용 목적으로 34.1%가 출퇴근 확인을 위한 본인인증이라고 응답하였다. 다음으로는 주민센타 등 공공기관의 민원 서비스 본인 인증 32.8%, 스마트폰 잠금해제 30.7%, 건물 출입을 위한 본인인증 25.9%, 금융거래를 위한 본인인증 17.9%, 투표를 위한 본인인증 5.5% 순이었다.

2) 목적별 생체인식기술 사용에 대한 의견

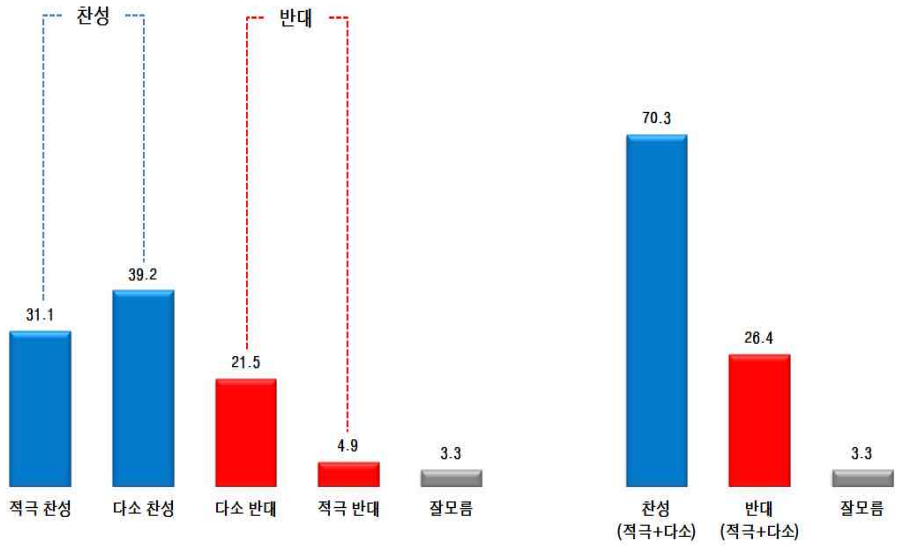
[표26] 목적별 생체인식기술 사용에 대한 의견

구분	① 적극 찬성	② 다소 찬성	①+② 찬성	③+④ 반대	③ 다소 반대	④ 적극 반대	⑤ 잘모름
금 융 거 래	14.4	34.0	48.4	44.4	27.1	17.3	7.2
출퇴근 확인	15.5	43.8	59.3	30.7	19.5	11.2	10.0
보 안 목 적	27.7	44.9	72.6	21.9	16.5	5.4	5.5

시민들의 목적별 생체인식기술 사용에 대한 의견을 물어보았다. 그 결과 금융거래 목적의 생체인식기술 사용 의향에 대해서는 44.4%가 부정적이며, 출퇴근 확인용 생체인식기술 사용에 대해서는 30.7%가 반대했으며, 보안 목적의 생체인식기술 사용에 대해서는 21.9%가 반대 의견이었다.

다른 사용 목적에 비해 금융거래 목적의 생체인식기술 사용에 대해서는 다소 조심스러운 태도를 보이고 있음을 알 수 있다. 출퇴근 확인이나 보안 목적의 사용보다는 사용 규모가 광범위하고 피해 발생시 그 규모와 심각성이 크다는 인식 때문인 것으로 생각된다.

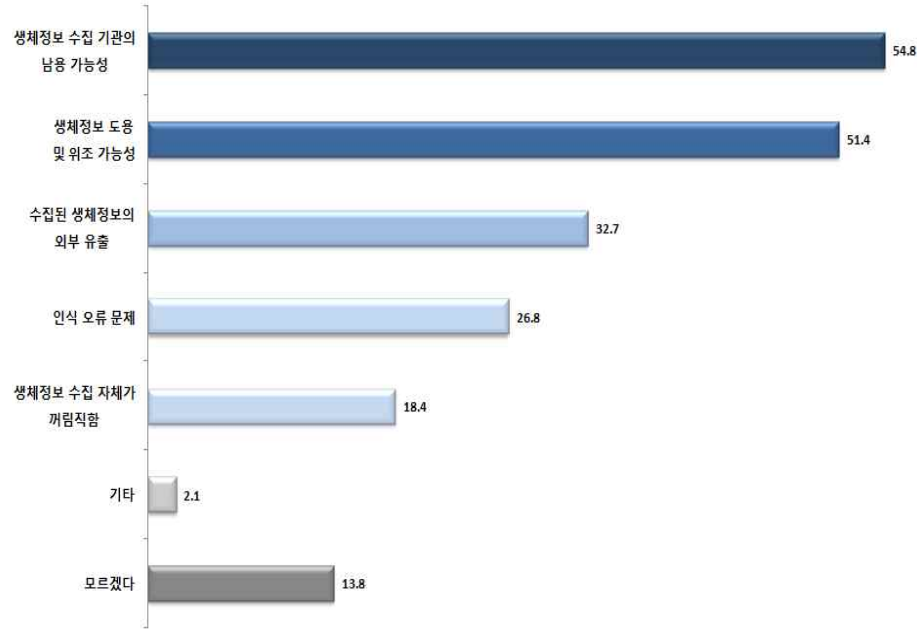
3) 국가의 지문정보 수집에 대한 의견



[그림 38] 국가의 지문정보 수집에 대한 의견

시민들은 국가의 지문정보 수집에 대한 의견에 대하여는 70.3%가 찬성한다(적극 찬성 31.1% + 다소 찬성 39.2%)고 응답한 반면, 26.4%는 반대한다(다소 반대 21.5% + 적극 반대 4.9%)고 응답하였다. 국가에 의한 지문정보 수집은 이미 오래 전부터 시행되어 온 것이기에 상대적으로 거부감이 덜한 것으로 보여진다.

4) 생체인식기술을 통한 본인인증 시스템에 대한 우려

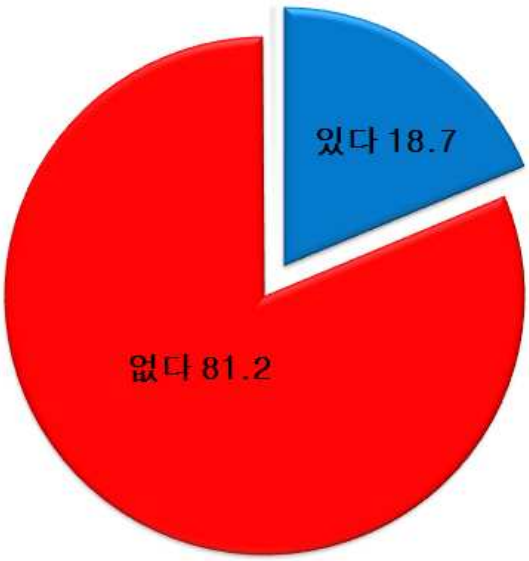


[그림 39] 생체인식기술을 통한 본인인증 시스템에 대한 우려

일반 시민들은 생체인식기술을 통한 본인인증 시스템에 대한 우려로 54.8%가 생체정보 수집 기관의 남용 가능성이라고 응답하였다. 다음으로는 생체정보 도용 및 위조 가능성 51.4%, 수집된 생체정보의 외부 유출 32.7%, 인식 오류 문제 26.8%, 생체정보 수집 자체가 꺼림칙함 18.4% 순이었다.

일반 시민들은 생체인식 기술의 활용과 관련하여 수집 기관을 신뢰할 수 없는 문제를 가장 크게 생각하고 있음을 알 수 있다. 수집 기관의 보안 수준 및 능력, 수집 기관의 불법적 사용 가능성 등에 대한 우려가 총체적으로 담겨 있다고 생각된다.

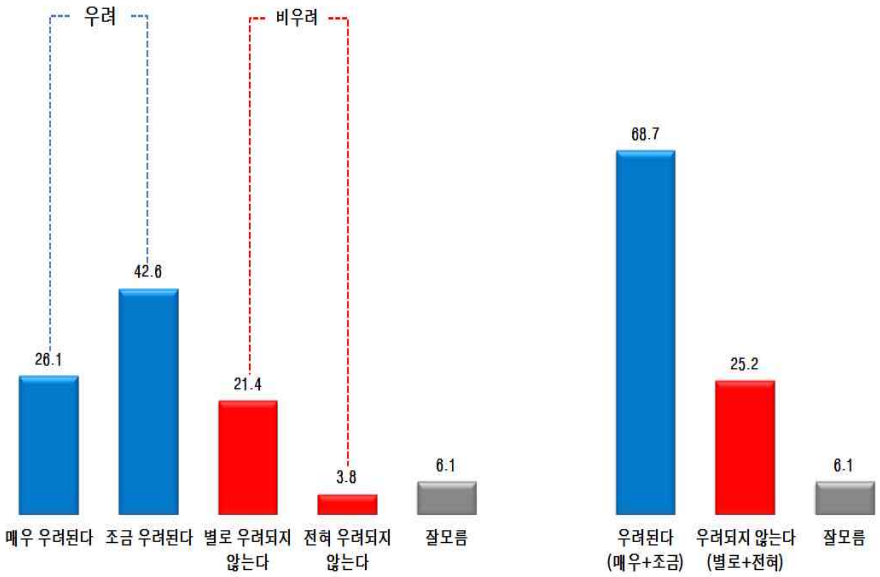
5) 신체 정보 및 건강관리기술 사용 여부



[그림 40] 신체 정보 및 건강관리기술 사용 경험

시계, 스마트폰의 어플 등을 통해 신체 정보 및 건강 정보를 측정하거나 입력하여 건강관리를 하는 기술을 이용해 본 경험이 있는지 물어보았을 때 81.2%가 없다고 응답한 반면, 18.7%만 있다고 응답하였다. 생체인식 정보 기술에 비해 더 상용화되거나 보편화되지 않은 현실임을 알 수 있다.

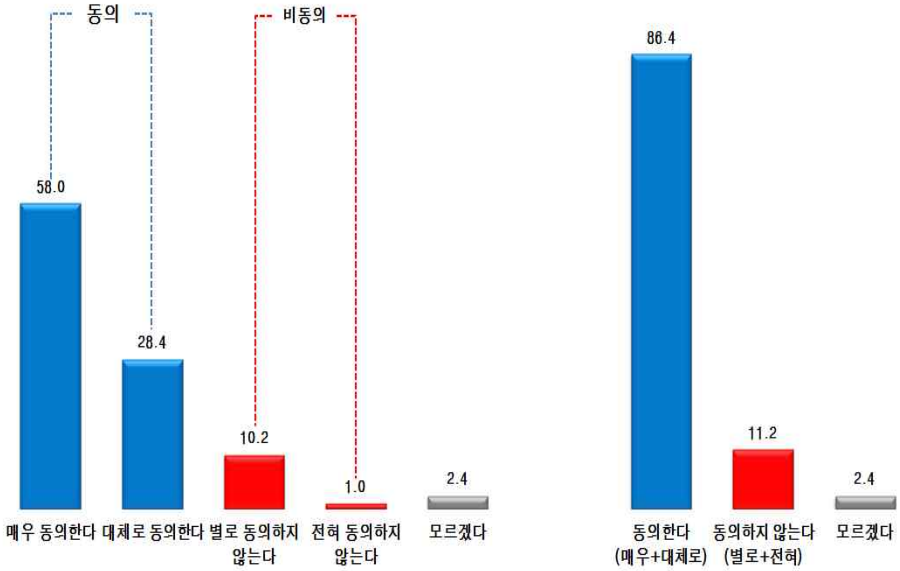
6) 수집된 신체정보 및 건강정보의 유출에 대한 우려



[그림 41] 신체정보 및 건강정보 유출 우려

시민들은 수집된 신체정보 및 건강정보의 유출 우려에 대하여 68.7%가 우려된다(매우 우려된다 26.1% + 조금 우려된다 42.6%)고 응답한 반면, 25.2%는 우려되지 않는다(별로 우려되지 않는다 21.4% + 전혀 우려되지 않는다 3.8%)고 응답하였다. 생체인식 정보에 비해 유출 우려가 더 큼을 알 수 있다. 이는 생체인식 정보에 견줘 정보 보안 및 보호에 대한 논의나 대책이 부족한 현실의 한 단면을 반영하는 것이다.

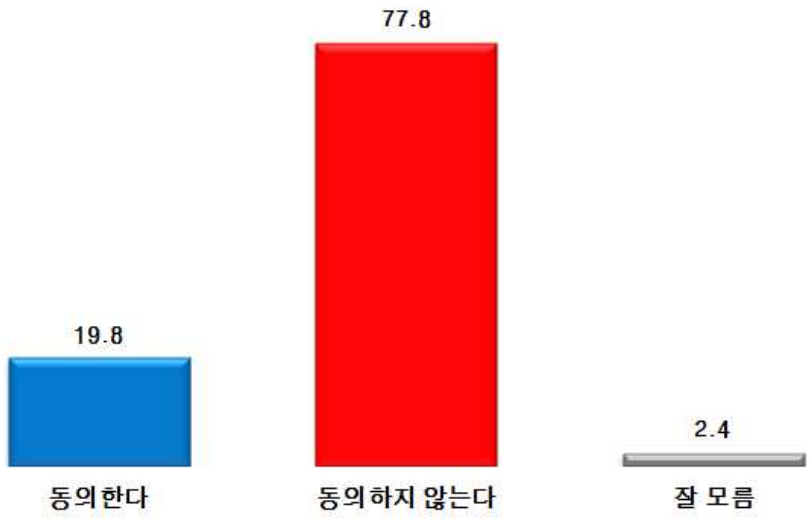
7) 생체인식 정보와 건강정보의 보호 수준에 대한 의견



[그림 42] 생체인식 정보와 건강정보 보호 수준에 대한 의견

“생체인식 정보와 건강정보는 다른 개인정보에 비해 더 엄격하게 규제되고 보호되어야 한다”는 명제에 대한 동의 여부를 물었을 때, 시민들은 86.4%가 동의한다(매우 동의한다 58.0% + 대체로 동의한다 28.4%)고 응답한 반면, 11.2%는 동의하지 않는다(별로 동의하지 않는다 10.2% + 전혀 동의하지 않는다 1.0%)고 응답하였다. 생체인식 정보와 건강정보는 다른 정보에 비해 더 철저히 관리되고 규제되어야 한다고 생각하고 있었다.

8) 수집된 의료정보 제공에 대한 동의(제약・보험회사)



[그림 43] 의료정보의 영리업체 제공에 대한 의견

시민들은 수집된 의료정보의 영리업체 제공에 대하여 77.8%가 동의하지 않는다고 응답한 반면, 19.8%는 동의한다고 응답하였다. 진료과정에서 수집된 의료정보를 영리업체에 제공하는 것에 대해서는 반대 의견이 다수임을 알 수 있다.

9) 목적별 의료정보 제공에 대한 동의(N=778)

[표 27] 목적별 의료정보 제공에 대한 의견

구 분	① 동의한다	② 동의하지 않는다	③ 잘 모름
통계·학술연구	37.8	60.1	2.1
대 가 제 공	18.7	77.5	3.8

수집된 의료정보의 영리업체 제공에 동의하지 않는 시민(N=778)들 중 통계·학술연구 목적으로의 의료정보 제공에 대하여 37.8%가 동의한 반면, 60.1%는 동의하지 않았다. 의료정보에 대한 대가 제공시 영리업체 제공하는 것에 대하여서도 18.7%만이 동의한 반면, 77.5%는 동의하지 않았다. 의료 정보의 경우는 경제적 대가 여부와 상관없이 영리업체에 제공하는 것에 반대하는 이들이 많았고, 통계, 학술목적의 의료정보 제공에 대해서도 반대하는 이들이 더 많았다. 의료 정보에 대해서는 매우 민감하게 느끼고 있다는 것을 알 수 있다.

마. 개인 특성별 세부 분석

1) 생체인식기술 사용 여부

생체인식기술 사용 여부에 대해 있다는 응답은 성별로는 남자(43.5%), 연령별로는 30대(49.6%), 만 19세 이상 20대(47.4%), 40대(45.5%), 지역별로는 서울(44.0%), 인천/경기권(44.0%), 직업별로는 의사/변호사 등 전문직(57.6%), 사무직(52.9%), 학생(49.2%)에서 상대적으로 많았다.

[표 28] 생체인식기술 사용 경험 응답표

		합계		① 있다	② 없다	③ 잘모르겠다
		%	사례수	%	%	%
전체		100.0	1,000	37.8	60.9	1.3
성별	남자	100.0	495	43.5	55.4	1.1
	여자	100.0	505	32.1	66.3	1.6
연령별	19세이상 20대	100.0	177	47.4	50.7	1.9
	30대	100.0	179	49.6	50.4	.0
	40대	100.0	208	45.5	54.5	.0
	50대	100.0	199	38.3	60.3	1.4
	60대 이상	100.0	237	14.3	82.5	3.2
광역지역별	서울	100.0	198	44.0	55.6	.4
	부산/경남권	100.0	157	32.5	65.9	1.5
	대구/경북권	100.0	101	36.9	60.2	2.9
	인천/경기권	100.0	297	44.0	55.2	.8
	호남권	100.0	101	21.2	73.5	5.3
	충청권	100.0	104	33.8	66.2	.0
	강원권	100.0	30	34.8	65.2	.0
	제주권	100.0	12	36.1	63.9	.0
직업별	사무직	100.0	218	52.9	46.8	.3
	영업직	100.0	15	45.0	55.0	.0
	의사/변호사 전문직	100.0	78	57.6	35.5	6.8
	공무원/교원	100.0	21	23.6	76.4	.0
	판매/서비스	100.0	108	32.5	65.3	2.2
	정보통신서비스	100.0	11	39.7	60.3	.0
	농/임/축/어업	100.0	30	21.1	73.9	5.0
	생산직	100.0	25	30.3	69.7	.0
	학생	100.0	85	49.2	49.5	1.3
	무직/기타	100.0	408	27.0	72.3	.7
인터넷 사용시간	1시간이하	100.0	397	26.7	70.9	2.4
	1-2시간	100.0	202	41.0	59.0	.0
	2-3시간	100.0	128	39.2	60.0	.8
	3시간이상	100.0	273	50.8	48.0	1.1
생체인식경험	있다	100.0	378	100.0	.0	.0
	없다	100.0	609	.0	100.0	.0

생체인식기술 사용 목적에 대해 출퇴근 확인을 위한 본인인증이라는 응답은 성별로는 남자(38.6%), 연령별로는 30대(39.9%), 40대(37.4%), 지역별로는 인천/경기권(48.6%), 직업별로는 영업직(80.0%), 생산직(70.7%), 정보통신서비스(54.7%)에서 상대적으로 많았다.

생체인식기술 사용 목적에 대해 공공기관 민원 서비스 본인인증이라는 응답은 성별로는 여자(40.0%), 연령별로는 60대 이상(44.4%), 50대(43.1%), 지역별로는 충청권(52.3%), 대구/경북권(38.0%), 직업별로는 판매/서비스(45.1%), 공무원/교원(36.6%)에서 상대적으로 많았다.

[표 29] 목적별 생체인식기술 사용 경험 응답표

		합계		① 금융거래를 위한 본인인증	② 건물 출입을 위한 본인인증	③ 출퇴근 확인을 위한 본인인증	④ 투표를 위한 본인인증	⑤ 스마트폰 잠금 해제	⑥ 주민센타 등 공공기관
		%	사례수	%	%	%	%	%	%
전체		100.0	378	17.9	25.9	34.1	5.5	30.7	32.8
성별	남자	100.0	215	22.2	30.5	38.6	3.1	36.5	27.3
	여자	100.0	162	12.2	19.8	28.2	8.6	22.9	40.0
연령별	19세이상 20대	100.0	84	20.7	31.8	35.5	3.4	60.6	18.2
	30대	100.0	89	15.2	22.0	39.9	4.9	42.3	32.2
	40대	100.0	95	25.1	19.8	37.4	2.1	13.8	33.8
	50대	100.0	76	10.8	29.8	32.4	4.6	15.1	43.1
	60대 이상	100.0	34	14.0	30.3	10.4	23.2	8.1	44.4
광역지역별	서울	100.0	87	12.6	25.2	34.1	6.6	40.6	24.0
	부산/경남권	100.0	51	27.4	31.0	16.9	8.6	23.9	24.0
	대구/경북권	100.0	37	26.8	16.5	23.3	.0	33.5	38.0
	인천/경기권	100.0	131	16.2	27.3	48.6	3.3	26.1	35.8
	호남권	100.0	21	16.8	22.0	34.3	22.6	24.6	28.9
	충청권	100.0	35	14.9	19.3	21.0	.0	32.2	52.3
	강원권	100.0	10	16.8	51.3	34.0	9.6	35.3	34.5
	제주권	100.0	4	23.1	34.6	.0	7.7	30.8	34.6
직업별	사무직	100.0	115	21.9	24.6	48.9	4.5	39.0	29.8
	영업직	100.0	7	20.0	15.6	80.0	.0	.0	35.6
	의사/변호사 전문직	100.0	45	23.5	40.6	51.9	.0	29.3	23.7
	공무원/교원	100.0	5	57.8	.0	30.3	.0	11.8	36.6
	판매/서비스	100.0	35	10.8	18.8	19.0	9.2	40.6	45.1
	정보통신서비스	100.0	4	45.3	.0	54.7	.0	100.0	.0
	농/임/축/어업	100.0	6	21.8	78.2	.0	.0	.0	.0
	생산직	100.0	8	.0	.0	70.7	.0	.0	29.3
	학생	100.0	42	13.0	32.2	8.3	17.3	59.1	13.4
	무직/기타	100.0	110	13.5	23.0	22.1	4.4	12.4	46.0
생체인식경험	있다	100.0	378	17.9	25.9	34.1	5.5	30.7	32.8
인터넷 사용시간	1시간이하	100.0	106	13.2	16.5	24.9	13.5	21.7	35.4
	1-2시간	100.0	83	24.7	33.6	29.4	4.7	38.2	28.8
	2-3시간	100.0	50	4.9	28.3	20.1	.0	38.2	32.5
	3시간이상	100.0	139	22.2	27.8	49.1	1.7	30.3	33.3

2) 금융거래 목적의 생체인식기술 사용 의향

금융거래 목적의 생체인식기술사용 의향에 대해 '그렇다(매우 그렇다+조금 그렇다)'이라는 응답은 성별로는 남자(53.4%), 연령별로는 만19세 이상 20대(60.6%), 40대(53.6%), 50대(53.5%), 지역별로는 서울(55.6%), 인천/경기권(51.5%), 직업별로는 공무원/교원(92.2%), 정보통신서비스(78.3%), 사무직(60.3%), 학생(58.5%)에서 상대적으로 많았다.

생체인식기술을 사용한 경험 여부에 따라 분류해 보면 사용경험이 있는 이들은 60.3%가 '그렇다'고 응답하였고, 사용경험이 없는 이들은 41.8%가 '그렇다'고 응답하였다. 상대적으로 생체인식기술을 사용한 경험이 있는 이들이 금융거래 목적의 생체인식기술 사용에도 거부감이 없는 것으로 나타났다.

[표 30] 금융거래목적의 생체인식 정보 이용에 대한 의견 응답표

		합계		① 매우 그렇다	② 조금 그렇다	①+② 그런편	③+④ 그렇지 않은편	③ 별로 그렇지 않다	④ 전혀 그렇지 않다	⑤ 잘모름/무응답
		%	사례수	%	%	%	%	%	%	%
전체		100.0	1,000	14.4	34.0	48.4	44.4	27.1	17.3	7.2
성별	남자	100.0	495	18.3	35.2	53.4	43.2	26.1	17.0	3.4
	여자	100.0	505	10.6	32.8	43.4	45.5	28.1	17.5	11.1
연령별	19세이상 20대	100.0	177	23.6	37.0	60.6	36.2	20.5	15.7	3.2
	30대	100.0	179	14.3	36.9	51.2	43.2	26.0	17.3	5.6
	40대	100.0	208	14.1	39.5	53.6	36.0	26.4	9.6	10.4
	50대	100.0	199	14.6	38.9	53.5	41.7	24.7	16.9	4.8
	60대 이상	100.0	237	7.8	20.5	28.3	60.9	35.5	25.5	10.8
광역지역별	서울	100.0	198	13.4	42.3	55.6	40.9	27.1	13.8	3.4
	부산/경남권	100.0	157	17.3	29.3	46.6	38.4	21.0	17.4	15.0
	대구/경북권	100.0	101	17.4	31.4	48.9	42.2	23.2	19.0	8.9
	인천/경기권	100.0	297	15.0	36.5	51.5	44.3	27.8	16.4	4.3
	호남권	100.0	101	15.4	28.6	44.0	47.3	30.6	16.6	8.7
	충청권	100.0	104	4.4	30.2	34.5	56.8	33.6	23.1	8.7
	강원권	100.0	30	21.8	20.0	41.8	51.2	31.1	20.1	7.0
	제주권	100.0	12	15.3	29.2	44.4	51.4	26.4	25.0	4.2
직업별	사무직	100.0	218	18.9	41.3	60.3	37.3	23.8	13.4	2.5
	영업직	100.0	15	15.9	25.8	41.7	49.3	31.2	18.1	9.0
	의사/변호사 전문직	100.0	78	27.3	28.1	55.4	40.8	22.8	18.0	3.8
	공무원/교원	100.0	21	30.6	61.6	92.2	7.8	2.5	5.3	.0
	판매/서비스	100.0	108	9.1	22.9	32.1	58.9	31.0	27.8	9.1
	정보통신서비스	100.0	11	12.0	66.3	78.3	21.7	10.9	10.9	.0
	농/임/축/어업	100.0	30	19.8	32.8	52.6	47.4	34.1	13.4	.0
	생산직	100.0	25	2.4	39.0	41.4	50.2	36.0	14.2	8.5
	학생	100.0	85	21.4	37.1	58.5	39.4	22.1	17.3	2.1
	무직/기타	100.0	408	9.0	31.2	40.2	47.8	30.2	17.6	12.0
인터넷 사용시간	1시간이하	100.0	397	10.9	27.3	38.2	49.5	30.1	19.5	12.3
	1-2시간	100.0	202	19.7	36.2	55.9	42.3	23.6	18.7	1.8
	2-3시간	100.0	128	12.3	41.7	54.0	35.7	24.0	11.7	10.3
	3시간이상	100.0	273	16.6	38.3	55.0	42.5	26.9	15.6	2.5
생체인식경험	있다	100.0	378	20.8	39.5	60.3	33.6	22.5	11.1	6.1
	없다	100.0	609	10.6	31.2	41.8	50.3	29.7	20.6	7.9

3) 출퇴근 확인용 생체인식기술 사용에 대한 의견

출퇴근 확인용 생체인식기술 사용에 대하여 '찬성한다'라는 응답은 연령별로는 만 19세 이상 20대(76.0%), 50대(67.0%), 지역별로는 서울(65.0%), 대구/경북권(64.3%), 호남권(62.4%), 직업별로는 공무원/교원(74.9%), 학생(69.8%), 의사/변호사 등 전문직(67.5%)에서 상대적으로 많았다.

생체인식기술을 사용한 경험 여부에 따라 분류해 보면 사용경험이 있는 이들은 71.8%가 '그렇다'고 응답하였고, 사용경험이 없는 이들은 52.5%가 '그렇다'고 응답하였다. 상대적으로 생체인식기술을 사용한 경험이 있는 이들이 출퇴근 목적의 생체인식기술 사용에 더 거부감이 없는 것으로 나타났다.

