국가인권위원회 토론회

지문 등 생체정보이용, 무엇이 문제인가

일시 : 2004. 11. 23.(화) 10:00~12:30

장소 : 국가인권위원회 배움터 1

주최 : 국가인권위원회

싣는 순서

<발제문>

생체인식과 개인정보보호

이은우(변호사, 법무법인 지평)

<토론문>

■ 생체인식과 개인정보보호

권영빈(교수, 중앙대학교 정보대학원장)

■ 생체정보활용의 인권적 쟁점과 사회적 통제

박원석(참여연대 시민권리팀장)

■ 생체인식정보는 구성원을 존중하는 방향으로

정연수(한국정보보호진흥원 개인정보보호팀장)

■ 생체정보의 인권적 특성

한상희(교수, 건국대 법학과)

생체인식(Biometrics)과 개인정보 보호

이은우(변호사, 법무법인 지평)

1. 생체인식[1](Biometrics[2])

1) 국내에서는 Biometrics를 대체로 생체인식이라고 번역하고 있다. 다음은 두산대백과사전의 생체인식에 대한 항목의 설명이다.

생체인식(生體認識, Biometrics) 개인의 독특한 생체정보를 추출하여 정보화시키는 인증방식. 지문·목소리·눈동자 등 사람마다 다른 특징을 인식시켜 비밀번호로 활용하는 것이다. 즉, 인간의 신체적·행동적 특징을 자동화된 장치로 측정하여 개인식별의 수단으로 활용하는 모든 것을 가리킨다. 지문·얼굴·홍채·정맥 등 신체 특징과 목소리·서명 등 행동 특징을 활용하는 분야로 나뉜다. 얼굴모양이나 음성·지문·홍채 등과 같은 개인특성은 열쇠나 비밀번호처럼 타인에게 도용이나 복제될 수 없으며, 변경되거나 분실할 위험성이 없어 보안분야에 활용된다. 특히 이용자에 대한 사후 추적이 가능하여 관리면에서도 안전한 시스템을 구축할 수 있다는 장점이 있다. 생체인식 중 가장 먼저 자동화된 기술은 손바닥모양 인식이다. 개인마다 손가락 길이가 다르다는 점에 착안하여 수천명의 손가락 형태를 분석하여 데이터화하였다. 피부의 표피 밑층인 진피에서 만들어진 지문은 진피부분이 손상되지 않는 한 평생 변하지 않는 특성을 갖기 때문에 지문인식(finger scan)은 개개인을 인식하는 방법으로 오래 전부터 보편적으로 사용되었다. 지문인식 시스템의 원리는 지문의 골이나 곡점 등 지문이미지의 특징점을 파악하여 저장된 원본데이터와 일치하는지를 비교하는 것이다. 정맥인식(vein recognition) 기술은 손등이나 손목 혈관의 형태를 인식하는 기법으로, 적외선을 사용하여 혈관을 투시한 후 잔영을 이용하여 신분확인을 한다. 이는 복제가 거의 불가능하여 높은 보안성을 갖지만 하드웨어 구성이 복잡하고 전체적인 시스템 비용이 커서 활용범위가 제한된다. 손바닥 인식은 사람의 손바닥에 분포되어 있는 손금을 이용하는 것으로 개개인의 손금은 모두 독특한 패턴을 가지고 있다는 점에서 착안되었다. 홍채인식(iris scan)은 사람마다 고유한 특성을 가진 안구의 홍채패턴을 이용한 것으로 데이터의 정확성, 안정성, 사용편리성, 처리속도 면에서 지문 또는 망막인식에 비해 가장 발전한 보안시스템이다. 홍채는 생후 1~2년 내에 고유한 패턴이 형성되어 평생 변하지 않으며, 8~25㎝ 정도 떨어진 상태에서 자동초점조절 카메라로 홍채패턴을 인식하는 비접촉 방식이기 때문에 사용시 거부감이 없고, 2초내 신분판별이 가능한 최첨단 생체인식 시스템이다. 음성인식은 사람의 억양과 말하는 습관에 따른 음의 높낮이 정보가 모두 고유한 특징을 갖고 있다는 점에서 출발하였다. 전화나 마이크 등을 통해 전달된 음성의 특징을 분석한 뒤 가장 근접한 결과를 찾아내는 시스템으로, 다른 생체인식 분야와 달리 원격지에서도 전화를 이용하여 신분을 확인할 수 있고, 사용하기 위한 별도의 교육이 필요하지 않으며 시스템 가격이 저렴하다는 장점이 있다. 그러나 감기나 기타 요인에 의해 목이 쉬었을 때, 의도적으로 타인의 목소리를 흉내내거나 주변환경에 큰 소음이 있을 경우에는 취약하다. 얼굴인식은 기계에 접

가. 생체인식이란?

'생체인식'이란 자동화된 장치에 의하여 개인의 신체적, 행동적 특성을 통하여 신원을 인증(authentification)하거나, 신원을 식별(identification)하는 것을 말한다.[3] 따라서 사진을 육안으로 보고 신원을 인증하거나 식별하는 것은 자동장치에 의한 것이 아니므로 생체인식에 해당하지 않는다[4]. 그러나 자동화된 장치의 도움을 받아 인간에 의해 신원의 인증이나 식별이 이루어지는 경우는 여기에 포함된다고 해석한다.[5]

나. 신원 인증, 신원 식별의 의미와 필요성

(1) 신원 인증(authentification)과 신원 식별(identification)의 의미

신원 인증(authentification)이란 '그'가 '그 사람'인지를 확인하는 것이다. 이것은 그 사람이 접근할 권한을 가지고 있는 자인지, 거래를 할 권한이 있는 자인지, 처분을 할 수 있는 권한이 있는 자인지 등을 확인하는 것이다. 즉, 이는 "나는 내가 나라고 하는 사람과 같은 사람인가?"(Am I the one I pretend to be?)라는 질문에 대한 대답이다. 그리고 이것은 한 사람과 한 사람, 1:1의 비교의 문제이다[6]. 인증은 동일인인지 여부만 확

촉할 필요없이 카메라로 쉽게 판별할 수 있는 보안기술이다. 사람마다 다른 얼굴 데이터베이스를 만들어 놓고, 입력된 얼굴영상을 데이터베이스의 얼굴들과 비교하는 방법이다. 그러나 사용자의 기분에 따라 표정이 변하고, 주위 조명에 영향을 많이 받는다는 어려움이 있다.

2) 이는 생명(life)을 뜻하는 그리스어 bio와, 측정(the measure of)을 뜻하는 그리스어 metrics로 이루어진 조어이다.

3) International Biometrics Group(IBG)의 정의. www.ibg.org OECD 보고서 2.

4) OECD

5) OECD

6) 3페이지.

인하는 것이므로, 확인의 대상이 되는 그 사람이 누구인지 몰라도 된다.

신원 식별(identification)은 '그'가 '누구'인지를 식별해 냄으로써 누구를 찾아내거나, 누가 아닌 자를 확인하거나, 누구를 배제하기 위한 것이다. 이는 "내가 누구인가?"라는 질문에 대한 대답이다. 여러 사람 중에서 한 사람을 확인해 내는 것이므로 1:다수의 비교의 문제이다. 신원 식별을 하려면 데이터베이스화된 집중된 정보가 있어야 한다.[7] 인증이나 신원 식별은 그 목적에 따라, 그 수준에는 천차만별의 차이가 있을 수 있다. 낮은 수준의 인증이나 신원 식별은 익명으로도 이루어질 수 있다.

(2) 인증과 신원 식별의 각 수단별 장단점

인증과 신원 식별의 방법을 다음의 다섯 가지 유형으로 분류할 수 있다.[8]

(i) 알고 있는 것에 의하여(something the claimant knows) : 비밀번호(password)

(ii) 보유하고 있는 '징표'에 의하여(something the claimant owns) : 신분증, 징표(token), 열쇠 등

(iii) 그 사람 자신에 의하여(something the claimant is) : 생체인식(biometrics)

(iv) 그 사람의 실재에 의하여(claimant is at a particular place) : 직접 대면

(v) 제3자의 확인에 의하여

이러한 방법 중 알고 있는 것 즉, 비밀번호에 의한 방식은 휴대가 필

7) 3페이지.
8) JILT 5페이지

요없어 간편하기는 한데, 잊어버리거나, 제3자가 추측을 통해서 알아내거나, 유출될 가능성이 있다. 가지고 있는 것, '징표'에 의한 방식은 비밀번호보다 안전성이 뛰어난 방법으로 사용된다. 그러나 휴대해야 하므로 불편하고, 잊어버리고 놓고 올 수가 있고, 다른 사람이 훔쳐가거나, 잃어버릴 경우에는 타인이 신분도용을 할 위험이 있다. '징표'에 다른 방법을 추가하여 사용하기도 한다. 생체정보에 의한 방식은 휴대가 간편하고, 잊어버릴 위험이 없고, 분실이나 도난의 위험은 적으나, 비용이 많이 들고, 프라이버시 침해의 위험성이 크다.[9]

신원 인증이나 신원 식별시에는 안전성과 확실성을 높이기 위해서 이들 방법을 함께 사용하는 경우가 많다. 예를 들어 사진이 들어있는 신분증과 서명, 크레딧 카드와 서명, 지문과 비밀번호처럼 여러 요소를 혼합하여 사용하면 그만큼 인증이나 신원 식별 과정에서의 오류를 줄일 수 있기 때문이다.[10] 한편 생체정보 중에서 흔히 사용되는 것으로는 육체적 특성으로 지문・얼굴・홍채・정맥・손금・손모양 등이 있고, 행동적 특성으로는 음성과 자판 입력특징(keystroke dynamics), 서명, 필적 등이 있는데, 생체정보도 두서너 가지의 생체정보를 같이 활용하는 경우가 많다.[11]

(3) 인증과 신원 식별의 목적

인증과 신원 식별을 하는 이유 즉, 상대방이 누구인지나, 또는 상대방이 누가 아닌지를 알고 싶어하는 이유는 여러 가지가 있다.

첫째, 사회생활이나 거래에서 상대방을 확인하여 관계를 맺거나, 거래

9) 3페이지.
10) 3페이지.
11) 3페이지.

를 하기 위한 목적에서이다. 상대방 확인의 목적은 다양할 것이며, 그 목적에 따라 적절한 확인의 수준이 있다. 단순한 채팅이나, 일회적인 사소한 거래인 경우에는 상대방이 누구인지를 상세히 알 필요는 없고, 익명으로도 충분할 것인데, 부동산의 거래나, 결혼과 같은 중대한 법률관계나 신분관계의 형성시에는 확실한 신원 인증이나 식별이 필요하다.

