情 報 保 護 學 會 誌
第 15 卷 第 6 號, 2005. 12

생체정보 이용과 프라이버시 보호

전 명 근*, 문 기 영**

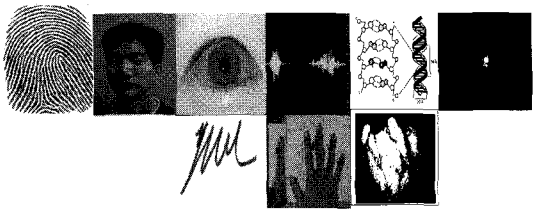
요 약

정보 통신의 발달로 네트워크를 통한 개인 신원의 확인이나 인증의 필요성이 증가하고 있다. 기존의 패스워드에 의한 개인 확인방법은 비교적 구현이 용이한 반면에 타인에게 노출되어 오용될 수 있는 가능성이 높으며, 다수의 패스워드를 기억에 의존하여 관리하는 것도 쉽지 않은 형편이다. 이에 개인의 고유한 생체적 특징에 기반을 둔 생체인식 시스템이 다양한 분야에서 사용되고 있으나, 이를 둘러싼 프라이버시 침해 논의로 그 적용이 제약 받고 있는 것이 현실이다. 이에 본고에서는 생체정보와 프라이버시의 관계를 살펴보기 위해 먼저 생체정보 이용에 있어서의 프라이버시 침해요인을 분석하고, 이에 대한 국제적 동향과 프라이버시 영향평가에 대해서 알아본다. 다음으로 현재 우리 주변에서 생체인식시스템과 관련하여 주요 이슈로 다루어지고 있는 US-VISIT, 지문날인, 생체여권, CCTV에 의한 방범 시스템과 같은 국내외의 활용 현황들을 알아보고 생체정보보호를 위한 정책동향을 살펴보고자 한다.

Ⅰ. 서 론

정보통신의 발달로 기업은 물론 개인도 다양한 정보를 축적하고 있으며 이를 네트워크를 통하여 손쉽게 전파 할 수 있을 뿐만 아니라 대규모로 공유할 수 있는 환경이 이미 구축 되어 있다. 더욱이 인터넷의 발달로 촉발된 전자상거래의 규모는 큰 규모로 늘어나고 있으며, 이에 따라 기존의 단순한 형태의 개인 확인 및 검증방법의 한계를 극복하여, 절도나 누출에 의하여 도용 될 수 없으며 변경되거나 분실할 위험성도 없는 새로운 형태의 신분검증 방법에 대한 연구 분야인 바이오메트릭스(Biometrics)분야의 연구가 활발히 진행되고 있다.

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 있는데 주요 대상 기법은 그림 1과 같이, 정적인 생체특징으로 지문, 홍채, 얼굴, 손등혈관, 망막 혈관, 손금, 귀모양, DNA를 사용하고 있으며, 동적인 생체특징으로 음성, 온라인 서명인식, 걸음새, key stroke



〔그림 1〕 생체인식기법에서 널리 사용되는 생체특징

등을 사용하고 있다.[1]

한편, 정보보호를 위해서 채택되고 있는 생체인식 시스템이 역으로 개인의 신체적 정보라는 개인정보를 침해하고 있다는 논란이 광범위하게 일고 있다. 이는 결국 개인의 프라이버시와 연결된 문제라고 할 수 있는데, 프라이버시는 넓은 영토의 소수에 의해 이루어진 마을단위의 공동체에서는 중요한 문제가 아니었으나, 산업혁명을 거치면서 더욱더 중요한 인간의 가치로 자리 매김 됨에 따라, 19세기 말 무렵 미국의 사법관들에 의해 논의되어 오던 것이 1888년 법관 Cooley에 의해 "인간의 신체에 대한 권리는 완전한 불가침의 권리, 즉 혼자 있을 수 있는 권리(the right to be let alone)"로 최초로 규정된 후 광범위한 시민권

본 연구는 한국전자통신연구원(ETRI)의 위탁연구지원에 의해 수행되었습니다.
* 충북대학교 전기전자컴퓨터공학부 (mgchun@chungbuk.ac.kr)
** 한국전자통신연구원 정보보호연구단 생체인식기술연구팀 (kymoon@etri.re.kr)

의 행사로 하나로 자리를 잡게 된다.

프라이버시는 많은 경우 도덕적이거나 혹은 헌법적인 권리로서 논의된다. 따라서 각 나라별로 이를 위한 별도의 법률적 제도나 사회적 제도 등을 별도로 두고 있는 실정이나, 학자들 간에는 이를 권리로 보기보다는 하나의 이해관계내지 관심사로 보는 경향도 있다. 이러한 프라이버시도 다음과 같이 몇 가지로 나눌 수 있다. 첫째, 신체의 프라이버시로 개개인의 신체의 보전에 관한 것으로 강제적인 면역주사 접종, 개인의 동의 없는 혈액 수혈, 강제적인 불임시술, 그리고 체액이나 신체정보 샘플을 취득하는 행위에 관한 논의들을 포함하고 있다. 둘째, 개인적 행위의 프라이버시로, 행위적인 모든 측면을 포함하는 것으로 특별히 민감한 문제, 예를 들어 성적인 기호나 버릇, 정치적 행위, 종교적 행위들로서 사적인 것과 공적인 공간 모두를 포함한다. 셋째, 사적 통신의 프라이버시로, 다른 사람이나 기관의 감시 없이 다양한 매체를 통하여 사적인 통신을 할 수 있도록 개인이 요구 할 수 있는 측면을 말한다. 마지막은 개인 데이터의 프라이버시로, 개개인은 자기 자신의 데이터가 다른 사람이나 기관에 의해서 자동적으로 접근이 가능하지 않도록 요구할 수 있다. 비록 데이터가 타인이나 기관에 의해서 가공 처리 될지라도 개인은 반드시 그 데이터와 그의 이용에 따른 상당한 부분의 통제권을 행사할 수 있어야 한다.