[표 31] 출퇴근 확인용 생체인식기술 사용에 대한 의견 응답표

		합계		① 적극 찬성	② 다소 찬성	①+② 찬성	③+④ 반대	③ 다소 반대	④ 적극 반대	⑤ 잘모름/무응답
		%	사례수	%	%	%	%	%	%	%
전체		100.0	1,000	15.5	43.8	59.3	30.7	19.5	11.2	10.0
성별	남자	100.0	495	17.4	43.0	60.4	30.5	19.8	10.7	9.1
	여자	100.0	505	13.7	44.6	58.2	30.9	19.2	11.6	10.9
연령별	19세이상 20대	100.0	177	24.6	51.4	76.0	16.2	10.8	5.4	7.8
	30대	100.0	179	14.6	43.5	58.0	38.8	22.5	16.4	3.1
	40대	100.0	208	12.9	44.2	57.1	35.4	23.6	11.8	7.5
	50대	100.0	199	17.8	49.2	67.0	28.0	18.7	9.3	5.0
	60대 이상	100.0	237	9.8	33.4	43.3	33.4	20.9	12.5	23.3
광역지역별	서울	100.0	198	16.5	48.5	65.0	30.4	21.4	9.0	4.6
	부산/경남권	100.0	157	14.9	42.0	57.0	30.1	16.3	13.8	12.9
	대구/경북권	100.0	101	15.7	48.7	64.3	20.2	11.5	8.7	15.5
	인천/경기권	100.0	297	16.6	42.0	58.6	31.0	20.7	10.4	10.3
	호남권	100.0	101	13.9	48.5	62.4	31.2	19.9	11.3	6.4
	충청권	100.0	104	14.0	40.9	54.9	36.8	20.8	16.0	8.3
	강원권	100.0	30	14.6	18.1	32.6	39.2	35.8	3.3	28.2
	제주권	100.0	12	9.7	38.9	48.6	44.4	15.3	29.2	6.9
직업별	사무직	100.0	218	13.4	46.6	60.0	38.2	27.6	10.6	1.9
	영업직	100.0	15	13.8	40.9	54.8	36.3	18.1	18.1	9.0
	의사/변호사 전문직	100.0	78	21.8	45.7	67.5	31.0	17.7	13.3	1.5
	공무원/교원	100.0	21	25.0	49.9	74.9	25.1	13.9	11.1	.0
	판매/서비스	100.0	108	13.4	36.8	50.2	39.7	18.8	20.9	10.1
	정보통신서비스	100.0	11	16.8	43.4	60.3	39.7	28.9	10.9	.0
	농/임/축/어업	100.0	30	8.6	55.0	63.6	21.3	11.9	9.4	15.1
	생산직	100.0	25	19.4	37.4	56.8	30.0	21.8	8.2	13.2
	학생	100.0	85	24.7	45.0	69.8	12.5	7.8	4.7	17.7
	무직/기타	100.0	408	13.9	42.9	56.8	28.6	18.7	9.9	14.6
인터넷 사용시간	1시간이하	100.0	397	12.3	39.8	52.0	30.6	19.6	11.1	17.3
	1-2시간	100.0	202	16.7	44.6	61.3	30.3	19.5	10.8	8.4
	2-3시간	100.0	128	21.3	45.0	66.3	32.7	17.5	15.2	1.1
	3시간이상	100.0	273	16.7	48.4	65.1	30.1	20.5	9.7	4.7
생체인식경험	있다	100.0	378	19.3	52.6	71.8	22.3	15.6	6.7	5.8
	없다	100.0	609	13.4	39.1	52.5	35.6	21.8	13.8	12.0

4) 보안 목적의 생체인식기술 사용에 대한 의견

보안목적의 생체인식기술 사용에 대하여 '찬성한다'라는 응답은 성별로는 여자(74.2%), 연령별로는 만 19세 이상 20대(84.2%), 50대(79.2%), 지역별로는 제주권(83.3%), 호남권(77.1%), 강원권(76.2%), 직업별로는 영업직(100.0%), 정보통신서비스(100.0%), 공무원/교원(88.8%)에서 상대적으로 많았다.

생체인식기술을 사용한 경험 여부에 따라 분류해 보면 사용경험이 있는 이들은 77.7%가 '그렇다'고 응답하였고, 사용경험이 없는 이들은 70.1%가 '그렇다'고 응답하였다. 보안 목적의 생체인식기술 사용과 관련해서는 생체인식기술 사용 경험 여부가 큰 영향을 미치지 않았다.

[표 32] 보안 목적의 생체인식기술 사용에 대한 의견 응답표

		합계		① 적극 찬성	② 다소 찬성	①+② 찬성	③+④ 반대	③ 다소 반대	④ 적극 반대	⑤ 잘모름/무응답
		%	사례수	%	%	%	%	%	%	%
전체		100.0	1,000	27.7	44.9	72.6	21.9	16.5	5.4	5.5
성별	남자	100.0	495	26.7	44.1	70.8	24.1	18.5	5.5	5.1
	여자	100.0	505	28.6	45.6	74.2	19.9	14.6	5.3	5.9
연령별	19세이상 20대	100.0	177	34.8	49.4	84.2	15.2	9.2	6.0	.6
	30대	100.0	179	25.3	43.7	69.0	27.1	20.6	6.5	3.9
	40대	100.0	208	28.2	42.3	70.6	25.2	21.7	3.5	4.2
	50대	100.0	199	29.3	49.9	79.2	18.3	14.7	3.6	2.5
	60대 이상	100.0	237	22.2	40.4	62.7	23.4	16.0	7.4	13.9
광역지역별	서울	100.0	198	32.1	44.1	76.1	20.3	16.9	3.4	3.6
	부산/경남권	100.0	157	25.3	45.8	71.1	17.9	11.7	6.2	10.9
	대구/경북권	100.0	101	20.1	53.1	73.2	21.2	16.6	4.6	5.5
	인천/경기권	100.0	297	30.3	42.7	73.0	22.4	18.8	3.5	4.6
	호남권	100.0	101	28.5	48.7	77.1	21.4	14.7	6.7	1.5
	충청권	100.0	104	19.9	39.0	59.0	35.7	22.3	13.4	5.3
	강원권	100.0	30	30.7	45.5	76.2	9.3	7.7	1.7	14.5
	제주권	100.0	12	34.7	48.6	83.3	16.7	4.2	12.5	.0
직업별	사무직	100.0	218	28.9	49.6	78.5	19.7	15.8	4.0	1.7
	영업직	100.0	15	44.9	55.1	100.0	.0	.0	.0	.0
	의사/변호사 전문직	100.0	78	28.2	49.4	77.7	19.4	15.1	4.3	2.9
	공무원/교원	100.0	21	26.7	62.1	88.8	11.2	11.2	.0	.0
	판매/서비스	100.0	108	30.9	42.1	73.0	18.3	15.0	3.3	8.7
	정보통신서비스	100.0	11	36.7	63.3	100.0	.0	.0	.0	.0
	농/임/축/어업	100.0	30	21.6	43.2	64.9	15.9	15.9	.0	19.2
	생산직	100.0	25	11.3	55.3	66.6	33.4	23.5	9.9	.0
	학생	100.0	85	26.9	44.8	71.7	23.1	12.1	11.0	5.2
	무직/기타	100.0	408	26.8	39.9	66.7	26.1	19.5	6.6	7.2
인터넷 사용시간	1시간이하	100.0	397	28.6	43.9	72.5	18.2	12.0	6.2	9.3
	1-2시간	100.0	202	22.9	53.1	75.9	22.4	18.2	4.2	1.6
	2-3시간	100.0	128	28.4	39.0	67.4	25.4	20.1	5.3	7.2
	3시간이상	100.0	273	29.4	43.1	72.5	25.5	20.2	5.3	1.9
생체인식경험	있다	100.0	378	31.4	46.3	77.7	18.2	14.5	3.6	4.1
	없다	100.0	609	25.4	44.6	70.1	23.5	17.4	6.1	6.5

5) 국가의 지문정보 수집에 대한 의견

국가의 지문 정보 수집에 대하여 '찬성한다'라는 응답은 성별로는 남자(72.7%), 연령별로는 만 19세 이상 20대(75.4%), 50대(74.4%), 지역별로는 강원권(82.7%), 제주권(80.6%), 부산/경남권(75.7%), 직업별로는 영업직(100.0%), 생산직(88.8%)에서 상대적으로 많았다.

국가의 지문 정보 수집 의견에 대한 찬반을 평균 인터넷 사용 시간과 관련하여 재분석하여 보면 하루 인터넷 사용 시간 평균이 1시간 이하인 이들의 찬성률이 73.3%인데 견줘, 하루 인터넷 사용 시간 평균이 3시간 이상인 이들의 찬성률은 65.1%로 다소 낮아져, 정보통신에 대한 접근성이 높은 이들이 상대적으로 국가의 지문정보 수집에 대한 반대 의견이 높은 것으로 나타났다.

[표 33] 국가의 지문정보 수집에 대한 의견 응답표

		합계		① 적극 찬성	② 다소 찬성	①+② 찬성	③+④ 반대	③ 다소 반대	④ 적극 반대	⑤ 잘모름/무응답
		%	사례수	%	%	%	%	%	%	%
전체		100.0	1,000	31.1	39.2	70.3	26.4	21.5	4.9	3.3
성별	남자	100.0	495	33.2	39.5	72.7	24.9	20.1	4.8	2.5
	여자	100.0	505	29.0	38.8	67.9	28.0	22.9	5.1	4.1
연령별	19세이상 20대	100.0	177	32.6	42.8	75.4	23.2	20.2	3.1	1.4
	30대	100.0	179	28.3	37.1	65.4	32.2	26.4	5.9	2.4
	40대	100.0	208	32.9	36.2	69.1	28.0	21.8	6.2	2.9
	50대	100.0	199	33.5	40.9	74.4	23.5	18.6	4.9	2.1
	60대 이상	100.0	237	28.5	39.2	67.7	25.6	21.0	4.6	6.7
광역지역별	서울	100.0	198	35.3	38.6	73.9	24.7	20.7	4.1	1.4
	부산/경남권	100.0	157	34.2	41.5	75.7	19.3	15.5	3.8	5.0
	대구/경북권	100.0	101	27.7	41.2	68.9	24.6	22.2	2.4	6.5
	인천/경기권	100.0	297	29.8	38.2	68.0	30.0	24.6	5.4	2.0
	호남권	100.0	101	22.5	31.5	54.1	37.6	27.4	10.1	8.4
	충청권	100.0	104	31.5	42.2	73.8	25.3	20.7	4.5	1.0
	강원권	100.0	30	35.0	47.7	82.7	17.3	15.3	2.0	.0
	제주권	100.0	12	40.3	40.3	80.6	15.3	2.8	12.5	4.2
직업별	사무직	100.0	218	32.2	41.6	73.9	24.7	19.8	4.9	1.5
	영업직	100.0	15	50.0	50.0	100.0	.0	.0	.0	.0
	의사/변호사 전문직	100.0	78	30.9	36.3	67.2	26.2	21.3	4.9	6.5
	공무원/교원	100.0	21	32.2	35.6	67.8	26.6	20.2	6.4	5.6
	판매/서비스	100.0	108	35.6	38.7	74.2	24.5	21.2	3.3	1.3
	정보통신서비스	100.0	11	15.1	15.1	30.3	69.7	40.9	28.9	.0
	농/임/축/어업	100.0	30	34.0	35.6	69.6	30.4	23.7	6.7	.0
	생산직	100.0	25	37.8	51.0	88.8	11.2	6.8	4.4	.0
	학생	100.0	85	33.3	40.7	74.0	24.7	22.8	2.0	1.2
	무직/기타	100.0	408	27.9	38.1	66.1	28.7	23.3	5.4	5.2
인터넷 사용시간	1시간이하	100.0	397	31.8	41.6	73.3	21.0	17.2	3.8	5.6
	1-2시간	100.0	202	29.5	39.0	68.5	29.6	25.1	4.6	1.9
	2-3시간	100.0	128	37.4	37.1	74.5	23.9	20.0	3.9	1.6
	3시간이상	100.0	273	28.3	36.7	65.1	33.1	25.8	7.3	1.8
생체인식경험	있다	100.0	378	31.4	40.9	72.3	26.8	22.2	4.6	1.0
	없다	100.0	609	30.9	38.2	69.2	26.4	21.3	5.0	4.5

6) 생체인식기술을 통한 본인인증 시스템에 대한 우려

생체인식기술을 통한 본인인증시스템에 대한 우려로 생체정보 수집 기관의 남용 가능성이라는 응답은 성별로는 여자(56.7%), 연령별로는 30대(62.2%), 40대(61.3%), 지역별로는 강원권(65.2%), 호남권(59.8%), 인천/경기권(58.9%), 서울(58.6%), 직업별로는 공무원/교원(75.1%), 농/임/축/어업(72.1%), 정보통신서비스(68.6%), 영업직(63.1%)에서 상대적으로 많았다.

생체인식기술을 통한 본인인증시스템에 대한 우려로 생체정보 도용 및 위조 가능성이라는 응답은 연령별로는 30대(59.7%), 40대(59.0%), 만19세 이상 20대(58.3%), 지역별로는 충청권(72.2%), 직업별로는 공무원/교원(69.2%), 사무직(62.3%), 정보통신서비스(61.4%), 학생(61.3%)에서 상대적으로 많았다.

[표 34] 생체인식기술을 통한 본인인증 시스템에 대한 우려 응답표

		합계		① 인식 오류 문제	② 생체정보위조 가능성	③ 생체정보의 외부 유출	④ 생체정보의 오남용 가능성	⑤ 수집 자체가 꺼림직함	⑥ 기타	⑦ 잘 모름
		%	사례수	%	%	%	%	%	%	%
전체		100.0	1,000	26.8	51.4	32.7	54.8	18.4	2.1	13.8
성별	남자	100.0	495	24.6	51.0	38.4	52.8	18.2	3.2	11.8
	여자	100.0	505	29.0	51.7	27.2	56.7	18.6	1.0	15.8
연령별	19세이상 20대	100.0	177	34.9	58.3	32.5	47.8	15.2	3.8	7.5
	30대	100.0	179	26.1	59.7	41.0	62.2	7.4	1.4	2.2
	40대	100.0	208	28.6	59.0	29.5	61.3	13.8	1.4	6.3
	50대	100.0	199	24.6	51.8	37.3	51.7	21.2	1.2	12.3
	60대 이상	100.0	237	21.6	33.0	25.5	51.3	30.8	2.5	35.2
광역지역별	서울	100.0	198	33.7	48.4	27.4	58.6	16.4	4.2	11.3
	부산/경남권	100.0	157	30.1	50.8	40.8	42.6	18.1	1.0	16.6
	대구/경북권	100.0	101	34.6	50.9	32.7	57.7	14.0	.0	10.1
	인천/경기권	100.0	297	28.7	49.7	30.6	58.9	16.5	1.6	13.9
	호남권	100.0	101	7.8	48.6	33.9	59.8	24.1	2.0	23.6
	충청권	100.0	104	12.5	72.2	32.2	46.0	25.3	.0	11.8
	강원권	100.0	30	35.0	37.2	42.6	65.2	12.8	.0	7.1
	제주권	100.0	12	19.4	30.6	37.5	31.9	47.2	33.3	.0
직업별	사무직	100.0	218	20.4	62.3	42.4	57.1	12.6	1.1	3.9
	영업직	100.0	15	59.1	49.3	27.8	63.7	.0	.0	.0
	의사/변호사 전문직	100.0	78	32.3	51.6	20.2	44.6	14.1	5.7	31.4
	공무원/교원	100.0	21	16.4	69.2	19.3	75.1	19.9	.0	.0
	판매/서비스	100.0	108	33.7	54.6	28.3	52.9	18.0	.0	12.4
	정보통신서비스	100.0	11	18.0	61.4	30.3	68.6	.0	21.7	.0
	농/임/축/어업	100.0	30	21.9	34.7	26.6	72.1	29.6	.0	15.1
	생산직	100.0	25	5.5	50.0	65.7	47.1	31.7	.0	.0
	학생	100.0	85	32.1	61.3	32.3	49.9	10.1	2.7	11.6
	무직/기타	100.0	408	27.5	42.8	30.5	54.4	23.7	2.2	18.9
생체인식경험	있다	100.0	378	36.0	51.2	30.8	57.0	10.2	3.1	11.8
	없다	100.0	609	21.4	52.0	34.2	54.3	23.8	1.5	12.9
인터넷사용시간	1시간이하	100.0	397	22.9	44.5	27.6	49.4	25.4	2.9	27.2
	1-2시간	100.0	202	31.2	52.0	43.9	60.5	9.0	.0	3.3
	2-3시간	100.0	128	22.7	56.2	42.5	48.6	23.1	.0	7.0
	3시간이상	100.0	273	31.2	58.7	27.2	61.3	13.0	3.4	5.2

7) 신체 정보 및 건강관리기술 사용 여부

신체정보 및 건강관리기술 사용 여부에 대하여 '있다'라는 응답은 성별로는 남자(23.1%), 연령별로는 30대(30.8%), 만 19세 이상 20대(29.9%), 지역별로는 서울(22.9%), 직업별로는 정보통신서비스(69.7%), 영업직(49.0%), 공무원/교원(31.0%), 사무직(29.9%)에서 상대적으로 많았다.

[표 35] 신체 정보 및 건강관리기술 사용 경험 응답표

		합계		① 있다	② 없다	③ 모르겠다
		%	사례수	%	%	%
전체		100.0	1,000	18.7	81.2	.1
성별	남자	100.0	495	23.1	76.9	.0
	여자	100.0	505	14.3	85.5	.2
연령별	19세이상 20대	100.0	177	29.9	70.1	.0
	30대	100.0	179	30.8	69.2	.0
	40대	100.0	208	18.7	81.3	.0
	50대	100.0	199	11.1	88.3	.5
	60대 이상	100.0	237	7.3	92.7	.0
광역지역별	서울	100.0	198	22.9	76.6	.5
	부산/경남권	100.0	157	19.8	80.2	.0
	대구/경북권	100.0	101	13.7	86.3	.0
	인천/경기권	100.0	297	17.9	82.1	.0
	호남권	100.0	101	20.7	79.3	.0
	충청권	100.0	104	17.2	82.8	.0
	강원권	100.0	30	12.5	87.5	.0
	제주권	100.0	12	4.2	95.8	.0
직업별	사무직	100.0	218	29.9	70.1	.0
	영업직	100.0	15	49.0	51.0	.0
	의사/변호사 전문직	100.0	78	19.1	80.9	.0
	공무원/교원	100.0	21	31.0	69.0	.0
	판매/서비스	100.0	108	10.4	89.6	.0
	정보통신서비스	100.0	11	69.7	30.3	.0
	농/임/축/어업	100.0	30	5.0	95.0	.0
	생산직	100.0	25	9.7	90.3	.0
	학생	100.0	85	25.3	74.7	.0
	무직/기타	100.0	408	11.8	88.0	.3
생체인식경험	있다	100.0	378	27.5	72.2	.3
	없다	100.0	609	13.6	86.4	.0
인터넷사용시간	1시간이하	100.0	397	7.5	92.5	.0
	1-2시간	100.0	202	23.9	75.6	.5
	2-3시간	100.0	128	27.1	72.9	.0
	3시간이상	100.0	273	27.0	73.0	.0

8) 수집된 신체정보 및 건강정보의 유출에 대한 우려

수집된 신체정보 및 건강정보 유출에 대하여 '우려된다(매우 우려된다+조금 우려된다)'라는 응답은 성별로는 여자(73.1%), 연령별로는 40대(76.9%), 30대(71.6%), 지역별로는 제주권(90.3%), 충청권(78.1%), 인천/경기권(73.3%), 직업별로는 생산직(84.6%), 의사/변호사 등 전문직(76.4%), 사무직(73.7%)에서 상대적으로 많았다.

[표36] 수집된 신체정보 및 건강정보의 유출에 대한 우려 응답표

		합계		① 매우 우려된다	② 조금 우려된다	①+② 우려됨	③+④ 우려안됨	③ 별로 우려되지 않는다	④ 전혀 우려되지 않는다	⑤ 잘모름/무응답
		%	사례수	%	%	%	%	%	%	%
전체		100.0	1,000	26.1	42.6	68.7	25.2	21.4	3.8	6.1
성별	남자	100.0	495	24.2	40.0	64.1	29.0	24.3	4.7	6.8
	여자	100.0	505	28.0	45.1	73.1	21.4	18.5	2.8	5.6
연령별	19세이상 20대	100.0	177	24.0	40.0	63.9	34.8	26.8	8.0	1.3
	30대	100.0	179	28.5	43.2	71.6	26.0	23.6	2.4	2.4
	40대	100.0	208	27.9	49.0	76.9	19.0	16.5	2.6	4.1
	50대	100.0	199	23.0	44.8	67.9	29.1	25.2	4.0	3.0
	60대 이상	100.0	237	26.8	36.5	63.3	19.4	16.9	2.5	17.3
광역지역별	서울	100.0	198	22.9	43.9	66.8	28.3	25.8	2.5	4.9
	부산/경남권	100.0	157	26.9	39.8	66.7	27.3	24.4	2.9	6.0
	대구/경북권	100.0	101	24.8	38.6	63.4	36.6	29.5	7.1	.0
	인천/경기권	100.0	297	26.2	47.1	73.3	19.7	15.6	4.0	7.0
	호남권	100.0	101	23.1	34.1	57.2	31.4	26.8	4.6	11.4
	충청권	100.0	104	33.1	45.1	78.1	14.6	11.8	2.8	7.2
	강원권	100.0	30	21.4	38.1	59.4	32.5	27.6	4.9	8.1
	제주권	100.0	12	52.8	37.5	90.3	5.6	5.6	.0	4.2
직업별	사무직	100.0	218	26.6	47.0	73.7	23.0	20.2	2.8	3.4
	영업직	100.0	15	13.0	40.1	53.1	46.9	36.5	10.4	.0
	의사/변호사 전문직	100.0	78	29.8	46.6	76.4	15.8	13.5	2.3	7.8
	공무원/교원	100.0	21	22.0	36.0	58.0	42.0	38.5	3.5	.0
	판매/서비스	100.0	108	30.8	40.8	71.7	21.5	15.7	5.8	6.8
	정보통신서비스	100.0	11	26.0	26.0	52.0	48.0	39.0	9.0	.0
	농/임/축/어업	100.0	30	15.9	32.2	48.1	26.1	26.1	.0	25.8
	생산직	100.0	25	34.9	49.7	84.6	11.2	11.2	.0	4.2
	학생	100.0	85	23.2	40.1	63.3	36.0	29.6	6.4	.7
	무직/기타	100.0	408	25.4	41.6	66.9	25.3	21.7	3.6	7.8
인터넷 사용 시간	1시간이하	100.0	397	23.9	40.7	64.6	24.2	20.3	3.8	11.3
	1-2시간	100.0	202	33.0	42.9	75.9	22.2	20.0	2.2	1.9
	2-3시간	100.0	128	30.0	45.1	75.0	20.3	14.7	5.6	4.7
	3시간이상	100.0	273	22.3	43.8	66.1	31.1	27.1	4.0	2.8
생체인식경험	있다	100.0	378	24.0	44.8	68.8	27.1	22.5	4.6	4.1
	없다	100.0	609	27.1	41.1	68.3	24.1	20.8	3.3	7.6

9) 생체인식 정보와 건강정보의 보호 수준에 대한 의견

“생체인식 정보와 건강정보의 보호를 더 엄격히 해야한다”는 의견에 대하여 ‘동의한다(매우 동의한다+대체로 동의한다)’라는 응답은 연령별로는 30대(93.5%), 40대(92.9%), 지역별로는 충청권(95.2%), 강원권(92.2%), 제주권(91.7%), 직업별로는 사무직(91.7%), 영업직(91.0%)에서 상대적으로 많았다.

[표37] 생체인식 정보와 건강정보의 보호 수준에 대한 의견 응답표

		합계		① 매우 동의 한다	② 대체로 동의 한다	①+② 동의 함	③+④ 동의 않음	③ 별로 동의 하지 않는다	④ 전혀 동의 하지 않는다	⑤ 잘모름/무응답
		%	사례수	%	%	%	%	%	%	%
전체		100.0	1,000	58.0	28.4	86.4	11.2	10.2	1.0	2.4
성별	남자	100.0	495	56.8	28.7	85.5	12.7	11.5	1.2	1.8
	여자	100.0	505	59.1	28.1	87.3	9.9	9.0	.9	2.9
연령별	19세이상 20대	100.0	177	50.1	31.7	81.8	17.3	15.6	1.6	1.0
	30대	100.0	179	61.2	32.3	93.5	5.7	3.9	1.9	.8
	40대	100.0	208	64.0	29.0	92.9	7.1	6.6	.5	.0
	50대	100.0	199	54.5	32.9	87.4	9.6	9.0	.5	3.1
	60대 이상	100.0	237	59.1	18.8	77.9	16.1	15.3	.7	6.0
광역지역별	서울	100.0	198	55.1	35.3	90.4	8.8	7.7	1.1	.8
	부산/경남권	100.0	157	51.9	24.1	76.0	14.5	14.0	.5	9.5
	대구/경북권	100.0	101	61.6	26.9	88.5	10.0	10.0	.0	1.5
	인천/경기권	100.0	297	57.9	30.5	88.3	10.8	9.7	1.1	.9
	호남권	100.0	101	58.0	17.4	75.5	23.8	19.9	3.9	.7
	충청권	100.0	104	66.7	28.5	95.2	3.5	3.5	.0	1.4
	강원권	100.0	30	61.7	30.4	92.2	5.8	5.8	.0	2.0
	제주권	100.0	12	72.2	19.4	91.7	8.3	8.3	.0	.0
직업별	사무직	100.0	218	58.0	33.7	91.7	8.1	6.0	2.0	.2
	영업직	100.0	15	56.4	34.6	91.0	9.0	9.0	.0	.0
	의사/변호사 전문직	100.0	78	65.1	22.4	87.4	12.6	12.6	.0	.0
	공무원/교원	100.0	21	60.8	27.1	87.8	12.2	12.2	.0	.0
	판매/서비스	100.0	108	54.6	31.7	86.3	13.1	12.6	.5	.6
	정보통신서비스	100.0	11	66.3	15.7	82.0	18.0	18.0	.0	.0
	농/임/축/어업	100.0	30	49.9	18.5	68.4	24.1	24.1	.0	7.5
	생산직	100.0	25	51.5	24.1	75.6	10.4	10.4	.0	14.0
	학생	100.0	85	46.6	30.0	76.6	23.4	21.3	2.1	.0
	무직/기타	100.0	408	60.6	26.7	87.3	8.6	7.8	.8	4.1
인터넷 사용시간	1시간이하	100.0	397	56.0	24.3	80.3	14.4	13.0	1.4	5.3
	1-2시간	100.0	202	63.6	29.2	92.8	6.2	5.9	.3	1.0
	2-3시간	100.0	128	58.5	28.0	86.5	13.1	12.2	.9	.4
	3시간이상	100.0	273	56.4	34.1	90.5	9.5	8.4	1.1	.0
생체인식경험	있다	100.0	378	57.0	30.2	87.2	11.0	9.7	1.2	1.8
	없다	100.0	609	59.4	27.6	87.0	10.4	9.5	.9	2.5

10) 의료정보의 영리업체 제공에 대한 의견

수집된 의료정보의 영리업체 제공에 대하여 '동의하지 않는다'는 응답은 성별로는 남자(79.7%), 연령별로는 30대(91.4%), 지역별로는 서울(83.6%), 인천/경기권(83.2%), 직업별로는 정보통신서비스(100.0%), 판매/서비스(86.6%), 영업직(84.0%)에서 상대적으로 많았다.