둘째, 인증이나 신원 식별을 통해 조직이나 집단의 구성원을 확정하거나, 자신이나 자신의 조직과 관계를 맺는 자들의 정보를 수집, 분석하여 여러 가지 계획을 세우는데 기초로 삼기 위한 목적도 있다. 예를 들어 국가에서 국민들의 신분등록을 통해서 여러 가지 계획을 세운다거나, 기업에서 직원들의 신원 등록을 통해서 인적자원을 관리하는 것, 기업이 고객의 정보를 파악하여 마케팅이나 생산의 계획을 세우는 것 등이 그것이다.

셋째, 인증이나 신원 식별을 통해 조직이나 집단의 구성원에 대한 관리와 통제를 효과적이고 강력하게 하기 위해서다. 이는 인증이나 신원 식별의 직접적인 목표로 되기도 하지만, 인증이나 신원 식별의 부수적인 효과로 간접적으로 나타나기도 한다. 예를 들어 기업에서 신원 인증 장치를 통한 출입통제 시스템을 채택할 경우 이것은 집단의 구성원에 대한 관리와 통제장치로 작동하게 된다. 그리고 인증이나 신원 식별이 이루어지는 경우에는 그와 결합되어 그 사람의 정보가 공개되는 것이므로, 이는 그 사람에 대한 감시가 된다.

(4) 인증이나 신원 식별이 증가하게 되는 이유

정보처리기술의 혁명적인 발전은 수집되는 정보의 양과 질의 수준을 높였으며, 정보의 활용도를 전례없이 높였다. 그래서 많은 학자들은 현

대사회를 정보가 이윤창출과 지배의 중요한 원천이 되는 정보사회라고 부르기도 한다.

이러한 정보사회의 도래와 함께 정보수집의 중요한 수단이 되는 인증과 신원 식별의 중요성도 점점 더 커지고 있다. 인증과 신원 식별을 통해 얻어내는 정보의 가치나, 가공해서 생산해 낼 수 있는 정보의 가치가 과거와는 비교할 수 없을만큼 높아지고, 그 비용도 아주 저렴해짐으로써, 인증과 신원 식별이 폭발적으로 늘어나고 있는 것이다. 기업이나 국가나 고용주는 인증이나 신원 식별을 통해 개인이나 집단에 대한 수 많은 정보를 수집해 정보를 분석함으로써, 보다 유리한 계획을 세우고, 보다 강력하고 공고한 지배와 통제(정치적, 경제적, 사회적, 문화적 지배와 통제)를 할 수 있는 것이다. 물론 전자상거래의 발달로 원격거래가 이루어짐으로써 어떤 관계맺기나 거래시에 상대방을 확인해야 할 필요가 커지고, 사기나 불법행위를 막고 안전을 지키기 위하여 인증이나 신원 식별이 필요하기도 하다.

2. 생체인식의 작동과정과 종류

가. 생체정보의 특징

생체정보는 각각의 생체정보마다 고유의 특성이 있지만, 가장 중요하고 기본적인 특성은 다음의 3가지이다.[12].

첫째, 보편성(universal)이다. 생체정보는 모든 사람에게 다 있다는 특징이 있다. 물론 일부의 사람은 생체인식 정보가 확실하지 않아서 생체

12) 위 3페이지

인식 기기가 등록을 하지 못하거나, 인식을 하지 못하는 경우도 있다.

둘째, 고유성(unique)이다. 생체정보는 사람마다 각기 고유하다는 특징이 있다. 물론 고유한 정보를 자동화된 시스템으로 식별해 낼 수 있는지는 다른 문제이다.

셋째, 영구성(permanent)이다. 생체정보는 대체로 잘 변하지 않기 때문에 평생 변하지 않는 특징을 가지고 있다. 물론 생체정보에 따라서 약간씩은 변할 수도 있다. 그 외에도 생체정보는 소량의 정보로도 분석, 가공에 따라 대량의 정보를 알아낼 수 있다는 점 등의 특징이 있다.

다. 활용되는 생체정보

1) 지문정보

지문은 손가락의 땀구멍의 융기부분의 무늬이다. 이것은 보편성, 고유성, 불변성을 골고루 잘 갖춘 생체정보이다. 지문의 형태는 고리형(loop), 반원형(arch), 나선형(whorl)의 세 가지[13]로 나누어 볼 수 있다. 이러한 지문의 특징적인 정보들을 추출하여 아래 그림과 같이 소량의 정보(아래의 것은 약 250,700바이트)로 저장하는 것이다.

---

13) 

2) DNA

DNA 인식은 단백질로 구성된 유전인자감식 방법이다. 고도의 정밀성이 특징인 이 기술은 정밀한 단백질 분석기기를 사용해야 함은 물론 감식 시간이 많이 걸린다.

3) 망막

사람 안구 뒷면에 있는 망막의 모세혈관의 패턴을 적외선으로 안구를 투시하여 읽어낸다. 망막을 이용한 이 검색 기술은 고도의 보안성을 주지만 사용자가 안경을 벗어야 하는 등의 불편과 사용자의 거부감이 있어 많은 사람이 사용하는 곳에는 적합치 않다. 홍채 인식은 홍채패턴을 이용하는 것으로 사용자가 검색기에 가까이 서서 카메라에 초점을 맞추어 약 5초 정도 주시해야 하는 것이 불편하고 사용자의 거부감이 있다. 망막과 홍채인식은 둘 다 가격이 비싼 것이 흠이다.

3) 얼굴 인식

얼굴 인식은 각 개인 얼굴의 특징을 이용하는 것이다. 입력된 화상으로 부터 각 개인 마다 독특한 부위를 측정단위로 추출하는 것인데 독특한 부위가 어떠한 곳 인지를 결정하는데 이 기술의 정확도가 달려있다. 또한, 얼굴 인식 기술은 사용자의 기분과 상황에 따라 표정이 변한다는 것을 감안해야 하고 주위 빛의 방향에 따라 많은 영향을 받게 되는 등 아직은 완벽한 솔루션의 제시가 어려운 실정이다.

4) 손형태 인식

개인마다 손가락의 길이가 다르다는 점에 착안해서 만든 본인확인 시스템이다 . 그러나 기기의 크기가 크고 타인을 본인으로 잘못 인식하는 오인식률이 높아 고도의 보안을 요구하는 곳에는 적용하기에 부적합하다. 가격 또한 높다.

5) 정맥 인식

표피 가까이 놓여있는 정맥 중 손등이나 손목의 혈관 패턴을 인식하는 기술이다. 적외선을 사용하여 혈관을 투시한 후 잔영을 이용하여 본인확인을 하게 된다 . 어느 정도의 보안성이 있기는 하나, 기기가 크다는 점과 가격이 매우 높다는 단점이 있다.

6) 음성 인식

원격지에서도 전화를 이용하여 본인 확인을 할 수 있다는 것과 사용방법을 따로 익히지 않아도 되는 편리함이 있다. 또한, 기기의 가격이 매우 저렴하다는 장점도 있다. 그러나 음성은 환경에 따라 그리고 감정에 따라 쉽게 변한다는 점이 매우 어려운 부분이다. 또한, 목소리를 흉내내는 경우 남을 나로 인식할 수 있으며 , 사용 환경의 높은 소음이 변수로 작용하기도 한다.

7) 필체 인식

개개인의 독특한 글씨체를 본인 확인 측정 단위로 이용하는 것이다. 남이 흉내 낼 수 있음은 물론 복제하여 사용할 수 있어 보안성이 상당히 떨어진다.

라. 생체인식 시스템의 작동과정

생체인식 시스템은 생체인식 기기에 생체정보를 등록하는 과정과 구별, 검색하는 과정으로 나뉜다.

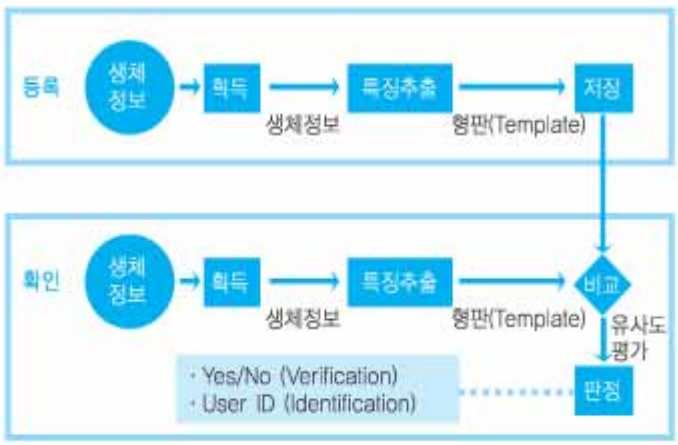
등록하는 과정에서 정보주체는 생체인식 장치(예를 들자면 지문인식기)를 통해 생체정보 샘플을 제공한다(생체정보 샘플 1; raw data). 생체정보 시스템은 원시 정보로부터 생체 특징을 추출하여 중요 정보만 저장(추출 정보 1: template data)하고, 원시 정보는 안전하게 처리한다. 이 추출 정보는 생체정보 시스템을 통해 취득된 원시 정보에서 불필요한 정보를 제외하고 특징만을 코드화 한 것이다. 예를 들어 지문인식 시스템의 경우 지문 이미지 자체를 저장하여 사용하는 것이 아니라, 지문 특징을 400byte 내외로 Code화 하여 사용함으로써 효율적인 저장과 식별이 가능하도록 한다.[14] 추출 정보는 중앙집중화된 데이터베이스에 저장되거나, 스마트카드나 자기카드에 저장된다.

검색하는 과정에서는 정보주체가 생체인식 장치를 사용하여 생체정보 샘플을 제출하면(생체정보 샘플 2 ; raw data), 검체로부터 중요정보를 추출하고, 제공받은 샘플은 안전하게 처리한다. 추출된 중요정보(추출정보 2 ; template data)를 검색 식별 엔진에 넣고 처리하여, 동일한 것으로 판단되는 추출 정보를 찾아낸다. 1:1의 식별인 경우에는 대조되는 정보의 동일성 여부만을 판단하고, 1:다수의 식별인 경우에는 동일한 추출

14) 니트젠 '생체인식기술이란?'

정보를 찾아내는 것이다.[15]

(2) 오류율(FAR/FRR)

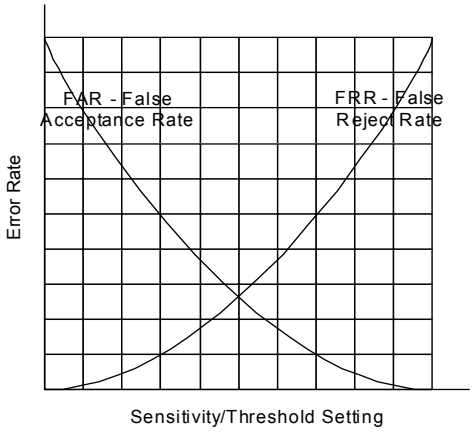


[그림 1] 생체인식 프로세스

생체인식 시스템의 정확성은 두 가지 측면에서 측정된다. 하나는 잘못 승인할 가능성인 오승인율(FAR; false accepta- nce rate)이고, 다른 하나는 잘못 거절할 가능성인 오거절율(FRR; false reject rate)이다. 양자는 서로 반비례하는 관계에 있다. 두 위험성을 가장 적절하게 조화시킬 수 있는 지점으로 민감도를 결정하게 된다. 이를 민감도 결정점(threshold, sensitivity/ threshold setting)이라고 한다[16].

