

생체정보 프라이버시 보호정책 동향

충북대학교 전기전자컴퓨터공학부 교수 전 명 근

▷▷▷ 생체인식 특집

- 생체인식 산업동향 및 전망
- 생체인식 기술현황 및 전망
- 국내·외 생체인식기술 표준화 동향
- 국내·외 생체인식제품 시험·평가 동향
- 생체정보 프라이버시 보호정책 동향**
- 국내 생체인식산업 육성 방안

1. 서론

오늘날 우리는 급속도로 발전하는 정보사회에 살고 있다. 이러한 정보사회는 정보의 생성, 저장, 처리, 운반, 검색 기능이 상호 연결된 통신망 환경 하에서 다양한 형태의 정보 서비스가 이루어지는 사회이다. 한편 이러한 정보화 사회가 주는 편리함과 유익성에 비례하여 매우 위험하고 파괴적인 역기능이 뒤따르고 있다. 특히, 인가 받지 않은 불법 사용자로 인한 정보시스템의 파괴, 개인 신상 비밀의 누설 및 유출, 불건전 정보의 유통 등과 같은 정보화의 역기능으로 인해 고통 받고 있다. 자신이 소유하고 있는 정보가 자신도 모르는 사이에 침해받고 있으며, 적절하게 보호되지 못하는 정보들로 인해 막대한 피해를 보는 상황이 현실로 드러나고 있다.

정보화 사회에서 기업은 물론 개인도 질 높은 정보를 축적하고 있으며, 이러한 축적된 정보는 네트워크를 통하여 손쉽게 전파될 수 있을 뿐더러 효과적으로 공유될 수 있는 환경이 이미 구축되어 있다. 따라서, 이러한 네트워크화된 사회에서 정보의 교환이나 상거래에 있어서 인가된 대상자와 그렇지 않은 사람을 구별하여, 정보를 보호하거나 안전한 상거래를 이룩하는 일은 어느 때 보다도 중요하다. 이러한 시대적 상황에 부응하여 패스워드와 같은 기존의 단순한 형태의 개인 확인 및 검증방법의 한계를 극복하여, 절도나 누

출에 의하여 도용될 수 없으며 변경되거나 분실할 위험성도 없는 새로운 형태의 신분검증 방법에 대한 연구가 바이오메트릭스(Biometrics) 분야이다.

생체인식기법이라고 번역되는 바이오메트릭스는 “자동화된 방법으로 특정 개인의 특성을 검증하거나 신분을 인식하기 위해, 측정 가능한 물리적 특성 또는 개인의 생체학적 특징을 연구하는 학문”으로 정의될 수 있다. 그러나 생체인식기법은 기술의 특성상 개인의 신체적 특징을 사용하는 관계로 신체의 자유에 해당하는 프라이버시 침해 요인과 자신의 동의 없이 자신의 생체 정보가 취득되어 자신을 감시하는 목적으로 사용될 수 있으리라는 부정적인 견해가 상존하는 것이 현실이다. 이에 본 고에서는 생체인식과 관련된 프라이버시 논의를 살펴보고 이와 관련된 그간의 논의점들과 국내외의 정책 현황에 대하여 살펴보고자 한다.

2. 생체정보와 프라이버시

프라이버시(privacy)를 Oxford 사전에서는 다음과 같이 정의하고 있다.

- The state of being alone and not watched or disturbed by other people
 - 다른 사람에 의해 방해 받거나 감시받지 않고 혼자 있는 상태
- The state of being free from the attention of the public
 - 대중의 관심으로부터 자유로운 상태

프라이버시란 기본적으로 다른 사람에 의해 간섭받지 않고 홀로 자신의 세계에 머무르는 상태나 권리를 일컫는 말이라고 할 수 있다. 프라이버시는 비록 시대적, 사회적, 문화적으로 통일된 의미를 가지고 있지 않지만 서구에서 정리되어 왔던 과정을 추적함으로써 그 정

의를 구체화 나갈 수 있다. 미국의 법관이던 Cooley는 1888년 프라이버시를 “인간의 신체에 대한 권리는 불가침의 권리 즉, 혼자 있을 수 있는 권리(the right to be alone)이다”라고 법률적으로 최초로 규정한 바 있다.