[표38] 의료정보의 영리업체 제공에 대한 의견 응답표

		합계		① 동의한다	② 동의하지 않는다	③ 잘 모름
		%	사례수	%	%	%
전체		100.0	1,000	19.8	77.8	2.4
성별	남자	100.0	495	18.2	79.7	2.1
	여자	100.0	505	21.3	76.0	2.8
연령별	19세이상 20대	100.0	177	32.5	66.2	1.3
	30대	100.0	179	8.6	91.4	.0
	40대	100.0	208	14.0	82.7	3.4
	50대	100.0	199	21.3	77.3	1.4
	60대 이상	100.0	237	22.4	72.4	5.1
광역지역별	서울	100.0	198	14.8	83.6	1.6
	부산/경남권	100.0	157	27.3	68.9	3.8
	대구/경북권	100.0	101	22.0	76.6	1.4
	인천/경기권	100.0	297	15.3	83.2	1.5
	호남권	100.0	101	24.2	72.3	3.5
	충청권	100.0	104	19.4	76.4	4.3
	강원권	100.0	30	24.9	72.7	2.4
	제주권	100.0	12	48.6	47.2	4.2
직업별	사무직	100.0	218	18.0	82.0	.0
	영업직	100.0	15	16.0	84.0	.0
	의사/변호사 전문직	100.0	78	26.3	70.6	3.1
	공무원/교원	100.0	21	16.1	83.9	.0
	판매/서비스	100.0	108	13.4	86.6	.0
	정보통신서비스	100.0	11	.0	100.0	.0
	농/임/축/어업	100.0	30	20.3	74.7	5.0
	생산직	100.0	25	25.2	74.8	.0
	학생	100.0	85	28.1	71.9	.0
	무직/기타	100.0	408	19.9	75.1	5.0
생체인식경험	있다	100.0	378	20.3	77.2	2.5
	없다	100.0	609	19.9	77.7	2.4
인터넷 사용시간	1시간이하	100.0	397	22.5	73.1	4.4
	1-2시간	100.0	202	22.3	76.5	1.2
	2-3시간	100.0	128	9.6	88.8	1.6
	3시간이상	100.0	273	18.6	80.5	.9

11) 통계적・학술 목적의 의료정보 제공에 대한 동의

수집된 의료정보의 통계·학술연구 목적으로 제공에 대하여 '동의하지 않는다'는 응답은 연령별로는 만 19세 이상 20대(75.0%), 지역별로는 충청권(80.6%), 직업별로는 학생(76.5%), 사무직(73.9%), 판매/서비스(70.9%)에서 상대적으로 많았다.

[표39] 통계적 · 학술 목적의 의료정보 제공에 대한 의견 응답표

		합계		① 동의한다	② 동의하지 않는다	③ 잘 모름
		%	사례수	%	%	%
전체		100.0	778	37.8	60.1	2.1
성별	남자	100.0	395	38.2	61.8	.0
	여자	100.0	384	37.4	58.5	4.1
연령별	19세이상 20대	100.0	117	25.0	75.0	.0
	30대	100.0	164	38.3	61.7	.0
	40대	100.0	172	35.4	63.5	1.2
	50대	100.0	154	42.3	55.4	2.2
	60대 이상	100.0	172	44.6	49.5	6.0
광역지역별	서울	100.0	166	34.0	64.8	1.2
	부산/경남권	100.0	108	51.5	48.5	.0
	대구/경북권	100.0	77	35.2	64.8	.0
	인천/경기권	100.0	247	38.5	59.4	2.0
	호남권	100.0	73	36.0	52.2	11.8
	충청권	100.0	79	19.4	80.6	.0
	강원권	100.0	22	74.9	25.1	.0
	제주권	100.0	6	35.3	64.7	.0
직업별	사무직	100.0	178	25.5	73.9	.6
	영업직	100.0	13	58.4	41.6	.0
	의사/변호사 전문직	100.0	55	41.4	58.6	.0
	공무원/교원	100.0	18	48.7	51.3	.0
	판매/서비스	100.0	94	27.9	70.9	1.1
	정보통신서비스	100.0	11	82.0	18.0	.0
	농/임/축/어업	100.0	22	51.3	34.1	14.6
	생산직	100.0	19	33.5	66.5	.0
	학생	100.0	61	23.5	76.5	.0
	무직/기타	100.0	307	46.5	50.2	3.3
생체인식경험	있다	100.0	291	38.6	61.4	.0
	없다	100.0	473	37.1	59.6	3.3
인터넷 사용시간	1시간이하	100.0	291	41.8	53.9	4.3
	1-2시간	100.0	154	36.0	64.0	.0
	2-3시간	100.0	114	31.3	68.7	.0
	3시간이상	100.0	219	37.3	61.2	1.5

12) 대가 제공시 의료정보 제공에 대한 동의

의료정보에 대한 대가 제공시 영리업체 제공하는 것에 대하여 '동의하지 않는다'는 응답은 성별로는 남자(79.7%), 연령별로는 30대(83.6%), 50대(82.0%), 지역별로는 강원권(97.2%), 제주권(88.2%), 직업별로는 생산직(100.0%), 의사/변호사 등 전문직(94.7%)에서 상대적으로 많았다.

[표40] 대가 제공시 의료정보 제공에 대한 의견 응답표

		합계		① 동의한다	② 동의하지 않는다	③ 잘 모름
		%	사례수	%	%	%
전체		100.0	778	18.7	77.5	3.8
성별	남자	100.0	395	17.7	79.7	2.6
	여자	100.0	384	19.6	75.2	5.1
연령별	19세이상 20대	100.0	117	26.5	73.5	.0
	30대	100.0	164	14.7	83.6	1.7
	40대	100.0	172	20.4	76.9	2.7
	50대	100.0	154	16.5	82.0	1.6
	60대 이상	100.0	172	17.4	70.9	11.6
광역지역별	서울	100.0	166	19.2	80.8	.0
	부산/경남권	100.0	108	35.6	58.4	5.9
	대구/경북권	100.0	77	25.1	71.1	3.9
	인천/경기권	100.0	247	15.3	82.1	2.6
	호남권	100.0	73	12.5	80.2	7.3
	충청권	100.0	79	9.2	79.8	11.0
	강원권	100.0	22	2.8	97.2	.0
	제주권	100.0	6	11.8	88.2	.0
직업별	사무직	100.0	178	10.9	87.2	1.9
	영업직	100.0	13	60.7	39.3	.0
	의사/변호사 전문직	100.0	55	5.3	94.7	.0
	공무원/교원	100.0	18	18.8	81.2	.0
	판매/서비스	100.0	94	23.5	73.9	2.6
	정보통신서비스	100.0	11	27.7	72.3	.0
	농/임/축/어업	100.0	22	22.9	64.7	12.3
	생산직	100.0	19	.0	100.0	.0
	학생	100.0	61	26.6	73.4	.0
	무직/기타	100.0	307	21.3	71.8	7.0
생체인식경험	있다	100.0	291	22.1	76.2	1.6
	없다	100.0	473	16.8	78.1	5.0
인터넷 사용시간	1시간이하	100.0	291	13.0	78.5	8.5
	1-2시간	100.0	154	18.4	79.8	1.8
	2-3시간	100.0	114	21.7	76.3	2.0
	3시간이상	100.0	219	24.8	75.2	.0

바. 시민 인식 조사 결과 요약 및 결론

조사 대상자의 61%는 생체인식기술을 사용한 경험이 없었다. 아직까지는 생체인식기술을 이용한 생체인식 정보 활용이 보편화되지 않았음을 알 수 있다.

금융거래시 생체인식기술을 활용하는 것에 대해서 시민의 44%가 반대하였다. 시민들은 다른 사용 목적에 비해 금융거래 목적의 생체인식기술 사용에 대해서 특히 조심스러운 태도를 보였다. 출퇴근 확인이나 보안 목적의 사용보다는 사용 규모가 광범위하고 피해 발생시 그 규모와 심각성이 크다는 인식 때문인 것으로 생각된다.

조사대상자의 55%가 생체인식 기술 활용시 생체인증 정보 수집 기관의 정보 남용 가능성을 우려했다. 생체인식 정보 도용 및 위조 가능성을 우려하는 시민도 51%에 달했고, 수집된 생체인식 정보의 외부 유출을 우려하는 시민도 33%에 이르렀다. 일반 시민들은 생체인식 기술의 활용과 관련하여 정보 수집 기관의 정보 보안 능력 및 의지를 가장 우려한다는 것을 알 수 있다. 도용 및 위조시 그 피해가 크고 심각하기 때문에 도용 및 위조 가능성에 대해서도 크게 우려하고 있었다.

조사 대상자의 81%가 시계, 스마트폰의 어플 등을 통해 신체 정보 및 건강 정보를 측정하거나 입력하여 건강관리를 하는 기술을 이용해 본 적이 없다고 응답하였다. 이러한 기술은 생체인식 기술에 비해 더 보편화되지 않은 상태임을 알 수 있다.

모바일 기기 등을 활용한 건강관련 정보 수집에 대해 일반 시민의 69%가 개인 건강 정보의 유출을 우려하는 것으로 조사되었다. 생체인식 정보에 견줘 모바일 기기 등을 통한 건강관련 정보 유출 위험을 더 크게 인식하고 있었다. 이는 생체인식 정보에 견줘 모바일 기기를 활용한 건강관련 정보 보안 및 보호에 대한 논의나 대책이 부족한 현실의 한 단면을

반영하는 것이다.

일반 시민의 86%는 생체인식 정보와 건강 정보는 다른 개인정보에 비해 더 엄격하게 규제되고 보호되어야 한다고 생각하고 있었다. 생체인식 정보와 건강 정보는 더욱 민감한 개인정보로 인식하고 있었다.

생체인식 기술 및 모바일 기기 등을 활용한 건강관리서비스가 보편화되지 않은 상태이지만, 일반 시민들은 이러한 서비스 활용에 필수적인 생체인식 정보 및 건강관련 정보 보호 수준에 상당한 우려를 하고 있었다. 특히 금융서비스 목적의 생체인식 정보 활용 및 모바일 기기 등을 활용한 건강관리서비스 목적의 건강관련 정보 활용에 대해 우려가 컸다.

시민들은 관련 정보 수집 기관의 정보 보호 수준에 대해 가장 큰 우려를 하고 있었고, 도용 및 위조 가능성에 대한 우려도 컸다. 일반 시민들은 생체인식 정보와 건강관련 정보에 대해서는 일반 개인정보 보호 수준보다 더 엄격한 규제와 보호를 요구했다.

제5장

바이오 정보 관련 국내외 법제도 현황

제5장 바이오 정보 관련 국내외 법제도 현황

본 연구가 대상으로 하는 바이오 정보는 개인을 식별할 수 있는 신체적, 행동적 특징에 관한 정보를 기계가 가독할 수 있도록 처리한 생체인식 정보(biometric data), DNA 유전정보(genetic data) 및 웨어러블 디바이스나 스마트기기 어플리케이션을 이용한 라이프로그(LifeLog)형 건강관련 정보(data concerning health)를 포함한다. 이들 정보는 순차적으로 한국 법제도에 포함되어 원칙적으로 규율받아 왔으나 용어와 규율 체계에 있어 통일성이 부족한 측면이 있다. 반면 유럽에서 최근 제정된 개인정보보호규정(General Data Protection Regulation)은 생체인식 정보(biometric data for the purpose of uniquely identifying a natural person), 유전정보(genetic data) 및 건강관련 정보(data concerning health)를 구분하되 같은 규범 하에서 규율하고 있다.

참고로, 진단서, 처방전, 진료기록, 전자의무기록 등 “의료제공의 필요성 여부를 판단하기 위하여 또는 의료제공을 행하기 위하여 진료 등을 통해서 얻은 환자의 건강상태 등에 관한 정보”로서 개인 진료정보(medical data)는 건강정보의 전통적인 분야로서 의료법에 의해 보호받고 있지만 본 연구에서는 다루지 않는다.

가. 국내 현황

한국 법제도에서 바이오 정보는 우선 개인정보로서 보호된다. '개인정보자기결정권'을 헌법에 열거되지 아니한 국민의 기본권으로 인정한 2005년 결정에서 헌법재판소는 개인정보를 다음과 같이 보았다.

> 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다.
>
> – 헌법재판소 2005.05.26, 99헌마513, 판례집 제17권 제1집, 668, 682

이러한 헌법적 원칙에 따라 2011년 제정된 「개인정보 보호법」은 개인정보를 다음과 같이 규정하였다.

> 「개인정보 보호법」
>
> 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
>
> 1. "개인정보"란 살아 있는 개인에 관한 정보로서 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.
>
> [2011.3.29, 제정]

연혁적으로 개인정보 보호법이 제정되기 전부터 정보통신망에서 '개인정보'에 대한 규율을 시작한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법')의 경우 일찍이 개인정보 보호법과 같은 개념으로 개인정보를 정의해 왔다. 이러한 규범 체계는 국제 개인정보 보호 규범이 규율하고 있는 개인정보의 개념이 대체로 이와 유사하다는 사실에서 유래한 것이다.

> 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
>
> 제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.
>
> 6. "개인정보"란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
>
> [1999.2.8, 전부개정]

결국 바이오 정보는 살아 있는 개인에 관한 정보로서 개인을 알아볼 수 있는 정보이기에 개인정보 보호 관련 법률들이 규율하는 개인정보에 해당하는 것이다. 직접적으로 개인을 식별할 수 있는 원본 생체정보뿐 아니라, 신체의 일부 이미지(생체영상)를 특정한 인식기술 또는 알고리즘을 이용하여 분석·추출한 특성 값으로서의 생체 특징정보 역시 간접적으로 다른 정보와 쉽게 결합하여 개인을 식별할 수 있다는 점에서 개인정보에 해당한다.

이와 같은 생체 특징정보는 원본 생체정보로부터 특징을 추출하여 수학적 포맷으로 변환한 것이므로, 개인정보에 해당하지 않거나 보호 수준이 다른 개인정보로 보일 수도 있다. 실제로 헌법재판소의 경우 「디엔에이신원확인정보의 이용 및 보호에 관한 법률」 부칙 제2조 제1항 위헌확인 사건

에서 “디엔에이신원확인정보는 단순한 숫자에 불과하고 이로부터 어떠한 개인의 유전적 특성에 대한 유전정보를 확인할 수 없고 동일인 여부의 확인기능만을 한다. 따라서 데이터베이스에 수록되는 디엔에이신원확인정보는 개인정보 누설의 염려가 적어 그 자체로 개인의 존엄과 인격권에 심대한 영향을 미칠 수 있는 민감한 정보라고 보기 어렵고, 개인식별을 위하여 필요한 사항만이 포함된 최소한의 정보라고 할 수 있다.(헌재 2014. 8. 28. 2011헌마28 등)”고 하여 원본정보보다 보호 수준이 낮은 개인정보라고 보기도 했다. 그러나 박정훈(2012)은, 생체 특징정보가 개인정보인지 여부와 관련하여 다음과 같은 이유에서 이 역시 원본정보 만큼 민감한 개인정보에 해당할 수 있다고 보았다. 첫째로, 다른 정보와 용이하게 대조함으로써 특정한 개인을 식별할 수 있을 경우에는 개인정보이다. 따라서 원본 생체정보의 특징을 템플릿화·데이터베이스화를 한 개인정보처리자가 이 특징정보를 성명·주민등록번호 등의 속성정보와 연동한 형태로 보유하고 있을 경우에는 개인정보에 해당하게 된다. 둘째로, 생체특징정보로부터 원본정보를 복원할 수 있는 가능성도 있다. 종래에는 특징정보로부터 원본정보를 복원하는 것은 불가능하다고 알려져 왔다. 그러나 최근 기술적 연구에 의해 완전한 복원까지는 불가능해도 인증시스템을 사칭할 수 있는 정도의 복원을 할 수 있다고 한다. 따라서 이러한 기술이나 능력을 가진 자에게는 특징정보도 개인정보에 해당할 가능성이 있는 것이다.

바이오 정보가 개인정보인 이상, 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 헌법상 기본권인 개인정보자기결정권에 대한 제한에 해당한다(헌법재판소, 2015). 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다. 따라서 이에 대한 제한은 법률에 의해 구체적으로 규율되어야 한다.

「개인정보 보호법」은 다음과 같이 개인정보 처리와 정보주체의 권리에 대한 원칙을 제시하고 있다.

「개인정보 보호법」

제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.

⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.

1. 개인정보의 처리에 관한 정보를 제공받을 권리

2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리

3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리

4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리

5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

개인정보의 수집·이용과 관련하여 「개인정보 보호법」은 구체적으로 개인정보를 수집하여 그 수집 목적의 범위에서 이용할 수 있는 경우를 다음과 같이 열거하고 있다. 첫째, 정보주체의 동의를 받은 경우, 둘째, 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 셋째, 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우, 넷째, 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우, 다섯째, 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우, 여섯째, 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우이고 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다(제15조 제1항).

더불어 개인정보처리자가 정보주체로부터 개인정보 수집·이용에 대한 동의를 받을 때는 ① 개인정보의 수집·이용 목적 ② 수집하려는 개인정보의 항목 ③ 개인정보의 보유 및 이용 기간 ④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 등에 대해 정보주체에게 알려야 한다(제15조 제2항).

한편 개인정보를 수집할 당시 정보주체로부터 동의받은 목적 외로 이

용하고 제공하는 것은 원칙적으로 금지된다(제18조 제1항). 그럼에도 불구하고 개인정보처리자는 다음에 열거하는 경우에 해당할 때 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 첫째, 정보주체로부터 별도의 동의를 받은 경우, 둘째, 다른 법률에 특별한 규정이 있는 경우, 셋째, 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우, 넷째, 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우, 다섯째, 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우, 여섯째, 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우, 일곱째, 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우, 여덟째, 법원의 재판업무 수행을 위하여 필요한 경우, 아홉째, 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우가 그것이다. 다만 다섯째부터 아홉째까지의 경우는 공공기관의 경우로 한정한다.

그밖에 「개인정보 보호법」은 개인정보의 열람(제35조), 개인정보의 정정·삭제(제36조), 개인정보의 처리정지 등(제37조) 정보주체의 권리도 보장하고 있다. 또한 침해소지가 높은 여권번호, 운전면허번호, 외국인등록번호 등 개인을 고유하게 구별하기 위하여 부여된 고유식별정보(제24조)와 주민등록번호의 처리(제24조의2)는 원칙적으로 제한된다.

한편 「개인정보 보호법」은 개인정보 영향평가를 규정하고 있다(제33조). 공공기관의 경우, 대통령령으로 정하는 기준에 해당하는 개인정보파일의

운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(영향평가)를 하고 그 결과를 행정자치부장관에게 제출하여야 한다.

이때 대통령령으로 정하는 기준은 ① 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일 ② 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일 ③ 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일 ④ 법 제33조제1항에 따른 개인정보 영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일의 변경된 부분 등이다(동법 시행령 제35조).

행정자치부장관이 위 영향평가 결과에 대하여 의견을 제시하려면 개인정보 보호위원회의 심의·의결을 거쳐야 한다(동법 제3항). 그러나 개인정보보호위원회는 개인정보 영향평가기관이 2014년 3월 현재 11개 기관에 불과하는 등 영향평가 제도가 현재 가지고 있는 문제점을 지적한 바 있다[131]. 2015년 7월 24일 개정시행된 「개인정보 보호법」은 '개인정보 침해요인 평가'규정을 신설하였다(동법 제8조의2). 중앙행정기관의 장은 소관 법령의 제정 또는 개정을 통하여 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우에는 개인정보 보호위원회에 개인정보 침해요인 평가를 요청하도록 하고, 요청을 받은 보호위원회는 해당 법령의 개인정보 침해요인을 분석·검토하여 그 법령의 소관기관의 장에게 그 개선을 위하여 필요한 사항을 권고할 수 있도록 한 조항으로서, 이 조항이 실질적인 평가 제도로서 기능할 수 있을지 지켜볼 필요가 있다.

131) 개인정보보호위원회, "2016 년도 개인정보보호 시행계획 의결 건" 결정, 2015. 4. 27.

바이오 정보와 관련하여 주목해서 살펴볼 조항은 민감정보 관련 조항이다. 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보나 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 정보로서 동법 시행령에 의해 규정된 유전정보, 범죄경력자료 등이 민감정보에 해당되어 그 처리가 제한된다.

민감정보를 특별히 보호하는 규정을 두게 된 이유는 다음과 같다. 개인정보는 개인의 사생활 더 나아가서는 개인의 생명·신체·재산상 안전에 중대한 영향을 미칠 수 있으므로 모두 신중하게 다루어야 하지만, 특히 사회적 차별을 야기하거나 현저히 인권을 침해할 우려가 있는 민감한 개인정보는 보다 엄격히 보호되어야 한다(행정안전부, 2011: 142p).

유럽연합의 경우 개인정보보호지침(95/46/EC)에 의해 1995년부터 특정 범주의 정보 처리(The processing of special categories of data) 조항을 두고 민감정보를 보호해 왔다. 유럽연합 제29조 개인정보보호 작업반[132]은 민감정보를 특별히 보호하는 이유에 대하여 “잘못 사용되었을 경우 일반적인 ‘보통’ 개인정보에서보다 프라이버시권이나 차별받지 않을 권리 등 개인의 기본적 권리에 심각한 결과를 초래할 수 있기 때문”이라고 설명하였다. 특히 건강이나 성정체성에 관한 정보는 그것이 공개되는 등 잘못 사용되었을 경우 그 피해를 회복할 수 없고 개인에게는 물론 그의 사회활동에도 장기간에 걸친 영향을 끼칠 것이라고 보았다. 이러한 이유에서 유럽연합은 그 속성상 민감한 정보를 처리하는 것은 다른 개인정보에 비하여 특별한 조치와 조건에 의해 이루어져야 한다고 보았다. 예를 들어 환자정보를 상업적으로 이용하는 등 프라이버시 침해로부터 건강정보를 보호하기 위해서는 특별한 조치가 취해져야 하는 것이다(Article 29 Data

132) 제29조 개인정보보호 작업반(Article 29 Data Protection Working Party)은 개인정보 보호에 전문화된 유럽연합의 자문기구로서(The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data), 유럽연합 개인정보보호지침(95/46/EC) 제29조에 의하여 설치되었다.

Protection Working Party, 2011).

우리 「개인정보 보호법」에서도 라이프로그(LifeLog)형 건강관련 정보나 유전정보의 경우 원칙적으로 민감정보로 분류되어 보호받는다. 건강·유전정보가 그 처리에 있어 특별한 보호가 필요한 이유는 이러한 정보가 본인의 신체에 각인된 고유한 개인정보이기 때문이다. 만약 이런 정보가 정보주체의 명확하고 추가적인 동의 없이 타인에게 공개될 경우 심각한 사생활의 침해를 가져올 수 있으며, 한번 공개된 정보는 변경 또는 교체로 회복하는 것이 현실적으로 불가능하다는 점에서 보호의 필요성이 더 크다(이한주, 2014).

「개인정보 보호법」

제23조(민감정보의 처리 제한) ①개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. [개정 2016.3.29]

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우

2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

「개인정보 보호법」

제18조(민감정보의 범위) 법 제23조 각 호 외의 부분 본문에서 “대통령령으로 정하는 정보”란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.

1. 유전자검사 등의 결과로 얻어진 유전정보
2.「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보

한편, 생체인식 정보도 다음과 같은 이유에서 원칙적으로 민감한 성격을 가진다. 첫째, 교환이 불가능한 정보이다. ID·패스워드 등은 누설된 경우에 변경할 수 있지만, 얼굴·지문·홍채 등을 간단히 바꿀 수는 없다. 이 같은 생체인식 정보의 성질로 인해 보안확보를 목적으로 이용할 경우 기밀성(confidentiality)·완전성(integrity) 및 가용성(availability)을 담보할 수 있어 향후에 더욱 보급이 확대될 것은 분명하다. 둘째, 부가적인 정보가 추출될 우려를 배제할 수 없다. 예를 들어 얼굴 화상으로부터 인종·건강상태·정신상태 등 본인인증과는 무관한 정보가 추출되어 이용될 위험도 있다. 셋째, 무의식중에 정보가 취득되기 쉽다. 특히, 얼굴 화상의 경우 현재의 정보환경을 고려할 때 본인이 의식하지 않는 사이에 원격시스템을 통해 간단히 취득할 수 있다(박정훈, 2012). 유럽연합 제29조 개인정보보호 작업반 역시 위 2011년 의견서에서 유전정보와 생체인식 정보의 포함을 지지하였다.

그러나「개인정보 보호법」은 모든 생체인식 정보를 민감정보로서 포함하고 있지 않다. 예를 들어 지문은 개인의 고유성, 동일성을 나타내고 정보주체를 타인으로부터 식별가능하게 하는 개인정보이지만(헌법재판소, 2005), 현행 개인정보 보호법에서는 민감정보로 규율되고 있지 않다. 또 민족 또는 인종적 기원을 드러낼 수 있는 유전정보는 민감정보로서 보호받고 있지만, 국제 규범에서 통상 민감정보로서 보호하고 있는 민족 또는 인종적 기원에 대한 보호를 우리 법률은 명시하고 있지 않다. 어플리케이션이나 기기 등으로 수집되는 개인정보 또한 모두가 건강정보는 아닐 수 있다. 다만 진료정보인 경우이거나 직접적으로나 간접적으로 건강 상태나 위험에 대해 판단할 수 있는 원본 감지

정보인 경우, 혹은 건강상태나 건강위험에 대한 결론을 도출하는 경우는 민감정보에 포함되는 건강관련 정보로서 보호될 수 있을 것이다.

한편, 본인인증수단으로서 생체인식 정보에 대한 수집 및 이용이 증가하면서 일부 법률들이 생체인식 정보에 대해 규정하고 구체적인 규율 대상에 포함하기 시작하였다.

우선 전자서명 및 전자거래 관련 법률들에서는 다음과 같이 '생체정보'를 규정하고 있다(밑줄은 필자, 이하 같음).

「전자서명법」

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

13. "개인정보"라 함은 생존하고 있는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향·영상 및 생체특성 등에 관한 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

[2001.12.31, 전문개정]

「전자금융거래법」

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

10. "접근매체"라 함은 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 다음 각 목의 어느 하나에 해당하는 수단 또는 정보를 말한다.

라. 이용자의 생체정보

[2006.4.28, 제정]

(구)정보통신부는 특별히 '바이오 정보보호 가이드라인'을 제정하여 더욱 명확히 생체인식 정보를 보호하고자 하였다(정보통신부, 2007). 단, 2005년 11월 29일 먼저 제정된 '생체정보보호 가이드라인'과 달리 생체인식 정보에 대한 명명을 '바이오 정보'로 하였다.

바이오 정보보호 가이드라인

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. "바이오 정보"라 함은 지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함한다.

[2007. 9. 제정]

특히 2009년 정보통신망법 시행령은 정보통신망에서 생체인식 정보가 송수신되는 경우 그 기술적·관리적 보호조치를 규정하는 차원에서 '바이오 정보'에 대한 규정을 포함하였다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제15조(개인정보의 보호조치) ④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.