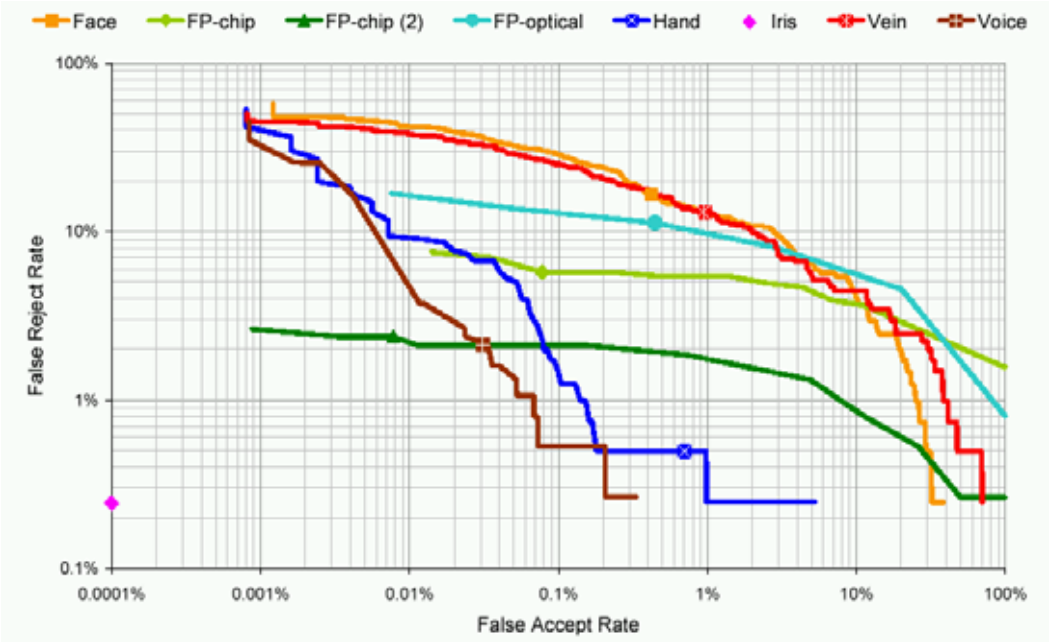
15) * 16
16) * 18

FRR과 FAR의 관계



Source: Mansfield, T. et al. (2001), "Biometric Product Testing Final Report", CESG report, 19www.cesg.gov.uk/site/ast/biometrics/media/ BiometricTest Reportpt1.pdf, accessed 20 April 2004.

여러 생체인식 시스템의 오류율 사례



Note : This figure is taken from the CESG evaluation made in 2000 with a limited number of participants: this figure is for illustration purposes only; actual performance of individual biometrics will vary depending upon context.

Source : Mansfield,et(2001), "Biometric Product Testing Final Report", CESG report, 19 www.cesg.gov.uk/site/ast/biometrics/media/Biometr icTestReportpt1. pdf, accessed 20 April 2004.

(3) 채취실패율(failure to acquire), 등록실패율(failure to enroll)

채취실패율은 생체인식의 채취에 실패할 확률이다. 예를 들어 지문정보의 경우 손에 상처가 난 경우나, 지문이 흐려져서 잘 드러나지 않는 경우, 이물질이 붙어 있는 경우(반창고 등)에는 생체정보의 채취에 실패할 수 있는데, 이런 일이 발생할 가능성이다. 채취의 기준을 엄격하게 할 수록 채취실패율은 높아지나, 오승인율은 낮아진다. 등록실패율은 생체정보 샘플로부터 중요정보를 추출하는 것에 실패할 확률이다.

3. 생체인식기술의 활용사례

가. 국내의 사례

(1) 국가에 의한 활용

(가) 지문정보와 주민등록증, AFIS

국가가 생체인식기술을 활용하고 있는 대표적인 사례는 주민등록증

을 발급받으면서 채취하는 지문정보이다. 현재 주민등록증 뒷면에는 오른손 엄지손가락 지문이 수록되어 있는데, 이것뿐만 아니라, 주민등록증을 발급받을 때, 열손가락 지문을 날인받아서 이를 경찰청에 보내 데이터베이스로 구축하고, 자동지문인식시스템(AFIS)과 연동하여 범죄수사나 범죄예방을 위한 불심검문 등에 활용하고 있다. 특히 열손가락 지문을 날인받아서 이를 경찰청에 보내는 행위, 이를 경찰청에서 데이터베이스로 구축한 행위, 이를 자동지문인식시스템과 연동하여 범죄수사나 범죄예방활동에 사용하는 행위는 아무런 법적 근거도 없이 이루어지는 것이라는 점에서 충격스러운 일이다.

(나) 유전자정보은행

최근 정부는 성범죄자의 유전자정보은행을 구축하기 위한 여론 형성 작업을 하고 있다[17]. 그리고 미아찾기 사업을 위하여 유전자정보은행을

17) 유전자 자료은행이란 강력범들의 DNA 프로필을 DNA 분석기법을 이용해 분석한 결과를 데이터베이스화한 것이다. 범죄사건의 증거물에서 용의자의 DNA 프로필이 확보될 경우 이를 검색해 신원을 확인하는 국가 차원의 과학수사 정보관리 시스템을 구축하는 것이다. 즉 범죄자 등의 DNA형을 엄격한 절차에 따라 전산자료로 기록·관리하여 범죄수사 및 신원 식별 등의 자료로 활용하는 것. 국립과학수사연구소와 대검찰청 등 수사당국에서는 '재범을 방지하고, 과학수사를 지향한다' 는 취지에서 유전자 자료은행을 설립할 것을 주장해왔다. 유전자 자료은행의 자료가 수사실무를 담당하고 있는 기관에 사건해결의 중요한 실마리를 제공할 수 있다는 판단에서다.

2002년 2월 서울 성북경찰서 관내에서 발생한 강도 강간 살인사건 수사 때 담배꽁초와 피해자의 몸 등에서 서로 다른 3명의 DNA 프로필을 확보해 범인을 검거할 수 있었다. 그리고 이들의 DNA 프로필을 이용해 미제 사건을 검색, 2002년 1월부터 2개월에 걸쳐 발생한 성북경찰서 내 또 다른 강간사건과 남부경찰서, 안양경찰서, 청주서부경찰서의 강간사건도 이들의 소행임을 확인할 수 있었다.

미제 사건 해결 얼마든 가능

10여년 전에 일어났던 화성경찰서 9차 및 10차 연쇄 강간 살인사건의 용의자 DNA형과 대전·충청 일원에서 다수의 여성을 강간한 강간범, 용산경찰서의 10여명의 강간 용의자 DNA 프로필 등이 모두 확보되어 있어 이들 사건도 조만간 해결될 것으로 기대된다.

구축하고 있다. 이것은 보호시설의 미성년자의 유전자정보를 구축하기 위해서 벌이는 사업이다.

(다) 무인민원발급기

정부는 무인민원발급기라고 하여 민원서류의 원격발급을 위하여 지문정보를 활용하고 있다. 이것은 지문정보데이터베이스가 새로운 용도로 사용되기 시작한 첫 사례라는 점에서 앞으로 지문정보데이터베이스의 활용범위를 확장하는 전주곡이 될 가능성이 있다.

(2) 정부・기업・학교의 직원・학생을 대상으로 한 사용

(가) 정부에서 생체정보를 이용하고 있는 사례로 보도를 통해 알려진 것으로는 지문정보를 이용한 공무원증의 발급, 출입시스템의 구축 사례가 있다. 이때 이용되는 생체정보는 지문정보로 알려져 있다.

(나) 기업에서 사원의 생체정보를 출입시스템 등에 활용하고 있는 사례는 많이 있을 것으로 보이는데, 그 실태는 아직 파악되고 있지 않다. 이를 파악할 수 있는 법적 근거도 없다.

(다) 대학교의 학생과 직원을 대상으로 한 사용의 경우는 공주대학교의 지문인식 시스템 도입, 연세대학교 지문인식 시스템 도입, 전북대의 지문인식 시스템 도입시도 사례가 있다.

(3) 기업이 소비자를 대상으로 한 사용 또는 소비자의 개별적 사용

몇몇 은행에서 고객의 지문정보를 등록받아 이를 본인 인증의 수단으로 사용하고 있다. 그리고 엘지마트에서는 지문정보를 등록받아 회원의 인증수단으로 사용하고 있다. 상호저축은행 등이 대출서비스를 하면서 주민등록증의 지문정보와 대조하여 신원을 확인하는 경우도 있었다. 한편 지방자치단체에서 행정자치부의 지문정보를 민간기업에게 개방하여 개인 신분 인증의 수단으로 사용할 수 있게 해 주겠다고 하여 큰 반발을 사고, 철회한 경우도 있다. 어떤 회사는 미성년자의 지문정보를 등록받아 미아발생시에 활용하여 쉽게 미아를 찾을 수 있게 한다는 명목으로 미성년자의 지문정보를 등록받는 경우도 있었다. 그리고 여러 기업에서 DNA 정보를 수집하기도 하였다.

한편 생체인식을 개별적으로 사용할 수 있게 한 경우로는 개인용 컴퓨터에 지문인식 시스템을 도입하여, 등록한 지문이 일치하지 않는 경우에는 컴퓨터의 로그인이 되지 않도록 한 제품을 판매한 사례가 있다. 그리고 지문인식 도어락의 경우는 지문을 이용한 문단속 시스템이다.

나. 해외사례

(1) 국가신분증

영국에서 새로 도입하려는 국가신분증에는 지문, 홍채정보가 포함되게 되어 있어서 큰 논란을 일으키고 있다. 유럽연합의 국가 중에도 스위스처럼 생체정보를 국가신분증에 담으려는 나라도 있다. 미국의 경우 운전면허증에 생체정보를 담으려는 시도가 있었으며, 여권에 생체정보를 담아야 한다는 법안이 통과되어 시행되고 있는데, 현재 큰 반발을 사고 있다.