또 다른 논의는 바로 생체인식을 둘러싼 논의이다. 인터넷이나 개인의 신분확인이 필요한 공항 출입국에 있어서 생체정보를 사용함에 따라, 이를 개인적 프라이버시의 침해로 보고 여러 단체나 개인이 문제를 제기하고 있다. 개인의 생체정보를 강제적으로 취득하는 경우라면 이는 명백히 위에서 언급된 '신체의 프라이버시'를 침해한 경우에 해당되며, 생체데이터는 자기 자신을 나타내는 고유의 식별자로서 이는 어떠한 개인 데이터보다도 자기 통제권이 요구되는 '개인 데이터 프라이버시'의 영역에 속하는 문제라고 할 수 있다. 생체정보를 이용한 인식기법은 다양하게 존재하며, 따라서 각 분야에서 발생하는 프라이버시 침해의 양태가 매우 다양하다고 할 수 있다.

이러한 생체정보시스템의 구축은 필연적으로 보다 많은 생체정보를 요구하고 이는 일반인들의 프라이버시 침해 논란을 야기 시키리라 생각 된다. 따라서 본 연구에서는 이러한 문제점을 분석해 보고자 한다. 2장에서 생체인식과 프라이버시와의 관계를 알아보고, 3장에서는 생체정보와 프라이버시 현황 및 문제점에 대하여 사회적 여러 이슈들을 살펴본 후 4장에서 결론을 맺고자 한다.

II. 생체인식과 프라이버시

2.1 생체정보와 프라이버시

생체인식분야는 프라이버시의 관점에서 보면 다른 어떤 분야보다도 다양한 논의의 한가운데 위치하고 있다고 할 수 있다. 생체인식의 분야에 종사하는 사람의 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.[2] 생체인식 기술은 개인의 신분을 밝혀내거나 인증하는 긍정적 역할을 함으로서 신분확인과 관련된 다양한 범죄행위를 적발하거나 예방할 수 있다. 그러나 생체인식 기술은 본인의 동의 없이 개인이나 그와 관련된 모든 거래나 컴퓨터상의 변동자료를 추적할 수 있으며, 다양한 개인적인 정보를 특정개인과 관련하여 지속적으로 축적하는데 사용할 수 있다. 몇몇 국가에서는 벌써 이러한 프라이버시의 위험에 관한 논의가 다양한 매체나 대중의 주목을 받아 생체인식 기술을 대중화하여 적용하는데 장애물로 작용하고 있는 것이 사실이다.

생체인식 기술은 본인임을 증명하는데 뿐만 아니라, 필요하다면 특정개인과 그와 관련된 거래를 추적하는데 사용될 수 있다. 현재에도 신용카드를 이용하여 사용자를 추적 할 수 있으나, 사용자의 개인 신분확인이 되지 않는 관계로 완벽하게 이루어 질 수는 없다. 따라서 생체인식기술의 옹호자들은 사기꾼들이 훔친 카드를 더 이상 사용 할 수 없는 것을 제외하고는 아무것도 바뀌는 것이 없다고 이야기한다. 또한, 지문이나 홍채 등의 원영상이 중앙 데이터베이스에 저장되는 것이 불필요하여, 한번 생체정보가 등록이 되면 지문 원영상 등은 파괴가 되고 디지털 템플릿의 복사본만이 사용자가 소지하고 있는 카드에 담기게 되어 결과적으로 개인의 프라이버시 침해는 없다는 주장한다. 그러나 이러한 주장에는 여러 가지 고려할 사항이 있다.[3] 만약에 카드가 분실되거나 망실되었을 경우에 각 개인이 실제로 '등록 센터'에 가서 자신의 신분카드 제시와 함께 지문을 채취하는 과정을 거치지 않고 어떻게 재발급 받을 수 있을 것인지가 문제가 된다. 반면에, 지문을 중앙관리 하는 경우에는 생체템플릿을 포함하는 카드를 재발급하거나 인터넷을 통하여 다운로드 할 수 있는 등의 방법이 있다. 이런 경우에 어딘가 사이버

공간상에 존재하는 지문영상과 템플릿을 저장하는 중앙 데이터베이스를 생각 할 수 있다.