1. 비밀번호의 일방향 암호화 저장
2. 주민등록번호, 계좌정보 및 바이오 정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다) 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장

[2014.11.28, 일부개정]

이처럼 여러 법률이 생체인식 정보를 '생체정보' 혹은 '바이오 정보'로 서로 다르게 규정하여 흩어져서 규율하고 있다는 사실은 그 용어와 규범체계상의 통일이 필요하다는 점을 역설한다. 더불어 정보통신망법 시행령에서 주의 깊게 살펴보아야 할 점은, 바이오 정보가 비밀번호와 함께 본래 일방향 암호화의 대상이었으나 '생체인식 정보 활용'을 위해 2014년 11월 그 보호 수준을 완화하였다는 사실이다. 이로써 생체인식 정보를 처리하는 개인정보 처리자 혹은 이 정보를 제공받은 제3자는 생체인식 정보의 암호를 복호화하여 이용하는 것이 가능해진 것이다.

위 법률들을 종합적으로 살펴보면, 바이오 정보는 일반적으로 개인정보로서의 성격을 가지기 때문에, 개인정보 보호에 관한 제반 규정들이 적용된다. 즉 개인정보의 수집·이용·제공에 관한 원칙적 규정 및 개인정보의 기술적·관리적 보호조치 등 제반 개인정보 보호규정들이 바이오 정보에도 동일하게 적용된다. 건강관련 정보나 유전정보 등 일부 정보의 경우에는 민감정보로서 규율된다.

다만, 특수한 영역에서 사용되는 생체인식 정보의 경우, 해당 영역 특별법들이 우선적으로 적용된다. 앞서도 살펴보았던 「전자금융거래법」, 「전자서명법」, 정보통신망법 시행령 외에도, 지문의 경우 「주민등록법」, 「여권법」, 「인감증명법」, 「형의 실효 등에 관한 법률」, 「경범죄 처벌법」, 「실종아동등의 보호 및 지원에 관한 법률」에 따라 국가 행정에서 요구되는 때가 있으며(심우민, 2016 참조), 유전정보의 경우 「디엔에이신원확인정보의 이용 및 보호에 관한 법률」, 「실종아동등의 보호 및 지원에 관한 법률」에서 요구되는 때가 있다.

주목할 점은 이들 바이오 정보의 처리가 예외적으로 인정되는 경우도 있다는 점이다. 통계작성 및 학술연구 목적으로 사용할 경우 개인정보 보호법의 다음 조항에 의해 정보주체에게 별도의 동의를 받지 않아도 익명화한 후 사용할 수 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.

4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우

2005년 제정된 생명윤리 및 안전에 관한 법률(이하 '생명윤리법')에서는 인체유래물과 유전정보를 규율하고 있는데, 인간대상연구를 할 때 인체유래물의 처리와 관련하여 다음과 같이 익명 처리의 원칙을 규정하고 있다.

「생명윤리 및 안전에 관한 법률」

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

11. "인체유래물"(人體由來物)이란 인체로부터 수집하거나 채취한 조직·세포·혈액·체액 등 인체 구성물 또는 이들로부터 분리된 혈청, 혈장, 염색체, DNA(Deoxyribonucleic acid), RNA(Ribonucleic acid), 단백질 등을 말한다.
14. "유전정보"란 인체유래물을 분석하여 얻은 개인의 유전적 특징에 관한 정보를 말한다.
17. "개인식별정보"란 연구대상자와 배아·난자·정자 또는 인체유래물의 기증자(이하 "연구대상자등"이라 한다)의 성명·주민등록번호 등 개인을 식별할 수 있는 정보를 말한다.
18. "개인정보"란 개인식별정보, 유전정보 또는 건강에 관한 정보 등 개인에 관한 정보를 말한다.
19. "익명화"(匿名化)란 개인식별정보를 영구적으로 삭제하거나, 개인식별정보의 전부 또는 일부를 해당 기관의 고유식별기호로 대체하는 것을 말한다.

제18조(개인정보의 제공) ① 인간대상연구자는 제16조제1항에 따라 연구대상자로부터 개인정보를 제공하는 것에 대하여 서면동의를 받은 경우에는 기관위원회의 심의를 거쳐 개인정보를 제3자에게 제공할 수 있다.

② 인간대상연구자가 제1항에 따라 개인정보를 제3자에게 제공하는 경우에는 익명화하여야 한다. 다만, 연구대상자가 개인식별정보를 포함하는 것에 동의한 경우에는 그러하지 아니하다.

제38조(인체유래물등의 제공)

② 인체유래물연구자가 제1항에 따라 인체유래물등을 다른 연구자에게 제공하는 경우에는 익명화하여야 한다. 다만, 인체유래물 기증자가 개인식별정보를 포함하는 것에 동의한 경우에는 그러하지 아니하다.

제43조(인체유래물등의 제공)

② 인체유래물은행의 장은 인체유래물등을 타인에게 제공하는 경우에는 익명화하여야 한다. 다만, 인체유래물 기증자가 개인식별정보를 포함하는 것에 동의한 경우에는 그러하지 아니하다.

제44조(인체유래물은행의 준수사항)

② 인체유래물은행이 제38조제1항 및 제53조제1항에 따라 인체유래물등을 제공받은 경우에는 익명화하여야 한다.

④ 인체유래물은행의 장은 보건복지부령으로 정하는 바에 따라 인체유래물등의 익명화 방안이 포함된 개인정보 보호 지침을 마련하고, 개인정보 관리 및 보안을 담당하는 책임자를 지정하여야 한다.

생명윤리법에서 '익명화'(匿名化)란 매우 핵심적인 인체유래물의 보호수단이고, 그 방법은 개인식별정보를 영구적으로 삭제하거나, 개인식별정보의 전부 또는 일부를 해당 기관의 고유식별기호로 대체하는 것이다(제2조제19호). 그런데 개인식별정보의 전부 또는 일부를 기관의 고유식별기호로

대체한다는 것은, 이 정보가 해당 기관에서 보유한 고유식별기호와 결합하면 개인이 식별되는 상태라는 의미이다. 이는 「개인정보 보호법」에서 '다른 정보와 쉽게 결합하여 개인을 식별할 수 있는 정보'도 개인정보로서 보호하고 있다는 점과 큰 차이를 보인다. 「개인정보 보호법」은 익명화를 '특정 개인을 알아볼 수 없는 형태', 즉 직간접적으로 더 이상 개인정보로 규정할 수 없는 상태로서 규정하고 있다(제18조 제2항 제4호). 특히 빅데이터 시대에는 가명 등 비식별화 처리를 하였더라도 다른 데이터셋을 결합하는 경우 개인의 식별 가능성이 매우 높아진다. 이런 상황에서 대체 등 특정한 방법으로 처리하였다는 이유로 민감한 개인정보에 대한 보호조치를 다한 것으로 간주하는 생명윤리법의 접근방식은 다소 위험하다 아니할 수 없다.

나. 해외 현황

1) 유럽

가) 일반 원칙

유럽에서 그간 개인정보 처리에 있어 가장 주요하게 간주되어 온 기준은 1995년 유럽연합 개인정보보호지침이다(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 이하 '95/46/EC 지침'). 그밖에 유럽인권협약(European Convention on Human Rights)에서도 제8조에서 개인정보 보호를 규정하고 있으며 유럽인권재판소는 이 협약에 따른 판결을 통해 건강 정보를 규율해 왔다.

유럽인권협약[133)]

제8조(사생활 및 가족생활을 존중받을 권리)

1. 모든 사람은 그의 사생활, 가정생활, 주거 및 통신을 존중받을 권리를 가진다.

2. 법률에 합치되고, 국가안보, 공공의 안전 또는 국가의 경제적 복리, 질서유지와 범죄의 방지, 보건 및 도덕의 보호, 또는 다른 사람의 권리 및 자유를 보호하기 위하여 민주사회에서 필요한 경우 이외에는, 이 권리의 행사에 대하여는 어떠한 공공당국의 개입도 있어서는 아니된다.

133) 번역문 : 미네소타 대학 인권도서관.
http://hrlibrary.umn.edu/instree/K-z17euroco.html

2008년 12월, 유럽인권재판소는 위 협약에 따라 영국의 피의자 DNA 데이터베이스에 대하여 인권침해를 결정하였다. 당시 영국에서는 경찰이 유죄판결이 확정되지 않은 피의자의 지문, DNA 프로필과 세포 샘플을 수집하여 무기한 보관하고 있었다. 유럽인권재판소는 피의자 개인정보의 무차별적 보관은 사생활에 대한 권리 침해라고 보았다.

유럽은 지문, 디지털사진, 홍채와 같은 생체인식 정보는 물론 세포 샘플 역시 개인을 식별하는 개인정보로 보고 있다. 이와 관련하여 95/46/EC 지침은 오랫동안 규율해 왔는 바, 관련 조항을 아래에서 주요하게 살펴보기로 한다.

우선 건강에 대한 정보(information on health)는 일반 개인정보보다 한층더 보호되어야 할 '특별한 범주의 정보 처리'(SPECIAL CATEGORIES OF PROCESSING)에서 규정하고 있다. 이 규정은 우리 법률을 비롯한 국제 규범에서 통상 민감정보(sensitive personal data)로 분류하고 있는 범주의 개인정보에 대한 보호를 다루고 있다. 제8조 제1항은 민감정보의 보호 대상과 보호 방법을 열거하고 있고 제2항과 제3항은 예외적인 적용제외 사유를 열거하고 있다.

유럽연합 개인정보보호지침(95/46/EC)

제8조 (특별한 범주의 정보 처리)

1. 회원국은 민족 또는 인종적 기원, 정치적 성향, 종교 또는 철학적 신념, 노동조합 회원자격이 나타나는 개인정보의 처리를 금지하여야 하고, 그리고 건강 또는 성생활에 관련된 정보의 처리를 금하여야 한다.
2. 다음 각 호에 해당하는 경우에는 제1항의 규정을 적용하지 아니한다.
   (a) 정보주체가 당해 정보의 처리에 명백하게 동의를 한 경우. 다만, 회원국의 법이 제1항에서 정한 금지가 정보주체의 동의에 의하여 해제되지 않는다고 규정하는 경우에는 제외한다.

(b) 고용법 분야와 관련하여, 관리자의 의무와 특정권리를 수행할 목적에 필요한 처리가 적절한 보호조건을 규정한 국내법에 의하여 수권된 경우

(c) 정보주체가 신체적 또는 법적으로 동의를 할 수 없는 경우 정보주체 또는 다른 사람의 중대한 이익을 보호하기 위하여 필요한 처리의 경우

(d) 정치적, 철학적, 종교적 또는 노동조합의 목적을 수행하는 재단, 사단 또는 기타 비영리단체에게 적절하게 보장된 정당한 활동의 과정에서 수행되는 처리. 다만, 단체의 회원 또는 당해 단체의 목적과 관련한 정규적인 접촉을 가지는 사람에 관련된 처리에 한하고, 정보가 정보주체의 동의가 없이는 제3자에게 공개되지 않을 것을 조건으로 한다.

(e) 정보주체에 의하여 공공연히 공개된 정보에 관한 처리 또는 소송의 제기, 소송의 수행 또는 소송의 방어에 필요한 처리

3. 정보의 처리가 예방의학, 의학적 진단, 의료보호 또는 치료의 제공 또는, 건강관리 서비스의 운영 등의 목적을 위하여 요구되는 정보의 처리의 경우, 그리고 국내법과, 직업적 비밀유지의 의무가 있는 국가의 관할 기관 또는 동등한 비밀유지 의무가 있는 기타의 자(者)에 의하여 제정된 규칙에 따라 보건을 위한 전문적 동기에 의하여 정보가 처리되는 경우에는 제1항은 적용하지 아니한다.

4. 회원국은 실질적 공익을 위하여 적절한 보호조건을 규정할 것을 조건으로 하여 국내법 또는 감독기관의 결정에 의하여 제2항에서 정한 것 이외의 적용면제 사항을 정할 수 있다.

5. 범죄, 범죄의 평결 또는 보안조치와 관련한 정보의 처리는 공공기관의 통제하에서만 가능하고, 적절한 특정의 보호조건이 국내법에 규정되어 있다면 적절한 특정의 보호조건을 규정한 국내규정에 따라 회원국은 예외를 인정할 수 있다. 그러나 범죄의 평결에 관한 등록부는 공공기관의 통제하에서만 유지할 수 있다.

회원국은 행정적 제재 또는 민사사건의 판결과 관련한 정보를 공공기관의 통제하에서 처리하도록 규정할 수 있다.

6. 제4항과 제5항에 규정된 제1항의 예외 사항은 위원회에 통지되어야 한다.

7. 회원국은 국내 신원증명번호 또는 일반적으로 적용되는 기타 신분증이 처리될 수 있는 조건을 결정하여야 한다.

민감정보의 처리와 일반 개인정보의 처리가 다른 점은 '계약 관계'가 적법한 처리를 위한 일반적인 근거로는 간주되지 않는다는 점이다(European Union Agency for Fundamental Rights·Council of Europe, 2014 : 87p). 만일 민감정보가 정보주체와의 계약에서 처리될 수 있으려면, 이들 정보의 이용에는 계약체결에 대한 합의에 더하여, 별개의 명시적인 동의가 요구된다. 민감정보를 나타내는 물품이나 서비스에 대한 정보주체의 명시적인 요청은 명시적인 동의와 같은 것으로 간주된다. 예를 들어 항공편을 예약하려는 탑승객이 항공사에 휠체어와 유대교식 식사를 요청한다면, 항공사는 건강 및 종교적 신념을 드러내는 정보의 처리에 대한 별도의 동의 없이도 이 정보를 처리할 수 있다.

결국 개인정보가 민감정보이건 아니건 정보주체의 동의가 필요하며 특히 민감정보의 경우 그 동의가 명시적이야(explicit) 적법한 것이다. 다만 정보주체가 비정상적인 위험에 처하거나 소송 등으로 정보주체가 공개한 경우 예외를 인정받는다. 또한 민감정보건 아니건 정보주체의 중대한 이익을 위해서는 처리될 수 있다. 민감정보의 경우 정보주체가 의식불명이거나 부재중이어서 연락이 불가능하여 의사결정을 위한 질문이 불가능할 경우가 이에 해당한다.

타인의 정당한 이익으로 간주되어 정보주체의 동의 없이 민감정보를 처리할 수 있는 경우로는, 정보주체가 신체적 또는 법적으로 동의를 할 수 없는 경우, 고용법과 관련하여 특별히 위험한 작업장에서 건강정보를 처리하거나 휴일 등 종교적 신념과 관련한 정보를 처리하는 경우, 정치적, 철학적, 종교적 또는 노동조합의 목적을 수행하는 재단, 단체 또는 기타 비영리 단체가 회원이나 후원자, 관련 조직에 대한 정보를 처리하는 경우(이 정보는 그 자체로 정보주체의 종교적이거나 정치적 신념을 드러낸다는 점에서 민감하다), 법률에 따라 법원이나 행정기관이 소송을 제기, 수행하거나 방어하기 위해 처리하는 경우 등이 해당한다. 이 가운데 고용법과 관련하여

적법하게 민감정보를 처리하려면 사용자가 노동자나 구직자에게 건강 상태에 대한 자료를 직접 요청해야 한다. 고용적합성 평가, 예방의학적 요건 충족, 사회적 급여의 제공 등을 위해서는 건강검진을 실시할 수 있다. 특히 건강정보는 정보주체가 명확하게 인지할 수 있도록 설명 후 동의(informed consent)를 받은 경우이거나 국내법이 허용하고 있는 경우를 제외하고는, 노동자 자신에게서 직접 수집해야 한다(European Union Agency for Fundamental Rights·Council of Europe, 2014 : 172p).

95/46/EC 지침 제8조 제3항의 경우 의료제공자가 진단, 치료를 위해 건강정보를 처리하는 경우 예외로 규정하고 있다. 특별한 보호조건에 따라 '의료제공자'로 간주되는 개인은 특별한 직업적 비밀유지 의무의 적용을 받는다. 또 제8조 제4항의 경우 개인정보가 실질적 공익을 위하여 처리되고, 국내법 또는 감독기관의 결정에 의해 제공되고, 국내법 또는 감독기관이 정보주체의 이익을 효과적으로 보호할 수 있는 충분한 보호조건을 보장한 경우에 예외적으로 처리될 수 있다고 보았다. 그에 대한 예로서는 각국이 구축하고 있는 전자건강정보파일시스템을 들수 있다. 이런 시스템은 환자치료과정에서 의료제공자로부터 수집한 건강정보의 처리를 허용하며 국내에서 같은 환자를 다루는 다른 의료제공자의 접근이 가능하다. 유럽에서 전자건강정보파일은 많은 우려를 사 왔다. 국내 전자파일은 손쉽게 국경을 오갈수 있기 때문이다. 유럽연합 제29조 개인정보보호 작업반은 그런 시스템 구축의 법적 근거로 환자 정보를 처리하는 일반 규정인 제3항을 들 수 없다고 보았다. 시스템이 안전하게 운영되기 위해 필요한 보호규정을 포함하여 명확한 법률적 근거를 요구하는 제4항을 충족해야 이런 시스템의 운영이 적법한 것이다(European Union Agency for Fundamental Rights·Council of Europe, 2014 : 90p).

한편, 95/46/EC 지침은 건강 정보를 높은 수준으로 보호하고 있지만 어떤 정보가 대상인지 명확히 밝히지 않았다. 특히 스마트기기 어플리케이션

이나 웨어러블 디바이스를 통해 처리되는 라이프로그(LifeLog)형 건강관련 정보가 늘어나는 환경 속에서, 이들 정보가 어떤 경우 민감정보로서 보호되는 건강관련 정보에 해당하는지 명확해질 필요가 있다. 모바일과 웨어러블 기술이 빠르게 발전하고 자가측정 어플리케이션 및 기기들이 인기를 끌면서 정보주체들은 자신의 성격, 정신, 신체, 행동 양태, 소재에 대한 모든 측면을 등록하고 있다. 이들 어플리케이션과 기기를 이용하면 어떤 경우 정보주체의 건강에 대한 판단을 내릴 수 있고 이들을 다르게 취급할 수도 있다. 긍정적으로 보면 도움이 되지만 부정적인 측면이나 기대 밖의 이용이 있을 수도 있다. 어플리케이션과 기기로부터 생성되는 정보가 개인의 건강 상태에 대한 정보를 담고 있지 않은 경우도 있을 수 있다.

이런 '회색 지대'를 다루기 위하여 제29조 개인정보보호 작업반은 2015년 "어플리케이션 및 기기와 건강 정보"에 대한 서한을 통해 다음과 같이 제안하였다(Article 29 Data Protection Working Party, 2015).

> 다음에서 처리되는 개인정보는 건강정보이다.
>
> 1. 본질적이거나 명백한 진료정보인 경우
> 2. 그 자체로나 다른 정보와 결합하여 실질적인 건강 상태나 위험에 대한 판단을 도출할 수 있는 원본 감지정보
> 3. 판단의 정확성, 적당성, 적절성 여부는 불문하고 개인의 건강상태나 건강위험에 대한 결론을 도출하는 경우

즉, 어플리케이션과 기기 등으로 수집되는 개인정보가 진료정보인 경우이거나 직접적으로나 간접적으로 건강 상태에 대해 판단할 수 있는 원본 감지정보인 경우, 혹은 건강 상태에 대한 판단 그 자체인 경우에는 민감정보에 포함되는 건강관련 정보로서 보호된다.

그밖에 민감정보의 목적외 제3자 제공과 관련하여, 2013년 유럽사법재판소는 진료기록의 경우 “유럽인권협약 제8조가 보장하고 있는 사생활의 권리 존중에 부합하지 않는 공개를 방지하기 위해 충분한 보호규정 없이는” 수사기관에게 제공될 수 없다고 보았다[134].

2003년 유럽은 “privacy best practice in deployment of biometric systems”(이하 ‘Best Practice’)이라는 보고서를 공개하였다. 이 보고서에서는 95/46/EC 지침에서 법적으로 요청되는 사항과 실무운용상 권장사항이 기술되어 있는데, 법령에 근거한 이용, 생체인식 정보(biometric data)의 취급에 관한 검토, 프라이버시 보호기술(Privacy Enhancing Technologies)의 검토라는 세 가지 측면을 다루고 있다. 박정훈(2012)은 Best Practice 중에서 주목해야 할 점을 세 가지로 꼽았다. 첫째, 생체인식 정보가 95/46/EC 지침상 “개인정보”에 해당하는지 여부의 문제이다. 이점에 대해서는 사진·목소리·지문 등의 생체인식 정보가 원칙적으로 개인정보에 포함할 수 있다고 하면서도 어플리케이션마다 엄밀히 검토할 경우 이들 정보가 개인정보에 해당하지 않을 수 있다고 한다. 또한 생체인식 정보의 개인정보 해당성에 대해서는 원본정보와 이를 템플릿화한 특징정보, 양자를 구별하여 분석하고 있다. 둘째로, 생체인식 정보와 95/46/EC 지침에서 보호하고 있는 「민감정보」와의 관계에 대한 문제이다. 생체인식 정보로부터 본인확인 목적으로 이용되는 것 이외의 정보가 밝혀질 우려도 있다는 점이다. 예를 들자면 의료·민족·인종, 특정한 행동에 관한 정보, 성생활에 관한 정보 등과 같이 민감정보가 추출될 위험이 있다고 지적하고 있다. 셋째로, 95/46/EC 지침상 「처리의 안전성」과 관련하여 이 보고서에서는 생체인식 정보를 될 수 있는 한 신속하게 부호화해서 원본정보를 무효화할 것, 중앙집중 데이터베이스보다 분산저장형을 채택할 것을 권장하고 있다.

특히 분산저장의 원칙은 특정된 목적을 위해 수집된 개인정보는 다른 기

134) http://hudoc.echr.coe.int/eng?i=001-120071#{"itemid":["001-120071"]}

관에서 다른 목적을 위해 수집된 개인정보와 원칙적으로 통합되지 않고 분리된 상태로 유지되어야 한다는 의미이다. 어떤 기관이 보유하고 있는 개인정보를 데이터베이스를 구축·통합하거나 다른 기관에 제공한다든가 자동검색시스템을 통해 개인정보를 공동으로 활용한다든가 하는 것은 원칙적으로 금지되는 것이다. 독일 연방헌법재판소는 이러한 원칙에서 특히 국가행정조직이 보유한 개인정보를 다른 목적으로 이용할 소지가 있는 개별 행정부서들에 대해 정보 접근을 차단해야 한다고 판결한 바 있다(권건보, 2005). 전자주민증을 도입한 유럽 국가들 중에서도 생체인식 정보의 민감성을 우려하여 일부는 지문정보 수록 여부를 선택하게 하였고 데이터베이스를 분산하여 구축하였다(Statewatch, 2011)[135].

2003년 유럽연합 제29조 개인정보보호 작업반은 생체인식 정보의 적법한 처리와 관련한 원칙을 구체화하였다. 첫째, 생체인식 정보는 대부분의 경우 지침 제2조의 개인정보에 해당한다. 둘째, 생체인식 정보가 출입 관리를 위해서 취득되었을 경우, 이를 정신상태의 평가나 직장의 감시용도로 이용해서는 안 된다. 셋째, 생체인식 정보를 취득할 때, 목적 및 관리자의 정보를 제시하여야 한다. 원격적으로 생체인식 정보를 취득할 경우에는 특별한 주의가 요구된다. 넷째, 생체인식 정보를 처리할 경우에 원칙적으로 본인동의가 필요하다. 다섯째, 정보의 처리가 정보주체의 권리에 특별한 위험을 초래할 경우에는 감독기관에 의한 사전적인 검사를 거쳐야 한다. 여섯째, 개인정보처리자는 기술적·조직적인 보안대책을 강구하여야만 한다. 예를 들자면 암호화, 암호키의 보호, 접근통제 등이다. 일곱째, 생체인식 정보가 인종·민족·건강상태 등의 민감정보에 해당하는 것으로 간주될 경우에는 특별한 보호를 필요로 한다(박정훈, 2012; 김경환, 2016).

135) 예를 들어 독일은 개인번호나 지문을 중앙정부 차원에서 관리하지 않으며, 전자 기능의 삽입과 지문 수록은 선택 사항이다. 이탈리아는 전자기능이 선택이며 지문 수록은 명시적으로 시민이 의사를 표시할 때만 이루어지고, 데이터베이스는 분산하여 구축하였다. 벨기에는 국가신분증에 지문을 수록하지 않고 데이터베이스를 분산시켰다.

특히 제29조 작업반은 아동의 생체인식 정보 처리에 대하여 엄격한 입장을 밝혔다. 학교나 구내식당 출입을 위해 아동의 지문, 홍채, 손윤곽 등 생체인식 정보를 처리하는 것은 목표에 비례적이지 않고 침해적이라는 것이다. 아동 생체인식 정보의 처리는 반드시 목표에 비례적이어야 한다. 법정대리인은 아동의 생체인식 정보 처리에 쉽게 반대할 수 있어야 한다. 아동이 생체인식 정보의 처리에 반대하는 경우 카드 등 대체수단이 지급되어야 한다(Article 29 Data Protection Working Party, 2009).

2012년 유럽연합 제29조 개인정보보호 작업반은 생체인식 정보의 보호절차에 대하여 좀더 구체적인 의견을 발표하였다. 우선 일반 원칙으로서 생체인식 정보에 대해 강력한 기술적 보안조치를 적용할 것을 권장한다. 신체에 각인된 바이오 정보의 특성상 한번 유출되면 그 피해를 회복하기 어렵기 때문이다. 둘째, 생체인식 기술에 프라이버시 중심설계를 적용한다. 셋째, 생체인식 기술에 프라이버시 영향평가를 실시한다. 마지막으로 의견서는 기술적이고 조직적인 차원에서 생체인식 기술을 보호하기 위해 취할 수 있는 다양한 수단을 제시하였다. 기술적인 수단으로는, ▲원본정보가 아닌 생체 특징정보의 사용 ▲중앙집중형보다 개인기기 분산저장형 권장 ▲갱신과 파기 보장 ▲암호화 저장 ▲속임수 방지 ▲생체암호(Biometric Encryption) 선호 ▲목적달성 후 자동삭제 ▲목적내 데이터베이스 규모의 최소화 및 식별정보 분리 등을 제시하였다(Article 29 Data Protection Working Party, 2012).

나) 개인정보보호규정(GDPR)의 원칙

유럽연합 집행부는 2014년 4월, 95/46/EC 지침을 개선하여 새로운 유럽 개인정보보호규정(General Data Protection Regulation, GDPR)[136]을 의결하

136) 번역문 : 개인정보 보호위원회. 단, 일부 용어의 경우 필자가 인용과정에서 수정하였다.
http://www.pipc.go.kr/cmt/not/ntc/selectBoardArticle.do?nttId=5139&bbsId=

였다. 민감정보는 제9조 특정범주의 개인정보 처리(Processing of special categories of personal data)에 포함되어 있는데, GDPR은 유전정보, 생체인식 정보, 건강관련 정보를 명시적으로 모두 민감정보에 포함하였다.

이 법에서 사용되는 정의는 다음과 같다. 우선, 유전정보(Genetic data)는 개인의 유전적 또는 후천적으로 얻은 유전자 특성에 관한 개인정보로 정의되어야 하며 이 유전자 특성은 염색체 분석, 데옥시리보핵산(DNA) 분석 또는 리보핵산(RNA) 분석 등 해당 개인으로부터 채취한 생물학적 샘플 분석에서 얻은 결과 또는 다른 요소 분석을 통해 이에 상응하는 정보를 획득하여 얻은 결과이다. 생체인식 정보(biometric data)는 얼굴 영상이나 지문 정보처럼 개인을 고유하게 식별하거나 확인할 목적으로, 개인의 신체, 생리, 행동 특성에 관하여 특수하게 기술적으로 처리한 결과 발생한 개인정보를 의미한다. 건강관련 정보(data concerning health)는 의료 서비스의 제공을 비롯하여 개인의 건강 상태에 관한 정보를 나타내는 개인의 신체 또는 정신 건강에 관한 개인 정보를 의미한다(제4조 정의).