(2) 기업, 학교, 공공영역

외국의 경우도 우리의 경우와 비슷하다. 기업에서 노동자의 출입통제를 위해서 생체정보를 수집하고 생체인식 시스템을 설치하는 예가 많이 있다. 캐나다의 프라이버시위원회는 기업이 출입시스템으로 목소리 정보를 수집하려는 것에 대하여, 노동자들이 이를 이용하여 전화감시를 할 수도 있다는 우려를 받아들여, 비록 회사가 목소리 정보를 출입시스템에만 사용하겠다고 약속하더라도 전용의 우려는 있으므로, 도입하지 않는 것이 좋다는 권고를 하기도 하였다.

대학에서 생체인식 시스템을 도입하려는 사례, 공공도서관에서 생체인식 시스템을 도입하려는 사례, 공항에 생체인식 시스템을 도입하려는 사례는 많이 있다.

4. 생체인식정보의 활용의 문제점과 통제방안

가. 생체인식정보의 활용은 개인정보와 개인의 인권을 보호하는가, 개인정보 보호와 인권보호의 적인가?

신원의 인증이나 신분 확인은 정당한 권한이 있는 자를 식별하여 그에 합당한 권한을 행사할 수 있도록 해 주는 수단이 되므로, 온라인상에서나 오프라인 상에서 부당한 비밀의 침해를 방지하고 안전성을 높여주는 긍정적인 역할을 한다. 특히 생체인식은 비밀번호 방식이나 증표 제시 방식의 경우 분실 또는 도난의 가능성이 있고, 타인에게 유출되거나, 타인이 추측을 통해서 알아낼 가능성이 있는데, 생체인식 정보는 그런

위험이 없다는 점이 장점으로 제시되어 왔다. 그리고 다른 방식보다 훨씬 더 정확하다는 점이 장점으로 제시되어 왔다. 그러나 한편으로는 아래에서 보는 바와 같이 생체인식은 매우 민감한 정보로 개인정보 침해나, 표현의 자유나 행동권의 침해와 같은 위험을 내포하고 있기도 하다.

나. 생체인식의 위험성

(1) 유일식별자(Uinque Identifier)와 데이터베이스의 위험

생체정보는 유일성, 불변성, 보편성을 가지고 있기 때문에 유일식별자로 기능한다. 따라서 이를 바탕으로 데이터베이스화되기 쉽다. 생체정보에서 중요정보를 추출할 경우, 소량의 정보로 추출이 가능하므로, 적은 비용으로 데이터베이스를 구축할 수 있다. 이 경우 생체정보는 개인의 데이터베이스의 유일식별자가 된다. 이는 평생 변하지 않는 유일식별자로서 전세계에서 고유한 범세계적인 유일식별자로 기능할 수 있다. 이처럼 생체정보와 결합된 정보는 평생동안 축적될 수 있게 된다.

(2) 전용가능성[18]

생체정보가 애초에 수집된 목적과는 다른 목적으로 전용될 수 있다. 예를 들어 사회보장을 위하여 지문정보를 등록했는데(2중 수급을 방지하기 위하여 2중 등록을 막기 위해), 지문정보가 다른 용도로 활용되는 경우 발생하는 문제이다. 한편 샘플에서 특징을 추출한 추출정보(template data)로부터는 원래의 생체정보로 전환할 수 없고, 따라서 표준화되어

18) OECD 11.

있지 않는한 생체정보를 전용할 가능성은 없다는 것이 일반적인 인식인데, 최근의 연구결과에 의하면 반드시 그렇지도 않다고 한다.

(3) 연동가능성(LINK)

생체정보가 유일식별자의 성질을 가지고 있기 때문에 데이터베이스 연결의 고리로 역할을 할 수 있다.(link)[19] 예를 들어서 금융기관의 지문정보와 결합된 거래기록은 행정자치부의 지문정보, 경찰청의 지문정보와 연동될 수 있다. 이것은 정보의 확장가능성을 의미하며, 목적구속성의 원칙에 반하는 문제가 있다.

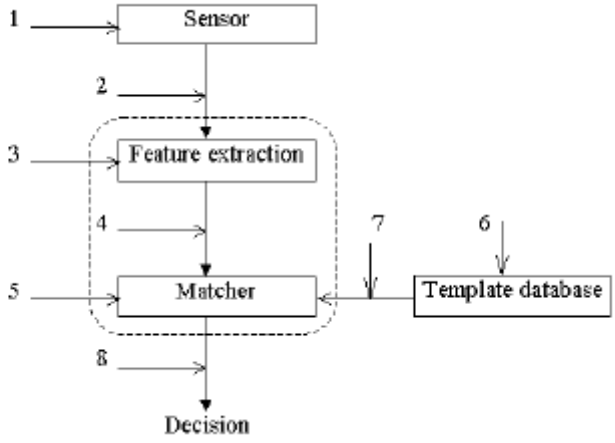
(4) 동의없는 사용의 가능성[20]

생체정보 중에는 신원 식별자의 자발적인 선택에 의존하여 수집되는 정보가 있고, 신원 식별자 몰래 수집될 수 있는 정보가 있다. 생체정보는 정보마다 다양한 편차를 보인다. 얼굴 인식은 신원 식별자 모르게 CCTV로 수집되어 이루어질 수 있다. CCTV는 오늘날 광범위하게 사용되고 있다. AC 닐슨이라는 회사는 쇼핑객들의 얼굴을 인식하여, 그들의 쇼핑습관을 추적하게 하는 기술에 대한 특허권을 가지고 있다고 한다.[21] 컵에 남아 있는 지문으로 지문 정보는 수집할 수 있다.[22] 이처럼 지문정보도 얼마든지 신원 식별자 몰래 은밀하게 수집할 수 있다. 그 반면에 손모양은 지문보다는 은밀하게 수집될 수 있는 가능성이 낮다.[23] 오늘날

19) EFF
20) OECD 11
21) OECD 12.
22) FBI IAFIS
23) The Functions of Biometric Identification Devices, National Biometric Test Center, San

홍채 정보의 인식은 18 내지 24 인치의 거리가 떨어져 있어도 작동된다고 한다. 홍채정보의 수집도 그만큼 또는 그보다 더 멀리서도 가능하다고 한다. 홍채정보는 신원 식별자 모르게 수집될 수 있는 것이다.[24] 그러나 망막정보는 홍채정보보다 은밀하게 수집될 가능성이 낮다. DNA도 은밀하게 수집되기 아주 쉽다.

[생체인식 시스템에 대한 공격][25]



1 유형은 센서에 가짜의 생체정보(a fake biometric)를 제출하는 공격(가짜 지문, 얼굴, 홍채)

2. 전에 가로챈 생체정보를 제공하는 공격(replay)

3. 공격자가 특징을 추출하는 추출기를 공격하여 공격자가 원하는 특징을 추출하도록 함.

Jose State University.

24) OECD 12

25) Attacks on Biometric Systems: A Case Study in Fingerprints, 2페이지. Umut Uludag, Anil K. Jain. Michigan State University, N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 223-228, 2001.

4. 특징을 추출한 정보를 공격자가 가로채서 다른 것으로 바꿈.

5. 식별장치를 공격하여 승인율을 높여 놓는 공격

6. 저장되어 있는 추출정보를 공격함. 추출정보를 추가하거나 기존의 추출정보를 수정하거나 제거함.

7. 저장된 추출정보(the template database)의 전송과정을 공격함.

8. 식별장치의 승인여부의 판단결과를 무력화함

(4) 시스템의 취약성[26)]

생체인식 시스템에 대한 공격은 위와 같이 아주 다양하게 존재한다. 입력 단계에서부터 센서에 가짜의 생체정보(a fake biometric)를 제출하는 공격(가짜 지문, 얼굴, 홍채)이 있기도 하고, 전에 가로챈 생체정보를 제공하는 공격(replay)도 있다. 타인을 협박하여 그 자의 생체정보를 자신의 이름으로 제출하게 하는 방법도 있고, 시스템에 따라서는 지문인식 시스템의 표면에 입김을 불어서 직전에 사용한 사람의 지문을 드러나게 하여 이를 다시 사용하기도 한다(Latent print attacks). 그리고 공격자가 특징을 추출하는 추출기를 공격하여 공격자가 원하는 특징을 추출하도록 하기도 하고, 아예 대량의 정보로 집중 공격하여 시스템의 서비스 거부를 유도하기도 한다. 특징을 추출한 정보를 공격자가 가로채서 다른 것으로 바꾸거나, 식별장치를 공격하여 승인율을 높여 놓는 공격하기도 한다. 그리고 무차별 정보를 제출하여 승인을 얻기도 한다. 이것은 생체

26) Manfred U. A. Bromba
The following list compiles the most important attacks to biometric security components. It depends on the actual application, against which attacks security measures are necessary.

인식 시스템의 잘못된 승인이 이루어질 가능성(FAR)의 수치에 따라서 성공가능성이 결정된다.

저장되어 있는 추출정보를 공격하기도 하고, 추출정보를 추가하거나 기존의 추출정보를 수정하거나 제거하기도 하고, 저장된 추출정보(the template database)의 전송과정을 공격하기도 하고, 식별장치의 승인여부의 판단결과를 무력화하기도 한다. 그리고 그 밖에 트로이의 목마 등 전통적인 공격도 한다.

(6) 오류의 가능성

생체인식 시스템의 오류 가능성은 아주 다양한 분야에서 나타난다. 등록불가의 경우가 있다. 예를 들어 지문시스템의 경우 지문이 닳아서 없어진 경우는 등록이 되지 않을 수 있다. 잘못 인식할 가능성이 있다.

(7) 감시(Surveillance)

생체정보는 유일식별자이기 때문에 생체정보의 활용은 언제든지 정보의 축적을 가능하게 하고, 축적된 정보의 집적시는 그 정보주체에 대한 전면적인 추적과 감시가 가능하게 된다. 이런 위험은 특히 생체정보를 template 방식으로 처리하는 경우 더 크다. 전자상거래가 생체정보를 이용해서 인증과 신원 식별을 한다면, 모든 거래기록이 집적될 수 있는 것이다. 생체정보의 활용은 프라이버시를 파괴하고, 자유를 위험에 빠뜨릴 것이다(George Tomko)[27].

27) OECD 11

5. 대응방안

가. 개인정보영향평가

(1) 생체인식 시스템의 도입은 그것이 미치는 영향이 매우 크고, 보편 유일식별자로 데이터베이스화 및 데이터베이스 연동 등 남용의 위험이 크므로 반드시 사전에 영향평가를 실시하여 당해 생체인식 시스템의 도입이 적절한 수단인지, 도입되는 구체적인 방식은 적절한지를 사전에 검토하고, 그 과정에 해당 정보주체의 참여를 보장하는 것이 중요하다.