프라이버시 보호를 표방한 법률은 1970년에 서독에서 발효된 데이터보호법을 시작으로 1973년에는 스웨덴에서 국가 차원의 법률이 제정되었으며 미국은 1974년에 프라이버시 법을 제정하였다. 이즈음 하여, 프라이버시에 관한 유럽국가들 사이의 법적, 제도적 불일치는 상호 무역에 장애로 대두되게 되었고 이러한 위협을 극복하기 위하여, 유럽평의회에 의해서 1981년에 체계화하게 되었다.

위와 같은 법률들은 초기의 프라이버시의 개념과는 다르게 다음과 같은 적극적 의미의 프라이버시 의미를 포함하고 있다. 첫째 현대 사회의 도래와 더불어 개인간의 접촉은 더욱 빈번하여지고 사회와 국가의 안녕을 위하여도 타인과 격리되어 ‘혼자 있을 권리’가 보장될 수 있는 사회적 환경은 거의 불가능하다. 둘째, 정보통신의 발전과 더불어 개인의 정보나 데이터가 쉽게 확산될 수 있으며 때로는 영리적인 목적을 위하여 개인의 정보가 거래될 수 있는 사회 경제적 환경이 도래하였다는 점이다. 따라서 소극적으로 사회와의 격리를 통해서 개인의 프라이버시를 지키는 것은 불가능하며 노출될 수밖에 없는 개인의 정보를 지키기 위해 적극적으로 자신의 정보를 스스로 통제할 수 있는 제도적 장치를 마련하는 데 초점을 두고 있다고 할 수 있다.

각 국가에서는 관련된 법률을 제정함에 있어서 ‘개인 데이터’, ‘개인정보’, ‘프라이버시’의 개념을 혼용하여 사용하고 있다. ‘데이터’라는 용어는 주로 유럽의 국가에서 많이 사용하게 되는데 이는 유럽국가간의 상거래에 있어서 보험이나 은행업과 다국적 기업에 있어서 개인의 신용과 같은 데이터가 국경을 넘어서 주고받을 때 생기는 문제에 초점을 두었다고 할 수 있다. 반면에 개인주의적 성향이 강한 미국에서는 개인의 혼자 있을 권리에 바탕을 둔 프라이버시라는 용어를 사용하여 프라이버시 법을 제정하였음을 알 수 있다. 반면에 일본은

1980년의 OECD의 권고안에 따라 1988년 “행정기관이 보유하는 전자계산 처리에 다른 개인정보의 보호에 관한 법률”을 제정하였다. 우리나라는 1994년에 프라이버시 관련법으로는 처음으로 ‘공공기관의 개인정보보호에 관한 법률’을 공포하였다. 동 법률의 제2조 제 2항에 따르면 개인정보란 다음과 같이 정의되어 있다.

“생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보로서 용이하게 결합하여 식별할 수 있는 것을 포함한다)”

비록 국가적으로 프라이버시 관련 법령을 제정함에 있어서 다양한 변형이 있으나, 그들간에는 많은 공통점을 발견할 수 있다. 이는 이들이 공통의 뿌리를 가지고 있으며 유럽위원회, OECD, EU와 같은 국제적인 기구에 의해서 지속적인 압력이 행사되었기 때문에 가능하였다. 이와 같이 프라이버시는 많은 경우 도덕적이거나 혹은 헌법적인 권리로서 논의된다. 이러한 프라이버시는 다음과 같이 몇 가지로 나눌 수 있다.

○ 신체의 프라이버시

- 개인의 신체의 자유에 관한 것으로 강제적인 면역 주사 접종, 개인의 동의 없는 혈액 수혈, 강제적인 불임시술, 그리고 체액이나 신체정보 샘플을 취득하는 행위에 관한 논의들을 포함하고 있다.

○ 개인적 행위의 프라이버시

- 개인의 행위에 기반한 모든 측면을 포함하는 것으로 특별히 민감한 문제, 예를 들어 성적인 기호나 버릇, 정치적 행위, 종교적 행위들로서 사적인 것과 공적인 공간 모두를 포함한다.

○ 개인 데이터의 프라이버시

- 개인은 자기 자신의 데이터가 다른 사람이나 기관에 의해서 자동적으로 접근이 가능하지 않도록 요구할 수 있다. 비록 데이터가 타인이나 기관에 의해서 가공 처리될지라도 개인은 반드시 그 데이터와 그의 이용에 따른 상당한 부분의 통제권을 행사할 수 있어야 한다.