제9조

특정범주의 개인정보 처리

1. 인종이나 민족, 정견, 종교나 철학적 신념, 노조 가입여부가 드러나는 개인정보의 처리와 유전정보(genetic data) 또는 개인을 특정하게 식별할 목적의 생체인식 정보(biometric data), 또는 건강관련 정보(data concerning health), 성생활, 성적 취향에 관한 정보의 처리는 금지된다.

2. 다음 각 호에 해당하는 경우에는 제1항은 적용되지 않는다

(a) 정보 주체가 단일 또는 복수의 특정 목적으로 특정범주의 개인정보를 처리하는 데 명백한 동의를 제공한 경우. 단, 유럽연합 또는 회원국 법률에서 제1항에 규정된 금지조문을 정보주체가 철회할 수 없다고 명시하는 경우는 제외된다.

BBSMSTR_000000000112&bbsTyCode=BBST03&bbsAttrbCode=BBSA03&authFlag=Y&pageIndex=1

(b) 정보주체의 기본권 및 이익에 대해 적절한 안전장치를 제공하는 회원국 법률에 따른 단체협약이나 유럽연합 또는 회원국 법률이 허용하는 범위에서, 고용, 사회안보와 사회보호법 분야에서 정보처리자 또는 정보주체의 특정권리를 행사하고 이들의 의무를 수행하기 위한 목적으로 처리가 필요한 경우;

(c) 정보주체가 물리적 또는 법률적으로 동의를 제공할 수 없는 경우로 정보주체 또는 다른 사람의 생명과 관련된 이익을 보호하는 데 필요한 경우;

(d) 정치적, 철학적, 종교적 또는 노동조합의 목적을 지닌 재단, 조합, 비영리기관이 적절한 안정 조치를 갖추어 수행하는 합법적인 활동의 과정에서, 그리고 해당 처리가 그 목적에 맞게 관련 기관의 회원 또는 이전 회원 또는 관련 단체와 정기적으로 접촉하는 사람에 한하여 관련된다는 조건과, 정보주체의 동의 없이 이러한 개인정보를 기관 외부에 제공하지 않는다는 조건에 따른 합법적 활동의 과정에서 처리가 수행되는 경우;

(e) 정보주체가 명백히 공개한 개인정보를 처리하는 경우;

(f) 청구권의 입증이나 행사, 또는 방어를 목적으로, 또는 법원이 사법능력을 행사하는 때마다 처리가 필요한 경우

(g) 개인정보보호권의 본질을 존중하고 정보주체의 기본권 및 이익을 보호하기 위해 적절하고 구체적인 조치를 제공하며, 추구하는 목적에 비례하는 유럽연합 또는 회원국 법률에 근거하여, 중요한 공익상의 이유로 처리가 필요한 경우,

(h) 유럽연합 법률이나 회원국 법률, 의료전문가와의 계약, 제3항에 규정된 조건 및 안전조치에 따라 예방의학이나 직업의학의 목적으로 또는 직원의 업무능력 평가나 의학적 진단, 의료나 사회복지 및 치료의 제공, 또는 의료나 사회 복지 제도 및 서비스의 관리를 위해 처리가 필요한 경우;

(i) 직무상 기밀 등, 정보주체의 권리와 자유를 보호하기 위해 적절하고 구체적인 조치를 규정하는 유럽연합 또는 회원국 법률에 근거하여, 회원국 간 중대한 건강위협으로부터 보호하거나 높은 수준의 의료 품질 및 안전성과 의약품이나 의학장비를 보장하기 위함 등, 공중보건 분야에서 공익 상의 이유로 처리가 필요한 경우;

(j) 추구하는 목적에 비례하고 개인정보보호권의 본질을 존중하며 정보주체의 기본권 및 이익을 보호하기 위해 적절하고 구체적인 조치를 규정하는 유럽연합 또는 회원국 법률에 근거한 제 89조 (1)항에 따라, 공익상의 기록보관 목적이나 과학 및 역사 연구 목적, 또는 통계목적을 위해 처리가 필요한 경우.

3. 제1항에 언급된 개인정보는 해당 개인정보가 유럽연합 또는 회원국 법률이나 국가 관련기관이 수립한 규정에 따른 직무상 비밀 의무를 적용 받는 전문가의 책임에 의해 또는 책임 하에 처리되는 경우, 또는 유럽연합 또는 회원국 법률이나 관련 국가기관에 수립한 규정에 따른 비밀의 의무에 적용 받는 또 다른 개인에 의해 이러한 개인정보가 처리되는 경우, 제2항의 (h)에 규정된 목적을 위해 처리될 수 있다.

4. 회원국은 유전정보나 생체인식 정보, 건강관련 정보와 관련하여, 제한을 포함한 추가 조건을 유지 또는 도입할 수 있다.

GDPR의 민감정보 처리 원칙을 95/46/EC 지침과 비교하였을 때 다음과 같이 요약할 수 있다(Bird & Bird, 2016). 첫째, GDPR의 민감정보는 명시적으로 '개인을 고유하게 식별하는' '유전정보'와 '생체인식 정보(biometric data)'를 포함한다. 둘째, GDPR의 민감정보 처리 기준은 95/46/EC 지침보다 폭넓은 건강정보와 건강관리 영역을 규율하지만, 일반적으로는 95/46/EC 지침의 처리 기준을 따른다. 셋째, 회원국은 유전정보, 생체인식 정보, 건강관련 정보의 처리 제한 등 관련 요건을 새롭게 제시할 수 있다. 특히 이 부분은 유럽이 바이오 정보의 보호와 관련하여 특별한 관심을 기울였음을 짐작케 한다.

GDPR 해설전문 51에서는 민감정보의 처리와 관련하여 다음과 같이 구체적으로 설명하고 있다.

(51) 개인정보의 특성상, 기본권과 자유와 관련해 특히 민감한 개인정보는 기본권 및 자유 침해의 리스크를 야기할 수 있기 때문에 구체적인 보호를 받아야 한다. 이러한 정보에는 인종 또는 민족출신을 드러나는 개인정보도 포함되어야 하며, 이 법에서의 '인종출신'이라는 단어의 사용이 유럽연합이

인종을 분리하려는 이론을 용인한다는 의미가 아니다. 사진정보처리는 특정 개인 식별이나 인증 가능한 구체적인 기술적 수단을 통해 처리되는 경우에 한해서만 생체[인식] 정보의 정의에 해당되기 때문에, 시스템적으로 민감처리로 분류되지 않는다. 이러한 개인정보는, 회원국의 법률이 공익 또는 정보 처리자에게 부여된 공적 권한을 이행하기 위한 직무의 수행 또는 법적 의무의 준수를 위해 이 법의 규칙 적용을 변경하고자 개인정보에 대한 구체적인 조문을 규정할 수 있다는 사실을 고려하여 이 법에 따라 구체적인 상황에서 처리가 허용되는 경우가 아닌 이상, 처리되어서는 안 된다. 이러한 처리에 대한 구체적인 요건과 함께, 이 법의 일반적인 원칙 및 기타 규정은 특히 합법적 처리를 위한 조건과 관련하여 적용되어야 한다. 특정 범주의 개인정보 등의 처리에 대한 일반적인 금지로부터의 일부 제외는 명백하게 제공되어야하는데, 특히 정보주체가 명백한 동의를 제공한 경우나 특별한 필요성이 있는 경우로, 특정 협회나 재단의 기본적 자유의 행사를 허용하는 목적으로 하는 합법적 활동과정에서 처리가 수행되는 경우 그러하다.

‘사진’ 처리의 경우 일부는 민감정보에 속하지만 자동적으로 민감정보에 포함되지는 않는다. 사진정보가 고유한 식별성을 과도하게 드러내거나 전자여권 등 생체인식 정보로서 개인을 인증할 때에만 민감정보에 포함된다.

민감정보의 처리의 적용을 배제하는 GDPR의 제9조 제2항의 경우 일반적으로는 95/46/EC 지침과 유사하다. 정보주체의 명백한 동의를 규정한 (a), 고용, 사회안보와 사회보호법 등의 목적에서 회원국 법률의 허용 범위에 대한 (b), 정보주체가 물리적 또는 법률적으로 동의를 제공할 수 없는 경우로 정보주체 또는 다른 사람의 생명과 관련된 이익을 보호하는 데 필요한 경우에 대한 (c), 정치적, 철학적, 종교적 또는 노동조합의 목적을 지닌 재단, 조합, 비영리기관이 적절한 안정 조치를 갖추어 수행하는 합법적

인 활동에 대한 (d), 정보주체가 명백히 공개한 개인정보를 처리하는 경우에 대한 (e), 사법 분야에서 처리하는 경우에 대한 (f)가 그렇다. 공익을 위한 민감정보 처리의 경우 법률에 의해 가능하도록 한 (g)항의 경우에도 95/46/EC 지침 제8조 제4항의 구조와 유사하되 보다 더 구체적이다.

건강관련 정보의 경우 95/46/EC 지침 제8조 제3항의 구조와 유사하지만 목적별로 더욱 상세하게 규정하였다. (h)와 (i)의 경우 각각 의약 분야에서 공식적인 법률에 따른 규제 및 이용과, 사회보험제공자간 건강정보를 공유하기 위한 목적이라는 차이가 있다. 두 조건의 경우 추가적인 비밀유지 의무를 필요로 한다.

(j) 의 경우, 공익적인 기록보관 목적이나 과학 및 역사 연구 목적, 또는 통계목적을 위해 처리될 경우 최소수집 등 적절한 안전조치를 준수하고 민감정보의 처리가 가능하도록 하였다. 제9조 제4항에서는 특히 각국 법률이 유전정보, 생체인식 정보, 건강정보 관련해서는 처리제한 등 추가적인 조건을 부여할 수 있도록 규정하였다.

GDPR은 정보주체를 보호하기 위해 여러 가지 제도를 추가적으로 규정하였다. 그 중 제25조에서 규정하고 있는 '개인정보보호 중심설계 및 설정(Data protection by design and by default)'가 주목을 받고 있다. 개인정보 처리자는 개인정보의 처리 수단을 결정한 시점과 처리 당시 시점에서, 정보 최소화 등 개인정보보호의 원칙을 이행하고 본 규정의 요건을 충족하고 정보주체의 권리를 보호하기 위해, 처리에 필요한 안전조치를 포함하기 위해 고안된 가명처리 등, 적절한 기술 및 관리 조치를 이행해야 한다(by Design). 또 개인정보 처리자는 기본설정을 통해, 처리의 개별 특정목적에 필요한 정도에 한하여 개인정보가 처리될 수 있도록 보장하기 위한 적절한 기술 및 관리 조치를 이행해야 한다(by Default).

이런 조항들은 개인정보에 대한 정보주체의 권리를 실질화하기 위하여

상품이나 서비스의 구상·기획 단계에서부터 적용할 것을 제안받고 있는 프라이버시 중심설정(Privacy by Default), 프라이버시 중심설계(Privacy by Design)의 원칙을 국제규범화한 것으로 평가받고 있다. 프라이버시 중심설계란, 캐나다 온타리오 개인정보보호감독관인 카부키안 박사가 1990년대 “미래의 프라이버시는 단지 법률이나 규제 체제 준수만으로 보장할 수 없다. 프라이버시 보장은 기관들이 시행 과정에서 기본설정으로 채택해야만 한다”는 취지로 고안한 개념이다. 우리나라에서는 국가인권위원회가 2013년 <정보인권 보고서>에서 빅데이터 환경에서 프라이버시 중심설계의 도입을 제언한 바 있다.

프라이버시 중심설계의 실시는 7대 원칙에 따른다. 7대 원칙은 ① 사후대응이 아니라 사전 대비, 문제점을 고치는 것이 아니라 사전 예방할 것 ② 프라이버시 보호를 시스템의 기본 설정값(default)으로 설정할 것 ③ 모든 활동계획에 프라이버시를 포함할 것 ④ 포괄적 기능성을 보장할 것, 즉 상호대체(Zero-Sum)가 아닌 상호보완(Positive-Sum)으로 전환 ⑤ 전체의 생명주기상에서 보안을 고려할 것 ⑥ 가시성과 투명성을 기반으로 이해당사자에게 항상 공개되도록 할 것 ⑦ 사용자 중심의 설계와 운영으로 개인의 프라이버시가 존중되도록 할 것 등이다(Ann Cavoukian, 2013).

유럽네트워크정보보호원(ENISA)는 2014년 발표한 보고서에서 공학적인 방법으로 어떻게 프라이버시 및 개인정보보호 중심설계를 구현할 수 있는지에 대해 다루고 있다. 보고서에서 제시한 8가지 설계 전략은 ① 최소화(Minimize) ② 숨기기(Hide) ③ 분리(Separate) ④ 총계(Aggregate) ⑤ 통지(Inform) ⑥ 통제(Control) ⑦ 강화(Enforce) ⑧ 입증(Demonstrate)이다(김혜리 외, 2016).

한편 GDPR의 경우 개인정보 영향평가도 적극적으로 도입하였다. 특히 제35조와 해설전문 91에서는 생체인식 정보 등 민감정보의 대규모 처리에 대해서는 개인정보 영향평가가 적용되어야 한다는 점을 명시하고 있다. 우

리나라에서는 국가인권위원회가 2013년 <정보인권 보고서>에서 빅데이터 환경에서 개인정보 영향평가의 의무적 도입을 제언한 바 있다.

> 제35조
> 개인정보 영향평가
>
> 3. 제1항에 규정된 개인정보 영향평가는 특히 다음 각 호의 경우 요구되어야 한다.
>
> (b) 제9조 (1)항에 규정된 특정범주의 개인정보에 대한 대규모 처리나 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보에 대한 처리

더불어 GDPR은 '프로파일링'(profiling)을 규정하고 이를 제한하는 조항들을 도입하였다. 우선 '프로파일링'이란, "개인에 관한 특정한 개인적 측면을 평가하기 위해, 특히 개인의 업무능력, 경제 상황, 건강, 개인의 성향이나 관심사, 신뢰도, 행동, 위치, 이동에 관한 측면을 분석 및 예측하기 위해 개인정보를 사용하는 모든 개인정보의 자동처리 형태를 의미한다"(제4조(4)). 유럽연합 역외의 개인정보처리자라 하더라도 정보주체에 대한 결정을 할 때나, 정보주체의 개인적 선호, 행동과 태도를 분석하거나 예상하는 프로파일링 기법 같은 개인정보처리 기술을 잠재적·계속적으로 사용하여 개인을 인터넷에서 추적하는 경우에는 이 법의 적용을 받는다(해설전문 24).

정보주체는 프로파일링 유무와 해당 프로파일링의 결과에 대해 고지 받아야 한다(해설전문 60). 구체적으로 정보주체는 프로파일링 등 자동 의사결정의 유무, 관련 논리(logic)에 관한 유의미한 정보와 이러한 정보주체에 대한 처리의 유의성과 예상되는 결과에 대해 수집 시점에 정보를 제공받을 권리가 있으며(제13조 및 제14조), 같은 정보에 대해 열람권이 있고(제15

조), 프로파일링에 대해 언제든지 반대할 권리를 갖는다(제21조).

무엇보다 정보주체는 프로파일링 등, 본인에 관한 법적 효력을 초래하거나 이와 유사하게 본인에게 중대한 영향을 미치는 자동 처리에만 의존하는 결정의 적용을 받지 않을 권리를 갖는다(제22조). 특히 바이오 정보를 비롯한 민감정보에 기반해서 판단이 이루어져서는 안 된다. 단, 제9조 (2)항의 (a)와 (g)가 적용되고 또한 정보주체의 권리와 자유, 정당한 이유를 보호하는 적절한 조치가 시행되는 경우는 예외로 한다.

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, 개인정보 영향평가가 반드시 필요하다(제35조). 생체인식 정보의 처리를 따라 특정 개인에 대한 결정을 내릴 때에도 개인정보 영향평가가 이루어져야 한다(해설전문 91). 기업들의 취업규칙에는 프로파일링 등 자동 처리만을 근거로 한 결정을 따르지 않을 권리 등 정보주체의 권리 및 이 권리를 행사하기 위한 수단이 명시되어야 한다(제47조). 다만 프로파일링에 대한 이상의 규제들은 정보주체 또는 제3자의 권리와 자유를 보호하는데 필요하고 비례하는 수준에서 부과될 수 있다(해설전문 73).

특히 직접 마케팅을 목적으로 개인정보를 처리하는 경우, 정보주체는 최초 또는 추가 처리와 관련 있는지 여부와 상관없이, 이러한 직접 마케팅과 관련한 범위에 해당하는 프로파일링 등, 이러한 처리에 대해 언제든지 무상으로 반대할 권리를 갖는다. 이 권리는 정보주체가 명백하게 인지할 수 있도록 제공되어야 하며 다른 기타 정보와는 별도로 명백하게 제시되어야 한다(해설전문 70).

한편, GDPR에서는 빅데이터 시대 높아지는 식별성과 그 보호에 관련하여 익명정보와 가명처리를 구분하여 다루고 있다. '가명처리'는 추가 정보의 사용 없이 더 이상 특정 정보주체를 식별할 수 없는 방식으로 수행된 개

인정보의 처리를 의미하며, 이 경우, 해당 추가정보는 별도로 보관되며 개인정보가 식별된 또는 식별될 수 있는 개인에게 해당되지 않도록 보장하기 위한 기술 및 관리조치가 적용된다(제4조(5)). 개인을 더이상 식별될 수 없는 익명정보는 개인정보가 아니며, 통계목적 및 연구 목적 등을 위한 익명정보의 처리에는 이 법이 적용되지 않는다. 가명처리 정보는 개인정보의 식별 위험성을 줄이는 보호조치가 될 수는 있지만, 추가 정보를 이용하여 개인을 식별할 수 있기에 여전히 개인정보로 간주한다. 이 점은 다음 해설 전문의 서술들에서 잘 드러난다.

(26) 개인정보보호원칙은 식별되었거나 또는 식별될 수 있는 개인에 관한 일체의 정보에 적용될 수 있다. 가명처리 정보는, 추가 정보를 이용하여 개인을 식별할 수 있는 정보로서 식별할 수 있는 개인정보로 간주되어야 한다. 어떤 개인이 식별가능한지를 판단하기 위해서는 특정개인의 식별 등 처리자 또는 제3자 모두가 개인을 직접 또는 간접적으로 확인하기 위해 사용할 것으로 합리적으로 예상되는(reasonably likely) 모든 수단을 고려해야 한다. 개인을 식별하기 위해 사용될 것으로 합리적으로 예상되는 수단인지를 확인하기 위해서는, 식별하기 위해 소요되는 비용과 시간 등 객관적인 요소를 모두 고려하고, 처리 당시 가용한 기술과 기술적 발전을 모두 고려하여야 한다. 익명정보에는 개인정보보호원칙이 적용되지 않는다. 다시 말해서 이 원칙은 식별되었거나 또는 식별될 수 있는 개인과 관련되지 않는 정보 또는 그런 방식으로 익명처리되어 더 이상 식별될 수 없는 정보주체에는 적용되지 않는다. 따라서 이 법은 통계목적 및 연구 목적 등을 위한 익명정보의 처리에는 적용되지 않는다.

(28) 개인정보의 가명처리는 해당 정보주체가 갖는 위험성을 줄일 수 있으며 정보처리자와 수탁처리자가 그들의 개인정보보호의 의무를 준수할 수 있도록 돕는다. 이 법에서 명시적으로 가명처리를 도입하는 것은 다른 개인정보보호 조치를 배제할 의도가 아니다. (가명처리를 했다고 해서 정보보호 조치가 면제되는 것이 아니다.)

즉, 연구나 통계 목적을 위해 민감정보의 처리가 필요한 경우, 앞서 살펴본 제9조 제2항 (j)에 명시되어 있다시피, 목적에 비례적이고 본질적인 권리를 존중하며 적절하고 구체적인 보호수단을 제공하는 경우 제89조 제1항에 따라 이를 처리할 수 있다. 그리고 '공익을 위한 유지보존의 목적, 과학이나 역사 연구의 목적 또는 통계 목적에서의 개인 정보 처리에 적용되는 안전조치 및 적용의 일부 제외'를 규정하고 있는 제89조 제1항은 이와 같은 목적에서 개인정보를 처리할 경우 가명처리 등 기술·관리적 보호수단을 적용해야 하고, 다만 '정보주체를 식별할 수 없거나 더 이상 식별할 수 없는 개인정보의 추가 처리', 즉 익명화를 우선적으로 적용해야 한다. 다만, 불가피한 경우 각국이 법률에 의해 동의권 행사 등 정보주체의 권리를 제한할 수 있도록 하였다.

제89조

공익을 위한 유지보존의 목적, 과학이나 역사 연구의 목적 또는 통계 목적에서의 개인 정보 처리에 적용되는 안전조치 및 적용의 일부 제외

1. 공익을 위한 유지보존의 목적, 과학이나 역사적 연구의 목적 또는 통계 목적에서의 개인정보 처리는 본 규정에 따른 정보주체의 권리와 자유를 위해 적절한 안전조치의 적용을 받아야 한다. 그 같은 안전조치를 통해 특히 정보 최소화의 원칙을 보장하기 위한 기술·관리적 조치가 구비되어 있어야 한다. 상기 목적들이 이 같은 방식으로 충족될 수 있다면 기술·관리적 조치에 가명처리가 포함될 수 있다. 정보주체를 식별할 수 없거나 더 이상 식별할 수 없는 개인정보의 추가 처리를 통해 상기 목적들이 충족될 수 있는 경우, 그 목적들은 이 같은 방식으로 충족되어야 한다.

2. 개인정보가 과학이나 역사적 연구 목적 또는 통계 목적으로 처리되는 경우, 유럽연합 또는 회원국 법률은 제15, 16, 18조 및 제21조에 명시되고 본 조문 1호의 조건 및 안전조치에 따른 권리로 인해 특정 목적의 달성이

> 불가능하거나 심각하게 저해될 가능성이 있고 적용의 일부 제외가 그 같은 목적의 충족에 요구되는 한, 해당 권리의 적용을 일부 제외하도록 규정할 수 있다. (중략)

이때 GDPR의 가명처리, 익명정보의 구분을 적용해 보면, 공익을 위한 유지보존의 목적, 과학이나 역사 연구의 목적 또는 통계 목적에서의 개인정보 처리라 하더라도 가명처리는 개인정보로서 정보주체의 동의 등 절차에 따라 처리해야 하고, 익명정보는 개인정보가 아니므로 이 법의 적용이 배제된다. 이런 구조는 우리 개인정보 보호법 제18조 제2항 제4호에서 "통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우" 정보주체의 동의가 없어도 목적 외로 이용하거나 제3자에게 제공할 수 있도록 한 예외 규정과 유사한 규율이다.

2) 미국

미국은 생체인식 정보와 관련하여, 연방 차원에서 이에 대한 보호를 규정한 법률은 존재하지 않는다. 그러나 생체인식 정보의 민감함을 인식하여 몇 가지 조치를 연방 차원에서 취하고 있다(박정훈, 2012). 연방정부는 생체인식 정보를 '개인식별 가능정보'(personally identifiable information)로 분류하였다. 2006년 의회는 생체인식 정보를 도용하는 것에 대해 형사처벌을 하도록 입법하였다.

다만 미국은 법률 체계상 그 보호 대상으로 개인정보라는 개념 대신 '개인식별 가능정보'라는 개념을 채택함에 따라 이를 제한적으로 보호하고 있다. 그 보호 방법 또한 재식별이 불가능하거나 복원 불가능하다는 의미의 익명화(anonymization)가 아닌 비식별화(de-identification)를 적용하고

있다. 이는 '식별자 제거' 정도의 수준을 의미하며 일정한 조치를 하기만 하면 재식별 가능성이 있더라도 해당 법령의 규율을 배제한다는 의미이다(이은우, 2016).

특히 미국은 민간부문 개인정보보호가 '자율규제'를 원칙으로 하고 있기 때문에 생체인식 정보에 대해서도 자율규제를 전제로 가이드라인을 마련하는 경향이 일반적이다. 그러나 박정훈(2012)에 따르면 다음과 같이 주법에 따라 때로는 민간부문을 아울러 생체인식 정보를 엄격하게 보호하는 경우가 있다.

우선, 2001년 텍사스 주 정부법(Texas Statute Government Code) '제560장 생체인식 식별자'(Chapter 560. Biometric Identifier)의 제560.001조 정의에서 "생체인식 식별자는 눈동자패턴·홍채패턴·지문·음성·손바닥형상·얼굴형을 대상으로 한다"고 규정하고 있다. 제560.002조는 생체인식 식별자의 공개에 대해서 "개인의 생체인식 식별자를 보유하는 정부기관은 본인의 동의없이 생체인식 식별자를 매매·임대 또는 제3자에게 공개해서는 안 된다. 또한 생체인식 식별자가 누설되지 않도록 상당히 주의하여 보관·전송하여야 한다"고 규정하고 있다.

2008년 일리노이 주 '생체인식 정보 프라이버시법'(Biometric Information Privacy Act of 2008)은 제10조 정의에서 '생체인식 식별자'(Biometric Identifier)는 망막 혹은 홍채 스캔, 지문, 성문, '손과 얼굴의 지형도'(hand or face geometry)의 스캔을 대상으로 한다고 규정한다. 그리고 제15조 보유·수집·공개·파기에서 "생체인식 식별자나 생체인식 정보를 보유한 사적 기관은 대중에 공개된 정책을 가지고 있어야 하고, 초기 보유목적이 만족되었거나 3년의 기간을 한계로 보유기간과 영구적 삭제일정에 대한 지침을 설정해 두어야 한다. 관할법원에서 발부한 유효한 영장(warranty)이나 소환장(subpoena)이 없는 한, 사적기관이 보유한 생체인식 식별자나 정보는 설정된 보유기간과 파기지침을 준수하여 처리되어야 한다"고 규정하고 있다. 2015년 7월, 일리노이 주법이 SNS 등에서 생체인

식 정보를 상업적 목적으로 수집할 경우 동의를 구하도록 한 일리노이 주법에 대한 최초의 소송이 제기되어 진행중이다[137].

또한 뉴저지 주에서는 생체인식 식별자 프라이버시법(Biometric Identifier Privacy Act)의 제정을 2002년과 2006년에 시도하였으나 회기만료에 의한 법안 자동폐기로 입법에 성공하지 못한 바 있다. 생체인식 식별자의 정의, 보호 내용은 텍사스 주정부법과 같지만 텍사스 주법이 정부기관만을 대상으로 하고 있음에 반해, 생체인식 식별자를 보유하는 모든 자를 대상으로 하고 있다는 점이 다르다. 그리고 위반자에 대하여는 벌칙이 있어 2만 5,000달러 이하의 벌금에 처하도록 하고 있다.

캘리포니아·노스다코타·위스콘신·미주리 등 4개주 법률에서는 고용자들이 근로자들에게 피부 아래에 삽입하여 식별정보를 전송하는 마이크로칩들의 사용을 강제하지 못하도록 규정하고 있다. 그러나 이들 법은 근로자들의 자발적인 마이크로칩의 장착을 금지하는 것은 아니다.