(2) 평가항목

(가) 정보별 민감도 평가

우선 각 정보별 민감도를 평가해야 한다. 각 정보별 민감도는 사용되는 기술, 운용방식에 따라 다를 수 있다. 정보가 식별력이 높을수록, 신원 식별자의 인식이나 동의 없이도 몰래 수집하는 것이 가능할수록, 다른 시스템과의 범용성이 클수록, 이미 축적되어 있는 정보가 많을수록, 변화가능성이 적을수록 개인정보 침해의 위험이 크다고 볼 수 있다. 아래의 자료는 IBG(International Biometrics Group)가 생체정보별 민감도를 평가한 표이다.[28]

28) IBG, 생체정보와 프라이버시, 윤재석, 한국정보보호진흥원.

[표 1] 생체인식 기술별 프라이버시 위험 평가

생체인증기술	긍정적 프라이버시 측면	부정적 프라이버시 측면	위험 평가
손가락 인식 (Finger-scan)	·각기 다른 시스템에 다른 손가락 정보제공 가능 ·상이한 템플릿과 고리즘을 제공하는 업체가 많음	·공공 부문에 저장된 정보가 많음 ·범죄 수사에서 자주 이용 ·강력한 식별 능력	·확인/ 식별 : 고 ·명확/ 불명확 : 중 ·행동학적/생리학적 : 고 ·자발적/비자발적 : 중 **·위험 평가 : 고**
망막 인식 (Retina-scan)	·사용자의 적극적인 동의와 협조가 있어야 함	·매우 강력한 식별 기능	·확인/ 식별 : 고 ·명확/ 불명확 : 저 ·행동학적/생리학적 : 고 ·자발적/비자발적 : 저 **·위험평가 : 중**
얼굴 인식 (Facial-scan)	·머리모양, 수염 등으로 변화를 줌으로써 이용자의 동의 없이 이를 식별할 가능성 감소	·동의나 인지없이 쉽게 촬영가능 ·기존에 수집·저장된 많은 양의 이미지를 사용하는 것이 가능	·확인/ 식별 : 고 ·명확/ 불명확 : 고 ·행동학적/생리학적 : 중 ·자발적/비자발적 : 고 **·위험평가 : 고**
음성 인식 (Voice-scan)	·사용자는 반드시 등록된 패스워드를 말해야 함 ·음성만을 통한 식별은 용이하지 않음	·사용자의 동의나 인지 없이 수집될 수 있음	·확인/ 식별 : 저 ·명확/ 불명확 : 고 ·행동학적/생리학적 : 저 ·자발적/비자발적 : 중 **·위험평가 : 중**
서명 인식 (Signature-scan)	·서명은 행동학적 성격이 강하며 자의적으로 수정 가능	·위조나 변조가 용이	·확인/ 식별 : 저 ·명확/ 불명확 : 저 ·행동학적/생리학적 : 저 ·자발적/비자발적 : 저 **·위험평가 : 저**
홍채 인식 (Iris scan)	·사용자의 동의가 필수적 ·홍채 이미지는 범죄수사에 이용되지 않음	·매우 강력한 식별 기능 ·대부분의 홍채 템플릿은 단일한 장비에 의해 식별 가능함	·확인/ 식별 : 고 ·명확/ 불명확 : 저 ·행동학적/생리학적 : 고 ·자발적/비자발적 : 중 **·위험평가 : 고**
키스트록 인식 (Key stroke -scan)	·행동학적 성격이 강하며 변화가능성이 높음	·동의나 인지없이 수집 가능	·확인/ 식별 : 저 ·명확/ 불명확 : 중 ·행동학적/생리학적 : 저 ·자발적/비자발적 : 저 **·위험평가 : 저**
손모양 인식 (Hand-scan)	·생리학적 생체정보이나 식별을 위해 사용가능성 적음 ·적절한 기구사용이 필요	--	·확인/ 식별 : 저 ·명확/ 불명확 : 저 ·행동학적/생리학적 : 중 ·자발적/비자발적 : 저 **·위험평가 : 저**

예를 들어 손의 경우를 보면 지문인식 시스템과 손가락의 형태를 인식하는 시스템이 있는데, 전자가 후자보다 훨씬 개인정보의 측면에서 위험성이 크다. 왜냐하면 지문인식의 경우는 신원 식별자 몰래 수집할 가능성도 크며, 오류율도 낮고, 이미 국가기관(행정자치부, 경찰청)에서 많은 정보를 축적해 놓고 있기 때문이다.

(나) 시스템의 민감도 평가

생체정보 뿐만 아니라 시스템도 종합적으로 분석하여 민감도를 평가해야 한다. 여기에서의 평가항목으로는 이용자에게 얼마나 시스템의 운영에 대하여 설명을 했는지, 시스템 이용이나 등록이 필수적인가 아닌가, 생체정보의 자료를 중앙집권적인 데이터베이스에 수록하는가, 아니면 분산해서 수록하는가, 자료의 보관은 얼마나 오래 하는가, 사용하는 용도는 무엇인가 등이 평가되어야 한다.

프라이버시 침해 가능성 낮음	항목별 구분	프라이버시 침해 가능성 높음
명확	↔ 이용자의 시스템 운영 이해 여부	불명확
선택적	↔ 시스템 등록이 선택적인가 혹은 의무적인가	의무적
고정된 기한	↔ 시스템의 사용기한	무기한
사적 부문	↔ 시스템 적용 영역	공적 부문
개인-소비자	↔ 상호작용 시 이용자 지위	피고용인-시민
개인	↔ 생체인증 정보 소유	기관
개인 저장	↔ 생체인증 정보 저장 장소	중앙 저장
행동학적	↔ 적용되는 생체인증 기술 유형	생리학적
자발적	↔ 이용자의 자발적 정보제공인가 아닌가의 여부	피동적

(다) 목적에 따른 적정한 인증이나 신원 식별 수단의 채택

이러한 개인정보영향평가를 통해서 목적에 따른 적절한 인증이나 신원 식별수단을 채택할 수 있도록 판단을 내릴 수 있을 것이다. 인증이나 신원 식별수단의 선택시에는 데이터베이스화 여부, 축적의 기간, 용도, 관리감독, 보안, 개인의 접근, 전용가능성, 대안의 존재여부 등을 고려하여 적합한 방식을 채택할 수 있다.

나. 기술적 대응

인증이나 신원 식별 시스템을 채택할 경우, 시스템의 안전성을 기술적 측면에서 고려해야 한다. 그래서 기술적으로 가장 안전성이 높은 방법을 채택해야 하고, 여러 가지 기술적 위험을 방지하기 위한 설계가 있어야 한다. 예를 들어 가장 덜 침해적인 방법을 선택하도록 하고, 앞서 본 시스템 결함을 예방할 수 있는 시스템 설계를 해야 한다.

다. 인증이나 신원 식별 시스템의 채택시의 고려사항

(1) 가장 덜 침해적인 인증이나 신원식별 시스템의 채택

인증이나 신원 식별이 필요한지를 검토한 후, 필요한 경우에는 그 필요성에 맞는 가장 덜 침해적인 인증이나 신원식별 시스템을 채택한다.

(2) 시스템의 설계

시스템에 대하여 이용자가 투명하게 그 운영방식을 이해할 수 있어야 하며, 자신의 정보가 어떻게 처리되는지, 어떤 위험이 있는지를 명확하게 이해할 수 있어야 한다. 그리고 이용자에게 선택의 여지가 있어야 한다. 그리고 인증과 신원 식별의 목적으로 한정하고, 다른 목적으로의 전용을 엄격하게 제한해야 하고, 보관하는 정보의 양을 최소화하고, 목적을 달성한 경우 폐기하도록 해야 한다.

(3) 참여

인증이나 신원 식별의 주체가 이러한 모든 것을 결정하는데 참여하고, 관여할 수 있어야 한다.

토 론 문

생체인식과 개인 정보보호
권영빈

생체정보 활용의 인권적 쟁점과 사회적 통제
박원석

생체인식정보는 구성원을 감시하고 구속하는 것이 아니라 존중하고
보호하는 방향으로 이용되어야.
정연수

생체정보의 인권적 특성
한상희

<토론문>

생체인식과 개인 정보보호

권영빈(중앙대학교 정보대학원장)

1. 생체인식/RFID 등 신기술의 도입은 필요악?

- 개인에 대한 자동식별 기술
- 무인 자동화의 선봉장
- IT 기술의 미래: 한국의 IT 기술 선봉장
- 개인정보 침해의 우려 등장: 국내의 유출 심각, 단지 신기술만의 문제아님

2. 국제화의 고려

- 미국의 US-VISIT 프로그램: 전세계에 대하여 생체여권 / 비자의 의무화
- ICAO의 생체여권 표준화 작업, ILO의 선원 수첩 표준화 - 생체정보의 활용 의무화
- 향후 네트워크를 통한 정보의 교환 - 상호 호혜적 관점, 국내의 정보 없을 시 교환 불가

3. 개인정보의 보호

- 첨단 서비스 : 자원자 중심. 예를 들어 미국-캐나다 간 자동인식 시스템

- 개인 정보의 보호 : 법적, 제도적 보완 필요. 법적인 토대 위에 제공. 무단 사용 또는 유출의 금지

- 제도화에 따른 처벌 제도 마련, 사용자 지침의 확립 등

국제화, 국내 제도의 보완에 따른 신기술의 도입 필요성

현재도 정보는 유출 중 - 지침과 제도의 정비, 사용자 교육에 따른 인권의 보호

<토론문>

생체정보 활용의 인권적 쟁점과 사회적 통제

박원석(참여연대 시민권리국장)

1. 들어가며

생체정보는 아직 용어상 일반인들에게 낯선 것처럼 보일 수 있으나, 실제 점진적으로 그 활용이 일반화되고 있다. 이와 관련하여 지난 2001년 미국의 메사추세스공대(MIT)가 발행하는 Technology Review는 생체인식기술(biometric technology)을 "세계를 바꿀 새롭게 출현하는 10대 기술 중의 하나"로 지정한 바 있다.[1)]

최근 서울시는 일부지역에 한정되어 있던 CCTV를 25개 모든 구로 확대 설치하겠다는 방침을 밝힌바 있다. 이러한 방침은 범죄예방이라는 공공의 목적에도 불구하고 본인의 동의 없이 무차별적으로 화상정보를 수집함으로써 프라이버시권을 침해하는 것이며, 이렇게 수집된 화상 정보가 디지털 인식 기술과 결합된 생체정보 DB로 구축되어, 그 활용범위가 애초의 목적을 넘어 확대될 수 있다는 우려 또한 배제할 수 없다. 또한 지문, 유전자 DB 등 우리사회에서 생체정보의 수집과 이용은 이미 낯선 현상이 아니다.

이같은 상황에서 생체정보활용이 야기하는 인권의 문제들을 예측, 진단하고 이에 대한 대책을 검토하는 것은 필수적이라 할 수 있을 것이다.