이러한 생체정보의 중안관리의 문제점은 지문과 같은 생체특징이 개인의 신분을 나타내는 하나의 개인 식별자로 작용하여 특정인의 모든 거래를 추적하거나 개인적 정보를 그와 연관시키는데 사용될 수 있다는 것이다. 공공의 장소를 이용하기 위하여 지문인식을 이용하였는데, 우연히 그 장소에서 범죄가 발생하여 본의 아니게 모든 출입자들이 용의자 선상에 오르고 이들의 신분이 중앙에 저장되어 있는 지문데이터베이스에 의해 색출되는 상황이 온다면 이는 분명 프라이버시 침해의 소지가 있게 된다.

그러나 다른 한편으로 생체정보는 자신의 민감한 개인정보를 보호하기 위한 수단으로도 사용 될 수 있다. 타인 사칭 문제의 범위와 규모가 확대됨에 따라 지문과 같은 강력한 생체인식이 정보들이 생체인식의 긍정적인 도구로써 그 사용이 확대되고 있다. 예를 들면, 우리나라에서는 동사무소에서 인감증명서를 발급하는 등의 개인적 공문서 발급 등에 지문인식을 이용한 본인 확인여부를 수행하고 있으며, 미국 입법부는 중요하고도 민감한 의료기록에 대한 접근을 제한하기 위해서 생체인식과 같은 강력한 인식 시스템을 요구하고 있다.

한편, 특정 응용프로그램 개발자들은 익명의 접근을 허용하는 수단으로서 생체인식의 사용을 도모해왔는데, 이러한 응용 프로그램은 사용자의 이름을 직접적으로 사용하지 않는 대신 사용자에 고유한 정보를 색인화 할 수 있으며 사용자 접근 시에 특정 생체인식을 수행하게 된다. 더욱이 보다 안전한 생체인식 시스템을 통한 자동화된 접근 방식을 요구함으로서 시스템 관리자는 특별한 정보에 대한 모든 접근을 추적하고 정보 시스템 내에서 작업을 수행하는 사용자들에 대한 관리 기능을 향상시키는 것이 가능하다. 따라서 지문과 같은 생체정보를 사용함으로서 개인 정보를 저장하고 있는 시스템의 무결성을 보다 명확히 향상시키는 것이 가능하다.

그럼에도 불구하고 생체인식은 세 가지의 체계적인 프라이버시 문제점들을 불러일으킨다.[4] 첫째, 의도하지 않은 기능적 범위(Unintended functional scope)로, 생체인식 식별자들의 기원이 생물학적이기 때문에 정보 수집자들이 조사된 생체인식 측정값으로부터 부가적인(통계적일 수 있는) 개인 정보를 얻을 수도 있다. 예를 들면 특정 기형의 지문은 특정 유전적 변이와 통계적으로 관련지울 수도 있다. 둘째, 의도하지 않은 응용 범위(Unintended application scope) : 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. 부가적으로 생체인식 식별자들은 광범위하고 다양한 어플리케이션에 등록된 각 개인들의 행위 정보와 연계시키는 것이 가능하다. 생체인식반대론자들은 종종 이러한 잠재성을 각 개인에 대한 지배력을 높이고 정부나 기업과 같은 조직의 힘을 증가시키기 위한 수단으로서 이해한다. 셋째, 비밀스런 인식(Covert recognition)이다. 개인의 얼굴 정보와 같은 생체인식 표본을 소유자 모르게 얻는 것이 가능한데 이러한 경우에는 미리 등록된 사람들에 대한 비밀 인식이 허용된다. 결론적으로 어떤 특정 상황 하에서 익명으로 남고자 하는 사람은 생체인식으로 인해 자신의 프라이버시가 부정될 수도 있다.

2.2 생체인식시스템에서의 프라이버시 분석

공공분야나 개인기업 등에서 생체인식 시스템에 대한 구현을 고려하고 있다면 이와 관련된 프라이버시 문제들에 대해 확실한 이해를 갖고 있는 것은 큰 도움이 된다. 이러한 이해는 그것을 사용하게 될 시민이나, 회사원들 혹은 고객들에게 프라이버시 문제를 설명하는데 필요할 뿐만 아니라 생체인식 시스템의 저변을 확대하는 데에도 필요하기 때문이다. 생체인식 시스템에서 프라이버시 문제는 두 가지 분명한 영역으로 나누어 생각할 수 있는데 개인 프라이버시 영향(Personal Privacy Impact)과 정보프라이버시 영향(Informational Privacy Impact)이 그것이다.[5] 개인 프라이버시 영향은 개인 검증(Verification) 혹은 식별(Identification)의 목적으로 생체인식 데이터를 제공하는 과정과 관련된 프라이버시 충돌과 관련되며, 정보프라이버시 영향은 생체인식 데이터 혹은 생체인식 식별자와 관련된 데이터의 오용과 관련된 프라이버시 충돌과 관련된다. 이러한 두 가지 영역의 문제들을 적절히 취급하지 않을 경우 생체인식 시스템의 구현을 무산시키거나 현재 성공적으로 진행되고 있는 생체인식 기술의 활용이 순조롭지 못할 수 가 있다.