위에서 살펴본 것과 같이 프라이버시의 개념은 남들로부터 간섭받지 않을 소극적 개념에서 출발하여 개인의 정보를 스스로 통제할 수 있는 적극적 개념으로 발전하여 왔다. 생체인식기법이란 지문이나 얼굴, 홍채패턴, DNA 검사와 같은 개인의 신체정보를 이용하여 개인인증을 수행하는 기법이라는 것을 생각하면 필연적으로 대상자의 신체적 정보를 취득함으로써 ‘신체의 프라이버시’를 침해할 수 있는 요소를 포함하고 있으며, 우연한 장소에서 검출된 나의 지문이나 인지하지 못하는 사이에 카메라에 잡힌 나의 얼굴 영상에 의해서 나의 ‘개인적 행위의 프라이버시’를 심각하게 위협받을 수 있다. 더욱이 나의 생체 정보는 여러 개인정보 중에서 나를 가장 잘 식별해 낼 수 있는 것으로 이것이 유출되거나 오용되었을 경우에 ‘개인 데이터의 프라이버시’를 침해받을 수 있다.

그러나 여기서 생체인식 기법이 개인정보보호를 위한 하나의 중요한 기법이라는 점을 상기할 필요가 있다. 기존의 주민등록번호나 신분증에 의한 개인 식별이나 인증방법 보다도 타인을 사칭하기가 어려우며, 인식 기법의 발전과 유비쿼터의 환경의 도래에 힘입어 언제 어디서나 안심하고 나의 신분을 확인받을 수 있는 장점이 있기 때문이다. 결국 모든 기술의 발전에 있어서 혜택을 줄 수 있는 부분과 그것의 역기능을 막기 위한 노력이 동시에 필요한 것처럼 생체정보 프라이버시 보호를 위한 여러 가지 정책이 고려되고 있다.

3. 생체정보 프라이버시 보호 정책

생체인식분야는 프라이버시의 관점에서 보면 다른 어떤 분야보다도 다양한 논의의 한가운데 위치하고 있다고 할 수 있다. 생체인식의 분야에 종사하는 사람들의 경우에는 프라이버시에 관한 논의를 불식시키면서 생체인식 분야의 사용을 촉진시키려 하는 반면에 프라이버시 보호를 위해 적극적으로 나서는 사람의 입장에서는 생체인식 기술에 대하여 일종의 두려움을 가지고 있다. 생체인식 기술은 개인의 신분을 밝혀내거나 인증하는 긍정적 역할을 함으로서 신분확인과 관련된 다양한 범죄행위를 적발하거나 예방할 수 있으며, 이는 정보통신의 발달과 더불어 나날이 증가하는 온라인 세상에서는 더욱더 그 가치를 나타낼 수 있다. 그러나 생체인식 기술은 본인의 동의 없이 개인이나 그와 관련된 모든 거래나 컴퓨터 상의 변동자료를 추적할 수 있으며, 다양한 개인적인 정보를 특정개인과 관련하여 지속적으로 추적하는데 사용할 수 있다. 통상 생체인식은 다음과 같은 세 가지의 체계적인 프라이버시 문제에 관한 논쟁을 불러 일으킨다.

○ 의도하지 않은 기능적 응용

- 생체인식 식별자들의 기원이 생물학적이기 때문에 정보 수집자들이 조사된 생체인식 측정값으로부터 부가적인 개인 정보를 얻을 수도 있다. 예를 들면 특정 기형의 지문은 특정 유전적 변이와 통계적으로 관련지을 수 있다.

○ 의도하지 않은 기술적 응용

- 지문과 같은 강력한 생체인식 식별자는 바람직하지 못한 의도하지 않은 인식의 가능성을 가지고 있다. 예를 들면 안전상의 이유로 인해 합법적으로 다른 이름을 사용하고자 하는 사람이 자신의

지문으로 인해 원래의 자신으로 인식되어지는 경우이다.

○ 인지되지 않는 상황에서의 인식

- 얼굴과 같은 생체정보는 대상자 모르게 카메라를 이용하여 촬영함으로써 사용이 가능한데 이러한 경우에는 미리 등록된 사람들에 대한 비밀스런 인식이 수행될 수 있다. 즉, 어떤 특정 상황 하에서 익명으로 남고자 하는 사람은 생체인식으로 인해 자신의 프라이버시가 침해될 수도 있다.