1) Woodward D. John et al, Biometrics: A Look at Facial Recognition,(Arlington, 2003, RAND) p3

2. 생체정보의 활용 추이와 현황

현재 활용되고 있는 또는 활용가능성이 높은 생체인식 수단은 지문날인(fingerprinting), 망막검사(iris scan), 홍채검사(retinal scan), DNA 감식, 얼굴인식(facial recognition), 손/손가락 형상인식(hand/finger geometry), 음성인식(speaker/voice recognition) 등의 육체적 특성(physical characteristic)에 따른 생체정보를 활용하는 방식과 필적(handwriting), 서명(dynamic signature verification), 자판입력의 동태(keystroke dynamics) 생체정보를 통한 개인 식별 및 인증과 같은 행동적 특성(behavioral characteristic)을 분석하는 방식으로 나누어 볼 수 있다.

일반적으로 육체적 특성에 따른 생체정보가 보다 정확하게 개인을 식별할 수 있게 해주는 것으로 알려져 있으며, 육체적 특성에 따른 생체정보는 또한 각각 식별력, 수집의 용이성, 비용의 효과성 면에서 차이를 갖고 있다. 이러한 생체정보는 독자적인 식별, 인증 수단으로 활용될 뿐만 아니라, 기존의 개인 식별, 인증 수단인 비밀번호, 키, 카드 등과 융합, 혼용되는 방식으로 식별력과 보안성을 높이고 있다.

생체인식 기술을 개인 식별 및 인증의 수단으로 활용하는 추이는 그 위험성에 대한 우려와 지적에도 불구하고 전 세계적으로 빠른 속도로 확대되고 있다. 이미 많이 알려진 국제적인 사례로는 9.11 사건이후 미국이 비자면제국가들의 입국자들을 대상으로 지문과 사진을 채취하여 데이터베이스와 대조하는 이른바 US-VISIT 프로그램을 들 수 있을 것이다. 더 나아가 미국은 비자 면제국가로부터의 입국자들에게도 이를 적용하겠다는 방침을 세웠으며, 이에 해당하는 유럽국가들 및 일본 등에도 지문 등 생체정보가 담긴 생체여권으로 갱신할 것을 요구했다. 그러나, 미국의 국토안보부(Department of Homeland Security)의 주도하에 도입된 이

신원인식 시스템은 테러방지라는 명목에도 불구하고 매우 형식적인 개인정보영향평가를 거치는 등 미국 내부로부터도 인권침해의 소지가 크다는 비판을 받아왔다.[2]

연관된 사례로 최근 EU 국가들의 내무장관들은 룩셈부르크에서 회의를 열어 2006년부터 여권소지자의 얼굴특성 및 지문에 관한 데이터칩이 내장된 생체여권을 도입하기로 합의했다.[3] 이 회의에서 오스트리아, 핀란드, 네덜란드 등 몇 나라들이 이러한 방안에 대한 일부 우려를 표명했지만, 사실상 EU 국가들의 생체여권 도입은 기정사실화 되었으며, 이는 곧 같은 기준을 유럽에 입국하는 다른 나라들에게도 적용하려는 경향으로 나타날 가능성이 크며, 여타 지역으로까지 빠르게 확산될 것으로 예상된다.

생체정보의 이용은 위의 사례와 같은 국가안보 목적에 그치는 것이 아니라, 영국, 독일 등을 비롯한 유럽 국가들에서의 일부 생체정보를 포함한 스마트카드형 신분증제 도입 논란 등에서 볼 수 있듯 여타 국가정책적인 목적으로 그 활용범위를 확대해 나가는 추세에 있다. 민간영역에서 또한 상거래상의 목적, 방범용 등으로 화상 인식 등 생체인식 기술을 활용해 왔으며, 사회보험, 은행거래 등에 생체정보를 이용한 신원인식 시스템을 도입하고자 하는 시도는 지속적으로 확대되고 있다.

국내적으로도 공공기관 및 민간영역에서 생체정보의 수집 및 활용을

2) 2003년 조셉 리버만 미 상원의원은 이와 관련하여 국토안보부가 US-VISIT 생체인식 기술의 프라이버시 침해여부에 대해 충분한 평가가 이루어지지 않았다고 비판한 바 있다.

3) "Europe likely to opt for biometric passports", News.com http://news.com.com/Europe+opts+for+biometric+pasports/2100-1012_3-5429679.html?tag=nefd.hed

본격화하려는 시도로 논란이 일고 있다. 가장 대표적인 생체정보 이용의 사례로 뚜렷한 법적 근거 없이 정부가 임의적으로 구축한 전 국민 지문 DB가 애초의 목적범위를 넘어 공공기관의 폭 넓은 개인 식별 수단으로 공유되고 있으며, 민간영역에까지 이를 공유하거나, 유사한 형태의 DB 구축을 통해 상업적인 목적의 식별수단으로 활용하려는 시도도 나타나고 있다. 또한 여전히 논란이 진행 중인 미아찾기와 강력범죄 예방, 수사 목적으로 검찰, 경찰 그리고 보건복지부가 추진해 온 유전자DB 구축사업은 이미 구상의 단계를 넘어 일정 수준의 DB를 구축했으며, 이를 확대하기 위한 독자적인 법, 제도를 추진했던 단계까지 와 있다.[4)]

3. 생체정보 이용이 가져오는 잠재이익의 평가

오늘날 정보화 기술이 기업, 정부조직의 사업이나 행정적인 기능 및 효율성 향상에 성공적으로 기여하고 있는 것은 부인할 수 없는 사실이다. 그러나, 정보화 기술이 성공적으로 적용된 경우는 그러한 기술이 '제어할 수 있는 규모', '제한된 지리적 범위', '단일한 목적'과 '분명한 목표' 하에 시행된 공통점을 갖고 있다.[5)] 반면, 많은 실패 및 부작용의 사례들도 지속적으로 발생하고 있으며, 특히 디지털 기반의 정보 시스템은 한번 시행되면 종종 예기치 못한 사회적 결과와 비용 및 정보화에 대한 환상을 깨뜨리는 결과를 초래할 수 있다는 점을 유념해야 한다.

생체정보 이용을 지지하는 입장에서는 생체정보 기반 신원인식 시스

4) 검찰은 지난 94년부터 유전자 DB 사업을 본격화해오고 있으며, 98년에는 <유전자정보은행설립에 관한 법률(안)>을 마련했던 바 있다. 경찰 또한 지난 95년 <유전자자료관리 및 보호에 관한 법률(안)>을 내부적으로 마련했던 것으로 알려지고 있다.

5) Davis G. Simon, "Assessing Biometircs and Privacy and Touching Big Brother",Information Technology & Privacy Vol 7, No 4 1994,

템이 가져올 잠재적 이익 및 효과를 강조한다. 이러한 이익에는 여러 가지가 거론될 수 있겠지만, 요약하면, 다음과 같은 측면들이 포함된다.

- 행정 비용의 절감
- 개인 식별의 통합성 향상
- 정보의 통합성 향상
- 정보 접근성의 향상
- 서비스 전달의 속도 향상
- 연구 및 통계의 정확성과 질의 향상
- 커뮤니케이션의 기술적 보안 수준의 향상[6]

이중에도 특히 비용효과와 보안수준의 향상은 종종 생체정보 이용의 필요성을 뒷받침하는 대표적인 논리로 제시되곤 한다. 그러나, 문제는 이러한 잠재적인 이익의 측면을 인정한다 하더라도 이같은 이익이 큰 부작용 없이 달성될 수 있는 것인가에 대한 의문이 제기되며, 부작용을 상쇄할 만큼의 효과를 갖는 것인가를 입증할 만한 근거가 없다는 것이다.

정부차원의 대규모의 정보화 계획의 시행이 애초 예상했던 것에 비해 그 비용효과가 매우 떨어진다는 것은 여러 나라의 사례를 통해 나타나고 있다. 일례로 미국과 호주등에서 공공영역의 데이터를 연결하기 위한 계획은 여전히 그 목표가 이루어졌는지 불분명하며, 양 연방정부의 감사기관들은 이러한 계획이 비용절감 효과가 있다는데 의문을 제기해왔다.[7] 이처럼 정보화 기술의 시행의 잠재적 이익을 달성하는 것은 어렵고 종종

6) Ibid
7) Ibid

기대에 미치지 못하거나, 예측하지 못했던 엉뚱한 결과로 나타난다.

생체정보처럼 민감하고 복잡한 시스템의 구축은 그러한 기술이 가져올 잠재적인 이익을 부각시키기 전에, 예상되는 제반 문제점 등을 포함한 사회적 영향을 종합적으로 검토, 분석, 평가하고 이에 관한 합의를 만들어 가는 과정이 충실히 선행되어야 한다.

4. 생체정보 이용의 위험성 및 인권적 쟁점

생체정보 이용의 위험성은 발표문에도 제시되어 있듯 다각도로 제기된다. 불변의 신체적 특성에 따른 개인별 고유정보의 DB 구축이 일반화되는 것 자체가 위험한 것이며, 이렇게 구축된 생체정보는 그 정보의 특성상 목적범위를 벗어난 전용 또는 이용의 확장에 따른 위험성에 직면한다. 또한 정보처리의 오류, 자동화된 시스템이 외부의 공격을 받을 가능성 등 기술적 결함에 따른 위험성도 간과할 수 없다.

그러나, 무엇보다 위험한 것은 생체정보와 같은 높은 수준의 개인 식별, 인증은 시스템을 관장하는 기관의 개인들에 대한 힘의 우위를 확인하는 수단이 된다는 것이다. 이는 곧 사회구성원들의 개인성(individuality)의 약화를 의미하며, 의도적으로 또는 결과적으로 자유와 인권을 위험에 빠뜨리고 국가 또는 기업의 개인에 대한 감시와 통제의 강화, 첨단화를 야기하는 것이다.

개인의 정보에 대한 국가기구의 무질서 또는 목적별, 기능별 분리에 따른 제한적 관리는 국가의 감시와 통제로부터 개인의 자유로움을 보장한다. 그러나, 디지털 인식 기술이 결합된 생체정보의 활용은 기존의 개

인 식별 및 인증 수단에 비해 정보시스템의 획일화 가능성이 크며, 국가나 기업이 더욱 고도화된 개인정보를 수집, 통합, 이용하는 프라이버시 역진적인 방향으로 작용할 가능성이 높다. 프라이버시 보호는 획일적인 정보 시스템을 집적, 구축하려는 것에 대한 저항을 포함한다는 점을 감안할 때, 앞서 살펴본 것처럼 프라이버시 역진적인 생체정보 시스템을 구축, 확산하려는 시도들에 대한 특별한 경계가 필요한 상황이다.