한편 생체인식 정보에 특화된 보호 법률이 아니더라도 유출통지 등 주법으로 규제하는 대상 개인정보의 개념에 생체인식 정보를 포함하는 법률을 두고 있는 주들도 늘어나고 있다. 2015년에 와이오밍 주[138]와 코네티컷 주[139] 개인정보 보호 관련 법률에서 생체인식 정보를 포함한 개정안이 통

137) “States Writing Biometric-Capture Laws May Look to Illinois”, Hunton&Williams 2015. 7. 31, https://www.huntonprivacyblog.com/2015/07/31/states-writing-biometric-capture-laws-may-look-illinois/

138) “Two Wyoming Bills Amending the State’s Breach Notification Statute Are Headed to the Governor”, Hunton&Williams 2015. 2. 27, https://www.huntonprivacyblog.com/2015/02/27/two-wyoming-bills-amending-states-breach-notification-statute-headed-governor/

139) “Connecticut Passes New Data Protection Measures into Law”, Hunton&Williams 2015. 7. 23, https://www.huntonprivacyblog.com/2015/07/23/connecticut-passes-new-data-protection-measures-law/

과되었으며 뉴욕 주 의회[140]에는 유사한 내용의 법안이 발의되었다.

미국에서는 최근 민감한 건강정보의 빅데이터 처리를 둘러싼 논란이 커지고 있다. '타겟'이라는 대형마트는 고객의 구매행태에 대한 빅데이터 분석을 통해 임신 사실을 예측하여 사회적 논란이 일었다[141]. 한국인의 처방정보를 사간 혐의로 그 한국지부가 형사기소되어 2016년 현재 재판을 받고 있는[142] IMS health 등 빅데이터 업체들이 처방정보를 수집 판매하는 행위도 미국 현지에서 논란이 계속되고 있다. 특히 처방정보의 보호와 관련하여, 2008년 처방정보의 상업적 사용을 제한한 뉴햄프셔주법이 적법하다는 판결이 있었는데, 유사한 내용의 버몬트주법에 대해서는 2011년 6월 23일 연방대법원이 표현의 자유 침해 결정을 내렸다. 다만 처방정보의 기밀성이 부인된 것은 아니라서 이와 관련한 주법들은 좀더 명확한 용어로 개선될 것으로 보인다 (Marcia M. Boumil 외, 2012; Christopher R. Smith, 2012).

이러한 사건들의 영향으로 미국은 최근 연방정부 차원에서 빅데이터 시대 프라이버시 보호를 위한 여러 가지 정책을 추진하겠다는 계획을 세우고 있다. 예를 들어 2014년에 발표된 백악관 보고서(Big Data: Seizing Opportunities, Preserving Values)는 빅데이터 활용 촉진과 동시에 프라이버시 보호를 위한 정부 차원의 규제가 진행되어야 한다고 지적하고 있다. 빅데이터 분석의 목적 외 활용이나, 차별적인 효과도 규제해야 한다는 입장을 밝혔다. 생체인식 정보 등 바이오 정보가 그 대상이 되는 경우 이런 규제의 대상이 될 것으로 예상되고 있다.

---

140) "Data Security Act Introduced in New York State Assembly", Hunton&Williams 2015. 4. 8, https://www.huntonprivacyblog.com/2015/04/24/data-security-act-introduced-new-york-state-assembly/

141) "부모도 모르는 딸의 임신, 대형마트는 알고 있다", 한겨레 2016. 2. 11. http://www.hani.co.kr/arti/economy/economy_general/729868.html

142) "검찰은 IMS 기소했는데…정부는 개인정보 빗장 풀 조짐", 한겨레 2016. 7. 18. http://www.hani.co.kr/arti/economy/it/752755.html

3) 기타 국제 규범

박정훈(2012)은 생체인식 정보의 보호와 관련한 국제 규범에 관해 다음과 같이 정리하였다.

우선 국제생체인식산업협회(International Biometric Industry Association, IBIA)는 1999년 「프라이버시 지침」(Privacy Guidelines)에서 다음과 같이 생체인식 정보의 보호 방향을 제시하였다. 첫째, 생체인식 정보에 관한 지침: 생체인식 정보는 개인정보로부터 분리·구별되는 전자코드이며, 부정한 접근에 대한 방벽(barrier)이 된다. 정보의 오용이나 본인·사법당국의 동의 없는 공개를 방지할 필요가 있다. 둘째, 민간부분에 관한 지침: 생체인식 정보의 수집·보존·액세스·사용 및 목적 외 이용에 대한 개인의 권리에 관한 명시적인 정책수립이 추진되어야 한다. 셋째, 공공부문에 관한 지침: 정보 수집·액세스·보존·이용에 관한 요건을 정한 명확한 법적 기준의 규정이 필요하다. 넷째, 민·관 양부문에 관한 지침: 생체인식 데이터베이스의 비밀성과 완전성의 보존·유지를 위한 적절한 운용 및 기술적 관리 방법이 적용되어야 한다.

이는 2014년 보다 더 구체적인 10원칙으로 발전하였다(김경환, 2016). ① 개인 식별 목적 외로 사용되는 경우에는 이를 통지할 것 ② 상황에 맞추어 개인에게 옵트인 또는 옵트아웃 기회를 제공할 것 ③ (목적 제한) 수집 목적을 벗어나 사용하지 말고 생체인식 정보와 관련 없는 개인정보로 식별하지 말 것 ④ (목적 특정) 수집시 목적을 특정할 것 ⑤ (정보의 품질) 정보의 정확성과 완전성을 유지할 것 ⑥ (사용자 제한) 사용자의 접근을 통제할 것 ⑦ (보안 안전) 수집되어 보관 중인 정보의 보안을 유지할 것 ⑧ (공개) 보유된 정보를 개인이 파악할 수 있는 절차를 제공할 것 ⑨ (책임성) 주기적으로 독립적인 감사를 시행할 것 ⑩ (문제해결과 구제) 유출시 절차 등이다.

OECD(경제협력개발기구)는 2004년 보고서(Directorate for Science, Technology and Industry, Committee for Information, Computer

and Communications Policy, Biometric-Based Technologies)에서, 생체인식 정보의 이용에 수반한 문제로서 a) 예측 불가능한 목적 이외로의 이용(function creep)의 문제, b) 감시 수단으로서의 이용에 관한 문제, c) 동의원칙에 근거하는 이용과 투명성확보의 문제를 제시하였다. 더불어 이들 문제에 대한 검토사항으로서 ① 법제도(생체인식 정보의 이용에 관계되는 법제정비의 문제), ② 지침이나 과제해결을 위한 기본체계의 방향성(생체인식 정보의 이용에 관련한 기본원칙이나 지침의 수립, 다양한 과제에 부응한 대응책의 기본이념), ③ 기술적 검토과제(기밀성·완전성이나 프라이버시증진기술 - PETs - 의 이용 등)를 들었다.

국제바이오 정보그룹(International Biometric Group: IBG)은 “바이오프라이버시 계획(BioPrivacy Initiative)”의 “모범 사례(BioPrivacy Best Practices)”로서 25개 항목을 제시하였다. 1. 범위의 한정, 2. 보편적인 고유 식별자의 작성에 대해서, 3. 생체인식 정보 보유의 한정, 4. 잠재적인 시스템성능의 평가, 5 무관계인 정보의 수집 또는 보존에 대해서, 6. 오리지널 생체인식 정보의 보유에 대해서, 7. 생체인식 정보의 보호, 8. 조회·판정결과의 보호, 9. 시스템에의 액세스 제한, 10. 생체인식 정보의 분리, 11. 시스템의 종료, 12. 「등록거부」의 자유, 13. 생체인식에 관계되는 정보의 수집 및 액세스, 14. 익명에 의한 등록, 15. 제3자에 의한 책임, 감사 및 감독, 16. 감사 정보의 완전한 공개, 17. 시스템 목적의 공개, 18. 등록의 공개, 19. 매칭의 공개, 20. 생체인식 정보의 이용에 관한 공개, 21. 선택적·의무적 등록의 공개, 22. 시스템의 관리·감독 책임자의 공개, 23. 등록·인증절차의 공개, 24. 생체인식 정보의 보호 및 시스템보호의 공개, 25. 삭제절차의 공개 등이다.

2014년 3월 8일 독일 개인정보보호감독관 회의에서 발표된 결의문은 최근 급증한 온라인 얼굴인식 시스템에 대한 우려를 담았다. 이와 같은 생체인식 기술을 사용할 때 온라인 회사들이 포괄적인 이용약관과 별도로 정보

주체의 동의를 구하는 등 합법적 기준을 준수할 것을 촉구하였다. 회사들이 '정당한 이익'의 범위에서 이 정보들을 처리하는 것은 생체 특징정보를 기존 정보와 비교하기 위해 임시적으로 처리하는 경우에 한정해야 하고 그 후 지체 없이 삭제되어야 하며, 그 사실을 정보주체에 고지해야 한다. 정보주체의 동의를 받을 수 없는 제3자가 생체 특징정보를 보관하는 것은 불법이다[143].

이런 국제규범들이 누적되어 옴에 따라, 세계 여러 나라가 바이오 정보를 보호하는 입법 체계를 갖추게 되었다. 그 보호 정도는 조금씩 다르지만 많은 국가들이 '민감정보'의 일환으로 바이오 정보를 보호하고 있음을 주목할 필요가 있다. 일반 개인정보보다 더 엄격한 보호를 적용하는 '민감정보'의 개념을 법정화하고 있는 국가의 경우, 이를 바이오 정보에 대해 적용하여 보호하는 현황은 다음과 같다(DLA Piper, 2016).

143) "German DPAs Adopt Resolutions on Employee Privacy, Facial Recognition and EU Draft Regulation", Hunton&Williams 2014. 4. 3, https://www.huntonprivacyblog.com/2014/04/03/german-dpas-adopt-resolutions-employee-privacy-facial-recognition-eu-draft-regulation/

[표41] 표 세계 각국 바이오 정보 보호 현황

국가	민감정보에 포함된 바이오 정보
앙골라	건강관련 정보(유전정보 포함) * '민감정보' 뿐 아니라 비디오감시 역시 개인정보처리방침 특별공개 의무대상
아르헨티나	건강관련 정보
호주	건강관련 정보, 유전정보, 생체인식 정보(템플릿화한 생체 특징정보 포함)
오스트리아	건강관련 정보
벨기에	건강관련 정보
보스니아 헤르체코비나	건강관련 정보, 유전정보, 생체인식 정보
브라질	건강관련 정보, 유전정보, 생체인식 정보
캐나다	* '민감정보' 규정은 없으나 건강관련 정보의 경우에는 온라인 행태광고에서 옵트아웃 적용 금지
카보베르데	건강관련 정보, 유전정보 * '민감정보' 뿐 아니라 비디오감시 역시 특별보안조치 의무대상
칠레	신체적·정신적 건강상태 정보
중국	* 일반적으로 생체인식 정보는 일반 개인정보. 다만 처리자의 특성에 따라 유전정보, 지문정보가 민감정보에 포함될수 있음
콜롬비아	건강관련 정보, 생체인식 정보
크로아티아	건강관련 정보
키프로스	건강관련 정보
체코 공화국	건강상태 정보, 유전정보, 생체인식 정보
덴마크	건강관련 정보
에스토니아	건강상태나 (신체적·정신적) 장애 정보, 유전정보, 생체인식 정보(지문, 장문(掌紋), 홍채, 유전정보 등)
핀란드	건강상태, 질병, 장애 정보, 처치 등 정보
프랑스	건강관련 정보
독일	건강관련 정보
가나	건강관련 정보
지브롤터	건강관련 정보
그리스	건강관련 정보 및 건강관련 기관 소속정보
건지 섬	신체적·정신적 건강이나 상태
온두라스	건강관련 정보, 신체적·정신적 상태

헝가리	건강 및 중독 관련 정보
아이슬란드	건강관련 정보(유전정보, 알콜·처방약품·마취제 사용정보 포함)
인도	신체적·생리적·정신적 건강상태, 진료기록 및 내역, 생체인식 정보(지문, 망막·홍채, 성문(聲門), 표정, 손동작, 유전정보) * 단, 공공부문 제외
아일랜드	신체적·정신적 건강 및 상태
이스라엘	건강상태
이탈리아	건강관련 정보 * 유전정보, 생체인식 정보의 경우에는 고지의무 * 생체인식 정보의 경우 특별보안조치 의무대상 * 진료기록, 생체인식 정보의 경우 유출통지
일본	신체적·정신적 건강 및 상태
라트비아	건강관련 정보 * '민감정보' 뿐 아니라, 비디오감시, 유전정보(생체인식 정보) 처리시 감독기구에 등록의무
레소토	건강관련 정보
리투아니아	건강관련 정보
룩셈부르크	건강관련 정보(유전정보 포함) * 유전정보, 생체인식 정보 처리 뿐 아니라 비디오 녹화 감시는 감독기구 사전허가 필요 * 특히 유전정보는 정보주체의 생명을 보호하거나 예방 의학, 의료적 진단, 요양, 치료가 필요할 때에만 처리 가능
마카오	건강관련 정보(유전정보 포함)
마케도니아	건강상태 관련 정보(유전정보, 생체인식 정보 포함)
마다가스카르	생체인식 정보, 유전정보, 건강관련 정보
말레이시아	신체적·정신적 건강 및 상태
몰타	건강관련 정보
모리셔스	신체적·정신적 건강관련 정보
멕시코	현재 및 장래의 건강상태, 유전정보
모나코	건강관련 정보, 유전정보
몬테네그로	건강상태 * 정보주체 동의없는 생체인식 정보의 처리를 위해서는 감독기구 사전허가 필요
모로코	건강관련 정보(유전정보 포함)
네덜란드	건강관련 정보
나이지리아	건강관련 정보

노르웨이	건강관련 정보 * 비디오감시의 경우 고지의무
페루	생체인식 정보, 건강관련 정보
필리핀	건강관련 정보, 유전정보, 정부가 발행한 과거 및 현재의 진료기록
폴란드	건강, 유전, 중독 관련 정보
포르투갈	건강관련 정보(유전정보 포함)
루마니아	신체적·정신적 건강상태, 유전정보, 생체인식 정보 * 법적 근거 없는 '민감정보'의 처리 및 비디오감시는 감독기구 사전신고 필요(개인용도나 공공장소 감시는 제외)
러시아	건강상태, 생체인식 정보 * 생체인식 정보에는 특별보안조치 의무대상
세이셸	* '민감정보' 규정은 없으나 신체적·정신적 건강관련 정보는 특별보호조치
슬로바키아	생체인식 정보, 정신적 상태
남아프리카 공화국	건강관련 정보, 생체인식 정보
스페인	건강관련 정보
스웨덴	건강관련 정보
스위스	건강관련 정보 * 관련 판단을 가능케 하는 개인 프로파일도 포함
대만	의료적 치료, 유전정보, 건강검진 정보
트리니다드토바고	신체적·정신적 건강 및 상태
터키	건강관련 정보, 생체인식 정보
아랍에미리트	건강관련 정보
우크라이나	건강관련 정보 * 건강상태, 생체인식 정보, 유전정보 처리시 감독기구 고지의무
영국	신체적·정신적 건강 및 상태
미국	* 몇 개 주에서 진료정보, 건강보험번호, 생체인식 정보에 대해 유출 통지
우루과이	건강관련 정보

위에서 보다시피 민감정보를 보호하고 있는 대부분의 국가에서 건강관련 정보 뿐 아니라 생체인식 정보, 유전정보를 민감정보에 포함하여 보호하고

있다. 바이오 정보에 대한 우리나라의 현행 규율과 비교하여 눈에 띄는 점은, 민감정보를 보호하고 있는 대부분의 국가에서 건강관련 정보, 유전정보 뿐 아니라 생체인식 정보를 민감정보에 포함하여 보호하고 있다. 호주, 보스니아 헤르체코비나, 브라질, 콜롬비아, 체코 공화국, 에스토니아, 인도, 마케도니아, 마다가스카르, 루마니아, 러시아, 슬로바키아, 남아프리카 공화국, 터키 등은 생체인식 정보를 민감정보로서 규율하고 있다. 특히 호주는 생체인식 정보 뿐 아니라 템플릿화한 생체 특징정보도 법률에 명시하여 보호하고 있다. 유럽연합에서 입법한 GDPR이 위 바이오 정보에 대해 전체적으로 민감정보에 포함하였다는 점을 감안하여 볼 때, 유럽연합 회원국이 GDPR을 본격적으로 시행할 2017년 이후로는 더 많은 국가들이 바이오 정보를 민감정보에 포함하여 규율하는 체계를 갖출 것으로 예상된다.

몇몇 국가들에서는 감독기구들의 역할이 눈에 띈다. 라트비아는 건강관련 정보 및 생체인식 정보 처리시 감독기구에 등록의무가 있고, 룩셈부르크는 유전정보, 생체인식 정보의 처리와 비디오 녹화 감시에 감독기구의 사전 허가가 필요할 뿐 아니라 유전정보는 정보주체의 생명을 보호하거나 예방 의학, 의료적 진단, 요양, 치료가 필요할 때에만 처리가 가능하다. 몬테네그로에서는 정보주체의 동의 없이 생체인식 정보를 처리하려면 감독기구의 사전허가가 필요하고, 루마니아에서는 법적 근거가 없는 바이오 정보의 처리 및 비디오감시를 하려면 감독기구에 사전 신고를 해야 한다. 우크라이나의 경우 건강상태, 생체인식 정보, 유전정보 처리시 감독기구에 고지의무가 있다.

특별한 보호조치들을 실시하는 국가들도 있다. 이탈리아, 러시아는 생체인식 정보에 특별보안조치를 의무화하고 있다. 스위스의 경우 건강관련 정보에 국한되어 있기는 하지만 해당 개인정보 뿐 아니라 관련 판단을 가능케 하는 개인 프로파일에 대해서도 민감정보로서 보호하고 있다. GDPR은 전체적으로 프로파일링에 대한 처리를 제한하고 이에 대한 정보주체의 고

지, 열람권 및 반대권 등을 보장하는 규정들을 두고 있다. 특히 민감정보에 기반한 프로파일링의 결과 적용은 원칙적으로 금지하고 있다.

최근에는 프랑스의 생체인식 정보에 대한 규율이 눈에 띈다. 2016년 9월 27일, 프랑스 개인정보 감독기구(CNIL)는 작업장 내 생체인식 정보 사용에 대해 새로운 결정을 발표했다. 추적가능한 생체인식 정보와 그렇지 않은 생체인식 정보를 구분하여 규율하였던 기존 결정을 파기하고, '모든' 생체인식 정보는 추적가능한 개인정보로 본다는 내용이다. 다만 정보주체가 자신의 생체특성 정보에 대한 통제권을 행사하지 못하는 경우 감독기구가 더 강하게 규제한다. 프랑스에서 모든 생체인식 정보의 처리는 CNIL의 사전 허가가 필요하다. CNIL은 생체인식 정보에 대한 이번 결정에서 2018년 무렵 프랑스에서 시행될 GDPR에 따라 개인정보 영향평가 뿐 아니라 프라이버시 중심설계 및 프라이버시 중심설정도 고려하였다고 한다[144].

다. 시사점

해외의 보호 수준을 감안할 때 바이오 정보의 수집, 이용, 결합, 제공 및 판매 등 처리와 관련한 국내 법률의 규범은 다소 모호한 수준이다. 반면 세계 여러 나라가 생체인식 정보, 유전정보, 건강관련 정보를 민감정보로서 특별한 보호를 규정하고 있는 경향은 우리에게 시사하는 바가 크다.

우선 생체인식 정보와 관련하여 그 민감성에 부합하는 보호규정을 정비할 필요가 있다. 특히 여러 법령에서 서로 다른 용어로 정의하고 있는 '생체인식 정보'의 법령용어를 정비하여야 한다. 또한 생체인식 정보를 비롯하

144) "CNIL Publishes New Rules on Biometric Access Control in the Workplace", Hunton&Williams 2016. 9. 30, https://www.huntonprivacyblog.com/2016/09/30/cnil-publishes-new-rules-biometric-access-control-workplace/

여 유전정보 및 건강관련 정보 등 바이오 정보 전체적으로 통일적인 규율을 적용할 수 있어야 한다.

바이오 정보에 대한 보호를 위하여 현행 「개인정보 보호법」상의 민감정보에 대한 보호 조치를 제고할 필요가 있다. 특히 개인정보처리자가 민감정보의 처리를 위해 정보주체로부터 동의를 구할 때 그 동의 요건을 보다 명시적으로 규정할 필요가 있다.

바이오 정보 보호의 민감성에 비추어 가장 중요한 것은 사전 예방이다. 그런 의미에서 현재 제도적 영향력을 크게 발휘하고 있지 못한 개인정보 영향평가 제도 또한 실질화하여 바이오 정보의 처리에 적용할 수 있어야 한다. 더불어 프라이버시 중심설계(Privacy by design) 및 프라이버시 중심설정(Privacy by default)에 대해 적극적으로 도입할 필요가 있다. 실효성을 거두고 있지 못한 개인정보 감독기구의 독립성 강화도 필수적이다. 개인정보 영향평가의 강화, 프라이버시 중심설계 및 설정 및 감독 강화는 유럽 제29조 개인정보보호 작업반은 물론 국가인권위원회도 2013년 <정보인권 보고서>에서 제언한 바 있다.

단기적으로는 위와 같은 내용으로 현행 개인정보 보호 관련 법령을 정비하여 생체인식 정보를 비롯한 바이오 정보를 보호할 수 있겠다. 장기적으로는 바이오 정보 보호에 관해 특화된 법률을 마련할 필요도 있어 보인다. 바이오 정보가 처리되는 모든 생애주기에 있어 목적제한, 최소수집, 비례성, 적합성, 투명성, 안전장치가 보장될 필요가 있다.

제6장

정책 제언

제6장 정책 제언

가. 개인정보 보호 관련 법률 개선 사항

1) 생체인식 정보의 법령용어 정비

생체인식 정보의 규율과 관련한 우선적인 문제점으로는 현재 여러 법령에서 '생체정보' 및 '바이오 정보'의 개념을 혼재하여 사용하고 있는 점을 들 수 있다. 심우민(2016)은 '바이오 정보'라는 용어사용은 법문의 국문사용 원칙을 별론으로 하더라도 생명 및 유전공학 등의 분야에서 활용되고 있는 바이오 정보(bioinformation)의 개념과 다소 혼동될 여지가 있으므로 개선할 필요가 있다고 지적하였다.

생체인식 정보의 구체적인 정의로는 "얼굴 영상이나 지문 정보처럼 개인을 고유하게 식별하거나 확인할 목적으로, 개인의 신체, 생리, 행동 특성에 관하여 특수하게 기술적으로 처리한 결과 발생한 개인정보"로 규정한 GDPR을 참고할 수 있다.

현행 정보통신망법 시행령 상의 정의에 따르면 생체인식 정보는 "지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함"한다. 그러나 식별 또는 확인 목적 이상으로 생체인식 정보의 정의를 확대할 경우 일반적인 사진정보가 모두 이 정의에 따른 규율 대상이 되어 혼선이 빚어질 우려가 있다.

이에 GDPR은 생체인식 정보를 '개인을 특정하게 식별할 목적의 생체인식 정보(biometric data for the purpose of uniquely identifying a natural person)'로 한정하고 있음을 참고할 필요가 있다. 특히 해설전문

은 사진정보가 고유한 식별성을 과도하게 드러내거나 전자여권 등 생체인식 정보로서 개인을 인증할 때에만 민감정보에 포함된다고 설명하고 있다.

[개선권고]

‘개인을 특정하게 식별할 목적의 생체인식 정보(biometric data for the purpose of uniquely identifying a natural person)’를 의미하는 법령용어를 ‘생체인식 정보’로 일관되게 정비한다.

2) 민감정보로서 바이오 정보 규정과 보호

생체인식 정보를 민감정보로서 규율하고 있는 국가가 증가하고 있을 뿐 아니라 유럽연합은 전체적으로 GDPR을 통하여 생체인식 정보를 민감정보에 포함하였다. 이로써 유럽연합은 생체인식 정보, 유전정보 및 진료정보를 포함한 건강관련 정보에 대하여 통일된 규범을 적용하고 있다.

우리 「개인정보 보호법」에서는 정보주체에게 별도로 동의를 받은 경우이거나 법령에서 특별히 요구하거나 허용하는 경우에만 민감정보를 처리할 수 있다. 유전정보 및 건강관련 정보는 민감정보에 포함되어 있으나 생체인식 정보는 포함되어 있지 않다.

이에 생체인식 정보를 「개인정보 보호법」상 민감정보로 포함하여 유전정보 및 건강관련 정보 등 여타의 바이오 정보와 통일적인 규율을 적용할 수 있어야 한다. 나아가 생체인식 정보를 규정한 개별 법률에서도 민감정보에 부합하는 강화된 기술적·관리적 보호수준을 적용해야 한다.

더불어, 어플리케이션과 기기 등으로 수집되는 개인 건강관련 정보가 점점 늘어나는 추세를 반영하여, 이 정보가 진료정보인 경우이거나 직접적으로나 간접적으로 건강 상태에 대해 판단할 수 있는 원본 감지정보인 경우,

혹은 건강 상태에 대한 판단 그 자체인 경우에는 민감정보에 포함되는 건강관련 정보로서 명확히 보호할 필요가 있다.

[개선권고]

민감정보로서 바이오 정보를 명확히 규정하고 전체적으로 통일적이고 강화된 보호 규정을 적용한다.

3) 바이오 정보의 처리에 대한 정보주체의 동의권 강화

민감정보로서 바이오 정보는 원칙적으로 정보주체의 동의나 법률적 근거 없이 처리할 수 없다. 그러나 이때 정보주체의 동의권 행사가 실질적으로 이루어지지 않으면 민감정보로서의 규율 체계 또한 제대로 작동한다고 볼 수 없다는 점이 문제이다. 유럽연합 제29조 개인정보보호 작업반 역시 동의가 잘못될 경우 이는 환상에 불과하며 이후 개인정보 처리의 잘못된 명분이 될수 있다는 점을 우려하고 있다. 이에 작업반은 동의의 정의에 대한 의견에서 민감정보에 대한 '동의'가 '명시적(explicit)'이어야 한다는 점을 강조하며 명시적 동의의 요건에 대하여 설명하였다(Article 29 Data Protection Working Party, 2011).

유럽연합의 95/46/EC 지침이나 GDPR 모두 민감정보의 처리에는 일반 개인정보의 처리에 대한 동의와 달리 정보주체의 '명시적 동의'가 필요하다고 규정하고 있다. 이때 '명시적'이라 함은 정보주체가 개인정보의 '특정한(particular)' 사용과 공개에 대하여 서면이나 구두로 동의 의사를 '능동적으로(actively)' 표시하는 것을 의미한다. 능동적이라는 것은 통상 개인정보 처리자가 왜 개인정보를 수집하고 처리하는지를 명확히 설명한 종이 또는 전자 문서를 제시하고 정보주체가 이에 수기로 직접 서명하는 형식을 의미해 왔다. 그러나 작업반은 민감정보 처리에 대한 동의의 경우 종이 또는 전

자 문서에 의한 통상적인 동의로는 충분치 않다고 본다. 민감정보에 대한 동의 요건이 일반 개인정보처럼 '서면'에 의한 동의가 아니라 '명시적 동의'를 규정하고 있다는 차이점에 주목해야 한다는 것이다.

민감정보에 대한 동의는 정보주체가 동의를 표시하기 위해 적극적인 행동을 취해야 한다. 반대의사를 밝히지 않으면 동의하는 것으로 간주하는 옵트아웃이나 사전에 체크된 동의조항은 명시적 동의가 아니다. 온라인의 경우 버튼 클릭이나 확인 메일, 웹사이트 아이콘 클릭 등이 명시적 동의에 해당한다. 의료기록에 접근할 수 있는 전자의료카드를 발급받기 위해 온라인에서 특정한 디지털 유형으로 서명하는 것도 명시적 동의로 간주될 수 있다.