위와 같은 생체정보에 대한 프라이버시의 침해 위험에 관한 논의가 다양한 매체나 대중의 주목을 받아 생체인식 기술을 대중화하여 적용하는데 장애물로 작용하고 있는 것이 사실이다. 그러나 대부분의 경우 생체정보를 '개인정보'의 일종으로 보고 개인정보보호법이라는 큰 틀에서 다루고 있다. 이때, 각국의 개인정보정책에 기본이 되는 철학을 제시하고 있는 것이 1980년에 제시된 다음과 같이 8개 원칙으로 이루어진 OECD의 개인정보 보호 가이드라인이다.

○ 수집제한의 원칙(Collection Limitation Principle)

- 개인적 데이터의 수집은 제한되어야 하며, 그러한 데이터는 반드시 합법적이고 정당한 방법에 의해, 데이터 제공자의 동의나 인지하에 얻어져야 한다.

○ 데이터의 정확성 원칙(Data Quality Principle)

- 개인의 데이터는 반드시 사용목적에 부합되며, 정확하고 완벽하며 최신의 것이어야 함.

○ 목적 규범의 원칙(Purpose Specification Principle)

- 데이터 수집의 목적은 그것이 수집될 때 규범화되어야 하며, 이후의 사용에도 반드시 이러한 목적에 부합되는 경우로 제한되어야 한다.

○ 사용제한의 원칙(Use Limitation Principle)

- 개인 데이터는 공개되어서는 안되며, 앞의 원칙에서 규범화된 목표에 부합하지 않게 사용되어서는 안된다. 단, 데이터 제공자의 동의나 법률에 의한 것은 예외로 함.

○ 안전보호장치의 원칙(Security Safeguard Principle)

- 개인적인 데이터는 데이터의 공개나 수정 파괴와 같은 위험에 대하여 바람직한 보호장치에 의해 보호되어야 한다.

○ 공개의 원칙(Openness Principle)

- 개인 데이터에 대한 개발장치, 설치와 활용에 대

하여 일반적인 공개 원칙이 있어야 한다.

○ 개인 참가의 원칙(Individual Participation Principle)

- 개인은 필요한 경우에는 자신에 대한 데이터의 소재를 합리적인 시간내에 합리적인 비용과 방법에 의해 통지받을 권리가 있다.

○ 책임의 원칙(Accountability Principle)

- 데이터 수집자에게는 앞의 원칙들을 실시하기 위한 조치에 따라 책임이 부여되어야 한다.

위와 같은 OECD의 개인정보보호 가이드라인 8개가 지켜진다면 생체정보 프라이버시와 관련되어 걱정되어지고 있는 ‘의도하지 않은 기능적 응용’, ‘의도하지 않은 기술적 응용’과 ‘인지되지 않는 상황에서의 인식’과 같은 우려는 상당부분 해소될 수 있을 것으로 시민사회에서는 받아들여지고 있다.

현재, OECD 회원국인 우리나라가 헌법이 보장하고 있는 국민 사생활의 비밀과 자유를 보장하는 측면에서 제정한 주요 프라이버시 보호 관련 법률은 다음과 같다.

표 1. 프라이버시 보호 관련법 현황

| 법의 명칭 | 제정연월 | 목적 |
|----------------------|------------------------|--|
| 공공기관의개인정보보호에관한법률 | 1994년 1월 7일(법률4734호) | 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함 |
| 공공기관의정보공개에관한법률 | 1996년 12월 31일(법률5242호) | 공공기관이 보유 관리하는 정보에 대한 국민의 공개청구 및 공공기관의 공개의무에 관하여 필요한 사항을 정함 |
| 전자거래기본법 | 1998년 12월 24일 | 전자상거래의 안정성과 신뢰성을 확보 |
| 정보통신망이용촉진및정보보호등에관한법률 | 2001년 1월 16일 | 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함 |
| 전자상거래등에서의소비자보호에관한법률 | 2002년 3월 30일 | 전자상거래에 있어서 통신판매업자 등이 준수하여야 할 사항을 규정하여 공정한 거래질서를 확립 |