생체정보의 이용은 또한 비단 프라이버시 침해에 국한되지 않는, 여타의 인권적인 문제들을 야기할 수 있다. 일례로 지문, 얼굴, DNA 등의 생체정보는 식별력이 높으면서도 특성상 본인의 동의 없이도 수집될 수 있는 것들로 이러한 정보의 수집 및 이용은 정보의 자기결정권을 침해함은 물론 '신체의 자유'를 침해하는 요소 또한 포함하고 있다.

생체정보의 이용은 또한 '평등권'을 침해하고 '차별'을 심화시키는 요인으로 작용할 수 있다. US-VISIT 프로그램의 경우 이슬람교도등 중동지역으로부터의 입국자들이 집중적으로 얼굴대조를 받는 등 차별을 당할 수 있다는 우려가 제기되었으며, 국내적으로도 검찰 경찰, 보건복지부가 추진 중인 유전자 DB에 보험회사 등이 지대한 관심을 보이고 있는데, 이는 유전자 감식이 본인이나 가계의 질병의 예측과 위험도 평가의 결정적 자료로 이용될 수 있기 때문이다. 즉, 이 같은 유전자 DB가 애초의 목적 범위에서 벗어나 그 이용이 확대될 경우, 장애인이나 특정 질병을 가진 사람들에 대한 사회적인 차별을 더욱 심화시키는 요인이 될 우려가 있다.

현재 지문 DB는 범죄발생시 수사목적의 대조로 폭넓게 이용되고 있는데, 이러한 목적의 지문 DB는 일정하게 전국민을 잠재적인 범죄자로

보는 측면이 있으며, 지문대조 방식 또한 심증이나 정황에 따른 혐의자 또는 동일 전과자를 대상으로 무차별적으로 이루어지고 있어 중요한 형사적 권리인 '무죄추정의 원칙'을 침해한다는 비판도 제기되고 있다. 특정 강력범죄 수감자를 대상으로 시행하겠다는 유전자 DB 구축계획 또한 같은 맥락에서 비판의 대상이 되고 있다.

5. 결론을 대신하여: 생체정보 이용의 사회적 통제가 필요하다

생체정보의 활용은 기존의 개인 식별 및 인증수단에 비해 정확성과 보안성이 높은 장점을 갖고 있으며, 제한적인 순기능을 할 수 있는 측면을 포함하고 있다. 반면, 고유한 신체적 특성을 담고 있는 민감한 정보로 국가기구 또는 민간에 의해 일반적인 신원인식 시스템으로 구축될 시 정보의 전용, 이용범위 확대, 시스템의 안전성의 위험을 초래할 수 있는 프라이버시 침해적 요소가 큰 위험한 정보이기도 하다. 또한 충분한 설명에 기초한 정당한 수집이 아닌 본인의 동의 없는 수집이 가능하다는 점, 그 이용이 확산될 시 차별 등 여타의 인권문제를 야기할 수 있는 점 등에서 그 도입 및 이용을 신중히 고려해야 할 사안이다.

생체정보는 이처럼 여러 가지 문제를 야기 할 수 있기 때문에 특정한 목적과 범위 내에서 이를 도입한다 하더라도 도입에 앞서 공론화 및 이를 통한 사회적 통제가 필요한 영역이라 할 수 있다. 이와 연관되어 정보화와 관련된 각종 신기술의 도입과 관련하여 개인정보영향평가제도(Privacy Impact Assesment)를 실시하자는 제안과 논의가 국내적으로도 활발하게 이루어지고 있으며, 설득력을 얻고 있다. 그러나, 현재 제안되어 있는 개인정보영향평가지침은 신기술이 야기 할 수 있는 문제점들에 대한 예방조치로서 효과를 얻기 보다는 현재의 환경영향평가가 그러하

듯 특정한 시스템의 도입이나 사업을 정당화시켜주는 형식적인 통과의례로 이용될 가능성이 적지 않다. 따라서, 단순한 개인정보영향평가를 넘어서, 생체정보의 이용에 관한 공론화 및 사회적 합의의 과정이 필요하며, 특히 생체정보라는 민감한 개인정보의 이용이 가져올 영향을 평가하는 점을 감안할 때 정보 주체의 관점과 이익이 충실히 반영되는 형태의 공론화는 필수적이라 할 수 있을 것이다. 보완적인 모델로 제시될 수 있는 것이 '참여적 기술영향 평가'이다. 이는 기존의 결과중심적인 기술영향평가에 갖는 과학기술에 대한 도구적이며 전문가중심적인 관점에 대한 비판적 검토를 통해 나온 과학기술에 대한 새로운 접근방법으로 과학기술을 하나의 사회적 과정으로 보고 전문가나 이해관계자만이 아닌 일반시민들을 포함하여 '학습'과 '논쟁'을 유발시키는 새로운 조류의 기술영향평가라 할 수 있다.[8] 참여적 기술영향평가는 주로 유럽에서 광범위하게 실시되고 있으며 대표적인 모델로는 합의회의, 시민배심원제,[9] 시나리오 워크숍 등을 꼽을 수 있다.

8) 김병수, 생체인식 기술의 발전과 프라이버시 침해 가능성, 생체정보와 프라이버시 토론회 자료집 7쪽

9) 국내에서는 지난 2001년 2월 환경,시민단체들이 공동주최로 '인간유전정보 이용에 관한 시민배심원 회의(미아찾기 유전자 DB)를 개최했던 바 있다. 당시 12명의 시민배심원들은 전문가 및 관련업계 관계자들로부터 강의, 토론을 들은 후 DNA를 이용한 가족찾기라는 대의명분에도 불구하고 사회적합의가 없는 무리한 유전자 정보은행의 설립은 반대한다는 의견을 표명한 바 있다.

<토론문>

생체인식정보는 구성원을 감시하고 구속하는 것이 아니라 존중하고 보호하는 방향으로 이용되어야

정연수(한국정보보호진흥원 개인정보보호팀장)

1. 문제제기

○ 통제가 필요한가 ?

○ 어떤 위험성이 있는가 ? 그 위험성이 특별한 것인가 ?

○ 어떤 보호가 필요한가 ?

2. 개선방안

○ 새로운 첨단과학기술이나 정보통신 기술의 도입에 대한 통제 필요

- 새로운 기술의 발전이나 도입을 제한하고자 하는 것이 아니라

- 새롭게 발전하는 기술들의 긍정적인 측면은 살리면서 부정적인 측면을 제거하면서 사회 구성원의 권리가 침해되지 않도록

○ 생체인식과 같은 새로운 기술은 간편하고 비용효과적이지만, 개인의 사생활과 자율을 위험에 빠뜨리게 할 가능성

- 통제되지 않은 생체인증은 자신에 관한 정보를 통제하는 능력을 침해할 수 있다.

- 생체정보는 일반적인 개인정보와 달리 정보 그 자체가 개인을 직접적으로 나타낼 수 있는 정보이기 때문에 생체정보의 수집과 저장 및

이용은 일반적인 개인정보의 보호 보다 더욱 세심한 접근과 분석이 요구

○ 생체인식은 오류의 가능성을 가지고 있으므로, 인권 관련 분야에서는 유일한 인증기능이 아닌 보완적인 기능으로서 역할 수행 필요

- 스트레스, 건강, 환경조건, 시간제약 등의 요인은 사람과 기계간의 상호작용에 영향을 미쳐 일관적이지 못함

○ 생체정보의 수집・이용・저장 등에서의 자기통제권의 절차와 방법은 다른 개인정보보호와 같다.

- 가장 큰 위험은 DB 연계를 위한 식별자로 활용되는 것(특히, 국가 DB와 연결될 경우)

- 생체인식DB 사이의 비교가능성을 어렵게 함으로써 프라이버시 침해에 대한 의구심 해소가 선결

3. 법제 정비방안

○ 주요사례 : 동사무소에서 인감증명 발행시 지문DB사용(강남구 등)

- 지문 DB 사용이 문제인가 ?

- 법적 근거가 없어서인가 ?

→ 원래 수집 목적외 다른 용도로 사용하면서 국민적 합의 절차가 없었음

○ 입법이 필요한가 ?

- 현행 개인정보의 정의에 생체정보도 포함되므로, 생체정보보호만을 위한 입법은 불필요하다고 보여짐

- 다만, 적용대상이 현행은 민간분야에 적용되지 않은 영역이 많으

나, 논의 중인 정통부 법안, 정부혁신위원회 법안 등 어떤 법률이 제정되더라도 문제는 해결될 것임

○ 보호 시 고려할 방안

- 필요성, 비례성 원칙의 확인
- 데이터 최소화·절약원칙 명시 : 유전자정보를 신원확인 목적으로 취득한 경우 특정한 제3자 정보 추출 금지
- 관리주체의 임의적 판단재량의 축소
- 개인에게 통제권과 선택권을 부여
- 원데이터의 삭제와 형판의 암호화
- 사회 제반 관련기관의 감시 강화
- 기술적 기준의 마련

4. 결론

○ 현재는 지문정보가 일반적으로 활용되는 추세이지만, 향후 생체인식 관련 논의는 개별적으로 논의될 필요

- 지문, 홍채, 유전자정보, 정맥 등은 각기 위험도와 대응방안이 다름

<토론문>

생체정보의 인권적 특성

한상희(건국대 법대 교수)

1. 개인정보보호의 헌법적 의미 - 기본권과 민주적 역감시

오늘날 개인정보보호의 문제는 두 가지 측면에서 헌법적 문제를 야기한다. 그 첫째는 개인정보통제권을 중심으로 하는 개인의 주관적 공권으로서의 측면이며, 그 둘째는 정보권력에 대항하면서 정보과정에 참여할 수 있는 민주주의의 측면이다. 이중 전자의 경우는 개인의 사생활의 비밀과 자유에 관한 우리 헌법 기본권편의 요청이 전면에 나서는 것이기도 하지만, 동시에 그것은 인간생활의 자율성과 해방성을 확보하는 필요충분의 조건으로 존재하기도 한다. 반면 후자의 경우는 이러한 인간의 자율성·해방성을 근거로 자신에 관한 정보의 흐름에 스스로 관여함으로써 그 정보가 적나라한 권력으로 전이되지 않고 공동의 이익을 위한, 혹은 사회적 미덕의 실현을 위한 물적 자원으로서의 의미를 획득할 수 있도록 하는 것을 의미한다. 그래서 개인정보보호제도는 그 자체 주관적 이익의 실현에 기여할 뿐 아니라 객관적 법질서의 형성·운용이라는 측면에도 기여하게 된다. 특히 오늘날 정보기술의 발전으로 인하여 최고속의 정보네트워크가 형성될 수 있고 이, 네트워크를 이용하여 기존의 권력집단들-정치권력이든 경제권력이든 아니면 사용자권력이든-이 자신들의 권력을 강화할 수 있는 가장 효율적이고 능동적인 메카니즘을 구축할 수 있는 상황에서는 이러한 개인정보제도의 정착과 그 효율적 제도는 그 무엇보다 우선적으로 요청되는 헌법적 당위라고도 할 것이다.