한편 바이오 정보의 특성상 정보주체의 동의는 원본정보와 특징정보에 대하여 각각 명시적으로 이루어질 필요가 있다. 또 동의를 요구하는 관계가 의료제공자-환자, 사용자-근로자처럼 상대적으로 한쪽이 취약한 조건일 수 있다는 점을 감안하여 정보주체가 충분한 정보를 제공받고 개인정보처리자와 분리된 공간에서 자율적으로 결정할 수 있도록 동의 절차에 관한 구체적인 규정 마련이 요구된다(박경태·최병인, 2014).

특히 최근에는 유전정보나 건강관련 정보 등 민감정보를 학술연구 목적으로 사용할 때 그 민감성을 적절히 보호하고 정보주체에게 좀더 능동적인 선택권을 보장하기 위하여 설명 후 동의(informed consent), 역동적 동의(dynamic consent), 증진된 동의(enhanced consent) 등 동의 요건에 대한 다양한 제도 연구가 이루어지고 있음도 참고할 필요가 있다[145].

[개선권고]

바이오 정보의 처리에 대한 정보주체의 동의 요건을 강화한다.

---

145) Edwin Morley-Fletcher, "Enhanced Consent: a vision for Patient Data Protection and Data Management", http://www.lynkeus.eu/wp-content/uploads/2015/10/Enhanced-consent_Lisbon-ICT15-emf-20-10-15_Discussion-paper.pdf.

4) 바이오 정보에 대한 개인정보 영향평가 실시

생체인식 정보의 처리에 국한되어 있기는 하지만 유럽연합 제29조 개인정보보호 작업반은 바이오 정보에 대하여 개인정보 영향평가의 실시를 권고하였다(Article 29 Data Protection Working Party, 2012).

작업반은 영향평가가 개인정보 처리와 관련된 위험에 대해 평가하는 것이자 이런 위험을 줄이기 위해 고안된 추가적인 수단을 정의하는 것이라고 설명하였다. 영향평가는 위험을 규명하는 데에서 더 나아가, 처리자가 개인정보에 대한 위험을 줄이기 위해 어떠한 적절한 해결책을 실행할 수 있는지, 적정한 보호 수단을 제시할 수 있어야 한다는 것이다.

특히 작업반은 기기 제조업체, 최종 고객 등 모든 관련기관이 시스템 설계 단계의 필수요소로 영향평가를 실행할 것을 권고하였다. 영향평가가 고려할 점은 다음과 같다. ① 수집되는 정보의 특성 ② 정보수집의 목적 ③ 시스템의 정확성 ④ 법적 근거와 동의 취득 등 그 준수사항 ⑤ 보안 기술 및 절차를 의미할 기기 접근과 처리자 안팎의 정보공유 정도 ⑥ 생체인식 기술 대신 신분증을 쓰는 등 덜 침해적인 수단의 채택 여부 ⑦ 보관 기간 및 파기와 관련한 의사결정 내용 ⑧ 정보주체의 권리.

유럽 GDPR의 경우 민감정보의 대규모 처리에 대해서는 개인정보 영향평가가 의무적으로 적용되어야 한다고 규정하고 있다. 우리나라에서는 국가인권위원회가 2013년 <정보인권 보고서>에서 빅데이터 환경에서 개인정보 영향평가의 의무적 도입을 제언한 바 있다.

이에, 「개인정보 보호법」에 규정되어 있지만 현재 제도적 영향력을 크게 발휘하고 있지 못한 개인정보 영향평가 제도를 실질화하여 바이오 정보의 처리에 적용할 수 있어야 한다.

현재 우리 개인정보 보호법 시행령에 따르면 민감정보의 경우 5만 건 이상 처리하는 공공기관만을 대상으로 영향평가를 실시하고 있다. 침해소지가 큰 바이오 정보의 경우, 공공기관 뿐 아니라 민간기관도 영향평가를 의

무화하고 그 대상 기준 또한 현재의 5만 건보다 대폭 확대할 필요가 있다.

[개선권고]
개인정보 영향평가를 실질화하여 바이오 정보의 처리에 대하여 실시한다.

5) 바이오 정보에 대한 프라이버시 중심 설계 적용

유럽 GDPR이 '개인정보보호 중심설계 및 설정(Data protection by design and by default)'을 규정하고 이를 바이오 정보를 비롯한 민감정보에 적용함으로써 프라이버시 중심설계가 주요 법제도 개선 과제로 주목을 받고 있다. 국가인권위원회 또한 2013년 <정보인권 보고서>에서 빅데이터 환경에서 프라이버시 중심설계의 도입을 제언한 바 있다. 특히 신체에 각인되어 있는 바이오 정보의 특성상 이 정보에 대한 오남용은 한번만으로도 정보인권에 치명적인 침해를 가져올 수 있다는 점에서 사전적인 예방으로서 프라이버시 중심설계가 더욱 필요하다.

프라이버시 중심설계의 고안자인 카부키안 박사는 바이오 정보에 대한 프라이버시 중심설계에 대하여서도 몇 가지 안을 제시하였다[146]. 예를 들어 일 대 다수 비교(one-to-many comparison) 생체인식에 적용될 수 있는 프라이버시 중심설계로는 추적불가능한 생체암호(Biometric Encryption, BE) 기술을 들고 있다. BE는 생체인식 정보를 시스템에 저장하지 않고 생체정보와 디지털 키를 결합하거나 생체정보로부터 디지털 키를 생성하는 등 생체적으로 암호화

146) 카부키안 감독관은 9가지 주요 영역에 걸쳐 60여 종 이상의 보고서를 발행하였다고 밝혔는데 ① 대중교통에서 CCTV/감시 카메라 ② 카지노와 게임시설에서 생체인식 정보 ③ 스마트미터와 스마트그리드 ④ 모바일 기기 및 통신 ⑤ 근거리무선통신(NFC) ⑥ RFID와 감지 기술 ⑦ IP 지리정보 재설계 ⑧ 원격의료 ⑨ 빅데이터와 데이터 분석 등이다(Ann Cavoukian, 2013).

된 키를 사용한다. 따라서 생체정보 이미지 원본이나 템플릿이 저장되어 남지 않는다(Ann Cavoukian, 2014). 헬스케어 모니터링 기기에도 프라이버시 중심 설계가 유용하다고 한다(Ann Cavoukian, 2011).

유럽연합 제29조 개인정보보호 작업반은 2012년 의견서에서 생체인식 정보에 프라이버시 중심설계를 적용하는 문제를 상세히 다룬 바 있다 (Article 29 Data Protection Working Party, 2012). 작업반은 생체인식 시스템을 설계할 때 단계별로 ① 위험 분석 혹은 영향평가에 기반한 요구사항의 특정, ② 설계가 어떻게 요구사항을 충족할지에 대한 설명과 정당화, ③ 기능검사와 보안검사를 통한 검증, ④ 최종 설계의 규제 체제 준수 확인 등의 절차를 밟아 프라이버시 중심설계를 실시할 것을 권고하였다.

또 작업반은 관련 기관별로 실시할 수 있는 프라이버시 중심설계의 유형도 제시하였다. 우선 제조업체들(manufacturers)은 신기술과 센서를 설계할 때 생체 특징정보 생성후 원본 생체정보를 자동삭제하도록 하거나, 생체인식 기술을 저장할 때 암호를 사용하는 등으로 프라이버시 중심설계 원칙을 실시해야 한다. 프라이버시 친화적인 생체인식 기술을 개발하기 위한 노력도 필요하다. 통합업체들(integrators, 자사 제품에 생체인식 기술을 통합하는 회사들 - 필자)과 재판매업체들(resellers)은 판매 예정인 최종 제품을 정의할 때 프라이버시 친화적인 기술을 선택하고 최종 제품에 데이터베이스 분산 등 보안 수단을 추가하는 식으로 프라이버시 중심설계 원칙을 실시해야 한다. 생체인식 기술의 고객(장래의 개인정보처리자)은 생체인식 시스템을 요청하거나 시스템의 기술적 요소를 정의할 때 프라이버시 중심설계 원칙을 적용할 수 있어야 하고, 제조업체나 통합업체는 제품에 이를 위한 유연성을 보장해야 한다. 몇몇 제조업체들이 비인가된 접근을 방지하기 위해 생체인식 리더기에 암호 요소나 안티풀링(anti-pulling) 및 안티탬퍼(anti-tamper) 스위치를 포함하고 있다는 사실을 성공사례로 볼 수 있다.

프라이버시 중심설계는 우리 법률에 아직 도입되지 않은 개념이다. 바이

오 정보의 각 특성에 부합하는 프라이버시 중심설계의 구체적인 방안에 대해서는 좀더 연구가 필요하겠으나, 국내에도 프라이버시 중심설계의 원칙적 도입이 필요해 보인다. 특히 바이오 정보를 처리하는 서비스와 기기 등에 대해서는 기획, 설계단계에서부터 프라이버시 중심설계를 제도적으로 보장하는 방안이 마련되어야 할 것이다.

[개선권고]
프라이버시 중심설계를 도입하여 바이오 정보의 처리에 대하여 적용한다.

6) 바이오 정보에 대한 감독 강화

사전 혹은 사후적으로 바이오 정보의 오남용을 방지하기 위해서는 이를 제도적으로 감독하는 체제가 수립될 필요가 있다. 라트비아, 룩셈부르크, 몬테네그로, 루마니아, 우크라이나, 프랑스 등 여러 국가가 바이오 정보의 처리에 대하여 감독기구들이 사전 혹은 사후적으로 강력한 규제를 하고 있다.

우리의 경우에도 바이오 정보의 처리가 정보주체의 권리에 특별한 위험을 초래할 것으로 보일 때 이를 특정하여 개인정보 보호위원회 등 감독기관에 의한 사전 심의를 거치도록 제도화할 필요가 있어 보인다.

다만 현재 「개인정보 보호법」에 의해 대통령 산하에 설치된 개인정보 보호위원회의 경우 그 예산 및 인사에 대한 권한이 정부에 종속되어 있어 충분히 독립적으로 활동하기에 한계가 있다. 국가인권위원회는 2013년 <정보인권 보고서>에서 “개인정보보호위원회를 명실상부한 독립기구로 재편”할 것을 제언한 바 있다.

[개선권고]
바이오 정보에 대하여 독립적인 개인정보 감독기구의 사전 사후 감독을 강화한다.

7) 바이오 정보에 대한 특별한 보호조치

유럽연합 제29조 개인정보보호 작업반은 2012년 의견서에서 생체인식 정보의 특수성에 부합하는 기술적인 보호수단을 제시한 바 있다(Article 29 Data Protection Working Party, 2012). ▲원본정보가 아닌 특징정보의 사용 ▲중앙집중형보다 분산저장형 권장 ▲갱신과 파기 보장 ▲암호화 저장 ▲속임수 방지 ▲생체암호(Biometric Encryption) 선호 ▲목적달성 후 자동삭제 ▲목적내 데이터베이스 규모의 최소화 및 식별정보 분리 등의 기술적 보호수단은 바이오 정보 일반에도 적용할 필요가 있다.

작업반은 생체인식 정보의 유출 등 사고가 발생하였을 때 이를 대체할 수 있도록, 원본정보로부터 복수의 독립적인 특징정보가 추출될 수 있어야 한다고 강조하였다. 또 생체인식 시스템은 식별자와의 결합을 파기할 수 있는 방식으로 설계되어야 하는데 이는 때로 생체인식 정보를 갱신할 필요가 있거나 동의를 철회하였을 경우 삭제할 수 있어야 하기 때문이다.

이처럼 신체에 각인되어 있는 특성상 유출될 경우 쉽게 대체되거나 회복이 불가능하다는 점에서, 바이오 정보는 특징정보를 생성한 후 처리 목적을 달성한 것으로 보고 원본정보 삭제를 원칙으로 삼을 필요가 있다.[147] 특수한 경우 원본정보의 보관이 가능하지만 이는 식별자를 구분하여 저장하도록 한다. 제20대 국회에서 발의된 개인정보 보호법 일부개정법률안(강효

147) 생체인식 정보의 경우, 특징정보(템플릿 정보)도 유출 가능성이 있기 때문에, 그 위험성을 제한하기 위한 '재발급 가능한 템플릿' 기술의 개발도 필요하다.

상의원 대표발의, 의안번호 2030)에서는 비록 생체인식 정보에 국한되어 있기는 하지만 “개인정보처리자는 생체정보를 보관함에 있어 가공되지 아니한 원본정보를 보관하는 경우에는 그 원본정보와 성명·주민등록번호 등 정보주체를 식별할 수 있는 대통령령으로 정하는 개인정보를 별도로 분리하여 보관하여야” 하고(안 제24조의3 제2항), “개인정보처리자가 생체정보의 원본정보로부터 특징정보를 생성한 경우에는 지체 없이 해당 원본정보를 복구·재생할 수 없도록 파기하여야 한다. 다만, 다른 법률에서 허용하는 경우 또는 정보주체의 동의가 있는 경우에는 해당 원본정보를 보관할 수 있다”고(안 제24조의3 제3항) 규정하고 있다는 점을 참고해볼 수 있다.

또한 바이오 정보의 민감성을 고려하여 원칙적으로 대규모 집적을 회피할 필요가 있다. 바이오 정보가 오남용되는 것을 방지하기 위하여 설계 단계에서부터 분산저장도 요구된다. 제29조 개인정보보호 작업반은 분산저장이 개인 리더기로부터 네트워크에 이르기까지 아우르는 개념이라고 보았다. 분산형 시스템은 생체인식 정보주체가 물리적으로 자신의 생체정보를 보다 잘 보호할 수 있는 환경을 제공하고, 탈취되거나 표적으로 삼을 수 있는 대상이 하나로 집중되지 않는다는 장점을 가지고 있다.

한편, 「개인정보 보호법」은 개인정보의 범위를 살아있는 자연인에 관한 정보로 한정함으로써 사망자의 정보보호에 대한 규정을 두고 있지 않다. 그러나 사망자의 유전정보 등 바이오 정보가 공개되는 경우 사망자뿐만 아니라 그 유족에게 피해를 줄 수 있는 가능성이 있기 때문에 관련 심의위원회 등을 두어 필요한 경우에 한해서만 식별정보를 제거한 후 처리하는 등 특별한 보호가 요구된다(박경태·최병인, 2014; 이한주, 2014).

생체인식 정보가 건강관련 정보를 노출하는 등 정보의 민감성이 배가되는 경우에는 추가적인 보호조치를 취하도록 보호하는 방안을 검토해볼 수 있다.

제3자 제공은 법원의 영장을 원칙적으로 요구해야 한다. 다만 통계작성

및 학술연구 목적으로 이용하고자 할 때는 더이상 식별될 수 없는 형태로 익명화해야 할 것이고 그 입증 책임은 개인정보처리자에 두는 것이 바람직하다. 익명화와 달리 가명 처리 등 결합 정보를 통해 개인이 식별되는 비식별화 조치를 할 경우에는 개인정보 처리의 일환으로서 원칙적으로 정보주체의 동의권 행사가 보장되어야 한다.

마지막으로, 민감한 개인 프로파일링 처리가 늘어나는 빅데이터 시대를 대비한 보호 조치 또한 규정할 필요가 있다. 바이오 정보에 기반한 프로파일링과 자동화된 의사결정은 원칙적으로 제한되어야 한다. 특히 바이오 정보는 그 자체로 의료·민족·인종, 특정한 행동에 관한 정보, 성생활에 관한 정보 등과 같이 민감정보가 추출될 위험이 있다. 따라서 이를 기반으로 프로파일링을 처리하는 경우 반드시 정보주체의 별도 동의를 얻도록 제한해야 한다. 유럽 GDPR은 전체적으로 프로파일링에 대한 처리를 제한하고 이에 대한 정보주체의 고지, 열람권 및 반대권 등을 보장하는 규정들을 두고 있다. 특히 민감정보에 기반한 프로파일링의 결과 적용을 원칙적으로 금지하고 있다는 점을 참고할 수 있다.

[개선권고]

바이오 정보의 민감한 특성을 고려한 특별한 보호조치를 도입한다. 이는 ▲원본정보가 아닌 특징정보의 사용 ▲중앙집중형보다 분산저장형 권장 ▲갱신과 파기 보장 ▲암호화 저장 ▲목적달성 후 자동삭제 ▲목적내 데이터베이스 규모의 최소화 및 식별정보 분리 ▲프로파일링 규제 등을 포함한다.

나. 기관별 과제 제안

바이오 정보의 보호를 위하여 국회, 정부, 기업 등 각 주체들이 향후 검토, 수행해야 할 과제들을 다음과 같이 도출할 수 있다.

1) 국회

○ 개인정보 보호 관련 법률 개선

앞서 서술된 개인정보 보호 관련 법률 개선 사항은 대부분 관련 법률 제·개정으로 반영될 필요가 있다. 생체정보, 생체인식 정보, 유전정보, 건강관련 정보의 정의를 명확하게 규정하고, 개인정보 보호법, 정보통신망법, 전자금융거래법, 생명윤리 및 안전에 관한 법률 등 관련 법률이 통일성을 유지할 수 있도록 정비할 필요가 있다.

또한, 민감정보로서 생체인식 정보를 비롯한 바이오 정보의 보호 강화, 바이오 정보에 대한 동의 요건의 강화, 프라이버시 중심 설계의 도입, 개인정보 감독기구 강화, 바이오 정보에 대한 특별한 보호조치 등 바이오 정보 보호 강화를 위한 규정들을 개인정보 보호법에 반영할 필요가 있다.

이와 함께, 바이오 정보 보호에 대하여 별도의 법률을 두어 특별히 보호할 것인지에 대하여 장기적인 과제로 검토가 요구된다. 바이오 정보가 처리되는 모든 생애주기에 있어 목적제한, 최소수집, 비례성, 적합성, 투명성, 안전장치 등의 원칙이 보장되어야 한다.

○ 수사 목적의 개인정보 수집에 대한 규제 강화

고도화된 생체인식 장치들이 구체적인 법률적 근거나 사회적인 검토없이 수사기관의 자체적인 판단만으로 도입되고 있는 것은 문제이다. 통상 수사기관에 의한 개인정보 수집은 경찰법 3조, 경찰관직무집행법 2조상 '치안정보의 수집, 작성 및 배포' 조항에 의해 정당화되는데, 기술발전으로 인해 심각해지는 프라이버시 침해의 위험성을 고려할 때 이것이 충분한지는 의

문이다. 또한, 수사기관이 과거에도 범죄 용의자의 지문, 얼굴 등 바이오 정보를 비롯한 개인정보를 수집해왔다고 하더라도, 첨단기술을 이용한 자동화된 수집, 데이터베이스의 구축, 자동화된 검색 기능 등을 고려할 때 개인에게 미치는 영향은 과거와 비할 바 없이 커졌다. 수사기관의 개인정보 수집 및 이용에 대해서 법적 근거 및 사회적 감독 체제의 마련이 필요하다.

○ 전 국민 지문날인에 대한 재검토 및 법적 근거 마련

비록 헌법재판소가 2005년에 이어 2015년 5월에도 지문날인 제도에 대해 합헌 결정(2011헌마731 주민등록법 시행령별지 제30호 서식위헌확인)을 내리기는 했지만, 현행 지문날인 제도는 열손가락 지문날인과 경찰청이 이 정보를 보관하는 것에 대한 구체적인 법적 규정을 가지고 있지 않다. 국회는 만17세 이상의 모든 국민의 열손가락 지문정보를 수집할 필요성에 대해서 검토하고, 수집이 필요하다고 하더라도 '그 목적과 대상, 범위, 기한 등의 요건'을 구체화하는 입법을 할 필요가 있다.[148)]

148) 헌법재판소 역시 결정문에서 "국가는 개인정보자기결정권을 제한함에 있어 개인정보의 수집·보관·이용 등의 주체, 목적, 대상 및 범위 등을 법률에 구체적으로 규정함으로써 그 법률적 근거를 보다 명확히 하는 것이 바람직하므로, 지문정보의 수집·보관·활용에 있어서도 그 목적과 대상, 범위, 기한 등의 요건을 구체적으로 규정하는 입법개선의 노력이 필요하다"고 지적한 바 있다. 한편, 김일환(2012)은 "헌법재판소 다수의견은 주민등록법 제17조의8 등 위헌확인 사건에서 주민등록법상 지문정보의 수집을 합헌이라고 결정하여 과거의 비민주적이고 반법치적으로 도입되었던 지문날인제도의 합헌성을 인정하였을 뿐만 아니라, 이렇게 수집된 지문정보를 그대로 경찰청장에게 넘겨 이를 전산화하고 이용하는 것 또한 인용하여 지식정보사회에서 개인정보의 새로운 침해를 허용하였다. 우리는 헌법재판소의 위와 같은 결정을 통하여 과거의 잘못된 기본권침해를 바로잡지 못하면 지식정보사회에서 우리가 과거에 상상할 수 없었던 새로운 기본권침해를 받을 수 있음을 인식해야 한다. 경찰청장이 보관·전산화하고 있는 지문정보를 범죄수사활동, 대형사건사고나 변사자가 발생한 경우의 신원확인, 타인의 인적사항 도용 방지 등 각종 신원확인의 목적을 위하여 이용함으로써 달성할 수 있게 되는 공익이 그로 인한 정보주체의 불이익에 비하여 더 크다고 헌법재판소 다수의견은 주장하고 있지만 소수의견이 정확하게 지적하고 있듯이 범죄전력이 없는 모든 일반 국민의 열손가락의 회전지문과 평면지문 일체를 법

○ 영상정보처리기기 및 얼굴인식 기술에 대한 법제 개선

현행 개인정보 보호법은 CCTV와 같은 영상정보처리기기에 대한 규정을 두고 있지만, 통합관제센터, 블랙박스, 바디캠, 드론 등 그 규제 대상에서 제외되어 있거나 수집된 영상정보를 얼굴인식 기술을 사용하여 분석하는 것에 대해서는 규율하고 있지 못하다. CCTV외 영상정보처리장치를 규율할 수 있는 내용을 포함하는 한편, CCTV 등 영상정보처리장치가 한정된 목적으로만 사용되고 목적 외 용도로 사용되지 못하도록 엄격하게 제한할 필요가 있다. 또한, 지능형 CCTV 등 진화하는 영상정보처리기기에 의한 개인정보 수집 및 얼굴인식 기술은 기존의 영상정보 수집에 비해 프라이버시에 대한 침해 수준이 높기 때문에 대상이 특정되지 않은 무차별 검색이나 실시간 검색 등은 보다 엄격하게 규제할 필요가 있다.

○ 전자적 노동감시 통제를 위한 법제 마련

사업장 내와 같이 사업주와 근로자 사이의 불균등한 권력관계 하에서 정보주체의 '동의'는 실질적인 의미를 갖지 못한다. 현재 국내에는 노동감시를 규제하는 입법이 마련되어 있지 않다. 따라서 국회는 노동감시를 규제할 수 있는 법제를 시급히 마련할 필요가 있다. 이미 국가인권위원회는 2007년 11월 27일, 노동부장관에게 사업장의 각종 전자감시를 적극적으로 규제할 수 있도록 별도의 특별법 제정과 이에 포함시켜야 할 인권보호의 구체적 내용들을 권고하였으나 정부는 이 권고를 수용하지 않았다.[149] 또한, 국가인권위원회는 2014년 '정보통신기기에 의한 노동인권침해 실태조사' 결과를 발표하면서, 노동자에 대한 전자감시는 강력한 금지가 원칙이

적 근거 없이 경찰청장이 수집, 보관, 전산화하고 있다가 이를 그 범위, 대상, 기한 등 어떠한 제한도 없이 일반적인 범죄수사목적 등에 활용하는 것은 개인정보자기결정권에 대한 최소한의 침해라고 할 수 없다."고 헌법재판소의 결정을 비판하고 있다.

149) 국가인권위원회 결정 2007.11.12, 사업장 전자감시에서 근로자의 인권보호를 위한 법령·제도 개선권고

고, 극히 예외(기술 유출, 절도 등)적으로만 허용해야 한다는 입장과 함께, 전자노동감시에 따른 개인정보보호 가이드라인 및 입법방향을 제시한 바 있다.[150]

○ 디엔에이 관련 법제의 개선

디엔에이법에서는 DNA 신원확인 정보의 활용에 대해서만 규제하고 있다. 그러나 실제 수사과정에서는 Y 염색체, 미토콘드리아 DNA, 생물학적 특성을 추측할 수 있는 차세대염기서열 분석 등이 사용되고 있어 이에 대한 법적 규제가 시급하다. 또한, 현재 11개인 DNA 데이터베이스 입력 범죄 대상을 입법 취지에 맞게 흉악범으로 축소해야한다. 집행유예, 벌금형까지 DNA를 채취해 평생 보관하는 것이 적절한 것인지 재검토되어야 한다.

DNA 집단검색에 대한 규정이 마련되어야 한다. 수사상의 필요에 의해 특정 지역 거주자나 일정 규모 이상의 시민들의 DNA를 채취할 경우에는 채취 목적, 규모, DNA 활용 범위 등에 규정이 필요하다. 데이터베이스에 입력된 특정인과 유전정보를 공유하는 친족들에 대한 검색은 금지되어야 한다.

6.25 전사자 유해 발굴 사업에 사용되고 있는 DNA 정보 수집, 활용 동의서 양식을 수정해 신원확인 목적의 유전자 검사만 가능하도록 해야 한다. 법률적 기반 없이 추진되고 있는 군인들에 대한 혈액 채취는 중단되어야 한다.

실종아동 등의 DNA 데이터베이스에서는 채취 대상을 엄격히 제한할 필요가 있다. 법률 제정의 취지는 실종아동의 신상정보가 부족하거나 장기미아일 경우 DNA 신원확인 정보를 활용하는 것이었다. 그러나 최근 채취 대상이 정신지체 장애인이나 치매 환자로까지 확대 되었으며, 실종아동도 만18세까지로 확대되었고, 신상정보가 명확하거나 굳이 필요하지 않은 경우에도 채취되고 있는 실태가 개선되어야 한다.

---

150) 국가인권위원회(2014), 정보통신기기에 의한 노동인권 침해실태조사 주요 내용, 2014.1.14

○ 스마트기기나 웨어러블 디바이스를 통해 수집된 건강관련 정보의 보호

아직까지 스마트기기나 웨어러블 디바이스를 통해 수집된 건강관련 정보에 대해 개인정보 보호법이나 의료법에 저촉이 되는지에 여부를 놓고 판별하는 사례는 발생하지 않았으나, 점차 관련 기기의 활용도가 높아짐에 따라 충분한 법적 보호 장치가 마련되어야 한다.

피드백 서비스 제공을 위한 어플리케이션은 기업의 클라우드에 개인의 건강관련 정보가 수집되고 저장될 수밖에 없다. 이 경우 현재의 법률에 저촉될 가능성이 크고 유출 위험성이 더욱 커지므로, 이에 대한 법적, 제도적 보완이 필요하다. 아울러 최근 각종 건강관련 정보 어플리케이션을 통합 관리할 수 있는 플랫폼(예: 애플 헬스킷)에서는 각 어플리케이션 간에 건강관련 정보가 공유될 수 있으므로 이에 대한 제도적 대책이 필요하다.