위와 같은 기존의 법률과 별도로 급증하는 개인정보 보호에 관한 사회적 요구를 반영하기 위하여 정부와 여당에서는 각각 별도의 ‘개인정보보호기본법’을 마련하여 국회의 상정을 앞두고 있으며, 이와는 별도로 시민단체와 민주노동당이 공동으로 법률안을 마련해 놓은 상태이다. 이러한 다수의 법률안들의 주요 쟁점사항은 개인정보보호를 전담하는 독립기구의 설치와 그에 따르는 감독 권한의 범위를 어디까지 할 것인가에 있다. 또한 미국 캐나다 등 선진국에서 시행하고 있는 개인정보사 전영향 평가제의 도입여부가 뜨거운 쟁점으로 되어 있다. 이에 대하여 시민 단체들에서는 개인정보의 알 권리 보장과 형사처벌까지 가능토록 처벌기준을 강화하는 것은 물론 집단소송제까지 주장하고 있다. 이에 반하여 전자상거래 관련 업계에서는 선진국에서조차 프라이버시 영향 평가는 전자정부에 대하여 국민의 프라이버시와 개인정보에 미치는 영향에 대한 평가를 제도화 한 것으로 이를 민간영역에까지 확대 적용하는 것은 관련 시장의 위축과 혼란을 야기할 것이라며 크게 반발하고 있는 상황이다.

한편, 정보통신부와 정보보호진흥원은 금년 3월 11일 광대역 통합망과 유비쿼터스 네트워크 등 안전한 ‘u코리아’ 구현을 위해 2008년까지 4년간 2354억원을 투입하는 것을 골자로 하는 ‘중장기 정보보호 로드맵’을 발표한 바 있다. 따라서 생체정보에 대한 프라이버시 보호 정책도 이러한 틀 속에서 논의되어지리라 생각된다.

4. 결론

생체인식 시스템은 일부의 사람들에게 개인적 존엄이나 권리, 혹은 개인적 공간에 대해 프라이버시 침해적인 것으로 이해되고 있다. 예를 들어 지문이나 손모양 같은 생체적 특징들을 측정을 위해 제공해야 하는 것은

불쾌하거나 비인간적인 것으로 보일 수 있다. 아마도 이러한 생체인식 시스템 자체에 부정적인 이미지를 제공하여 준 것은 조지오웰 작품의 ‘1984’가 아닐까 생각된다. 소설 속의 빅 브라더와 같이 개인의 사적 영역에 까지 감시의 눈을 떼지 않도록 하게 하는 기술적 배경이 생체인식 기술이 되지 않을까 우려하는 시선이다. 그러나 조지오웰이 1949년, 스탈린 체제와 같은 전체주의 국가를 생각하며 1984년의 미래를 담은 이 소설의 시대 배경보다 20여년의 세월이 흐른 지금의 문명사회에서 그러한 우려는 지나친 것이 아닌가 생각된다. 그러한 빅 브라더의 존재 여부는 기술자체의 문제라기보다는 인류 문명이 발전해 나가면서 구축하게 되는 법체제나 정치체제의 시공간에서 생겨날 수 있는 공동체가 가지는 가치관의 문제가 아닐까 생각된다. 인터넷의 경우, 그것의 부정적 기능을 논하는 사람도 있지만, 오히려 우리 사회의 투명도를 높이고 특정기관이나 개인이 시민을 감시하거나 조정하는 것을 어렵게 하는 긍정적인 측면이 크다고 생각된다.

이런 점에서, 사회의 안전성과 건전성을 향상시키기 위해서는 다소간의 개인적 프라이버시가 양보되어야 한다는 시각과, 인권의 개념으로 프라이버시 문제를 바라볼 경우에는 서로가 상충되는 점이 있다. 우리나라 헌법 17조는 “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다”라고 명시함으로써 개인의 프라이버시를 존중하고 있다. 반면에 헌법 37조 2항에는 “국민의 모든 자유와 권리는 국가안전보장 질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있으며, 제한하는 경우에도 자유와 권리의 본질적인 내용을 침해할 수 없다”라고 명시하고 있다. 이러한 헌법의 정신을 따르자면, 사회의 안전과 공공복리를 위해 생체인식 시스템의 적용 및 확대는 가능하나, 이때에도 최대의 개인의 권리를 존중하되 엄격히 프라이버시 침해를 막는 법률적 장치가 필요하며, 이러한 프라이버시 보호 정책 또한 기술의 발전과 병행하여 더욱더 공고해지리라 생각된다. **TTA**