2. 개인정보보호의 영역 - 국가감시, 소비자감시 및 작업장감시

국가감시(state surveillance)는 안보와 질서, 행정의 효율성이라는 점에서는 正의 기능을 수행하기도 하지만, 역으로 감시의 대상인 국민들의 입장에서 보면 단순한 사생활의 침해 수준을 넘어, 권력의 적나라한 통로로서 기능하기도 한다. 그리고 이 과정에서 자기지배원리의 현저한 왜곡현상이 수반되기도 한다. 제반의 국가과정에 적극적으로 참여하는 능동적 시민으로서의 국민이 아니라, 국가는 자신이 수집, 관리하는 정보에 의하여 실제의 생활과는 괴리된 프로파일을 만들고 이에 따라 그 국가작용의 내용과 형식, 절차를 결정함으로써 사회내에는 현실의 시민이 아닌 가상적 시민(virtual citizen)만이 존재하고 되고 여기서 파생되는 시민의 소외현상은 민주주의의 가장 본질적인 내용까지 침해하게 되는 극단적 상황까지도 예견할 수 있게 하는 것이다.

소비자감시의 문제는 이러한 국가감시와는 약간 다른 맥락에서 이루어진다. R. Whitaker가 "분산된, 그러나 동의에 의한 판옵티콘(decednt-ered, consensual panopticon)"이라고 명명한 다차원적 감시구조는 소비자들에 대한 정보를 끊임없이 수집하고 분석하며, 그것을 다시 하나의 상품으로 가공하여 유통하는, 그럼으로써 생활세계가 다시 경제에 의하여 종속되고 또 가공되는 포디즘적 역기능이 야기되고 있는 것이다. 뿐만 아니라, 정보통신서비스나 콘텐츠 자체가 상품화되고 이것이 다시 거대기업이나 초국가기업에 의하여 독점적으로 유통되면서 개인의 자아실현을 위한 공간으로 구축될 수도 있는 사이버공간 자체가 경제권력에 의하여 왜곡되는 현상 또한 무시할 수 없다.

작업장 감시의 체제는 최소한 외관상으로도 쌍방향적 형태를 띠고 있는 소비자 감시와는 달리, 작업장 감시의 경우는 국가감시와 마찬가지로 일방향성을 띠고 있다. 즉, 「고용계약」에 의하여 일정한 지위를 획득한

자-노동자-에 대하여 감시자-관리자, 사용자-가 일방적으로 그 행동이나 성과, 성품등을 감시하고 이에 대하여 노동자는 복종해야 되는, 바로 이 점에서 국가감시의 틀과 조금도 다를 것이 없는 구조를 띤다. 바로 이 점에서 작업장 감시는 국가감시의 적자인 셈이다.

이에 오늘날과 같은 정보화사회에서 급격한 성장세를 보이고 있는 정보권력(그것은 국가일수도, 민간기업일수도 있다)의 문제는 단순히 개인의 주관적 공권으로서의 기본권문제의 수준에서 다루는 것으로 그쳐서는 아니될 필요가 나타난다. 오히려 그 감시에 대응하는 일종의 대항감시의 체제를 어떻게 online상으로나 offline상으로 구축할 수 있을 것인가, 혹은 정보권력에 의한 중앙집중적감시로 인하여 발생하는 권력의 집중가능성은 어떻게 제어할 수 있을 것인가? 그리고 그것을 뒷받침하는 헌법적 요청은 어떻게 구성될 수 있을 것인가 하는 실천적 문제들을 제기한다. 여기서 (헌)법은 개인정보보호의 실체 혹은 개인정보소유·이용권의 실체에 대한 문제보다는 오히려 정보기술과 사회, 국가를 연결지우고 체계화하는 일련의 구조형성(architecturing)의 부분에 관심을 기울이게 된다. 이 정보기술이 어떠한 과정과 절차에 의하여, 어떠한 목적으로 이용될 수 있으며, 그에 관하여는 어떠한 법적 관계들이 구축될 수 있을 것인가가 주된 관심이라는 것이다. 나아가 감시기술의 통제, 또는 감시방법의 규율과 같은 실체문제보다는 오히려 감시와 관련한 정책의 결정과정, 감시결과의 활용을 위한 일련의 절차, 감시결과에 대한 법적 효과의 부여, 그리고 이 모든 것에 대한 공개와 국민적 참여의 가능성 등의 문제가 중요하다는 것이다.

3. 생체정보와 기타 개인정보

이러한 아키텍쳐의 설정에 있어 심각히 고려하여야 할 사항중의 하나

로서 생체정보의 문제가 나타난다. 대체로 일반적인 개인정보(이하 「일반개인정보」라 함)와 개인생체정보는 다음 몇 가지 점에서 법규율의 차이를 야기할 정도의 상이점을 보인다.

첫째 개인정보는 모두가 일신에 부착된 것이기는 하지만, 그 부착의 정도는 두 유형의 개인정보에 따라 다르다. 일반개인정보는 신체보다는 주로 행동이나 관계 등 외형적 상태에 의하여 산출되거나 혹은 그로부터 인지되는 경우가 대부분이다. 즉, 성명, 연령, 키, 체격뿐 아니라 가족·친교관계, 소속정당, 취미나 취향 등 모두가 생활과정에서 삶이 외화되는 가운데 그 정보가 생성되고 또 이 과정에서 집적된다. 반면 지문, 동공, 혈관, 유전자 등 생체정보의 경우 그것은 신체 그 자체로부터(만) 획득될 수 있고 따라서 일반개인정보에 비하여 훨씬 더 강한 일신전속성을 보인다.

둘째, 일반개인정보의 경우 따라서 의사소통적 정보라 할 수 있다. 그것은 대면적 관계를 통해서 거의 대부분 획득될 수 있으며, 경우에 따라서는 약간의 관찰만으로도 그 필요한 정보의 대부분이 드러나게 된다. 반면 개인생체정보의 경우 별도의 획득절차나 작업이 필요하다. 유전자검사, 지문판별, 혈관대조 등 고도의 과학·기술적 확인의 작업이 있어야만 그 정보의 특성이 판별될 수 있는 것이다.

셋째, 또한 일반개인정보의 경우 인간과 인간의 관계에서 도출되는 것이 많은 만큼 그의 집적·처리로부터 상당한 부가가치의 생성이 가능하다. 예컨대, 도시집단 젊은이들의 취향을 분석함으로써 그 지역에 필요한 상품의 생산·공급의 계획을 세운다든가, 집거노인들의 행동특성을 분석함으로써 사회복지사들의 방문서비스의 질을 고양시킬 수 있는 방법을 모색하는 것 등이 이에 해당한다. 반면 개인생체정보의 경우 인간과 인간의 관계에 관한 정보라기보다는 오히려 고립된 인간-단자적 인간의

동일성에 관한 정보에 집중되어 있다. 따라서 그 정보의 활용도는 대부분 그 당사자의 동일성확인에 그치게 된다. 즉, 그것은 일반개인정보에 비하여 부가가치의 생산에 소모되기 보다는 오히려 정보주체의 동일성 확인을 전제로 하는 다양한 감시의 체계에 활용되기 십상일뿐더러-특히 작업장 감시에서 가장 많이 사용될 것으로 보여진다- 경우에 따라서는 일정한 집단·속성의 인간들을 구별하고 그들을 사회생활관계로부터 배제·배척하는 수단으로 이용될 수 있는 여지가 강하다.

4. 법적 규율의 차별화

바로 이러한 차이로 인하여 양자의 법적 처우는 달라질 수밖에 없다. 개인생체정보의 경우에는 일반개인정보와는 달리 그 수집과 분석, 처리, 활용의 모든 면에 있어 가장 집중적인 감시와 감독, 그리고 정보주체의 참여의 과정이 요청되는 것이다. 오늘의 발제는 이를 지향한 것이되, 그에 첨가하여 두어가지만 지적하는 것으로 결론에 대신하고자 한다.

첫째, 개인정보보호제도가 가지는 기본권보호의 측면과 더불어 민주주의의 실현이라는 측면을 고려할 때 개인정보를 단순히 개인의 주관적 이익만에 봉사하는 것이라는 식의 이론구성은 곤란하다. 특히 개인생체정보의 중요성을 감안한다면 더더욱 그러하다. 즉, 개인정보를 그 정보주체의 개인적 재산권과 같은 개념으로 간주하면서 동의에 의하여 양도가능한 것으로 치환해 버리는 것은 정말 곤란하다. 설령 개인이 동의에 의하여 정보를 제공하더라도 그 정보의 수집·처리·관리자는 그 정보에 대한 배타적 지배권을 가지는 것이 아니라 한정된 이용권만을 가지는 것이며 이 이용권은 언제나 정보주체의 참여를 보장하는 한도내에서만 행사되어야 한다고 보아야 할 것이다.

둘째, 개인의 신체에 대한 부착의 정도가 강한 개인생체정보의 경우

정보제공에 대한 정보주체의 동의요건과 그 동의에 기한 생체정보사용 범위는 반드시 구체적으로 특정되어야 하며, 일단 그 사용범위를 벗어나는 경우 그 정보는 폐기되어야 하는 것을 원칙을 하여야 할 것이다. 예컨대, 갑의 생체정보를 그의 동의하에 을이 A의 목적을 위하여 사용하고 그 목적이 달성된 경우 을은 곧장 갑의 그 생체정보를 폐기하여야 하며, 어떠한 경우에도 그것을 병과 같은 제3자에 이전하거나 혹은 B와 같은 제3의 목적을 위하여 전용하는 경우는 허용하지 않는 것이 바람직하다. 환언하자면 이 경우 병이나 또는 제3의 목적을 위한 사용의 경우에는 별도로 갑의 동의를 획득하고 별도의 생체정보채취·수집의 작업을 거치도록 할 필요가 있다. 만일 그렇게 하지 않고 일반적인 경우와 같이 추상적인 동의만을 가지고 개인생체정보를 다른 목적 혹은 제3자와 공유하게 되는 경우 정보주체는 자신이 알지 못하는 사이에 자신의 정체성·동일성에 대한 지속적인 감시하에 놓이게 될 것이기 때문이다.

셋째, 개인생체정보침해에 대한 집단소송제도와 징벌적 손해배상제도의 도입은 무엇보다도 선행적으로 고려되어야 할 사항이다. 뿐만 아니라, 현재처럼 개인정보보호의 시스템이 제대로 구축되지 않은 상태에서 개인생체정보가 '동의'의 허울을 덮어쓰고 자유로이 유통되는 상황은 결코 바람직하지 않다. 가능한 한 조속히 개인생체정보보호 시스템이 구축되어야 할 것이지만, 그 이전이라도 일반개인정보의 보호시스템의 구축도 서둘러야 할 것이다.