개인적 프라이버시의 문제는 정보의 프라이버시 문제 보다 훨씬 더 특정 문화, 국가, 혹은 계층 내에서 나타날 가능성이 크다. 특정 그룹은 법죄자 색출에 주로 사용되었던 지문인식에 대한 부정적 인식으로 인하여 지문 인식이나 채취에 대해 강한 거부감을 표시할

수 있다. 어떤 문화권에서는 이와 다르게 얼굴 사진에 대해 반대적인 입장을 취할 수 있다. 또한, 정보 프라이버시의 문제는 생체인식 정보에 대한 인증되지 않은 수집, 사용, 보유, 그리고 공개와 같은 문제들과 깊이 관련되어 있다. 이러한 문제들은 개인이 그가 가진 개인적 정보에 대한 접근과 사용을 통제할 수 있는 권리를 갖고 있다는 근본적인 프라이버시 개념에 기초하고 있다. 생체인식적 데이터는 개인적 데이터일 뿐만 아니라 매우 민감하며 대체 불가능한 개인적 정보로 간주되기 때문에, 생체인식 시스템에 있어서 정보 프라이버시는 매우 특별한 문제이다. 중앙집중화 된 생체 데이터베이스, 추적, 감시, 혹은 빅브라더식 운영과 관련된 두려움은 모두 정보 프라이버시 문제를 표현한 것이다.

개인적 프라이버시 문제와는 반대로 정보 프라이버시의 문제는 어느 정도까지는 데이터의 획득이나 관리에 대한 체계적인 접근 방식을 통해 설명 가능하다. 이론적으로, 정보 수집에 대한 제한 뿐만 아니라 정보에 대한 완전한 보호가 보장된다면, 정보 프라이버시의 문제는 대부분의 개인에게 있어서 만족스러운 것이 될 것이다. 즉, 개인의 정보통제권을 근간으로 OECD 권고안의 '안전보장 장치의 원칙'과 '개인 참가의 원칙'이 지켜진다면 정보프라이버시 문제는는 상당부분 해소 될 수 있다.

정보 프라이버시에 대한 체계적인 접근 방식은 다음과 같은 개념들과 결합되어져야 한다. 첫째, 부당한 정보 수집으로 생체인식 정보의 부당한 수집은 정보 프라이버시의 주된 관심사이다. 부당한 정보 수집은 생체인식 데이터베이스와 개인의 동의가 없거나 개인이 알지 못하는 사이에 수행되는 매칭 과정을 증가시킨다. 특히, 얼굴 인식은 동의 없이 생체인식 데이터를 획득하기 위해 사용될 가능성이 있다. 둘째, 부당한 사용으로, 생체인식 데이터에 대한 부당한 사용은 생체인식으로 인해 프라이버시에 대해 제기될 수 있는 가장 심각한 위협으로 보여 진다. 부당한 사용은 상업 혹은 정부의 데이터베이스에 대한 검색을 위하여 사용되는 것을 포함하여 최초의 의도보다 보다 더 광범위하게 생체인식 데이터를 사용하는 방식들을 포함하고 있다.

생체인식 데이터 접근에 대해 허용된 범위를 넘어서는 공공 및 개인 기업에서의 사용 등은 생체정보를 제공하는 사람들에게 가장 위협적인 요소로 인식되고 있다. 이는 OECD 권고안의 ' 목적 규범의 원칙'과 '사용제한의 원칙'에 깊이 연관되어 있는 사항으로 생체정보의 이용은 수집 당시에 명시된 목적에 부합되는 용도로만 사용되어야 한다. 셋째, 부당한 생체인식 정보 유지로, 생체인식 정보를 필요 이상으로 오랜 기간 저장하고 있다면 이 또한 프라이버시의 침해 요소로 작용할 수 있다. 당초의 생체인식 시스템에서 규정한 목적을 달성하였다면 저장하고 있던 생체정보는 마땅히 파기해야 할 것이다. 그렇지 않은 경우 추후의 기술의 발전에 따라 다른 용도로 생체정보가 이용될 가능성이 많아지고 이는 생체정보 제공자에게 잠재적인 프라이버시 침해요소로 작용할 가능성이 많다. 또한 넷째, 부당한 공개로, 생체인식 정보를 다른 공공 기관이나 개인적 영역의 조직에 대하여 부당하게 공개하는 것은 개인이 자신의 데이터에 대하여 소유하고 있는 정보에 대한 통제권을 침해하는 것이다. 부당한 공개는 생체인식 데이터가 최초에 의도된 목표가 아닌 다른 용도로 사용될 가능성을 높여 준다. 마지막으로 다섯 번째, 개인참가의 배제로, 생체인식 시스템 당담자의 책임과 권한이 명확해야 하며, 생체정보를 제공한 사람은 당초의 의도에 맞게 생체인식 시스템이 동작하고 있는지 이를 알 수 있도록 해야 하며 본인의 생체정보가 어디에 어떻게 사용되고 있는지에 대한 문의 사항이 있다면 이를 질의 하고 합리적인 시간내에 이에 대한 답변을 들을 수 있어야 한다.