미국처럼 스마트폰 웨어러블 디바이스는 물론 어플리케이션까지 포함한 관련 법규정을 제정할 필요가 있으며, 여기에는 한국의 특수성(주요 민간보험회사들이 주요 IT기업은 물론 주요 의료기관까지 거느린 대기업의 계열사인 상황, 전국민건강보험의 존재)이 적극 고려될 필요가 있다.

2) 정부

○ 생체인식 시스템에 대한 투명한 공개

정부(특히 수사기관)는 공공영역의 생체인식 기기 도입 현황 및 생체인식 정보 보유 현황, 생체인식 시스템의 법적 근거 및 운용 정책, 생체인식 시스템 보호조치 등 생체인식 시스템과 관련한 정보를 투명하게 공개하여야 한다.

○ 생체인식 시스템의 신중한 도입 및 개인정보 영향평가

공공기관에서 생체인식 시스템을 도입할 경우 그 필요성을 심도 있게 검토할 필요가 있다. 생체인식 기술에 과도한 신뢰를 두어서는 안 된다. 생체인식 기술 자체에 내재된 오류 가능성을 고려해야 하며, 생체인식 기술을

대체할 대안적인 방법을 고려해야 한다. 지문인식기 도입을 고려하는 경우, 지문이 훼손된 사람이나 지문인식기의 사용을 원하지 않는 정보주체의 의사를 존중해야 하며, 나아가 그 설치 목적에 비례하여 생체인식 시스템의 도입이 필수적인지 검토해야 한다. 생체인식 시스템을 도입할 경우에도 생체인식 시스템을 운용하는 사람이 그에 필요한 지식을 갖출 수 있도록 교육되어야 하며, 생체인식 기기의 정확도에 대해서도 주기적인 점검이 필요하다. 이러한 일련의 검토를 효과적으로 수행하기 위해 생체인식 시스템에 대한 개인정보 영향평가를 수행할 필요가 있다.

○ CCTV 통합관제센터 운영 재검토

수사기관은 CCTV를 애초의 설치목적 외로 활용해서는 안 된다. 현재 구체적인 법률적 근거가 없이 추진되고 있는 CCTV 통합관제센터의 운영 중단을 재검토하여야 한다. 법률적 근거가 없는 유사 생체인식 기술의 도입을 추진해서는 안 된다.

○ 바이오 정보 오남용에 대한 사회적 감독 강화

사전 혹은 사후적으로 바이오 정보의 오남용을 방지하기 위해서는 이를 제도적으로 감독하는 체제가 수립될 필요가 있다. 국내에는 이미 개인정보 감독기구인 개인정보보호위원회가 존재한다. 개인정보보호위원회는 바이오 정보의 처리가 정보주체의 권리에 특별한 위험을 초래할 경우 사전 심의를 거치도록 하는 등 감독기구로서의 역할을 강화해야 한다. 이를 위해 현행 개인정보보호위원회의 독립성과 권한을 강화하기 위한 제도적 기반이 마련된 필요도 있다.

○ 웨어러블 디바이스의 부작용을 방지하기 위한 연구 및 관리

현재 웨어러블 디바이스의 효용성과 정확성에 대한 학계 차원에서 회의

적인 검토가 이루어지고 있다. 정부는 관련 업체나 이해를 가진 기관에서 생성되고 있는 정보에만 의존해서는 안 되며 정부 차원에서 객관적인 정보를 수입하여 이를 국민들에게 알릴 필요가 있다.

효용성, 정확성, 보안 문제가 해결되지 않은 상태에서 웨어러블 디바이스 사용에 대하여 민간보험 적용이 이루어지는 것은 건강관련 정보 유관 산업에 대한 과도한 거품을 생산할 수 있으며, 공적 보험에까지 영향을 줄 수 있는 문제이기 때문에 정부차원의 시급한 개입과 관리가 필요하다.

또한, 건강관련 정보와 관련된 문제점들에 대한 대비책이 제대로 갖춰지지 않은 상황에서 국가차원의 만성질환관리사업에 웨어러블 디바이스를 활용하는 것은 심각히 재고되어야 한다.

주요 민간보험회사들이 주요 IT기업은 물론 의료기관까지 포괄하고 있는 대기업의 계열사인 한국의 특수성을 고려하여 이를 관리·감독할 별도의 부서나 기관을 둘 필요가 있다.

3) 기업

○ 생체인식 기술의 신중한 도입 및 대체수단 제공

공공기관과 마찬가지로 민간 업체에서도 생체인식 기술 도입을 검토할 경우, 그 필요성 및 운영방안 등을 그 도입 목적에 비례적인지 우선 검토할 필요가 있다. 도입이 필요할 경우에도 이를 원하지 않는 사람을 위한 대체수단을 제공해야 한다.

○ 생체인식 정보 보호를 위한 기술 및 자율규제 개발

생체인식 기술 업계 혹은 이와 연계된 서비스 업계는 생체인식 정보에 대하여 일반 개인정보보다 높은 수준의 보안 장치를 마련해야 한다. 즉, 동일한 목적을 달성하면서도 개인의 프라이버시 침해를 최소화할 수 있는 기술 개발 및 서비스 설계(예를 들어, 재발급 가능한 템플릿 기술, 생체인식

정보의 분산 저장 등)를 위해 노력해야 한다. 또한 생체인식 기술의 정확도를 과장해서는 안 된다. 생체인식 기술업계 자체적으로 이용자의 프라이버시를 보호할 수 있는 자율규제 기준을 만들어 시행할 필요가 있다.

○ 건강관련 정보 활용에 대한 신중한 접근

스마트기기 어플리케이션이나 웨어러블 디바이스를 생산하는 기업은 건강관련 정보가 다른 정보보다 훨씬 민간한 정보임을 인식하고 별도의 관련 법적, 제도적 정비가 진행되기 전까지는 일단 기존의 개인정보 보호법과 의료법의 원칙에 입각하여 정보의 취급에 신중해야 한다. 건강관련 정보를 취급하는 스마트기기 어플리케이션과 웨어러블 디바이스가 이 정보를 기기 자체에서만 기록·저장되는 것을 원칙으로 할 필요가 있다.

○ 정보주체의 권리 보장

바이오 관련 기술이나 서비스를 제공할 때 사용자, 이용자, 환자 등 정보주체의 권리를 보장해야 한다. 페이스북의 '이름표 추천' 기능과 같이 생체인식 정보를 본인의 동의 없이 노출하는 서비스의 제공을 지양하여야 한다. 건강관련 정보의 경우 원칙적으로 스마트기기 어플리케이션이나 웨어러블 디바이스에서 수집된 건강관련 정보가 본인의 동의 혹은 대상자가 수집 사실을 인지할 수 있도록 명확히 고지하지 않고 수집되거나 제3자에게 제공되어서는 안 된다.

○ 프로파일링 처리에 대한 정보주체의 권리 보장

바이오 정보에 기반하여 소비자나 노동자 등 특정 개인에 대한 판단을 내릴 경우, 생체인식 기술에만 의존하는 판단을 배제하고, 프로파일링 처리에 대한 정보주체의 권리를 보장해야 한다.

참고 문헌

- 구본권(2014), 『당신을 공유하시겠습니까?』, 어크로스.
- 국가인권위원회(2013), 『정보인권보고서』
- 권건보(2005), 『개인정보보호와 자기정보통제권』, 경인문화사.
- 권석준(2014), 『개인별 맞춤의료 구현을 위한 산업 기술 개발 동향』, BRIC View 2014-T02.
- 권창국, 방충원(2013) 『DNA 데이터베이스의 재 고찰: YSTR 분석 및 가계검색(Familial Search)을 통한 데이터베이스의 우회적 확장문제』, 한국경찰학회보 15권 6호
- 금융결제원(2015), 『바이오인증활성화방안』, <금융분야바이오인증 활성화전략세미나>, 2015년 7월 30일.
- 금융보안원(2016), 『바이오 정보 사고사례 및 대응방안 조사』, 2016년 3월 4일.
- 김경환(2016), 『바이오 정보(Biometrics)와 신산업발전』, 법무법인 민후, http://www.minwho.kr/bbs/board.php?bo_table=archive&sca=%B0%B3%C0%CE%C1%A4%BA%B8.
- 김동진(2016), 『바이오인증 최신 활용 및 보안 동향』, 전자금융과 금융보안, 2016년 7월.
- 김병수(2005) 『유전자감식기술의 사회윤리적 쟁점. 생명윤리』, 6(1), pp.13~23, 한국생명윤리학회
- 김병수(2014) 『한국생명공학논쟁』, 알렙
- 김봉수(2015), 『범죄수사상 생체정보의 수집 및 활용에 대한 규범적 통제』, 법학논총, pp.35(2), pp.255~276.

○ 김일환(2012), 『주민등록법상 지문정보의 목적 외 이용에 대한 헌법적 고찰』, 公法硏究 第41輯 第1號, 한국공법학회.
○ 김장원, 홍승균, 정한민(2014), 『웨어러블 컴퓨팅 환경에서의 센서 역할 및 활용 방향』, 주간기술동향 2014년 7월 23일, 정보통신기술진흥센터.
○ 김재성(2013), 『모바일 바이오인식 신융합기술 및 표준화 동향』, Internet & Security Focus 2013년 3월호, pp.54~78.
○ 김주한(2015), 『빅데이터 기반 개인 맞춤의료 서비스』, BioINpro 13호, 생명공학정책연구센터.
○ 김진숙(2014), 『미국의 개인 의료정보와 원격의료기기 보안의 취약 사례』, 의료정책포럼 2014 vol.12. no.3.
○ 김치원(2015), 『디지털 헬스케어의 역습』 발표자료, 2015년 1월 28일.
○ 김한주(2014), 『스마트 웨어러블(사용자 관점에서의 접근)』, 주간기술동향, 2014년 10월 1일, 정보통신기술진흥센터.
○ 김혜리, 홍승필, 박수민(2016), 『개인정보보호 가이드라인 연구 : 사물인터넷 환경의 개인정보 보호 사례 연구 분석을 통해』, 보안공학연구논문지 Vol.13, pp.155~168
○ 미래창조과학부, 산업통상자원부(2015), 『K-ICT 스마트 디바이스 육성 방안(안)』, 2015년 9월 22일.
○ 박경태, 최병인(2014), 『연구대상자 개인정보보호에 관한 고찰』, 한국의료법학회지 제22권 제2호.
○ 박광만, 석왕헌, 고순주(2014), 『The Next Smart Thing: 웨어러블 디바이스』, 한국전자통신연구원.
○ 박노형(2010), 『EU 및 영국의 개인정보 보호법제 연구』, 법제처.
○ 박정훈(2012), 『바이오매트릭스의 이용에 따른 법적 과제』, 慶熙法

學 제47권 제4호.
○ 박정훈, 김행문(2008),『생체정보 프라이버시의 쟁점 및 정책 시사점 - 전자여권 사례를 중심으로』, 정보화정책 제15권 제3호, 2008년 가을호.
○ 송초롱, 박재혁, 이재우(2015).『바이오 인식 기술 적용 현황 및 서비스 문제점 연구』. 정보보호학회지, pp.25(3), pp.66~76.
○ 심수민(2014),『2014 웨어러블 디바이스 산업백서』, 디지에코보고서, 2014년 1월 10일.
○ 심우민(2016),『스마트 시대의 생체정보 보호를 위한 입법과제』, 이슈와 논점, 제1129호.
○ 심홍진(2014),『빅데이터와 라이프로깅(Life-logging): 현황과 전망』, ICT 인문사회융합 동향 Vol. 01, 2014년 3월호.
○ 윤재호, 홍진실(2016),『바이오인증기술 최신 동향 및 정책과제』, 2016년 8월.
○ 이숭덕 外(2011),『가족관계를 이용한 DNA데이터베이스 검색』, The Korean Jounal of Legal Medicine, pp.92~97
○ 이윤희, 이중정(2016),『생체신호 모니터링 디바이스』, KISTI maket report 2016-25.
○ 이은우(2004),『지문 등 생체정보이용, 무엇이 문제인가』, 국가인권위원회 토론회 2004년 11월 23일.
○ 이은우(2016),『마케팅 활용 목적 빅데이터 활용과 판매 - 개인정보 플랫폼 기업의 탐욕과 비식별화 조치 가이드라인』, 빅데이터 시대 개인정보 보호를 위한 정책토론회, 2016년 9월 7일, 권은희 의원 주최.
○ 이재득(2014),『바이오인식 기술의 금융서비스 적용 현황 및 발전과제』, 지급결제와 정보기술 제57호, 2014년 7월.

○ 이제관(2015),『헬스케어 웨어러블 디바이스 적용기술 서비스 사례와 주요과제』, 대한병원정보협회 발표 슬라이드.
○ 이한주(2014),『개인의료정보보호법 제정의 필요성과 입법방향』, 한국의료법학회지, 22(1), 177-208.
○ 장상수(2015),『핀테크(Fintech)가 정보보호산업에 미치는 영향에 대한 고찰』, Internet & Security Focus, 2015년 2월.
○ 장여경(2013),『DNA 데이터베이스와 감시, 시민과학 98호, 시민과학센터』
○ 장하나(2014),『<CCTV 통합관제센터> 현황 최초 전수조사 발표』, 2014년 3월 24일, http://act.jinbo.net/wp/wp-content/uploads/2014/03/20140324report.pdf.
○ 정보통신부(2007),『바이오 정보보호 가이드라인』
○ 조남수 外(2013),『연쇄 성 폭행범 검거를 위한 강력하고 효과적인 DNA 정보의 적용』, 과학수사학 Vol.7 No.2
○ 진보네트워크센터(2016),『정보인권의 이해』, 2016년 7월 28일, http://guide.jinbo.net/digital-rights.
○ 최보성(2015),『웨어러블 기술 및 시장동향』, S&T Market Report vol.26, 2015년 2월호, 연구성과실용화진흥연구원.
○ 최우현(2015),『바이오인식기술을 활용한 지급결제방법에 관한 연구』, 2015년 6월.
○ 최윤희, 정혜린(2015),『모바일 세계가 주목하는 미래 스마트헬스케어산업』, e-KIET 산업경제정보 제609호(2015-06), 산업연구원.
○ 편석준(2016),『웨어러블 디바이스의 현재 가치와 미래』, 기계저널 : 大韓機械學會誌 v.56 no.2.
○ 한국법제연구원(2013),「정보통신기기에 의한 노동인권 침해 실태조사」,『2013년도 국가인권위원회 인권상황실태조사 연구용역보고

서』, 2013년 12월 21일.
○ 한국정보보호산업협회(2015), 『2015 국내 정보보호산업 실태조사』, 한국인터넷진흥원 발주 보고서, 2015년 12월.
○ 한국정보화진흥원(2016), 『2015 정보화통계집』, 2016년 1월.
○ 행정안전부(2011), 『개인정보 보호법령 및 지침·고시 해설』.
○ 허영, 양종수, 박경환, 차순주, 최덕주, 황경훈(2013), 『개인건강기록(PHR) 서비스 기술 및 산업동향』, KEIT PD Issue Report, November 2013, Vol 13-11.
○ 헌법재판소(2005), 99헌마513, 판례집 제17권 제1집, 2005년 5월 26일.
○ Healthcare Business(2014), 『모바일 심전도 AliveCor: 기대와 현실의 괴리』, 2014년 8월 25일.
○ HT R&D 이슈리포트(2013), 『맞춤의료(Personalized Medicine) R&D 조사분석 보고서』.
○ Forbes(2014), 『IBM And Epic Apply Predictive Analytics To Electronic Health Records』, 2014년 2월 19일.
○ IT World(2015), 『생체인식 기술의 장단점, 그리고 프라이버시』, IDG Tech Report, 2015년 11월 20일.
○ KB금융지주경영연구소(2014), 『KB 지식 비타민 : 금융산업에서 생체인식 기술의 활용 현황과 전망』. 2014년 6월 2일.
○ Am Fam Physician(2004), 『U.S. Preventive Services Task Force - Screening for Coronary Heart Disease with Electrocardiography: Recommendation Statement』, 2004 Jun 15;69(12):2891-2894.
○ Ann Cavoukian(2011), 『Privacy by Design Strong Privacy Protection - Now, and Well into the Future』, A Report on the State of PbD to the 33rd International Conference of

Data Protection and Privacy Commissioners, https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf

○ Ann Cavoukian(2013), 『Privacy by Design』, Information and Privacy Commissioner of Ontario, https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-primer.pdf

○ Ann Cavoukian(2014), 『Privacy by Design Solutions for Biometric One-to-Many Identification Systems』, Information and Privacy Commissioner of Ontario, http://www.ontla.on.ca/library/repository/mon/28006/327359.pdf

○ Article 29 Data Protection Working Party(2009), 『Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)』, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf

○ Article 29 Data Protection Working Party(2011), 『Advice paper on special categories of data ("sensitive data")』, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf.

○ Article 29 Data Protection Working Party(2011), 『Opinion 15/2011 on the definition of consent』, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

○ Article 29 Data Protection Working Party(2012), 『Opinion 3/2012 on developments in biometric technologies』,

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

○ Article 29 Data Protection Working Party(2014), 『Opinion 05/2014 on Anonymisation Techniques』, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

○ Article 29 Data Protection Working Party(2015), 『ANNEX - health data in apps and devices』, Letter from the ART 29 WP to the European Commission, DG CONNECT on mHealthpdf, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

○ BCC Research(2014), 『Wearable Computing: Technology, Applications and Global markets』, February, 2014.

○ BCC Reseach(2014), 『Mobile health technology & Global market』, March 2014.

○ Bird & Bird(2016), 『Sensitive data and lawful processing』, http://www.twobirds.com/~/media/pdfs/gdpr-pdfs/25--guide-to-the-gdpr--sensitive-data-and-lawful-processing.pdf?la=en.

○ Brian Dolan(2014), 『In-Depth: Revisiting Topol's Top Ten Digital Health Targets』, mobihealthnews, April 25, 2014

○ Center on Privacy&Technology at Georgetown Law(2016), 『The Perpetual Line-UP, Unregulated Police Face Recognition in America』, https://www.perpetuallineup.org.

○ Christopher R. Smith(2012), 『SOMEBODY'S WATCHING ME:

PROTECTING PATIENT PRIVACY IN PRESCRIPTION HEALTH INFORMATION』, Vermont Law Review [Vol. 36:931], http://lawreview.vermontlaw.edu/wp-content/uploads/2012/09/16-Smith.pdf.

- DLA Piper(2016), 『DLA Piper's Data Protection Laws of the World Handbook』, 2016. 10. 31.
- Espicom(2013), 『Worldeide Medical Market Forcast to 2018』.
- European Union Agency for Fundamental Rights·Council of Europe(2014), 『Handbook on European data protection law』, 함인선 역, 2015, 유럽정보보호법, 전남대학교 출판부, http://www.echr.coe.int/Documents/Handbook_data_protection_KOR.pdf
- IDC Research, Inc(2015), 『IDC News Letter』, 2015.4.6.
- IDC Research, Inc(2016), 『IDC press release: IDC Forecasts Wearables Shipments to Reach 213.6 Million Units Worldwide in 2020 with Watches and Wristbands Driving Volume While Clothing and Eyewear Gain Traction』, 15 Jun 2016.
- IDC Research, Inc(2016), 『Worldwide Quarterly Device Trackers』, June 15 2016.
- John M. Jakicic et al(2016), 『Effect of Wearable Technology Combined With a Lifestyle Intervention on Long-term Weight LossThe IDEA Randomized Clinical Trial』, JAMA. 2016;316(11).
- John M. Butler (2010), 『Fundamentals of Forensic DNA Typing』, Academic Press
- Marcia M. Boumil, Kaitlyn Dunn, Nancy Ryan, Katrina Clearwater(2012), 『Prescription Data Mining, Medical Privacy and the First Amendment:

The U.S. Supreme Court in Sorrell v. IMS Health Inc.』, Annals of Health Law [Volume 21, Winter 2012], http://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1007&context=annals.

- Privacy International(2013), 『Biometrics: Friends or foe of privacy?』, 2013.12.13.
- Rupinder Saini, Narinder Rana(2014), 『Comparision of Various Biometric Methods』, International Journal of Advances in Science and Technology(IJAST), Vol2 Issue 1, March 2014, Science Publications.
- Statewatch(2011), 『Statewatch Briefing: ID Cards in the EU: Current state of play』, http://www.statewatch.org/analyses/no-107-national-ID-cards-questionnaire.pdf
- Young DR, Tun Z, Honda K, Matoba R. (2001), 『Identifying sex chromosome abnormalities in forensic DNA testing using amelogenin and sex chromosome short tandem repeats』, J Forensic Sci., 46(2), 346-348.

부 록

바이오 정보 활용 및 보호에 관한 인식, 태도 조사

안녕하십니까? 본 조사는 국가인권위원회가 본 기관에 용역을 주어 진행되는 조사이며, 바이오 정보 활용 및 보호에 대한 인식, 태도 등을 파악함으로써 정보 인권 보호를 위한 정책을 마련하고자 함입니다. 본 설문지의 모든 문항에는 맞고 틀리는 답이 없으므로 본인의 솔직한 의견을 있는 그대로 대답하여 주시면 감사하겠습니다. 설문내용 및 응답자에 대한 모든 비밀은 철저하게 보장되며, 모아진 설문지는 통계목적으로만 이용되어 집니다. 이 조사에 대하여 의문사항이 있으시면 (사)인도주의실천의사협의회(전화 02-766-6024, Fax 02-766-6025)로 연락하여 주십시오. 감사합니다.

2016. 9

국가인권위원회

(사) 인도주의실천의사협의회

1. 최근 지문, 정맥, 홍채 등을 이용한 생체인식 기술이 실생활에 도입되고 있습니다. 귀하는 가정이나 직장, 은행 공공기관 등에서 손가락의 지문, 눈의 홍채, 손의 정맥을 이용해 본인 인식을 현재까지 한 번이라도 해 본 경험이 있습니까?

① 있다 → 문 2-1
② 없다 → 문 3
③ 잘 모르겠다 → 문 3

2-1. (있다면) 다음의 본인 인식 방법 중 경험한 것 모두 표시 해 주십시오 (중복 체크)

① 지문을 이용한 본인 인증
② 눈의 홍채를 이용한 본인 인증
③ 손의 정맥을 이용한 본인 인증
④ 기타 _____

2-2. (사용 경험이 있는 분만) 귀하가 사용한 생체인식 시스템은 어떤 목적으로 사용된 것입니까? (중복 체크)

① 금융 거래를 위한 본인 인증
② 건물 출입을 위한 본인 인증
③ 출퇴근 확인을 위한 본인 인증
④ 투표를 위한 본인 인증
⑤ 스마트폰 잠금 해제
⑥ 주민센타등 공공기관의 민원 서비스 본인 인증
⑦ 기타(구체적으로 :)
⑧ 모르겠다

3. 귀하는 금융 거래를 위해 지문이나 홍채 등을 통한 본인 인증을 할 의향이 있으십니까?

① 매우 그렇다.
② 조금 그렇다.
③ 별로 그렇지 않다.
④ 매우 그렇지 않다.
⑤ 잘 모름

4. 귀하는 출퇴근 확인용으로 지문이나 홍채 등을 통한 본인 인증을 하는 것에 대해 찬성하십니까?

① 적극 찬성
② 다소 찬성
③ 다소 반대
④ 적극 반대
⑤ 잘 모름

5. 귀하는 공항이나 건물 등의 보안 목적으로 지문이나 홍채 등을 통한 본인 인증을 하는 것에 대해 찬성하십니까?

① 적극 찬성
② 다소 찬성
③ 다소 반대
④ 적극 반대
⑤ 잘 모름

6. 현재 주민등록증 발급 시 국민의 열 손가락 지문을 채취, 보관, 이용하고 있습니다. 귀하는 성인이 된 전 국민의 열 손가락 지문을 국가가 수집하는 것에 대해 찬성하십니까?

① 적극 찬성
② 다소 찬성
③ 다소 반대
④ 적극 반대
⑤ 잘 모름

7. 생체정보를 이용한 본인 인증 시스템에 대해 귀하가 가장 우려하는 점은 무엇입니까? (2개를 골라주세요)

① 제대로 인식하지 못하는 인식 오류 문제
② 내 생체정보가 도용되거나 위조될 가능성
③ 수집된 생체정보의 외부 유출
④ 생체정보를 수집한 기관이 다른 목적으로 남용할 가능성
⑤ 생체정보 수집 자체가 꺼림직 함
⑥ 기타(　　)
⑦ 잘 모르겠다

8. 귀하는 시계, 스마트폰의 어플 등을 통해 귀하의 신체 정보 및 건강 정보를 측정하거나 입력하여 건강관리를 하는 기술을 이용해 본 적이 있습니까?

① 있다
② 없다
③ 모르겠다

9. 귀하는 시계, 스마트폰의 어플 등을 통해 수집되는 귀하의 신체 정보 및 건강 정보의 유출 위험에 대해 어떻게 생각하십니까?

① 매우 우려된다.
② 조금 우려된다.
③ 별로 우려되지 않는다.
④ 전혀 우려되지 않는다.
⑤ 잘 모름

10. 귀하는 생체정보와 건강정보는 다른 개인정보에 비해 더 엄격하게 규제되고 보호되어야 한다고 생각하십니까?

① 매우 동의한다
② 대체로 동의한다
③ 별로 동의하지 않는다
④ 전혀 동의하지 않는다
⑤ 모르겠다

11. 귀하는 병원에서 진료 과정에서 수집된 귀하의 의료정보, 질병정보를 제약기업, 보험회사 등 영리 업체에 제공하는 것에 대해 동의하십니까? 동의하지 않으시겠습니까?

① 대체로 동의한다 → 문 14(자료분류를 위한 질문)
② 동의 하지 않는다 → 문 12
③ 잘 모름 → 문 14(자료분류를 위한 질문)

12. 그럼 통계작성이나 학술연구목적이라면 병원에서 진료 과정에서 수집된 귀하의 의료정보, 질병정보를 제약기업, 보험회사 등 영리업체에 제공하는 것에 동의하시겠습니까?

① 대체로 동의한다
② 동의 하지 않는다
③ 잘 모름

13. 그럼 귀하에게 대가가 주어진다면 귀하의 의료정보나 질병정보를 제약기업, 보험회사 등 영리 업체에 제공하는 것에 동의하시겠습니까?

① 대체로 동의한다
② 동의 하지 않는다
③ 잘 모름

14. 귀하의 성별은?
① 남성 ②여성 ③ 기타

15. 귀하의 연령대는?
① 20대 ②30대 ③40대 ④50대 ⑤ 60대 이상

16. 귀하가 하루에 PC나 모바일을 통해 인터넷을 이용하는 시간은?
① 1시간 이하 ② 1시간 - 2시간
③ 2시간 - 3시간 ④ 3시간 이상

17. 귀하의 직업은 무엇입니까?

① 사무직

② 영업직

③ 의사/변호사 등 전문직

④ 공무원/교원

⑤ 판매/서비스직

⑥ 정보통신 서비스

⑦ 농/임/축산/어업

⑧ 생산직

⑨ 학생

⑩ 기타

⑪ 무직

바이오 정보 수집, 이용 실태조사

| 인쇄일 | 2016년 11월 29일
| 발행일 | 2016년 11월 29일
| 발행처 | 국가인권위원회
| 주 소 | 서울시 중구 삼일대로 340 나라키움 저동빌딩
http://www.humanrights.go.kr
| 문의전화 | 인권정책과 02)2125-9950
| F A X | 02)2125-9835
| E-mail | research@humanrights.go.kr
| 제작 | 유성프린팅

ISBN : 978-89-6114-529-9 93330 비매품