위에서 살펴보았듯이 생체인식과 관련된 프라이버시 문제는 생체인식 기법 자체가 개인의 신체적 또는 행위적 프라이버시에 해당되는 생체적 특징 (지문, 얼굴, 홍채, 혈관 패턴 등) 및 행위적 정보(서명, 음성, 걸음걸이 등)에 근거하는 관계로 이를 제공하는 대상자에 대한 개인적 프라이버시 영향을 충분히 고려해야만 한다. 한편으로는, 이러한 생체정보가 수집되고 저장되어진 순간에는 이들이 중요한 개인정보로 인식되어 정보 프라이버시 문제가 중요한 고려 대상이 된다. 기존의 개인신상에 관한 개인정보들은 그 데이터 자체가 가지는 영향만을 가지고 있었다면, 개인의 생체 정보는 추후의 기술 발달과 더불어 최초로 의도하지 않은 방향으로의 적용 가능성이 있는 여러 가지 요소가 있음을 알 수 있다.

2.3 생체인식에서의 프라이버시 영향 평가

생체인식 시스템의 프라이버시 위험 평가는 응용되는 분야의 여러 가지 특성 측면을 고려하여 평가 할 수 있는데, 응용되는 행태에 따른 잠재적인 프라이버시 위협은 다음의 특징들에 의해 정의될 수 있다[5]. 그 주요 내용 들을 살펴보면 다음과 같다. 첫째, 공개

적 대 비공개적(Overt vs. Covert)으로 공개적 생체인식 시스템이 되기 위해서는 생체데이터의 수집에 대상자의 동의가 있었는지의 여부가 주요한 판단 기준이 된다. 극히 일부의 강제적인 법집행 분야에서 비공개적 시스템 구축을 할 수 있으나 이럴 경우 프라이버시 침해적인 생체인식 시스템이 되는 것은 피할 수 없다. 둘째, 선택적 대 강제적(Opt-In vs. Mandatory)으로 생체시스템의 사용여부가 대상자의 자유의사에 따라 선택될 수 있는지 아니면 의무적으로 사용해야만 하는지의 여부에 달려 있다. 가령 생체인식을 통하여 종업원의 근태를 관리한다고 했을 때 이는 강제적 생체인식시스템이 될 수 있다. 통상은 국가기관의 필요에 의해서 강제적으로 행하는 경우가 많으며 이런 경우에는 선택적인 시스템에 비해 직접적으로 프라이버시를 침해 할 수 있는 소지가 많아진다. 셋째, 고정 대 고정되지 않은 기간(Fixed vs. Indefinite Duration)으로 특정 해당 사안에 따라 생체정보가 사용되는 고정기간 사용방식이 이러한 시간제한이 없는 생체인식 시스템에 비하여 프라이버시 침해적인 요소를 상대적으로 적게 가지고 있다고 할 수 있다. 운영기간이 명기되지 않은 경우에는 추후에 다른 용도로 전용하여 사용될 수 있는 가능성이 높아진다고 할 수 있다. 넷째, 개인적 대 데이터베이스 저장(Personal storage vs. Database Storage)으로 생체정보 템플릿이 어디에 저장되는 지의 여부가 중요한 영향을 미친다. 데이터베이스에 저장되어진 경우에 광범위하게 사용될 수 있는 관계로 개인의 PC나 스마트카드 등에 저장되어지는 경우보다 잠재적으로 프라이버시 침해요소가 크다고 할 수 있다.

위와 같은 위험 요소들을 감안하여 IBG에서는 프라이버시 동조적이며 프라이버시 보호적인 운영을 위해 고려해야 할 사항과 운영지침을 제시하고 있다. 이러한 지침은 작은 규모의 물리적 접근 시스템으로부터 국가 단위에 걸친 인식 프로그램에 이르는 생체인식응용 시스템에 두루 적용될 수 있다고 생각 된다. 이러한 지침의 각 항목들은 모든 생체인식 시스템에 모든 지침서 항목들이 준수 되어야 한다는 것을 의미하지는 않는다. 즉, 몇 개의 항목에서 지침서 항목에 어긋난 것이 있다고 해서 그것이 바로 대상 생체인식 시스템을 프라이버시-침해적인 것으로 만드는 것은 아니다. 지침서의 각 항목은 크게 네 개의 영역 즉, (1) 범위와 성능에서는 사용범위 제한, 일반적이며 유일한 식별자의 확립, 생체인식 정보의 저장 제한, 잠재적 시스템 성능에 대한 평가, 원시 생체인식 표본의 저장을 들 수 있다. (2) 데이터 보호에서는 생체인식 정보의 보호, Post-Match 비교의 보호, 시스템 접근에 대한 제한, 생체인식 정보의 차별화, 시스템 종료를 들 수 있다. (3)개인적 데이터에 대한 사용자의 제어에서는 등록해제(Unenroll) 능력, 생체인식-관련 정보에 대한 정정 및 접근, 익명 등록을 들 수 있으며 (4) 공개, 검사, 기록보존, 감시 등의 항목에서는 제삼자에 의한 기록보존, 감사, 그리고 감시, 감사 데이터의 완전 공개, 시스템 목적 공개, 등록 공개, 비교 결과 공개, 생체인식 정보의 사용에 대한 공개, 선택/강제적인 등록에 대한 공개, 시스템 운영과 감시에 대해 책임이 있는 개인과 단체에 대한 공개, 등록, 검증 그리고 식별 과정에 대한 공개, 생체인식 정보 보호와 시스템 보호의 공개 등을 들 수 있다.

Ⅲ. 생체정보와 프라이버시 현황 및 해결

3.1 생체정보와 관련된 프라이버시 현황

생체인식과 관련하여 프라이버시 침해의 문제가 본격적으로 대두 된 것은 미국의 2001슈퍼볼 경기장에서 비롯되었다. 이때 모인, 10만 여명의 관중들을 대상으로 3,000여명의 지명수배자 얼굴리스트와 자동비교하는 시스템에 의하여 19명의 지명 수배자를 검거하는 일이 발생했다.

이에 대하여 미국 내에서는 많은 논의들이 있었다. 미국정부가 공공장소에서 얼굴인식 기술을 이용하는 것에 반대하는 가장 근본적인 취지는 이것이 프라이버시에 대한 미국헌법상의 권리를 위반한다는 것이다. American Civil Liberties(ACLU)에 의해서 제기된 이러한 반대의 핵심적인 취지는 미국정부에 의한 이러한 활동들이 미국의 수정헌법 4조 즉, "영장에 의하지 아니하고 압수수색을 당하지 아니한다. 영장에는 수색장소와 물건 사람들이 명시되어야 한다."라는 조항을 위반 하였다고 주장하고 있다. 그럼에도 불구하고, 모든 법리 해석자들은 근본적으로 공공장소에서의 얼굴인식이 헌법에 논의된 "수색"에 해당되지 않는다는 데 동의한다. 이와 관련된 John Woodard는[6] "현존의 법 체제 하에서, 수퍼볼에서 사용된 얼굴인식은 거의 완전히 합헌적이다. 대법원은 정부의 조치가 개인의 합리적인 프라이버시에 대한 기대를 침해하는 경우에는 이것은 수색에 해당한다고 해석했다. 그러나 법정은 또한 개인의 얼굴의 특징, 음성, 필체 등과 같이 계속해서 공공에게 노출되는 물리적 특징들에 대해서는 합리적인 프라이버시를 기대할 수 없다고 주장했

다. 따라서 비록 정부가 수행하는 조치가 '합리적'이라는 것은 일반적으로 조사대상이 되는 개인이 어느 정도 불법적인 행위에 가담하고 있음을 수정헌법 4조에서 요구하고 있을지라도, 수퍼볼에서 관중의 얼굴을 스캔하는 것은 법적인 수색에 해당되지 않는다."

이러한 논의에 대해서 전문가들은 컴퓨터화 된 얼굴인식 기술의 적용 범위의 확장에 맞추어 개인의 프라이버시 권리에 대한 최고 법정의 전통적 해석이 바뀌어야 한다고 주장한다. 또 다른 단순한 우려는 개인이 비디오 감시가 행해지는 공공장소에 들어가는 경우 개인의 신상이 노출된다는 것이다. 명확한 문제는 사람들이 자신을 그러한 감시에 내맡길지의 여부를 선택할 수 있어야 한다는 것이다.

한편, 국내에서도 생체인식을 둘러싼 여러 가지 논의가 있었다. 정부와 사업자들은 시민단체들이 생체정보의 부정적인 측면만을 부각시킨다고 불만이고, 시민단체들은 정부가 제도적 보안장치 없이 너무 앞서나간다며 프라이버시 침해에 대한 우려의 목소리를 높이고 있다. 얼굴인식과 관련되어 많은 논란은 불러일으킨 것은 방범용 CCTV 의 설치이다. 2004년 8월에 360도 회전가능하며 100m 줌 기능이 있는 CCTV 272대를 갖는 강남구 관제센터 오픈되어 여성모니터링 요원 15명과 경찰 등 22명이 3교대 하면서 24시간 관내 상황을 모니터링하고 있다. 최근에 일어났던 런던 연쇄폭탄 테러범의 검거에서 보듯이 거의 무방비로 노출되어 있는 공공시설에서 발생할 수 있는 여러 위협으로부터 시민의 안전을 위한 지키기 위한 CCTV 등을 이용한 감시 체제는 향후에 더욱더 필요해지리라 생각 된다.

한편, 이러한 시스템의 운영에 대하여 시민단체들은 방범용 CCTV는 촬영범위가 넓고 사람에 초점을 맞추기 때문에 프라이버시 침해요소가 크고 촬영 각도나 녹화 보존 기간 등 근거 법령이 전혀 없는 상태이며 누구든 본인의 동의 없이는 카메라를 들이 대지 말아야 하며, 그것을 특정한 목적으로 사용하지 말아야 한다고 주장하고 있다. 이와 관련하여 국가인권위원회는 2004년 5월 "CCTV 등 무인단속 장치가 국민의 사생활을 침해 할 수 있다"며 국회의장과 행정자치부장관에게 법적기준 마련을 권고하여 놓고 있는 상황이다.

국내에 있어서 지문인식과 관련하게 주된 논의는 주민등록증 제도와 깊이 연관이 되어 있다. 대부분의 국가들은 국민의 신분관계를 확인하기 위하여 신분등록 제도를 두고 있으나, 국가 신분증제도는 부분적으로 채택하고 있다. 우리나라를 비롯하여 동일 싱가포르 스웨덴 스위스 덴마크와 같은 나라들은 국가신분증 제도를 채택하고 있는 반면에, 미국 캐나다 호주 뉴질랜드와 같은 경우에는 사회보장 카드나 사회보험 카드가 사용되고 있을 뿐이다.

우리나라의 경우 만 17세가 되면 일률적으로 발급받게 되어 있는 주민등록증 제도는 1968년 5월 29일 주민 등록법 제 1차 개정 때 도입되었다. 당초의 개정법에는 "18세 이상의 주민에 대하여 주민등록증을 발급할 수 있다"고 하여 강제적인 발급을 규정하고 있지 않으나, 1970년 1월 1일 제 2차 개정 때, 치안상 필요한 경우에 한하여 주민등록증을 제시하도록 함으로써 간첩이나 불순분자를 용이하게 식별 색출하여 반공태세를 강화하기 위하여 모든 주민 등록 자에 대하여 주민 등록증을 발급하도록 법적 의무를 부여하였다. 이때 주민등록법 제 17조 8항의 주민등록증 발급규정에 의해서, 대상자의 인적 사항과 함께 열 손가락의 지문을 채취 하도록 하고 있다.

이에 대하여 그간 시민단체에서는 현행 열손가락 지문날인 제도는 국회가 제정한 법률에 근거하지 않고 오직 대통령령에만 근거하여 이뤄질 수 있다며 오직 법적 근거 없이 시행령의 별지 서식에만 의해 기본권이 제한되고 있는 것이 법률 유보 원칙에 반한다고 밝히고 있다. 이에 2004년 3월, 만 17세의 청소년 3명이 지문날인제도에 대한 헌법소원을 낸 바 있다. 지난 99년 주민등록증 발급 과정시 날인한 지문을 경찰이 당사자 동의 없이 수사정보로 활용한 것에 대해 헌법소원이 제기된 적이 있으나, 지문날인 제도 자체에 대해 헌법소원이 제기된 것은 이번이 처음이다. 이에 대해 헌법재판소는 2005년 5월 결정문에서 지문날인제도가 17세 이상 모든 국민의 지문정보를 구체적 사건과 관련 없이 범죄수사목적 등에 이용하는 것이 개인정보에 대한 과도한 수집이라는 의문이 있을 수 있으나, 범죄자 등 특정인의 지문정보만 보관해서는 17세 이상 모든 국민의 지문정보를 보관하는 경우와 같은 수준의 신원확인기능을 도저히 수행할 수 없다며 합헌결정을 내린바있다.

한편 국외적으로는 지문을 사용한 생체인식과 관련하여 논란이 되고 있는 것이 US-VISIT(United States Visitors and Immigration Status Indicator) 프로그램과 생체여권의 도입이다. US-VISIT 프로그램은 미국의 9.11 테러이후에 자국의 보호를 위하여 2004년 1월 5일부터 미국내 115개 공항과 14개 항만을 통해 입국하는 비자 비면제국가 외국인

을 상대로 출입국 기기를 통하여 지문채취 및 사진 촬영을 의무화하고 있다. 이에 국내에서는 미국이 자국을 방문하는 외국인들의 지문을 취득하여 인식하는 US-VISIT 시스템을 가동한 것에 대해 한국 등 대다수 외국인 입국자들에게 지문 채취와 사진 촬영을 요구하고 있는 미국의 조처가 테러 예방에 실효를 거둘지 의문스럽고, 프라이버시를 침해할 우려가 있다고 지적하고 있다. 또한 미국 내 미국시민민권연맹(ACLU)과 같은 시민단체도 정부가 이번 조치로 수집한 자료를 범죄자 추적등 특정 목적 외에 활용할 수 있다며 프라이버시 침해를 우려하고 있다.

한편, 생체여권의 도입에 대하여 국내에서는 생체인식포럼이 주관이 되어 인천공항 이용자 500명을 포함하여 전국의 일반시민 1,500여명을 대상으로 의식조사를 한 바가 있다[7]. 이에 따르면 출입국 심사와 관련한 불편함을 감소시키고 여권의 위조 변조 방지와 테러방지 및 국가 안보를 위해 생체여권을 사용할 의향이 있느냐는 물음에 83.8%가 의향이 있다고 응답하고 있다. 사용 의향과 무관하게 국가적으로 생체여권이 도입될 경우, 개인 생체정보를 제공할 의향을 묻는 질문에는 응답자 가운데 71.4%가 의향이 있는 것으로 나타났다.

생체여권이나 US-VISIT의 프로그램에서 개인의 생체정보, 특히 지문 정보를 이용하는 것에 대해서 국내외의 많은 시민단체에서 개인의 프라이버시와 관련하여 문제를 제기하고 있다. 특히, 여권의 발급이나 입국 시에 채취된 생체정보가 어떠한 분야에 어느 정도의 기한까지만 사용되는지에 대한 명확한 규정이 필요한 상황이라고 할 수 있다. 그러나 한편으로는 잦은 국외 여행을 하게 되는 출입국자에게는 생체여권 등의 도입을 통하여 신속한 출입국 처리를 기대하는 측면도 무시 할 수 없는 부분이다.

3.2 생체정보 보호를 위한 정책동향

생체정보 이용의 활성화를 위해서 정책적인 관점으로 봐서 가장 시급한 것인 법적 제도적 장치의 보완이다. 앞의 CCTV의 설치나 지문날인에 있어서 시민단체에서의 주요 주장은 생체정보를 이용하는 법적 근거를 확실히 해 달라는데 있다. 개인 정보보호에 관하여 국제적으로나 국내에서 많은 공감대를 형성하고 있는 것이 OECD의 가이드라인이다.[8] 모두 8개의 원칙으로 이루어진 가이드라인은 세계 각국의 개인정보보호에 관한 법률제정에 영향을 주어 왔으며, 우리나라의 경우에도 국회에서 제정을 추진 중인 개인정보보호에 관한 기본법의 골격을 이루고 있기도 하다.

그러나 생체정보의 경우 개인 정보 영역에 속한다고 할 수 있으나, 앞의 2장에서 언급된 바와 같이 개인의 다양한 신체정보와 유일식별자로의 사용 가능성 등으로 인하여 별도의 제도적 장치의 필요성이 대두되어 왔다. 이에 서혜석 국회의원이 주관이 되어 정통부와 정보보호진흥원이 마련한 생체정보보호 가이드라인에 대해 공청회를 가진 바 있다.[9] 모두 3장 13조로 구성된 가이드라인은 신원 확인을 위해 생체정보를 수집하거나, 이용하는데 있어서 준수해야할 생체정보보호에 과한 중요 사항을 정함으로서 생체정보의 안전한 이용환경을 조성하고, 개인의 이익을 보호하는 것을 목적으로 하고 있다. 향후에 몇 번의 공청회를 거치면서 여러 그룹의 의사가 반영되어 다듬어 진다면 생체정보 이용의 활성화를 위한 좋은 초석이 되리라 생각된다.

Ⅳ. 결 론

오늘날 우리는 급속도로 발전하는 정보사회에 살고 있다. 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. 이러한 추세에 맞추어서 국내외의 정보보안 시장은 날로 커지고 있으며, 개인 인증을 위한 확실한 수단으로서의 생체인식 기법의 채택도 날로 증가 하고 있다. 따라서 이와 동반하여 프라이버시에 관한 논의는 더욱더 커질 것으로 예상되어 이에 대한 깊이 있는 이해가 필요하다. 사회의 안전성과 건전성을 향상시키기 위해서는 다소간의 개인적 프라이버시가 양보 되어야 한다는 시각과, 인권의 개념으로 프라이버시 문제를 바라볼 경우에는 서로가 상충 되는 점이 있다.

우리나라 헌법 17조는 "모든 국민은 사생활의 비밀과 자유를 침해 받지 아니한다"라고 명시함으로서 개인의 프라이버시를 존중하고 있다. 반면에 헌법 37조 2항에는 "국민의 모든 자유와 권리는 국가안전보장 질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한 할 수 있으며, 제한하는 경우에도 자유와 권리의 본질적인 내용을 침해 할 수 없다"라고 명시하고 있다. 이러한 헌법의 정신을 따르자면, 사회의 안전과 공공복리를 위해 생체인식 시스템의 적용 및

확대는 가능하나, 이때에도 최대한 개인의 권리를 존중하되 엄격히 이의 침해를 막는 법률적, 기술적 장치가 필요하다고 할 수 있다.

참 고 문 헌

[1] 전명근, 생체인식(Biometric) 총론, 한국정보통신교육원, 2002.

[2] www.ibia.org

[3] Roger Clarke, Biometrics and Privacy, http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html, 2001

[4] S. Prabhakar, S. Pankanti, A. Jain, Biometric Recognition: Security and Privacy Concerns, IEEE Security & Privacy

[5] International Biometric Group, Biometrics and Privacy, 2004

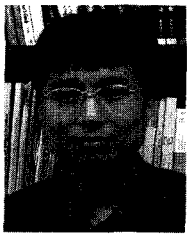
[6] J. D. Woodward, "Super bowl surveillance: Facing up to biometrics," www.rand.org/publicatoins/IP/IP209

[7] 생체인식포럼, 생체인식 여권도입사업에 대한 시민의식 조사 보고서, 2003.

[8] A. Marcella, Privacy Handbook, John Wiley & Sons, 2003.

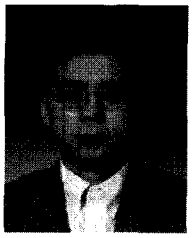
[9] 생체정보보호 가이드라인 제정을 위한 공청회 자료, 2005년 7월 11일.

〈著 者 紹 介〉



전 명 근 (Myung Geun Chun)

1987년 : 부산대학교 전자공학과(학사)
1989년 : 한국과학기술원 전기 및 전자공학과(공학석사)
1993년 : 한국과학기술원 전기 및 전자공학 과(공학박사)
1993년~1996년 : 삼성전자 자동화연구소 선임연구원
2000년~2001년 : University of Alberta 방문교수
1996년~현재 : 충북대학교 전기전자 컴퓨터공학부 교수
〈관심분야〉 Biometrics, 감정인식, 지능시스템



문 기 영 (Ki-young Moon)

1986년 : 경북대학교 전자공학과 학사
1989년 : 경북대학교 대학원 전자공학과 석사
1992년~1994년: (주)대우정보시스템 기술연구소 전임연구원
1994년 3월~현재: 한국전자통신연구원 정보보호연구단 생체인식기술연구팀 팀장
〈관심분야〉 생체인식, 웹서비스 보안, 분산 시스템